NetScaler 13.1

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

Notes de mise à jour de NetScaler

June 20, 2023

Les notes de mise à jour décrivent comment le logiciel a changé dans une version particulière et les problèmes connus pour exister dans cette version.

Le document des notes de version comprend tout ou partie des sections suivantes :

- **Nouveautés** : les améliorations et autres modifications publiées dans la version.
- **Problèmes résolus** : Problèmes résolus dans la version.
- **Problèmes connus** : problèmes qui existent dans la version.
- **Points à noter** : Les aspects importants à garder à l'esprit lors de l'utilisation de la version.
- **Limitations** : les limitations qui existent dans la version.

> **Remarque**
>
> - Les étiquettes [# XXXXXX] figurant dans les descriptions des problèmes sont des identifiants de suivi internes utilisés par l'équipe NetScaler.
> - Ces notes de publication ne documentent pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

Notes de mise à jour pour NetScaler 13.1 à 49.13 Build

July 31, 2023

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent dans la version 13.1 à 49.13 de NetScaler.

Remarques

- Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.
- Les versions 13.1 à 49.13 et ultérieures corrigent les vulnérabilités de sécurité décrites dans CTX561482.

Nouveautés

Les améliorations et modifications disponibles dans les versions 13.1 à 49.13.

Réseau

- **La propagation des commandes est désactivée pendant la synchronisation HA. Pour les configurations à**
  haute disponibilité, la propagation des commandes est désactivée pendant la synchronisation HA afin d'éviter les échecs de propagation des commandes lors de la synchronisation HA.

  [NSHELP-34253]

Plateforme

- **Prise en charge de l'affichage des informations de version du logiciel NetScaler à l'aide de balises d'instance AWS**

  Les informations de version de NetScaler VPX sont désormais ajoutées au champ de balise d'instance AWS. Grâce à cette modification, vous pouvez désormais connaître la version du logiciel sans vous connecter à l'instance NetScaler. Pour ajouter ces informations lors du démarrage de l'instance NetScaler, le rôle IAM par défaut nécessite l'autorisation « ec2:CreateTags ».

  [NSPLAT-25066]

Problèmes résolus

Les problèmes résolus dans les versions 13.1 à 49.13.

Authentification, autorisation et audit

- Un NetScaler configuré avec une stratégie d'authentification OAuth peut se bloquer lorsqu'un certificat de courbe elliptique est lié au VPN de manière globale.

  [NSHELP-34795]

- Une erreur HTTP 404 s'affiche lorsqu'un utilisateur tente de s'authentifier auprès d'un NetScaler configuré par GSLB après l'expiration de la session.

  [NSHELP-34336]

Gestion des bots

- Les attaques de rediffusion de sessions par empreinte digitale d'un robot sont abandonnées lorsque l'action d'empreinte digitale de l'appareil est définie sur LOG, RESET ou REDIRECT.

  [NSBOT-1117]

CallHome

- Call Home envoie des données de télémétrie au serveur de support technique NetScaler même si la fonctionnalité est désactivée.

  [NSHELP-33240]

Équilibrage de charge

- Le NetScaler secondaire peut se bloquer lorsque les conditions suivantes sont remplies :
  - Dans une configuration à haute disponibilité, un grand nombre de serveurs d'équilibrage de charge sont configurés avec des groupes d'équilibrage de charge.
  - Pendant que la synchronisation est en cours, l'opération définie est exécutée sur l'un des serveurs d'équilibrage de charge du groupe d'équilibrage de charge.

  [NSHELP-34225]

Divers

- Lorsqu'un profil réseau est configuré dans un domaine de trafic autre que celui par défaut et utilisé dans la configuration AppFlow, les ports système sont épuisés et le trafic est affecté.

  [NSHELP-34544]

NetScaler Gateway

- La page d'accueil de NetScaler Gateway peut ne pas énumérer les applications lorsque vous essayez d'y accéder en mode VPN sans client à l'aide d'un navigateur mobile.

  [NSHELP-35541, NSCXLCM-1132, NSCXLCM-1212, NSCXLCM-1248]

Web App Firewall NetScaler

- La base de données de réputation IP peut ne pas être mise à jour par Webroot si vous utilisez la licence perpétuelle sur NetScaler.

  [NSHELP-33965]

Réseau

- Dans une configuration à haute disponibilité, le nœud secondaire se bloque lorsqu'un itinéraire est supprimé du nœud dans le cadre de la synchronisation HA pendant que vous le modifiez.

  [NSHELP-34927]

- Dans une configuration à haute disponibilité, le nœud show ha peut afficher une sortie incorrecte lorsque les deux conditions suivantes sont remplies :
  - Les pulsations cardiaques HA ne sont échangées que via une seule interface ou un seul canal.
  - L'interface ou le canal est désactivé.

  [NSHELP-34193]

Plateforme

- Lorsque vous créez un profil cloud pour ajouter le service AWS Autoscaling à une instance NetScaler VPX, il peut échouer si les stratégies de contrôle des services sont configurées globalement.

  [NHELP-35562]

- Dans une configuration de paire HA sur la plate-forme AWS, les interfaces NetScaler VPX ne migraient pas correctement lors d'un basculement pour la configuration suivante :
  - Le déploiement HA se trouve dans la même zone.
  - Plusieurs interfaces utilisent le même sous-réseau.

  [NSHELP-35369]

- Après une mise à niveau du microprogramme, l'interface de gestion d'une appliance NetScaler MPX 5900/8900 peut tomber en panne. Par conséquent, l'appliance est inaccessible.

  [NSHELP-31587]

Interface utilisateur

- Les sessions utilisateur sont mal calculées si le même utilisateur est lié à deux partitions différentes. Les deux partitions peuvent être par défaut, non définies par défaut, ou les deux.

  [NSHELP-34971]

- Lorsque vous modifiez une expression de stratégie d'autorisation dans l'interface utilisateur de NetScaler Gateway, l'option **AAA** n'apparaît pas dans la liste déroulante « Expression Editor ».

  [NSHELP-33509]

- Lorsqu'un utilisateur consulte la liaison dans une stratégie de commutation de contenu, les détails du serveur virtuel de commutation de contenu ne s'affichent pas sur la même ligne sous **Afficher les liaisons**.

  [NSHELP-33149]

Problèmes connus

Les problèmes qui existent dans les versions 13.1 à 49.13.

Authentification, autorisation et audit

- L'appliance NetScaler peut se bloquer lorsque le serveur virtuel d'authentification est utilisé dans une partition autre que celle par défaut.

  [NSHELP-32054, NSCXLCM-640]

- Après une mise à niveau de Citrix SSO pour iOS, les notifications push que vous recevez à des fins d'authentification peuvent ne pas être accompagnées d'un son.

  [NHELP-27525]

- Les administrateurs ne peuvent pas effectuer de journalisation personnalisée des échecs d'authentification dus à des informations d'identification non valides. Ce problème se produit car les stratégies du répondeur NetScaler ne détectent pas les erreurs liées aux échecs de connexion.

  [NSAUTH-11151]

- Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante. `show adfsproxyprofile <profile name>`

  Solution : Connectez-vous au principal NetScaler actif du cluster et exécutez la commande. `show adfsproxyprofile <profile name>` Il afficherait l'état du profil proxy.

  [NSAUTH-5916]

- La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

  - L'option Tester l'accessibilité LDAP est ouverte.
  - Les informations d'identification de connexion non valides sont renseignées et envoyées.
  - Les identifiants de connexion valides sont renseignés et envoyés.

  Solution : fermez et ouvrez l'option Tester l'accessibilité LDAP.

  [NSAUTH-2147]

Gestion des bots

- L'appliance NetScaler peut se bloquer si la stratégie BOT utilise une action de journal avec des règles de stratégie complexes.

  [NSHELP-34999]

Équilibrage de charge

- Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

  [NSLB-7679]

- Le NetScaler peut se bloquer lorsque vous faites référence à un service basé sur un nom de domaine (DBS) une fois que la séquence de conditions suivante est remplie :

  1. Une entrée de localisation est configurée pour l'adresse IP à laquelle le nom de domaine DBS est résolu.
  2. Le nom de domaine DBS est supprimé, ce qui entraîne une réponse NXDOMAIN de la part du serveur de noms.
  3. L'entrée de localisation est supprimée.

  [NSHELP-35370]

- Dans de rares cas, une appliance NetScaler peut se bloquer et générer un core dump lorsque les conditions suivantes sont remplies :

  - La sonde de surveillance DNS basée sur TCP est utilisée pour surveiller un service principal.
  - La mémoire de l'appliance est insuffisante.

  [NSHELP-35289]

- Une utilisation élevée du processeur peut être observée si la proximité statique est configurée comme méthode GSLB et si la recherche de l'emplacement du client à partir de la base de données échoue.

  [NSHELP-33823]

- Dans les informations de contact SOA, lorsque vous entrez une adresse e-mail contenant plus d'un point (par exemple, `john.doe.example.com`), cela se traduit par [!`john@doe.example.com`[](`https://issues.citrite.net/images/icons/mail_small.png`)](`mailto:john@doe.example.com`). Vous pouvez désormais utiliser une barre oblique inverse () comme personnage d'évasion. Par conséquent, `john.doe.example.com` se traduit par [`john.doe@example.com` (`mailto:john@doe.example.com`).

  [NHELP-33610]

- Le NetScaler peut se bloquer en raison d'un problème de synchronisation entre la récupération des enregistrements limitant le débit et le processus de vieillissement des enregistrements.

  [NSHELP-33349]

- Le format serviceGroupName dans l'interruption `entityofs` pour le groupe de services est le suivant :
  `<service(group)name>?<ip/DBS>?<port>`

Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (« ? ») est utilisé comme séparateur. NetScaler envoie l'interruption avec le point d'interrogation (« ? »). Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Divers

- Lorsqu'une synchronisation forcée a lieu dans une configuration de haute disponibilité, l'appliance exécute la commande « set urlfiltering parameter » sur le nœud secondaire.
  Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre « TimeOfDaytoUpdateDB ».

  [NSSWG-849]

- NetScaler Gateway signale à NetScaler ADM les demandes d'accès autorisé en cas d'échec de l'authentification unique. Par conséquent, la page Gateway > Gateway Insight de l'interface utilisateur de NetScaler ADM affiche des rapports d'échec SSO incorrects provoquant de fausses alarmes.

  [NHELP-27992]

- Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

  [NSHELP-22409]

- Dans un déploiement de cluster, si vous exécutez la commande « forcer la synchronisation du cluster » sur un nœud non CCO, le fichier ns.log contient des entrées de journal dupliquées.

  [NSANINFRA-2850, NSGI-1293]

- Lorsque vous installez NetScaler ADM sur un cluster Kubernetes, cela ne fonctionne pas comme prévu car les processus requis peuvent ne pas s'exécuter.

  Solution : redémarrez le module Gestion.

  [NSAN INFRA-1504]

- Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

  [GOPHDX-1055]

- Dans une configuration à haute disponibilité, lors d'un basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

  [GOPHDX-1050]

NetScaler Gateway

- Parfois, un NetScaler sur lequel VPN et AppFlow sont configurés peut se bloquer, entraînant un basculement HA.

  [NSHELP-35734, NSCXLCM-1247]

- Après une mise à niveau, il peut arriver que l'interface graphique de NetScaler ne soit pas accessible via HTTP si vous êtes connecté à un VPN via NetScaler Gateway.

  [NSHELP-35015]

- Lorsque l'accès VPN sans client avancé est configuré sur NetScaler Gateway, les pages peuvent ne pas être chargées à partir des URL enregistrées dans les favoris.

  [NSHELP-33771]

- Parfois, lorsque vous parcourez les schémas, le message d'erreur « Impossible de lire le type de propriété non défini » apparaît.

  [NSHELP-21897]

- L'option du système d'exploitation Windows ne figure pas dans la liste déroulante Expression Editor pour les stratégies de pré-authentification et les actions d'authentification sur l'interface graphique de NetScaler. Toutefois, si vous avez déjà configuré l'analyse du système d'exploitation Windows sur une version précédente de NetScaler à l'aide de l'interface graphique ou de l'interface de ligne de commande, la mise à niveau n'a aucune incidence sur les fonctionnalités. Vous pouvez utiliser l'interface de ligne de commande pour apporter des modifications, si nécessaire.

  Solution :

  Utilisez les commandes CLI pour la configuration.

  - Pour configurer une action EPA avancée dans l'authentification nFactor, utilisez la commande suivante.

    ```
    add authentication epaAction adv_win_scan -csecexpr "sys.client_expr
    ("sys_0_WIN-OS_NAME_anyof_WIN-10[COMMENT: Windows OS]")"
    ```

  - Pour configurer une action de pré-authentification classique, utilisez les commandes suivantes.

    ```
    add aaa preauthenticationaction win_scan_action ALLOW
    add aaa preauthenticationpolicy win_scan_policy "CLIENT.SYSTEM('WIN
    -OS_NAME_anyof_WIN-10[COMMENT: Windows OS]')EXISTS"win_scan_action
    ```

  [CGOP-22966]

- Pour utiliser la fonctionnalité Always On VPN avant de se connecter à Windows, il est recommandé de mettre à niveau votre NetScaler Gateway vers la version 13.0 ou ultérieure. Cela vous

permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

[CGOP-19355]

- Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une stratégie de session depuis l'interface graphique de NetScaler.

  [CGOP-11830]

- Dans Outlook Web App (OWA) 2013, cliquez sur **Options** dans le menu Paramètres pour afficher une boîte de dialogue **d'erreur critique** . De plus, la page ne répond plus.

  [CGOP-7269]

Appliance NetScaler SDX

- Des pertes de paquets sont visibles sur une instance VPX hébergée sur une appliance NetScaler SDX si les conditions suivantes sont remplies :
  - Le mode d'allocation du débit est en rafale.
  - Il existe une grande différence entre le débit et la capacité maximale de rafale.

[NSHELP-21992]

Web App Firewall NetScaler

- Vous ne pouvez pas modifier ou supprimer les règles de relaxation des scripts intersites JSON à l'aide de l'interface graphique NetScaler si les règles sont configurées avec une paire clé-valeur.

  [NHELP-35610]

Réseau

- Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

  [NSNET-25299]

- Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :
  - L'appliance NetScaler BLX est dotée d'un faible nombre de « pages volumineuses ». Par exemple, 1G.
  - L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

Le problème est enregistré sous forme de message d'erreur dans « /var/log/ns.log » :

- « BLX-DPDK:DPDK Mempool n'a pas pu être initialisé pour PE-x »

Remarque : x est un nombre <= nombre de processus de travail.

Solution : allouez un grand nombre de « pages volumineuses », puis redémarrez l'appliance.

[NSNET-25173]

- Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

  [NSNET-24449]

- Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

  - Désactiver
  - Activer
  - Réinitialiser

  [NSNET-16559]

- L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

  « Les paquets suivants ont des dépendances non satisfaites : blx-core-libs:i386 : PreDepends : libc6:i386 (>= 2.19) mais ils ne sont pas installables »

  Solution : exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

  - dpkg –add-architecture i386
  - apt-get update
  - apt-get install libc6:i386

  [NSNET-14602]

- Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

  [NSNET-5233]

- L'appliance NetScaler n'enregistre pas les messages d'erreur d'authentification SNMPv3 dans le fichier journal NetScaler (» /var/log/ns.log «).

  [NSHELP-33909]

- Lorsque la limite de mémoire d'une partition d'administration est modifiée dans un dispositif NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

  [NSHELP-21082]

Plateforme

- Certains packages python ne sont pas installés lorsque vous rétrogradez l'appliance NetScaler de la version 13.1-4.x et des versions supérieures vers l'une des versions suivantes :
  - Toute version 11.1
  - 12.1-62.21 et versions antérieures
  - 13.0-81.x et versions antérieures

  [NSPLAT-21691]

- Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande « rm cloudprofile » pour supprimer le profil.

  [NSPLAT-4520]

- Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran du premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
  Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

  [NSPLAT-4451]

- Si le NetScaler SDX secondaire d'une configuration HA est configuré avec un cœur de processeur partagé et que les pulsations HA sont échangées via un VLAN, il tente sans succès de passer au nœud principal.

  [NSHELP-32412, NSCXLCM-789]

Stratégies

- Les connexions peuvent être bloquées si la taille du traitement des données est supérieure à la taille de la mémoire tampon TCP par défaut configurée.

  Solution : définissez la taille de la mémoire tampon TCP sur la taille maximale des données qui doivent être traitées.

  [NSPOLICY-1267]

SSL

- Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

  Solution :

  1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
  2. Enregistrez la configuration.

  [NSSSL-9572]

- Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

  [NSSSL-6478]

- Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

  [NSSSL-6213]

- Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
  ERROR: crl refresh disabled

  [NSSSL-6106]

- L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

  [NSSSL-4427]

- Un message d'avertissement incorrect, « Avertissement : aucun chiffrement utilisable configuré sur le serveur/service SSL » s'affiche si vous essayez de modifier le protocole ou le chiffrement SSL dans le profil SSL.

  [NSSSL-4001]

- Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

  [NSSSL-3184, NSSSL-1379, NSSSL-1394]

- Le trafic DTLS sur NetScaler peut entraîner une accumulation importante de mémoire, car la mémoire n'est pas correctement libérée lors de la gestion d'un vol de liaison retransmis par un client.

  [NHELP-35359]

Système

- Lorsque NetScaler reçoit une requête HTTP CONNECT sur une connexion TCP client, il ne réutilise pas la connexion TCP précédente au serveur sur laquelle une réponse HTTP « Authentification proxy 407 requise » est déjà envoyée. NetScaler transmet plutôt la requête HTTP CONNECT via une nouvelle connexion TCP au serveur principal. Le transfert de la demande sur une nouvelle connexion TCP rompt les protocoles d'authentification par proxy tels que NTLM, qui nécessitent l'échange de plusieurs messages d'authentification HTTP sur la même connexion TCP.

  Solution :

  1. Ajoutez un profil HTTP personnalisé qui marque les requêtes HTTP entrantes à l'aide de la méthode CONNECT comme NON VALIDES et garantit également que les requêtes HTTP marquées comme INVALID ne sont PAS supprimées.

```
add ns httpprofile fw-proxy-http-prof -markConnReqInval ENABLED -
dropInvalReqs DISABLED
```

  1. Liez ce profil HTTP personnalisé au serveur virtuel d'équilibrage de charge qui est utilisé pour équilibrer la charge du pool de serveurs proxy directs.

```
set lb vs fw-proxy-vs -httpprofileName fw-proxy-http-prof
```

  Remarque : Les stratégies relatives aux fonctionnalités de NetScaler n'évaluent pas les requêtes HTTP ni les réponses marquées comme NON VALIDES.

  [NSHELP-35717, NSCXLCM-1514]

- L'appliance NetScaler configurée avec un service SSL se bloque lorsqu'elle reçoit un paquet de contrôle TCP FIN suivi d'un paquet de contrôle TCP RESET.

  [NSHELP-31656]

- Un RTT élevé est observé pour une connexion TCP si la condition suivante est remplie :

  - une fenêtre de congestion maximale élevée (> 4 Mo) est définie
  - L'algorithme TCP NILE est activé

  Pour qu'une appliance NetScaler utilise l'algorithme NILE pour le contrôle de la congestion, les conditions doivent dépasser le seuil de démarrage lent, qui est associé à la fenêtre de congestion maximale

  Ainsi, jusqu'à ce que la fenêtre de congestion maximale configurée soit atteinte, NetScaler continue d'accepter des données et se retrouve avec un RTT élevé.

  [NSHELP-31548]

- Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

[NSBASE-18295]

- Dans de rares cas, les flux créés avant la création du flux WebSocket HTTP/2 peuvent être interrompus lorsque la connexion côté serveur du WebSocket se ferme.

  Ce problème se produit car l'appliance NetScaler ne prend pas en charge le multiplexage des connexions pour HTTP/2 WebSocket.

  Solution : désactivez le multiplexage des connexions pour le profil HTTP2 associé à l'aide de la commande suivante :

```
“set httpProfile <name> [-conMultiplex (              DISABLED )]”
ENABLED
```

  [NSBASE-17449]

- L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement HDX Insight SkipFlow lorsqu'un type de transport LogStream est configuré pour Insight.

  [NSBASE-8506]

Interface utilisateur

- Dans l'interface graphique de NetScaler, le lien « Aide » présent sous l'onglet « Tableau de bord » est cassé.

  [NSUI-14752]

- L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

  Solution : configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de l'interface de ligne de commande NetScaler.

  [NSUI-13024]

- Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

  [NSUI-6838]

- Lorsque vous configurez une stratégie de répondeur ou une stratégie de réécriture sur l'interface graphique de NetScaler sans ajouter de valeurs dans les champs **Log Action** et **AppFlow Action**, qui ne sont pas obligatoires, l'erreur suivante s'affiche :

  “Nom non valide ; les noms doivent commencer par un caractère alphanumérique ou un trait de soulignement et ne doivent contenir que des caractères alphanumériques, ‘_’, ‘%23’, ‘.’, ‘ ‘, ‘:’, ‘@’, ‘=’ or ‘-‘ [logAction,]”

Solution : ajoutez de la valeur aux champs **Log Action** et **AppFlow Action** lors de la configuration d'une stratégie de répondeur ou d'une stratégie de réécriture.

[NHELP-35726]

- Si le champ **Valeur** de la page **Configurer les actions LB** contient des espaces, l'interface graphique n'affiche aucun message d'erreur. Lorsque vous modifiez le champ **Valeur** contenant des espaces, l'interface graphique remplace l'espace par une virgule, ce qui entraîne une configuration non valide.

  [NSHELP-35532]

- Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

  1. Mettez à niveau l'appliance NetScaler vers l'une des versions
     - 13.0 52.24 build
     - 12.1 57.18 build
     - 11.1 65.10 build
  2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
  3. Rétrogradez l'appliance NetScaler vers une version antérieure.

  Pour afficher la liste de ces utilisateurs du système à l'aide de l'interface de ligne de commande : À l'invite de commandes, tapez :

  ```
  query ns config -changedpassword [-config <full path of the configuration
   file (ns.conf)>]
  ```

  Solution : Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

  - Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
  - Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
  - Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

  Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html.

  [NSCONFIG-3188]

Notes de publication pour la version 13.1—48.47 de NetScaler

July 18, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1—48.47 de NetScaler.

Remarques

- Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Nouveautés

Les améliorations et modifications disponibles dans les versions 13.1—48.47.

Équilibrage de charge

- **Amélioration de la méthode d'équilibrage de charge de proximité statique**

  Actuellement, lorsque vous configurez la méthode d'équilibrage de charge de proximité statique et qu'il existe plusieurs serveurs situés à différents emplacements, un serveur est choisi en fonction de l'adresse IP du client plutôt que de l'adresse IP de bouclage NetScaler. Par conséquent, le temps de réponse peut être plus long dans certains cas. Le paramètre ProximityFromSelf est ajouté aux paramètres d'équilibrage de charge et au profil d'équilibrage de charge pour réduire le temps de réponse, en sélectionnant un serveur plus proche de NetScaler plutôt que du client.
  Pour plus d'informations, consultez la section Proximité statique pour l'emplacement de NetScaler.

  [NSLB-9530]

- **La synchronisation complète du GSLB n'est pas déclenchée lorsque l'état HA change**

  La synchronisation GSLB complète n'est plus déclenchée lorsque l'état HA change soit sur le site GSLB principal, soit sur les sites subordonnés. Auparavant, la synchronisation complète avec les sites subordonnés était déclenchée même lorsque les nœuds HA étaient synchronisés et qu'aucune modification de la configuration GSLB n'avait été apportée pendant la transition d'état HA. En ne lançant pas la synchronisation GSLB complète, les modifications de configuration incrémentielles après le changement d'état HA se synchronisent désormais plus rapidement avec les sites subordonnés.

  [NSLB-9477]

- Le**moniteur Oracle ECV prend en charge les derniers protocoles d'authentification Oracle**
  Le moniteur NetScaler Oracle ECV prend désormais en charge toutes les versions d'Oracle jusqu'à 21c et tous les protocoles d'authentification basés sur un mot de passe.

  Pour plus d'informations, consultez Oracle ECV Monitor.

  [NSHELP-9819]

Web App Firewall NetScaler

- **Amélioration de la fonctionnalité de limite de débit**

  Vous pouvez désormais limiter le type de trafic et ajouter des conditions supplémentaires dans la fonction de limite de débit BOT à l'aide des paramètres de type de limite de débit et de condition de limite de débit. Pour plus d'informations, consultez la section Détection de bots.

  [NSWAF-9535]

Réseau

- **Un fichier de configuration unifié pour les configurations NetScaler, les configurations de routage dynamique et la configuration du module de sécurité matérielle**

  L'appliance NetScaler prend désormais en charge un fichier de configuration unifié (unified.conf) qui contient les configurations NetScaler (ns.conf), les configurations de routage dynamique (zebos.conf) et les configurations du module de sécurité matérielle (HSM) (chrystoki.conf).

  Le fichier de configuration unifié fournit une vue unique des différents types de configurations. Ce fichier de configuration unifié est uniquement destiné à la visualisation et ne peut pas être utilisé pour appliquer des configurations dans un autre dispositif NetScaler.

  Le chemin complet du fichier de configuration unifiée dans l'appliance NetScaler est le suivant : « /nsconfig/unified.conf ». Vous pouvez accéder au fichier de configuration unifié à l'aide de l'invite de commande du shell. Le fichier de configuration unifié est uniquement pris en charge pour les appliances NetScaler autonomes et les configurations à haute disponibilité.

  [NSNET-27559]

- **Ports réseau VMware VMXNET3 en tant que ports DPDK : prise en charge des appliances NetScaler BLX**

  Une appliance NetScaler BLX intégrée à une machine virtuelle hôte Linux exécutée sur une plateforme de virtualisation VMware prend désormais en charge les ports réseau VMXNET3 en tant que ports DPDK.

  [NSNET-27244]

Plateforme

- **Support pour le mode IMDSv2 de l'instance AWS EC2**

  Le mode Instance Metadata Service Version 2 (IMDSv2) pour l'instance AWS EC2 est désormais pris en charge dans l'appliance NetScaler. IMDSv1 et IMDSv2 sont deux modes disponibles pour accéder aux métadonnées d'instance à partir d'une instance AWS EC2 en cours d'exécution. IMDSv2 est plus sécurisé que IMDSv1. Auparavant, l'IMDSv2 n'était pas pris en charge par NetScaler. Ainsi, lorsque l'instance AWS EC2 utilisait le mode IMDSv2, l'appliance NetScaler remplaçait la route statique par défaut après un redémarrage à froid.

  [NSPLAT-21205]

Système

- Prise en**charge de la stratégie de réponse pour le protocole proxy sur un serveur virtuel de type TCPRN**
  NetScaler prend désormais en charge la stratégie de réponse pour le protocole proxy sur un serveur virtuel de type TCP.rn

  Auparavant, la stratégie de répondeur pour le protocole proxy n'était prise en charge que sur un serveur virtuel de type HTTP.rn

  Pour plus d'informations, consultez la section Proxy Protocol.

  [NSHELP-33193]

Interface utilisateur

- **Balises HTML dans les expressions de stratégie de l'interface graphique NetScaler**

  Les balises HTML sont désormais prises en charge dans l'interface graphique de NetScaler lors de la création d'expressions de stratégie.

  [NSUI-18918]

- **Catégorie de filtre CVE dans la page d'affichage des critères de filtre de signature**

  Le CVE est ajouté en tant que catégorie dans la liste des **critères de filtre d'affichage** de la page d' **affichage des signatures** . Utilisez CVE comme option de filtre pour afficher uniquement les détails liés au journal dans la fenêtre **Résultats filtrés** sur la droite.

  [NSUI-18512, NSCXLCM-616]

Problèmes résolus

Les problèmes qui sont résolus dans les versions 13.1—48.47.

Authentification, autorisation et audit

- Dans un déploiement NetScaler en cluster, vous ne pouvez pas lier une action d'attribution à une stratégie d'authentification.

  [NSHELP-33974]

- **Lorsque NetScaler est configuré en tant que fournisseur de services SAML, la validation de l'assertion SAML peut échouer en raison d'un problème d'analyse de la balise SAML:StatusCode.**

  [NSHELP-33574]

- Lorsque vous modifiez un profil de session sur la page Sécurité > AAA - Trafic des applications > Stratégies > Stratégies et profils de session > Profils de session, l'option « Authentification unique aux applications Web » est activée même si elle était définie sur OFF lors de la création du profil de session.

  [NSHELP-33067]

- Le chiffrement ou le déchiffrement du secret OTP peut échouer avec des attributs à valeurs multiples.

  [NSHELP-31057]

Équilibrage de charge

- Lorsqu'un NetScaler configuré en tant que serveur ADNS reçoit une requête via le protocole UDP ou TCP, il envoie la réponse en fonction de la configuration. Toutefois, si plusieurs requêtes sont envoyées via la même session TCP ou UDP, seule la réponse à la première requête est correctement envoyée. La stratégie DNS active UNDEF pour les requêtes suivantes sur la même connexion.

  [NSLB-10103]

- NetScaler peut se bloquer lorsque la séquence de conditions suivante est remplie :

  1. Les services GSLB sont liés aux serveurs virtuels GSLB par ordre de priorité.
  2. La méthode d'équilibrage de charge du serveur virtuel GSLB est identique à la méthode d'équilibrage de charge de sauvegarde.
  3. Tous les services GSLB sont indépendants du serveur virtuel GSLB.
  4. Le serveur virtuel GSLB est supprimé.

  [NSHELP-34694]

- Les pertes de paquets sont observées dans NetScaler en raison d'un retard dans la collecte des statistiques. Le retard est dû au fait que plusieurs groupes de services sont liés à la même adresse IP de service sur différents ports.

[NSHELP-34171, NSCXLCM-319]

- La commande « Afficher le nom du serveur » affiche l'état du service comme étant inconnu même si le service est lié au serveur.

  [NSHELP-33668]

- NetScaler peut se bloquer et vider le noyau si un grand nombre de groupes de services GSLB autoscale sont configurés.

  [NSHELP-33545]

- L'appliance NetScaler déclenche une alerte SNMP incorrecte en cas de connexion serveur élevée en raison d'un calcul erroné du nombre de serveurs.

  [NSHELP-31582]

NetScaler Gateway

- Un NetScaler avec un proxy ICA activé sur NetScaler Gateway peut se bloquer lors d'un déploiement DMZ à double saut.

  [NSHELP-33369]

- Dans un déploiement NetScaler en cluster, lorsque le paramètre ICA Only est défini sur ON, NetScaler Gateway ne parvient pas par intermittence à déconnecter les sessions utilisateur, même lorsque le paramètre de temporisation forcée est activé.

  [NSHELP-33014]

- Les signets RDP ajoutés pour des utilisateurs spécifiques sont affichés pour les autres utilisateurs qui n'ont pas ajouté ces URL à leurs favoris.

  [NSHELP-29904]

- Lors de l'effacement des configurations à l'aide de l'interface graphique ou de la CLI, une appliance NetScaler peut se bloquer lorsque les entités liées à la Secure Token Authority (STA) sont effacées.

  [CGOP-23152]

Appliance NetScaler SDX

- Dans de rares cas, un NetScaler SDX peut se bloquer et ne pas être accessible en raison de valeurs indésirables dans certains champs, tels que l'adresse IP.

  [NSHELP-34925]

Web App Firewall NetScaler

- L'appliance NetScaler peut se bloquer en raison d'informations d'en-tête HTTP non valides. Ce problème se produit lorsque les conditions suivantes sont remplies :
  - Une violation SQL/XSS se produit dans le corps de la requête HTTP.
  - La journalisation détaillée est définie sur « PatternPayloadHeader ».

  [NSHELP-35297]
- NetScaler signale un nombre de compteurs de requêtes du Web Application Firewall supérieur au nombre total de compteurs de demandes, car le compteur de demandes est incrémenté deux fois pour les requêtes XML.

  [NSHELP-34591]
- Dans de rares cas, NetScaler peut consommer davantage de mémoire lorsque la limite du corps des publications est définie sur une valeur plus élevée.

  [NSHELP-34507]

Réseau

- Lorsque vous redémarrez NetScaler CPX après avoir enregistré la configuration, NetScaler CPX ne démarre pas.

  [NSNET-28691]
- L'appliance NetScaler peut supprimer les paquets reçus en raison d'un problème de temporisation interne visant à nettoyer les mappages temporaires IPv6 obsolètes sur l'appliance.

  [NSHELP-34607]
- Lors de la configuration de BGP, la ligne de commande VTYSH ne s'exécute pas automatiquement et n'affiche aucune suggestion de commande lorsque vous appuyez sur la touche de tabulation après avoir saisi la commande de redistribution.

  [NSHELP-34332]
- En mode Layer-3 avec PMTU activé, l'appliance NetScaler supprime au lieu de transférer les paquets ICMP marqués de la mention « Fragmentation requise mais bit DF défini » pour le trafic ESP.

  [NSHELP-34318]
- Dans une configuration NAT (LSN) à grande échelle, l'appliance NetScaler peut se bloquer en raison d'un problème interne lié à la gestion des files d'attente LSN.

  [NSHELP-33499]

Plateforme

- L'appliance NetScaler se bloque si le VRID est lié à un canal LA dont aucune interface membre n'est configurée.

  [NSPLAT-26707]

- Si NetScaler VPX sur Azure utilise Azure Accelerated Networking, les interfaces de virtualisation des E/S à racine unique (SR-IOV) d'Azure Accelerated Networking peuvent être détachées et rattachées dynamiquement par Azure pendant l'exécution de NetScaler. En raison du détachement et du rattachement dynamiques de la carte réseau, NetScaler peut ne pas répondre dans certains scénarios.

  [NSHELP-34515, NSCXLCM-171, NSCXLCM-908]

- Lorsque vous essayez d'arrêter une appliance NetScaler SDX, l'appliance redémarre au lieu de s'arrêter dès la première tentative. Ce comportement peut se produire lorsque l'appliance génère un core dump alors qu'elle essaie de s'arrêter.

  [NSHELP-33276, NSHELP-33192]

Stratégies

- Dans une configuration HA, l'expression REGEX_REPLACE peut entrer en boucle si elle est configurée avec l'option ALL et une chaîne de remplacement vide, ce qui entraîne un basculement.

  [NSHELP-34640]

SSL

- Dans une configuration de cluster, vous ne pouvez pas associer un profil par défaut ou personnalisé à un service interne SSL.

  [NSSSL-12763]

- La validation des certificats à signature croisée échoue lorsqu'il existe une longue chaîne et que l'un des certificats intermédiaires de la chaîne est un certificat racine à signature croisée.

  [NSHELP-34615]

- Une appliance NetScaler, contenant des puces Intel Coleto ou Intel Lewisburg, peut tomber en panne pendant la phase de renégociation principale si le serveur homologue négocie un chiffrement différent de celui qu'il a initialement négocié.

  [NSHELP-34324]

- Une appliance NetScaler contenant des puces Intel Coleto ou Intel Lewisburg peut se bloquer si le chiffrement DH 512 est utilisé lors d'un échange de clés.

[NSHELP-34094]

- Dans une configuration de cluster qui comporte uniquement des chiffrements personnalisés liés à des services internes, le groupe de chiffrement DEFAULT est également lié aux services internes lorsque vous mettez à niveau la configuration du cluster de la version 13.0 vers la version 13.1.

  [NSHELP-33883]

Système

- Le module d'audit SYSLOG d'une appliance NetScaler peut se bloquer et vider plusieurs fichiers principaux après la mise à niveau de l'appliance vers une version ultérieure à la version 13.0—88.16.

  [NSHELP-33505]

- Une appliance NetScaler peut se bloquer lorsqu'elle reçoit une réponse HTTP 1xx (par exemple « 100 Continuer ») des serveurs principaux lorsque le paramètre RetryOnTimeout est configuré dans la configuration AppQoE.

  [NSHELP-33438]

- Les horodatages des messages Syslog sont incorrects pendant la période d'été.

  [NSHELP-30137]

Interface utilisateur

- Vous ne pouvez pas sélectionner le profil HTTP lors de la création d'un serveur virtuel HTTP_QUIC à l'aide de l'interface graphique. Ce problème se produit car le profil HTTP est désactivé pour la création d'un serveur virtuel HTTP_QUIC.

  [NSUI-18816]

- Sur l'interface graphique, vous ne pouvez pas créer de stratégie d'authentification avancée associée à une action par e-mail. Cela est dû au fait que, lorsque vous créez la stratégie d'authentification, l'option E-mail ne figure pas dans la liste déroulante du champ Type d'action.

  [NSHELP-35065]

- Dans une configuration de cluster, l'ajout des fichiers du jeu de modèles à l'aide de l'interface de ligne de commande ou de l'interface graphique échoue.

  [NSHELP-34996]

- La connexion d'un utilisateur à une partition autre que celle par défaut peut échouer lorsque l'interface graphique ou l'API NITRO est utilisée.

  [NSHELP-34849]

- Le démon HTTPD peut se bloquer lorsqu'il fait face à une exception lors du traitement d'une requête HTTP GET groupée de l'API NITRO.

  [NSHELP-34399]

- La fonctionnalité de sauvegarde et de restauration d'une appliance NetScaler peut ne pas effectuer une sauvegarde correcte de l'appliance lorsqu'elle contient 6 partitions d'administration ou plus.

  [NSHELP-34370]

- Dans l'interface graphique de NetScaler, vous ne pouvez pas lier une stratégie d'équilibrage de charge à des serveurs virtuels de type UDP et SSL car ces options ne sont pas répertoriées sous **Protocole** sur la page **LB Policy Manager** .

  [NSHELP-33724]

- L'erreur suivante apparaît sur l'interface utilisateur de NetScaler lorsqu'il existe une énorme différence entre la configuration enregistrée et la configuration en cours d'exécution :

  « Erreur lors de la récupération de la configuration »

  [NSHELP-32752]

- Lorsque vous configurez la fonctionnalité de partition d'administration sur NetScaler et que vous exécutez en continu des commandes de configuration dans la partition du nœud secondaire, l'enregistrement des configurations sur la partition du nœud secondaire à l'aide de la commande `save ns config` peut échouer.

  [NSHELP-31663]

- Sur l'interface graphique de NetScaler, l'écran Configuration enregistrée ou en cours d'exécution (Système > Diagnostics) affiche de manière incorrecte les balises HTML au lieu d'afficher du texte brut.

  [NSHELP-27169]

- L'ajout d'un profil réseau pour un service d'équilibrage de charge DTLS peut échouer lorsque vous utilisez l'interface graphique NetScaler.

  [NSHELP-23676]

Problèmes connus

Les problèmes qui existent dans la version 13.1—48.47.

Authentification, autorisation et audit

- L'appliance NetScaler peut se bloquer lorsque le serveur virtuel d'authentification est utilisé dans une partition autre que celle par défaut.

  [NSHELP-32054, NSCXLCM-640]

- Un NetScaler se bloque lorsque les conditions suivantes sont remplies :

  - L'authentification par certificat basée sur 401 s'effectue via un serveur virtuel d'équilibrage de charge.
  - Aucune stratégie d'authentification n'est liée à un serveur virtuel d'authentification.
  - La journalisation des débogues est activée.

  [NSAUTH-13259]

- Les administrateurs ne peuvent pas effectuer de journalisation personnalisée des échecs d'authentification dus à des informations d'identification non valides. Ce problème se produit car les stratégies du répondeur NetScaler ne détectent pas les erreurs liées aux échecs de connexion.

  [NSAUTH-11151]

- Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante. `show adfsproxyprofile <profile name>`

  Solution : Connectez-vous au principal NetScaler actif du cluster et exécutez la commande. `show adfsproxyprofile <profile name>` Il afficherait l'état du profil proxy.

  [NSAUTH-5916]

- La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

  - L'option Tester l'accessibilité LDAP est ouverte.
  - Les informations d'identification de connexion non valides sont renseignées et envoyées.
  - Les identifiants de connexion valides sont renseignés et envoyés.

  Solution : fermez et ouvrez l'option Tester l'accessibilité LDAP.

  [NSAUTH-2147]

Gestion des bots

- L'appliance NetScaler peut se bloquer si la stratégie BOT utilise une action de journal avec des règles de stratégie complexes.

  [NSHELP-34999]

Équilibrage de charge

- Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

  [NSLB-7679]

- Dans de rares cas, une appliance NetScaler peut se bloquer et générer un core dump lorsque les conditions suivantes sont remplies :

  - La sonde de surveillance DNS basée sur TCP est utilisée pour surveiller un service principal.
  - La mémoire de l'appliance est insuffisante.

  [NSHELP-35289]

- Le format serviceGroupName dans l'interruption `entityofs` pour le groupe de services est le suivant :
  `<service(group)name>?<ip/DBS>?<port>`

  Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (« ? ») est utilisé comme séparateur. NetScaler envoie l'interruption avec le point d'interrogation (« ? »). Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

  [NSHELP-28080]

Divers

- Lorsqu'une synchronisation forcée a lieu dans une configuration à haute disponibilité, l'appliance exécute la commande « set urlfiltering parameter » dans le nœud secondaire.
  Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre « TimeOfDaytoUpdateDB ».

  [NSSWG-849]

- Lorsqu'une configuration de cluster est inactive, la messagerie nœud à nœud (NNM) peut ajouter un délai de 20 millisecondes pour les paquets ping d'une taille sndbuf spécifiée (commande ping avec option -S).

  [NSHELP-34774]

- Le registre de liste AlwaysOnAllow ne fonctionne pas comme prévu si la valeur du registre est supérieure à 2000 octets.

  [NSHELP-31836]

- Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

  [NSHELP-22409]

NetScaler Gateway

- Sur un appareil Mac utilisant Chrome, l'extension VPN se bloque lors de l'accès à deux noms de domaine complets.

  [NSHELP-32144]

- Le message personnalisé du journal des défaillances EPA ne s'affiche pas sur le portail NetScaler Gateway. Au lieu de cela, le message « erreur interne » s'affiche.

  [NSHELP-31434]

- Parfois, l'ouverture de session automatique de Windows ne fonctionne pas lorsqu'un utilisateur se connecte à l'ordinateur Windows en mode de service permanent. Le tunnel de la machine ne passe pas au tunnel utilisateur et au message « Connexion… » s'affiche dans l'interface utilisateur du plug-in VPN.

  [NSHELP-31357, CGOP-21192, NSCXLCM-612]

- Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil always on `networkAccessOnVPNFailure` de `fullAccess` à `onlyToGateway`.

  [NSHELP-30236]

- Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

  - L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
  - L'appliance est configurée pour une authentification basée sur des certificats avec l'authentification à deux facteurs « désactivée »

  [NSHELP-23584]

- Parfois, lorsque vous parcourez les schémas, le message d'erreur « Impossible de lire le type de propriété non défini » apparaît.

  [NSHELP-21897]

- Dans une configuration de cluster NetScaler, HDX Insight et Gateway Insight ne peuvent pas être activés simultanément.

  [CGOP-23570]

- L'option du système d'exploitation Windows ne figure pas dans la liste déroulante Expression Editor pour les stratégies de pré-authentification et les actions d'authentification sur l'interface graphique de NetScaler. Toutefois, si vous avez déjà configuré l'analyse du système d'exploitation Windows sur une version précédente de NetScaler à l'aide de l'interface graphique ou de l'interface de ligne de commande, la mise à niveau n'a aucune incidence sur

les fonctionnalités. Vous pouvez utiliser l'interface de ligne de commande pour apporter des modifications, si nécessaire.

Solution :

Utilisez les commandes CLI pour la configuration.

- Pour configurer l'action EPA avancée dans l'authentification nFactor, utilisez la commande suivante.
  ```
  add authentication epaAction adv_win_scan -csecexpr "sys.client_expr
  ("sys_0_WIN-OS_NAME_anyof_WIN-10[COMMENT: Windows OS]")
  ```
- Pour configurer une action de pré-authentification classique, utilisez les commandes suivantes.
  ```
  add aaa preauthenticationaction win_scan_action ALLOW
  add aaa preauthenticationpolicy win_scan_policy "CLIENT.SYSTEM('WIN
  -OS_NAME_anyof_WIN-10[COMMENT: Windows OS]')EXISTS"win_scan_action
  ```

[CGOP-22966]

- Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

  [CGOP-19355]

- Le rapport Gateway Insight affiche de manière incorrecte la valeur « Local » au lieu de « SAML » dans le champ Type d'authentification en cas d'échec d'erreur SAML.

  [CGOP-13584]

- Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

  [CGOP-13511]

- Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

  [CGOP-13493]

- Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une stratégie de session depuis l'interface graphique de NetScaler.

  [CGOP-11830]

- Dans Outlook Web App (OWA) 2013, cliquez sur **Options** dans le menu Paramètres pour afficher une boîte de dialogue **d'erreur critique** . De plus, la page ne répond plus.

  [CGOP-7269]

Appliance NetScaler SDX

- Des pertes de paquets sont visibles sur une instance VPX hébergée sur une appliance NetScaler SDX si les conditions suivantes sont remplies :
  - Le mode d'allocation du débit est en rafale.
  - Il existe une grande différence entre le débit et la capacité maximale de rafale.

  [NSHELP-21992]

Réseau

- Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

  [NSNET-25299]

- Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :
  - L'appliance NetScaler BLX est dotée d'un faible nombre de « pages volumineuses ». Par exemple, 1G.
  - L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

  Le problème est enregistré sous forme de message d'erreur dans « /var/log/ns.log » :
  - « BLX-DPDK:DPDK Mempool n'a pas pu être initialisé pour PE-x »

  Remarque : x est un nombre <= nombre de processus de travail.

  Solution : allouez un grand nombre de « pages volumineuses », puis redémarrez l'appliance.

  [NSNET-25173]

- Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

  [NSNET-24449]

- Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :
  - Désactiver
  - Activer
  - Réinitialiser

  [NSNET-16559]

- L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

  « Les paquets suivants ont des dépendances non satisfaites : blx-core-libs:i386 : PreDepends : libc6:i386 (>= 2.19) mais ils ne sont pas installables »

  Solution : exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

  - dpkg –add-architecture i386
  - apt-get update
  - apt-get install libc6:i386

  [NSNET-14602]

- Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

  [NSNET-5233]

- Il est possible que l'appliance NetScaler ne génère pas de messages d'interruption SNMP « Cold-Start » après un redémarrage à froid.

  [NSHELP-27917]

- Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

  [NSHELP-21082]

Plateforme

- Certains packages python ne sont pas installés lorsque vous rétrogradez l'appliance NetScaler de la version 13.1-4.x et des versions supérieures vers l'une des versions suivantes :

  - Toute version 11.1
  - 12.1-62.21 et versions antérieures
  - 13.0-81.x et versions antérieures

  [NSPLAT-21691]

- Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud

correspondante de l'instance NetScaler. Utilisez la commande « rm cloudprofile » pour supprimer le profil.

[NSPLAT-4520]

- Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
  Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

  [NSPLAT-4451]

- Si le NetScaler SDX secondaire d'une configuration HA est configuré avec un cœur de processeur partagé et que les pulsations HA sont échangées via un VLAN, il tente sans succès de passer au nœud principal.

  [NSHELP-32412]

Stratégies

- Les connexions peuvent être bloquées si la taille du traitement des données est supérieure à la taille de la mémoire tampon TCP par défaut configurée.

  Solution : définissez la taille de la mémoire tampon TCP sur la taille maximale des données qui doivent être traitées.

  [NSPOLICY-1267]

SSL

- Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

  Solution :

  1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
  2. Enregistrez la configuration.

  [NSSSL-9572]

- Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

  [NSSSL-6478]

- Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

  [NSSSL-6213]

- Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
  ERROR: crl refresh disabled

  [NSSSL-6106]

- L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

  [NSSSL-4427]

- Un message d'avertissement incorrect, « Avertissement : aucun chiffrement utilisable configuré sur le serveur/service SSL » s'affiche si vous essayez de modifier le protocole ou le chiffrement SSL dans le profil SSL.

  [NSSSL-4001]

- Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

  [NSSSL-3184, NSSSL-1379, NSSSL-1394]

- Les clients TLS basés sur OpenSSL 3.x mettent fin à une connexion prématurément, à moins que le serveur n'accuse réception de l'annonce du client concernant la prise en charge de la RFC 5746 (Renegotiation Indication Extension or Secure Renegotiation). Les serveurs virtuels frontaux ignorent cette publicité lorsque la renégociation est désactivée, ce qui entraîne des échecs de connexion. Grâce à ce correctif, les serveurs virtuels frontaux reconnaissent désormais la publicité même lorsque la renégociation est désactivée, ce qui améliore la compatibilité.

  [NSHELP-35120]

Système

- NetScaler peut se bloquer si toutes les conditions suivantes sont remplies :
  - Les événements, les journaux d'audit ou les métriques sont activés dans le profil d'analyse ou les paramètres AppFlow.
  - Une stratégie de réécriture côté réponse est configurée.

  [NSHELP-35550]

- Un NetScaler avec authentification multifactorielle configurée se bloque lors d'une évaluation des stratégies.

  [NSHELP-33674]

- L'appliance NetScaler configurée avec un service SSL se bloque lorsqu'elle reçoit un paquet de contrôle TCP FIN suivi d'un paquet de contrôle TCP RESET.

  [NSHELP-31656]

- Un RTT élevé est observé pour une connexion TCP si la condition suivante est remplie :

  - une fenêtre de congestion maximale élevée (> 4 Mo) est définie
  - L'algorithme TCP NILE est activé

  Pour qu'une appliance NetScaler utilise l'algorithme NILE pour le contrôle de la congestion, les conditions doivent dépasser le seuil de démarrage lent, qui est associé à la fenêtre de congestion maximale

  Ainsi, jusqu'à ce que la fenêtre de congestion maximale configurée soit atteinte, NetScaler continue d'accepter des données et se retrouve avec un RTT élevé.

  [NSHELP-31548]

- Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

  [NSBASE-18295]

- Dans de rares cas, les flux créés avant la création du flux WebSocket HTTP/2 peuvent être interrompus lorsque la connexion côté serveur du WebSocket se ferme.

  Ce problème se produit car l'appliance NetScaler ne prend pas en charge le multiplexage des connexions pour HTTP/2 WebSocket.

  Solution : désactivez le multiplexage des connexions pour le profil HTTP2 associé à l'aide de la commande suivante :

  ```
  set httpProfile <name> [-conMultiplex ( ENABLED | DISABLED )]
  ```

  [NSBASE-17449]

- L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

  [NSBASE-8506]

Interface utilisateur

- Dans l'interface graphique de NetScaler, le lien « Aide » présent sous l'onglet « Tableau de bord » est cassé.

  [NSUI-14752]

- L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution : configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de l'interface de ligne de commande NetScaler.

[NSUI-13024]

- Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

  [NSUI-6838]

- Dans une configuration à haute disponibilité des appliances NetScaler BLX, le nœud principal peut ne plus répondre en bloquant toute demande de CLI ou d'API.

  Solution : redémarrez le nœud principal.

  [NSCONFIG-6601]

- Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

  1. Mettez à niveau l'appliance NetScaler vers l'une des versions
     - 13.0 52.24 build
     - 12.1 57.18 build
     - 11.1 65.10 build
  2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
  3. Rétrogradez l'appliance NetScaler vers une version antérieure.

  Pour afficher la liste de ces utilisateurs du système à l'aide de l'interface de ligne de commande : À l'invite de commandes, tapez :

  ```
  query ns config -changedpassword [-config <full path of the configuration
   file (ns.conf)>]
  ```

  Solution : Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

  - Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
  - Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
  - Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

  Pour plus d'informations, voir How to reset root administrator (nsroot) password.

  [NSCONFIG-3188]

Notes de publication pour la version 13.1-45.64 de NetScaler

June 2, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1-45.64 de NetScaler.

Remarques

- Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.
- Les versions 13.1-45.61 et ultérieures corrigent les failles de sécurité décrites dans l'article CTX477714.
- La version 13.1-45.64 remplace la version 13.1-45.61 et la version 13.1-45.63. Toutefois, si vous avez effectué la mise à niveau vers la version 13.1-45.61, vous pouvez constater une perte de configuration. Voir CTX547038 pour les étapes de correction.
- La version 13.1-45.63 inclut des correctifs pour NSSSL-12761 et NSHELP-35058, ainsi que toutes les améliorations et corrections de bugs disponibles dans la version 13.1-45.61.
- La version 13.1-45.64 inclut le correctif pour NSBASE-18162 (NSHELP-35288), ainsi que toutes les améliorations et corrections de bogues disponibles dans la version 13.1-45.63.

Nouveautés

Les améliorations et modifications disponibles dans la version 13.1-45.64.

Appliance NetScaler SDX

- **Contrôles supplémentaires lors de la mise à niveau d'une appliance SDX**

  Désormais, la mise à niveau de l'appliance NetScaler SDX ne sera pas autorisée si la connexion Secure Shell (SSH) du service de gestion vers XenServer/Citrix Hypervisor échoue.

  [NSSVM-5114]

- **Activer ou désactiver la complexité des mots de passe lors de la création de profils d'administrateur**

  L'appliance NetScaler SDX prend désormais en charge l'activation ou la désactivation de la complexité des mots de passe sur les instances VPX à l'aide de l'interface graphique ou de la CLI.

  - Lorsque la complexité du mot de passe est activée, la longueur minimale requise est de 4 caractères, contre 6 caractères auparavant.

- Lorsque la complexité du mot de passe est désactivée, la longueur minimale requise est de 1 caractère.

[NSSVM-4889]

Web App Firewall NetScaler

- **Configuration de l'authentification par proxy pour NetScaler Web App Firewall, les robots et la réputation IP**

  Vous pouvez désormais configurer l'authentification par proxy pour les mises à jour des signatures de NetScaler Web App Firewall, les mises à jour des signatures de robots et les mises à jour de réputation. L'authentification par proxy fournit un niveau de sécurité supplémentaire à votre appliance. L'appliance NetScaler sur laquelle l'authentification par proxy est activée s'authentifie auprès du serveur proxy avant de télécharger les mises à jour depuis Internet. Vous pouvez ainsi protéger vos appareils contre les téléchargements malveillants.
  Pour configurer l'authentification par proxy, spécifiez le nom d'utilisateur et le mot de passe du proxy dans les paramètres des fonctionnalités de sécurité suivantes :

  - Web App Firewall NetScaler. Pour plus d'informations, consultez la section Paramètres du moteur
  - Bot. Pour plus d'informations, consultez la section Détection de bots.
  - Réputation IP. Pour plus d'informations, voir Réputation IP

  [NSWAF-9532]

- **L'attribut apache_mode est obsolète**

  L'attribut `apache_mode` du paramètre `invalidPercentHandling` de la commande `add appfw profile` est obsolète.

  [NSWAF-4110]

Équilibrage de charge

- **Augmentation du nombre maximum d'entrées personnalisées**

  Vous pouvez désormais ajouter un maximum de 3 000 entrées d'emplacement personnalisées pour spécifier les qualificatifs d'emplacement pour les plages d'adresses IP. Ces entités sont utilisées dans la méthode de proximité statique GSLB et dans les stratégies de correspondance de localisation.

  Pour plus d'informations, voir Ajouter des entrées personnalisées à une base de données de proximité statique.

  [NSLB-9755]

Réseau

- **Support de configuration automatique pour l'appliance NetScaler BLX**

  Les fonctionnalités de configuration automatique suivantes sont ajoutées pour l'appliance NetScaler BLX :

  - Vous pouvez configurer l'appliance NetScaler BLX pour ajouter automatiquement tous les ports NIC de l'hôte Linux en tant que ports dédiés pour l'appliance. Pour cette configuration automatique, vous devez définir le `blx-managed-host` paramètre sur 1 et commenter les deux lignes contenant le **`interface`** paramètre dans le fichier de configuration NetScaler BLX ().`blx.conf` L'appliance y ajoute automatiquement tous les ports NIC de l'hôte Linux en tant que ports dédiés. En outre, l'appliance détecte automatiquement les ports NIC compatibles avec DPDK et les lie au module DPDK VFIO sur l'hôte Linux.
  - Vous pouvez configurer une appliance NetScaler BLX en mode dédié pour définir automatiquement l'adresse NSIP et la passerelle par défaut de l'appliance. Pour cette configuration automatique, vous devez définir `blx-managed-host` sur 1 et commenter les lignes contenant les paramètres `ipaddress` et **`default`** dans le fichier de configuration NetScaler BLX (`blx.conf`). L'appliance sélectionne l'un de ses ports NIC dédiés comme port par défaut sur lequel la route de passerelle ayant la priorité la plus élevée est présente sur l'hôte Linux. L'adresse IP du port par défaut et la passerelle par défaut sont définies comme l'adresse NSIP et la passerelle par défaut pour l'appliance NetScaler BLX.

  [NSNET-27468]

- **Support de RHEL version 9.x pour les appliances NetScaler BLX**

  L'appliance NetScaler BLX est désormais prise en charge sur les plateformes Red Hat Enterprise Linux (RHEL) version 9.x.

  [NSNET-27421]

Stratégies

- **Possibilité d'utiliser l'outil NSPEPI sur les appliances NetScaler BLX et CPX**

  Les outils de configuration NSPEPI et Check invalid sont désormais pris en charge dans les appliances NetScaler CPX et BLX.

  [NSPOLICY-4872]

SSL

- **Poursuivre l'établissement de connexion SSL avec un nom de serveur inconnu**

L'appliance NetScaler permet désormais à l'établissement de connexion SSL de se poursuivre même pour un nom de serveur inconnu, et laisse au client le soin de décider d'abandonner ou de terminer l'établissement de connexion.

Auparavant, l'appliance avait mis fin à l'établissement de connexion SSL lorsqu'elle avait reçu un bonjour client avec un nom de serveur inconnu.

[NSSSL-10918]

Système

- Prise en**charge de la compression pour la méthode de requête HTTP PUT**
  Une appliance NetScaler compresse désormais la réponse HTTP reçue du serveur pour les requêtes HTTP qui utilisent la méthode de requête PUT.

  [NSHELP-32695]

- **Configurer la fréquence d'exportation du collecteur de métriques**

  Par défaut, le collecteur de métriques prend en charge l'exportation de données analytiques de séries chronologiques toutes les 30 secondes. Vous pouvez désormais le configurer sous la forme d'une valeur comprise entre 30 et 300 secondes afin de pouvoir décider de l'intervalle d'exportation des données de profil d'analyse des séries chronologiques depuis NetScaler.

  [NSBASE-17561]

- **Support pour l'exportation directe des journaux d'audit vers Splunk**

  La journalisation des audits vous permet de consigner les états de NetScaler et les informations d'état collectées par les différents modules de NetScaler. Vous pouvez exporter les journaux d'audit de NetScaler vers Splunk et obtenir des informations pertinentes utiles pour la résolution des problèmes. Cette fonctionnalité vous permet d'utiliser le collecteur d'événements HTTP fourni par Splunk pour envoyer des journaux d'audit via HTTP (ou HTTPS) directement de votre NetScaler à Splunk.

  [NSBASE-17559]

- **Support pour le multiplexage des connexions WebSocket HTTP/2**

  L'appliance NetScaler prend désormais en charge le multiplexage des connexions WebSocket. Les connexions WebSocket sont prises en charge via HTTP/2. Vous pouvez activer les connexions WebSocket à l'aide de l'interface de ligne de commande ou de l'interface graphique.

  [NSBASE-17307]

Problèmes résolus

Les problèmes qui sont résolus dans la version 13.1-45.64.

AppFlow

- Le collecteur de métriques de l'instance NetScaler cesse de répondre par intermittence. Par conséquent, chaque fois que le collecteur de métriques cesse de répondre, un intervalle (30 secondes) de données analytiques peut ne pas être exporté.

  [NSHELP-34048]

Authentification, autorisation et audit

- Sur certaines appliances NetScaler sur lesquelles le GSLB est activé, la redirection du serveur virtuel d'authentification vers le serveur virtuel d'équilibrage de charge échoue en raison d'un calcul d'URL non valide.

  [NSHELP-33459]

- Lorsque NetScaler est utilisé comme fournisseur OpenID (OAuth IdP) et que GSLB est configuré avec ce fournisseur, l'authentification OAuth auprès de la partie qui se fie (RP) échoue lors de la validation du jeton, ce qui peut entraîner un échec d'authentification au niveau de la partie relais OAuth (RP).

  [NSHELP-3345]

- L'appliance NetScaler peut se bloquer lorsqu'elle est configurée en tant que fournisseur de services SAML et que les certificats SSL sont mis à jour.

  [NSHELP-33243, NSHELP-32966, NSHELP-33242, NSHELP-34366]

- L'authentification OAuth sur une appliance NetScaler échoue en raison de problèmes liés à l'analyse des jetons.

  [NSHELP-31573]

Gestion des bots

- L'appliance NetScaler tente de télécharger les données de base de données IP lorsque la fonctionnalité de réputation IP est désactivée.

  [NSHELP-34488]

Mise en cache

- Une appliance NetScaler peut redémarrer si la valeur Max-Age de l'en-tête Cache-Control pour les objets mis en cache est modifiée sur le serveur principal.

  [NSHELP-34078]

- Dans une configuration de cluster, les informations de stratégie globale du cache affichées dans l'interface graphique ou la CLI sont incomplètes lorsque la configuration du cluster est accessible à l'aide de l'adresse CLIP.

  [NSCACHE-521]

Appliance NetScaler SDX

- Une appliance NetScaler SDX peut se bloquer lors de la tentative d'accès à « Core Allocation » depuis le tableau de bord du service de gestion.

  [NSHELP-34537]

- Parfois, une appliance NetScaler SDX peut ne pas se comporter comme prévu si les unités cryptographiques asymétriques (ACU) et les unités cryptographiques symétriques (SCU) attribuées à une instance VPX ne sont pas un multiple du cœur du moteur de paquets (PE). C'est-à-dire un nombre de 1000* cœurs PE.

  [NSHELP-34389]

- Le service de gestion (SVM) peut se bloquer lors de la modification de l'une des propriétés d'une instance VPX à partir de l'interface utilisateur du service de gestion.

  [NSHELP-34297]

- Lorsque vous essayez de modifier l'adresse IP de prise en charge dans une appliance NetScaler SDX en accédant à **Configuration > Système > Assistant de configuration > Réseau de gestion > Modifier l'adresse IP de prise en charge, les modifications ne**sont pas enregistrées. Les modifications sont bloquées lorsque vous cliquez sur « Oui » dans l'invite. Une erreur de référence non définie s'affiche dans le navigateur.

  Correctif : Vérifiez l'objet non défini avant de le référencer.

  [NSHELP-34141]

NetScaler Gateway

- Après une mise à niveau, l'appliance NetScaler peut se bloquer lorsque HDX Insight est activé.

  [NSHELP-35058]

- Après une mise à niveau, l'appliance NetScaler peut se bloquer lors du lancement d'une connexion proxy RDP.

  [NSHELP-33420]

- Le profil Always On n'est pas défini dans une action de session VPN lorsque l'action de session VPN est reconfigurée.

[NSHELP-33396]

- Après une mise à niveau, une appliance NetScaler peut se bloquer lors de la première synchronisation HA.

  [NSHELP-32957]

Web App Firewall NetScaler

- L'appliance NetScaler peut se bloquer pendant le déploiement de la haute disponibilité si les règles de signature du Web App Firewall contiennent l'un des objets suivants :
  - Patsets
  - Ensembles de données
  - Cartes à cordes
  - Expressions nommées

  [NSHELP-34338]

- Lorsque vous exportez des règles de relaxation, le téléchargement prend plus de temps et le fichier n'est pas entièrement téléchargé. Ce problème se produit si la taille du fichier est supérieure à 5 Mo.

  [NSHELP-34044]

- Lorsque la stratégie du Web App Firewall est mise à jour sur le vserver, les problèmes suivants sont observés :
  - L'interface graphique et la CLI de NetScaler n'ont pas répondu ou ont pris plus de temps que d'habitude.
  - L'utilisation du processeur par paquets est passée à 100 %
  - Le nombre de sessions de persistance a été augmenté.

  [NSHELP-33975]

- La règle de relaxation par injection de commandes JSON risque de ne pas fonctionner si elle contient un point-virgule (;) ou un point (.) dans la règle de relaxation.

  [NSHELP-33606]

Équilibrage de charge

- L'appliance NetScaler se bloque lorsque les conditions suivantes sont remplies et que vous dissociez tous les services et que vous les liez à nouveau.
  - Un serveur virtuel d'équilibrage de charge est configuré à l'aide de la méthode basée sur le hachage.

- Les services sont liés à ce serveur virtuel par priorité.

[NSHELP-34314]

- Dans une configuration HA, l'appliance NetScaler se bloque lorsque le groupe de services lié à plusieurs serveurs virtuels est supprimé.

  [NSHELP-34029]

- L'erreur suivante peut apparaître lors de l'ajout ou de la modification d'une configuration d'équilibrage de charge sur une appliance NetScaler :

  La configuration est peut-être incohérente. Vérifiez avec la commande « show configstatus » ou redémarrez.

  Ce problème se produit lorsque la commande set lb vserver est utilisée avec les paramètres HttpsRedirectURL et RedirectFromPort.

  [NSHELP-33912]

- Dans de rares cas, nsmap se bloque. Par conséquent, certaines appliances NetScaler qui utilisent des bases de données de géolocalisation peuvent ne pas fonctionner comme prévu.

  [NSHELP-33840]

- Si les services sont désactivés puis activés dans une configuration de haute disponibilité, certains moniteurs peuvent passer à l'état SKIP_OFS en cas de basculement.

  [NSHELP-33717]

- La commande show cs vserver n'affiche pas le paramètre de règle, même si le paramètre est configuré dans la stratégie de commutation de contenu et lié au serveur virtuel de commutation de contenu.

  [NSHELP-33506]

- Lors de la mise en miroir des connexions, l'appliance NetScaler se bloque lorsque la stratégie de réécriture est supérieure à 30 octets.

  [NSHELP-32902]

- Une alerte SNMP est générée même si l'utilisation de la bande passante se situe dans la limite configurée. Ce problème se produit lors de la comparaison de deux types de données différents et l'un des paramètres est inchangé lors de l'incrémentation.

  [NSHELP-32509]

- Une appliance NetScaler dont la mise en miroir des connexions est configurée se bloque lorsque les paquets Jumbo sont envoyés.

  [NSHELP-31072]

- L'appliance NetScaler VPX se bloque lorsque les conditions suivantes sont remplies :

1. L'option autosync est utilisée pour synchroniser la configuration avec d'autres sites GSLB.
2. Le numéro d'incarnation utilisé pour récupérer le cache GSLB est un multiple de 1024.

[NSHELP-30075]

- Dans une configuration GSLB, le certificat SSL est absent des sites subordonnés. Ce problème se produit lorsque l'option de synchronisation automatique est activée et que les sites subordonnés possèdent des certificats SSL qui ne sont pas disponibles sur le site principal.

  [NSHELP-29309]

Divers

- Lorsque vous exécutez le script « ns_hw_err.bash » sur l'appliance NetScaler, le message d'erreur suivant s'affiche :
  « erreur : impossible d'ouvrir le fichier 'ns_hw_plugins.py' : [Errno 2] Aucun fichier ou répertoire de ce type »

  [NSHELP-32991]

- Dans une configuration de cluster, la synchronisation automatique des fichiers échoue lorsque l'adresse IP du cluster est configurée dans un sous-réseau différent de celui de l'adresse NSIP.

  [NSHELP-29988]

Plateforme

- Après avoir mis à niveau l'appliance ADC vers la version 13.1 build 42.47, sur certains déploiements VPX dans le cloud public, vous pouvez observer le basculement des services HTTP et TCP entre les états UP et DOWN.

  [NSPLAT-26310]

- Sur une appliance SDX exécutant la version 4.08 du microprogramme BMC, lorsque vous effectuez une mise à niveau groupée depuis la version 13.0 build 84.X, la mise à niveau du microprogramme de gestion des lumières (LOM) vers la version 4.14 pendant le démarrage du système peut rester bloquée par intermittence et expirer au bout de 30 minutes.

  [NSPLAT-26148]

- Dans une configuration HA d'une instance NetScaler VPX sur le cloud AWS, le contenu du fichier « cloud-ha-daemon.log » qui est stocké à l'emplacement /var/log/ est imprimé deux fois au lieu d'une.

  [NSPLAT-25687]

- Sur une appliance NetScaler SDX, les instances VPX peuvent fonctionner avec la valeur de débit minimale configurée dans le cadre du mode rafale, même si un débit suffisant est disponible dans l'appliance SDX pour gérer les rafales de trafic.

  [NSHELP-33875, NSHELP-34667]

- Sur les plateformes NetScaler MPX 9100, MPX 9100T, MPX 16000 et MPX 16000T, l'appliance peut apparaître sans licence si l'ID d'hôte de licence change.

  [NSHELP-33745, NSHELP-33756, NSHELP-33801]

SSL

- Les commandes permettant de lier une paire de clés de certificat et une courbe ECC à un service SSL, à un groupe de services ou à un service interne ne sont pas enregistrées dans la configuration (ns.conf).

  [NSSSL-12761]

- Après la mise à niveau vers la version 13.1 build 37.x, il se peut que vous ne puissiez pas négocier à l'aide du protocole TLSv1.0 même si la configuration n'a pas changé.

  [NSHELP-34345]

Système

- Les réponses HTTP compressées par l'appliance NetScaler peuvent provoquer des défaillances dans certains clients HTTP (S) en raison de l'ajout d'espaces en début de ligne dans la valeur du champ d'en-tête de réponse HTTP Content-Length.

  [NSHELP-3460]

- L'appliance NetScaler configurée pour enregistrer tous les en-têtes HTTP se bloque lorsqu'une requête ou une réponse HTTP est reçue avec plus de 20 en-têtes longs.

  [NSHELP-34145]

- L'appliance NetScaler peut se bloquer si un collecteur AppFlow de type rest est configuré dans la partition d'administration.

  [NSHELP-33600]

- Dans NetScaler version 13.1 build 33.47 et versions ultérieures, vous ne pouvez pas activer ou désactiver les événements, les métriques et les paramètres du journal d'audit à l'aide de l'interface graphique ou de la CLI.

  [NSHELP-33247]

- Un client gRPC ne parvient pas à analyser l'en-tête d'état du gRPC lorsque la condition suivante est remplie :
  - L'en-tête d'état gRPC est ajouté à la fois dans l'en-tête de début et dans l'en-tête de fin au lieu d'être ajouté uniquement dans l'en-tête de fin.

  [NSHELP-31640]
- Une fuite de mémoire peut se produire dans l'appliance NetScaler si les deux conditions suivantes sont remplies :
  - La fonctionnalité de compression HTTP est activée.
  - La connexion est réinitialisée au milieu de la transaction.

  [NSHELP-30631]
- Une appliance Citrix ADC peut se bloquer lorsqu'un serveur virtuel compatible HTTP/2 génère une réponse à une demande HTTP/2, au lieu de transmettre la demande au service principal.

  [NSBASE-18162, NSHELP-35288]
- La réponse gRPC en en-tête uniquement envoyée par l'appliance NetScaler aux clients ne contient ni l'état ni le message gRPC.

  [NSBASE-17802]

Interface utilisateur

- Si vous utilisez des partitions d'administration, vous ne pouvez pas supprimer un certificat SSL à l'aide de l'interface graphique.

  [NSHELP-34429]
- Dans l'interface graphique de NetScaler, la colonne **Bound To** de la page **Configurer la liaison à la stratégie de commutation de contenu** affiche la chaîne « CS Virtual Server » au lieu du nom réel du serveur virtuel de commutation de contenu auquel la stratégie est liée.

  [NSHELP-34374]
- La configuration d'un service alternatif pour un profil HTTP peut échouer lorsque vous utilisez l'interface graphique de NetScaler.

  [NSHELP-34304]
- Lors de la liaison du profil AppFW à l'expression du journal, le paramètre state est défini sur activé par défaut. Toutefois, lorsque le système est mis à niveau, le paramètre est réinitialisé sur désactivé.

  [NSHELP-34187]

- Le téléchargement de tous les fichiers principaux présents sur la page « Diagnostic » (« Système > Diagnostic ») de l'interface graphique de NetScaler peut échouer avec une erreur.

  [NSHELP-33644]

- Dans l'interface utilisateur graphique de NetScaler, lorsque vous cliquez sur le bouton Modifier pour un type d'interruption SNMP spécifique, les détails d'un piège SNMP de type générique s'affichent à la place du piège SNMP de type spécifique.

  [NSHELP-33520]

- Les appels nominaux du SDK NITRO Python GET échouent avec le message d'erreur « réponse de la variable locale référencée avant l'affectation » pour les ressources suivantes :

  - `appfwhtmlerrorpage`
  - `appfwjsonerrorpage`
  - `appfwprotofile`
  - `appfwsignatures`
  - `appfwwsdl`
  - `appfwxmlerrorpage`
  - `appfwxmlschema`
  - `botsignature`
  - `responderhtmlpage`

  [NSHELP-32525]

- Dans une configuration de cluster, l'opération `show HTTP monitor` effectuée sur l'adresse CLIP n'affiche pas les codes de réponse HTTP à valeurs multiples.

  [NSCONFIG-7107]

Problèmes connus

Les problèmes qui existent dans la version 13.1-45.64.

Authentification, autorisation et audit

- L'appliance NetScaler peut se bloquer lorsque le serveur virtuel d'authentification est utilisé dans une partition autre que celle par défaut.

  [NSHELP-32054]

- Les administrateurs ne peuvent pas effectuer de journalisation personnalisée des échecs d'authentification dus à des informations d'identification non valides. Ce problème se produit car les stratégies du répondeur NetScaler ne détectent pas les erreurs liées aux échecs de connexion.

[NSAUTH-11151]

- Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante. `show adfsproxyprofile <profile name>`

  Solution : Connectez-vous au principal NetScaler actif du cluster et exécutez la commande. `show adfsproxyprofile <profile name>` Il afficherait l'état du profil proxy.

  [NSAUTH-5916]

- La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

  - L'option Tester l'accessibilité LDAP est ouverte.
  - Les informations d'identification de connexion non valides sont renseignées et envoyées.
  - Les identifiants de connexion valides sont renseignés et envoyés.

  Solution : fermez et ouvrez l'option Tester l'accessibilité LDAP.

  [NSAUTH-2147]

NetScaler Gateway

- Les ressources de l'intranet qui se chevauchent avec une plage d'adresses IP usurpée ne sont pas accessibles lorsque le tunnel partagé est défini sur OFF sur le client Citrix Secure Access.

  [NSHELP-34334]

- La connexion VPN permanente échoue par intermittence au démarrage en raison de l'accessibilité du serveur Gateway.

  [NSHELP-33500]

- Si les valeurs de registre associées à Citrix Secure Access sont supérieures à 1 500 caractères, le collecteur de journaux ne parvient pas à recueillir les journaux d'erreurs.

  [NSHELP-33457]

- Lorsque vous utilisez le pilote Windows Filtering Platform (WFP), l'accès à l'intranet ne fonctionne parfois pas une fois le VPN reconnecté.

  [NSHELP-32978]

- Le client Citrix Secure Access, version 21.7.1.2 et versions ultérieures, ne parvient pas à effectuer la mise à niveau vers des versions ultérieures pour les utilisateurs ne disposant pas de droits d'administration. Ce problème s'applique uniquement si la mise à niveau du client Citrix Secure Access est effectuée à partir d'une appliance NetScaler.

  [NSHELP-32793]

- Lorsque les utilisateurs cliquent sur l'onglet Page d'accueil de l'écran Citrix Secure Access pour Windows, la page affiche l'erreur de refus de connexion.

  [NSHELP-32510]

- Sur un appareil Mac utilisant Chrome, l'extension VPN se bloque lors de l'accès à deux noms de domaine complets.

  [NSHELP-32144]

- Dans certains cas, si les paramètres de proxy sont vides dans NetScaler Gateway 13.0 ou 13.1, Citrix SSO crée des paramètres de proxy incorrects.

  [NSHELP-31970]

- Les connexions directes aux ressources situées en dehors du tunnel établi par Citrix Secure Access peuvent échouer en cas de retard ou de congestion important.

  [NSHELP-31598]

- Le message personnalisé du journal des défaillances EPA ne s'affiche pas sur le portail NetScaler Gateway. Au lieu de cela, le message « erreur interne » s'affiche.

  [NSHELP-31434]

- Parfois, l'ouverture de session automatique de Windows ne fonctionne pas lorsqu'un utilisateur se connecte à l'ordinateur Windows en mode de service permanent. Le tunnel de la machine ne passe pas au tunnel utilisateur et au message « Connexion… » s'affiche dans l'interface utilisateur du plug-in VPN.

  [NSHELP-31357, CGOP-21192, NSHELP-34211]

- Lorsque Always on est configuré, le tunnel utilisateur échoue en raison du numéro de version incorrect (1.1.1.1) dans le fichier aoservice.exe.

  [NSHELP-30662]

- Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil « NetworkAccessOnVPNFailure » de « FullAccess » à « OnlyToGateway ».

  [NSHELP-30236]

- La page d'accueil de la passerelle ne s'affiche pas immédiatement après que le plug-in de passerelle a réussi à établir le tunnel VPN. Pour résoudre ce problème, la valeur de registre suivante est introduite.

  HKLMSoftwareCitrixSecure Access ClientSecureChannelResetTimeoutSeconds
  Type: DWORD

  Par défaut, cette valeur de registre n'est ni définie ni ajoutée. Lorsque la valeur de « SecureChannelResetTimeoutSeconds » est 0 ou n'est pas ajoutée, le correctif pour gérer le délai ne fonctionne pas, ce qui est le comportement par défaut. L'administrateur doit définir ce registre sur

le client pour activer le correctif (c'est-à-dire afficher la page d'accueil immédiatement après que le plug-in de passerelle ait établi le tunnel VPN avec succès).

[NSHELP-30189]

- Le client VPN Windows n'honore pas l'alerte « Notification de fermeture SSL » du serveur et envoie la demande de connexion de transfert sur la même connexion.

  [NSHELP-29675]

- L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

  [NSHELP-28551]

- Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

  [NSHELP-28404]

- Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

  - L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
  - L'appliance est configurée pour l'authentification basée sur des certificats avec l'authentification à deux facteurs « désactivée »

  [NSHELP-23584]

- Parfois, lorsque vous parcourez les schémas, le message d'erreur « Impossible de lire le type de propriété non défini » apparaît.

  [NSHELP-21897]

- Dans une configuration de cluster NetScaler, HDX Insight et Gateway Insight ne peuvent pas être activés simultanément.

  [CGOP-23570]

- L'option du système d'exploitation Windows ne figure pas dans la liste déroulante Expression Editor pour les stratégies de pré-authentification et les actions d'authentification sur l'interface graphique de NetScaler. Toutefois, si vous avez déjà configuré l'analyse du système d'exploitation Windows sur une version précédente de NetScaler à l'aide de l'interface graphique ou de l'interface de ligne de commande, la mise à niveau n'a aucune incidence sur les fonctionnalités. Vous pouvez utiliser l'interface de ligne de commande pour apporter des modifications, si nécessaire.

  Solution :

  Utilisez les commandes CLI pour la configuration.

- Pour configurer l'action EPA avancée dans l'authentification nFactor, utilisez la commande suivante.
  add authentication epaAction adv_win_scan -csecexpr "sys.client_expr("sys_0_WIN-OS_NAME_anyof_WIN-10[COMMENT: Windows OS]")"
- Pour configurer une action de pré-authentification classique, utilisez les commandes suivantes.
  add aaa preauthenticationaction win_scan_action ALLOW
  add aaa preauthenticationpolicy win_scan_policy "CLIENT.SYSTEM('WIN-OS_NAME_anyof_WIN-10[COMMENT: Windows OS]') EXISTS" win_scan_action

[CGOP-22966]

- Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

  [CGOP-19355]

- Le rapport Gateway Insight affiche de manière incorrecte la valeur « Local » au lieu de « SAML » dans le champ Type d'authentification en cas d'échec d'erreur SAML.

  [CGOP-13584]

- Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

  [CGOP-13511]

- Lorsqu'une connexion ICA est lancée à partir d'un Receiver MAC version 19.6.0.32 ou Citrix Virtual Apps and Desktops version 7.18, la fonctionnalité HDX Insight est désactivée.

  [CGOP-13494]

- Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

  [CGOP-13493]

- Lorsque vous acceptez les connexions hôtes locales depuis le navigateur, la boîte de dialogue Accepter la connexion pour macOS affiche du contenu en anglais, quelle que soit la langue sélectionnée.

  [CGOP-13050]

- Le texte « Page d'accueil » dans l' application Citrix SSO > Page d'accueil est tronqué pour certaines langues.

  [CGOP-13049]

- Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une stratégie de session depuis l'interface graphique de NetScaler.

  [CGOP-11830]

- Dans Outlook Web App (OWA) 2013, cliquez sur **Options** dans le menu Paramètres pour afficher une boîte de dialogue **d'erreur critique** . De plus, la page ne répond plus.

  [CGOP-7269]

Équilibrage de charge

- Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

  [NSLB-7679]

- Le format serviceGroupName dans l'interruption `entityofs` pour le groupe de services est le suivant :
  `<service(group)name>?<ip/DBS>?<port>`

  Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (« ? ») est utilisé comme séparateur. NetScaler envoie l'interruption avec le point d'interrogation (« ? »). Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

  [NSHELP-28080]

Divers

- Lorsqu'une synchronisation forcée a lieu dans une configuration à haute disponibilité, l'appliance exécute la commande « set urlfiltering parameter » dans le nœud secondaire.
  Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre « TimeOfDaytoUpdateDB ».

  [NSSWG-849]

- Le registre de liste AlwaysOnAllow ne fonctionne pas comme prévu si la valeur du registre est supérieure à 2000 octets.

  [NSHELP-31836]

- Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

  [NSHELP-22409]

Réseau

- Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

  [NSNET-25299]

- Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :

  - L'appliance NetScaler BLX est dotée d'un faible nombre de « pages volumineuses ». Par exemple, 1G.
  - L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

  Le problème est enregistré sous forme de message d'erreur dans « /var/log/ns.log » :

  - « BLX-DPDK:DPDK Mempool n'a pas pu être initialisé pour PE-x »

  Remarque : x est un nombre <= nombre de processus de travail.

  Solution : allouez un grand nombre de « pages volumineuses », puis redémarrez l'appliance.

  [NSNET-25173]

- Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

  [NSNET-24449]

- Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

  - Désactiver
  - Activer
  - Réinitialiser

  [NSNET-16559]

- L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

  « Les paquets suivants ont des dépendances non satisfaites : blx-core-libs:i386 : PreDepends : libc6:i386 (>= 2.19) mais ils ne sont pas installables »

  Solution : exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

  - dpkg –add-architecture i386
  - apt-get update

- apt-get install libc6:i386

[NSNET-14602]

- Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

  [NSNET-5233]

- Il est possible que l'appliance NetScaler ne génère pas de messages d'interruption SNMP « Cold-Start » après un redémarrage à froid.

  [NSHELP-27917]

- Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

  [NSHELP-21082]

Plateforme

- Certains packages python ne sont pas installés lorsque vous rétrogradez l'appliance NetScaler de la version 13.1-4.x et des versions supérieures vers l'une des versions suivantes :
  - Toute version 11.1
  - 12.1-62.21 et versions antérieures
  - 13.0-81.x et versions antérieures

  [NSPLAT-21691]

- Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande « rm cloudprofile » pour supprimer le profil.

  [NSPLAT-4520]

- Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
  Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

  [NSPLAT-4451]

- L'appliance NetScaler se bloque si le VRID est lié à un canal LA dont aucune interface membre n'est configurée.

  Solution : configurez les interfaces membres pour un canal LA avant de lier le VRID au canal LA.

  [NSPLAT-26707]

Stratégies

- Les connexions peuvent être bloquées si la taille du traitement des données est supérieure à la taille de la mémoire tampon TCP par défaut configurée.

  Solution : définissez la taille de la mémoire tampon TCP sur la taille maximale des données à traiter.

  [NSPOLICY-1267]

SSL

- Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

  Solution :

  1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
  2. Enregistrez la configuration.

  [NSSSL-9572]

- Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

  [NSSSL-6478]

- Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

  [NSSSL-6213]

- Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
  ERROR: crl refresh disabled

  [NSSSL-6106]

- L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

[NSSSL-4427]

- Un message d'avertissement incorrect, « Avertissement : aucun chiffrement utilisable configuré sur le serveur/service SSL » s'affiche si vous essayez de modifier le protocole ou le chiffrement SSL dans le profil SSL.

  [NSSSL-4001]

- Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

  [NSSSL-3184, NSSSL-1379, NSSSL-1394]

Système

- Un RTT élevé est observé pour une connexion TCP si la condition suivante est remplie :
  - une fenêtre de congestion maximale élevée (> 4 Mo) est définie
  - L'algorithme TCP NILE est activé

  Pour qu'une appliance NetScaler utilise l'algorithme NILE pour le contrôle de la congestion, les conditions doivent dépasser le seuil de démarrage lent, qui est associé à la fenêtre de congestion maximale

  Ainsi, jusqu'à ce que la fenêtre de congestion maximale configurée soit atteinte, NetScaler continue d'accepter des données et se retrouve avec un RTT élevé.

  [NSHELP-31548]

- La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client .

  [NSHELP-21240]

- Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

  [NSHELP-10972]

- Dans de rares cas, les flux créés avant la création du flux WebSocket HTTP/2 peuvent être interrompus lorsque la connexion côté serveur du WebSocket se ferme.

  Ce problème se produit car l'appliance NetScaler ne prend pas en charge le multiplexage des connexions pour HTTP/2 WebSocket.

  Solution : désactivez le multiplexage des connexions pour le profil HTTP2 associé à l'aide de la commande suivante :


```
“set httpProfile <name> [-conMultiplex (                DISABLED )]”
ENABLED
```

[NSBASE-17449]

- Dans un déploiement de cluster, si vous exécutez la commande « forcer la synchronisation du cluster » sur un nœud non CCO, le fichier ns.log contient des entrées de journal dupliquées.

  [NSBASE-16304, NSGI-1293]

- Lorsque vous installez NetScaler ADM sur un cluster Kubernetes, cela ne fonctionne pas comme prévu car les processus requis peuvent ne pas s’exécuter.

  Solution : redémarrez le module Gestion.

  [NSBASE-15556]

- L’adresse IP du client et l’adresse IP du serveur sont inversées dans l’enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

  [NSBASE-8506]

Interface utilisateur

- Dans l’interface graphique de NetScaler, le lien « Aide » présent sous l’onglet « Tableau de bord » est cassé.

  [NSUI-14752]

- L’assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

  Solution : configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l’aide de l’interface graphique ou de l’interface de ligne de commande NetScaler.

  [NSUI-13024]

- Si vous créez une clé ECDSA à l’aide de l’interface graphique, le type de courbe n’est pas affiché.

  [NSUI-6838]

- Dans une configuration à haute disponibilité des appliances NetScaler BLX, le nœud principal peut ne plus répondre en bloquant toute demande de CLI ou d’API.

  Solution : redémarrez le nœud principal.

  [NSCONFIG-6601]

- Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

  1. Mettez à niveau l'appliance NetScaler vers l'une des versions
     - 13.0 52.24 build
     - 12.1 57.18 build
     - 11.1 65.10 build
  2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
  3. Rétrogradez l'appliance NetScaler vers une version antérieure.

  Pour afficher la liste de ces utilisateurs du système à l'aide de l'interface de ligne de commande : À l'invite de commandes, tapez :

  ```
  query ns config -changedpassword [-config <full path of the configuration
   file (ns.conf)>]
  ```

  Solution : Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

  - Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
  - Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
  - Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

  Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html.

  [NSCONFIG-3188]

Notes de publication pour la version 13.1-42.47 de NetScaler

June 20, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1-42.47 de NetScaler.

Remarques

- Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

Nouveautés

Les améliorations et modifications disponibles dans la version 13.1-42.47.

Gestion des bots

- **Support pour arrêter les téléchargements de réputation IP dans les paramètres du bot**

  Après avoir désactivé la fonctionnalité de réputation IP, définissez le **profil non intrusif par défaut** sur **BOT_BYPASS dans les paramètres de gestion des bots** NetScaler. Cette configuration arrête les téléchargements de réputation IP.

  Pour modifier les paramètres de gestion des robots, accédez à **Sécurité > Gestion des robots NetScaler > Modifier les paramètres de gestion des robots NetScaler.**

  [NSBOT-1050, NSHELP-34310, NSHELP-33835, NSHELP-34410]

- **De nouvelles violations de bots apparaissent dans l'interface graphique de NetScaler ADM**

  Les violations de bot suivantes ont récemment été introduites dans l'interface graphique de NetScaler ADM :

  - Aucun en-tête d'agent utilisateur
  - En-têtes d'agent utilisateur multiples

  Un serveur d'applications utilise les informations d'en-tête de l'agent utilisateur pour en savoir plus sur une demande entrante. Certaines demandes de bot peuvent avoir plusieurs en-têtes d'agent utilisateur ou aucun en-tête d'agent utilisateur. Vous pouvez détecter ces violations de bots à l'aide d'un profil de gestion des bots NetScaler. Utilisez ensuite l'interface graphique NetScaler ADM pour surveiller les violations commises par les robots. Pour plus d'informations, consultez la section Catégories de violations.

  [NSBOT-1023]

Appliance NetScaler SDX

- **La prise en charge du SD-WAN est obsolète dans le service de gestion**

  À partir de la version 13.1 build 42.x et des versions ultérieures, la prise en charge du SD-WAN est supprimée par l'appliance NetScaler SDX.

  [NSSVM-5465]

- **Les champs « Gateway » et « Nexthop » sont facultatifs lors du provisionnement ou de la modification du VPX**

  Dans un service de gestion d'appliances NetScaler SDX, les champs `Gateway` et `Nexthop` ne sont plus obligatoires pour le provisionnement, la modification, la sauvegarde ou la restauration de VPX lorsque les conditions suivantes sont remplies :

  - L'une des options suivantes est vraie :
    - L'option « Gérer via le réseau interne » est activée pour VPX.
    - L'adresse IP VPX se trouve dans le même sous-réseau que l'adresse IP du service de gestion.
  - VPX est fourni avec la version 13.0-88.9 ou 13.1-37.8 et leurs versions supérieures.

  Pour plus d'informations, consultez Provisionner des instances NetScaler.

  [NSSVM-5307]

NetScaler Gateway

- **Possibilité d'activer la propagation des bits DF pour EDT par défaut**

  Sur l'appliance NetScaler Gateway, l'option PMTUD (EDT path Maximum Transmission Unit Discovery) est désormais activée par défaut pour appliquer les bits DF. Cette option empêche la fragmentation EDT qui pourrait entraîner une dégradation des performances ou l'échec de l'établissement d'une session. Auparavant, cette option était désactivée par défaut. Les administrateurs devaient activer l'option à l'aide des paramètres ICA.

  [CGOP-22615]

Web App Firewall NetScaler

- **Utilisez l'interface de ligne de commande ou l'API pour activer les signatures dans votre NetScaler Web App Firewall**

  Vous pouvez désormais activer les signatures individuelles dans votre NetScaler Web App Firewall via des commandes CLI ou des appels d'API. Pour ce faire, sélectionnez les signatures en fonction de leur identifiant ou de leur catégorie, puis définissez des actions. Auparavant, vous pouviez activer les signatures uniquement en chargeant un fichier de signature.

  Example-1:

  ```
  import appfw signature DEFAULT object_name -sigRuleId 1001 9882 2000
  1250 810 -Enabled ON -Action LOG BLOCK
  ```

  Exemple-2 :

  ```
  import appfw signature DEFAULT object_name -sigCategory web-misc -
  Enabled ON -Action LOG BLOCK
  ```


Voir, Pour ajouter des signatures individuelles à l'aide de la CLI.

[NSWAF-9333]

- **Nouveaux modèles de correspondance pour les signatures du NetScaler Web App Firewall**

  Pour les signatures du NetScaler Web App Firewall, vous pouvez désormais sélectionner les nouveaux modèles de correspondance suivants :

  - Injection de commande
  - Grammaire des injections SQL
  - Grammaire de l'injection de commandes

  Le NetScaler Web App Firewall recherche le modèle sélectionné et classe l'attaque par catégorie.

  Remarque : Vous pouvez modifier les modèles de règles de signature uniquement pour les signatures personnalisées.

  Pour plus d'informations, consultez la section Ajouter des modèles de règles de signature.

  [NSWAF-9280]

- **Configurer des listes globales pour contourner le WAF ou refuser les demandes**

  Vous pouvez désormais configurer des listes globales dans un profil NetScaler Web App Firewall pour contourner le Web App Firewall ou refuser des demandes. Si les demandes entrantes correspondent à la liste de contournement globale, elles ignorent le Web App Firewall dans NetScaler. Si les demandes entrantes correspondent à la liste de refus globale, NetScaler Web App Firewall bloque ces demandes et applique l'action définie.

  Les listes de contournement et de refus prennent en charge les adresses URL, IPv4 et IPv6. Vous pouvez les spécifier à l'aide de littéraux, de PCRE et d'expressions. Pour plus d'informations, consultez Gérer les listes globales pour contourner le WAF ou refuser les demandes.

  [NSWAF-8981]

- **Simplification de la création du profil NetScaler Web App Firewall pour protéger contre les CVE**

  Protégez votre appliance NetScaler en appliquant une signature appropriée dans le NetScaler Web App Firewall. Vous souhaiterez peut-être protéger l'appliance contre les CVE sans effectuer d'autres contrôles de sécurité. Dans ce cas, vous pouvez désormais créer un profil qui désactive les vérifications restantes à partir du NetScaler Web App Firewall.

  Dans un profil NetScaler Web App Firewall, sélectionnez l'option **CVE** par défaut. Avec cette option, il vous suffit d'ajouter et de lier une signature. Il désactive automatiquement les contrôles restants. Auparavant, vous deviez désactiver manuellement les contrôles de sécurité du profil un par un.

  Pour plus d'informations, consultez la section Création de profils de Web App Firewall.

[NSWAF-8970]

Plate-forme

- **Support pour VMware vSphere 8.0.0b**

  L'instance NetScaler VPX prend désormais en charge VMware vSphere 8.0.0b (build 20513097).

  [NSPLAT-25844]

- **Prise en charge de plusieurs services avec le même groupe Autoscaling dans le cloud public**

  Pour la fonctionnalité d'autoscaling principale dans le cloud public, l'instance NetScaler VPX prend désormais en charge plusieurs services avec le même groupe d'autoscaling. Cette fonctionnalité est prise en charge sur les clouds Azure, AWS et GCP. Dans l'interface graphique de NetScaler, vous pouvez créer différents profils de cloud pour différents services (en utilisant différents ports) avec le même groupe d'autoscaling dans le cloud.

  Auparavant, la prise en charge des instances NetScaler VPX était limitée à un seul service par groupe d'autoscaling. Vous avez dû ajouter différents groupes de mise à l'échelle automatique pour différents services.

  [NSPLAT-21596]

- **Support pour la carte réseau Mellanox ConnectX-4 avec SR-IOV sur l'hyperviseur VMware ESXi**

  L'instance NetScaler VPX prend désormais en charge la carte réseau Mellanox ConnectX-4 avec SR-IOV sur l'hyperviseur VMware ESXi.

  [NSPLAT-20295]

Stratégies

- **Augmentation de la limite de modèles pouvant être liés à un ensemble de modèles**

  Dans une appliance NetScaler, vous pouvez désormais lier 50 000 modèles à un ensemble de modèles. Avec le fichier de jeu de modèles, seuls 10 000 modèles peuvent être liés à un jeu de modèles. De plus, si le jeu de modèles est utilisé pour le streaming, seuls 5 000 modèles peuvent être liés à cet ensemble de modèles. Un modèle défini pour le streaming est utilisé dans le paramètre de recherche de l'action de réécriture, le corps HTTP ou l'expression basée sur la charge utile TCP. Auparavant, vous ne pouviez lier que 5 000 modèles à un jeu de modèles.

  [NSPOLICY-2733]

- **Prise en charge de toutes les expressions associées aux en-têtes et aux charges utiles UDP côté client et côté serveur**

Les améliorations suivantes sont apportées aux en-têtes et aux charges utiles UDP côté client et côté serveur :

- Les expressions associées au protocole UDP sont divisées en expressions côté client et côté serveur.
- Auparavant, la prise en charge n'était disponible que pour les expressions côté client et les mêmes expressions étaient utilisées pour le côté serveur.
- Le protocole UDP prend désormais en charge les expressions côté serveur. Cette expression peut être utilisée pour extraire le port source UDP, le port de destination, la longueur, la somme de contrôle et la charge utile.
- Les expressions côté client sont également améliorées pour extraire la longueur, la somme de contrôle et la charge utile d'un paquet UDP donné.
- Pour des raisons de rétrocompatibilité, si une expression côté client est utilisée côté serveur, elle continue d'être prise en charge. Citrix vous recommande d'utiliser les expressions côté serveur pour le côté serveur.

Pour plus d'informations, consultez la section Expressions pour les données TCP, UDP et VLAN.

[NSPOLICY-1829]

SSL

- **Prise en charge de la validation des certificats à signature croisée**

  L'appliance NetScaler prend désormais en charge la validation des certificats à signature croisée. Si un certificat est signé par plusieurs émetteurs, la validation est réussie s'il existe au moins un chemin valide vers le certificat racine.

  Auparavant, si l'un des certificats de la chaîne de certificats était signé de manière croisée et comportait plusieurs chemins d'accès au certificat racine, l'appliance ADC ne recherchait qu'un seul chemin. Et si ce chemin n'était pas valide, la validation échouait.

  [NSSSL-11259]

Système

- **Prise en charge de l'exportation de métriques directement vers Prometheus depuis l'appliance NetScaler**

  NetScaler prend désormais en charge l'exportation directe des métriques vers Prometheus. Grâce à cette fonctionnalité, Prometheus extrait les métriques directement des instances NetScaler sans avoir besoin d'un exportateur externe. Auparavant, une ressource d'exportation était requise en dehors de l'appliance pour exporter les métriques de NetScaler vers le serveur Prometheus.

Pour plus d'informations, consultez la section Surveillance de NetScaler et des applications à l'aidede Prometheus.

[NSBASE-17100]

Interface utilisateur

- **Support d'une limite de téléchargement de 8 Mo pour l'API `systemfile` NITRO**

  La limite de téléchargement maximale pour l'API `systemfile` NITRO a été augmentée de 2 Mo à 8 Mo.

  [NSCONFIG-7089]

- **Prise en charge des valeurs numériques de 64 bits dans les réponses de l'API NITRO**

  Auparavant, l'appliance NetScaler renvoyait un entier non signé ou une valeur de type de propriété long sous forme de chaîne dans la réponse de l'API NITRO car la réponse entière n'était pas prise en charge pour ces types. En outre, l'appliance a renvoyé une valeur stats-counter rate de type double sous la forme d'un entier.

  Les API NITRO prennent désormais en charge les entiers 64 bits. Cette prise en charge permet à l'appliance de renvoyer les informations suivantes dans les réponses de l'API NITRO :

  - la valeur entière exacte au lieu d'une chaîne pour un type de données entier non signé ou entier long.
  - la valeur de contre-taux sérialisée exacte au lieu d'un entier.

  Un nouveau paramètre de requête `largeintsupport` a été introduit pour activer la prise en charge des entiers 64 bits dans les API NITRO.

  Lorsque cette valeur `largeintsupport` est définie `yes` dans une demande d'API NITRO, l'appliance NetScaler renvoie la valeur entière exacte, dans la réponse de l'API NITRO. La fonctionnalité précédente est conservée lorsqu'elle `largeintsupport` est définie sur `no`, qui est également le paramètre par défaut.

  [NSCONFIG-5399]

Problèmes résolus

Les problèmes résolus dans la version 13.1-42.47.

Authentification, autorisation et audit

- Lorsqu'une appliance NetScaler est mise à niveau, les utilisateurs ne peuvent pas accéder à l'appliance NetScaler à l'aide de l'authentification RADIUS.

[NSHELP-33200]

- Sur l'interface graphique de NetScaler, la section **Stratégies de réponse** de la page **Serveur virtuel d'authentification** n'affiche pas les stratégies de cache du type de répondeur.

  [NSHELP-33111]

- L'authentification de passerelle via un client CWA ou des clients VPN natifs peut échouer en raison de chaînes manquantes dans le `ns_aaa_relaystate_param_whitelist` patset.

  [NSHELP-33054]

- L'usurpation d'identité SSO Kerberos avec des types de chiffrement avancés peut échouer lorsqu'un nom d'utilisateur principal incorrect est utilisé dans les informations d'identification SSO.

  [NSHELP-32890, NSHELP-34087]

Gestion des bots

- L'appliance NetScaler se bloque lors du traitement d'une signature de bot si le format du fichier de signature n'est pas valide.

  [NSHELP-33690]

- Dans l'interface utilisateur graphique de NetScaler, la signature du bot définie par l'utilisateur affiche une version de base incorrecte.

  [NSHELP-33546]

Appliance NetScaler SDX

- Lorsque vous mettez à niveau une appliance NetScaler SDX, dans de rares cas, l'événement incorrect suivant apparaît dans l'interface graphique du service de gestion :

  « La version SVM et la version Hypervisor ne sont pas compatibles »

  [NSHELP-32949]

NetScaler Gateway

- Un dispositif NetScaler Gateway se bloque lors de l'évaluation d'une stratégie pour une URL VPN.

  [NSHELP-33683, CGOP-20369, NSHELP-34002, NSHELP-34030, NSHELP-34052, NSHELP-34076, NSHELP-34077, NSHELP-34100, NSHELP-34151, NSHELP-34180, NSHELP-34243, NSHELP-34276, NSHELP-34327, NSHELP-34402]

- Après la mise à niveau d'une appliance NetScaler, les URL du proxy RDP ne fonctionnent pas avec le thème du portail X1 et le message « Objet Http/1.1 Not Found » s'affiche.

  [NSHELP-33676, NSHELP-33845, NSHELP-33921, NSHELP-34032]

- Lorsqu'une appliance NetScaler est mise à niveau, elle peut se bloquer lors du traitement du trafic UDP.

  [NSHELP-33417, NSHELP-34031]

- Après la mise à niveau d'une appliance NetScaler, les URL du proxy RDP deviennent inaccessibles et le message d'erreur « Http/1.1 Object Not Found » s'affiche. Ce problème se produit lorsque les paramètres personnalisés des URL RDP contiennent des espaces.

  [NSHELP-33333]

- Dans une configuration de haute disponibilité de NetScaler Gateway, les appliances principale et secondaire peuvent tomber en panne lors d'un basculement.

  [NSHELP-33198, NSHELP-33483]

- Certaines sessions VPN peuvent être effacées ou supprimées de l'appliance ADC secondaire après un basculement.

  [NSHELP-33125]

- L'appliance NetScaler Gateway peut se bloquer si HDX Insight est activé et qu'un utilisateur se connecte à StoreFront immédiatement après s'être déconnecté.

  [NSHELP-32907, NSHELP-33079, NSHELP-33289]

- Dans de rares cas, l'appliance NetScaler peut se bloquer lors de l'extraction d'un moniteur STA dans le cadre d'un déploiement VPN.

  [NSHELP-32893]

- Après la mise à niveau d'une appliance NetScaler Gateway, la section Configuration > Intégrer aux produits NetScaler ne s'affiche pas dans l'interface graphique de NetScaler.

  [NSHELP-32335]

- L'analyse EPA visant à vérifier le certificat CA d'un appareil client échoue sur l'appliance NetScaler lorsque les certificats CA appartiennent à des domaines différents.

  [NSHELP-32118]

- Le plug-in Citrix EPA pour macOS se bloque lorsque GSLB est activé sur une appliance NetScaler.

  [CGOP-22722]

Web App Firewall NetScaler

- Dans le pare-feu NetScaler Web App, lorsque vous activez le streaming et les contrôles de cohérence sur le terrain, cela retarde le transfert de la charge utile vers le serveur d'origine. Par conséquent, la méthode POST pour la charge utile échoue.

  [NSHELP-33700]

- La redirection de piratage de cookie supprime les paramètres de requête de l'URL de la demande. Par conséquent, la demande redirigée peut échouer.

  [NSHELP-33633, NSHELP-33812]

Équilibrage de charge

- Le nœud secondaire risque de se bloquer si vous utilisez le même serveur virtuel GSLB comme sauvegarde pour plusieurs serveurs virtuels GSLB.

  [NSHELP-33400, NSHELP-34247]

- L'appliance NetScaler ne répond pas avec l'adresse IP de service correcte pour la requête de domaine GSLB si les paramètres suivants sont configurés sur le serveur virtuel GSLB :

  1. L'option ECS est activée.
  2. La proximité statique est configurée comme méthode d'équilibrage de charge.

  [NSHELP-32879]

Réseau

- Dans une configuration haute disponibilité en mode INC, en cas de non-correspondance entre les versions HA, le nœud secondaire peut apprendre des itinéraires non valides à partir du nœud principal.

  [NSHELP-33948]

- Dans une appliance NetScaler avec le routage OSPF configuré, la route par défaut n'est pas installée même lorsque la route par défaut OSPF LSA est présente.

  [NSHELP-33070]

- Certains paquets entrants `nstrace` d'une session SSH peuvent afficher de manière incorrecte un numéro d'interface de réception et un identifiant VLAN différents lorsque toutes les conditions suivantes sont remplies :

  - Les routes ECMP pour le client de la session SSH sont présentes sur l'appliance NetScaler.
  - La session SSH est inactive pendant quelques secondes.

  [NSHELP-32734]

- Le chargement du fichier SNMP MIB vers un outil Network Morning peut échouer car le nom du piège SNMP indiqué `dataStreamRateLimitHit` dans le fichier n'est pas en majuscule.

  [NSHELP-32634]

- Dans une configuration NAT 64 à grande échelle, l'appliance NetScaler peut se bloquer en raison d'un problème de non-correspondance interne du moteur de paquets.

  [NSHELP-31985]

- Dans une configuration GSLB où l'une des adresses IP du site GSLB est configurée dans une partition d'administration, les demandes ARP pour cette adresse IP de site GSLB provenant de routeurs en amont n'atteignent pas la partition d'administration. Ce problème se produit lorsque toutes les conditions suivantes sont remplies :

  - Un VLAN partagé est lié à la partition d'administration.
  - Une adresse IP SNIP, par exemple SNIP-1, située dans le même sous-réseau que l'adresse IP du site GSLB est présente sur le VLAN partagé.
  - Une autre adresse IP SNIP, par exemple SNIP-2, dans le même sous-réseau que l'adresse IP du site GSLB est ajoutée et SNIP-1 est supprimée.

  [NSHELP-30552]

Plate-forme

- Pour un NetScaler VPX version 13.1 build 37.38 sur un hyperviseur VMware ESX avec interfaces VMXNET3, vous pouvez observer le comportement suivant dans la configuration HA :

  La paire NetScaler VPX HA n'est pas configurée car la communication entre les nœuds HA n'est pas établie. Par conséquent, l'état du nœud homologue est affiché comme INCONNU.

  [NSPLAT-25677]

- Lorsque vous fournissez des données utilisateur avant le démarrage dans un modèle OVF à partir du client ESX vSphere, l'hôte ESXi n'applique pas la configuration préalable au démarrage.

  [NSPLAT-24233, NSPLAT-25551]

- La résolution DNS échoue si vous configurez plus de trois noms de serveurs DNS dans l'option DHCP définie dans AWS VPC. Ce problème se produit dans les instances NetScaler VPX dont les versions sont antérieures à la version 13.1 build 42.x.

  [NSHELP-33171]

- Sur la plate-forme NetScaler SDX 8015/8400/8600, vous pouvez constater une augmentation de la consommation de mémoire sur Xen Server.

  [NSHELP-32260]

- Vous pouvez rencontrer des blocages de transmission sur une appliance NetScaler SDX dotée d'une interface 10G lorsqu'un trafic important est envoyé sur cette interface.

  [NSHELP-31232]

SSL

- Un serveur virtuel se bloque en raison de l'échec d'une connexion TLS1.3, car l'appliance NetScaler manque de mémoire et une demande d'allocation de mémoire échoue lors du démarrage d'une liaison TLS 1.3.

  Avec ce correctif, la connexion TLS 1.3 échoue mais l'appliance ne se bloque pas.

  [NSSSL-12200]

- Un serveur virtuel peut mettre fin de manière incorrecte à une prise de contact TLS 1.3 avec une `decrypt_error` alerte si les conditions suivantes sont remplies :

  - Le client s'authentifie à l'aide d'un certificat.
  - Le serveur virtuel est configuré pour effectuer une vérification de l'état du certificat à l'aide d'un OCSP ou d'une CRL.
  - Le client envoie des messages Certificate et CertificateVerify dans le même enregistrement TLS.

  [NSHELP-33355]

- Après avoir dissocié le chiffrement DEFAULT, lorsque vous désactivez une version de protocole sur un serveur virtuel et que vous essayez ultérieurement de lier un chiffrement avec ce protocole répertorié dans la description, le message d'erreur suivant s'affiche.

  `No usable ciphers configured on the SSL vserver/service`

  Ce message est incorrect car le chiffrement est pris en charge par d'autres protocoles activés sur le serveur virtuel. Par exemple,

  Nom du chiffrement : TLS1-ECDHE-RSA-AES256-SHA
  Description : SSLv3 Kx=ECC-DHE Au=RSA Enc=AES(256) Mac=SHA1 HexCode=0xc014

  Ce chiffrement est pris en charge pour tous les protocoles à partir de SSLv3 (SSLv3, TLS1, TLS11, TLS12). Lorsque vous désactivez SSLv3 sur un serveur virtuel, puis que vous essayez de lier ce chiffrement à ce serveur virtuel, l'avertissement s'affiche même si les protocoles TLS1, TLS11 et TLS12 sont toujours activés sur le serveur virtuel.

  Avec ce correctif, l'avertissement s'affiche uniquement lorsqu'aucun chiffrement n'est pris en charge pour la configuration.

  [NSHELP-32739]

- L'appliance NetScaler n'autorise pas la configuration de certificats antérieurs à `notBefore date` 1970.

  [NSHELP-32677]

- L'appliance NetScaler peut se bloquer si les conditions suivantes sont remplies :
  - Un client envoie les premières données de TLS1.3 dans le message Client Hello à un serveur virtuel SSL Insight.
  - Les chiffrements ECDHE sont activés sur ce serveur virtuel.

  [NSHELP-31560]

Système

- Les applications client qui ne sont pas conformes à la norme RFC (RFC 7230) peuvent échouer après une mise à niveau vers NetScaler 13.1. Cet échec est dû à un contrôle de conformité obligatoire appliqué à l'appliance NetScaler afin de se conformer à la RFC 7230.

  Dans le cadre du correctif, cette vérification de conformité spécifique est déplacée sous le paramètre de profil HTTP « -MarkRFC7230NoncompliantInval ».**“** Les clients peuvent désactiver ce contrôle de conformité qui était précédemment appliqué.

  [NSHELP-34046]

- Une appliance NetScaler peut se bloquer lorsque les deux conditions suivantes sont remplies :
  - Le dispositif d'inspection du contenu envoie une réponse de réinitialisation (RST) à l'appliance ADC et l'une des ressources du système de prévention des intrusions (IPS) n'est pas correctement effacée.
  - La même ressource IPS est accessible lors de transactions ultérieures.

  [NSHELP-33691]

- Dans certains cas, une appliance NetScaler peut se bloquer lors du traitement d'un accusé de réception correctif envoyé par une connexion au serveur dont l'état est TIME_WAIT.

  [NSHELP-33469]

- Une appliance NetScaler peut se bloquer lorsqu'elle essaie d'accéder à des ressources sur l'ICAP libéré. Cette condition se produit lorsque l'ICAP est en mode de modification de réponse (RESPMOD).

  [NSHELP-33403]

- L'appliance NetScaler n'est pas en mesure d'envoyer des données Logstream depuis des partitions de manière cohérente.

  [NSHELP-33237]

- L'appliance NetScaler abandonne la connexion lorsqu'elle ne parvient pas à analyser la valeur fragmentée. Ce problème se produit lorsque l'en-tête Transfer-Encoding comporte plusieurs valeurs et que Chunked n'est pas la première valeur.

  [NSHELP-32420]

- L'appliance NetScaler peut se bloquer si elle traite un paquet ACK correctif lié à une connexion TCP côté serveur.

  [NSHELP-32290]

- L'appliance NetScaler configurée avec un service SSL se bloque lorsqu'elle reçoit un paquet de contrôle TCP FIN suivi d'un paquet de contrôle TCP RESET.

  [NSHELP-31656]

Interface utilisateur

- Lorsque vous créez un profil NetScaler Web App Firewall de type JSON et que vous essayez de mettre à jour les **paramètres du profil**, l' **objet d'erreur JSON** affiche une liste vide.

  [NSUI-18453]

- Un compte utilisateur système lié à un ensemble de partitions d'administration peut ne pas être en mesure d'accéder à la partition par défaut via les API NITRO, même si l'option Autoriser la partition par défaut est activée dans le cadre des paramètres globaux du système.

  [NSHELP-33990]

- Le lien vers les profils de gestion des robots NetScaler s'affiche de manière incorrecte sur la page **Gestion du trafic > Commutation de contenu** . Lorsque vous cliquez sur ce lien, une page blanche s'affiche. Ce problème se produit si vous liez une stratégie de bot au serveur virtuel de commutation de contenu.

  [NSHELP-33697]

- La connexion à l'interface graphique de NetScaler échoue si votre nom d'utilisateur ou votre nom de domaine comporte un caractère spécial.

  [NSHELP-33684]

- Lorsque vous effacez les configurations NetScaler en cours d'exécution, la session de gestion NetScaler créée par une configuration TACACS classique est déconnectée même lorsque le `RBAconfig` paramètre est défini sur NON.

  [NSHELP-33655]

- Lorsqu'un utilisateur consulte la liaison dans une stratégie de commutation de contenu, les détails du serveur virtuel de commutation de contenu ne s'affichent pas sur la même ligne sous **Afficher les liaisons**.

[NSHELP-33149]

- **Prise en charge de l'option de mise hors tension dans l'API NITRO d'arrêt**

  L'API `shutdown` NITRO prend désormais en charge l'option « -p now » pour arrêter et éteindre une appliance NetScaler.

  Exemple :

  Dans l'exemple suivant de requête curl, l'API `shutdown` NITRO est utilisée avec l'option « -p now » pour arrêter et éteindre une appliance NetScaler dont l'adresse IP est 192.0.0.33.

  'curl -v -X POST -H Content-Type: application/json -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/install?warning=yes -d '{"shutdown": {"args":"-p now"}}'

  [NSHELP-32915]

- Après avoir créé un profil pour NetScaler Web App Firewall et essayé de générer le rapport de configuration du pare-feu d'applications dans **Système > Rapports**, l'erreur suivante s'affiche :

  « Impossible de charger le document PDF. »

  [NSHELP-32469]

- Dans la configuration du cluster, l'option TFTP n'est pas affichée dans la liste des protocoles lors de la création d'un serveur virtuel à l'aide de l'interface graphique NetScaler.

  [NSHELP-32036]

- Sur l'interface graphique de NetScaler, la page Fichiers journaux du système (Configuration > Système > Audit > Messages Syslog) et la page Journaux (Configuration > Authentification > Journaux) ne parviennent pas à charger les fichiers journaux.

  [NSHELP-30868]

- Sur l'interface graphique de NetScaler, l'écran Configuration enregistrée ou en cours d'exécution (Système > Diagnostics) affiche de manière incorrecte les balises HTML au lieu d'afficher du texte brut.

  [NSHELP-27169]

- Lors de l'affichage des stratégies liées à une étiquette de stratégie de commutation de contenu dans l'interface graphique de NetScaler, seules 25 stratégies sont affichées, même si d'autres stratégies sont liées à cette étiquette de stratégie.

  [NSHELP-23428]

Problèmes connus

Les problèmes qui existent dans la version 13.1-42.47.

AppFlow

- HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

  [NSINSIGHT-943]

Authentification, autorisation et audit

- Les administrateurs ne peuvent pas effectuer de journalisation personnalisée des échecs d'authentification dus à des informations d'identification non valides. Ce problème se produit car les stratégies du répondeur NetScaler ne détectent pas les erreurs liées aux échecs de connexion.

  [NSAUTH-11151]

- Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante. `show adfsproxyprofile <profile name>`

  Solution : Connectez-vous au principal NetScaler actif du cluster et exécutez la commande. `show adfsproxyprofile <profile name>` Il afficherait l'état du profil proxy.

  [NSAUTH-5916]

- La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

  - L'option Tester l'accessibilité LDAP est ouverte.
  - Les informations d'identification de connexion non valides sont renseignées et envoyées.
  - Les identifiants de connexion valides sont renseignés et envoyés.

  Solution : fermez et ouvrez l'option Tester l'accessibilité LDAP.

  [NSAUTH-2147]

Appliance NetScaler SDX

- Des pertes de paquets sont visibles sur une instance VPX hébergée sur une appliance NetScaler SDX si les conditions suivantes sont remplies :

  - Le mode d'allocation du débit est en rafale.
  - Il existe une grande différence entre le débit et la capacité maximale de rafale.

  [NSHELP-21992]

NetScaler Gateway

- Si les valeurs de registre associées à Citrix Secure Access sont supérieures à 1 500 caractères, le collecteur de journaux ne parvient pas à recueillir les journaux d'erreurs.

  [NSHELP-33457]

- Lorsque vous utilisez le pilote Windows Filtering Platform (WFP), l'accès à l'intranet ne fonctionne parfois pas une fois le VPN reconnecté.

  [NSHELP-32978]

- Le client Citrix Secure Access, version 21.7.1.2 et versions ultérieures, ne parvient pas à effectuer la mise à niveau vers des versions ultérieures pour les utilisateurs ne disposant pas de droits d'administration. Ce problème s'applique uniquement si la mise à niveau du client Citrix Secure Access est effectuée à partir d'une appliance NetScaler.

  [NSHELP-32793]

- Lorsque les utilisateurs cliquent sur l'onglet Page d'accueil de l'écran Citrix Secure Access pour Windows, la page affiche l'erreur de refus de connexion.

  [NSHELP-32510]

- Sur un appareil Mac utilisant Chrome, l'extension VPN se bloque lors de l'accès à deux noms de domaine complets.

  [NSHELP-32144]

- Dans certains cas, si les paramètres de proxy sont vides dans NetScaler Gateway version 13.0 ou 13.1, Citrix SSO crée des paramètres de proxy incorrects.

  [NSHELP-31970]

- Le contrôle de journalisation des débogues pour le client Citrix Secure Access est désormais indépendant de NetScaler Gateway et peut être activé ou désactivé depuis l'interface utilisateur du plug-in pour la machine et le tunnel utilisateur.

  [NSHELP-31968]

- Les connexions directes aux ressources situées en dehors du tunnel établi par Citrix Secure Access peuvent échouer en cas de retard ou de congestion important.

  [NSHELP-31598]

- Le message personnalisé du journal des défaillances EPA ne s'affiche pas sur le portail NetScaler Gateway. Au lieu de cela, le message « erreur interne » s'affiche.

  [NSHELP-31434]

- Parfois, l'ouverture de session automatique de Windows ne fonctionne pas lorsqu'un utilisateur se connecte à l'ordinateur Windows en mode de service permanent. Le tunnel de la machine ne

passe pas au tunnel utilisateur et au message « Connexion… » s'affiche dans l'interface utilisateur du plug-in VPN.

[NSHELP-31357, CGOP-21192, NSHELP-34211]

- Lorsque Always on est configuré, le tunnel utilisateur échoue en raison du numéro de version incorrect (1.1.1.1) dans le fichier aoservice.exe.

  [NSHELP-30662]

- Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil « NetworkAccessOnVPNFailure » de « FullAccess » à « OnlyToGateway ».

  [NSHELP-30236]

- La page d'accueil de la passerelle ne s'affiche pas immédiatement après que le plug-in de passerelle a réussi à établir le tunnel VPN. Pour résoudre ce problème, la valeur de registre suivante est introduite.

  HKLMSoftwareCitrixSecure Access ClientSecureChannelResetTimeoutSeconds
  Type: DWORD

  Par défaut, cette valeur de registre n'est ni définie ni ajoutée. Lorsque la valeur de « SecureChannelResetTimeoutSeconds » est 0 ou n'est pas ajoutée, le correctif pour gérer le délai ne fonctionne pas, ce qui est le comportement par défaut. L'administrateur doit définir ce registre sur le client pour activer le correctif (c'est-à-dire afficher la page d'accueil immédiatement après que le plug-in de passerelle ait établi le tunnel VPN avec succès).

  [NSHELP-30189]

- Le client VPN Windows n'honore pas l'alerte « Notification de fermeture SSL » du serveur et envoie la demande de connexion de transfert sur la même connexion.

  [NSHELP-29675]

- L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

  [NSHELP-28551]

- Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

  [NSHELP-28404]

- Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

  - L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
  - L'appliance est configurée pour une authentification basée sur des certificats avec l'authentification à deux facteurs « désactivée »

[NSHELP-23584]

- Parfois, lorsque vous parcourez les schémas, le message d'erreur « Impossible de lire le type de propriété non défini » apparaît.

  [NSHELP-21897]

- Dans une configuration de cluster NetScaler, HDX Insight et Gateway Insight ne peuvent pas être activés simultanément.

  [CGOP-23570]

- L'option du système d'exploitation Windows ne figure pas dans la liste déroulante Expression Editor pour les stratégies de pré-authentification et les actions d'authentification sur l'interface graphique de NetScaler. Toutefois, si vous avez déjà configuré l'analyse du système d'exploitation Windows sur une version précédente de NetScaler à l'aide de l'interface graphique ou de l'interface de ligne de commande, la mise à niveau n'a aucune incidence sur les fonctionnalités. Vous pouvez utiliser l'interface de ligne de commande pour apporter des modifications, si nécessaire.

  Solution :

  Utilisez les commandes CLI pour la configuration.

  - Pour configurer l'action EPA avancée dans l'authentification nFactor, utilisez la commande suivante.
    add authentication epaAction adv_win_scan -csecexpr "sys.client_expr("sys_0_WIN-OS_NAME_anyof_WIN-10[COMMENT: Windows OS]")"
  - Pour configurer une action de pré-authentification classique, utilisez les commandes suivantes.

    ```
    add aaa preauthenticationaction win_scan_action ALLOW
    add aaa preauthenticationpolicy win_scan_policy "CLIENT.SYSTEM('WIN-OS_NAME_anyof_WIN-10[COMMENT: Windows OS]')EXISTS"win_scan_action
    ```

  [CGOP-22966]

- Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

  [CGOP-19355]

- Le rapport Gateway Insight affiche de manière incorrecte la valeur « Local » au lieu de « SAML » dans le champ Type d'authentification en cas d'échec d'erreur SAML.

  [CGOP-13584]

- Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

  [CGOP-13511]

- Lorsqu'une connexion ICA est lancée à partir d'un Receiver MAC version 19.6.0.32 ou Citrix Virtual Apps and Desktops version 7.18, la fonctionnalité HDX Insight est désactivée.

  [CGOP-13494]

- Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

  [CGOP-13493]

- Lorsque vous acceptez les connexions hôtes locales depuis le navigateur, la boîte de dialogue Accepter la connexion pour macOS affiche du contenu en anglais, quelle que soit la langue sélectionnée.

  [CGOP-13050]

- Le texte « Page d'accueil » dans l' application Citrix SSO > Page d'accueil est tronqué pour certaines langues.

  [CGOP-13049]

- Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une stratégie de session depuis l'interface graphique de NetScaler.

  [CGOP-11830]

- Dans Outlook Web App (OWA) 2013, cliquez sur **Options** dans le menu Paramètres pour afficher une boîte de dialogue **d'erreur critique** . De plus, la page ne répond plus.

  [CGOP-7269]

Équilibrage de charge

- Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

  [NSLB-7679]

- Le format serviceGroupName dans l'interruption `entityofs` pour le groupe de services est le suivant :
  `<service(group)name>?<ip/DBS>?<port>`

  Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (« ? ») est utilisé comme séparateur. NetScaler envoie

l'interruption avec le point d'interrogation (« ? »). Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Divers

- Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, l'appliance exécute la commande `set urlfiltering parameter` dans le nœud secondaire.
  Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre « TimeOfDaytoUpdateDB ».

  [NSSWG-849]

- Le registre de liste AlwaysOnAllow ne fonctionne pas comme prévu si la valeur du registre est supérieure à 2000 octets.

  [NSHELP-31836]

- Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

  [NSHELP-22409]

Réseau

- Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

  [NSNET-25299]

- Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :

  - L'appliance NetScaler BLX se voit attribuer un faible nombre de `hugepages`. Par exemple, 1G.
  - L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

  Le problème est enregistré sous forme de message d'erreur dans « /var/log/ns.log » :

  - `BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x`

  Remarque : x est un nombre <= nombre de processus de travail.

  Solution : attribuez un nombre élevé de, `hugepages` puis redémarrez l'appliance.

[NSNET-25173]

- Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

  [NSNET-24449]

- Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

  - Désactiver
  - Activer
  - Réinitialiser

  [NSNET-16559]

- L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

  ```
  The following packages have unmet dependencies: blx-core-libs:i386 :
  PreDepends: libc6:i386 (>= 2.19)but it is not installable
  ```

  Solution : exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

  - `dpkg --add-architecture i386`
  - `apt-get update`
  - `apt-get install libc6:i386`

  [NSNET-14602]

- Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

  [NSNET-5233]

- Il est possible que l'appliance NetScaler ne génère pas de messages d'interruption SNMP « Cold-Start » après un redémarrage à froid.

  [NSHELP-27917]

- Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

  [NSHELP-21082]

Plate-forme

- Certains packages python ne sont pas installés lorsque vous rétrogradez l'appliance NetScaler de la version 13.1-4.x et des versions supérieures vers l'une des versions suivantes :
  - Toute version 11.1
  - 12.1-62.21 et versions antérieures
  - 13.0-81.x et versions antérieures

  [NSPLAT-21691]

- Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande `rm cloudprofile` pour supprimer le profil.

  [NSPLAT-4520]

- Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
  Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

  [NSPLAT-4451]

Stratégies

- Les connexions peuvent être bloquées si la taille du traitement des données est supérieure à la taille de la mémoire tampon TCP par défaut configurée.

  Solution : définissez la taille de la mémoire tampon TCP sur la taille maximale des données à traiter.

  [NSPOLICY-1267]

SSL

- Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

  Solution :

  1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
  2. Enregistrez la configuration.

[NSSSL-9572]

- Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

  [NSSSL-6478]

- Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

  [NSSSL-6213]

- Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
  `ERROR: crl refresh disabled`

  [NSSSL-6106]

- L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

  [NSSSL-4427]

- Un message d'avertissement incorrect, « Avertissement : aucun chiffrement utilisable configuré sur le serveur/service SSL » s'affiche si vous essayez de modifier le protocole ou le chiffrement SSL dans le profil SSL.

  [NSSSL-4001]

- Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

  [NSSSL-3184, NSSSL-1379, NSSSL-1394]

Système

- Un RTT élevé est observé pour une connexion TCP si la condition suivante est remplie :
  - une fenêtre de congestion maximale élevée (> 4 Mo) est définie
  - L'algorithme TCP NILE est activé

  Pour qu'une appliance NetScaler utilise l'algorithme NILE pour le contrôle de la congestion, les conditions doivent dépasser le seuil de démarrage lent, qui est associé à la fenêtre de congestion maximale

  Ainsi, jusqu'à ce que la fenêtre de congestion maximale configurée soit atteinte, NetScaler continue d'accepter des données et se retrouve avec un RTT élevé.

  [NSHELP-31548]

- La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client .

  [NSHELP-21240]

- Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

  [NSHELP-10972]

- Dans de rares cas, les flux créés avant la création du flux WebSocket HTTP/2 peuvent être interrompus lorsque la connexion côté serveur du WebSocket se ferme.

  Ce problème se produit car l'appliance NetScaler ne prend pas en charge le multiplexage des connexions pour HTTP/2 WebSocket.

  Solution : désactivez le multiplexage des connexions pour le profil HTTP2 associé à l'aide de la commande suivante :

  ```
  set httpProfile <name> [-conMultiplex ( ENABLED | DISABLED )]
  ```

  [NSBASE-17449]

- Dans un déploiement de cluster, si vous exécutez la commande « forcer la synchronisation du cluster » sur un nœud non CCO, le fichier ns.log contient des entrées de journal dupliquées.

  [NSBASE-16304, NSGI-1293]

- Lorsque vous installez NetScaler ADM sur un cluster Kubernetes, cela ne fonctionne pas comme prévu car les processus requis peuvent ne pas s'exécuter.

  Solution : redémarrez le module Gestion.

  [NSBASE-15556]

- L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

  [NSBASE-8506]

Interface utilisateur

- Dans l'interface graphique de NetScaler, le lien « Aide » présent sous l'onglet « Tableau de bord » est cassé.

  [NSUI-14752]

- L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution : configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de l'interface de ligne de commande NetScaler.

[NSUI-13024]

- Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

  [NSUI-6838]

- Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

  - Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

  Solution : effectuez un basculement HA manuel successif uniquement une fois la synchronisation HA terminée (les deux nœuds sont en état de réussite de la synchronisation).

  [NSHELP-25598]

- Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

  1. Mettez à niveau l'appliance NetScaler vers l'une des versions
     - 13.0 52.24 build
     - 12.1 57.18 build
     - 11.1 65.10 build
  2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
  3. Rétrogradez l'appliance NetScaler vers une version antérieure.

  Pour afficher la liste de ces utilisateurs du système à l'aide de l'interface de ligne de commande : À l'invite de commandes, tapez :

  ```
  query ns config -changedpassword [-config <full path of the configuration
   file (ns.conf)>]
  ```

  Solution : Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

  - Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
  - Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.

- Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, consultez /en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html.

[NSCONFIG-3188]

Notes de publication pour la version 13.1-37.38 de NetScaler

May 5, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1-37.38 de NetScaler.

Remarques

- Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.
- La version 13.1-37.39 du bundle NetScaler SDX remplace la version 13.1-37.38.

Nouveautés

Les améliorations et modifications disponibles dans la version 13.1-37.38.

Appliance NetScaler SDX

- **Amélioration du processus de mise à niveau**

  Dans une appliance NetScaler SDX, le processus de mise à niveau nécessite désormais un seul redémarrage au lieu de deux redémarrages.

  [NSSVM-5299]

- **Suppression de la prise en charge des instances tierces de l'interface utilisateur SDX**

  Une appliance NetScaler SDX ne prend plus en charge les instances tierces depuis l'interface utilisateur. La vue **Instances tierces** est supprimée de l'onglet **Configuration** de l'interface utilisateur SDX.

  Solution : si vous souhaitez toujours utiliser les instances tierces dans le service de gestion, suivez la procédure suivante.

  1. Connectez-vous au shell du service de gestion.

2. Créez un fichier « .ThirdPartyVM » dans le répertoire « /mpsconfig ».
3. Redémarrez le service de gestion en exécutant la `svmd restart` commande dans le shell du service de gestion.

[NSSVM-5229]

NetScaler Gateway

- **Support du drapeau HttpOnly sur les cookies d'authentification**

  L'indicateur HttpOnly est désormais pris en charge sur les cookies d'authentification des scénarios VPN, à savoir les cookies NSC_Authentication, AuditingC et NSC_TMAS. Le cookie d'authentification NSC_TMAS est utilisé lors de l'authentification nFactor et le cookie NSC_Authentication, AuditingC est utilisé pour la session authentifiée. Le HttpOnlyFlag sur un cookie limite l'accès aux cookies à l'aide de l'option de cookie de document JavaScript. Cela permet de prévenir le vol de cookie dû à des scripts intersites.

  [CGOP-14004]

Équilibrage de charge

- **Configuration de l'état TROFS différé automatiquement**

  Vous pouvez configurer le déplacement progressif des membres d'un groupe de services vers l'état TROFS lorsque les adresses IP sont supprimées de la réponse DNS. Lorsque le TROFS à temporisation automatique est activé, NetScaler attend le délai de réponse le plus élevé sur tous les moniteurs connectés au groupe de services avant de faire passer les membres à l'état TROFS.

  Pour plus d'informations, voir Configurer la mise à l'échelle automatique des groupes de services basée sur le domaine.

  [NSLB-9371]

Réseau

- **Support DPDK pour les appliances NetScaler BLX sur des hôtes Linux équipés de processeurs AMD**

  Les appliances NetScaler BLX installées sur des hôtes Linux équipés de processeurs AMD prennent désormais en charge le protocole DPDK. L'appliance détecte automatiquement les ports NIC compatibles DPDK spécifiés sur l'hôte Linux. L'appliance les initialise ensuite en mode DPDK. Après le démarrage de l'appliance NetScaler BLX, les ports DPDK sont ajoutés en tant que ports dédiés à l'appliance.

Au lieu de spécifier un ou plusieurs ports de carte réseau compatibles DPDK dans le fichier « blx.conf », vous devez spécifier tous les ports de carte réseau compatibles DPDK qui font partie du même groupe IOMMU. Dans le cas contraire, les ports NIC compatibles avec DPDK sont ajoutés en tant que ports dédiés non DPDK à l'appliance NetScaler BLX.

[NSNET-19219]

Plateforme

- **Performances améliorées pour les instances à cœur partagé dans GCP**

  Dans une instance NetScaler VPX, le paramètre de rendement du processeur est activé par défaut pour les instances à cœur partagé dans GCP. Cela permet d'améliorer les performances dans GCP pour les instances à cœur partagé. Pour plus d'informations sur les types de machines à cœur partagé sur GCP, consultez la documentation Google Cloud.

  Dans une configuration ADC HA avec des instances à cœur partagé dans GCP, le message d'avertissement suivant s'affiche lors de la connexion :

  Pour des performances et une disponibilité élevées, nous vous recommandons de passer d'une machine à cœur partagé à une instance à usage général ou à des types d'instances optimisés pour le calcul et la mémoire sur Google Cloud Platform.

  [NSPLAT-23748]

- **Support pour l'instance NetScaler VPX sur Azure série DV5**

  L'instance NetScaler VPX sur le cloud Azure peut désormais s'exécuter sur les machines virtuelles Azure de la série DV5.

  [NSPLAT-22730]

- **Support pour la plateforme NetScaler MPX 16000**

  Cette version prend en charge la plate-forme NetScaler MPX 16000. Cette plate-forme possède deux processeurs 16 cœurs et 128 Go (16 x 8 Go DIMM) de mémoire. L'appliance fournit au total huit ports SFP+ 25G et quatre ports Ethernet QSFP28 100G.
  Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-hardware-platforms/mpx/netscaler-hardware-platforms/mpx-16000.html.

  [NSPLAT-25436]

- **Support pour la plateforme NetScaler SDX 16000**

  Cette version prend en charge la plate-forme NetScaler SDX 16000. Cette plate-forme possède deux processeurs 16 cœurs et 256 Go (16 x 16 Go DIMM) de mémoire. L'appliance fournit au total huit ports SFP+ 25G et quatre ports Ethernet QSFP28 100G.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-hardware-platforms/sdx/hardware-platforms/sdx-16000.html.

[NSPLAT-21608]

SSL

- **Prise en charge des notifications récurrentes jusqu'à l'expiration du certificat**

  L'appliance NetScaler envoie désormais une notification par jour jusqu'à l'expiration du certificat. Auparavant, une seule notification était envoyée un certain nombre de jours avant l'expiration du certificat.

  [NSSSL-11874]

Système

- **Alarme SNMP pour signaler une défaillance de connexion Syslog**

  Une nouvelle alarme SNMP « SyslogConnectionDropped » a été introduite dans l'appliance NetScaler pour signaler un échec de connexion réseau à un serveur Syslog externe.

  [NSBASE-16823]

Interface utilisateur

- Lorsque vous chargez un ou plusieurs fichiers de licence avec des dates Subscription Advantage différentes, NetScaler ADM ne peut pas les fusionner dans un pool unique. Par conséquent, une instance NetScaler ne peut pas vérifier la capacité si elle dépasse la limite d'un fichier de licence.

  [NSCONFIG-6590, NSHELP-30854]

Problèmes résolus

Les problèmes résolus dans la version 13.1-37.38.

AppFlow

- Une fois AppFlow configuré, l'appliance NetScaler réinitialise une connexion TCP si elle reçoit une réponse HTTP fragmentée vide de la part du serveur principal.

  Ce problème se produit lorsque le paramètre « ClientSideMeasurements » est activé pour l'action AppFlow associée.

  [NSHELP-32250]

Authentification, autorisation et audit

- L'action d'authentification NO_AUTHN ne persiste pas après le redémarrage d'une appliance NetScaler si l'appliance possède la licence Standard Edition.

  [NSHELP-32522]

- Dans une configuration GSLB de NetScaler Gateway, une connexion proxy en boucle entre les sites GSLB peut être détectée si les conditions suivantes sont remplies :

  - Tous les sites GSLB ne sont pas sur la même version.
  - NetScaler Gateway est configuré avec une authentification avancée.

  [NSHELP-32487]

- L'appliance NetScaler supprime le suffixe du jeu de caractères dans l'en-tête Content-Type et l'envoie `Content-Type: application/x-www-form-urlencoded` si vous avez configuré les deux options suivantes.

  - Authentification basée sur un formulaire SSO
  - `nsapimgr knob - nsapimgr_wr.sh -ys call=ns_formsso_use_ctype_simple_enable knob`

  [NSHELP-31977]

- Vous pouvez rencontrer des problèmes lors de la déconnexion si l'authentification SAML est configurée.

  [NSHELP-31962]

- L'authentification unique (SSO) échoue si l'authentification unique est activée pour le trafic qui ne possède pas le jeton porteur requis pour gérer l'authentification unique.

  [NSHELP-31362]

Mise en cache

- Une appliance NetScaler se bloque lorsque le contenu mis en cache est diffusé aux clients.

  [NSHELP-31760]

- Une appliance NetScaler peut se bloquer si les valeurs des paramètres « max_age » et « s_maxage » ne sont pas définies de manière dynamique dans le bloc de contrôle du cache.

  [NSHELP-27758]

Appliance NetScaler SDX

- Dans l'interface graphique d'une appliance NetScaler SDX, lorsqu'un utilisateur ajoutait un objet de défaillance à une règle d'événement, les champs de saisie étaient vulnérables aux at-

taques de script intersite et rendaient la sécurité de la page vulnérable aux scripts intersites stockés. Pour éviter ce problème, les champs de saisie sont désormais nettoyés afin de garantir la validité de la saisie par l'utilisateur.

[NSHELP-32600]

NetScaler Gateway

- L'appliance NetScaler se bloque si l'une ou les deux fonctionnalités de Gateway Insight et Web Insight sont activées.

  [NSHELP-33345, NSHELP-33347]

- Parfois, le proxy RDP ne fonctionne pas en présence d'un broker de connexion.

  [NSHELP-33063]

- Les applications peuvent ne pas démarrer via NetScaler Gateway en raison de l'épuisement des ports de l'appliance NetScaler Gateway.

  [NSHELP-32418]

- L'appliance NetScaler Gateway configurée pour l'accès VPN sans client peut se bloquer lors du traitement d'une session fictive.

  [NSHELP-32399]

- L'appliance NetScaler Gateway peut se bloquer si HDX Insight est activé.

  [NSHELP-32120]

- Lorsque des sessions UDP sont lancées, des connexions périmées semblent exister même après la fermeture des sessions. Cependant, il ne s'agit pas de véritables connexions périmées, mais d'un problème avec le compteur.

  [NSHELP-32009]

- Lorsqu'un utilisateur ouvre une session sur l'appliance NetScaler et que Citrix Workspace n'est pas installé, le lien permettant de télécharger Citrix Workspace pointe de manière incorrecte vers Citrix Receiver.

  [NSHELP-31877]

- Les enregistrements d'échec d'authentification de Gateway Insight indiquent que le nom d'utilisateur est « Anonymous » lorsque NOAUTH est configuré comme premier facteur et que l'authentification du second facteur échoue en raison d'informations d'identification non valides. Ce problème se produit uniquement si la configuration est effectuée à l'aide du visualiseur nFactor car le premier facteur est configuré en tant que NOAUTH, par conception dans le visualiseur nFactor.

  [NSHELP-31795]

- La commande « show vpn icaconnection » n'affiche pas correctement les numéros de série des connexions ICA. Ce problème se produit car le numéro de série est réinitialisé arbitrairement lorsque la commande « show vpn icaconnection » est exécutée.

  [CGOP-22205]

Web App Firewall NetScaler

- Une appliance NetScaler autonome ou le mode secondaire d'une configuration HA peut se bloquer si vous configurez un objet de signature pour NetScaler Web App Firewall sur les versions logicielles suivantes :
  - 13.0 build 88.5 et versions ultérieures
  - 13.1 build 33.41 et versions ultérieures

  [NSHELP-33250]

- Une fuite de mémoire se produit dans une appliance NetScaler lorsque vous configurez `cookieHijackingAction` le blocage, l'enregistrement ou les statistiques.

  [NSHELP-33187]

- Dans NetScaler Web App Firewall, lorsque vous fournissez un protocole à l'en-tête du type de contenu (application/pkcs7-signature), l'en-tête est analysé de manière incorrecte. Par conséquent, le pare-feu bloque les requêtes valides.

  [NSHELP-32844]

- Certaines règles de relaxation ne sont pas importées lors de la restauration d'un profil WAF.

  [NSHELP-32729]

- NetScaler Web App Firewall met parfois du temps à détecter l'injection de commande. Par conséquent, Pitboss redémarre l'appliance NetScaler.

  [NSHELP-32654]

- Des cookies légitimes sont placés dans le journal tout en affichant des journaux de violation des cookie dupliqués.

  [NSHELP-32369]

Équilibrage de charge

- Dans certains scénarios, les serveurs liés à un groupe de services affichent une valeur de cookie non valide. Vous pouvez voir la valeur de cookie correcte dans les journaux de suivi.

  [NSHELP-21196]

Divers

- L'appliance NetScaler définit la taille de la mémoire tampon pour la fonctionnalité de journalisation du serveur Web sur une valeur par défaut incorrecte de 3 Mo au lieu de 16 Mo.

  [NSHELP-32429]

Réseau

- Dans une configuration de cluster NetScaler BLX, les opérations suivantes échouent sans aucun message d'erreur :
  - Effacer la configuration au niveau de base de force (« clear config -force basic »)
  - Effacement de la configuration au niveau force étendu (« clear config -force extended »)
  - Effacer la configuration au niveau force extended+ (« clear config -force extended+ »)

  [NSNET-27132]
- Dans une configuration à haute disponibilité, le nœud principal peut se bloquer en raison d'une corruption de la mémoire lors de l'effacement d'un grand nombre de sessions LSN.

  [NSHELP-32467]
- L'appliance NetScaler peut se bloquer si toutes les conditions suivantes sont remplies :
  - L'ACL basé sur le TTL expire
  - L'appliance NetScaler dispose d'un grand nombre de listes de contrôle d'accès configurées.

  [NSHELP-31307]

Plateforme

- Lorsque vous désactivez l'interface Mellanox sur une appliance NetScaler MPX, le commutateur homologue lié à l'interface est affiché en état Link Up au lieu d'être en mode Link Down.

  [NSPLAT-24422]
- L'instance NetScaler VPX supprime les paquets d'un client si les deux conditions suivantes sont remplies :
  - L'instance VPX est hébergée sur VMware Cloud on AWS à l'aide d'un adaptateur VMXNET3.
  - L'adaptateur VMXNET3 ne parvient pas à générer le hachage RSS pour le paquet.

  [NSHELP-33150]

Stratégies

- Dans une appliance NetScaler, les politiques de commutation de contenu qui sont migrées des politiques classiques vers des politiques avancées à l'aide de l'outil NSPEPI peuvent ne pas fonctionner lorsque les conditions suivantes sont remplies :
  - Les stratégies sont liées au vserver de commutation de contenu.
  - Le paramètre « CaseSensitive » est réglé sur OFF.

  [NSHELP-31951]

SSL

- Une appliance NetScaler peut se bloquer lors d'une prise de contact TLS 1.3 lorsqu'un serveur virtuel est configuré pour utiliser des clés privées stockées dans Azure Key Vault.

  [NSHELP-32451]

- Une appliance NetScaler se bloque si les conditions suivantes sont remplies :
  - Un client envoie un bonjour à un autre client avant que la prise de contact ne soit terminée.
  - La demande contient un ensemble spécial de chiffrements dans le premier bonjour du client.

  [NSHELP-32422]

- L'interface graphique de NetScaler, accessible via une adresse IP de cluster (CLIP), n'affiche pas les liaisons de certificat de serveur vers un serveur virtuel SSL.

  [NSHELP-31602]

- La vérification de la réponse OCSP peut échouer lors d'une interception SSL si aucun certificat CA valide n'est présent dans le bundle de certificats par défaut. L'échec se produit parce que la vérification de la réponse OCSP a été effectuée de manière incorrecte en utilisant le bundle de certificats par défaut au lieu du bundle de certificats configuré.

  [NSHELP-30594]

Système

- Lorsqu'un serveur NetScaler ADM reçoit un trafic HTTP important avec des URL uniques, il consomme beaucoup de mémoire. Par conséquent, le serveur NetScaler ADM devient inaccessible.

  [NSHELP-32922]

- Dans une appliance NetScaler, la structure de modification de l'en-tête entraîne une corruption de la mémoire. Cette condition se produit lorsque les cookies qui doivent être consommés par l'appliance NetScaler sont supprimés dans un ordre particulier avant d'être transférés.

[NSHELP-32799]

- L'authentification VPN échoue lorsque la méthode PATCH est utilisée dans la requête HTTP. Ce problème se produit car la méthode HTTP PATCH est reconnue comme une méthode d'authentification inconnue.

  [NSHELP-32214]

- Lorsque vous utilisez la fonction d'inspection du contenu, l'insertion de l'en-tête Rewrite avec charge utile risque de ne pas fonctionner correctement.

  [NSHELP-30088]

Interface utilisateur

- La page de licence du service de gestion n'actualise pas les informations de licence regroupées lorsque vous visitez le nœud de licence ou que vous les actualisez. Au lieu de cela, les informations de licence regroupées sont actualisées uniquement lorsque vous vous déconnectez puis que vous vous reconnectez.

  [NSHELP-33203]

- Lorsqu'un utilisateur consulte la liaison dans une stratégie de commutation de contenu, les détails du serveur virtuel de commutation de contenu ne s'affichent pas sur la même ligne sous **Afficher les liaisons**.

  [NSHELP-33149]

- Lorsqu'un utilisateur lie une stratégie de trafic à un serveur virtuel de commutation de contenu ou d'équilibrage de charge, les détails de liaison n'apparaissent pas dans l'interface graphique.

  [NSHELP-32751]

- La mise à niveau ou la rétrogradation d'une appliance NetScaler vers l'une des versions suivantes à l'aide de l'interface graphique NetScaler peut échouer :

  - Version 13.1 build 30.52
  - Version 13.1 build 27.59

  [NSHELP-32673]

- L'erreur suivante s'affiche lors de la création ou de la modification d'un serveur virtuel avec le protocole DNS et DNS_TCP hébergé sur une partition personnalisée à l'aide de l'interface graphique NetScaler :

  ```
  Error: Invalid object name [lbvserver_scpolicy_binding]
  ```

  [NSHELP-32534]

- Les problèmes suivants apparaissent dans l'interface graphique de NetScaler :

- À l'aide de l'interface graphique NetScaler, si un certificat de serveur est lié à un serveur virtuel SSL, la liaison du certificat n'apparaît pas dans l'interface graphique. Les liaisons des certificats CA apparaissent comme d'habitude sur l'interface graphique.
- Cliquez sur le bouton Masquer pour les stratégies de répondeur intégrées pour masquer également les stratégies de répondeur créées manuellement.

Dans une configuration de cluster, les problèmes supplémentaires suivants apparaissent dans l'interface graphique de NetScaler :

- La liaison d'un groupe de chiffrement à un service interne échoue avec une erreur.
- Les actions de réécriture intégrées ne sont pas masquées dans l'interface graphique.

[NSHELP-32499]

- Dans une appliance NetScaler dotée de partitions d'administration, le paramètre « ns » défini dans la partition est perdu après un redémarrage. Cette condition se produit en raison d'une configuration intégrée incorrecte.

  [NSHELP-32486]

- La page de connexion de l'appliance NetScaler peut ne pas afficher le nom d'utilisateur valide une fois que l'utilisateur s'est connecté.

  [NSHELP-31759]

- Dans une configuration à haute disponibilité, les configurations chiffrées sont perdues sur le nœud secondaire après la synchronisation de la configuration HA.

  [NSHELP-30897]

Problèmes connus

Les problèmes qui existent dans la version 13.1-37.38.

AppFlow

- HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

  [NSINSIGHT-943]

Authentification, autorisation et audit

- Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

  [NSHELP-563]

- L'authentification DUO échoue si la fonctionnalité Content Security Policy (CSP) est activée sur l'appliance NetScaler.

  [NSAUTH-12687]

- Les administrateurs ne peuvent pas effectuer de journalisation personnalisée des échecs d'authentification dus à des informations d'identification non valides. Ce problème se produit car les politiques du répondeur NetScaler ne détectent pas les erreurs liées aux échecs de connexion.

  [NSAUTH-11151]

- Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante. `show adfsproxyprofile <profile name>`

  Solution : Connectez-vous au principal NetScaler actif du cluster et exécutez la commande. `show adfsproxyprofile <profile name>` Il afficherait l'état du profil proxy.

  [NSAUTH-5916]

- La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

  - L'option Tester l'accessibilité LDAP est ouverte.
  - Les informations d'identification de connexion non valides sont renseignées et envoyées.
  - Les identifiants de connexion valides sont renseignés et envoyés.

  Solution : fermez et ouvrez l'option Tester l'accessibilité LDAP.

  [NSAUTH-2147]

Appliance NetScaler SDX

- Des pertes de paquets sont visibles sur une instance VPX hébergée sur une appliance NetScaler SDX si les conditions suivantes sont remplies :

  - Le mode d'allocation du débit est en rafale.
  - Il existe une grande différence entre le débit et la capacité maximale de rafale.

  [NSHELP-21992]

NetScaler Gateway

- Le client Citrix Secure Access, version 21.7.1.2 et versions ultérieures, ne parvient pas à effectuer la mise à niveau vers des versions ultérieures pour les utilisateurs ne disposant pas de droits d'administration. Ce problème s'applique uniquement si la mise à niveau du client Citrix Secure Access est effectuée à partir d'une appliance NetScaler.

[NSHELP-32793]

- Lorsque les utilisateurs cliquent sur l'onglet Page d'accueil de l'écran Citrix Secure Access pour Windows, la page affiche l'erreur de refus de connexion.

  [NSHELP-32510]

- Sur un appareil Mac utilisant Chrome, l'extension VPN se bloque lors de l'accès à deux noms de domaine complets.

  [NSHELP-32144]

- Dans certains cas, si les paramètres de proxy sont vides dans NetScaler Gateway version 13.0 ou 13.1, Citrix SSO crée des paramètres de proxy incorrects.

  [NSHELP-31970]

- Le contrôle de journalisation des débogues pour le client Citrix Secure Access est désormais indépendant de NetScaler Gateway et peut être activé ou désactivé depuis l'interface utilisateur du plug-in pour la machine et le tunnel utilisateur.

  [NSHELP-31968]

- Les connexions directes aux ressources situées en dehors du tunnel établi par Citrix Secure Access peuvent échouer en cas de retard ou de congestion important.

  [NSHELP-31598]

- Le message personnalisé du journal des défaillances EPA ne s'affiche pas sur le portail NetScaler Gateway. Au lieu de cela, le message « erreur interne » s'affiche.

  [NSHELP-31434]

- Parfois, l'ouverture de session automatique de Windows ne fonctionne pas lorsqu'un utilisateur se connecte à l'ordinateur Windows en mode de service permanent. Le tunnel de la machine ne passe pas au tunnel utilisateur et au message « Connexion… » s'affiche dans l'interface utilisateur du plug-in VPN.

  [NSHELP-31357, CGOP-21192]

- Lorsque Always on est configuré, le tunnel utilisateur échoue en raison du numéro de version incorrect (1.1.1.1) dans le fichier aoservice.exe.

  [NSHELP-30662]

- Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil « NetworkAccessOnVPNFailure » de « Always on » de à. `fullAccess onlyToGateway`

  [NSHELP-30236]

- La page d'accueil de la passerelle ne s'affiche pas immédiatement après que le plug-in de passerelle a réussi à établir le tunnel VPN. Pour résoudre ce problème, la valeur de registre suivante est introduite.

  HKLMSoftwareCitrixSecure Access ClientSecureChannelResetTimeoutSeconds
  Type: DWORD

  Par défaut, cette valeur de registre n'est ni définie ni ajoutée. Lorsque la valeur de « SecureChannelResetTimeoutSeconds » est 0 ou n'est pas ajoutée, le correctif pour gérer le délai ne fonctionne pas, ce qui est le comportement par défaut. L'administrateur doit définir ce registre sur le client pour activer le correctif (c'est-à-dire afficher la page d'accueil immédiatement après que le plug-in de passerelle ait établi le tunnel VPN avec succès).

  [NSHELP-30189]

- Le client VPN Windows n'honore pas l'alerte « Notification de fermeture SSL » du serveur et envoie la demande de connexion de transfert sur la même connexion.

  [NSHELP-29675]

- Vous remarquerez peut-être certaines adresses IP internes de Citrix dans le fichier rdx.js.

  [NSHELP-28682]

- L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

  [NSHELP-28551]

- Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

  [NSHELP-28404]

- Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :
  - L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
  - L'appliance est configurée pour l'authentification basée sur des certificats avec l'authentification à deux facteurs « désactivée »

  [NSHELP-23584]

- Parfois, lorsque vous parcourez les schémas, le message d'erreur « Impossible de lire le type de propriété non défini » apparaît.

  [NSHELP-21897]

- Dans une configuration de cluster NetScaler, HDX Insight et Gateway Insight ne peuvent pas être activés simultanément.

  [CGOP-22849]

- Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

  [CGOP-19355]

- L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

  [CGOP-13621]

- Le rapport Gateway Insight affiche de manière incorrecte la valeur « Local » au lieu de « SAML » dans le champ Type d'authentification en cas d'échec d'erreur SAML.

  [CGOP-13584]

- Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

  [CGOP-13511]

- Lorsqu'une connexion ICA est lancée à partir d'un Receiver MAC version 19.6.0.32 ou Citrix Virtual Apps and Desktops version 7.18, la fonctionnalité HDX Insight est désactivée.

  [CGOP-13494]

- Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

  [CGOP-13493]

- Lors de l'acceptation des connexions hôtes locales depuis le navigateur, la boîte de dialogue Accepter la connexion pour macOS affiche le contenu en anglais, quelle que soit la langue sélectionnée.

  [CGOP-13050]

- Le texte « Page d'accueil » dans l' application Citrix SSO > Page d'accueil est tronqué pour certaines langues.

  [CGOP-13049]

- Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

  [CGOP-11830]

- Dans Outlook Web App (OWA) 2013, le fait de cliquer sur **Options** dans le menu Paramètres affiche une boîte de dialogue **Erreur critique** . De plus, la page ne répond plus.

  [CGOP-7269]

Équilibrage de charge

- Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

  [NSLB-7679]

- Le format ServiceGroupName utilisé dans le trap `entityofs` pour le groupe de services est le suivant :
  `<service(group)name>?<ip/DBS>?<port>`

  Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (« ? ») est utilisé comme séparateur. NetScaler envoie le piège avec le point d'interrogation (« ? «). Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

  [NSHELP-28080]

Divers

- Lorsqu'une synchronisation forcée a lieu dans une configuration à haute disponibilité, l'appliance exécute la commande « set urlfiltering parameter » dans le nœud secondaire.
  Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre « TimeOfDaytoUpdateDB ».

  [NSSWG-849]

- Le registre de liste AlwaysOnAllow ne fonctionne pas comme prévu si la valeur du registre est supérieure à 2000 octets.

  [NSHELP-31836]

- Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

  [NSHELP-22409]

Réseau

- Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

  [NSNET-25299]

- Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :

- L'appliance NetScaler BLX est dotée d'un faible nombre de « pages volumineuses ». Par exemple, 1G.
- L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

Le problème est enregistré sous forme de message d'erreur dans « /var/log/ns.log » :

- « BLX-DPDK:DPDK Mempool n'a pas pu être initialisé pour PE-x »

Remarque : x est un nombre <= nombre de processus de travail.

Solution : allouez un grand nombre de « pages volumineuses », puis redémarrez l'appliance.

[NSNET-25173]

- Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

  [NSNET-24449]

- Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

  - Désactiver
  - Activer
  - Réinitialiser

  [NSNET-16559]

- L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

  « Les paquets suivants ont des dépendances non satisfaites : blx-core-libs:i386 : PreDepends : libc6:i386 (>= 2.19) mais ils ne sont pas installables »

  Solution : exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

  - dpkg –add-architecture i386
  - apt-get update
  - apt-get dist-upgrade
  - apt-get install libc6:i386

  [NSNET-14602]

- Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

- Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

  [NSHELP-21082]

Plateforme

- Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande « rm cloudprofile » pour supprimer le profil.

  [NSPLAT-4520]

- Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
  Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

  [NSPLAT-4451]

- Sur la plate-forme NetScaler SDX 8015/8400/8600, vous pouvez constater une augmentation de la consommation de mémoire sur Xen Server.
  Solution : exécutez la commande suivante sur Xen Server, puis redémarrez l'appliance.
  /opt/xensource/libexec/xen-cmdline –set-xen "dom0_mem=1024M,max:1024M"

  [NSHELP-32260]

Stratégies

- Les connexions peuvent être bloquées si la taille du traitement des données est supérieure à la taille de la mémoire tampon TCP par défaut configurée.

  Solution : définissez la taille de la mémoire tampon TCP sur la taille maximale des données à traiter.

  [NSPOLICY-1267]

SSL

- Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

Solution :

1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
2. Enregistrez la configuration.

[NSSSL-9572]

- Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

  [NSSSL-6478]

- Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

  [NSSSL-6213]

- Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
  ERREUR : actualisation des CRL désactivée

  [NSSSL-6106]

- L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

  [NSSSL-4427]

- Un message d'avertissement incorrect, « Avertissement : aucun chiffrement utilisable configuré sur le serveur/service SSL » s'affiche si vous essayez de modifier le protocole ou le chiffrement SSL dans le profil SSL.

  [NSSSL-4001]

- Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

  [NSSSL-3184, NSSSL-1379, NSSSL-1394]

Système

- Un RTT élevé est observé pour une connexion TCP si la condition suivante est remplie :
  - une fenêtre de congestion maximale élevée (> 4 Mo) est définie
  - L'algorithme TCP NILE est activé

  Pour qu'une appliance NetScaler utilise l'algorithme NILE pour le contrôle de la congestion, les conditions doivent dépasser le seuil de démarrage lent, qui est associé à la fenêtre de congestion maximale

Ainsi, jusqu'à ce que la fenêtre de congestion maximale configurée soit atteinte, NetScaler continue d'accepter des données et se retrouve avec un RTT élevé.

[NSHELP-31548]

- La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client.

  [NSHELP-21240]

- Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

  [NSHELP-10972]

- Dans de rares cas, les flux créés avant la création du flux WebSocket HTTP/2 peuvent être interrompus lorsque la connexion côté serveur du WebSocket se ferme.

  Ce problème se produit car l'appliance NetScaler ne prend pas en charge le multiplexage des connexions pour HTTP/2 WebSocket.

  Solution : désactivez le multiplexage des connexions pour le profil HTTP2 associé à l'aide de la commande suivante :

  ```
  set httpProfile <name> [-conMultiplex ( ENABLED | DISABLED )]
  ```

  [NSBASE-17449]

- Dans un déploiement de cluster, si vous exécutez la commande « forcer la synchronisation du cluster » sur un nœud non CCO, le fichier ns.log contient des entrées de journal dupliquées.

  [NSBASE-16304, NSGI-1293]

- Lorsque vous installez NetScaler ADM sur un cluster Kubernetes, cela ne fonctionne pas comme prévu car les processus requis peuvent ne pas s'exécuter.

  Solution : redémarrez le module Gestion.

  [NSBASE-15556]

- L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

  [NSBASE-8506]

Interface utilisateur

- Pour la fonction de réécriture MQTT, vous ne pouvez pas supprimer une expression à l'aide de l'éditeur d'expression dans l'interface graphique.

  Solution : utilisez la commande d'ajout ou de modification d'action de type MQTT via l'interface de ligne de commande.

[NSUI-18049]

- Dans l'interface graphique de NetScaler, le lien « Aide » présent sous l'onglet « Tableau de bord » est cassé.

  [NSUI-14752]

- L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

  Solution : configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de l'interface de ligne de commande NetScaler.

  [NSUI-13024]

- Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

  [NSUI-6838]

- Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

  - Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

  Solution : effectuez un basculement HA manuel successif uniquement une fois la synchronisation HA terminée (les deux nœuds sont en état de réussite de la synchronisation).

  [NSHELP-25598]

- Dans une configuration à haute disponibilité des appliances NetScaler BLX, le nœud principal peut ne plus répondre en bloquant toute demande de CLI ou d'API.

  Solution : redémarrez le nœud principal.

  [NSCONFIG-6601]

- Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

  1. Mettez à niveau l'appliance NetScaler vers l'une des versions
     - 13.0 52.24 build
     - 12.1 57.18 build
     - 11.1 65.10 build
  2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
  3. Rétrogradez l'appliance NetScaler vers une version antérieure.

Pour afficher la liste de ces utilisateurs du système à l'aide de l'interface de ligne de commande : À l'invite de commandes, tapez :

```
query ns config -changedpassword [-config <full path of the configuration
 file (ns.conf)>]
```

Solution : Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

- Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
- Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
- Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, voir How to reset root administrator (nsroot) password.

[NSCONFIG-3188]

Notes de publication pour la version 13.1-33.54 de NetScaler

May 5, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1-33.54 de NetScaler.

Remarques

- Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.
- Les versions 13.1-33.47 et ultérieures corrigent les failles de sécurité décrites dans https://support.citrix.com/article/CTX463706.
- La version 33.54 remplace la version 33.52, la version 33.49 et la version 33.47.
- La version 33.54 inclut des correctifs pour les problèmes suivants : NSHELP-33250, NSHELP-33345 et NSHELP-33063.
- La version 33.52 incluait un correctif pour le problème suivant : NSHELP-32907.
- La version 33.49 incluait des correctifs pour les problèmes suivants : NSHELP-32709, NSHELP-32697, NSHELP-32410, NSHELP-31790, NSHELP-31478 et NSCONFIG-7098.

Nouveautés

Les améliorations et modifications disponibles dans la version 13.1-33.54.

Gestion des bots

- **Nouvelles expressions liées au BOT**

  Les expressions suivantes sont ajoutées et peuvent être utilisées lorsque le profil BOT est configuré en mode journalisation :

  - `HTTP.REQ.BOT.IS_SUSPECTED` - Renvoie la valeur true si le client est soupçonné d'être un BOT.
  - `HTTP.REQ.BOT.TYPE.EQ(<bot type>)` - Renvoie la valeur true si le type BOT du client est identique à l'argument. Valeurs possibles des types de BOT : GOOD, BAD et UNKNOWN.
  - `HTTP.REQ.BOT.TYPE.NE(<bot type>)` - Renvoie la valeur true si le type BOT du client n'est pas identique à l'argument. Valeurs possibles des types de BOT : GOOD, BAD et UNKNOWN.
  - `HTTP.REQ.BOT.TYPE.ENUM_NAME` - Renvoie le type BOT sous forme de chaîne. Par exemple, BON, MAUVAIS, INCONNU.
  - `HTTP.REQ.BOT.DETECTION_METHODS` - Liste des techniques de détection à l'aide desquelles un client est détecté en tant que BOT.

  [NSBOT-842]

NetScaler Gateway

- Lorsque SmartControl est configuré, la fiabilité des sessions est prise en charge même si la session d'authentification, d'autorisation et d'audit correspondante n'existe pas. La demande de reconnexion reçue par l'appliance NetScaler de la part de l'appareil client après la restauration suite à une interruption du réseau est traitée même si la session d'authentification, d'autorisation et d'audit correspondante n'existe pas.

  [CGOP-21040]

Web App Firewall NetScaler

- **Nouveau profil Web App Firewall par défaut**

  Un nouveau profil par défaut, appelé core, est désormais disponible avec les principales protections WAF. Les contrôles suivants sont activés dans le profil principal :

  - Injection SQL basée sur la grammaire
  - Injection CMD basée sur la grammaire

- XSS
- BOF
- Expressions de blocs

[NSWAF-9133]

- **Support de mots clés personnalisés pour la charge utile JSON**

  Vous pouvez ajouter des mots-clés de votre choix et vérifier si ces mots-clés configurés sont présents dans la charge utile JSON. Si les mots clés configurés sont détectés dans les demandes entrantes, vous pouvez configurer l'appliance NetScaler pour bloquer les demandes, mettre à jour les journaux ou incrémenter les compteurs de journaux.

  L'avantage est que vous pouvez ajouter des mots-clés qui ne sont pas couverts par les contrôles d'injection SQL et d'injection de commandes et ainsi réduire le nombre de faux positifs.

  [NSWAF-9076]

Plateforme

- **Empêcher l'utilisation non autorisée des licences NetScaler**

  Pour toute mise à niveau de l'appliance NetScaler vers la version 13.1, le système de licences NetScaler applique désormais la validation des licences conformément à la date d'expiration des Customer Success Services. Si cette date est antérieure à la date d'éligibilité aux Customer Success Services, la licence existante ne fonctionnera pas sur la version mise à niveau de l'appliance ADC. Ce comportement peut empêcher l'utilisation non autorisée des licences.

  Pour obtenir la liste des produits NetScaler et leurs dates d'éligibilité, consultez. https://support.citrix.com/article/CTX111618/citrix-product-customer-success-services-eligibility-dates

  [NSPLAT-24522]

- **Gestion de la suppression dynamique des cartes réseau dans le réseau accéléré Azure**

  Une instance NetScaler VPX peut désormais gérer de manière fluide les suppressions dynamiques et le rattachement des cartes réseau supprimées dans le réseau accéléré Azure.

  Azure peut supprimer la carte réseau à fonction virtuelle (VF) de virtualisation des E/S à racine unique (SR-IOV) du réseau accéléré pour ses activités de maintenance de l'hôte. Chaque fois qu'une carte réseau est supprimée d'une machine virtuelle Azure, l'instance NetScaler VPX affiche l'état de l'interface comme étant Link Down et le trafic passe uniquement par l'interface virtuelle. Une fois la carte réseau supprimée reconnectée, les instances VPX utilisent la carte réseau VF SR-IOV reconnectée. Ce processus se déroule sans problème et ne nécessite aucune configuration.

  [NSPLAT-23300]

- **Support pour Python 3.7**

  L'appliance NetScaler prend désormais en charge Python 3.7 car Python 2.7 est obsolète.

  Vous devez mettre à jour vos scripts Python actuels pour qu'ils soient compatibles avec Python 3.7.

  [NSPLAT-20832]

SSL

- **Prise en charge des notifications récurrentes jusqu'à l'expiration du certificat**

  L'appliance NetScaler envoie désormais une notification par jour jusqu'à l'expiration du certificat. Auparavant, une seule notification était envoyée un certain nombre de jours avant l'expiration du certificat.

  [NSSSL-11874]

- **Augmentation de la longueur de l'adresse e-mail dans une demande de création de certificat**

  Sur une appliance NetScaler, la limite d'adresse e-mail dans une demande de création de certificat est désormais portée à 255 caractères. Auparavant, la limite était de 39 caractères.

  [NSSSL-10917]

- **Support pour Thales Luna HSM sur les plateformes Intel Coleto et Intel Lewisburg**

  Thales Luna HSM est désormais compatible avec les plateformes basées sur les puces SSL NetScaler, Intel Coleto et Intel Lewisburg.

  Les appliances suivantes sont livrées avec des puces Intel Coleto :

  - MPX 5900
  - MPX/SDX 8900
  - MPX/SDX 15000
  - MPX/SDX 15000-50G
  - MPX/SDX 26000
  - MPX/SDX 26000-50S
  - MPX/SDX 26000-100 G

  Les plateformes suivantes sont livrées avec des puces Intel Lewisburg :

  - MPX 9100
  - SDX 9100

  [NSSSL-9707]

Système

- **Nouveau paramètre ajouté dans le profil HTTP**

  Un nouveau paramètre PassProtocolUpgrade est ajouté au profil HTTP pour empêcher les attaques sur les serveurs principaux. Selon l'état de ce paramètre, l'en-tête de mise à niveau est transmis dans la demande envoyée au serveur principal ou supprimé avant l'envoi de la demande.

  - Si le paramètre PassProtocolUpgrade est activé, l'en-tête de mise à niveau est transmis au back-end. Le serveur accepte la demande de mise à niveau et l'informe dans sa réponse.
  - Si ce paramètre est désactivé, l'en-tête de mise à niveau est supprimé et la demande restante est envoyée au backend.

  Le paramètre PassProtocolUpgrade est ajouté aux profils suivants :

  - nshttp_default_profile ACTIVÉ par défaut
  - nshttp_default_strict_validation DISABLED by default
  - nshttp_default_internal_apps DISABLED by default
  - nshttp_default_http_quic_profile ACTIVÉ par défaut

  Citrix recommande de désactiver ce paramètre par défaut. Pour plus de détails, consultez le Guide de déploiement sécurisé de NetScaler.

  [NSBASE-17423]

- **Prise en charge de plusieurs profils chronologiques**

  L'appliance NetScaler prend désormais en charge jusqu'à trois configurations de profils chronologiques.
  Vous pouvez configurer chaque profil de série chronologique de manière à avoir les caractéristiques suivantes :

  - Son collecteur
  - fichier de schéma contenant l'ensemble de compteurs requis à exporter par le collecteur de métriques
  - Format de données dans lequel les métriques peuvent être exportées.
  - Possibilité d'activer ou de désactiver les mesures, les journaux d'audit et les événements.

  Grâce à la prise en charge de plusieurs profils de séries chronologiques, le collecteur de métriques peut exporter simultanément un ensemble différent (en fonction du fichier de schéma configuré) de mesures vers différents collecteurs dans différents formats (AVRO, Prometheus, Influx).

  Pour plus d'informations, voir Configuration de la fonctionnalité AppFlow.

  [NSBASE-16809]

- Le Syslog n'est pas exporté via TCP à un intervalle de temps spécifique. En raison de cette situation, le Syslog reste indéfiniment dans la mémoire tampon d'audit, ce qui donne l'impression que les journaux sont manquants. Ce Syslog n'est envoyé que lorsque la mémoire tampon est pleine.

  Avec ce correctif, le Syslog est exporté via TCP lorsque la mémoire tampon d'audit est pleine, ou toutes les 20 secondes, selon la première éventualité.

  [NSBASE-16698]

- **Support de délestage cryptographique pour QUIC**

  L'appliance NetScaler prend désormais en charge le transfert du traitement cryptographique du logiciel vers le matériel, ce qui accélère les transactions QUIC. L'appliance NetScaler est équipée de puces matérielles SSL qui effectuent l'accélération cryptographique de manière transparente.

  Pour plus d'informations, voir QUIC.

  [NSBASE-12046]

Interface utilisateur

- **Communication RPC sécurisée basée sur le paramètre TLS 1.2 pour les services internes**

  Après la mise à niveau d'une appliance NetScaler vers la version 13.1 build 33.x ou ultérieure à partir de l'une des versions suivantes, l'option « sécurisée » pour le nœud RPC est activée ou désactivée sur la base du paramètre TLS 1.2 (activé ou désactivé) présent pour les services RPCS et KRPCS internes.

  - Version 13.0 build 64.35 ou antérieure
  - Version 12.1 build 61.18 ou antérieure

  La communication RPC est cryptée entre les nœuds NetScaler des configurations suivantes si l'option « Secure » est activée :

  - Haute disponibilité
  - Cluster :
  - GSLB

  L'option « sécurisée » utilise le protocole sécurisé TLS1.2 et les numéros de port 3008 et 3009 pour la connexion RPC entre les nœuds NetScaler.

  Pour garantir la sécurité des communications RPC, Citrix recommande d'effectuer les opérations suivantes avant de mettre à niveau ces configurations :

  - Le protocole TLS 1.2 doit être activé pour les services internes du RPC et du KRPCS :
    * nsrpcs-127.0.0.1-3008

    * nskrpcs-127.0.0.1-3009
    * nsrpcs-::1l-3008
  - Les versions 3008 et 3009 doivent être débloquées dans les pare-feux situés entre les nœuds NetScaler.

Vous pouvez activer ou désactiver l'option sécurisée à l'aide de la CLI ou de l'interface graphique NetScaler.

[NSCONFIG-6485]

- **Support pour l'agrégateur de licences NetScaler CPX**

  Vous pouvez désormais utiliser l'agrégateur de licences NetScaler CPX, un nouveau microservice Kubernetes fourni par NetScaler, pour obtenir des licences pour NetScaler CPX. Lorsque vous démarrez NetScaler CPX, vous devez configurer la variable d'environnement CLA avec l'adresse IP ou le nom de domaine de l'agrégateur de licences NetScaler CPX. Si la variable d'environnement est configurée, l'agrégateur de licences NetScaler CPX vérifie les licences agrégées pour tous les NetScaler CPX connectés.

  [NSCONFIG-6394]

- Prise en**charge des options asynchrones pour l'installation de l'API NITRO**
  Une nouvelle option « async » a été introduite dans l'API « install NITRO ». L'option « async » renvoie l'identifiant de tâche de l'opération d'installation, qui peut être utilisé dans l'appel d'API « nsjob NITRO » pour récupérer les détails de l'état de l'opération d'installation.

  Exemple :

  Dans l'exemple de requête curl suivant, l'API d'installation NITRO est utilisée avec l'option async. La charge utile de réponse contient l'ID de tâche 2.

  Curl request:
  "curl -v -X POST -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/install?warning=yes -d '{"install": {"url": "https://example-repo.citrite.net/build-13.1-36.11_nc_64.tgz", "async":"1"}}"'

  Charge utile de réponse :

  "{ "install":{ "url": "<file path>", "y": false, "l": false, "a": false, "enhancedupgrade": false, "resizeswapvar": false, "async": true, "id": "2" }"

  Dans l'exemple de requête curl suivant, l'API « nsjob » NITRO est utilisée pour récupérer les détails d'état de l'identifiant de tâche 2, qui est l'identifiant de l'opération d'installation.

  Curl request:
  "curl -v -X GET -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/nsjob/2"

  Charge utile de réponse :

”{ “errorcode”: 0, “message”: “Done”, “severity”: “NONE”, “nsjob”: [

{ “name”: “install”, “id”: “2”, “status”: “Success”, “progress”: “nInstallation has completed.nnReboot is required for configuration changes to take effect.Installation succeeded. Reboot required.n”, “timeelapsed”: 148, “errorcode”: “5221”, “message”: “The configuration changes will not take effect until the system is rebootedn” }

]}”

[NSCONFIG-5870]

Problèmes résolus

Les problèmes résolus dans la version 13.1-33.54.

Authentification, autorisation et audit

- L’appliance NetScaler arrête de traiter les demandes en raison d’une fuite de mémoire dans le module MEM_SSLVPN.

  [NSHELP-32646]

- La page d’ouverture de session d’authentification de NetScaler Gateway Duo ne se charge pas avec les thèmes d’interface utilisateur autres que RFWebUI.

  [NSHELP-32463]

- Lors de l’enregistrement de votre appareil auprès de l’appliance NetScaler Gateway, le message « Échec de l’enregistrement push » s’affiche pour Citrix Secure Access (Citrix SSO).

  [NSHELP-32461]

- Si les authentifications LDAP et SAML sont configurées en cascade, une page d’erreur s’affiche lors de la connexion.

  [NSHELP-32378]

- Parfois, l’authentification auprès de la passerelle à l’aide de l’application Citrix Workspace échoue.

  [NSHELP-32333]

- L’authentification SAML échoue si la fonctionnalité CSP (Content Security Policy) est activée sur l’appliance NetScaler.

  [NSHELP-32203]

Mise en cache

- Une appliance NetScaler peut se bloquer si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

  [NSHELP-22942]

Appliance NetScaler SDX

- Dans une appliance NetScaler SDX, l'option Clean Install ne fonctionne pas lorsque vous rétrogradez de la version 13.1 build 30.52 vers une version ou une version inférieure.

  [NSSVM-5419]

- Quelques fichiers de configuration du module de sécurité matérielle (HSM) redondants sont également sauvegardés lorsque les instances NetScaler VPX sont sauvegardées à l'aide de SDX et ADM.

  [NSHELP-32539]

- Le syslog du service de gestion de l'appliance NetScaler SDX affiche la date deux fois de manière incorrecte.

  [NSHELP-32311]

NetScaler Gateway

- L'appliance NetScaler se bloque si l'une ou les deux fonctionnalités de Gateway Insight et Web Insight sont activées.

  [NSHELP-33345]

- Parfois, le proxy RDP ne fonctionne pas en présence d'un broker de connexion.

  [NSHELP-33063]

- L'appliance NetScaler Gateway peut se bloquer si HDX Insight est activé et qu'un utilisateur se connecte à StoreFront immédiatement après s'être déconnecté.

  [NSHELP-32907, NSHELP-33079, NSHELP-33289]

- L'analyse EPA de l'adresse MAC basée sur Patset ne fonctionne pas de la même manière que la numérisation du certificat de l'appareil.

  [NSHELP-32760]

- L'appliance NetScaler supprime tout paquet HTTP dont la méthode d'authentification est inconnue et qui est utilisé pour le trafic d'authentification. La méthode d'authentification inconnue interrompt le déploiement en provoquant des problèmes d'équilibrage de charge si des serveurs

virtuels d'authentification et d'autorisation sont utilisés pour le trafic d'authentification. La méthode d'authentification inconnue est désactivée par défaut.

[NSHELP-32709]

- La boîte de dialogue « Transférer la connexion » n'affiche pas le bouton Transférer.

  [NSHELP-32614]

- L'appliance NetScaler se bloque lors du traitement de la demande de déconnexion POST /Citrix-AuthService/AuthService.asmx depuis le serveur StoreFront lorsque l'URL de rappel est configurée sur StoreFront.

  [NSHELP-32207]

- Dans un dispositif NetScaler Gateway, les paramètres VPN globaux ne prennent pas effet s'ils ne sont pas définis au niveau de l'action de session.

  Avant de mettre à niveau votre configuration de haute disponibilité, assurez-vous de désactiver manuellement la synchronisation HA sur l'appliance secondaire. Pour plus de détails, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-ha-pair.html

  [NSHELP-31478, CGOP-21737]

- Le titre de la page de connexion à NetScaler Gateway et les thèmes du portail ne s'affichent pas correctement.

  [NSHELP-29202]

- Lors de la configuration du pool IIP (adresse IP et masque), si l'adresse IP ne correspond pas à la première adresse IP de la plage, la CLI et l'interface graphique de NetScaler n'affichent qu'un seul bloc et pas tous.

  Exemple :
  bind vpn vserver vpn_ssl -intranetIP 172.168.1.1 255.255.255.0
  bind vpn vserver vpn_ssl -intranetIP 172.168.2.1 255.255.255.0

  Dans ce cas, l'interface de ligne de commande ou l'interface graphique affichée lors de l'affichage du serveur vpn vpn_ssl affiche uniquement le pool 172.168.2.1 et non 172.168.2.2.

  [NSHELP-29084]

Web App Firewall NetScaler

- Une appliance NetScaler autonome ou le mode secondaire d'une configuration HA peut se bloquer si vous configurez un objet de signature pour NetScaler Web App Firewall sur les versions logicielles suivantes :

  - 13.0 build 88.5 et versions ultérieures
  - 13.1 build 33.41 et versions ultérieures

  [NSHELP-33250]

- Une mise à jour de signature WAF échoue lorsqu'un serveur proxy et un port proxy sont configurés. Pendant le processus de mise à jour automatique des signatures qui s'exécute toutes les heures, l'appliance ADC contacte l'hôte de mise à jour automatique pour télécharger les fichiers mis à jour au lieu de passer par le serveur proxy et le port proxy configurés. Par conséquent, un échec de mise à jour est observé lorsque l'hôte de mise à jour automatique n'est pas accessible.

  [NSHELP-32613]

- L'appliance NetScaler peut se bloquer si les conditions suivantes sont remplies :

  - La charge sur l'appareil est élevée.
  - Des modifications de configuration sont en cours.
  - La suppression d'une signature prend beaucoup de temps.

  [NSHELP-32454]

- Les attaques par répétition d'une session par empreinte digitale d'un appareil bot sont enregistrées plutôt que supprimées.

  [NSHELP-31949]

Équilibrage de charge

- Toute modification apportée au groupe de services entraîne des modifications du hachage des cookie lorsque l' `useencryptedPersistenceCookie` option est activée dans la `set lb param` commande.

  [NSHELP-32697]

- Dans de rares cas, une appliance NetScaler peut se bloquer et générer un core dump lorsque la persistance basée sur l'ID de session SSL et le traitement basé sur les tickets de session SSL sont activés sur un serveur virtuel de commutation de contenu.

  [NSHELP-32228]

- L'état du moniteur LDAP reste actif même si les attributs configurés ne sont pas présents sur le serveur.

  [NSHELP-32025]

Divers

- Lorsqu'il `ns_hw_err.bash` est exécuté sur une appliance NetScaler pour détecter des problèmes matériels, l'erreur « Disque dur introuvable lors du démarrage » peut apparaître même

lorsqu'un disque sain est présent.

[NSHELP-31571]

- Un nœud de cluster entre dans une boucle de paquets lorsque les conditions suivantes sont remplies :
  - Un paquet UDP avec une adresse IP de destination sous la forme CLIP est envoyé à un nœud de cluster.
  - Le CCO a changé d'un nœud à l'autre pendant la durée de vie de l'instance de cluster.

[NSHELP-30804]

Réseau

- NetScaler CPX ne parvient pas à récupérer la configuration d'itinéraire par défaut après un crash lorsque vous utilisez la configuration de démarrage basée sur des fichiers avec ConfigMaps. Ce comportement entraîne une perte de connectivité.

  [NSNET-27124]

- L'appliance NetScaler peut ajouter une somme de contrôle IP incorrecte à l'en-tête IP des paquets UDP.

  [NSHELP-32587]

- Dans une configuration de cluster NetScaler BLX, VTYSH peut ne pas démarrer si les conditions suivantes sont remplies :
  - L'hôte Linux est redémarré, ce qui entraîne une mise en boucle du processus NetScaler BLX Route Health Injection (RHI).

  [NSHELP-32473]

- Lorsque vous supprimez un serveur virtuel, l'appliance NetScaler définit incorrectement l'état VIP RHI associé sur DOWN si les conditions suivantes sont remplies :
  - Le serveur virtuel possède des serveurs virtuels de sauvegarde.
  - Le serveur virtuel est à l'état DOWN et au moins un serveur virtuel de sauvegarde est à l'état UP.

  [NSHELP-29972]

Plateforme

- Une appliance NetScaler exécutée sur un processeur AMD peut se bloquer au démarrage, lorsque vous mettez à niveau la version logicielle vers la version 13.1 build 30.x.

  [NSPLAT-24968, NSHELP-32808]

- Le basculement haute disponibilité ne fonctionne pas dans les clouds AWS et GCP. Le processeur de gestion peut atteindre 100 % de sa capacité dans les clouds AWS et GCP, ainsi que dans NetScaler VPX sur site. Ces deux problèmes sont provoqués lorsque les conditions suivantes sont remplies :

  1. Lors du premier démarrage de l'appliance NetScaler, vous n'enregistrez pas le mot de passe demandé.
  2. Ensuite, vous redémarrez l'appliance NetScaler.

  [NSPLAT-22013]

- Lorsqu'une appliance NetScaler SDX contenant des cartes réseau Mellanox est mise à niveau à partir d'une version dans laquelle le filtrage VLAN est désactivé et que le service de gestion tente de désactiver le filtrage VLAN dans le cadre de la mise à niveau, l'opération échoue. Par conséquent, le filtrage VLAN est activé pour toutes les interfaces et tous les canaux.

  [NSHELP-32759]

- Après une mise à niveau du microprogramme, l'interface de gestion d'une appliance NetScaler MPX 5900/8900 peut tomber en panne. Par conséquent, l'appliance est inaccessible.

  [NSHELP-31587]

Stratégies

- Une appliance NetScaler peut se bloquer lors de l'ajout d'une politique avec patset lorsque les conditions suivantes sont remplies :

  – L'indicateur associé à NSB est défini dans le mauvais ordre pour le scénario Rewrite TCP.

  [NSHELP-31064]

SSL

- Lorsqu'un serveur virtuel reçoit un enregistrement TLS 1.3 dont le remplissage n'est pas valide, il envoie une alerte fatale « decode_error » au lieu d'une alerte « message inattendu ».

  [NSSSL-11890]

- Sur les plateformes NetScaler MPX et SDX dotées d'un matériel d'accélération cryptographique compatible Intel QAT, le type de persistance SOURCEIP est appliqué de manière incohérente aux demandes envoyées aux serveurs virtuels via des connexions TLS 1.3. En d'autres termes, les demandes envoyées depuis une adresse IP source unique peuvent être distribuées à plusieurs serveurs principaux différents.

  [NSHELP-32410, NSHELP-32895, NSHELP-32572, NSHELP-32688]

- Une appliance NetScaler contenant une carte SSL Cavium peut se bloquer lors de l'envoi d'un message d'alerte DTLS au client.

  [NSHELP-32031]

- Une appliance NetScaler peut se bloquer si la règle d'authentification par certificat est évaluée et déclenchée deux fois lors de la même demande.

  [NSHELP-31785]

Système

- Vous pouvez activer la fonctionnalité AppFlow dans la partition d'administration uniquement après avoir activé le mode ULFD dans la partition par défaut.

  [NSHELP-32670]

- L'appliance NetScaler peut traiter une demande HTTP comme une demande non valide lorsqu'une méthode de requête HTTP partielle est présente dans un segment TCP entrant.

  [NSHELP-32462]

- Une appliance NetScaler peut se bloquer si les conditions suivantes sont remplies :
  - Lors de combinaisons HTTP2 et SSL à forte utilisation de la mémoire, l'appliance NetScaler ne parvient pas à allouer de la mémoire.

  [NSHELP-32255]

- Une appliance NetScaler se bloque dans une configuration VPN lorsque la capture de paquets nstrace est démarrée avec des filtres IP ou PORT.

  [NSHELP-31790]

- Un client gRPC ne parvient pas à analyser l'en-tête d'état du gRPC lorsque la condition suivante est remplie :
  - L'en-tête d'état gRPC est ajouté à la fois dans l'en-tête de début et dans l'en-tête de fin au lieu d'être ajouté uniquement dans l'en-tête de fin.

  [NSHELP-31640]

- Lorsque SACK est activé, l'appliance NetScaler ne retransmet pas le dernier segment TCP d'un octet de la liste de retransmission pour la raison suivante : l'appliance utilise le dernier segment TCP d'un octet comme segment fictif pour marquer la fin de la liste de retransmission.

  [NSHELP-28778]

Interface utilisateur

- Vous ne pouvez pas lier un service GSLB à un serveur virtuel GSLB à l'aide de l'interface graphique de NetScaler car la liste des services GSLB sous GSLB Service Binding> GSLB **Service Binding > GSLB Services s'affiche vide.**

  [NSHELP-32236]

- La modification d'un itinéraire statique à l'aide de l'interface graphique NetScaler (système > réseau > routes) peut échouer de manière incorrecte avec le message d'erreur suivant :

  - « Argument requis manquant [passerelle] »

  [NSHELP-32024]

- Dans une configuration HA/Cluster, la synchronisation de la configuration échoue si vous avez configuré des clés SSH autres que RSA. Par exemple, les clés ECDSA ou DSA.

  [NSHELP-31675]

- Dans l'interface graphique de NetScaler, s'il existe une destination d' **interruptions SNMP existante sous System>SNMP>Traps**, la modification de cette destination échoue avec le message d'erreur suivant :

  - « Erreur lors de la récupération du trap SNMP »

  [NSHELP-31661]

- L'interface graphique de l'appliance NetScaler n'affiche pas le nombre correct des politiques IDP SAML et OAuth configurées.

  [NSHELP-31480]

- Dans une appliance NetScaler, lors de l'utilisation de l'interface graphique, le problème suivant apparaît sur la page de politique du répondeur :

  - Les stratégies de réponse personnalisées créées peuvent être affichées sous les stratégies de réponse intégrées.

  [NSHELP-31428]

- Dans une configuration NetScaler HA, le problème suivant est observé dans l'interface graphique de NetScaler après avoir enregistré une configuration et cliqué sur le bouton d'actualisation :

  - L'interface graphique affiche de manière incorrecte le point orange sur le bouton Enregistrer, même si aucune modification de configuration non enregistrée n'est présente sur l'appliance.

  [NSHELP-30031]

- Les statistiques du serveur virtuel GSLB ne sont pas disponibles en mode partition d'administration.

  [NSHELP-28524]

- Une appliance NetScaler qui a retiré des licences auprès de NetScaler ADM passe en période de grâce lorsqu'elle se déconnecte d'ADM. L'appliance apparaît sans licence dans ADM et continue pendant la période de grâce, même après sa reconnexion à ADM.

  [NSCONFIG-7098]

Problèmes connus

Les problèmes qui existent dans la version 13.1-33.54.

AppFlow

- HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

  [NSINSIGHT-943]

Authentification, autorisation et audit

- L'authentification de passerelle via un client CWA ou des clients VPN natifs peut échouer en raison de chaînes manquantes dans le `ns_aaa_relaystate_param_whitelist` patset.

  Solution :

  ```
  bind policy patset ns_aaa_relaystate_param_whitelist "citrixauthwebviewdone
  ://"-index 1 -charset ASCII

  bind policy patset ns_aaa_relaystate_param_whitelist "citrixsso://"-
  index 2 -charset ASCII

  bind policy patset ns_aaa_relaystate_param_whitelist "citrixng://"-
  index 3 -charset ASCII
  ```

  [NSHELP-33054]

- L'appliance NetScaler supprime le suffixe du jeu de caractères dans l'en-tête Content-Type et l'envoie `Content-Type: application/x-www-form-urlencoded` si vous avez configuré les deux options suivantes.

  - Authentification basée sur un formulaire SSO
  - `nsapimgr knob - nsapimgr_wr.sh -ys call=ns_formsso_use_ctype_simple_enable knob`

[NSHELP-31977]

- Vous pouvez rencontrer des problèmes lors de la déconnexion si l'authentification SAML est configurée.

  [NSHELP-31962]

- Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

  [NSHELP-563]

- Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante. `show adfsproxyprofile <profile name>`

  Solution : Connectez-vous au principal NetScaler actif du cluster et exécutez la commande. `show adfsproxyprofile <profile name>` Il afficherait l'état du profil proxy.

  [NSAUTH-5916]

- La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

  - L'option Tester l'accessibilité LDAP est ouverte.
  - Les informations d'identification de connexion non valides sont renseignées et envoyées.
  - Les identifiants de connexion valides sont renseignés et envoyés.

  Solution : fermez et ouvrez l'option Tester l'accessibilité LDAP.

  [NSAUTH-2147]

Mise en cache

- Une appliance NetScaler se bloque lorsque le contenu mis en cache est diffusé aux clients.

  [NSHELP-31760]

- Une appliance NetScaler peut se bloquer si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

  [NSHELP-22942]

Appliance NetScaler SDX

- Des pertes de paquets sont visibles sur une instance VPX hébergée sur une appliance NetScaler SDX si les conditions suivantes sont remplies :

  - Le mode d'allocation du débit est en rafale.

- Il existe une grande différence entre le débit et la capacité maximale de rafale.

[NSHELP-21992]

NetScaler Gateway

- Le client Citrix Secure Access, version 21.7.1.2 et versions ultérieures, ne parvient pas à effectuer la mise à niveau vers des versions ultérieures pour les utilisateurs ne disposant pas de droits d'administration. Ce problème s'applique uniquement si la mise à niveau du client Citrix Secure Access est effectuée à partir d'une appliance NetScaler.

  [NSHELP-32793]

- Lorsque les utilisateurs cliquent sur l'onglet Page d'accueil de l'écran Citrix Secure Access pour Windows, la page affiche l'erreur de refus de connexion.

  [NSHELP-32510]

- Sur un appareil Mac utilisant Chrome, l'extension VPN se bloque lors de l'accès à deux noms de domaine complets.

  [NSHELP-32144]

- Les utilisateurs ne peuvent pas se connecter au VPN en raison de défaillances intermittentes de l'EPA.

  [NSHELP-32138]

- L'authentification nFactor avec un certificat client facultatif échoue lorsqu'il n'existe aucun certificat client approprié sur l'appareil.

  [NSHELP-32127]

- L'appliance NetScaler Gateway peut se bloquer si HDX Insight est activé.

  [NSHELP-32120]

- Dans une configuration en cluster, l'appliance NetScaler se bloque lors de l'envoi de la requête CGP_FINISH_REQUEST au client.

  [NSHELP-32029]

- Lorsque des sessions UDP sont lancées, des connexions périmées semblent exister même après la fermeture des sessions. Cependant, il ne s'agit pas de véritables connexions périmées, mais d'un problème avec le compteur.

  [NSHELP-32009]

- Dans certains cas, si les paramètres de proxy sont vides dans NetScaler Gateway version 13.0 ou 13.1, Citrix SSO crée des paramètres de proxy incorrects.

  [NSHELP-31970]

- Le contrôle de journalisation des débogues pour le client Citrix Secure Access est désormais indépendant de NetScaler Gateway et peut être activé ou désactivé depuis l'interface utilisateur du plug-in pour la machine et le tunnel utilisateur.

  [NSHELP-31968]

- Le lien de la page d'accueil sur l'interface utilisateur de Citrix Secure Access ne fonctionne pas si Microsoft Edge est le navigateur par défaut.

  [NSHELP-31894]

- Lorsqu'un utilisateur ouvre une session sur l'appliance NetScaler et que Citrix Workspace n'est pas installé, le lien permettant de télécharger Citrix Workspace pointe de manière incorrecte vers Citrix Receiver.

  [NSHELP-31877]

- Les enregistrements d'échec d'authentification de Gateway Insight indiquent que le nom d'utilisateur est « Anonymous » lorsque NOAUTH est configuré comme premier facteur et que l'authentification du second facteur échoue en raison d'informations d'identification non valides. Ce problème se produit uniquement si la configuration est effectuée à l'aide du visualiseur nFactor car le premier facteur est configuré en tant que NOAUTH, par conception dans le visualiseur nFactor.

  [NSHELP-31795]

- Les connexions directes aux ressources situées en dehors du tunnel établi par Citrix Secure Access peuvent échouer en cas de retard ou de congestion important.

  [NSHELP-31598]

- Le message personnalisé du journal des défaillances EPA ne s'affiche pas sur le portail NetScaler Gateway. Au lieu de cela, le message « erreur interne » s'affiche.

  [NSHELP-31434]

- Parfois, l'ouverture de session automatique de Windows ne fonctionne pas lorsqu'un utilisateur se connecte à l'ordinateur Windows en mode de service permanent. Le tunnel de la machine ne passe pas au tunnel utilisateur et au message « Connexion… » s'affiche dans l'interface utilisateur du plug-in VPN.

  [NSHELP-31357, CGOP-21192]

- Les stratégies de routage basé sur des stratégies (PBR) ne prennent pas effet pour le trafic DNS via VPN.

  [NSHELP-31123]

- Lorsque Always on est configuré, le tunnel utilisateur échoue en raison du numéro de version incorrect (1.1.1.1) dans le fichier aoservice.exe.

[NSHELP-30662]

- Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil « NetworkAccessOnVPNFailure » de « FullAccess » à « OnlyToGateway ».

  [NSHELP-30236]

- La page d'accueil de la passerelle ne s'affiche pas immédiatement après que le plug-in de passerelle a réussi à établir le tunnel VPN. Pour résoudre ce problème, la valeur de registre suivante est introduite.

  HKLMSoftwareCitrixSecure Access ClientSecureChannelResetTimeoutSeconds
  Type: DWORD

  Par défaut, cette valeur de registre n'est ni définie ni ajoutée. Lorsque la valeur de « SecureChannelResetTimeoutSeconds » est 0 ou n'est pas ajoutée, le correctif pour gérer le délai ne fonctionne pas, ce qui est le comportement par défaut. L'administrateur doit définir ce registre sur le client pour activer le correctif (c'est-à-dire afficher la page d'accueil immédiatement après que le plug-in de passerelle ait établi le tunnel VPN avec succès).

  [NSHELP-30189]

- Le client VPN Windows n'honore pas l'alerte « Notification de fermeture SSL » du serveur et envoie la demande de connexion de transfert sur la même connexion.

  [NSHELP-29675]

- Lors de la configuration du pool IIP (adresse IP et masque), si l'adresse IP ne correspond pas à la première adresse IP de la plage, la CLI et l'interface graphique de NetScaler n'affichent qu'un seul bloc et pas tous.

  Exemple :
  bind vpn vserver vpn_ssl -intranetIP 172.168.1.1 255.255.255.0
  bind vpn vserver vpn_ssl -intranetIP 172.168.2.1 255.255.255.0

  Dans ce cas, l'interface de ligne de commande ou l'interface graphique affichée lors de l'affichage du serveur vpn vpn_ssl affiche uniquement le pool 172.168.2.1 et non 172.168.2.2.

  Solution : utilisez la première adresse IP de la plage pour configurer les blocs IIP.

  Exemple :

  bind vpn vserver vpn_ssl -intranetIP 172.168.1.0 255.255.255.0
  bind vpn vserver vpn_ssl -intranetIP 172.168.2.0 255.255.255.0

  [NSHELP-29084]

- Dans certains cas, le code de validation du serveur échoue lorsque le certificat de serveur est approuvé. Par conséquent, les utilisateurs finaux ne peuvent pas accéder à la passerelle.

  [NSHELP-28942]

- Vous remarquerez peut-être certaines adresses IP internes de Citrix dans le fichier rdx.js.

  [NSHELP-28682]

- L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

  [NSHELP-28551]

- Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

  [NSHELP-28404]

- Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

  - L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
  - L'appliance est configurée pour l'authentification basée sur des certificats avec l'authentification à deux facteurs « désactivée »

  [NSHELP-23584]

- Parfois, lorsque vous parcourez les schémas, le message d'erreur « Impossible de lire le type de propriété non défini » apparaît.

  [NSHELP-21897]

- La commande « show vpn icaconnection » n'affiche pas correctement les numéros de série des connexions ICA. Ce problème se produit car le numéro de série est réinitialisé arbitrairement lorsque la commande « show vpn icaconnection » est exécutée.

  [CGOP-22205]

- Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

  [CGOP-19355]

- L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

  [CGOP-13621]

- Le rapport Gateway Insight affiche de manière incorrecte la valeur « Local » au lieu de « SAML » dans le champ Type d'authentification en cas d'échec d'erreur SAML.

  [CGOP-13584]

- Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

  [CGOP-13511]

- Lorsqu'une connexion ICA est lancée à partir d'un Receiver MAC version 19.6.0.32 ou Citrix Virtual Apps and Desktops version 7.18, la fonctionnalité HDX Insight est désactivée.

  [CGOP-13494]

- Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

  [CGOP-13493]

- Lors de l'acceptation des connexions hôtes locales depuis le navigateur, la boîte de dialogue Accepter la connexion pour macOS affiche le contenu en anglais, quelle que soit la langue sélectionnée.

  [CGOP-13050]

- Le texte « Page d'accueil » dans l' application Citrix SSO > Page d'accueil est tronqué pour certaines langues.

  [CGOP-13049]

- Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

  [CGOP-11830]

- Dans Outlook Web App (OWA) 2013, le fait de cliquer sur **Options** dans le menu Paramètres affiche une boîte de dialogue **Erreur critique** . De plus, la page ne répond plus.

  [CGOP-7269]

Web App Firewall NetScaler

- NetScaler Web App Firewall met parfois du temps à détecter l'injection de commande. Par conséquent, Pitboss redémarre l'appliance NetScaler.

  [NSHELP-32654]

- Les attaques par répétition d'une session par empreinte digitale d'un appareil bot sont enregistrées plutôt que supprimées.

  [NSHELP-31949]

Équilibrage de charge

- Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

  [NSLB-7679]

- L'appliance NetScaler ne répond pas avec l'adresse IP de service correcte pour la requête de domaine GSLB si les paramètres suivants sont configurés sur le serveur virtuel GSLB :

  1. L'option ECS est activée.
  2. La proximité statique est configurée comme méthode d'équilibrage de charge.

  [NSHELP-32879]

- Une appliance NetScaler peut se bloquer et vider le noyau si le script de surveillance utilisateur renvoie une réponse de plus de 1 024 octets.

  [NSHELP-32097]

- L'état du moniteur LDAP reste actif même si les attributs configurés ne sont pas présents sur le serveur.

  [NSHELP-32025]

- En raison d'une situation de concurrence rare, il peut y avoir des incohérences entre le site local et le site distant. Cette incohérence peut être due au fait que le site distant n'apprend pas le membre dynamique à partir du site local.

  La suppression des membres dynamiques sur le site distant peut échouer en raison d'un problème lors de la communication entre les moteurs de paquets.

  [NSHELP-31982]

- Les requêtes SNMP WALK correspondant à l'OID vServerAdvancessLConfigTable génèrent un vidage du cœur lorsque l'ordre de priorité des serveurs virtuels est configuré.

  [NSHELP-31704]

- Le format ServiceGroupName utilisé dans le trap `entityofs` pour le groupe de services est le suivant :
  `<service(group)name>?<ip/DBS>?<port>`

  Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (« ? ») est utilisé comme séparateur. NetScaler envoie le piège avec le point d'interrogation (« ? «). Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

  [NSHELP-28080]

- Dans certains scénarios, les serveurs liés à un groupe de services affichent une valeur de cookie non valide. Vous pouvez voir la valeur de cookie correcte dans les journaux de suivi.

  [NSHELP-21196]

Divers

- Lorsqu'une synchronisation forcée a lieu dans une configuration à haute disponibilité, l'appliance exécute la commande « set urlfiltering parameter » dans le nœud secondaire.
  Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre « TimeOfDaytoUpdateDB ».

  [NSSWG-849]

- Le registre de liste AlwaysOnAllow ne fonctionne pas comme prévu si la valeur du registre est supérieure à 2000 octets.

  [NSHELP-31836]

- Un nœud de cluster entre dans une boucle de paquets lorsque les conditions suivantes sont remplies :

  - Un paquet UDP avec une adresse IP de destination sous la forme CLIP est envoyé à un nœud de cluster.
  - Le CCO a changé d'un nœud à l'autre pendant la durée de vie de l'instance de cluster.

  Solution : vous pouvez éviter ou mettre fin à cette boucle de paquets en appliquant une ACL de suppression pour ce paquet UDP spécifique avec l'adresse IP de destination comme adresse CLIP.

  [NSHELP-30804]

- Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

  [NSHELP-22409]

Réseau

- Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

  [NSNET-25299]

- Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :

- L'appliance NetScaler BLX est dotée d'un faible nombre de « pages volumineuses ». Par exemple, 1G.
- L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

Le problème est enregistré sous forme de message d'erreur dans « /var/log/ns.log » :

- « BLX-DPDK:DPDK Mempool n'a pas pu être initialisé pour PE-x »

Remarque : x est un nombre <= nombre de processus de travail.

Solution : allouez un grand nombre de « pages volumineuses », puis redémarrez l'appliance.

[NSNET-25173]

- Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

  [NSNET-24449]

- Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

  - Désactiver
  - Activer
  - Réinitialiser

  [NSNET-16559]

- L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

  « Les paquets suivants ont des dépendances non satisfaites : blx-core-libs:i386 : PreDepends : libc6:i386 (>= 2.19) mais ils ne sont pas installables »

  Solution : exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

  - dpkg –add-architecture i386
  - apt-get update
  - apt-get dist-upgrade
  - apt-get install libc6:i386

  [NSNET-14602]

- Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

- Lorsque ECMP est configuré sur une appliance NetScaler, le problème suivant peut être observé pour une connexion d'équilibrage de charge SSH :
  - L'appliance NetScaler envoie le premier paquet via un itinéraire différent de celui utilisé pour les autres paquets du même flux.

  [NSHELP-32089]

- L'appliance NetScaler peut se bloquer dans certains scénarios lorsque les conditions suivantes sont remplies :
  - L'appliance NetScaler reçoit plusieurs premiers fragments avec des décalages différents.
  - L'appliance NetScaler ne réassemble pas les fragments.

  [NSHELP-32084]

- Dans une configuration d'équilibrage de charge avec l'option « sans session » activée sur le serveur virtuel et l'ECMP côté serveur, le problème suivant peut être observé :
  - L'appliance NetScaler envoie les paquets à un serveur toujours par le même itinéraire.

  [NSHELP-32061]

- L'appliance NetScaler peut se bloquer si toutes les conditions suivantes sont remplies :
  - L'ACL basé sur le TTL expire
  - L'appliance NetScaler dispose d'un grand nombre de listes de contrôle d'accès configurées.

  [NSHELP-31307]

- Lorsque vous supprimez un serveur virtuel, l'appliance NetScaler définit incorrectement l'état VIP RHI associé sur DOWN si les conditions suivantes sont remplies :
  - Le serveur virtuel possède des serveurs virtuels de sauvegarde.
  - Le serveur virtuel est à l'état DOWN et au moins un serveur virtuel de sauvegarde est à l'état UP.

  [NSHELP-29972]

- Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

  [NSHELP-21082]

Plateforme

- Le basculement haute disponibilité ne fonctionne pas dans les clouds AWS et GCP. Le processeur de gestion peut atteindre 100 % de sa capacité dans les clouds AWS et GCP, ainsi que dans NetScaler VPX sur site. Ces deux problèmes sont provoqués lorsque les conditions suivantes sont remplies :

  1. Lors du premier démarrage de l'appliance NetScaler, vous n'enregistrez pas le mot de passe demandé.
  2. Ensuite, vous redémarrez l'appliance NetScaler.

  [NSPLAT-22013]

- Lorsque vous effectuez une mise à niveau d'une version 13.0/12.1/11.1 vers une version 13.1 ou que vous rétrogradez d'une version 13.1 vers une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances NetScaler. Ce problème est résolu pour les versions suivantes de NetScaler :

  - 13.1-4.x
  - 13.0-82.31 et versions ultérieures
  - 12.1-62.21 et versions ultérieures

  Les packages python ne sont pas installés lorsque vous rétrogradez les versions de NetScaler de 13.1-4.x vers l'une des versions suivantes :

  - Toute version 11.1
  - 12.1-62.21 et versions antérieures
  - 13.0-81.x et versions antérieures

  [NSPLAT-21691]

- Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande « rm cloudprofile » pour supprimer le profil.

  [NSPLAT-4520]

- Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
  Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

  [NSPLAT-4451]

- Sur la plate-forme NetScaler SDX 8015/8400/8600, vous pouvez constater une augmentation de la consommation de mémoire sur Xen Server.

Solution : exécutez la commande suivante sur Xen Server, puis redémarrez l'appliance. /opt/xensource/libexec/xen-cmdline –set-xen "dom0_mem=1024M,max:1024M"

[NSHELP-32260]

- À partir de la version 13.1 de NetScaler, l'appliance NetScaler ne démarre pas dans un hyperviseur ESXi doté de plus de 8 interfaces réseau VMXNET3.

  [NSHELP-31266]

Stratégies

- Les connexions peuvent être bloquées si la taille du traitement des données est supérieure à la taille de la mémoire tampon TCP par défaut configurée.

  Solution : définissez la taille de la mémoire tampon TCP sur la taille maximale des données à traiter.

  [NSPOLICY-1267]

- Dans une appliance NetScaler, les politiques de commutation de contenu qui sont migrées des politiques classiques vers des politiques avancées à l'aide de l'outil NSPEPI peuvent ne pas fonctionner lorsque les conditions suivantes sont remplies :

  - Les stratégies sont liées au vserver de commutation de contenu.
  - Le paramètre « CaseSensitive » est réglé sur OFF.

  [NSHELP-31951]

- Une appliance NetScaler peut se bloquer lors de l'ajout d'une politique avec patset lorsque les conditions suivantes sont remplies :

  - L'indicateur associé à NSB est défini dans le mauvais ordre pour le scénario Rewrite TCP.

  [NSHELP-31064]

SSL

- Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

  Solution :

  1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
  2. Enregistrez la configuration.

  [NSSSL-9572]

- Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

  [NSSSL-6478]

- Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

  [NSSSL-6213]

- Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
  ERREUR : actualisation de la CRL désactivée

  [NSSSL-6106]

- L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

  [NSSSL-4427]

- Un message d'avertissement incorrect, « Avertissement : aucun chiffrement utilisable configuré sur le serveur/service SSL » s'affiche si vous essayez de modifier le protocole ou le chiffrement SSL dans le profil SSL.

  [NSSSL-4001]

- Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

  [NSSSL-3184, NSSSL-1379, NSSSL-1394]

- Une appliance NetScaler contenant une carte SSL Cavium peut se bloquer lors de l'envoi d'un message d'alerte DTLS au client.

  [NSHELP-32031]

- Une poignée de main SSL peut échouer si la séquence de conditions suivante est remplie :

  1. Hello Verify Request (HVR) est activé sur DTLS.
  2. L'appliance NetScaler envoie un HVR au client.
  3. Le client ne reçoit pas le HVR.
  4. Le client essaie de retransmettre le bonjour au premier client au lieu de répondre au HVR avec un cookie de session.

  Remarque : En réponse au message d'accueil retransmis au client, l'appliance ADC envoie le HVR au client trois fois au maximum. Si aucune réponse appropriée n'est reçue, l'appliance échoue à la négociation.

  [NSHELP-31808]

- Une appliance NetScaler peut se bloquer si la règle d'authentification par certificat est évaluée et déclenchée deux fois lors de la même demande.

  [NSHELP-31785]

- L'interface graphique de NetScaler, accessible via une adresse IP de cluster (CLIP), n'affiche pas les liaisons de certificat de serveur vers un serveur virtuel SSL.

  [NSHELP-31602]

- La vérification de la réponse OCSP peut échouer lors d'une interception SSL si aucun certificat CA valide n'est présent dans le bundle de certificats par défaut. L'échec se produit parce que la vérification de la réponse OCSP a été effectuée de manière incorrecte en utilisant le bundle de certificats par défaut au lieu du bundle de certificats configuré.

  [NSHELP-30594]

- Une appliance NetScaler peut se bloquer lors du traitement du trafic SSL en mode logiciel.

  [NSHELP-29996]

Système

- Dans une appliance NetScaler, la structure de modification de l'en-tête entraîne une corruption de la mémoire. Cette condition se produit lorsque les cookies qui doivent être consommés par l'appliance NetScaler sont supprimés dans un ordre particulier avant d'être transférés.

  [NSHELP-32799]

- Dans une appliance NetScaler, la valeur par défaut du paramètre « MaxHeaderFieldLen » dans le profil HTTP provoque le problème suivant.
  - Échec du trafic après la mise à niveau vers la version 13.0

  [NSHELP-32079]

- Une appliance NetScaler peut se bloquer lorsque AppFlow est activé uniquement côté client.

  [NSHELP-31892]

- L'appliance NetScaler configurée avec un service SSL se bloque lorsqu'elle reçoit un paquet de contrôle TCP FIN suivi d'un paquet de contrôle TCP RESET.

  [NSHELP-31656]

- Un client gRPC ne parvient pas à analyser l'en-tête d'état du gRPC lorsque la condition suivante est remplie :
  - L'en-tête d'état gRPC est ajouté à la fois dans l'en-tête de début et dans l'en-tête de fin au lieu d'être ajouté uniquement dans l'en-tête de fin.

[NSHELP-31640]

- Un RTT élevé est observé pour une connexion TCP si la condition suivante est remplie :
  - une fenêtre de congestion maximale élevée (> 4 Mo) est définie
  - L'algorithme TCP NILE est activé

  Pour qu'une appliance NetScaler utilise l'algorithme NILE pour le contrôle de la congestion, les conditions doivent dépasser le seuil de démarrage lent, qui est associé à la fenêtre de congestion maximale

  Ainsi, jusqu'à ce que la fenêtre de congestion maximale configurée soit atteinte, NetScaler continue d'accepter des données et se retrouve avec un RTT élevé.

  [NSHELP-31548]

- Dans une appliance NetScaler, le problème suivant est observé lors de l'activation de la configuration HTTP/2 pour une adresse IP virtuelle (VIP) de commutation de contenu ou d'équilibrage de charge.
- Lorsque vous utilisez la fonction d'inspection du contenu, l'insertion de l'en-tête Rewrite avec charge utile risque de ne pas fonctionner correctement.

  [NSHELP-30088]

- La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client.

  [NSHELP-21240]

- Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

  [NSHELP-10972]

- Dans un déploiement de cluster, si vous exécutez la commande « forcer la synchronisation du cluster » sur un nœud non CCO, le fichier ns.log contient des entrées de journal dupliquées.

  [NSBASE-16304, NSGI-1293]

- Lorsque vous installez NetScaler ADM sur un cluster Kubernetes, cela ne fonctionne pas comme prévu car les processus requis peuvent ne pas s'exécuter.

  Solution : redémarrez le module Gestion.

  [NSBASE-15556]

- L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

  [NSBASE-8506]

Interface utilisateur

- Pour la fonction de réécriture MQTT, vous ne pouvez pas supprimer une expression à l'aide de l'éditeur d'expression dans l'interface graphique.

  Solution : utilisez la commande d'ajout ou de modification d'action de type MQTT via l'interface de ligne de commande.

  [NSUI-18049]

- Dans l'interface graphique de NetScaler, le lien « Aide » présent sous l'onglet « Tableau de bord » est cassé.

  [NSUI-14752]

- L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

  Solution : configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de l'interface de ligne de commande NetScaler.

  [NSUI-13024]

- Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

  [NSUI-6838]

- Après avoir créé un profil pour NetScaler Web App Firewall et essayé de générer le rapport de configuration du pare-feu d'applications dans **Système > Rapports**, l'erreur suivante s'affiche :

  « Impossible de charger le document PDF. »

  [NSHELP-32469]

- Dans une configuration haute disponibilité (HA), lors de la récupération de l'adresse IP locale pour l'outil nsconf, le problème suivant est observé.

  - Échec de la connexion à l'hôte local. Cet échec se produit si le mot de passe du nœud RPC est différent pour les nœuds principaux et secondaires dans la configuration HA.

  Solution : dans une configuration HA, assurez-vous que le mot de passe du nœud RPC pour le nœud principal et le nœud secondaire est identique.

  [NSHELP-32083]

- Dans la version 13.0 de NetScaler, le bouton **OK** de la page **Configurer le service de serveur virtuel d'équilibrage de charge prioritaire** est grisé.

  [NSHELP-32007]

- La page de connexion de l'appliance NetScaler peut ne pas afficher le nom d'utilisateur valide une fois que l'utilisateur s'est connecté.

  [NSHELP-31759]

- Dans une configuration HA/Cluster, la synchronisation de la configuration échoue si vous avez configuré des clés SSH autres que RSA. Par exemple, les clés ECDSA ou DSA.

  [NSHELP-31675]

- Dans l'interface graphique de NetScaler, s'il existe une destination d' **interruptions SNMP existante sous System>SNMP>Traps**, la modification de cette destination échoue avec le message d'erreur suivant :

  - « Erreur lors de la récupération du trap SNMP »

  [NSHELP-31661]

- L'interface graphique de l'appliance NetScaler n'affiche pas le nombre correct des politiques IDP SAML et OAuth configurées.

  [NSHELP-31480]

- Dans une appliance NetScaler, lors de l'utilisation de l'interface graphique, le problème suivant apparaît sur la page de politique du répondeur :

  - Les stratégies de réponse personnalisées créées peuvent être affichées sous les stratégies de réponse intégrées.

  [NSHELP-31428]

- Dans une configuration NetScaler HA, le problème suivant est observé dans l'interface graphique de NetScaler après avoir enregistré une configuration et cliqué sur le bouton d'actualisation :

  - L'interface graphique affiche de manière incorrecte le point orange sur le bouton Enregistrer, même si aucune modification de configuration non enregistrée n'est présente sur l'appliance.

  [NSHELP-30031]

- Les statistiques du serveur virtuel GSLB ne sont pas disponibles en mode partition d'administration.

  [NSHELP-28524]

- Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

  - Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

Solution : effectuez un basculement HA manuel successif uniquement une fois la synchronisation HA terminée (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

- Dans une configuration à haute disponibilité des appliances NetScaler BLX, le nœud principal peut ne plus répondre en bloquant toute demande de CLI ou d'API.

  Solution : redémarrez le nœud principal.

  [NSCONFIG-6601]

- Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

  1. Mettez à niveau l'appliance NetScaler vers l'une des versions
     - 13.0 52.24 build
     - 12.1 57.18 build
     - 11.1 65.10 build
  2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
  3. Rétrogradez l'appliance NetScaler vers une version antérieure.

  Pour afficher la liste de ces utilisateurs du système à l'aide de l'interface de ligne de commande : À l'invite de commandes, tapez :

  ```
  query ns config -changedpassword [-config <full path of the configuration
   file (ns.conf)>]
  ```

  Solution : Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

  - Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
  - Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
  - Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

  Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html.

  [NSCONFIG-3188]

Notes de publication pour la version 13.1—30.52 de NetScaler

May 5, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1—30.52 de NetScaler.

Remarques

Ce document de notes de version n'inclut pas de correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

Nouveautés

Les améliorations et modifications disponibles dans la version 13.1 à 30.52.

Réseau

Prise en charge du format Asdot pour BGP ASN 4 octets

L'appliance NetScaler prend désormais en charge la configuration et l'affichage de numéros de système autonomes (ASN) BGP sur 4 octets au format asdot tel que défini dans la RFC 5396. L'appliance NetScaler prend globalement en charge les deux formats suivants pour les ASN BGP :

- asplain - Notation de valeur décimale dans laquelle les ASN de 2 et 4 octets sont représentés par leur valeur décimale. Par exemple, 65527 est un ASN de 2 octets et 234567 est un ASN de 4 octets.
- asdot - Notation par points du système autonome où les ASN de 2 octets sont représentés par leur valeur décimale (comme dans asplain) et les ASN de 4 octets sont représentés par une notation à points. Par exemple, 65527 est un ASN de 2 octets et 3,37959 est un ASN de 4 octets. (3,37959 est un format asdot pour le nombre décimal 234567).

[NSNET-26101]

Support d'Amazon Linux 2 sur le cloud AWS pour les appliances NetScaler BLX

L'appliance NetScaler BLX est désormais prise en charge sur Amazon Linux 2 sur le cloud AWS. Le NetScaler BLX permet de fonctionner avec AWS Elastic Network Adapters (ENA) en tant que ports DPDK sur Amazon Linux 2.

[NSNET-25802]

Répartition uniforme des sondes de surveillance sur les routes disponibles

De la version 13.1 à 30.x, l'appliance NetScaler utilise l'algorithme de hachage basé sur les cinq tuples suivants pour sélectionner un itinéraire pour une sonde de surveillance d'équilibrage de charge.

- Adresse IP source
- Port source
- Adresse IP de destination
- Port de destination
- Numéro de protocole

La sélection des routes sur la base des informations de cinq tuples garantit une répartition uniforme des sondes de surveillance sur les itinéraires disponibles. Cette répartition uniforme évite la surcharge du trafic sur un itinéraire.

Pour plus d'informations, veuillez consulter https://docs.citrix.com/en-us/citrix-adc/current-release/networking/ip-routing/route-selection-based-on-five-tuples.html.

[NSNET-24646]

SSL

Prise en charge de la solution multi-agrafage OCSP

Lorsque le protocole TLS 1.3 est utilisé, tous les certificats intermédiaires incluent désormais l'extension de réponse OCSP dans la réponse à la demande d'état du client. Auparavant, seul le certificat du serveur incluait cette extension dans la réponse à la demande d'état du client.

[NSSSL-9281]

Interface utilisateur

Optimisation de la commande `show ns licenseserverpool` pour récupérer les licences en moins de temps

Lorsque vous exécutez la commande `show ns licenseserverpool`, la récupération des licences prend moins de temps. Un nouveau paramètre `licensemode` est ajouté à la commande `add ns licenseserver` pour spécifier le mode de licence. Ainsi, la commande `show ns licenseserverpool` affiche uniquement les licences en fonction du mode de licence spécifié. Si vous souhaitez un inventaire de toutes les licences, utilisez la commande `show ns licenseserverpool -get alllicenses`.

Auparavant, la commande `show ns licenseserverpool` permettait d'afficher toutes les licences quel que soit le mode de licence configuré. Par conséquent, la commande prenait plus de temps à récupérer toutes les licences.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/licensing.html#citrix-adc-self-managed-pool-license

[NSCONFIG-6961]

Support pour la licence Self Managed Pool

L'appliance NetScaler prend désormais en charge la licence Self Managed Pool, qui simplifie et automatise le téléchargement des fichiers de licence vers le serveur de licences après l'achat. Vous pouvez utiliser NetScaler ADM pour créer un cadre de licence comprenant une bande passante ou un processeur virtuel communs et le pool d'instances.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/licensing.html#citrix-adc-self-managed-pool-license

[NSCONFIG-6592]

Support pour l'agrégateur de licences NetScaler CPX

Vous pouvez désormais utiliser l'agrégateur de licences NetScaler CPX, un nouveau microservice Kubernetes fourni par NetScaler, pour obtenir des licences pour NetScaler CPX. Lorsque vous démarrez NetScaler CPX, vous devez configurer la variable d'environnement CLA avec l'adresse IP ou le nom de domaine de l'agrégateur de licences NetScaler CPX. Si la variable d'environnement est configurée, l'agrégateur de licences NetScaler CPX vérifie les licences agrégées pour tous les NetScaler CPX connectés.

[NSCONFIG-6394]

Problèmes résolus

Les problèmes qui sont traités dans la version 13.1-30.52.

Authentification, autorisation et audit

L'appliance NetScaler peut se bloquer si l'URL des métadonnées SAML de la configuration ne se termine pas par une barre oblique inverse (/) ou ne contient pas de barre oblique inverse (/).

[NSHELP-31937]

Si vous avez configuré un serveur Syslog, vous verrez un seul journal lié à SAML sur deux lignes.

[NSHELP-31750]

Il peut y avoir des problèmes de réécriture d'applications lors de l'application de stratégies de réécriture pour la stratégie de sécurité du contenu (CSP) sur un serveur virtuel d'authentification.

[NSHELP-31583]

Les caractères non-ASCII sont enregistrés dans nsvpn.log lorsque l'action LDAP est configurée sur un nom de domaine complet au lieu d'une adresse IP.

[NSHELP-27281]

L'interface graphique de NetScaler n'affiche pas les politiques de cache par défaut liées à un serveur virtuel VPN.

[NSHELP-26874]

Appliance NetScaler SDX

Dans une appliance NetScaler SDX, la création ou la modification des groupes de systèmes échouent.

[NSHELP-32359]

L'appliance NetScaler SDX n'envoie pas d'interruptions SNMP pour l'utilisation du disque de l'hyperviseur à NetScaler ADM.

[NSHELP-32323]

Dans une appliance NetScaler SDX, la liste blanche des VLAN n'est pas mise à jour avec la valeur correcte pour les interfaces Mellanox attribuées à une instance NetScaler VPX.

[NSHELP-31849]

Lorsque vous mettez à niveau une appliance NetScaler SDX, même si la version de l'hyperviseur est la même pour la version actuelle et pour la version SDX mise à niveau, l'événement incorrect suivant est signalé dans l'interface graphique du service de gestion :

Incompatibilité des versions de la SVM et de l'hyperviseur

[NSHELP-31769]

L'installation d'un certificat SSL sur une appliance NetScaler SDX échoue si le nom du certificat ou le nom de clé contient un espace.

[NSHELP-31711]

Parfois, le téléchargement du fichier de script de post-installation (postinst.sh) vers Citrix Hypervisor échoue lors de la mise à niveau de la plate-forme, lorsque vous mettez à niveau l'appliance NetScaler SDX du microprogramme 13.0 vers le microprogramme 13.1.

[NSHELP-31125]

NetScaler Gateway

Dans une configuration en cluster, l'appliance NetScaler se bloque lors de l'envoi de la requête CGP_FINISH_REQUEST au client.

[NSHELP-32029]

Parfois, une appliance NetScaler peut se bloquer lors de l'attribution d'une adresse IP intranet à un client.

[NSHELP-31712]

Les stratégies de routage basé sur des stratégies (PBR) ne prennent pas effet pour le trafic DNS via VPN.

[NSHELP-31123]

Lorsque la politique EPA classique et l'authentification nFactor sont configurées, les événements Gateway Insight relatifs à une authentification réussie ne sont pas envoyés à NetScaler Application Delivery Management.

[NSHELP-30901]

Vous pouvez voir une ligne supplémentaire pour les journaux NS_AUDITLOG_STR* dans le fichier ns_aaa_json.c.

[NSHELP-28160]

Vous ne pouvez pas dissocier une stratégie d'autorisation classique à l'aide de l'interface graphique. Toutefois, vous pouvez utiliser l'interface de ligne de commande pour dissocier la stratégie d'autorisation d'authentification, d'autorisation et d'audit.

Avec ce correctif, vous pouvez désormais dissocier la stratégie d'autorisation à l'aide de l'interface graphique.

[NSHELP-27064]

Gateway Insight n'affiche pas d'informations précises sur les utilisateurs du VPN.

[NSHELP-23937]

La vulnérabilité de signalement des journaux ne capture pas l'adresse IP source du client. Ces journaux sont les suivants :

- Suppression de la requête HTTP avec en-tête/version non valide
- Traversée de chemin détectée
- « /vpns/ » trouvé dans un endroit indésirable
- Suppression des requêtes HTTP non valides

[CGOP-18190]

Web App Firewall NetScaler

Sur une appliance NetScaler, la console peut être inondée de messages de journal et l'appliance peut envoyer des requêtes DNS au fournisseur de services de cloud public Webroot. Cela se produit parce

que la fonctionnalité de réputation IP, lorsqu'elle est désactivée, s'exécute toutes les cinq minutes au lieu d'une fois toutes les 24 heures.

[NSWAF-9299]

Équilibrage de charge

Une appliance NetScaler peut se bloquer et vider le noyau si le script de surveillance utilisateur renvoie une réponse de plus de 1 024 octets.

[NSHELP-32097]

Dans de rares cas, une appliance NetScaler peut tomber en panne et vider le cœur si le traitement DNSSEC est activé et que la configuration de la zone DNS est présente.

[NSHELP-31993]

En raison d'une situation de concurrence rare, il peut y avoir des incohérences entre le site local et le site distant. Cette incohérence peut être due au fait que le site distant n'apprend pas le membre dynamique à partir du site local.

La suppression des membres dynamiques sur le site distant peut échouer en raison d'un problème lors de la communication entre les moteurs de paquets.

[NSHELP-31982]

Les requêtes SNMP WALK correspondant à l'OID vServerAdvancessLConfigTable génèrent un vidage du cœur lorsque l'ordre de priorité des serveurs virtuels est configuré.

[NSHELP-31704]

Réseau

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si les conditions suivantes sont remplies :

- L'appliance NetScaler BLX est affectée à un nombre élevé de. `hugepages` Par exemple, 16 Go.

Le problème est consigné en tant que message d'erreur dans `/var/log/ns.log` :

- `EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Too many open files`

[NSNET-24727]

Lorsque ECMP est configuré sur une appliance NetScaler, le problème suivant peut être observé pour une connexion d'équilibrage de charge SSH :

- L'appliance NetScaler envoie le premier paquet via un itinéraire différent de celui utilisé pour les autres paquets du même flux.

[NSHELP-32089]

L'appliance NetScaler peut se bloquer dans certains scénarios lorsque les conditions suivantes sont remplies :

- L'appliance NetScaler reçoit plusieurs premiers fragments avec des décalages différents.
- L'appliance NetScaler ne réassemble pas les fragments.

[NSHELP-32084]

Dans une configuration d'équilibrage de charge avec `sessionless` option activée sur le serveur virtuel et ECMP côté serveur, le problème suivant peut être observé :

- L'appliance NetScaler envoie les paquets à un serveur toujours par le même itinéraire.

[NSHELP-32061]

Dans une configuration NAT44 à grande échelle, l'appliance NetScaler peut se bloquer lors de la réception du trafic SIP pour la raison suivante :

- En raison d'une entrée de filtrage obsolète.

[NSHELP-28895]

Plateforme

Sur une appliance NetScaler SDX, la taille de l'anneau est augmentée de 1024 à 2048 entrées pour les interfaces Mellanox.

[NSPLAT-24539]

La rotation des journaux échoue pour les fichiers stockés dans le dossier **/var/log/waagent** et occupe plus d'espace disque. Cet échec se produit lorsque vous appliquez une configuration de sauvegarde issue d'une instance NetScaler VPX sur une autre instance NetScaler VPX hébergée sur le cloud Azure à l'aide de la fonctionnalité de restauration.

[NSHELP-31599]

À partir de la version 13.1 de NetScaler, l'appliance NetScaler ne démarre pas dans un hyperviseur ESXi doté de plus de 8 interfaces réseau VMXNET3.

[NSHELP-31266]

Stratégies

Dans une appliance NetScaler, ce qui suit est observé.

- Problèmes liés à la comptabilité de la mémoire dans certains cas inhabituels.
- Problèmes liés à l'allocation/désallocation de mémoire de certaines entités.

Le suivi de l'allocation/désallocation de certaines entités a également été ajouté/amélioré.

[NSHELP-29215]

SSL

Lorsque les paires de clés de certificat RSA et ECDSA sont liées à un serveur virtuel et que le pair prend en charge un algorithme de signature compatible, le serveur TLS 1.3 sélectionne la paire de clés de certificat ECDSA. Auparavant, le serveur TLS 1.3 sélectionnait la paire de clés de certificat RSA. Avec cette modification, le serveur TLS 1.3 se comporte désormais de la même manière que le serveur TLS 1.2.

[NSSSL-11650]

Le serveur TLS 1.3 renvoie une `decode_error` alerte lorsqu'il rencontre un message de poignée de main TLS 1.3 divisé (fragmenté) entre plusieurs enregistrements TLS. Cela peut avoir un impact sur la réussite de la négociation si le client s'authentifie avec un certificat et que le certificat du client est supérieur à la taille d'enregistrement TLS maximale (environ 16 Ko).

[NSSSL-2940]

Une poignée de main SSL peut échouer si la séquence de conditions suivante est remplie :

1. Hello Verify Request (HVR) est activé sur DTLS.
2. L'appliance NetScaler envoie un HVR au client.
3. Le client ne reçoit pas le HVR.
4. Le client essaie de retransmettre le premier bonjour client au lieu de répondre au HVR avec un cookie de session.Remarque : En réponse au message Hello client retransmis, l'appliance ADC envoie le HVR au client au maximum trois fois. Si aucune réponse appropriée n'est reçue, l'appliance échoue à la négociation.

[NSHELP-31808]

Une appliance NetScaler configurée pour traiter le trafic SSL peut se bloquer si l'utilisation de la mémoire dépasse 80 %.

[NSHELP-29996]

Système

Une appliance NetScaler se bloque dans le flux de configuration des actions Syslog. Ce blocage est observé lors de la synchronisation de la haute disponibilité sur le nœud secondaire.

[NSHELP-32254, NSHELP-32397]

Dans un dispositif NetScaler, la valeur par défaut du `maxHeaderFieldLen` paramètre dans le profil HTTP provoque le problème suivant.

- Échec du trafic après la mise à niveau vers la version 13.0

[NSHELP-32079]

Une appliance NetScaler peut se bloquer lorsque AppFlow est activé uniquement côté client.

[NSHELP-31892]

Une appliance NetScaler peut se bloquer lorsque les conditions suivantes sont remplies :

- Le profil d'analyse et la stratégie AppFlow sont liés, et l' `httpAllHdrs` option est activée pour le profil.

[NSHELP-30628]

Dans une appliance NetScaler, le problème suivant est observé lors de l'activation de la configuration HTTP/2 pour une adresse IP virtuelle (VIP) de commutation de contenu ou d'équilibrage de charge.

- Une augmentation de la latence pouvant atteindre 100 ms lors du transfert de l'en-tête HTTP/2 et des blocs de données vers le site Web via l'appliance NetScaler.

[NSHELP-30094, NSHELP-34672]

Interface utilisateur

Dans une configuration haute disponibilité (HA), lors de la récupération de l'adresse IP locale pour l'outil nsconf, le problème suivant est observé.

- Échec de la connexion à l'hôte local. Cet échec se produit si le mot de passe du nœud RPC est différent pour les nœuds principaux et secondaires dans la configuration HA.

[NSHELP-32083]

L'exception suivante apparaît dans le SDK de l'API Python lors de la tentative de suppression d'une liaison de paire de clés de certificat et de serveur virtuel SSL.
TypeError : impossible de concaténer les objets « str » et « bool »

[NSHELP-31746]

Les détails des statistiques du serveur d'équilibrage de charge ne sont pas alignés correctement dans le tableau de bord de l'interface graphique NetScaler.

[NSHELP-20752]

Problèmes connus

Les problèmes qui existent dans les versions 13.1 à 30.52.

AppFlow

HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

[NSINSIGHT-943]

Authentification, autorisation et audit

Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

[NSHELP-563]

Le LoginSchema DualAuthPushOrOTP.xml ne s'affiche pas correctement dans l'écran de l'éditeur de schéma de connexion de l'interface graphique NetScaler.

[NSAUTH-6106]

Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante.
`show adfsproxyprofile <profile name>`

Solution :

Connectez-vous au principal NetScaler actif du cluster et exécutez la `show adfsproxyprofile <profile name>` commande. Il afficherait l'état du profil proxy.

[NSAUTH-5916]

La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

- L'option Tester l'accessibilité LDAP est ouverte.
- Les informations d'identification de connexion non valides sont renseignées et envoyées.
- Les identifiants de connexion valides sont renseignés et envoyés.

Solution :

Fermez et ouvrez l'option Tester l'accessibilité LDAP.

[NSAUTH-2147]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, si le CLAG est créé sur une carte réseau Mellanox, le MAC CLAG est modifié lorsque l'instance VPX est redémarrée. Le trafic vers l'instance VPX s'arrête après le redémarrage car la table MAC contient l'ancienne entrée MAC CLAG.

[NSSVM-4333]

NetScaler Gateway

Sur un appareil MAC utilisant Chrome, l'extension VPN se bloque lors de l'accès à deux noms de domaine complets.

[NSHELP-32144]

Les connexions directes aux ressources situées en dehors du tunnel établi par Citrix Secure Access peuvent échouer en cas de retard ou de congestion important.

[NSHELP-31598]

Lorsque Always on est configuré, le tunnel utilisateur échoue en raison du numéro de version incorrect (1.1.1.1) dans le fichier aoservice.exe.

[NSHELP-30662]

Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil « NetworkAccessOnVPNFailure » de « FullAccess » à « OnlyToGateway ».

[NSHELP-30236]

La page d'accueil de la passerelle ne s'affiche pas immédiatement après que le plug-in de passerelle a réussi à établir le tunnel VPN. Pour résoudre ce problème, la valeur de registre suivante est introduite.

\HKLM\Software\Citrix\Secure Access Client\SecureChannelResetTimeoutSeconds
Type: DWORD

Par défaut, cette valeur de registre n'est ni définie ni ajoutée. Lorsque la valeur de `SecureChannelResetTimeoutS` est 0 ou n'est pas ajoutée, le correctif pour gérer le délai ne fonctionne pas, ce qui est le comportement par défaut. L'administrateur doit définir ce registre sur le client pour activer le correctif (c'est-à-dire afficher la page d'accueil immédiatement après que le plug-in de passerelle ait établi le tunnel VPN avec succès).

[NSHELP-30189]

Le client VPN Windows n'honore pas l'alerte « Notification de fermeture SSL » du serveur et envoie la demande de connexion de transfert sur la même connexion.

[NSHELP-29675]

Parfois, le code de validation du serveur échoue lorsque le certificat du serveur est approuvé. Par conséquent, les utilisateurs finaux ne peuvent pas accéder à la passerelle.

[NSHELP-28942]

Vous remarquerez peut-être certaines adresses IP internes de Citrix dans le fichier rdx.js.

[NSHELP-28682]

L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

[NSHELP-28551]

Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

[NSHELP-28404]

Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

- L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
- L'appliance est configurée pour l'authentification basée sur des certificats avec authentification à deux facteurs `off`

[NSHELP-23584]

Parfois, lorsque vous parcourez les schémas, le message d'erreur `Cannot read property 'type 'of undefined` s'affiche.

[NSHELP-21897]

Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet d'utiliser les améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

[CGOP-19355]

L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

[CGOP-13621]

Le rapport Gateway Insight affiche incorrectement la valeur `Local` plutôt que `SAML` dans le champ **Type d'authentification** en cas d'échec d'erreur SAML.

[CGOP-13584]

Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

[CGOP-13511]

Lorsqu'une connexion ICA est lancée à partir d'un Receiver MAC version 19.6.0.32 ou Citrix Virtual Apps and Desktops version 7.18, la fonctionnalité HDX Insight est désactivée.

[CGOP-13494]

Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

[CGOP-13493]

Lorsque vous acceptez les connexions hôtes locales depuis le navigateur, la boîte de dialogue **Accepter la connexion** pour macOS affiche du contenu en anglais, quelle que soit la langue sélectionnée.

[CGOP-13050]

Le texte `Home Page` de l'application Citrix SSO > Page d'accueil est tronqué dans certaines langues.

[CGOP-13049]

Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

[CGOP-11830]

Dans Outlook Web App (OWA) 2013, cliquez sur **Options** dans le menu **Paramètres** pour afficher une boîte de dialogue **d'erreur critique** . De plus, la page ne répond plus.

[CGOP-7269]

Équilibrage de charge

Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

[NSLB-7679]

Dans une configuration haute disponibilité (HA), les routes sont abandonnées sur le nouveau nœud principal et ne sont pas réapprises lorsque la condition suivante est remplie.

- La suppression dynamique de route et le basculement HA se produisent en même temps en raison d'une défaillance critique de l'interface.

[NSHELP-32264]

Le format ServiceGroupName dans le `entityofs` piège pour le groupe de services est le suivant : `<service(group)name>?<ip/DBS>?<port>`

Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (?) est utilisé comme séparateur. NetScaler envoie le piège avec le point d'interrogation ()?. Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Dans certains scénarios, les serveurs liés à un groupe de services affichent une valeur de cookie non valide. Vous pouvez voir la valeur de cookie correcte dans les journaux de suivi.

[NSHELP-21196]

Divers

Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, l'appliance exécute la commande `set urlfiltering parameter` sur le nœud secondaire.
Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre `TimeOfDayToUpdateDB`.

[NSSWG-849]

Le registre de liste AlwaysOnAllow ne fonctionne pas comme prévu si la valeur du registre est supérieure à 2000 octets.

[NSHELP-31836]

Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

[NSHELP-22409]

Réseau

Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

[NSNET-25299]

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :

- L'appliance NetScaler BLX se voit attribuer un faible nombre de. `hugepages` Par exemple, 1G.
- L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

Le problème est consigné en tant que message d'erreur dans `/var/log/ns.log` :

- `BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x`

Remarque : x est un nombre <= nombre de processus de travail.

Solution :

Attribuez un nombre élevé de, `hugepages` puis redémarrez l'appliance.

[NSNET-25173]

Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

[NSNET-24449]

Les opérations d'interface suivantes ne sont pas prises en charge pour les X710 10G (i40e) interfaces Intel sur une appliance NetScaler BLX avec DPDK :

- Désactiver
- Activer
- Réinitialiser

[NSNET-16559]

L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solution :

Exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

- dpkg –add-architecture i386
- apt-get update
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

[NSHELP-21082]

Plateforme

Lorsque vous effectuez une mise à niveau d'une version 13.0/12.1/11.1 vers une version 13.1 ou que vous rétrogradez d'une version 13.1 vers une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances NetScaler. Ce problème est résolu pour les versions suivantes de NetScaler :

- 13.1-4.x

- 13.0—82.31 et versions ultérieures
- 12.1—62.21 et versions ultérieures

Les packages python ne sont pas installés lorsque vous rétrogradez les versions de NetScaler de 13.1-4.x vers l'une des versions suivantes :

- Toute version 11.1
- 12.1-62.21 et versions antérieures
- 13.0-81.x et versions antérieures

[NSPLAT-21691]

Dans une configuration de cluster sur une appliance NetScaler SDX, il existe une incompatibilité CLAG MAC sur le deuxième nœud et CLIP si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous ajoutez une autre instance VPX au cluster et à la configuration CLAG.

Par conséquent, le trafic vers l'instance VPX s'arrête.

[NSPLAT-21049]

Dans une configuration de cluster sur une appliance NetScaler SDX, le premier nœud tombe en panne en raison d'une incompatibilité d'adresses MAC entre CLIP et la table MAC, si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous supprimez le deuxième nœud du cluster.

[NSPLAT-21042]

Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande `rm cloudprofile` pour supprimer le profil.

[NSPLAT-4520]

Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

[NSPLAT-4451]

Stratégies

Les connexions peuvent se bloquer si la taille des données de traitement est supérieure à la taille de tampon TCP par défaut configurée.Solution : définissez la taille du tampon TCP sur la taille maximale

des données à traiter.

[NSPOLICY-1267]

SSL

Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

Solution :

1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
2. Enregistrez la configuration.

[NSSSL-9572]

Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

[NSSSL-6478]

Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

[NSSSL-6213]

Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier Key Vault comme type HSM.
ERREUR : actualisation des CRL désactivée

[NSSSL-6106]

L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

[NSSSL-4427]

Un message d'avertissement incorrect `Warning: No usable ciphers configured on the SSL vserver/service`, s'affiche si vous essayez de modifier le protocole SSL ou le chiffrement dans le profil SSL.

[NSSSL-4001]

Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA. [NSSSL-3184, NSSSL-1379, NSSSL-1394]

Après la mise à niveau d'une appliance NetScaler SDX vers la version 13.1 build 21.50 ou ultérieure, le déchiffrement SSL et la comparaison MAC peuvent échouer. Par conséquent, vous pouvez voir des

échecs d'établissement de liaison SSL, un battement d'état VPX, une indisponibilité de l'interface utilisateur de l'instance VPX et une panne des serveurs virtuels et de l'application.

Remarque : Ce problème est observé sur les plates-formes SDX 8900, SDX 15000, SDX 15000-50G, SDX 26000 et SDX 26000-50S.

[NSHELP-31672]

Système

La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client.

[NSHELP-21240]

Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

[NSHELP-10972]

Dans un déploiement de cluster, si vous exécutez la commande `force cluster sync` sur un nœud non CCO, le fichier ns.log contient des entrées de journal en double. [NSBASE-16304, NSGI-1293]

Lorsque vous installez NetScaler ADM sur un cluster Kubernetes, cela ne fonctionne pas comme prévu car les processus requis peuvent ne pas s'exécuter.

Solution : redémarrez le module Gestion.

[NSBASE-15556]

L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

[NSBASE-8506]

L'appliance NetScaler configurée avec un service SSL se bloque lorsqu'elle reçoit un paquet de contrôle TCP FIN suivi d'un paquet de contrôle TCP RESET.

[NSHELP-31656]

Interface utilisateur

Pour la fonction de réécriture MQTT, vous ne pouvez pas supprimer une expression à l'aide de l'éditeur d'expression dans l'interface graphique.

Solution :

Utilisez la commande d'action add ou edit de type MQTT via l'interface de ligne de commande.

[NSUI-18049]

Dans l'interface graphique de NetScaler, le `Help` lien présent sous l' `Dashboard` onglet est rompu.

[NSUI-14752]

L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution :

Configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de la CLI de NetScaler.

[NSUI-13024]

Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

[NSUI-6838]

Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

- Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

Solution :

Effectuez le basculement HA manuel successif uniquement après la fin de la synchronisation HA (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

Dans une configuration à haute disponibilité des appliances NetScaler BLX, le nœud principal peut ne plus répondre en bloquant toute demande de CLI ou d'API.

Solution :

Redémarrez le nœud principal.

[NSCONFIG-6601]

Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

1. Mettez à niveau l'appliance NetScaler vers l'une des versions suivantes :
   - 13.0 52.24 build
   - 12.1 57.18 build
   - 11.1 65.10 build
2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration.
3. Rétrogradez l'appliance NetScaler vers une version antérieure.

Pour afficher la liste de ces utilisateurs système à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solution :

Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

- Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
- Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
- Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notes de publication pour la version 13.1—27.59 de NetScaler

May 5, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1—27.59 de NetScaler.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

Nouveautés

Les améliorations et modifications disponibles dans les versions 13.1-27.59.

Authentification, autorisation et audit

Permettre aux utilisateurs d'utiliser la configuration Intune NAC v2 avec les nouvelles API Microsoft Graph

Vous pouvez désormais utiliser la configuration Intune NAC v2 avec les nouvelles API Microsoft Graph au lieu des API AAD Graph obsolètes.

Pour plus d'informations, consultez Intégration à Microsoft Intune et support étendu pour Azure AD Graph.

[NSAUTH-11897]

Gestion des bots

Stylebook pour la gestion des WAF/Bot sur les appareils NetScaler Gateway

Vous pouvez désormais configurer les politiques WAF et BOT pour les appareils NetScaler Gateway afin de protéger la page de connexion de Gateway. Deux nouveaux livres de style par défaut sont désormais disponibles pour la gestion des WAF/Bot sur les appareils NetScaler Gateway :

- Stylebook pour la protection du site d'ouverture de session de NetScaler Gateway à l'aide de WAF et BOT
- Stylebook pour la protection du site d'ouverture de session à NetScaler Gateway à l'aide de WAF et de BOT avec violations de sécurité WAF et Bot

Pour utiliser le Stylebook par défaut pour la gestion des WAF/bot sur la passerelle, accédez à Applications > Configuration > StyleBooks. Saisissez le nom du StyleBook dans le champ de recherche et appuyez sur la touche Entrée . Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/stylebooks/how-to-use-default-stylebooks.html%23to-create-a-configuration-from-a-default-stylebook

[NSBOT-755]

Activation de la fonctionnalité de détection des bots pour tous les droits NetScaler Premium

La fonctionnalité de détection des bots ainsi que les contrôles de signature et de réputation IP sont désormais activés par défaut pour tous les droits NetScaler premium.

Vous pouvez consulter le trafic de bots arrivant dans votre environnement et les mesures prises par l'appliance NetScaler. En outre, l'appliance ADC enregistre les informations de trafic de bot suivantes dans les messages du journal SNMP :

- Nombre de robots détectés
- Les deux principales catégories de robots détectées
- L'endroit où vous pouvez trouver plus de détails sur les robots détectés

Pour plus d'informations, consultez la section Détection des robots.

[NSBOT-752]

Web App Firewall NetScaler

Activation automatique des nouvelles signatures

Vous pouvez désormais sélectionner **Activer automatiquement les nouvelles signatures** pour autoriser l'activation automatique des nouvelles règles de signature WAF par défaut après une mise à jour.

[NSWAF-8825]

Champs confidentiels d'un profil WAF

Vous pouvez désormais ajouter des champs confidentiels dans un profil WAF. Ces champs sont masqués et ne sont pas capturés dans les journaux ADC lorsqu'une violation se produit. Auparavant, vous pouviez ajouter ces champs uniquement à l'aide de paramètres.

[NSWAF-8525]

Support de mots clés personnalisé pour la charge utile HTML

Vous pouvez ajouter des mots clés de votre choix et vérifier si ces mots clés configurés sont présents dans la charge utile HTML. Si les mots clés configurés sont détectés dans les demandes entrantes, vous pouvez configurer l'appliance NetScaler pour bloquer les demandes, mettre à jour les journaux ou incrémenter les compteurs de journaux.

Grâce à cette fonctionnalité, vous pouvez ajouter des mots-clés qui ne sont pas couverts par les contrôles d'injection SQL et d'injection de commandes et ainsi réduire les faux positifs.

[NSWAF-8520]

Approche basée sur la grammaire pour la détection des injections de commandes dans les charges utiles HTML

La solution NextGen NetScaler Web App Firewall est désormais améliorée pour prendre en charge l'approche basée sur la grammaire pour la détection des injections de commandes. Cette approche réduit les faux positifs dans les charges utiles HTML.

Auparavant, seule l'approche basée sur les modèles était prise en charge.

[NSWAF-8270]

Réseau

Vous pouvez désormais utiliser le port NSIP:8080 sur NetScaler CPX pour la configuration du serveur virtuel. Auparavant, ce port était réservé et n'était pas disponible pour la configuration utilisateur.

[NSNET-25399]

Prise en charge des tunnels Geneve dans une configuration de cluster

Les tunnels de Genève sont désormais pris en charge dans une configuration en cluster d'appliances NetScaler.

[NSNET-24773]

Améliorations pour inclure le niveau de gravité lors de l'envoi de messages d'interruption SNMP

L'appliance NetScaler VPX inclut désormais le niveau de gravité des messages d'interruption SNMP sous forme de liaison variable. Utilisez la commande suivante avec l'option **SeverityInfoIntrap** :

- **set snmp option -severityInfoInTrap ENABLED**

Lorsque cette option est activée, le niveau de gravité de l'interruption est inclus dans le message d'interruption SNMP.

[NSNET-21603]

Plateforme

Prise en charge des adresses IPv6 pour la haute disponibilité de NetScaler dans AWS

La paire de haute disponibilité NetScaler VPX prend désormais en charge les adresses IPv6 dans la même zone de disponibilité AWS. Auparavant, seules les adresses IPv4 étaient prises en charge.

[NSPLAT-16672]

Interface utilisateur

Microsoft a arrêté la prise en charge du navigateur Internet Explorer à partir de juin 2022. Pour plus d'informations, veuillez consulter https://support.microsoft.com/en-us/windows/internet-explorer-help-23360e49-9cd3-4dda-ba52-705336cc0de2.

À partir de la version 13.1 27.x de NetScaler, l'appliance NetScaler ne prend plus en charge Internet Explorer pour accéder à son interface graphique.

Lorsque vous accédez à l'interface graphique de NetScaler à l'aide d'Internet Explorer, l'appliance NetScaler affiche un message indiquant qu'Internet Explorer n'est pas pris en charge. Il recommande également une liste des navigateurs pris en charge pour accéder à l'interface graphique.

[NSUI-18224]

Demande de confirmation pour l'activation ou la désactivation d'une fonctionnalité dans l'interface graphique de NetScaler

L'interface graphique de NetScaler vous invite désormais à confirmer l'opération lorsque vous activez ou désactivez une fonctionnalité NetScaler dans l'interface graphique. L'invite de confirmation empêche toute activation ou désactivation accidentelle d'une fonctionnalité NetScaler.

[NSUI-18098]

Problèmes résolus

Les problèmes qui sont traités dans la version 13.1-27.59.

Authentification, autorisation et audit

Les stratégies de réécriture pour les points de terminaison tels que ne `/logon/LogonPoint/Resources/List and /cgi/Resources/List` sont pas prises en charge.

[NSHELP-29488]

Appliance NetScaler SDX

Les paramètres de fuseau horaire de la machine virtuelle Citrix Service ne fonctionnent pas comme prévu.

[NSHELP-32114]

Dans une appliance NetScaler SDX, une utilisation plus importante de la mémoire est détectée en raison d'un volume élevé de traitement de données SNMP.

[NSHELP-30222]

L'application SNMP Walk exécutée sur l'appliance NetScaler SDX pour le SDX-ROOT-MIB : :XenTable prend plus de temps que prévu.

[NSHELP-30085]

NetScaler Gateway

Parfois, les utilisateurs ne peuvent pas accéder aux signets en mode VPN avancé sans client.

[NSHELP-30939]

L'appliance NetScaler Gateway configurée en mode proxy ICA pour la connexion audio UDP peut se bloquer en raison d'une corruption de la mémoire.

[NSHELP-30919]

Le lancement de l'application ICA échoue dans les conditions suivantes :

- La fonctionnalité de stratégie de sécurité du contenu (CSP) est activée.
- L'utilisateur se connecte à partir d'un navigateur, mais utilise l'application Citrix Workspace pour lancer l'application.

[NSHELP-30534]

L'appliance NetScaler Gateway peut se bloquer lors de l'analyse des canaux lorsque HDX Insight est activé et que NSAP est désactivé.

[NSHELP-30029]

Gateway Insight signale un faux échec d'authentification avant même que l'utilisateur n'envoie les informations d'identification pour la connexion lorsque la règle d'authentification est configurée pour correspondre à l'une des demandes du flux de connexion.

[NSHELP-29313]

Le lancement de l'application échoue après la saisie de vos informations d'identification si le profil de session contient le nom de domaine complet de StoreFront. L'erreur suivante s'affiche.

« Erreur interne du serveur Http/1.1 43531 »

Avec ce correctif, les clients peuvent saisir le nom de domaine complet au lieu de l'adresse WI du profil de session sur IP.

[NSHELP-26671]

Web App Firewall NetScaler

Les journaux pour `No user-agent header action` et `multi user-agent header action` peuvent utiliser de manière incorrecte le message de journal de la vérification de la réputation IP.

[NSHELP-31935]

Une appliance NetScaler peut se bloquer lors du traitement des recherches de signatures BOT avec des serveurs DNS lents.

[NSHELP-31642]

L'appliance NetScaler peut se bloquer si le script intersite est activé dans la règle de signature.

[NSHELP-31617]

Équilibrage de charge

Dans certains cas, l'état du service n'est pas synchronisé avec l'état du moniteur.

[NSHELP-31747]

L'appliance NetScaler se bloque lors de la suppression du serveur de noms si les conditions suivantes sont remplies :

- Le serveur DNS et le serveur de noms sont configurés sur la même adresse IP et le même port.
- La stratégie d'écoute est définie sur le serveur DNS.

[NSHELP-31142]

Une appliance NetScaler peut se bloquer lors d'une configuration claire si des entrées de persistance sont présentes et qu'un grand nombre de serveurs virtuels d'équilibrage de charge fictifs et de serveurs virtuels de groupe sont configurés.

[NSHELP-30051]

La création d'un service virtuel générique échoue si une configuration WIHOME non résolue existe sur l'appliance NetScaler.

[NSHELP-25627]

Divers

Dans une appliance NetScaler, lorsqu'un disque dur supplémentaire est ajouté à l'appliance, un lien vers le `/var/nslog` fichier est créé dans le dossier de crash. `/var/crash/nslog` Les fichiers `newnslog` disponibles dans le dossier crash ne sont pas collectés dans le dossier du collecteur généré par le support technique.

[NSHELP-31354]

L'appliance NetScaler SWG peut se bloquer lorsque la mémoire allouée à une ressource n'est pas libérée, ce qui entraîne une utilisation élevée de la mémoire même en l'absence de trafic.

[NSHELP-31290]

Dans une configuration de cluster NetScaler avec une authentification système par clé publique configurée, le problème suivant est observé :

- VTYSH n'affiche pas les informations de tous les nœuds du cluster sur le coordinateur de configuration du cluster (CCO).

[NSHELP-28762]

Plateforme

Sur la plate-forme SDX 26000 (SDX 26100-100G, 26160-100G, 26200-100G, 26250-100G), le nombre maximal de cœurs de processeur pouvant être attribués à une seule instance VPX passe de 26 à 25 cœurs de processeur.

[NSPLAT-21233]

La licence BYOL ne peut pas être appliquée à une instance NetScaler VPX exécutée sur la plateforme cloud ALI.

[NSHELP-31546]

SSL

L'appliance NetScaler SDX se bloque lorsque des unités de chiffrement sont attribuées à une instance VPX et que la configuration jumbo est activée.

[NSHELP-30950]

Une appliance NetScaler peut tomber en panne dans les scénarios suivants :

- Un moniteur d'équilibrage de charge de type SSL et un service SSL portent le même nom
- Un service SSL est renommé
- Un moniteur d'équilibrage de charge est supprimé

[NSHELP-30445]

Si l'interception SSL est activée et que les serveurs DNS ne renvoient pas de réponse DNS valide, l'accès au site Web est bloqué.

[NSHELP-30201]

Une appliance NetScaler se bloque lorsque toutes les conditions suivantes se produisent :

- Une paire de clés de certificat RSA par défaut est liée à un service interne.
- Une paire de clés de certificat non RSA est liée au même service.
- La synchronisation HA se produit.

[NSHELP-30084]

Les personnalisations qui font partie du fichier rc.netscaler ne sont pas appliquées car ce fichier n'est pas exécuté lors de l'initialisation du système.

[NSHELP-31914]

Système

L'appliance NetScaler se bloque lorsque l'appliance NetScaler ADM qui gère possède une MTU réseau supérieure à 1 500.

[NSHELP-30835]

Une appliance NetScaler dotée de la configuration de mesure côté client peut corrompre une variable et provoquer l'échec du chargement de la page dans les conditions suivantes :

- La réponse HTTP contient une variable javascript supérieure à 2 000 octets.

[NSHELP-30026]

Dans une appliance NetScaler, si vous dissociez les politiques globales avancées par défaut et enregistrez la configuration, les modifications ne seront pas répercutées lors du prochain redémarrage.

[NSHELP-19867]

L'appliance NetScaler supprime les paquets qui contiennent des en-têtes HTTP personnalisés avec un point dans le champ du nom de l'en-tête. Cette action se produit car le paramètre AllowOnlyWordCharactersAndHyphen est activé par défaut dans le profil HTTP par défaut.

À partir de la version 13.1-27.x, le paramètre AllowOnlyWordCharactersAndHyphen dans le jeu de profils HTTP par défaut est désactivé par défaut. Toutefois, Citrix vous recommande de laisser ce paramètre activé pour une meilleure sécurité.

[NSBASE-16722]

Interface utilisateur

Vous ne pouvez pas dissocier les membres des groupes de services d'équilibrage de charge à l'aide de l'interface graphique de la version NetScaler version 13.0 version 85.15.

[NSHELP-31474]

La page **Système > Diagnostics** de l'interface graphique de NetScaler n'affiche pas les détails de la page pour les clients disposant d'une licence avancée.

[NSHELP-31330]

L'enregistrement d'une trace de paquets peut ne pas fonctionner comme prévu sur une partition d'administration.

[NSHELP-31321]

La reconnexion à l'appliance NetScaler échoue avec l'erreur suivante lorsqu'elle `CTRL+C` est saisie lors de l'exécution de la `show run` commande dans l'interface CLI :

- `Invalid username or password`

Ce problème se produit si les caractères de la clé et du mot de passe sont identiques.

[NSHELP-30817]

En raison d'une séquence d'installation de mise à niveau incorrecte, le problème suivant se produit dans l'appliance NetScaler.

- L'image du noyau est d'abord mise à jour et après quelques étapes, les clés de chiffrement sont copiées. Entre ces étapes, une défaillance se produit et l'appliance ADC affiche une nouvelle image. Les clés de chiffrement manquantes dans la nouvelle image entraînent un échec du déchiffrement et une configuration manquante.

[NSHELP-30755]

Problèmes connus

Les problèmes qui existent dans les versions 13.1-27.59.

AppFlow

HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

[NSINSIGHT-943]

Authentification, autorisation et audit

Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

[NSHELP-563]

Le LoginSchema DualAuthPushOrOTP.xml ne s'affiche pas correctement dans l'écran de l'éditeur de schéma de connexion de l'interface graphique NetScaler.

[NSAUTH-6106]

Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante.
`show adfsproxyprofile <profile name>`

Solution :

Connectez-vous au principal NetScaler actif du cluster et exécutez la `show adfsproxyprofile <profile name>` commande. Il afficherait l'état du profil proxy.

[NSAUTH-5916]

La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

- L'option Tester l'accessibilité LDAP est ouverte.
- Les informations d'identification de connexion non valides sont renseignées et envoyées.
- Les identifiants de connexion valides sont renseignés et envoyés.

Solution :

Fermez et ouvrez l'option Tester l'accessibilité LDAP.

[NSAUTH-2147]

Mise en cache

Une appliance NetScaler peut se bloquer si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

[NSHELP-22942]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, si le CLAG est créé sur une carte réseau Mellanox, le MAC CLAG est modifié lorsque l'instance VPX est redémarrée. Le trafic vers l'instance VPX s'arrête après le redémarrage car la table MAC contient l'ancienne entrée MAC CLAG.

[NSSVM-4333]

Dans une appliance NetScaler SDX, la liste blanche des VLAN n'est pas mise à jour avec la valeur correcte pour les interfaces Mellanox attribuées à une instance NetScaler VPX.

[NSHELP-31849]

Lorsque vous mettez à niveau une appliance NetScaler SDX, même si la version de l'hyperviseur est la même pour les versions SDX actuelles et mises à niveau, l'événement incorrect suivant est signalé dans l'interface graphique du service de gestion :

Incompatibilité des versions de la SVM et de l'hyperviseur

[NSHELP-31769]

L'installation d'un certificat SSL sur une appliance NetScaler SDX échoue si le nom du certificat ou le nom de clé contient un espace.

[NSHELP-31711]

NetScaler Gateway

Les connexions directes aux ressources situées en dehors du tunnel établi par Citrix Secure Access peuvent échouer en cas de retard ou de congestion important.

[NSHELP-31598]

Lorsque Always on est configuré, le tunnel utilisateur échoue en raison du numéro de version incorrect (1.1.1.1) dans le fichier aoservice.exe.

[NSHELP-30662]

Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil « NetworkAccessOnVPNFailure » de « FullAccess » à « OnlyToGateway ».

[NSHELP-30236]

La page d'accueil de la passerelle ne s'affiche pas immédiatement après que le plug-in de passerelle a réussi à établir le tunnel VPN. Pour résoudre ce problème, la valeur de registre suivante est introduite.

\HKLM\Software\Citrix\Secure Access Client\SecureChannelResetTimeoutSeconds
Type: DWORD

Par défaut, cette valeur de registre n'est ni définie ni ajoutée. Lorsque la valeur de `SecureChannelResetTimeoutS` est 0 ou n'est pas ajoutée, le correctif pour gérer le délai ne fonctionne pas, ce qui est le comportement par défaut. L'administrateur doit définir ce registre sur le client pour activer le correctif (c'est-à-dire afficher la page d'accueil immédiatement après que le plug-in de passerelle ait établi le tunnel VPN avec succès).

[NSHELP-30189]

Le client VPN Windows n'honore pas l'alerte « Notification de fermeture SSL » du serveur et envoie la demande de connexion de transfert sur la même connexion.

[NSHELP-29675]

Dans certains cas, le code de validation du serveur échoue lorsque le certificat de serveur est approuvé. Par conséquent, les utilisateurs finaux ne peuvent pas accéder à la passerelle.

[NSHELP-28942]

Vous remarquerez peut-être certaines adresses IP internes de Citrix dans le fichier rdx.js.

[NSHELP-28682]

L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

[NSHELP-28551]

Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

[NSHELP-28404]

Vous ne pouvez pas dissocier une stratégie d'autorisation classique à l'aide de l'interface graphique. Toutefois, vous pouvez utiliser l'interface de ligne de commande pour dissocier la stratégie d'autorisation d'authentification, d'autorisation et d'audit.

Avec ce correctif, vous pouvez désormais dissocier la stratégie d'autorisation à l'aide de l'interface graphique.

[NSHELP-27064]

Gateway Insight n'affiche pas d'informations précises sur les utilisateurs du VPN.

[NSHELP-23937]

Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

- L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
- L'appliance est configurée pour l'authentification par certificat avec une authentification à deux facteurs. `off`

[NSHELP-23584]

Parfois, lorsque vous parcourez les schémas, le message d'erreur `Cannot read property 'type 'of undefined` s'affiche.

[NSHELP-21897]

Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

[CGOP-19355]

L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

[CGOP-13621]

Le rapport Gateway Insight affiche de manière incorrecte la valeur `Local` plutôt que `SAML` dans le champ Type d'authentification en cas d'échec d'erreur SAML.

[CGOP-13584]

Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

[CGOP-13511]

Lorsqu'une connexion ICA est lancée à partir d'un Receiver MAC version 19.6.0.32 ou Citrix Virtual Apps and Desktops version 7.18, la fonctionnalité HDX Insight est désactivée.

[CGOP-13494]

Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

[CGOP-13493]

Lors de l'acceptation des connexions hôtes locales depuis le navigateur, la boîte de dialogue Accepter la connexion pour macOS affiche le contenu en anglais, quelle que soit la langue sélectionnée.

[CGOP-13050]

Le texte `Home Page` de l'application Citrix SSO > Page d'accueil est tronqué dans certaines langues.

[CGOP-13049]

Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

[CGOP-11830]

Dans Outlook Web App (OWA) 2013, le fait de cliquer sur **Options** dans le menu Paramètres affiche une boîte de dialogue **Erreur critique** . De plus, la page ne répond plus.

[CGOP-7269]

Web App Firewall NetScaler

Une appliance NetScaler peut se bloquer lors du traitement des recherches de signatures BOT avec des serveurs DNS lents.

[NSHELP-31642]

L'appliance NetScaler peut se bloquer si le script intersite est activé dans la règle de signature.

[NSHELP-31617]

Équilibrage de charge

Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

[NSLB-7679]

Dans certains cas, l'état du service n'est pas synchronisé avec l'état du moniteur.

[NSHELP-31747]

L'appliance NetScaler peut tomber en panne et vider le noyau si les conditions suivantes sont remplies :

- La proximité statique ou RTT est utilisée comme méthode d'équilibrage de charge principale ou de secours.
- La persistance de l'adresse IP source est activée

[NSHELP-31735]

Le format ServiceGroupName dans le `entityofs` piège pour le groupe de services est le suivant : `<service(group)name>?<ip/DBS>?<port>`

Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (?) est utilisé comme séparateur. NetScaler envoie le piège avec le point d'interrogation ()?. Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Dans certains scénarios, les serveurs liés à un groupe de services affichent une valeur de cookie non valide. Vous pouvez voir la valeur de cookie correcte dans les journaux de suivi.

[NSHELP-21196]

Divers

Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, l'appliance exécute la commande `set urlfiltering parameter` dans le nœud secondaire.
Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre `TimeOfDayToUpdateDB`.

[NSSWG-849]

Le registre de liste AlwaysOnAllow ne fonctionne pas comme prévu si la valeur du registre est supérieure à 2000 octets.

[NSHELP-31836]

Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

[NSHELP-22409]

Réseau

Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

[NSNET-25299]

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :

- L'appliance NetScaler BLX se voit attribuer un faible nombre de. `hugepages` Par exemple, 1G.
- L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

Le problème est consigné en tant que message d'erreur dans /var/log/ns.log :

- BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x

Remarque : x est un nombre <= nombre de processus de travail.

Solution :

Attribuez un nombre élevé de, hugepages puis redémarrez l'appliance.

[NSNET-25173]

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si les conditions suivantes sont remplies :

- L'appliance NetScaler BLX est affectée à un nombre élevé de. hugepages Par exemple, 16 Go.

Le problème est consigné en tant que message d'erreur dans /var/log/ns.log :

- EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Too many open files

Solution :

Utilisez l'une des solutions de contournement suivantes pour résoudre ce problème :

- Augmentez la limite de fichiers ouverts sur l'hôte Linux en utilisant la commande ulimit ou en modifiant le fichier limits.conf.
- Réduisez le nombre de hugepages alloués.

[NSNET-24727]

Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

[NSNET-24449]

Les opérations d'interface suivantes ne sont pas prises en charge pour les X710 10G (i40e) interfaces Intel sur une appliance NetScaler BLX avec DPDK :

- Désactiver
- Activer
- Réinitialiser

[NSNET-16559]

L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solution :

Exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

- dpkg –add-architecture i386
- apt-get update
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

[NSHELP-21082]

Plateforme

Le basculement haute disponibilité ne fonctionne pas dans les clouds AWS et GCP. Le processeur de gestion peut atteindre 100 % de sa capacité dans les clouds AWS et GCP, ainsi que dans NetScaler VPX sur site. Ces deux problèmes sont provoqués lorsque les conditions suivantes sont remplies :

1. Lors du premier démarrage de l'appliance NetScaler, vous n'enregistrez pas le mot de passe demandé.
2. Ensuite, vous redémarrez l'appliance NetScaler.

[NSPLAT-22013]

Lorsque vous effectuez une mise à niveau d'une version 13.0/12.1/11.1 vers une version 13.1 ou que vous rétrogradez d'une version 13.1 vers une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances NetScaler. Ce problème est résolu pour les versions suivantes de NetScaler :

- 13.1-4.x
- 13.0-82.31 et versions ultérieures
- 12.1-62.21 et versions ultérieures

Les packages python ne sont pas installés lorsque vous rétrogradez les versions de NetScaler de 13.1-4.x vers l'une des versions suivantes :

- Toute version 11.1

- 12.1-62.21 et versions antérieures
- 13.0-81.x et versions antérieures

[NSPLAT-21691]

Dans une configuration de cluster sur une appliance NetScaler SDX, il existe une incompatibilité CLAG MAC sur le deuxième nœud et CLIP si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous ajoutez une autre instance VPX au cluster et à la configuration CLAG.

Par conséquent, le trafic vers l'instance VPX s'arrête.

[NSPLAT-21049]

Dans une configuration de cluster sur une appliance NetScaler SDX, le premier nœud tombe en panne en raison d'une incompatibilité d'adresses MAC entre CLIP et la table MAC, si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous supprimez le deuxième nœud du cluster.

[NSPLAT-21042]

Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande `rm cloudprofile` pour supprimer le profil.

[NSPLAT-4520]

Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

[NSPLAT-4451]

À partir de la version 13.1 de NetScaler, l'appliance NetScaler ne démarre pas dans un hyperviseur ESXi doté de plus de 8 interfaces réseau VMXNET3.

[NSHELP-31266]

Stratégies

Les connexions peuvent se bloquer si la taille des données de traitement est supérieure à la taille de tampon TCP par défaut configurée.Solution : définissez la taille du tampon TCP sur la taille maximale des données à traiter.

[NSPOLICY-1267]

SSL

Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

Solution :

1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
2. Enregistrez la configuration.

[NSSSL-9572]

Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

[NSSSL-6478]

Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

[NSSSL-6213]

Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
ERREUR : actualisation des CRL désactivée

[NSSSL-6106]

L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

[NSSSL-4427]

Un message d'avertissement incorrect `Warning: No usable ciphers configured on the SSL vserver/service`, s'affiche si vous essayez de modifier le protocole SSL ou le chiffrement dans le profil SSL.

[NSSSL-4001]

Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA. [NSSSL-3184, NSSSL-1379, NSSSL-1394]

Une appliance NetScaler peut tomber en panne dans les scénarios suivants :

- Un moniteur d'équilibrage de charge de type SSL et un service SSL portent le même nom
- Un service SSL est renommé
- Un moniteur d'équilibrage de charge est supprimé

[NSHELP-30445]

Système

La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client.

[NSHELP-21240]

Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

[NSHELP-10972]

Dans un déploiement de cluster, si vous exécutez la commande `force cluster sync` sur un nœud non CCO, le fichier ns.log contient des entrées de journal en double. [NSBASE-16304, NSGI-1293]

Lorsque vous installez NetScaler ADM sur un cluster Kubernetes, cela ne fonctionne pas comme prévu car les processus requis peuvent ne pas s'exécuter.

Solution : redémarrez le module Gestion.

[NSBASE-15556]

L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

[NSBASE-8506]

Interface utilisateur

Pour la fonction de réécriture MQTT, vous ne pouvez pas supprimer une expression à l'aide de l'éditeur d'expression dans l'interface graphique.

Solution :

Utilisez la commande d'action add ou edit de type MQTT via l'interface de ligne de commande.

[NSUI-18049]

Dans l'interface graphique de NetScaler, le `Help` lien présent sous l' `Dashboard` onglet est rompu.

[NSUI-14752]

L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution :

Configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de la CLI de NetScaler.

[NSUI-13024]

Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

[NSUI-6838]

Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

- Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

Solution :

Effectuez le basculement HA manuel successif uniquement après la fin de la synchronisation HA (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

Dans une configuration à haute disponibilité des appliances NetScaler BLX, le nœud principal peut ne plus répondre en bloquant toute demande de CLI ou d'API.

Solution :

Redémarrez le nœud principal.

[NSCONFIG-6601]

Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

1. Mettez à niveau l'appliance NetScaler vers l'une des versions suivantes :
    - 13.0 52.24 build
    - 12.1 57.18 build
    - 11.1 65.10 build
2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
3. Rétrogradez l'appliance NetScaler vers une version antérieure.

Pour afficher la liste de ces utilisateurs système à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solution :

Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

- Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.

- Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
- Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notes de publication pour la version 13.1-24.38 de NetScaler

May 5, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1-24.38 de NetScaler.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

Les versions 13.1-24.38 et ultérieures corrigent les failles de sécurité décrites dans la section https://support.citrix.com/article/CTX457836.

Nouveautés

Améliorations et modifications disponibles dans Build 13.1-24.38.

Équilibrage de charge

Prise en charge du basculement de connexion pour le mode INC haute disponibilité

NetScaler prend désormais en charge le basculement de connexion pour le mode INC à haute disponibilité lorsque toutes les conditions suivantes sont remplies :

- Le type de service du serveur virtuel est ANY.
- Le mode est DSR (MAC, IPTUNNEL ou TOS).
- USIP est activé sur les services liés au serveur virtuel.

[NSLB-9121]

Prise en charge des dossiers CAA

L'appliance NetScaler prend désormais en charge l'ajout d'enregistrements d'autorisation de l'autorité de certification (CAA). L'enregistrement CAA est un type d'enregistrement DNS (Domain Name System) qui permet aux propriétaires de domaine de spécifier quelle autorité de certification (CA) peut émettre des certificats SSL pour le domaine.

Cette amélioration fournit un niveau de protection supplémentaire à votre présence sur le Web. Le fait de ne pas disposer d'enregistrements CAA peut entraîner un risque de sécurité, car n'importe qui peut générer une demande de signature de certificat (CSR) pour le domaine et faire signer le certificat par n'importe quelle autorité de certification.

[NSLB-9007]

Plateforme

Sur la plate-forme NetScaler SDX 8015, la version de gestion des lumières (LOM) est passée de 3.21 à 3.56.

Sur les plateformes NetScaler SDX 14000, SDX 14000-40G, SDX 14000-40S et SDX 14000-FIPS, la version LOM est mise à niveau de la version 4.08 à la version 4.14.

[NSPLAT-23416]

Support pour le backend NetScaler Autoscale sur Azure avec VMSS dans tous les groupes de ressources

L'instance NetScaler VPX prend désormais en charge la mise à l'échelle automatique du back-end Azure entre les groupes de ressources dans les scénarios suivants :

Les instances Azure VMSS et NetScaler VPX sont déployées dans le même réseau virtuel Azure.
Les instances Azure VMSS et NetScaler VPX sont déployées dans différents réseaux virtuels Azure qui font partie du même abonnement Azure. Ces deux réseaux virtuels doivent être connectés à l'aide de la fonctionnalité d'appairage de réseaux virtuels d'Azure.

Cette fonctionnalité vous permet de séparer les applications et les ressources réseau dans différents groupes de ressources.

Auparavant, le back-end Autoscale de NetScaler sur Azure ne fonctionnait que si les instances VMSS et NetScaler VPX étaient déployées dans le même groupe de ressources.

[NSPLAT-16664]

Système

Compteurs d'abonnement sur le collecteur de métriques

L'appliance NetScaler prend désormais en charge une option permettant de s'abonner à des compteurs sur le collecteur de métriques.
Le collecteur de mesures prend en charge l'exportation de données d'analyse de séries chronologiques toutes les 30 secondes dans différents formats tels que AVRO, le format Prometheus et le format Influx DB. Le collecteur de metrics prend en charge la mise à jour dynamique des compteurs qui vous permet d'ajouter les compteurs requis à un fichier de schéma. Vous pouvez configurer le nom du fichier de schéma à l'aide de l'interface CLI. Le collecteur de métriques lit les noms de compteurs à partir du fichier de schéma et les exporte.

Auparavant, le collecteur de metrics ne prenait en charge que l'exportation d'un ensemble prédéfini de compteurs au moment de la compilation. Toute modification de la liste des compteurs nécessitait une mise à niveau de build.
Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html.

[NSBASE-11595]

Interface utilisateur

Configurer les alertes d'expiration des licences NetScaler

Vous pouvez désormais configurer l'appliance NetScaler pour effectuer les opérations d'alerte suivantes pendant un nombre de jours spécifié avant l'expiration d'une licence NetScaler :

- Affiche une bannière d'alerte d'expiration de licence sur l'interface graphique de NetScaler.
- Envoie des interruptions SNMP contenant les informations d'expiration de licence à intervalles réguliers aux écouteurs de trap configurés si l'alarme `NS_LICENSE_EXPIRY` SNMP est activée.

[NSCONFIG-6360]

Problèmes résolus

Les problèmes qui sont résolus dans Build 13.1-24.38.

Authentification, autorisation et audit

Dans une configuration de passerelle unifiée, dans de rares cas, une page de reconnexion peut s'afficher lorsque vous accédez à des services derrière la passerelle unifiée, même après que l'authentification a réussi.

[NSHELP-31148, NSHELP-27994]

L'authentification unique basée sur les formulaires échoue pour les serveurs principaux qui envoient des paramètres clé-valeur dans la requête URL.

[NSHELP-30975]

L'appliance NetScaler peut se bloquer en raison d'une allocation de mémoire importante en raison de l'absence d'une URL cible dans la configuration OAuth.

[NSHELP-30963]

Vous pouvez rencontrer des problèmes intermittents avec l'authentification RADIUS lors de l'utilisation de Chrome en mode navigation privée.

[NSHELP-30944]

Le module d'authentification, d'autorisation et d'audit de l'appliance NetScaler peut se bloquer en raison d'une longueur de mot de passe entrante manquante ou incorrecte entre le moteur de paquets et l'authentification, l'autorisation et l'audit.

[NSHELP-30911]

L'appliance NetScaler se bloque lors de l'opération de poussée de nFactor.

[NSHELP-30577]

Il peut y avoir un échec intermittent lors de la connexion au serveur d'échange Outlook via l'application Outlook en raison d'un ajout d'en-tête incorrect par l'appliance NetScaler.

[NSHELP-30555]

L'appliance NetScaler peut se bloquer en raison d'une corruption de la mémoire en cas d'échec de la communication cœur à cœur.

[NSHELP-30275]

L'authentification unique échoue lors d'une session d'authentification lorsque l'événement de changement de mot de passe est déclenché. Ce problème se produit uniquement si le paramètre PersistentLogin attempts est activé.

[NSHELP-28085]

Dans certains cas, un message `invalid credentials` d'erreur s'affiche pendant le processus d'authentification RADIUS. L'erreur s'affiche lorsque l'appliance NetScaler est accessible depuis un appareil client à l'aide du navigateur Google Chrome.

[NSHELP-27113]

Lorsqu'une appliance NetScaler effectue une recherche de groupes LDAP imbriqués, certaines informations sur les groupes provenant de l'Active Directory sont manquées en raison d'un comportement non valide de l'appliance NetScaler. L'appliance ADC prend une valeur incorrecte même lorsque le paramètre `groupSearchSubAttribute` est configuré correctement.

[NSHELP-26316]

L'appliance NetScaler vide le cœur lorsque NOAUTH est configuré comme premier facteur et Negotiate comme facteur suivant dans le flux d'authentification basé sur 401.

[NSHELP-25203]

Appliance NetScaler SDX

Sur une interface graphique NetScaler SDX, l'affichage des serveurs NTP peut geler l'interface utilisateur si le fichier de configuration NTP (ntp.conf) ne contient que des espaces sur l'une des lignes.

[NSHELP-31530]

Sur une appliance NetScaler SDX dotée de cartes réseau Mellanox, la modification du débit d'une instance VPX dotée de cartes réseau Mellanox redémarre l'instance VPX.

[NSHELP-31305]

Après la mise à niveau d'une appliance NetScaler SDX vers la version 13.1 build 21.50 ou ultérieure, le déchiffrement SSL et la comparaison MAC peuvent échouer. Par conséquent, vous pouvez voir des échecs d'établissement de liaison SSL, un battement d'état VPX, une indisponibilité de l'interface utilisateur de l'instance VPX et une panne des serveurs virtuels et de l'application.

Remarque : Ce problème est observé sur les plates-formes SDX 8900, SDX 15000, SDX 15000-50G, SDX 26000 et SDX 26000-50S.

[NSHELP-31672]

NetScaler Gateway

Dans de rares cas, l'appliance NetScaler configurée avec un serveur virtuel VPN peut se bloquer après une connexion réussie à NetScaler Gateway.

[NSHELP-31481]

Dans une configuration ICA DTLS, l'appliance NetScaler Gateway se bloque lors du traitement du ticket STA.

[NSHELP-31211]

L'appliance NetScaler enregistre de manière incorrecte le `UDPFLOWSTAT` message indiquant que le trafic correspond au trafic UDP refusé par une politique d'autorisation. `Allowed`

[NSHELP-29542]

Une fuite de mémoire est observée dans une appliance NetScaler lorsqu'un proxy sortant est configuré.

[NSHELP-29234]

La page Session des utilisateurs actifs n'affiche pas toutes les sessions utilisateur actives sauf si le nombre d'entrées est passé à 2000 par page.

Avec ce correctif, un nouveau lien `All user session` (NetScaler Gateway -> Surveiller les connexions > Toutes les sessions utilisateur) est ajouté dans l'interface utilisateur d'administration qui répertorie toutes les sessions et connexions utilisateur.

[NSHELP-29151]

La sortie de commande `show vpn icaConnection` n'affiche pas correctement les numéros de série des connexions ICA. Ce problème se produit car le numéro de série est réinitialisé arbitrairement lors de l'exécution de `show vpn icaconnection`.

[NSHELP-25646]

Web App Firewall NetScaler

Une stratégie de Web App Firewall peut être enregistrée deux fois dans le fichier de configuration (`ns.conf`).

[NSHELP-30899]

Dans l'injection SQL WAF contenant une citation (guillemet simple, guillemet double ou coche inverse), les guillemets d'ouverture et de clôture doivent être présents pour marquer le modèle comme une attaque. Toutefois, lorsqu'un commentaire est présent dans le pattern, la citation finale n'est pas requise.

[NSHELP-30379]

Équilibrage de charge

Le préfixe d'étendue n'est pas défini correctement lorsque ECS est activé sur l'appliance ADC et que l'emplacement est introuvable. Ce problème entraîne la création d'une entrée de persistance incorrecte. L'entrée de persistance incorrecte est créée en fonction de l'adresse IP LDNS au lieu de l'adresse IP ECS reçue dans la demande pour la méthode GSLB basée sur la proximité non statique.

[NSHELP-30846]

Dans un scénario de course rare, le moteur de paquets peut tomber en panne avec Core Dump lorsque la configuration suivante est présente sur l'appliance NetScaler :

- Le serveur virtuel GSLB est configuré avec la persistance basée sur l'adresse IP source et la journalisation DNS est activée sur le profil DNS lié au service ADNS.
- Le serveur d'équilibrage de charge DNS est configuré sans que la journalisation DNS soit activée sur le profil DNS.

[NSHELP-29791]

Divers

L'interface utilisateur jQuery du portail est mise à jour de la version 1.12.1 vers la version 1.13.1 afin de corriger la vulnérabilité décrite dans les Bulletins de sécurité : CVE-2021-41182, CVE-2021-41183 et CVE-2021-41184.

[NSHELP-30209]

Réseau

Sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure), une appliance NetScaler BLX est toujours déployée en mode partagé, quels que soient les paramètres du fichier de configuration BLX (). `/etc/blx/blx.conf` Ce problème se produit car `mawk`, qui est présent par défaut sur les systèmes Linux basés sur Debian, n'exécute pas certaines des commandes awk présentes dans le fichier `blx.conf`.

[NSNET-14603]

Dans une configuration NAT44 à grande échelle, l'appliance NetScaler peut se bloquer lors de la réception du trafic SIP pour la raison suivante :

- Les entrées de filtrage et de mappage LSN ne sont pas présentes dans l'appliance.

[NSHELP-30225]

L'appliance NetScaler peut se bloquer si vous dissociez un ensemble de données d'une règle ACL alors que certains paquets correspondent à la règle ACL.

[NSHELP-30221]

Dans une configuration NAT44 à grande échelle, l'appliance NetScaler peut se bloquer lors de la réception du trafic SIP pour la raison suivante :

- Le nombre de références de session n'est pas nul lors de la suppression d'une entrée de filtrage

[NSHELP-29348]

Plateforme

Sur une appliance NetScaler SDX dotée d'une image à bundle unique (SBI) et de versions VPX 13.1-24.x ou ultérieures, le déploiement actif-actif utilisant le VRRP sur les cartes réseau Fortville est pris en charge. Ce déploiement n'est pas pris en charge en mode L2.

Les points suivants s'appliquent au déploiement :

- Citrix recommande de supprimer la configuration VRID du service de gestion avant de mettre à niveau ou de rétrograder l'instance VPX associée. Ajoutez la configuration VRID à partir du service de gestion une fois l'opération de mise à niveau ou de rétrogradation terminée.

- Si vous ne suivez pas la recommandation précédente, vous devez redécouvrir manuellement les instances VPX à partir du service de gestion pour activer la convergence VRRP.

[NSHELP-30670]

Le basculement HA pour l'instance NetScaler VPX sur le cloud GCP et AWS échoue lorsque le mot de passe d'un nœud RPC contient un caractère spécial.

[NSHELP-28600]

Stratégies

Dans certains scénarios, une appliance NetScaler peut se bloquer lorsqu'une action d'attribution est utilisée avec l'opération clear pour une variable AppExpert.

[NSHELP-29766]

SSL

Une appliance NetScaler MPX/SDX 14000 FIPS peut se bloquer en raison de l'utilisation continue d'API pour les opérations de chiffrement, par des applications internes telles que SAML, sur une certaine période.

[NSHELP-27952]

Système

Le collecteur REST est en panne même lorsque le paramètre AppFlow `TimeSeriesOverNSIP` est activé.

[NSHELP-30759]

Dans une appliance NetScaler, un problème de latence est observé dans les transactions HTTP/2 si les conditions suivantes sont remplies :

- La configuration SSL HTTP/2 est activée sur le service back-end
- Le service ne supporte pas le protocole HTTP/2.

[NSHELP-30020]

L'appliance NetScaler signale une fausse alarme SNMP sur les compteurs d'inondation du service SYN.

[NSHELP-28710, NSHELP-28713]

Interface utilisateur

Si une appliance NetScaler configurée avec des licences groupées est mise à niveau, l'appliance peut redémarrer avec une configuration partielle.

[NSHELP-30926]

Dans une appliance NetScaler, la liaison de la politique de cache pour remplacer la politique globale ou globale par défaut à l'aide de l'interface graphique échoue avec l'erreur suivante :

- Argument obligatoire manquant.

Cette erreur n'apparaît pas lors de la liaison de la stratégie de cache à l'aide de l'interface CLI.

[NSHELP-30826]

Le filtre de recherche n'est pas disponible pour la clé « Nom » sur la page Gérer les certificats > CSR de l'interface graphique NetScaler.

[NSHELP-30274]

Problèmes connus

Les problèmes qui existent dans la version 13.1-24.38.

AppFlow

HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

[NSINSIGHT-943]

Authentification, autorisation et audit

Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

[NSHELP-563]

Le LoginSchema DualAuthPushOrOTP.xml ne s'affiche pas correctement dans l'écran de l'éditeur de schéma de connexion de l'interface graphique NetScaler.

[NSAUTH-6106]

Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante.
`show adfsproxyprofile <profile name>`

Solution :

Connectez-vous au principal NetScaler actif du cluster et exécutez la `show adfsproxyprofile <profile name>` commande. Il afficherait l'état du profil proxy.

[NSAUTH-5916]

La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

- L'option Tester l'accessibilité LDAP est ouverte.
- Les informations d'identification de connexion non valides sont renseignées et envoyées.
- Les identifiants de connexion valides sont renseignés et envoyés.

Solution :

Fermez et ouvrez l'option Tester l'accessibilité LDAP.

[NSAUTH-2147]

Mise en cache

Une appliance NetScaler peut se bloquer si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

[NSHELP-22942]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, si le CLAG est créé sur une carte réseau Mellanox, le MAC CLAG est modifié lorsque l'instance VPX est redémarrée. Le trafic vers l'instance VPX s'arrête après le redémarrage car la table MAC contient l'ancienne entrée MAC CLAG.

[NSSVM-4333]

L'installation d'un certificat SSL sur une appliance NetScaler SDX échoue si le nom du certificat ou le nom de clé contient un espace.

[NSHELP-31711]

NetScaler Gateway

Lorsque Always on est configuré, le tunnel utilisateur échoue en raison du numéro de version incorrect (1.1.1.1) dans le fichier aoservice.exe.

[NSHELP-30662]

Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil « NetworkAccessOnVPNFailure » de « FullAccess » à « OnlyToGateway ».

[NSHELP-30236]

La page d'accueil de la passerelle ne s'affiche pas immédiatement après que le plug-in de passerelle a réussi à établir le tunnel VPN. Pour résoudre ce problème, la valeur de registre suivante est introduite.
\ HKLM \ Software \ Citrix \ Secure Access Client
SecureChannelResetTimeoutSeconds Type : DWORD

[NSHELP-30189]

Le client VPN Windows n'honore pas l'alerte « Notification de fermeture SSL » du serveur et envoie la demande de connexion de transfert sur la même connexion.

[NSHELP-29675]

Dans certains cas, le code de validation du serveur échoue lorsque le certificat de serveur est approuvé. Par conséquent, les utilisateurs finaux ne peuvent pas accéder à la passerelle.

[NSHELP-28942]

Vous remarquerez peut-être certaines adresses IP internes de Citrix dans le fichier rdx.js.

[NSHELP-28682]

L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

[NSHELP-28551]

Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

[NSHELP-28404]

Vous ne pouvez pas dissocier une stratégie d'autorisation classique à l'aide de l'interface graphique. Toutefois, vous pouvez utiliser l'interface de ligne de commande pour dissocier la stratégie d'autorisation d'authentification, d'autorisation et d'audit.

Avec ce correctif, vous pouvez désormais dissocier la stratégie d'autorisation à l'aide de l'interface graphique.

[NSHELP-27064]

Gateway Insight n'affiche pas d'informations précises sur les utilisateurs du VPN.

[NSHELP-23937]

Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

- L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
- L'appliance est configurée pour l'authentification par certificat avec une authentification à deux facteurs. `off`

[NSHELP-23584]

Parfois, lorsque vous parcourez les schémas, le message d'erreur `Cannot read property 'type 'of undefined` s'affiche.

[NSHELP-21897]

Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

[CGOP-19355]

L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

[CGOP-13621]

Le rapport Gateway Insight affiche de manière incorrecte la valeur `Local` plutôt que `SAML` dans le champ Type d'authentification en cas d'échec d'erreur SAML.

[CGOP-13584]

Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

[CGOP-13511]

Lorsqu'une connexion ICA est lancée à partir d'un Receiver MAC version 19.6.0.32 ou Citrix Virtual Apps and Desktops version 7.18, la fonctionnalité HDX Insight est désactivée.

[CGOP-13494]

Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

[CGOP-13493]

Lors de l'acceptation des connexions hôtes locales depuis le navigateur, la boîte de dialogue Accepter la connexion pour macOS affiche le contenu en anglais, quelle que soit la langue sélectionnée.

[CGOP-13050]

Le texte `Home Page` de l'application Citrix SSO > Page d'accueil est tronqué dans certaines langues.

[CGOP-13049]

Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

[CGOP-11830]

Dans Outlook Web App (OWA) 2013, le fait de cliquer sur **Options** dans le menu Paramètres affiche une boîte de dialogue **Erreur critique** . De plus, la page ne répond plus.

[CGOP-7269]

Équilibrage de charge

Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

[NSLB-7679]

Le format ServiceGroupName dans le `entityofs` piège pour le groupe de services est le suivant : `<service(group)name>?<ip/DBS>?<port>`

Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (?) est utilisé comme séparateur. NetScaler envoie le piège avec le point d'interrogation ()?. Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Dans certains scénarios, les serveurs liés à un groupe de services affichent une valeur de cookie non valide. Vous pouvez voir la valeur de cookie correcte dans les journaux de suivi.

[NSHELP-21196]

Divers

Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, l'appliance exécute la commande `set urlfiltering parameter` dans le nœud secondaire.
Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre `TimeOfDayToUpdateDB`.

[NSSWG-849]

Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

[NSHELP-22409]

Réseau

Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

[NSNET-25299]

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :

- L'appliance NetScaler BLX se voit attribuer un faible nombre de. `hugepages` Par exemple, 1G.
- L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

Le problème est consigné en tant que message d'erreur dans `/var/log/ns.log` :

- `BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x`

Remarque : x est un nombre <= nombre de processus de travail.

Solution :

Attribuez un nombre élevé de, `hugepages` puis redémarrez l'appliance.

[NSNET-25173]

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si les conditions suivantes sont remplies :

- L'appliance NetScaler BLX est affectée à un nombre élevé de. `hugepages` Par exemple, 16 Go.

Le problème est consigné en tant que message d'erreur dans `/var/log/ns.log` :

- `EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Too many open files`

Solution :

Utilisez l'une des solutions de contournement suivantes pour résoudre ce problème :

- Augmentez la limite de fichiers ouverts sur l'hôte Linux en utilisant la commande `ulimit` ou en modifiant le fichier `limits.conf`.
- Réduisez le nombre de `hugepages` alloués.

[NSNET-24727]

Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

[NSNET-24449]

Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

- Désactiver
- Activer
- Réinitialiser

[NSNET-16559]

L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solution :

Exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

- dpkg –add-architecture i386
- apt-get update
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

[NSHELP-21082]

Plateforme

Le basculement haute disponibilité ne fonctionne pas dans les clouds AWS et GCP. Le processeur de gestion peut atteindre 100 % de sa capacité dans les clouds AWS et GCP, ainsi que dans NetScaler VPX sur site. Ces deux problèmes sont provoqués lorsque les conditions suivantes sont remplies :

1. Lors du premier démarrage de l'appliance NetScaler, vous n'enregistrez pas le mot de passe demandé.
2. Ensuite, vous redémarrez l'appliance NetScaler.

[NSPLAT-22013]

Lorsque vous effectuez une mise à niveau d'une version 13.0/12.1/11.1 vers une version 13.1 ou que vous rétrogradez d'une version 13.1 vers une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances NetScaler. Ce problème est résolu pour les versions suivantes de NetScaler :

- 13.1-4.x
- 13.0-82.31 et versions ultérieures
- 12.1-62.21 et versions ultérieures

Les packages python ne sont pas installés lorsque vous rétrogradez les versions de NetScaler de 13.1-4.x vers l'une des versions suivantes :

- Toute version 11.1
- 12.1-62.21 et versions antérieures
- 13.0-81.x et versions antérieures

[NSPLAT-21691]

Dans une configuration de cluster sur une appliance NetScaler SDX, il existe une incompatibilité CLAG MAC sur le deuxième nœud et CLIP si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous ajoutez une autre instance VPX au cluster et à la configuration CLAG.

Par conséquent, le trafic vers l'instance VPX s'arrête.

[NSPLAT-21049]

Dans une configuration de cluster sur une appliance NetScaler SDX, le premier nœud tombe en panne en raison d'une incompatibilité d'adresses MAC entre CLIP et la table MAC, si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous supprimez le deuxième nœud du cluster.

[NSPLAT-21042]

Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande `rm cloudprofile` pour supprimer le profil.

[NSPLAT-4520]

Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

[NSPLAT-4451]

À partir de la version 13.1 de NetScaler, l'appliance NetScaler ne démarre pas dans un hyperviseur ESXi doté de plus de 8 interfaces réseau VMXNET3.

[NSHELP-31266]

Stratégies

Les connexions peuvent se bloquer si la taille des données de traitement est supérieure à la taille de tampon TCP par défaut configurée.Solution : définissez la taille du tampon TCP sur la taille maximale des données à traiter.

[NSPOLICY-1267]

SSL

Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

Solution :

1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
2. Enregistrez la configuration.

[NSSSL-9572]

Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

[NSSSL-6478]

Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

[NSSSL-6213]

Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
ERREUR : actualisation des CRL désactivée

[NSSSL-6106]

L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

[NSSSL-4427]

Un message d'avertissement incorrect `Warning: No usable ciphers configured on the SSL vserver/service`, s'affiche si vous essayez de modifier le protocole SSL ou le chiffrement dans le profil SSL.

[NSSSL-4001]

Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA. [NSSSL-3184, NSSSL-1379, NSSSL-1394]

Sur les appliances certifiées FIPS MPX 8900 et MPX 15000, l'exécution du trafic ECDHE peut provoquer une fuite de mémoire.

[NSHELP-30744]

Les personnalisations qui font partie du fichier rc.netscaler ne sont pas appliquées car ce fichier n'est pas exécuté lors de l'initialisation du système.

[NSHELP-31914]

Système

La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client.

[NSHELP-21240]

Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

[NSHELP-10972]

Dans un déploiement de cluster, si vous exécutez la commande `force cluster sync` sur un nœud non CCO, le fichier ns.log contient des entrées de journal en double. [NSBASE-16304, NSGI-1293]

Lorsque vous installez NetScaler ADM sur un cluster Kubernetes, cela ne fonctionne pas comme prévu car les processus requis peuvent ne pas s'exécuter.

Solution : redémarrez le module Gestion.

[NSBASE-15556]

L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

[NSBASE-8506]

L'appliance NetScaler supprime les paquets contenant des en-têtes HTTP personnalisés marqués d'un point (»). «) dans le champ du nom de l'en-tête. Cette action se produit parce que le paramètre `allowOnlyWordCharactersAndHyphen` est activé par défaut dans le profil HTTP par défaut.

Solution : désactivez cette option `allowOnlyWordCharactersAndHyphen` dans le profil HTTP par défaut. Citrix vous recommande toutefois de le laisser activé.

[NSBASE-16722]

Interface utilisateur

Pour la fonction de réécriture MQTT, vous ne pouvez pas supprimer une expression à l'aide de l'éditeur d'expression dans l'interface graphique.

Solution :

Utilisez la commande d'action add ou edit de type MQTT via l'interface de ligne de commande.

[NSUI-18049]

Dans l'interface graphique de NetScaler, le `Help` lien présent sous l' `Dashboard` onglet est rompu.

[NSUI-14752]

L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution :

Configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de la CLI de NetScaler.

[NSUI-13024]

Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

[NSUI-6838]

Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

- Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

Solution :

Effectuez le basculement HA manuel successif uniquement après la fin de la synchronisation HA (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

Dans une configuration à haute disponibilité des appliances NetScaler BLX, le nœud principal peut ne plus répondre en bloquant toute demande de CLI ou d'API.

Solution :

Redémarrez le nœud principal.

[NSCONFIG-6601]

Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

1. Mettez à niveau l'appliance NetScaler vers l'une des versions suivantes :

- 13.0 52.24 build
- 12.1 57.18 build
- 11.1 65.10 build

1. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
2. Rétrogradez l'appliance NetScaler vers une version antérieure.

Pour afficher la liste de ces utilisateurs système à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solution :

Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

- Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
- Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
- Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Remarques

May 5, 2023

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1—21.50 de NetScaler.

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

Les versions 13.1-21.50 et ultérieures corrigent les vulnérabilités de sécurité décrites dans la section https://support.citrix.com/article/CTX457048.

Nouveautés

Les améliorations et les modifications disponibles dans les versions 13.1 à 21.50.

Gestion des bots

Technique de limite de débit de bot basée sur la position géographique de l'utilisateur

La technique de détection de la limite de débit des bots vous permet désormais de limiter le trafic des robots en fonction de la position géographique de l'utilisateur. Dans cette configuration, vous pouvez définir un nom de pays comme une valeur similaire à l'URL ou au nom du cookie. Ce faisant, vous pouvez appliquer différentes limites de taux pour différents pays. Auparavant, la technique de détection pouvait limiter le trafic uniquement en fonction de l'adresse IP, de la session ou de l'URL du client.

[NSBOT-753]

Technique améliorée d'empreinte digitale de l'appareil (DFP) pour la détection des navigateurs sans tête

Un pirate informatique peut accéder aux ressources du serveur via un navigateur sans tête en automatisant des processus tels que la création de comptes multi-utilisateurs, la réservation de billets, la suppression des prix, le bourrage d'identifiants, les attaques par rotation de tickets, etc.

La technique de détection d'empreintes digitales (DFP) dans un profil de bot est désormais améliorée avec intelligence pour détecter les robots sans tête et les pilotes Web. Pour limiter le trafic des robots du navigateur sans tête, vous devez activer l'option Détection du navigateur sans tête ainsi que la fonction de détection d'empreintes digitales de l'appareil.

[NSBOT-747]

Web App Firewall NetScaler

Relaxation fine pour les attaques par injection de commande JSON

L'appliance NetScaler vous permet désormais de configurer une relaxation précise pour les attaques par injection de commandes JSON.

[NSWAF-8511]

Relaxation fine pour les attaques par script intersite JSON

L'appliance NetScaler vous permet désormais de configurer une relaxation précise pour les attaques JSON Cross-Site Scripting.

[NSWAF-8510]

Relaxation affinée pour les attaques par injection JSON SQL

L'appliance NetScaler vous permet désormais de configurer une relaxation précise pour les attaques par injection JSON SQL.

[NSWAF-8509]

Équilibrage de charge

Messages d'erreur de l'API État souhaité amélioré

Le message d'erreur affiché lorsque l'adresse IP d'un membre du groupe de services est déjà associée à d'autres entités NetScaler telles que le serveur virtuel CS, est amélioré. La raison de l'échec est désormais clairement indiquée dans le message d'erreur. Auparavant, la raison de l'échec du message d'erreur n'était pas claire.

[NSLB-9005]

L'API État souhaité prend en charge la réutilisation des adresses IP et des noms de serveurs existants

L'API d'état souhaité prend désormais en charge la liaison des membres d'un groupe de services à un groupe de services, même si l'adresse IP d'un membre du groupe de services correspond à un serveur existant. L'adresse IP et le nom du serveur existant sont réutilisés lors de la liaison du membre du groupe de services.

Auparavant, lorsque l'adresse IP correspondait, la liaison des membres du groupe de services à un groupe de services ne réussissait pas.

[NSLB-9004]

Réseau

Prise en charge des liaisons basées sur le CIDR dans les jeux de données IPv4 pour les listes de contrôle d'accès étendues

La liste ACL étendue prend désormais en charge les ensembles de données IPv4 contenant des plages d'adresses IPv4 spécifiées dans la notation CIDR.

[NSNET-24452]

Le logiciel bénéficie d'un support Side Scaler Side Scaler pour l'appliance NetScaler BLX en mode DPDK

Une appliance NetScaler BLX en mode DPDK et configurée avec un plus grand nombre de moteurs de paquets ne prend pas en charge un port NIC avec un nombre inférieur de files d'attente d'envoi (Tx) et de réception (Rx).

Une appliance NetScaler BLX en mode DPDK n'utilise pas de port NIC si les deux conditions suivantes sont remplies :

- L'appliance possède un port NIC qui prend en charge un nombre limité de files d'attente d'envoi (Tx) et de files d'attente de réception (Rx). Par exemple, 7.
- L'appliance est configurée avec un plus grand nombre de moteurs de paquets. Par exemple, 28.

Pour résoudre ce problème, à partir de la version 13.1 21.x, l'appliance NetScaler BLX utilise le software receive side scaling (RSS) pour distribuer efficacement les paquets reçus sur les ports NIC entre plusieurs moteurs de paquets.

Le module RSS logiciel attribue une paire de files d'attente logiques Rx et Tx à chaque port de carte réseau. La paire de files d'attente est ensuite mappée au moteur de paquets PE-0.

Pour chaque paquet dans la file d'attente Rx d'un port NIC, le PE-0 sélectionne un moteur de paquets à l'aide d'un algorithme de hachage RSS. PE-0 envoie ensuite le paquet au moteur de paquets sélectionné pour traitement. Une fois le traitement du paquet terminé, PE-0 envoie le paquet à la file d'attente Tx du port NIC.

[NSNET-23133]

Configurez le service d'interface graphique HTTP interne à l'aide de l'interface graphique NetScaler, de la CLI NetScaler ou des API NetScaler NITRO

Sur une appliance NetScaler, `/etc/httpd.conf` il s'agit du fichier de configuration du service d'interface graphique HTTP interne qui gère les connexions à l'interface graphique de NetScaler.

Au lieu d'utiliser le `httpd.conf` fichier pour configurer le service d'interface graphique HTTP interne, vous pouvez désormais utiliser l'interface graphique NetScaler, la CLI NetScaler ou les API NetScaler NITRO. Par exemple, vous pouvez utiliser l'interface de ligne de commande NetScaler pour modifier le nombre maximum de clients pouvant se connecter simultanément au service HTTP interne.

Le service GUI HTTP interne possède le format de nom suivant : `nshttpd-gui-<loop back IP address>-80`

Utilisez les opérations de commande du service NetScaler pour configurer le service d'interface graphique HTTP interne.

[NSNET-20350]

Plateforme

Support pour la plateforme NetScaler MPX 9100

Cette version prend en charge la plate-forme NetScaler MPX 9100. Il inclut les modèles MPX 9110, MPX 9120 et MPX9130. Pour plus d'informations, consultez NetScaler MPX9100.

[NSPLAT-23308]

Support pour la plateforme NetScaler SDX 9100

Cette version prend en charge la plate-forme NetScaler SDX 9100. Il inclut les modèles SDX 9120 et SDX 9130. Pour plus d'informations, consultez NetScaler SDX9100.

[NSPLAT-23299]

Améliorez les performances SSL-TPS sur les clouds AWS et GCP

Vous pouvez obtenir de meilleures performances SSL-TPS sur les clouds AWS et GCP en répartissant les poids du moteur de paquets (PE) de manière égale. Pour ce faire, exécutez la commande suivante sur l'interface de ligne de commande NetScaler pour définir le mode PE :

```
set cpuparam pemode [CPUBOUND | Default]
```

Dans un cloud Azure, les pondérations PE sont réparties de manière égale par défaut. Cette fonctionnalité n'améliore aucune performance pour les instances Azure.

[NSPLAT-22570]

Support de la mise à jour 3c de VMware ESXi 7.0 sur une instance NetScaler VPX

L'instance NetScaler VPX prend désormais en charge la mise à jour 3c de VMware ESXi version 7.0 (build 19193900).

[NSPLAT-22468]

SSL

Afficher les détails de l'utilisation des puces SSL sur les plateformes NetScaler

À partir de la version 13.1 build 21.x, des compteurs sont ajoutés pour afficher plus de détails sur l'utilisation des puces SSL sur les plates-formes MPX et SDX livrées avec les puces Intel Coleto et la plate-forme MPX 9100 (Lewisburg). Sur les plateformes non prises en charge, ces compteurs affichent une valeur de 0,0.

Pour plus d'informations, consultez la section Prise en charge des plates-formes basées sur des puces SSL Intel Coleto et Lewisberg.

[NSSSL-10996]

Prise en charge des certificats et des chiffrements ECDSA avec DTLS

Les certificats et les chiffrements ECDSA peuvent désormais être utilisés sur des entités DTLS, telles que des serveurs et des services virtuels.

[NSSSL-9535]

Système

Améliorations liées à l'envoi des détails du client dans l'en-tête de l'option TCP

- L'appliance NetScaler insère désormais l'adresse IP du client dans le dernier paquet ACK de l'établissement de liaison à trois voies en plus du premier paquet de données. Auparavant, l'appliance n'envoyait l'adresse IP du client que dans le premier paquet de données.
- L'appliance NetScaler prend désormais en charge l'envoi du port client dans l'option TCP pour la configuration du mode insertion. Un paramètre `Send Client Port in Tcp Option` (`sendClientPortInTcpOption`) a été introduit dans le profil TCP pour activer ou désactiver cette fonctionnalité.

[NSBASE-15635]

Problèmes résolus

Les problèmes qui sont résolus dans les versions 13.1 à 21.50.

Authentification, autorisation et audit

L'appliance NetScaler peut se bloquer en cas d'erreur lors de la mise à jour de la paire de clés de certificat SSL utilisée dans la configuration SAML. Pour résoudre ce problème, vous pouvez dissocier le certificat, le mettre à jour, puis le lier à nouveau.

[NSHELP-30270]

Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler si la demande de connexion via SAML contient des espaces autres que « » (guillemets simples). Avec ce correctif, tous les espaces sont autorisés.

[NSHELP-29773]

Lors de l'envoi d'une requête AS_REQ pour un utilisateur délégué, qui fait partie de KCD SSO, l'appliance NetScaler sélectionne un type de cryptage avec la priorité suivante lorsque le contrôleur de domaine (DC) publie tous les types de cryptage.

1. ETYPE_ARCFOUR_HMAC_MD5
2. ETYPE_AES128_CTS_HMAC_SHA1_96
3. ETYPE_AES256_CTS_HMAC_SHA1_96Instead of

4. ETYPE_AES256_CTS_HMAC_SHA1_96
5. ETYPE_AES128_CTS_HMAC_SHA1_96
6. ETYPE_ARCFOUR_HMAC_MD5

[NSHELP-28681]

Parfois, l'authentification peut échouer lorsque Authentification, autorisation et auditing.Login.Password est utilisé.

[NSHELP-28101]

L'appliance NetScaler peut entrer dans une boucle SSO avec le serveur principal et entraîner une accumulation de mémoire si les deux conditions suivantes sont remplies.

- L'appliance ADC effectue une négociation et des authentifications SSO NTLM avec le serveur principal.
- Le serveur principal ne parvient pas à effectuer les deux authentifications.

[NSHELP-27757]

L'appliance NetScaler peut se bloquer lorsque la synchronisation de la session et de la configuration des clés se produit entre la carte contrôleur principale et la carte contrôleur secondaire.

[NSHELP-26891]

Appliance NetScaler SDX

Un message incorrect s'affiche en cas d'échec d'une nouvelle installation car la partition d'usine ne dispose pas de suffisamment d'espace.

[NSHELP-30136]

Le champ de fond de panier de la page Ajouter un nœud de cluster n'est plus obligatoire sauf si l'une des conditions suivantes est remplie :

- Le groupe de nœuds existe déjà pour les grappes de couche 3.
- Il s'agit d'un cluster de couche 2.

[NSHELP-29701]

NetScaler Gateway

Les utilisateurs du client VPN ne peuvent pas se déconnecter correctement si SAML et EPA sont configurés en tant que facteurs successifs dans une authentification nFactor. Avec ce correctif, les utilisateurs peuvent se déconnecter sans problème.

[NSHELP-30193]

Dans une configuration NetScaler GSLB et VPN SSL, une fuite de mémoire est observée lors du traitement d'une connexion DTLS ICA. Par conséquent, la connexion est interrompue et la mémoire s'accumule.

[NSHELP-30182]

Le lancement de PCoIP Apps and Desktops échoue lorsqu'il est lancé à partir d'un navigateur et le message d'erreur `VMware client missing` s'affiche. Ce problème se produit car le protocole `vmware-view` n'est pas ajouté à la liste des protocoles autorisés.

[NSHELP-30062]

L'analyse EPA pour vérifier la dernière analyse complète du système antivirus échoue sur macOS.

[NSHELP-29571]

Le tunnel complet du VPN NetScaler Gateway ne fonctionne pas comme prévu si la réponse binaire est activée. Par conséquent, le cookie NSAAC est corrompu. Avec ce correctif, la réponse binaire fonctionne dans les plug-ins VPN précédents. Citrix vous recommande toutefois d'utiliser le dernier plug-in VPN compatible avec la réponse JSON.

[NSHELP-28729]

Équilibrage de charge

Une appliance NetScaler partitionnée peut vider le noyau lors du traitement d'un paquet de requête DNS avec un en-tête supplémentaire (EDNS).

[NSHELP-30796]

Dans un déploiement DNS à mise à l'échelle automatique, les membres dans l'état TROFS ne détectent pas et ne réagissent pas à l'échec du contrôle de santé.

[NSHELP-29628]

L'appliance NetScaler peut se bloquer lors de la liaison de la politique de réécriture au serveur virtuel d'équilibrage de charge si les conditions suivantes sont remplies :

1. L'évaluation de la seconde expression remplace les variables d'état de stratégie de la première expression en cours.
2. Les variables d'état de stratégie DETERMINE_SERVICES sont remplacées par la règle définie par le serveur virtuel d'équilibrage de charge.

[NSHELP-29449]

Le temps de réponse Monitor affiché lorsque vous exécutez la commande *show service* est parfois incorrect.

[NSHELP-28994]

Les messages de nouvelle tentative SMPP sont envoyés à tous les nœuds d'un cluster, même lorsque la demande aboutit. Ce scénario entraîne une consommation de mémoire élevée sur l'appliance NetScaler.

[NSHELP-28332]

Réseau

Lors de la mise à niveau d'une appliance NetScaler BLX vers la version 13.1 build 17.x, l'appliance peut ne pas démarrer.

[NSNET-25002]

L'installation d'une appliance NetScaler BLX sur un hôte Linux basé sur RHEL échoue si le module `jsonschema` python est absent sur l'hôte.

[NSNET-24638]

La mise à niveau d'une appliance NetScaler BLX avec DPDK échoue si toutes les conditions suivantes sont remplies :

- L'appliance NetScaler BLX s'exécute sur un hôte Linux basé sur Debian
- La mise à niveau s'effectue à partir de NetScaler version 13.0 build 82.x ou antérieure vers la version 13.1 build 17.x.

[NSNET-24622]

Lorsque vous configurez une règle ACL ICMP après avoir configuré une règle ACL TCP avec des paramètres de port, le problème suivant peut être observé :

- L'appliance NetScaler ajoute également de manière incorrecte les mêmes paramètres de port de l'ACL TCP à l'ACL ICMP.

[NSHELP-31114]

La modification d'une adresse IP privée dans une règle INAT à l'aide de l'interface graphique échoue si la condition suivante est remplie :

- Le basculement de connexion est activé sur la règle INAT.

[NSHELP-30792]

Sur la console série d'une appliance NetScaler, l'invite VTYSH ou l'invite shell peuvent n'afficher aucune sortie.

[NSHELP-30446]

La modification d'un profil réseau auquel est déjà lié un ensemble d'adresses IP peut échouer avec l'erreur suivante :

- `IP set is already bound to the network profile`

[NSHELP-29363]

Dans une configuration NAT44 à grande échelle, l'appliance NetScaler peut se bloquer lors de la réception du trafic SIP pour la raison suivante :

- Le nombre de références de filtrage et de mappage est différent de zéro pour le module LSN de l'appliance.

[NSHELP-28842]

Plateforme

La console série d'une instance NetScaler VPX hébergée sur le cloud Azure n'est pas accessible lorsque la machine virtuelle en est aux premiers stades de démarrage.

[NSPLAT-23010]

Lors du basculement de NetScaler VPX HA, le mouvement des adresses IP Elastic dans le cloud AWS échoue si vous configurez un IPSet sans lier l'IPSet à aucune adresse IP.

[NSHELP-29425]

SSL

La suite de chiffrement RC4 échoue lors d'une négociation SSL avec un message `Illegal parameter error`.

[NSSSL-11463]

L'appliance NetScaler se bloque lorsque l'interception SSL est activée et qu'il existe plusieurs demandes parallèles pour accéder à un serveur principal avec un certificat expiré.

[NSHELP-29520]

Dans une configuration de cluster, vous pouvez rencontrer les problèmes suivants :

- Commande manquante pour la liaison de la paire de clés de certificat par défaut aux services internes SSL sur le CLIP. Toutefois, si vous effectuez une mise à niveau à partir d'une version antérieure, vous devrez peut-être lier la paire de clés de certificat par défaut aux services internes SSL concernés sur le CLIP.
- Différence de configuration entre le CLIP et les nœuds de la commande set par défaut pour les services internes.
- Commande de liaison de chiffrement par défaut manquante aux entités SSL dans la sortie de la commande show running config exécutée sur un nœud. L'omission n'est qu'un problème d'affichage et n'a aucun impact fonctionnel. La liaison peut être visualisée à l'aide de la commande `<entity> <name>` show ssl.

[NSHELP-25764]

Système

L'appliance NetScaler se bloque si l'une des conditions suivantes se produit :

- L'action Syslog est configurée avec le nom de domaine et vous effacez la configuration à l'aide de l'interface graphique ou de l'interface de ligne de commande.
- La synchronisation haute disponibilité se produit sur le nœud secondaire. [NSHELP-30987, NSHELP-28121, NSHELP-29843]

Tous les paquets de données transférés depuis une appliance NetScaler ne possèdent pas la valeur TTL configurée, mais la valeur envoyée par le client ou le serveur.

[NSHELP-30683]

L'appliance NetScaler n'est pas en mesure de transmettre certains paquets de données non HTTP aux serveurs principaux.

[NSHELP-30192]

Dans certains scénarios, l'appliance NetScaler ne transmet pas certains paquets HTTP au serveur principal si les conditions suivantes sont remplies :

- Si une fonctionnalité de NetScaler clone en interne des paquets HTTP.

[NSHELP-29958]

L'appliance NetScaler peut ajouter de manière incorrecte une adresse IPv4 à un enregistrement AppFlow associé à une transaction IPv6.

[NSHELP-29261]

Une appliance NetScaler peut se bloquer lors de la réexécution d'une réponse fragmentée du module ICAP vers le client.

[NSHELP-28788]

L'échec de Pitboss se produit lors de la mise en boucle d'un grand nombre de paquets dans la file d'attente de retransmission.

[NSHELP-26071]

Certains messages SYSLOG sont supprimés lors de la connexion à un serveur SYSLOG externe à l'aide du protocole TCP.

[NSHELP-24522]

Dans certains scénarios, la capture de paquets nstrace omet tous les paquets si vous appliquez le filtre basé sur l'adresse IP.

[NSHELP-23483]

Interface utilisateur

Le filtrage du cache peut ne pas fonctionner comme prévu sur l'interface graphique de NetScaler.

[NSHELP-30392]

Lorsqu'une appliance NetScaler est configurée pour utiliser un serveur d'authentification externe, l'exécution des commandes stat peut être retardée, quel que soit le paramètre RBAonResponse défini à désactiver globalement. Le paramètre peut être désactivé depuis l'interface graphique ou l'interface de ligne de commande.

[NSHELP-30289]

L'interface graphique NetScaler ne traite pas les appels RAPI, ce qui empêche certains composants de l'interface graphique de répondre.

[NSHELP-30231]

Dans certains cas, il se peut que vous ne puissiez pas charger les clés SSL à partir de l'onglet Clés SSL de l'interface graphique de NetScaler.

[NSHELP-28870]

La réponse de l'API pour une requête NITRO GET avec un filtre peut contenir des informations supplémentaires même si elles ne sont pas mentionnées dans le filtre.

[NSHELP-28598]

Le chargement et l'ajout d'un fichier de liste de révocation de certificats (CRL) échouent dans la configuration d'une partition d'administration.

[NSHELP-20988]

Problèmes connus

Les problèmes qui existent dans les versions 13.1 à 21.50.

AppFlow

HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

[NSINSIGHT-943]

Authentification, autorisation et audit

Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

[NSHELP-563]

Le LoginSchema DualAuthPushOrOTP.xml ne s'affiche pas correctement dans l'écran de l'éditeur de schéma de connexion de l'interface graphique NetScaler.

[NSAUTH-6106]

Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante.
`show adfsproxyprofile <profile name>`

Solution :

Connectez-vous au principal NetScaler actif du cluster et exécutez la `show adfsproxyprofile <profile name>` commande. Il afficherait l'état du profil proxy.

[NSAUTH-5916]

La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

- L'option Tester l'accessibilité LDAP est ouverte.
- Les informations d'identification de connexion non valides sont renseignées et envoyées.
- Les identifiants de connexion valides sont renseignés et envoyés.

Solution :

Fermez et ouvrez l'option Tester l'accessibilité LDAP.

[NSAUTH-2147]

Mise en cache

Une appliance NetScaler peut se bloquer si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

[NSHELP-22942]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, si le CLAG est créé sur une carte réseau Mellanox, le MAC CLAG est modifié lorsque l'instance VPX est redémarrée. Le trafic vers l'instance VPX s'arrête après le redémarrage car la table MAC contient l'ancienne entrée MAC CLAG.

[NSSVM-4333]

Sur une appliance NetScaler SDX dotée de cartes réseau Mellanox, la modification du débit d'une instance VPX dotée de cartes réseau Mellanox redémarre l'instance VPX.

[NSHELP-31305]

Après la mise à niveau d'une appliance NetScaler SDX vers la version 13.1 build 21.50 ou ultérieure, le déchiffrement SSL et la comparaison MAC peuvent échouer. Par conséquent, vous pouvez voir des échecs d'établissement de liaison SSL, un battement d'état VPX, une indisponibilité de l'interface utilisateur de l'instance VPX et une panne des serveurs virtuels et de l'application.

Remarque : Ce problème est observé sur les plates-formes SDX 8900, SDX 15000, SDX 15000-50G, SDX 26000 et SDX 26000-50S.

[NSHELP-31672]

NetScaler Gateway

Dans certains cas, Citrix Secure Access pour macOS abandonne les connexions en raison de problèmes avec certains protocoles non DNS utilisant le port 53, tels que STUN.

[NSHELP-31004]

Lorsque Always on est configuré, le tunnel utilisateur échoue en raison du numéro de version incorrect (1.1.1.1) dans le fichier aoservice.exe.

[NSHELP-30662]

Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil « NetworkAccessOnVPNFailure » de « FullAccess » à « OnlyToGateway ».

[NSHELP-30236]

Le client VPN Windows n'honore pas l'alerte « Notification de fermeture SSL » du serveur et envoie la demande de connexion de transfert sur la même connexion.

[NSHELP-29675]

Dans certains cas, le code de validation du serveur échoue lorsque le certificat de serveur est approuvé. Par conséquent, les utilisateurs finaux ne peuvent pas accéder à la passerelle.

[NSHELP-28942]

L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

[NSHELP-28551]

Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

[NSHELP-28404]

Vous ne pouvez pas dissocier une stratégie d'autorisation classique à l'aide de l'interface graphique. Toutefois, vous pouvez utiliser l'interface de ligne de commande pour dissocier la stratégie d'autorisation d'authentification, d'autorisation et d'audit.

Avec ce correctif, vous pouvez désormais dissocier la stratégie d'autorisation à l'aide de l'interface graphique.

[NSHELP-27064]

Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

- Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

Solution :

Effectuez le basculement HA manuel successif uniquement après la fin de la synchronisation HA (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

Gateway Insight n'affiche pas d'informations précises sur les utilisateurs du VPN.

[NSHELP-23937]

Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

- L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
- L'appliance est configurée pour l'authentification par certificat avec une authentification à deux facteurs. `off`

[NSHELP-23584]

Parfois, lorsque vous parcourez les schémas, le message d'erreur `Cannot read property 'type 'of undefined` s'affiche.

[NSHELP-21897]

Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

[CGOP-19355]

L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

[CGOP-13621]

Le rapport Gateway Insight affiche de manière incorrecte la valeur `Local` plutôt que `SAML` dans le champ Type d'authentification en cas d'échec d'erreur SAML.

[CGOP-13584]

Dans une configuration à haute disponibilité, lors d'un basculement NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

[CGOP-13511]

Lorsqu'une connexion ICA est lancée à partir d'un Receiver MAC version 19.6.0.32 ou Citrix Virtual Apps and Desktops version 7.18, la fonctionnalité HDX Insight est désactivée.

[CGOP-13494]

Lorsque la fonction EDT Insight est activée, les canaux audio peuvent parfois échouer en cas de divergence réseau.

[CGOP-13493]

Lors de l'acceptation des connexions hôtes locales depuis le navigateur, la boîte de dialogue Accepter la connexion pour macOS affiche le contenu en anglais, quelle que soit la langue sélectionnée.

[CGOP-13050]

Le texte `Home Page` de l'application Citrix SSO > Page d'accueil est tronqué dans certaines langues.

[CGOP-13049]

Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

[CGOP-11830]

Dans Outlook Web App (OWA) 2013, le fait de cliquer sur **Options** dans le menu Paramètres affiche une boîte de dialogue **Erreur critique** . De plus, la page ne répond plus.

[CGOP-7269]

Équilibrage de charge

Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

[NSLB-7679]

Le format ServiceGroupName dans le `entityofs` piège pour le groupe de services est le suivant : `<service(group)name>?<ip/DBS>?<port>`

Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (?) est utilisé comme séparateur. NetScaler envoie le piège avec

le point d'interrogation ()?. Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Divers

Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, l'appliance exécute la commande `set urlfiltering parameter` sur le nœud secondaire.
Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre `TimeOfDayToUpdateDB`.

[NSSWG-849]

Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

[NSHELP-22409]

Réseau

Dans une appliance NetScaler BLX compatible DPDK, les VLAN balisés ne sont pas pris en charge pour les ports NIC Intel i350 DPDK. Ceci est observé car il s'agit d'un problème connu présent sur le pilote DPDK.

[NSNET-25299]

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :

- L'appliance NetScaler BLX se voit attribuer un faible nombre de. `hugepages` Par exemple, 1G.
- L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

Le problème est consigné en tant que message d'erreur dans `/var/log/ns.log` :

- `BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x`

Remarque : x est un nombre <= nombre de processus de travail.

Solution :

Attribuez un nombre élevé de, `hugepages` puis redémarrez l'appliance.

[NSNET-25173]

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si les conditions suivantes sont remplies :

- L'appliance NetScaler BLX est affectée à un nombre élevé de. `hugepages` Par exemple, 16 Go.

Le problème est consigné en tant que message d'erreur dans `/var/log/ns.log` :

- `EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Too many open files`

Solution :

Utilisez l'une des solutions de contournement suivantes pour résoudre ce problème :

- Augmentez la limite de fichiers ouverts sur l'hôte Linux en utilisant la commande `ulimit` ou en modifiant le fichier `limits.conf`.
- Réduisez le nombre de `hugepages` alloués.

[NSNET-24727]

Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

[NSNET-24449]

Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

- Désactiver
- Activer
- Réinitialiser

[NSNET-16559]

L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solution :

Exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

- dpkg –add-architecture i386
- apt-get update
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent,

la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

[NSHELP-21082]

Plateforme

Le basculement haute disponibilité ne fonctionne pas dans les clouds AWS et GCP. Le processeur de gestion peut atteindre 100 % de sa capacité dans les clouds AWS et GCP, ainsi que dans NetScaler VPX sur site. Ces deux problèmes sont provoqués lorsque les conditions suivantes sont remplies :

1. Lors du premier démarrage de l'appliance NetScaler, vous n'enregistrez pas le mot de passe demandé.
2. Ensuite, vous redémarrez l'appliance NetScaler.

[NSPLAT-22013]

Lorsque vous effectuez une mise à niveau d'une version 13.0/12.1/11.1 vers une version 13.1 ou que vous rétrogradez d'une version 13.1 vers une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances NetScaler. Ce problème est résolu pour les versions suivantes de NetScaler :

- 13.1-4.x
- 13.0—82.31 et versions ultérieures
- 12.1—62.21 et versions ultérieures

Les packages python ne sont pas installés lorsque vous rétrogradez les versions de NetScaler de 13.1-4.x vers l'une des versions suivantes :

- Toute version 11.1
- 12.1-62.21 et versions antérieures
- 13.0-81.x et versions antérieures

[NSPLAT-21691]

Dans une configuration de cluster sur une appliance NetScaler SDX, il existe une incompatibilité CLAG MAC sur le deuxième nœud et CLIP si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous ajoutez une autre instance VPX au cluster et à la configuration CLAG.

Par conséquent, le trafic vers l'instance VPX s'arrête.

[NSPLAT-21049]

Dans une configuration de cluster sur une appliance NetScaler SDX, le premier nœud tombe en panne en raison d'une incompatibilité d'adresses MAC dans les tables CLIP et MAC, si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous supprimez le deuxième nœud du cluster.

[NSPLAT-21042]

Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande `rm cloudprofile` pour supprimer le profil.

[NSPLAT-4520]

Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

[NSPLAT-4451]

À partir de la version 13.1 de NetScaler, l'appliance NetScaler ne démarre pas dans un hyperviseur ESXi doté de plus de 8 interfaces réseau VMXNET3.

[NSHELP-31266]

Stratégies

Les connexions peuvent se bloquer si la taille des données de traitement est supérieure à la taille de tampon TCP par défaut configurée.Solution : définissez la taille du tampon TCP sur une taille maximale de données à traiter.

[NSPOLICY-1267]

Dans certains scénarios, une appliance NetScaler peut se bloquer lorsqu'une action d'attribution est utilisée avec l'opération clear pour une variable AppExpert.

[NSHELP-29766]

SSL

Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

Solution :

1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
2. Enregistrez la configuration.

[NSSSL-9572]

Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

[NSSSL-6478]

Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

[NSSSL-6213]

Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
ERREUR : actualisation des CRL désactivée

[NSSSL-6106]

L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

[NSSSL-4427]

Un message d'avertissement incorrect `Warning: No usable ciphers configured on the SSL vserver/service`, s'affiche si vous essayez de modifier le protocole SSL ou le chiffrement dans le profil SSL.

[NSSSL-4001]

Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

[NSSSL-3184, NSSSL-1379, NSSSL-1394]

Sur les appliances certifiées FIPS MPX 8900 et MPX 15000, l'exécution du trafic ECDHE peut provoquer une fuite de mémoire.

[NSHELP-30744]

Les personnalisations qui font partie du fichier rc.netscaler ne sont pas appliquées car ce fichier n'est pas exécuté lors de l'initialisation du système.

[NSHELP-31914]

Système

La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client.

[NSHELP-21240]

Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

[NSHELP-10972]

Dans un déploiement de cluster, si vous exécutez la commande `force cluster sync` sur un nœud non CCO, le fichier ns.log contient des entrées de journal en double. [NSBASE-16304, NSGI-1293]

Lorsque vous installez NetScaler ADM sur un cluster Kubernetes, cela ne fonctionne pas comme prévu car les processus requis peuvent ne pas s'exécuter.

Solution : redémarrez le module Gestion.

[NSBASE-15556]

L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

[NSBASE-8506]

L'appliance NetScaler supprime les paquets contenant des en-têtes HTTP personnalisés marqués d'un point (»). «) dans le champ du nom de l'en-tête. Cette action se produit parce que le paramètre `allowOnlyWordCharactersAndHyphen` est activé par défaut dans le profil HTTP par défaut.

Solution : désactivez cette option `allowOnlyWordCharactersAndHyphen` dans le profil HTTP par défaut. Citrix vous recommande toutefois de le laisser activé.

[NSBASE-16722]

Interface utilisateur

Pour la fonction de réécriture MQTT, vous ne pouvez pas supprimer une expression à l'aide de l'éditeur d'expression dans l'interface graphique.

Solution :

Utilisez la commande d'action add ou edit de type MQTT via l'interface de ligne de commande.

[NSUI-18049]

Dans l'interface graphique de NetScaler, le `Help` lien présent sous l' `Dashboard` onglet est rompu.

[NSUI-14752]

L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution :

Configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de la CLI de NetScaler.

[NSUI-13024]

Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

[NSUI-6838]

Dans une configuration à haute disponibilité des appliances NetScaler BLX, le nœud principal peut ne plus répondre en bloquant toute demande de CLI ou d'API.

Solution :

Redémarrez le nœud principal.

[NSCONFIG-6601]

Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

1. Mettez à niveau l'appliance NetScaler vers l'une des versions suivantes :

- 13.0 52.24 build
- 12.1 57.18 build
- 11.1 65.10 build

1. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
2. Rétrogradez l'appliance NetScaler vers une version antérieure.

Pour afficher la liste de ces utilisateurs système à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

```
query ns config -changedpassword [-config <full path of the configuration
file (ns.conf)>]
```

Solution :

Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

- Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées précédemment), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
- Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.

- Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, voir How to reset root administrator (nsroot) password.

[NSCONFIG-3188]

Notes de publication pour la version 13.1—17.42 de NetScaler

May 5, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1—17.42 de NetScaler.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

Nouveautés

Améliorations et modifications disponibles dans les versions 13.1 à 17.42.

Gestion des bots

Support pour l'adressage IPv6

La gestion des robots NetScaler prend désormais en charge l'adressage IPv6 (Internet Protocol Version 6) pour les techniques de détection des robots.

[NSBOT-690]

NetScaler Gateway

Propagation des bits DF pour EDT via NetScaler Gateway

L'appliance NetScaler Gateway prend désormais en charge l'application des bits DF pour la fonctionnalité EDT Path Maximum Transmission Unit Discovery (PMTUD). La fonction de découverte du MTU de chemin permet de déterminer dynamiquement l'unité de transmission maximale (MTU) lors de l'établissement d'une session EDT. L'application des bits DF empêche la fragmentation EDT qui pourrait entraîner une dégradation des performances ou l'échec de l'établissement d'une session.

Dans les versions précédentes, NetScaler Gateway prenait en charge le chemin EDT MTUD mais ne prenait pas en charge l'application des bits DF.

[CGOP-18438]

Web App Firewall NetScaler

Prise en charge améliorée de l'apprentissage de plusieurs violations de script intersite (XSS)

Le processus d'apprentissage de NetScaler Web App Firewall est désormais amélioré afin de réduire le nombre de faux positifs lors d'attaques par script intersites.

Lorsque l'apprentissage est activé, vous pouvez apprendre toutes les violations d'une demande et éventuellement appliquer un assouplissement à toutes les balises/attributs/modèles en même temps. Auparavant, vous ne pouviez signaler qu'une seule violation à la fois et vous deviez répéter le processus pour plusieurs violations.

Par exemple, s'il y a 15 balises personnalisées dans une charge utile entraînant chacune une violation, vous pouvez appliquer un assouplissement pour la première violation et exécuter la demande pour marquer une autre balise personnalisée en tant que violation. Le processus doit être répété pour appliquer une relaxation à toutes les balises personnalisées une par une.

[NSWAF-7545]

Équilibrage de charge

Option permettant d'activer ou de désactiver les membres du groupe de services Autoscale LB et GSLB

Vous pouvez désormais activer ou désactiver directement des membres spécifiques d'un groupe de services Autoscale LB ou GSLB (basé sur DNS). Par conséquent, la gestion d'un groupe de services Autoscale LB ou GSLB (basé sur DNS) est désormais facilitée.

Auparavant, vous deviez activer ou désactiver un groupe de services Autoscale LB ou GSLB entier pour activer ou désactiver un membre individuel. Seuls les groupes de services non autoscale avaient la possibilité d'activer ou de désactiver un membre individuel.

[NSLB-8109]

Réseau

Amélioration des statistiques ISSU

Les deux améliorations suivantes ont été ajoutées aux statistiques ISSU :

- Une option `dumpsession` (`Dump Session`) a été ajoutée à l'opération `show migration` pour afficher la liste des connexions existantes actuellement desservies par l'ancien nœud principal. L'opération de migration d'exposition avec l'option `dumpsession` doit être exécutée uniquement sur le nouveau nœud principal.
- L'opération de migration d'exposition (sans option) affiche désormais les informations supplémentaires suivantes relatives à l'opération de migration ISSU :
- Nombre total de connexions traitées dans le cadre de l'opération de migration ISSU
- Nombre de connexions restantes en cours de traitement dans le cadre de l'opération de migration ISSU

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/issu-high-availability.html .

[NSNET-23577]

Surveillez l'utilisation des ports sur une appliance NetScaler pour les connexions dorsales à l'aide du SNMP

Vous pouvez utiliser l'alarme `PORT-ALLOC-EXCEED` SNMP pour surveiller l'utilisation des ports sur une appliance NetScaler pour les connexions dorsales.

`PORT-ALLOC-EXCEED` L'alarme SNMP inclut les `normal-threshold` paramètres `high-threshold` et, qui spécifient le total des ports alloués aux adresses IP détenues par NetScaler sous forme de pourcentages. Par exemple, si le `high-threshold` paramètre est défini sur 90, l'appliance NetScaler génère et envoie des messages d'interruption lorsque l'événement suivant se produit :

- lorsque le pourcentage d'allocation de ports dépasse 90 % sur l'une des adresses IP appartenant à NetScaler pour les connexions dorsales

Les alertes SNMP vous aident à déterminer si vous avez besoin d'un plus grand nombre d'adresses IP appartenant à NetScaler si les ports libres disponibles sont presque épuisés.

[NSNET-21719]

Prise en charge du protocole GENEVE

Une appliance NetScaler prend désormais en charge le protocole GENEVE (Generic Network Virtualization Encapsulation) tel que défini dans la RFC 8926.

La virtualisation des serveurs et l'architecture du cloud computing ont augmenté la demande de réseaux isolés de couche 2 dans un centre de données. La limite VLAN de 4094 s'est révélée inadéquate et des protocoles d'encapsulation tels que VXLAN et NVGRE ont été introduits pour surmonter cette limite.

Ces protocoles diffèrent principalement dans la mise en œuvre du plan de contrôle. Le protocole GENEVE ne définit pas de spécifications pour le plan de contrôle. Le protocole laisse à l'implémentation le soin de définir les spécifications du plan de contrôle.

Le protocole GENEVE est une technologie d'encapsulation qui vise à créer des réseaux de superposition de couche 2 sur une infrastructure de couche 3 en encapsulant des trames de couche 2 dans des paquets UDP. Chaque VLAN est identifié par un identifiant 24 bits unique appelé VNID. Seul le même ID de segment (VNID) peut communiquer entre eux.

Une appliance NetScaler prend en charge l'encapsulation GENEVE sur le port UDP 6081.

[NSNET-21717]

Configurer l'accès SSH à l'hôte Linux exécutant une appliance NetScaler BLX en mode dédié

Par défaut, l'accès SSH à un hôte Linux exécutant l'appliance NetScaler BLX en mode dédié ne peut pas être effectué via les interfaces dédiées de l'appliance.

Vous pouvez configurer l'accès SSH à l'hôte Linux via les interfaces dédiées de l'appliance NetScaler BLX. Cette fonctionnalité est utile dans un hôte Linux à interface unique exécutant une appliance NetScaler BLX en mode dédié.

Vous pouvez configurer l'accès SSH direct à l'hôte Linux dans l'un des types suivants :

- Fournissez un accès SSH sur le port 9022 de NetScaler IP (NSIP) de l'appliance NetScaler BLX. - `<NetScaler IP address (NSIP)>:9022`
- Définissez une nouvelle adresse IP dans le sous-réseau de NetScaler IP (NSIP) et fournissez un accès SSH sur le port 22. - `<new IP address on the NetScaler IP address (NSIP) subnet>:22`
  De plus, tous les autres ports de l'hôte Linux sont accessibles via la nouvelle adresse IP. Par exemple, un `rsyslog` serveur fonctionnant sur l'hôte Linux sur le port 514/UDP est désormais accessible sur le port 514 de la nouvelle adresse IP.

[NSNET-21586]

Déploiement simplifié d'une appliance NetScaler BLX avec ports DPDK

La procédure de déploiement d'une appliance NetScaler BLX avec des ports DPDK a été simplifiée grâce aux améliorations suivantes :

- L'appliance NetScaler BLX utilise désormais des bibliothèques compilées avec la version 20.11.1 de DPDK. L'appliance charge automatiquement le module noyau DPDK VFIO sur l'hôte Linux.
- Le `dpdk-config` paramètre a été supprimé du fichier de configuration NetScaler BLX ()`blx.conf`. Le `worker-processes` paramètre existant s'applique désormais également à

l'appliance NetScaler BLX dotée de ports DPDK. `worker-processes` Spécifie le nombre de moteurs de paquets pour une appliance NetScaler BLX. En d'autres termes, `worker-processes` il s'agit désormais d'un paramètre commun à l'appliance NetScaler BLX quel que soit son mode (partagé, dédié ou DPDK). Si `worker-process` ce n'est pas le cas, l'appliance NetScaler BLX est configurée avec 1 moteur de paquets par défaut.

- Le paramètre `interfaces` spécifie désormais les ports de carte réseau compatibles DPDK en plus des ports de carte réseau autres que DPDK. L'appliance NetScaler BLX détecte automatiquement les ports NIC compatibles DPDK (le cas échéant) dans la liste des ports spécifiée dans le paramètre. `interfaces` L'appliance lie ensuite les ports NIC compatibles DPDK détectés au module VFIO DPDK sur l'hôte Linux. Après le démarrage de l'appliance NetScaler BLX, les ports NIC DPDK et non DPDK sont automatiquement ajoutés dans le cadre de l'appliance.
- Le `dpdk-non-uio-intf` paramètre, qui spécifie les ports NIC Mellanox liés au DPDK, a été supprimé du fichier de configuration NetScaler BLX ().`blx.conf` Le `interfaces` paramètre spécifie désormais les ports NIC Mellanox à utiliser comme ports DPDK dans l'appliance NetScaler BLX. Avant de spécifier les ports NIC Mellanox pour l'appliance NetScaler BLX, les bibliothèques Mellanox OFED DPDK et les modules du noyau doivent être installés sur l'hôte Linux. L'appliance NetScaler BLX détecte automatiquement les ports NIC Mellanox spécifiés et les initialise en mode DPDK. Après le démarrage de l'appliance NetScaler BLX, les ports NIC Mellanox liés au DPDK sont ajoutés dans le cadre de l'appliance.
- Un nouveau paramètre a `total-hugepage-mem` été introduit dans le fichier de configuration NetScaler BLX (`blx.conf`) pour configurer le `hugepages` pour DPDK sur l'hôte Linux. Le paramètre `total-hugepage-mem` spécifie la taille de `hugepages` en Mo ou Go (par exemple, 1024 Mo et 2 Go).
- Lors de la mise à niveau d'une appliance NetScaler BLX avec des ports DPDK, le module de mise à niveau convertit automatiquement les configurations existantes au nouveau format dans le fichier de configuration () de NetScaler BLX.`blx.conf`

[NSNET-20524]

Surveillez les ports libres disponibles sur une appliance NetScaler pour une nouvelle connexion principale

Pour communiquer avec les serveurs physiques ou d'autres appareils homologues, l'appliance NetScaler utilise une adresse IP appartenant à Citrix comme adresse IP source. L'appliance NetScaler gère un pool d'adresses IP et sélectionne dynamiquement une adresse IP lors de la connexion à un serveur. En fonction du sous-réseau dans lequel le serveur physique est placé, l'appliance décide de l'adresse IP à utiliser. Ce pool d'adresses est utilisé pour envoyer du trafic et surveiller les sondes.

Vous pouvez afficher le nombre total de ports libres disponibles sur les adresses IP détenues par NetScaler pour une nouvelle connexion principale. Ces informations vous aident à déterminer s'il est nécessaire de disposer d'un plus grand nombre d'adresses IP appartenant à NetScaler si les ports

libres disponibles sont presque épuisés.

Vous pouvez fournir les informations suivantes à l'appliance NetScaler afin de calculer le nombre total de ports libres disponibles pour une nouvelle connexion principale :

- Adresse IP appartenant à Citrix (facultatif)
- Adresse IP de destination
- Port de destination
- Protocole TCP ou non TCP

[NSNET-20410]

Plateforme

Prise en charge des configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler sur l'hyperviseur KVM

Vous pouvez désormais appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler sur l'hyperviseur KVM. Par conséquent, une configuration client sur une instance VPX peut être configurée en beaucoup moins de temps.

[NSPLAT-21571]

Exclure le dossier nstrace des partitions d'administration NetScaler lors de l'opération de sauvegarde

Dans une appliance NetScaler avec des partitions d'administration, l'opération de sauvegarde du dossier nstrace est exclue. Cela permet de réduire la taille globale de sauvegarde de NetScaler sans perdre de données importantes.

[NSPLAT-21433]

Stratégies

Prise en charge de la notation de sous-réseau CIDR dans les adresses IPv4 et IPv6 pour l'ensemble de données de stratégie

Les jeux de données de stratégie pour les adresses IPv4 et IPv6 autorisent désormais la valeur liée à des sous-réseaux utilisant la notation CIDR (par exemple, a.b.c.d/n). La notation CIDR spécifie l'adresse et la plage du sous-réseau. Auparavant, il n'était pas possible d'ajouter des sous-réseaux dans les jeux de données de stratégie.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/appexpert/pattern-sets-data-seta/configuring-data-sets.html

[NSPOLICY-3828]

SSL

Désactiver les protocoles non sécurisés sur les services SSL frontaux d'une appliance NetScaler

Les scans de sécurité standard peuvent déclencher une alerte concernant les protocoles non sécurisés sur les services SSL frontaux créés par défaut lors du démarrage d'une appliance NetScaler. Pour éviter de telles alertes, ces protocoles sont désormais désactivés par défaut sur les services SSL frontaux lorsque les appliances démarrent. Des exemples de protocoles non sécurisés sont SSLv3, TLv1 et TLSv1.1.

Lorsque le profil SSL par défaut est activé, un nouveau profil SSL est créé dans lequel ces protocoles sont désactivés. Ce nouveau profil est lié aux services SSL frontaux (ns_default_ssl_profile_internal_frontend_serv
Ce profil est modifiable.

[NSSSL-9985]

Prise en charge des certificats signés à l'aide des algorithmes RSASSA-PSS

Toutes les plateformes NetScaler prennent désormais en charge les certificats signés à l'aide des algorithmes RSASSA-PSS. Ces algorithmes sont pris en charge dans la validation du chemin d'accès au certificat X.509.

[NSSSL-9289]

Problèmes résolus

Les problèmes qui sont traités dans les versions 13.1 à 17.42.

Authentification, autorisation et audit

L'appliance NetScaler se bloque si l'URL ADFSPIP est définie sur Type. `http://` ADFSPIP ne prend en charge que les types d'URL `https://`.

[NSHELP-29838]

L'appliance NetScaler peut se bloquer lors d'un flux d'IdP SAML en cas de retard important dans le traitement des demandes.

[NSHELP-29789]

Les stratégies de réécriture pour les points de terminaison tels que ne `/logon/LogonPoint/Resources/List and /cgi/Resources/List` sont pas prises en charge.

[NSHELP-29488]

Dans de rares cas, l'appliance NetScaler peut se bloquer en raison d'une position incorrecte du journal.

[NSHELP-29267]

Une appliance NetScaler configurée pour s'authentifier à l'aide du fournisseur de services OAuth ne peut pas être configurée avec 'client-secrete_post' pour s'authentifier avec IDP TokenEndpoint.

Avec ce correctif, la méthode d'authentification `client_secret_basic` est ajoutée à la fonctionnalité de fournisseur de services OAuth d'ADC lorsqu'il communique avec le point de terminaison du jeton de l'IdP.

[NSHELP-28945]

Une appliance NetScaler peut ne pas répondre lorsque l'authentification SAML est en cours et que des certificats X.509 d'une taille de 1 800 octets ou plus sont utilisés dans l'authentification SAML.

[NSHELP-28608]

L'expression Authentication, Authorization, and Auditing.User.Attribute peut donner une valeur vide dans l'appliance NetScaler multicœur lorsque le mot de passe utilisateur est modifié à son expiration.

[NSHELP-28419]

L'appliance NetScaler, lorsqu'elle est configurée en tant que partie associée à OAuth, n'ajoute pas les informations des champs « e-mail » et « nom d'utilisateur » extraites du jeton d'identification à l'attribut de hachage de la session d'authentification, d'autorisation et d'audit.

[NSHELP-28262]

Lorsque les métadonnées SAML sont configurées, une fuite de mémoire est observée avec les certificats SSL.

[NSHELP-27846]

Lorsqu'un utilisateur effectue une déconnexion SAML, la déconnexion ne se produit pas immédiatement et le message d'erreur suivant s'affiche :

```
Unsupported mechanisms found in Assertion; Please contact your administrator
.
```

Cette erreur est due au fait que le fournisseur d'identités configuré par le client utilise une technique de codage d'URL différente pour coder le paramètre d'algorithme de signature dans la réponse. Ce correctif prend désormais en charge le codage du paramètre d'algorithme de signature dans une réponse SAML à l'aide de plusieurs techniques de codage d'URL.

[NSHELP-27621]

Parfois, si nFactor est configuré, une adresse IP incorrecte est enregistrée dans le message de déconnexion.

[NSHELP-26692]

L'appliance NetScaler se bloque si les deux conditions suivantes sont remplies.

- L'OTP d'e-mail est configuré
- Le serveur de messagerie ne répond pas ou il y a un problème de réseau avec le serveur de messagerie

[NSHELP-26137]

Dans une configuration à haute disponibilité, l'appliance NetScaler se bloque lorsqu'une synchronisation forcée est initiée.

[NSAUTH-11876]

Intune NAC v2 n'est pas pris en charge pour Android 11 et versions ultérieures.

[NSAUTH-11872]

Les administrateurs ne peuvent pas utiliser l'outil de connectivité LDAP ou RADIUS si le mot de passe contient un certain caractère spécial ou si les arguments comportent un espace.

[NSAUTH-11322]

Gestion des bots

Lorsque le défi CAPTCHA est en cours, la gestion des robots NetScaler ne respecte pas la valeur configurée définie par l'utilisateur pour les nouvelles tentatives de CAPTCHA.

[NSBOT-801]

CallHome

L'enregistrement de CallHome peut échouer pour les appliances NetScaler MPX utilisant des licences groupées. L'enregistrement échoue car CallHome utilise un numéro de série incorrect pour enregistrer les appliances auprès du serveur de support NetScaler.

[NSHELP-28667]

Appliance NetScaler SDX

Lorsque vous restaurez une appliance NetScaler SDX à partir de la sauvegarde, la chaîne d'invite CLI n'est pas restaurée.

[NSHELP-30238]

Sur une appliance NetScaler SDX 115xx, la restauration d'un VPX doté d'un nombre élevé de cœurs de processeur (3 à 5 cœurs) peut échouer si la sauvegarde de l'appliance contient trois instances ou plus.

[NSHELP-30135]

Sur une appliance NetScaler SDX, la valeur par défaut pour déclencher l'alarme en cas d'`Hypervisor Disk Usage High` alerte est augmentée à 98 %.

[NSHELP-29688]

Lorsque la valeur de la vitesse d'interface est supérieure à 4 Gbit/s, une valeur incorrecte est renvoyée en raison d'un dépassement d'entier.

[NSHELP-29658]

Dans de rares cas, l'inventaire ADC ne s'effectue pas sur une appliance NetScaler SDX.

[NSHELP-29607]

Sur une appliance NetScaler SDX, le service de gestion n'envoie pas de notifications syslog ni par e-mail si des pannes d'alimentation, de tension ou de disque surviennent plusieurs fois.

[NSHELP-29443]

NetScaler Gateway

Les utilisateurs ne peuvent pas lancer le plug-in EPA ou le plug-in VPN après une mise à niveau vers les versions de navigateur Chrome 98 ou Edge 98. Pour résoudre ce problème, effectuez les opérations suivantes :

1. Pour la mise à niveau du plug-in VPN, les utilisateurs finaux doivent se connecter à l'aide du client VPN pour la première fois pour obtenir le correctif sur leurs machines. Lors des tentatives de connexion suivantes, les utilisateurs peuvent choisir le navigateur ou le plug-in à connecter.
2. Dans le cas d'utilisation EPA uniquement, les utilisateurs finaux n'auront pas le client VPN pour se connecter à la passerelle. Dans ce cas, effectuez les opérations suivantes :
    a) Connectez-vous à la passerelle à l'aide d'un navigateur.
    b) Attendez que la page de téléchargement apparaisse et téléchargez le fichier nsepa_setup.exe.
    c) Après le téléchargement, fermez le navigateur et installez le fichier nsepa_setup.exe.
    d) Redémarrez le client.

[NSHELP-30641]

Dans une configuration haute disponibilité avec configuration TCP SYSLOG, un nœud peut se bloquer pendant le basculement HA ou lors d'une opération de réinitialisation de la configuration.

[NSHELP-29251]

Sur la page du portail NetScaler Gateway, l'icône du **lien proxy RDP** ne change pas avec le thème du portail RFWebUI.

[NSHELP-28974]

Après la mise à niveau de l'appliance NetScaler Gateway vers la version 13.0, la configuration du proxy dans le profil de session ne fonctionne pas comme prévu. La connexion proxy est contournée pour le proxy NS non HTTP configuré.

Exemple :
add vpn sessionAction-proxy NS -httpProxy 192.0.2.0:24 -sslProxy 192.0.2.0:24

Dans cet exemple, -HttpProxy fonctionne comme prévu mais -SSLProxy ne fonctionne pas.

[NSHELP-28640]

L'appliance NetScaler Gateway se bloque lors du traitement de STA dans DTLS Audio car la mémoire allouée n'est pas réinitialisée.

[NSHELP-28432]

L'appliance NetScaler enregistre les messages périmés liés au processus VPND qui est obsolète.

[NSHELP-28163]

L'accès à StoreFront via un serveur virtuel VPN échoue si StoreFront est accessible via un serveur virtuel d'équilibrage de charge de sauvegarde.

[NSHELP-27852]

L'appliance NetScaler Gateway peut se bloquer lors de la reconnexion à une session ICA existante.

[NSHELP-27441]

Vous ne pouvez pas dissocier une stratégie d'autorisation classique à l'aide de l'interface graphique. Toutefois, vous pouvez utiliser l'interface de ligne de commande pour dissocier la stratégie d'autorisation d'authentification, d'autorisation et d'audit.

Avec ce correctif, vous pouvez désormais dissocier la stratégie d'autorisation à l'aide de l'interface graphique.

[NSHELP-27064]

Web App Firewall NetScaler

Une mise à niveau vers la bibliothèque XML version 2.9.12 entraîne la rupture des fichiers XML liés à la signature WAF pendant l'analyse.

[NSWAF-8662]

La protection contre l'injection de commande JSON apparaît `Not blocked` dans le message ns.log, même si la demande HTTP a été bloquée par le module Web App Firewall.

[NSHELP-29709]

Le message de journal du Web App Firewall s'affiche `BAD URL` pour les violations d'attribut d'URL de script intersite (XSS), et le terme n' `Bad URL` est pas clair quant à la catégorie à laquelle il appartient (comme une balise, un modèle ou un attribut).

[NSHELP-29358]

L'URL de publication de l'empreinte digitale du dispositif bot peut échouer si la stratégie de gestion des bots est activée sur un serveur virtuel d'équilibrage de charge de type SSL.

[NSHELP-29198]

L'ID de signature 1048 du Web App Firewall bloque le chargement de la page NetScaler Gateway.

[NSHELP-29113]

Une appliance NetScaler peut se bloquer si les modules suivants sont activés :

- Web App Firewall avec contrôles de sécurité avancés.
- Comté d'Appqoe.

[NSHELP-28251]

Équilibrage de charge

Lorsqu'un membre du groupe de services DNS de type Autoscale est dans l'état TROFS et si le même membre est à nouveau ajouté au groupe, l'état de ce membre n'est pas propagé.

[NSHELP-29493]

La synchronisation incrémentielle échoue pour `add dns action` et les commandes `add location` dont les expressions de stratégie contiennent des caractères génériques.

[NSHELP-29301]

Certains membres du groupe de services ne sont pas supprimés de la liste des groupes de services Autoscale en cas de conflit entre un membre lié statiquement et des enregistrements DNS résolus dynamiquement. Ce problème entraîne une corruption de la mémoire.

[NSHELP-28949]

L'état du groupe de services affiché dans les commandes show et stat est incohérent.

[NSHELP-28931]

Dans de rares cas, la configuration de la base de données d'emplacements peut être absente du fichier de configuration (ns.conf).

[NSHELP-28570]

Les moniteurs de type SQL ou Oracle se bloquent lorsque l'homologue envoie une demande de réinitialisation de la connexion existante.

[NSHELP-28478]

Dans un déploiement activé pour la persistance, un serveur virtuel incorrect est stocké lors de l'enregistrement contextuel.

[NSHELP-28342]

La configuration de persistance d'un groupe LB est perdue après un basculement HA ou lors du redémarrage de l'appliance NetScaler.

[NSHELP-28071]

L'état configuré du moniteur par défaut est désactivé même lorsque le moniteur par défaut est lié à un service.

[NSHELP-27669]

Divers

Le problème suivant se produit après la mise à niveau de l'appliance vers NetScaler version 12.1 build 63.22 :

- L'API de recherche d'extensions peut ne pas fonctionner après la mise à niveau.

[NSHELP-29860]

Réseau

Une appliance NetScaler peut tomber en panne si toutes les conditions suivantes sont remplies :

- Un itinéraire d'équilibrage de charge est configuré dans un domaine de trafic sur l'appliance.
- Une opération de configuration claire est effectuée sur l'appliance.

[NSNET-23847]

Dans une configuration NAT44 à grande échelle, l'appliance NetScaler peut se bloquer lors de la réception du trafic SIP pour la raison suivante :

- Le module LSN ne trouve pas le service lors de la décrémentation du nombre de références ou de la suppression du service.

[NSHELP-29134]

Dans un déploiement NAT44 à grande échelle, l'appliance NetScaler peut se bloquer lors de la réception du trafic SIP pour la raison suivante :

- Le module LSN a accédé à l'emplacement mémoire d'un service déjà supprimé.

[NSHELP-28815]

Dans une appliance NetScaler dotée d'un nombre pair de moteurs de paquets (PE), l'appliance affiche de manière incorrecte l'état des interfaces actives comme étant inactives d'un ensemble d'interfaces redondantes (canaux LR). Ce problème n'a aucune incidence sur les fonctionnalités de l'appliance NetScaler.

[NSHELP-28099]

L'appliance NetScaler peut ne pas générer de messages d' `coldStart` interruption SNMP après un redémarrage à froid.

[NSHELP-27917]

Plateforme

La commande `ntpdate` se bloque, ce qui entraîne un vidage de mémoire.

[NSHELP-29649]

SSL

Une appliance NetScaler MPX 7500 se bloque si une suite de chiffrement EXPORT est utilisée.

[NSSSL-11294]

Dans de rares cas, un plantage peut survenir pendant le traitement DTLS sur les plateformes suivantes :

- MPX 5900
- MPX/SDX 8900
- MPX/SDX 15000
- MPX/SDX 15000-50G
- MPX/SDX 26000
- MPX/SDX 26000-50S
- MPX/SDX 26000-100 G

[NSHELP-29538]

Dans une configuration haute disponibilité, le type de certificat n'est pas correctement synchronisé entre les nœuds principal et secondaire.

[NSHELP-27589]

Dans un déploiement VPN, l'appliance NetScaler récupère une session SSL pour la réutiliser depuis le cache afin de communiquer avec le serveur proxy ou principal. Pour ce faire, il ne fait pas correspondre le SNI reçu du client au SNI présent dans la session mise en cache.

Par conséquent, le SNI n'est pas envoyé ou un autre SNI est envoyé en fonction des données mises en cache.

[NSHELP-27439]

Système

Une fuite de mémoire est observée dans une appliance NetScaler lors de l'effacement de la mémoire allouée aux ressources du système de prévention des intrusions (IPS).

[NSHELP-29992]

Les opérations de configuration qui associent des profils SSL et des clés de certificat SSL à un serveur virtuel HTTP QUIC peuvent échouer lors du déploiement d'un cluster NetScaler.

[NSHELP-29655]

Une deuxième demande sur la même connexion client échoue si les conditions suivantes sont remplies :

- clientSideMeasurements est activé.
- La demande HEAD est reçue.

[NSHELP-29353]

Dans certains scénarios, une appliance NetScaler peut tomber en panne dans les conditions suivantes :

- Les trames Jumbo TCP sont utilisées.
- La persistance est configurée sur un serveur virtuel d'équilibrage de charge TCP.

[NSHELP-29162]

Une appliance NetScaler se bloque si les conditions suivantes sont remplies :

- L'option de mesures côté client est activée dans l'action AppFlow.
- Les en-têtes de segment se situent sur la limite du paquet.

[NSHELP-29049]

Une appliance NetScaler réinitialise une connexion si la taille du pipeline HTTP (une ou plusieurs requêtes) dépasse 128 Ko. Le problème se produit car la taille du pipeline est strictement limitée à 128 Ko.

[NSHELP-28846]

Un système de prévention des intrusions (IPS) NetScaler observe un problème lié à la politique de réécriture lors de l'insertion ou de la modification de données si les conditions suivantes sont remplies :

- L'appliance NetScaler envoie des paquets de données au serveur IPS avant l'ouverture de la connexion au serveur principal.

[NSHELP-28496]

Dans une configuration haute disponibilité, la synchronisation haute disponibilité des configurations de partition d'administration échoue sur le nœud secondaire pour la raison suivante :

- Problèmes de mémoire insuffisante dus à d'énormes charges de configuration sur le nœud secondaire

[NSHELP-28409]

Lorsqu'un client réinitialise une connexion avec plusieurs flux TCP, l'enregistrement de transaction côté serveur n'est pas envoyé, ce qui entraîne l'absence d'enregistrements L4 pour ces flux de données.

[NSHELP-28281]

Dans une connexion TCP, l'appliance NetScaler peut supprimer un paquet FIN, reçu d'un serveur, au lieu de le transmettre au client si toutes les conditions suivantes sont remplies :

- La mise en mémoire tampon TCP est activée.
- Le serveur envoie le paquet FIN et le paquet de données séparément.

[NSHELP-27274]

Dans une configuration en cluster, la `set ratecontrol` commande ne fonctionne qu'après le redémarrage de l'appliance NetScaler.

[NSHELP-21811]

Lorsqu'une appliance NetScaler reçoit un paquet TCP hors service avec l'indicateur FIN défini, les problèmes suivants peuvent être observés :

- L'appliance NetScaler envoie un SACK incorrect, indiquant que l'appliance a reçu un paquet TCP hors service de 2 octets au lieu d'un octet.
- L'appliance NetScaler n'accuse pas réception du paquet TCP FIN en recevant des paquets TCP dans l'ordre.

[NSBASE - 15735]

Interface utilisateur

Vous pouvez accidentellement dissocier un certificat SSL car aucune confirmation n'est demandée. Avec ce correctif, lorsque l'utilisateur clique sur un certificat lié, il demande une confirmation avant de dissocier un certificat.

[NSUI-17897]

La modification d'une règle RNAT basée sur une ACL, pour laquelle le basculement de connexion est déjà activé, à l'aide de l'interface graphique NetScaler peut échouer avec l'erreur suivante :

- `Invalid argument value [connfailover]`

[NSHELP-29243]

Lors de la configuration ou de la vérification des certificats SSL à l'aide de l'interface graphique NetScaler, l'erreur `Directory doesn't exist` peut apparaître. Ce problème se produit lorsqu'un nom de fichier comportant deux points consécutifs (`..`) existe dans le dossier **SSL**/`nsconfig`/`ssl`.

[NSHELP-28589]

Dans une configuration haute disponibilité, la synchronisation HA peut échouer pour une liaison de jeu de modèles de stratégie intégrée, si le jeu de modèles de stratégie intégré a été modifié sur le nœud principal.

[NSHELP-28460]

Lorsque vous désélectionnez l'option sécurisée pour le nœud RPC dans l'interface graphique ADC, le message d'erreur suivant s'affiche :

Prérequis pour l'argument manquant [ValidateCert, Secure==Oui]

[NSHELP-28239]

Lorsque l'utilisateur essaie de modifier la taille de page d'une liste dans les vues du panneau latéral, la page est déformée.

[NSHELP-28220]

Une barre oblique inverse supplémentaire est introduite de manière incorrecte si des caractères spéciaux sont utilisés dans les arguments de certaines commandes SSL, telles que `create ssl rsakey` et `create ssl cert`.

[NSHELP-27378]

La commande ping ou ping6 avec l'option interface (-I) peut échouer avec l'erreur suivante :

- **`interface`** `option not supported`

[NSHELP-26962]

Problèmes connus

Les problèmes qui existent dans les versions 13.1 à 17.42.

AppFlow

HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

[NSINSIGHT-943]

Authentification, autorisation et audit

Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

[NSHELP-563]

Le LoginSchema DualAuthPushOrOTP.xml ne s'affiche pas correctement dans l'écran de l'éditeur de schéma de connexion de l'interface graphique NetScaler.

[NSAUTH-6106]

Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante.
`show adfsproxyprofile <profile name>`

Solution :

Connectez-vous au principal NetScaler actif du cluster et exécutez la `show adfsproxyprofile <profile name>` commande. Il afficherait l'état du profil proxy.

[NSAUTH-5916]

La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

- L'option Tester l'accessibilité LDAP est ouverte.
- Les informations d'identification de connexion non valides sont renseignées et envoyées.
- Les identifiants de connexion valides sont renseignés et envoyés.

Solution :

Fermez et ouvrez l'option Tester l'accessibilité LDAP.

[NSAUTH-2147]

Mise en cache

Une appliance NetScaler peut se bloquer si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

[NSHELP-22942]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, si le CLAG est créé sur une carte réseau Mellanox, le MAC CLAG est modifié lorsque l'instance VPX est redémarrée. Le trafic vers l'instance VPX s'arrête après le redémarrage car la table MAC contient l'ancienne entrée MAC CLAG.

[NSSVM-4333]

NetScaler Gateway

Dans certains cas, le code de validation du serveur échoue lorsque le certificat de serveur est approuvé. Par conséquent, les utilisateurs finaux ne peuvent pas accéder à la passerelle.

[NSHELP-28942]

Dans une configuration de haute disponibilité de NetScaler Gateway, le nœud secondaire peut se bloquer si Gateway Insight est activé.

[NSHELP-28856]

L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

[NSHELP-28551]

Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

[NSHELP-28404]

Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

- Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

Solution :

Effectuez le basculement HA manuel successif uniquement après la fin de la synchronisation HA (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

Gateway Insight n'affiche pas d'informations précises sur les utilisateurs du VPN.

[NSHELP-23937]

Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

- L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
- L'appliance est configurée pour l'authentification par certificat avec une authentification à deux facteurs. `off`

[NSHELP-23584]

Parfois, lorsque vous parcourez les schémas, le message d'erreur `Cannot read property 'type 'of undefined` s'affiche.

[NSHELP-21897]

Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

[CGOP-19355]

L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

[CGOP-13621]

Le rapport Gateway Insight affiche incorrectement la valeur `Local` plutôt que `SAML` dans le champ **Type d'authentification** en cas d'échec d'erreur SAML.

[CGOP-13584]

Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

[CGOP-13511]

Lorsque vous acceptez les connexions hôtes locales depuis le navigateur, la boîte de dialogue **Accepter la connexion** pour macOS affiche du contenu en anglais, quelle que soit la langue sélectionnée.

[CGOP-13050]

Le texte de `Home Page` l' **application Citrix SSO > Page d'accueil** est tronqué pour certaines langues.

[CGOP-13049]

Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

[CGOP-11830]

Dans Outlook Web App (OWA) 2013, cliquez sur **Options** dans le menu **Paramètres** pour afficher une boîte de dialogue **d'erreur critique** . De plus, la page ne répond plus.

[CGOP-7269]

Dans un déploiement de cluster, si vous exécutez la commande `force cluster sync` sur un nœud non CCO, le fichier ns.log contient des entrées de journal en double.

[CGOP-6794]

Équilibrage de charge

Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

[NSLB-7679]

Le format ServiceGroupName dans le `entityofs` piège pour le groupe de services est le suivant : `<service(group)name>?<ip/DBS>?<port>`

Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (?) est utilisé comme séparateur. NetScaler envoie le piège avec le point d'interrogation ()?. Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Divers

Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, l'appliance exécute la commande `set urlfiltering parameter` sur le nœud secondaire.
Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre `TimeOfDayToUpdateDB`.

[NSSWG-849]

Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

[NSHELP-22409]

Réseau

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si toutes les conditions suivantes sont remplies :

- L'appliance NetScaler BLX se voit attribuer un faible nombre de. `hugepages` Par exemple, 1G.
- L'appliance NetScaler BLX est affectée à un nombre élevé de processus de travail. Par exemple, 28.

Le problème est consigné en tant que message d'erreur dans `/var/log/ns.log` :

- `BLX-DPDK:DPDK Mempool could Not be Initialized for PE-x`

Remarque : x est un nombre <= nombre de processus de travail.

Solution :

Attribuez un nombre élevé de, `hugepages` puis redémarrez l'appliance.

[NSNET-25173]

Une appliance NetScaler BLX avec DPDK peut ne pas redémarrer si les conditions suivantes sont remplies :

- L'appliance NetScaler BLX est affectée à un nombre élevé de. `hugepages` Par exemple, 16 Go.

Le problème est consigné en tant que message d'erreur dans `/var/log/ns.log` :

- `EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Too many open files`

Solution :

Utilisez l'une des solutions de contournement suivantes pour résoudre ce problème :

- Augmentez la limite de fichiers ouverts sur l'hôte Linux en utilisant la commande `ulimit` ou en modifiant le fichier `limits.conf`.
- Réduisez le nombre de `hugepages` alloués.

[NSNET-24727]

Le redémarrage d'une appliance NetScaler BLX en mode DPDK peut prendre un peu plus de temps en raison de la fonctionnalité de simplicité de DPDK.

[NSNET-24449]

Après une mise à niveau de l'appliance NetScaler BLX 13.0 61.x vers la version 13.0 64.x, les paramètres du fichier de configuration BLX sont perdus. Le fichier de configuration BLX est ensuite réinitialisé par défaut.

[NSNET-17625]

Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

- Désactiver
- Activer
- Réinitialiser

[NSNET-16559]

Sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure), une appliance NetScaler BLX est toujours déployée en mode partagé, quels que soient les paramètres du fichier de configuration BLX ().`/etc/blx/blx.conf` Ce problème se produit car `mawk`, qui est présent par défaut sur les systèmes Linux basés sur Debian, n'exécute pas certaines des commandes `awk` présentes dans le fichier `blx.conf`.

Solution :

Effectuez l'installation `gawk` avant d'installer une appliance NetScaler BLX. Vous pouvez exécuter la commande suivante dans l'interface de ligne de commande de l'hôte Linux pour effectuer l'installation de `gawk` :

- apt-get install gawk

[NSNET-14603]

L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solution :

Exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

- dpkg –add-architecture i386
- apt-get update
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

[NSHELP-21082]

Plateforme

Le basculement haute disponibilité ne fonctionne pas dans les clouds AWS et GCP. Le processeur de gestion peut atteindre 100 % de sa capacité dans les clouds AWS et GCP, ainsi que dans NetScaler VPX sur site. Ces deux problèmes sont provoqués lorsque les conditions suivantes sont remplies :

1. Lors du premier démarrage de l'appliance NetScaler, vous n'enregistrez pas le mot de passe demandé.
2. Ensuite, vous redémarrez l'appliance NetScaler.

[NSPLAT-22013]

Lorsque vous effectuez une mise à niveau d'une version 13.0/12.1/11.1 vers une version 13.1 ou que vous rétrogradez d'une version 13.1 vers une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances NetScaler. Ce problème est résolu pour les versions suivantes de NetScaler :

- 13.1-4.x
- 13.0—82.31 et versions ultérieures
- 12.1—62.21 et versions ultérieures

Les packages python ne sont pas installés lorsque vous rétrogradez les versions de NetScaler de 13.1-4.x vers l'une des versions suivantes :

- Toute version 11.1
- 12.1-62.21 et versions antérieures
- 13.0-81.x et versions antérieures

[NSPLAT-21691]

Dans une configuration de cluster sur une appliance NetScaler SDX, il existe une incompatibilité CLAG MAC sur le deuxième nœud et CLIP si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous ajoutez une autre instance VPX au cluster et à la configuration CLAG.

Par conséquent, le trafic vers l'instance VPX s'arrête.

[NSPLAT-21049]

Dans une configuration de cluster sur une appliance NetScaler SDX, le premier nœud tombe en panne en raison d'une incompatibilité d'adresses MAC entre CLIP et la table MAC, si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous supprimez le deuxième nœud du cluster.

[NSPLAT-21042]

Lorsque vous supprimez un paramètre Autoscale ou un ensemble d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande `rm cloudprofile` pour supprimer le profil.

[NSPLAT-4520]

Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran du premier utilisateur (FTU) de la configuration du profil cloud Autoscale s'affiche.
Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Configurez toujours le profil cloud sur le nœud principal.

[NSPLAT-4451]

Le basculement HA pour l'instance NetScaler VPX sur le cloud GCP et AWS échoue lorsque le mot de passe d'un nœud RPC contient un caractère spécial.

[NSHELP-28600]

Stratégies

Les connexions peuvent se bloquer si la taille des données de traitement est supérieure à la taille de tampon TCP par défaut configurée.Solution : définissez la taille du tampon TCP sur la taille maximale des données à traiter.

[NSPOLICY-1267]

SSL

Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

Solution :

1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
2. Enregistrez la configuration.

[NSSSL-9572]

Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

[NSSSL-6478]

Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

[NSSSL-6213]

Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier Key Vault comme type HSM.
ERREUR : actualisation des CRL désactivée

[NSSSL-6106]

L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

[NSSSL-4427]

Un message d'avertissement incorrect `Warning: No usable ciphers configured on the SSL vserver/service`, s'affiche si vous essayez de modifier le protocole SSL ou le chiffrement dans le profil SSL.

[NSSSL-4001]

Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

[NSSSL-3184]

Système

La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres **max_concurrent_stream du client** .

[NSHELP-21240]

Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

[NSHELP-10972]

Un problème est observé lors de la génération des rapports PCI DSS sur l'interface graphique de NetScaler (Navigation : **Système > Rapports > Générer un rapport PCI**DSS).

[NSBASE-16225]

L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

[NSBASE-8506]

L'appliance NetScaler supprime les paquets contenant des en-têtes HTTP personnalisés marqués d'un point (»). «) dans le champ du nom de l'en-tête. Cette action se produit parce que le paramètre `allowOnlyWordCharactersAndHyphen` est activé par défaut dans le profil HTTP par défaut.

Solution : désactivez cette option `allowOnlyWordCharactersAndHyphen` dans le profil HTTP par défaut. Citrix vous recommande toutefois de le laisser activé.

[NSBASE-16722]

Interface utilisateur

Pour la fonction de réécriture MQTT, vous ne pouvez pas supprimer une expression à l'aide de l'éditeur d'expression dans l'interface graphique.

Solution :

Utilisez la commande d'action add ou edit de type MQTT via l'interface de ligne de commande.

[NSUI-18049]

Dans l'interface graphique de NetScaler, le `Help` lien présent sous l' `Dashboard` onglet est rompu.

[NSUI-14752]

L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution :

Configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de la CLI de NetScaler.

[NSUI-13024]

Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

[NSUI-6838]

Le chargement et l'ajout d'un fichier de liste de révocation de certificats (CRL) échouent dans la configuration d'une partition d'administration.

[NSHELP-20988]

Lorsque vous rétrogradez la version 13.0-71.x d'une appliance NetScaler vers une version antérieure, certaines API NITRO peuvent ne pas fonctionner en raison des modifications des autorisations de fichiers.

Solution :

Modifiez l'autorisation pour `/nsconfig/ns.conf` à 644.

[NSCONFIG-4628]

Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

1. Mettez à niveau l'appliance NetScaler vers l'une des versions suivantes :
    - 13.0 52.24 build
    - 12.1 57.18 build
    - 11.1 65.10 build
2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
3. Rétrogradez l'appliance NetScaler vers une version antérieure.

Pour afficher la liste de ces utilisateurs système à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solution :

Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

1. Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
2. Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
3. Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notes de publication pour la version 13.1—12.51 de NetScaler

May 5, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1—12.51 de NetScaler.

Les versions 13.1—12.51 remplacent les builds 13.1—12.50.

Cette version inclut également un correctif pour le problème suivant : NSWAF-8668.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

Nouveautés

Améliorations et modifications disponibles dans les versions 13.1 à 12.51.

Authentification, autorisation et audit

Prise en charge des dernières versions des API NAC Intune

La prise en charge par NetScaler Gateway du contrôle d'accès réseau (NAC) d'Intune est désormais améliorée pour les dernières versions des API NAC d'Intune.

[NSAUTH-9722]

Prise en charge du déploiement actif-actif GSLB pour l'authentification nFactor à l'aide du proxy de connexion

La prise en charge est désormais ajoutée pour le déploiement actif-actif GSLB pour l'authentification nFactor à l'aide du proxy de connexion. Ce support s'applique à la fois à NetScaler Gateway et aux scénarios d'authentification, d'autorisation et d'audit.
Actuellement, si divers facteurs sont configurés dans l'authentification nFactor et si la passerelle est configurée pour GSLB, l'authentification peut être interrompue si la demande du client arrive sur différents sites GSLB.

Par exemple, si LDAP est configuré en tant que premier facteur et RADIUS en tant que deuxième facteur, l'authentification peut être interrompue dans le scénario suivant.

- Demande du client pour LDAP atterrir sur le site GSLB 1.
- La demande Radius atterrit sur le site 2 du GSLB.
  Le proxy de connexion est désormais utilisé pour acheminer la demande vers les sites GSLB appropriés afin de terminer l'authentification et de servir le trafic.

[NSAUTH-7141]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, le service de gestion interroge les instances NetScaler en arrière-plan pour des opérations telles que les certificats SSL, les fonctions réseau et l'audit de configuration. Vous pouvez désormais activer et désactiver ce sondage en fonction de vos besoins. La désactivation de ce sondage améliore les performances du service de gestion et des instances ADC.

[NSSVM-4991]

Web App Firewall NetScaler

Journalisation détaillée pour les contrôles de sécurité JSON (SQL, CMD et XSS)

L'appliance NetScaler vous permet désormais de configurer un paramètre de niveau de journal détaillé pour enregistrer les détails des violations, tels que le modèle, la charge utile du modèle et les détails de l'en-tête HTTP pour les contrôles de sécurité JSON. Les détails du journal sont ensuite envoyés au serveur NetScaler ADM à des fins de surveillance et de dépannage. Le message de consignation verbeux n'est pas stocké dans le fichier ns.log.

[NSWAF-8269]

Stratégies de journal d'audit Web App Firewall Classic obsolètes

Pour lier globalement les stratégies de Web App Firewall, un nouveau type de liaison global `APPFW_GLOBAL` est désormais configurable dans les commandes `bind audit syslogGlobal` et

`bind audit nslogGlobal`. Les stratégies de journal d'audit liées globales sont évaluées dans le contexte de journalisation du Web App Firewall.

[NSWAF-406]

Équilibrage de charge

Prise en charge des stratégies de réécriture pour le protocole MQTT

La fonction de réécriture prend désormais en charge le protocole MQTT. Vous pouvez configurer la stratégie de réécriture pour effectuer des actions en fonction des paramètres des demandes du client MQTT et des réponses du serveur.

[NSLB-8661]

Ordre de priorité pour les services

La fonction Ordre de priorité pour les services vous permet de hiérarchiser l'ordre des services ou des groupes de services en fonction des préférences de sélection de l'équilibrage de charge. Vous pouvez désormais configurer l'ordre de sélection des services lorsque vous liez les services ou les groupes de services aux serveurs virtuels LB ou GSLB. Un nouveau paramètre, -order, `<number>` est ajouté aux commandes de liaison pour configurer la préférence de sélection de service.

Par défaut, le numéro de commande le plus bas a la priorité la plus élevée. Toutefois, vous pouvez différer ce comportement de sélection par défaut. À l'aide des nouvelles commandes d'action et de stratégie LB, vous pouvez désormais configurer l'ordre de sélection des services en fonction du trafic client entrant.

La fonction d'ordre de priorité pour les services imite le comportement de la fonctionnalité de chaîne de serveurs virtuels principale et de sauvegarde avec moins de commandes de configuration.

[NSLB-8039]

Réseau

Insérez l'adresse IP du client dans l'en-tête externe du tunnel IP pour une configuration d'équilibrage de charge sans session

Dans une configuration d'équilibrage de charge sans session avec les paramètres suivants, l'appliance d'encapsulation NetScaler utilise une adresse SNIP au lieu de l'adresse IP du client comme adresse IP source dans l'en-tête externe du tunnel IP.

- Serveur virtuel d'équilibrage de charge :
- mode de redirection (m) : tunnel IP

- sans session : activé
- Paramètre global du tunnel IP :
- utiliser l'adresse IP source du client (UseClientSourceIP) : activé

Toutefois, dans certains scénarios, le désencapsulateur du tunnel (un NetScaler principal ou un serveur principal) doit connaître l'adresse IP du client.

Pour répondre à cette exigence, l'appliance d'encapsulation NetScaler utilise désormais l'adresse IP du client comme adresse IP source dans l'en-tête externe du tunnel IP.

Pour plus d'informations, consultez Configurer l'équilibrage de charge en mode DSR à l'aide d'IP sur IP.

[NSNET-21804]

Plateforme

L'image VMware ESXi démarre jusqu'à la version matérielle virtuelle 13

Lorsque vous déployez une instance NetScaler VPX à partir de l'image VMware ESXi (12.1 et versions ultérieures), par défaut, la machine virtuelle fournit la version matérielle 13.

[NSPLAT-21416]

Prise en charge des séries de contrôleurs Ethernet Intel X710 et XL710 sur Citrix Hypervisor

Vous pouvez désormais configurer une instance NetScaler VPX exécutée sur Citrix Hypervisor à l'aide de la virtualisation des E/S à racine unique (SR-IOV) avec les cartes réseau suivantes :

- Intel X710 10 Go
- Intel XL710 40 Go

[NSPLAT-21410]

Déployez une paire haute disponibilité VPX à l'aide d'adresses IP privées avec un VPC partagé AWS

Vous pouvez désormais déployer une paire haute disponibilité VPX à l'aide d'adresses IP privées sur différentes zones AWS avec des Clouds privés virtuels (VPC) partagés AWS. Le partage de VPC permet à plusieurs comptes AWS de créer leurs ressources d'application dans des VPC partagés et gérés de manière centralisée. Vous pouvez créer des instances NetScaler VPX dans AWS Shared VPC. Le VPC partagé réduit le nombre de VPC que vous créez et gérez, tout en utilisant des comptes distincts pour la facturation et le contrôle d'accès.

[NSPLAT-21401]

SSL

Nouvelle expression pour détecter les logiciels malveillants basée sur l'empreinte digitale SSL JA3

Une nouvelle expression SSL, CLIENT.SSL.JA3_FINGERPRINT, est ajoutée pour aider à identifier toute demande malveillante en comparant la demande à l'empreinte digitale JA3 configurée.

Exemple :

```
add ssl policy ja3_pol -rule "CLIENT.SSL.JA3_FINGERPRINT.EQ(bb4c15a90e93a25ddc1627439
)"-action reset
```

[NSSSL-10156]

Prise en charge de bundle de certificats dans le cluster

Les bundles de certificats sont désormais pris en charge dans une configuration de cluster.

[NSSSL-9854]

Prise en charge du bundle de certificats SSL

La fonctionnalité de bundle de certificats a été améliorée pour traiter le lot en tant qu'entité. Il n'est donc pas nécessaire de créer des fichiers pour chaque certificat intermédiaire. Deux bundles de certificats peuvent désormais partager une partie de la chaîne de certificats intermédiaires. Vous pouvez également ajouter une paire de clés de certificat à l'aide du même certificat de serveur et de la même clé qui font également partie d'un bundle de certificats. La suppression du bundle de certificats est également simplifiée.

Auparavant, l'ajout d'un bundle de certificats ajoutait plusieurs commandes dans la configuration. Vous ne pouvez pas ajouter un autre bundle de certificats si deux ensembles partageaient un certificat intermédiaire commun. La suppression était également un processus manuel.

[NSSSL-9425]

Système

Les commandes liées à l'injection html ont été supprimées dans la version 13.1. Cette modification supprime tout le code principal.

[NSBASE-14742]

Problèmes résolus

Les problèmes qui sont traités dans les versions 13.1 à 12.51.

Authentification, autorisation et audit

L'appliance NetScaler se bloque si l'OTP de messagerie est configuré.

[NSHELP-29312]

L'outil de chiffrement OTP natif n'autorise pas les caractères spéciaux dans le nom de l'appareil.

[NSHELP-28795]

Lorsque vous vous connectez à l'appliance NetScaler, un champ de mot de passe vide s'affiche lorsque les deux conditions suivantes sont remplies.

- L'authentification à deux facteurs Duo est configurée
- Le thème du portail RFWebUI est utilisé

[NSHELP-27868]

L'accès à un service est refusé si les conditions suivantes sont remplies :

- Le service est lié à un serveur virtuel d'authentification.
- L'authentification 401 est configurée sur le service et le serveur virtuel auquel le service est lié.

[NSHELP-26903]

Dans de rares cas, le nœud secondaire d'une configuration haute disponibilité peut se bloquer si la condition suivante est remplie.

- Les `aaa groups` et/ou `aaa users` sont configurés sur l'appliance NetScaler.

[NSHELP-26732]

Si le mot de passe administrateur des services LDAP, RADIUS ou TACACS contient des guillemets doubles («), l'appliance NetScaler le supprime lors de la `Test Connectivity` vérification, ce qui entraîne un échec de connexion.

[NSHELP-23630]

Appliance NetScaler SDX

Sur les plateformes NetScaler SDX 14000-40G, 15000 et 15000-50G, le réglage de la vitesse de l'interface à l'aide de l'interface de ligne de commande échoue.

[NSHELP-29388]

Lorsque vous modifiez le profil sur une instance ADC hébergée sur la plateforme NetScaler SDX, vous remarquerez peut-être des entrées supplémentaires pour la `save config` commande dans le fichier journal.

[NSHELP-29343]

Sur une appliance NetScaler SDX, un agent SNMP exécuté dans le service de gestion renvoie un code d'erreur incorrect pour les OID inexistants.

[NSHELP-29209]

Les données de la table d'événements ADC peuvent désormais être triées sur plusieurs pages si le nombre total d'enregistrements de données est inférieur à 5 000.

[NSHELP-29170]

NetScaler Gateway

L'appliance NetScaler peut se bloquer si l'EPA est configuré et qu'il n'y a pas suffisamment de mémoire disponible.

[NSHELP-28329]

Le répertoire /var/NetScaler/logon/LogonPoint/custom/ n'est pas créé après une mise à niveau si le répertoire n'était pas présent initialement.

[NSHELP-28223]

Vous pouvez voir une ligne supplémentaire pour les journaux NS_AUDITLOG_STR* dans le fichier ns_aaa_json.c.

[NSHELP-28160]

L'enregistrement DNS ne fonctionne pas une fois la connexion VPN établie.

Pour résoudre ce problème, vous devez activer le bouton nsapimgr, nsapimgr_wr.sh -ys call=toggle_vpn_configure

[NSHELP-27760]

Parfois, lors de la connexion au transfert, les sous-réseaux IP Intranet s'affichent incorrectement côté client.

[NSHELP-26904]

La latence ICA d'une session est enregistrée de manière incorrecte à 64 000 ms dans Citrix Director lorsque la latence L7 est activée. La latence L7 est activée lorsque le bouton `nsapimgr enable_ica_l7_latency` est réglé sur 1.

[NSHELP-23459]

Le fichier journal Gateway Insight est inondé du message suivant lorsque les utilisateurs se connectent à l'appliance NetScaler Gateway et accèdent aux applications ICA.

```
GwInsight: Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
 zero Oct 25 23:01:31 <local0.err> 10.217.24.1Oct 25 23:01:31 <local0.err
> 10.217.24.101 10/26/2021:06:01:31 GMT NSGWTHDR 0-PPE-0 : default SSLVPN
```



```
 Message 10491736 0 : GwInsight: Func=ns_aaa_copy_email_id_to_vpn_record
input hash_attrs_len is zero
```

[CGOP-19685]

La fonctionnalité de favoris d'entreprise du portail NetScaler Gateway prend uniquement en charge les protocoles suivants. Tous les autres signets sont bloqués. `http://`, `https://`, `rdp://` et `ftp://`.

[CGOP-19543]

Web App Firewall NetScaler

Si vous utilisez des signatures WAF, après la mise à niveau de la génération, vous devez mettre à jour toutes les signatures WAF, y compris les signatures par défaut, vers la dernière version. Réactivez ensuite les règles de signature requises.

[NSWAF-8668]

Dans certains cas, une appliance NetScaler peut se bloquer lorsque des URL d'interception sont générées automatiquement dans le système de gestion des robots.

[NSHELP-29339]

Équilibrage de charge

Le groupe de services GSLB ne peut pas gérer les mises à jour du moniteur en raison d'une valeur ENUM manquante dans les commandes ayant échoué.

[NSHELP-29050]

L'appliance NetScaler se bloque alors qu'elle tente de libérer de la mémoire allouée sur une partition différente de celle dont elle est libérée.

[NSHELP-29038]

Si un enregistrement DNS de type ZONE est disponible pour le domaine parent, la requête pour le domaine enfant avec un enregistrement NS existant génère un enregistrement SOA du domaine parent au lieu de l'enregistrement NS du domaine enfant.

[NSHELP-28793]

L'appliance NetScaler peut ne pas répondre à une requête de domaine GSLB avec l'adresse IP du service GSLB attendue, si le serveur virtuel GSLB est configuré comme suit : Type de
persistance : adresse IP source Algorithme d'équilibrage de charge : proximité statique Méthode d'équilibrage de
charge de
sauvegarde : temps aller-retour (RTT)

[NSHELP-28668]

L'état du groupe de services Autoscale basé sur le domaine d'équilibrage de charge ou GSLB reste INACTIF si vous utilisez un port générique.

[NSHELP-28548]

Le dernier message de réponse ne s'affiche pas correctement pour les moniteurs liés à des groupes de services GSLB.

[NSHELP-28393]

La valeur CookieTimeout n'est pas correctement définie pendant l'opération GET, ce qui entraîne l'échec de l'opération de mise à jour du serveur virtuel CS.

[NSHELP-27979]

Une appliance NetScaler peut échouer lors de la gestion de la sonde de surveillance pour un moniteur de type mysql, ce qui entraîne éventuellement le redémarrage du système.

[NSHELP-27953]

Divers

L'instance NetScaler CPX, exécutée sur un système Linux avec une architecture 64 bits et 1 To de stockage de fichiers, peut désormais charger des fichiers de certificat et de clé.

[NSHELP-28986]

La correspondance du modèle de jeu d'URL échoue pour les domaines standard IDNA2008.

[NSHELP-28902]

Lorsque le transfert basé sur Mac (MBF) est activé pour VXLAN, la session TCP avec état n'était pas établie.

[NSHELP-27125]

Réseau

La mise à niveau d'une appliance NetScaler dotée de partitions d'administration peut entraîner des pertes de configuration si les conditions suivantes sont remplies :

- Si la totalité de la mémoire système disponible est allouée aux partitions d'administration.

[NSNET-23031]

LIMITATIONS -

L'ID VLAN 2 est réservé pour un usage interne

L'ID VLAN 2 est réservé pour un usage interne pour les déploiements en mode pont et aucun. NetScaler CPX lie toutes les interfaces, autres que la 0/1, à l'ID VLAN 2 et le MTU (unités de transmission maximales) du VLAN ID 2 est défini comme étant égal au MTU de l'interface eth0. Si vous souhaitez configurer le VLAN et lier l'interface avec celui-ci, définissez le MTU sur le VLAN sur le MTU de l'interface tel que configuré sur Linux, si le MTU de l'interface est inférieur à 1500 octets.

[NSNET-22807]

Une appliance NetScaler BLX en mode DPDK peut se bloquer si un profil de pare-feu d'applications Web est configuré avec des contrôles de protection de sécurité avancés.

[NSNET-22654]

L'appliance NetScaler peut se bloquer lors de la création d'une sonde de surveillance pour le service associé si les conditions suivantes sont remplies :

- Profil réseau avec un ensemble d'adresses IP qui possède au moins une adresse IPv4 et aucune adresse IPv6. Le profil réseau est lié à un moniteur, qui est défini sur un service IPv6.
- Profil réseau avec un ensemble d'adresses IP qui possède au moins une adresse IPv6 et aucune adresse IPv4. Le profil réseau est lié à un moniteur, défini sur un service IPv4.

[NSHELP-29382]

Dans une appliance NetScaler, les connexions de données FTP passives peuvent être perdues suite à un échec d'allocation de mémoire.

[NSHELP-26522]

Plateforme

Les instances NetScaler VPX qui utilisent le pilote VMXNET3 peuvent se bloquer de manière aléatoire si l'instance s'exécute sur l'une des versions NetScaler suivantes :

- NetScaler 13.1 version 4.x
- NetScaler 13.1 version 9.x

[NSHELP-29120]

Stratégies

Une appliance NetScaler peut se bloquer dans les conditions suivantes :

- Une action de message d'audit est configurée avec l'expression de générateur de chaînes avec une ou plusieurs fonctions REGEX appliquées au corps d'une demande.
- Un profil de pare-feu d'application configuré avec l'option Streaming activée.

Par exemple, HTTP.REQ.BODY(10000000).REGEX_SELECT(re/name=[^\r\n]*[\r\n]+/).

[NSHELP-27895]

SSL

Une appliance NetScaler se bloque lors du traitement d'une requête HTTP si l'action de politique est définie sur `Forward` pour une politique déjà liée au point de liaison de la demande.

[NSHELP-29115]

Une appliance NetScaler se bloque si les étapes suivantes sont suivies :

1. Un moniteur de type SSL est ajouté.
2. Une paire de clés de certificat est liée au moniteur.
3. Le moniteur est retiré.
4. Un autre moniteur portant le même nom est ajouté.
5. La paire de clés de certificat est mise à jour.

[NSHELP-28666]

Toutes les adresses IP d'un certificat SAN sont désormais affichées. Auparavant, seule la dernière adresse IP SAN de toutes les adresses IP du certificat SAN était affichée.

[NSHELP-27336]

L'établissement de liaison SSL échoue si vous utilisez des chiffrements DH avec un HSM externe.

[NSHELP-25307]

Système

Lorsqu'une appliance NetScaler reçoit une trame HTTP/2 GOWAY d'un client, elle réinitialise de manière incorrecte tous les flux dont l'ID de flux est supérieur à l'ID promis (dernier identifiant de flux initié par le pair).

[NSHELP-29328]

Sur un NetScaler ADM, l'agent ADM peut signaler une utilisation élevée de la mémoire en raison d'un problème dans l'agent ADM.

[NSHELP-29285]

L'appliance NetScaler se bloque lorsque toutes les conditions suivantes sont remplies :

- Une action d'inspection de contenu, avec une adresse IP de serveur, utilise les données internes d'un service s'il est déjà configuré.
- Par conséquent, les données internes du service sont également supprimées lorsque l'action de CI est supprimée.
- Lorsque le service proprement dit est supprimé, l'appliance NetScaler tente d'accéder aux données internes déjà supprimées et de les supprimer.

[NSHELP-28293]

Dans une appliance NetScaler dotée de partitions d'administration, l' `nstrace` utilitaire peut ne pas s'exécuter correctement dans une partition autre que celle par défaut

[NSBASE-15738]

Dans une configuration de cluster, un nœud avec la priorité CCO est déconnecté d'Open vSwitch (OVS) en raison de problèmes de réseau. Une fois que le nœud a rejoint la configuration du cluster, il ne reçoit pas le dernier cookie SYN.

[NSBASE-14419]

Interface utilisateur

Les instances ADC en mode cluster configurées avec une capacité groupée tombent en panne. Ce problème se produit lorsqu'un nom d'hôte est configuré dans les nœuds du cluster et si les nœuds mettent plus de temps à se connecter au serveur de licences ADM au démarrage.

[NSHELP-28613]

L'interface graphique de NetScaler peut générer de manière incorrecte un bundle de support technique de cluster composé d'un seul nœud au lieu de tous les nœuds du cluster.

[NSHELP-28606]

La génération d'un bundle de support technique de cluster à l'aide de l'interface graphique NetScaler peut échouer avec une erreur.

[NSHELP-28586]

Dans une interface NetScaler CLI, les options permettant de lier les commandes ne sont pas automatiquement renseignées si vous appuyez sur la `<Tab>` touche tout en saisissant la commande dans l'invite de commandes.

Par exemple, tapez la commande suivante et lorsque vous utilisez la touche `<Tab>`, les objets ne sont pas remplis automatiquement.

```
bind authentication vserver <authvservername> -policy <Tab>.
```

Ici, le serveur virtuel d'authentification peut être lié à plusieurs types d'objets tels que la stratégie RADIUS, la stratégie Idappolicy, la stratégie de certificat, la stratégie TACAS, la stratégie d'authentification avancée, etc.

[NSCONFIG-6340]

Problèmes connus

Les problèmes qui existent dans les versions 13.1 à 12.51.

AppFlow

HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

[NSINSIGHT-943]

Authentification, autorisation et audit

Dans certains cas, une fuite de mémoire est observée dans un dispositif NetScaler si la fonctionnalité SSO est utilisée avec un serveur proxy.

[NSHELP-27744]

Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

[NSHELP-563]

Le LoginSchema DualAuthPushOrOTP.xml ne s'affiche pas correctement dans l'écran de l'éditeur de schéma de connexion de l'interface graphique NetScaler.

[NSAUTH-6106]

Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante.
`show adfsproxyprofile <profile name>`

Solution :

Connectez-vous au principal NetScaler actif du cluster et exécutez la `show adfsproxyprofile <profile name>` commande. Il afficherait l'état du profil proxy.

[NSAUTH-5916]

La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

- L'option Tester l'accessibilité LDAP est ouverte.
- Les informations d'identification de connexion non valides sont renseignées et envoyées.
- Les identifiants de connexion valides sont renseignés et envoyés.

Solution :

Fermez et ouvrez l'option Tester l'accessibilité LDAP.

[NSAUTH-2147]

Mise en cache

Une appliance NetScaler peut se bloquer si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

[NSHELP-22942]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, si le CLAG est créé sur une carte réseau Mellanox, le MAC CLAG est modifié lorsque l'instance VPX est redémarrée. Le trafic vers l'instance VPX s'arrête après le redémarrage car la table MAC contient l'ancienne entrée MAC CLAG.

[NSSVM-4333]

NetScaler Gateway

Dans certains cas, le code de validation du serveur échoue lorsque le certificat de serveur est approuvé. Par conséquent, les utilisateurs finaux ne peuvent pas accéder à la passerelle.

[NSHELP-28942]

Parfois, après la déconnexion du VPN, le résolveur DNS ne parvient pas à résoudre les noms d'hôtes, car les suffixes DNS sont supprimés lors de la déconnexion du VPN.

[NSHELP-28848]

L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

[NSHELP-28551]

Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

[NSHELP-28404]

Le plug-in Windows peut se bloquer pendant l'authentification.

[NSHELP-28394]

Gateway Insight n'affiche pas d'informations précises sur les utilisateurs du VPN.

[NSHELP-23937]

Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

- L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On

- L'appliance est configurée pour l'authentification par certificat avec une authentification à deux facteurs. `off`

[NSHELP-23584]

Parfois, lorsque vous parcourez les schémas, le message d'erreur `Cannot read property 'type 'of undefined` s'affiche.

[NSHELP-21897]

Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet de tirer parti des améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

[CGOP-19355]

L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

[CGOP-13621]

Le rapport Gateway Insight affiche de manière incorrecte la valeur `Local` plutôt que `SAML` dans le champ Type d'authentification en cas d'échec d'erreur SAML.

[CGOP-13584]

Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

[CGOP-13511]

Lors de l'acceptation des connexions hôtes locales depuis le navigateur, la boîte de dialogue Accepter la connexion pour macOS affiche le contenu en anglais, quelle que soit la langue sélectionnée.

[CGOP-13050]

Le texte `Home Page` de l'application Citrix SSO > Page d'accueil est tronqué dans certaines langues.

[CGOP-13049]

Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

[CGOP-11830]

Dans Outlook Web App (OWA) 2013, le fait de cliquer sur **Options** dans le menu Paramètres affiche une boîte de dialogue **Erreur critique** . De plus, la page ne répond plus.

[CGOP-7269]

Dans un déploiement de cluster, si vous exécutez la commande `force cluster sync` sur un nœud non CCO, le fichier ns.log contient des entrées de journal en double.

[CGOP-6794]

Équilibrage de charge

Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

[NSLB-7679]

Le format ServiceGroupName dans le `entityofs` piège pour le groupe de services est le suivant : `<service(group)name>?<ip/DBS>?<port>`

Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (?) est utilisé comme séparateur. NetScaler envoie le piège avec le point d'interrogation ()?. Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Divers

Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, l'appliance exécute la commande `set urlfiltering parameter` dans le nœud secondaire.
Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre `TimeOfDayToUpdateDB`.

[NSSWG-849]

Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

[NSHELP-22409]

Réseau

Après une mise à niveau de l'appliance NetScaler BLX 13.0 61.x vers la version 13.0 64.x, les paramètres du fichier de configuration BLX sont perdus. Le fichier de configuration BLX est ensuite réinitialisé par défaut.

[NSNET-17625]

Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

- Désactiver
- Activer

- Réinitialiser

[NSNET-16559]

Sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure), une appliance NetScaler BLX est toujours déployée en mode partagé, quels que soient les paramètres du fichier de configuration BLX (). `/etc/blx/blx.conf` Ce problème se produit car `mawk`, qui est présent par défaut sur les systèmes Linux basés sur Debian, n'exécute pas certaines des commandes awk présentes dans le fichier `blx.conf`.

Solution :

Effectuez l'installation `gawk` avant d'installer une appliance NetScaler BLX. Vous pouvez exécuter la commande suivante dans l'interface de ligne de commande de l'hôte Linux pour effectuer l'installation de `gawk` :

- apt-get install gawk

[NSNET-14603]

L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solution :

Exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

- dpkg –add-architecture i386
- apt-get update
- apt-get dist-upgrade
- apt-get install libc6:i386

[NSNET-14602]

Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

Dans une configuration haute disponibilité, en cas de non-correspondance de version HA entre les deux nœuds, les routes dynamiques ne sont pas synchronisées avec le nœud secondaire. Le nœud secondaire n'est pas accessible si son accessibilité dépend des itinéraires dynamiques.

En guise de solution, les routes dynamiques sont synchronisées avec le nœud secondaire même en cas de non-concordance de version HA.

[NSHELP-28326]

Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

[NSHELP-21082]

Plateforme

Le basculement haute disponibilité ne fonctionne pas dans les clouds AWS et GCP. Le processeur de gestion peut atteindre 100 % de sa capacité dans les clouds AWS et GCP, ainsi que dans NetScaler VPX sur site. Ces deux problèmes sont provoqués lorsque les conditions suivantes sont remplies :

1. Lors du premier démarrage de l'appliance NetScaler, vous n'enregistrez pas le mot de passe demandé.
2. Ensuite, vous redémarrez l'appliance NetScaler.

[NSPLAT-22013]

Lorsque vous effectuez une mise à niveau d'une version 13.0/12.1/11.1 vers une version 13.1 ou que vous rétrogradez d'une version 13.1 vers une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances NetScaler. Ce problème est résolu pour les versions suivantes de NetScaler :

- 13.1-4.x
- 13.0-82.31 et versions ultérieures
- 12.1-62.21 et versions ultérieures

Les packages python ne sont pas installés lorsque vous rétrogradez les versions de NetScaler de 13.1-4.x vers l'une des versions suivantes :

- Toute version 11.1
- 12.1-62.21 et versions antérieures
- 13.0-81.x et versions antérieures

[NSPLAT-21691]

Provisioning d'une instance VPX avec la version 12.0 XVA échoue sur une appliance NetScaler SDX exécutant la version 13.1.

Seules les versions 12.1 et ultérieures de VPX sont prises en charge. Mettez à niveau la version VPX avant de mettre à niveau le SBI vers la version 13.1.

[NSPLAT-21442]

Dans une configuration de cluster sur une appliance NetScaler SDX, il existe une incompatibilité CLAG MAC sur le deuxième nœud et CLIP si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous ajoutez une autre instance VPX au cluster et à la configuration CLAG.

Par conséquent, le trafic vers l'instance VPX s'arrête.

[NSPLAT-21049]

Dans une configuration de cluster sur une appliance NetScaler SDX, le premier nœud tombe en panne en raison d'une incompatibilité d'adresses MAC entre CLIP et la table MAC, si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous supprimez le deuxième nœud du cluster.

[NSPLAT-21042]

Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande `rm cloudprofile` pour supprimer le profil.

[NSPLAT-4520]

Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran de premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

[NSPLAT-4451]

Stratégies

Les connexions peuvent se bloquer si la taille des données de traitement est supérieure à la taille de tampon TCP par défaut configurée.Solution : définissez la taille du tampon TCP sur la taille maximale des données à traiter.

[NSPOLICY-1267]

SSL

Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

Solution :

1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
2. Enregistrez la configuration.

[NSSSL-9572]

La commande Mettre à jour n'est pas disponible pour les commandes d'ajout suivantes :

- add azure application
- add azure keyvault
- add ssl certkey with hsmkey option

[NSSSL-6484]

Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

[NSSSL-6478]

Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

[NSSSL-6213]

Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
ERREUR : actualisation des CRL désactivée

[NSSSL-6106]

L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

[NSSSL-4427]

Un message d'avertissement incorrect `Warning: No usable ciphers configured on the SSL vserver/service`, s'affiche si vous essayez de modifier le protocole SSL ou le chiffrement dans le profil SSL.

[NSSSL-4001]

Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

[NSSSL-3184]

Système

La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client.

[NSHELP-21240]

Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

[NSHELP-10972]

Lors du traitement de grands flux de trafic gRPC, la fenêtre annoncée par TCP augmente de façon exponentielle, entraînant une utilisation élevée de la mémoire.

[NSBASE-15447]

L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

[NSBASE-8506]

Interface utilisateur

Pour la fonction de réécriture MQTT, vous ne pouvez pas supprimer une expression à l'aide de l'éditeur d'expression dans l'interface graphique.

Solution :

Utilisez la commande d'action add ou edit de type MQTT via l'interface de ligne de commande.

[NSUI-18049]

Dans l'interface graphique de NetScaler, le `Help` lien présent sous l' `Dashboard` onglet est rompu.

[NSUI-14752]

L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution :

Configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de la CLI de NetScaler.

[NSUI-13024]

Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

[NSUI-6838]

Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

- Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

Solution :

Effectuez le basculement HA manuel successif uniquement après la fin de la synchronisation HA (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

Lorsque vous rétrogradez la version 13.0-71.x d'une appliance NetScaler vers une version antérieure, certaines API Nitro peuvent ne pas fonctionner en raison des modifications des autorisations de fichier.

Solution :

Modifiez l'autorisation pour `/nsconfig/ns.conf` à 644.

[NSCONFIG-4628]

Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

1. Mettez à niveau l'appliance NetScaler vers l'une des versions suivantes :

- 13.0 52.24 build
- 12.1 57.18 build
- 11.1 65.10 build

1. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
2. Rétrogradez l'appliance NetScaler vers une version antérieure.

Pour afficher la liste de ces utilisateurs système à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solution :

Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

- Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées ci-dessus), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
- Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
- Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notes de publication pour la version 13.1—9.60 de NetScaler

May 5, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1—9.60 de NetScaler.

Remarques

Ce document de notes de publication n'inclut pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

Nouveautés

Améliorations et modifications disponibles dans les versions 13.1 à 9.60.

Gestion des bots

Prise en charge du protocole IPv6 pour la réputation IP

La fonctionnalité de réputation IP du NetScaler Web App Firewall prend désormais en charge le protocole IPv6 pour la configuration des politiques et une protection de sécurité renforcée contre les adresses IP erronées qui envoient des demandes indésirables.

Les catégories de menaces suivantes sont prises en charge pour le protocole IPv6.

- Sources de spam
- Exploits Windows
- Attaques Web
- Botnets
- Scanners
- Déni de service
- Réputation
- Phishing
- Proxy
- Réseau

- Fournisseurs de cloud
- Menaces mobiles
- Proxy Tor

[NSBOT-585]

Catégories de fournisseurs de services de cloud public Webroot pour les signatures de robots

La détection des bots NetScaler basée sur la technique de réputation IP est améliorée pour détecter si un client entrant est une adresse IP de cloud public. La fonction de réputation IP doit être activée avec la configuration de la fonction de gestion des robots. L'appliance NetScaler peut utiliser les catégories de fournisseurs de services de cloud public Webroot pour valider l'adresse IP du client par rapport à la base de données d'adresses IP du fournisseur de services cloud à des fins d'évaluation des politiques.

Vous trouverez ci-dessous les types de cloud public qui peuvent être liés à un profil de bot.

- AWS
- GCP
- Azure
- Oracle
- IBM
- Salesforce

[NSBOT-50]

Appliance NetScaler SDX

Prise en charge de la restauration d'un dispositif SDX avec une licence groupée

La prise en charge de la restauration d'une appliance NetScaler SDX utilisant une licence groupée a été ajoutée. La page de licence a également été améliorée. Vous pouvez désormais ajouter et modifier des licences à partir de cette page.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/sdx/current-release/configuring-management-service/backup-restore.html%23restore-the-appliance

[NSSVM-4750]

Les utilisateurs peuvent désormais modifier les profils d'administrateur, sur une appliance NetScaler SDX, pour appliquer les nouvelles informations d'identification aux instances ADC.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/sdx/current-release/provision-netscaler-instances.html%23update-an-admin-profile

[NSSVM-4409]

Les journaux de la partition d'usine sont désormais inclus dans le bundle « techsupport » pour capturer tout historique de réinitialisation d'usine.

[NSSVM-2190]

NetScaler Gateway

Analyse EPA pour les adresses MAC sur liste blanche

Vous pouvez configurer une analyse EPA pour les adresses MAC sur liste blanche sans avoir à lister toutes les adresses IP de l'expression. Au lieu de cela, vous pouvez utiliser des jeux de motifs pour cette configuration. Avant la version 13.1 de NetScaler, toutes les adresses MAC figurant sur la liste blanche devaient être spécifiées dans le cadre d'une expression EPA.

[CGOP-17928]

Web App Firewall NetScaler

Soutien pour une protection de sécurité supplémentaire

Deux nouveaux comptoirs de relaxation sont ajoutés pour prendre en charge les contrôles de sécurité supplémentaires suivants. Les données sont utilisées pour suivre les relaxations périmées dans la configuration.

- Protection du type de contenu
- Protection contre les injections JSON Cmd

[NSWAF-6950]

Réseau

Nouvelle bande passante et licences locales basées sur des abonnements pour les appliances NetScaler BLX

Les licences locales par abonnement basées sur la bande passante suivantes sont désormais disponibles pour les appliances NetScaler BLX.

- Abonnement NetScaler VPX/BLX 10 Mbit/s Standard, Advanced, Premium Edition
- Abonnement NetScaler VPX/BLX 100 Gbit/s Standard, Advanced, Premium Edition

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc-blx/current-release/licensing-blx.html

[NSNET-21527]

Prise en charge des collecteurs métriques dans les appliances NetScaler BLX

Les appliances NetScaler BLX prennent désormais en charge la fonctionnalité NetScaler Metrics Collector.

[NSNET-15095]

Plateforme

Prise en charge des configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler sur l'hyperviseur VMware ESX

Vous pouvez désormais appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler sur l'hyperviseur VMware ESX. Ainsi, dans certains cas, une configuration spécifique ou une instance VPX est mise en place en beaucoup moins de temps.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/deploying-vpx/install-vpx-on-esx/apply-preboot-userdata-on-esx-vpx.html

[NSPLAT-21021]

Support de la mise à jour 1d de VMware ESX 7.0 sur une instance NetScaler VPX

L'instance NetScaler VPX prend désormais en charge la mise à jour 1d de VMware ESX version 7.0 (build 17551050).

[NSPLAT-19667]

Stratégies

Expression de stratégie pour renvoyer le chemin d'URL avec suffixe dépouillé

NetScaler prend désormais en charge une nouvelle expression de politique, `HTTP.REQ.URL.STRIP_SUFFIX` qui renvoie le chemin de l'URL avec le suffixe supprimé.

Exemple :

URL : /testsite/file5.html

HTTP.REQ.URL.STRIP_SUFFIX renvoie le texte sous la forme `/testsite/file5`

[NSPOLICY-825]

Système

Prise en charge de multipath TCP version 1

L'appliance NetScaler prend désormais en charge la version 1 du protocole Multipath TCP (MPTCP) en plus de la prise en charge existante de la version 0 du protocole MPTCP. La prise en charge de MPTCP version 1 est conforme à la RFC 8684.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/system/tcp-configurations.html

[NSBASE-9237]

Prise en charge du moniteur de santé gRPC

Une appliance NetScaler prend désormais en charge un moniteur de santé gRPC pour vérifier l'état de santé du serveur. Le moniteur de santé gRPC vérifie la santé globale du service gRPC ou la santé d'un service particulier.

Le protocole de vérification de l'état est implémenté en configurant les paramètres gRPC, GRPCHealthCheck, GRPCStatusCode et GRPCServiceName dans la configuration du moniteur HTTP2. Un client implémentant le protocole demande au serveur son état (sain, non sain, inconnu ou service non implémenté) et le serveur répond par un message d'état.

[NSBASE-6455]

Interface utilisateur

Licence d'enregistrement et de départ NetScaler BLX

Vous pouvez attribuer des licences aux appliances NetScaler BLX à la demande depuis NetScaler Application Delivery Management (ADM). Le logiciel ADM stocke et gère les licences, qui ont un cadre de licences qui fournit un provisionnement de licences évolutif et automatisé.

Une appliance NetScaler BLX peut récupérer la licence auprès de NetScaler ADM lorsqu'une appliance NetScaler BLX est déployée. Lorsqu'une appliance NetScaler BLX est supprimée ou détruite, elle vérifie sa licence auprès du logiciel NetScaler ADM.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc-blx/current-release/licensing-blx.html

[NSCONFIG-5777]

Utilisation des outils d'automatisation NITRO

La connexion au service NetScaler ADM capture désormais l'utilisation d'outils d'automatisation tels qu'Ansible, Terraform ou NITRO SDK.

[NSCONFIG-4515]

Problèmes résolus

Les problèmes qui sont traités dans les versions 13.1 à 9.60.

Authentification, autorisation et audit

Une appliance NetScaler peut tomber en panne si les conditions suivantes sont remplies.

1. L'appareil est soumis à une pression de mémoire.
2. La journalisation d'audit est activée et définie au niveau INFO.
3. L'authentification des utilisateurs est en cours.

[NSHELP-29053]

Si une appliance NetScaler est configurée pour l'attribut `SameSite` cookie et l'attribut Domain pour l'authentification, l'authentification échoue. Cela se produit parce que la valeur de l'attribut de `SameSite` cookie et l'attribut de domaine ne sont pas séparés par un point-virgule.

[NSHELP-28971]

Une appliance NetScaler peut tomber en panne si les conditions suivantes sont remplies.

1. L'appareil est soumis à une pression de mémoire.
2. SAML est configuré comme l'une des méthodes d'authentification.

[NSHELP-28855]

Une URL de déconnexion (`/cgi/tmlogout`) incorrecte est renvoyée lorsqu'un serveur virtuel VPN est configuré en tant que SP SAML. Le problème se produit car l'URL de déconnexion incorrecte est générée dans les métadonnées SAML.

[NSHELP-28726]

Dans certains cas, dans un environnement multicœur, un navigateur client ne parvient pas à accéder aux ressources derrière un serveur virtuel Authentification, autorisation et auditing-TM.

[NSHELP-28474]

Dans une configuration haute disponibilité de NetScaler, certaines commandes d'authentification s'affichent lors de la configuration de l'interface de ligne de commande en raison d'un problème de synchronisation.

[NSHELP-28448]

Si l'authentification unique du formulaire est activée, l'appliance NetScaler répond à une demande d'informations d'identification émanant du serveur principal en ajoutant un formulaire ainsi que l'en-tête du type de contenu. Cet ajout entraîne la duplication des en-têtes s'il en existe déjà un.

[NSHELP-28405]

L'appliance NetScaler renvoie une erreur de validation du serveur si le schéma de `DualAuthOrPush.xml` connexion est utilisé.

[NSHELP-28063]

`SameSite` les attributs des cookie ne sont pas ajoutés aux cookies d'authentification si une appliance NetScaler est configurée pour une authentification basée sur 401.

[NSHELP-27764]

Dans certains cas, un message `invalid credentials` d'erreur s'affiche pendant le processus d'authentification RADIUS. L'erreur s'affiche lorsque l'appliance NetScaler est accessible depuis un appareil client à l'aide du navigateur Google Chrome.

[NSHELP-27113]

L'appliance NetScaler peut se bloquer lors de l'extraction d'un groupe Active Directory si le nom distinctif d'un groupe extrait est NULL.

[NSHELP-26899]

Le nom de domaine SSO incorrect est renseigné pour l'utilisateur connecté si Authentication, autorisation et auditing.USER.DOMAIN est utilisé dans l'expression.

[NSHELP-26443]

Dans certains cas, une fuite NSB est observée dans une appliance NetScaler lorsque la fonctionnalité SSO est utilisée avec un serveur proxy.

[NSHELP-25492]

Mise en cache

Des informations d'en-tête supplémentaires sont envoyées dans la réponse du cache si le paramètre `insertAge` est activé dans la commande `set cache contentGroup`.

[NSHELP-27772]

Une appliance NetScaler peut se bloquer si les valeurs des `s_maxage` paramètres `Max_age` et ne sont pas définies de manière dynamique dans le bloc de contrôle du cache.

[NSHELP-27758]

Une appliance NetScaler peut tomber en panne si les conditions suivantes sont remplies :

- L'appliance propose du contenu à partir de son cache intégré.
- Le contenu mis en cache est revalidé.
- Une nouvelle demande est envoyée à ADC par un client différent pour le même objet mis en cache.

[NSHELP-22596]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, l'alarme System is not under grace est générée en continu au lieu d'une seule fois lorsque la licence SDX n'est pas en cours de période de grâce.

[NSHELP-28740]

Le service de gestion d'une appliance NetScaler SDX affiche la vitesse d'interface des gestionnaires SNMP en Kbits/Mbit/s au lieu de bits par seconde.

[NSHELP-28724]

Les chaînes communautaires des destinations d'interruptions SNMP v2 sont masquées sur une appliance NetScaler SDX.

[NSHELP-28625]

Sur une appliance NetScaler SDX, vous pouvez modifier le débit d'une instance VPX même après la période de grâce de licence groupée (30 jours).

[NSHELP-28553]

En raison d'une mise à niveau de la version Python, le chargement du SDK Python du service de gestion peut échouer en raison d'erreurs de syntaxe.

[NSHELP-27897]

Sur une appliance NetScaler SDX, la valeur par défaut pour déclencher l'alarme `Hypervisor Disk Usage High` est augmentée à 98 %.

[NSHELP-27854]

Sur une appliance NetScaler SDX, une interface faisant partie d'un canal de gestion s'affiche avec le canal de gestion si la séquence de conditions suivante est remplie :

1. L'instance VPX fait partie d'un cluster.
2. Le canal de gestion est créé.

[NSHELP-27487]

NetScaler Gateway

Les bits de licence VPN SSL ne sont pas définis pour VPX sur le marché GCP. Par conséquent, les abonnés à Marketplace ne peuvent pas utiliser le VPN SSL sur GCP.

[NSHELP-29107]

Une appliance NetScaler peut se bloquer lors du traitement du trafic UDP.

[NSHELP-28802]

L'appliance NetScaler peut se bloquer lors de la connexion au VPN si une politique AppFlow avec la règle HTTP est liée à un NetScaler Gateway.

[NSHELP-28705]

La page de connexion à NetScaler Gateway peut ne pas se charger pour les utilisateurs 3G/Tethered.

[NSHELP-28367]

Dans de rares cas, l'appliance NetScaler Gateway peut se bloquer lors du transfert de connexion lors de l'accès à une session libérée.

[NSHELP-28022]

L'appliance NetScaler se bloque lors du traitement du trafic ESP (Encapsulating Security Payload) entrant et l'association de sécurité (SA) est introuvable.

[NSHELP-27991]

Vous pouvez rencontrer des problèmes avec la connexion au transfert si SAML est configuré comme dernier facteur dans l'authentification nFactor et que l'EPA classique est également configuré.

[NSHELP-27983]

L'appliance NetScaler peut se bloquer si les deux conditions suivantes sont remplies.

- L'appliance est déployée pour le mode proxy ICA.
- La fonctionnalité Gateway Insight pour le flux ICA est activée.

[NSHELP-27982]

Dans de rares cas, la page du portail NetScaler Gateway n'affiche pas le bouton **Télécharger** du plug-in EPA sur le navigateur Internet Explorer.

[NSHELP-27849]

L'appliance NetScaler Gateway peut se bloquer si le mode asynchrone est bloqué et que vous modifiez la configuration de la politique de commutation de contenu.

[NSHELP-27570]

Une appliance NetScaler peut se bloquer lors du traitement du trafic UDP.

[NSHELP-27536]

Le fichier de signets personnels des utilisateurs ne peut pas être copié d'une appliance NetScaler Gateway vers une autre appliance.

[NSHELP-27389]

L'appliance NetScaler Gateway peut se bloquer si une option client VPN inconnue est définie dans la politique de session.

[NSHELP-27380]

Parfois, l'appliance NetScaler Gateway peut se bloquer lors de l'accès à un emplacement mémoire non valide.

[NSHELP-27343]

L'appliance NetScaler Gateway redémarre de manière inattendue en raison d'un afflux de messages de journal VPN SSL dans le fichier ns.log local lorsque Gateway Insight est activé.

[NSHELP-27040]

La localisation du portail NetScaler Gateway n'est pas compatible avec le navigateur Internet Explorer.

[NSHELP-26822]

L'interface graphique de NetScaler Gateway affiche le message `Invalid IP or Port` lors de la modification d'un profil de session VPN.

[NSHELP-26722]

La sortie `show audit messages` n'affiche pas les derniers journaux si vous modifiez le serveur Syslog dans les paramètres globaux du Syslog.

[NSHELP-19430]

Web App Firewall NetScaler

Le moteur d'apprentissage de NetScaler Web App Firewall apprend les règles de format des champs uniquement lorsqu'une violation est observée.

[NSWAF-7677]

Une appliance NetScaler peut tomber en panne si les conditions suivantes sont remplies :

- Le proxy de cookie Web App Firewall est activé.
- Le cookie de session et le cookie persistant portent le même nom.

[NSHELP-28181]

Équilibrage de charge

Si les valeurs des paramètres du moniteur utilisateur et des commandes associées au moniteur intégré comportent un espace entre le texte, la valeur du paramètre est tronquée et le texte suivant l'espace est ignoré.

Exemple :

```
add lb monitor ftp_user USER -scriptName nsftp.pl -scriptArgs `file=
    test.txt;username=NS user;password=test123` -dispatcherIP 127.0.0.1
    -dispatcherPort 3013`
<!--NeedCopy-->
```


Dans cet exemple, le nom d'utilisateur est défini sur `NS user` mais seul `NS` est envoyé et le texte qui suit est tronqué en raison de l'espace.

[NSLB-8915]

Les sites principaux et secondaires VPX se sont plantés après avoir configuré le groupe de services GSLB avec Autoscale activé.

[NSHELP-28530]

Dans une configuration HA, une appliance NetScaler perd sa connectivité car la mémoire du NSB n'est pas libérée après l'envoi de la réponse HTTP lors de la surveillance de la sonde HTTP.

[NSHELP-28466]

Parfois, dans un système multi-PE, les groupes basés sur des domaines ne reprennent pas l'état UP après quelques défaillances du système. Ce problème est dû à une situation de concurrence entre l'interface de ligne de commande et les moniteurs internes.

[NSHELP-27965]

Dans certains cas, une appliance NetScaler peut se bloquer lorsque la commande de configuration show running est émise.

[NSHELP-27815]

Dans une configuration de cluster, lorsqu'un ou plusieurs nœuds passent à `DOWN` l'état, le nœud de sauvegarde peut ne pas rejoindre le groupe de nœuds de cluster. Cet échec entraîne l'échec de certaines fonctionnalités de NetScaler.

[NSHELP-27664]

Une appliance NetScaler peut ne pas insérer d'identifiant de paquet approprié dans les réponses lorsque des demandes RADIUS en pipeline sont reçues. En raison de ce problème, le client reçoit une réponse non valide.

[NSHELP-27391]

La configuration GSLB peut être partiellement perdue si les conditions suivantes sont remplies :

- L'appliance NetScaler est redémarrée.
- Le service ADNS est configuré avec la même adresse IP que celle du site GSLB distant.

[NSHELP-26816]

Lorsqu'un grand nombre de services GSLB sont configurés sur plusieurs sites GSLB ayant une latence réseau élevée, l'état des services GSLB peut ne pas être mis à jour sur le site GSLB distant.

[NSHELP-23799]

Divers

La commande `add URLF categorization` ne parvient pas à mettre à jour la base de données, ce qui entraîne une erreur interne.

[NSSWG-1315]

L'appliance NetScaler peut se bloquer après la reprise du traitement si les conditions suivantes sont remplies :

- La fonction de proxy de transfert SSL est utilisée.
- Les informations de protocole pour une demande de proxy de transfert SSL sont reçues en plusieurs paquets asynchrones. L'appliance interrompt le traitement des paquets et le reprend après avoir reçu tous les détails du protocole pour la demande.

[NSHELP-28447]

Lorsqu'un appareil en ligne envoie un message personnalisé suivi d'une réinitialisation, l'appliance NetScaler réinitialise la connexion avant de transmettre la réponse du périphérique en ligne au client.

[NSHELP-27676]

Réseau

L'instance NetScaler VPX peut se bloquer lorsque les conditions suivantes sont remplies :

- Un grand nombre de connexions de données FTP sont présentes.
- Un basculement se produit sur l'appliance NetScaler.
- Une connexion NATPCB côté client ou serveur est effacée.

[NSHELP-27816]

Dans une configuration haute disponibilité, l'adresse SNIP activée pour le routage dynamique n'est pas exposée à VTYSH au redémarrage si la condition suivante est remplie :

- Une adresse SNIP activée pour le routage dynamique est liée au VLAN partagé dans une partition autre que celle par défaut.

Dans le cadre du correctif, l'appliance NetScaler n'autorise désormais pas la liaison d'une adresse SNIP activée par le routage dynamique au VLAN partagé dans une partition autre que celle par défaut

[NSHELP-24000]

Plateforme

L'instance NetScaler VPX dans le cloud AWS se bloque lors du redémarrage à chaud de l'appliance NetScaler.

[NSPLAT-21979]

Une instance NetScaler VPX dotée de la version logicielle 13.1 build 4.43 ne prend pas en charge la famille d'instances C5n dans le cloud AWS.

[NSPLAT-21451]

Sur l'instance NetScaler VPX sur le cloud Azure et sur le serveur Microsoft Hyper-V, dans certaines situations, des pertes de paquets de congestion peuvent se produire du côté transmission de l'interface virtuelle Hyper-V. Ces pertes de paquets peuvent bloquer les transmissions depuis l'appliance NetScaler.

[NSHELP-28375]

Sur les plateformes NetScaler MPX 5900 et MPX 8900, un numéro de plate-forme incorrect s'affiche sur l'écran LCD.

[NSHELP-28207]

L'état de la plate-forme SDX apparaît comme INCONNU dans la console LOM. Il s'agit uniquement d'un problème d'affichage et n'a aucun impact fonctionnel.

[NSHELP-20009]

Stratégies

Un NetScaler peut se bloquer si le type de service FIX est utilisé en mode couche 2 et couche 3.

[NSHELP-28468]

Une appliance NetScaler peut se bloquer si l'expression MATCHES () est utilisée dans le protocole non basé sur TCP.

[NSHELP-26062]

SSL

L'ajout d'une paire de clés de certificat peut échouer en raison d'un échec d'allocation de mémoire. Par conséquent, la recherche de la paire de clés de certificat de l'autorité de certification échoue et l'appliance se bloque.

[NSHELP-28197]

La renégociation de l'établissement de connexion SSL peut échouer sur les plateformes NetScaler MPX si des politiques asynchrones sont configurées sur le serveur virtuel SSL.

[NSHELP-27870]

L'appliance NetScaler n'accepte pas de réponse OCSP si elle ne possède pas l'en-tête HTTP correspondant à la longueur du contenu.

[NSHELP-27039]

Le nom du certificat d'autorité de certification qui a émis la CRL est tronqué à 32 caractères, même si le nom d'une clé de certificat peut comporter jusqu'à 64 caractères. Ce problème se produit car le champ CRL est limité à 32 caractères.

[NSHELP-26986]

Sur une appliance NetScaler MPX/SDX 14000 FIPS, vous pouvez constater des fuites de mémoire lorsque vous utilisez la configuration EDT avec une taille de datagramme EDT supérieure à 1 Ko.

[NSHELP-25375]

Système

Lorsqu'une instance NetScaler est enregistrée sur NetScaler ADM, des erreurs d'allocation de ports apparaissent dans les compteurs ADC.

[NSHELP-28779]

Après une mise à niveau vers NetScaler version 13.0 build 64-x et versions ultérieures, trop de journaux d'avertissement contenant un message sont reçus. `Unexpected data received from the server on probe connection for SSL_BRIDGE service type - Server.`

[NSHELP-28656]

Une appliance NetScaler exécutant la version 13.0 build 82.x et les versions ultérieures peut se bloquer si elle `ns mode pmtud` est activée et si des partitions sont utilisées.

[NSHELP-28068]

Si la taille d'en-tête reçue est supérieure à la taille maximale de la table d'en-tête, l'appliance réinitialise la taille de la table à zéro. Par conséquent, les requêtes HTTP2 échouent après quelques demandes.

[NSHELP-27977]

Le pointeur de collecteur AppFlow référencé par le profil analytique est endommagé.

[NSHELP-27924]

Si ADM a des transactions en attente dans la file d'attente, il signale aléatoirement une alerte critique en cas d'utilisation élevée de la mémoire.

[NSHELP-27913]

Le délai d'expiration TCP zombie vide les connexions serveur ou client actives en raison du délai de demi-fermeture du côté le plus rapide de la connexion.

[NSHELP-27502]

L'option TCP de chaînage des connexions est ajoutée aux connexions NetScaler RPC. Le problème entraîne un problème d'interopérabilité avec la communication des sites GSLB.

[NSHELP-27417]

Une augmentation des retransmissions de paquets est observée dans les déploiements de clusters MPTCP dans le cloud public si le jeu de liens est désactivé.

[NSHELP-27410]

Une appliance NetScaler peut envoyer un paquet TCP non valide ainsi que des options TCP telles que des blocs SACK, un horodatage et un ACK de données MPTCP sur les connexions MPTCP.

[NSHELP-27179]

Le client NSWL enregistre parfois des données à plusieurs reprises à partir du moteur de paquets (PE-0), tandis que les journaux des autres moteurs de paquets sont ignorés.

[NSHELP-27138]

Une appliance NetScaler peut tomber en panne si les conditions suivantes sont remplies :

- Lors de la gestion des enregistrements de métadonnées Logstream.
- La fonctionnalité AppFlow est activée.

[NSHELP-26942]

Une incompatibilité entre les enregistrements Logstream est observée entre l'appliance NetScaler et le chargeur de données.

[NSHELP-25796]

Interface utilisateur

Pour un serveur virtuel, lorsque vous modifiez un paramètre sous **Paramètres du trafic** dans l'interface graphique de NetScaler (version 13.1 build 4.43), le message d'erreur suivant s'affiche :

```
Invalid argument [pq]
```

[NSHELP-29492]

Le problème suivant est observé si une opération est effectuée pour lire le fichier `ns.conf`. Par exemple, `show ns saved config`.

- Le processus HTTPD peut se figer, ce qui rend l'interface graphique et l'API NITRO inaccessibles.

[NSHELP-28249]

Lorsque vous désélectionnez l'option sécurisée pour un nœud RPC dans l'interface graphique ADC, le message d'erreur suivant s'affiche :

Prérequis pour l'argument manquant [ValidateCert, Secure==Oui]

[NSHELP-28239]

Dans une configuration de cluster, les entités singleton ou globales avec deux mots de passe ou plus peuvent échouer sur un nœud au cours d'un processus de synchronisation de configuration pour la raison suivante :

- Si le premier mot de passe de la séquence est ignoré, le déchiffrement du mot de passe suivant échoue sur le nœud de synchronisation. Le déchiffrement échoue car il recherche la clé locale CCoS, qui n'est pas présente sur le nœud de synchronisation.

[NSHELP-28035]

Après la mise à niveau d'une installation haute disponibilité ou d'une configuration de cluster vers la version 13.0 build 74.14 ou ultérieure, la synchronisation de la configuration peut échouer pour la raison suivante :

- Les clés `ssh_host_rsa_key` privées et publiques ne sont pas une paire incorrecte.

[NSHELP-27834]

Dans une configuration à haute disponibilité, une appliance NetScaler peut se bloquer lors d'un processus d'authentification de l'utilisateur du système, si les conditions suivantes sont remplies :

- Le calcul du hachage du mot de passe prend plus de temps pour manquer cinq pulsations cardiaques.

[NSHELP-27066]

Les détails des statistiques du serveur d'équilibrage de charge ne sont pas alignés correctement dans le tableau de bord de l'interface graphique NetScaler.

[NSHELP-20752]

La dissociation de l'URL de limitation de débit d'un profil de bot entraîne une erreur interne de la base de données.

[NSCONFIG-6231]

L'appliance NetScaler renvoie `Zero` de manière incorrecte certains paramètres GSLB et statistiques dans les appels d'API NITRO.

[NSCONFIG-6104]

Une appliance NetScaler activée en mode couleur de la CLI affiche les messages texte de réussite de la CLI en blanc au lieu de les afficher en vert.

[NSCONFIG-5689]

Si une appliance NetScaler BLX est licenciée à l'aide de NetScaler ADM, la licence peut échouer après la mise à niveau de l'appliance vers la version 13.0 build 83.x.

[NSCONFIG-4834]

Optimisation vidéo

Une appliance NetScaler peut se bloquer en raison d'un échec d'allocation de mémoire lorsque la fonctionnalité d'optimisation vidéo est activée.

[NSHELP-28752]

Problèmes connus

Les problèmes qui existent dans les versions 13.1 à 9.60.

AppFlow

HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

[NSINSIGHT-943]

Authentification, autorisation et audit

Dans de rares cas, l'appliance NetScaler peut se bloquer en raison d'une position incorrecte du journal.

[NSHELP-29267]

L'expression Authentication, Authorization, and Auditing.User.Attribute peut donner une valeur vide dans une appliance NetScaler multicœur lorsque le mot de passe utilisateur est modifié à son expiration.

[NSHELP-28419]

Dans certains cas, une fuite de mémoire est observée dans un dispositif NetScaler si la fonctionnalité SSO est utilisée avec un serveur proxy.

[NSHELP-27744]

L'appliance NetScaler se bloque si les deux conditions suivantes sont remplies.

- L'OTP d'e-mail est configuré
- Le serveur de messagerie ne répond pas ou il y a un problème de réseau avec le serveur de messagerie

[NSHELP-26137]

Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

[NSHELP-563]

Le LoginSchema DualAuthPushOrOTP.xml ne s'affiche pas correctement dans l'écran de l'éditeur de schéma de connexion de l'interface graphique NetScaler.

[NSAUTH-6106]

Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante.
`show adfsproxyprofile <profile name>`

Solution :

Connectez-vous au principal NetScaler actif du cluster et exécutez la `show adfsproxyprofile <profile name>` commande. Il afficherait l'état du profil proxy.

[NSAUTH-5916]

La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

- L'option Tester l'accessibilité LDAP est ouverte.
- Les informations d'identification de connexion non valides sont renseignées et envoyées.
- Les identifiants de connexion valides sont renseignés et envoyés.

Solution :

Fermez et ouvrez l'option Tester l'accessibilité LDAP.

[NSAUTH-2147]

Mise en cache

Une appliance NetScaler peut se bloquer si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

[NSHELP-22942]

Call Home

L'enregistrement de CallHome peut échouer pour les appliances NetScaler MPX utilisant des licences groupées. L'enregistrement échoue car CallHome utilise un numéro de série incorrect pour enregistrer les appliances auprès du serveur de support NetScaler.

[NSHELP-28667]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, si le CLAG est créé sur une carte réseau Mellanox, le MAC CLAG est modifié lorsque l'instance VPX est redémarrée. Le trafic vers l'instance VPX s'arrête après le redémar-

rage car la table MAC contient l'ancienne entrée MAC CLAG.

[NSSVM-4333]

Sur une appliance NetScaler SDX, le service de gestion n'envoie pas de notifications syslog ni par e-mail si des pannes d'alimentation, de tension ou de disque surviennent plusieurs fois.

[NSHELP-29443]

NetScaler Gateway

Lorsque le tunnel partagé est défini sur la résolution `Reverse`, DNS pour les domaines intranet échoue.

[NSHELP-29371]

Dans une configuration haute disponibilité avec configuration TCP SYSLOG, un nœud peut se bloquer pendant le basculement HA ou lors d'une opération de réinitialisation de la configuration.

[NSHELP-29251]

Sur la page du portail NetScaler Gateway, l'icône du **lien proxy RDP** ne change pas avec le thème du portail RFWebUI.

[NSHELP-28974]

Dans certains cas, le code de validation du serveur échoue lorsque le certificat de serveur est approuvé. Par conséquent, les utilisateurs finaux ne peuvent pas accéder à la passerelle.

[NSHELP-28942]

Parfois, après la déconnexion du VPN, le résolveur DNS ne parvient pas à résoudre les noms d'hôtes, car les suffixes DNS sont supprimés lors de la déconnexion du VPN.

[NSHELP-28848]

Après la mise à niveau de l'appliance NetScaler Gateway vers la version 13.0, la configuration du proxy dans un profil de session ne fonctionne pas comme prévu. La connexion proxy est contournée pour le proxy NS non HTTP configuré.

Exemple :

```
add vpn sessionAction-proxy NS -httpProxy 192.0.2.0:24 -sslProxy 192.0.2.0:24
```

Dans cet exemple, -HttpProxy fonctionne comme prévu mais -SSLProxy ne fonctionne pas.

[NSHELP-28640]

L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

[NSHELP-28551]

Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

[NSHELP-28404]

Le plug-in Windows peut se bloquer pendant l'authentification.

[NSHELP-28394]

L'accès à StoreFront via un serveur virtuel VPN échoue si StoreFront est accessible via un serveur virtuel d'équilibrage de charge de sauvegarde.

[NSHELP-27852]

L'appliance NetScaler Gateway peut se bloquer lors de la reconnexion à une session ICA existante.

[NSHELP-27441]

Vous ne pouvez pas dissocier une stratégie d'autorisation classique à l'aide de l'interface graphique. Toutefois, vous pouvez utiliser l'interface de ligne de commande pour dissocier la stratégie d'autorisation d'authentification, d'autorisation et d'audit.

Avec ce correctif, vous pouvez désormais dissocier la stratégie d'autorisation à l'aide de l'interface graphique.

[NSHELP-27064]

L'appliance NetScaler se bloque si l'une des conditions suivantes se produit :

- L'action Syslog est configurée avec le nom de domaine et vous effacez la configuration à l'aide de l'interface graphique ou de l'interface de ligne de commande.
- La synchronisation haute disponibilité se produit sur le nœud secondaire.

Solution :

Créez une action Syslog avec l'adresse IP du serveur Syslog au lieu du nom de domaine du serveur Syslog.

[NSHELP-25944]

Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

- Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

Solution :

Effectuez le basculement HA manuel successif uniquement après la fin de la synchronisation HA (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

Gateway Insight n'affiche pas d'informations précises sur les utilisateurs du VPN.

[NSHELP-23937]

Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

- L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
- L'appliance est configurée pour l'authentification par certificat avec une authentification à deux facteurs. `off`

[NSHELP-23584]

Parfois, lorsque vous parcourez les schémas, le message d'erreur `Cannot read property 'type 'of undefined` s'affiche.

[NSHELP-21897]

Si vous souhaitez utiliser le VPN Always On avant la fonctionnalité Windows Logon, il est recommandé de passer à NetScaler Gateway 13.0 ou version ultérieure. Cela vous permet d'appliquer les améliorations supplémentaires introduites dans la version 13.0 qui ne sont pas disponibles dans la version 12.1.

[CGOP-19355]

L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

[CGOP-13621]

Le rapport Gateway Insight affiche de manière incorrecte la valeur `Local` plutôt que `SAML` dans le champ Type d'authentification en cas d'échec d'erreur SAML.

[CGOP-13584]

Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

[CGOP-13511]

Lorsque vous acceptez les connexions hôtes locales depuis le navigateur, la boîte de dialogue **Accepter la connexion** pour macOS affiche du contenu en anglais, quelle que soit la langue sélectionnée.

[CGOP-13050]

Le texte de `Home Page` l' **application Citrix SSO > Page d'accueil** est tronqué pour certaines langues.

[CGOP-13049]

Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

[CGOP-11830]

Dans Outlook Web App (OWA) 2013, cliquez sur **Options** dans le menu **Paramètres** pour afficher une boîte de dialogue **d'erreur critique** . De plus, la page ne répond plus.

[CGOP-7269]

Dans un déploiement de cluster, si vous exécutez la commande `force cluster sync` sur un nœud non CCO, le fichier ns.log contient des entrées de journal en double.

[CGOP-6794]

Web App Firewall NetScaler

L'URL de publication de l'empreinte digitale du dispositif bot peut échouer si la stratégie de gestion des bots est activée sur un serveur virtuel d'équilibrage de charge de type SSL.

[NSHELP-29198]

Une appliance NetScaler peut se bloquer si les modules suivants sont activés :

- Web App Firewall avec contrôles de sécurité avancés.
- Comté d'Appqoe.

[NSHELP-28251]

Équilibrage de charge

Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

[NSLB-7679]

La synchronisation incrémentielle échoue pour `add dns action` et les commandes `add location` dont les expressions de stratégie contiennent des caractères génériques.

[NSHELP-29301]

L'état du groupe de services affiché dans les commandes show et stat est incohérent.

[NSHELP-28931]

Si un enregistrement DNS de type ZONE est disponible pour le domaine parent, la requête pour le domaine enfant avec un enregistrement NS existant génère un enregistrement SOA du domaine parent au lieu de l'enregistrement NS du domaine enfant.

[NSHELP-28793]

Le format ServiceGroupName dans le `entityofs` piège pour le groupe de services est le suivant : `<service(group)name>?<ip/DBS>?<port>`

Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (?) est utilisé comme séparateur. NetScaler envoie le piège avec le point d'interrogation ()?. Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Divers

Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, l'appliance exécute la commande `set urlfiltering parameter` sur le nœud secondaire.
Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre `TimeOfDayToUpdateDB`.

[NSSWG-849]

L'instance NetScaler CPX, exécutée sur un système Linux avec une architecture 64 bits et 1 To de stockage de fichiers, peut désormais charger des fichiers de certificat et de clé.

[NSHELP-28986]

Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

[NSHELP-22409]

Réseau

Une appliance NetScaler peut tomber en panne si toutes les conditions suivantes sont remplies :

- Un itinéraire d'équilibrage de charge est configuré dans un domaine de trafic sur l'appliance.
- Une opération de configuration claire est effectuée sur l'appliance.

[NSNET-23847]

Après une mise à niveau de l'appliance NetScaler BLX 13.0 61.x vers la version 13.0 64.x, les paramètres du fichier de configuration BLX sont perdus. Le fichier de configuration BLX est ensuite réinitialisé par défaut.

[NSNET-17625]

Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

- Désactiver

- Activer
- Réinitialiser

[NSNET-16559]

Sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure), une appliance NetScaler BLX est toujours déployée en mode partagé, quels que soient les paramètres du fichier de configuration BLX ().`/etc/blx/blx.conf` Ce problème se produit car `mawk`, qui est présent par défaut sur les systèmes Linux basés sur Debian, n'exécute pas certaines des commandes `awk` présentes dans le fichier `blx.conf`.

Solution :

Effectuez l'installation `gawk` avant d'installer une appliance NetScaler BLX. Vous pouvez exécuter la commande suivante dans l'interface de ligne de commande de l'hôte Linux pour effectuer l'installation de `gawk` :

- apt-get install gawk

[NSNET-14603]

L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solution :

Exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :

- `dpkg --add-architecture i386`
- `apt-get update`
- `apt-get dist-upgrade`
- `apt-get install libc6:i386`

[NSNET-14602]

Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

Dans une configuration NAT44 à grande échelle, l'appliance NetScaler peut se bloquer lors de la réception du trafic SIP pour la raison suivante :

- Le module LSN ne trouve pas le service lors de la décrémentation du nombre de références ou de la suppression du service.

[NSHELP-29134]

Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

[NSHELP-21082]

Plateforme

Le basculement haute disponibilité ne fonctionne pas dans les clouds AWS et GCP. Le processeur de gestion peut atteindre 100 % de sa capacité dans les clouds AWS et GCP, ainsi que dans NetScaler VPX sur site. Ces deux problèmes sont provoqués lorsque les conditions suivantes sont remplies :

1. Lors du premier démarrage de l'appliance NetScaler, vous n'enregistrez pas le mot de passe demandé.
2. Ensuite, vous redémarrez l'appliance NetScaler.

[NSPLAT-22013]

Lorsque vous effectuez une mise à niveau d'une version 13.0/12.1/11.1 vers une version 13.1 ou que vous rétrogradez d'une version 13.1 vers une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances NetScaler. Ce problème est résolu pour les versions suivantes de NetScaler :

- 13.1-4.x
- 13.0—82.31 et versions ultérieures
- 12.1—62.21 et versions ultérieures

Les packages python ne sont pas installés lorsque vous rétrogradez les versions de NetScaler de 13.1-4.x vers l'une des versions suivantes :

- Toute version 11.1
- 12.1-62.21 et versions antérieures
- 13.0-81.x et versions antérieures

[NSPLAT-21691]

Provisioning d'une instance VPX avec la version 12.0 XVA échoue sur une appliance NetScaler SDX exécutant la version 13.1.

Seules les versions 12.1 et ultérieures de VPX sont prises en charge. Mettez à niveau la version VPX avant de mettre à niveau le SBI vers la version 13.1.

[NSPLAT-21442]

Dans une configuration de cluster sur une appliance NetScaler SDX, il existe une incompatibilité CLAG MAC sur le deuxième nœud et CLIP si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous ajoutez une autre instance VPX au cluster et à la configuration CLAG.

Par conséquent, le trafic vers l'instance VPX s'arrête.

[NSPLAT-21049]

Dans une configuration de cluster sur une appliance NetScaler SDX, le premier nœud tombe en panne en raison d'une incompatibilité d'adresses MAC dans les tables CLIP et MAC, si les conditions suivantes sont remplies :

- Le CLAG est créé sur une carte réseau Mellanox.
- Vous supprimez le deuxième nœud du cluster.

[NSPLAT-21042]

Lorsque vous supprimez un paramètre Autoscale ou un ensemble d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande `rm cloudprofile` pour supprimer le profil.

[NSPLAT-4520]

Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran du premier utilisateur (FTU) de la configuration du profil cloud Autoscale s'affiche.
Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

[NSPLAT-4451]

Les instances NetScaler VPX qui utilisent le pilote VMXNET3 peuvent se bloquer de manière aléatoire si l'instance s'exécute sur l'une des versions NetScaler suivantes :

- NetScaler 13.1 version 4.x
- NetScaler 13.1 version 9.x

[NSHELP-29120]

Stratégies

Les connexions peuvent se bloquer si la taille des données de traitement est supérieure à la taille de la mémoire tampon TCP par défaut configurée.Solution : définissez la taille de la mémoire tampon TCP sur la taille maximale des données à traiter.

[NSPOLICY-1267]

SSL

Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

Solution :

1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
2. Enregistrez la configuration.

[NSSSL-9572]

Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

[NSSSL-6478]

Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

[NSSSL-6213]

Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier KEYVAULT comme type HSM.
ERREUR : actualisation des CRL désactivée

[NSSSL-6106]

L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

[NSSSL-4427]

Un message d'avertissement incorrect `Warning: No usable ciphers configured on the SSL vserver/service`, s'affiche si vous essayez de modifier le protocole SSL ou le chiffrement dans le profil SSL.

[NSSSL-4001]

Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

[NSSSL-3184]

Dans une configuration haute disponibilité, le type de certificat n'est pas correctement synchronisé entre les nœuds principal et secondaire.

[NSHELP-27589]

Système

Lorsqu'une appliance NetScaler reçoit une trame HTTP/2 GOWAY d'un client, elle réinitialise de manière incorrecte tous les flux dont l'ID de flux est supérieur à l'ID promis (dernier identifiant de flux initié par le pair).

[NSHELP-29328]

L'en-tête X-Forwarder n'est pas ajouté à certaines demandes envoyées par l'appliance NetScaler au serveur principal.

[NSHELP-29142]

Une appliance NetScaler se bloque si les conditions suivantes sont remplies :

- L'option de mesures côté client est activée dans l'action AppFlow.
- Les en-têtes de segment se situent sur la limite du paquet.

[NSHELP-29049]

Dans une configuration haute disponibilité, la synchronisation haute disponibilité des configurations de partition d'administration échoue sur le nœud secondaire pour la raison suivante :

- Problèmes de mémoire insuffisante dus à d'énormes charges de configuration sur le nœud secondaire

[NSHELP-28409]

Dans une connexion TCP, l'appliance NetScaler peut supprimer un paquet FIN, reçu d'un serveur, au lieu de le transmettre au client si toutes les conditions suivantes sont remplies :

- La mise en mémoire tampon TCP est activée.
- Le serveur envoie le paquet FIN et le paquet de données séparément.

[NSHELP-27274]

L'échec de Pitboss se produit lors de la mise en boucle d'un grand nombre de paquets dans la file d'attente de retransmission.

[NSHELP-26071]

La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client.

[NSHELP-21240]

Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

[NSHELP-10972]

Dans une appliance NetScaler dotée de partitions d'administration, l' `nstrace` utilitaire peut ne pas s'exécuter correctement dans une partition autre que celle par défaut

[NSBASE-15738]

Lors du traitement de grands flux de trafic gRPC, la fenêtre annoncée par TCP augmente de façon exponentielle, entraînant une utilisation élevée de la mémoire.

[NSBASE-15447]

L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

[NSBASE-8506]

Interface utilisateur

Dans l'interface graphique de NetScaler, le `Help` lien présent sous l' `Dashboard` onglet est rompu.

[NSUI-14752]

L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution :

Configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de la CLI de NetScaler.

[NSUI-13024]

Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

[NSUI-6838]

Lors de la configuration ou de la vérification des certificats SSL à l'aide de l'interface graphique NetScaler, l'erreur `Directory doesn't exist` peut apparaître. Ce problème se produit lorsqu'un nom de fichier comportant deux points consécutifs (`..`) existe dans le dossier SSL `/nsconfig/ssl`.

Solution :

Supprimez ou déplacez ces fichiers du dossier `/nsconfig/ssl`.

[NSHELP-28589]

Dans une configuration haute disponibilité, la synchronisation HA peut échouer pour une liaison de jeu de modèles de stratégie intégrée, si le jeu de modèles de stratégie intégré a été modifié sur le nœud principal.

[NSHELP-28460]

Lorsque l'utilisateur essaie de modifier la taille de page d'une liste dans les vues du panneau latéral, la page est déformée.

[NSHELP-28220]

La commande Ping ou ping6 avec l'option interface (-I) peut échouer avec l'erreur suivante :

- `interface option not supported`

[NSHELP-26962]

Le chargement et l'ajout d'un fichier de liste de révocation de certificats (CRL) échouent dans la configuration d'une partition d'administration.

[NSHELP-20988]

Lorsque vous rétrogradez la version 13.0-71.x d'une appliance NetScaler vers une version antérieure, certaines API NITRO peuvent ne pas fonctionner en raison des modifications des autorisations de fichiers.

Solution :

Modifiez l'autorisation pour `/nsconfig/ns.conf` à 644.

[NSCONFIG-4628]

Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

1. Mettez à niveau l'appliance NetScaler vers l'une des versions suivantes :
   - 13.0 52.24 build
   - 12.1 57.18 build
   - 11.1 65.10 build
2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
3. Rétrogradez l'appliance NetScaler vers une version antérieure.

Pour afficher la liste de ces utilisateurs système à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solution :

Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

- Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées précédemment), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
- Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.

- Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/13/system/ns-ag-aa-intro-wrapper-con/ns-ag-aa-reset-default-amin-pass-tsk.html

[NSCONFIG-3188]

Notes de publication pour la version 13.1—4.44 de NetScaler

May 5, 2023

Ce document des notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 13.1—4.44 de NetScaler.

Remarques

- Ce document de notes de version n'inclut pas de correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.
- Les versions 21.9.1.2 et ultérieures du client Citrix Secure Access (anciennement connu sous le nom de plug-in NetScaler Gateway pour Windows) contiennent le correctif pour. https://support.citrix.com/article/CTX341455 Le plug-in NetScaler Gateway pour Windows version 21.9.1.2 est inclus dans la version 13.1—4.44 de NetScaler.
- Les versions 13.1—4.44 et ultérieures corrigent les failles de sécurité décrites dans https://support.citrix.com/article/CTX330728.
- La version 4.44 remplace la version 4.43.
- Cette version inclut également un correctif pour le problème suivant : NSHELP-29519.

Nouveautés

Les améliorations et modifications disponibles dans les versions 13.1—4.44.

Authentification, autorisation et audit

La traversée du domaine racine vers le domaine arborescente pour l'authentification SSO Kerberos est prise en charge

La traversée du domaine racine vers le domaine Tree est désormais prise en charge lors de l'authentification SSO Kerberos pour le serveur principal à partir de l'appliance NetScaler. Pour plus d'informations, veuillez consulter https://docs.citrix.com/en-us/citrix-adc/current-release/aaa-tm/single-sign-on-types/kerberos-single-sign-on/setup-citrix-adc-single-sign-on.html.

[NSAUTH-9836]

Gestion des bots

Journalisation détaillée pour la gestion des robots NetScaler

Si le trafic entrant est identifié comme étant un bot, l'appliance NetScaler vous permet désormais de configurer la fonctionnalité de journalisation détaillée du bot pour enregistrer des détails d'en-tête HTTP supplémentaires, tels que l'adresse du domaine, l'URL, l'en-tête de l'agent utilisateur et l'en-tête du cookie. Les détails du journal sont ensuite envoyés au serveur ADM à des fins de surveillance et de dépannage. Le message de consignation verbeux n'est pas stocké dans le fichier ns.log.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/bot-management/bot-detection.html

[NSBOT-273]

Appliance NetScaler SDX

Améliorations apportées à la page de formation du cluster sur une appliance NetScaler SDX

Les modifications suivantes sont apportées à l'interface graphique de la `Add Node to Cluster` page. Le système invite désormais l'utilisateur à ajouter une adresse SNIP tout en ajoutant un nouveau nœud à un cluster. Ces améliorations résolvent les problèmes de sécurité liés à la vérification stricte de l'adresse IP source.

- Un champ facultatif pour SNIP est désormais fourni.
- Un `Add` bouton est également fourni pour créer des SNIP dynamiquement tout en ajoutant un nœud à l'adresse IP du cluster (CLIP).

[NSSVM-4170]

Un administrateur NetScaler SDX peut désormais déverrouiller un utilisateur avant l'expiration de l'intervalle de verrouillage. Le verrouillage n'est pas applicable si un utilisateur se connecte au service de gestion via la console. L'intervalle de verrouillage passe également de quelques secondes à quelques minutes. Valeur minimale = 1 minute. Valeur maximale = 30 minutes.

Pour déverrouiller un utilisateur à l'aide de l'interface graphique :

1. Accédez à **Configuration > Système > Administration des utilisateurs > Utilisateurs**.
2. Sélectionnez l'utilisateur à déverrouiller.
3. Cliquez sur **Déverrouiller**.**Pour déverrouiller un utilisateur à l'aide de l'interface de ligne de commande :**

À l'invite de commande, tapez :


```
set systemuser id=`<ID>` unlock=true
<!--NeedCopy-->
```

[NSSVM-4144]

NetScaler Gateway

Nouvelles langues prises en charge

Le portail utilisateur de NetScaler Gateway est désormais disponible en russe, en coréen et en chinois (traditionnel).

[CGOP-17095]

Prise en charge de l'authentification OAuth-OpenID Connect pour Gateway Insight

NetScaler Gateway Insight signale désormais les événements liés à l'authentification OAuth-OpenID Connect (connexions utilisateur réussies et échecs).

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/analytics/gateway-insight.html

[CGOP-16907]

Web App Firewall NetScaler

Extraction d'adresses IP du client à l'aide d'une expression de stratégie avancée

L'appliance NetScaler utilise une expression de politique avancée pour extraire l'adresse IP du client à partir d'un en-tête de requête HTTP, d'un corps de requête ou d'une URL de requête. La valeur extraite est ensuite envoyée au serveur ADM pour la journalisation d'audit, les informations de sécurité et le calcul de la géolocalisation du client.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/bot-management/bot-detection.html

[NSWAF-7260]

Option d'activation pour le mécanisme de détection de BOT TPS

L'option Activer est désormais disponible pour chaque règle de détection de bot TPS dans la configuration du profil de bot. Par défaut, la valeur est ON.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/bot-management/bot-detection.html

[NSHELP-25777]

Équilibrage de charge

Prise en charge de la redirection HTTP vers HTTPS sur les serveurs virtuels de commutation de contenu

Les serveurs virtuels de commutation de contenu du type de service SSL prennent désormais en charge la redirection du trafic HTTP. Deux nouveaux paramètres : `HttpsRedirectUrl` et `RedirectFromPort` sont ajoutés à la commande `add cs vserver`. Tout le trafic HTTP arrivant sur le port spécifié dans le paramètre `RedirectFromPort` est redirigé vers l'URL spécifiée dans le paramètre `HttpsRedirectUrl`. S'il n' `HttpsRedirectUrl` est pas configuré, le trafic HTTP est redirigé vers la valeur de l'en-tête de l'hôte dans la requête HTTP entrante.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/ssl/how-to-articles/ssl-config-https-vserver-to-accept-http-traffic.html

[NSLB-8224]

Prise en charge de la synchronisation de la commande save config sur les sites GSLB distants

Vous pouvez maintenant synchroniser la commande `save ns config` sur des sites GSLB distants. Pour activer cette fonctionnalité, un nouveau paramètre `GSLBSyncSaveConfigCommand` est ajouté à la commande `set gslb parameter`. Après avoir activé l'option `GSLBSyncSaveConfigCommand`, la commande `save ns config` est traitée comme une autre commande GSLB et est synchronisée avec les sites GSLB distants. Vous devez activer l'option `AutomaticConfigSync` pour synchroniser la commande `save ns config`.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/global-server-load-balancing/synchronizing-configuration-in-gslb-setup/real-time-synchronization.html

[NSLB-7831]

Prise en charge des arguments de script sécurisés pour les moniteurs utilisateur

Un nouveau paramètre, `-secureargs`, est ajouté à la commande `add lb monitor`. Ce paramètre stocke les arguments du script dans un format chiffré au lieu d'un format de texte brut. Vous pouvez sécuriser les données sensibles liées aux scripts du moniteur utilisateur à l'aide de ce paramètre, par exemple, le nom d'utilisateur et le mot de passe. Citrix vous recommande d'utiliser un paramètre `-secureargs` au lieu du paramètre `-scriptargs` pour toutes les données sensibles liées aux scripts. Si vous choisissez d'utiliser les deux paramètres ensemble, le script spécifié dans `-scriptname` doit accepter les arguments dans l'ordre : `<scriptargs> <secureargs>`. En d'autres termes, vous devez spécifier les premiers paramètres dans `<scriptargs>` et le reste des

paramètres dans `<secureargs>` en conservant l'ordre défini pour les arguments. Les arguments sécurisés ne s'appliquent qu'au répartiteur interne.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/load-balancing/load-balancing-custom-monitors/configure-user-monitor.html

[NSLB-6314]

Réseau

Prise en charge des jeux de données de type numérique pour les ACL étendues

L'appliance NetScaler prend désormais en charge le jeu de données de type numérique pour les ACL étendues. Vous pouvez utiliser le jeu de données de type de numéro pour spécifier le port source ou le port de destination ou les deux pour une règle ACL étendue.

[NSNET-20235]

Prise en charge de RHI pour une adresse VIP liée à un IPset

Une appliance NetScaler annonce une adresse VIP liée à un IPSet en tant que route du noyau si toutes les conditions suivantes sont remplies :

- L' `host route` option est activée pour l'adresse VIP.
- L'IPSet est lié à une configuration, par exemple, des serveurs virtuels d'équilibrage de charge multi-IP.

[NSNET-20209]

Prise en charge de l'enregistrement de NetScaler CPX auprès d'ADM à l'aide de montages en volume

NetScaler CPX prend désormais en charge l'enregistrement auprès de NetScaler ADM en utilisant des montages de volumes via Kubernetes ConfigMaps et Secret. NetScaler CPX lance l'enregistrement auprès de l'agent ADM avec les détails de configuration dérivés des montages de volumes situés dans le système de fichiers de NetScaler CPX.

[NSNET-19058]

Plateforme

Support de la mise à jour 2a de VMware ESX 7.0 sur une instance NetScaler VPX

L'instance NetScaler VPX prend désormais en charge la mise à jour 2a de VMware ESX version 7.0 (build 17867351).

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/deploying-vpx/supported-hypervisors-features-limitations.html

[NSPLAT-20104]

Support du processeur AMD pour l'instance NetScaler VPX sur ESXi

L'instance NetScaler VPX de l'hyperviseur VMware ESXi prend désormais en charge les processeurs AMD. Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/deploying-vpx/install-vpx-on-esx.html

[NSPLAT-17853]

Support pour l'abonnement NetScaler VPX 5000 sur Azure Marketplace

Le plan d'abonnement NetScaler VPX 5000 est désormais pris en charge sur Azure Marketplace. Ce plan basé sur un abonnement offre les licences suivantes :

- Standard
- Advanced
- Premium

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/deploying-vpx/deploy-vpx-on-azure.html#citrix-adc-vpx-licensing

[NSPLAT-13663]

Stratégies

Prise en charge des champs d'en-tête IP dans l'expression de stratégie avancée

L'expression de stratégie avancée vous permet désormais de récupérer les champs d'en-tête suivants à partir d'un paquet IP.

- DSCP
- ECN
- TTL
- Version
- Identification
- Longueur de la tête
- Checksum d'en-tête
- Options
- Charge utile

[NSPOLICY-2441]

Suppression des fonctionnalités obsolètes à partir de la version 13.1 de NetScaler

De nombreuses fonctionnalités obsolètes sont désormais supprimées et ne sont plus configurables sur une appliance NetScaler.

Ces informations incluent :

- La fonction de filtrage (également connue sous le nom de filtrage de contenu ou CF) : actions, stratégies et liaison.
- Les fonctionnalités SPDY, Sure Connect (SC), Priority Queuing (PQ), HTTP Denial of Service (DoS) et HTML Injection.
- Stratégies classiques pour SSL, la commutation de contenu, la redirection du cache, la compression et le pare-feu d'application.
- Les paramètres `url` et `domain` dans les stratégies de commutation de contenu.
- Expressions classiques dans les règles de persistance de l'équilibrage de charge.
- Le paramètre `pattern` dans les actions de réécriture.
- Le paramètre `bypassSafetyCheck` dans les actions de réécriture.
- `SYS.EVAL_CLASSIC_EXPR` dans les expressions avancées.
- L'entité `patclass` de configuration.
- La valeur `HTTP.REQ.BODY` sans argument dans les expressions avancées.
- Préfixes Q et S dans les expressions avancées.
- Le paramètre `policyType` du paramètre cmp. (commande CLI `set cmp parameter`.)

Comme déjà documenté, vous pouvez utiliser l' `nspepi` outil pour la conversion. Vous devez exécuter l'outil sur une appliance NetScaler version 13.0 ou 12.1.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/appexpert/policies-and-expressions/introduction-to-policies-and-exp/classic-policy-deprecation-faq.html

De plus, pour utiliser la dernière version des outils afin de migrer de la configuration classique vers la configuration avancée, et des domaines de trafic vers les partitions d'administration, consultez https://github.com/citrix/ADC-scripts

[NSPOLICY-186]

Système

Afficher les statistiques du pont QUIC

La commande `stat`de pont QUIC fournit désormais un résumé détaillé des statistiques de pont QUIC.

[NSBASE-13883]

Suppression des fonctionnalités obsolètes dans NetScaler 13.1 et versions ultérieures

Les fonctionnalités obsolètes suivantes et leurs configurations ne sont plus prises en charge et sont supprimées de l'appliance NetScaler :

- SureConnect (SC)
- Queueing prioritaire (PQ)
- Protection DoS HTTP (HDOSP)
- `HTMLInjection`

Comme alternative, Citrix vous recommande d'utiliser AppQoE pour SureConnect, Priority Queueing et HTTP DoS Protection et d'utiliser des mesures côté client pour `HTMLInjection`.

Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-adc/current-release/appexpert/policies-and-expressions/introduction-to-policies-and-exp/classic-policy-deprecation-faq.html

[NSBASE 13780]

Interface utilisateur

Prise en charge de l'API par lots pour les appels NITRO

L'appliance NetScaler prend désormais en charge `batchapi` l'API. L' `batchapi` API peut gérer plusieurs appels NITRO en une seule demande et ainsi minimiser le trafic réseau. Vous pouvez effectuer les opérations suivantes à l'aide de la commande `batchapi` :

- Vous pouvez utiliser l'API par lots pour créer, mettre à jour et supprimer simultanément plusieurs ressources hétérogènes.
- Vous pouvez utiliser l'API par lots pour obtenir plusieurs ressources hétérogènes.

[NSCONFIG-4061]

Problèmes résolus

Les problèmes qui sont résolus dans la version 13.1—4.44.

Authentification, autorisation et audit

Lorsque vous liez un moniteur LDAP à un service, le moniteur tombe en panne car l'appliance NetScaler envoie un mot de passe incorrect à Active Directory.

[NSHELP-27961]

Dans un AD à cascade multiple, le compte d'un utilisateur n'est pas verrouillé si un utilisateur n'est pas trouvé dans la dernière cascade.

[NSHELP-27948]

Lorsqu'une appliance NetScaler est configurée pour l'authentification SAML, elle vide le cœur lors de l'utilisation d'un certificat autre que RSA.

[NSHELP-27813]

Dans certains cas, une appliance NetScaler peut se bloquer lors du traitement de la demande d'authentification de certains utilisateurs lorsque l'accès basé sur les rôles est configuré.

[NSHELP-27655]

Les utilisateurs ne peuvent pas se connecter via l'application Citrix Workspace si Azure AD est configuré en tant qu'IdP OAuth sur le serveur virtuel d'authentification NetScaler.

[NSHELP-27462]

Dans certains cas, l'authentification SAML échoue avec l'application Workspace si l'on accède à l'application via StoreFront.

[NSHELP-27338]

Dans certains cas, une requête HTTP POST envoyée à un serveur virtuel Authentication, Authorization and Auditing-TM n'est pas traitée correctement si la demande ne contient pas de cookie d'authentification. Le corps POST est perdu pendant le traitement.

[NSHELP-27227]

L'appliance NetScaler se bloque fréquemment lors du traitement de l'authentification, de l'autorisation et de l'Auditing-TM et du trafic basé sur 401 LB.

[NSHELP-27094]

Dans certains cas, une appliance NetScaler se bloque lors de l'authentification des utilisateurs pour NetScaler Gateway et du déploiement d'authentification, d'autorisation et d'audit (gestion du trafic).

[NSHELP-26555]

En cas de saisie d'un OTP incorrect, un message d'erreur `Email Auth failed. No further action to` **`continue`** s'affiche.

[NSHELP-26400]

Dans certains scénarios, la commande de groupe d'authentification, d'autorisation et d'audit de liaison peut échouer si le nom de la stratégie est plus long que le nom de l'application intranet.

[NSHELP-25971]

Une appliance NetScaler configurée en tant que fournisseur d'identité SAML (IdP) tronque l'état du relais fourni par le fournisseur de services (SP) s'il contient des guillemets.

[NSHELP-20131]

La vérification du test de connectivité réseau échoue en raison d'un problème de déchiffrement du mot de passe. Toutefois, la fonctionnalité d'authentification fonctionne correctement.

[NSAUTH-10216]

Gestion des bots

Dans le mécanisme de détection de robot Transaction Per Second (TPS), le serveur d'applications principal renvoie une réponse 304 lors de la récupération de réponse après le défi CAPTCHA.

[NSBOT-626]

Mise en cache

Dans une configuration haute disponibilité, la synchronisation HA échoue pour le paramètre de cache `memLimit` lors d'un basculement HA.

[NSHELP-28428]

Dans une configuration haute disponibilité, le nœud principal se bloque après avoir accédé à un pointeur NULL au lieu d'un objet mis en cache.

[NSHELP-26967]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, la restauration de l'instance peut échouer si l'instance a été créée avec la version logicielle 13.0-76.x ou antérieure.

[NSHELP-28429]

Dans une appliance NetScaler SDX, le service de gestion signale une utilisation incorrecte des données des instances ADC.

[NSHELP-28208]

Sur une appliance NetScaler SDX, vous ne pouvez pas modifier l'invite CLI dans la console du service de gestion.

[NSHELP-28030]

Sur une appliance NetScaler SDX, le service de gestion peut signaler une utilisation élevée de la mémoire d'environ 80 % en raison de l'augmentation du nombre de tâches et de planificateurs exécutés dans l'inventaire.

[NSHELP-27805]

Sur une appliance NetScaler SDX, la mise à niveau peut échouer si les fichiers système (snmpd.conf et ntp.conf) contiennent des caractères de retour.

[NSHELP-27713]

Sur une appliance NetScaler SDX, le service de gestion peut signaler une utilisation élevée de la mémoire d'environ 80 % en raison de l'augmentation du nombre de tâches et de planificateurs exécutés dans l'inventaire.

[NSHELP-27396]

NetScaler Gateway

Les utilisateurs peuvent observer un échec de lancement de session RDP lors d'une mise à niveau vers la dernière version.

[NSHELP-29519]

Un message d'erreur apparaît lorsque vous tentez de modifier les attributs CSS d'un thème personnalisé.

[NSHELP-28648]

L'ouverture de session à Citrix Workspace échoue si les stratégies de répondeur qui peuvent passer à un état bloqué pendant l'évaluation sont liées au serveur virtuel.

[NSHELP-27819]

Lors de l'accès à l'appliance NetScaler Gateway à l'aide du VPN sans client, un core dump peut être généré.

[NSHELP-27653]

L'appliance NetScaler Gateway peut se bloquer lors du traitement du trafic UDP initié par le serveur.

[NSHELP-27611]

Les utilisateurs peuvent voir les boîtes aux lettres des autres utilisateurs lorsqu'ils se connectent à Microsoft Outlook. Pour contourner ce problème, désactivez le multiplexage.

[NSHELP-27538]

Une appliance NetScaler peut se bloquer si les commandes liées à EDT, telles que `clearconfigkill ica connection`, ou `stop dtls listener` sont traitées par l'appliance.

[NSHELP-27398]

L'appliance NetScaler Gateway peut se bloquer lors du traitement du trafic UDP.

[NSHELP-27317]

L'appliance NetScaler Gateway se bloque lorsqu'une politique syslog est liée à un serveur virtuel et que l'action syslog correspondante est modifiée.

[NSHELP-27171]

Les journaux NetScaler peuvent être inondés de messages de journal `GwInsight: Func=ns_sslvpn_send_app_launch_fail_record Appflow policy evaluation has failed` lorsque Gateway Insight est activé.

[NSHELP-26750]

L'appliance NetScaler Gateway se bloque lorsque vous essayez d'effacer la configuration si les deux conditions suivantes sont remplies :

- Un profil SSL et une paire de clés de certificat sont liés au moniteur TCP par défaut.
- Le même moniteur TCP par défaut est lié à une action Syslog.

[NSHELP-26685]

Lorsque vous entrez le FQDN en tant que proxy sur la page Créer un profil de trafic NetScaler Gateway, le message s'affiche. `Invalid Proxy Value`

[NSHELP-26613]

Lors de la création d'un profil client RDP à l'aide de l'interface graphique NetScaler, un message d'erreur s'affiche lorsque les conditions suivantes sont remplies :

- Une clé pré-partagée (PSK) par défaut est configurée.
- Vous essayez de modifier le minuteur de validité du cookie RDP dans le champ Validité du cookie RDP (secondes).

[NSHELP-25694]

L'OID SNMP envoie un ensemble incorrect de connexions actuelles au serveur virtuel VPN.

[NSHELP-25596]

L'appliance CITRIX ADC se bloque lorsque plusieurs clients de plug-in VPN utilisent des certificats X.509 d'une taille de 1 800 octets ou plus pour configurer un tunnel.

[NSHELP-25195]

Si vous renommez un serveur virtuel VPN lié à un serveur STA, l'état du serveur STA apparaît en panne lorsque vous exécutez la commande show.

[NSHELP-24714]

Dans de rares cas, l'appliance NetScaler Gateway peut se bloquer si l'adresse IP de l'intranet (IIP) est activée et si des connexions initiées par le serveur vers l'adresse IIP sont établies.

[NSHELP-23819]

La sortie de la commande `show tunnel global` inclut des noms de stratégie avancés. Auparavant, la sortie n'affichait pas les noms de stratégie avancés.

Exemple :

Nouvelle sortie :


```
> show tunnel global
Policy Name: ns_tunnel_nocmp Priority: 0

Policy Name: ns_adv_tunnel_nocmp Type: Advanced policy
Priority: 1
Global bindpoint: REQ_DEFAULT

Policy Name: ns_adv_tunnel_msdocs Type: Advanced policy
Priority: 100
Global bindpoint: RES_DEFAULT
Done
>
<!--NeedCopy-->
```

Sortie précédente :

```
> show tunnel global
Policy Name: ns_tunnel_nocmp Priority: 0 Disabled

Advanced Policies:

Global bindpoint: REQ_DEFAULT
Number of bound policies: 1

Done
<!--NeedCopy-->
```

[NSHELP-23496]

Si vous avez configuré la gestion des comptes RADIUS pour l'événement de démarrage/arrêt ICA, l'ID de session dans la demande de gestion de compte RADIUS pour le démarrage ICA est affiché sous la forme de zéro.

[NSHELP-22576]

Web App Firewall NetScaler

Dans une configuration de cluster NetScaler, l'un des nœuds se bloque si un ou plusieurs nœuds sont mis à niveau à partir de NetScaler version 12.0, 12.1 ou 13.0 build 52.x ou de versions antérieures. Le blocage se produit en raison d'une incompatibilité du format et de la taille des cookie du Web App Firewall.

[NSWAF-7689]

Dans Web App Firewall, le paramètre `Cookie-transformation` fractionne les valeurs du cookie côté réponse s'il a une virgule comme délimiteur.

[NSHELP-28411]

Une appliance NetScaler peut se bloquer si des violations d'injection de commandes sont observées dans un ordre spécifique et si les conditions suivantes sont remplies :

- Plusieurs cookies sont présents dans la demande
- `URLDecodeRequestCookies` la fonctionnalité est désactivée

[NSHELP-28365]

Une appliance NetScaler peut afficher une utilisation élevée de la mémoire lors de l'analyse des réponses HTTP pour lesquelles l'attribut Samesite et la fonctionnalité Web Application Firewall sont activés.

[NSHELP-27722]

La fonctionnalité de piratage de cookie ne prend pas en charge le navigateur Internet Explorer car les navigateurs Internet Explorer ne réutilisent pas les connexions SSL. En raison de cette limitation, plusieurs redirections sont envoyées pour une demande entraînant éventuellement une `MAX REDIRECTS EXCEEDED` erreur dans le navigateur Internet Explorer.

[NSHELP-27193]

Après une mise à niveau vers NetScaler version 13.0 build 76.29 et lorsque la fonctionnalité de téléchargement de fichiers est activée sur l'appliance, le problème suivant est observé :

- Les contrôles de protection par script SQL et intersite bloquent le processus de téléchargement de fichiers pour toutes les applications Web.

[NSHELP-27140]

Équilibrage de charge

Dans une configuration GSLB, l'état des services distants n'est pas mis à jour une fois les statistiques effacées sur le site GSLB. Pour contourner le problème, effacez à nouveau les statistiques sur le même site GSLB. L'état des services distants est ensuite mis à jour.

[NSHELP-28169]

Dans une configuration haute disponibilité, le nœud secondaire peut se bloquer si les conditions suivantes sont remplies :

- La quantité de mémoire physique sur les deux nœuds est différente l'une de l'autre.
- Les sessions de données ne sont pas correctement synchronisées.

[NSHELP-26503]

Dans une configuration de cluster, l'adresse IP du service GSLB n'est pas affichée dans l'interface graphique lorsqu'on y accède via des liaisons de serveur virtuel GSLB. Il ne s'agit que d'un problème d'affichage et il n'y a aucun impact sur la fonctionnalité.

[NSHELP-20406]

Divers

Une appliance NetScaler ajoute des informations L2 supplémentaires lorsqu'un tunnel ou des serveurs virtuels de type de service (TOS) sont créés.

[NSHELP-27825]

Réseau

Après la mise à niveau d'une appliance NetScaler BLX (version 13.0 build 82.x) exécutée sur un hôte Linux basé sur Debian, SSH ne fonctionne pas comme prévu en mode partagé.

[NSNET-23020]

Après la mise à niveau d'une appliance NetScaler BLX vers la version 13.1 build 4.x, le pare-feu de l'application Web peut bloquer de manière incorrecte une demande ne comportant aucun en-tête de type de contenu.

[NSNET-21415]

Dans une appliance NetScaler BLX, le NSVLAN lié à des non-dpdk interfaces balisées peut ne pas fonctionner comme prévu. NSVLAN lié avec des non-dpdk interfaces non balisées fonctionne correctement.

[NSNET-18586]

Dans une appliance NetScaler, la couche de pilote interne peut utiliser une mémoire tampon de données incorrecte, ce qui entraîne une corruption des données, ce qui entraîne à son tour le blocage de l'appliance.

[NSHELP-27858]

Problème résolu :

NetScaler CPX déployé en tant que sidecar et connecté à plusieurs réseaux n'a pas pu choisir l'adresse IP source correcte pour le sous-réseau de destination.

[NSHELP-27810]

Dans une configuration haute disponibilité, la synchronisation HA peut échouer pour les configurations de profil WAF et de fichier d'emplacement.

[NSHELP-27546]

Les boucles de paquets sont observées dans une configuration d'équilibrage de charge si toutes les conditions suivantes sont remplies :

- Le serveur virtuel est configuré pour écouter sur le port 80 et le paramètre de basculement de connexion (`connfailover`) est défini sur stateless.
- Le serveur virtuel reçoit deux paquets de demandes qui ont :
  - Port source = 80
  - Port de destination = numéro autre que 80
  - Adresse IP de destination = adresse IP (VIP) du serveur virtuel

[NSHELP-22431]

Plateforme

`Failed to create target instance` un message d'erreur s'affiche sur la console GCP même si vous ne créez aucune instance cible. Ce problème se produit lorsque vous ne disposez pas de l'autorisation `compute.targetInstances.get` IAM dans votre compte de service GCP. À partir de cette version, NetScaler VPX crée des instances cibles uniquement pour les machines virtuelles qui utilisent la fonctionnalité VIP Scaling.

[NSPLAT-20952]

L'appliance NetScaler génère des alertes de limite de débit de faux paquets par seconde (PPS) avant même que l'appliance NetScaler n'atteigne sa limite de PPS pour la licence.

[NSHELP-26935]

Stratégies

La variable NS avec une portée globale ne fonctionne pas pour le trafic HTTP/2.

[NSHELP-27095]

SSL

Dans une configuration de cluster, lorsque deux certificats installés sont les émetteurs d'un certificat de serveur doté de l'extension OCSP AIA, l'appliance devient inaccessible si vous supprimez le certificat de serveur.

[NSHELP-28058]

Dans une configuration haute disponibilité, l'actualisation automatique des LCR échoue par intermittence si les deux conditions suivantes sont remplies :

- Les fichiers sont synchronisés entre le nœud principal et le nœud secondaire.

- Le fichier CRL est en cours de téléchargement à partir du serveur CRL en même temps.

[NSHELP-27435]

Sur une appliance NetScaler, une fausse notification d'expiration de certificat est enregistrée le jour suivant lorsqu'une paire de clés de certificat est ajoutée avec -ExpiryMonitor activé.

[NSHELP-27348]

Dans une base de données de cluster, la liaison n'est pas mise à jour correctement si vous liez une stratégie SSL à un serveur virtuel au point de liaison Hello du client plusieurs fois et avec des priorités différentes. Par conséquent, une erreur apparaît lorsque vous supprimez la stratégie, même après la dissolution de la liaison du serveur virtuel.

[NSHELP-27301]

L'appliance NetScaler se bloque lors du redémarrage si vous modifiez le nom du certificat intégré (`ns-server-certificate`) dans le fichier de configuration.

[NSHELP-26858]

Dans une configuration de cluster, vous pouvez rencontrer les problèmes suivants :

- Commande manquante pour la liaison de la paire de clés de certificat par défaut aux services internes SSL sur le CLIP. Toutefois, si vous effectuez une mise à niveau à partir d'une version antérieure, vous devrez peut-être lier la paire de clés de certificat par défaut aux services internes SSL concernés sur le CLIP.
- Différence de configuration entre le CLIP et les nœuds de la commande set par défaut pour les services internes.
- Commande de liaison de chiffrement par défaut manquante aux entités SSL dans la sortie de la commande show running config exécutée sur un nœud. L'omission n'est qu'un problème d'affichage et n'a aucun impact fonctionnel. La liaison peut être visualisée à l'aide de la commande `show ssl <entity> <name>`.

[NSHELP-25764]

Système

Une appliance NetScaler peut se bloquer avec une réponse ICAP OPTIONS. Le problème se produit lorsque la valeur d'en-tête autorisée contient une valeur autre que 204.

[NSHELP-27879]

Dans AppFlow, le nombre d'octets de couche 4 pour les enregistrements de flux ne correspond pas aux transactions du serveur virtuel HTTP. La valeur de comptage est inférieure à la valeur du nombre d'octets du serveur virtuel de couche 7.

[NSHELP-27495]

Le compteur TCPCurClientConn affiche une valeur élevée si l'appliance NetScaler est enregistrée sur NetScaler ADM.

[NSHELP-27463]

Une appliance NetScaler peut se bloquer lorsque la fonctionnalité AppFlow est désactivée puis réactivée.

[NSHELP-27236]

Dans de rares cas, une appliance NetScaler peut envoyer des numéros de séquence TCP SACK incorrects au client lors du transfert depuis le serveur principal. Le problème se produit si l'option TCP Selective ACK (SACK) est activée dans un profil TCP.

[NSHELP-24875]

Une appliance NetScaler peut se bloquer lorsqu'une politique contenant l' `HTTP.REQ.*` expression est liée au point de liaison RESPONSE du serveur `HTTP_QUIC` virtuel. Le problème ne se produit pas si vous liez la même stratégie à un serveur virtuel de type HTTP ou SSL avec un serveur `HTTP_QUIC` virtuel.

[NSBASE-14612]

Interface utilisateur

Dans l'interface graphique du Gestionnaire de stratégies de compression, impossible de lier une stratégie de compression à un protocole HTTP en spécifiant un point de liaison et un type de connexion appropriés.

[NSUI-17682]

Lorsque vous récupérez le contenu d'un fichier à partir d'une instance ADC à l'aide de la commande `show systemfile`, un message d'erreur d'échec de téléchargement apparaît sur la console ADC. Le problème se produit si le contenu du fichier commence par des octets NULL.

[NSHELP-28227]

Le flot `admautoregd` SYSLOG entraîne une mauvaise classification et un mauvais diagnostic de la définition des ressources client
(CRD) en raison d'un problème système interne (fichier binaire Python manquant).

Correction : pour arrêter de surveiller le `admautoregd` processus après 30 minutes si le binaire python est toujours manquant.

[NSHELP-28185]

Il peut y avoir une perte de configuration si une instance VPX sur AWS, configurée avec KEK est mise à niveau vers NetScaler version 13.0 build 76.x ou ultérieure. Toutes les données sensibles chiffrées à l'aide de KEK échouent si la configuration est chargée après un redémarrage.

[NSHELP-28010]

Une barre oblique inverse supplémentaire est incorrectement introduite si des caractères spéciaux sont utilisés dans les arguments de certaines commandes SSL, telles que `create ssl rsakey` et `create ssl cert`.

[NSHELP-27378]

Dans une configuration haute disponibilité, la synchronisation HA ou la propagation HA peut échouer si l'une des conditions suivantes est remplie :

- Le mot de passe du nœud RPC comporte des caractères spéciaux.
- Le mot de passe du nœud RPC comporte 127 caractères (nombre maximal de caractères autorisés).

[NSHELP-27375]

L'outil `nsconfigaudit` peut se bloquer si la taille du fichier de configuration d'entrée est très importante.

[NSHELP-27263]

Vous ne pouvez pas lier un service ou un groupe de services à un serveur virtuel d'équilibrage de charge prioritaire à l'aide de l'interface graphique NetScaler.

[NSHELP-27252]

La fonctionnalité de création de rapports peut cesser de fonctionner si l'horloge système est mise à jour sur une appliance NetScaler.

[NSHELP-25435]

Dans une appliance NetScaler VPX, une opération de capacité définie peut échouer après l'ajout d'un serveur de licences. Le problème se produit car les composants liés à Flexera prennent plus de temps à initialiser en raison du grand nombre de licences prises en charge de type check-in and check-out (CICO)

[NSHELP-23310]

L'appel GET de l'API `botprofile_logexpression_binding` NITRO ne renvoie aucune réponse si l'expression de journal est liée à un profil de bot.

[NSCONFIG-5490]

Dans une configuration de cluster, lorsque vous liez un profil Web App Firewall avec des règles affinées, puis avec des `non-fine-graned` règles à la même URL, les règles affinées sont supprimées de la base de données. Par conséquent, seules les règles non affinées sont affichées sur l'adresse IP du cluster.

[NSCONFIG-5389]

Problèmes connus

Les problèmes qui existent dans les versions 13,1-4.44.

AppFlow

HDX Insight ne signale pas d'échec du lancement d'une application provoqué par un utilisateur qui tente de lancer une application ou un bureau auquel l'utilisateur n'a pas accès.

[NSINSIGHT-943]

Authentification, autorisation et audit

Une URL de déconnexion (`/cgi/tmlogout`) incorrecte est renvoyée lorsqu'un serveur virtuel VPN est configuré en tant que SP SAML. Le problème se produit car l'URL de déconnexion incorrecte est générée dans les métadonnées SAML.

[NSHELP-28726]

Dans certains cas, une fuite de mémoire est observée dans un dispositif NetScaler si la fonctionnalité SSO est utilisée avec un serveur proxy.

[NSHELP-27744]

Dans de rares cas, le nœud secondaire d'une configuration haute disponibilité peut se bloquer si la condition suivante est remplie.

- Le `aaa groupsaaa users` ou les deux sont configurés sur l'appliance NetScaler.

[NSHELP-26732]

Une appliance NetScaler n'authentifie pas les tentatives de connexion par mot de passe dupliqué et empêche le verrouillage des comptes.

[NSHELP-563]

Le LoginSchema DualAuthPushOrOTP.xml ne s'affiche pas correctement dans l'écran de l'éditeur de schéma de connexion de l'interface graphique NetScaler.

[NSAUTH-6106]

Le profil proxy ADFS peut être configuré dans un déploiement de cluster. L'état d'un profil proxy est affiché de manière incorrecte comme vide lors de l'exécution de la commande suivante.
`show adfsproxyprofile <profile name>`

Solution :

Connectez-vous au principal NetScaler actif du cluster et exécutez la `show adfsproxyprofile <profile name>` commande. Il afficherait l'état du profil proxy.

[NSAUTH-5916]

La page Configurer le serveur LDAP d'authentification sur l'interface graphique de NetScaler ne répond plus si vous suivez les étapes suivantes :

- L'option Tester l'accessibilité LDAP est ouverte.
- Les informations d'identification de connexion non valides sont renseignées et envoyées.
- Les identifiants de connexion valides sont renseignés et envoyés.

Solution :

Fermez et ouvrez l'option Tester l'accessibilité LDAP.

[NSAUTH-2147]

Mise en cache

Une appliance NetScaler peut se bloquer si la fonctionnalité de mise en cache intégrée est activée et que la mémoire de l'appliance est insuffisante.

[NSHELP-22942]

Appliance NetScaler SDX

Sur une appliance NetScaler SDX, la création d'une instance ADC à l'aide d'une image XVA de la version logicielle 12.0 échoue. Par conséquent, l'instance est inaccessible.

[NSHELP-28408]

NetScaler Gateway

Parfois, après la déconnexion du VPN, le résolveur DNS ne parvient pas à résoudre les noms d'hôtes, car les suffixes DNS sont supprimés lors de la déconnexion du VPN.

[NSHELP-28848]

Après la mise à niveau de l'appliance NetScaler Gateway vers la version 13.0, la configuration du proxy dans le profil de session ne fonctionne pas comme prévu. La connexion proxy est contournée pour le proxy NS non HTTP configuré.

Exemple :
add vpn sessionAction -proxy NS -httpProxy 192.0.2.0:24 -sslProxy 192.0.2.0:24

Dans cet exemple, -HttpProxy fonctionne comme prévu mais -SSLProxy ne fonctionne pas.

[NSHELP-28640]

L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.

[NSHELP-28551]

Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

[NSHELP-28404]

Le plug-in Windows peut se bloquer pendant l'authentification.

[NSHELP-28394]

L'appliance NetScaler se bloque si l'une des conditions suivantes se produit :

- L'action Syslog est configurée avec le nom de domaine et vous effacez la configuration à l'aide de l'interface graphique ou de l'interface de ligne de commande.
- La synchronisation haute disponibilité se produit sur le nœud secondaire.

Solution :

Créez une action Syslog avec l'adresse IP du serveur Syslog au lieu du nom de domaine du serveur Syslog.

[NSHELP-25944]

Gateway Insight n'affiche pas d'informations précises sur les utilisateurs du VPN.

[NSHELP-23937]

Le plug-in VPN n'établit pas de tunnel après l'ouverture de session Windows, si les conditions suivantes sont remplies :

- L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On
- L'appliance est configurée pour l'authentification par certificat avec une authentification à deux facteurs. `off`

[NSHELP-23584]

Parfois, lorsque vous parcourez les schémas, le message d'erreur `Cannot read property 'type 'of undefined` s'affiche.

[NSHELP-21897]

L'échec du lancement de l'application dû à un ticket STA non valide n'est pas signalé dans Gateway Insight.

[CGOP-13621]

Le rapport Gateway Insight affiche incorrectement la valeur `Local` plutôt que `SAML` dans le champ **Type d'authentification** en cas d'échec d'erreur SAML.

[CGOP-13584]

Dans une configuration à haute disponibilité, lors du basculement de NetScaler, le nombre de SR augmente au lieu du nombre de basculements dans NetScaler ADM.

[CGOP-13511]

Lorsque vous acceptez les connexions hôtes locales depuis le navigateur, la boîte de dialogue **Accepter la connexion** pour macOS affiche du contenu en anglais, quelle que soit la langue sélectionnée.

[CGOP-13050]

Le texte de `Home Page` l' **application Citrix SSO > Page d'accueil** est tronqué pour certaines langues.

[CGOP-13049]

Un message d'erreur s'affiche lorsque vous ajoutez ou modifiez une politique de session depuis l'interface graphique de NetScaler.

[CGOP-11830]

Dans Outlook Web App (OWA) 2013, cliquez sur **Options** dans le menu **Paramètres** pour afficher une boîte de dialogue **d'erreur critique** . De plus, la page ne répond plus.

[CGOP-7269]

Dans un déploiement de cluster, si vous exécutez la commande `force cluster sync` sur un nœud non CCO, le fichier ns.log contient des entrées de journal en double.

[CGOP-6794]

Web App Firewall NetScaler

L'ID de signature 1048 du Web App Firewall bloque le chargement de la page NetScaler Gateway.

[NSHELP-29113]

Équilibrage de charge

Dans une configuration haute disponibilité, les sessions d'abonné du nœud principal peuvent ne pas être synchronisées avec le nœud secondaire. C'est un cas rare.

[NSLB-7679]

Le groupe de services GSLB ne peut pas gérer les mises à jour du moniteur en raison d'une valeur ENUM manquante dans les commandes ayant échoué.

[NSHELP-29050]

L'appliance NetScaler peut ne pas répondre à une requête de domaine GSLB avec l'adresse IP du service GSLB attendue, si le serveur virtuel GSLB est configuré comme suit : Type de persistance : adresse IP source Algorithme d'équilibrage de charge : proximité statique Méthode d'équilibrage de

charge de
sauvegarde : temps aller-retour (RTT)

[NSHELP-28668]

Les sites principaux et secondaires VPX se sont plantés après avoir configuré le groupe de services GSLB avec Autoscale activé.

Solution : n'ajoutez
pas de serveurs virtuels fictifs, tels que le serveur virtuel de commutation de contenu lorsque vous ajoutez un service GSLB ou liez un port IP à un groupe de services GSLB.

[NSHELP-28530]

Dans une configuration HA, une appliance NetScaler perd sa connectivité car la mémoire du NSB n'est pas libérée après l'envoi de la réponse HTTP lors de la surveillance de la sonde HTTP.

[NSHELP-28466]

Le format ServiceGroupName dans le `entityofs` piège pour le groupe de services est le suivant : `<service(group)name>?<ip/DBS>?<port>`

Dans le format de déroutement, le groupe de services est identifié par une adresse IP ou un nom et un port DBS. Le point d'interrogation (?) est utilisé comme séparateur. NetScaler envoie le piège avec le point d'interrogation ()?. Le format apparaît de la même manière dans l'interface graphique de NetScaler ADM. C'est le comportement attendu.

[NSHELP-28080]

Divers

Lorsqu'une synchronisation forcée a lieu dans une configuration haute disponibilité, l'appliance exécute la commande `set urlfiltering parameter` sur le nœud secondaire.
Par conséquent, le nœud secondaire ignore toute mise à jour planifiée jusqu'à la prochaine heure planifiée mentionnée dans le paramètre `TimeOfDayToUpdateDB`.

[NSSWG-849]

La correspondance du modèle de jeu d'URL échoue pour les domaines standard IDNA2008.

[NSHELP-28902]

Lorsque le transfert basé sur Mac (MBF) est activé pour VXLAN, la session TCP avec état n'était pas établie.

[NSHELP-27125]

Une appliance NetScaler peut redémarrer en raison de la stagnation du processeur de gestion si un problème de connectivité survient avec le fournisseur tiers de filtrage d'URL.

[NSHELP-22409]

Réseau

Une appliance NetScaler BLX en mode DPDK peut se bloquer si un profil de pare-feu d'applications Web est configuré avec des contrôles de protection de sécurité avancés.

Solution :

Supprimez la configuration de protection de sécurité avancée pour WAF.

[NSNET-22654]

Après une mise à niveau de l'appliance NetScaler BLX 13.0 61.x vers la version 13.0 64.x, les paramètres du fichier de configuration BLX sont perdus. Le fichier de configuration BLX est ensuite réinitialisé par défaut.

[NSNET-17625]

Les opérations d'interface suivantes ne sont pas prises en charge pour les `X710 10G (i40e)` interfaces Intel sur une appliance NetScaler BLX avec DPDK :

- Désactiver
- Activer
- Réinitialiser

[NSNET-16559]

Sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure), une appliance NetScaler BLX est toujours déployée en mode partagé, quels que soient les paramètres du fichier de configuration BLX ().`/etc/blx/blx.conf` Ce problème se produit car `mawk`, qui est présent par défaut sur les systèmes Linux basés sur Debian, n'exécute pas certaines des commandes `awk` présentes dans le fichier `blx.conf`.

Solution :

Effectuez l'installation `gawk` avant d'installer une appliance NetScaler BLX. Vous pouvez exécuter la commande suivante dans l'interface de ligne de commande de l'hôte Linux pour effectuer l'installation de `gawk` :

- apt-get install gawk

[NSNET-14603]

L'installation d'une appliance NetScaler BLX peut échouer sur un hôte Linux basé sur Debian (Ubuntu version 18 et ultérieure) avec l'erreur de dépendance suivante :

```
The following packages have unmet dependencies: blx-core-libs:i386 :
PreDepends: libc6:i386 (>= 2.19)but it is not installable
```

Solution :

Exécutez les commandes suivantes dans l'interface de ligne de commande hôte Linux avant d'installer une appliance NetScaler BLX :


```
- dpkg --add-architecture i386
- apt-get update
- apt-get dist-upgrade
- apt-get install libc6:i386
<!--NeedCopy-->
```

[NSNET-14602]

Dans certains cas de connexions de données FTP, l'appliance NetScaler effectue uniquement une opération NAT et non un traitement TCP sur les paquets pour la négociation TCP MSS. Par conséquent, la MTU d'interface optimale n'est pas définie pour la connexion. Ce paramètre MTU incorrect entraîne une fragmentation des paquets et a un impact sur les performances du processeur.

[NSNET-5233]

Dans le cadre d'un déploiement NAT à grande échelle de deux appliances NetScaler dans une configuration haute disponibilité, l'ALG IPsec peut ne pas fonctionner correctement si l'une ou l'autre option de la configuration haute disponibilité est `stayprimary` définie. `staysecondary`

[NSNET-1646]

Lorsqu'une limite de mémoire de partition d'administration est modifiée dans l'appliance NetScaler, la limite de mémoire tampon TCP est automatiquement définie sur la nouvelle limite de mémoire de la partition d'administration.

[NSHELP-21082]

Dans une configuration haute disponibilité (HA), si l'ARP gratuit (GARP) est désactivé, le routeur amont risque de ne pas diriger le trafic vers le nouveau serveur principal après un basculement HA.

[NSHELP-20796]

Plateforme

Lorsque vous effectuez une mise à niveau d'une version 13.0/12.1/11.1 vers une version 13.1 ou que vous rétrogradez d'une version 13.1 vers une version 13.0/12.1/11.1, certains packages python ne sont pas installés sur les appliances NetScaler. Ce problème est résolu pour les versions suivantes de NetScaler :

- 13.1-4.x
- 13.0—82.31 et versions ultérieures
- 12.1—62.21 et versions ultérieures

Les packages python ne sont pas installés lorsque vous rétrogradez les versions de NetScaler de 13.1-4.x vers l'une des versions suivantes :

- Toute version 11.1

- 12.1-62.21 et versions antérieures
- 13.0-81.x et versions antérieures

[NSPLAT-21691]

Provisioning d'une instance VPX avec la version 12.0 XVA échoue sur une appliance NetScaler SDX exécutant la version 13.1.

Seules les versions 12.1 et ultérieures de VPX sont prises en charge. Mettez à niveau la version VPX avant de mettre à niveau le SBI vers la version 13.1.

[NSPLAT-21442]

Lorsque vous supprimez un paramètre de mise à l'échelle automatique ou un jeu d'échelle de machine virtuelle d'un groupe de ressources Azure, supprimez la configuration de profil cloud correspondante de l'instance NetScaler. Utilisez la commande `rm cloudprofile` pour supprimer le profil.

[NSPLAT-4520]

Dans une configuration haute disponibilité sur Azure, lors de la connexion au nœud secondaire via l'interface graphique, l'écran du premier utilisateur (FTU) pour la configuration du profil cloud à mise à l'échelle automatique s'affiche.
Solution : ignorez l'écran et connectez-vous au nœud principal pour créer le profil cloud. Le profil cloud doit toujours être configuré sur le nœud principal.

[NSPLAT-4451]

Les instances NetScaler VPX qui utilisent le pilote VMXNET3 peuvent se bloquer de manière aléatoire si l'instance s'exécute sur l'une des versions NetScaler suivantes :

- NetScaler 13.1 version 4.x
- NetScaler 13.1 version 9.x

[NSHELP-29120]

Stratégies

Les connexions peuvent se bloquer si la taille des données de traitement est supérieure à la taille de tampon TCP par défaut configurée.Solution : définissez la taille du tampon TCP sur une taille maximale de données à traiter.

[NSPOLICY-1267]

SSL

Sur un cluster hétérogène d'appliances NetScaler SDX 22000 et NetScaler SDX 26000, il y a une perte de configuration des entités SSL si l'appliance SDX 26000 est redémarrée.

Solution :

1. Sur le CLIP, désactivez SSLv3 sur toutes les entités SSL existantes et nouvelles, telles que le serveur virtuel, le service, le groupe de services et les services internes. Par exemple, `set ssl vserver <name> -SSL3 DISABLED`.
2. Enregistrez la configuration.

[NSSSL-9572]

La commande Mettre à jour n'est pas disponible pour les commandes d'ajout suivantes :

```
1 -  add azure application
2 -  add azure keyvault
3 -  add ssl certkey with hsmkey option
4 <!--NeedCopy-->
```

[NSSSL-6484]

Vous ne pouvez pas ajouter d'objet Azure Key Vault si un objet Azure Key Vault d'authentification est déjà ajouté.

[NSSSL-6478]

Vous pouvez créer plusieurs entités d'application Azure avec le même ID client et le même secret client. L'appliance NetScaler ne renvoie aucune erreur.

[NSSSL-6213]

Le message d'erreur incorrect suivant s'affiche lorsque vous supprimez une clé HSM sans spécifier `KEYVAULT` de type HSM.
ERREUR : `crl refresh disabled`

[NSSSL-6106]

L'actualisation automatique de la clé de session apparaît incorrectement comme désactivée sur une adresse IP de cluster. (Cette option ne peut pas être désactivée.)

[NSSSL-4427]

Un message d'avertissement incorrect `Warning: No usable ciphers configured on the SSL vserver/service`, s'affiche si vous essayez de modifier le protocole SSL ou le chiffrement dans le profil SSL.

[NSSSL-4001]

Un ticket de session expiré est honoré sur un nœud non-CCO et sur un nœud HA après un basculement HA.

[NSSSL-3184]

Une appliance NetScaler se bloque lors du traitement d'une requête HTTP si l'action de politique est définie sur `Forward` pour une politique déjà liée au point de liaison de la demande.

[NSHELP-29115]

Système

Une fuite de fenêtre TCP est observée lorsqu'une appliance NetScaler traite des trames d'en-tête HTTP/2.

[NSHELP-28475]

Lorsqu'un client réinitialise une connexion avec plusieurs flux TCP, l'enregistrement de transaction côté serveur n'est pas envoyé, ce qui entraîne l'absence d'enregistrements L4 pour ces flux de données.

[NSHELP-28281]

Dans une configuration en cluster, la `set ratecontrol` commande ne fonctionne qu'après le redémarrage de l'appliance NetScaler.

Solution :

Utilisez la commande `nsapimgr_wr.sh -ys icmp_rate_threshold=<new value>`.

[NSHELP-21811]

La valeur MAX_CONCURRENT_STREAMS est définie sur 100 par défaut si l'appliance ne reçoit pas le cadre de paramètres max_concurrent_stream du client.

[NSHELP-21240]

Les compteurs mptcp_cur_session_without_subflow décrémentent incorrectement à une valeur négative au lieu de zéro.

[NSHELP-10972]

L'adresse IP du client et l'adresse IP du serveur sont inversées dans l'enregistrement SkipFlow HDX Insight lorsque le type de transport LogStream est configuré pour Insight.

[NSBASE-8506]

Interface utilisateur

Dans l'interface graphique de NetScaler, le `Help` lien présent sous l' `Dashboard` onglet est rompu.

[NSUI-14752]

L'assistant de création/surveillance du CloudBridge Connector peut ne plus répondre ou ne parvient pas à configurer un connecteur CloudBridge.

Solution :

Configurez les connecteurs Cloudbridge en ajoutant des profils IPsec, des tunnels IP et des règles PBR à l'aide de l'interface graphique ou de la CLI de NetScaler.

[NSUI-13024]

Si vous créez une clé ECDSA à l'aide de l'interface graphique, le type de courbe n'est pas affiché.

[NSUI-6838]

Le problème suivant est observé si une opération est effectuée pour lire le fichier `ns.conf`. Par exemple, `show ns saved config`.

- Le processus HTTPD peut se figer, ce qui rend l'interface graphique et l'API NITRO inaccessibles.

[NSHELP-28249]

Dans une configuration haute disponibilité, les sessions utilisateur VPN sont déconnectées si la condition suivante est remplie :

- Si au moins deux opérations manuelles de basculement HA successives sont effectuées lorsque la synchronisation HA est en cours.

Solution :

Effectuez le basculement HA manuel successif uniquement après la fin de la synchronisation HA (les deux nœuds sont en état de réussite de la synchronisation).

[NSHELP-25598]

Le chargement et l'ajout d'un fichier de liste de révocation de certificats (CRL) échouent dans la configuration d'une partition d'administration.

[NSHELP-20988]

Lorsque vous rétrogradez la version 13.0-71.x d'une appliance NetScaler vers une version antérieure, certaines API NITRO peuvent ne pas fonctionner en raison des modifications des autorisations de fichiers.

Solution :

Modifiez l'autorisation pour `/nsconfig/ns.conf` à 644.

[NSCONFIG-4628]

Si vous (administrateur système) effectuez toutes les étapes suivantes sur une appliance NetScaler, les utilisateurs du système risquent de ne pas se connecter à l'appliance NetScaler rétrogradée.

1. Mettez à niveau l'appliance NetScaler vers l'une des versions suivantes :
   - 13.0 52.24 build
   - 12.1 57.18 build
   - 11.1 65.10 build
2. Ajoutez un utilisateur système ou modifiez le mot de passe d'un utilisateur système existant, puis enregistrez la configuration, et
3. Rétrogradez l'appliance NetScaler vers une version antérieure.

Pour afficher la liste de ces utilisateurs système à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

```
query ns config -changedpassword [-config <full path of the configuration file (ns.conf)>]
```

Solution :

Pour résoudre ce problème, utilisez l'une des options indépendantes suivantes :

- Si l'appliance NetScaler n'est pas encore rétrogradée (étape 3 des étapes mentionnées précédemment), rétrogradez l'appliance NetScaler à l'aide d'un fichier de configuration précédemment sauvegardé (ns.conf) de la même version.
- Tout administrateur système dont le mot de passe n'a pas été modifié lors de la version mise à niveau peut se connecter à la version rétrogradée et mettre à jour les mots de passe des autres utilisateurs du système.
- Si aucune des options ci-dessus ne fonctionne, un administrateur système peut réinitialiser les mots de passe des utilisateurs système.

Pour plus d'informations, consultez Comment réinitialiser le mot de passe de l'administrateur racine.

[NSCONFIG-3188]

L'une des opérations de mise à niveau de NetScaler suivantes peut entraîner un échec de connexion pour les comptes utilisateur du système local :

- de la version NetScaler 13.0-83.x à la version NetScaler 13.1-4.x
- de la version NetScaler 12.1-63.x à la version NetScaler 13.1-4.x
- de la version NetScaler 12.1-63.x à la version NetScaler 13.0-82.x

Ce problème se produit uniquement pour les comptes d'utilisateurs du système local qui répondent à l'une des conditions suivantes :

- le mot de passe utilisateur a été modifié pour le compte système local sur la version NetScaler (13.0-83.x ou 12.1-63.x) avant d'effectuer l'opération de mise à niveau.
- le compte utilisateur du système local a été ajouté sur la version NetScaler (13.0-83.x ou 12.1-63.x) avant d'effectuer l'opération de mise à niveau.

Solution :

Un administrateur système peut réinitialiser le mot de passe des comptes d'utilisateurs du système local confrontés au problème d'échec de connexion.

Pour plus d'informations, consultez Comment réinitialiser le mot de passe de l'administrateur racine.

[NSCONFIG-5650]

Démarrez avec NetScaler

July 31, 2023

Cette rubrique décrit les fonctionnalités de base et les détails de configuration d'un dispositif NetScaler. Les administrateurs système et réseau qui installent et configurent l'équipement réseau peuvent se référer au contenu.

Comprendre NetScaler

L'appliance NetScaler est un commutateur d'applications qui effectue une analyse du trafic spécifique aux applications afin de distribuer, d'optimiser et de sécuriser intelligemment le trafic réseau de couche 4 et de couche 7 (L4—L7) pour les applications Web. Par exemple, une appliance NetScaler équilibre la charge des décisions relatives à des requêtes HTTP individuelles plutôt qu'à des connexions TCP de longue durée. La fonction d'équilibrage de charge permet de ralentir la défaillance d'un serveur avec moins de perturbations pour les clients. Les fonctionnalités ADC peuvent être classées en gros comme suit :

1. Commutation de données
2. Sécurité du pare-feu
3. Optimisation
4. Infrastructure des stratégies
5. Flux de paquets

Commutation de données

Lorsqu'il est déployé devant des serveurs d'applications, un NetScaler garantit une distribution optimale du trafic grâce à la manière dont il dirige les demandes des clients. Les administrateurs peuvent segmenter le trafic des applications en fonction des informations contenues dans le corps d'une demande HTTP ou TCP, et en fonction des informations d'en-tête L4—L7 telles que l'URL, le type de données d'application ou le cookie. De nombreux algorithmes d'équilibrage de charge et des contrôles de santé complets des serveurs améliorent la disponibilité des applications en garantissant que les demandes des clients sont dirigées vers les serveurs appropriés.

Sécurité du pare-feu

La sécurité et la protection de NetScaler protègent les applications Web contre les attaques de la couche application. Une appliance ADC autorise les demandes légitimes des clients et peut bloquer les demandes malveillantes. Il fournit des défenses intégrées contre les attaques par déni de service (DoS) et prend en charge des fonctionnalités qui protègent contre les pics légitimes du trafic applicatif

qui, autrement, submergeraient les serveurs. Un pare-feu intégré disponible protège les applications Web contre les attaques de la couche application, y compris les exploits par débordement de tampon, les tentatives d'injection SQL, les attaques de script intersite, etc. En outre, le pare-feu fournit une protection contre le vol d'identité en sécurisant les informations confidentielles de l'entreprise et les données sensibles des clients.

Optimisation

L'optimisation décharge les opérations gourmandes en ressources, telles que le traitement Secure Sockets Layer (SSL), la compression des données, la persistance du client, la mise en mémoire tampon TCP et la mise en cache du contenu statique et dynamique des serveurs. Cela améliore les performances des serveurs de la batterie de serveurs et accélère donc les applications. Une appliance ADC prend en charge plusieurs optimisations TCP transparentes qui atténuent les problèmes causés par une latence élevée et des liaisons réseau encombrées. Cela accélère la livraison des applications tout en n'exigeant aucune modification de configuration pour les clients ou les serveurs.

Infrastructure des stratégies

Une stratégie définit les détails spécifiques du filtrage et de la gestion du trafic sur un NetScaler. Il se compose de deux parties : l'expression et l'action. L'expression définit les types de demandes auxquels la stratégie correspond. L'action indique à l'appliance ADC ce qu'il faut faire lorsqu'une demande correspond à l'expression. Par exemple, l'expression peut correspondre à un modèle d'URL spécifique pour une attaque de sécurité avec le paramètre configuré pour supprimer ou réinitialiser la connexion. Chaque stratégie a une priorité, et les priorités déterminent l'ordre dans lequel les stratégies sont évaluées.

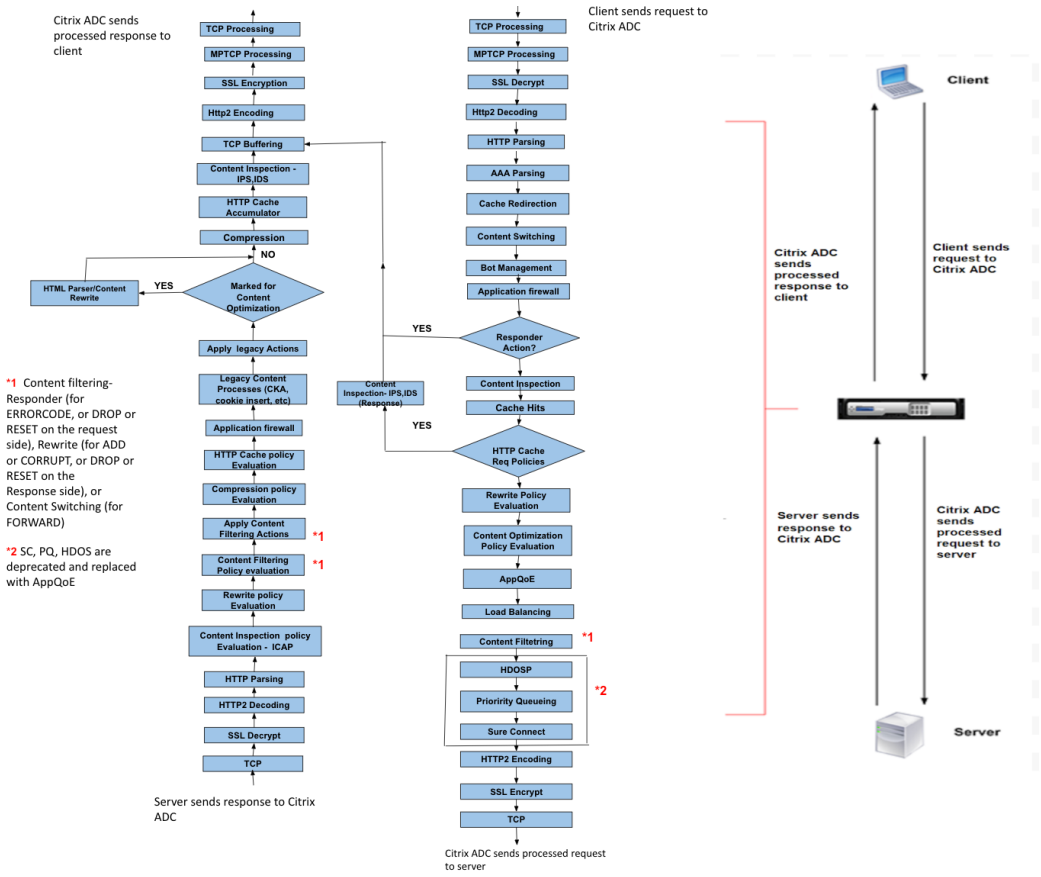
Lorsqu'un dispositif ADC reçoit du trafic, la liste de stratégies appropriée détermine comment traiter le trafic. Chaque stratégie de la liste contient une ou plusieurs expressions, qui définissent ensemble les critères auxquels une connexion doit répondre pour correspondre à la stratégie.

Pour tous les types de stratégie, à l'exception de la réécriture, l'appliance implémente uniquement la première stratégie ayant une correspondance de demande. Pour les stratégies de réécriture, l'appliance ADC évalue les stratégies dans l'ordre et effectue les actions associées dans le même ordre. La priorité des stratégies est importante pour obtenir les résultats souhaités.

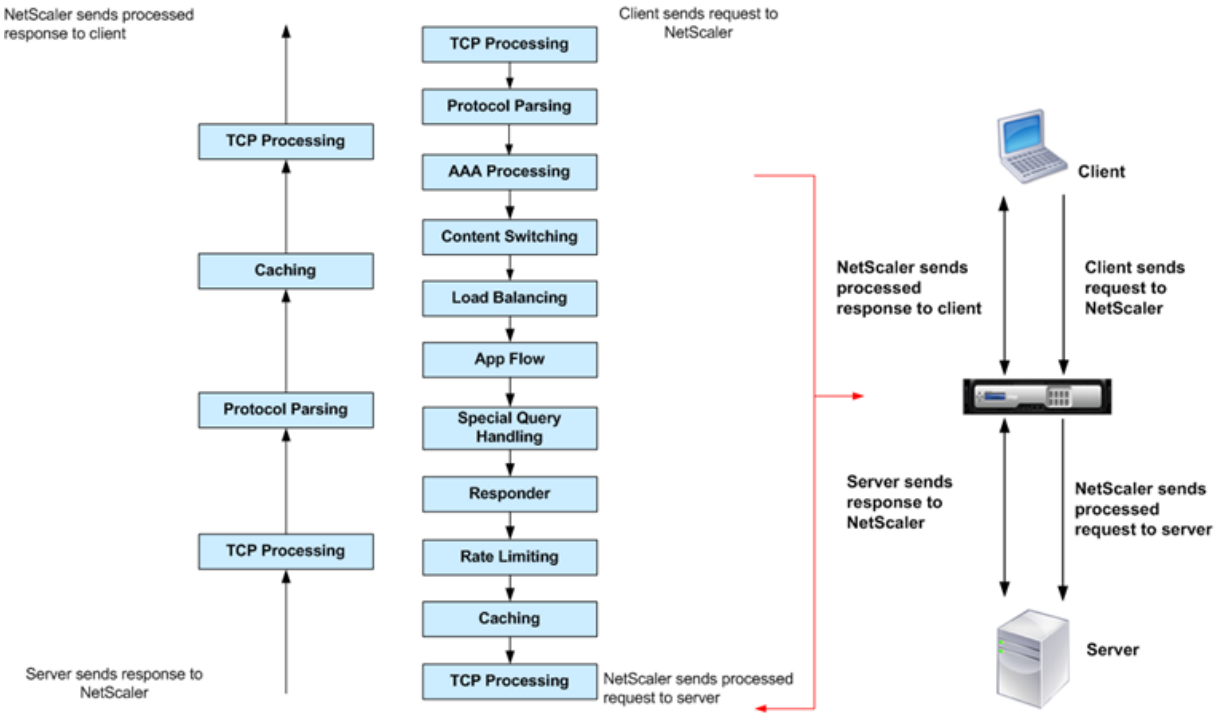
Flux de paquets

Selon les besoins, vous pouvez choisir de configurer plusieurs fonctionnalités. Par exemple, vous pouvez choisir de configurer à la fois la compression et le déchargement SSL. Par conséquent, un paquet sortant peut être compressé puis chiffré avant d'être envoyé au client.

La figure suivante montre le flux de paquets HTTP2 dans l'appliance NetScaler.



La figure suivante montre le flux de traitement des requêtes de flux de données dans l'appliance NetScaler. DataStream est pris en charge pour les bases de données MySQL et MS SQL. Pour plus d'informations sur la fonctionnalité DataStream, consultez DataStream.



> **Remarque :** Si le trafic concerne un serveur virtuel de commutation de contenu, l'appliance évalue les stratégies dans l'ordre suivant :
>
> 1. lié au remplacement global.
> 2. lié au serveur virtuel d'équilibrage de charge.
> 3. lié au serveur virtuel de commutation de contenu.
> 4. lié à la valeur par défaut globale.
>
> De cette façon, si une règle de stratégie est vraie et que gotopriorityexpression a la valeur END, nous arrêtons toute évaluation ultérieure de la stratégie.
> Dans le cas de la commutation de contenu, si aucun serveur virtuel d'équilibrage de charge n'est sélectionné ou lié au serveur virtuel de commutation de contenu, nous évaluons les stratégies de répondeur liées uniquement au serveur virtuel de commutation de contenu.

Limitation du système

Il existe des limites du système pour chaque fonctionnalité de NetScaler lorsque vous installez le logiciel NetScaler 9.2 ou version ultérieure. Pour plus d'informations, consultez l'article Citrix, CTX118716.

Où se situe une appliance NetScaler dans le réseau ?

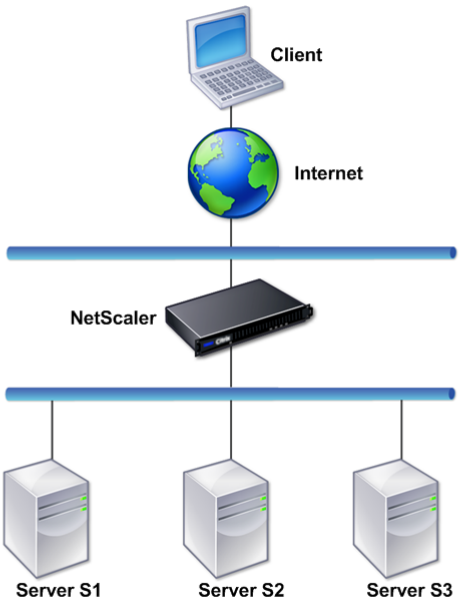
May 5, 2023

Une appliance NetScaler se trouve entre les clients et les serveurs, de sorte que les demandes des clients et les réponses du serveur passent par elle. Dans une installation classique, les serveurs virtuels configurés sur l'appliance fournissent des points de connexion que les clients utilisent pour accéder aux applications derrière l'appliance. Dans ce cas, l'appliance possède des adresses IP publiques associées à ses serveurs virtuels, tandis que les serveurs réels sont isolés dans un réseau privé. Il est également possible de faire fonctionner l'appareil en mode transparent en tant que pont L2 ou routeur L3, ou même de combiner certains aspects de ces modes et d'autres.

Modes de déploiement physique

Une appliance NetScaler résidant logiquement entre les clients et les serveurs peut être déployée selon l'un des deux modes physiques suivants : en ligne et à bras unique. En mode en ligne, plusieurs interfaces réseau sont connectées à différents segments Ethernet et l'appliance est placée entre les clients et les serveurs. L'appliance possède une interface réseau distincte pour chaque réseau client et une interface réseau distincte pour chaque réseau de serveurs. L'appliance et les serveurs peuvent exister sur différents sous-réseaux dans cette configuration. Les serveurs peuvent se trouver sur un réseau public et les clients peuvent accéder directement aux serveurs via l'appliance, l'appliance appliquant de manière transparente les fonctionnalités L4-L7. Généralement, les serveurs virtuels (décrits plus loin) sont configurés pour fournir une abstraction des serveurs réels. La figure suivante montre un déploiement en ligne classique.

Figure 1. Déploiement en ligne



En mode monobras, une seule interface réseau de l'appliance est connectée à un segment Ethernet. Dans ce cas, l'appliance n'isole pas les côtés client et serveur du réseau, mais fournit un accès aux applications via des serveurs virtuels configurés. Le mode One-Arm permet de simplifier les modifications réseau nécessaires à l'installation de NetScaler dans certains environnements.

Pour obtenir des exemples de déploiement en ligne (à deux bras) et à un bras, reportez-vous à la section Présentation des topologies communes de réseau.

NetScaler en tant que périphérique L2

Une appliance NetScaler fonctionnant comme un périphérique L2 est censée fonctionner en mode L2. En mode L2, l'appliance ADC transfère les paquets entre les interfaces réseau lorsque toutes les conditions suivantes sont remplies :

- Les paquets sont destinés à l'adresse MAC (Media Access Control) d'un autre appareil.
- L'adresse MAC de destination se trouve sur une autre interface réseau.
- L'interface réseau est membre du même réseau local virtuel (VLAN).

Par défaut, toutes les interfaces réseau sont membres d'un VLAN prédéfini, le VLAN 1. Les demandes et réponses du protocole ARP (Address Resolution Protocol) sont transmises à toutes les interfaces réseau membres du même VLAN. Pour éviter de créer des ponts, le mode L2 doit être désactivé si un autre périphérique L2 fonctionne en parallèle avec l'appliance NetScaler.

Pour plus d'informations sur la façon dont les modes L2 et L3 interagissent, consultez Modes de transfert de paquets.

Pour plus d'informations sur la configuration du mode L2, reportez-vous à la section « Activer et désactiver le mode de couche 2 » dans Modes de transfert de paquets.

NetScaler en tant que périphérique de transfert de paquets

Une appliance NetScaler peut fonctionner comme un périphérique de transfert de paquets, et ce mode de fonctionnement est appelé mode L3. Lorsque le mode L3 est activé, l'appliance transmet tous les paquets unicast reçus qui sont destinés à une adresse IP n'appartenant pas à l'appliance, s'il existe un itinéraire vers la destination. L'appliance peut également acheminer des paquets entre des VLAN.

Dans les deux modes de fonctionnement, L2 et L3, l'appliance supprime généralement les paquets qui se trouvent dans :

- Trames de multidiffusion
- Trames de protocole inconnues destinées à l'adresse MAC d'une appliance (non IP et non ARP)
- Protocole Spanning Tree (sauf si BridgeBPDU est ON)

Pour plus d'informations sur la façon dont les modes L2 et L3 interagissent, consultez Modes de transfert de paquets.

Pour plus d'informations sur la configuration du mode L3, voir Modes de transfert de paquets.

How a NetScaler appliance communicates with clients and servers

May 5, 2023

Une appliance NetScaler est généralement déployée devant un parc de serveurs et fonctionne comme un proxy TCP transparent entre les clients et les serveurs, sans nécessiter de configuration côté client. Ce mode de fonctionnement de base est appelé technologie de commutation de requêtes et constitue le cœur des fonctionnalités de NetScaler. La commutation de demandes permet à une appliance de multiplexer et de décharger les connexions TCP, de maintenir des connexions persistantes et de gérer le trafic au niveau de la demande (couche application). Cela est possible car l'appliance peut séparer la demande HTTP de la connexion TCP sur laquelle la demande est envoyée.

Selon la configuration, une appliance peut traiter le trafic avant de transmettre la demande à un serveur. Par exemple, si le client tente d'accéder à une application sécurisée sur le serveur, l'appliance peut effectuer le traitement SSL nécessaire avant d'envoyer le trafic vers le serveur.

Pour faciliter un accès efficace et sécurisé aux ressources du serveur, une appliance utilise un ensemble d'adresses IP appelées collectivement adresses IP appartenant à NetScaler. Pour gérer votre trafic réseau, vous attribuez des adresses IP appartenant à NetScaler à des entités virtuelles qui deviennent les éléments constitutifs de votre configuration. Par exemple, pour configurer l'équilibrage de charge, vous créez des serveurs virtuels pour recevoir les demandes des clients et les distribuer aux services, qui sont des entités représentant les applications présentes sur vos serveurs.

Comprendre les adresses IP détenues par NetScaler

Pour fonctionner en tant que proxy, une appliance NetScaler utilise diverses adresses IP. Les principales adresses IP détenues par NetScaler sont les suivantes :

- Adresse IP NetScaler (NSIP)

  L'adresse NSIP est l'adresse IP utilisée pour la gestion et l'accès général au système à l'appliance elle-même, ainsi que pour la communication entre les appliances dans une configuration haute disponibilité.

- Adresse IP (VIP) du serveur virtuel

  Une adresse VIP est l'adresse IP associée à un serveur virtuel. Il s'agit de l'adresse IP publique à laquelle les clients se connectent. Une appliance gérant un large éventail de trafic peut avoir de nombreux VIP configurés.

- Adresse IP du sous-réseau (SNIP)

  Une adresse SNIP est utilisée pour la gestion des connexions et la surveillance des serveurs. Vous pouvez spécifier plusieurs adresses SNIP pour chaque sous-réseau. Les adresses SNIP peuvent être liées à un VLAN.

- Ensemble d'adresses IP

  Un ensemble d'adresses IP est un ensemble d'adresses IP configurées sur l'appliance en tant que SNIP. Un ensemble d'adresses IP est identifié avec un nom significatif qui aide à identifier l'utilisation des adresses IP qu'il contient.

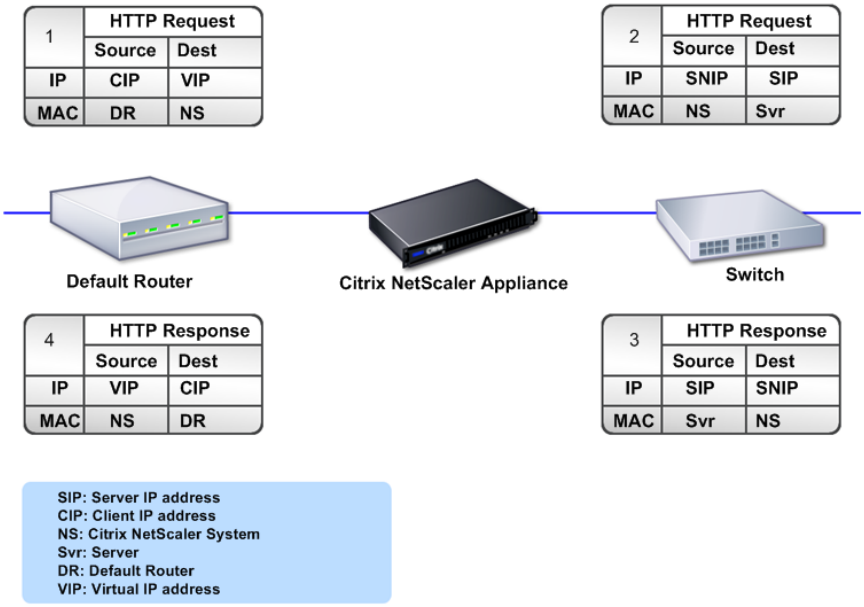
- Profil net

  Un profil réseau (ou profil réseau) contient une adresse IP ou un ensemble d'adresses IP. Un profil réseau peut être lié à des serveurs virtuels, à des services, à des groupes de services ou à des moniteurs d'équilibrage de charge ou de commutation de contenu. Lors de la communication avec des serveurs physiques ou des homologues, l'appliance utilise les adresses spécifiées dans le profil comme adresses IP source.

Comment les flux de trafic sont gérés

Comme une appliance NetScaler fonctionne comme un proxy TCP, elle traduit les adresses IP avant d'envoyer des paquets à un serveur. Lorsque vous configurez un serveur virtuel, les clients se connectent à une adresse VIP sur l'appliance NetScaler au lieu de se connecter directement à un serveur. Selon les paramètres du serveur virtuel, l'appliance sélectionne un serveur approprié et envoie la demande du client à ce serveur. Par défaut, l'appliance utilise une adresse SNIP pour établir des connexions avec le serveur, comme illustré dans la figure suivante.

Figure 1. Connexions basées sur un serveur virtuel



En l'absence de serveur virtuel, lorsqu'une appliance reçoit une demande, elle la transmet de manière transparente au serveur. C'est ce qu'on appelle le mode de fonctionnement transparent. Lorsqu'elle fonctionne en mode transparent, une appliance traduit les adresses IP source des demandes clientes entrantes en adresse SNIP mais ne modifie pas l'adresse IP de destination. Pour que ce mode fonctionne, le mode L2 ou L3 doit être configuré de manière appropriée.

Dans les cas où les serveurs ont besoin de l'adresse IP réelle du client, l'appliance peut être configurée pour modifier l'en-tête HTTP en insérant l'adresse IP du client sous forme de champ supplémentaire, ou configurée pour utiliser l'adresse IP du client au lieu d'une adresse SNIP pour les connexions aux serveurs.

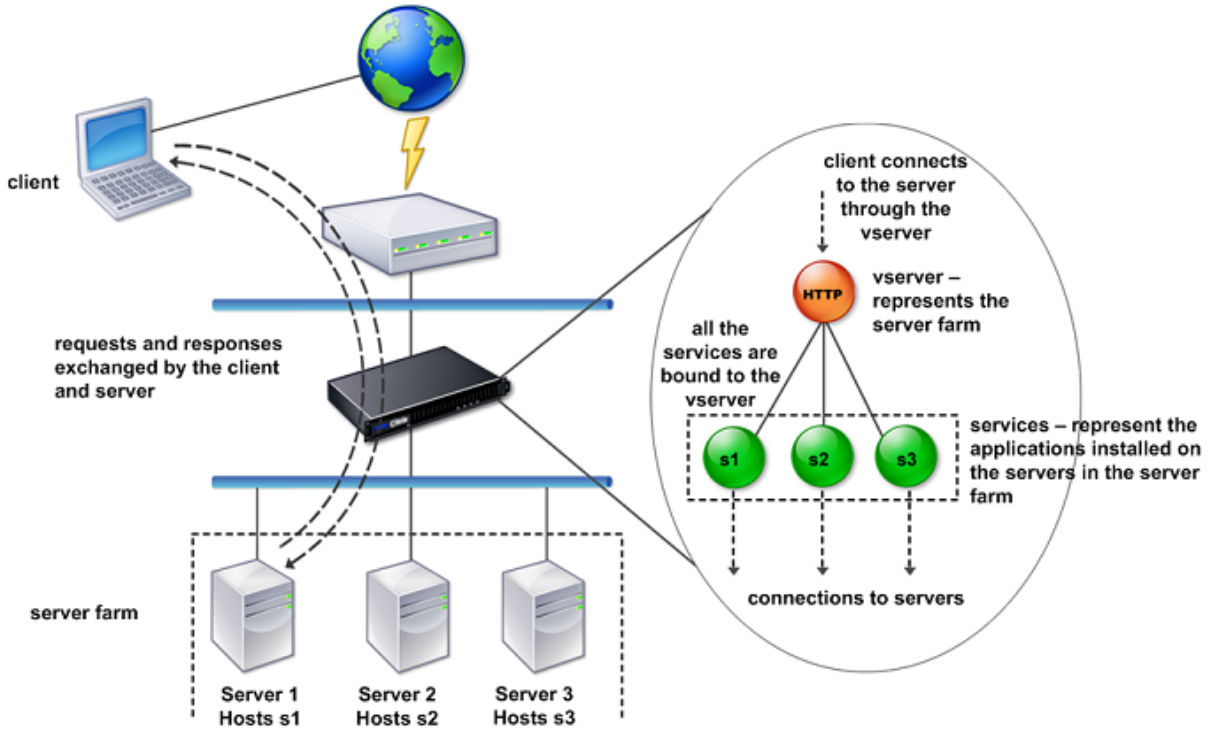
Éléments constitutifs de la gestion du trafic

La configuration d'une appliance NetScaler repose généralement sur une série d'entités virtuelles qui servent de blocs de base pour la gestion du trafic. L'approche modulaire permet de séparer les flux de trafic. Les entités virtuelles sont des abstractions qui représentent généralement des adresses IP, des ports et des gestionnaires de protocoles pour le traitement du trafic. Les clients accèdent aux applications et aux ressources par le biais de ces entités virtuelles. Les entités les plus couramment utilisées sont les serveurs et les services virtuels. Les serveurs virtuels représentent des groupes de

serveurs au sein d'une batterie de serveurs ou d'un réseau distant, et les services représentent des applications spécifiques sur chaque serveur.

La plupart des fonctionnalités et des paramètres de trafic sont activés via des entités virtuelles. Par exemple, vous pouvez configurer un dispositif pour compresser toutes les réponses du serveur à un client connecté à la batterie de serveurs via un serveur virtuel particulier. Pour configurer l'appliance pour un environnement particulier, vous devez identifier les fonctionnalités appropriées, puis choisir la bonne combinaison d'entités virtuelles pour les fournir. La plupart des fonctionnalités sont fournies par le biais d'une cascade d'entités virtuelles liées les unes aux autres. Dans ce cas, les entités virtuelles sont comme des blocs assemblés dans la structure finale d'une application livrée. Vous pouvez ajouter, supprimer, modifier, lier, activer et désactiver les entités virtuelles pour configurer les fonctionnalités. La figure suivante montre les concepts abordés dans cette section.

Figure 2. Comment fonctionnent les éléments constitutifs de la gestion du trafic



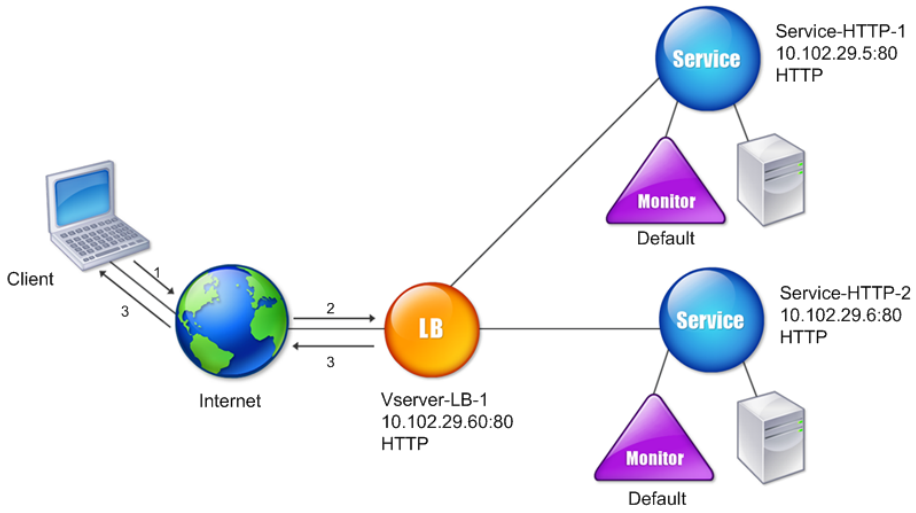
Une configuration d'équilibrage de charge simple

Dans l'exemple illustré dans la figure suivante, l'appliance NetScaler est configurée pour fonctionner comme un équilibreur de charge. Pour cette configuration, vous devez configurer des entités virtuelles spécifiques à l'équilibrage de charge et les lier dans un ordre spécifique. En tant qu'équilibreur de charge, une appliance distribue les demandes des clients sur plusieurs serveurs et optimise ainsi l'utilisation des ressources.

Les éléments de base d'une configuration d'équilibrage de charge classique sont les services et les

serveurs virtuels d'équilibrage de charge. Les services représentent les applications présentes sur les serveurs. Les serveurs virtuels font abstraction des serveurs en fournissant une adresse IP unique à laquelle les clients se connectent. Pour garantir que les demandes des clients sont envoyées à un serveur, vous devez lier chaque service à un serveur virtuel. En d'autres termes, vous devez créer des services pour chaque serveur et les lier à un serveur virtuel. Les clients utilisent l'adresse VIP pour se connecter à une appliance NetScaler. Lorsque l'appliance reçoit des demandes clients envoyées à l'adresse VIP, elle les envoie à un serveur déterminé par l'algorithme d'équilibrage de charge. L'équilibrage de charge utilise une entité virtuelle appelée moniteur pour vérifier si un service configuré spécifique (serveur plus application) est disponible pour recevoir des demandes.

Figure 3. Serveur virtuel d'équilibrage de charge, services et moniteurs



Outre la configuration de l'algorithme d'équilibrage de charge, vous pouvez configurer plusieurs paramètres qui influent sur le comportement et les performances de la configuration d'équilibrage de charge. Par exemple, vous pouvez configurer le serveur virtuel pour maintenir la persistance en fonction de l'adresse IP source. L'appliance dirige ensuite toutes les demandes provenant d'une adresse IP spécifique vers le même serveur.

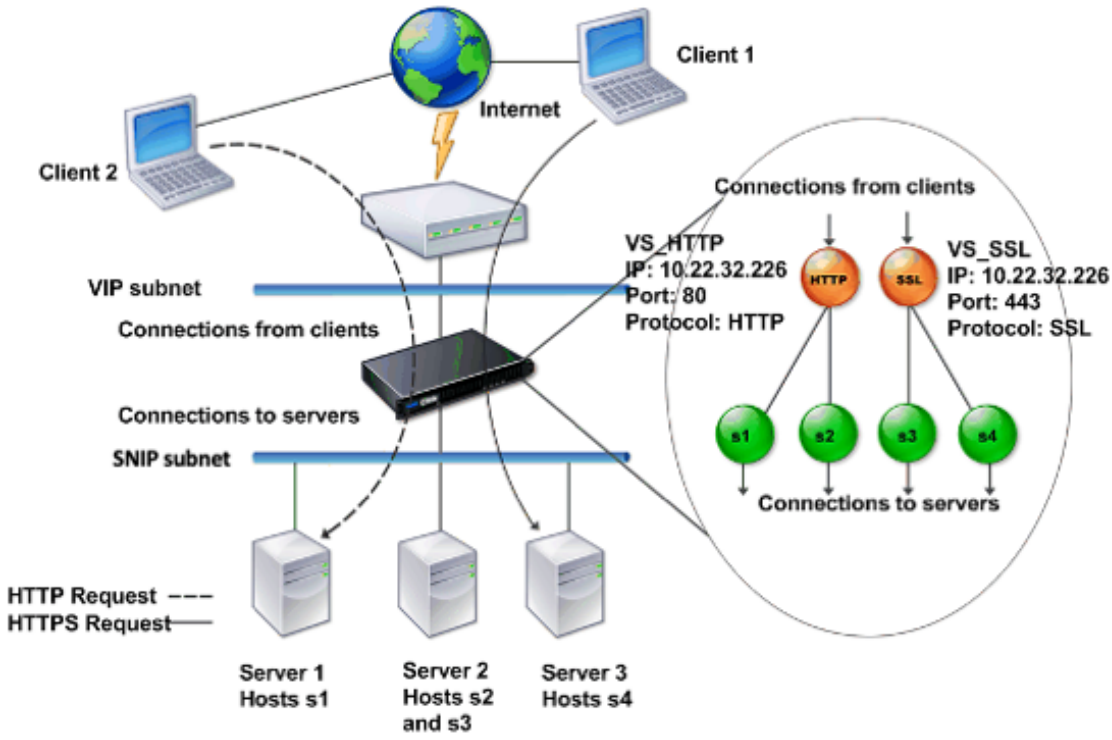
Comprendre les serveurs virtuels

Un serveur virtuel est une entité nommée NetScaler que les clients externes peuvent utiliser pour accéder aux applications hébergées sur les serveurs. Il est représenté par un nom alphanumérique, une adresse IP virtuelle (VIP), un port et un protocole. Le nom du serveur virtuel n'a qu'une signification locale et est conçu pour faciliter l'identification du serveur virtuel. Lorsqu'un client tente d'accéder à des applications sur un serveur, il envoie une demande au VIP au lieu de l'adresse IP du serveur physique. Lorsque l'appliance reçoit une demande à l'adresse VIP, elle met fin à la connexion au serveur virtuel et utilise sa propre connexion avec le serveur pour le compte du client. Les paramètres de port et de protocole du serveur virtuel déterminent les applications que le serveur virtuel représente. Par exemple, un serveur Web peut être représenté par un serveur virtuel et un service dont le port et le protocole sont définis respectivement sur 80 et HTTP. Plusieurs serveurs virtuels peuvent utiliser la même adresse VIP mais des protocoles et des ports différents.

Les serveurs virtuels sont des points de fourniture de fonctionnalités. La plupart des fonctionnalités, telles que la compression, la mise en cache et le déchargement SSL, sont normalement activées sur un serveur virtuel. Lorsque l'appliance reçoit une demande à une adresse VIP, elle choisit le serveur virtuel approprié en fonction du port sur lequel la demande a été reçue et de son protocole. L'appliance traite ensuite la demande en fonction des fonctionnalités configurées sur le serveur virtuel.

Dans la plupart des cas, les serveurs virtuels fonctionnent en tandem avec les services. Vous pouvez lier plusieurs services à un serveur virtuel. Ces services représentent les applications qui s'exécutent sur les serveurs physiques d'une batterie de serveurs. Une fois que l'appliance a traité les demandes reçues à une adresse VIP, elle les transmet aux serveurs conformément à l'algorithme d'équilibrage de charge configuré sur le serveur virtuel. La figure suivante illustre ces concepts.

Figure 4. Plusieurs serveurs virtuels avec une seule adresse VIP



La figure précédente montre une configuration composée de deux serveurs virtuels avec une adresse VIP commune mais des ports et des protocoles différents. Deux services sont liés à chacun des serveurs virtuels. Les services s1 et s2 sont liés à VS_HTTP et représentent les applications HTTP sur les serveurs 1 et 2. Les services s3 et s4 sont liés à VS_SSL et représentent les applications SSL sur les serveurs 2 et 3 (le serveur 2 fournit à la fois des applications HTTP et SSL). Lorsque l'appliance reçoit une requête HTTP à l'adresse VIP, elle traite la demande conformément aux paramètres de VS_HTTP et l'envoie au serveur 1 ou au serveur 2. De même, lorsque l'appliance reçoit une demande HTTPS à l'adresse VIP, elle la traite conformément aux paramètres de VS_SSL et l'envoie au serveur 2 ou au serveur 3.

Les serveurs virtuels ne sont pas toujours représentés par des adresses IP, des numéros de port ou des protocoles spécifiques. Ils peuvent être représentés par des caractères génériques, auquel cas ils sont appelés serveurs virtuels génériques. Par exemple, lorsque vous configurez un serveur virtuel avec un caractère générique au lieu d'un VIP, mais avec un numéro de port spécifique, l'appliance intercepte et traite tout le trafic conforme à ce protocole et destiné au port prédéfini. Pour les serveurs virtuels utilisant des caractères génériques plutôt que des adresses VIP et des numéros de port, l'appliance intercepte et traite tout le trafic conformément au protocole.

Les serveurs virtuels peuvent être regroupés dans les catégories suivantes :

- Serveur virtuel d'équilibrage de charge

  Reçoit et redirige les demandes vers un serveur approprié. Le choix du serveur approprié

dépend de la méthode d'équilibrage de charge configurée par l'utilisateur.

- Serveur virtuel de redirection de cache

  Redirige les demandes de contenu dynamique des clients vers les serveurs d'origine et les demandes de contenu statique vers les serveurs de cache. Les serveurs virtuels de redirection de cache fonctionnent souvent conjointement avec des serveurs virtuels d'équilibrage de charge.

- Serveur virtuel de commutation de contenu

  Dirige le trafic vers un serveur en fonction du contenu demandé par le client. Par exemple, vous pouvez créer un serveur virtuel de commutation de contenu qui dirige toutes les demandes d'images des clients vers un serveur qui diffuse uniquement des images. Les serveurs virtuels de commutation de contenu fonctionnent souvent conjointement avec des serveurs virtuels d'équilibrage de charge.

- Serveur virtuel de réseau privé virtuel (VPN)

  Déchiffre le trafic tunnelisé et l'envoie aux applications intranet.

- Serveur virtuel SSL

  Reçoit et déchiffre le trafic SSL, puis le redirige vers un serveur approprié. Le choix du serveur approprié est similaire au choix d'un serveur virtuel d'équilibrage de charge.

Comprendre les services

Les services représentent des applications sur un serveur. Bien que les services soient normalement associés à des serveurs virtuels, en l'absence d'un serveur virtuel, un service peut toujours gérer le trafic spécifique à l'application. Par exemple, vous pouvez créer un service HTTP sur une appliance NetScaler pour représenter une application de serveur Web. Lorsque le client tente d'accéder à un site Web hébergé sur le serveur Web, l'appliance intercepte les requêtes HTTP et crée une connexion transparente avec le serveur Web.

En mode service uniquement, une appliance fonctionne comme un proxy. Il met fin aux connexions client, utilise une adresse SNIP pour établir une connexion au serveur et traduit les adresses IP source des demandes clientes entrantes en une adresse SNIP. Bien que les clients envoient des requêtes directement à l'adresse IP du serveur, celui-ci les considère comme provenant de l'adresse SNIP. L'appliance traduit les adresses IP, les numéros de port et les numéros de séquence.

Un service est également un point d'application de fonctionnalités. Prenons l'exemple de l'accélération SSL. Pour utiliser cette fonctionnalité, vous devez créer un service SSL et lier un certificat SSL au service. Lorsque l'appliance reçoit une demande HTTPS, elle déchiffre le trafic et l'envoie, en texte clair, au serveur. Seul un ensemble limité de fonctionnalités peut être configuré dans le cas d'un service uniquement.

Les services utilisent des entités appelées moniteurs pour suivre l'état des applications. Chaque service est associé à un moniteur par défaut, basé sur le type de service. Conformément aux paramètres configurés sur le moniteur, l'appliance envoie des sondes à l'application à intervalles réguliers pour déterminer son état. Si les sondes échouent, l'appliance marque le service comme étant hors service. Dans ce cas, l'appliance répond aux demandes des clients par un message d'erreur approprié ou redirige la demande selon les politiques d'équilibrage de charge configurées.

Présentation de la gamme de produits NetScaler

May 5, 2023

La gamme de produits NetScaler optimise la fourniture d'applications sur Internet et les réseaux privés, en combinant la sécurité au niveau des applications, l'optimisation et la gestion du trafic dans une seule appliance intégrée. Vous pouvez installer une appliance NetScaler dans votre salle des serveurs et y acheminer toutes les connexions vers vos serveurs gérés. Les fonctionnalités NetScaler que vous activez et les politiques que vous définissez sont ensuite appliquées au trafic entrant et sortant.

Une appliance NetScaler peut être intégrée à n'importe quel réseau en complément des équilibreurs de charge, des serveurs, des caches et des pare-feux existants. Il ne nécessite aucun logiciel supplémentaire côté client ou serveur et peut être configuré à l'aide de l'interface graphique Web et des utilitaires de configuration CLI de NetScaler.

Cette rubrique comprend les sections suivantes :

- Plateformes matérielles NetScaler
- Éditions NetScaler
- Versions prises en charge sur le matériel ADC
- Navigateurs compatibles

Plateformes matérielles NetScaler

Le matériel NetScaler est disponible sur de nombreuses plateformes qui présentent différentes spécifications matérielles :

Plateforme matérielle NetScaler MPX

Plate-forme matérielle NetScaler SDX

Éditions NetScaler

Le système d'exploitation NetScaler est disponible en trois éditions :

- Standard
- Advanced
- Premium

Les éditions Standard et Advanced proposent des fonctionnalités limitées. Des licences de fonctionnalités sont requises pour toutes les éditions.

Pour plus d'informations sur les éditions du logiciel NetScaler, consultez la fiche technique des éditions NetScaler.

Pour plus d'informations sur la façon d'obtenir et d'installer des licences, consultez Licences.

Versions prises en charge sur le matériel NetScaler

Consultez les tableaux de matrice de compatibilité suivants pour toutes les plateformes matérielles NetScaler et les versions logicielles prises en charge sur ces plateformes :

Matrice de compatibilité matérielle/logicielle NetScaler MPX

Matrice de compatibilité matérielle/logicielle NetScaler SDX

Navigateurs compatibles

Pour accéder à l'interface graphique de NetScaler, votre poste de travail doit disposer d'un navigateur Web compatible.

Le tableau suivant répertorie les navigateurs compatibles pour les versions 12.0, 12.1 et 13.0 de l'interface graphique NetScaler :

Système d'exploitation	Navigateur	Versions
Windows 7 et versions ultérieures	Internet Explorer	11, Edge et versions ultérieures
Windows 7 et versions ultérieures	Mozilla Firefox	45 et versions ultérieures
Windows 7 et versions ultérieures	Chrome	60 et versions ultérieures
MAC	Mozilla Firefox	45 et versions ultérieures
MAC	Safari	10.1.1 et versions ultérieures

Les versions de navigateur compatibles pour NetScaler 11.1 sont les suivantes :

Système d'exploitation	Navigateur	Versions
Windows 7 et versions ultérieures	Internet Explorer	8, 9, 10, 11, Edge
Windows 7 et versions ultérieures	Mozilla Firefox	45 et versions ultérieures
Windows 7 et versions ultérieures	Chrome	60 et versions ultérieures
MAC	Mozilla Firefox	45 et versions ultérieures
MAC	Safari	10.1.1 et versions ultérieures

Installer le matériel

May 5, 2023

Avant d'installer une appliance NetScaler, consultez la liste de contrôle préalable à l'installation.

Pour utiliser l'appliance SDX, vous devez effectuer les tâches suivantes en suivant les instructions données dans les ressources fournies dans le tableau. Effectuez les tâches dans l'ordre indiqué.

Tâche

Description

1. Lisez les informations de sécurité, les mises en garde, les avertissements et autres informations

   Lisez les informations de mise en garde et de danger que vous devez connaître avant d'installer le produit.

2. Préparer l'installation

   Déballez votre appareil et assurez-vous que toutes les pièces ont été livrées, préparez le site et le rack, et suivez les consignes de sécurité électrique de base avant d'installer votre nouvel appareil.

3. Installer le matériel

   Montez l'appliance en rack, installez les émetteurs-récepteurs (si disponibles) et connectez l'appliance au réseau et à une source d'alimentation.

4. Configurez l'appliance.

   Configurez les paramètres initiaux de l'appliance NetScaler à l'aide de l'interface graphique ou de la console série.

Suivez les étapes décrites dans les documentations suivantes pour effectuer ces tâches :

- Documentation sur le matériel NetScaler MPX
- Documentation sur le matériel NetScaler SDX

Accès à une appliance NetScaler

May 5, 2023

Une appliance NetScaler possède à la fois une interface de ligne de commande (CLI) et une interface graphique. L'interface graphique inclut un utilitaire de configuration pour configurer l'appliance et un utilitaire statistique, appelé Dashboard. Pour l'accès initial, toutes les appliances sont livrées avec l'adresse IP NetScaler (NSIP) par défaut 192.168.100.1 et le masque de sous-réseau par défaut 255.255.0.0. Vous pouvez attribuer un nouveau NSIP et un masque de sous-réseau associé lors de la configuration initiale.

Si vous rencontrez un conflit d'adresse IP lors du déploiement de plusieurs unités NetScaler, recherchez les causes possibles suivantes :

- Avez-vous sélectionné un NSIP qui est une adresse IP déjà attribuée à un autre appareil de votre réseau ?
- Avez-vous attribué le même NSIP à plusieurs appliances NetScaler ?
- Le NSIP est accessible sur tous les ports physiques. Les ports d'un NetScaler sont des ports hôtes et non des ports de commutateur.

Le tableau suivant récapitule les méthodes d'accès disponibles.

Méthode d'accès	Port	Adresse IP par défaut requise ? (OUI/N)
LIGNE DE COMMANDE	Console	N
CLI et GUI	Ethernet	O

Interface de ligne de commande

Accédez à l'interface de ligne de commande localement en connectant une station de travail au port de console, ou à distance en vous connectant via le Secure Shell (SSH) depuis n'importe quelle station de travail du même réseau.

Connectez-vous à l'interface de ligne de commande via le port de console

L'appliance dispose d'un port de console permettant de le connecter à un poste de travail informatique. Pour vous connecter à l'appliance, vous avez besoin d'un câble croisé série et d'une station de travail dotée d'un programme d'émulation de terminal.

Pour vous connecter à l'interface de ligne de commande via le port de console, procédez comme suit :

1. Connectez le port de la console à un port série de la station de travail. Pour plus d'informations, voir Connecter le câble de la console.
2. Sur le poste de travail, démarrez HyperTerminal ou tout autre programme d'émulation de terminal. Si l'invite d'ouverture de session ne s'affiche pas, vous devrez peut-être appuyer sur ENTER une ou plusieurs fois pour l'afficher.
3. Dans Nom d'utilisateur, tapez `nsroot`. Dans Mot de passe, tapez `nsroot` et si ce mot de passe ne fonctionne pas, essayez de saisir le numéro de série de l'appliance. Le code à barres du numéro de série est disponible à l'arrière de l'appliance.

Connectez-vous à l'interface de ligne de commande à l'aide de SSH

Le protocole SSH est la méthode d'accès à distance préférée pour accéder à distance à une appliance depuis n'importe quel poste de travail du même réseau. Vous pouvez utiliser SSH version 1 (SSH1) ou SSH version 2 (SSH2).

Si vous ne disposez pas d'un client SSH fonctionnel, vous pouvez télécharger et installer l'un des programmes clients SSH suivants :

- PuTTY

  Logiciel Open Source pris en charge sur de multiples plateformes. Disponible à :

  http://www.chiark.greenend.org.uk/~sgtatham/putty/

- `Vandyke` Logiciel SecureCRT

  Logiciels commerciaux pris en charge sur la plate-forme Windows. Disponible à :

  http://www.vandyke.com/products/securecrt/

Ces programmes sont testés par l'équipe NetScaler, qui a vérifié qu'ils fonctionnent correctement avec une appliance NetScaler. D'autres programmes peuvent également fonctionner correctement, mais ils n'ont pas été testés.

Pour vérifier que le client SSH est correctement installé, utilisez-le pour vous connecter à n'importe quel appareil de votre réseau qui accepte les connexions SSH.

Pour vous connecter à une appliance NetScaler à l'aide d'un client SSH, procédez comme suit :

1. Sur votre poste de travail, démarrez le client SSH.

2. Pour la configuration initiale, utilisez l'adresse IP par défaut (NSIP), qui est 192.168.100.1. Pour un accès ultérieur, utilisez le NSIP qui a été attribué lors de la configuration initiale. Sélectionnez SSH1 ou SSH2 comme protocole.
3. Dans Nom d'utilisateur, tapez `nsroot`. Dans Mot de passe, tapez `nsroot` et si ce mot de passe ne fonctionne pas, essayez de saisir le numéro de série de l'appliance. Le code à barres du numéro de série est disponible à l'arrière de l'appliance. Par exemple.

```
login as: nsroot


Using keyboard-interactive authentication.


Password:


Last login: Tue Jun 16 10:37:28 2009 from 10.102.29.9




Done


>


<!--NeedCopy-->
```

Interface graphique NetScaler

> **Important :**
>
> Une paire de clés de certificat est requise pour l'accès HTTPS à l'interface graphique de Citric ADC. Sur l'ADC, une paire de clés de certificat est automatiquement liée aux services internes. Sur une appliance MPX ou SDX, la taille de clé par défaut est de 1024 octets, et sur une instance VPX, la taille de clé par défaut est de 512 octets. Cependant, la plupart des navigateurs actuels n'acceptent pas une clé de moins de 1024 octets. Par conséquent, l'accès HTTPS à l'utilitaire de configuration VPX est bloqué.

De plus, si aucune licence n'est présente sur une appliance MPX au démarrage, que vous ajoutez une licence ultérieurement et que vous redémarrez l'appliance, vous risquez de perdre la liaison du certificat.

Citrix vous recommande d'installer une paire de clés de certificat d'au moins 1 024 octets sur l'appliance pour un accès HTTPS à l'interface graphique. Installez également une licence appropriée avant de démarrer l'appliance.

L'interface graphique inclut un utilitaire de configuration et un utilitaire de statistiques, appelés Dashboard, auxquels vous pouvez accéder via une station de travail connectée à un port Ethernet de l'appliance.

La configuration système requise pour la station de travail exécutant l'interface graphique est la suivante :

- Pour les postes de travail Windows, un processeur Pentium 166 MHz ou supérieur.
- Pour les postes de travail basés sur Linux, une plate-forme Pentium exécutant le noyau Linux v2.2.12 ou supérieur, et les `glibc` versions 2.12-11 ou ultérieures. Un minimum de 32 Mo de RAM est requis, et 48 Mo de RAM sont recommandés. La station de travail doit prendre en charge le mode couleur 16 bits, les gestionnaires de fenêtres KDE et KWM utilisés conjointement, avec des affichages réglés sur des hôtes locaux.
- Pour les postes de travail basés sur Solaris, un Sun exécutant Solaris 2.6, Solaris 7 ou Solaris 8.

Votre poste de travail doit disposer d'un navigateur Web pris en charge pour accéder à l'utilitaire de configuration et au Tableau de bord.

Le tableau suivant répertorie les navigateurs compatibles avec les versions 12.1, 13.0 et 13.1 de NetScaler GUI :

Système d'exploitation	Navigateur	Versions
Windows 10 et versions ultérieures	Bord	110.1587.63 et versions ultérieures
Windows 10 et versions ultérieures	Mozilla Firefox	102 et versions ultérieures
Windows 10 et versions ultérieures	Chrome	108 et versions ultérieures
MAC	Mozilla Firefox	10.0.1 et versions ultérieures
MAC	Safari	15.5 et versions ultérieures

Utiliser l'interface graphique de NetScaler

Une fois connecté à l'utilitaire de configuration, vous pouvez configurer l'appliance via une interface graphique qui inclut une aide contextuelle.

Pour vous connecter à l'interface graphique, procédez comme suit :

1. Ouvrez votre navigateur Web et entrez l'adresse IP NetScaler (NSIP) en tant qu'adresse HTTP. Si vous n'avez pas encore configuré la configuration initiale, entrez le NSIP (http://192.168.100.1) par défaut. La page de connexion à NetScaler s'affiche.

   Remarque : Si vous disposez de deux appliances NetScaler dans une configuration haute disponibilité, n'accédez pas à l'interface graphique en saisissant l'adresse IP de l'appliance NetScaler secondaire. Si vous le faites et que vous utilisez l'interface graphique pour configurer l'appliance secondaire, vos modifications de configuration ne sont pas appliquées à l'appliance NetScaler principale.

2. Dans la zone de texte Nom d'utilisateur, tapez `nsroot`.
3. Dans la zone de texte Mot de passe, saisissez le mot de passe administratif que vous avez attribué au `nsroot` compte lors de la configuration initiale et cliquez sur **Connexion**. Si ce mot de passe ne fonctionne pas, essayez de saisir le numéro de série de l'appliance. Le code à barres du numéro de série est disponible à l'arrière de l'appliance.

   Pour accéder à l'aide en ligne, sélectionnez Aide dans le menu Aide situé dans le coin supérieur droit.

Utiliser l'utilitaire statistique

Dashboard, l'utilitaire de statistiques, est une application basée sur un navigateur qui affiche des graphiques et des tableaux sur lesquels vous pouvez surveiller les performances d'une appliance NetScaler.

Pour vous connecter au Dashboard, procédez comme suit :

1. Ouvrez votre navigateur Web et saisissez le NSIP en tant qu'adresse HTTP. La page de connexion à NetScaler s'affiche.
2. Dans la zone de texte Nom d'utilisateur, tapez `nsroot`.
3. Dans la zone de texte Mot de passe, saisissez le mot de passe administratif que vous avez attribué au `nsroot` compte lors de la configuration initiale. Si ce mot de passe ne fonctionne pas, essayez de saisir le numéro de série de l'appliance. Le code à barres du numéro de série est disponible à l'arrière de l'appliance.

Configurer ADC pour la première fois

June 2, 2023

Pour la configuration initiale d'une appliance NetScaler MPX, voir Configuration initiale d'une appliance NetScalerMPX.

Pour la configuration initiale d'une appliance NetScaler SDX, voir Configuration initiale d'une appliance NetScalerSDX.

API NITRO

Vous pouvez utiliser l'API NITRO pour configurer l'appliance NetScaler. NITRO expose ses fonctionnalités via des interfaces REST (Representational State Transfer). Par conséquent, les applications NITRO peuvent être développées dans n'importe quel langage de programmation. En outre, pour les applications qui doivent être développées avec Java, .NET ou Python, les API NITRO sont exposées par le biais de bibliothèques pertinentes qui sont packagées en tant que kits de développement logiciel (SDK) séparés. Pour plus d'informations, voir API NITRO.

Sécurisez votre déploiement NetScaler

May 5, 2023

Pour maintenir la sécurité tout au long du cycle de vie du déploiement de l'appliance NetScaler, Citrix vous recommande de prendre en compte les aspects de sécurité suivants :

- Sécurité physique
- Sécurité des appareils
- Sécurité du réseau
- Administration et gestion

Différents déploiements peuvent nécessiter différentes considérations de sécurité. Les directives de déploiement sécurisé de NetScaler fournissent des conseils de sécurité généraux pour vous aider à choisir un déploiement sécurisé approprié en fonction de vos exigences de sécurité spécifiques.

Pour plus d'informations sur les directives relatives au déploiement sécurisé de l'appliance NetScaler, consultez les directives de déploiement sécurisé de NetScaler.

Configurer la haute disponibilité

May 8, 2023

Vous pouvez déployer deux appliances NetScaler dans une configuration haute disponibilité, dans laquelle une unité accepte activement les connexions et gère les serveurs tandis que l'unité secondaire surveille la première. L'appliance NetScaler qui accepte activement les connexions et gère les serveurs est appelée unité principale et l'autre unité est appelée unité secondaire dans

une configuration haute disponibilité. En cas de défaillance de l'unité principale, l'unité secondaire devient l'unité principale et commence à accepter activement les connexions.

Chaque appliance NetScaler d'une paire haute disponibilité surveille l'autre en envoyant des messages périodiques, appelés messages de pulsation ou bilans de santé, afin de déterminer la santé ou l'état du nœud homologue. Si une vérification de l'état d'une unité principale échoue, l'unité secondaire tente à nouveau la connexion pour une période spécifique. Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Si une nouvelle tentative ne réussit pas à la fin de la période spécifiée, l'unité secondaire prend le relais de l'unité principale dans un processus appelé basculement. La figure suivante montre deux configurations de haute disponibilité, l'une en mode à un bras et l'autre en mode à deux bras.

Figure 1. Haute disponibilité en mode monobras

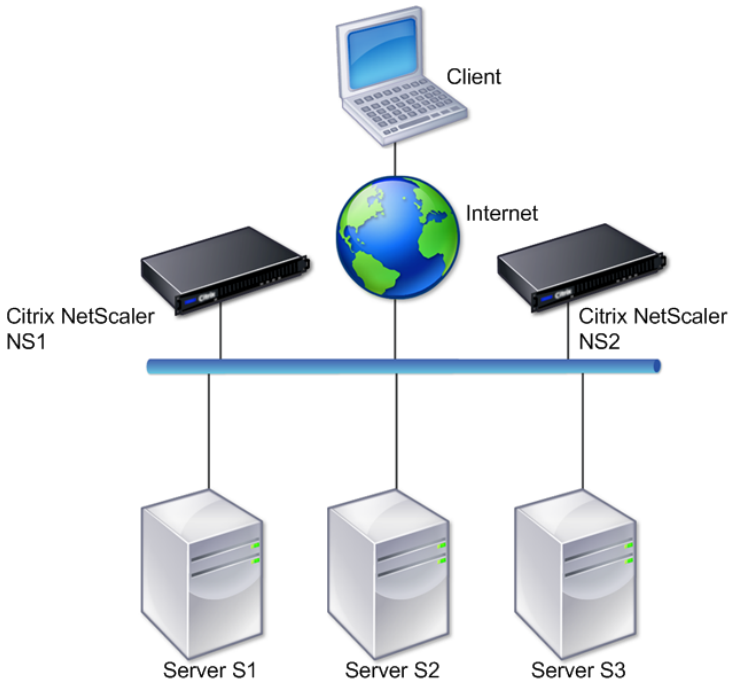
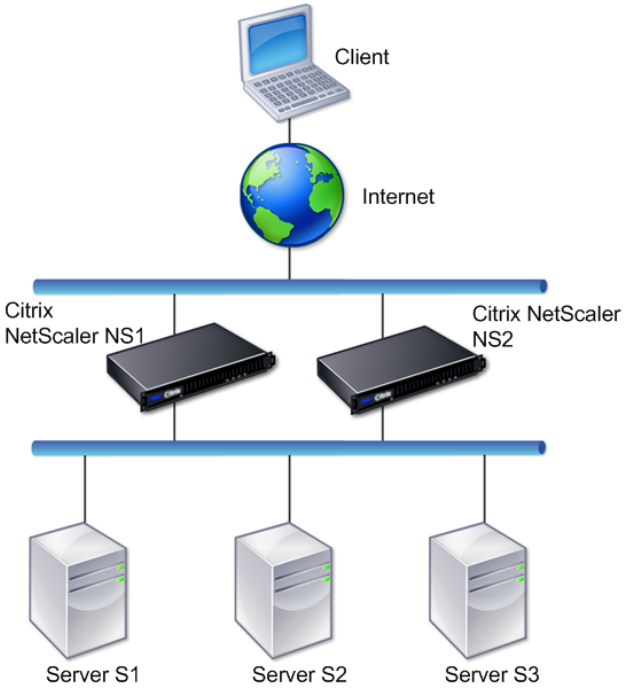


Figure 2. Haute disponibilité en mode deux bras



Dans une configuration à bras unique, NS1 et NS2 ainsi que les serveurs S1, S2 et S3 sont connectés au commutateur.

Dans une configuration à deux bras, le NS1 et le NS2 sont connectés à deux commutateurs. Les serveurs S1, S2 et S3 sont connectés au second commutateur. Le trafic entre le client et les serveurs passe par NS1 ou NS2.

Pour configurer un environnement de haute disponibilité, configurez une appliance ADC comme principale et une autre comme secondaire. Effectuez les tâches suivantes sur chacune des appliances ADC :

- Ajoutez un nœud.
- Désactivez la surveillance de la haute disponibilité pour les interfaces non utilisées.

Ajouter un nœud

Un nœud est une représentation logique d'une appliance NetScaler homologue. Il identifie l'unité homologue par ID et NSIP. Une appliance utilise ces paramètres pour communiquer avec l'homologue et suivre son état. Lorsque vous ajoutez un nœud, les unités principale et secondaire échangent des messages de pulsation de manière asynchrone. L'ID du nœud est un entier qui ne doit pas être supérieur à 64.

Par le biais de la CLI

Pour ajouter un nœud à l'aide de l'interface de ligne de commande, procédez comme suit :

À l'invite de commandes, tapez les commandes suivantes pour ajouter un nœud et vérifier que le nœud a bien été ajouté :

- ajouter un nœud HA \ <id> \ <IPAddress>
- afficher le nœud HA \ <id>

Exemple

```
add HA node 0 10.102.29.170
 Done
> show HA node 0
1)      Node ID:      0
        IP:   10.102.29.200 (NS200)
        Node State: UP
        Master State: Primary
        SSL Card Status: UP
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 1:0:41:50 (days:hrs:min:
           sec)
<!--NeedCopy-->
```

Grâce à l'interface graphique

Pour ajouter un nœud à l'aide de l'interface graphique, procédez comme suit :

1. Accédez à **Système** > **Haute disponibilité** .
2. Cliquez sur **Ajouter** dans l'onglet **Nœuds** .
3. Sur la page **Créer un nœud HA**, dans la zone de texte **Adresse IP du nœud distant**, tapez l'adresse NSIP (par exemple, 10.102.29.170) du nœud distant.
4. Assurez-vous que la case **Configurer le système distant pour qu'il participe à la configuration de la haute disponibilité** est cochée. Indiquez les informations de connexion du nœud distant dans les zones de texte situées sous Informations de **connexion au système distant**.
5. Cochez la case **Désactiver le moniteur HA sur les interfaces/canaux inactifs** pour désactiver le moniteur HA sur les interfaces inactives.

Vérifiez que le nœud que vous avez ajouté apparaît dans la liste des nœuds de l'onglet Nœuds.

Désactiver la surveillance de la haute disponibilité pour les interfaces non utilisées

Le moniteur de haute disponibilité est une entité virtuelle qui surveille une interface. Vous devez désactiver le moniteur pour les interfaces qui ne sont pas connectées ou qui ne sont pas utilisées pour le trafic. Lorsque le moniteur est activé sur une interface dont l'état est DOWN, l'état du nœud passe à NOT UP. Dans une configuration haute disponibilité, un nœud principal passant à l'état NOT UP peut provoquer un basculement en haute disponibilité. Une interface est marquée comme étant DÉSACTIVÉE dans les conditions suivantes :

- L'interface n'est pas connectée
- L'interface ne fonctionne pas correctement
- Le câble reliant l'interface ne fonctionne pas correctement

Par le biais de la CLI

Pour désactiver le moniteur de haute disponibilité pour une interface non utilisée à l'aide de l'interface de ligne de commande, procédez comme suit :

À l'invite de commandes, tapez les commandes suivantes pour désactiver le moniteur de haute disponibilité pour une interface non utilisée et vérifier qu'il est désactivé :

- désactiver l'interface \ <id> -HAmonitor
- afficher l'interface \ <id>

  Exemple

```
> set interface 1/8 -haMonitor OFF
 Done
> show interface 1/8
        Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
        flags=0x4000 <ENABLED, DOWN, down, autoneg, 802.1q>
        MTU=1514, native vlan=1, MAC=00:d0:68:15:fd:3d, downtime
           238h55m44s
        Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
                 throughput 0

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
           Muted(0)
        Bandwidth thresholds are not set.
<!--NeedCopy-->
```

  Lorsque le moniteur de haute disponibilité est désactivé pour une interface non utilisée, la sortie de la commande show interface pour cette interface n'inclut pas « HAMON ». «

Grâce à l'interface graphique

Pour désactiver le moniteur de haute disponibilité pour les interfaces non utilisées à l'aide de l'interface graphique, procédez comme suit :

1. Accédez à Système > Réseau > Interfaces.
2. Sélectionnez l'interface pour laquelle le moniteur doit être désactivé.
3. Cliquez sur Ouvrir. La boîte de dialogue Modifier l'interface s'affiche.
4. Dans HA Monitoring, sélectionnez l'option OFF.
5. Cliquez sur OK.
6. Vérifiez que, lorsque l'interface est sélectionnée, « Surveillance HA : OFF » apparaît dans les détails en bas de la page.

Modifier le mot de passe d'un nœud RPC

May 5, 2023

Pour communiquer avec d'autres appliances NetScaler, chaque appliance doit connaître les autres appliances, notamment comment s'authentifier sur l'appliance NetScaler. Les nœuds RPC sont des entités système internes utilisées pour la communication système à système des informations de configuration et de session. Un nœud RPC existe sur chaque appliance NetScaler et stocke des informations, telles que les adresses IP de l'autre appliance NetScaler et les mots de passe utilisés pour l'authentification. L'appliance NetScaler qui contacte l'autre appliance NetScaler vérifie le mot de passe dans le nœud RPC.

> **Remarque :**
>
> Après la mise à niveau d'une appliance NetScaler vers la version 13.1 build 33.x ou ultérieure à partir de l'une des versions suivantes, l' `secure` option pour le nœud RPC est activée ou désactivée en fonction du paramètre TLS 1.2 (activé ou désactivé) présent pour les services RPCS et KRPCS internes.
>
> - Version 13.0 build 64.35 ou antérieure
> - Version 12.1 build 61.18 ou antérieure
>
> La communication RPC est cryptée entre les nœuds NetScaler des configurations suivantes si l'option est activée : `Secure`
>
> - Haute disponibilité
> - Cluster :
> - GSLB
>
> L' `secure` option utilise le protocole sécurisé TLS1.2 et les numéros de port 3008 et 3009 pour la

connexion RPC entre les nœuds NetScaler.

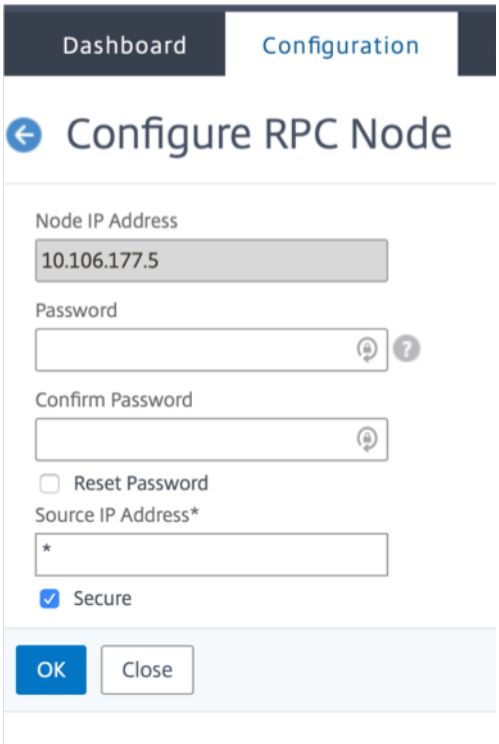
Pour garantir la sécurité des communications RPC, Citrix recommande d'effectuer les opérations suivantes avant de mettre à niveau ces configurations :

- Le protocole TLS 1.2 doit être activé pour les services internes du RPC et du KRPCS :
  - `nsrpcs-127.0.0.1-3008`
  - `nskrpcs-127.0.0.1-3009`
  - `nsrpcs-::1l-3008`
- Les versions 3008 et 3009 doivent être débloquées dans les pare-feux situés entre les nœuds NetScaler.

Vous pouvez activer ou désactiver `secure` cette option à l'aide de la CLI NetScaler ou de l'interface graphique.

Pour modifier le mot de passe d'un nœud RPC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **RPC.**
2. Dans le volet **RPC**, sélectionnez le nœud, puis cliquez sur **Modifier**.
3. Dans **Configurer le nœud RPC**, tapez le nouveau mot de passe.
4. Dans **Adresse IP source**, tapez l'adresse IP du nœud existant à utiliser pour communiquer avec le nœud du système homologue.



5. Sélectionnez **Sécurisé**, puis cliquez sur **OK**.

> **Remarque**
>
> Pour renforcer la sécurité, Citrix vous recommande d'activer l'option **Secure** sur les nœuds RPC. Lorsque vous activez l'option **Secure**, l'appliance chiffre toutes les communications RPC envoyées d'un nœud ADC vers d'autres nœuds ADC, sécurisant ainsi la communication RPC. Cette communication sécurisée utilise le port numéro 3008. Si le pare-feu entre les nœuds ADC bloque le port numéro 3008, débloquez-le et continuez. Sinon, la synchronisation et la propagation de la configuration risquent d'échouer.

Pour modifier le mot de passe d'un nœud RPC à l'aide de l'interface de ligne de commande

Sur la ligne de commande, saisissez les commandes suivantes :

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]
show ns rpcNode
<!--NeedCopy-->
```

Exemple :

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>

<!--NeedCopy-->
```

Configurez un dispositif FIPS pour la première fois

May 5, 2023

> **Remarque**
>
> - La FAQ FIPS se trouve ici : FAQ FIPS.

Une paire de clés de certificat est requise pour l'accès HTTPS à l'utilitaire de configuration et pour les appels de procédure distante sécurisés. Les nœuds RPC sont des entités système internes utilisées pour la communication système à système des informations de configuration et de session. Un nœud RPC existe sur chaque appliance. Ce nœud stocke le mot de passe, qui est vérifié par rapport à celui fourni par l'appliance de contact. Pour communiquer avec d'autres appliances NetScaler, chaque appliance doit connaître les autres appliances, notamment comment s'authentifier sur l'autre appliance. Les nœuds RPC conservent ces informations, qui incluent les adresses IP des autres appliances NetScaler et les mots de passe utilisés pour s'authentifier sur chacune d'elles.

Sur une appliance virtuelle NetScaler MPX, une paire de clés de certificat est automatiquement liée aux services internes. Sur une appliance FIPS, une paire de clés de certificat doit être importée dans le module de sécurité matérielle (HSM) d'une carte FIPS. Pour ce faire, vous devez configurer la carte FIPS, créer une paire de clés de certificat et la lier aux services internes.

Configurez le protocole HTTPS sécurisé à l'aide de l'interface

Pour configurer un HTTPS sécurisé à l'aide de l'interface de ligne de commande, procédez comme suit

1. Initialisez le module de sécurité matérielle (HSM) sur la carte FIPS de l'appliance. Pour plus d'informations sur l'initialisation du HSM, consultez l'un des liens suivants :
   - Pour MPX : configurez le HSM.
   - Pour SDX : configurez le HSM pour une instance sur une appliance FIPS SDX 14030/14060/14080.
2. Si l'appliance fait partie d'une configuration de haute disponibilité, activez la carte SIM. Pour plus d'informations sur l'activation de la carte SIM sur les appliances principale et secondaire, voir Configurer les appliances FIPS dans une configuration haute disponibilité.
3. Importez la clé FIPS dans le HSM de la carte FIPS de l'appliance. À l'invite de commande, tapez :

   ```
   import ssl fipskey serverkey -key ns-server.key -inform PEM
   ```

4. Ajoutez une paire de clés de certificat. À l'invite de commande, tapez :

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. Liez la clé de certificat créée à l'étape précédente aux services internes suivants. À l'invite de commande, tapez :

   ```
   bind ssl service nshttps-127.0.0.1-443 -certkeyname server

   bind ssl service nshttps-::11-443 -certkeyname server
   ```


Configurez le HTTPS sécurisé à l'aide de l'interface graphique

Pour configurer le protocole HTTPS sécurisé à l'aide de l'interface graphique, procédez comme suit :

1. Initialisez le module de sécurité matérielle (HSM) sur la carte FIPS de l'appliance. Pour plus d'informations sur l'initialisation du HSM, consultez l'un des liens suivants :
   - Pour MPX : configurez le HSM.
   - Pour SDX : configurez le HSM pour une instance sur une appliance FIPS SDX 14030/14060/14080.
2. Si l'appliance fait partie d'une configuration de haute disponibilité, activez le système d'information sécurisé (SIM). Pour plus d'informations sur l'activation de la carte SIM sur les appliances principale et secondaire, voir Configurer les appliances FIPS dans une configuration haute disponibilité.
3. Importez la clé FIPS dans le HSM de la carte FIPS de l'appliance. Pour plus d'informations sur l'importation d'une clé FIPS, reportez-vous à la section Importer une clé FIPS existante .
4. Accédez à **Gestion du trafic > SSL > Certificats**.
5. Dans le volet d'informations, cliquez sur Installer.
6. Dans la boîte de dialogue Install Certificate, saisissez les détails du certificat.
7. Cliquez sur Créer, puis sur Fermer.
8. Accédez à **Traffic Management > Load Balancing > Services**.
9. Dans le volet de détails, sous l'onglet Action, cliquez sur Services internes.
10. Sélectionnez dans `nshttps-127.0.0.1-443` la liste, puis cliquez sur Ouvrir.
11. Dans l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis sur OK.
12. Sélectionnez dans `nshttps-::1-443` la liste, puis cliquez sur Ouvrir.
13. Dans l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis sur OK.
14. Cliquez sur OK.

Configurer un RPC sécurisé à l'aide de la CLI

Pour configurer un RPC sécurisé à l'aide de l'interface de ligne de commande, procédez comme suit :

1. Initialisez le module de sécurité matérielle (HSM) sur la carte FIPS de l'appliance. Pour plus d'informations sur l'initialisation du HSM, consultez l'un des liens suivants :
   - Pour MPX : configurez le HSM.
   - Pour SDX : configurez le HSM pour une instance sur une appliance FIPS SDX 14030/14060/14080.
2. Activez le système d'information sécurisé (SIM). Pour plus d'informations sur l'activation de la carte SIM sur les appliances principale et secondaire, voir Configurer les appliances FIPS dans une configuration haute disponibilité.
3. Importez la clé FIPS dans le HSM de la carte FIPS de l'appliance. À l'invite de commande, tapez :


```
import ssl fipskey serverkey -key ns-server.key -inform PEM
```

4. Ajoutez une paire de clés de certificat. À l'invite de commande, tapez :

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. Liez la paire de clés de certificat aux services internes suivants. À l'invite de commande, tapez :

   ```
   bind ssl service nsrpcs-127.0.0.1-3008 -certkeyname server

   bind ssl service nskrpcs-127.0.0.1-3009 -certkeyname server

   bind ssl service nsrpcs-::1l-3008 -certkeyname server
   ```

6. Activez le mode RPC sécurisé. À l'invite de commande, tapez :

   ```
   set ns rpcnode \<IP address\> -secure YES
   ```

   Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.

Configurer RPC sécurisé à l'aide de l'interface graphique

Pour configurer un RPC sécurisé à l'aide de l'interface graphique, procédez comme suit :

1. Initialisez le module de sécurité matérielle (HSM) sur la carte FIPS de l'appliance. Pour plus d'informations sur l'initialisation du HSM, consultez l'un des liens suivants :
   - Pour MPX : configurez le HSM.
   - Pour SDX : configurez le HSM pour une instance sur une appliance FIPS SDX 14030/14060/14080.
2. Activez le système d'information sécurisé (SIM). Pour plus d'informations sur l'activation de la carte SIM sur les appliances principale et secondaire, Configurez les appliances FIPS dans une configuration haute disponibilité.
3. Importez la clé FIPS dans le HSM de la carte FIPS de l'appliance. Pour plus d'informations sur l'importation d'une clé FIPS, consultez la section Importer une clé FIPS existante .
4. Accédez à **Gestion du trafic > SSL > Certificats**.
5. Dans le volet d'informations, cliquez sur Installer.
6. Dans la boîte de dialogue Install Certificate, saisissez les détails du certificat.
7. Cliquez sur Créer, puis sur Fermer.
8. Accédez à **Traffic Management > Load Balancing > Services**.
9. Dans le volet de détails, sous l'onglet Action, cliquez sur Services internes.
10. Sélectionnez nsrpcs-127.0.0.1-3008 dans la liste, puis cliquez sur Ouvrir.
11. Dans l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis sur OK.
12. Sélectionnez nskrpcs-127.0.0.1-3009 dans la liste, puis cliquez sur Ouvrir.
13. Dans l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis sur OK.

14. Sélectionnez dans `nsrpcs-::11-3008` la liste, puis cliquez sur Ouvrir.
15. Dans l'onglet Paramètres SSL, dans le volet Disponible, sélectionnez le certificat créé à l'étape 7, cliquez sur Ajouter, puis sur OK.
16. Cliquez sur OK.
17. Accédez à **Système > Réseau > RPC**.
18. Dans le volet d'informations, sélectionnez l'adresse IP, puis cliquez sur Ouvrir.
19. Dans la boîte de dialogue Configurer le nœud RPC, sélectionnez Sécurisé.
20. Cliquez sur OK.

Topologies réseau communes

May 5, 2023

Comme décrit dans la section « Mode de déploiement physique » de la section Où s'intègre une appliance NetScaler dans leréseau ? , vous pouvez déployer l'appliance NetScaler soit en ligne entre les clients et les serveurs, soit en mode monobras. Le mode Inline utilise une topologie à deux bras, qui est le type de déploiement le plus courant.

Configuration d'une topologie commune à deux bras

Dans une topologie à deux bras, une interface réseau est connectée au réseau client et une autre interface réseau est connectée au réseau du serveur, garantissant ainsi que tout le trafic transite par l'appliance. Cette topologie peut vous obliger à reconnecter votre matériel et peut également entraîner une interruption momentanée. Les variantes de base de la topologie à deux bras sont les sous-réseaux multiples, généralement avec l'appliance sur un sous-réseau public et les serveurs sur un sous-réseau privé, et le mode transparent, avec l'appliance et les serveurs sur le réseau public.

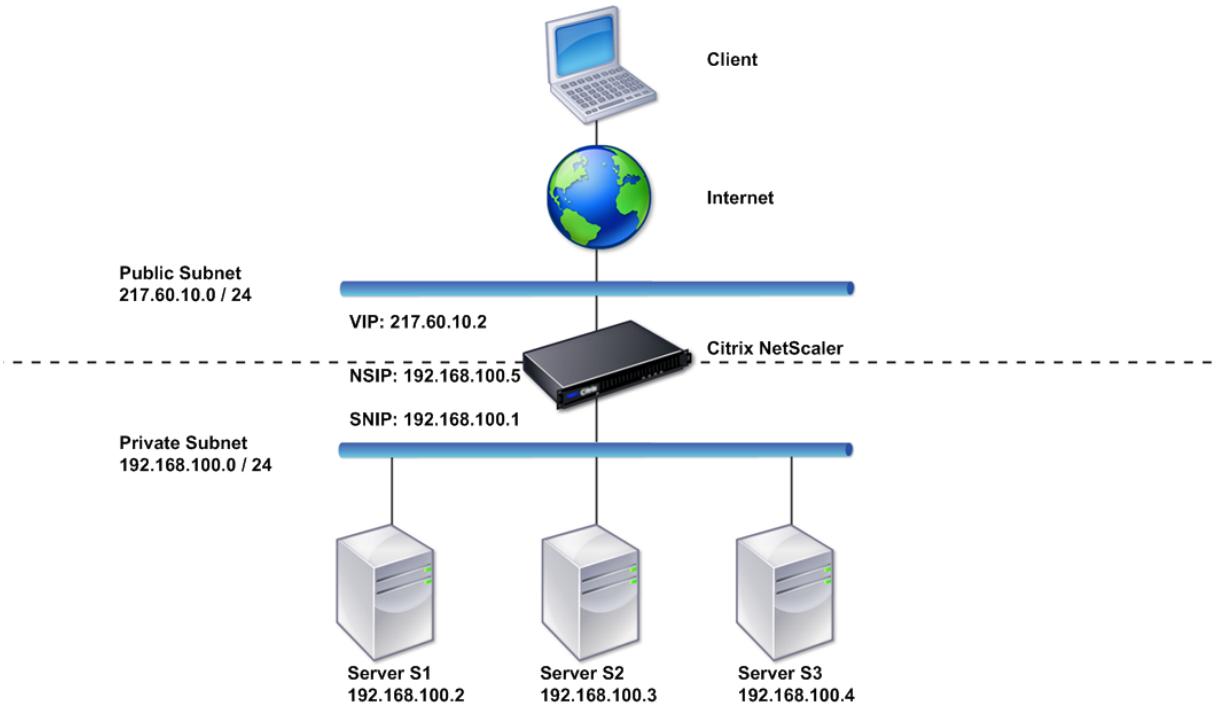
Configuration d'une topologie simple à deux bras et à sous-réseaux multiples

L'une des topologies les plus couramment utilisées intègre l'appliance NetScaler entre les clients et les serveurs, avec un serveur virtuel configuré pour gérer les demandes des clients. Cette configuration est utilisée lorsque les clients et les serveurs résident sur des sous-réseaux différents. Dans la plupart des cas, les clients et les serveurs résident respectivement sur des sous-réseaux publics et privés.

Prenons l'exemple d'une appliance déployée en mode à deux bras pour gérer les serveurs S1, S2 et S3, avec un serveur virtuel de type HTTP configuré sur l'appliance et avec des services HTTP exécutés sur les serveurs. Les serveurs se trouvent sur un sous-réseau privé et un SNIP est configuré sur l'appliance pour communiquer avec les serveurs. L'option Utiliser le SNIP (USNIP) doit être activée sur l'appliance afin qu'elle utilise le SNIP au lieu du MIP.

Comme le montre la figure suivante, le VIP se trouve sur le sous-réseau public 217.60.10.0 et le NSIP, les serveurs et le SNIP se trouvent sur le sous-réseau privé 192.168.100.0/24.

Figure 1. Diagramme de topologie pour le mode à deux bras, plusieurs sous-réseaux



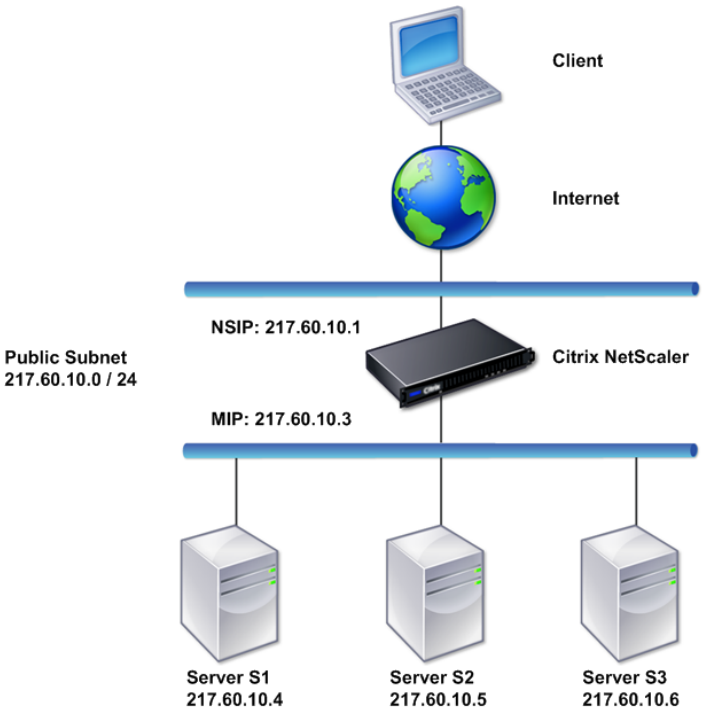
Pour déployer une appliance NetScaler en mode à deux bras avec plusieurs sous-réseaux, procédez comme suit :

1. Configurez le NSIP et la passerelle par défaut, comme décrit dans Configuration de l'adresse IP NetScaler (NSIP).
2. Configurez le SNIP, comme décrit dans Configuration des adresses IP de sous-réseau.
3. Activez l'option USNIP, comme décrit dans la section Pour activer ou désactiver le mode USNIP .
4. Configurez le serveur virtuel et les services, comme décrit dans la section Création d'un serveur virtuel et la section Configuration des services .
5. Connectez l'une des interfaces réseau à un sous-réseau privé et l'autre interface à un sous-réseau public.

Configurez une topologie transparente simple à deux bras

Utilisez le mode transparent si les clients ont besoin d'accéder directement aux serveurs, sans qu'aucun serveur virtuel n'intervienne. Les adresses IP du serveur doivent être publiques car les clients doivent pouvoir y accéder. Dans l'exemple illustré dans la figure suivante, une appliance NetScaler est placée entre le client et le serveur, de sorte que le trafic doit passer par l'appliance. Vous devez activer le mode L2 pour relier les paquets. Le NSIP et le MIP se trouvent sur le même sous-réseau public, 217.60.10.0/24.

Figure 2. Diagramme topologique pour le mode transparent à deux bras



Pour déployer une appliance NetScaler en mode transparent à deux bras, procédez comme suit

1. Configurez le NSIP et la passerelle par défaut, comme décrit dans Configuration de l'adresse IP NetScaler (NSIP).
2. Activez le mode L2, comme décrit dans Activation et désactivation du mode de couche 2.
3. Configurez la Gateway par défaut des serveurs gérés en tant que MIP.
4. Connectez les interfaces réseau aux ports appropriés du commutateur.

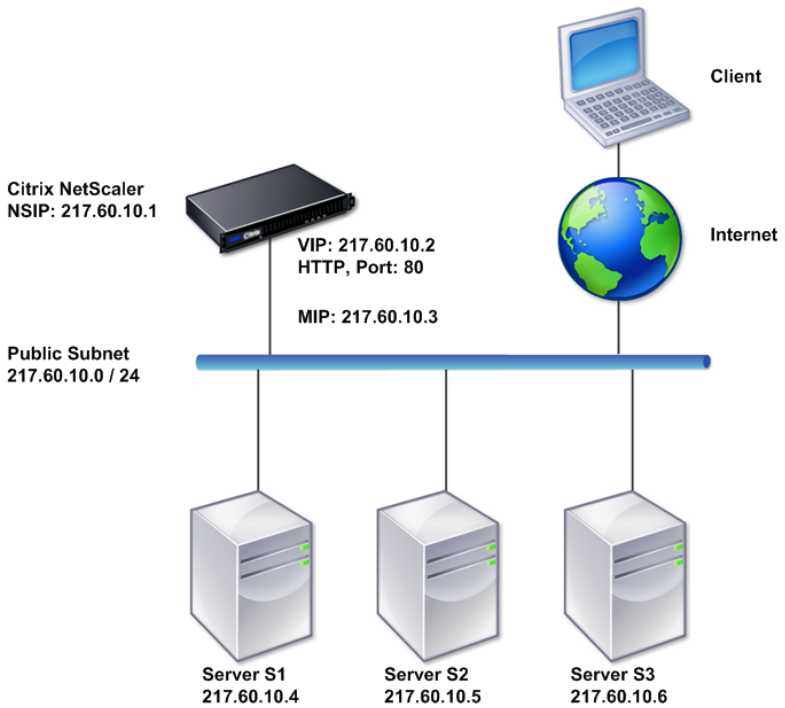
Configurez des topologies à bras unique communes

Les deux variantes de base de la topologie à un bras concernent un seul sous-réseau et plusieurs sous-réseaux.

Configuration d'une topologie de sous-réseau simple à un seul bras

Vous pouvez utiliser une topologie à bras unique avec un seul sous-réseau lorsque les clients et les serveurs résident sur le même sous-réseau. Prenons l'exemple d'une appliance NetScaler déployée en mode monobras pour gérer les serveurs S1, S2 et S3. Un serveur virtuel de type HTTP est configuré sur une appliance ADC et les services HTTP s'exécutent sur les serveurs. Comme le montre la figure suivante, l'adresse IP NetScaler (NSIP), l'adresse IP mappée (MIP) et les adresses IP du serveur se trouvent sur le même sous-réseau public, 217.60.10.0/24.

Figure 3. Diagramme de topologie pour le mode à bras unique, sous-réseau unique



Pour déployer une appliance NetScaler en mode monobras avec un seul sous-réseau, procédez comme suit :

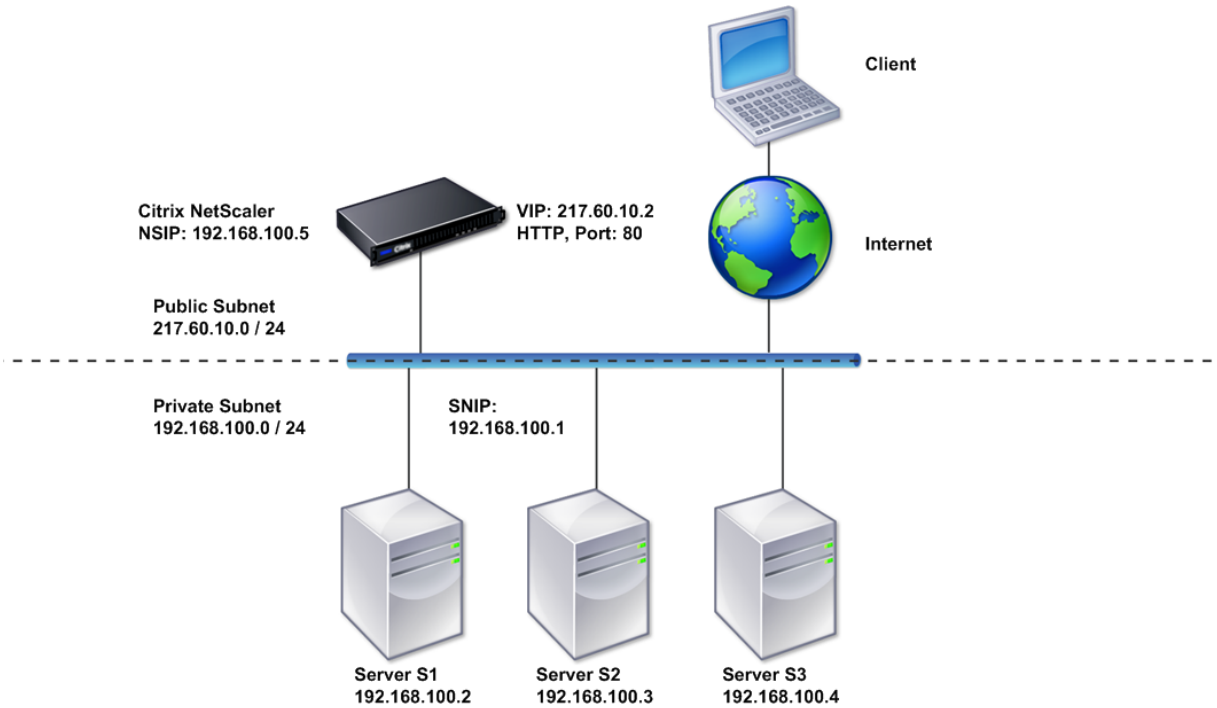
1. Configurez le NSIP et la passerelle par défaut, comme décrit dans, comme décrit dans Configuration de l'adresse IP NetScaler (NSIP).

2. Configurez le serveur virtuel et les services, comme décrit dans la section Création d'un serveur virtuel et la section Configuration des services .
3. Connectez l'une des interfaces réseau au commutateur.

Configuration d'une topologie simple à un bras et à plusieurs sous-réseaux

Vous pouvez utiliser une topologie à bras unique avec plusieurs sous-réseaux lorsque les clients et les serveurs résident sur les différents sous-réseaux. Prenons l'exemple d'une appliance NetScaler déployée en mode monobras pour gérer les serveurs S1, S2 et S3, les serveurs étant connectés au commutateur SW1 du réseau. Un serveur virtuel de type HTTP est configuré sur l'appliance et les services HTTP s'exécutent sur les serveurs. Ces trois serveurs se trouvent sur le sous-réseau privé, c'est pourquoi une adresse IP de sous-réseau (SNIP) est configurée pour communiquer avec eux. L'option Utiliser l'adresse IP du sous-réseau (USNIP) doit être activée pour que l'appliance utilise le SNIP au lieu d'un MIP. Comme le montre la figure suivante, l'adresse IP virtuelle (VIP) se trouve sur le sous-réseau public 217.60.10.0/24 ; les adresses IP NSIP, SNIP et du serveur se trouvent sur le sous-réseau privé 192.168.100.0/24.

Figure 4. Diagramme de topologie pour le mode à bras unique, plusieurs sous-réseaux



Pour déployer une appliance NetScaler en mode monobras avec plusieurs sous-réseaux, procédez

comme suit :

1. Configurez le NSIP et la passerelle par défaut, comme décrit dans Configuration de l'adresse IP NetScaler (NSIP).
2. Configurez le SNIP et activez l'option USNIP, comme décrit dans Configuration des adresses IP de sous-réseau.
3. Configurez le serveur virtuel et les services, comme décrit dans la section Création d'un serveur virtuel et la section Configuration des services .
4. Connectez l'une des interfaces réseau au commutateur.

Paramètres de gestion du système

May 5, 2023

Une fois votre configuration initiale en place, vous pouvez configurer les paramètres pour définir le comportement de l'appliance NetScaler et faciliter la gestion des connexions. Vous disposez d'un certain nombre d'options pour gérer les requêtes et les réponses HTTP. Les modes de routage, de pontage et de transfert basés sur MAC sont disponibles pour gérer les paquets non adressés à l'appliance NetScaler. Vous pouvez définir les caractéristiques de vos interfaces réseau et les agréger. Pour éviter les problèmes de synchronisation, vous pouvez synchroniser l'horloge Citrix avec un serveur NTP (Network Time Protocol). L'appliance NetScaler peut fonctionner dans différents modes DNS, notamment en tant que serveur de noms de domaine (ADNS) faisant autorité. Vous pouvez configurer le protocole SNMP pour la gestion du système et personnaliser la journalisation des événements système par Syslog. Avant le déploiement, vérifiez que votre configuration est complète et correcte.

Paramètres système

May 5, 2023

La configuration des paramètres système inclut des tâches de base telles que la configuration des ports HTTP pour permettre le maintien de la connexion et le déchargement du serveur, la définition du nombre maximum de connexions pour chaque serveur et la définition du nombre maximum de demandes par connexion. Vous pouvez activer l'insertion de l'adresse IP du client dans les cas où une adresse IP proxy ne convient pas, et vous pouvez modifier la version du cookie HTTP.

Vous pouvez également configurer une appliance NetScaler pour ouvrir des connexions FTP sur une plage contrôlée de ports plutôt que sur des ports éphémères pour les connexions de données. Cela améliore la sécurité, car l'ouverture de tous les ports du pare-feu n'est pas sécurisée. Vous pouvez définir la plage entre 1 024 et 64 000.

Avant le déploiement, parcourez les listes de vérification pour vérifier votre configuration. Pour configurer les paramètres HTTP et la plage de ports FTP, utilisez l'interface graphique NetScaler.

Vous pouvez modifier les types de paramètres HTTP décrits dans le tableau suivant.

Type de paramètre : Informations sur le port HTTP

Spécifie : Les ports HTTP du serveur Web utilisés par vos serveurs gérés. Si vous spécifiez les ports, l'appliance effectue une commutation de demande pour toute demande client dont le port de destination correspond à un port spécifié.

> Remarque : Si une demande client entrante n'est pas destinée à un service ou à un serveur virtuel spécifiquement configuré sur l'appliance, le port de destination de la demande doit correspondre à l'un des ports HTTP configurés globalement. Cela permet à l'appliance de maintenir la connexion et de décharger le serveur.

Type de paramètre : Limites

Spécifie : le nombre maximum de connexions à chaque serveur géré et le nombre maximum de demandes envoyées via chaque connexion. Par exemple, si vous définissez le nombre maximum de connexions sur 500 et que l'appliance gère trois serveurs, elle peut ouvrir un maximum de 500 connexions à chacun des trois serveurs. Par défaut, l'appliance peut créer un nombre illimité de connexions à tous les serveurs qu'elle gère. Pour spécifier un nombre illimité de demandes par connexion, définissez le nombre maximum de demandes sur 0.

> Remarque : Si vous utilisez le serveur HTTP Apache, vous devez définir Max Connections comme étant égal à la valeur du paramètre MaxClients dans le fichier Apache httpd.conf. La définition de ce paramètre est facultative pour les autres serveurs Web.

Type de paramètre : Insertion IP du client

Spécifie : Activer/désactiver l'insertion de l'adresse IP du client dans l'en-tête de requête HTTP. Vous pouvez spécifier un nom pour le champ d'en-tête dans la zone de texte adjacente. Lorsqu'un serveur Web géré par une appliance reçoit une adresse IP de sous-réseau, le serveur l'identifie comme étant l'adresse IP du client. Certaines applications ont besoin de l'adresse IP du client à des fins de journalisation ou pour déterminer dynamiquement le contenu à diffuser par le serveur Web.

Vous pouvez activer l'insertion de l'adresse IP réelle du client dans la demande d'en-tête HTTP envoyée par le client à un, à certains ou à tous les serveurs gérés par l'appliance. Vous pouvez ensuite accéder à l'adresse insérée en apportant une modification mineure au serveur (à l'aide d'un module Apache, d'une interface ISAPI ou d'une interface NSAPI).

Type de paramètre : Version du cookie

Spécifie : La version du cookie HTTP à utiliser lorsque la persistance de COOKIEINSERT est configurée sur un serveur virtuel. La version par défaut, la version 0, est le type le plus courant sur Internet. Vous pouvez également spécifier la version 1.

Type de paramètre : Demandes/Réponses

Spécifie : Options permettant de gérer certains types de demandes et d'activer/désactiver la journalisation des réponses d'erreur HTTP.

Type de paramètre : Insertion d'en-tête de serveur

Spécifie : insérez un en-tête de serveur dans les réponses HTTP générées par Netscaler.

Pour configurer les paramètres HTTP à l'aide de l'interface graphique, procédez comme suit :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres HTTP**.
3. Dans la boîte de dialogue **Configurer les paramètres HTTP**, spécifiez les valeurs de certains ou de tous les paramètres qui apparaissent sous les titres répertoriés dans le tableau ci-dessus.
4. Cliquez sur **OK**.

Pour définir la plage de ports FTP à l'aide de l'interface graphique, procédez comme suit :

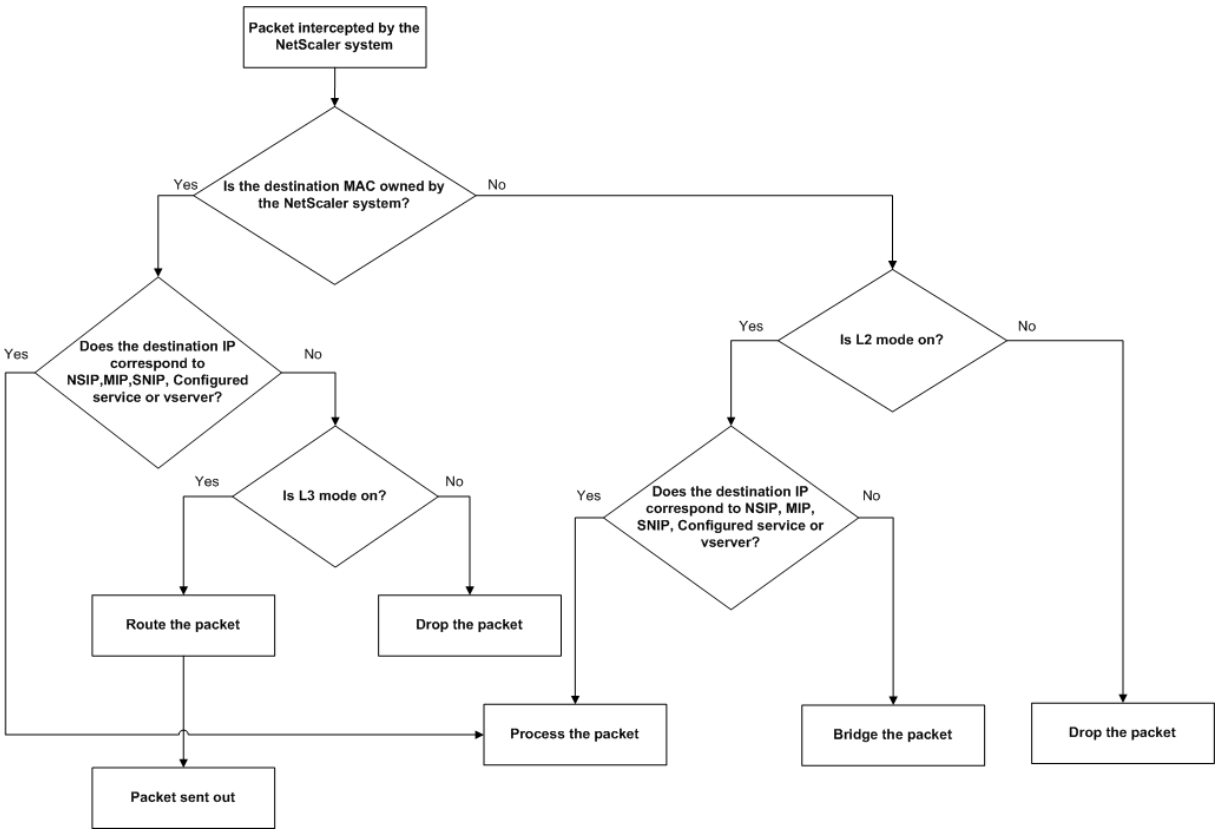
1. Dans le volet de navigation, ouvrez **Système**, puis cliquez sur **Paramètres**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux du système**.
3. Sous **Plage de ports FTP,** dans les zones de texte **Port de départ** et **Port de fin**, tapez les numéros de port le plus bas et le plus élevé, respectivement, pour la plage que vous souhaitez spécifier (par exemple, 5000 et 6000).
4. Cliquez sur **OK**.

Modes de transfert de paquets

May 5, 2023

L'appliance NetScaler peut acheminer ou relier des paquets qui ne sont pas destinés à une adresse IP appartenant à l'appliance (c'est-à-dire que l'adresse IP n'est pas le NSIP, un MIP, un SNIP, un service configuré ou un serveur virtuel configuré). Par défaut, le mode L3 (routage) est activé et le mode L2 (pontage) est désactivé, mais vous pouvez modifier la configuration. L'organigramme suivant montre comment l'appliance évalue les paquets et les traite, les achemine, les relie ou les supprime.

Figure 1. Interaction entre les modes de couche 2 et de couche 3



Une appliance peut utiliser les modes suivants pour transférer les paquets qu'elle reçoit :

- Mode couche 2 (L2)
- Mode couche 3 (L3)
- Mode de transfert basé sur Mac

Activer et désactiver le mode couche 2

Le mode de couche 2 contrôle la fonction de transfert (pontage) de la couche 2. Vous pouvez utiliser ce mode pour configurer une appliance NetScaler afin qu'elle se comporte comme un périphérique de couche 2 et qu'elle relie les paquets qui ne lui sont pas destinés. Lorsque ce mode est activé, les paquets ne sont transférés vers aucune des adresses MAC, car les paquets peuvent arriver sur n'importe quelle interface de l'appliance et chaque interface possède sa propre adresse MAC.

Lorsque le mode de couche 2 est désactivé (ce qui est la valeur par défaut), l'appliance supprime les paquets qui ne sont pas destinés à l'une de ses adresses MAC. Si un autre périphérique de couche 2 est installé en parallèle avec l'appliance, le mode de couche 2 doit être désactivé pour empêcher les boucles de pontage (couche 2). Vous pouvez utiliser l'utilitaire de configuration ou la ligne de commande pour activer le mode de couche 2.

Remarque : L'appliance ne prend pas en charge le protocole Spanning Tree. Pour éviter les boucles, si vous activez le mode L2, ne connectez pas deux interfaces de l'appliance au même domaine de

diffusion.

Pour activer ou désactiver le mode de couche 2 à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour activer/désactiver le mode de couche 2 et vérifier qu'il a été activé/désactivé :

- enable ns mode <Mode>
- disable ns mode <Mode>
- show ns mode

Exemples

```
    > enable ns mode l2
    Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 ON
    .
    .
    .
    Done
    >

    > disable ns mode l2
    Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 OFF
    .
    .
    .
    Done
    >
<!--NeedCopy-->
```

Pour activer ou désactiver le mode de couche 2 à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.

2. Dans le volet d'informations, sous **Modes** et **fonctionnalités**, cliquez sur **Configurer les modes**.
3. Dans la boîte de dialogue **Configurer les modes**, pour activer le mode de couche 2, activez la case à cocher **Mode de couche 2** . Pour désactiver le mode de couche 2, désactivez la case à cocher.
4. Cliquez sur **OK**. Le message **Enable/Disable Mode(s)?** s'affiche dans le volet d'informations.
5. Cliquez sur **Oui**.

Activer et désactiver le mode couche 3

Le mode de couche 3 contrôle la fonction de transfert de la couche 3. Vous pouvez utiliser ce mode pour configurer une appliance NetScaler afin qu'elle examine sa table de routage et transfère les paquets qui ne lui sont pas destinés. Lorsque le mode de couche 3 est activé (ce qui est le mode par défaut), l'appliance effectue des recherches de table de routage et transmet tous les paquets qui ne sont destinés à aucune adresse IP appartenant à l'appliance. Si vous désactivez le mode de couche 3, l'appliance supprime ces paquets.

Activer ou désactiver le mode de couche 3 à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour activer/désactiver le mode de couche 3 et vérifier qu'il a été activé/désactivé :

- enable ns mode <Mode>
- disable ns mode <Mode>
- show ns mode

Exemples

```
> enable ns mode l3
Done
> show ns mode

Mode Acronym Status
------- ------- ------
1) Fast Ramp FR ON
2) Layer 2 mode L2 OFF
.
.
.
9) Layer 3 mode (ip forwarding) L3 ON
.
.
```



```
15      .
16      Done
17      >
18
19      > disable ns mode l3
20      Done
21      > show ns mode
22
23      Mode Acronym Status
24      ------- ------- ------
25      1) Fast Ramp FR ON
26      2) Layer 2 mode L2 OFF
27      .
28      .
29      .
30      9) Layer 3 mode (ip forwarding) L3 OFF
31      .
32      .
33      .
34      Done
35      >
36  <!--NeedCopy-->
```

Activer ou désactiver le mode de couche 3 à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Dans le volet d'informations, sous **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.
3. Dans la boîte de dialogue **Configurer les modes**, pour activer le mode de couche 3, activez la case à cocher **Mode de couche 3 (transfert IP)** . Pour désactiver le mode de couche 3, désactivez la case à cocher.
4. Cliquez sur **OK**. Le message **Enable/Disable Mode(s)?** s'affiche dans le volet d'informations.
5. Cliquez sur **Oui**.

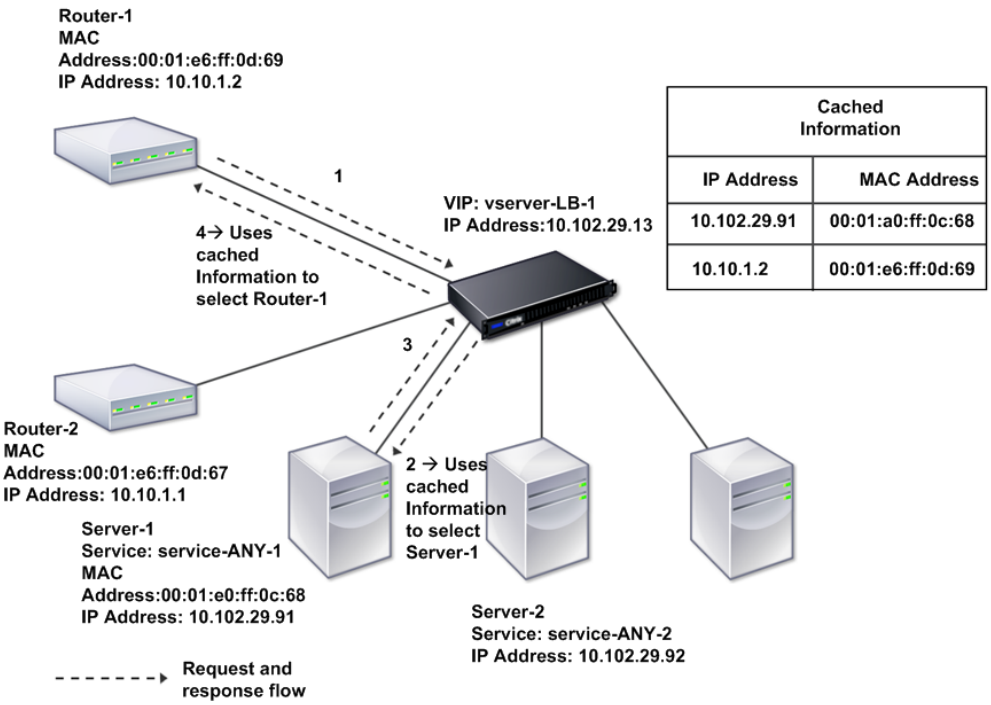
Activer et désactiver le mode de transfert basé sur Mac

Vous pouvez utiliser le transfert basé sur MAC pour traiter le trafic plus efficacement et éviter les recherches sur plusieurs itinéraires ou ARP lors du transfert de paquets, car l'appliance NetScaler mémorise l'adresse MAC de la source. Pour éviter les recherches multiples, l'appliance met en cache l'adresse MAC source de chaque connexion pour laquelle elle effectue une recherche ARP et renvoie les données à la même adresse MAC.

Le transfert basé sur Mac est utile lorsque vous utilisez des périphériques VPN, car l'appliance garantit que tout le trafic passant par un VPN particulier passe par le même périphérique VPN.

La figure suivante montre le processus de transfert basé sur Mac.

Figure 2. Processus de transfert basé sur Mac



Lorsque le transfert basé sur MAC est activé, l'appliance met en cache l'adresse MAC des éléments suivants :

- La source (un périphérique de transmission tel qu'un routeur, un pare-feu ou un périphérique VPN) de la connexion entrante.
- Le serveur qui répond aux demandes.

Lorsqu'un serveur répond par l'intermédiaire d'un appareil, l'appliance définit l'adresse MAC de destination du paquet de réponse sur l'adresse mise en cache, garantissant ainsi que le trafic circule de manière symétrique, puis transmet la réponse au client. Le processus contourne les fonctions de recherche de table de routage et de recherche ARP. Toutefois, lorsqu'une appliance initie une connexion, elle utilise les tables ARP et la route pour la fonction de recherche. Pour activer le transfert basé sur Mac, utilisez l'utilitaire de configuration ou la ligne de commande.

Certains déploiements nécessitent que les chemins entrants et sortants passent par différents routeurs. Dans ces situations, le transfert basé sur MAC rompt la conception de la topologie. Pour un site

d'équilibrage de charge de serveur global (GSLB) qui nécessite que les chemins entrants et sortants passent par différents routeurs, vous devez désactiver le transfert basé sur MAC et utiliser le routeur par défaut de l'appliance comme routeur sortant.

Lorsque le transfert basé sur MAC est désactivé et que la connectivité de couche 2 ou 3 est activée, une table de routage peut spécifier des routeurs distincts pour les connexions sortantes et entrantes. Pour désactiver le transfert basé sur Mac, utilisez l'utilitaire de configuration ou la ligne de commande.

Activer ou désactiver le transfert basé sur Mac à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour activer/désactiver le mode de transfert basé sur Mac et vérifier qu'il a été activé/désactivé :

- <enable ns mode <Mode>
- <disable ns mode <Mode>
- <show ns mode
  Example

  "‘ pre codeblock

  ```
  enable ns mode mbf
  Done
  show ns mode
  ```

  ```
  1   Mode                          Acronym           Status
  2   -------                       -------           ------   1)  Fast
      Ramp                     FR                ON   2)  Layer 2
      mode                  L2                OFF   .   .   .   6)
      MAC-based forwarding        MBF               ON   .   .   .
        Done  >
  ```

  ```
  disable ns mode mbf
  Done
  show ns mode
  ```

  ```
  1   Mode                          Acronym           Status
  2   -------                       -------           ------   1)  Fast
      Ramp                     FR                ON   2)  Layer 2
      mode                  L2                OFF   .   .   .   6)
      MAC-based forwarding        MBF               OFF   .   .   .
         Done  >  <!--NeedCopy--> ```
  ```

Pour activer ou désactiver le transfert basé sur Mac à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.

2. Dans le volet d'informations, sous le groupe **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.
3. Dans la boîte de dialogue **Configurer les modes**, pour activer le mode de transfert basé sur **MAC, activez la case à cocher Transfert basé sur MAC** . Pour désactiver le mode de transfert basé sur Mac, désactivez la case à cocher.
4. Cliquez sur **OK**. Le message **Enable/Disable Mode(s)?** s'affiche dans le volet d'informations.
5. Cliquez sur **Oui**.

Interfaces réseau

May 5, 2023

Les interfaces NetScaler sont numérotées selon la notation slot/port. Outre la modification des caractéristiques des interfaces individuelles, vous pouvez configurer des réseaux locaux virtuels pour restreindre le trafic à des groupes d'hôtes spécifiques. Vous pouvez également regrouper les liens en canaux à haut débit.

Réseaux locaux virtuels

L'appliance NetScaler prend en charge le port (couche 2) et les réseaux locaux virtuels (VLAN) balisés IEEE802.1Q. Les configurations VLAN sont utiles lorsque vous devez restreindre le trafic à certains groupes de stations. Vous pouvez configurer une interface réseau pour qu'elle appartienne à plusieurs VLAN à l'aide du balisage IEEE 802.1q.

Vous pouvez lier vos VLAN configurés à des sous-réseaux IP. L'appliance ADC (si elle est configurée comme routeur par défaut pour les hôtes des sous-réseaux) effectue ensuite le transfert IP entre ces VLAN.

L'appliance NetScaler prend en charge les types de VLAN suivants.

- VLAN par défaut

  Par défaut, les interfaces réseau d'une appliance NetScaler sont incluses dans un seul VLAN basé sur les ports en tant qu'interfaces réseau non balisées. Ce VLAN par défaut possède un VID de 1 et existe en permanence. Il ne peut pas être supprimé et son VID ne peut pas être modifié.

- VLAN basés sur les ports

  Un ensemble d'interfaces réseau qui partagent un domaine de diffusion de couche 2 commun et exclusif définit l'appartenance à un VLAN basé sur des ports. Vous pouvez configurer plusieurs VLAN basés sur des ports. Lorsque vous ajoutez une interface à un nouveau VLAN en tant que membre non balisé, elle est automatiquement supprimée du VLAN par défaut.

- VLAN balisé

  Une interface réseau peut être un membre balisé ou non d'un VLAN. Chaque interface réseau est un membre non balisé d'un seul VLAN (son VLAN natif). L'interface réseau non balisée transmet les trames du VLAN natif sous forme de trames non balisées. Une interface réseau balisée peut faire partie de plusieurs VLAN. Lorsque vous configurez le balisage, assurez-vous que les paramètres VLAN correspondent aux deux extrémités du lien. Vous pouvez utiliser l'utilitaire de configuration pour définir un VLAN balisé (nsvlan) auquel tous les ports peuvent être liés en tant que membres balisés du VLAN. La configuration de ce VLAN nécessite le redémarrage de l'appliance ADC et doit donc être effectuée lors de la configuration initiale du réseau.

Chaînes agrégées de liens

L'agrégation de liens combine les données entrantes provenant de plusieurs ports en une seule liaison haut débit. La configuration du canal d'agrégation de liens augmente la capacité et la disponibilité du canal de communication entre une appliance NetScaler et les autres appareils connectés. Un lien agrégé est également appelé canal.

Lorsqu'une interface réseau est liée à un canal, les paramètres de canal ont priorité sur les paramètres d'interface réseau. Une interface réseau ne peut être liée qu'à un seul canal. La liaison d'une interface réseau à un canal d'agrégation de liens modifie la configuration du VLAN. En d'autres termes, la liaison d'interfaces réseau à un canal les supprime des VLAN auxquels elles appartenaient à l'origine et les ajoute au VLAN par défaut. Toutefois, vous pouvez lier le canal à l'ancien VLAN ou à un nouveau. Par exemple, si vous avez lié les interfaces réseau 1/2 et 1/3 à un VLAN avec l'ID 2, puis que vous les liez au canal agrégé de liens LA/1, les interfaces réseau sont déplacées vers le VLAN par défaut, mais vous pouvez les lier au VLAN 2.

Remarque : Vous pouvez également utiliser le protocole LACP (Link Aggregation Control Protocol) pour configurer l'agrégation de liens. Pour plus d'informations, voir Configuration de l'agrégation de liens à l'aide du protocole de contrôle d'agrégation de liens.

Synchronisation de l'horloge

May 5, 2023

Vous pouvez configurer votre appliance NetScaler pour synchroniser son horloge locale avec un serveur NTP (Network Time Protocol). Cela garantit que son horloge dispose des mêmes paramètres de date et d'heure que les autres serveurs de votre réseau. NTP utilise le port 123 du protocole UDP (User Datagram Protocol) comme couche de transport. Ajoutez des serveurs NTP dans le fichier de configuration NTP afin que l'appliance reçoive régulièrement des mises à jour de ces serveurs.

Si vous n'avez pas de serveur NTP local, vous trouverez une liste des serveurs NTP publics en libre accès sur le site officiel de NTP à l'adresse http://www.ntp.org.

Pour configurer la synchronisation de l'horloge sur votre appliance, procédez comme suit :

1. Ouvrez une session sur la ligne de commande et saisissez la commande shell.
2. À l'invite du shell, copiez le fichier ntp.conf du répertoire /etc vers le répertoire /nsconfig. Si le fichier existe déjà dans le répertoire /nsconfig, assurez-vous de supprimer les entrées suivantes du fichier ntp.conf :

   ```
   restrict localhost

   restrict 127.0.0.2
   ```

   Ces entrées ne sont requises que si vous souhaitez exécuter l'appareil en tant que serveur de temps. Toutefois, cette fonctionnalité n'est pas prise en charge sur l'appliance NetScaler.
3. Modifiez /nsconfig/ntp.conf en saisissant l'adresse IP du serveur NTP souhaité sous le serveur du fichier et en restreignant les entrées.
4. Créez un fichier nommé rc.netscaler dans le répertoire /nsconfig, si le fichier n'existe pas déjà dans le répertoire.
5. Modifiez /nsconfig/rc.netscaler en ajoutant l'entrée suivante : `/bin/sh /etc/ntpd_ctl full_start`.

   Cette entrée démarre le service ntpd. et vérifie le fichier ntp.conf.

   Si vous ne voulez pas forcer la synchronisation de l'heure lorsqu'il y a une grande différence, vous pouvez définir la date manuellement, puis relancer ntpd. Vous pouvez vérifier le décalage horaire entre l'appliance et le serveur de temps en exécutant la commande suivante dans le shell :

   ```
   ntpdate -q <IP address or domain name of the NTP server>
   <!--NeedCopy-->
   ```

6. Redémarrez l'appliance pour activer la synchronisation de l'horloge.

   Remarque : Si vous souhaitez démarrer la synchronisation de l'heure sans redémarrer l'appliance, entrez l'une des commandes suivantes à l'invite du shell :

   ```
   /usr/sbin/ntpd -c /nsconfig/ntp.conf -g -p /var/run/ntpd.pid -l /
       var/log/ntpd.log &

   or

   /bin/sh /etc/ntpd_ctl full_start

   ```



```
<!--NeedCopy-->
```

Configuration DNS

May 5, 2023

Vous pouvez configurer une appliance NetScaler pour qu'elle fonctionne comme un serveur de noms de domaine autorisé (ADNS), un serveur proxy DNS, un résolveur final ou un redirecteur. Vous pouvez ajouter des enregistrements de ressources DNS tels que des enregistrements SRV, des enregistrements AAAA, des enregistrements A, des enregistrements MX, des enregistrements NS, des enregistrements CNAME, des enregistrements PTR et des enregistrements SOA. En outre, l'appliance peut équilibrer la charge sur les serveurs DNS externes.

Une pratique courante consiste à configurer une appliance en tant que transitaire. Pour cette configuration, vous devez ajouter des serveurs de noms externes. Après avoir ajouté les serveurs externes, vous devez vérifier que votre configuration est correcte.

Vous pouvez ajouter, supprimer, activer et désactiver des serveurs de noms externes. Vous pouvez créer un serveur de noms en spécifiant son adresse IP, ou vous pouvez configurer un serveur virtuel existant en tant que serveur de noms.

Lors de l'ajout de serveurs de noms, vous pouvez spécifier des adresses IP ou des adresses IP virtuelles (VIP). Si vous utilisez des adresses IP, l'appliance équilibre la charge des demandes adressées aux serveurs de noms configurés de manière circulaire. Si vous utilisez des VIP, vous pouvez spécifier n'importe quelle méthode d'équilibrage de charge.

Ajouter un serveur de noms à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour ajouter un serveur de noms et vérifier la configuration :

- `<add dns nameServer \<IP\>`
- `<show dns nameServer \<IP\>`

Exemple

```
> add dns nameServer 10.102.29.10
 Done
> show dns nameServer 10.102.29.10
1)       10.102.29.10  -  State: DOWN
 Done

```



```
<!--NeedCopy-->
```

Ajouter un serveur de noms à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **DNS** > **Serveurs de noms**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un serveur de noms**, sélectionnez **Adresse IP**.
4. Dans la zone de texte **Adresse IP**, tapez l'adresse IP du serveur de noms (par exemple, 10.102.29.10). Si vous ajoutez un serveur de noms externe, désactivez la case à cocher **Local** .
5. Cliquez sur **Créer**, puis sur **Fermer**.
6. Vérifiez que le serveur de noms que vous avez ajouté s'affiche dans le volet **Serveurs de noms** .

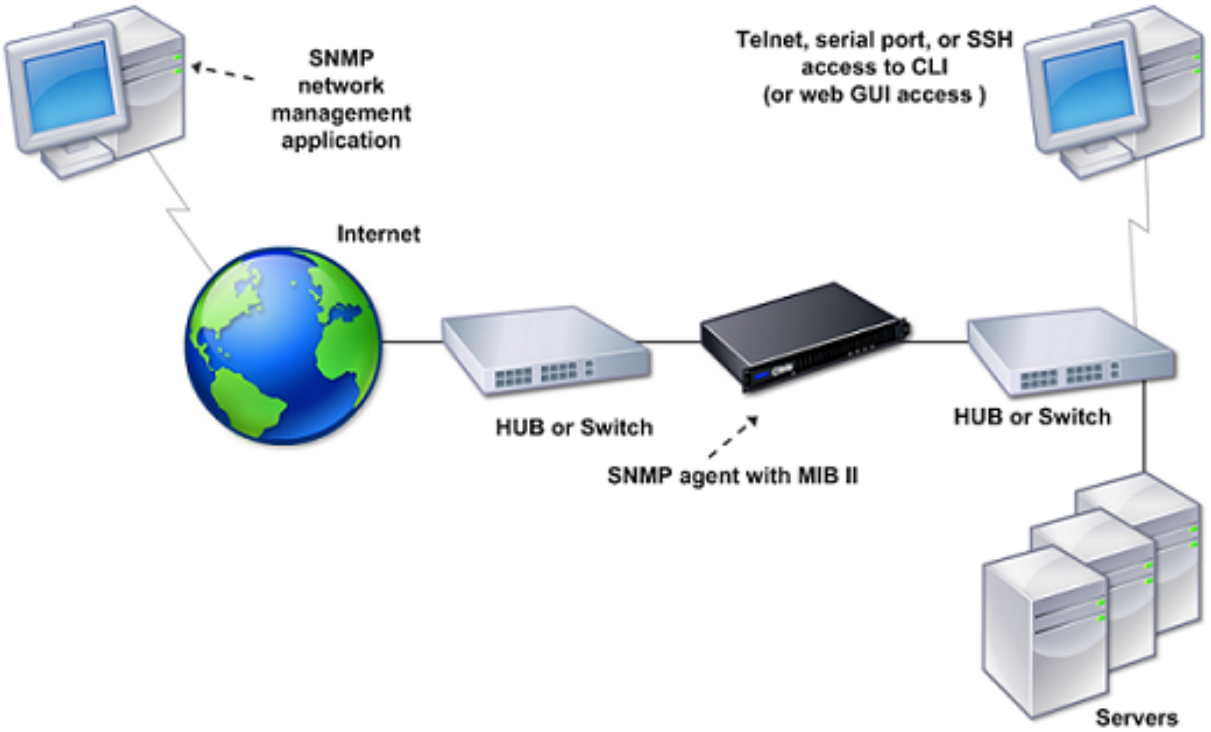
Configuration SNMP

May 8, 2023

L'application de gestion réseau SNMP (Simple Network Management Protocol), exécutée sur un ordinateur externe, interroge l'agent SNMP sur l'appliance NetScaler. L'agent recherche dans la base d'informations de gestion (MIB) les données demandées par l'application de gestion réseau et envoie les données à l'application.

La surveillance SNMP utilise des pièges, des messages et des alarmes. Les messages d'interruption SNMP sont des événements asynchrones que l'agent génère pour signaler des conditions anormales, signalées par des alarmes. Par exemple, si vous souhaitez être informé lorsque l'utilisation du processeur est supérieure à 90 %, vous pouvez configurer une alarme correspondant à cette situation. La figure suivante montre un réseau avec une appliance NetScaler sur laquelle le SNMP est activé et configuré.

Figure 1. SNMP sur l'appliance NetScaler



L'agent SNMP d'une appliance NetScaler prend en charge les versions 1 (SNMPv1), SNMP 2 (SNMPv2) et SNMP version 3 (SNMPv3). Comme il fonctionne en mode bilingue, l'agent peut gérer les requêtes SNMPv2, telles que les requêtes Get-Bulk et SNMPv1. L'agent SNMP envoie également des pièges conformes à SNMPv2 et prend en charge les types de données SNMPv2, tels que counter64. Les gestionnaires SNMPv1 (programmes sur d'autres serveurs qui demandent des informations SNMP à l'appliance ADC) utilisent le fichier NS-MIB-SMIV1.mib lors du traitement des requêtes SNMP. Les gestionnaires SNMPv2 utilisent le fichier NS-MIB-SMIv2.mib.

L'appliance NetScaler prend en charge les MIB spécifiques à l'entreprise suivants :

- Un sous-ensemble de groupes MIB-2 standard. Fournit les groupes MIB-2 SYSTEM, IF, ICMP, UDP et SNMP.
- Un MIB d'entreprise système. Fournit une configuration et des statistiques spécifiques au système.

Pour configurer le SNMP, vous devez spécifier quels gestionnaires peuvent interroger l'agent SNMP, ajouter des auditeurs d'interruptions SNMP qui recevront les messages d'interruption SNMP et configurer les alarmes SNMP.

Ajouter des gestionnaires SNMP

Vous pouvez configurer un poste de travail exécutant une application de gestion conforme à la version 1, 2 ou 3 du protocole SNMP pour accéder à un dispositif. Un tel poste de travail est appelé gestionnaire SNMP. Si vous ne spécifiez pas de gestionnaire SNMP sur l'appliance, celle-ci accepte et répond

aux requêtes SNMP provenant de toutes les adresses IP du réseau. Si vous configurez un ou plusieurs gestionnaires SNMP, l'appliance accepte et répond aux requêtes SNMP provenant uniquement de ces adresses IP spécifiques. Lorsque vous spécifiez l'adresse IP d'un gestionnaire SNMP, vous pouvez utiliser le paramètre netmask pour autoriser l'accès à partir de sous-réseaux entiers. Vous pouvez ajouter un maximum de 100 gestionnaires ou réseaux SNMP. Pour ajouter un gestionnaire SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un gestionnaire SNMP et vérifier la configuration :

```
add snmp manager <IPAddress> ... [-netmask <netmask>]
show snmp manager <IPAddress>
```

Exemple :

```
1 add snmp manager 10.102.29.5 -netmask 255.255.255.255
2 Done
3 show snmp manager 10.102.29.5
4 10.102.29.5 255.255.255.255
5 Done
6 <!--NeedCopy-->
```

Pour ajouter un gestionnaire SNMP à l'aide de l'interface graphique :

1. Dans le volet de navigation, développez **Système**, développez **SNMP**, puis cliquez sur **Managers**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un gestionnaire SNMP**, dans la zone de texte **Adresse IP**, tapez l'adresse IP du poste de travail exécutant l'application de gestion (par exemple, 10.102.29.5).
4. Cliquez sur **Créer**, puis sur **Fermer**.
5. Vérifiez que le gestionnaire SNMP que vous avez ajouté apparaît dans la section **Détails** en bas du volet.

Ajouter des écouteurs SNMP Traps

Après avoir configuré les alarmes, vous devez spécifier l'écouteur d'interruptions auquel l'appliance enverra les messages d'interruption. Outre la spécification de paramètres tels que l'adresse IP et le port de destination de l'écouteur d'interruptions, vous pouvez spécifier le type d'interruption (générique ou spécifique) et la version SNMP.

Vous pouvez configurer un maximum de 20 récepteurs d'interruptions pour recevoir des pièges génériques ou spécifiques.

Pour ajouter un écouteur d'interruptions SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour ajouter un piège SNMP et vérifier qu'il a bien été ajouté :

- `add snmp trap specific <IP>`
- `show snmp trap`

Exemple :

```
Trap type: SPECIFIC
Destination IP: 10.102.29.3
TD: 0
Destination Port: 162
Source IP: NetScaler IP
Version: V2
Min-Severity: -
AllPartition: DISABLED
Community: public
<!--NeedCopy-->
```

Pour ajouter un écouteur d'interruptions SNMP à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, développez **SNMP**, puis cliquez sur Traps **.**
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une destination d'interception SNMP**, dans la zone de texte **Adresse IP de destination**, tapez l'adresse IP (par exemple, 10.102.29.3).
4. Cliquez sur **Create**, puis cliquez sur **Close**.
5. Vérifiez que le piège SNMP que vous avez ajouté apparaît dans la section **Détails** en bas du volet.

Configurer les alarmes SNMP

Vous configurez les alarmes de manière à ce que l'appliance génère un message d'alerte lorsqu'un événement correspondant à l'une des alarmes se produit. La configuration d'une alarme consiste à activer l'alarme et à définir le niveau de gravité auquel un piège est généré. Il existe cinq niveaux de gravité : critique, majeur, mineur, avertissant et informatif. Un piège est envoyé uniquement lorsque la gravité de l'alarme correspond à la gravité spécifiée pour le piège.

Certaines alarmes sont activées par défaut. Si vous désactivez une alarme SNMP, l'appliance ne génère pas de messages d'interruption lorsque des événements correspondants se produisent. Par exemple, si vous désactivez l'alarme SNMP d'échec de connexion, l'appliance ne générera pas de message d'interruption en cas d'échec de connexion.

Pour activer ou désactiver une alarme à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver une alarme et vérifier qu'elle a été activée ou désactivée :

- définir l'alarme snmp \ <trapName> \ [-state ACTIVÉ | DÉSACTIVÉ \]
- Afficher l'alarme SNMP \ <trapName>

  Exemple

```
set snmp alarm LOGIN-FAILURE -state ENABLED
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
----- -------------- ---------------- ---- -------- --------- --------
LOGIN-FAILURE N/A N/A N/A ENABLED - ENABLED
Done
<!--NeedCopy-->
```

Pour définir la gravité de l'alarme à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir la gravité de l'alarme et vérifier que la gravité a été correctement définie :

- `set snmp alarm <trapName> [-severity <severity>]`
- `show snmp alarm <trapName>`

Exemple :

```
set snmp alarm LOGIN-FAILURE -severity Major
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
----- -------------- ---------------- ---- -------- --------- --------
LOGIN-FAILURE N/A N/A N/A ENABLED Major ENABLED
Done
<!--NeedCopy-->
```

Pour configurer les alarmes à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, développez SNMP, puis cliquez sur **Alarmes**.
2. **Dans le volet de détails, sélectionnez une alarme (par exemple, ÉCHEC DE CONNEXION), puis cliquez sur Ouvrir.**

3. Dans la boîte de dialogue **Configurer l'alarme SNMP**, pour activer l'alarme, sélectionnez Activé dans la liste déroulante **État** . Pour désactiver l'alarme, sélectionnez Désactivé.
4. Dans la liste déroulante **Gravité**, sélectionnez une option de gravité (par exemple, Majeur).
5. Cliquez sur **OK**, puis sur **Fermer**.
6. Vérifiez que les paramètres de l'alarme SNMP que vous avez configurée sont correctement configurés en consultant la section **Détails** en bas du volet.

Vérifiez la configuration

May 5, 2023

Une fois que vous avez terminé de configurer votre système, complétez les listes de contrôle suivantes pour vérifier votre configuration.

Liste de contrôle de configuration

- La version en cours d'exécution est la suivante :
- Il n'y a aucun problème d'incompatibilité. (Les problèmes d'incompatibilité sont documentés dans les notes de publication de la version.)
- Les paramètres du port (vitesse, duplex, contrôle du flux, surveillance) sont identiques à ceux du port du commutateur.
- Un nombre suffisant d'adresses IP SNIP ont été configurées pour prendre en charge toutes les connexions côté serveur pendant les heures de pointe.
  - Le nombre d'adresses IP SNIP configurées est :__
  - Le nombre attendu de connexions simultanées au serveur est le suivant :
    [] 62 000 [] 124 000 [] Autres____

Liste de contrôle de configuration de la topologie

Les routes ont été utilisées pour résoudre des serveurs sur d'autres sous-réseaux.

Les itinéraires saisis sont les suivants :

_____

- Si l'appliance NetScaler se trouve dans une topologie publique-privée, le NAT inversé a été configuré.
- Les paramètres de basculement (haute disponibilité) configurés sur l'appliance ADC sont résolus selon une configuration à un ou deux bras. Toutes les interfaces réseau non utilisées ont été désactivées :

_____

- Si l'appliance ADC est placée derrière un équilibreur de charge externe, la politique d'équilibrage de charge de l'équilibreur de charge externe n'est pas la « moindre connexion ».

  La politique d'équilibrage de charge configurée sur l'équilibreur de charge externe est la suivante :

_____

- Si l'appliance ADC est placée devant un pare-feu, le délai d'expiration de session sur le pare-feu est défini sur une valeur supérieure ou égale à 300 secondes.

  Remarque : Le délai d'inactivité de connexion TCP sur une appliance NetScaler est de 360 secondes. Si le délai d'expiration du pare-feu est également défini sur 300 secondes ou plus, l'appliance peut effectuer un multiplexage des connexions TCP de manière efficace car les connexions ne seront pas fermées plus tôt.

  La valeur configurée pour le délai d'expiration de la session est : _____

Liste de contrôle de configuration du serveur

- Le mode « Keep-alive » a été activé sur tous les serveurs.

  La valeur configurée pour le délai d'expiration du délai de conservation est : _____

- La passerelle par défaut a été définie sur la valeur correcte. (La passerelle par défaut doit être une appliance NetScaler ou un routeur en amont.) La passerelle par défaut est la suivante :

_____

- Les paramètres du port du serveur (vitesse, duplex, contrôle du flux, surveillance) sont les mêmes que ceux du port du commutateur.

_____

- Si le serveur Microsoft® Internet Information Server est utilisé, la mise en mémoire tampon est activée sur le serveur.
- Si un serveur Apache est utilisé, le paramètre MaxConn (nombre maximum de connexions) est configuré sur le serveur et sur l'appliance NetScaler.

  La valeur MaxConn (nombre maximum de connexions) qui a été définie est la suivante :

_____

- Si un serveur Netscape Enterprise est utilisé, le nombre maximum de requêtes par paramètre de connexion est défini sur l'appliance NetScaler. Le nombre maximum de demandes par valeur de connexion définie est de :

_____

Liste de contrôle pour la configuration des fonctionnalités logicielles

- La fonctionnalité du mode couche 2 doit-elle être désactivée ? (Désactivez si un autre périphérique de couche 2 fonctionne en parallèle avec une appliance NetScaler.)

  Motif de l'activation ou de la désactivation :

  _____

- La fonction de transfert sur Mac doit-elle être désactivée ? (Si l'adresse MAC utilisée par le trafic de retour est différente, elle doit être désactivée.)

  Motif de l'activation ou de la désactivation :

  _____

- La réutilisation basée sur l'hôte doit-elle être désactivée ? (Y a-t-il un hébergement virtuel sur les serveurs ?)

  Motif de l'activation ou de la désactivation :

  _____

- Les paramètres par défaut de la fonction de protection contre les surtensions doivent-ils être modifiés ?

  Motif de la modification ou de la non-modification :

  _____

Liste de contrôle d'accès

- Les adresses IP du système peuvent faire l'objet d'une requête ping depuis le réseau côté client.
- Les adresses IP du système peuvent être envoyées par ping depuis le réseau côté serveur.
- Le ou les serveurs gérés peuvent être soumis à un ping via NetScaler.
- Les hôtes Internet peuvent recevoir un ping à partir des serveurs gérés.
- Le ou les serveurs gérés sont accessibles via le navigateur.
- Internet est accessible à partir du ou des serveurs gérés à l'aide du navigateur.
- Le système est accessible via SSH.
- L'accès administrateur à tous les serveurs gérés fonctionne.

> Remarque : Lorsque vous utilisez l'utilitaire de ping, assurez-vous que ICMP ECHO est activé sur le serveur auquel vous envoyez un ping, sinon votre ping échouera.

Liste de contrôle du pare-feu

Les exigences suivantes en matière de pare-feu ont été satisfaites :

- UDP 161 (SNMP)
- UDP 162 (piège SNMP)
- TCP/UDP 3010 (INTERFACE GRAPHIQUE)
- HTTP 80 (INTERFACE GRAPHIQUE)
- TCP 22 (SSH)

Trafic d'équilibrage de charge sur une appliance NetScaler

May 5, 2023

La fonction d'équilibrage de charge répartit les demandes des clients sur plusieurs serveurs afin d'optimiser l'utilisation des ressources. Dans un scénario réel avec un nombre limité de serveurs fournissant des services à un grand nombre de clients, un serveur peut être surchargé et dégrader les performances du parc de serveurs. Une appliance NetScaler utilise des critères d'équilibrage de charge pour éviter les engorgements en transférant chaque demande client au serveur le mieux adapté pour traiter la demande lorsqu'elle arrive.

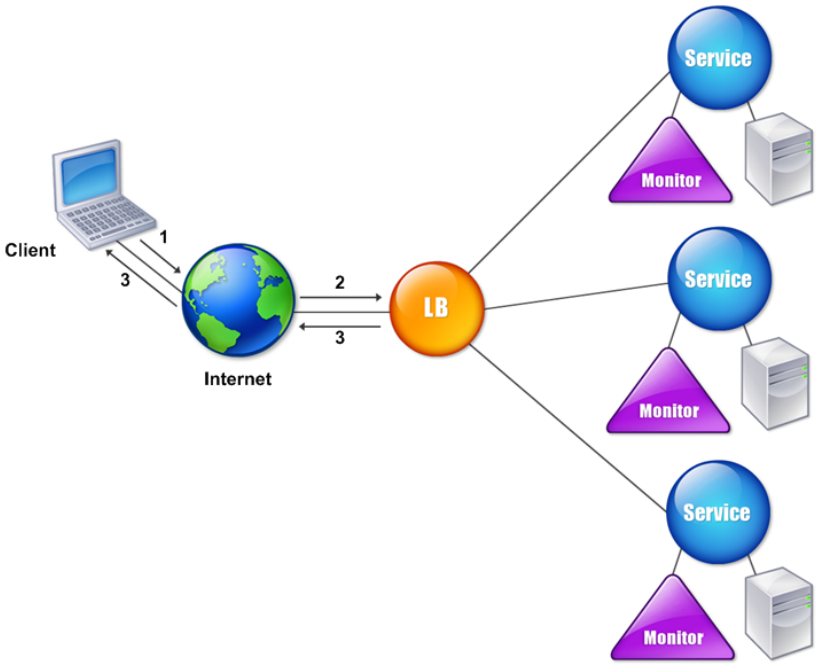
Pour configurer l'équilibrage de charge, vous devez définir un serveur virtuel pour mandater plusieurs serveurs d'une batterie de serveurs et équilibrer la charge entre eux.

Lorsqu'un client établit une connexion au serveur, un serveur virtuel met fin à la connexion client et initie une nouvelle connexion avec le serveur sélectionné, ou réutilise une connexion existante avec le serveur pour effectuer un équilibrage de charge. La fonction d'équilibrage de charge permet de gérer le trafic de la couche 4 (TCP et UDP) à la couche 7 (FTP, HTTP et HTTPS).

L'appliance NetScaler utilise un certain nombre d'algorithmes, appelés méthodes d'équilibrage de charge, pour déterminer comment répartir la charge entre les serveurs. La méthode d'équilibrage de charge par défaut est la méthode Least Connections.

Un déploiement d'équilibrage de charge classique comprend les entités décrites dans la figure suivante.

Figure 1. Architecture d'équilibrage de charge



Les entités fonctionnent comme suit :

- **Serveur virtuel**. Entité représentée par une adresse IP, un port et un protocole. L'adresse IP du serveur virtuel (VIP) est généralement une adresse IP publique. Le client envoie des demandes de connexion à cette adresse IP. Le serveur virtuel représente une banque de serveurs.
- **Un service**. Représentation logique d'un serveur ou d'une application exécutée sur un serveur. Identifie l'adresse IP du serveur, un port et un protocole. Les services sont liés aux serveurs virtuels.
- **Objet serveur**. Entité représentée par une adresse IP. L'objet serveur est créé lorsque vous créez un service. L'adresse IP du service est considérée comme le nom de l'objet serveur. Vous pouvez également créer un objet serveur, puis créer des services à l'aide de cet objet serveur.
- **Moniteur**. Entité qui suit l'état de santé des services. L'appliance sonde régulièrement les serveurs à l'aide du moniteur lié à chaque service. Si un serveur ne répond pas dans le délai de réponse spécifié et que le nombre de sondes spécifié échoue, le service est marqué comme étant inactif. L'appliance effectue ensuite l'équilibrage de la charge entre les services restants.

Équilibrage de charge

May 8, 2023

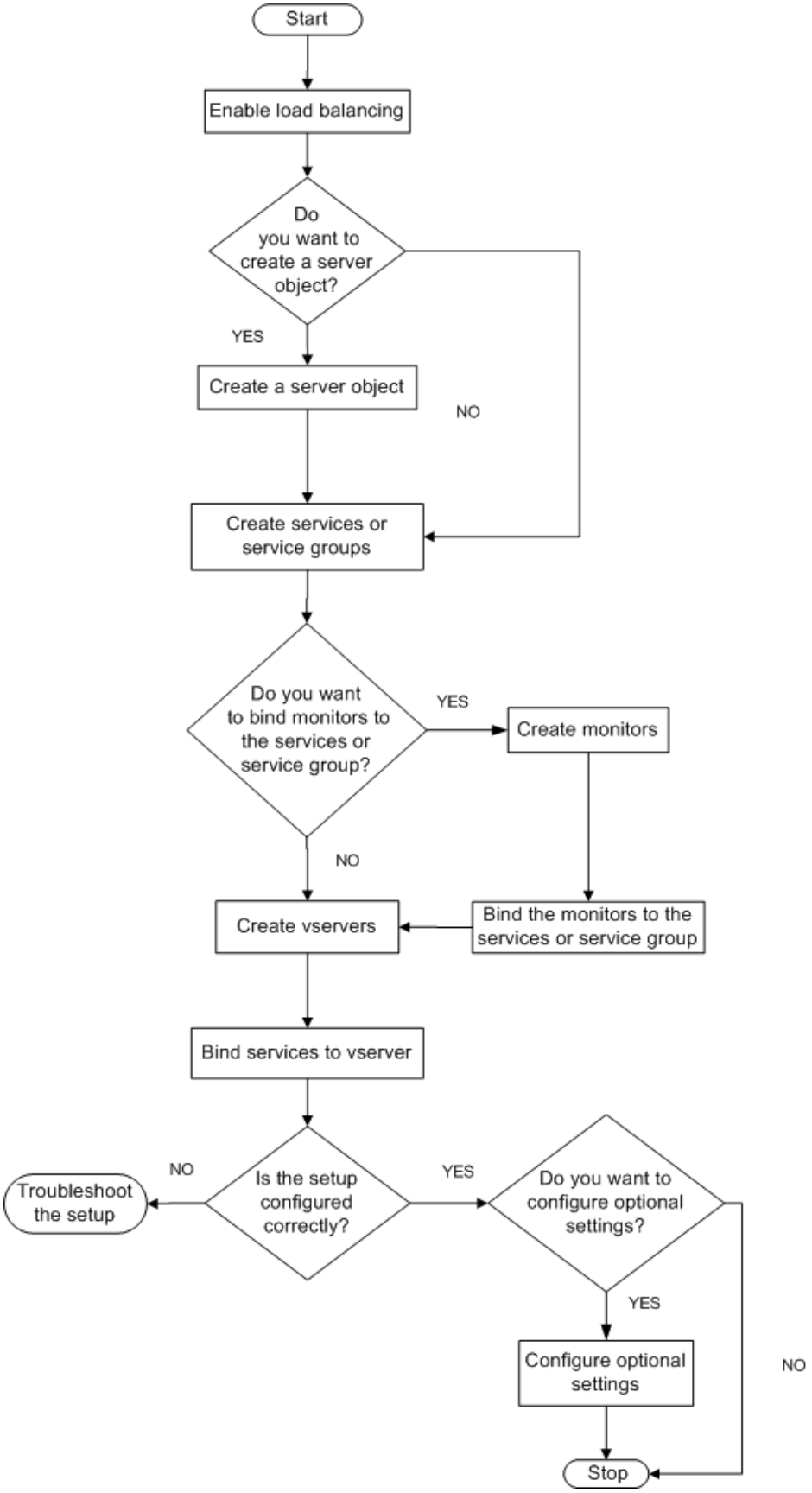
Pour configurer l'équilibrage de charge, vous devez d'abord créer des services. Vous créez ensuite des serveurs virtuels et liez les services aux serveurs virtuels. Par défaut, l'appliance NetScaler associe un moniteur à chaque service. Après avoir lié les services, vérifiez votre configuration en vous assurant que tous les paramètres sont corrects.

> Remarque : Après avoir déployé la configuration, vous pouvez afficher des statistiques qui montrent les performances des entités de la configuration. Utilisez l'utilitaire de statistiques ou la <vserverName> commande
> stat lb vserver \.

Vous pouvez éventuellement attribuer des poids à un service. La méthode d'équilibrage de charge utilise ensuite le poids attribué pour sélectionner un service. Pour commencer, vous pouvez toutefois limiter les tâches facultatives à la configuration de certains paramètres de persistance de base, à des sessions qui doivent maintenir une connexion à un serveur particulier et à certains paramètres de base de protection de la configuration.

L'organigramme suivant illustre la séquence des tâches de configuration.

Figure 1. Séquence de tâches pour configurer l'équilibrage de charge



Activer l'équilibrage de charge

Avant de configurer l'équilibrage de charge, assurez-vous que la fonction d'équilibrage de charge est activée.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer l'équilibrage de charge et vérifier qu'il est activé :

- activer la fonction lb
- show feature

  Exemple

  "‘ pre codeblock

  ```
  enable feature lb
  Done
  show feature
  ```

  ```
  1   Feature                  Acronym          Status
  2   -------                  -------          ------   1)  Web
      Logging                WL               OFF   2)  Surge
      Protection           SP               OFF   3)  Load Balancing
                LB               ON   .   .   .   9)  SSL
      Offloading             SSL              ON   .   .   .  Done
      <!--NeedCopy--> ```
  ```

Pour activer l'équilibrage de charge à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, puis cliquez sur Paramètres.
2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur Modifier les fonctionnalités de base.
3. Dans la boîte de dialogue Configurer les fonctionnalités de base, cochez la case Équilibrage de charge, puis cliquez sur OK.
4. Dans les fonctionnalités Activer/Désactiver ? message, cliquez sur Oui.

Configuration des services et d'un serveur virtuel

Lorsque vous avez identifié les services pour lesquels vous souhaitez équilibrer la charge, vous pouvez implémenter votre configuration initiale d'équilibrage de charge en créant les objets de service, en créant un serveur virtuel d'équilibrage de charge et en liant les objets de service au serveur virtuel.

Pour implémenter la configuration initiale d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour implémenter et vérifier la configuration initiale :

- <serviceType><ajouter un service \ \ <name> \ <IPaddress> \ <port>
- <port><ajouter lb vserver \ <vServerName> \ <serviceType> [\ \ <IPaddress> \]
- <name>vserver de laboratoire trind \ \ <serviceName>
- <afficher les liaisons de service \ <serviceName>

Exemple

```
> add service service-HTTP-1 10.102.29.5 HTTP 80
 Done
> add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
 Done
> bind lb vserver vserver-LB-1 service-HTTP-1
 Done
> show service bindings service-HTTP-1
    service-HTTP-1 (10.102.29.5:80) - State : DOWN

      1)      vserver-LB-1 (10.102.29.60:80) - State : DOWN
 Done
<!--NeedCopy-->
```

Pour implémenter la configuration initiale d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge.
2. Dans le volet de détails, sous Mise en route, cliquez sur Assistant d'équilibrage de charge et suivez les instructions pour créer une configuration d'équilibrage de charge de base.
3. Revenez au volet de navigation, développez Load Balancing, puis cliquez sur Virtual Servers.
4. Sélectionnez le serveur virtuel que vous avez configuré et vérifiez que les paramètres affichés au bas de la page sont correctement configurés.
5. Cliquez sur Ouvrir.
6. Vérifiez que chaque service est lié au serveur virtuel en confirmant que la case Actif est cochée pour chaque service sous l'onglet Services.

Paramètres de persistance

May 8, 2023

Vous devez configurer la persistance sur un serveur virtuel si vous souhaitez conserver les états des connexions sur les serveurs représentés par ce serveur virtuel (par exemple, les connexions utilisées dans le commerce électronique). L'appliance utilise ensuite la méthode d'équilibrage de charge configurée pour la sélection initiale d'un serveur, mais transmet à ce même serveur toutes les demandes ultérieures du même client.

Si la persistance est configurée, elle remplace les méthodes d'équilibrage de charge une fois le serveur sélectionné. Si la persistance configurée s'applique à un service en panne, l'appliance utilise les méthodes d'équilibrage de charge pour sélectionner un nouveau service, et le nouveau service devient persistant pour les demandes ultérieures du client. Si le service sélectionné est hors service, il continue de traiter les demandes en attente mais n'accepte pas les nouvelles demandes ou connexions. Une fois la période d'arrêt écoulée, les connexions existantes sont fermées. Le tableau suivant répertorie les types de persistance que vous pouvez configurer.

Type de persistance	Connexions persistantes
IP source, ID de session SSL, règle, DESTIP, SRCIPDESTIP	250K*
CookieInsert, URL passive, ID de serveur personnalisé	Limite de mémoire. Dans le cas de CookieInsert, si le délai d'expiration n'est pas égal à 0, n'importe quel nombre de connexions est autorisé jusqu'à ce que la mémoire soit limitée.

Le * tableau précédent fait référence aux éléments suivants :

250 000 sessions par cœur sont la valeur par défaut par moteur de paquets. Pour configurer 1 million d'entrées de session par moteur de paquets, exécutez la commande suivante :

```
set lb parameter -sessionsthreshold <1000000*number of PE>
```

Pour un système 3 PE, exécutez la commande suivante :

```
set lb parameter -sessionsthreshold 3000000
```

Tableau 1. Limitation du nombre de connexions persistantes simultanées

Si la persistance configurée ne peut pas être maintenue en raison d'un manque de ressources sur une appliance, les méthodes d'équilibrage de charge sont utilisées pour la sélection du serveur. La

persistance est maintenue pendant une période configurée, en fonction du type de persistance. Certains types de persistance sont spécifiques à certains serveurs virtuels. Le tableau suivant montre la relation.

Type de persistance Header 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge
IP source	OUI	OUI	OUI	OUI	OUI
Insert de cookie	OUI	OUI	NON	NON	NON
ID de session SSL	NON	OUI	NON	NON	OUI
URL passive	OUI	OUI	NON	NON	NON
ID de serveur personnalisé	OUI	OUI	NON	NON	NON
Rule	OUI	OUI	NON	NON	NON
SRCIPDESTIP	S/O	S/O	OUI	OUI	S/O
DESTIP	S/O	S/O	OUI	OUI	S/O

Tableau 2 Types de persistance disponibles pour chaque type de serveur virtuel

Vous pouvez également spécifier la persistance d'un groupe de serveurs virtuels. Lorsque vous activez la persistance sur le groupe, les demandes des clients sont dirigées vers le même serveur sélectionné, quel que soit le serveur virtuel du groupe qui reçoit la demande du client. Lorsque le temps configuré pour la persistance est écoulé, n'importe quel serveur virtuel du groupe peut être sélectionné pour les demandes des clients entrants.

Deux types de persistance couramment utilisés sont la persistance basée sur les cookies et la persistance basée sur les ID de serveur dans les URL.

Configurer la persistance en fonction des cookies

Lorsque vous activez la persistance basée sur les cookies, l'appliance NetScaler ajoute un cookie HTTP dans le champ d' **en-tête Set-Cookie** de la réponse HTTP. Le cookie contient des informations sur le service auquel les demandes HTTP doivent être envoyées. Le client enregistre le cookie et l'inclut dans toutes les demandes ultérieures, et l'ADC l'utilise pour sélectionner le service pour ces demandes. Vous pouvez utiliser ce type de persistance sur des serveurs virtuels de type HTTP ou HTTPS.

<NSC \ _XXXX> <ServiceIP>L' appliance NetScaler insère le cookie \= \ \ <ServicePort>

où :

- < <NSC_XXXX>est l'ID du serveur virtuel dérivé du nom du serveur virtuel.
- < \ <ServiceIP> est la valeur hexadécimale de l'adresse IP du service.
- < \ <ServicePort> est la valeur hexadécimale du port du service.

Si l' `useEncryptedPersistenceCookie` option est activée, l'ADC chiffre ServiceIP et ServicePort à l'aide de l'algorithme de hachage SHA2 lorsqu'il insère un cookie et déchiffre lorsqu'il reçoit un cookie.

Remarque : si le client n'est pas autorisé à stocker le cookie HTTP, les requêtes suivantes n'ont pas le cookie HTTP et la persistance n'est pas respectée.

Par défaut, l'appliance ADC envoie le cookie HTTP version 0, conformément à la spécification Netscape. Il peut également envoyer la version 1, conformément à la RFC 2109.

Vous pouvez configurer une valeur de délai d'expiration pour la persistance basée sur les cookies HTTP. Tenez compte de ce qui suit :

- Si la version 0 du cookie HTTP est utilisée, l'appliance NetScaler insère le temps universel coordonné (GMT) absolu de l'expiration du cookie (l'attribut expires du cookie HTTP), calculé comme la somme de l'heure GMT actuelle sur une appliance ADC et de la valeur du délai d'expiration.
- Si un cookie HTTP version 1 est utilisé, l'appliance ADC insère un délai d'expiration relatif (attribut Max-Age du cookie HTTP). Dans ce cas, le logiciel client calcule le délai d'expiration réel.

Remarque : La plupart des logiciels clients actuellement installés (navigateurs Microsoft Internet Explorer et Netscape) comprennent la version 0 du cookie HTTP ; cependant, certains proxies HTTP comprennent la version 1 du cookie HTTP.

Si vous définissez la valeur du délai d'expiration sur 0, l'appliance ADC ne spécifie pas le délai d'expiration, quelle que soit la version du cookie HTTP utilisée. Le délai d'expiration dépend alors du logiciel client, et ces cookies ne sont pas valides si ce logiciel est arrêté. Ce type de persistance ne consomme aucune ressource système. Par conséquent, il peut accueillir un nombre illimité de clients persistants.

Un administrateur peut modifier la version du cookie HTTP.

Pour modifier la version du cookie HTTP à l'aide de la CLI

À l'invite de commandes, tapez ;

```
set ns param [-cookieversion ( 0 | 1 )]
<!--NeedCopy-->
```

Exemple :

```
set ns param -cookieversion 1
<!--NeedCopy-->
```


Pour modifier la version du cookie HTTP à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**.
2. Dans le volet d'informations, cliquez sur Modifier les paramètres HTTP.
3. Dans la boîte de dialogue Configurer les paramètres HTTP, sous Cookie, sélectionnez Version 0 ou Version 1.

Remarque : Pour plus d'informations sur les paramètres, voir Configurer la persistance en fonction des cookies.

Pour configurer la persistance basée sur les cookies à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la persistance en fonction des cookies et vérifier la configuration :

```
set lb vserver <name> -persistenceType COOKIEINSERT

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: COOKIEINSERT (version 0)
    Persistence Timeout: 2 min
    .
    .
    .
 Done
<!--NeedCopy-->
```

Pour configurer la persistance basée sur les cookies à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la persistance (par exemple, vServer-LB-1), puis cliquez sur Ouvrir.

3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Méthode et persistance, dans la liste Persistence, sélectionnez COOKIEINSERT.
4. Dans la zone de texte Délai d'expiration (min), tapez la valeur du délai d'expiration (par exemple, 2).
5. Cliquez sur OK.
6. Vérifiez que le serveur virtuel pour lequel vous avez configuré la persistance est correctement configuré en sélectionnant le serveur virtuel et en affichant la section Détails en bas du volet.

Configuration de la persistance en fonction des ID de serveur dans les URL

L'appliance NetScaler peut maintenir la persistance en fonction des ID de serveur figurant dans les URL. Dans une technique appelée persistance passive d'URL, l'ADC extrait l'ID du serveur de la réponse du serveur et l'intègre dans la requête URL de la demande du client. L'ID du serveur est une adresse IP et le port est spécifié sous la forme d'un nombre hexadécimal. L'ADC extrait l'ID du serveur des demandes ultérieures du client et l'utilise pour sélectionner le serveur.

La persistance passive des URL nécessite la configuration d'une expression de charge utile ou d'une expression d'infrastructure de stratégie spécifiant l'emplacement de l'ID de serveur dans les demandes du client. Pour plus d'informations sur les expressions, voir Configuration et référence des stratégies.

Remarque : Si l'ID de serveur ne peut pas être extrait des demandes client, la sélection du serveur est basée sur la méthode d'équilibrage de charge.

Exemple : expression de charge utile

L'expression URLQUERY contains sid= configure le système pour extraire l'ID du serveur de la requête URL d'une requête client, après avoir mis en correspondance le jeton sid=. Ainsi, une demande avec l'URL `http://www.citrix.com/index.asp?\\&sid;=c0a864100050` est dirigée vers le serveur avec l'adresse IP 10.102.29.10 et le port 80.

La valeur du délai d'expiration n'affecte pas ce type de persistance, qui est maintenue tant que l'ID du serveur peut être extrait des demandes du client. Ce type de persistance ne consomme pas de ressources système, il peut donc accueillir un nombre illimité de clients persistants.

> Remarque : Pour plus d'informations sur les paramètres, voir Équilibrage de charge.

Pour configurer la persistance en fonction des ID de serveur dans les URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la persistance en fonction des ID de serveur dans les URL et vérifiez la configuration :

```
set lb vserver <name> -persistenceType URLPASSIVE

```



```
<show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: URLPASSIVE
    Persistence Timeout: 2 min
    .
    .
    .
Done
<!--NeedCopy-->
```

Pour configurer la persistance en fonction des ID de serveur dans les URL à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la persistance (par exemple, vServer-LB-1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Méthode et persistance, dans la liste Persistence, sélectionnez URLPASSIVE.
4. Dans la zone de texte Délai d'expiration (min), tapez la valeur du délai d'expiration (par exemple, 2).
5. Dans la zone de texte Règle, entrez une expression valide. Vous pouvez également cliquer sur Configurer en regard de la zone de texte Règle et utiliser la boîte de dialogue Créer une expression pour créer une expression.
6. Cliquez sur OK.
7. Vérifiez que le serveur virtuel pour lequel vous avez configuré la persistance est correctement configuré en sélectionnant le serveur virtuel et en affichant la section Détails en bas du volet.

Configurer les fonctionnalités pour protéger la configuration d'équilibrage de charge

August 20, 2021

Vous pouvez configurer la redirection d'URL pour fournir des notifications de dysfonctionnements du serveur virtuel, et vous pouvez configurer les serveurs virtuels de sauvegarde pour qu'ils prennent le relais si un serveur virtuel principal devient indisponible.

Configurer la redirection d'URL

Vous pouvez configurer une URL de redirection pour communiquer l'état de l'appliance en cas d'arrêt ou de désactivation d'un serveur virtuel de type HTTP ou HTTPS. Cette URL peut être un lien local ou distant. L'appliance utilise la redirection HTTP 302.

Les redirections peuvent être des URL absolues ou des URL relatives. Si l'URL de redirection configurée contient une URL absolue, la redirection HTTP est envoyée à l'emplacement configuré, quelle que soit l'URL spécifiée dans la requête HTTP entrante. Si l'URL de redirection configurée contient uniquement le nom de domaine (URL relative), la redirection HTTP est envoyée à un emplacement après avoir ajouté l'URL entrante au domaine configuré dans l'URL de redirection.

Remarque : si un serveur virtuel d'équilibrage de charge est configuré à la fois avec un serveur virtuel de sauvegarde et une URL de redirection, le serveur virtuel de sauvegarde a priorité sur l'URL de redirection. Dans ce cas, une redirection est utilisée lorsque les serveurs virtuels principal et de sauvegarde sont en panne.

Pour configurer un serveur virtuel pour rediriger les demandes client vers une URL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel afin de rediriger les demandes du client vers une URL et vérifier la configuration :

```
set lb vserver <name> -redirectURL <URL>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
    > set lb vserver vserver-LB-1 -redirectURL <http://www.newdomain.
       com/mysite/maintenance>
     Done
```



```
3      > show lb vserver vserver-LB-1
4          vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
5          State: DOWN
6          Last state change was at Wed Jun 17 08:56:34 2009 (+666 ms)
7          .
8          .
9          .
10         Redirect URL: <http://www.newdomain.com/mysite/maintenance>
11         .
12         .
13         .
14       Done
15     >
16 <!--NeedCopy-->
```

Pour configurer un serveur virtuel pour rediriger les requêtes client vers une URL à l'aide de l'interface graphique graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la redirection d'URL (par exemple, vserver-LB-1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Avancé, dans la zone de texte URL de redirection, tapez l'URL (par exemple `http://www.newdomain.com/mysite/maintenance`), puis cliquez sur OK.
4. Vérifiez que l'URL de redirection que vous avez configurée pour le serveur apparaît dans la section Détails au bas du volet.

Configurer les serveurs virtuels de sauvegarde

Si le serveur virtuel principal est hors service ou désactivé, l'appliance peut diriger les connexions ou les demandes du client vers un serveur virtuel de sauvegarde qui transfère le trafic client aux services. L'appliance peut également envoyer un message de notification au client concernant la panne ou la maintenance du site. Le serveur virtuel de sauvegarde est un proxy et est transparent pour le client.

Vous pouvez configurer un serveur virtuel de sauvegarde lorsque vous créez un serveur virtuel ou lorsque vous modifiez les paramètres facultatifs d'un serveur virtuel existant. Vous pouvez également configurer un serveur virtuel de sauvegarde pour un serveur virtuel de sauvegarde existant, créant ainsi un serveur virtuel de sauvegarde en cascade. La profondeur maximale des serveurs virtuels de sauvegarde en cascade est de 10. L'appliance recherche un serveur virtuel de sauvegarde qui est en service et y accède pour diffuser le contenu.

Vous pouvez configurer la redirection d'URL sur le serveur principal pour une utilisation lorsque les

serveurs virtuels principal et de sauvegarde sont en panne ou ont atteint leurs seuils de traitement des demandes.

Remarque : Si aucun serveur virtuel de sauvegarde n'existe, un message d'erreur s'affiche, sauf si le serveur virtuel est configuré avec une URL de redirection. Si un serveur virtuel de sauvegarde et une URL de redirection sont tous deux configurés, le serveur virtuel de sauvegarde a priorité.

Pour configurer un serveur virtuel de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur de sauvegarde et vérifier la configuration :

```
set lb vserver <name> [-backupVserver <string>]

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
    > set lb vserver vserver-LB-1 -backupVserver vserver-LB-2
     Done
    > show lb vserver vserver-LB-1
        vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jun 17 08:56:34 2009 (+661 ms)
        .
        .
        .
        Backup: vserver-LB-2
        .
        .
        .
     Done
    >
<!--NeedCopy-->
```

Pour configurer un serveur virtuel de sauvegarde à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le serveur virtuel de sauvegarde (par exemple, vserver-LB-1), puis cliquez sur Ouvrir.

3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Avancé, dans la liste Sauvegarder le serveur virtuel, sélectionnez le serveur virtuel de sauvegarde (par exemple, vServer-LB-2, puis cliquez sur OK.
4. Vérifiez que le serveur virtuel de sauvegarde que vous avez configuré apparaît dans la section Détails en bas du volet.

   Remarque : Si le serveur principal tombe en panne, puis remonte, et que vous souhaitez que le serveur virtuel de sauvegarde fonctionne comme serveur principal jusqu'à ce que vous rétablissiez explicitement le serveur virtuel principal, activez la case à cocher Désactiver le serveur principal lors de l'arrêt.

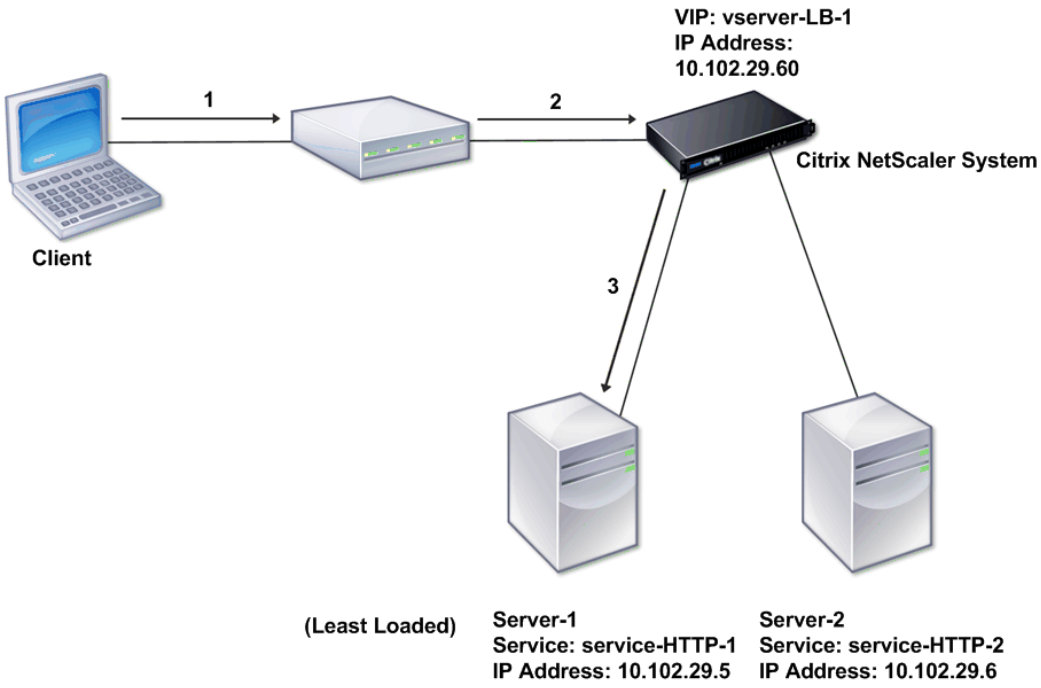
Scénario d'équilibrage de charge typique

May 5, 2023

Dans une configuration d'équilibrage de charge, les appliances NetScaler sont logiquement situées entre le client et la batterie de serveurs, et elles gèrent le flux de trafic vers les serveurs.

La figure suivante montre la topologie d'une configuration d'équilibrage de charge de base.

Figure 1. Topologie d'équilibrage de charge de base

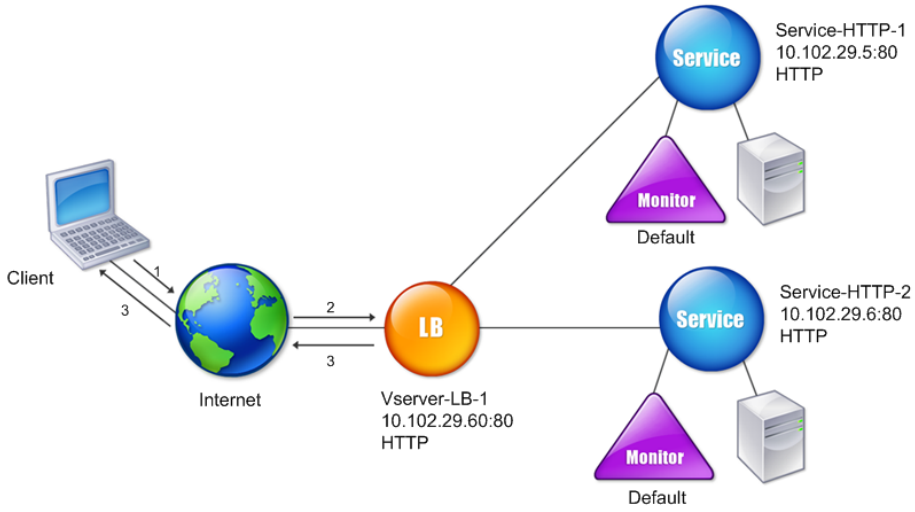


Le serveur virtuel sélectionne le service et l'attribue pour répondre aux demandes des clients. Prenons le scénario de la figure précédente, dans lequel les services Service-HTTP-1 et Service-HTTP-2 sont créés et liés au serveur virtuel nommé Virtual Server-LB-1. Virtual Server-LB-1 transmet la demande du client à Service-HTTP-1 ou Service-HTTP-2. Le système sélectionne le service pour chaque demande à l'aide de la méthode d'équilibrage de charge Least Connections. Le tableau suivant répertorie les noms et les valeurs des entités de base qui doivent être configurées sur le système.

Tableau 1. Valeurs des paramètres de configuration LB

La figure suivante montre les valeurs d'échantillon d'équilibrage de charge et les paramètres requis décrits dans le tableau précédent.

Figure 2. Modèle d'entité d'équilibrage de charge



Les tableaux suivants répertorient les commandes utilisées pour configurer cette configuration d'équilibrage de charge à l'aide de l'interface de ligne de commande.

Tâche	Commande
Pour activer l'équilibrage de charge	activer la fonction lb
Pour créer un service nommé Service-HTTP-1	ajouter le service Service-HTTP-1 10.102.29.5 HTTP 80
Pour créer un service nommé Service-HTTP-2	ajouter un service Service-HTTP-2 10.102.29.6 HTTP 80
Pour créer un serveur virtuel nommé vServer-LB-1	ajouter lb vserver vServer-LB-1 HTTP 10.102.29.60 80
Pour lier un service nommé Service-HTTP-1 à un serveur virtuel nommé vServer-LB-1	bind lb vserver vServer-LB-1 Service-HTTP-1
Pour lier un service nommé Service-HTTP-2 à un serveur virtuel nommé vServer-LB-1	bind lb vserver vServer-LB-1 Service-HTTP-2

Tableau 2 Tâches de configuration initiales

Pour plus d'informations sur les tâches de configuration initiales, voir Configuration de l'équilibrage de charge de base.

Tâche	Commande
Pour afficher les propriétés d'un serveur virtuel nommé vServer-LB-1	afficher lb vserver vServer-LB-1
Pour afficher les statistiques d'un serveur virtuel nommé vServer-LB-1	start lab vserver vServer-LB-1
Pour afficher les propriétés d'un service nommé Service-HTTP-1	afficher le service Service-HTTP-1
Pour consulter les statistiques d'un service nommé Service-HTTP-1	service d'état Service-HTTP-1
Pour afficher les liaisons d'un service nommé Service-HTTP-1	afficher les liaisons de service Service-HTTP-1

Tableau 3. Tâches de vérification

Tâche	Commande
Pour configurer la persistance sur un serveur virtuel nommé vServer-LB-1	set lb vserver vServer-LB-1 -PersistenceType SOURCEIP -PersistenceMask 255.255.255.255 -timeout 2
Pour configurer la persistance de COOKIEINSERT sur un serveur virtuel nommé vServer-LB-1	set lb vserver vServer-LB-1 -PersistenceType COOKIEINSERT
Pour configurer la persistance passive des URL sur un serveur virtuel nommé vServer-LB-1	set lb vserver vServer-LB-1 -PersistenceType URLPASSIVE
Pour configurer un serveur virtuel afin de rediriger la demande du client vers une URL sur un serveur virtuel nommé vServer-LB-1	définir lb vserver vServer-LB-1 -URL de redirection `http://www.newdomain.com/mysite/maintenance`
Pour définir un serveur virtuel de sauvegarde sur un serveur virtuel nommé vServer-LB-1	set lb vserver vServer-LB-1 -BackupvServer vServer-LB-2

Tableau 4. Tâches de personnalisation

Pour plus d'informations sur la configuration de la persistance, consultez Choix et configuration des

paramètres de persistance. Pour plus d'informations sur la configuration d'un serveur virtuel pour rediriger une demande client vers une URL et sur la configuration d'un serveur virtuel de sauvegarde, voir Configuration des fonctionnalités pour protéger la configuration d'équilibrage de charge.

Cas d'utilisation : comment forcer les options de cookie Secure et HttpOnly pour les sites Web à l'aide de l'appliance NetScaler

May 5, 2023

Les administrateurs Web peuvent forcer Secure, ou HttpOnly, ou les deux indicateurs sur l'ID de session et les cookies d'authentification générés par les applications Web. Vous pouvez modifier les entêtes Set-Cookie pour inclure ces deux options en utilisant un serveur virtuel d'équilibrage de charge HTTP et en réécrivant les politiques sur une appliance NetScaler.

- **HttpOnly** - Cette option sur un cookie oblige les navigateurs Web à renvoyer le cookie à l'aide du protocole HTTP ou HTTPS uniquement. Les méthodes non HTTP telles que les références JavaScript document.cookie ne peuvent pas accéder au cookie. Cette option permet de prévenir le vol de cookie dus à des scripts intersites.

  > REMARQUE
  >
  > Vous ne pouvez pas utiliser l'option HttpOnly lorsqu'une application Web a besoin d'accéder au contenu des cookies à l'aide d'un script côté client, tel que JavaScript ou une applet Java côté client. Vous pouvez utiliser la méthode mentionnée dans ce document pour réécrire uniquement les cookies générés par le serveur et non les cookies générés par l'appliance NetScaler. Par exemple, AppFirewall, persistance, cookies de session VPN, etc.

- **Sécurisé** : cette option sur un cookie fait en sorte que les navigateurs Web ne renvoient que la valeur du cookie lorsque la transmission est cryptée par SSL. Cette option peut être utilisée pour empêcher le vol de cookies par écoute de connexion.

> REMARQUE
>
> La procédure suivante ne s'applique pas aux serveurs virtuels VPN.

Pour configurer l'appliance NetScaler afin de forcer les indicateurs Secure et HttpOnly à un serveur virtuel HTTP existant à l'aide de l'interface de ligne de commande

1. Créez une action de réécriture.

   Cet exemple est configuré pour définir les indicateurs Secure et HttpOnly. Si l'une ou l'autre est manquante, modifiez-la si nécessaire pour d'autres combinaisons.


```
add rewrite action act_cookie_Secure replace_all http.RES.
    full_Header ""Secure; HttpOnly; path=/"" -search "regex(re!(
    path=/\\; Secure; HttpOnly)|(path=/\\; Secure)|(path=/\\;
    HttpOnly)|(path=/)!)"
<!--NeedCopy-->
```

Cette stratégie remplace toutes les instances de « path=/ », « path=/ ; Secure », « path=/ ; Secure ; HttpOnly » et « path=/ ; HttpOnly » par « Secure ; HttpOnly ; path=/ ». Cette expression régulière (regex) échoue si la casse ne correspond pas.

2. Créez une stratégie de réécriture pour déclencher l'action.

```
add rewrite policy rw_force_secure_cookie "http.RES.HEADER("Set-
    Cookie").EXISTS" act_cookie_Secure
<!--NeedCopy-->
```

3. Liez la stratégie de réécriture au serveur virtuel à sécuriser. Si `Secure` l'option est utilisée, un serveur virtuel SSL doit être utilisé.

```
bind lb vserver mySSLVServer -policyName rw_force_secure_cookie -
    priority 100 -gotoPriorityExpression NEXT -type RESPONSE
<!--NeedCopy-->
```

Exemples :

L'exemple suivant montre le cookie avant de définir l'indicateur HttpOnly.

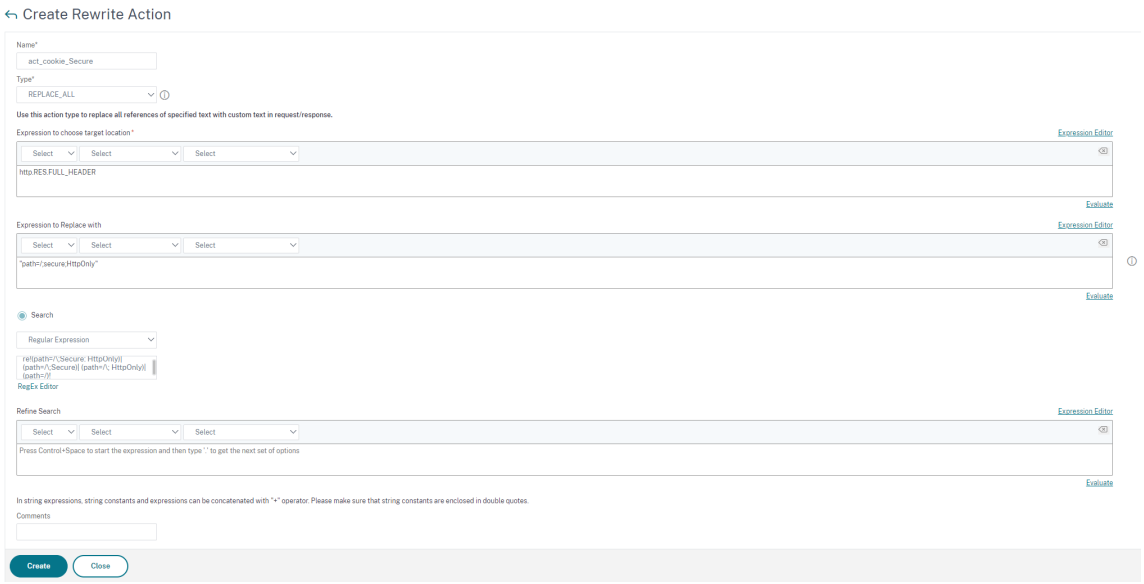
```
Set-Cookie: CtxsAuthId=C5614491; path=/Citrix/ProdWeb
<!--NeedCopy-->
```

L'exemple suivant montre le cookie après avoir défini l'indicateur HttpOnly.

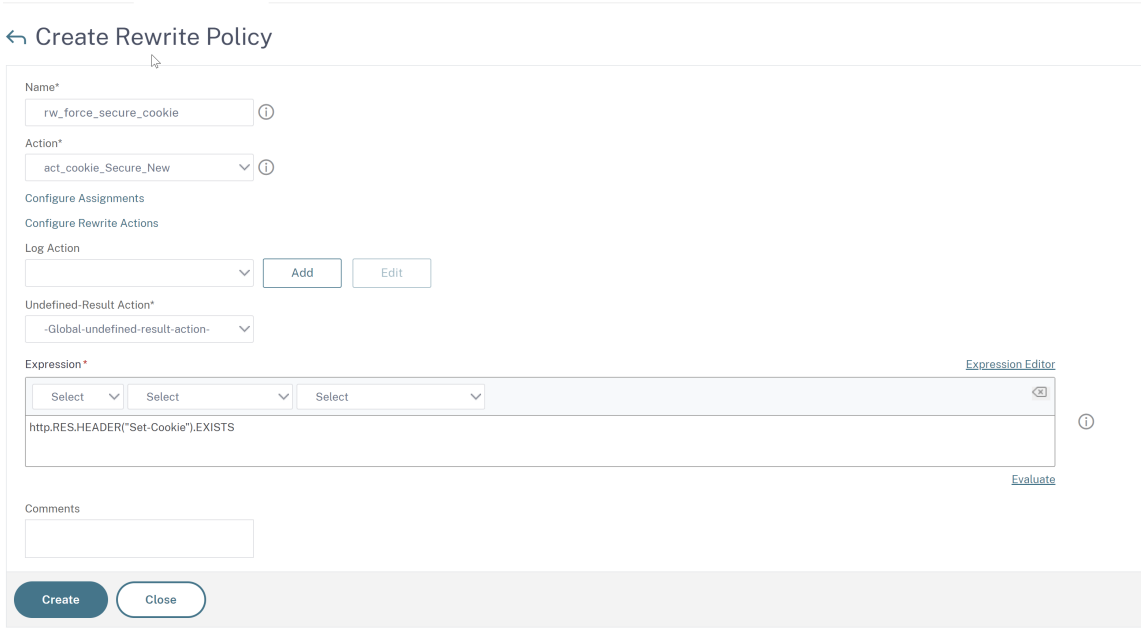
```
Set-Cookie: CtxsAuthId=C5614491; Secure; HttpOnly; path=/Citrix/ProdWeb
    /
<!--NeedCopy-->
```

Pour configurer l'appliance NetScaler de manière à forcer les indicateurs Secure et HttpOnly à un serveur virtuel HTTP existant à l'aide de l'interface graphique

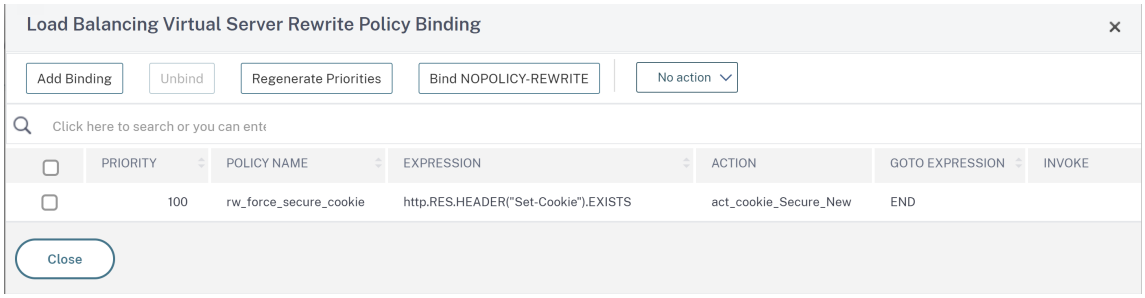
1. Accédez à **AppExpert > Réécriture > Actions**, puis cliquez sur **Ajouter** pour ajouter une nouvelle action de réécriture.



2. Accédez à **AppExpert > Réécriture > Stratégies**, puis cliquez sur **Ajouter** pour ajouter une nouvelle stratégie de réécriture.



3. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis liez la stratégie de réécriture (réponse) au serveur virtuel SSL correspondant.



Accélérez le trafic équilibré de charge en utilisant la compression

May 8, 2023

La compression est un moyen populaire d'optimiser l'utilisation de la bande passante, et la plupart des navigateurs Web prennent en charge les données compressées. Si vous activez la fonctionnalité de compression, l'appliance NetScaler intercepte les demandes des clients et détermine si le client peut accepter du contenu compressé. Après avoir reçu la réponse HTTP du serveur, la solution matérielle-logicielle examine le contenu pour déterminer s'il est compressible. Si le contenu est compressible, l'appliance le compresse, modifie l'en-tête de réponse pour indiquer le type de compression effectué et transfère le contenu compressé au client.

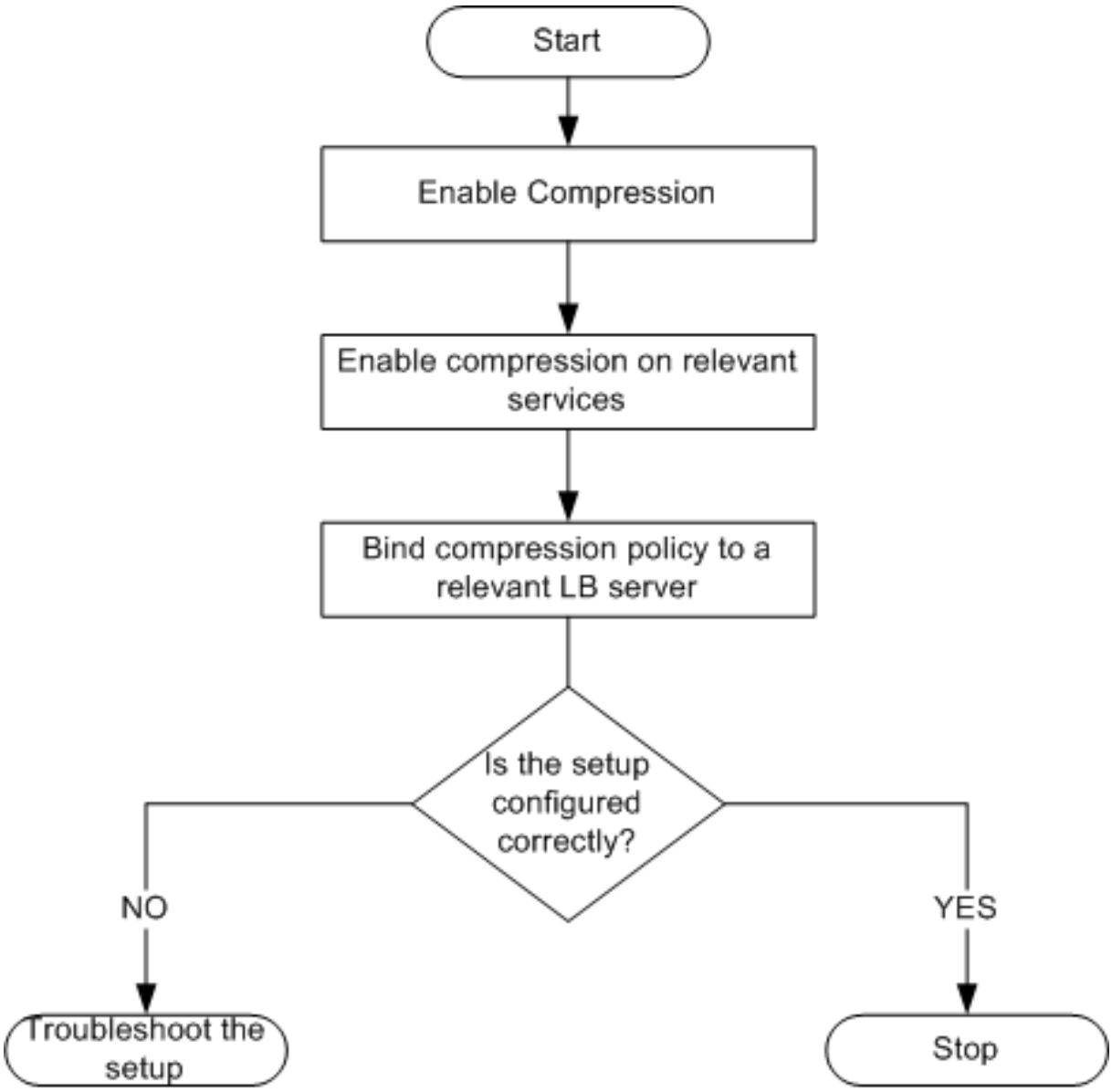
La compression NetScaler est une fonctionnalité basée sur des règles. Une stratégie filtre les demandes et les réponses pour identifier les réponses à compresser, et spécifie le type de compression à appliquer à chaque réponse. L'appliance fournit plusieurs stratégies intégrées pour compresser les types MIME courants tels que text/html, text/plain, text/xml, text/css, text/rtf, application/msword, application/vnd.ms-excel et application/vnd.ms-powerpoint. Vous pouvez également créer des stratégies personnalisées. La solution matérielle-logicielle ne compresse pas les types MIME compressés tels que les formats application/octet-stream, binary, bytes et image compressée tels que GIF et JPEG.

Pour configurer la compression, vous devez l'activer globalement et sur chaque service qui fournira des réponses que vous souhaitez compresser. Si vous avez configuré des serveurs virtuels pour l'équilibrage de charge ou la commutation de contenu, vous devez lier les stratégies aux serveurs virtuels. Dans le cas contraire, les stratégies s'appliquent à tout le trafic qui passe par l'appliance.

Séquence de tâches de configuration de compression

L'organigramme suivant montre la séquence des tâches de configuration de la compression de base dans une configuration d'équilibrage de charge.

Figure 1. Séquence de tâches de configuration de la compression



> Remarque : Les étapes de la figure ci-dessus supposent que l'équilibrage de charge a déjà été configuré.

Activer la compression

Par défaut, la compression n'est pas activée. Vous devez activer la fonction de compression pour permettre la compression des réponses HTTP envoyées au client.

Pour activer la compression à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la compression et vérifier la configuration :

- enable ns feature CMP
- show ns feature

```
    > enable ns feature CMP


    Done

    > show ns feature


           Feature                        Acronym              Status

           -------                        -------              ------

    1)     Web Logging                    WL                   ON

    2)     Surge Protection               SP                   OFF

    .

    7) Compression Control CMP ON
       .

    Done
<!--NeedCopy-->
```

Pour activer la compression à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, puis cliquez sur Paramètres.

2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur Modifier les fonctionnalités de base.
3. Dans la boîte de dialogue Configurer les fonctionnalités de base, activez la case à cocher Compression, puis cliquez sur OK.
4. Dans la ou les fonctions Activer/Désactiver ? , cliquez sur Oui.

Configurer les services pour compresser les données

Outre l'activation globale de la compression, vous devez l'activer sur chaque service qui distribuera les fichiers à compresser.

Pour activer la compression sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la compression sur un service et vérifier la configuration :

- set service \ <name> -CMP OUI
- afficher le service \ <name>

```
> show service SVC_HTTP1


SVC_HTTP1 (10.102.29.18:80) - HTTP


State: UP


Last state change was at Tue Jun 16 06:19:14 2009 (+737 ms)


Time since last state change: 0 days, 03:03:37.200


Server Name: 10.102.29.18


Server ID : 0   Monitor Threshold : 0


Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits


Use Source IP: NO
```



```
26
27
28 Client Keepalive(CKA): NO
29
30
31 Access Down Service: NO
32
33
34 TCP Buffering(TCPB): NO
35
36
37 HTTP Compression(CMP): YES
38
39
40 Idle timeout: Client: 180 sec   Server: 360 sec
41
42
43 Client IP: DISABLED
44
45
46 Cacheable: NO
47
48
49 SC: OFF
50
51
52 SP: OFF
53
54
55 Down state flush: ENABLED
56
57 1)      Monitor Name: tcp-default
58
59
60 State: DOWN     Weight: 1
61
62
63 Probes: 1095    Failed [Total: 1095 Current: 1095]
64
65
66 Last response: Failure - TCP syn sent, reset received.
67
68
69 Response Time: N/A
70
```



```
71
72 Done
73
74 <!--NeedCopy-->
```

Pour activer la compression sur un service à l'aide de l'interface graphique

1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans le volet d'informations, sélectionnez le service pour lequel vous souhaitez configurer la compression (par exemple, Service-HTTP-1), puis cliquez sur Ouvrir.
3. Sous l'onglet Avancé, sous Paramètres, activez la case à cocher Compression, puis cliquez sur OK.
4. Vérifiez que, lorsque le service est sélectionné, Compression HTTP (CMP) : ON apparaît dans la section **Détails** en bas du volet.

Liaison d'une stratégie de compression à un serveur virtuel

Si vous liez une stratégie à un serveur virtuel, la stratégie est évaluée uniquement par les services associés à ce serveur virtuel. Vous pouvez lier des stratégies de compression à un serveur virtuel à partir de la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge) ou de la boîte de dialogue Gestionnaire des stratégies de compression. Cette rubrique inclut des instructions pour lier des stratégies de compression à un serveur virtuel d'équilibrage de charge à l'aide de la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge).

Pour lier ou annuler la liaison d'une stratégie de compression à un serveur virtuel à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier ou délier une stratégie de compression à un serveur virtuel d'équilibrage de charge et vérifiez la configuration :

- <name>(lier|dissocier) lb vserver \ -PolicyName \ <string>
- afficher lb vserver \ <name>

Exemple :

```
1 > bind lb vserver lbvip -policyName ns_cmp_msapp
2 Done
3 > showlbserverlbvip
4
5 lbvip(8.7.6.6:80)-HTTPType:ADDRESS
6 State:UP
7 LaststatechangewasatThuMay2805:37:212009(+685ms)
```



```
Timesincelaststatechange:19days,04:26:50.470
EffectiveState:UP
ClientIdleTimeout:180sec
Downstateflush:ENABLED
DisablePrimaryVserverOnDown:DISABLED
PortRewrite:DISABLED
No.ofBoundServices:1(Total)1(Active)
ConfiguredMethod:LEASTCONNECTION
CurrentMethod:RoundRobin,Reason:Boundservice'sstatechangedtoUP
Mode:IP
Persistence:NONE
VserverIPandPortinsertion:OFF
Push:DISABLEDPushVServer:
PushMultiClients:NO
PushLabelRule:

BoundServiceGroups:
1)GroupName:Service-Group-1

1)Service-Group-1(10.102.29.252:80)-HTTPState:UPWeight:1

1)Policy:ns_cmp_msappPriority:0

Done

<!--NeedCopy-->
```

Pour lier ou délier une stratégie de compression à un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel auquel vous souhaitez lier ou annuler la liaison d'une stratégie de compression (par exemple, vServer-LB-1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Stratégies, cliquez sur Compression.
4. Procédez comme suit :
   - Pour lier une stratégie de compression, cliquez sur Insérer une stratégie, puis sélectionnez la stratégie que vous souhaitez lier au serveur virtuel.
   - Pour annuler la liaison d'une stratégie de compression, cliquez sur le nom de la stratégie que vous souhaitez délier du serveur virtuel, puis cliquez sur Unbind Policy.
5. Cliquez sur OK.

Sécurisez le trafic à charge équilibrée en utilisant SSL

May 5, 2023

La fonctionnalité de déchargement SSL de NetScaler améliore de manière transparente les performances des sites Web qui effectuent des transactions SSL. En déchargeant les tâches de chiffrement et de déchiffrement SSL gourmandes en CPU du serveur Web local vers l'appliance, le déchargement SSL garantit la livraison sécurisée des applications Web sans pénalisation des performances lorsque le serveur traite les données SSL. Une fois le trafic SSL déchiffré, il peut être traité par tous les services standard. Le protocole SSL fonctionne de manière transparente avec différents types de données HTTP et TCP et fournit un canal sécurisé pour les transactions utilisant ces données.

Pour configurer SSL, vous devez d'abord l'activer. Ensuite, vous configurez les services HTTP ou TCP et un serveur virtuel SSL sur l'appliance, puis liez les services au serveur virtuel. Vous devez également ajouter une paire de clés de certificat et la lier au serveur virtuel SSL. Si vous utilisez des serveurs Outlook Web Access, vous devez créer une action pour activer la prise en charge SSL et une stratégie pour appliquer l'action. Un serveur virtuel SSL intercepte le trafic chiffré entrant et le décrypte à l'aide d'un algorithme négocié. Le serveur virtuel SSL transmet ensuite les données déchiffrées aux autres entités de l'appliance pour un traitement approprié.

Pour plus d'informations sur le déchargement SSL, consultez Déchargement et accélérationSSL.

Séquence de tâches de configuration SSL

Pour configurer SSL, vous devez d'abord l'activer. Vous devez ensuite créer un serveur virtuel SSL et des services HTTP ou TCP sur l'appliance NetScaler. Enfin, vous devez lier un certificat SSL valide et les services configurés au serveur virtuel SSL.

Un serveur virtuel SSL intercepte le trafic chiffré entrant et le décrypte à l'aide d'un algorithme négocié. Le serveur virtuel SSL transmet ensuite les données décryptées aux autres entités de l'appliance NetScaler pour un traitement approprié.

L'organigramme suivant montre la séquence des tâches de configuration d'une configuration de déchargement SSL de base.

Figure 1. Séquence de tâches pour configurer le déchargement SSL

Activer le déchargement SSL

Commencez par activer la fonctionnalité SSL. Vous pouvez configurer des entités SSL sur l'appliance sans activer la fonctionnalité SSL, mais elles ne fonctionneront pas tant que vous n'aurez pas activé SSL.

Activer SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer le déchargement SSL et vérifier la configuration :

```
-  enable ns feature SSL
-  show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature ssl

Done


> show ns feature


Feature Acronym Status


------- ------- ------


1) Web Logging WL ON


2) SurgeProtection SP OFF


3) Load Balancing LB ON . . .


 9) SSL Offloading SSL ON


10) Global Server Load Balancing GSLB ON . .

```



```
29
30 Done >
31 <!--NeedCopy-->
```

Activer SSL à l'aide de l'interface graphique

Procédez comme suit :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Dans le volet d'informations, sous **Modes et fonctionnalités**, cliquez sur **Modifier les fonctionnalités de base**.
3. Activez la case à cocher **Déchargement SSL**, puis cliquez sur **OK**.
4. Dans la ou les **fonctions Activer/Désactiver ?**, cliquez sur **Oui**.

Créer des services HTTP

Un service de la solution matérielle-logicielle représente une application sur un serveur. Une fois configurés, les services sont désactivés jusqu'à ce que la solution matérielle-logicielle puisse atteindre le serveur sur le réseau et en surveiller l'état. Cette rubrique décrit les étapes de création d'un service HTTP.

Remarque : Pour le trafic TCP, effectuez les procédures suivantes, mais créez des services TCP à la place des services HTTP.

Ajouter un service HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un service HTTP et vérifier la configuration :

```
1 - add service <name> (<IP> | <serverName>) <serviceType> <port>
2 - show service <name>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add service SVC_HTTP1 10.102.29.18 HTTP 80
2
3
4  Done
5
6
7 > show service SVC_HTTP1
8
```



```
9
10          SVC_HTTP1 (10.102.29.18:80) - HTTP
11
12
13          State: UP
14
15
16          Last state change was at Wed Jul 15 06:13:05 2009
17
18
19          Time since last state change: 0 days, 00:00:15.350
20
21
22          Server Name: 10.102.29.18
23
24
25          Server ID : 0   Monitor Threshold : 0
26
27
28          Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
29
30
31          Use Source IP: NO
32
33
34          Client Keepalive(CKA): NO
35
36
37          Access Down Service: NO
38
39
40          TCP Buffering(TCPB): NO
41
42
43          HTTP Compression(CMP): YES
44
45
46          Idle timeout: Client: 180 sec   Server: 360 sec
47
48
49          Client IP: DISABLED
50
51
52          Cacheable: NO
53
```



```
54
55          SC: OFF
56
57
58          SP: OFF
59
60
61          Down state flush: ENABLED
62
63
64
65
66
67  1)      Monitor Name: tcp-default
68
69
70                  State: UP       Weight: 1
71
72
73                  Probes: 4       Failed [Total: 0 Current: 0]
74
75
76                  Last response: Success - TCP syn+ack received.
77
78
79                  Response Time: N/A
80
81
82   Done
83  <!--NeedCopy-->
```

Ajouter un service HTTP à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > Déchargement SSL > Services**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un service**, tapez le nom du service, l'adresse IP et le port (par exemple, SVC_HTTP1, 10.102.29.18 et 80).
4. Dans la liste **Protocole**, sélectionnez le type de service (par exemple, HTTP).
5. Cliquez sur **Créer**, puis sur **Fermer**. Le service HTTP que vous avez configuré apparaît dans la page Services.
6. Vérifiez que les paramètres que vous avez configurés sont correctement configurés en sélection-

nant le service et en affichant la section Détails en bas du volet.

Ajouter un serveur virtuel SSL

Dans une configuration de déchargement SSL de base, le serveur virtuel SSL intercepte le trafic chiffré, le déchiffre et envoie les messages en texte clair aux services liés au serveur virtuel. Le déchargement du traitement SSL gourmand en CPU vers l'appliance permet aux serveurs principaux de traiter un plus grand nombre de demandes.

Ajouter un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel SSL et vérifier la configuration :

```
1 -  add lb vserver <name> <serviceType> [<IPAddress> <port>]
2 -  show lb vserver <name>
3 <!--NeedCopy-->
```

> **Attention :** Pour garantir la sécurité des connexions, vous devez lier un certificat SSL valide au serveur virtuel SSL avant de l'activer.

Exemple :

```
1  > add lb vserver vserver-SSL-1 SSL 10.102.29.50 443
2    Done
3
4
5    > show lb vserver vserver-SSL-1
6
7
8    vserver-SSL-1 (10.102.29.50:443) - SSL Type: ADDRESS
9
10
11   State: DOWN[Certkey not bound] Last state change was at Tue Jun 16
        06:33:08 2009 (+176 ms)
12
13
14   Time since last state change: 0 days, 00:03:44.120
15
16
17   Effective State: DOWN Client Idle Timeout: 180 sec
18
19
20   Down state flush: ENABLED
```



```
21
22
23    Disable Primary Vserver On Down : DISABLED
24
25
26    No. of Bound Services : 0 (Total) 0 (Active)
27
28
29    Configured Method: LEASTCONNECTION Mode: IP
30
31
32    Persistence: NONE
33
34
35    Vserver IP and Port insertion: OFF
36
37
38    Push: DISABLED Push VServer: Push Multi Clients: NO Push Label Rule:
          Done
39  <!--NeedCopy-->
```

Ajouter un serveur virtuel SSL à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > Déchargement SSL > Serveurs virtuels**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un serveur virtuel (déchargement SSL)**, tapez le nom du serveur virtuel, l'adresse IP et le port.
4. Dans la liste **Protocole**, sélectionnez le type de serveur virtuel, par exemple SSL.
5. Cliquez sur **Créer**, puis sur **Fermer**.
6. Vérifiez que les paramètres que vous avez configurés sont correctement configurés en sélectionnant le serveur virtuel et en affichant la section Détails en bas du volet. Le serveur virtuel est marqué comme étant en panne car aucune paire de clés de certificat et de services n'y sont liés.

> **Attention :** Pour garantir la sécurité des connexions, vous devez lier un certificat SSL valide au serveur virtuel SSL avant de l'activer.

Liez les services au serveur virtuel SSL

Après avoir déchiffré les données entrantes, le serveur virtuel SSL transfère les données aux services que vous avez liés au serveur virtuel.

Le transfert de données entre la solution matérielle-logicielle et les serveurs peut être chiffré ou en texte clair. Si le transfert de données entre l'appliance et les serveurs est chiffré, l'intégralité de la transaction est sécurisée de bout en bout. Pour plus d'informations sur la configuration du système pour une sécurité de bout en bout, consultez Déchargement et accélération SSL.

Lier un service à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier un service au serveur virtuel SSL et vérifier la configuration :

```
- bind lb vserver <name> <serviceName>
- show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind lb vserver vserver-SSL-1 SVC_HTTP1



  Done


  > show lb vserver vserver-SSL-1 vserver-SSL-1 (10.102.29.50:443) -
     SSL Type:


  ADDRESS State: DOWN[Certkey not bound]


  Last state change was at Tue Jun 16 06:33:08 2009 (+174 ms)


  Time since last state change: 0 days, 00:31:53.70


  Effective State: DOWN Client Idle


  Timeout: 180 sec


  Down state flush: ENABLED Disable Primary Vserver On Down :
```



```
28
29
30    DISABLED No. of Bound Services : 1 (Total) 0 (Active)
31
32
33    Configured Method: LEASTCONNECTION Mode: IP Persistence: NONE Vserver
          IP and
34
35
36    Port insertion: OFF Push: DISABLED Push VServer: Push Multi Clients:
         NO Push Label Rule:
37
38
39
40
41
42    1) SVC_HTTP1 (10.102.29.18: 80) - HTTP
43
44
45    State: DOWN Weight: 1
46
47
48    Done
49  <!--NeedCopy-->
```

Liaison d'un service à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Déchargement SSL > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Sous l'onglet **Services**, dans la colonne **Actif**, cochez les cases en regard des services que vous souhaitez lier au serveur virtuel sélectionné.
4. Cliquez sur **OK**.
5. Vérifiez que le compteur Nombre de services liés dans la section Détails en bas du volet est incrémenté du nombre de services liés au serveur virtuel.

Ajouter une paire de clés de certificat

Un certificat SSL fait partie intégrante du processus d'échange de clés SSL et de chiffrement/déchiffrement. Le certificat est utilisé lors d'une connexion SSL pour établir l'identité du serveur SSL. Vous pouvez utiliser un certificat SSL valide et existant que vous possédez sur l'appliance NetScaler, ou créer votre propre certificat SSL. L'appliance prend en charge les certificats RSA jusqu'à 4096 bits.

Les certificats ECDSA avec seulement les courbes suivantes sont pris en charge :

- prime256v1 (P_256 sur ADC)
- secp384r1 (P_384 sur l'ADC)
- secp521r1 (P_521 sur ADC ; pris en charge sur VPX uniquement)
- secp224r1 (P_224 sur ADC ; pris en charge sur VPX uniquement)

> **Remarque :** Citrix vous recommande d'utiliser un certificat SSL valide qui a été émis par une autorité de certification approuvée. Les certificats non valides et les certificats auto-créés ne sont pas compatibles avec tous les clients SSL.

Avant qu'un certificat puisse être utilisé pour le traitement SSL, vous devez l'associer à la clé correspondante. La paire de clés de certificat est ensuite liée au serveur virtuel et utilisée pour le traitement SSL.

Ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

> **Remarque :** Pour plus d'informations sur la création d'une paire de clés de certificat ECDSA, voir Créer une paire de clés de certificat ECDSA.

À l'invite de commandes, tapez les commandes suivantes pour créer une paire de clés de certificat et vérifier la configuration :

```
1 - add ssl certKey <certkeyName> -cert <string> [-key <string>]
2 - show sslcertkey <name>
3 <!--NeedCopy-->
```

Exemple :

```
1  > add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-root.key
2
3   Done
4
5
6  > show sslcertkey CertKey-SSL-1
7
8
9     Name: CertKey-SSL-1 Status: Valid,
10
11
12    Days to expiration:4811 Version: 3
13
14
15    Serial Number: 00 Signature Algorithm: md5WithRSAEncryption Issuer:
         C=US,ST=California,L=San
16
17
```



```
18     Jose,O=Citrix ANG,OU=NS Internal,CN=de fault
19
20
21     Validity Not Before: Oct 6 06:52:07 2006 GMT Not After : Aug 17
           21:26:47 2022 GMT
22
23
24     Subject: C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS Internal,
           CN=d efault Public Key
25
26
27     Algorithm: rsaEncryption Public Key
28
29
30     size: 1024
31
32
33   Done
34 <!--NeedCopy-->
```

Ajouter une paire de clés de certificat à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > SSL > Certificats**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Installer le certificat**, dans la zone de texte Nom de la paire de clés de certificat, tapez un nom pour la paire de clés de certificat que vous souhaitez ajouter, par exemple CertKey-SSL-1.
4. Sous **Détails**, dans Nom du fichier de certificat, cliquez sur **Parcourir (Appliance)** pour localiser le certificat. Le certificat et la clé sont tous deux stockés dans le dossier /nsconfig/ssl/ de l'appliance. Pour utiliser un certificat présent sur le système local, sélectionnez Local.
5. Sélectionnez le certificat que vous souhaitez utiliser, puis cliquez sur **Sélectionner**.
6. Dans Nom du fichier de clé privée, cliquez sur **Parcourir (Appliance)** pour localiser le fichier de clé privée. Pour utiliser une clé privée présente sur le système local, sélectionnez Local.
7. Sélectionnez la clé que vous souhaitez utiliser, puis cliquez sur **Sélectionner**. Pour chiffrer la clé utilisée dans la paire de clés de certificat, tapez le mot de passe à utiliser pour le chiffrement dans la zone de texte Mot de passe.
8. Cliquez sur **Installer**.
9. Double-cliquez sur la paire de clés de certificat et, dans la fenêtre Détails du certificat, vérifiez que les paramètres ont été correctement configurés et enregistrés.

Liaison d'une paire de clés de certificat SSL au serveur virtuel

Après avoir associé un certificat SSL à la clé correspondante, liez la paire de clés de certificat au serveur virtuel SSL afin qu'elle puisse être utilisée pour le traitement SSL. Les sessions sécurisées nécessitent l'établissement d'une connexion entre l'ordinateur client et un serveur virtuel SSL sur l'appliance. Le traitement SSL est ensuite effectué sur le trafic entrant sur le serveur virtuel. Par conséquent, avant d'activer le serveur virtuel SSL sur l'appliance, vous devez lier un certificat SSL valide au serveur virtuel SSL.

Liez une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une paire de clés de certificat SSL à un serveur virtuel et vérifier la configuration :

```
-  bind ssl vserver <vServerName> -certkeyName <string>
-  show ssl vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind ssl vserver Vserver-SSL-1 -certkeyName CertKey-SSL-1

Done


> show ssl vserver Vserver-SSL-1




    Advanced SSL configuration for VServer Vserver-SSL-1:


    DH: DISABLED


    Ephemeral RSA: ENABLED Refresh Count: 0


    Session Reuse: ENABLED Timeout: 120 seconds


```



```
24       Cipher Redirect: ENABLED
25
26
27       SSLv2 Redirect: ENABLED
28
29
30       ClearText Port: 0
31
32
33       Client Auth: DISABLED
34
35
36       SSL Redirect: DISABLED
37
38
39       Non FIPS Ciphers: DISABLED
40
41
42       SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
43
44
45
46
47
48 1) CertKey Name: CertKey-SSL-1 Server Certificate
49
50
51 1) Cipher Name: DEFAULT
52
53
54    Description: Predefined Cipher Alias
55
56
57 Done
58 <!--NeedCopy-->
```

Liez une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > Déchargement SSL > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel auquel vous souhaitez lier la paire de clés de certificat, par exemple, vServer-SSL-1, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue **Configurer le serveur virtuel (déchargement SSL)**, sous l'onglet

Paramètres SSL, sous **Disponible**, sélectionnez la paire de clés de certificat que vous souhaitez lier au serveur virtuel. Cliquez ensuite sur **Ajouter**.

4. Cliquez sur **OK**.
5. Vérifiez que la paire de clés de certificat que vous avez sélectionnée apparaît dans la zone Configuré.

Configurer la prise en charge de Outlook Web

Si vous utilisez des serveurs Outlook Web Access (OWA) sur votre appliance NetScaler, vous devez configurer l'appliance pour insérer un champ d'en-tête spécial, FRONT-END-HTTPS : ON, dans les requêtes HTTP adressées aux serveurs OWA, afin que les serveurs génèrent des liens URL comme au lieu de. `https://http://`

Remarque : Vous pouvez activer la prise en charge d'OWA pour les serveurs et services virtuels SSL basés sur HTTP uniquement. Vous ne pouvez pas l'appliquer aux serveurs et services virtuels SSL basés sur TCP.

Pour configurer la prise en charge d'OWA, procédez comme suit :

- Créez une action SSL pour activer la prise en charge d'OWA.
- Créez une stratégie SSL.
- Liez la stratégie au serveur virtuel SSL.

Créer une action SSL pour activer la prise en charge d'OWA

Avant de pouvoir activer la prise en charge d'Outlook Web Access (OWA), vous devez créer une action SSL. Les actions SSL sont liées aux stratégies SSL et sont déclenchées lorsque les données entrantes correspondent à la règle spécifiée par la stratégie.

Créer une action SSL pour activer la prise en charge d'OWA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une action SSL afin d'activer la prise en charge d'OWA et de vérifier la configuration :

```
1 -  add ssl action <name> -OWASupport ENABLED
2 -  show SSL action <name>
3 <!--NeedCopy-->
```

Exemple :

```
1     > add ssl action Action-SSL-OWA -OWASupport enabled
2
```



```
3
4
5
6       Done
7
8
9       > show SSL action Action-SSL-OWA
10
11
12      Name: Action-SSL-OWA
13
14
15      Data Insertion Action: OWA
16
17
18      Support: ENABLED
19
20
21      Done
22  <!--NeedCopy-->
```

Créer une action SSL pour activer la prise en charge d'OWA à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > SSL > Stratégies**.
2. Dans le volet de détails, sous l'onglet **Actions**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action SSL**, dans la zone de texte Nom, tapez Action-SSL-OWA.
4. Sous Outlook Web Access, sélectionnez **Activé**.
5. Cliquez sur **Créer**, puis sur **Fermer**.
6. Vérifiez que Action-SSL-OWA apparaît dans la page **Actions SSL** .

Créer des stratégies SSL

Les stratégies SSL sont créées à l'aide de l'infrastructure de stratégies. Chaque stratégie SSL est liée à une action SSL, et l'action est exécutée lorsque le trafic entrant correspond à la règle configurée dans la stratégie.

Créer une stratégie SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une stratégie SSL et vérifier la configuration :

```
1 -  add ssl policy <name> -rule <expression> -reqAction <string>
2 -  show ssl policy <name>
3 <!--NeedCopy-->
```

Exemple :

```
1  > add ssl policy-SSL-1 -rule ns_true -reqaction Action-SSL-OWA
2
3  Done
4
5  > show ssl policy-SSL-1
6
7  Name: Policy-SSL-1 Rule: ns_true
8
9  Action: Action-SSL-OWA Hits: 0
10
11 Policy is bound to following entities
12
13 1) PRIORITY : 0
14
15 Done
16 <!--NeedCopy-->
```

Créer une stratégie SSL à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > SSL > Stratégies**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une stratégie SSL**, dans la zone de texte Nom, tapez le nom de la stratégie SSL (par exemple, Policy-SSL-1).
4. Dans **Demander** une action, sélectionnez l'action SSL configurée que vous souhaitez associer à cette stratégie (par exemple, Action-SSL-OWA). L'expression générale ns_true applique la stratégie à tout le trafic d'établissement de liaison SSL réussi. Toutefois, pour filtrer des réponses spécifiques, vous pouvez créer des stratégies avec un niveau de détail supérieur. Pour plus d'informations sur la configuration des expressions de stratégie granulaires, consultez Actions et stratégies SSL.
5. Dans **Expressions nommées**, choisissez l'expression générale intégrée ns_true et cliquez sur

Ajouter une expression. L'expression ns_true apparaît désormais dans la zone de texte Expression.

6. Cliquez sur **Créer**, puis sur **Fermer**.
7. Vérifiez que la stratégie est correctement configurée en sélectionnant la stratégie et en affichant la section Détails en bas du volet.

Liez la stratégie SSL au serveur virtuel SSL

Après avoir configuré une stratégie SSL pour Outlook Web Access, liez la stratégie à un serveur virtuel qui interceptera le trafic Outlook entrant. Si les données entrantes correspondent à l'une des règles configurées dans la stratégie SSL, la stratégie est déclenchée et l'action qui lui est associée est exécutée.

Liez une stratégie SSL à un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie SSL à un serveur virtuel SSL et vérifier la configuration :

```
- bind ssl vserver <vServerName> -policyName <string>
- show ssl vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind ssl vserver Vserver-SSL-1 -policyName Policy-SSL-1

 Done

> show ssl vserver Vserver-SSL-1

Advanced SSL configuration for VServer Vserver-SSL-1:

DH: DISABLED

Ephemeral RSA: ENABLED

Refresh Count: 0

Session Reuse: ENABLED

Timeout: 120 seconds

Cipher Redirect: ENABLED
```



```
20
21 SSLv2 Redirect: ENABLED
22
23 ClearText Port: 0
24
25 Client Auth: DISABLED
26
27 SSL Redirect: DISABLED
28
29 Non FIPS Ciphers: DISABLED
30
31 SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
32
33 1) CertKey Name: CertKey-SSL-1 Server Certificate
34
35 1) Policy Name: Policy-SSL-1 Priority: 0
36
37 1) Cipher Name: DEFAULT Description: Predefined Cipher Alias
38
39 Done
40 <!--NeedCopy-->
```

Liez une stratégie SSL à un serveur virtuel SSL à l'aide de l'interface graphique

Procédez comme suit :

1. Accédez à **Gestion du trafic > Déchargement SSL > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel (par exemple, vServer-SSL-1), puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le serveur virtuel (déchargement SSL)**, cliquez sur **Insérer une stratégie**, puis sélectionnez la stratégie que vous souhaitez lier au serveur virtuel SSL. Vous pouvez également double-cliquer sur le champ Priorité et saisir un nouveau niveau de priorité.
4. Cliquez sur **OK**.

Caractéristiques en un coup d'œil

May 5, 2023

Les fonctionnalités de NetScaler peuvent être configurées indépendamment ou en combinaison pour répondre à des besoins spécifiques. Bien que certaines fonctionnalités appartiennent à plusieurs

catégories, les nombreuses fonctionnalités de NetScaler peuvent généralement être classées dans les catégories suivantes : fonctionnalités de commutation d'applications et de gestion du trafic, fonctionnalités d'accélération des applications, fonctionnalités de sécurité et de pare-feu des applications, et fonctionnalité de visibilité des applications.

Pour comprendre l'ordre dans lequel les fonctions effectuent leur traitement, reportez-vous à la section Ordre de traitement des fonctionnalités .

Fonctions de commutation des applications et de gestion du trafic

May 5, 2023

Vous trouverez ci-dessous les fonctionnalités de commutation d'applications et de gestion du trafic.

Déchargement SSL

Décharge de manière transparente le chiffrement et le déchiffrement SSL des serveurs Web, libérant ainsi les ressources du serveur pour répondre aux demandes de contenu. SSL pèse lourdement sur les performances d'une application et peut rendre inefficaces de nombreuses mesures d'optimisation. Le déchargement et l'accélération SSL permettent d'appliquer tous les avantages de la technologie Citrix Request Switching au trafic SSL, garantissant une livraison sécurisée des applications Web sans dégrader les performances de l'utilisateur final.

Pour plus d'informations, voir Déchargement et accélération SSL.

Listes de contrôle d'accès

Compare les paquets entrants aux listes de contrôle d'accès (ACL). Si un paquet correspond à une règle ACL, l'action spécifiée dans la règle est appliquée au paquet. Sinon, l'action par défaut (ALLOW) est appliquée et le paquet est traité normalement. Pour que la solution matérielle-logicielle compare les paquets entrants aux listes de contrôle d'accès, vous devez appliquer les listes de contrôle d'accès. Toutes les ACL sont activées par défaut, mais vous devez les appliquer pour que l'appliance NetScaler puisse comparer les paquets entrants avec elles. Si une liste de contrôle d'accès n'est pas obligatoire pour faire partie de la table de choix, mais doit tout de même être conservée dans la configuration, elle doit être désactivée avant l'application des listes de contrôle d'accès. Une appliance ADC ne compare pas les paquets entrants aux listes ACL désactivées.

Pour plus d'informations, voir Liste de contrôle d'accès.

Équilibrage de charge

Les décisions d'équilibrage de charge sont basées sur une variété d'algorithmes, notamment le tourniquet, le moins de connexions, la moindre bande passante pondérée, le moins de paquets pondéré, le temps de réponse minimal et le hachage basé sur l'URL, l'adresse IP source du domaine ou l'adresse IP de destination. Les protocoles TCP et UDP sont tous deux pris en charge, de sorte que l'appliance NetScaler peut équilibrer la charge de tout le trafic qui utilise ces protocoles comme opérateur sous-jacent (par exemple, HTTP, HTTPS, UDP, DNS, NNTP et le trafic général du pare-feu). En outre, l'appliance ADC peut maintenir la persistance de la session en fonction de l'adresse IP source, du cookie, du serveur, du groupe ou de la session SSL. Il permet aux utilisateurs d'appliquer la vérification étendue du contenu (ECV) personnalisée aux serveurs, caches, pare-feu et autres périphériques d'infrastructure afin de s'assurer que ces systèmes fonctionnent correctement et fournissent le bon contenu aux utilisateurs. Il peut également effectuer des vérifications de l'état à l'aide d'URL ping, TCP ou HTTP, et l'utilisateur peut créer des moniteurs basés sur des scripts Perl.
Pour fournir une optimisation du WAN à grande échelle, les appliances CloudBridge déployées dans les centres de données peuvent être équilibrées par le biais d'appliances NetScaler. La bande passante et le nombre de sessions simultanées peuvent être considérablement améliorés.

Pour plus d'informations, voir Équilibrage de charge.

Domaines de trafic

Les domaines de trafic permettent de créer des partitions ADC logiques au sein d'une seule appliance NetScaler. Ils vous permettent de segmenter le trafic réseau pour différentes applications. Vous pouvez utiliser des domaines de trafic pour créer plusieurs environnements isolés dont les ressources n'interagissent pas entre elles. Une application appartenant à un domaine de trafic spécifique communique uniquement avec les entités et traite le trafic au sein de ce domaine. Le trafic appartenant à un domaine de trafic ne peut pas franchir la limite d'un autre domaine de trafic. Par conséquent, vous pouvez utiliser des adresses IP dupliquées sur l'appliance tant qu'une adresse n'est pas dupliquée dans le même domaine.

Pour plus d'informations, voir Domaines de trafic.

Traduction d'adresses réseau

La traduction d'adresses réseau (NAT) implique la modification des adresses IP source et/ou de destination, et/ou des numéros de port TCP/UDP, des paquets IP qui transitent par l'appliance NetScaler. L'activation de la NAT sur l'appliance renforce la sécurité de votre réseau privé et le protège d'un réseau public tel qu'Internet, en modifiant les adresses IP source de votre réseau lorsque les données transitent par l'appliance NetScaler.

L'appliance NetScaler prend en charge les types de traduction d'adresses réseau suivants :

INAT : Dans le NAT entrant (INAT), une adresse IP (généralement publique) configurée sur l'appliance NetScaler écoute les demandes de connexion pour le compte d'un serveur. Pour un paquet de demande reçu par l'appliance sur une adresse IP publique, l'ADC remplace l'adresse IP de destination par l'adresse IP privée du serveur. En d'autres termes, la solution matérielle-logicielle agit comme un proxy entre les clients et le serveur. La configuration INAT implique des règles INAT, qui définissent une relation 1:1 entre l'adresse IP de l'appliance NetScaler et l'adresse IP du serveur.

RNAT : dans Reverse Network Address Translation (RNAT), pour une session initiée par un serveur, l'appliance NetScaler remplace l'adresse IP source des paquets générés par le serveur par une adresse IP (type SNIP) configurée sur l'appliance. La solution matérielle-logicielle empêche ainsi l'exposition de l'adresse IP du serveur dans l'un des paquets générés par le serveur. Une configuration RNAT implique une règle RNAT, qui spécifie une condition. La solution matérielle-logicielle effectue un traitement RNAT sur les paquets qui correspondent à la condition.

Traduction NAT46 sans état : Latechnologie Stateless NAT46 permet la communication entre les réseaux IPv4 et IPv6, par le biais de la traduction de paquets IPv4 vers IPv6 et vice versa, sans conserver aucune information de session sur l'appliance NetScaler. Une configuration NAT46 sans état implique une règle INAT IPv4-IPv6 et un préfixe IPv6 NAT46.

Traduction NAT64 dynamique : la fonctionnalité NAT64 dynamique permet la communication entre les clients IPv4 et les serveurs IPv6 via la traduction de paquets IPv6 vers IPv4, et vice versa, tout en conservant les informations de session sur l'appliance NetScaler. Une configuration NAT64 avec état implique une règle NAT64 et un préfixe NAT64 IPv6.

Pour plus d'informations, voir Configuration de la traduction d'adresses réseau.

Prise en charge du protocole TCP multichemin

Les appliances NetScaler prennent en charge le protocole TCP multipath (MPTCP). MPTCP est une extension de protocole TCP/IP qui identifie et utilise plusieurs chemins disponibles entre les hôtes pour maintenir la session TCP. Vous devez activer MPTCP sur un profil TCP et le lier à un serveur virtuel. Lorsque MPTCP est activé, le serveur virtuel fonctionne comme une Gateway MPTCP et convertit les connexions MPTCP avec les clients en connexions TCP qu'il maintient avec les serveurs.

Pour plus d'informations, voir MPTCP (Multi-Path TCP).

Commutation de contenu

Détermine le serveur auquel envoyer la demande sur la base des stratégies de commutation de contenu configurées. Les règles de stratégie peuvent être basées sur l'adresse IP, l'URL et les en-têtes HTTP. Cela permet de prendre des décisions de changement en fonction des caractéristiques de l'utilisateur et de l'appareil, telles que l'identité de l'utilisateur, le type d'agent utilisé et le contenu demandé par l'utilisateur.

Pour plus d'informations, voir Commutation de contenu.

Équilibrage global de charge serveur (GSLB)

Étend les fonctionnalités de gestion du trafic d'un NetScaler pour inclure des sites Internet distribués et des entreprises internationales. Que les installations soient réparties sur plusieurs emplacements réseau ou sur plusieurs clusters en un seul emplacement, NetScaler maintient la disponibilité et répartit le trafic entre eux. Il prend des décisions DNS intelligentes pour empêcher les utilisateurs d'être envoyés vers un site en panne ou en surcharge. Lorsque la méthode GSLB basée sur la proximité est activée, NetScaler peut prendre des décisions d'équilibrage de charge en fonction de la proximité du serveur DNS local (LDNS) du client par rapport aux différents sites. Le principal avantage de la méthode GSLB basée sur la proximité est un temps de réponse plus rapide résultant de la sélection du site disponible le plus proche.

Pour plus d'informations, voir Global Server Load Balancing.

Routage dynamique

Permet aux routeurs d'obtenir automatiquement des informations de topologie, des itinéraires et des adresses IP des routeurs voisins. Lorsque le routage dynamique est activé, le processus de routage correspondant écoute les mises à jour des itinéraires et publie les itinéraires. Les processus de routage peuvent également être placés en mode passif. Les protocoles de routage permettent à un routeur en amont d'équilibrer la charge du trafic vers des serveurs virtuels identiques hébergés sur deux unités NetScaler autonomes à l'aide de la technique Equal Cost Multipath.

Pour plus d'informations, reportez-vous à la section Configuration des routes dynamiques.

Équilibrage de la charge de liaison

Équilibre la charge de plusieurs liaisons WAN et assure le basculement des liaisons, ce qui optimise davantage les performances du réseau et assure la continuité de l'activité. Garantit que les connexions réseau restent hautement disponibles, en appliquant un contrôle intelligent du trafic et des vérifications de l'état pour répartir efficacement le trafic sur les routeurs en amont. Identifie la meilleure liaison WAN pour acheminer le trafic entrant et sortant en fonction des stratégies et des conditions réseau, et protège les applications contre les défaillances de WAN ou de liaison Internet en fournissant une détection rapide des pannes et un basculement sur incident.

Pour plus d'informations, voir Équilibrage de charge de liaison.

Optimisation TCP

Vous pouvez utiliser des profils TCP pour optimiser le trafic TCP. Les profils TCP définissent la façon dont les serveurs virtuels NetScaler traitent le trafic TCP. Les administrateurs peuvent utiliser les profils TCP intégrés ou configurer des profils personnalisés. Après avoir défini un profil TCP, vous pouvez le lier à un seul serveur virtuel ou à plusieurs serveurs virtuels.

Voici quelques-unes des principales fonctionnalités d'optimisation qui peuvent être activées par les profils TCP :

- TCP Keep-Avie : vérifie l'état opérationnel des homologues à des intervalles de temps spécifiés pour éviter que la liaison ne soit interrompue.
- Accusé de réception sélectif (SACK) — Améliore les performances de transmission des données, en particulier dans les réseaux LFN (Long Fat Networks).
- Mise à l'échelle de la fenêtre TCP : permet un transfert efficace de données sur les réseaux longs (LFN).

Pour plus d'informations sur les profils TCP, voir Configuration des profils TCP.

CloudBridge Connector

La fonctionnalité NetScaler CloudBridge Connector, élément fondamental du framework Citrix OpenCloud, est un outil utilisé pour créer un centre de données étendu au cloud. L'OpenCloud Bridge vous permet de connecter une ou plusieurs appliances NetScaler ou appliances virtuelles NetScaler sur le cloud à votre réseau sans reconfigurer votre réseau. Les applications hébergées dans le cloud semblent s'exécuter sur un réseau d'entreprise contigu. L'objectif principal d'OpenCloud Bridge est de permettre aux entreprises de déplacer leurs applications vers le cloud tout en réduisant les coûts et le risque de défaillance des applications. En outre, OpenCloud Bridge augmente la sécurité du réseau dans les environnements cloud. Un pont OpenCloud est un pont réseau de couche 2 qui connecte une appliance NetScaler ou une appliance virtuelle NetScaler sur une instance cloud à une appliance NetScaler ou à une appliance virtuelle NetScaler sur votre réseau local. La connexion est établie via un tunnel qui utilise le protocole GRE (Generic Routing Encapsulation). Le protocole GRE fournit un mécanisme d'encapsulation de paquets provenant d'une grande variété de protocoles réseau à transférer via un autre protocole. Ensuite, la suite de protocoles IPSec (Internet Protocol security) est utilisée pour sécuriser la communication entre les pairs dans OpenCloud Bridge.

Pour plus d'informations, voir CloudBridge.

DataStream

La fonctionnalité NetScaler DataStream fournit un mécanisme intelligent de commutation de demande au niveau de la couche de base de données en distribuant les demandes en fonction de la requête SQL envoyée.

Lorsqu'il est déployé devant des serveurs de base de données, NetScaler assure une distribution optimale du trafic provenant des serveurs d'applications et des serveurs Web. Les administrateurs peuvent segmenter le trafic en fonction des informations contenues dans la requête SQL et en fonction des noms de base de données, des noms d'utilisateur, des jeux de caractères et de la taille des paquets.

Vous pouvez configurer l'équilibrage de charge pour basculer les demandes en fonction d'algorithmes d'équilibrage de charge, ou vous pouvez élaborer les critères de commutation en configurant la commutation de contenu pour prendre une décision en fonction des paramètres de requête SQL, tels que le nom d'utilisateur, les noms de base de données et les paramètres de commande. Vous pouvez également configurer des moniteurs pour suivre l'état des serveurs de base de données.

L'infrastructure de politique avancée de l'appliance NetScaler inclut des expressions que vous pouvez utiliser pour évaluer et traiter les demandes. Les expressions avancées évaluent le trafic associé aux serveurs de base de données MySQL. Vous pouvez utiliser des expressions basées sur les demandes (expressions commençant par MYSQL.CLIENT et MYSQL.REQ) dans des stratégies avancées pour prendre des décisions de changement de demande au niveau du point de liaison du serveur virtuel de commutation de contenu et des expressions basées sur les réponses (expressions commençant par MYSQL.RES) pour évaluer les réponses du serveur aux utilisateurs moniteurs de santé configurés.

> Remarque : DataStream est pris en charge pour les bases de données MySQL et MS SQL.

Pour plus d'informations, voir DataStream.

Fonctionnalités d'accélération des applications

May 5, 2023

- AppCompress

  Utilise le protocole de compression gzip pour fournir une compression transparente pour les fichiers HTML et texte. Le taux de compression typique de 4:1 permet de réduire jusqu'à 50 % les besoins en bande passante en dehors du datacenter. Cela permet également d'améliorer considérablement le temps de réponse de l'utilisateur final, car cela réduit la quantité de données devant être transmises au navigateur de l'utilisateur.

- Redirection de cache

  Gère le flux de trafic vers un proxy inverse, un proxy transparent ou une ferme de cache de proxy direct. Inspecte toutes les demandes, identifie les demandes ne pouvant pas être mises en cache et les envoie directement aux serveurs d'origine via des connexions persistantes. En redirigeant intelligemment les requêtes ne pouvant pas être mises en cache vers les serveurs

Web d'origine, l'appliance NetScaler libère les ressources du cache et augmente les taux de réussite du cache tout en réduisant la consommation globale de bande passante et les délais de réponse pour ces demandes.

Pour plus d'informations, voir Redirection du cache.

- AppCache

  Permet d'optimiser la diffusion du contenu Web et des données des applications en fournissant une mise en cache Web rapide en mémoire conforme aux normes HTTP/1.1 et HTTP/1.0 pour le contenu statique et dynamique. Ce cache intégré stocke les résultats des demandes d'applications entrantes même lorsqu'une demande entrante est sécurisée ou que les données sont compressées, puis réutilise les données pour répondre aux demandes ultérieures concernant les mêmes informations. En diffusant des données directement à partir du cache intégré, l'appliance peut réduire les temps de régénération des pages en éliminant la nécessité d'entonnoir les demandes de contenu statique et dynamique vers le serveur.

  Pour plus d'informations, consultez la section Mise en cache intégrée.

- Mise en mémoire tampon TCP

  Mémorise la réponse du serveur et la livre au client à la vitesse du client, déchargeant ainsi le serveur plus rapidement et améliorant ainsi les performances des sites Web.

Fonctionnalités de sécurité des applications et de pare-feu

May 5, 2023

Vous trouverez ci-dessous les fonctionnalités de sécurité et de pare-feu.

Défense contre les attaques par déni de service (DoS)

Détecte et arrête les attaques malveillantes par déni de service distribué (DDoS) et les autres types d'attaques malveillantes avant qu'elles n'atteignent vos serveurs, ce qui les empêche d'affecter les performances du réseau et des applications. L'appliance NetScaler identifie les clients légitimes et augmente leur priorité, empêchant ainsi les clients suspects de consommer un pourcentage disproportionné de ressources et de paralyser votre site. L'appliance offre une protection au niveau de l'application contre les types d'attaques malveillantes suivants :

- Attaques par inondation SYN
- Attaques de pipeline
- Attaques en forme de larme
- Attaques terrestres

- Attaques fraggle
- Attaques de connexion Zombie

L'appliance se défend de manière agressive contre ces types d'attaques en empêchant l'allocation de ressources serveur pour ces connexions. Cela permet d'isoler les serveurs du flot écrasant de paquets associé à ces événements.

L'appliance protège également les ressources réseau contre les attaques ICMP en utilisant la limitation de débit ICMP et l'inspection agressive des paquets ICMP. Il effectue un réassemblage IP puissant, supprime une variété de paquets suspects et mal formés et applique des listes de contrôle d'accès (ACL) au trafic du site pour une protection supplémentaire.

Pour plus d'informations, consultez AppQoE.

Filtrage de contenu

Offre une protection contre les attaques malveillantes des sites Web au niveau de la couche 7. L'appliance inspecte chaque demande entrante en fonction des règles configurées par l'utilisateur en fonction des en-têtes HTTP, et exécute l'action configurée par l'utilisateur. Les actions peuvent inclure la réinitialisation de la connexion, la suppression de la demande ou l'envoi d'un message d'erreur au navigateur de l'utilisateur. Cela permet à l'appliance de filtrer les demandes indésirables et de réduire l'exposition de vos serveurs aux attaques.

Cette fonctionnalité peut également analyser les requêtes HTTP GET et POST et filtrer les signatures erronées connues, ce qui lui permet de défendre vos serveurs contre les attaques HTTP.

Pour plus d'informations, voir Filtrage de contenu.

Répondeur

Fonctionne comme un filtre avancé et peut être utilisé pour générer des réponses de l'appliance vers le client. Certaines utilisations courantes de cette fonctionnalité sont la génération de réponses de redirection, les réponses définies par l'utilisateur et les réinitialisations.

Pour plus d'informations, voir Répondeur.

Réécriture

Modifie les en-têtes HTTP et le corps du texte. Vous pouvez utiliser la fonction de réécriture pour ajouter des en-têtes HTTP à une requête ou une réponse HTTP, apporter des modifications à des en-têtes HTTP individuels ou supprimer des en-têtes HTTP. Il vous permet également de modifier le corps HTTP des requêtes et des réponses.

Lorsque l'appliance reçoit une demande ou envoie une réponse, elle vérifie les règles de réécriture et, s'il existe des règles applicables, elle les applique à la demande ou à la réponse avant de la transmettre au serveur Web ou à l'ordinateur client.

Pour plus d'informations, voir Réécriture.

Protection contre les surtensions

Réglemente le flux des demandes des utilisateurs vers les serveurs et contrôle le nombre d'utilisateurs pouvant accéder simultanément aux ressources sur les serveurs, en mettant en file d'attente toute demande supplémentaire une fois que vos serveurs ont atteint leur capacité. En contrôlant la vitesse à laquelle les connexions peuvent être établies, l'appliance bloque les surtensions de demandes d'être transmises à vos serveurs, évitant ainsi la surcharge du site.

Pour plus d'informations, voir Protection contre les surtensions.

NetScaler Gateway

NetScaler Gateway est une solution d'accès sécurisé aux applications qui fournit aux administrateurs des politiques et des contrôles d'action granulaires au niveau des applications afin de sécuriser l'accès aux applications et aux données tout en permettant aux utilisateurs de travailler de n'importe où. Il offre aux administrateurs informatiques un point de contrôle unique et des outils pour garantir la conformité aux réglementations et les plus hauts niveaux de sécurité des informations à l'échelle de l'entreprise et à l'extérieur. En même temps, il offre aux utilisateurs un point d'accès unique (optimisé pour les rôles, les appareils et les réseaux) aux applications et données d'entreprise dont ils ont besoin. Cette combinaison unique de capacités permet de maximiser la productivité de la main-d'œuvre mobile d'aujourd'hui.

Pour plus d'informations, consultez la section NetScaler Gateway.

Pare-feu d'application

Protège les applications contre toute utilisation abusive par des pirates et des logiciels malveillants, tels que les attaques de script intersite, les attaques par débordement de la mémoire tampon, les attaques par injection SQL et la navigation forcée, en filtrant le trafic entre chaque serveur Web protégé et les utilisateurs qui se connectent à n'importe quel site Web sur ce serveur Web. Le pare-feu de l'application examine tout le trafic pour y trouver des preuves d'attaques sur la sécurité du serveur Web ou d'utilisation abusive des ressources du serveur Web, et prend les mesures appropriées pour empêcher ces attaques de se produire.

Pour plus d'informations, consultez Application Firewall.

Fonctionnalité de visibilité des applications

May 5, 2023

- Gestion de la diffusion des applications NetScaler

  NetScaler Application Delivery Management (ADM) est un collecteur hautes performances qui fournit une visibilité de bout en bout sur l'expérience utilisateur sur le trafic Web et HDX (ICA). Il collecte les enregistrements HTTP et ICA AppFlow générés par les appliances NetScaler et fournit des rapports analytiques couvrant les statistiques des couches 3 à 7. NetScaler ADM fournit une analyse approfondie des données en temps réel des cinq dernières minutes et des données historiques collectées au cours de la dernière heure, du dernier jour, de la dernière semaine et du dernier mois.

  Le tableau de bord analytique HDX (ICA) vous permet d'effectuer une analyse descendante à partir des utilisateurs HDX, des applications, des ordinateurs de bureau et même à partir des informations au niveau de la passerelle. De même, les analyses HTTP fournissent une vue d'ensemble des applications Web, des URL consultées, des adresses IP des clients et des adresses IP des serveurs, ainsi que d'autres tableaux de bord. L'administrateur peut explorer et identifier les points faibles à partir de n'importe lequel de ces tableaux de bord, en fonction du cas d'utilisation.

- Visibilité améliorée des applications grâce à AppFlow

  L'appliance NetScaler est un point de contrôle central pour tout le trafic des applications dans le centre de données. Il collecte des informations de flux et de session utilisateur utiles pour la surveillance des performances des applications, l'analyse et les applications de Business Intelligence. AppFlow transmet ces informations en utilisant le format IPFIX (Internet Protocol Flow Information Export), qui est une norme ouverte de l'Internet Engineering Task Force (IETF) définie dans la RFC 5101. IPFIX (la version normalisée de NetFlow de Cisco) est largement utilisé pour surveiller les informations de flux réseau. AppFlow définit de nouveaux éléments d'information pour représenter les informations au niveau de l'application.

  En utilisant UDP comme protocole de transport, AppFlow transmet les données collectées, appelées *enregistrements de flux*, à un ou plusieurs collecteurs IPv4. Les collecteurs regroupent les enregistrements de flux et génèrent des rapports en temps réel ou historiques.

  AppFlow fournit une visibilité au niveau des transactions pour les flux HTTP, SSL, TCP et SSL_TCP. Vous pouvez échantillonner et filtrer les types de flux que vous souhaitez surveiller.

  Pour limiter les types de flux à surveiller, en échantillonnant et en filtrant le trafic des applications, vous pouvez activer AppFlow pour un serveur virtuel. AppFlow peut également fournir des statistiques pour le serveur virtuel.

Vous pouvez également activer AppFlow pour un service spécifique, représentant un serveur d'applications, et surveiller le trafic vers ce serveur d'applications.

Pour plus d'informations, voir AppFlow.

- Analyses de flux

  Les performances de votre site Web ou de votre application dépendent de la façon dont vous optimisez la diffusion du contenu le plus fréquemment demandé. Des techniques telles que la mise en cache et la compression permettent d'accélérer la fourniture de services aux clients, mais vous devez être capable d'identifier les ressources les plus fréquemment demandées, puis de les mettre en cache ou de les compresser. Vous pouvez identifier les ressources les plus fréquemment utilisées en agrégeant des statistiques en temps réel sur le trafic du site Web ou des applications. Des statistiques telles que la fréquence d'accès à une ressource par rapport à d'autres ressources et la quantité de bande passante consommée par ces ressources vous aident à déterminer si ces ressources doivent être mises en cache ou compressées pour améliorer les performances du serveur et l'utilisation du réseau. Des statistiques telles que les temps de réponse et le nombre de connexions simultanées à l'application vous aident à déterminer si vous devez améliorer les ressources côté serveur.

  Si le site Web ou l'application ne change pas fréquemment, vous pouvez utiliser des produits qui collectent des données statistiques, puis analysent manuellement les statistiques et optimisent la diffusion du contenu. Toutefois, si vous ne souhaitez pas effectuer d'optimisations manuelles ou si votre site Web ou votre application est de nature dynamique, vous avez besoin d'une infrastructure capable non seulement de collecter des données statistiques, mais également d'optimiser automatiquement la fourniture de ressources en fonction de ces statistiques. Sur l'appliance NetScaler, cette fonctionnalité est fournie par la fonctionnalité Stream Analytics. La fonctionnalité fonctionne sur une seule appliance NetScaler et collecte des statistiques d'exécution en fonction des critères que vous définissez. Lorsqu'elle est utilisée avec les politiques NetScaler, cette fonctionnalité vous fournit également l'infrastructure dont vous avez besoin pour optimiser automatiquement le trafic en temps réel.

  Pour plus d'informations, voir Action Analytics.

Solutions NetScaler

May 5, 2023

Les solutions NetScaler simplifient la mise en place des configurations fréquemment déployées. Consultez cet espace de temps à autre pour d'autres solutions.

Cette section inclut les solutions suivantes.

- Configuration de NetScaler pour Citrix Virtual Apps and Desktops
- Préférence de zone optimisée Global Server Load Balancing (GSLB)
- Support d'Anycast dans NetScaler
- Déployez une plateforme de publicité numérique sur AWS avec NetScaler
- Améliorer l'analyse du flux de clics dans AWS à l'aide de NetScaler
- NetScaler dans un cloud privé géré par Microsoft Windows Azure Pack et Cisco ACI

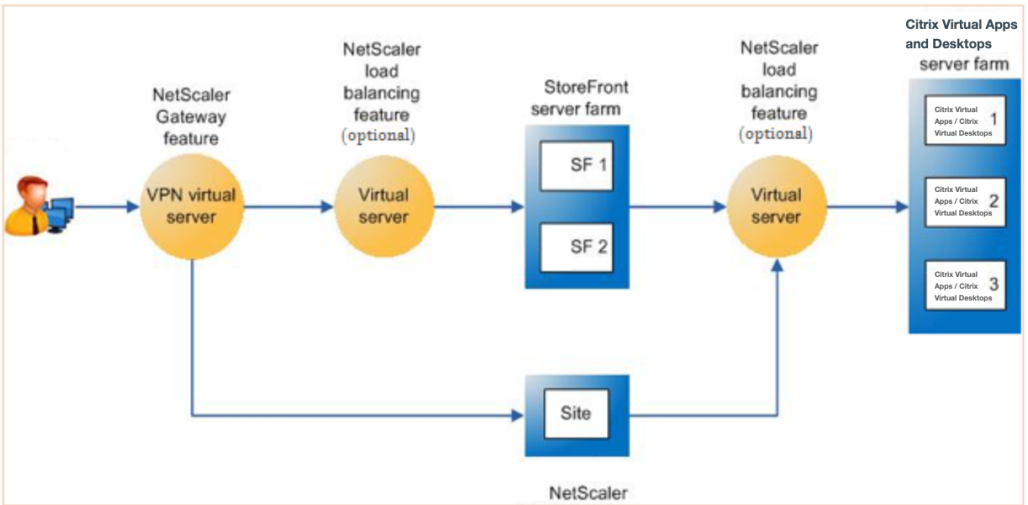
Configuration de NetScaler pour Citrix Virtual Apps and Desktops

May 5, 2023

Une appliance NetScaler peut fournir un accès distant sécurisé et équilibré à vos applications Citrix Virtual Apps and Desktops. Vous pouvez utiliser la fonctionnalité d'équilibrage de charge de NetScaler pour répartir le trafic sur le serveur Citrix Virtual Apps and Desktops. Vous pouvez utiliser la fonctionnalité NetScaler Gateway pour fournir un accès distant sécurisé aux serveurs.

NetScaler peut également accélérer et optimiser le flux de trafic et proposer des fonctionnalités de visibilité utiles pour les déploiements de Citrix Virtual Apps and Desktops.

Figure 1. Configuration de l'appliance NetScaler dans Citrix Virtual Apps and Desktops



La figure précédente montre les composants impliqués dans ce déploiement :

- **NetScaler Gateway.** Fournit l'URL pour l'accès des utilisateurs et assure la sécurité en authentifiant les utilisateurs.

- **Serveur virtuel d'équilibrage de charge NetScaler.** Équilibre la charge du trafic pour les serveurs StoreFront. Vous pouvez également déployer un serveur virtuel d'équilibrage de charge devant les serveurs Citrix Virtual Apps and Desktop pour équilibrer la charge des composants clés tels que XML Broker et le serveur Desktop Delivery Controller (DDC).
- **Citrix Virtual Apps and Desktops.** Fournit les applications auxquelles vos utilisateurs souhaitent accéder.

Pour configurer NetScaler pour Citrix Virtual Apps and Desktops à l'aide de l'interface graphique de NetScaler

Composants requis

- Les serveurs Citrix Virtual Apps and Desktop sont configurés et disponibles.
- Vous avez une connaissance pratique de NetScaler Gateway, NetScaler, Citrix Virtual Apps and Desktops et StoreFront
- Assurez-vous que vous avez configuré un serveur virtuel et un service et que vous avez lié le service au serveur virtuel. Pour plus d'informations, consultez :
  - Équilibre de charge Citrix Virtial Apps and Desktops
  - Équilibre de charge Citrix Virtial Apps and Desktops

Procédure :

1. Connectez-vous à l'appliance NetScaler et, dans l'onglet **Configuration**, cliquez sur **XenApp et XenDesktop**.
2. Dans le volet **Détails**, cliquez sur **Commencer**. Si la configuration existe sur NetScaler, cliquez sur le lien **Modifier** correspondant à chacune des sections que vous souhaitez modifier.
3. Sélectionnez le produit (StoreFront) qui, dans votre déploiement, fournit l'interface permettant d'accéder aux applications Citrix Virtual Apps and Desktops.
4. Configurez un accès à distance sécurisé.
   a) Dans la section **Paramètres de NetScaler Gateway**, spécifiez les détails du serveur virtuel VPN et cliquez sur **Continuer**.
   b) Dans la section **Certificat de serveur**, choisissez un certificat existant ou installez-en un nouveau et cliquez sur **Continuer**.
   c) Dans la section **Authentification**, configurez le mécanisme d'authentification principal à utiliser et spécifiez les détails du serveur ou utilisez un serveur existant et cliquez sur **Continuer**.
   d) Dans la section **StoreFront**, spécifiez les détails du serveur qui fournit l'interface permettant d'accéder aux applications, puis cliquez sur **Continuer**.
   e) Vous pouvez utiliser un serveur virtuel LB pointant vers plusieurs serveurs SF en tant que serveur StoreFront.

5. Cliquez sur **OK** pour terminer la configuration.

Préférence de zone optimisée Global Server Load Balancing (GSLB)

May 5, 2023

La préférence de zone basée sur GSLB est une fonctionnalité qui intègre Citrix Virtual Apps and Desktops, StoreFront et NetScaler pour permettre aux clients d'accéder au centre de données le plus optimisé en fonction de l'emplacement du client.

Dans le cadre d'un déploiement distribué de Citrix Virtual Apps and Desktops, StoreFront risque de ne pas sélectionner le centre de données optimal lorsque plusieurs ressources équivalentes sont disponibles à partir de plusieurs centres de données. Dans de tels cas, StoreFront sélectionne un centre de données de manière aléatoire. Il peut envoyer la demande à n'importe quel serveur Citrix Virtual Apps and Desktops de n'importe quel centre de données, quelle que soit la proximité du client qui fait la demande.

L'adresse IP du client est examinée lorsqu'une requête HTTP arrive à l'appliance NetScaler Gateway. L'adresse IP réelle du client est utilisée pour créer la liste de préférences du centre de données qui est transmise à StoreFront. Si l'appliance NetScaler est configurée pour insérer l'en-tête des préférences de zone, StoreFront 3.5 ou version ultérieure peut utiliser les informations fournies par l'appliance pour réorganiser la liste des contrôleurs de mise à disposition et se connecter à un contrôleur de mise à disposition optimal dans la même zone que le client. StoreFront sélectionne le serveur virtuel VPN de passerelle optimal pour la zone de centre de données sélectionnée, ajoute ces informations au fichier ICA avec les adresses IP appropriées et les envoie au client. StoreFront tente ensuite de lancer des applications hébergées sur les Delivery Controller du centre de données préféré avant d'essayer de contacter des contrôleurs équivalents dans d'autres centres de données.

Pour plus d'informations sur la configuration de cette solution, cliquez ici.

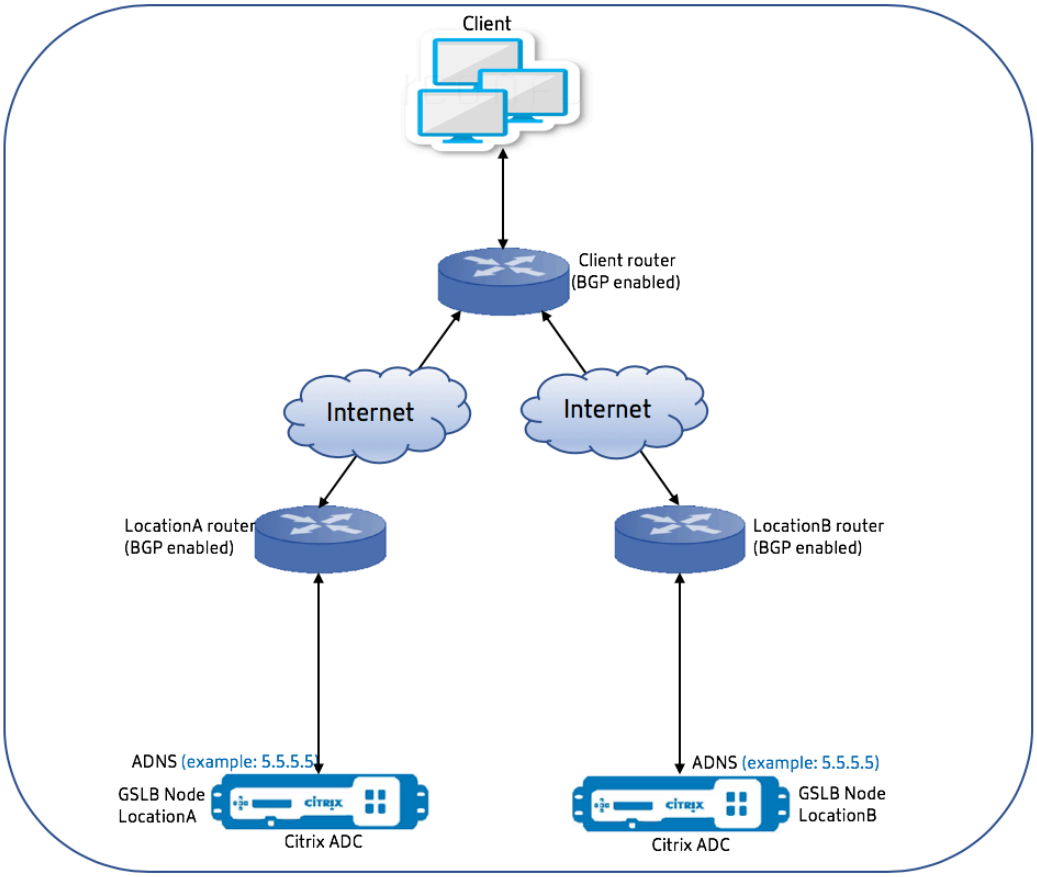
Support d'Anycast dans NetScaler

May 5, 2023

Anycast est un type de réseau dans lequel un ensemble de serveurs partagent une adresse IP. La demande du client est dirigée vers le serveur topographiquement le plus proche en fonction de ses tables de routage. Ce routage réduit les problèmes de latence, garantit une haute disponibilité et minimise les temps d'arrêt.

NetScaler prend en charge le réseau anycast grâce à l'équilibrage global de la charge des serveurs (GSLB) et aux fonctionnalités DNS.

Le schéma suivant illustre un diagramme topologique d'Anycast dans NetScaler.



Anycast GSLB

La fonctionnalité NetScaler GSLB assure l'équilibrage de charge sur les sites répartis dans le monde entier ainsi que la reprise après sinistre et garantit la disponibilité continue des applications.

En cas de panne, GSLB assure une reprise immédiate après sinistre en acheminant le trafic vers le centre de données le plus proche ou le plus performant. Toutefois, GSLB ne peut pas contrôler les éléments suivants :

- Comment le trafic DNS est acheminé vers les nœuds GSLB situés dans différents emplacements géographiques.
- Quel est le niveau de latence ajouté lorsque les requêtes DNS sont acheminées vers les nœuds GSLB ?

Dans une configuration GSLB classique, chaque centre de données possède un nœud GSLB configuré avec le serveur de noms de domaine autorisé (ADNS) spécifique au site pour recevoir les requêtes DNS. L'ADNS de chaque site est configuré en tant que serveur de noms dans le résolveur DNS. À mesure que le nombre de nœuds GSLB augmente, le nombre d'enregistrements de serveurs de noms augmente

également. Dans de tels cas, en cas de défaillance d'un centre de données, LDNS doit réessayer de résoudre le problème avec un autre serveur de noms. Cette nouvelle tentative augmente la latence de la résolution DNS.
De plus, chaque fois qu'un nœud GSLB est ajouté, les enregistrements du serveur de noms doivent être mis à jour.

Pour surmonter ces inconvénients, vous pouvez utiliser Anycast ADNS. Dans Anycast ADNS, une adresse IP ADNS unique est utilisée pour tous les nœuds GSLB et le trafic DNS est acheminé vers les nœuds GSLB à l'aide d'un routage dynamique.

Par exemple, si un site GSLB est en panne, la table de routage est mise à jour et le routage vers ce site est supprimé. Par conséquent, les requêtes DNS ne sont pas envoyées aux sites qui sont hors service. Par conséquent, il n'y a aucune nouvelle tentative.

Si un nouveau nœud GSLB est ajouté, la même adresse IP ADNS lui est attribuée. Le routage dynamique met automatiquement à jour les tables de routage avec des itinéraires vers de nouveaux sites en fonction des algorithmes de routage. Il n'est donc pas nécessaire de mettre à jour les enregistrements du serveur de noms DNS. Le déploiement de nouveaux sites GSLB est rendu plus simple et plus rapide grâce à Anycast.

Comment configurer une adresse IP ADNS en mode anycast

Activez le routage de l'hôte sur l'IP ADNS dans une appliance NetScaler et définissez le niveau RHI (Route Health Injection) approprié. La plupart du temps, il n'y aurait aucun serveur virtuel sur l'adresse IP ADNS et le niveau RHI doit donc être sélectionné sur AUCUN. L'activation de la route hôte sur l'adresse IP ADNS en fait une route du noyau. Vous pouvez ensuite activer le routage dynamique de votre choix et configurer le protocole de routage pour redistribuer les routes du noyau.

Configuration IP ADNS — Exemple

À l'invite de commandes, tapez ;

```
add service adns_public 5.5.5.5 ADNS 53

set ip 5.5.5.5 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
<!--NeedCopy-->
```

Configuration BGP dans le site GSLB — Exemple

```
Site1#sh run
!
hostname Site1
```



```
!
log syslog
log record-priority
!
ns route-install bgp
!
interface lo0
 ip address 127.0.0.1/8
 ipv6 address fe80::1/64
 ipv6 address ::1/128
!
interface vlan0
 ip address 10.102.148.94/25
 ipv6 address fe80::e84c:f4ff:fe74:4588/64
!
interface vlan2
 ip address 172.18.30.15/24
!
router bgp 5
 redistribute kernel -----> redistributing the kernel routes
 neighbor 172.18.30.30 remote-as 4
 neighbor 172.18.30.30 advertisement-interval 1
 neighbor 172.18.30.30 timers 4 16
!
End

Site1#
<!--NeedCopy-->
```

Table de routage du site GSLB - Exemple

```
Site1#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, I - Intranet
       * - candidate default

K       5.5.5.5/32 via 0.0.0.0 ---------------------------------------->
     Kernel Route for ADNS
C       10.102.148.0/25 is directly connected, vlan0
C       127.0.0.0/8 is directly connected, lo0
```



```
B       172.18.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       172.18.20.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
C       172.18.30.0/24 is directly connected, vlan2
B       192.168.3.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       192.168.5.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       192.168.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h

Gateway of last resort is not set
Site1#
<!--NeedCopy-->
```

DNS Anycast

Vous pouvez utiliser Anycast DNS pour les serveurs virtuels proxy DNS sur NetScaler. Lorsque plusieurs serveurs de noms DNS sont configurés, le résolveur DNS répond selon la méthode du round robin. Par exemple, si le résolveur ne reçoit aucune réponse du premier serveur, il passe au second serveur après expiration de la valeur de délai configurée. Le passage du premier serveur au second serveur augmente la latence de la résolution DNS. Si les résolveurs DNS sont configurés avec Anycast, cette latence peut être éliminée.

Configuration DNS — Exemple

À l'invite de commandes, tapez ;

```
add lb vserver dns DNS 5.5.5.50 53

set ip 5.5.5.50 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
<!--NeedCopy-->
```

Déployez une plateforme de publicité numérique sur AWS avec NetScaler

May 5, 2023

Compte tenu de la nature évolutive des plateformes numériques, un large éventail d'applications publicitaires est disponible. Par exemple, les réseaux sociaux, le publipostage, les vidéos, les bannières, les fenêtres contextuelles, les interstitiels, les médias enrichis, etc. Les annonceurs adoptent rapidement les réseaux de publicité vidéo, qui constituent près de 40 % du trafic publicitaire. Mais avec

l'utilisation croissante des mobiles par les utilisateurs modernes, la diffusion de publicités vidéo sur la plate-forme mobile a connu une augmentation considérable.

Les plateformes de publicité numérique sont confrontées à plusieurs défis. Certains des défis sont les suivants :

- Menaces de sécurité
- Coûts d'exploitation élevés
- Une large gamme d'appareils est disponible pour envoyer du trafic via Internet. Les différents protocoles de communication en temps réel posent les défis suivants :
  - WebRTC
  - Streaming adaptatif
  - UDP pour la vidéo, où WebRTC utilise UDP sur HTTP

Pour faire face au comportement complexe des plateformes publicitaires, la solution NetScaler, avec sa suite complète de capacités et de fonctionnalités bien intégrée à AWS, fournit un accès instantané, sécurisé et fiable à l'inventaire publicitaire numérique, en tout lieu et à tout moment. NetScaler joue un rôle essentiel dans la fourniture d'applications SaaS et Web pour les plateformes numériques.

Intégration de la plateforme de publicité numérique avec NetScaler

Présentation de la plateforme de publicité numérique

La plateforme de publicité numérique comprend les éléments clés suivants :

- Échange de publicités
- Réseau publicitaire
- Plateforme côté demande (DSP)
- Plateforme côté approvisionnement (SSP)
- Systèmes d'enchères en temps réel (RTB)

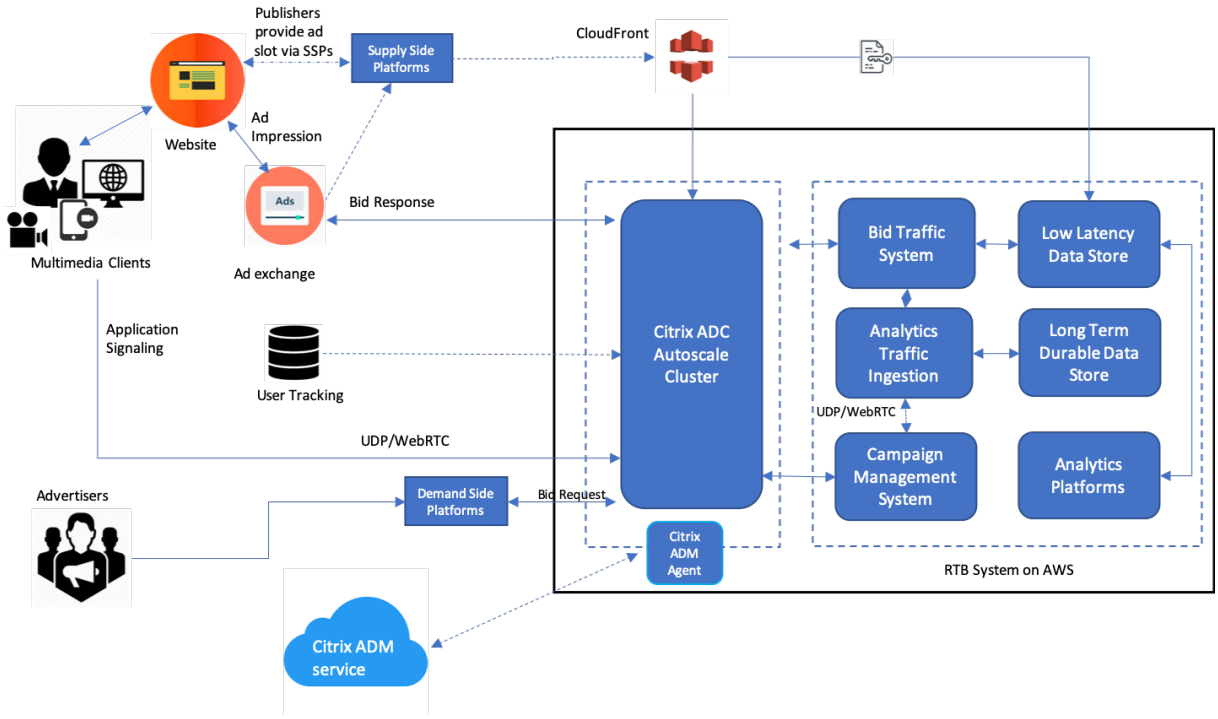
Voici un aperçu du processus suivi dans un système publicitaire.

- La première transaction a lieu lorsque l'utilisateur visite le site Web.
- Cela déclenche une demande d'enchère/de publicité (y compris les informations démographiques de l'utilisateur) qui est envoyée au serveur publicitaire ou à l'éditeur qui contacte un échange d'annonces.
- Les éditeurs d'annonces envoient la demande de publicité à un centre d'échange d'annonces via des SSP.
- L'Ad Exchange soumet cette demande et les données qui l'accompagnent au DSP pour indiquer qu'une impression ou une demande de publicité est disponible. Par conséquent, plusieurs annonceurs peuvent soumettre automatiquement des offres en temps réel pour placer leurs publicités.

- En attendant, les annonceurs doivent configurer leurs campagnes dans DSP. Utilisez les informations relatives à l'utilisateur issues de la plateforme de gestion des données (DMP) pour évaluer le montant qu'il est prêt à payer pour diffuser une publicité auprès de l'utilisateur.
- Les DSP soumettent ces offres en temps réel pour chaque impression publicitaire, car celle-ci est transmise à la plateforme d'échange de publicités.
- L'enchérisseur qui enchérit le plus dans un délai fixé par l'Ad Exchange ou les SSP obtient un créneau publicitaire accordé par les éditeurs pour diffuser leurs publicités. Dans le cas contraire, ils perdent la possibilité d'obtenir la publicité adaptée à leur groupe démographique clé.

Comment la plateforme de publicité numérique est intégrée à NetScaler

Le schéma suivant montre comment les différents composants de la plateforme publicitaire communiquent avec NetScaler et NetScaler Application Delivery Management (ADM) pour diffuser des publicités en ligne.



Comment NetScaler contribue

Dans le processus de publication de publicités, la solution NetScaler aide à gérer et à traiter l'afflux irrégulier de trafic d'enchères. Il fait office de point d'entrée pour l'ensemble du trafic afin de garantir l'évolutivité et la disponibilité dans toutes les zones de disponibilité. Pour répondre à la nature élastique du trafic publicitaire, il est déployé dans un groupe de mise à l'échelle automatique devant les applications Web et les serveurs de base de données.

La plateforme publicitaire sur AWS avec la solution NetScaler vous permet de bénéficier de performances en temps réel, d'une évolutivité élevée et d'une haute disponibilité dans le monde entier. Vous pouvez acheter et vendre des publicités multimédia, vidéo, mobiles et natives en temps réel. Cela réduit le coût opérationnel global et la latence liés à la gestion d'une plateforme publicitaire. Il s'agit du proxy le plus performant, doté de nombreuses fonctionnalités permettant de supprimer progressivement les serveurs principaux pendant Autoscale, de multiplexer les connexions et de garantir que le trafic des utilisateurs finaux n'est jamais affecté. NetScaler prend en charge l'équilibrage de charge des protocoles HTTP, UDP, WebRTC et RTSP utilisés sur les plateformes publicitaires.

NetScaler s'intègre de manière cohérente à l'environnement AWS grâce aux attributs clés suivants :

- Changement de contenu : passez à la plateforme appropriée en fonction du nom d'hôte.
- Protection de sécurité : utilisez la fonctionnalité de pare-feu des applications Web (WAF), la limitation du débit (via l'IP du client) et la protection contre les attaques DDoS.
- Mise à l'échelle automatique du trafic frontal et dorsal.
- Visibilité de bout en bout et détection des anomalies sur les appliances ADC à l'aide d'ADM.
- Faible latence

Comment NetScaler ADM y contribue

NetScaler utilise NetScaler ADM pour surmonter les défis suivants auxquels sont confrontées les plateformes de publicité numérique :

- Identifier les écarts de tendance par rapport aux performances attendues
- Analyse des performances des applications en temps réel
- Surveillance des capacités

Avantages de l'intégration de la plateforme publicitaire avec NetScaler et ADM

La solution NetScaler offre les fonctionnalités et avantages suivants aux fournisseurs de plateformes de publicité numérique.

Faible coût

- Intégrée au service AWS Autoscaling, l'instance NetScaler VPX peut augmenter ou réduire automatiquement vos ressources frontales et dorsales. Cela fournit une configuration sans contact adaptée à l'élasticité des plateformes publicitaires.
- Consolidation de la fourniture de tous les types de trafic à partir d'un seul point.

Pour plus d'informations sur AWS Autoscaling, voir Ajouter un service AWS Autoscaling principal.

Haute disponibilité

- Si une zone de disponibilité devient indisponible, NetScaler applique sa capacité de tolérance aux pannes pour détecter automatiquement les serveurs dans une autre zone de disponibilité, sans aucune interruption du trafic.
- En outre, Il met fin gracieusement aux serveurs en évitant la perte de connexions client.

Pour plus d'informations, voir Comment fonctionne la haute disponibilité sur AWS.

Analyse des performances des applications

Les analyses intelligentes de NetScaler ADM et les analyses des performances des applications garantissent de :

- Gagnez en visibilité sur les problèmes (anomalies de réponse du serveur, erreurs 5XX, etc.) qui nuisent à l'expérience de l'utilisateur final.
- Avertissez l'administrateur de prendre immédiatement des mesures correctives.

Pour plus d'informations, voir Indicateurs de performance pour l'analyse des applications.

Sécurité par pare-feu riche

Les failles de sécurité les plus courantes concernent les applications Web plutôt que les réseaux. Il est essentiel de protéger vos applications Web contre les accès non autorisés tels que les robots, les vols de données et les attaques au niveau de la couche applicative.

NetScaler fournit une sécurité complète et intégrée de couche 4 à 7 qui inclut :

- Web App Firewall (WAF) pour protéger vos applications Web, identifier et neutraliser les robots malveillants grâce à des signatures de robots régulièrement mises à jour et à une détection basée sur le comportement.
- Limitation des tarifs pour empêcher une plate-forme publicitaire d'être débordée.

Pour plus d'informations, consultez NetScaler Web App Firewall.

Sélectionnez le type d'instance AWS approprié pour la plate-forme publicitaire

Choisissez le type d'instance AWS approprié pour ADC en fonction des deux facteurs suivants :

- Nombre d'utilisateurs accédant simultanément à la plateforme publicitaire.
- Nombre moyen d'utilisateurs sur la plateforme.

Le NetScaler peut être déployé dans différentes instances EC2, notamment c5, c5n, m5, etc. Pour les plateformes publicitaires, utilisez les types d'instances AWS suivants :

- c5 ou c5n est approprié pour gérer le trafic SSL intense.
- c5.large peut gérer jusqu'à 1000 TPS SSL.

Pour plus d'informations, consultez la matrice de support VPX-AWS.

Améliorer l'analyse du flux de clics dans AWS à l'aide de NetScaler

May 5, 2023

Les clients accèdent de plus en plus aux produits de l'entreprise via diverses applications telles que les applications mobiles, les applications SaaS, etc. Par conséquent, les applications peuvent devenir une mine de données sur l'expérience client. Pour suivre le comportement des clients en ligne, les entreprises centrées sur le client forment des profils basés sur les données pour chacun de leurs clients à l'aide de ces données de comportement client.

Un flux de clics est une séquence ou un flux d'événements qui représentent les actions des utilisateurs (clics) sur un site Web ou une application mobile. Toutefois, la portée du parcours de clics s'étend au-delà des clics. Il comprend les recherches de produits, les impressions, les achats et tout événement de ce type pouvant être pertinent pour l'entreprise. La simple collecte et le stockage des données de l'expérience client n'ont pas beaucoup de valeur. Il est nécessaire de distribuer les données très complexes de manière transparente aux bons fournisseurs au bon moment. Les entreprises peuvent tirer profit des données et prendre rapidement des décisions conscientes pour améliorer leurs stratégies. Par conséquent, les entreprises utilisent de plus en plus l'analyse des flux de clics pour obtenir des informations sur le parcours de l'expérience client des applications.

Ce document vous permet de bien comprendre pourquoi les données Clickstream sont de la plus haute importance, comment elles sont collectées, stockées, distribuées et transformées en analyses significatives et exploitables.

NetScaler s'intègre à NetScaler ADM et ajoute de la valeur aux services AWS tels qu'Amazon Kinesis Data Firehose afin de fournir aux entreprises la meilleure solution d'analyse de sa catégorie qui s'articule autour des flux de clics des utilisateurs.

Cette solution NetScaler vous aide à résoudre des problèmes commerciaux complexes de manière efficace et extrêmement simple. NetScaler et AWS Kinesis aident à identifier les problèmes liés à un flux de travail mal conçu. NetScaler ADM permet de capturer les problèmes liés aux performances des applications Web et du réseau en appliquant des filtres appropriés. La combinaison de NetScaler avec NetScaler ADM et AWS Kinesis vous aide à gérer et à analyser l'énorme afflux de données de parcours de navigation à chaque phase. Cette solution est hautement disponible, évolutive, robuste et garantit que la livraison est continue et sécurisée. Ainsi, vous pouvez obtenir des informations exploitables.

Pourquoi les entreprises optent pour Clickstream Analytics ?

Les entreprises optent pour le flux de clics principalement pour comprendre comment les utilisateurs interagissent avec l'application et pour obtenir des informations sur l'amélioration des objectifs de l'application. Clickstream Analytics est un cas d'utilisation de récupération d'informations qui suit

le comportement de votre utilisateur, ses habitudes de navigation, etc. Clickstream Analytics vous donne des informations sur :

- Quel lien vos clients cliquent le plus souvent et à quel moment ?
- Où se trouvait le visiteur avant d'accéder à mon site Web ?
- Combien de temps le visiteur a-t-il passé sur chaque page ?
- Quand et où le visiteur a-t-il cliqué sur le bouton « retour » du navigateur Web ?
- Quels articles le visiteur a-t-il ajoutés (ou supprimés de) son panier d'achat ?
- À partir de quelle page le visiteur a-t-il quitté mon site Web ?

Service d'analyse pour gérer les données Clickstream à l'aide d'Amazon Kinesis

Vous pouvez utiliser Amazon Kinesis pour effectuer des analyses de flux de clics. Amazon kinesis permet l'analyse des flux de clics avec les services suivants :

- Amazon Kinesis Data Firehose
- Analyses de données Amazon Kinesis
- Amazon Kinesis Data Streams

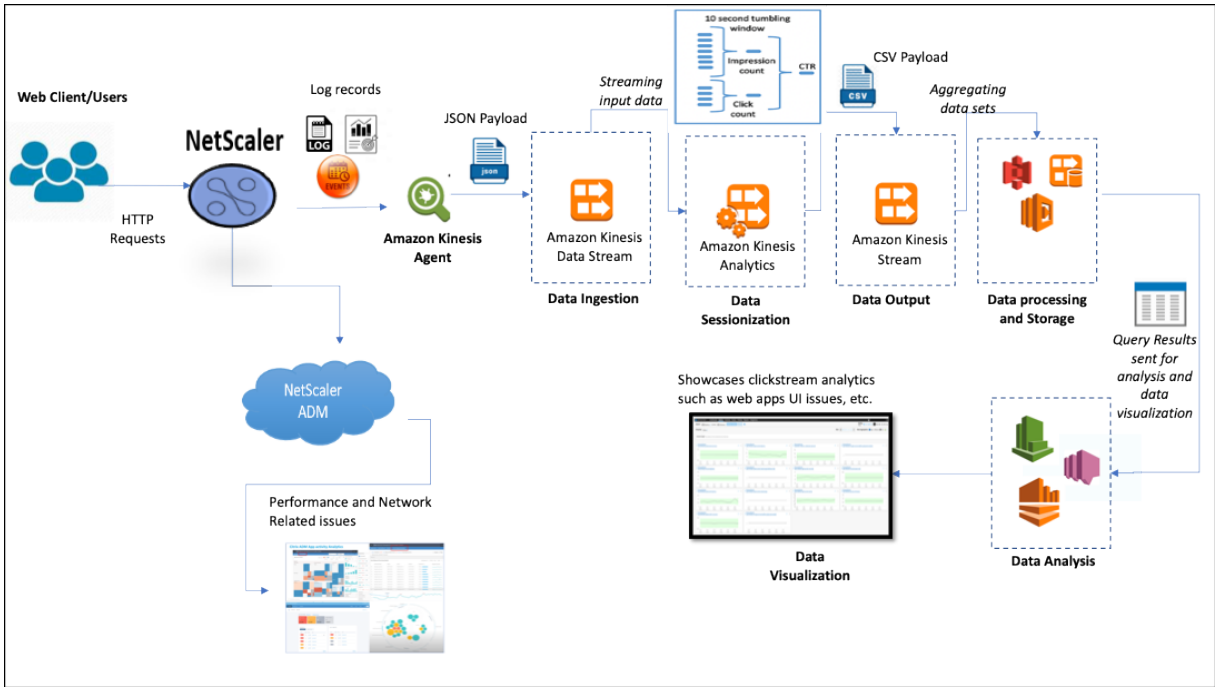
Avec Amazon Kinesis, vous pouvez collecter et analyser vos énormes ensembles de données à n'importe quelle échelle. AWS Kinesis peut gérer des données provenant de différentes sources, telles que :

- Applications mobiles et Web (par exemple, jeux, commerce électronique)
- Appareils IoT
- Applications de réseaux sociaux
- Services de trading financier
- Services géospatiaux

Comment NetScaler permet l'analyse des flux de clics

La solution NetScaler rassemble et fournit des informations de manière sécurisée sur les activités des utilisateurs, telles que les sites Web visités, la bande passante dépensée, le flux de navigation. Les entreprises analysent ce débit élevé et ces données de flux de clics continus pour corroborer l'efficacité des éléments suivants :

- Présentation du site
- Campagnes marketing
- Nouvelles fonctionnalités de l'application



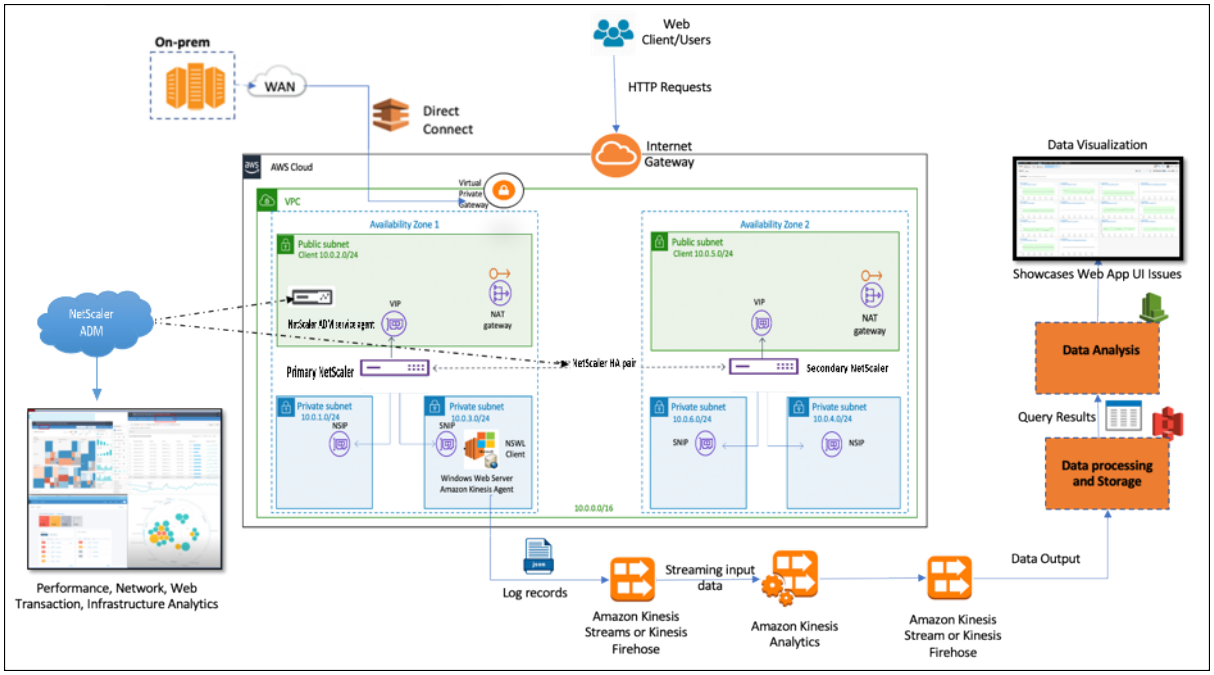
La capacité de NetScaler à fournir une protection réseau résiliente aux environnements d'entreprise permet de réduire considérablement le coût des serveurs en déchargeant les tâches de calcul intensives et en exécutant des sessions sur ces données. Cela aide les entreprises à identifier les événements en temps réel avec une haute disponibilité, une sécurité et une faible latence toujours.

Pour obtenir des informations de configuration, voir Configurer la solution NetScaler pour l'analyse du parcoursde navigation.

Comment NetScaler et NetScaler ADM complètent l'environnement AWS

Le diagramme suivant illustre le flux de travail des utilisateurs de bout en bout pour effectuer des analyses de flux de clics dans l'infrastructure AWS. Ce diagramme vous aide à comprendre les processus suivants :

- Comment l'utilisateur interagit avec NetScaler
- Comment NetScaler capture les actions des utilisateurs et génère des données de parcours de navigation
- Comment les données de parcours de clics sont transmises aux services AWS (Amazon Kinesis)
- Comment Amazon Kinesis traite les journaux de données et les stocke pour produire des analyses de flux de clics significatives



NetScaler s'intègre parfaitement à l'environnement AWS et à NetScaler ADM, qui aide les entreprises à être compatibles avec le volume variable et la nature diverse des données de parcours de navigation. Il fournit des services permettant de charger et d'analyser les connaissances en streaming en toute simplicité. Vous pouvez également créer des applications de connaissances en streaming personnalisées pour des besoins spécifiques.

Amazon Kinesis

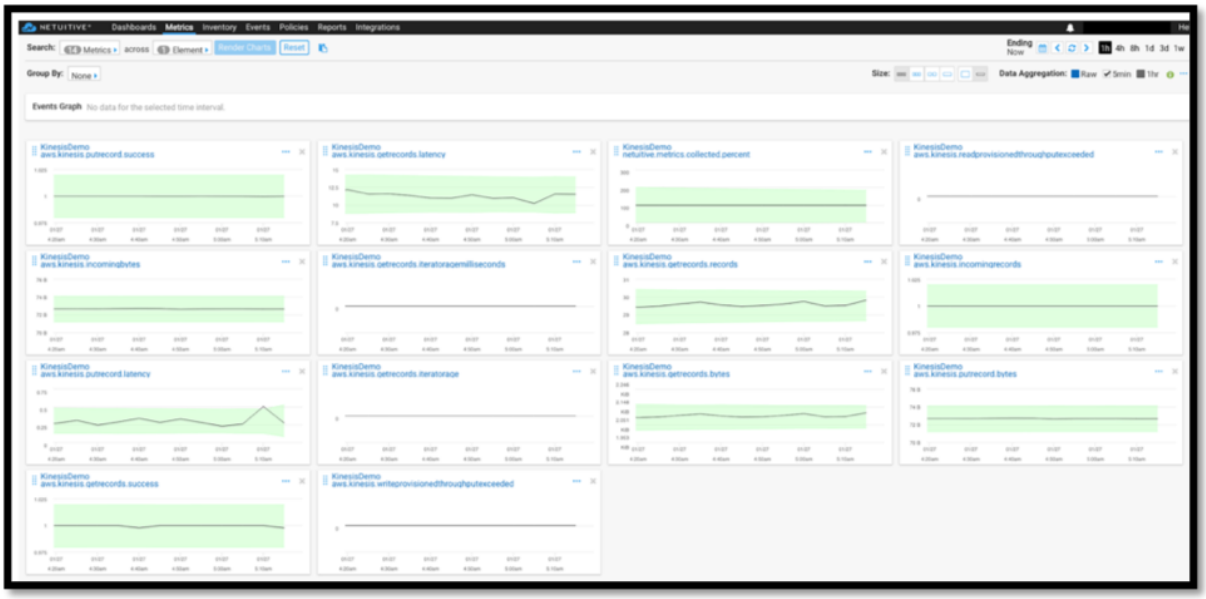
L'environnement AWS dispose de différents services qui analysent les événements utilisateur, les journaux et les métriques capturés par NetScaler. Les données peuvent être des flux de clics sur le site Web, des transactions financières, des flux de médias sociaux, des journaux informatiques et des événements de localisation.

- Amazon Kinesis Data Streams effectue des analyses dans des scénarios impliquant un flux de données en temps réel évolutif et durable qui peut capturer en continu des Go de données par seconde à partir de plusieurs sources.
- Amazon Kinesis Data Analytics peut être utilisé pour les scénarios avec une latence plus faible entre la génération de session, car l'agrégation des différents ensembles de données prend moins de temps.
- Amazon Kinesis Agent for Microsoft Windows collecte, analyse, filtre et diffuse les données d'entrée vers les flux de données Kinesis.
- Une fois les données stockées dans le cloud, vous pouvez implémenter le pipeline de données exact pour obtenir les résultats souhaités. Par exemple, vous pouvez utiliser ces informations dans Amazon Quick Sight, qui est un outil de visualisation utilisé pour créer des tableaux de

bord.

Le tableau de bord AWS Kinesis propose les offres suivantes :

- Présentation des problèmes d'interface utilisateur des applications Web
- Visualisations en temps quasi réel des mesures d'utilisation du Web telles que les événements par heure, le nombre de visiteurs et les référents.
- Analyse par session



Analyses NetScaler ADM

En utilisant NetScaler ADM avec NetScaler, vous pouvez obtenir une vue d'ensemble de tous les environnements professionnels. Les journaux capturés par NetScaler sont introduits dans NetScaler ADM, qui traite vos applications individuelles comme une entité unique. Vous pouvez obtenir des informations précieuses et résoudre efficacement les problèmes grâce aux fonctionnalités ADM suivantes :

- Analyses intelligentes
- Analyse des transactions Web
- Détection des anomalies
- Problèmes liés aux performances et au réseau

Le tableau de bord des services ADM suivant vous permet d'obtenir des informations précieuses pour résoudre efficacement les problèmes.

Comment NetScaler ADM est corrélé avec les analyses de Clickstream

Les données d'analyse des flux de clics peuvent être corrélées avec les analyses ADM pour décrire, prédire et améliorer les performances de l'application.

Pour plus d'informations sur NetScaler ADM, voir [NetScaler](https://docs.citrix.com/en-us/tech-zone/design/reference-architectures/citrix-adm.html#:~:text=Citrix%20Application%20Delivery%20Management%20(ADM)ADM %20is%20a%20centralized%20management%20solution. &text=Vous pouvez %20 utiliser %20ADM%20 vers, depuis %20A%20Single%2C%20Unifié%20Console.)

Par exemple, une organisation lors de l'analyse de ses journaux constate que la plupart des utilisateurs abandonnent leurs sites. Mais pour trouver la cause profonde de ce comportement utilisateur, ils doivent savoir quelle partie de leur application fonctionne mal. Avec les données d'analyse du parcours de navigation et les analyses ADM, vous pouvez obtenir les informations suivantes pour analyser la raison de l'abandon d'un site par les utilisateurs :

- L'utilisateur abandonne-t-il en raison d'erreurs de latence, 5xx ?
- Y a-t-il des erreurs SSL Handshake ?
- Y a-t-il une partie de l'application qui présente des problèmes de performances ou de réseau ?
- Y a-t-il une erreur 404 ou le temps de chargement de la page prend une éternité pour répondre, etc.

- Les clients sont-ils confrontés à des anomalies de réponse du serveur ?

Le service NetScaler ADM fournit des informations Web qui permettent aux administrateurs informatiques d'accélérer la résolution des problèmes grâce aux fonctionnalités suivantes :

- Fournit une surveillance intégrée et en temps réel de toutes les applications Web desservies par NetScaler.
- Obtenez une vue globale des performances de l'application en termes de temps, de latence et de comportement habituel de l'utilisateur grâce à des outils d'observabilité (tels que le graphique de service global).
- Effectuez des analyses intelligentes pour comprendre les anomalies de réponse du serveur.
- Les informations SSL contribuent à la résolution des erreurs 5xx et 4xx.
- Pour conserver les enregistrements de toutes les sessions Web qui incluent :
  - Journaux détaillés de chaque transaction Web
  - Fonction de recherche pour trouver les journaux pertinents
  - Possibilité d'isoler un utilisateur ADC-to-end par rapport à Problème ADC-to-Server

Types de données exportées par ADC pour Clickstream Analytics

NetScaler capture les différentes sources qui génèrent diverses formes de données, à savoir :

- Journaux du serveur Web

  La fonctionnalité de journalisation du serveur Web envoie les journaux des requêtes HTTP et HTTPS à un système client à des fins de stockage et de récupération. Ces journaux contiennent une énorme quantité de données, ce qui est difficile à comprendre et à comprendre. Les outils analytiques aident à la comprendre et à en apporter de la valeur. Pour plus d'informations sur la configuration, consultez la **section Configuration de la journalisation Web** de ce document.

- Syslogs

  Les Syslogs sont principalement utilisés pour la gestion des systèmes. La surveillance proactive du Syslog est rentable car elle réduit considérablement les temps d'arrêt des serveurs et autres périphériques de votre infrastructure. Syslog identifie les problèmes réseau critiques et les signale de manière proactive.

- Journaux d'accès

  Les journaux d'accès stockent des informations sur les événements survenus sur votre serveur Web. Par exemple, lorsqu'une personne visite votre site Web, un journal est enregistré et stocké pour fournir à l'administrateur du serveur Web des informations telles que l'adresse IP du visiteur, les pages qu'il consultait, les codes d'état, le navigateur utilisé. L'accès aux journaux peut être accablant, s'il y a un manque de connaissances appropriées pour les comprendre.
  Vous pouvez programmer l'intégration de votre système avec :

  - NetScaler pour une diffusion fluide

  - Kinesis pour obtenir des informations exploitables utiles aux entreprises

- Journaux d'audit

  La fonctionnalité de journalisation des audits vous permet de consigner les états de NetScaler et les informations d'état collectées par divers modules du noyau et dans les démons de niveau utilisateur.

- Journaux d'erreurs

  Le fichier journal des erreurs permet aux administrateurs de fournir plus d'informations concernant une erreur spécifique survenue sur le serveur Web.

Configurer la solution NetScaler pour l'analyse du parcours de navigation

La fonctionnalité de journalisation du serveur Web vous permet d'envoyer des journaux de requêtes HTTP et HTTPS à un système client à des fins de stockage et de récupération.

Pour configurer NetScaler pour la journalisation du serveur Web, vous devez :

- Activer la fonctionnalité de journalisation Web
- Configurez la taille de la mémoire tampon pour stocker temporairement les entrées du journal car le serveur de journaux Web s'exécute sur NetScaler.

Pour configurer la journalisation du serveur Web à l'aide de l'interface de ligne de commande :

1. Activez la fonctionnalité de journalisation du serveur Web.

```
enable ns feature WL
<!--NeedCopy-->
```

2. [Facultatif] Modifiez/configurez la taille de la mémoire tampon pour stocker les informations enregistrées.

```
set ns weblogparam -bufferSizeMB 60
<!--NeedCopy-->
```

3. Installez le client de journalisation Web NetScaler (NSWL). Pour plus d'informations, voir Installation du client de journalisation Web NetScaler (NSWL)
4. Installez le client NSWL sous Windows en effectuant les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

   a) Extrayez et copiez< release number >< build number > le fichier nswl_win–.zip du package sur un système Windows sur lequel vous souhaitez installer le client NSWL.

   b) Sur le système Windows, décompressez le fichier dans un répertoire (appelé < NSWL-HOME>). Les répertoires bin, samples et autres sont extraits.

c) À l'invite de commandes, exécutez la commande suivante à partir du < NSWL-HOME > répertoire \ bin :

```
nswl -install -f < path of the log.conf file >\log.conf
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour désinstaller le client NSWL, à l'invite de commandes, exécutez la commande suivante à partir du < NSWL-HOME > répertoire \ bin :

```
nswl -remove
<!--NeedCopy-->
```

5. Après avoir installé le client NSWL, configurez le client NSWL à l'aide de l'exécutable NSWL. Ces configurations sont stockées dans le fichier de configuration du client NSWL (log.conf).

   Exécutez les commandes suivantes à partir du répertoire dans lequel se trouve l'exécutable NSWL :

```
\ns\bin
<!--NeedCopy-->
```

6. Dans le fichier de configuration du client NSWL (log.conf), ajoutez l'adresse IP NetScaler (NSIP) à partir de laquelle le client NSWL collecte les journaux en exécutant la commande suivante dans l'invite de commande du système client :

```
nswl -addns -f < Path to the configuration(log.conf) file >\log.
   conf
<!--NeedCopy-->
```

7. Entrez le NSIP (adresse IP), le nom d'utilisateur `nsroot` et le mot de passe de l'appliance NetScaler sous la forme « identifiant de l'instance/mot de passe que vous avez défini » afin que :

   - Le client NSWL se connecte à l'ADC après avoir ajouté l'adresse IP NetScaler (NSIP) au fichier de configuration NSWL
   - ADC met en mémoire tampon les entrées du journal des demandes HTTP et HTTPS avant de les envoyer au client.
   - Le client peut filtrer les entrées (en modifiant le fichier log.conf) avant de les stocker.

> Remarque
>
> Modifiez le mot de passe par défaut pour NetScaler, puis poursuivez la configuration. Tapez la commande suivante pour modifier le mot de passe :


```
set system user nsroot -password <your password>
<!--NeedCopy-->
```

Configuration de l'agent Amazon Kinesis

Effectuez les étapes suivantes dans la console Web AWS pour configurer l'agent Amazon Kinesis :

1. Créez un fichier de configuration (appsettings.json) et déployez-le. Les fichiers de configuration définissent des ensembles de sources, de cuvettes et de tuyaux qui connectent les sources aux cuvettes, ainsi que des transformations facultatives.

   L'exemple suivant est un fichier de `appsettings.json` configuration complet qui configure Kinesis Agent pour diffuser les événements du journal des applications Windows vers Kinesis Data Firehose.

```
{

"Sources": [
    {

        "Id": "NSWLog",
        "SourceType": "DirectorySource",
        "Directory": "C:\Users\Administrator\Downloads\nswl_win
           -13.0-52.24\bin",
        "FileNameFilter": "*.log"
        "RecordParser": "TimeStamp",
        "TimestampFormat": "yyyy-MM-dddd HH:mm:ss.ffff", //
           Optional parameter required only by the timestamp
           record parser
        "TimeZoneKind": "UTC", //Local or UTC
        "SkipLines": 0 //Skip a number of lines at the beginning
           of each file
     }

    ],
"Sinks": [
    {

        "Id": "ApplicationLogKinesisFirehoseSink",
        "SinkType": "KinesisFirehose",
        "StreamName": "Delivery-ik-logs",
        "AccessKey": "Your Access Key",
        "SecretKey": "YourSecretKey",
        "Region": "ap-south-1"
```



```
26       }
27
28     ],
29  "Pipes": [
30     {
31
32     "Id": "ApplicationLogSourceToApplicationLogKinesisFirehoseSink
          ",
33     "SourceRef": "ApplicationLogSource",
34     "SinkRef": "ApplicationLogKinesisFirehoseSink"
35       }
36
37     ],
38  "Telemetrics":
39     {
40
41     "off": "true"
42       }
43
44   }
45
46  <!--NeedCopy-->
```

2. Configurez un agent Kinesis sur les sources de données pour collecter des données et les envoyer en continu à Amazon Kinesis Firehose/Kinesis Data Analytics. Pour plus d'informations, consultez Démarrage avec Amazon Kinesis Agent for Microsoft Windows.
3. Créez un flux de diffusion de données de bout en bout à l'aide d' Amazon Kinesis Firehose. Le flux de livraison transmet vos données de l'agent à la destination. La destination inclut Amazon Kinesis Analytics, Amazon Redshift, Amazon Elasticsearch service et Amazon S3. Pour la source, choisissez **Direct PUT ou d'autres sources** pour créer un flux de diffusion Kinesis Data Firehose.
4. Traitez les données de journal entrantes à l'aide de requêtes SQL dans Amazon Kinesis Analytics.
5. Chargez les données traitées depuis Kinesis Analytics vers Amazon Elasticsearch Service pour indexer les données.
6. Analysez et visualisez les données traitées à l'aide d'outils de visualisation, tels que Kibana et AWS QuickInsight Services.

Références

- Afficher et exporter des messages Syslog
- Citrix Networking pour Hybrid Multi Cloud
- Écriture dans AWK Kinesis Data Streams à l'aide de Kinesis Agent

NetScaler dans un cloud privé géré par Microsoft Windows Azure Pack et Cisco ACI

May 5, 2023

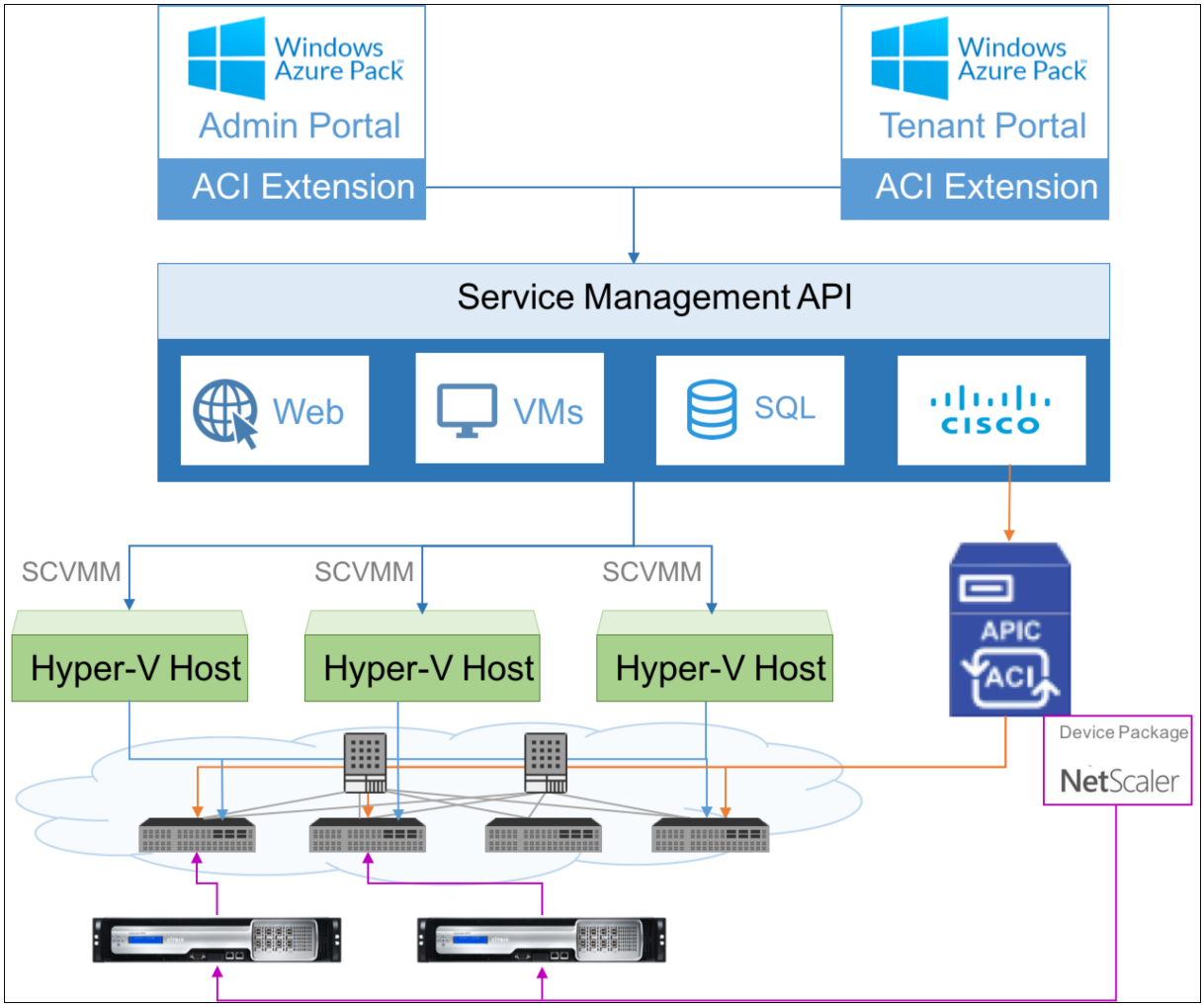
Vous pouvez utiliser une appliance NetScaler pour l'équilibrage de charge dans un cloud privé géré via Microsoft Windows Azure Pack. Le réseau du cloud privé est automatisé à l'aide de Cisco ACI et NetScaler.

Cette solution implique de nombreux points d'intégration, tels que Windows Azure Pack (WAP) vers Cisco APIC, Cisco APIC vers System Center Virtual Machine Manager (SCVMM) et Cisco APIC vers NetScaler. En tant que locataire du cloud privé, vous pouvez activer la NAT, fournir des services réseau et ajouter un équilibreur de charge.

Le WAP prend en charge les portails de locataires et d'administrateurs où un administrateur peut effectuer des tâches administratives telles que l'enregistrement ACI, la gamme VIP, l'association d'appareils NetScaler à un cloud de machines virtuelles, la création de comptes utilisateur locataires. Les locataires peuvent se connecter au portail des locataires WAP et configurer le réseau, les domaines de pont et le routage et le transfert virtuels (VRF), et utiliser les fonctionnalités d'équilibrage de charge et de RNAT de NetScaler.

> **Important**
>
> - Dans cette solution, l'appliance NetScaler fournit uniquement un équilibrage de charge de base.
> - Les locataires peuvent déployer plusieurs adresses VIP avec différents ports pour le même réseau, mais ils doivent s'assurer que la combinaison IP et port est unique.
> - Le package d'appareils NetScaler prend uniquement en charge le déploiement à contexte unique. Chaque locataire dispose d'une instance NetScaler dédiée.
> - Le WAP prend en charge les appliances NetScaler MPX et les appliances virtuelles NetScaler VPX, y compris les instances NetScaler VPX déployées sur la plateforme NetScaler SDX.

L'illustration suivante fournit une vue d'ensemble de la solution :



Composants requis

Assurez-vous que :

- Vous avez une connaissance conceptuelle des composants Cisco ACI et de NetScalers.
  - Pour plus d'informations sur Cisco ACI et ses composants, consultez la documentation du produit à l'adresse suivante : http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
  - Pour plus d'informations sur les NetScalers, consultez la documentation du produit NetScaler à l'adresse. http://docs.citrix.com/
- Tous les composants requis de Cisco ACI, y compris le Cisco APIC dans le centre de données, sont configurés et configurés. Pour plus d'informations sur Cisco ACI et ses composants, consultez la documentation du produit à l'adresse suivante : http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

- Vous savez comment intégrer Cisco ACI à Microsoft Windows Azure Pack. Consultez la documentation du produit à l'adresse : http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/virtualization/b_ACI_Virtualization_Guide_2_2_1.html.
- Vous avez une connaissance conceptuelle de Microsoft Windows Azure Pack. Consultez la documentation du produit à l'adresse : https://www.microsoft.com/en-in/cloud-platform/windows-azure-pack.
- Vous avez installé la version 11.1 ou ultérieure du logiciel NetScaler.
- Vous configurez les NetScalers dans Cisco ACI afin qu'ils puissent être gérés à l'aide de Cisco APIC.
- À partir de Cisco APIC, assurez-vous que :
  - La connectivité de gestion de Cisco APIC à NetScaler est établie.
  - Vous chargez le package du périphérique NetScaler version *11.1—52.3* et vous enregistrez le périphérique NetScaler dans Cisco ACI à l'aide de Cisco APIC.
  - Vous configurez l'appliance NetScaler dans le client commun de Cisco APIC et vous vous assurez qu'il n'y a aucun défaut dans Cisco APIC.
  - Vous avez configuré toutes les configurations spécifiques à l'APIC, telles que le pool VLAN, L3OutServicesDOM, L3Extout, le pool de ressources. Pour plus d'informations, consultez *la documentation Cisco*.

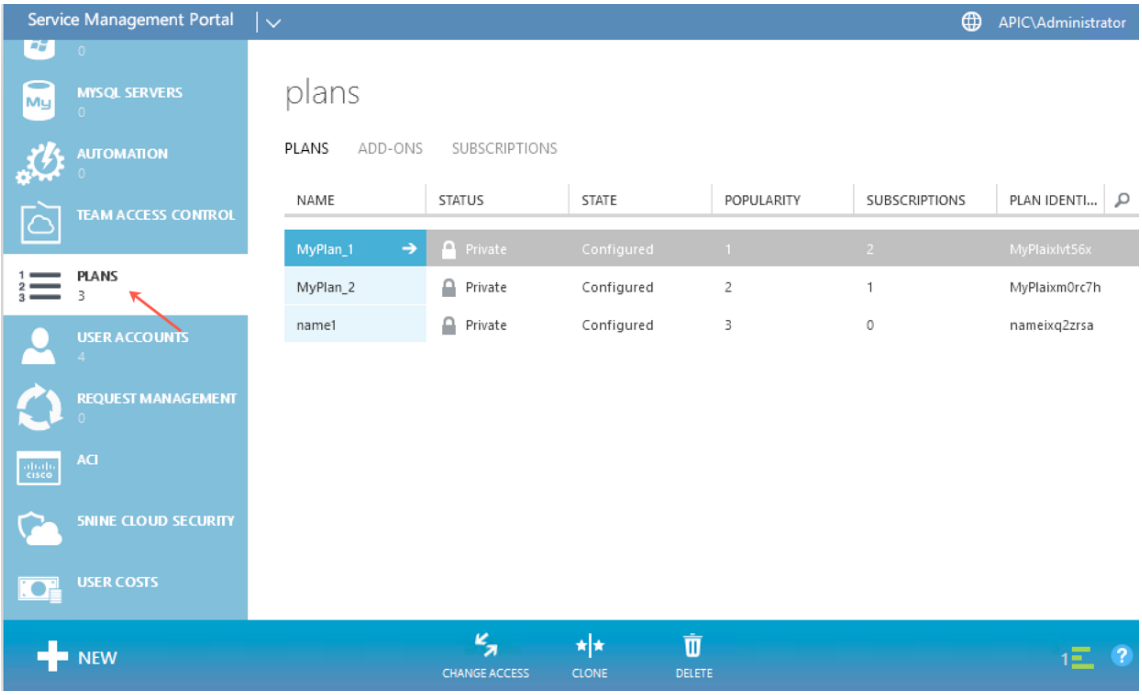
Création d'un équilibreur de charge NetScaler dans un plan du portail de gestion des services (portail d'administration)

May 5, 2023

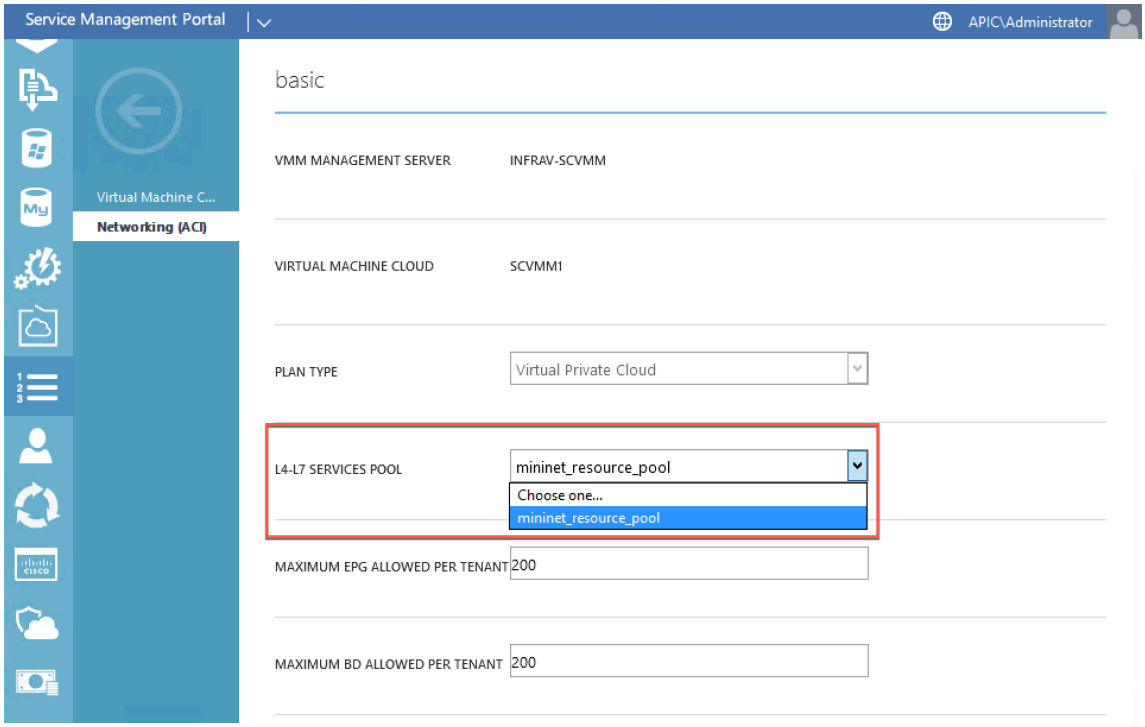
Le portail de gestion des services du WAP permet à un administrateur d'enregistrer Cisco APIC auprès du WAP et de créer un plan d'hébergement. Dans le cadre du plan, vous pouvez spécifier la plage VIP, associer l'équilibreur de charge NetScaler au plan et créer des comptes utilisateurs locataires.

Pour créer un équilibreur de charge NetScaler dans un plan du portail d'administration :

1. Connectez-vous au portail de gestion des services (portail d'administration).
2. Dans le volet de navigation, sélectionnez **PLANS**.



3. Dans le volet des plans, sélectionnez le plan auquel vous souhaitez ajouter un équilibreur de charge.
4. Dans le volet du plan sélectionné, sélectionnez **Mise en réseau (ACI)**.
5. Dans le volet **Mise en réseau (ACI)**, dans la liste déroulante **L4-L7 SERVICE POOL, sélectionnez le pool** de ressources L4-L7 que vous avez créé dans Cisco APIC.



6. Créez un compte utilisateur locataire et associez l'utilisateur au plan que vous avez créé.

Configuration d'un équilibreur de charge NetScaler à l'aide du portail de gestion des services (portail du locataire)

May 5, 2023

Dans le WAP, une fois que le locataire a créé le domaine de pont (BD), le VRF et un réseau, le locataire peut configurer un équilibreur de charge NetScaler via le portail de gestion des services (portail du locataire).

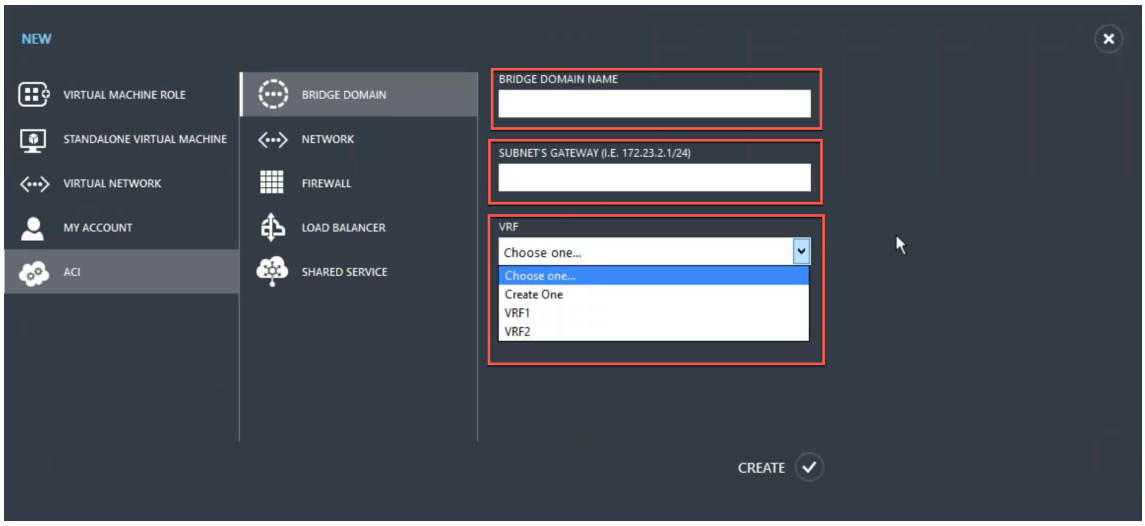
Pour configurer l'équilibreur de charge NetScaler dans le portail de gestion des services (portail du locataire)

1. Connectez-vous au portail de gestion des services (portail des locataires).
2. Créez un domaine de pont et un VRF, comme suit :

   a. Dans le volet de navigation, sélectionnez **ACI**.

   b. Cliquez sur **NOUVEAU**.

   c. Dans le volet **NOUVEAU**, sélectionnez **BRIDGE DOMAIN**.



   d. Dans le champ **DOMAINE DU PONT**, entrez le nom de domaine du pont (par exemple, BD01).

   e. (Facultatif) Dans le champ **PASSERELLE DU SOUS-RÉSEAU, entrez la passerelle** du sous-réseau (par exemple, 192.168.1.1/24).

   f. Dans le champ **VRF**, sélectionnez un VRF qui fait déjà partie de l'abonnement ou sélectionnez **Créer un VRF pour créer un** VRF.

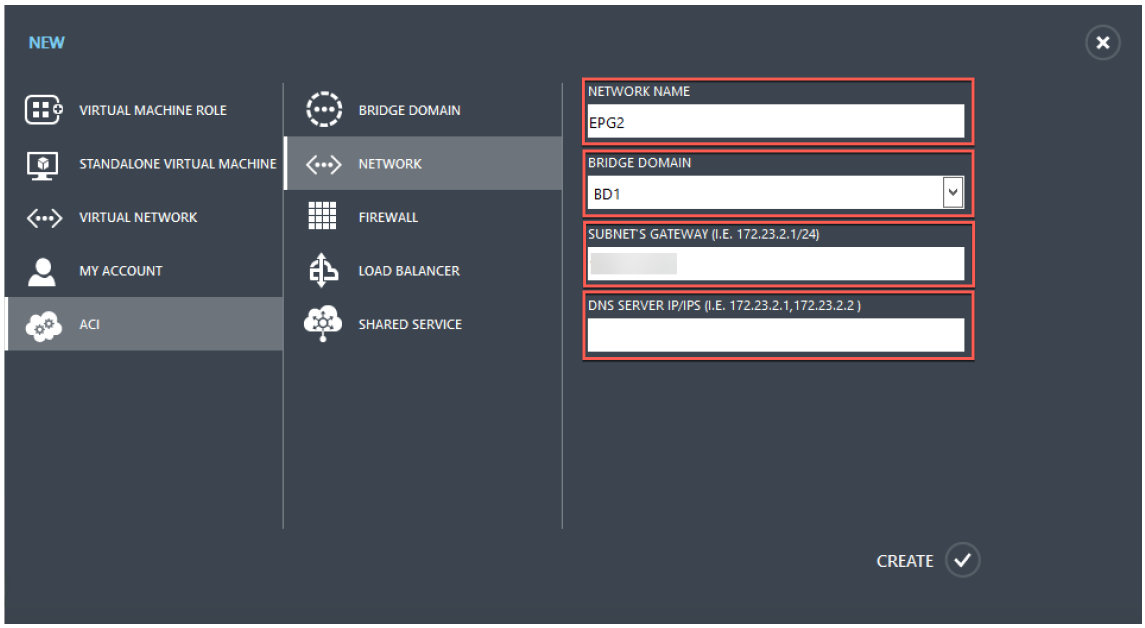
   g. Cliquez sur **CREATE**.

3. Créez un réseau et associez-le au domaine de pont que vous avez créé. Procédez comme suit :

   a. Dans le volet de navigation, sélectionnez **ACI**.

   b. Cliquez sur **NOUVEAU**.

   c. Dans le volet **NOUVEAU**, sélectionnez **RÉSEAU**.



   d. Dans le champ **NOM DU RÉSEAU**, entrez le nom du réseau (par exemple, S01).

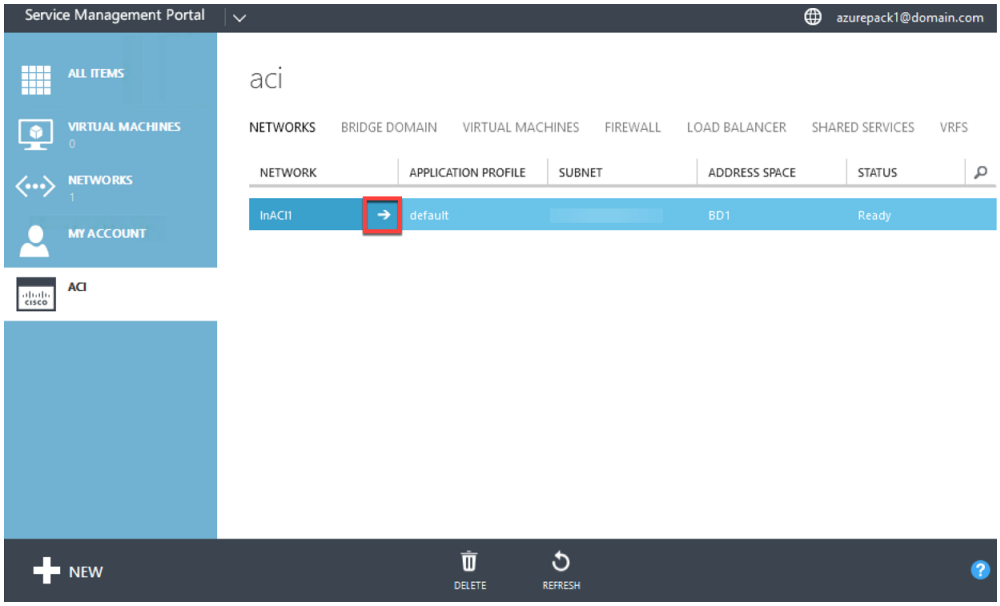
   e. Dans la liste déroulante **BRIDGE DOMAIN**, sélectionnez le domaine de bridge que vous avez créé. (par exemple, BD01).

   f. Dans le champ **GATEWAY** du sous-réseau, entrez l'adresse de la passerelle du sous-réseau (par exemple, 172.23.2.1/24).

   g. (Facultatif) Dans le champ **IP/IPS du serveur DNS**, entrez les détails du serveur DNS.

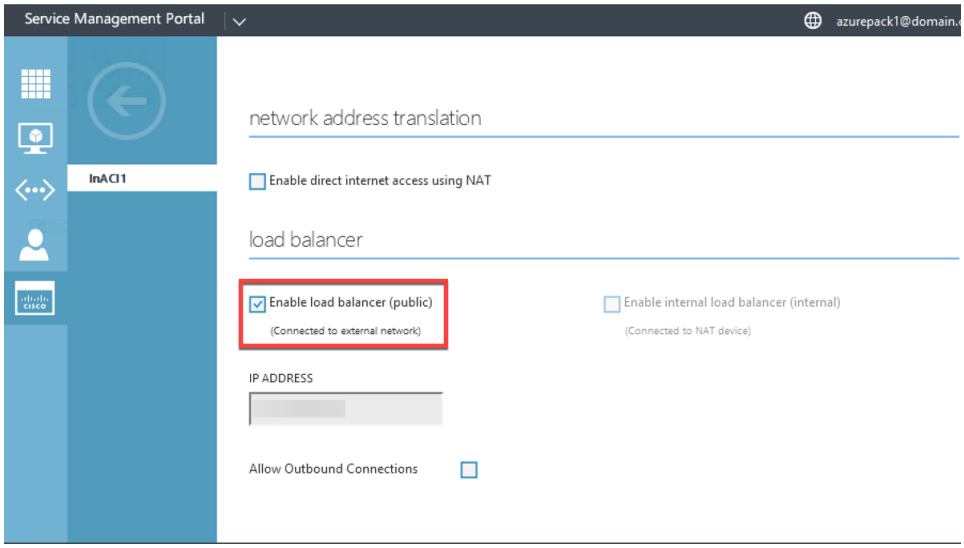
   h. Cliquez sur **CREATE**.

4. Dans le volet **ACI**, sélectionnez **NETWORKS**.

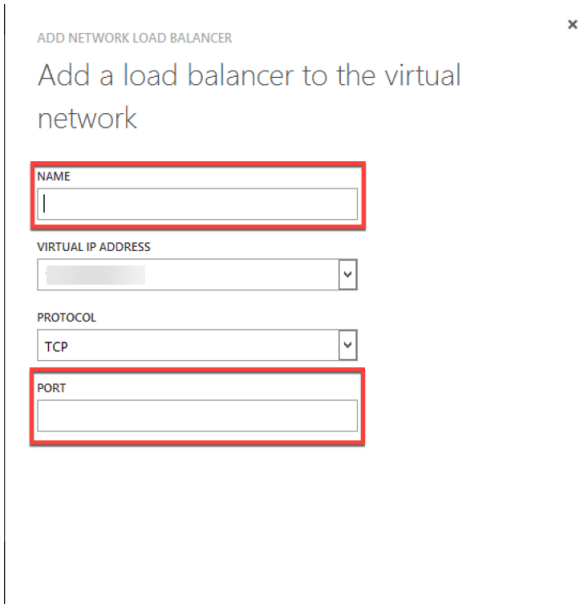


5. Double-cliquez sur le réseau que vous avez créé. Ensuite, dans le volet réseau, sélectionnez **Activer l'équilibreur de charge (public).** Dans le champ **ADRESSE IP**, un VIP est automatiquement attribué à partir de la plage VIP configurée par l'administrateur dans le portail d'administration. Pour plus d'informations, consultez la section Création d'un équilibreur de charge NetScaler dans un plan sur le portail de gestion des services (portail d'administration).

6. Double-cliquez sur le réseau que vous avez créé. Ensuite, dans le volet réseau, sélectionnez **Activer l'équilibreur de charge (public).** Dans le champ **ADRESSE IP**, un VIP est automatiquement attribué à partir de la plage VIP configurée par l'administrateur dans le portail d'administration. Pour plus d'informations, consultez la section Création d'un équilibreur de charge NetScaler dans un plan sur le portail de gestion des services (portail d'administration).



7. Dans le volet réseau, sélectionnez l'onglet **Load Balancers**, puis cliquez sur **AJOUTER**.



8. Dans le volet **AJOUTER UN ÉQUILIBREUR DE CHARGE RÉSEAU**, procédez comme suit :

   a. Dans le champ **NOM**, entrez le nom de l'équilibreur de charge.

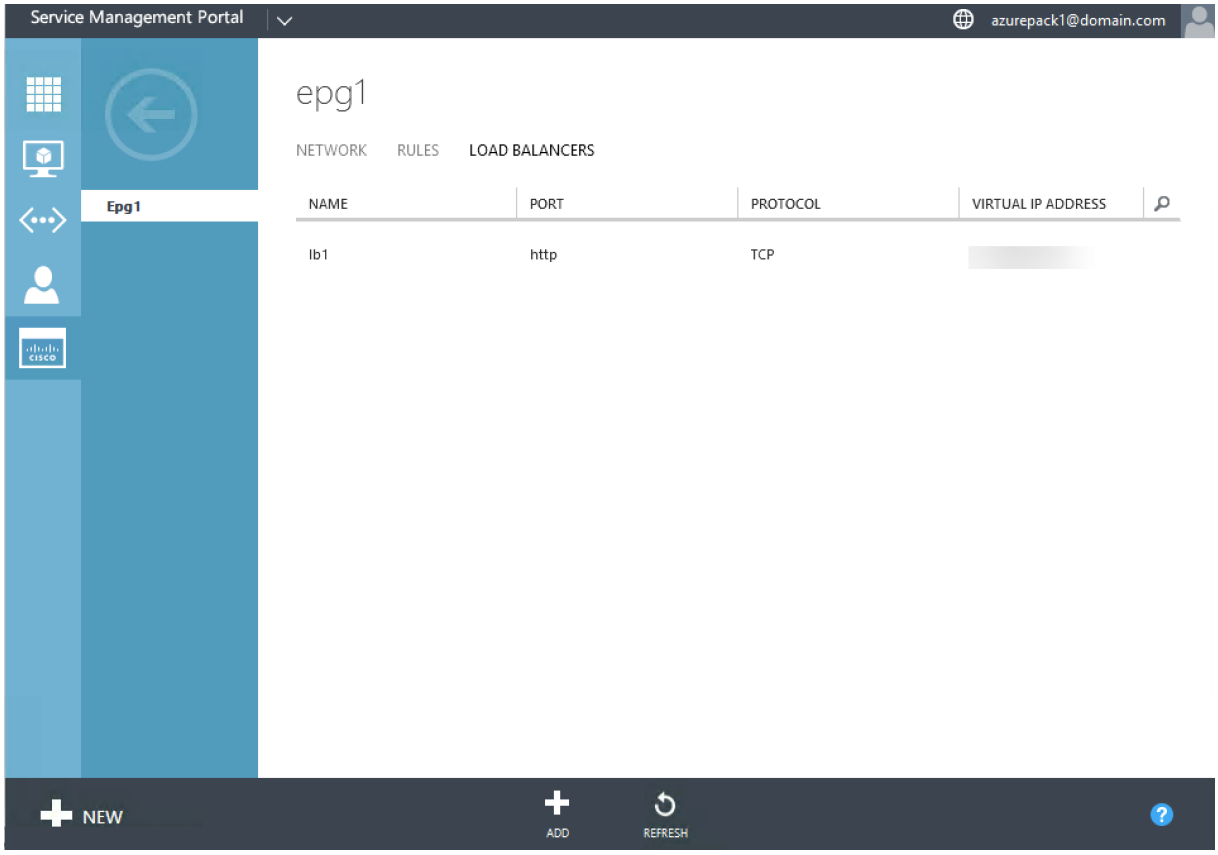
   b. Facultativement, dans le champ **ADRESSE IP VIRTUELLE**, attribuez à l'équilibreur de charge une adresse VIP issue de la plage VIP que vous avez définie précédemment.

   c. Dans le champ **PROTOCOLE**, sélectionnez éventuellement **TCP**.

   d. Dans le champ **PORT**, entrez le numéro de port.

9. Cliquez sur **CREATE**.

   L'équilibreur de charge NetScaler s'affiche dans l'onglet LOAD BALANCERS et l' **équilibreur** de charge NetScaler est prêt pour le chemin de données.



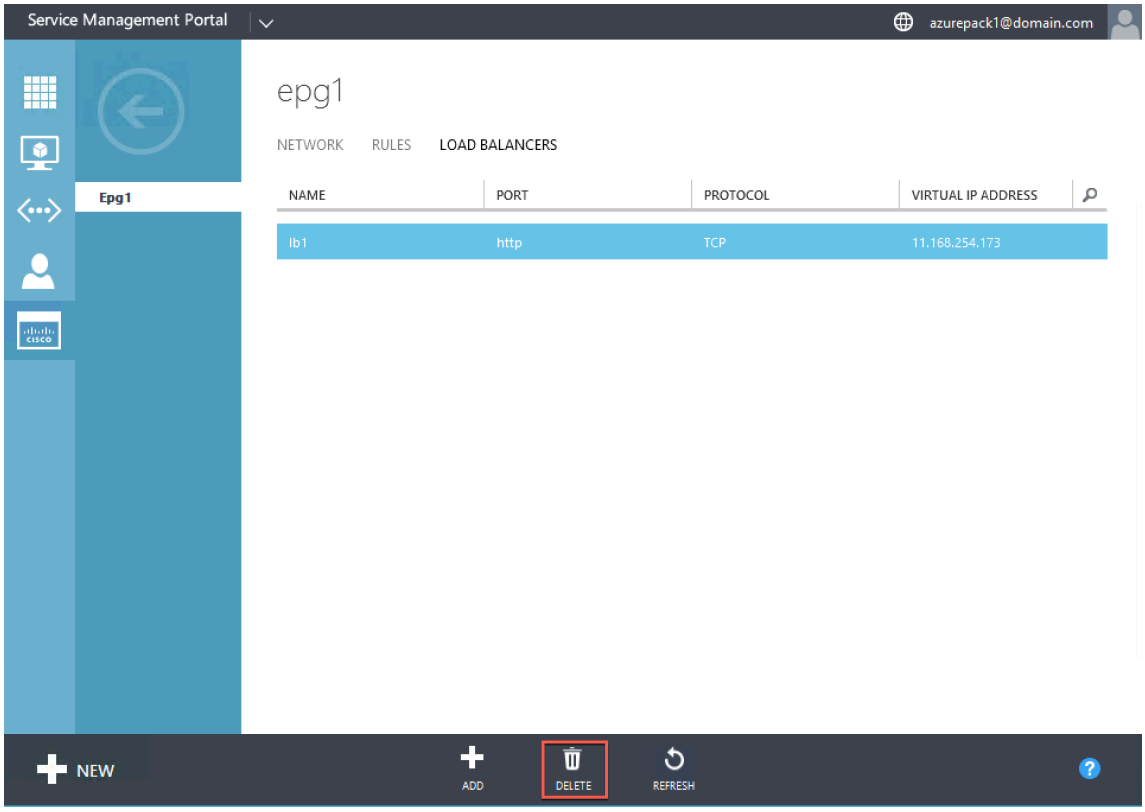
Supprimer un équilibreur de charge NetScaler du réseau

May 5, 2023

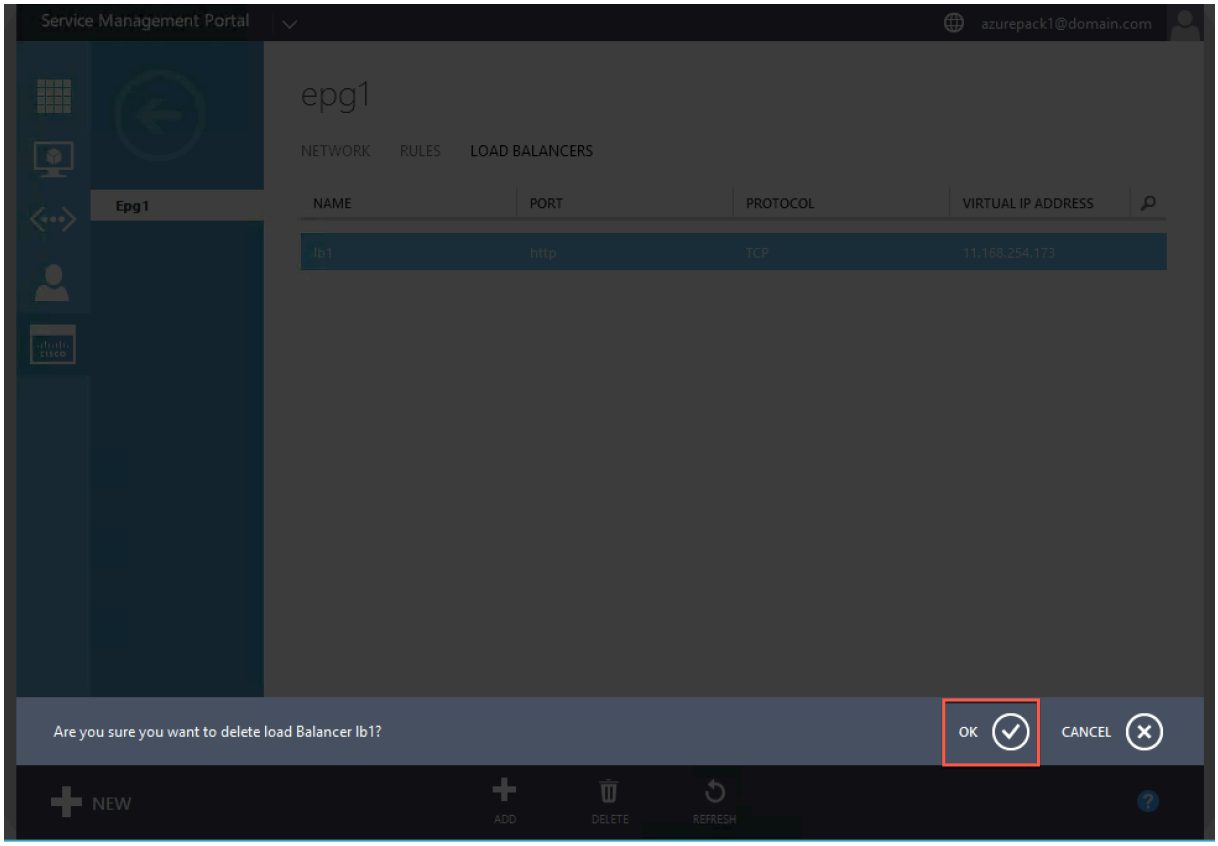
À l'aide du portail de gestion des services (portail des locataires), depuis le réseau, vous pouvez supprimer l'équilibreur de charge NetScaler que vous avez créé.

Pour supprimer un équilibreur de charge NetScaler du réseau :

1. Connectez-vous au portail de gestion des services (portail des locataires).
2. Dans le volet de navigation, sélectionnez **ACI**.
3. Dans le volet **ACI**, sous l'onglet **RÉSEAUX**, cliquez sur le réseau que vous avez créé.
4. **Dans le volet du réseau sélectionné, sélectionnez l'équilibreur de charge NetScaler et cliquez sur SUPPRIMER.**



5. Cliquez sur **OK** pour supprimer l'équilibreur de charge NetScaler.



Solution cloud native NetScaler pour les microservices basée sur Kubernetes

May 5, 2023

À mesure que les entreprises se transforment pour innover plus rapidement et se rapprocher de leurs clients, elles réorganisent leurs processus internes et éliminent les frontières au sein de leur organisation. Ils éliminent les silos pour rassembler les compétences appropriées au sein d'une même équipe. L'un des objectifs est de créer et de fournir des applications logicielles avec rapidité, agilité et efficacité. À cet égard, de plus en plus d'entreprises adoptent des architectures d'applications modernes basées sur des microservices.
À l'aide d'une architecture de microservices, vous pouvez créer des applications sous la forme d'ensembles de services faiblement couplés qui peuvent être déployés, mis à jour et dimensionnés indépendamment.

Le cloud native est une approche qui repose sur l'architecture de microservices pour créer et déployer des applications présentant les caractéristiques clés suivantes :

- Déploie des applications sous forme de microservices ou de conteneurs faiblement couplés

- Implique un très haut degré d'automatisation
- Met en œuvre des processus DevOps agiles et des flux de travail de livraison continue
- Centré sur les API pour l'interaction et la collaboration

Comment Kubernetes contribue-t-il à la transition vers le cloud natif ?

Pour fournir les niveaux d'agilité et de stabilité souhaités, les applications cloud natives nécessitent des niveaux élevés d'automatisation, de sécurité, de mise en réseau et de surveillance de l'infrastructure. Vous avez besoin d'un système d'orchestration de conteneurs capable de gérer efficacement les conteneurs à grande échelle. Kubernetes est devenue la plate-forme la plus populaire pour le déploiement et l'orchestration de conteneurs. Kubernetes résume la tâche complexe d'exécution, de déploiement et de gestion des conteneurs des développeurs et des opérateurs et planifie automatiquement les conteneurs entre un cluster de nœuds. Kubernetes et l'écosystème de la Cloud Native Computing Foundation (CNCF) vous aident à créer une plateforme pour des solutions cloud natives.

Voici certains des principaux avantages de l'utilisation de Kubernetes :

- Simplifie le déploiement des applications, qu'il s'agisse d'une infrastructure sur site, hybride ou dans un cloud public
- Accélère le développement et le déploiement d'applications
- Améliore l'agilité, la flexibilité et l'évolutivité des applications

Qu'est-ce que la solution cloud native de NetScaler ?

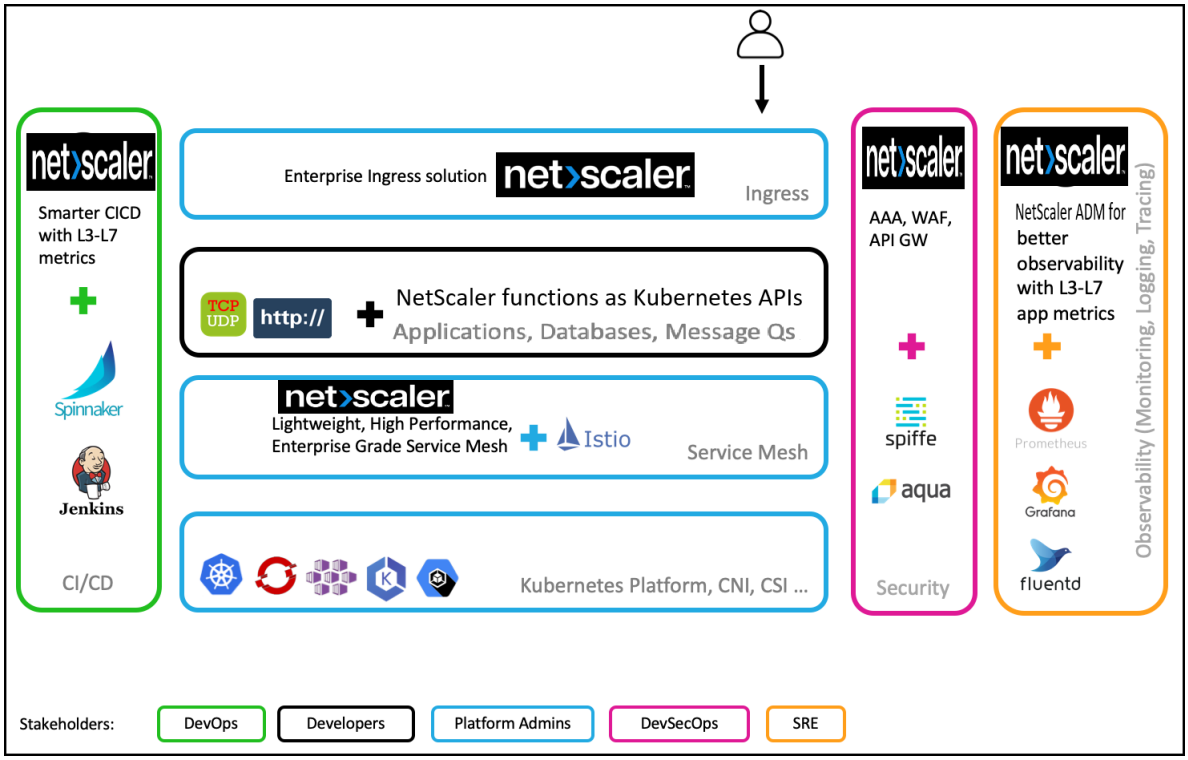
Pour optimiser les avantages de l'utilisation de Kubernetes en production, vous devez intégrer Kubernetes à plusieurs outils, à des composants provenant de fournisseurs et à code source ouvert. Garantir la fiabilité et la sécurité de leur application cloud native constitue un défi pour de nombreuses entreprises.
En tant que fournisseur de NetScalers de pointe, NetScaler propose une solution native NetScaler cloud pour relever les défis d'un environnement de production Kubernetes.

La solution cloud native de NetScaler tire parti de la gestion avancée du trafic, de l'observabilité et des fonctionnalités de sécurité complètes de NetScalers pour garantir une fiabilité et une sécurité de niveau professionnel. Il peut fournir une visibilité complète sur le trafic des applications dans votre environnement Kubernetes, générer des commentaires immédiats et vous aider à obtenir des informations pertinentes sur les performances des applications.

Le tableau suivant répertorie les principales exigences des différentes parties prenantes lors de la mise en œuvre d'une solution Ingress.

Parties prenantes	Fonction du poste	Besoins
Administrateurs de la plateforme	Garantir la disponibilité des clusters Kubernetes	Des méthodes plus simples pour gérer les applications déployées sur plusieurs clusters, ainsi que pour la gestion des opérations et du cycle de vie des plateformes
DevOps	Accélérez le déploiement des applications en production	Intégration au pipeline CI/CD, prise en charge de techniques de déploiement telles que Canary et Blue-Green pour un déploiement plus rapide
Développeurs	Développez et testez des microservices	Méthodes d'acheminement du trafic vers le cluster Kubernetes, suivi et débogage, limitation du débit pour les applications et authentification des applications
SRE	Garantir la disponibilité des applications pour respecter les accords de niveau de service	Télémétrie avancée pour les applications et l'infrastructure
SecOps	Assurer la conformité en matière de sécurité	Trafic entrant sécurisé, protection des API, maillage de services pour une communication sécurisée entre les microservices au sein du cluster Kubernetes

Le schéma suivant explique la solution cloud native de NetScaler et la manière dont elle répond aux différents défis auxquels sont confrontées les parties prenantes dans leur transition vers le cloud natif.



La solution cloud native de NetScaler offre les principaux avantages suivants :

- Fournit une solution Kubernetes Ingress avancée qui répond aux besoins des développeurs, des SRE, des DevOps et des administrateurs de réseaux ou de clusters.
- Élimine la nécessité de réécrire les applications existantes en fonction du trafic TCP ou UDP lors de leur migration vers un environnement Kubernetes.
- Sécurise les applications grâce aux politiques NetScaler présentées sous forme d'API Kubernetes.
- Permet de déployer des microservices performants pour le trafic Nord-Sud et le trafic Est-Ouest.
- Fournit une vue complète de tous les microservices à l'aide du graphe de service NetScaler ADM.
- Permet un dépannage plus rapide des microservices sur différents types de trafic, notamment TCP, UDP, HTTP, HTTPS et SSL.
- Sécurise les API.
- Automatise le pipeline CI/CD pour les déploiements Canary.
- Fournit des intégrations prêtes à l'emploi avec les outils open source de la CNCF.

Pour plus d'informations sur les différentes solutions cloud natives proposées par Citrix, consultez les liens suivants :

- Solution Kubernetes Ingress
- Service mesh
- Solutions pour l'observabilité
- Passerelle API pour Kubernetes

Composants de la solution cloud native NetScaler

Le tableau suivant explique les principaux composants de la solution native cloud NetScaler :

Composant	Description
Ingress Controller NetScaler	Ce conteneur est une implémentation du Kubernetes Ingress Controller pour gérer et acheminer le trafic vers votre cluster Kubernetes à l'aide de NetScalers (NetScaler CPX, VPX ou MPX). À l'aide de NetScaler Ingress Controller, vous pouvez configurer NetScaler CPX, VPX ou MPX conformément aux règles d'entrée et intégrer vos NetScalers à l'environnement Kubernetes.
Exportateur d'observabilité NetScaler	NetScaler Observability Exporter est un conteneur qui collecte des métriques et des transactions auprès de NetScalers et les transforme en formats adaptés (tels que JSON, AVRO) pour les terminaux pris en charge. Vous pouvez exporter les données collectées par NetScaler Observability Exporter vers le point de terminaison souhaité. En analysant les données exportées vers le terminal, vous pouvez obtenir des informations précieuses au niveau des microservices pour les applications fournies par proxy par NetScalers.
Adaptateur NetScaler xDS	L'adaptateur NetScaler xDS est un conteneur permettant d'intégrer NetScaler aux implémentations du plan de contrôle du maillage de services basées sur les API xDS (Istio, Consul, etc.). Il communique avec le plan de contrôle du maillage de service et écoute les mises à jour en agissant en tant que client gRPC pour le serveur API du plan de contrôle. Sur la base des mises à jour depuis le plan de contrôle, l'adaptateur NetScaler XDS génère la configuration NetScaler équivalente.

Composant	Description
NetScaler CPX	NetScaler CPX est un contrôleur de diffusion d'applications basé sur des conteneurs qui peut être provisionné sur un hôte Docker. NetScaler CPX permet aux clients de tirer parti des fonctionnalités du moteur Docker et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic NetScaler pour les applications basées sur des conteneurs. Vous pouvez déployer une ou plusieurs instances NetScaler CPX en tant qu'instances autonomes sur un hôte Docker.

Solution Kubernetes Ingress

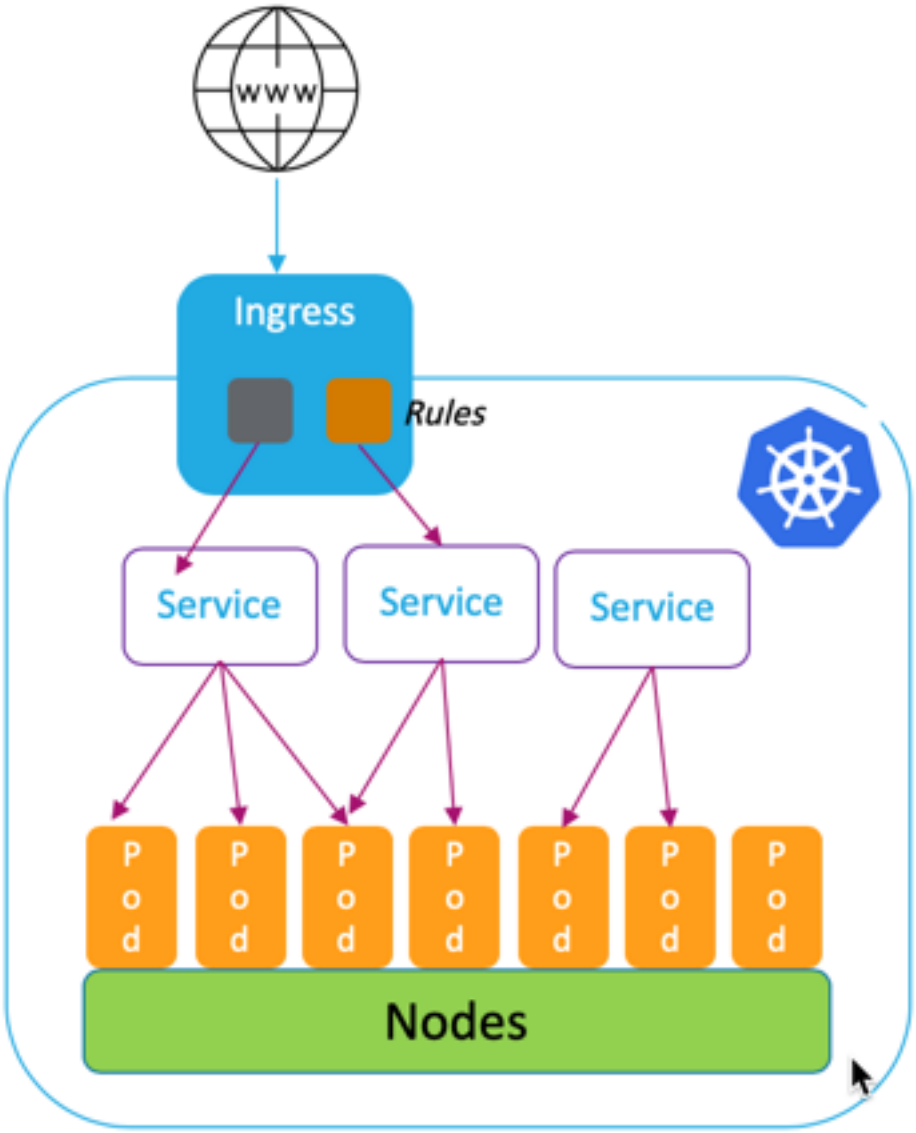
May 5, 2023

Cette rubrique fournit une vue d'ensemble de la solution Kubernetes Ingress fournie par NetScaler et explique ses avantages.

Qu'est-ce que Kubernetes Ingress ?

Lorsque vous exécutez une application à l'intérieur d'un cluster Kubernetes, vous devez fournir aux utilisateurs externes un moyen d'accéder aux applications depuis l'extérieur du cluster Kubernetes. Kubernetes fournit un objet appelé Ingress qui constitue le moyen le plus efficace d'exposer plusieurs services à l'aide d'une adresse IP stable. Un objet d'entrée Kubernetes est toujours associé à un ou plusieurs services et agit comme un point d'entrée unique permettant aux utilisateurs externes d'accéder aux services exécutés au sein du cluster.

Le schéma suivant explique le fonctionnement de Kubernetes Ingress.



L'implémentation de Kubernetes Ingress comprend les composants suivants :

- **Ressource d'entrée**. Une ressource Ingress vous permet de définir des règles d'accès aux applications depuis l'extérieur du cluster.
- **Contrôleur d'entrée**. Un contrôleur d'entrée est une application déployée dans le cluster qui interprète les règles définies dans l'entrée. Ingress Controller convertit les règles d'entrée en instructions de configuration pour une application d'équilibrage de charge intégrée au cluster. L'équilibreur de charge peut être une application logicielle exécutée dans votre cluster Kubernetes ou une appliance matérielle s'exécutant en dehors du cluster.
- **Dispositif d'entrée**. Un périphérique d'entrée est une application d'équilibrage de charge telle

que NetScaler CPX, VPX ou MPX qui effectue l'équilibrage de charge conformément aux instructions de configuration fournies par le contrôleur d'entrée.

Qu'est-ce que la solution Kubernetes Ingress de Citrix ?

Dans cette solution, NetScaler fournit une implémentation du contrôleur Kubernetes Ingress pour gérer et acheminer le trafic vers votre cluster Kubernetes à l'aide de NetScalers (NetScaler CPX, VPX ou MPX). Le NetScaler Ingress Controller intègre NetScalers à votre environnement Kubernetes et configure NetScaler CPX, VPX ou MPX conformément aux règles d'entrée.

Les solutions standard Kubernetes Ingress fournissent un équilibrage de charge uniquement à la couche 7 (trafic HTTP ou HTTPS). Parfois, vous devez exposer de nombreuses applications héritées qui reposent sur TCP, UDP ou applications et qui ont besoin d'un moyen d'équilibrer la charge de ces applications. La solution NetScaler Ingress Controller prend en charge le trafic TCP, TCP-SSL et UDP en plus de l'entrée HTTP ou HTTPS standard. En outre, il fonctionne de manière transparente sur plusieurs clouds ou centres de données sur site.

NetScaler fournit des politiques de gestion du trafic de niveau professionnel, telles que des politiques de réécriture et de réponse, pour équilibrer efficacement la charge du trafic au niveau de la couche 7. Toutefois, Kubernetes Ingress ne dispose pas de telles politiques de gestion du trafic de niveau entreprise. Avec la solution Kubernetes Ingress de Citrix, vous pouvez appliquer des politiques de réécriture et de réponse pour le trafic des applications dans un environnement Kubernetes à l'aide des CRD fournis par NetScaler.

La solution Kubernetes Ingress de Citrix prend également en charge le déploiement automatique de Canary pour votre pipeline d'applications CI/CD. Dans cette solution, NetScaler est intégré à la plateforme Spinnaker et sert de source pour fournir des mesures précises permettant d'analyser le déploiement de Canary à l'aide de Kayenta. Après avoir analysé les mesures, Kayenta génère un score agrégé pour le Canari et décide de promouvoir ou d'échouer la version Canary. Vous pouvez également réguler la distribution du trafic vers la version Canary à l'aide de l'infrastructure de règles NetScaler.

Le tableau suivant résume les avantages offerts par la solution Ingress de Citrix par rapport à Kubernetes Ingress.

Fonctionnalités	Kubernetes Ingress	Solution d'entrée de Citrix
Support HTTP et HTTPs	Oui	Oui
Routage d'URL	Oui	Oui
TLS	Oui	Oui
Équilibrage de charge	Oui	Oui

Fonctionnalités	Kubernetes Ingress	Solution d'entrée de Citrix
TCP, TCP-SSL	Non	Oui
UDP	Non	Oui
HTTP/2	Oui	Oui
Support de déploiement automatisé de Canary avec des outils CI/CD	Non	Oui
Prise en charge de l'application des politiques de réécriture et de réponse de NetScaler	Non	Oui
Authentification (autorisation ouverte (OAuth), protocole TLS mutuel (mTLS))	Non	Oui
Assistance pour l'application des politiques de limitation du débit Citrix	Non	Oui

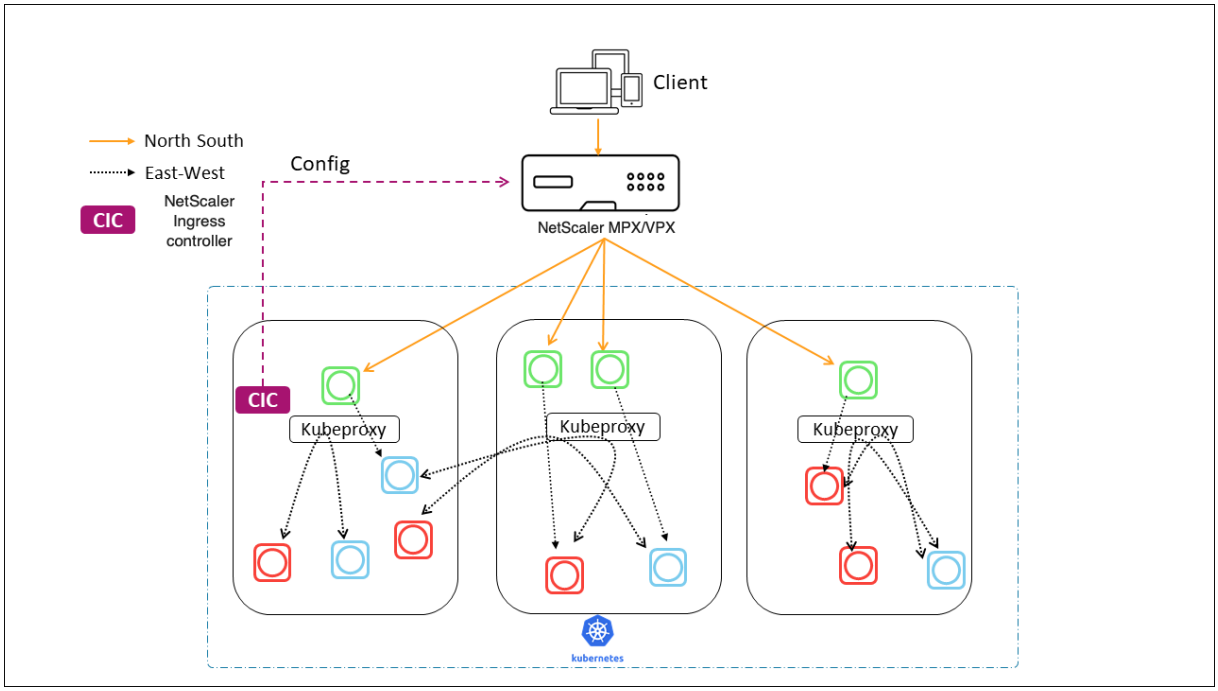
Options de déploiement pour la solution Kubernetes Ingress

La solution Kubernetes Ingress de NetScaler vous fournit une architecture flexible en fonction de la manière dont vous souhaitez gérer vos NetScalers et votre environnement Kubernetes.

Entrée unifiée (à un niveau)

Dans une architecture d'entrée unifiée (à un seul niveau), un appareil NetScaler MPX ou VPX déployé en dehors du cluster Kubernetes est intégré à l'environnement Kubernetes à l'aide du NetScaler Ingress Controller. Le NetScaler Ingress Controller est déployé en tant que pod dans le cluster Kubernetes et automatise la configuration des NetScalers en fonction des modifications apportées aux microservices ou aux ressources d'entrée. L'appareil NetScaler exécute des fonctions telles que l'équilibrage de charge, la terminaison TLS et l'optimisation du protocole HTTP ou TCP sur le trafic entrant, puis achemine le trafic vers le microservice approprié au sein d'un cluster Kubernetes. Cette architecture convient parfaitement aux scénarios dans lesquels la même équipe gère la plate-forme Kubernetes et d'autres infrastructures réseau, notamment les contrôleurs de distribution d'applications (ADC).

Le schéma suivant montre un déploiement utilisant l'architecture Ingress unifiée.



Une solution Ingress unifiée offre les principaux avantages suivants :

- Permet d'étendre les fonctionnalités de votre infrastructure NetScaler existante à l'environnement Kubernetes
- Vous permet d'appliquer des politiques de gestion du trafic pour le trafic entrant
- Fournit une architecture simplifiée adaptée aux équipes DevOps maîtrisant les réseaux
- Prend en charge la mutualisation

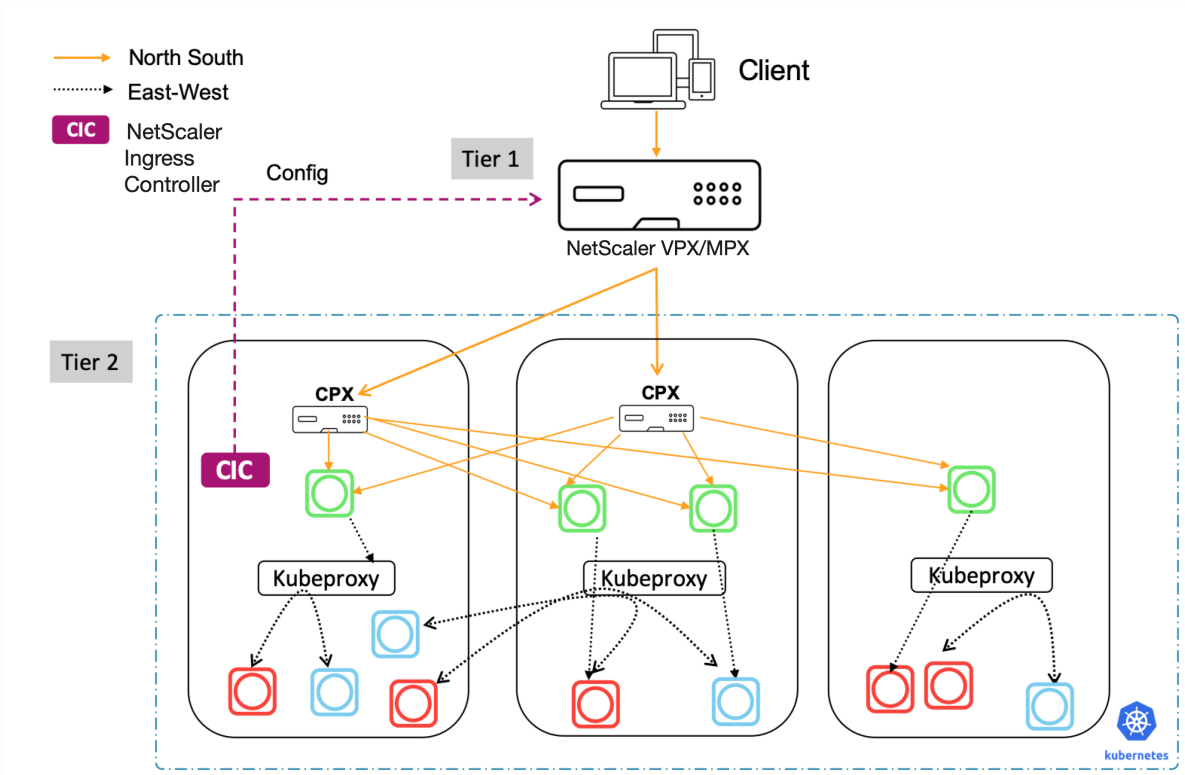
Entrée à deux niveaux

Dans une architecture à deux niveaux, NetScaler (MPX ou VPX) déployé en dehors du cluster Kubernetes agit au niveau 1 et équilibre la charge du trafic nord-sud vers les CPX NetScaler exécutés au sein du cluster. NetScaler CPX agit au niveau 2 et effectue l'équilibrage de charge pour les microservices au sein du cluster Kubernetes.

Dans les scénarios où des équipes distinctes gèrent la plate-forme Kubernetes et l'infrastructure réseau, l'architecture à deux niveaux convient le mieux.

Les équipes réseau utilisent NetScaler de niveau 1 pour des cas d'utilisation tels que le GSLB, la terminaison TLS sur la plate-forme matérielle et l'équilibrage de charge TCP. Les équipes de la plateforme Kubernetes peuvent utiliser NetScaler (CPX) de niveau 2 pour l'équilibrage de charge de la couche 7 (HTTP/HTTPS), le protocole TLS mutuel et l'observabilité ou la surveillance des microservices. Le NetScaler de niveau 2 (CPX) peut avoir une version logicielle différente de celle de NetScaler de niveau 1 pour s'adapter aux nouvelles fonctionnalités disponibles.

Le schéma suivant montre un déploiement avec une architecture à deux niveaux.



Une entrée à deux niveaux offre les principaux avantages suivants :

- Assure une grande rapidité de développement d'applications pour les développeurs ou les équipes de plateforme
- Permet d'appliquer des politiques de gestion du trafic pilotées par les développeurs pour les microservices au sein du cluster Kubernetes
- Permet l'évolutivité du cloud et la multilocation

Pour plus d'informations, consultez la documentation de NetScaler Ingress Controller.

Mise en route

Pour démarrer avec la solution Kubernetes Ingress de Citrix, vous pouvez essayer les exemples suivants :

- Équilibrage de la charge du trafic entrant avec NetScaler CPX dans Minikube
- Équilibrage de la charge du trafic d'entrée nord-sud à l'aide du proxy NetScaler CPX
- Équilibrage de la charge du trafic de microservices est-ouest à l'aide du proxy NetScaler CPX

Service mesh

May 5, 2023

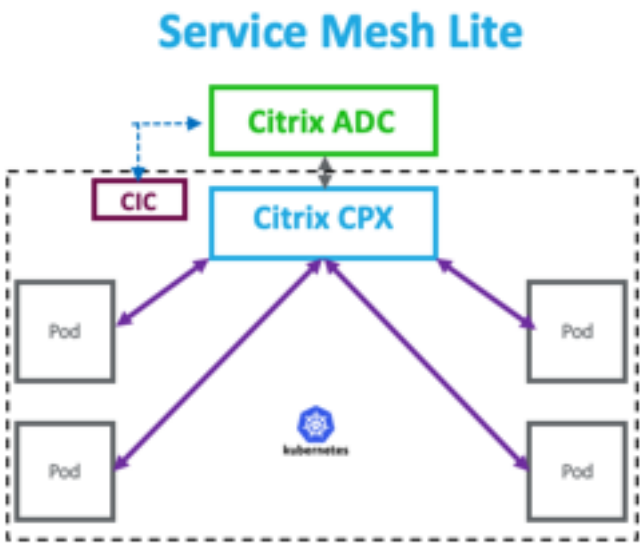
Un maillage de services est une couche d'infrastructure permettant de gérer les communications de service à service pour les applications cloud natives à l'aide d'API. Il permet de connecter, de sécuriser et de surveiller vos microservices. NetScaler propose deux solutions pour répondre à vos exigences en matière de maillage de services :

- Service mesh lite
- Service mesh (intégration de NetScaler à Istio)

Service mesh lite

Une implémentation à part entière du maillage de service-mesh est complexe et nécessite une courbe d'apprentissage abrupte. Si vous recherchez une implémentation simplifiée d'un maillage de services offrant des avantages similaires, NetScaler propose une solution moins complexe appelée service mesh lite. Dans cette solution, un NetScaler CPX fonctionne comme un équilibreur de charge centralisé dans le cluster Kubernetes et équilibre la charge du trafic est-ouest entre les microservices. NetScaler CPX applique les politiques relatives au trafic entrant et entre conteneurs.

Le schéma suivant montre une architecture Service Mesh Lite.



Pour plus d'informations, reportez-vous à la documentation Service Mesh Lite.

Service mesh (intégration de NetScaler à Istio)

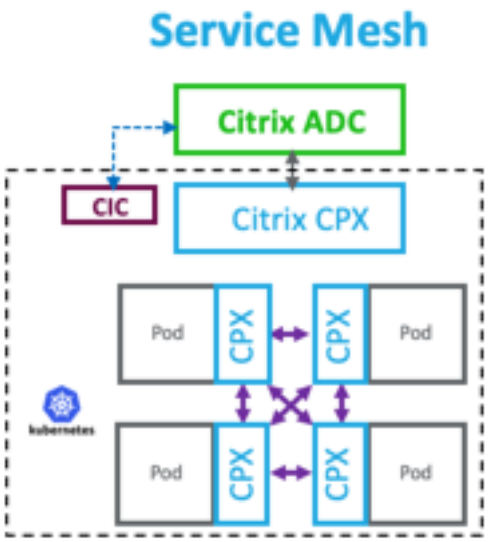
NetScaler fournit une solution de maillage de services en intégrant NetScaler à Istio. Istio, un maillage de services open source et indépendant de la plate-forme, est l'une des implémentations de maillage de services les plus populaires. En intégrant NetScaler à Istio, vous pouvez tirer parti des fonctionnalités de NetScaler pour sécuriser et optimiser le trafic des applications dans le maillage de services.

NetScaler peut être intégré à Istio des manières suivantes :

- NetScaler MPX, VPX ou CPX en tant que passerelle d'entrée Istio vers le maillage du service afin d'exposer le trafic vers le cluster Kubernetes.
- NetScaler CPX en tant que proxy annexe avec des conteneurs d'applications dans le maillage de services pour contrôler la communication entre les applications.

Vous pouvez utiliser l'une ou l'autre intégration indépendamment ou combiner les deux méthodes pour obtenir une solution de plan de données unifiée.

Le schéma suivant montre une architecture de maillage de services.



Le service mesh est idéal pour les applications hautement sécurisées et offre également les avantages suivants.

- Offre une gestion fine (modularisée) du trafic par conteneur
- Assure une observabilité, des analyses et une sécurité plus complètes (Mutual TLS) grâce à la mise en œuvre d'un sidecar
- Permet le déploiement automatique de Canary pour chaque conteneur grâce à NetScaler CPX intégré

- Prise en charge de la portabilité cloud
- Permet de décharger certaines des fonctions exécutées par les applications vers le sidecar
- Fournit une latence latence latérale inférieure
- Fournit des intégrations avec des outils open source
- Offre une évolutivité

Pour plus d'informations, consultez la documentation sur l' intégration de NetScaler à Istio.

Solutions pour l'observabilité

May 5, 2023

Dans une architecture basée sur les microservices, la visibilité des communications entre services est essentielle pour créer une architecture efficace et résiliente. Les méthodes traditionnelles de journalisation et de surveillance ne sont pas en mesure de relever les défis d'une architecture de microservices. Les solutions d'observabilité de Citrix vous permettent de voir ce qui se passe lorsque vos services interagissent les uns avec les autres et d'obtenir des informations pertinentes sur votre système.

NetScaler fournit les solutions suivantes pour répondre aux besoins d'observabilité de votre architecture de microservices :

- Graphe et analyses du service NetScaler ADM
- Exportateur d'observabilité NetScaler

Graphe et analyses du service NetScaler ADM

NetScaler Application Delivery Management (ADM) est une solution de gestion centralisée qui fournit une visibilité et une automatisation à l'échelle de l'entreprise pour les tâches de gestion qui doivent être exécutées sur plusieurs instances.

Dans une architecture de microservices, le dépannage est difficile car une seule demande d'utilisateur final peut s'étendre sur plusieurs microservices.

Le graphe et les analyses des services NetScaler ADM offrent une visibilité sur les interactions entre les microservices et aident à identifier et à résoudre les problèmes en fonction de divers indicateurs tels que la latence et les erreurs HTTP.

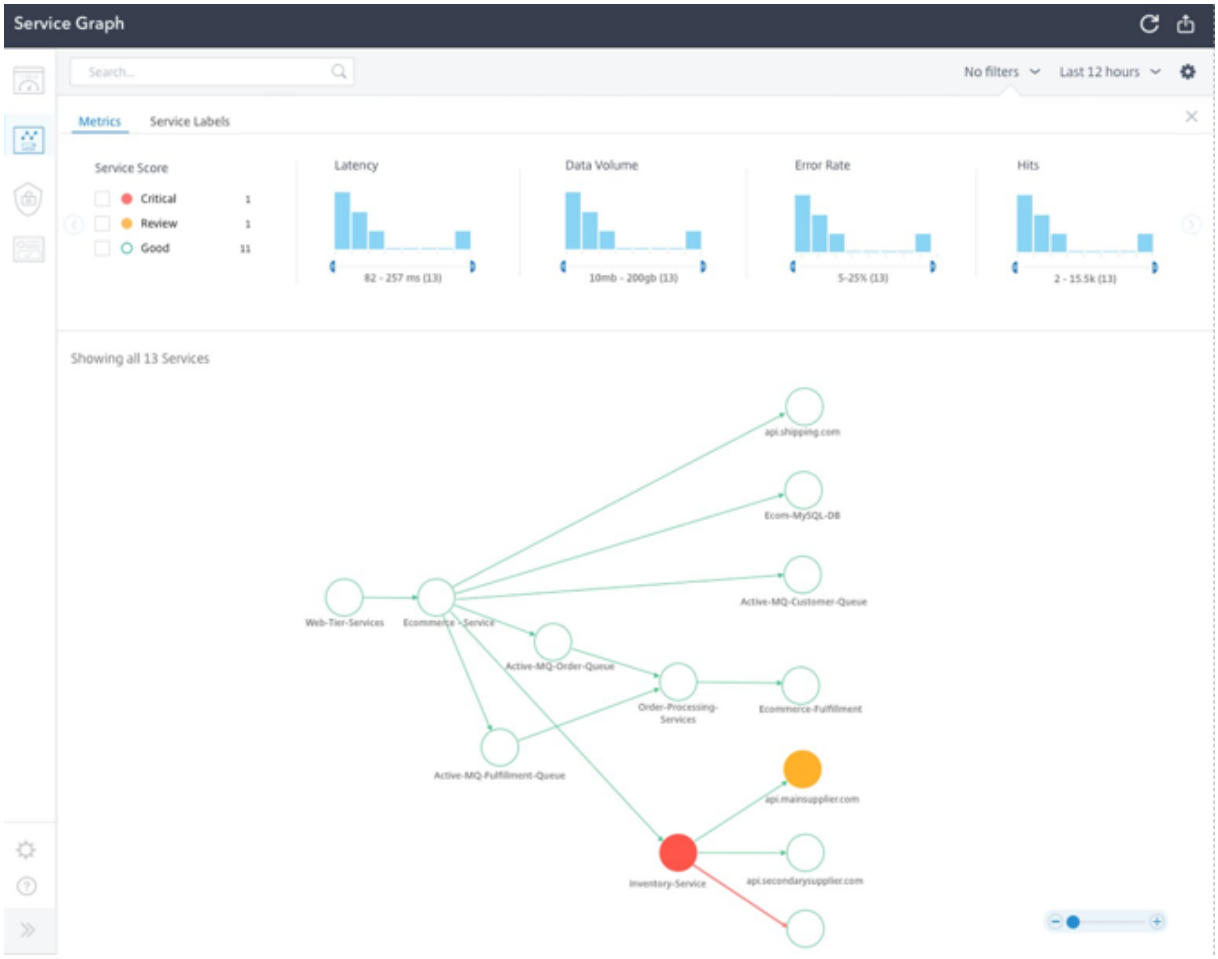
NetScaler ADM fournit également des analyses avancées basées sur des métriques et des journaux de transactions collectés par NetScaler.

La solution NetScaler ADM offre les avantages suivants :

- Fournit une interface unique pour les applications dans des conteneurs, sur site ou dans le cloud
- Offre une meilleure observabilité et un dépannage plus rapide pour les microservices

- Supporte le déploiement de Canary

Le schéma suivant montre un exemple de graphe de service pour une application contenant plusieurs microservices.



Pour plus d'informations sur la configuration du graphe de service et des analyses de NetScaler ADM, consultez la documentation du graphe de service .

Exportateur d'observabilité NetScaler

NetScaler Observability Exporter est un conteneur qui collecte des métriques et des transactions auprès de NetScalers et les transforme en formats adaptés (tels que JSON, AVRO) pour les terminaux pris en charge. Vous pouvez exporter les données collectées par NetScaler Observability Exporter vers le point de terminaison souhaité. En analysant les données, vous pouvez obtenir des informations précieuses au niveau des microservices pour les applications fournies par proxy par NetScalers.

Support de traçage distribué

Les traceurs distribués vous permettent de visualiser le flux de données entre vos microservices et d'identifier les goulots d'étranglement dans votre architecture de microservices. OpenTracing est une spécification et un ensemble standard d'API pour la conception et la mise en œuvre du suivi distribué.

NetScaler Observability Exporter implémente le traçage distribué pour NetScaler et prend actuellement en charge Zipkin en tant que traceur distribué.

Vous pouvez améliorer l'analyse des traces en utilisant Elasticsearch et Kibana avec Zipkin. Elasticsearch assure la conservation à long terme des données de trace. Kibana vous permet d'obtenir une vision beaucoup plus approfondie des données en fournissant un outil permettant d'explorer et de visualiser les messages du journal.

Collecte des transactions et support en streaming

NetScaler Observability Exporter prend en charge la collecte de transactions et leur diffusion vers les terminaux. Actuellement, NetScaler Observability Exporter prend en charge Elasticsearch et Kafka comme points de terminaison des transactions.

Pour plus d'informations, consultez la documentation de NetScaler Observability Exporter.

Activer les analyses à l'aide d'annotations dans le fichier YAML de NetScaler Ingress Controller

Vous pouvez activer l'analyse à l'aide du profil analytique défini comme une annotation intelligente dans Ingress ou service de type LoadBalancer configuration. Vous pouvez définir les paramètres spécifiques que vous devez surveiller en les spécifiant dans la configuration d'entrée ou de service de l'application. Pour plus d'informations sur l'activation de l'analyse à l'aide d'annotations, voir Analytics utilisant des annotations.

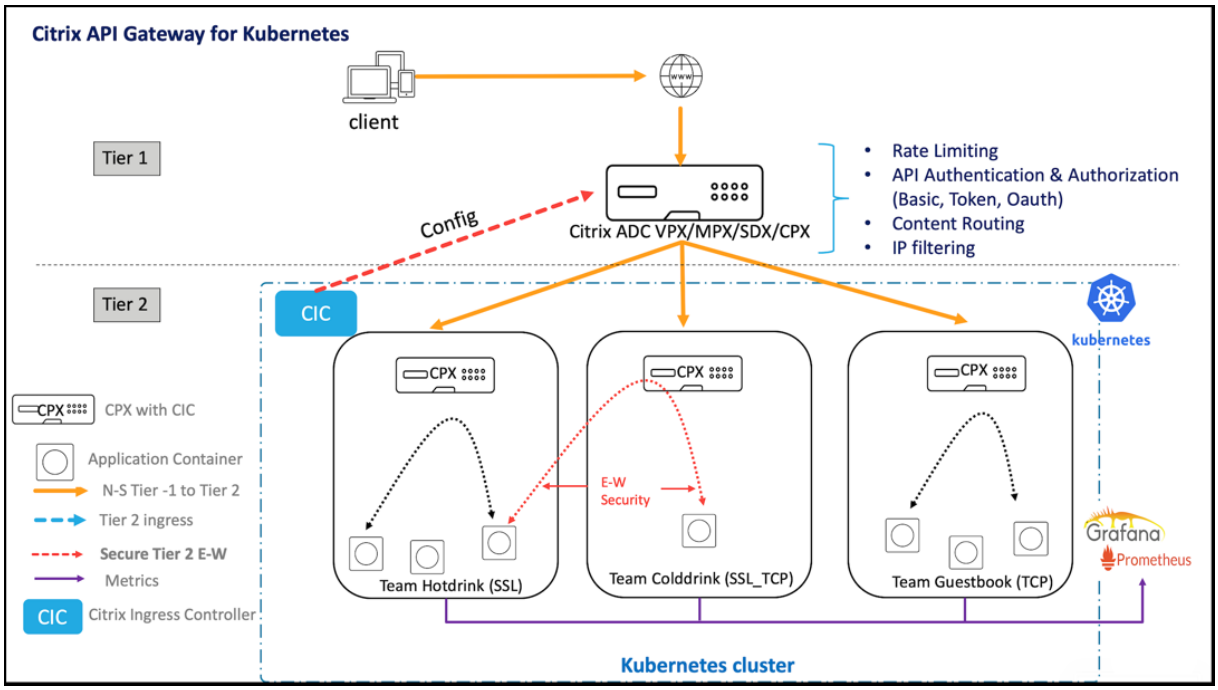
Passerelle API pour Kubernetes

May 5, 2023

Une passerelle API sert de point d'entrée unique pour vos API et garantit un accès sécurisé et fiable à plusieurs API et microservices de votre système.

NetScaler fournit une passerelle d'API de niveau entreprise pour le trafic d'API Nord-Sud vers le cluster Kubernetes. La passerelle
d'API s'intègre à Kubernetes via le NetScaler Ingress Controller et le NetScaler (NetScaler MPX, VPX ou CPX) déployé en tant que passerelle d'entrée pour les déploiements sur site ou dans le cloud.

Le schéma suivant illustre une topologie à deux niveaux pour la passerelle d'API.



À l'aide de la passerelle API proposée par Citrix, vous pouvez effectuer les fonctionnalités suivantes :

- Appliquer les stratégies d'authentification
- Limite tarifaire pour l'accès aux services
- Routage de contenu
- Transformation flexible et complète des transactions HTTP à l'aide des politiques de réécriture et de réponse
- Appliquer les stratégies de pare-feu des applications Web

Comment fonctionne la passerelle API

La passerelle d'API repose sur la passerelle d'entrée NetScaler et utilise des extensions d'API Kubernetes telles que des définitions de ressources personnalisées (CRD). À l'aide des CRD, vous pouvez configurer automatiquement NetScaler et la passerelle API dans la même instance.

NetScaler fournit les CRD suivants pour la passerelle d'API :

- CRD d'authentification
- Limite de taux CRD
- CRD de routage de contenu
- CRD de réécriture et de réponse
- WAF CRD

Principaux avantages de l'utilisation de la passerelle API

Voici les principaux avantages de la passerelle API offerte par Citrix :

- Utilise la gestion avancée du trafic et les fonctionnalités de sécurité complètes de NetScaler.
- Optimise vos déploiements en consolidant plusieurs fonctions réseau dans un seul composant de NetScaler Ingress Gateway.
- Réduit la complexité opérationnelle et les coûts liés au déploiement de plusieurs composants.
- Assure de meilleures performances pour le trafic de vos applications en réduisant les multiples sauts de déchiffrement TCP ou TLS tout en utilisant des composants distincts.
- Simplifie le déploiement et l'intégration dans vos environnements Kubernetes en utilisant directement des YAMLS ou des diagrammes de gestion.

Déploiement de la passerelle API

Pour plus d'informations sur la façon de configurer les fonctionnalités de la passerelle d'API à l'aide de CRD, consultez la documentation de NetScaler Ingress Controller :

- Authentification
- Limitation de débit
- Routage de contenu
- Stratégies de réécriture et de répondeur
- Stratégies de pare-feu pour applications Web

Utiliser NetScaler ADM pour résoudre les problèmes liés au réseau natif du cloud NetScaler

May 5, 2023

Vue d'ensemble

Ce document fournit des informations sur la façon dont vous pouvez utiliser NetScaler ADM pour fournir et surveiller des applications de microservice Kubernetes. Vous découvrirez également l'utilisation de l'interface de ligne de commande, des graphiques de service et du suivi pour permettre à la plateforme et aux équipes SRE de résoudre les problèmes.

Présentation des performances et de la latence

Cryptage TLS

Le protocole TLS est un protocole de cryptage conçu pour sécuriser les communications Internet. Une prise de contact TLS est le processus qui démarre une session de communication utilisant le cryptage TLS. Lors d'une poignée de main TLS, les deux parties communicantes échangent des messages pour s'accuser réception, se vérifier mutuellement, établir les algorithmes de chiffrement qu'ils utilisent et se mettre d'accord sur les clés de session. Les poignées de main TLS sont un élément fondamental du fonctionnement du protocole HTTPS.

Poignée de main TLS vs SSL

SSL (Secure Sockets Layer) était le protocole de cryptage original développé pour HTTP. TLS (Transport Layer Security) a remplacé SSL il y a quelque temps. Les poignées de main SSL sont maintenant appelées poignées de main TLS, bien que le nom « SSL » soit encore largement utilisé.

Quand se produit une prise de contact TLS ?

Une poignée de main TLS a lieu chaque fois qu'un utilisateur accède à un site Web via HTTPS et que le navigateur commence d'abord à interroger le serveur d'origine du site Web. Une prise de contact TLS se produit également chaque fois que d'autres communications utilisent HTTPS, y compris les appels d'API et les requêtes DNS sur HTTPS.

Les prises de contact TLS se produisent après l'ouverture d'une connexion TCP via une poignée de main TCP.

Que se passe-t-il lors d'une prise de contact TLS ?

- Lors d'une prise de contact TLS, le client et le serveur effectuent ensemble les opérations suivantes :
  - Spécifiez la version de TLS (TLS 1.0, 1.2, 1.3, etc.) qu'ils utilisent.
  - Déterminez les suites de chiffrement (voir la section suivante) qu'ils utilisent.
  - Authentifiez l'identité du serveur via la clé publique du serveur et la signature numérique de l'autorité de certification SSL.
  - Générez des clés de session pour utiliser le chiffrement symétrique une fois la prise de contact terminée.

Quelles sont les étapes d'une prise de contact TLS ?

- Les poignées de main TLS sont une série de datagrammes, ou messages, échangés par un client et un serveur. Une prise de contact TLS comporte plusieurs étapes, car le client et le serveur échangent les informations nécessaires pour terminer la prise de contact et permettre la poursuite de la conversation.

Les étapes exactes d'une négociation TLS varient en fonction du type d'algorithme d'échange de clés utilisé et des suites de chiffrement prises en charge par les deux parties. L'algorithme d'échange de

clés RSA est le plus souvent utilisé. Il se déroule comme suit :

1. Le message « bonjour client » : Le client initie la prise de contact en envoyant un message « bonjour » au serveur. Le message indique la version TLS prise en charge par le client, les suites de chiffrement prises en charge et une chaîne d'octets aléatoires appelée « client aléatoire ».
2. Le message « bonjour du serveur » : En réponse au message Hello du client, le serveur envoie un message contenant le certificat SSL du serveur, la suite de chiffrement choisie par le serveur et le « serveur aléatoire », une autre chaîne aléatoire d'octets générée par le serveur.
3. Authentification : Le client vérifie le certificat SSL du serveur auprès de l'autorité de certification qui l'a émis. Cela confirme que le serveur est bien celui qu'il prétend être et que le client interagit avec le véritable propriétaire du domaine.
4. Le secret prémaître: Le client envoie une autre chaîne aléatoire d'octets, le « secret prémaître ». Le secret prémaître est chiffré avec la clé publique et ne peut être déchiffré qu'avec la clé privée par le serveur. (Le client obtient la clé publique du certificat SSL du serveur.)
5. Clé privée utilisée : Le serveur déchiffre le secret du prémaster.
6. Clés de session créées : le client et le serveur génèrent des clés de session à partir du client aléatoire, du serveur aléatoire et du secret prémaître. Ils devraient parvenir aux mêmes résultats.
7. Le client est prêt : le client envoie un message « terminé » chiffré avec une clé de session.
8. Le serveur est prêt : le serveur envoie un message « terminé » chiffré avec une clé de session.
9. Chiffrement symétrique sécurisé obtenu : la prise de contact est terminée et la communication se poursuit à l'aide des clés de session.

Toutes les prises de contact TLS utilisent un cryptage asymétrique (clé publique et privée), mais toutes n'utilisent pas la clé privée dans le processus de génération des clés de session. Par exemple, une poignée de main éphémère Diffie-Hellman se déroule comme suit :

1. Client Hello : le client envoie un message Hello client avec la version du protocole, le caractère aléatoire du client et une liste de suites de chiffrement.

2. Bonjour du serveur : Le serveur répond avec son certificat SSL, sa suite de chiffrement sélectionnée et le serveur aléatoire. Contrairement à l'établissement de liaison RSA décrit dans la section précédente, le serveur inclut également dans ce message les informations suivantes (étape 3).

3. Signature numérique du serveur : Le serveur utilise sa clé privée pour chiffrer le client au hasard, le serveur aléatoire et son paramètre DH*. Ces données cryptées fonctionnent comme la signature numérique du serveur, établissant que le serveur possède la clé privée qui correspond à la clé publique du certificat SSL.

4. Signature numérique confirmée : le client déchiffre la signature numérique du serveur avec la clé publique, en vérifiant que le serveur contrôle la clé privée et qu'il est bien celui qu'il prétend être. Paramètre DH du client : Le client envoie son paramètre DH au serveur.

5. Le client et le serveur calculent le secret prémaître : au lieu que le client génère le secret prémaître et l'envoie au serveur, comme dans une poignée de main RSA, le client et le serveur

utilisent les paramètres DH qu'ils ont échangés pour calculer séparément un secret prémaître correspondant.

6. Clés de session créées : Maintenant, le client et le serveur calculent les clés de session à partir du secret prémaître, du hasard du client et du serveur, comme dans une poignée de main RSA.

   - Le client est prêt :
     même chose qu'une poignée de main RSA
   - Le serveur est prêt
   - Cryptage symétrique sécurisé obtenu

   *Paramètre DH : DH signifie Diffie-Hellman. L'algorithme Diffie-Hellman utilise des calculs exponentiels pour arriver au même secret prémaster. Le serveur et le client fournissent chacun un paramètre pour le calcul et, lorsqu'ils sont combinés, ils aboutissent à un calcul différent de chaque côté, avec des résultats égaux.

Pour en savoir plus sur le contraste entre les poignées de main éphémères Diffie-Hellman et d'autres types de poignées de main, et sur la manière dont elles permettent d'atteindre le secret de transmission, consultez cette documentation sur le protocole TLS.

Qu'est-ce qu'une suite de chiffrement ?

- Une suite de chiffrement est un ensemble d'algorithmes de chiffrement utilisés pour établir une connexion de communication sécurisée. (Un algorithme de chiffrement est un ensemble d'opérations mathématiques effectuées sur des données pour les rendre aléatoires.) Il existe différentes suites de chiffrement largement utilisées, et une partie essentielle de la prise de contact TLS consiste à déterminer quelle suite de chiffrement est utilisée pour cette poignée de main.

Pour commencer, reportez-vous à la section Référence : Documentation du protocole TLS.

Tableau de bord SSL de NetScaler Application Delivery Management

NetScaler Application Delivery Management (ADM) rationalise désormais tous les aspects de la gestion des certificats pour vous. Grâce à une console unique, vous pouvez établir des stratégies automatisées pour garantir l'émetteur, la force de clé et les algorithmes corrects, tout en gardant un œil étroit sur les certificats inutilisés ou bientôt expirés. Pour commencer à utiliser le tableau de bord SSL de NetScaler ADM et ses fonctionnalités, vous devez comprendre ce qu'est un certificat SSL et comment utiliser NetScaler ADM pour suivre vos certificats SSL.

Un certificat SSL (Secure Socket Layer), qui fait partie de toute transaction SSL, est un formulaire de données numérique (X509) qui identifie une société (domaine) ou un individu. Le certificat possède un composant de clé publique visible par tout client qui souhaite lancer une transaction sécurisée avec le serveur. La clé privée correspondante, qui réside en toute sécurité sur l'appliance Citrix Appli-

cation Delivery Controller (ADC), est utilisée pour effectuer le chiffrement et le déchiffrement des clés asymétriques (ou des clés publiques).

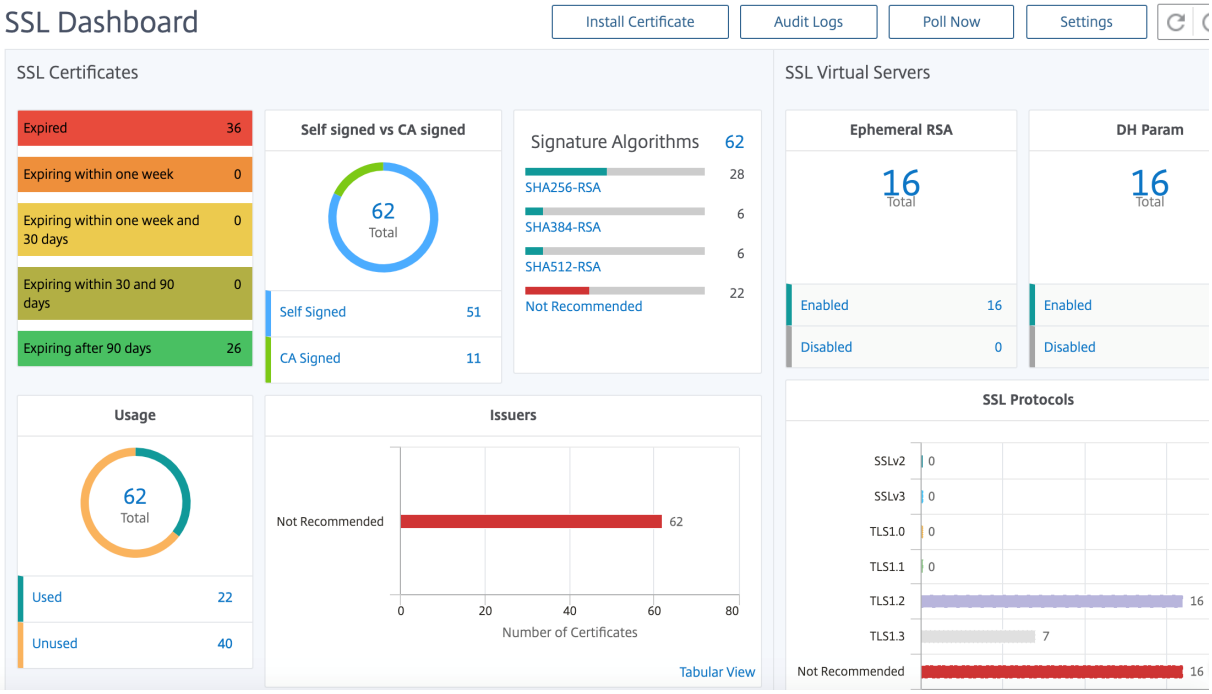
Vous pouvez obtenir un certificat SSL et une clé de l'une des manières suivantes :

- De la part d'une autorité de certification (CA) autorisée
- En générant un nouveau certificat SSL et une nouvelle clé sur l'appliance NetScaler

NetScaler ADM fournit une vue centralisée des certificats SSL installés sur toutes les instances NetScaler gérées. Sur le tableau de bord SSL, vous pouvez afficher des graphiques qui vous aident à suivre les émetteurs de certificats, les forces clés, les algorithmes de signature, les certificats expirés ou non utilisés, etc. Vous pouvez également voir la distribution des protocoles SSL qui s'exécutent sur vos serveurs virtuels et les clés qui y sont activées.

Vous pouvez également configurer des notifications pour vous informer lorsque les certificats sont sur le point d'expirer et inclure des informations sur les instances NetScaler qui utilisent ces certificats.

Vous pouvez lier les certificats d'une instance NetScaler à un certificat CA. Cependant, assurez-vous que les certificats que vous liez au même certificat d'autorité de certification ont la même source et le même émetteur. Après avoir lié les certificats à un certificat d'autorité de certification, vous pouvez les dissocier.



Pour commencer, consultez la documentation du tableau de bord SSL.

Intégrations tierces

La latence de l'application est mesurée en millisecondes et peut indiquer l'un des deux éléments suivants en fonction de la mesure utilisée. La méthode la plus courante de mesure de la latence est appelée « temps aller-retour » (ou RTT). RTT calcule le temps nécessaire à un paquet de données pour se déplacer d'un point à un autre sur le réseau et pour qu'une réponse soit renvoyée à la source. L'autre mesure est appelée « temps jusqu'au premier octet » (ou TTFB), qui enregistre le temps qu'il faut entre le moment où un paquet quitte un point du réseau et le moment où il arrive à destination. Le RTT est plus couramment utilisé pour mesurer la latence car il peut être exécuté à partir d'un point unique du réseau et ne nécessite pas l'installation d'un logiciel de collecte de données sur le point de destination (comme le fait TTFB).

En surveillant l'utilisation et les performances de la bande passante de votre application en temps réel, le service ADM facilite l'identification des problèmes et la résolution préventive des problèmes potentiels avant qu'ils ne se manifestent et n'affectent les utilisateurs de votre réseau. Cette solution basée sur les flux suit l'utilisation par interface, application et conversation, vous fournissant des informations détaillées sur l'activité de votre réseau.

Utiliser les outils Splunk

Les performances de l'infrastructure et des applications sont interdépendantes. Pour avoir une vue d'ensemble, SignalFX fournit une corrélation transparente entre l'infrastructure cloud et les microservices qui s'exécutent dessus. Si votre application échoue en raison d'une fuite de mémoire, d'un conteneur voisin bruyant ou de tout autre problème lié à l'infrastructure, SignalFX vous en informe. Pour compléter le tableau, l'accès en contexte aux journaux et aux événements Splunk permet un dépannage plus approfondi et une analyse des causes profondes.

Pour plus d'informations sur l'APM des microservices SignalFX et le dépannage avec Splunk, consultez les informations relatives à Splunk pour DevOps .

Prise en charge MongoDB

MongoDB stocke les données dans des documents flexibles de type JSON. Les champs de signification peuvent varier d'un document à l'autre et la structure des données peut être modifiée au fil du temps.

Le modèle de document correspond aux objets de votre code d'application, ce qui facilite l'utilisation des données.

Les requêtes à la demande, l'indexation et l'agrégation en temps réel fournissent de puissants moyens d'accéder à vos données et de les analyser.

MongoDB est une base de données distribuée, de sorte que la haute disponibilité, la mise à l'échelle horizontale et la distribution géographique sont intégrées et faciles à utiliser.

MongoDB est conçu pour répondre aux exigences des applications modernes grâce à une base technologique qui vous permet de :

- Le modèle de données du document, qui vous présente la meilleure façon de travailler avec les données.
- Une conception de systèmes distribués qui vous permet de placer intelligemment les données où vous le souhaitez.
- Une expérience unifiée qui vous donne la liberté d'exécuter n'importe où, ce qui vous permet de pérenniser votre travail et d'éliminer la dépendance vis-à-vis des fournisseurs.

Avec ces fonctionnalités, vous pouvez créer une plate-forme de données opérationnelles intelligente, soutenue par MongoDB. Pour plus d'informations, consultez la documentation MongoDB.

Comment équilibrer la charge du trafic entrant vers une application basée sur TCP ou UDP

Dans un environnement Kubernetes, une entrée est un objet qui permet d'accéder aux services Kubernetes depuis l'extérieur du cluster Kubernetes. Les ressources Kubernetes Ingress standard supposent que tout le trafic est basé sur HTTP et ne répond pas aux protocoles non HTTP tels que TCP, TCP-SSL et UDP. Par conséquent, les applications critiques basées sur les protocoles L7 tels que DNS, FTP, LDAP, ne peuvent pas être exposées à l'aide de Kubernetes Ingress standard.

La solution standard de Kubernetes consiste à créer un service de type LoadBalancer. Reportez-vous à la section Service Type LoadBalancer dans NetScaler pour plus d'informations.

La deuxième option consiste à annoter l'objet d'entrée. NetScaler Ingress Controller vous permet d'équilibrer la charge du trafic d'entrée basé sur TCP ou UDP. Il fournit les annotations suivantes que vous pouvez utiliser dans votre définition de ressource Kubernetes Ingress pour équilibrer la charge du trafic entrant basé sur TCP ou UDP :

- ingress.citrix.com/insecure-service-type : l'annotation permet l'équilibrage de charge L4 avec TCP, UDP ou ANY comme protocole pour NetScaler.
- ingress.citrix.com/insecure-port : l'annotation configure le port TCP. L'annotation est utile lorsque l'accès au microservice est requis sur un port non standard. Par défaut, le port 80 est configuré.

Pour plus d'informations, consultez Comment équilibrer la charge du trafic entrant vers une application basée sur TCP ou UDP.

Surveillez et améliorez les performances de vos applications basées sur TCP ou UDP

Les développeurs d'applications peuvent surveiller de près l'état de santé des applications basées sur TCP ou UDP à l'aide de puissants moniteurs (tels que TCP-ECV, UDP-ECV) intégrés à NetScaler. L'ECV (Extended Content Validation) surveille l'aide pour vérifier si l'application renvoie le contenu attendu ou non.

En outre, les performances de l'application peuvent être améliorées en utilisant des méthodes de persistance telles que l'adresse IP source. Vous pouvez utiliser ces fonctionnalités de NetScaler via des annotations intelligentes dans Kubernetes . Voici un exemple de ce type :

```
1 apiVersion: extensions/v1beta1
2 kind: Ingress
3 metadata:
4     name: mongodb
```



```
    annotations:
        ingress.citrix.com/insecure-port:  “80”
        ingress.citrix.com/frontend-ip:  “192.168.1.1”
        ingress.citrix.com/csvserver:  ‘{
 “l2conn” :” on”  }
 ’
        ingress.citrix.com/lbvserver:  ‘{
 “mongodb-svc” :{
 “lbmethod” :” SRCIPDESTIPHASH”  }
 }
 ’
        ingress.citrix.com/monitor:  ‘{
 “mongodbsvc” :{
 “type” :” tcp-ecv”  }
 }
 ’
Spec:
    rules:
    - host: mongodb.beverages.com
      http:
        paths:
        - path: /
          backend:
            serviceName: mongodb-svc
            servicePort: 80
<!--NeedCopy-->
```

Service de gestion de la diffusion des applications (ADM) NetScaler

Le service NetScaler ADM offre les avantages suivants :

- **Agile** — Facile à utiliser, à mettre à jour et à consommer. Le modèle de service de NetScaler ADM Service est disponible sur le cloud, ce qui facilite l’utilisation, la mise à jour et l’utilisation des fonctionnalités proposées. La fréquence des mises à jour, associée à la fonctionnalité de mise à jour automatique, améliore rapidement votre déploiement NetScaler.
- **Délai de rentabilisation** plus rapide — Réalisation plus rapide des objectifs commerciaux. Contrairement au déploiement sur site traditionnel, vous pouvez utiliser votre service NetScaler ADM en quelques clics. Vous économisez non seulement du temps d’installation et de configuration, mais vous évitez également de perdre du temps et des ressources en cas d’erreurs potentielles.
- **Gestion multisite** : volet unique de verre pour les instances dans les datacenters multi-sites. Avec le service NetScaler ADM, vous pouvez gérer et surveiller les NetScalers qui se trouvent dans différents types de déploiements. Vous disposez d’une gestion centralisée pour les

NetScalers déployés sur site et dans le cloud.

- **Efficacité opérationnelle** — Une façon optimisée et automatisée d'atteindre une productivité opérationnelle plus élevée. Avec le service NetScaler ADM, vos coûts d'exploitation sont réduits en économisant du temps, de l'argent et des ressources sur la maintenance et la mise à niveau des déploiements matériels traditionnels.

Graphique de service pour les applications Kubernetes

À l'aide du graphe de service pour la fonctionnalité d'application native au cloud de NetScaler ADM, vous pouvez :

- Garantir les performances globales des applications de bout en bout
- Identifiez les goulots d'étranglement créés par l'interdépendance des différents composants de vos applications
- Recueillez des informations sur les dépendances des différents composants de vos applications
- Surveiller les services au sein du cluster Kubernetes
- Surveiller quel service rencontre des problèmes
- Vérifiez les facteurs qui contribuent aux problèmes de performance
- Afficher la visibilité détaillée des transactions HTTP de service
- Analyser les mesures HTTP, TCP et SSL

En visualisant ces mesures dans NetScaler ADM, vous pouvez analyser la cause première des problèmes et prendre les mesures de dépannage nécessaires plus rapidement. Le graphique de service affiche vos applications dans divers services de composants. Ces services s'exécutant à l'intérieur du cluster Kubernetes peuvent communiquer avec divers composants à l'intérieur et à l'extérieur de l'application.

Pour commencer, reportez-vous à la section Configuration du graphique de service.

Graphique de service pour les applications Web à 3 niveaux

À l'aide de la fonction de graphe de service du tableau de bord de l'application, vous pouvez afficher :

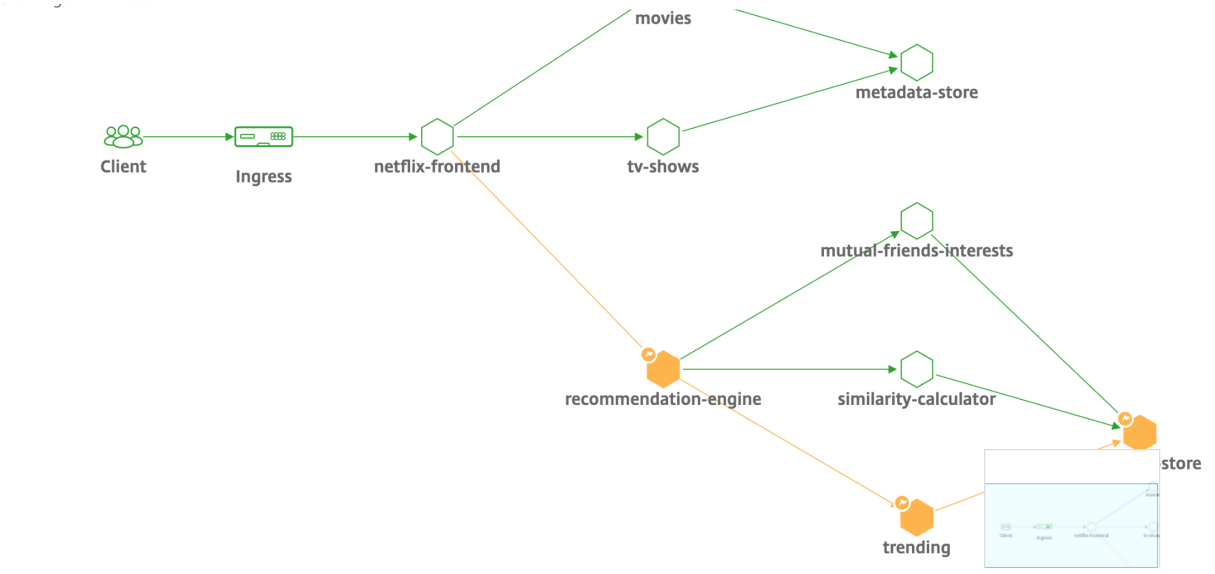
- Détails sur la configuration de l'application (avec un serveur virtuel de commutation de contenu et un serveur virtuel d'équilibrage de charge)
  - Pour les applications GSLB, vous pouvez afficher le centre de données, l'instance ADC, les serveurs virtuels CS et LB
- Transactions de bout en bout du client au service
- Emplacement à partir duquel le client accède à l'application
- Le nom du centre de données dans lequel les demandes des clients sont traitées et les métriques NetScaler du centre de données associées (uniquement pour les applications GSLB)
- Détails des mesures pour les serveurs clients, les services et les serveurs virtuels

- Si les erreurs proviennent du client ou du service
- L'état du service, tel que **Critique, Révision**et**Bon**. NetScaler ADM affiche l'état du service en fonction du temps de réponse du service et du nombre d'erreurs.
  - **Critique (rouge)** - Indique si le temps de réponse moyen du service est supérieur à 200 ms ET le nombre d'erreurs > 0
  - **Avis (orange)** - Indique si le temps de réponse moyen du service est supérieur à 200 ms OU le nombre d'erreurs > 0
  - **Bon (vert)** - Indique l'absence d'erreur et le temps de réponse moyen du service est inférieur à 200 ms
- L'état du client, tel que **Critique, Révision**et**Bon**. NetScaler ADM affiche l'état du client en fonction de la latence du réseau client et du nombre d'erreurs.
  - **Critique (rouge)**- Indique si la latence moyenne du réseau client est > 200 ms ET le nombre d'erreurs > 0
  - **Avis (orange)** - Indique lorsque la latence moyenne du réseau client est > 200 ms OU le nombre d'erreurs > 0
  - **Bon (vert)** - Indique l'absence d'erreur et la latence moyenne du réseau client est inférieure à 200 ms
- L'état du serveur virtuel, tel que **Critique, Révision**et**Bon**. NetScaler ADM affiche l'état du serveur virtuel en fonction du score de l'application.
  - **Critique (rouge)** - Indique lorsque le score de l'application est inférieur à 40
  - **Avis (orange)** - Indique quand le score de l'application se situe entre 40 et 75
  - **Bon (vert)** - Indique lorsque le score de l'application est > 75

Points à noter :

- Seuls les serveurs virtuels d'équilibrage de charge, de commutation de contenu et GSLB sont affichés dans le graphique de service.
- Si aucun serveur virtuel n'est lié à une application personnalisée, les détails ne sont pas visibles dans le graphique de service de l'application.
- Vous pouvez afficher les mesures des clients et des services dans le graphique des services uniquement si des transactions actives ont lieu entre des serveurs virtuels et une application Web.
- Si aucune transaction active n'est disponible entre les serveurs virtuels et l'application Web, vous pouvez uniquement afficher les détails dans le graphique de service en fonction des données de configuration telles que l'équilibrage de charge, la commutation de contenu, les serveurs virtuels GSLB et les services.
- Les mises à jour de la configuration de l'application peuvent prendre 10 minutes pour apparaître dans le graphique de service.

Pour plus d'informations, consultez la section Graphique de service pour les applications.



Pour commencer, consultez la documentation Service Graph.

Résolution des problèmes pour les équipes NetScaler

Examinons certains des attributs les plus courants pour le dépannage de la plate-forme NetScaler et comment ces techniques de dépannage s'appliquent aux déploiements de niveau 1 pour les topologies de microservices.

NetScaler possède une interface de ligne de commande (CLI) qui affiche les commandes en temps réel et est utile pour déterminer les configurations d'exécution, les statiques et la configuration des politiques. Cela est facilité par la commande **« SHOW »** .

SHOW - effectuer des opérations CLI ADC :

```
>Show running config (-summary -fullValues)

 Ability to search (grep command)
> “sh running config | -i grep vserver”

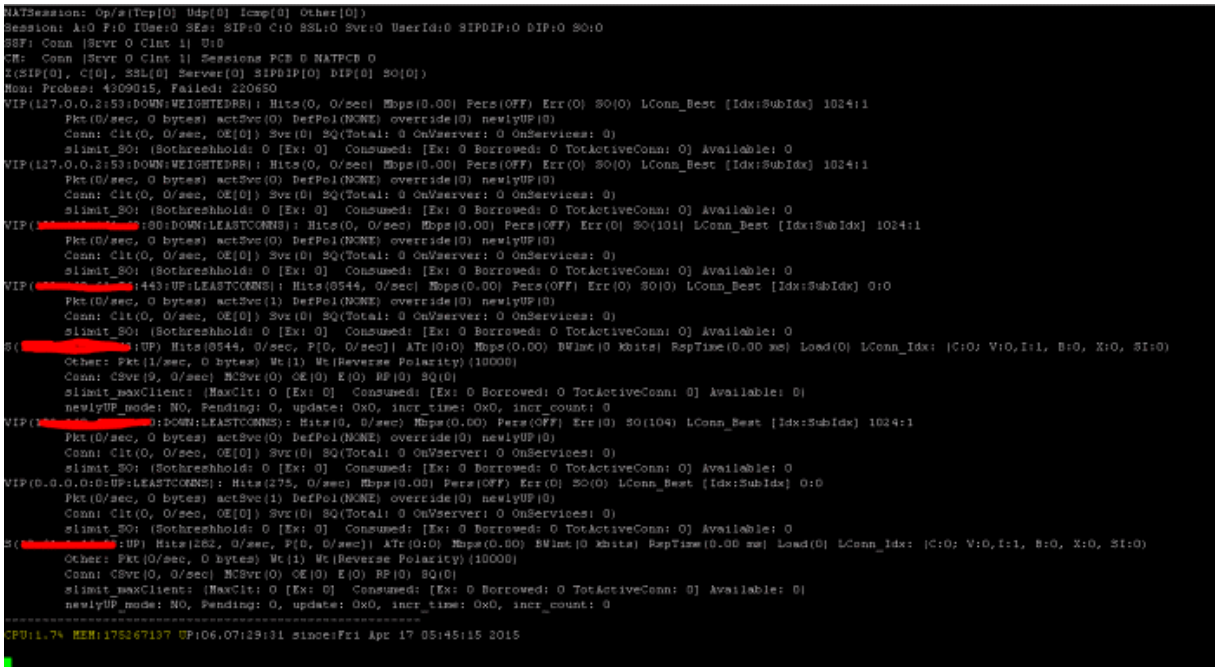
Check the version.
>Show license
   “sh license"
<!--NeedCopy-->
```

Afficher les statistiques SSL

```
>Sh ssl
        System
        Frontend
        Backend
```



```
5           Encryption
6  <!--NeedCopy-->
```



NetScaler dispose d'une commande permettant d'énumérer les statistiques de tous les objets sur la base d'un intervalle de compteur de sept (7) secondes. Cela est facilité par la commande **« STAT »** .

Télémétrie L3-L7 hautement granulaire par NetScaler

- Niveau système : utilisation du processeur et de la mémoire de l'ADC.
- Protocole HTTP : #Requests /Responses, split GET/POST, erreurs HTTP pour N-S et E-W (pour le service mesh lite uniquement, sidecar bientôt).
- SSL : #Sessions et #Handshakes pour le trafic N-S et E-W pour le service mesh lite uniquement.
- Protocole IP : #Packets reçu/envoyé, #Bytes reçu/envoyé, paquets #Truncated et recherche d'adresse #IP.
- NetScaler AAA : Séances #Active
- Interface : paquets multidiffusion #Total, #Total octets transférés et paquets #Jumbo reçus/envoyés.
- Serveur virtuel d'équilibrage de charge et serveur virtuel de commutation de contenu : #Packets, #Hits et #Bytes reçus/envoyés.

STAT - effectuer des opérations CLI ADC :

```
1  >Statistics
2   “stat ssl”
3  <!--NeedCopy-->
```



```
> stat ns

System overview

Up since        Thu Apr 16 19:45:15 2015
Packet CPU usage (%)                1.60
Management CPU usage (%)            0.80
Memory usage (MB)                    165
InUse Memory (%)                   17.03
Last Transition time Th...015
System state                         UP
Master state                    Primary
# SSL cards UP                         0
# SSL cards present                    0

System Disks                   Used (%) Available
/flash Used (%)                       17      1168
/var Used (%)                         13     11246

Throughput Statistics                    Rate (/s)               Total
Megabits received                                2               288237
Megabits transmitted                             3               345685

TCP Connections                  Client   Server
All client connections              158      272
Established client connections      158      145

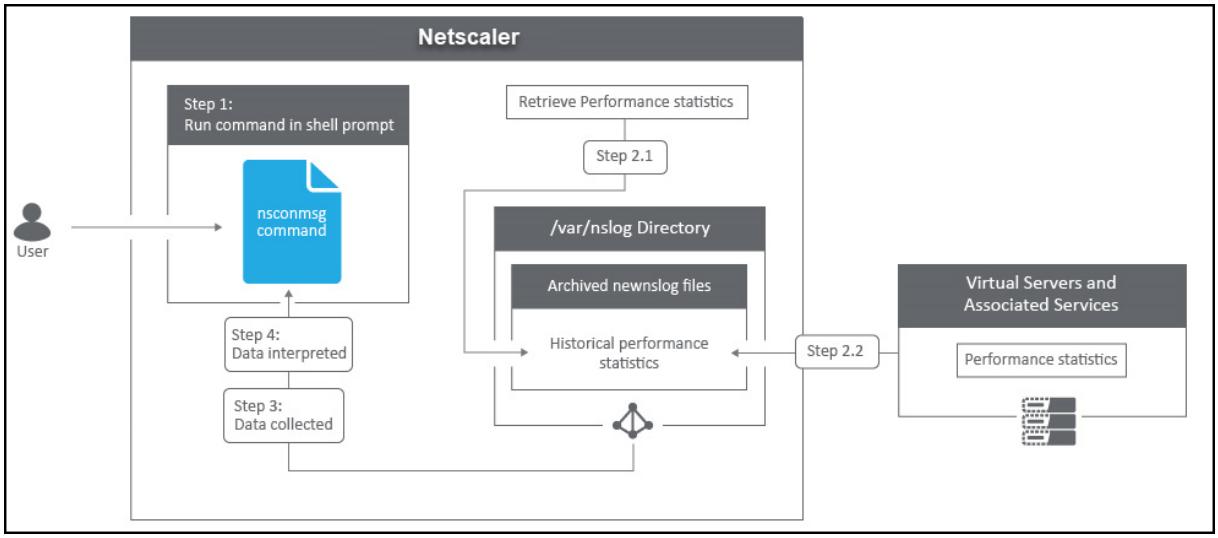
HTTP                                     Rate (/s)               Total
Total requests                                   0               191529
Total responses                                  0               263011
Request bytes received                        7007           1178810535
Response bytes received                     164477          12348432171

SSL                                      Rate (/s)               Total
```

NetScaler possède une structure d'archivage des journaux qui permet de rechercher des statistiques et des compteurs lors de la résolution d'erreurs spécifiques via la commande « **NSCONMSG** ».

NSCONMSG - fichier journal principal (format de données ns)

```
1      Cd/var/nslog
2
3       “Mac Moves”
4      nsconmsg -d current -g nic_err
5  <!--NeedCopy-->
```

Nstcpdump

Vous pouvez utiliser `nstcpdump` pour le dépannage de bas niveau. `nstcpdump` recueille des informations moins détaillées que `nstrace`. Ouvrez l'interface de ligne de commande ADC et tapez `shell`. Vous pouvez utiliser des filtres avec `nstcpdump` mais ne pouvez pas utiliser de filtres spécifiques aux ressources ADC. La sortie de vidage peut être visualisée directement dans l'écran CLI.

CTRL + C — Appuyez simultanément sur ces touches pour arrêter un `nstcpdump`.

`nstcpdump.sh dst host x.x.x.x` : affiche le trafic envoyé à l'hôte de destination.

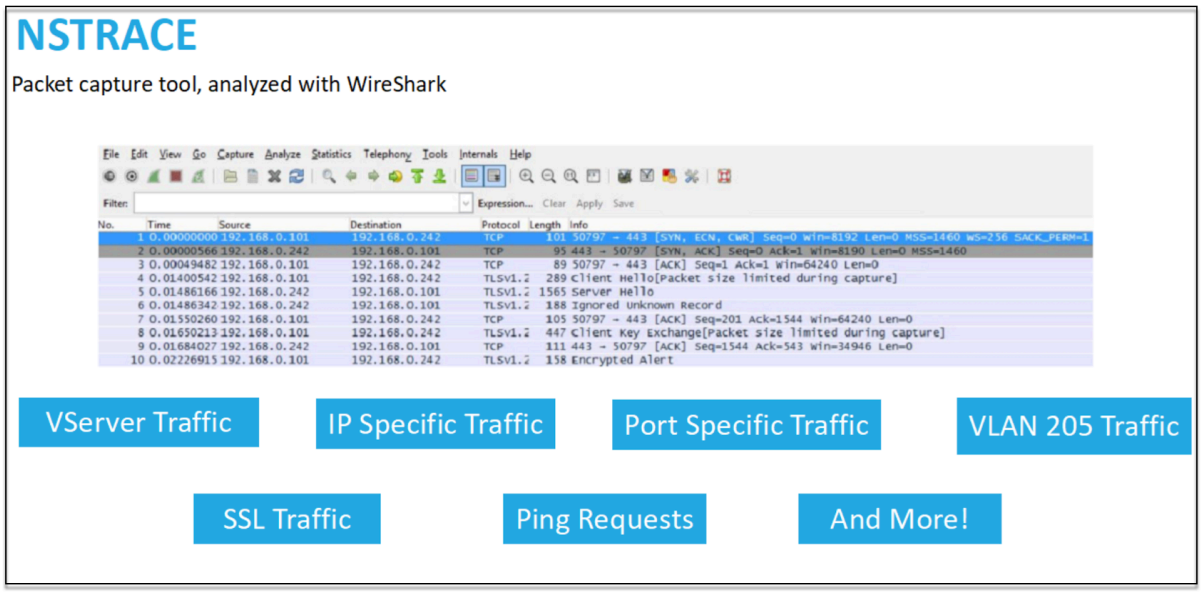
`nstcpdump.sh -n src host x.x.x.x` — Affiche le trafic provenant de l'hôte spécifié et ne convertit pas les adresses IP en noms (-n).

`nstcpdump.sh host x.x.x.x` — Affiche le trafic vers et depuis l'adresse IP de l'hôte spécifiée.


```
root@Netscaler1# nstcpdump.sh -c 10 dst host 192.168.0.242
reading from file -, link-type EN10MB (Ethernet)
21:45:45.834700 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [S], seq 1702255264, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sackOK],
length 0
21:45:45.836702 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 748367253, win 64240, length 0
21:45:45.837202 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [P.], ack 1, win 64240, length 232
21:45:45.839203 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 1544, win 64240, length 0
21:45:45.840244 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [P.], ack 1544, win 64240, length 342
21:45:45.847709 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [P.], ack 1619, win 64165, length 469
21:45:45.994744 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [P.], ack 2712, win 63072, length 581
21:45:46.002746 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 7092, win 64240, length 0
21:45:46.003250 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 15853, win 64240, length 0
21:45:46.009748 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 30455, win 64240, length 0
```

NSTRACE - fichier de suivi des paquets

NSTRACE est un outil de débogage de paquets de bas niveau destiné au dépannage des réseaux. Il vous permet de stocker des fichiers de capture que vous pouvez analyser davantage à l'aide des outils d'analyse. Les deux outils courants sont Network Analyzer et Wireshark.




```
> start nstrace -size 0
 Done
> stop nstrace
 Done
```


Une fois le fichier de capture NSTRACE créé dans /var/nstrace sur l'ADC, vous pouvez importer le fichier de capture dans Wireshark pour la capture de paquets et l'analyse du réseau.

SYSCTL - Informations détaillées sur l'ADC : description, modèle, plate-forme, processeurs, etc

```
1      sysctl -a grep hw.physmem
2
3      hw.physmem: 862306304
4      netscaler.hw_physmem_mb: 822
5  <!--NeedCopy-->
```

aaad.debug - Canal ouvert pour les informations de débogage d'authentification

```
process_radius Got RADIUS event
process_radius Received BAD_ACCESS_REJECT for: <username>
process_radius Sending reject.
send_reject_with_code Rejecting with error code 4001.
```

Pour plus d'informations sur la façon de résoudre les problèmes d'authentification via ADC ou ADC Gateway avec le module aaad.debug, consultez l'article de support aaad.debug.

Il est également possible d'obtenir des statistiques de performances et des journaux d'événements directement pour l'ADC. Pour plus d'informations à ce sujet, consultez le document de support ADC.

Dépannage pour les équipes SRE et plateformes

Flux de trafic Kubernetes

Nord/Sud :

- Le trafic Nord/Sud est le trafic circulant de l'utilisateur vers le cluster, via l'entrée.

Est/Ouest :

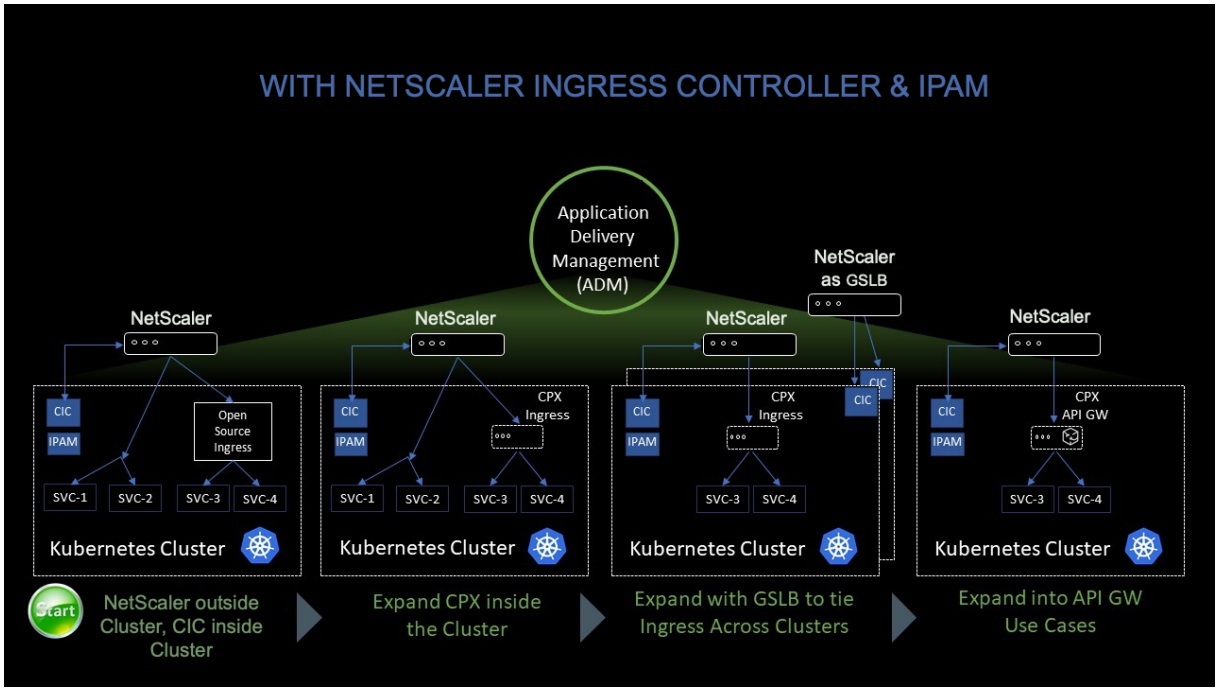
- Le trafic est/ouest est le trafic circulant autour du cluster Kubernetes : service à service ou service à magasin de données.

Comment NetScaler CPX équilibre la charge du flux de trafic est-ouest dans un environnement Kubernetes

Après avoir déployé le cluster Kubernetes, vous devez intégrer le cluster à ADM en fournissant les détails de l'environnement Kubernetes dans ADM. ADM surveille les modifications apportées aux ressources Kubernetes, telles que les services, les points de terminaison et les règles d'entrée.

Lorsque vous déployez une instance NetScaler CPX dans le cluster Kubernetes, elle s'enregistre automatiquement auprès d'ADM. Dans le cadre du processus d'enregistrement, ADM prend connaissance de l'adresse IP de l'instance CPX et du port sur lequel il peut atteindre l'instance pour la configurer à l'aide des API REST NITRO.

La figure suivante montre comment NetScaler CPX équilibre la charge du flux de trafic est-ouest dans un cluster Kubernetes.



Dans cet exemple,

Le nœud 1 et le nœud 2 des clusters Kubernetes contiennent des instances d'un service frontal et d'un service principal. Lorsque les instances NetScaler CPX sont déployées dans les nœuds 1 et 2, les instances NetScaler CPX sont automatiquement enregistrées auprès d'ADM. Vous devez intégrer manuellement le cluster Kubernetes à ADM en configurant les détails du cluster Kubernetes dans ADM.

Lorsqu'un client demande le service frontal, la charge de ressource d'entrée équilibre la demande entre les instances du service frontal sur les deux nœuds. Lorsqu'une instance du service frontal a besoin d'informations provenant des services principaux du cluster, elle dirige les demandes vers l'instance NetScaler CPX de son nœud. Cette instance NetScaler CPX équilibre la charge des demandes entre les services principaux du cluster, fournissant ainsi un flux de trafic est-ouest.

Graphique de service ADM pour les applications

La fonctionnalité graphique des services de NetScaler ADM vous permet de surveiller tous les services dans une représentation graphique. Cette fonctionnalité fournit également une analyse détaillée et des mesures utiles. Vous pouvez consulter les graphiques de service pour :

- Applications configurées sur toutes les instances NetScaler
- Applications Kubernetes
- Applications Web à 3 niveaux

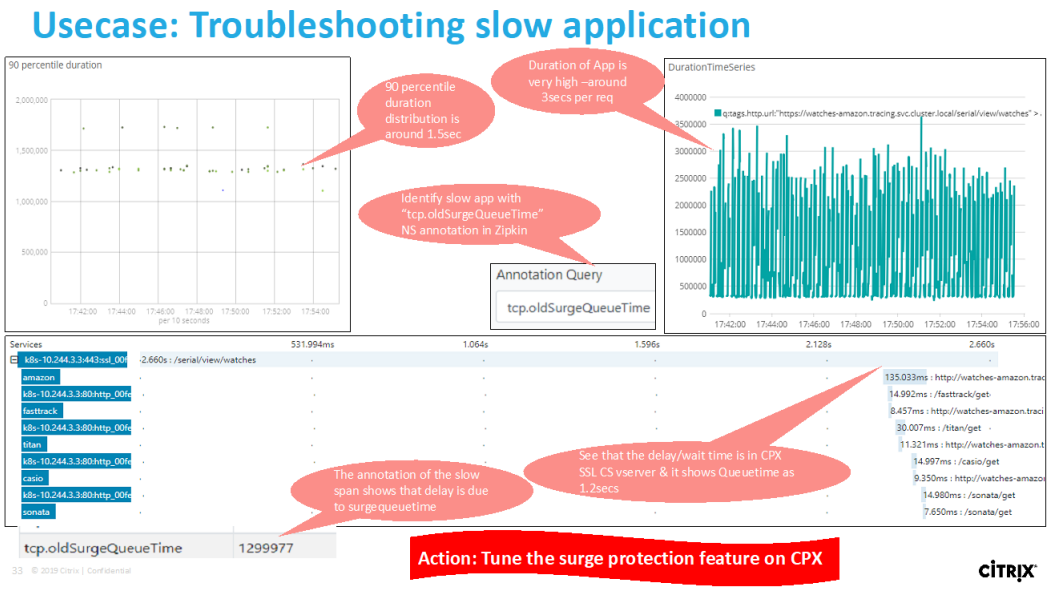
Pour commencer, consultez les détails dans le graphique de service.

Afficher les compteurs d'applications de microservices

Le graphique de service affiche également toutes les applications de microservice appartenant aux clusters Kubernetes. Toutefois, le pointeur de la souris sur un service permet d'afficher les détails des mesures.

Vous pouvez consulter les éléments suivants :

- Le nom du service
- Le protocole utilisé par le service tel que SSL, HTTP, TCP, SSL sur HTTP
- **Hits** — Nombre total d'accès reçus par le service
- **Temps de réponse du service** — Temps de réponse moyen pris par le service.
  (Temps de réponse = RTT client + demande le dernier octet — demande le premier octet)
- **Erreurs** — Les erreurs totales telles que 4xx, 5xx, et ainsi de suite
- **Volume de données** — Volume total de données traitées par le service
- **Espace de noms** — Espace de noms du service
- **Nom du cluster** — Nom du cluster où le service est hébergé
- **Erreurs SSL Server** : nombre total d'erreurs SSL provenant du service



Ces compteurs et journaux de transactions spécifiques peuvent être extraits via NetScaler Observability Exporter (COE) à l'aide d'une gamme de points de terminaison compatibles. Pour plus d'informations sur COE, consultez les sections suivantes.

Exportateur pour les statistiques de NetScaler

Il s'agit d'un serveur simple qui extrait les statistiques de NetScaler et les exporte via HTTP vers Prometheus. Prometheus peut ensuite être ajouté en tant que source de données à Grafana pour afficher graphiquement les statistiques de NetScaler.

Pour surveiller les statistiques et les compteurs des instances NetScaler, `citrix-adc-metric-exporter` vous pouvez les exécuter sous forme de conteneur ou de script. L'exportateur collecte des statistiques NetScaler telles que le nombre total d'accès à un serveur virtuel, le taux de requêtes HTTP, le taux de cryptage/déchiffrement SSL, etc. à partir des instances NetScaler et les conserve jusqu'à ce que le serveur Prometheus extrait les statistiques et les enregistre avec un horodatage. Grafana peut ensuite être pointé vers le serveur Prometheus pour récupérer les statistiques, les tracer, définir des alarmes, créer des cartes thermiques, générer des tableaux, etc. selon les besoins pour analyser les statistiques de NetScaler.

Les sections suivantes fournissent des détails sur la configuration de l'exportateur pour qu'il fonctionne dans un environnement tel qu'indiqué dans la figure. Une note sur les entités/métriques NetScaler que l'exportateur extrait par défaut et sur la manière de les modifier est également expliquée.

Pour plus d'informations sur Exporter pour NetScaler, consultez le GitHub de Metrics Exporter.

Suivi distribué du service ADM

Dans le graphique de service, vous pouvez utiliser la vue de suivi distribué pour :

- Analysez les performances globales du service.
- Visualisez le flux de communication entre le service sélectionné et ses services interdépendants.
- Identifier le service qui indique des erreurs et dépanner le service erroné
- Affichez les détails des transactions entre le service sélectionné et chaque service interdépendant.

Prérequis pour le suivi distribué ADM

Pour afficher les informations de suivi du service, vous devez :

- Assurez-vous qu'une application conserve les en-têtes de trace suivants, tout en envoyant tout trafic est-ouest :

- x-request-id
- x-b3-traceid
- x-b3-spanid
- x-b3-parentspanid
- x-b3-sampled
- x-b3-flags
- x-ot-span-context

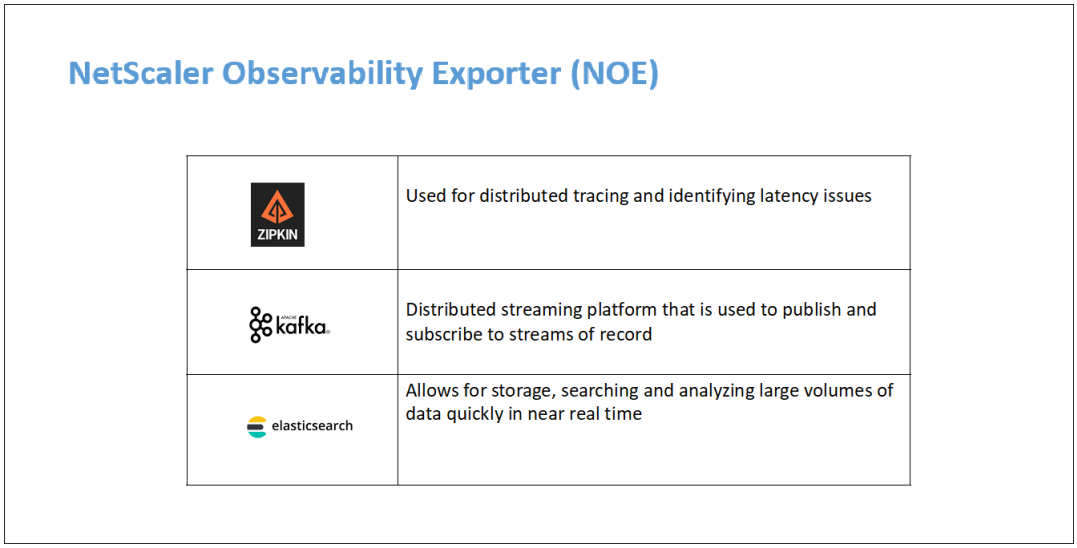
  - Mettez à jour le fichier YAML CPX avec NS_DISTRIBUTED_TRACING et la valeur sur YES. Pour commencer, consultez la section Suivi distribué.

Analyse de NetScaler Observability Exporter (COE)

NetScaler Observability Exporter est un conteneur qui collecte des métriques et des transactions auprès de NetScalers et les transforme en formats adaptés (tels que JSON, AVRO) pour les terminaux pris en charge. Vous pouvez exporter les données collectées par NetScaler Observability Exporter vers le point de terminaison souhaité. En analysant les données exportées vers le terminal, vous pouvez obtenir des informations précieuses au niveau des microservices pour les applications fournies par proxy par NetScalers.

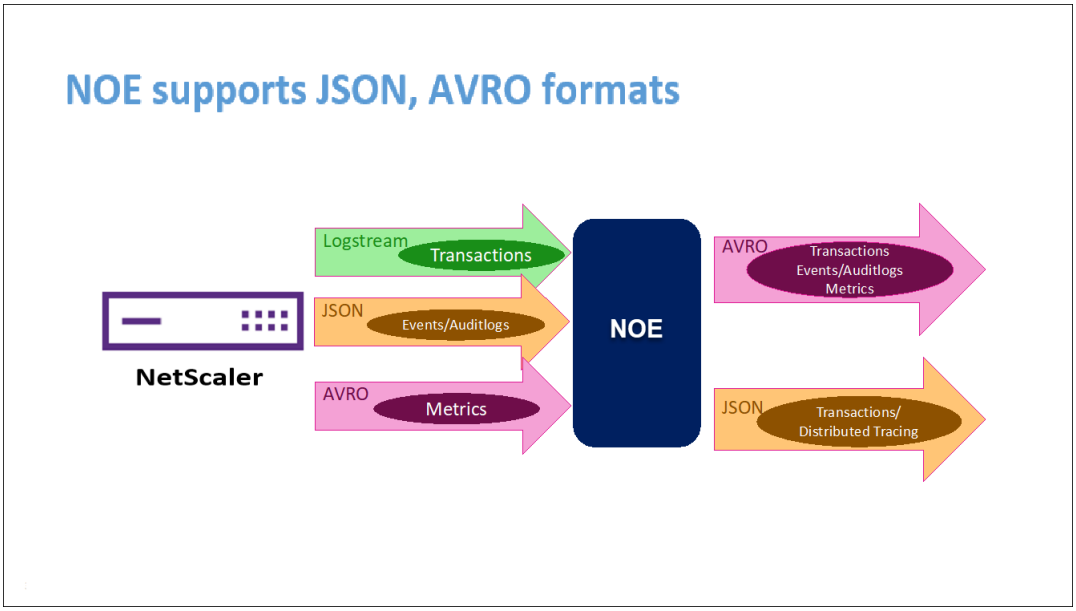
Pour plus d'informations sur COE, consultez COE GitHub.

COE avec Elasticsearch comme point de terminaison de transaction



Lorsque Elasticsearch est spécifié comme point de terminaison de la transaction, NetScaler Observability Exporter convertit les données au format JSON. Sur le serveur Elasticsearch, NetScaler Observ-

ability Exporter crée des index Elasticsearch pour chaque ADC sur une base horaire. Ces index sont basés sur les données, l'heure, l'UUID de l'ADC et le type de données HTTP (http_event ou http_error). Ensuite, l'exportateur NetScaler Observability télécharge les données au format JSON sous les index de recherche Elastic pour chaque ADC. Toutes les transactions régulières sont placées dans l'index http_event et toutes les anomalies sont placées dans l'index http_error.



Prise en charge du suivi distribué avec Zipkin

Dans une architecture de microservices, une seule demande d'utilisateur final peut s'étendre à plusieurs microservices, ce qui rend difficile le suivi d'une transaction et la résolution des sources d'erreurs. Dans de tels cas, les méthodes traditionnelles de surveillance des performances ne permettent pas de déterminer avec précision où les défaillances se produisent et quelle est la raison de ces mauvaises performances. Vous avez besoin d'un moyen de capturer des points de données spécifiques à chaque microservice traitant une demande et de les analyser pour obtenir des informations pertinentes.

Le suivi distribué répond à ce défi en fournissant un moyen de suivre une transaction de bout en bout et de comprendre comment elle est gérée sur plusieurs microservices.

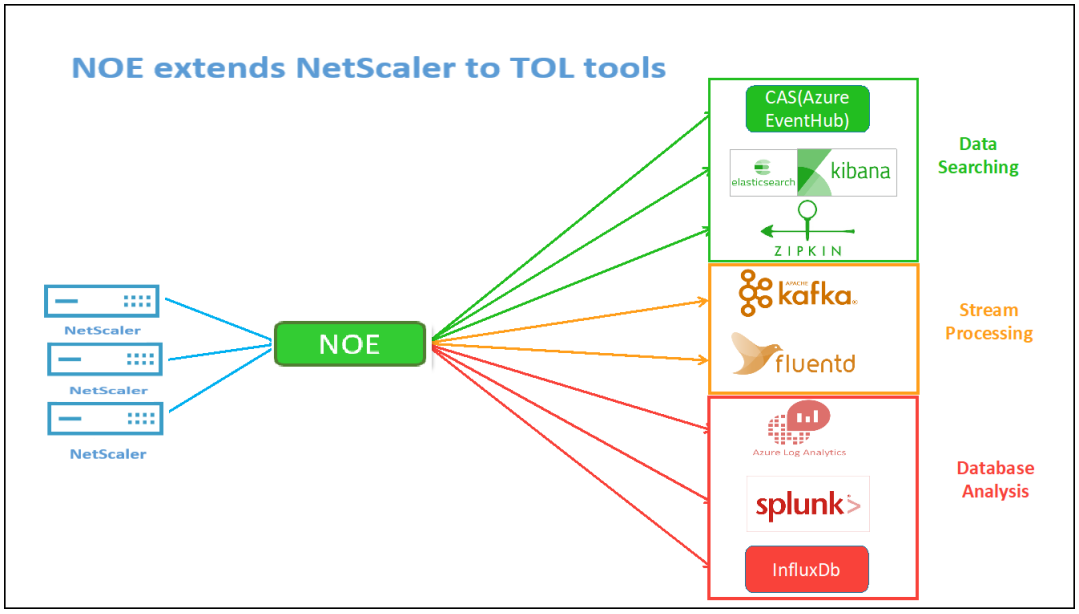
OpenTracing est une spécification et un ensemble standard d'API pour la conception et la mise en œuvre du suivi distribué. Les traceurs distribués vous permettent de visualiser le flux de données entre vos microservices et d'identifier les goulots d'étranglement dans votre architecture de microservices.

NetScaler Observability Exporter implémente le traçage distribué pour NetScaler et prend actuellement en charge Zipkin en tant que traceur distribué.

Actuellement, vous pouvez surveiller les performances au niveau de l'application à l'aide de NetScaler. À l'aide de NetScaler Observability Exporter avec NetScaler, vous pouvez obtenir des données de suivi

pour les microservices de chaque application via un proxy par votre NetScaler CPX, MPX ou VPX.

Pour commencer, consultez l' exportateur d'observabilité GitHub.

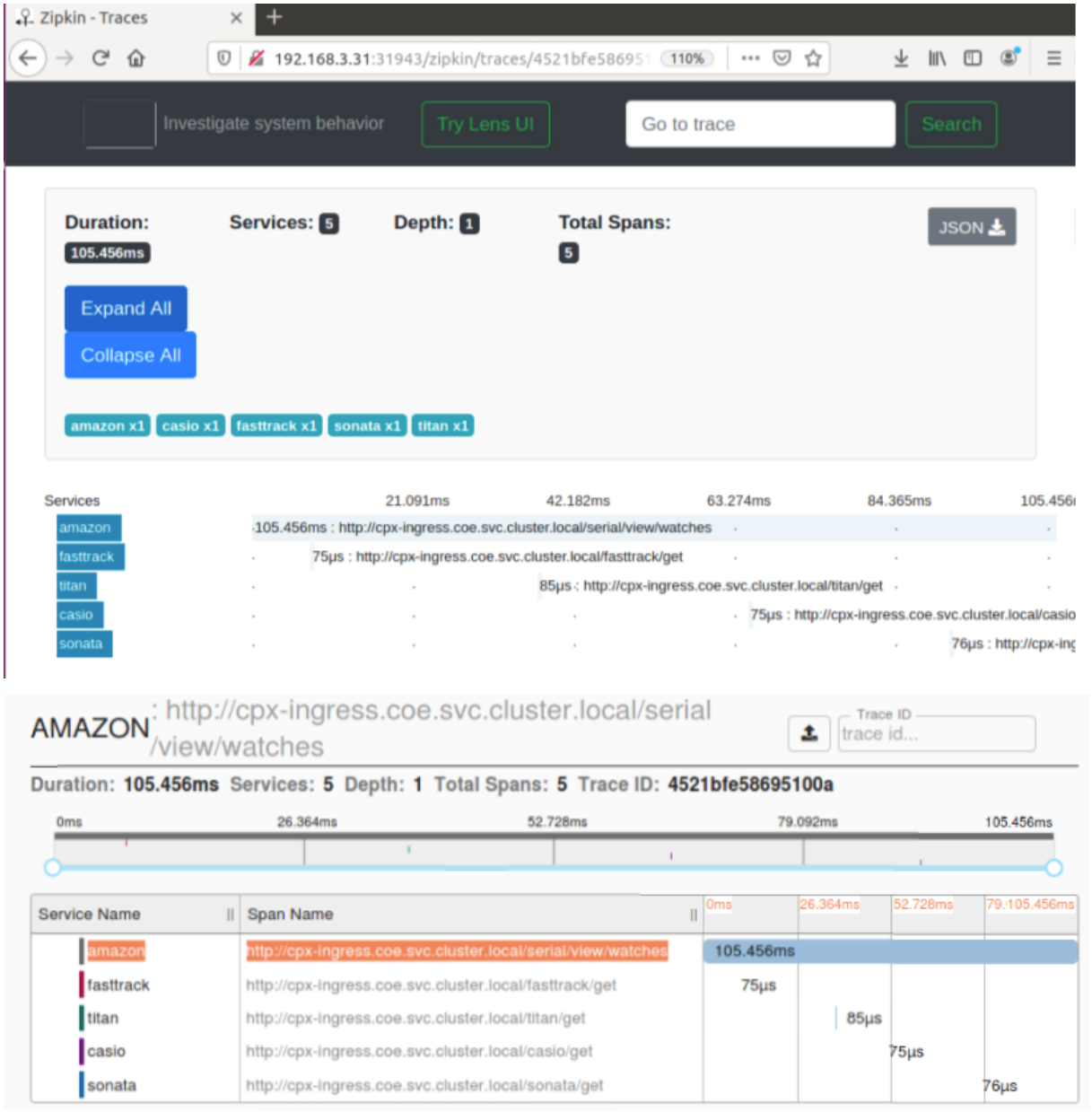


Zipkin pour le débogage des applications

Zipkin est un système de traçage distribué open source basé sur l'article de Dapper de Google. Dapper est le système de Google pour son système de traçage distribué en production. Google explique cela dans son article : « Nous avons conçu Dapper pour fournir aux développeurs de Google plus d'informations sur le comportement des systèmes distribués complexes ». L'observation du système sous différents angles est essentielle lors du dépannage, en particulier lorsqu'un système est complexe et distribué.

Les données de trace Zipkin suivantes identifient un total de 5 spans et 5 services liés à l'exemple d'application Watches. Les données de suivi montrent les données de portée spécifiques sur les 5 microservices.

Pour commencer, consultez Zipkin.



Exemple de plage Zipkin montrant la latence de l’application pour la demande initiale de chargement de

Services: amazon

Date Time	Relative Time	Annotation	Address
7/15/2020, 2:14:24 PM		Server Start	10.10.235.179:1719 (amazon)
7/15/2020, 2:14:24 PM	105.456ms	Server Finish	10.10.235.179:1719 (amazon)

Key	Value
component	py_zipkin
http.host	amazon:1719
http.method	GET
http.path	/serial/view/watches
http.url	http://cpx-ingress.coe.svc.cluster.local/serial/view/watches
Local Component	amazon
peer.address	10.10.235.190

Kibana pour l'affichage des données

Kibana est une interface utilisateur ouverte qui vous permet de visualiser vos données Elasticsearch et de naviguer dans Elastic Stack. Faites n'importe quoi, du suivi du chargement des requêtes à la compréhension de la façon dont les demandes circulent dans vos applications

Que vous soyez analyste ou administrateur, Kibana rend vos données exploitables en fournissant les trois fonctions clés suivantes :

- **Une plateforme d'analyse et de visualisation open source.** Utilisez Kibana pour explorer vos données Elasticsearch, puis créez de superbes visualisations et tableaux de bord.
- **Une interface utilisateur pour gérer la pile Elastic.** Gérez vos paramètres de sécurité, attribuez des rôles d'utilisateur, prenez des instantanés, regroupez vos données et bien plus encore, le tout depuis le confort d'une interface utilisateur Kibana.

- **Un hub centralisé pour les solutions Elastic.** De l'analyse des journaux à la découverte de documents en passant par le SIEM, Kibana est le portail d'accès à ces fonctionnalités et à d'autres.

Kibana est conçu pour utiliser Elasticsearch comme source de données. Considérez Elasticsearch comme le moteur qui stocke et traite les données, avec Kibana en tête.

Sur la page d'accueil, Kibana propose les options suivantes pour ajouter des données :

- Importez des données en utilisant le visualiseur de données de fichier.
- Configurez un flux de données vers Elasticsearch à l'aide de nos didacticiels intégrés. S'il n'existe aucun didacticiel pour vos données, consultez l' aperçu Beats pour en savoir plus sur les autres expéditeurs de données de la famille Beats.
- Ajoutez un exemple d'ensemble de données et faites un essai routier de Kibana sans charger de données vous-même.
- Indexez vos données dans Elasticsearch avec des API REST ou des bibliothèques clientes

Kibana utilise un modèle d'index pour indiquer les indices Elasticsearch à explorer. Si vous téléchargez un fichier, exécutez un didacticiel intégré ou ajoutez des exemples de données, vous obtenez un modèle d'index gratuitement et vous pouvez commencer à explorer. Si vous chargez vos propres données, vous pouvez créer un modèle d'index dans Stack Management.

Étape 1 : Configurer le modèle d'index pour Logstash

Étape 2 : Sélectionnez l'index et générez le trafic à remplir.

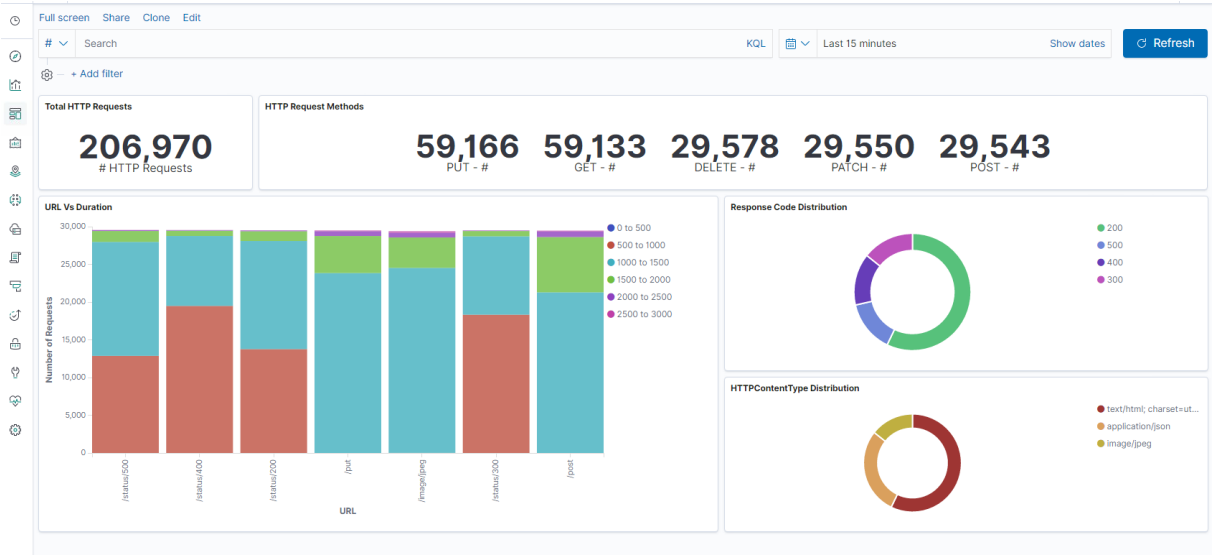
Étape 3 : générer une application à partir des données non structurées issues des flux de journaux.

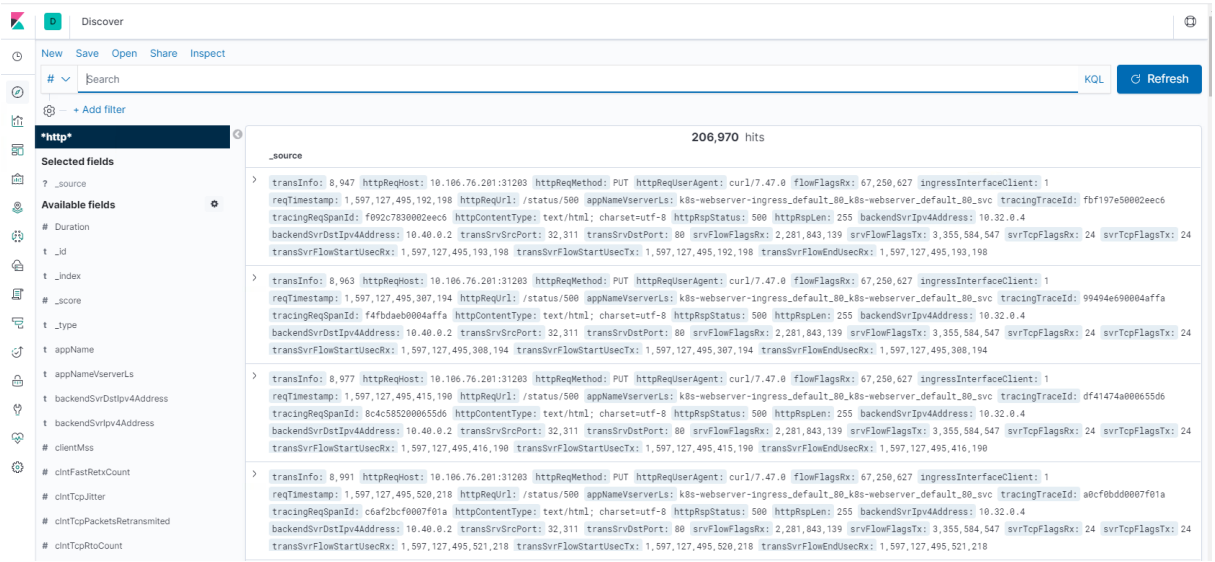
Étape 4 : Kibana met en forme l'entrée Logstash pour créer des rapports et des tableaux de bord.

- Plage de temps
- Vue tabulaire
- Nombre de visites en fonction de l'application.
  - IP de temps, agent, machine.OS, code de réponse (200), URL
  - Filtre sur les valeurs

Étape 5 : Visualisez les données dans un rapport d'agrégations.

- Agrégation des résultats dans un rapport graphique (secteur, graphique, etc.)





Déployer une instance NetScaler VPX

May 5, 2023

> **Remarque**
>
> La connexion au service NetScaler ADM est activée par défaut, après l'installation ou la mise à niveau de NetScaler ou NetScaler Gateway vers la version 13.0 build 61.xx et ultérieure. Pour plus d'informations, voir Gouvernance des données et connexion au service NetScaler ADM.

Le produit NetScaler VPX est une appliance virtuelle qui peut être hébergée sur une grande variété de plateformes de virtualisation et de cloud :

- Citrix Hypervisor
- VMware ESX
- Microsoft Hyper-V
- Linux KVM
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

Pour plus d'informations, consultez la fiche technique de NetScaler VPX.

Pour plus d'informations sur le provisionnement d'une instance NetScaler VPX sur une appliance SDX, consultez la section Provisioning d'instances NetScaler.

Gestion de la mise à disposition des applications NetScaler pour NetScaler VPX

Le logiciel NetScaler Application Delivery Management est une solution de gestion centralisée qui simplifie les opérations en fournissant aux administrateurs une visibilité à l'échelle de l'entreprise et en automatisant les tâches de gestion qui doivent être exécutées sur plusieurs instances.

Vous pouvez gérer et surveiller les instances NetScaler VPX en plus d'autres produits NetScaler tels que NetScaler Gateway, NetScaler SDX, NetScaler CPX et Citrix SD-WAN. Vous pouvez utiliser le logiciel Application Delivery Management pour gérer, surveiller et dépanner l'ensemble de l'infrastructure de livraison d'applications à partir d'une console unifiée unique.

Pour plus d'informations, consultez la documentation de NetScaler Application Delivery Management.

Matrice de prise en charge et directives d'utilisation

July 31, 2023

Ce document répertorie les différents hyperviseurs et fonctionnalités pris en charge sur une instance NetScaler VPX. Le document décrit également leurs consignes d'utilisation et leurs limitations connues.

Instance VPX sur Citrix Hypervisor

Version Citrix Hypervisor	SysID	Modèles VPX
8.2 pris en charge à partir de 13.0, 64.x, 8.0, 7.6, 7.1	450000	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10 G, VPX 15 G, VPX 25 G, VPX 40 G

Instance VPX sur l'hyperviseur VMware ESXi

Version ESX	Date de sortie d'ESX (AAAA/MM/JJ)	Numéro de build ESX	Version de NetScaler VPX	SysID	Modèles VPX
ESXi 8.0u1	2023/04/18	21495797	À partir de 13,1-45.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 8.0 c	2023/03/30	21493926	À partir de 13,1-45.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX (AAAA/MM/JJ)	Numéro de build ESX	Version de NetScaler VPX	SysID	Modèles VPX
ESXi 8.0	2022/10/11	20513097	13,1 à 42,x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
Mise à jour ESXi 7.0 3m	2023/05/03	21686933	À partir de 13,1-48.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
Mise à jour 3i d'ESXi 7.0	2022/12/08	20842708	13.1-37.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX (AAAA/MM/JJ)	Numéro de build ESX	Version de NetScaler VPX	SysID	Modèles VPX
Mise à jour 3f d'ESXi 7.0	2022/07/12	20036589	13,1-33.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
Mise à jour d'ESXi 7.0 3d	2022/03/29	19482537	À partir de 13,1-27.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0 update 3c	2022/01/27	19193900	À partir de 13.1-21.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX (AAAA/MM/JJ)	Numéro de build ESX	Version de NetScaler VPX	SysID	Modèles VPX
Mise à jour 2D d'ESX 7.0	2021/09/14	18538813	À partir de 13.1-9.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESX 7.0 update 2a	2021/04/29	17867351	13.1-4.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESX 7.0 update 1d	2021/02/02	17551050	13.0-82.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX (AAAA/MM/JJ)	Numéro de build ESX	Version de NetScaler VPX	SysID	Modèles VPX
ESX 7.0 update 1c	2020/12/17	17325551	13.0-79.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESX 7.0 update 1b	2020/10/06	16850804	13.0-76.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0b	2020/06/23	16324942	13.0-71.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX (AAAA/MM/JJ)	Numéro de build ESX	Version de NetScaler VPX	SysID	Modèles VPX
ESXi 7.0 GA	2020/04/02	15843807	13.0-71.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P04	2020/11/19	17167734	13.0-67.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P03	2020/08/20	16713306	13.0-67.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX (AAAA/MM/JJ)	Numéro de build ESX	Version de NetScaler VPX	SysID	Modèles VPX
ESXi 6.7 P02	2020/04/28	16075168	13.0-67.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P01	2019/12/05	15160138	13.0-67.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 Update 3	2019/08/20	14320388	13.0-58.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX (AAAA/MM/JJ)	Numéro de build ESX	Version de NetScaler VPX	SysID	Modèles VPX
ESXi 6.7 U2	2019/04/11	13006603	13.0-47.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.5 GA	2016/11/15	4564106	13.0-47.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.5 U1g	2018/3/20	7967591	13.0 47.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Version ESX	Date de sortie d'ESX (AAAA/MM/JJ)	Numéro de build ESX	Version de NetScaler VPX	SysID	Modèles VPX
ESXi 6.0 Update 3	2017/2/24	5050593	12.0-51.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.0 Express Patch 11	2017/10/5	6765062	12.0-56.x et versions ultérieures	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Instance VPX sur Microsoft Hyper-V

Version Hyper-V	SysID	Modèles VPX
2012, 2012 R2, 2016, 2019	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000

Instance VPX sur KVM générique

Version KVM générique	SysID	Modèles VPX
RHEL 7.4, RHEL 7.5 (à partir de NetScaler version 12.1 50.x), RHEL 7.6, RHEL 8.0, Ubuntu 16.04, Ubuntu 18.04, RHV 4.2	450070	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10 G, VPX 15 G. VPX 25G, VPX 40G, VPX 100G

Points à noter :

Lorsque vous utilisez les hyperviseurs KVM, tenez compte des points suivants.

- L'instance VPX est qualifiée pour les versions de version de l'Hypervisor mentionnées dans le tableau 1—4, et non pour les versions de correctifs dans une version. Toutefois, l'instance VPX devrait fonctionner de manière transparente avec les versions de correctifs d'une version prise en charge. Si ce n'est pas le cas, consignez un dossier de support pour le dépannage et le débogage.
- Avant d'utiliser RHEL 7.6, effectuez les étapes suivantes sur l'hôte KVM :
  1. Modifiez /etc/default/grub et ajoutez `"kvm_intel.preemption_timer=0"` à la variable `GRUB_CMDLINE_LINUX`.
  2. Régénérez le fichier grub.cfg à l'aide de la commande `"## grub2-mkconfig -o /boot/grub2/grub.cfg"`.
  3. Redémarrez la machine hôte.
- Avant d'utiliser Ubuntu 18.04, effectuez les étapes suivantes sur l'hôte KVM :
  1. Modifiez /etc/default/grub et ajoutez `"kvm_intel.preemption_timer=0"` à la variable `GRUB_CMDLINE_LINUX`.
  2. Régénérez le fichier grub.cfg à l'aide de la commande `"## grub-mkconfig -o /boot/grub/grub.cfg "`.
  3. Redémarrez la machine hôte.

Instance VPX sur AWS

Version AWS	SysID	Modèles VPX
S/O	450040	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX BYOL, VPX 8000, VPX 10G, VPX 15G et VPX 25G sont disponibles uniquement avec BYOL avec les types d'instances EC2 (C5, M5 et C5n)

> **Remarque :**
>
> L'offre VPX 25G ne fournit pas le débit de 25 Go d'AWS mais peut offrir un taux de transactions SSL plus élevé que l'offre VPX 15G.

Instance VPX sur Azure

Version Azure	SysID	Modèles VPX
S/O	450020	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX BYOL

Matrice des fonctionnalités VPX

	VPX on XenServer		VPX on VMware ESX				VPX on Microsoft Hyper-V	VPX on generic KVM			VPX on AWS	VPX on Azure	VPX on GCP
Features	**PV**	**SR-IOV**	**PV**	**SR-IOV**	**Emulated**	**PCI Passthrough**	**PV**	**PV**	**SR-IOV**	**PCI Passthrough**			
Multi-PE Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Clustering Support	Yes	Yes[1]	Yes	Yes[1]	Yes	Yes	Yes	Yes	Yes[1]	Yes	No	No	No
VLAN Tagging	Yes	Yes	Yes	Yes	Yes	Yes	Yes (only on 2012R2)	Yes	Yes	Yes	No	No	No
Detecting Link Events	No[2]	Yes[3]	No[2]	Yes[3]	No[2]	Yes[3]	No[2]	No[2]	Yes[3]	Yes[3]	No[2]	No[2]	No[2]
Interface Parameter Configuration	No	No	No	No	No	Yes	No	No	No	Yes	No	No	No
Static LA	Yes[2]	Yes[3]	Yes[2]	No	Yes[2]	Yes[3]	Yes[2]	Yes[2]	Yes[3]	Yes[3]	No	No	No
LACP	No	Yes[3]	Yes[2]	No	Yes[2]	Yes[3]	No	Yes[2]	Yes[3]	Yes[3]	No	No	No
Static CLAG	No	No	No	No	No	No	No	No	No	No	No	No	No
LACP CLAG	No	No	Yes[2]	No	Yes[2]	Yes[3]	No	Yes[2]	Yes[3]	Yes[3]	No	No	No
Hot-plug	No	No	No	No	No	No	No	No	No	No	Yes	No	No

Les nombres en exposant (1, 2, 3) utilisés dans le tableau précédent se réfèrent aux points suivants

avec une numérotation respective :

1. La prise en charge du clustering est disponible sur SRIOV pour les interfaces côté client et côté serveur, et non pour le fond de panier.
2. Les événements Interface DOWN ne sont pas enregistrés dans les instances NetScaler VPX.
3. Pour LA statique, le trafic peut toujours être envoyé sur l'interface dont l'état physique est DOWN.
4. Pour LACP, le périphérique homologue connaît l'événement DOWN de l'interface basé sur le mécanisme de délai d'expiration LACP.
    - Délai d'expiration court : 3 secondes
    - Délai d'attente long : 90 secondes
5. Pour LACP, ne partagez pas les interfaces entre les machines virtuelles.
6. Pour le routage dynamique, le temps de convergence dépend du protocole de routage car les événements de liaison ne sont pas détectés.
7. La fonctionnalité Routage statique surveillé échoue si vous ne liez pas les moniteurs à des routes statiques, car l'état de l'itinéraire dépend de l'état du VLAN. L'état du VLAN dépend de l'état de la liaison.
8. La détection de défaillance partielle ne se produit pas en haute disponibilité en cas de défaillance de liaison. Une condition cérébrale divisée à haute disponibilité peut se produire en cas de défaillance de liaison.
    - Lorsqu'un événement de lien (désactiver/activer, réinitialiser) est généré à partir d'une instance VPX, l'état physique du lien ne change pas. Pour LA statique, tout trafic initié par le pair est supprimé sur l'instance.
    - Pour que la fonctionnalité de balisage VLAN fonctionne, procédez comme suit :

    Sur VMware ESX, définissez l'ID VLAN du groupe de ports sur 1 à 4095 sur le vSwitch du serveur VMware ESX. Pour plus d'informations sur la définition d'un ID VLAN sur le vSwitch du serveur VMware ESX, consultez Solutions VLAN VMware ESX Server 3 802.1Q.

Navigateurs pris en charge

Système d'exploitation	Navigateur et versions
Windows 7	Internet Explorer - 8, 9, 10 et 11 ; Mozilla Firefox 3.6.25 et versions ultérieures ; Google Chrome - 15 et versions ultérieures

Système d'exploitation	Navigateur et versions
Windows 64 bits	Internet Explorer - 8, 9 ; Google Chrome - 15 et versions ultérieures
MAC	Mozilla Firefox - 12 et versions ultérieures ; Safari - 5.1.3 ; Google Chrome - 15 et versions ultérieures

Prise en charge des processeurs AMD pour les instances VPX

À partir de la version 13.1 de NetScaler, l'instance VPX prend en charge à la fois les processeurs Intel et AMD. Les appliances virtuelles VPX peuvent être déployées sur n'importe quel type d'instance doté d'au moins deux cœurs virtualisés et de plus de 2 Go de mémoire. Pour plus d'informations sur la configuration système requise, consultez la fiche technique de NetScaler VPX.

Plateformes VPX vs. Tableau matriciel NIC

Le tableau suivant répertorie les cartes réseau prises en charge sur une plate-forme VPX ou un cloud.

	Mellanox CX-3	Mellanox CX-4	Mellanox CX-5	Intel 82599 SRIOV VF	Intel X710/X722/XL710 SRIOV VF	Mode PCI-Passthrough Intel X710/XL710
VPX (ESXi)	Non	Oui	Non	Oui	Non	Oui
VPX (Citrix Hypervisor)	SO	SO	SO	Oui	Oui	Non
VPX (KVM)	Non	Oui	Non	Oui	Oui	Oui
VPX (Hyper-V)	SO	SO	SO	Non	Non	Non
VPX (AWS)	SO	SO	SO	Oui	SO	SO
VPX (Azure)	Oui	Oui	Oui	SO	SO	SO
VPX (GCP)	SO	SO	SO	SO	SO	SO

Directives d'utilisation

Suivez ces instructions d'utilisation :

- Nous vous recommandons de déployer une instance VPX sur les disques locaux du serveur ou sur des volumes de stockage SAN.

Consultez la section **Considérations relatives au processeur VMware ESXi** dans le document Meilleures pratiques en matière de performances pour VMware vSphere 6.5 . Voici un extrait :

- Il n'est pas recommandé que les machines virtuelles nécessitant beaucoup de CPU ou de mémoire soient installées sur un hôte ou un cluster surchargé.
- Dans la plupart des environnements, ESXi permet des niveaux significatifs de surcharge du processeur sans affecter les performances des machines virtuelles. Sur un hôte, vous pouvez exécuter plus de processeurs virtuels que le nombre total de cœurs de processeur physiques de cet hôte.
- Si un hôte ESXi devient saturé en processeur, c'est-à-dire que les machines virtuelles et les autres charges sur l'hôte exigent toutes les ressources CPU dont dispose l'hôte, les charges de travail sensibles à la latence risquent de ne pas fonctionner correctement. Dans ce cas, vous pouvez réduire la charge du processeur, par exemple en mettant hors tension certaines machines virtuelles ou en les migrant vers un autre hôte (ou en autorisant DRS à les migrer automatiquement).
- Citrix recommande la dernière version de compatibilité matérielle pour bénéficier des derniers ensembles de fonctionnalités de l'hyperviseur ESXi pour la machine virtuelle. Pour plus d'informations sur la compatibilité matérielle et la version ESXi, consultez la documentation VMware.
- Le NetScaler VPX est une appliance virtuelle haute performance sensible à la latence. Pour fournir les performances attendues, le dispositif nécessite la réservation du processeur virtuel, la réservation de la mémoire et l'épinglage du processeur virtuel sur l'hôte. En outre, l'hyper thread doit être désactivé sur l'hôte. Si l'hôte ne répond pas à ces exigences, des problèmes tels que basculement haute disponibilité, pic de processeur dans l'instance VPX, lenteur dans l'accès à l'interface de ligne de commande VPX, plantage du démon pit boss, pertes de paquets et faible débit se produisent.

Un Hypervisor est considéré comme surapprovisionné si l'une des deux conditions suivantes est remplie :

- Le nombre total de cœurs virtuels (vCPU) provisionnés sur l'hôte est supérieur au nombre total de cœurs physiques (PCPU).
- Le nombre total de machines virtuelles provisionnées consomme plus de vCPU que le nombre total de processeurs physiques.

  Si une instance est surapprovisionnée, il se peut que l'hyperviseur ne garantisse pas les ressources réservées (telles que le processeur, la mémoire et autres) pour l'instance en raison des surcharges de planification de l'hyperviseur, des bogues ou des limitations avec

l'hyperviseur. Ce comportement peut entraîner un manque de ressources CPU pour NetScaler et entraîner les problèmes mentionnés au premier point de la section Consignes **d'utilisation**. En tant qu'administrateurs, il est recommandé de réduire la location de l'hôte afin que le nombre total de vCPU provisionnés sur l'hôte soit inférieur ou égal au nombre total de processeurs physiques.

Exemple

Pour l'hyperviseur ESX, si le paramètre `%RDY%` d'un vCPU VPX est supérieur à 0 dans la sortie de la commande `esxtop`, l'hôte ESX est dit avoir des surcharges de planification, ce qui peut entraîner des problèmes de latence pour l'instance VPX.

Dans ce cas, réduisez la location sur l'hôte afin que `%RDY%` revienne toujours à 0. Vous pouvez également contacter le fournisseur de l'hyperviseur pour trier la raison du non-respect de la réservation de ressources effectuée.

- L'ajout à chaud n'est pris en charge que pour les interfaces PV et SRIOV avec NetScaler sur AWS. Les instances VPX avec interfaces ENA ne prennent pas en charge le branchement à chaud, et le comportement des instances peut être imprévisible en cas de tentative de connexion à chaud.
- La suppression à chaud via la console Web AWS ou l'interface CLI AWS n'est pas prise en charge avec les interfaces PV, SRIOV et ENA pour NetScaler. Le comportement des instances peut être imprévisible si la suppression à chaud est tentée.

Commandes pour contrôler l'utilisation du processeur du moteur de paquets

Vous pouvez utiliser deux commandes (`set ns vpxparam` et `show ns vpxparam`) pour contrôler le comportement d'utilisation du processeur du moteur de paquets (hors gestion) des instances VPX dans les environnements d'hyperviseur et de cloud :

- `set ns vpxparam [-cpuyield (YES | NO | DEFAULT)] [-masterclockcpu1 (YES | NO)]`

  Autoriser chaque machine virtuelle à utiliser des ressources CPU qui ont été allouées à une autre machine virtuelle mais qui ne sont pas utilisées.

  Paramètres `Set ns vpxparam` :

  -cpuyield : libère ou ne libère pas des ressources CPU allouées mais inutilisées.

  - **OUI** : autorise l'utilisation des ressources CPU allouées mais inutilisées par une autre machine virtuelle.
  - **NON** : réservez toutes les ressources CPU pour la machine virtuelle à laquelle elles ont été allouées. Cette option affiche un pourcentage plus élevé dans les environnements d'hyperviseur et de cloud pour l'utilisation du processeur VPX.
  - **DEFAULT** : Non.

> **Remarque :**
>
> Sur toutes les plateformes NetScaler VPX, l'utilisation du processeur virtuel sur le système hôte est de 100 %. Tapez la commande `set ns vpxparam -cpuyield YES` pour remplacer cette utilisation.

Si vous souhaitez définir les nœuds du cluster sur « rendement », vous devez effectuer les configurations supplémentaires suivantes sur CCO :

- Si un cluster est formé, tous les nœuds présentent « Yield=Default ».
- Si un cluster est formé à l'aide des nœuds déjà définis sur « Yield=YES », les nœuds sont ajoutés au cluster en utilisant le rendement « DEFAULT ».

> **Remarque :**
>
> Si vous souhaitez définir les nœuds du cluster sur « YIELD=YES », vous pouvez configurer uniquement après la formation du cluster, mais pas avant la formation du cluster.

-masterclockcpu1 : Vous pouvez déplacer la source d'horloge principale de CPU0 (CPU de gestion) vers CPU1. Ce paramètre a les options suivantes :

- **OUI** : Autorisez la machine virtuelle à déplacer la source d'horloge principale de CPU0 vers CPU1.
- **NON** : VM utilise CPU0 pour la source d'horloge principale. Par défaut, CPU0 est la principale source d'horloge.

- `show ns vpxparam`

  Affichez les paramètres `vpxparam` actuels.

Autres références

- Pour les produits Citrix Ready, visitez Citrix Ready Marketplace.
- Pour obtenir le support produit Citrix Ready, consultez la page FAQ.
- Pour les versions matérielles VMware ESX, consultez Mise à niveau de VMware Tools.

Optimisez les performances de NetScaler VPX sur VMware ESX, Linux KVM et Citrix Hypervisors

May 5, 2023

Les performances de NetScaler VPX varient considérablement en fonction de l'hyperviseur, des ressources système allouées et des configurations de l'hôte. Pour atteindre les performances

souhaitées, suivez d'abord les recommandations de la fiche technique VPX, puis optimisez-la davantage en utilisant les meilleures pratiques fournies dans ce document.

Instance NetScaler VPX sur des hyperviseurs VMware ESX

Cette section contient des détails sur les options et les paramètres configurables, ainsi que d'autres suggestions qui vous aideront à optimiser les performances de l'instance NetScaler VPX sur les hyperviseurs VMware ESX.

- Configuration recommandée sur les hôtes ESX
- NetScaler VPX avec interfaces réseau E1000
- NetScaler VPX avec interfaces réseau VMXNET3
- NetScaler VPX avec interfaces réseau relais SR-IOV et PCI

Configuration recommandée sur les hôtes ESX

Pour obtenir des performances élevées pour VPX avec les interfaces réseau E1000, VMXNET3, SR-IOV et PCI passthrough, suivez ces recommandations :

- Le nombre total de processeurs virtuels (vCPU) provisionnés sur l'hôte ESX doit être inférieur ou égal au nombre total de processeurs physiques (PCPU) sur l'hôte ESX.
- L'affinité NUMA (Non-Uniform Memory Access) et l'affinité CPU doivent être définies pour l'hôte ESX pour obtenir de bons résultats.

  — Pour trouver l'affinité NUMA d'une Vmnic, connectez-vous à l'hôte localement ou à distance, et tapez :

  ```
  #vsish -e get /net/pNics/vmnic7/properties | grep NUMA
  Device NUMA Node: 0
  <!--NeedCopy-->
  ```

  - Pour définir l'affinité NUMA et vCPU pour une machine virtuelle, consultez la documentation VMware.

NetScaler VPX avec interfaces réseau E1000

Effectuez les paramètres suivants sur l'hôte VMware ESX :

- Sur l'hôte VMware ESX, créez deux cartes réseau virtuelles à partir d'un commutateur pNIC. Plusieurs vNIC créent plusieurs threads Rx dans l'hôte ESX. Cela augmente le débit Rx de l'interface pNIC.
- Activez les VLAN au niveau du groupe de ports vSwitch pour chaque carte réseau virtuelle que vous avez créée.

- Pour augmenter le débit de transmission vNIC (Tx), utilisez un thread Tx distinct dans l'hôte ESX par vNIC. Utilisez la commande ESX suivante :
  - Pour ESX version 5.5 :

```
esxcli system settings advanced set -o /Net/NetTxWorldlet -i
<!--NeedCopy-->
```

  - Pour ESX version 6.0 et ultérieure :

```
esxcli system settings advanced set -o /Net/NetVMTxType -i 1
<!--NeedCopy-->
```

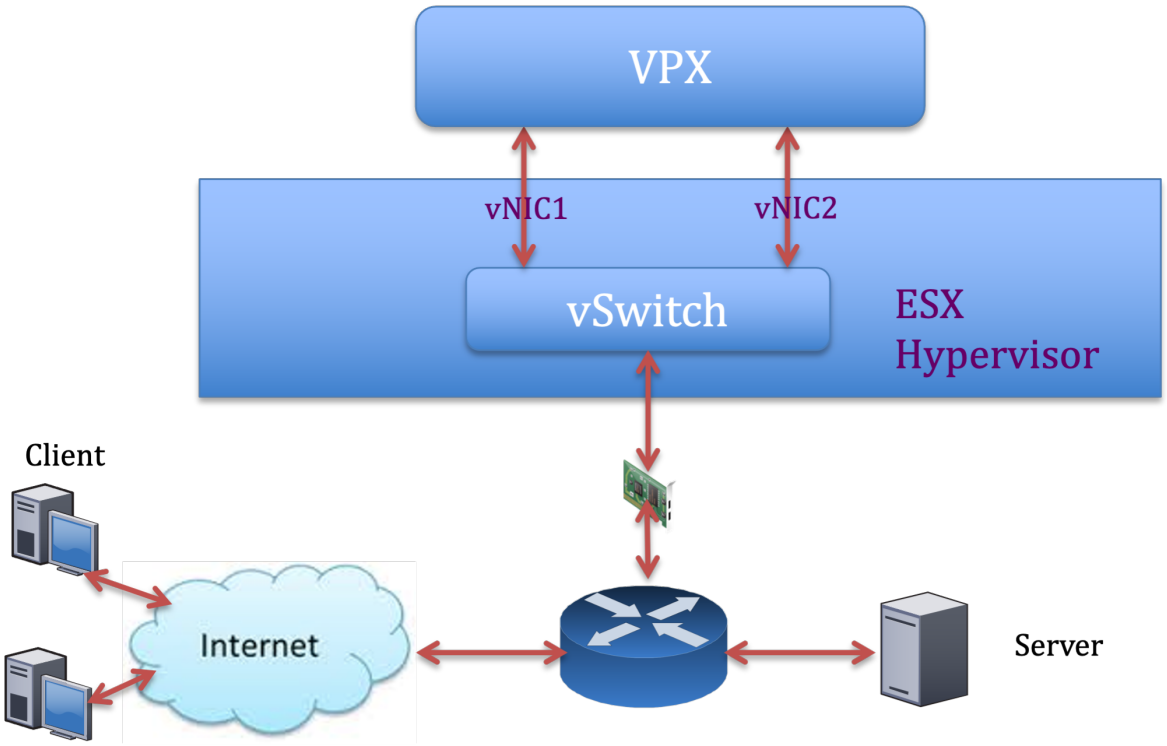
- Pour augmenter encore le débit de la carte réseau vNIC Tx, utilisez un thread d'achèvement Tx et une file d'attente de threads Rx par périphérique (NIC) distincts. Utilisez la commande ESX suivante :

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
<!--NeedCopy-->
```

> Remarque :
>
> Assurez-vous de redémarrer l'hôte VMware ESX pour appliquer les paramètres mis à jour.

Deux cartes réseau virtuelles par déploiement de PNIC

Voici un exemple de commande de topologie et de configuration pour le modèle de déploiement de **deux cartes réseau virtuelles par pNIC** qui offre de meilleures performances réseau.



Exemple de configuration de NetScaler VPX :

Pour réaliser le déploiement illustré dans l'exemple de topologie précédent, effectuez la configuration suivante sur l'instance NetScaler VPX :

- Côté client, liez le SNIP (1.1.1.2) à l'interface réseau 1/1 et activez le mode de balise VLAN.

```
bind vlan 2 -ifnum 1/1 - tagged
bind vlan 2 -IPAddress 1.1.1.2 255.255.255.0
<!--NeedCopy-->
```

- Côté serveur, liez le SNIP (2.2.2.2) à l'interface réseau 1/1 et activez le mode de balise VLAN.

```
bind vlan 3 -ifnum 1/2 - tagged
bind vlan 3 -IPAddress 2.2.2.2 255.255.255.0
<!--NeedCopy-->
```

- Ajoutez un serveur virtuel HTTP (1.1.1.100) et liez-le à un service (2.2.2.100).

```
add lb vserver v1 HTTP 1.1.1.100 80 -persistenceType NONE -
    Listenpolicy None -cltTimeout 180
add service s1 2.2.2.100 HTTP 80 -gslb NONE -maxClient 0 -maxReq
    0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
    180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
bind lb vserver v1 s1
<!--NeedCopy-->
```


> Remarque :
>
> Assurez-vous d'inclure les deux entrées suivantes dans la table de routage :
>
> - Sous-réseau 1.1.1.0/24 avec passerelle pointant vers SNIP 1.1.1.2
> - Sous-réseau 2.2.2.0/24 avec passerelle pointant vers SNIP 2.2.2.2

NetScaler VPX avec interfaces réseau VMXNET3

Pour obtenir des performances élevées pour VPX avec les interfaces réseau VMXNET3, effectuez les paramètres suivants sur l'hôte VMware ESX :

- Créez deux vNIC à partir d'un commutateur virtuel PNIC. Plusieurs vNIC créent plusieurs threads Rx dans l'hôte ESX. Cela augmente le débit Rx de l'interface pNIC.
- Activez les VLAN au niveau du groupe de ports vSwitch pour chaque carte réseau virtuelle que vous avez créée.
- Pour augmenter le débit de transmission vNIC (Tx), utilisez un thread Tx distinct dans l'hôte ESX par vNIC. Utilisez les commandes ESX suivantes :
  - Pour ESX version 5.5 :

```
1  esxcli system settings advanced set  -o /Net/NetTxWorldlet  -i
2  <!--NeedCopy-->
```

  - Pour ESX version 6.0 et ultérieure :

```
1   esxcli system settings advanced set -o /Net/NetVMTxType  -i 1
2   <!--NeedCopy-->
```

Sur l'hôte VMware ESX, effectuez la configuration suivante :

- Sur l'hôte VMware ESX, créez deux cartes réseau virtuelles à partir d'un vSwitch PNIC. Plusieurs vNIC créent plusieurs threads Tx et Rx dans l'hôte ESX. Cela augmente le débit Tx et Rx de l'interface pNIC.
- Activez les VLAN au niveau du groupe de ports vSwitch pour chaque carte réseau virtuelle que vous avez créée.
- Pour augmenter le débit Tx d'une vNIC, utilisez un thread d'achèvement Tx et une file d'attente de threads Rx par périphérique (NIC) distincts. Utilisez la commande suivante :

```
1  esxcli system settings advanced set -o /Net/
      NetNetqRxQueueFeatPairEnable -i 0
2  <!--NeedCopy-->
```

- Configurez une machine virtuelle pour qu'elle utilise un thread de transmission par vNIC, en ajoutant le paramètre suivant à la configuration de la machine virtuelle :


```
ethernetX.ctxPerDev = "1"
<!--NeedCopy-->
```

Pour plus d'informations, consultez la section Meilleures pratiques pour le réglage des performances des charges de travail Telco et NFV
dans vSphere

> Remarque :
>
> Assurez-vous de redémarrer l'hôte VMware ESX pour appliquer les paramètres mis à jour.

Vous pouvez configurer VMXNET3 en tant que **deux cartes réseau virtuelles par déploiement PNIC** . Pour plus d'informations, consultez la section Deux cartes réseau virtuelles par déploiement de pNIC.

NetScaler VPX avec interfaces réseau relais SR-IOV et PCI

Pour obtenir des performances élevées pour VPX avec des interfaces réseau SR-IOV et PCI passthrough, reportez-vous à la section Configuration recommandée sur les hôtes ESX.

Instance NetScaler VPX sur la plateforme Linux-KVM

Cette section contient des détails sur les options et paramètres configurables, ainsi que d'autres suggestions qui vous aideront à optimiser les performances de l'instance NetScaler VPX sur la plate-forme Linux-KVM.

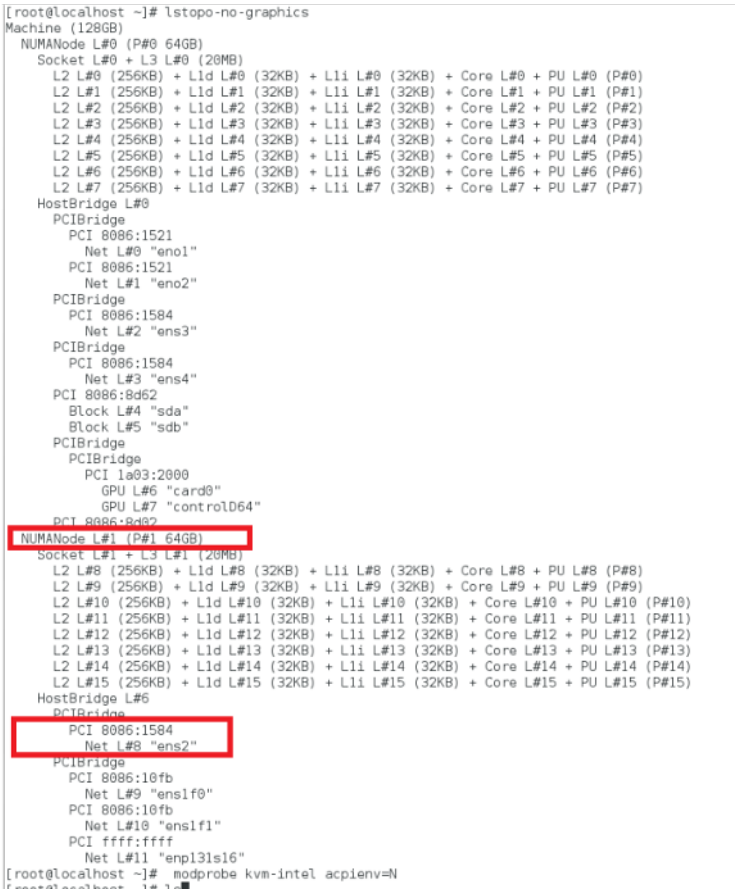
- Paramètres de performance pour KVM
- NetScaler VPX avec interfaces réseau photovoltaïque
- NetScaler VPX avec interfaces réseau relais SR-IOV et Fortville PCIe

Paramètres de performance pour KVM

Effectuez les paramètres suivants sur l'hôte KVM :

Recherchez le domaine NUMA de la carte réseau à l'aide de la `lstopo` commande :

Assurez-vous que la mémoire du VPX et du processeur est épinglée au même emplacement.
Dans la sortie suivante, la carte réseau 10G « ens2" est liée au domaine NUMA #1.



Allouez la mémoire VPX du domaine NUMA.

La `numactl` commande indique le domaine NUMA à partir duquel la mémoire est allouée. Dans la sortie suivante, environ 10 Go de RAM sont alloués à partir du nœud NUMA #0.

```
[root@localhost ~]# numactl --hardware
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 6 7
node 0 size: 65429 MB
node 0 free: 55854 MB
node 1 cpus: 8 9 10 11 12 13 14 15
node 1 size: 65536 MB
node 1 free: 52388 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
[root@localhost ~]#
```

Pour modifier le mappage des nœuds NUMA, procédez comme suit.

1. Modifiez le .xml du VPX sur l'hôte.

```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```


2. Ajoutez la balise suivante :

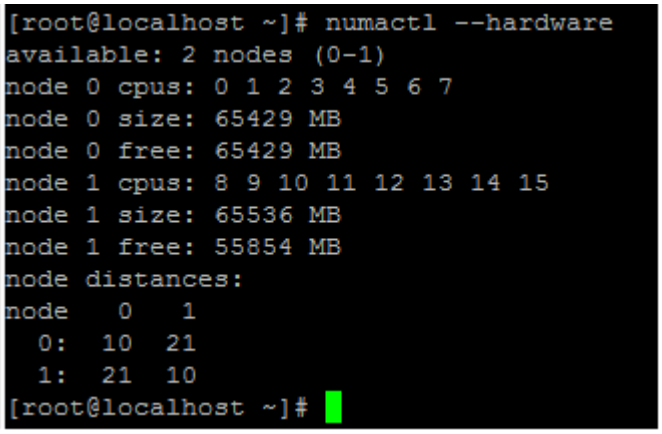
```
<numatune>
<memory mode="strict" nodeset="1"/>    This is the NUMA domain
   name
</numatune>
<!--NeedCopy-->
```

3. Arrêtez le VPX.
4. Exécutez la commande suivante :

```
virsh define /etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

   Cette commande met à jour les informations de configuration de la machine virtuelle avec les mappages de nœuds NUMA.

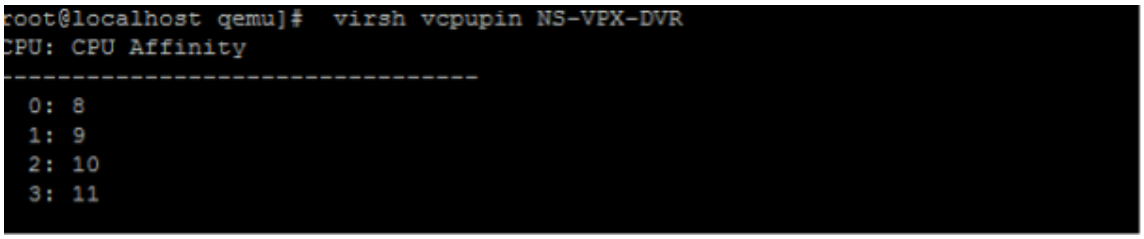
5. Mettez le VPX sous tension. Vérifiez ensuite la sortie de la `numactl -hardware` commande sur l'hôte pour voir les allocations de mémoire mises à jour pour le VPX.



Épinglez les vCPU de VPX aux cœurs physiques.

- Pour afficher les mappages vCPU vers PCPU d'un VPX, tapez la commande suivante

```
virsh vcpupin <VPX name>
<!--NeedCopy-->
```



Les vCPU 0—4 sont mappés sur les cœurs physiques 8 à 11.

- Pour afficher l'utilisation actuelle du PCPU, tapez la commande suivante :

```
mpstat -P ALL 5
<!--NeedCopy-->
```

```
[root@localhost qemu]# mpstat -P ALL 5
Linux 3.10.0-123.el7.x86_64 (localhost.localdomain)     05/17/2016      _x86_64_        (16 CPU)

02:26:20 PM  CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
02:26:25 PM  all    0.24    0.00    1.67    0.00    0.00    0.00    0.00   17.32    0.00   80.78
02:26:25 PM    0    0.20    0.00    1.00    0.00    0.00    0.00    0.00    0.00    0.00   98.80
02:26:25 PM    1    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    2    0.20    0.00    0.40    0.00    0.00    0.00    0.00    0.00    0.00   99.40
02:26:25 PM    3    0.00    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.80
02:26:25 PM    4    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    5    0.60    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.20
02:26:25 PM    6    0.40    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    7    1.62    0.00    1.42    0.00    0.00    0.00    0.00    0.00    0.00   96.96
02:26:25 PM    8    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM    9    0.00    0.00    7.60    0.00    0.00    0.00    0.00   92.40    0.00    0.00
02:26:25 PM   10    0.20    0.00    7.00    0.00    0.00    0.00    0.00   92.80    0.00    0.00
02:26:25 PM   11    0.00    0.00    8.60    0.00    0.00    0.00    0.00   91.40    0.00    0.00
02:26:25 PM   12    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   13    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   14    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   15    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
```

Dans cette sortie, 8 correspond au processeur de gestion et 9 à 11 aux moteurs de paquets.

- Pour changer le vCPU en épinglage PCPU, il existe deux options.
  - Modifiez-le au moment de l'exécution après le démarrage du VPX à l'aide de la commande suivante :

```
virsh vcpupin <VPX name> <vCPU id>  <pCPU number>
virsh vcpupin NetScaler-VPX-XML 0 8
virsh vcpupin NetScaler-VPX-XML 1 9
virsh vcpupin NetScaler-VPX-XML 2 10
virsh vcpupin NetScaler-VPX-XML 3 11
<!--NeedCopy-->
```

  - Pour apporter des modifications statiques au VPX, modifiez le `.xml` fichier comme précédemment avec les balises suivantes :

    1. Modifiez le fichier .xml du VPX sur l'hôte

```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

    2. Ajoutez la balise suivante :

```
<vcpu placement='static' cpuset='8-11'>4</vcpu>
    <cputune>
```



```
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>
<!--NeedCopy-->
```

3. Arrêtez le VPX.
4. Mettez à jour les informations de configuration de la machine virtuelle avec les mappages de nœuds NUMA à l'aide de la commande suivante :

```
virsh define /etc/libvirt/qemu/ <VPX_name>.xml
<!--NeedCopy-->
```

5. Mettez le VPX sous tension. Vérifiez ensuite la sortie de la `virsh vcpupin <VPX name>` commande sur l'hôte pour voir l'épinglage du processeur mis à jour.

Éliminez les frais généraux d'interruption de l'hôte.

- Détectez VM_EXITS à l'aide de la `kvm_stat` commande.

  Au niveau de l'hyperviseur, les interruptions de l'hôte sont mappées sur les mêmes processeurs sur lesquels les vCPU du VPX sont épinglés. Cela peut entraîner le retrait périodique des processeurs virtuels sur le VPX.

  Pour trouver les sorties de machine virtuelle effectuées par les machines virtuelles exécutant l'hôte, utilisez la `kvm_stat` commande.

```
[root@localhost ~]# kvm_stat -1  | grep EXTERNAL
kvm_exit(EXTERNAL_INTERRUPT)  1728349 27738
[root@localhost ~]#
<!--NeedCopy-->
```

  Une valeur supérieure de l'ordre de 1+M indique un problème.

  Si une seule machine virtuelle est présente, la valeur attendue est comprise entre 30 et 100 K. Tout ce qui dépasse peut indiquer qu'un ou plusieurs vecteurs d'interruption d'hôte sont mappés sur le même processeur.

- Détectez les interruptions de l'hôte et migrez les interruptions de l'hôte.

  Lorsque vous exécutez la `concatenate` commande pour le fichier « /proc/interrupts », elle affiche tous les mappages d'interruption de l'hôte. Si un ou plusieurs IRQ actifs sont mappés sur le même PCPU, le compteur correspondant est incrémenté.

  Déplacez toutes les interruptions qui se chevauchent avec les processeurs de votre NetScaler VPX vers les processeurs non utilisés :


```
echo 0000000f > /proc/irq/55/smp_affinity
0000000f - - > it is a bitmap, LSBs indicates that IRQ 55 can
   only be scheduled on pCPUs 0 - 3
<!--NeedCopy-->
```

- Désactivez la balance IRQ.

  Désactivez le démon d'équilibrage de l'IRQ, de sorte qu'aucune replanification ne se produise à la volée.

```
service irqbalance stop
service irqbalance show - To check the status
service irqbalance start - Enable if needed
<!--NeedCopy-->
```

  Assurez-vous d'exécuter la commande `kvm_stat` pour vous assurer qu'il n'y a pas beaucoup de compteurs.

NetScaler VPX avec interfaces réseau photovoltaïque

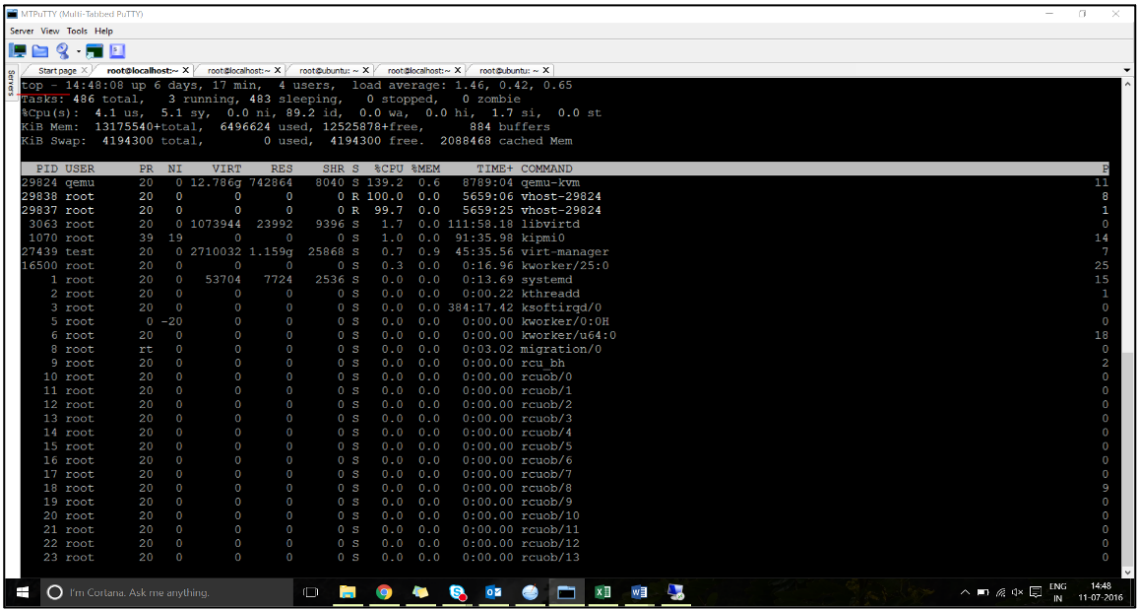
Vous pouvez configurer des interfaces réseau de para-virtualisation (PV), SR-IOV et PCIe passthrough en tant que déploiement de **deux cartes réseau virtuelles par pNIC** . Pour plus d'informations, consultez la section Deux cartes réseau virtuelles par déploiement de pNIC.

Pour des performances optimales des interfaces PV (virtio), procédez comme suit :

- Identifiez le domaine NUMA auquel le slot/carte d'interface réseau PCIe est lié.
- La mémoire et le processeur virtuel du VPX doivent être épinglés au même domaine NUMA.
- Le thread Vhost doit être lié aux processeurs du même domaine NUMA.

Liez les threads de l'hôte virtuel aux processeurs correspondants :

1. Une fois le trafic démarré, exécutez la `top` commande sur l'hôte.



2. Identifiez l'affinité du processus hôte virtuel (nommé sous le nom `vhost-<pid-of-qemu>`).
3. Liez les processus vHost aux cœurs physiques du domaine NUMA identifié précédemment à l'aide de la commande suivante :

```
taskset -pc <core-id> <process-id>
<!--NeedCopy-->
```

Exemple :

```
taskset -pc 12 29838
<!--NeedCopy-->
```

4. Les cœurs de processeur correspondant au domaine NUMA peuvent être identifiés à l'aide de la commande suivante :

```
[root@localhost ~]# virsh capabilities | grep cpu
<cpu>
    </cpu>
        <cpus num='8'>
            <cpu id='0' socket_id='0' core_id='0' siblings='0'/>
            <cpu id='1' socket_id='0' core_id='1' siblings='1'/>
            <cpu id='2' socket_id='0' core_id='2' siblings='2'/>
            <cpu id='3' socket_id='0' core_id='3' siblings='3'/>
            <cpu id='4' socket_id='0' core_id='4' siblings='4'/>
            <cpu id='5' socket_id='0' core_id='5' siblings='5'/>
            <cpu id='6' socket_id='0' core_id='6' siblings='6'/>
            <cpu id='7' socket_id='0' core_id='7' siblings='7'/>
        </cpus>
```



```
14
15          <cpus num='8'>
16          <cpu id='8' socket_id='1' core_id='0' siblings='8'/>
17          <cpu id='9' socket_id='1' core_id='1' siblings='9'/>
18          <cpu id='10' socket_id='1' core_id='2' siblings='10'/>
19          <cpu id='11' socket_id='1' core_id='3' siblings='11'/>
20          <cpu id='12' socket_id='1' core_id='4' siblings='12'/>
21          <cpu id='13' socket_id='1' core_id='5' siblings='13'/>
22          <cpu id='14' socket_id='1' core_id='6' siblings='14'/>
23          <cpu id='15' socket_id='1' core_id='7' siblings='15'/>
24          </cpus>
25
26      <cpuselection/>
27      <cpuselection/>
28
29  <!--NeedCopy-->
```

Liez le processus QEMU au cœur physique correspondant :

1. Identifiez les cœurs physiques sur lesquels le processus QEMU est exécuté. Pour plus d'informations, reportez-vous à la sortie précédente.
2. Liez le processus QEMU aux mêmes cœurs physiques auxquels vous liez les vCPU, à l'aide de la commande suivante :

```
1  taskset -pc 8-11 29824
2  <!--NeedCopy-->
```

NetScaler VPX avec interfaces réseau relais SR-IOV et Fortville PCIe

Pour des performances optimales des interfaces réseau relais SR-IOV et Fortville PCIe, procédez comme suit :

- Identifiez le domaine NUMA auquel le slot/carte d'interface réseau PCIe est lié.
- La mémoire et le processeur virtuel du VPX doivent être épinglés au même domaine NUMA.

Exemple de fichier XML VPX pour vCPU et épinglage de mémoire pour Linux KVM :

```
1      <domain type='kvm'>
2          <name>NetScaler-VPX</name>
3          <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>
4          <memory unit='KiB'>8097152</memory>
5          <currentMemory unit='KiB'>8097152</currentMemory>
6          <vcpu placement='static'>4</vcpu>
7
```



```
    <cputune>
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>

    <numatune>
    <memory mode='strict' nodeset='1'/>
    </numatune>

    </domain>
<!--NeedCopy-->
```

Instance NetScaler VPX sur Citrix Hypervisors

Cette section contient des détails sur les options et paramètres configurables, ainsi que d'autres suggestions qui vous aident à optimiser les performances de l'instance NetScaler VPX sur les hyperviseurs Citrix.

- Paramètres de performance pour Citrix Hypervisors
- NetScaler VPX avec interfaces réseau SR-IOV
- NetScaler VPX avec interfaces para-virtualisées

Paramètres de performance pour Citrix Hypervisors

Recherchez le domaine NUMA de la carte réseau à l'aide de la commande « xl » :

```
xl info -n
<!--NeedCopy-->
```

Épinglez les vCPU de VPX aux cœurs physiques.

```
xl vcpu-pin <Netsclaer VM Name>  <vCPU id>  <physical CPU id>
<!--NeedCopy-->
```

Vérifiez la liaison des vCPU.

```
xl vcpu-list
<!--NeedCopy-->
```

Allouez plus de 8 processeurs virtuels aux machines virtuelles NetScaler.

Pour configurer plus de 8 processeurs virtuels, exécutez les commandes suivantes à partir de la console Citrix Hypervisor :


```
xe vm-param-set uuid=your_vms_uuid VCPUs-max=16
xe vm-param-set uuid=your_vms_uuid VCPUs-at-startup=16
<!--NeedCopy-->
```

NetScaler VPX avec interfaces réseau SR-IOV

Pour des performances optimales des interfaces réseau SR-IOV, procédez comme suit :

- Identifiez le domaine NUMA auquel l'emplacement PCIe ou la carte réseau est lié.
- Épinglez la mémoire et le processeur virtuel du VPX au même domaine NUMA.
- Liez le vCPU Domain-0 au processeur restant.

NetScaler VPX avec interfaces para-virtualisées

Pour des performances optimales, deux cartes réseau virtuelles par PNIC et une configuration vNIC par pNIC sont recommandées, comme dans d'autres environnements PV.

Pour obtenir des performances optimales des interfaces para-virtualisées (netfront), procédez comme suit :

- Identifiez le domaine NUMA auquel l'emplacement PCIe ou la carte réseau est lié.
- Épinglez la mémoire et le processeur virtuel du VPX au même domaine NUMA.
- Liez le vCPU Domain-0 au processeur restant du même domaine NUMA.
- Épinglez les threads Rx/Tx hôtes de vNIC aux vCPU du domaine 0.

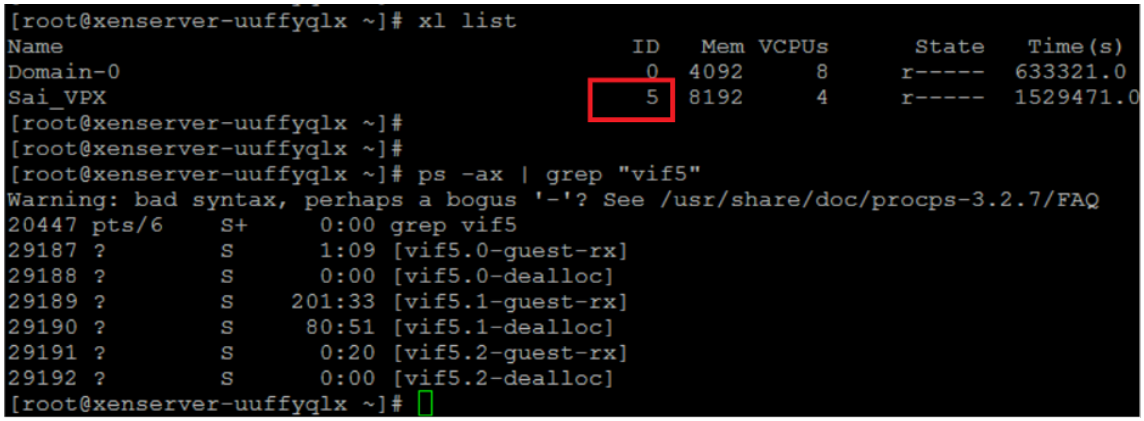
Épinglez les threads hôtes aux vCPU Domain-0 :

1. Recherchez l'ID Xen du VPX à l'aide de la `xl list` commande sur le shell hôte Citrix Hypervisor.
2. Identifiez les threads hôtes à l'aide de la commande suivante :

   ```
   ps -ax | grep vif <Xen-ID>
   <!--NeedCopy-->
   ```

   Dans l'exemple suivant, ces valeurs indiquent :

   - **vif5.0** - Les threads de la première interface allouée à VPX dans XenCenter (interface de gestion).
   - **vif5.1** - Les threads de la deuxième interface affectée à VPX et ainsi de suite.



3. Épinglez les threads aux vCPU du domaine 0 à l'aide de la commande suivante :

```
taskset  - pc <core-id> <process-id>
<!--NeedCopy-->
```

Exemple :

```
taskset -pc 1 29189
<!--NeedCopy-->
```

Appliquez les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler dans le cloud

June 20, 2023

Vous pouvez appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler dans un environnement cloud. Cette étape est abordée comme étape de **pré-démarrage** dans ce document. Par conséquent, dans certains cas, comme les licences groupées ADC, une instance VPX spécifique est mise en place en beaucoup moins de temps. Cette fonctionnalité est disponible dans Microsoft Azure, Google Cloud Platform et AWS Clouds.

Qu'est-ce que les données utilisateur

Lorsque vous provisionnez une instance VPX dans un environnement cloud, vous avez la possibilité de transmettre des données utilisateur à l'instance. Les données utilisateur vous permettent d'effectuer des tâches de configuration automatisées courantes, de personnaliser les comportements de démarrage des instances et d'exécuter des scripts après le démarrage de l'instance. Au premier démarrage, l'instance NetScaler VPX exécute les tâches suivantes :

- Lit les données utilisateur.

- Interprète la configuration fournie dans les données utilisateur.
- Applique la configuration nouvellement ajoutée au démarrage.

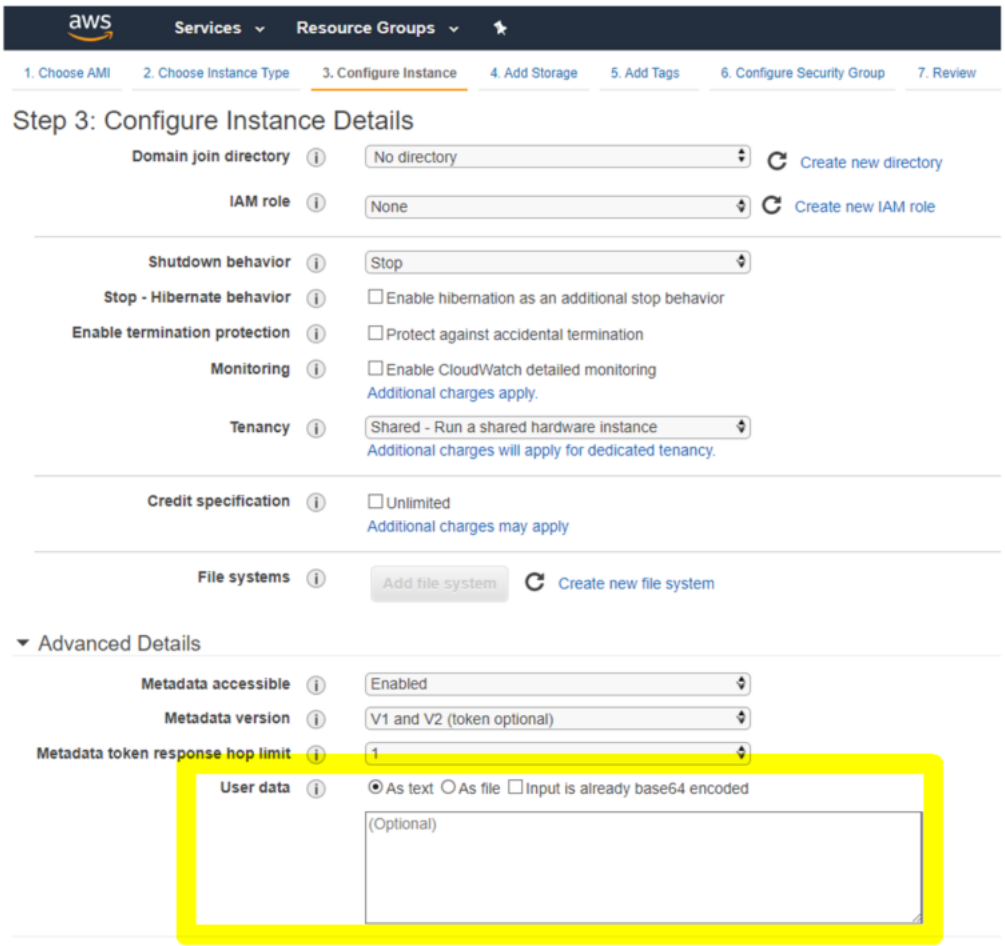
Comment fournir des données utilisateur de pré-démarrage dans une instance cloud

Vous pouvez fournir des données utilisateur de pré-démarrage à l'instance cloud au format XML. Différents clouds ont des interfaces différentes pour fournir des données utilisateur.

Fournir des données utilisateur de pré-démarrage à l'aide de la console AWS

Lorsque vous provisionnez une instance NetScaler VPX à l'aide de la console AWS, accédez à Configurer les détails de l'instance > Détails avancés, puis**fournissez la configuration des données utilisateur avant le démarrage dans le champ Données utilisateur.**

Pour obtenir des instructions détaillées sur chacune des étapes, voir Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS.
Pour plus d'informations, consultez la documentation AWS sur le lancement d'une instance.



> **Remarque :**
>
> Le mode AWS IMDSv2 uniquement pour la fonctionnalité de données utilisateur avant le démarrage est pris en charge à partir de NetScaler VPX version 13.1.48.x et versions ultérieures.

Fournir des données utilisateur de pré-démarrage à l'aide de l'AWS CLI

Saisissez la commande suivante dans l'interface de ligne de commande AWS :

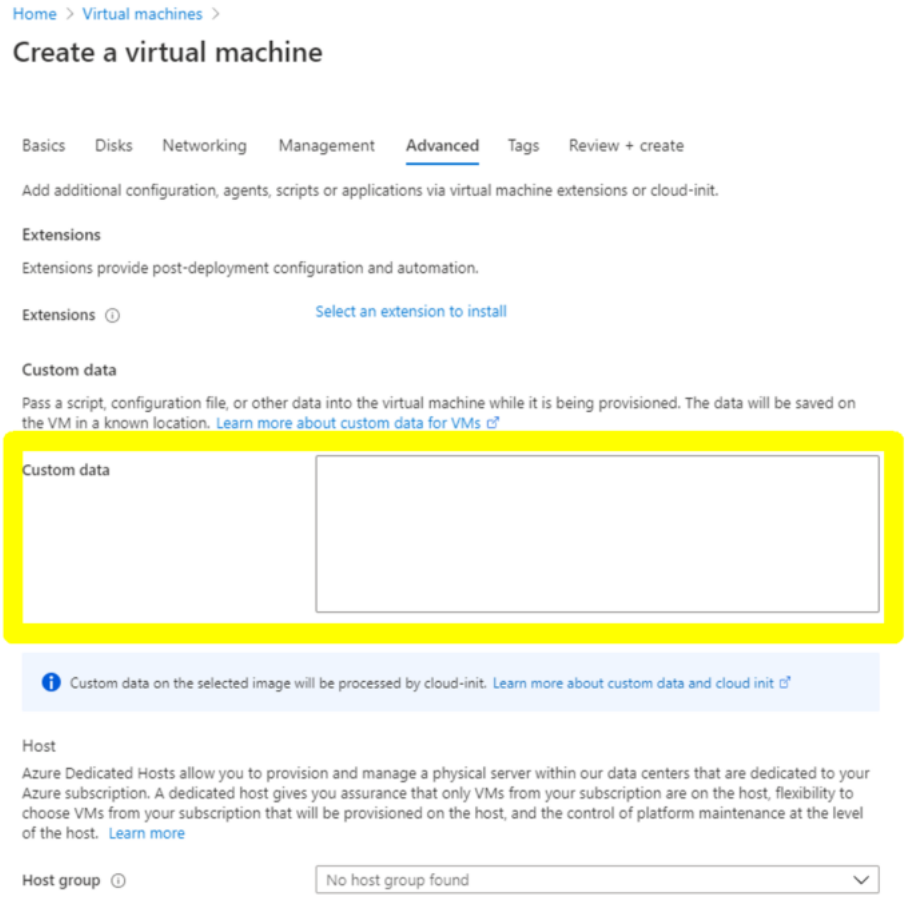
```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --user-data file://my_script.txt
<!--NeedCopy-->
```

Pour plus d'informations, consultez la documentation AWS sur les instances en cours d'exécution.

Pour plus d'informations, consultez la documentation AWS sur l'utilisation des données utilisateur d'instance.

Fournir des données utilisateur de pré-démarrage à l'aide de la console Azure

Lorsque vous provisionnez une instance NetScaler VPX à l'aide de la console Azure, accédez à l'onglet **Créer une machine virtuelle > Avancé** . Dans le champ **Données personnalisées**, indiquez la configuration des données utilisateur avant le démarrage.



Fournir des données utilisateur de pré-démarrage à l'aide de l'interface de ligne de commande Azure

Saisissez la commande suivante dans l'interface de ligne de commande Azure :

```
az vm create \
  --resource-group myResourceGroup \
  --name MyVm \
  --image debian \
  --custom-data MyCloudInitScript.txt \
<!--NeedCopy-->
```

Exemple :

```
az vm create --resource-group MyResourceGroup -name MyVm --image debian
    --custom-data MyCloudInitScript.txt
<!--NeedCopy-->
```

Vous pouvez transmettre vos données personnalisées ou votre configuration de pré-démarrage sous

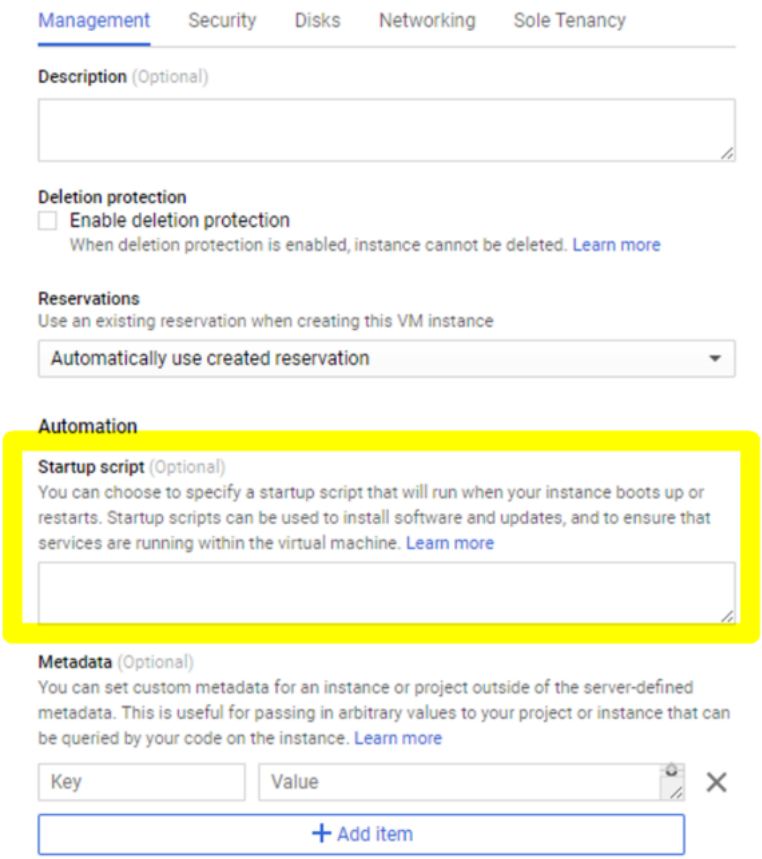
forme de fichier au paramètre « —custom-data ». Dans cet exemple, le nom de fichier est **MyCloudInitScript.txt**.

Pour plus d'informations, consultez la documentation Azure CLI.

Fournir des données utilisateur de pré-démarrage à l'aide de la console GCP

Lorsque vous provisionnez une instance NetScaler VPX à l'aide de la console GCP, renseignez les propriétés de l'instance. Développez **la gestion, la sécurité, les disques, la mise en réseau et la location exclusive**. Accédez à l'onglet **Gestion** . Dans la section **Automation**, indiquez la configuration des données utilisateur de **pré-démarrage dans le champ Script** de démarrage.

Pour des informations détaillées sur la création de l'instance VPX à l'aide de GCP, voir Déployer une instance NetScaler VPXsur Google Cloud Platform.



Fournir des données utilisateur de pré-démarrage à l'aide de l'interface de ligne de commande g

Saisissez la commande suivante dans l'interface de ligne de commande GCP :


```
gcloud compute instances create INSTANCE_NAMES --metadata-from-file=
    startup-script=LOCAL_FILE_PATH
<!--NeedCopy-->
```

metadata-from-file - Lit la valeur ou les données utilisateur à partir d'un fichier stocké dans le .

Pour plus d'informations, consultez la documentation de l'interface de ligne de commande gcloud

Format de données utilisateur de prédémarrage

Les données utilisateur de pré-démarrage doivent être fournies à l'instance cloud au format XML. Les données utilisateur de NetScaler avant le démarrage que vous fournissez via l'infrastructure cloud lors du démarrage peuvent comprendre les quatre sections suivantes :

- Configuration de NetScaler représentée par la balise. <NS-CONFIG>
- Démarrage personnalisé du NetScaler représenté par la balise <NS-BOOTSTRAP>.
- Stockage des scripts utilisateur dans NetScaler représentés par la balise. <NS-SCRIPTS>
- Configuration des licences regroupées représentée par la <NS-LICENSE-CONFIG> balise.

Vous pouvez fournir les quatre sections précédentes dans n'importe quel ordre dans la configuration de prédémarrage ADC.
Assurez-vous de suivre strictement la mise en forme affichée dans les sections suivantes tout en fournissant les données utilisateur de pré-démarrage.

> Remarque :
>
> La configuration complète des données utilisateur de pré-démarrage doit être incluse dans la <NS-PRE-BOOT-CONFIG> balise, comme illustré dans les exemples suivants.

Exemple 1 :

```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>          </NS-CONFIG>
     <NS-BOOTSTRAP>       </NS-BOOTSTRAP>
     <NS-SCRIPTS>         </NS-SCRIPTS>
     <NS-LICENSE-CONFIG>  </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Exemple 2 :

```
<NS-PRE-BOOT-CONFIG>
    <NS-LICENSE-CONFIG> </NS-LICENSE-CONFIG>
    <NS-SCRIPTS>        </NS-SCRIPTS>
    <NS-BOOTSTRAP>      </NS-BOOTSTRAP>
```



```
5      <NS-CONFIG>          </NS-CONFIG>
6  </NS-PRE-BOOT-CONFIG>
7  <!--NeedCopy-->
```

Utilisez la <NS-CONFIG> balise pour fournir les configurations NetScaler VPX spécifiques qui doivent être appliquées à l'instance VPX au stade de pré-démarrage.

> REMARQUE :
>
> La <NS-CONFIG> section doit comporter des commandes ADC CLI valides. Les CLI ne sont pas vérifiés pour les erreurs syntaxiques ou le format.

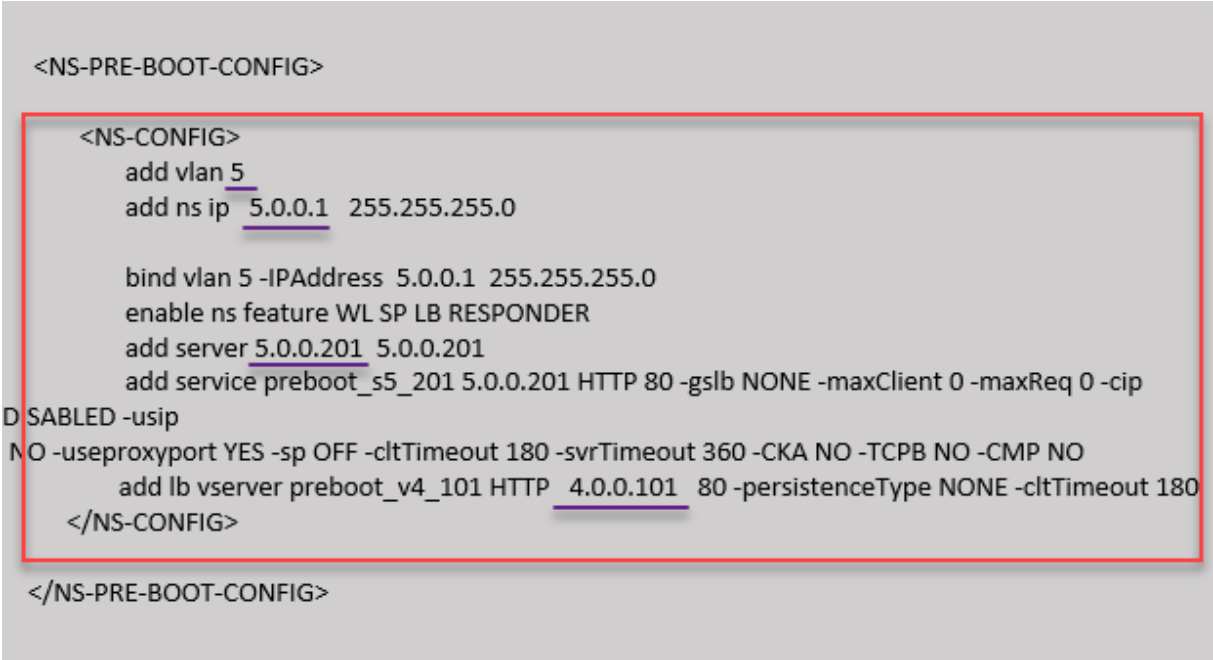
Configurations NetScaler

Utilisez la <NS-CONFIG> balise pour fournir les configurations NetScaler VPX spécifiques qui doivent être appliquées à l'instance VPX au stade de pré-démarrage.

> REMARQUE :
>
> La <NS-CONFIG> section doit comporter des commandes ADC CLI valides. Les CLI ne sont pas vérifiés pour les erreurs syntaxiques ou le format.

Exemple :

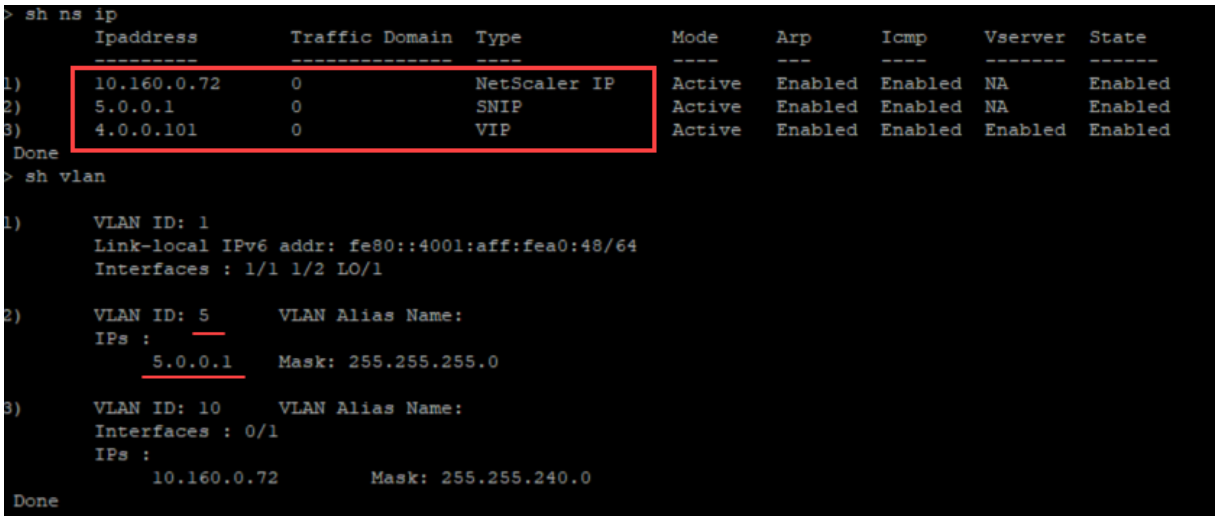
Dans l'exemple suivant, la <NS-CONFIG> section contient les détails des configurations. Un VLAN de l'ID « 5 » est configuré et lié au SNIP (5.0.0.1). Un serveur virtuel d'équilibrage de charge (4.0.0.101) est également configuré.

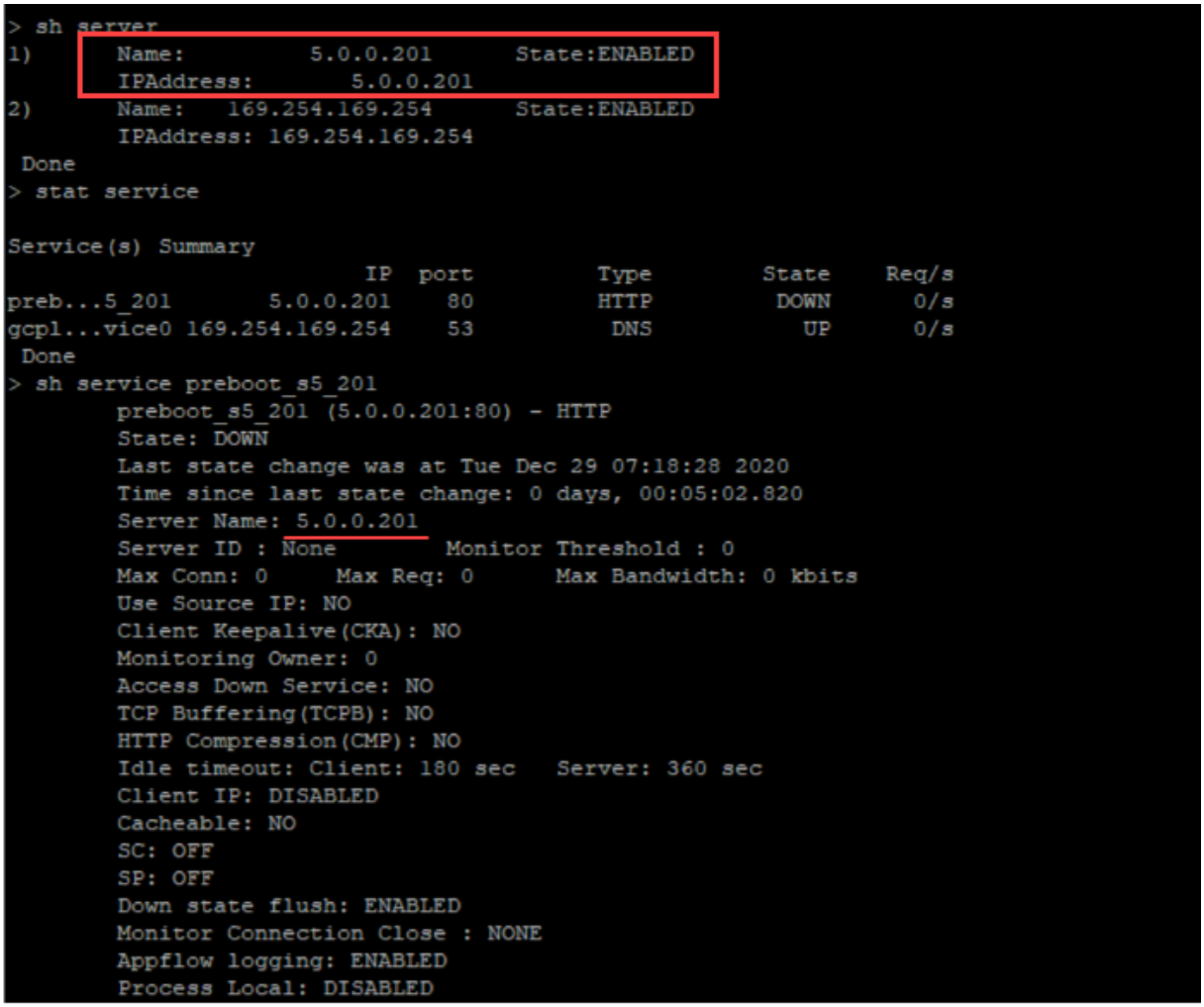


Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :


```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>
         add vlan 5
         add ns ip 5.0.0.1 255.255.255.0
         bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
         enable ns feature WL SP LB RESPONDER
         add server 5.0.0.201 5.0.0.201
         add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip
 NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -
    TCPB NO -CMP NO
         add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180
     </NS-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

L'instance NetScaler VPX propose la configuration appliquée dans la <NS-CONFIG> section, comme indiqué dans les illustrations suivantes.





Scripts utilisateur

Utilisez la <NS-SCRIPTS> balise pour fournir tout script qui doit être stocké et exécuté dans l'instance NetScaler VPX.

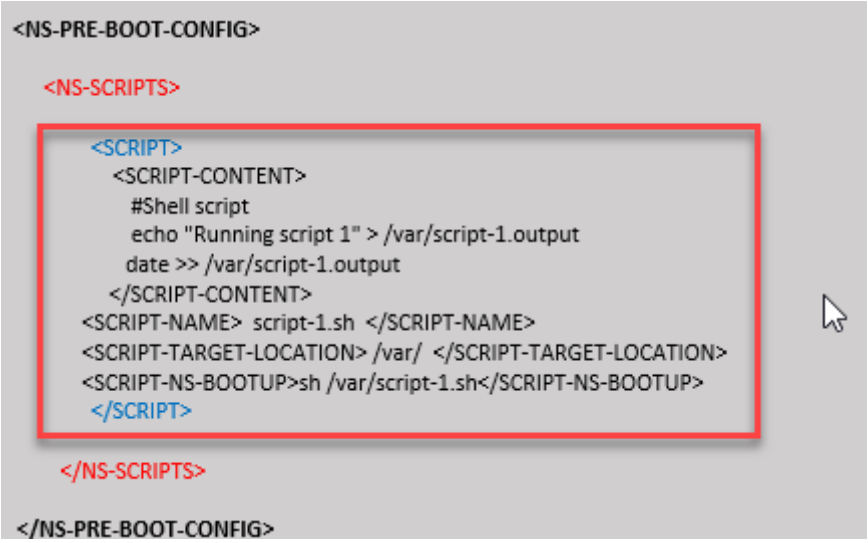
Vous pouvez inclure de nombreux scripts dans la <NS-SCRIPTS> balise. Chaque script doit être inclus dans la <SCRIPT> balise.
Chaque <SCRIPT> section correspond à un script et contient tous les détails du script à l'aide des sous-balises suivantes.

- **<SCRIPT-NAME>:** Indique le nom du fichier de script qui doit être stocké.
- **<SCRIPT-CONTENT>:** Indique le contenu du fichier qui doit être stocké.
- **<SCRIPT-TARGET-LOCATION>:** Indique l'emplacement cible désigné où ce fichier doit être stocké. Si l'emplacement cible n'est pas fourni, le fichier ou le script est enregistré par défaut dans le répertoire « /nsconfig ».
- **<SCRIPT-NS-BOOTUP>:** Spécifiez les commandes que vous utilisez pour exécuter le script.

- Si vous utilisez la section <SCRIPT-NS-BOOTUP>, les commandes fournies dans la section sont stockées dans “/nsconfig/nsafter.sh”, et les commandes sont exécutées après le démarrage du moteur de paquets dans le cadre de l’exécution de “nsafter.sh”.
- Si vous n’utilisez pas la section <SCRIPT-NS-BOOTUP>, le fichier de script est stocké à l’emplacement cible que vous spécifiez.

Exemple 1 :

Dans cet exemple, la balise <NS-SCRIPTS> contient des détails sur un seul script : script-1.sh. Le script “script-1.sh” est enregistré dans le répertoire « /var ». Le script est rempli avec le contenu spécifié et est exécuté avec la commande « sh /var/script-1.sh » après le démarrage du moteur de paquets.



Vous pouvez copier la configuration affichée dans la capture d’écran précédente à partir d’ici :

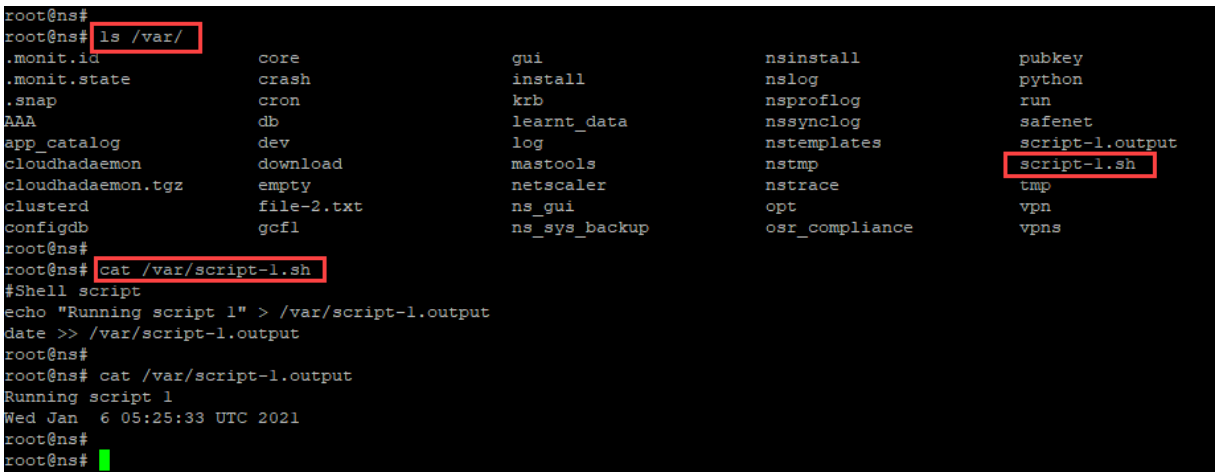
```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
    <SCRIPT>
            <SCRIPT-CONTENT>
                #Shell script
                echo "Running script 1" > /var/script-1.output
                date >> /var/script-1.output
            </SCRIPT-CONTENT>

                <SCRIPT-NAME> script-1.sh </SCRIPT-NAME>
                <SCRIPT-TARGET-LOCATION> /var/ </SCRIPT-TARGET-LOCATION
                    >
                <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP
                    >
        </SCRIPT>
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
```



```
16 <!--NeedCopy-->
```

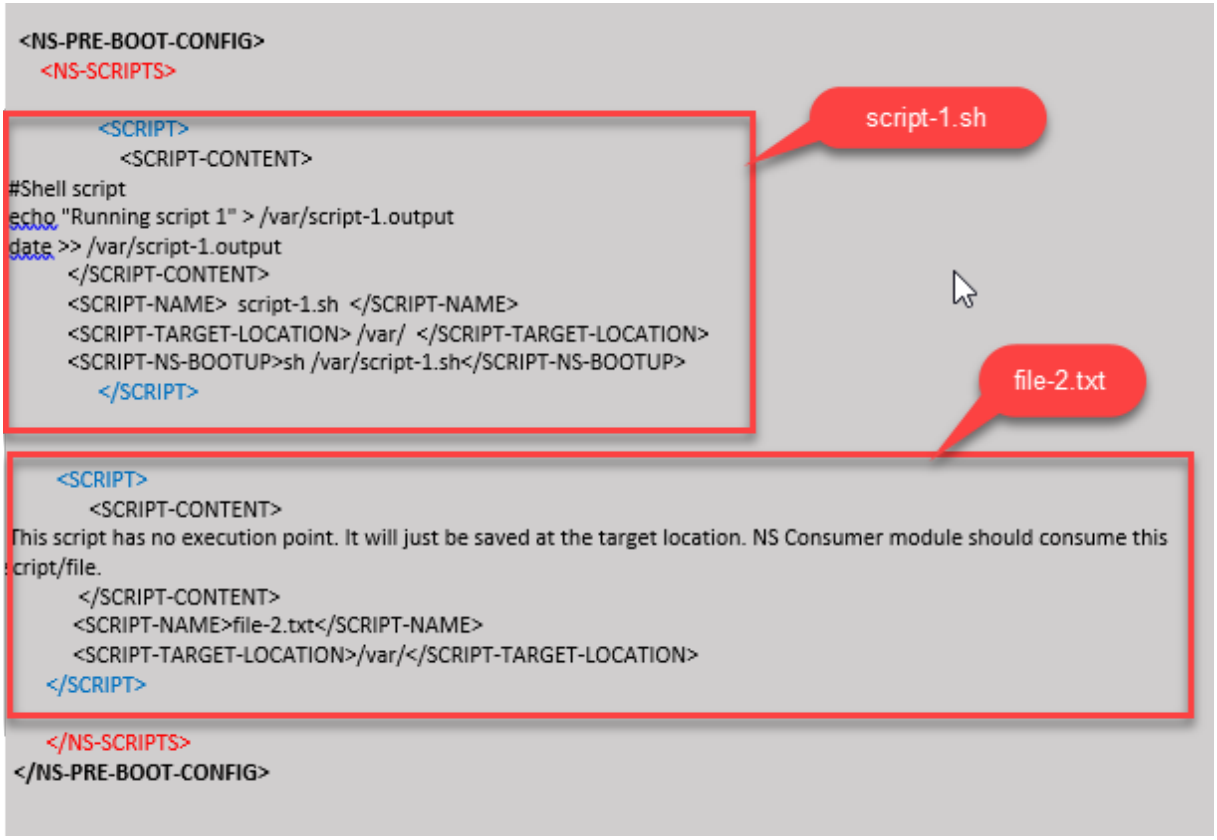
Dans l'instantané suivant, vous pouvez vérifier que le script "script-1.sh" est enregistré dans le répertoire « /var/ ». Le script "Script-1.sh" est exécuté et le fichier de sortie est créé de manière appropriée.



Exemple 2 :

Dans l'exemple suivant, la balise <NS-SCRIPTS> contient des détails sur deux scripts.

- Le premier script est enregistré sous le nom "script-1.sh" dans le répertoire « /var ». Le script est rempli avec le contenu spécifié et est exécuté avec la commande « sh /var/script-1.sh » après le démarrage du moteur de paquets.
- Le second script est enregistré sous le nom "file-2.txt" dans le répertoire « /var ». Ce fichier contient le contenu spécifié. Mais il n'est pas exécuté car la commande d'exécution de démarrage <SCRIPT-NS-BOOTUP> n'est pas fournie.



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
        <SCRIPT>
            <SCRIPT-CONTENT>
               #Shell script
               echo "Running script 1" > /var/script-1.output
               date >> /var/script-1.output
            </SCRIPT-CONTENT>

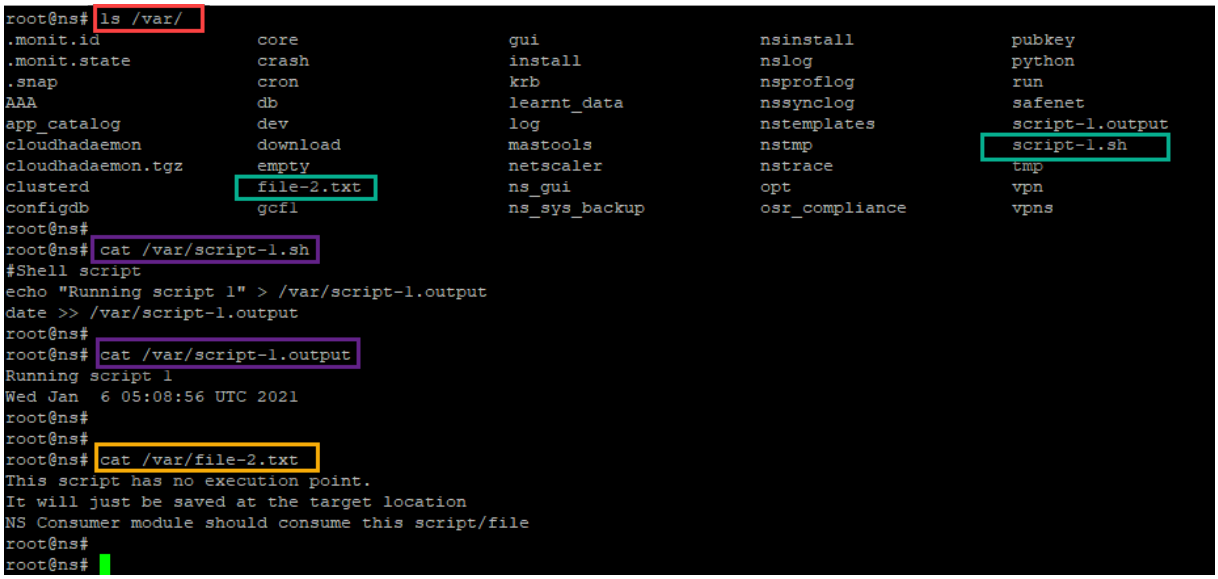
            <SCRIPT-NAME>  script-1.sh  </SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION> /var/  </SCRIPT-TARGET-LOCATION>
            <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>
            </SCRIPT>

        <SCRIPT>
            <SCRIPT-CONTENT>
                This script has no execution point.
                It will just be saved at the target location
                NS Consumer module should consume this script/file
            </SCRIPT-CONTENT>
```



```
            <SCRIPT-NAME>file-2.txt</SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION>/var/</SCRIPT-TARGET-LOCATION>
        </SCRIPT>
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Dans l'instantané suivant, vous pouvez vérifier que script-1.sh et file-2.txt sont créés dans le répertoire « /var/ ». Le fichier Script-1.sh est exécuté et le fichier de sortie est créé de manière appropriée.



Gestion des licences

Utilisez la balise <NS-LICENSE-CONFIG> pour appliquer les licences groupées NetScaler lors du démarrage de l'instance VPX. Utilisez la balise <LICENSE-COMMANDS> dans la section <NS-LICENSE-CONFIG> pour fournir les commandes de licence regroupées. Ces commandes doivent être valides syntaxiquement.

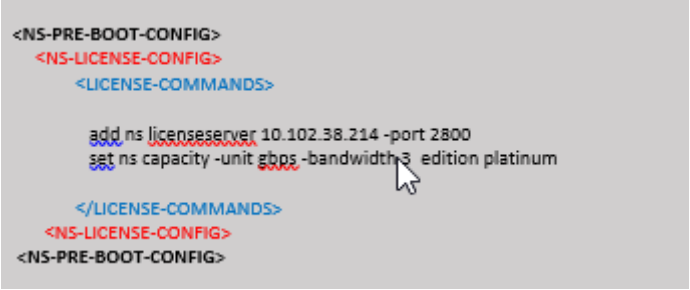
Vous pouvez spécifier les détails de licence regroupés tels que le type de licence, la capacité et le serveur de licences dans la section <LICENSE-COMMANDS> à l'aide des commandes de licences groupées standard. Pour plus d'informations, consultez la section Configurer les licences de capacité groupées NetScaler.

Après avoir appliqué le <NS-LICENSE-CONFIG>, le VPX arrive avec l'édition demandée au démarrage, et VPX tente d'extraire les licences configurées à partir du serveur de licences.

- Si la récupération de la licence est réussie, la bande passante configurée est appliquée à VPX.
- Si la récupération des licences échoue, la licence n'est pas extraite du serveur de licences dans les 10 à 12 minutes environ. Par conséquent, le système redémarre et entre dans un état sans licence.

Exemple :

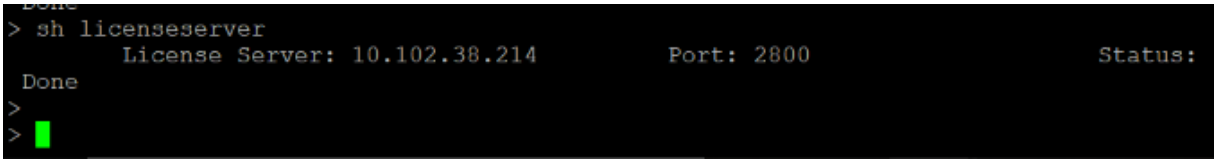
Dans l'exemple suivant, après avoir appliqué le <NS-LICENSE-CONFIG>, le VPX arrive avec l'édition Premium au démarrage, et VPX tente d'extraire les licences configurées à partir du serveur de licences (10.102.38.214).



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
   <NS-LICENSE-CONFIG>
        <LICENSE-COMMANDS>
            add ns licenseserver 10.102.38.214 -port 2800
            set ns capacity -unit gbps -bandwidth 3  edition platinum
        </LICENSE-COMMANDS>
    </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Comme indiqué dans l'illustration suivante, vous pouvez exécuter la commande « show license server » et vérifier que le serveur de licences (10.102.38.214) est ajouté au VPX.



Bootstrapping

Utilisez la balise <NS-BOOTSTRAP> pour fournir les informations de démarrage personnalisées. Vous pouvez utiliser les balises <SKIP-DEFAULT-BOOTSTRAP> et <NEW-BOOTSTRAP-SEQUENCE> dans la section <NS-BOOTSTRAP>. Cette section indique à l'appliance NetScaler s'il faut éviter ou non le bootstrap par défaut. Si le démarrage par défaut est évité, cette section vous offre la possibilité de fournir une nouvelle séquence de démarrage.

Configuration d'amorçage par défaut

La configuration d'amorçage par défaut de l'appliance NetScaler suit les attributions d'interface suivantes :

- **Eth0** - Interface de gestion avec une certaine adresse NSIP.
- **Eth1** - Interface client avec une certaine adresse VIP.
- **Eth2** - Interface serveur avec une certaine adresse SNIP.

Personnalisation de la configuration de bootstrap

Vous pouvez ignorer la séquence d'amorçage par défaut et fournir une nouvelle séquence d'amorçage pour l'instance NetScaler VPX. Utilisez la balise <NS-BOOTSTRAP> pour fournir les informations de démarrage personnalisées. Par exemple, vous pouvez modifier le démarrage par défaut, où l'interface de gestion (NSIP), l'interface VIP et l'interface orientée serveur (SNIP) sont toujours fournies dans un certain ordre.

Le tableau suivant indique le comportement d'amorçage avec les différentes valeurs autorisées pour les balises <SKIP-DEFAULT-BOOTSTRAP> et <NEW-BOOTSTRAP-SEQUENCE>.

SKIP-DEFAULT-BOOTSTRAP	NEW-BOOTSTRAP-SEQUENCE	Comportement Bootstrap
OUI	OUI	Le comportement d'amorçage par défaut est ignoré et une nouvelle séquence d'amorçage personnalisée fournie dans la section <NS-BOOTSTRAP> est exécutée.
OUI	NON	Le comportement d'amorçage par défaut est ignoré. Les commandes d'amorçage fournies dans la section <NS-CONFIG> sont exécutées.

Vous pouvez personnaliser la configuration d'amorçage à l'aide des trois méthodes suivantes :

- Fournissez uniquement les détails de l'interface
- Fournir les détails de l'interface ainsi que les adresses IP et le masque de sous-réseau
- Fournir des commandes liées au bootstrap dans la section <NS-CONFIG>

Méthode 1 : amorçage personnalisé en spécifiant uniquement les détails de l'interface

Vous spécifiez les interfaces de gestion, orientées client et orientées serveur, mais pas leurs adresses IP et masques de sous-réseau. Les adresses IP et les masques de sous-réseau sont renseignés en interrogeant l'infrastructure cloud.

Exemple d'amorçage personnalisé pour AWS

Vous fournissez la séquence d'amorçage personnalisée, comme illustré dans l'exemple suivant. Pour plus d'informations, voir Comment fournir des données utilisateur de pré-démarrage dans une instance cloud. L'interface Eth1 est assignée en tant qu'interface de gestion (NSIP), Eth0 comme interface client (VIP) et interface Eth2 en tant qu'interface serveur (SNIP). La section `<NS-BOOTSTRAP>` contient uniquement les détails de l'interface et non les détails des adresses IP et des masques de sous-réseau.

```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

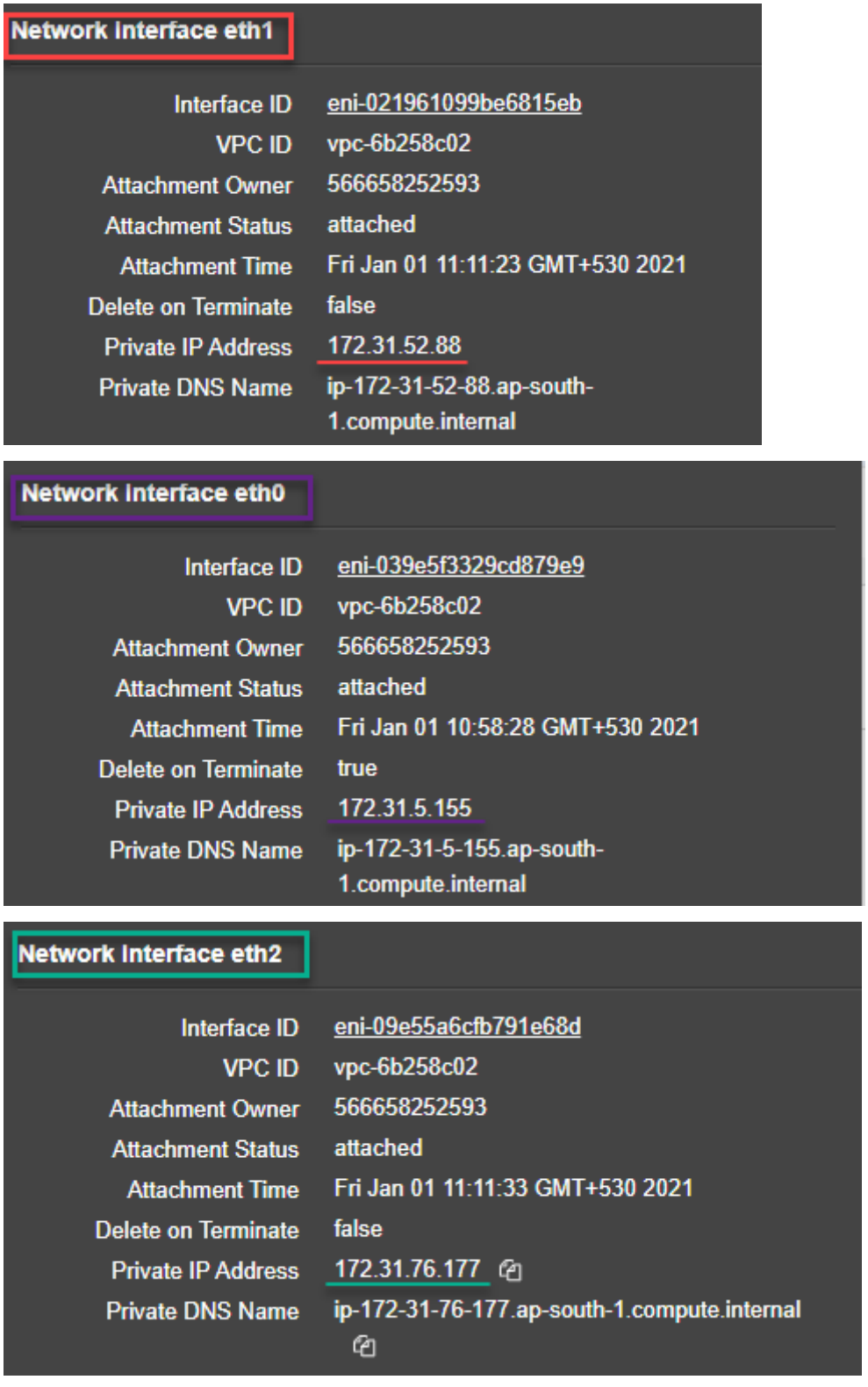
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

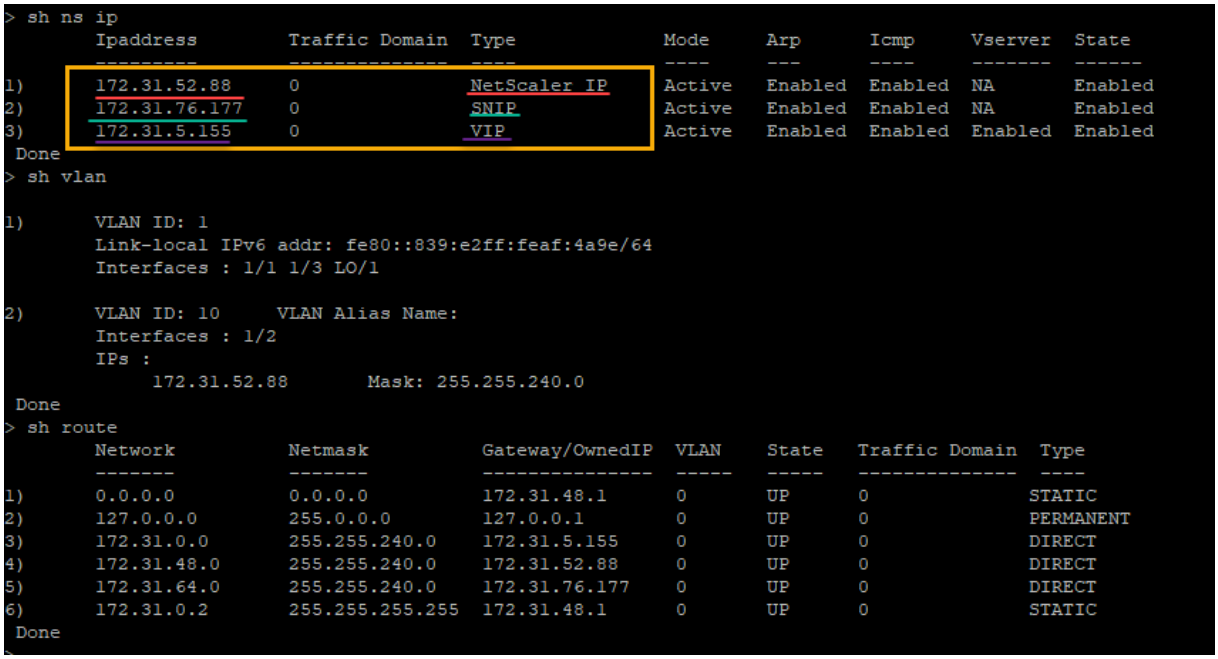
    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Une fois l'instance de machine virtuelle créée, dans le portail AWS, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

1. Accédez au **portail AWS > instances EC2**et sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Dans l'onglet **Description**, vous pouvez vérifier les propriétés de chaque interface réseau, comme illustré dans les illustrations suivantes.



Vous pouvez exécuter la commande `show nsip` dans l'interface de **ligne de commande ADC**et vérifier les interfaces réseau appliquées à l'instance NetScaler VPX lors du premier démarrage de l'appliance ADC.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
```

Exemple de bootstrap personnalisé pour Azure

Vous fournissez la séquence d'amorçage personnalisée, comme illustré dans l'exemple suivant. Pour plus d'informations, voir Comment fournir des données utilisateur de pré-démarrage dans une instance cloud. L'interface Eth2 est assignée en tant qu'interface de gestion (NSIP), Eth1 comme interface client (VIP) et interface Eth0 en tant qu'interface serveur (SNIP). La section <NS-BOOTSTRAP> contient uniquement les détails de l'interface et non les détails des adresses IP et des masques de sous-réseau.


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

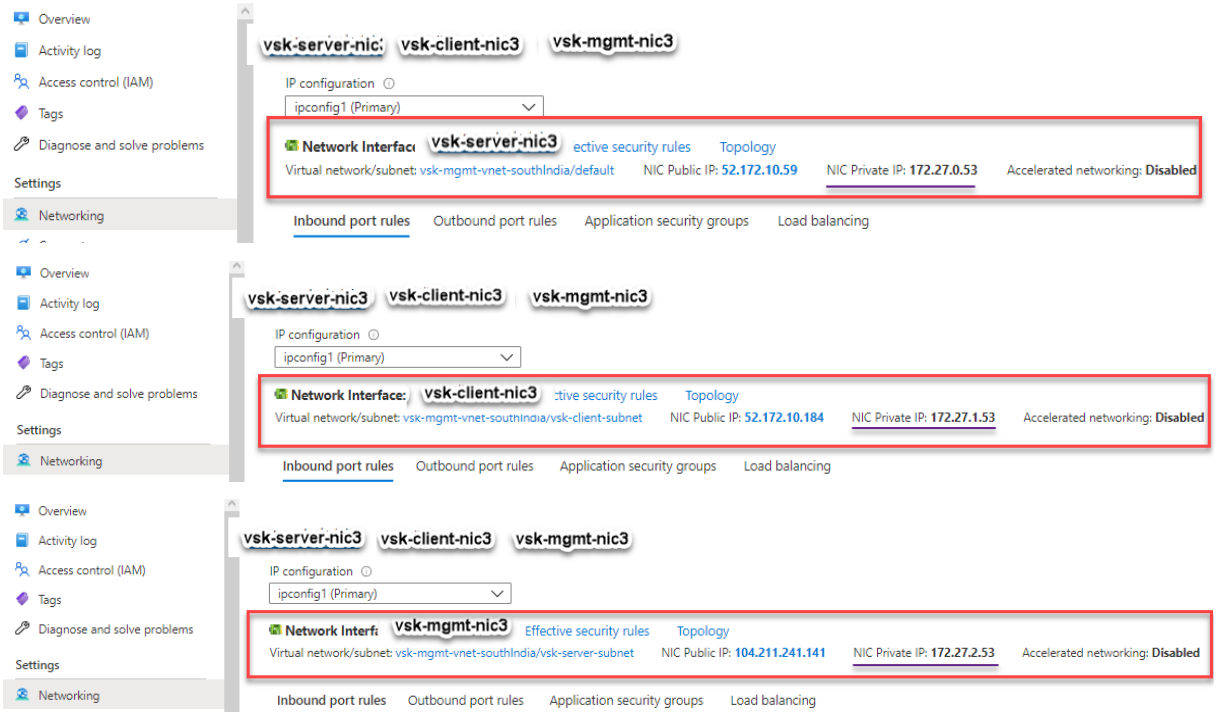
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```

Vous pouvez voir que l'instance NetScaler VPX est créée avec trois interfaces réseau. Accédez au **portail Azure > Instance de machine virtuelle > Mise en réseau**et vérifiez les propriétés réseau des trois cartes réseau, comme illustré dans les illustrations suivantes.



Vous pouvez exécuter la commande « show nsip » dans l'interface de ligne de commande ADC et véri-

fier que la nouvelle séquence d'amorçage spécifiée dans la section <NS-BOOTSTRAP> est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.53      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.53      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.27.1.53      0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.53        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.53      0       UP      0               DIRECT
4)      172.27.1.0       255.255.255.0    172.27.1.53      0       UP      0               DIRECT
5)      172.27.2.0       255.255.255.0    172.27.2.53      0       UP      0               DIRECT
6)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
7)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
8)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
>
```

Exemples de bootstrap personnalisés pour GCP

Vous fournissez la séquence d'amorçage personnalisée, comme illustré dans l'exemple suivant. Pour plus d'informations, voir Comment fournir des données utilisateur de pré-démarrage dans une instance cloud. L'interface Eth1 est assignée en tant qu'interface de gestion (NSIP), Eth0 comme interface client (VIP) et interface Eth2 en tant qu'interface serveur (SNIP). La section <NS-BOOTSTRAP> contient uniquement les détails de l'interface et non les détails des adresses IP et des masques de sous-réseau.


```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Une fois l'instance de machine virtuelle créée dans le portail GCP, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

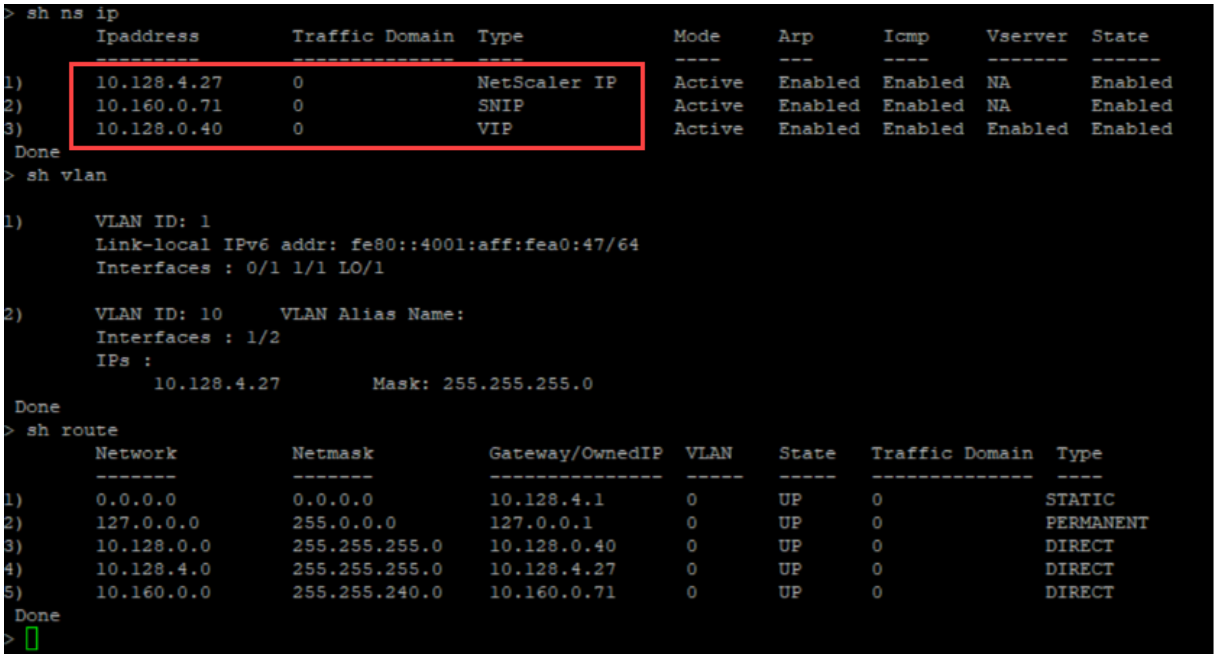
1. Sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Accédez aux propriétés de l'interface réseau et vérifiez les détails de la carte réseau comme suit :

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	10.160.0.71	–	35.244.56.180 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	10.128.0.40	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.27	–	34.93.241.147 (ephemeral)	Premium		View details

Public DNS PTR Record
None

Vous pouvez exécuter la commande `show nsip` dans l'interface de **ligne de commande ADC**et vérifier les interfaces réseau appliquées à l'instance NetScaler VPX lors du premier démarrage de l'appliance ADC.



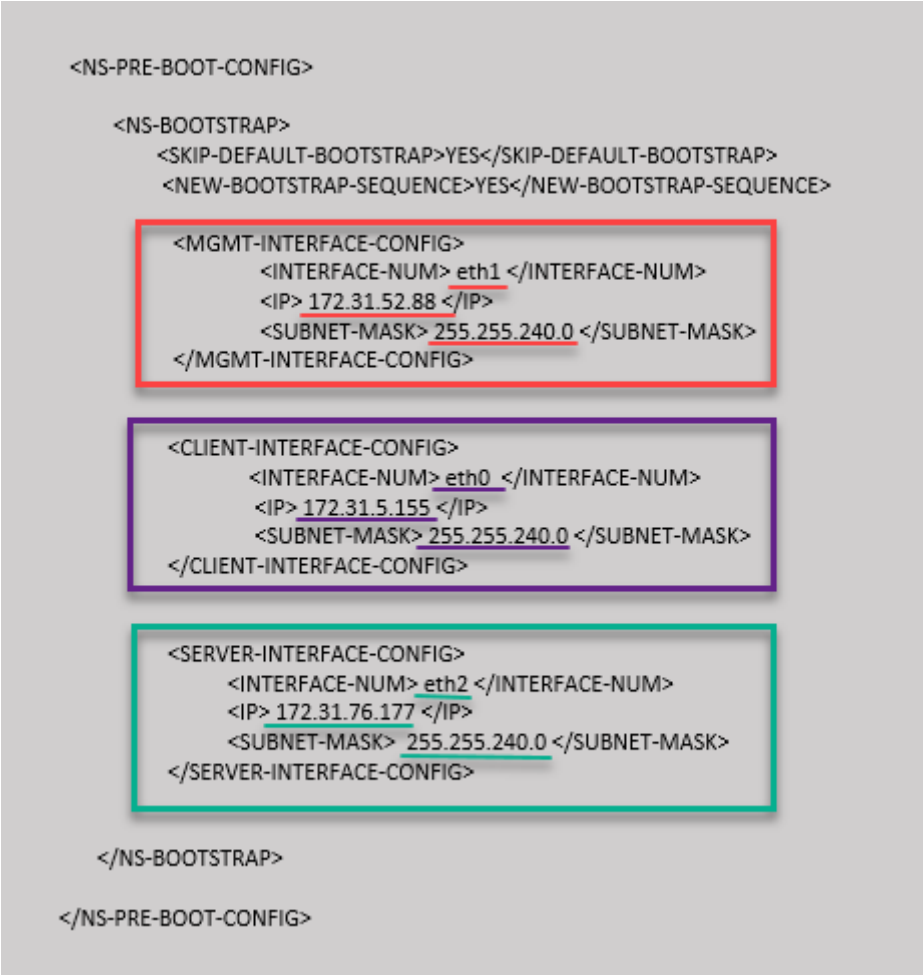
Méthode 2 : amorçage personnalisé en spécifiant les interfaces, adresses IP et masques de sous-réseau

Vous spécifiez les interfaces de gestion, orientées client et serveur, ainsi que leurs adresses IP et leur masque de sous-réseau.

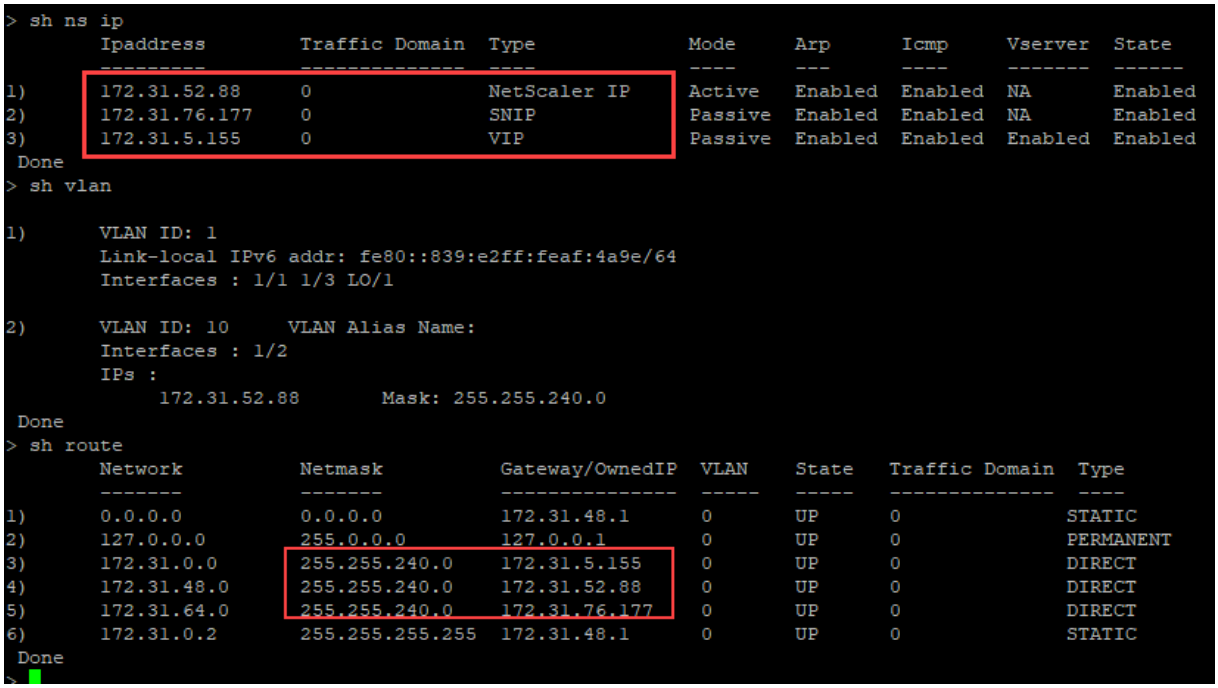
Exemples de bootstrap personnalisés pour AWS

Dans l'exemple suivant, vous ignorez le bootstrap par défaut et exécutez une nouvelle séquence d'amorçage pour l'appliance NetScaler. Pour la nouvelle séquence d'amorçage, vous spécifiez les détails suivants :

- **Interface de gestion :** Interface - Eth1, NSIP - 172.31.52.88 et masque de sous-réseau - 255.255.240.0
- **Interface client :** Interface - Eth0, VIP - 172.31.5.155 et masque de sous-réseau - 255.255.240.0.
- **Interface serveur :** Interface - Eth2, SNIP - 172.31.76.177 et masque de sous-réseau - 255.255.240.0.



Vous pouvez exécuter la commande `show nsip` dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la section `<NS-BOOTSTRAP>` est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Passive  Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Passive  Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Exemple de bootstrap personnalisé pour Azure

Dans l'exemple suivant, une nouvelle séquence d'amorçage pour ADC est mentionnée et l'amorçage par défaut est ignoré. Vous fournissez les détails de l'interface ainsi que les adresses IP et les masques de sous-réseau comme suit :

- Interface de gestion (eth2), NSIP (172.27.2.53) et masque de sous-réseau (255.255.255.0)
- Interface client (eth1), VIP (172.27.1.53) et masque de sous-réseau (255.255.255.0)
- Interface serveur (eth0), SNIP (172.27.0.53) et masque de sous-réseau (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
            <IP> 172.27.2.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>

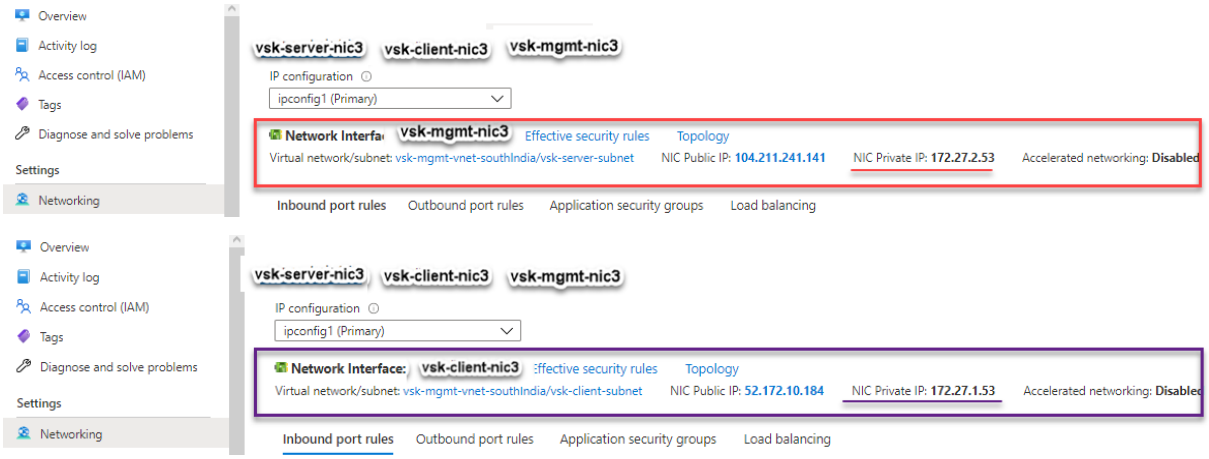
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
            <IP> 172.27.1.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
            </CLIENT-INTERFACE-CONFIG>

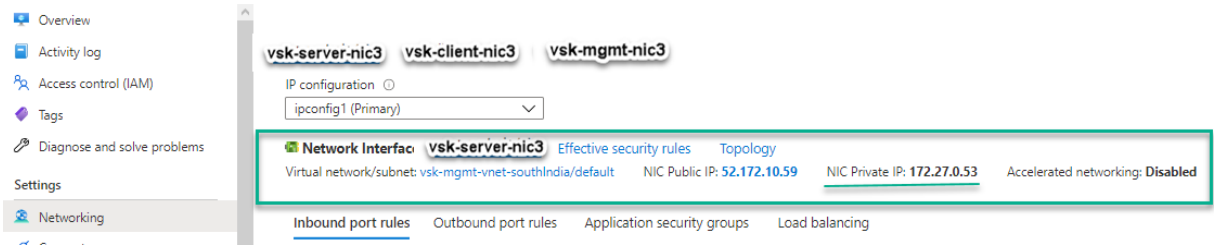
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
            <IP> 172.27.0.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```

Vous pouvez voir que l'instance NetScaler VPX est créée avec trois interfaces réseau. Accédez au **portail Azure > Instance de machine virtuelle > Mise en réseau**et vérifiez les propriétés réseau des trois cartes réseau, comme illustré dans les illustrations suivantes.





Vous pouvez exécuter la commande `show nsip` dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la section <NS-BOOTSTRAP> est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.53      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.53      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.27.1.53      0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.53        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.53      0       UP      0               DIRECT
4)      172.27.1.0       255.255.255.0    172.27.1.53      0       UP      0               DIRECT
5)      172.27.2.0       255.255.255.0    172.27.2.53      0       UP      0               DIRECT
6)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
7)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
8)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Exemple de bootstrap personnalisé pour GCP

Dans l'exemple suivant, une nouvelle séquence d'amorçage pour ADC est mentionnée et l'amorçage par défaut est ignoré. Vous fournissez les détails de l'interface ainsi que les adresses IP et les masques de sous-réseau comme suit :

- Interface de gestion (eth2), NSIP (10.128.4.31) et masque de sous-réseau (255.255.255.0)
- Interface client (eth1), VIP (10.128.0.43) et masque de sous-réseau (255.255.255.0)
- Interface serveur (eth0), SNIP (10.160.0.75) et masque de sous-réseau (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>
   <NS-BOOTSTRAP>
         <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
         <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
          <MGMT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth2 </INTERFACE-NUM>
               <IP> 10.128.4.31 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
           </MGMT-INTERFACE-CONFIG>
          <CLIENT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth1 </INTERFACE-NUM>
               <IP> 10.128.0.43 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </CLIENT-INTERFACE-CONFIG>
          <SERVER-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth0 </INTERFACE-NUM>
               <IP> 10.160.0.75 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </SERVER-INTERFACE-CONFIG>
   </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

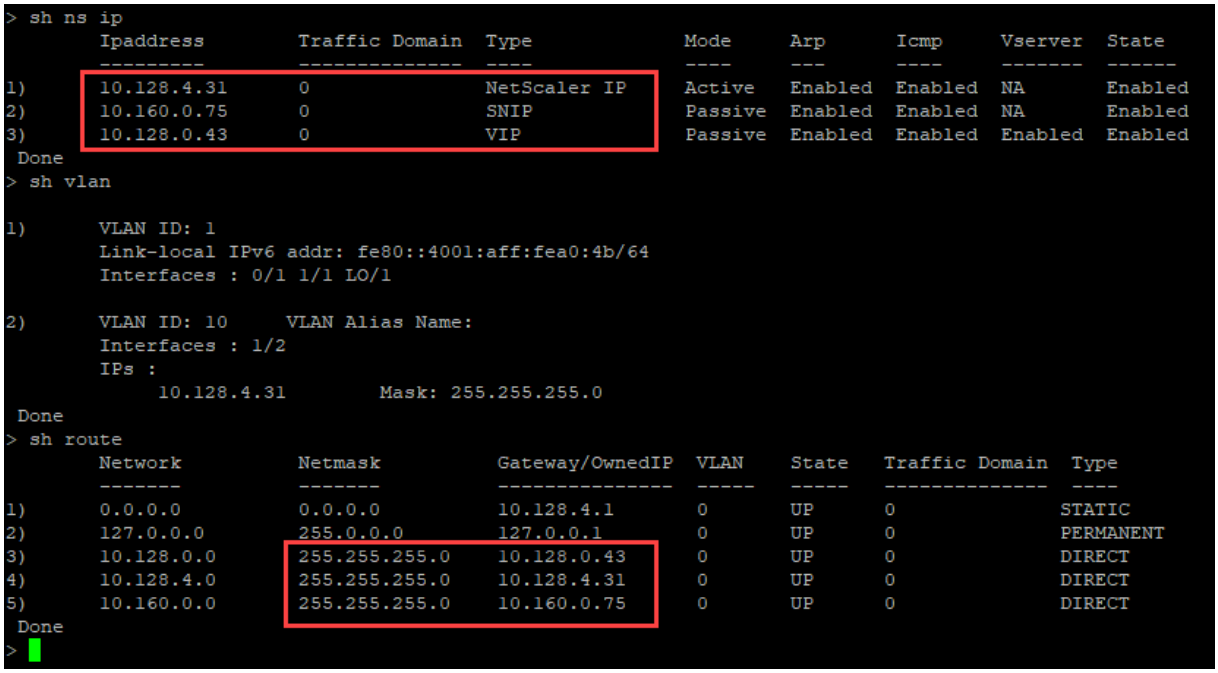
Une fois l'instance de machine virtuelle créée dans le portail GCP avec le bootstrap personnalisé, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

1. Sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Accédez aux propriétés de l'interface réseau et vérifiez les détails de la carte réseau comme suit.


Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	vsk-defnw-st-ip1 (10.160.0.75)	–	34.93.216.90 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	vsk-vpc-nw1-st-ip1 (10.128.0.43)	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	vsk-nw2-st-ip-1 (10.128.4.31)	–	34.93.202.214 (ephemeral)	Premium		View details

Vous pouvez exécuter la commande `show nsip` dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la section <NS-BOOTSTRAP> est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      10.128.4.31      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      10.160.0.75      0               SNIP             Passive  Enabled  Enabled  NA       Enabled
3)      10.128.0.43      0               VIP              Passive  Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:4b/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             10.128.4.31        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.128.4.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      10.128.0.0       255.255.255.0    10.128.0.43      0       UP      0               DIRECT
4)      10.128.4.0       255.255.255.0    10.128.4.31      0       UP      0               DIRECT
5)      10.160.0.0       255.255.255.0    10.160.0.75      0       UP      0               DIRECT
 Done
>
```

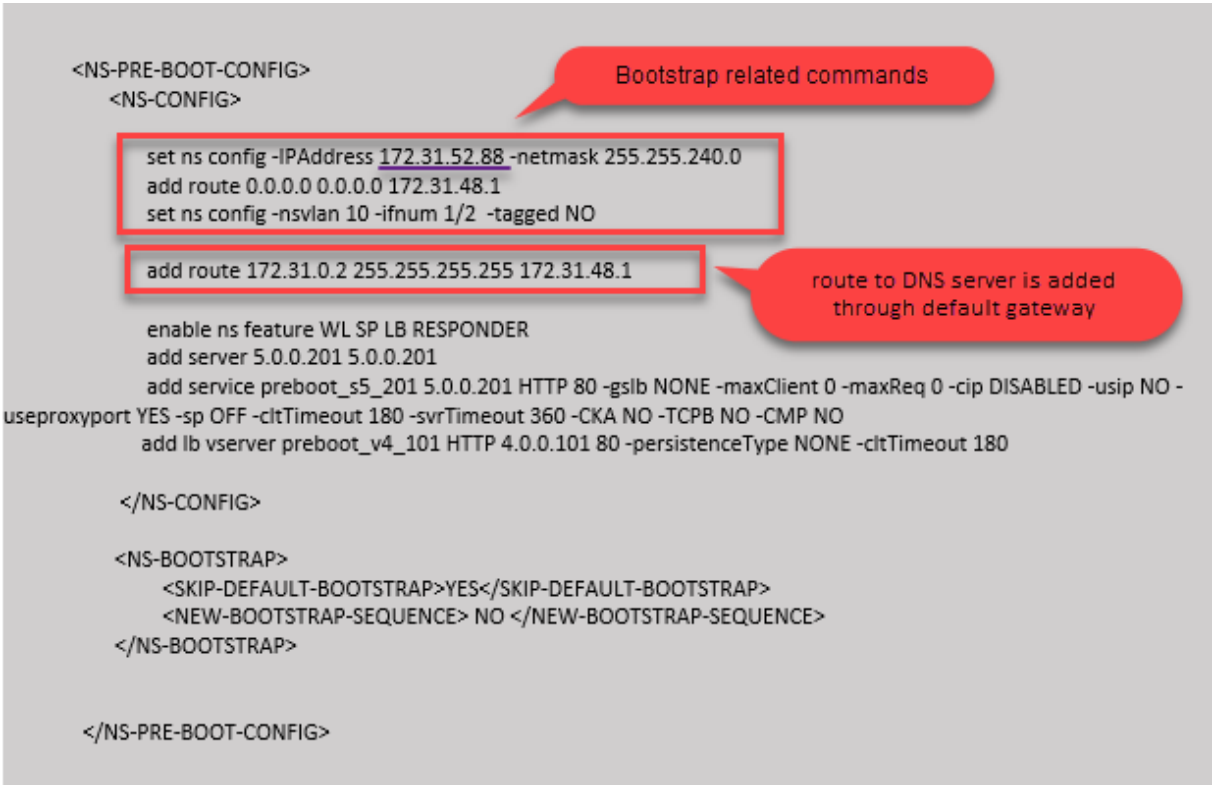
Méthode 3 : Bootstrap personnalisé en fournissant des commandes liées au bootstrap dans la section <NS-CONFIG>

Vous pouvez fournir les commandes associées au bootstrap dans la section <NS-CONFIG>. Dans la section <NS-BOOTSTRAP>, vous devez spécifier la valeur <NEW-BOOTSTRAP-SEQUENCE> « Non » pour exécuter les commandes d'amorçage de la section <NS-CONFIG>. Vous devez également fournir les commandes pour attribuer NSIP, routage par défaut et NSVLAN. En outre, fournissez les commandes pertinentes pour le cloud que vous utilisez.

Avant de fournir un bootstrap personnalisé, assurez-vous que votre infrastructure cloud prend en charge une configuration d'interface particulière.

Exemple d'amorçage personnalisé pour AWS

Dans cet exemple, les commandes liées au bootstrap sont fournies dans la section <NS-CONFIG>. La section <NS-BOOTSTRAP> indique que le démarrage par défaut est ignoré et que les informations d'amorçage personnalisées fournies dans la section <NS-CONFIG> sont exécutées. Vous devez également fournir les commandes permettant de créer NSIP, d'ajouter un itinéraire par défaut et d'ajouter un NSVLAN.



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>

        set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
        add route 0.0.0.0 0.0.0.0 172.31.48.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add route 172.31.0.2 255.255.255.255 172.31.48.1

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO - useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

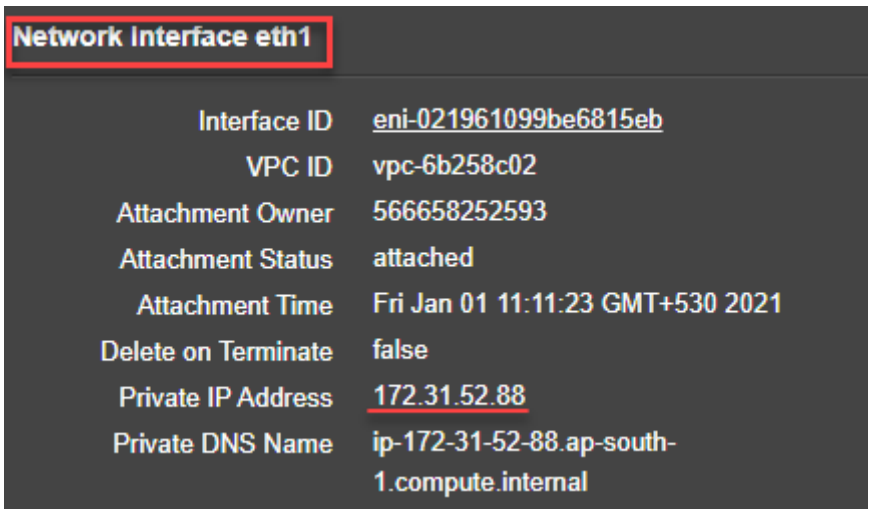
    <NS-BOOTSTRAP>
     <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
     <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
```

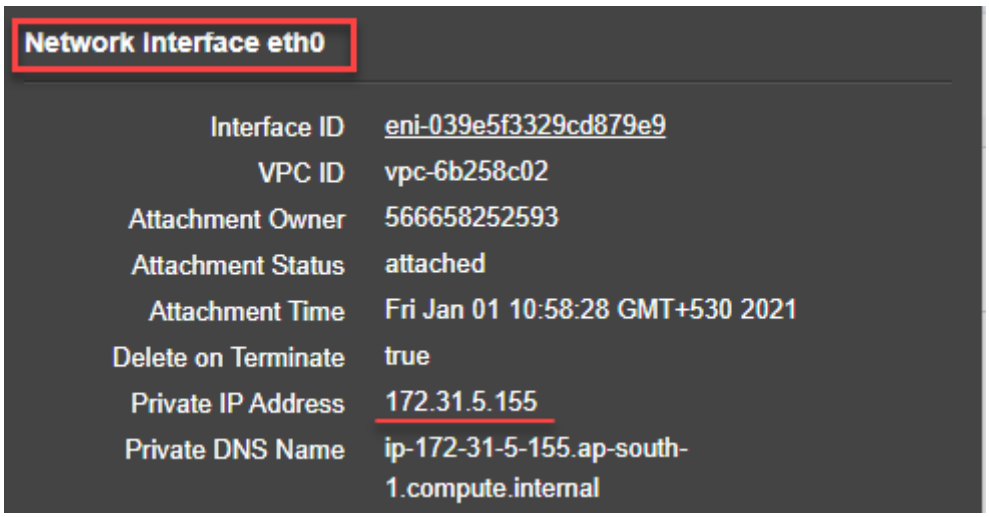


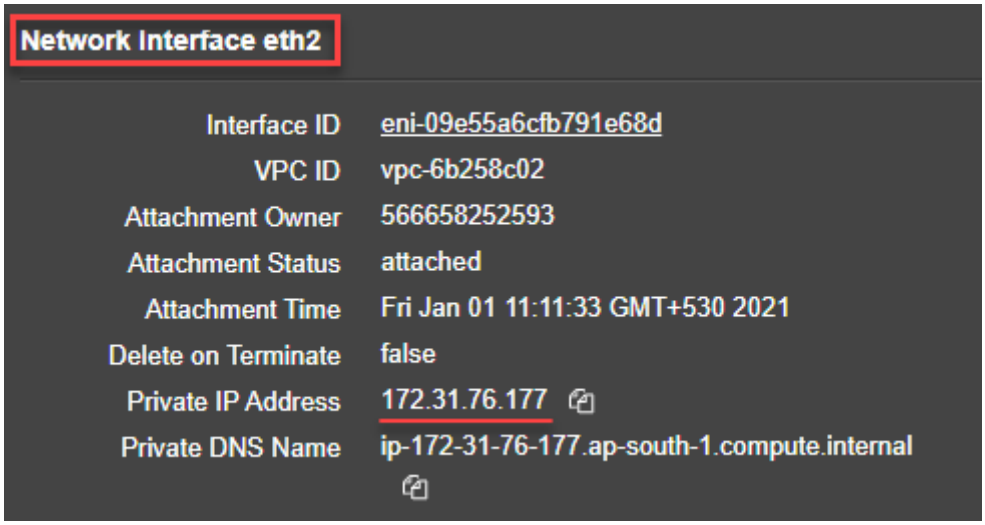
```
19      </NS-BOOTSTRAP>
20
21
22  </NS-PRE-BOOT-CONFIG>
23  <!--NeedCopy-->
```

Une fois l'instance de machine virtuelle créée, dans le portail AWS, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

1. Accédez au **portail AWS > instances EC2**et sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Dans l'onglet **Description**, vous pouvez vérifier les propriétés de chaque interface réseau, comme illustré dans les illustrations suivantes.







Vous pouvez exécuter la commande `show nsip` dans l'interface de **ligne de commande ADC**et vérifier les interfaces réseau appliquées à l'instance NetScaler VPX lors du premier démarrage de l'appliance ADC.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

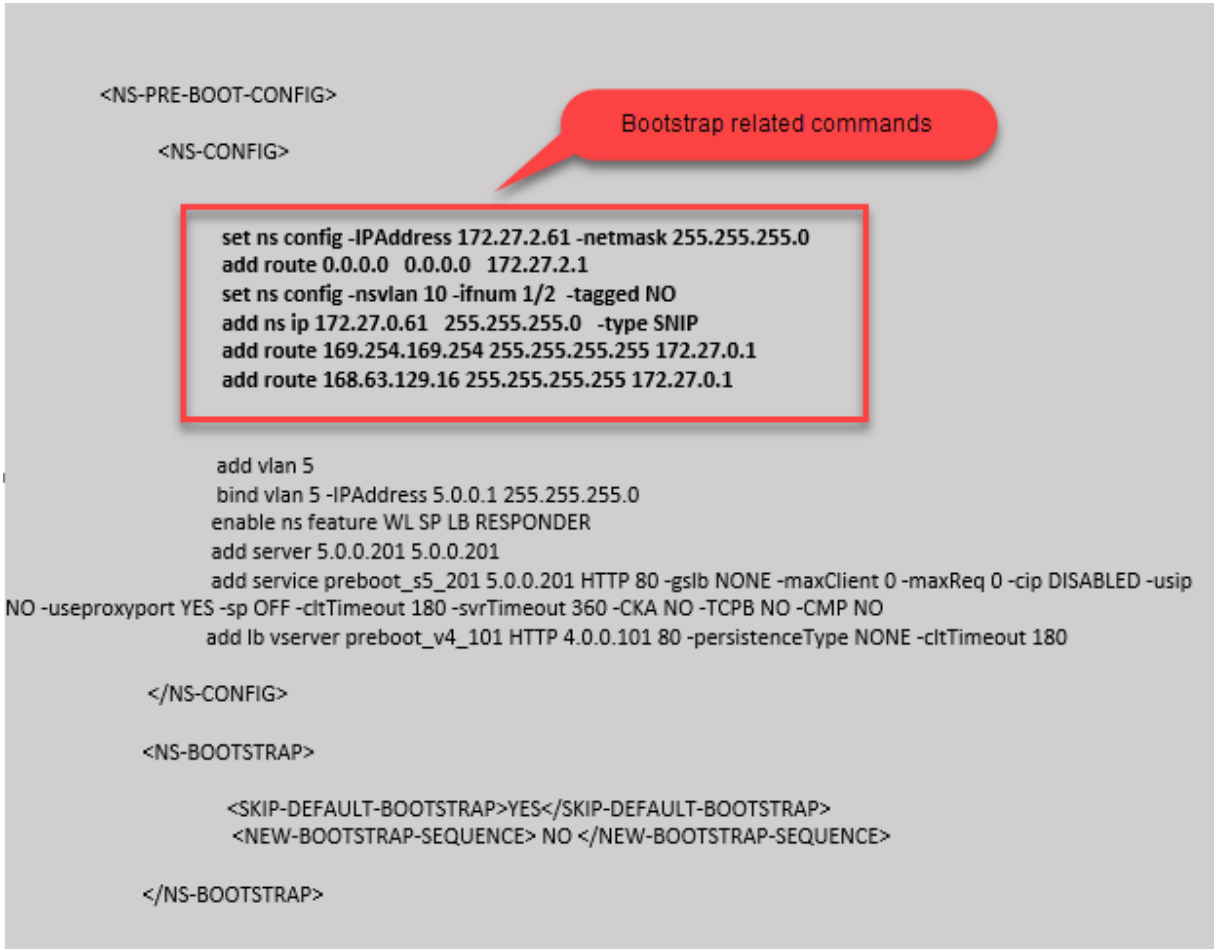
2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
4)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Exemple de bootstrap personnalisé pour Azure

Dans cet exemple, les commandes liées au bootstrap sont fournies dans la section <NS-CONFIG>. La section <NS-BOOTSTRAP> indique que le démarrage par défaut est ignoré et que les informations d'amorçage personnalisées fournies dans la section <NS-CONFIG> sont exécutées.

> Remarque :
>
> Pour le cloud Azure, le serveur de métadonnées d'instance (IMDS) et les serveurs DNS sont ac-

> cessibles uniquement via l'interface principale (Eth0). Par conséquent, si l'interface Eth0 n'est pas utilisée comme interface de gestion (NSIP), l'interface Eth0 doit au moins être configurée comme SNIP pour l'accès IMDS ou DNS pour fonctionner. La route vers le point de terminaison IMDS (169.254.169.254) et le point de terminaison DNS (168.63.129.16) via la passerelle d'Eth0 doit également être ajoutée.




```
<NS-PRE-BOOT-CONFIG>

   <NS-CONFIG>

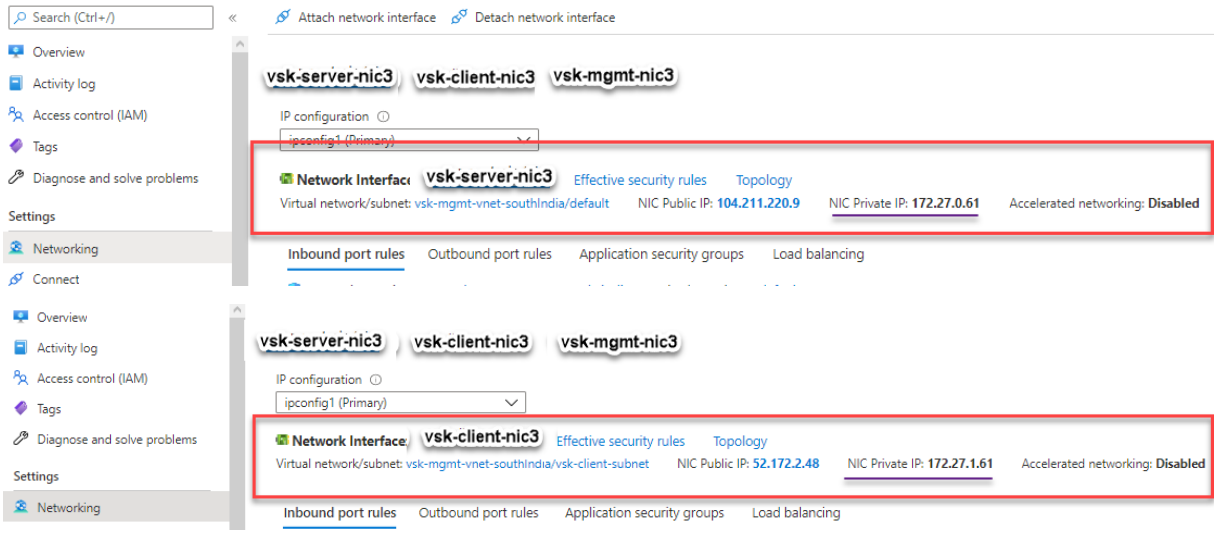
        set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0
        add route 0.0.0.0   0.0.0.0   172.27.2.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add ns ip 172.27.0.61   255.255.255.0   -type SNIP
        add route 169.254.169.254 255.255.255.255 172.27.0.1
        add route 168.63.129.16 255.255.255.255 172.27.0.1

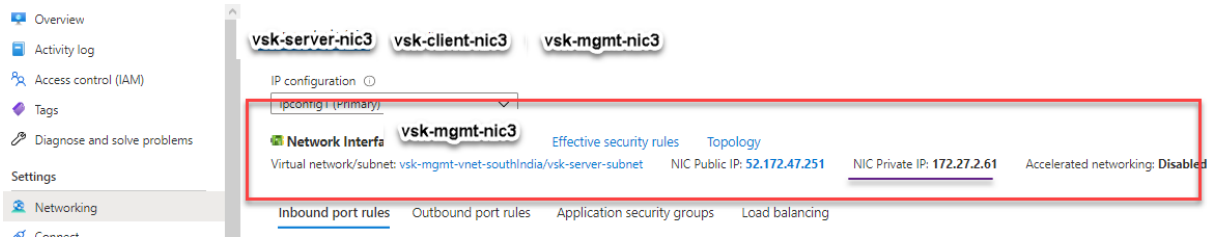
        add vlan 5
        bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
```



```
14          enable ns feature WL SP LB RESPONDER
15          add server 5.0.0.201 5.0.0.201
16          add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
               maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
               YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
                -CMP NO
17          add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
               persistenceType NONE -cltTimeout 180
18
19      </NS-CONFIG>
20
21      <NS-BOOTSTRAP>
22
23      <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
24      <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
25
26      </NS-BOOTSTRAP>
27
28  </NS-PRE-BOOT-CONFIG>
29  <!--NeedCopy-->
```

Vous pouvez voir que l'instance NetScaler VPX est créée avec trois interfaces réseau. Accédez au **portail Azure > Instance de machine virtuelle > Mise en réseau**et vérifiez les propriétés réseau des trois cartes réseau, comme illustré dans les illustrations suivantes.





Vous pouvez exécuter la commande `show nsip` dans l'interface de ligne de commande ADC et vérifier que la nouvelle séquence d'amorçage spécifiée dans la section <NS-BOOTSTRAP> est appliquée. Vous pouvez exécuter la commande « show route » pour vérifier le masque de sous-réseau.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      172.27.2.61      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.61      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

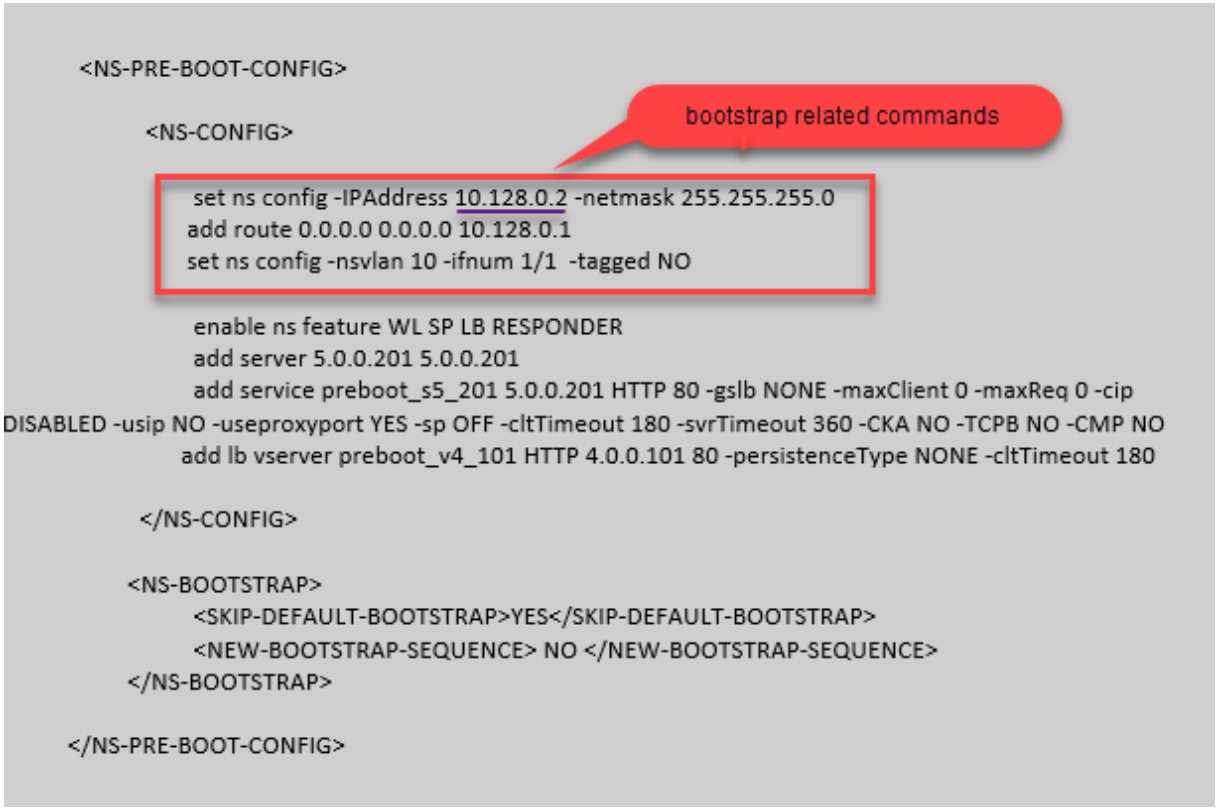
1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:9076/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 5      VLAN Alias Name:

3)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.61        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.61      0       UP      0               DIRECT
4)      172.27.2.0       255.255.255.0    172.27.2.61      0       UP      0               DIRECT
5)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
6)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
7)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Exemple de bootstrap personnalisé pour GCP

Dans cet exemple, les commandes liées au bootstrap sont fournies dans la section <NS-CONFIG>. La section <NS-BOOTSTRAP> indique que le démarrage par défaut est ignoré et que les informations d'amorçage personnalisées fournies dans la section <NS-CONFIG> sont appliquées.



Vous pouvez copier la configuration affichée dans la capture d'écran précédente à partir d'ici :

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>

        set ns config -IPAddress 10.128.0.2 -netmask 255.255.255.0
        add route 0.0.0.0 0.0.0.0 10.128.0.1
        set ns config -nsvlan 10 -ifnum 1/1  -tagged NO

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
```

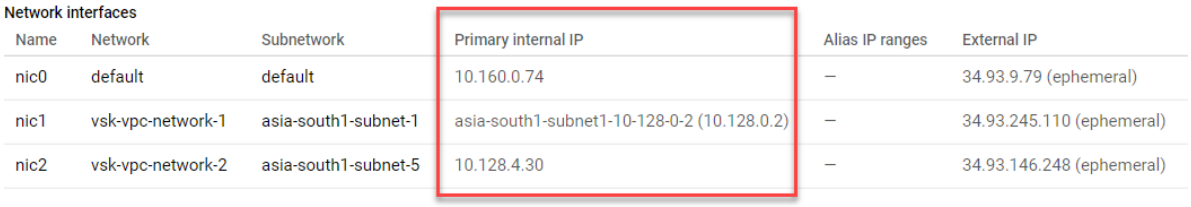


```
        <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Une fois l'instance de machine virtuelle créée dans le portail GCP avec le bootstrap personnalisé, vous pouvez vérifier les propriétés de l'interface réseau comme suit :

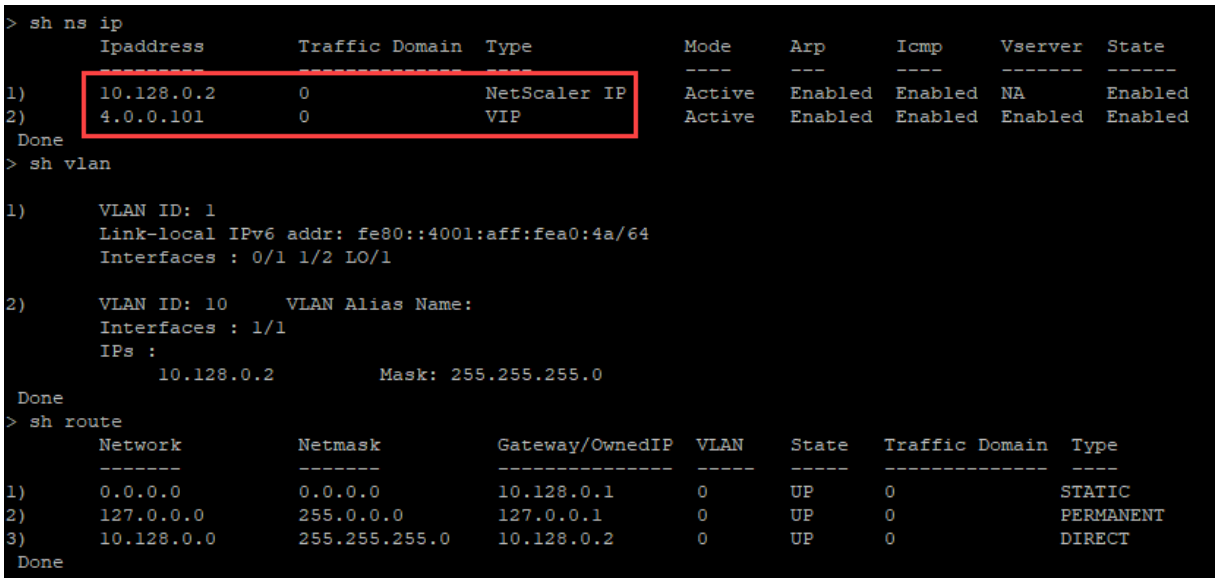
1. Sélectionnez l'instance que vous avez créée en fournissant les informations d'amorçage personnalisées.
2. Accédez aux propriétés de l'interface réseau et vérifiez les détails de la carte réseau, comme indiqué dans l'illustration.



Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP
nic0	default	default	10.160.0.74	–	34.93.9.79 (ephemeral)
nic1	vsk-vpc-network-1	asia-south1-subnet-1	asia-south1-subnet1-10-128-0-2 (10.128.0.2)	–	34.93.245.110 (ephemeral)
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.30	–	34.93.146.248 (ephemeral)

Vous pouvez exécuter la commande `show nsip` dans **ADC CLI**et vérifier que les configurations fournies dans la section `<NS-CONFIG>` précédente sont appliquées au premier démarrage de l'appliance ADC.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      10.128.0.2       0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:4a/64
        Interfaces : 0/1 1/2 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/1
        IPs :
             10.128.0.2         Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.128.0.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      10.128.0.0       255.255.255.0    10.128.0.2       0       UP      0               DIRECT
 Done
```

Impact de l'attachement et du détachement de cartes réseau dans AWS et Azure

AWS et Azure offrent la possibilité d'attacher une interface réseau à une instance et de détacher une interface réseau d'une instance. La fixation ou le détachement d'interfaces peuvent modifier la position de l'interface. Citrix vous recommande donc de ne pas détacher les interfaces de l'instance

NetScaler VPX. Si vous détachez ou attachez une interface lorsque le bootstrap personnalisé est configuré, l'instance NetScaler VPX réattribue l'adresse IP principale de l'interface nouvellement disponible à la position de l'interface de gestion en tant que NSIP. Si aucune autre interface n'est disponible après celle que vous avez détachée, la première interface devient l'interface de gestion de l'instance NetScaler VPX.

Par exemple, une instance NetScaler VPX est proposée avec 3 interfaces : Eth0 (SNIP), Eth1 (NSIP) et Eth2 (VIP). Si vous détachez l'interface Eth1 de l'instance, qui est une interface de gestion, ADC configure la prochaine interface disponible (Eth2) comme interface de gestion. Ainsi, l'instance NetScaler VPX est toujours accessible via l'adresse IP principale de l'interface Eth2. Si Eth2 n'est pas non plus disponible, l'interface restante (Eth0) devient l'interface de gestion. Par conséquent, l'accès à l'instance NetScaler VPX continue d'exister.

Considérons une affectation différente des interfaces comme suit : Eth0 (SNIP), Eth1 (VIP) et Eth2 (NSIP). Si vous détachez Eth2 (NSIP), car aucune nouvelle interface n'est disponible après Eth2, la première interface (Eth0) devient l'interface de gestion.

Améliorez les performances SSL-TPS sur les plateformes de cloud public

May 5, 2023

Vous pouvez obtenir de meilleures performances SSL-TPS sur les nuages AWS et GCP en répartissant les poids du moteur de paquets (PE) de manière égale. L'activation de cette fonctionnalité peut entraîner une légère baisse du débit HTTP d'environ 10 à 12 %.

Sur les clouds AWS et GCP, les instances NetScaler VPX dotées de 10 à 16 processeurs virtuels ne présentent aucune amélioration des performances car les poids des PE sont répartis de manière égale par défaut.

> Remarque :
>
> Dans le cloud Azure, les poids PE sont également distribués par défaut. Cette fonctionnalité n'améliore aucune performance pour les instances Azure.

Configurer le mode PE à l'aide de l'interface de ligne de commande NetScaler

Après avoir défini le mode PE, vous devez redémarrer le système pour que les modifications de configuration prennent effet.

À l'invite de commande, tapez :

```
set cpuparam pemode [CPUBOUND | Default]
<!--NeedCopy-->
```


Lorsque le mode PE est réglé sur CPUBOUND, les poids PE sont également répartis.
Lorsque le mode PE est défini sur DEFAULT, les pondérations PE sont définies sur les valeurs par défaut.

> Remarque :
>
> Cette commande est spécifique au nœud. Dans une configuration de haute disponibilité ou de cluster, vous devez exécuter la commande sur chaque nœud. Si vous exécutez la commande sur CLIP, l'erreur suivante se produit :
> `Operation not permitted on CLIP`

Pour afficher l'état du mode PE configuré, exécutez la commande suivante :

```
1 show cpuparam
2 <!--NeedCopy-->
```

Exemple :

```
1 > show cpuparam
2     Pemode:  CPUBOUND
3  Done
4 <!--NeedCopy-->
```

Appliquer la configuration du mode PE au premier démarrage de l'appliance NetScaler dans le cloud

Pour appliquer la configuration du mode PE lors du premier démarrage de l'appliance NetScaler dans le cloud, vous devez créer un `/nsconfig/.cpubound.conf` fichier à l'aide du script personnalisé. Pour plus d'informations, voir Appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler dans le cloud.

Installation d'une instance NetScaler VPX sur un serveur bare metal

May 5, 2023

Un bare metal est un serveur physique entièrement dédié qui assure une isolation physique, entièrement intégré à l'environnement cloud. Il est également connu sous le nom de serveur à locataire unique. La location individuelle permet d'éviter l'effet de voisinage bruyant. Avec le métal nu, vous n'êtes pas témoin de l'effet de voisinage bruyant car vous êtes le seul utilisateur.

Un serveur bare metal installé avec un hyperviseur vous fournit une suite de gestion pour créer des machines virtuelles sur le serveur. L'hyperviseur n'exécute pas les applications en mode natif. Son objectif est de virtualiser vos charges de travail sur des machines virtuelles distinctes afin de bénéficier de la flexibilité et de la fiabilité de la virtualisation.

Conditions préalables à l'installation d'une instance NetScaler VPX sur des serveurs bare metal

Un serveur bare metal doit être obtenu auprès d'un fournisseur de cloud répondant à toutes les exigences système de l'hyperviseur concerné.

Installation de l'instance NetScaler VPX sur des serveurs bare metal

Pour installer des instances NetScaler VPX sur un serveur bare metal, vous devez d'abord vous procurer un serveur bare metal doté de ressources système adéquates auprès d'un fournisseur de cloud. Sur ce serveur bare metal, tous les hyperviseurs pris en charge tels que Linux KVM, VMware ESX, Citrix Hypervisor ou Microsoft Hyper-V doivent être installés et configurés avant de déployer l'instance NetScaler VPX.

Pour plus d'informations sur la liste des différents hyperviseurs et fonctionnalités pris en charge sur une instance NetScaler VPX, consultez la matrice de supportet les directives d'utilisation.

Pour plus d'informations sur l'installation des instances NetScaler VPX sur différents hyperviseurs, consultez la documentation correspondante.

- **Citrix Hypervisor :** voir Installer une instance NetScaler VPXsur Citrix Hypervisor.
- **VMware ESX :** voir Installation d'une instance NetScaler VPX sur VMware ESX.
- **Microsoft Hyper-V :** voir Installation d'une instance NetScaler VPX surun serveur Microsoft Hyper-V.
- **Plateforme KVM Linux :** voir Installation d'une instance NetScaler VPX sur la plate-forme Linux-KVM.

Installation d'une instance NetScaler VPX sur Citrix Hypervisor

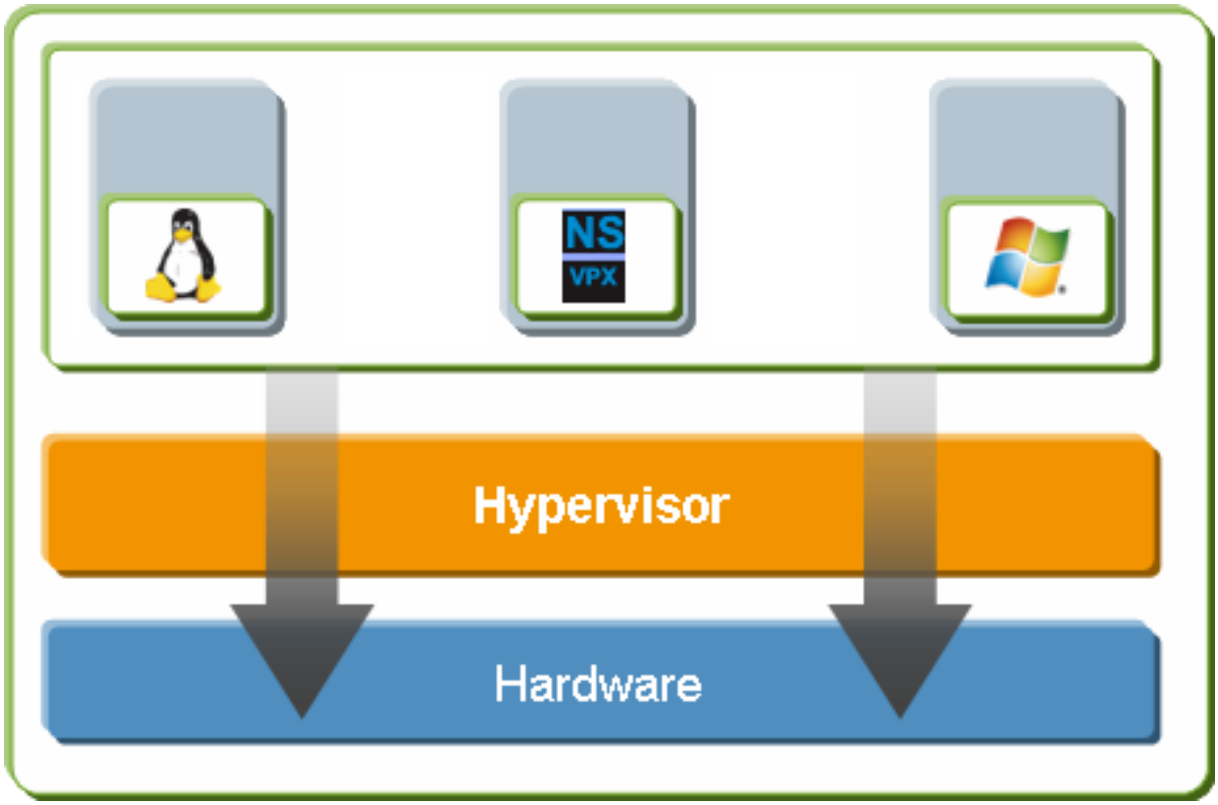
July 31, 2023

Pour installer des instances VPX sur Citrix Hypervisor, vous devez d'abord installer l'hyperviseur sur une machine disposant de ressources système adéquates. Pour effectuer l'installation de l'instance NetScaler VPX, vous utilisez Citrix XenCenter, qui doit être installé sur une machine distante pouvant se connecter à l'hôte Hypervisor via le réseau.

Pour plus d'informations sur l'hyperviseur, consultez la documentation Citrix Hypervisor.

La figure suivante montre l'architecture de solution « bare metal » de l'instance NetScaler VPX sur Hypervisor.

Chiffre. Une instance NetScaler VPX sur Citrix Hypervisor



Conditions préalables à l'installation d'une instance NetScaler VPX sur Hypervisor

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Installez Hypervisor version 6.0 ou ultérieure sur du matériel répondant à la configuration minimale requise.
- Installez XenCenter sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Obtenez les fichiers de licence du dispositif virtuel. Pour plus d'informations sur les licences des appliances virtuelles, consultez le Guide des licences NetScaler.

Configuration matérielle requise pour l'hyperviseur

Le tableau suivant décrit la configuration matérielle minimale requise pour une plate-forme Hypervisor exécutant une instance NetScaler VPX.

Tableau 1 Configuration système minimale requise pour l'hyperviseur exécutant une instance VPX nCore

Composant	Exigences
UC	2 processeurs x86 64 bits ou plus avec assistance à la virtualisation (Intel-VT) activée. Pour exécuter l'instance NetScaler VPX, la prise en charge matérielle de la virtualisation doit être activée sur l'hôte de l'hyperviseur. Assurez-vous que l'option BIOS pour la prise en charge de la virtualisation n'est pas désactivée. Pour plus de détails, consultez la documentation du BIOS.
RAM	3 Go
Espace disque	Stockage connecté localement (PATA, SATA, SCSI) avec 40 Go d'espace disque. Remarque : L'installation de l'hyperviseur crée une partition de 4 Go pour le domaine de contrôle de l'hôte de l'hyperviseur. L'espace restant est disponible pour l'instance NetScaler VPX et d'autres machines virtuelles.
Carte d'interface réseau	Une carte réseau 1 Gbit/s ; recommandé : deux cartes réseau 1 Gbit/s

Pour plus d'informations sur l'installation de l'hyperviseur, consultez la documentation sur l'hyperviseur à l'adresse http://support.citrix.com/product/xens/.

Le tableau suivant répertorie les ressources informatiques virtuelles que l'hyperviseur doit fournir pour chaque dispositif virtuel VPX nCore.

Tableau 2 Ressources informatiques virtuelles minimales requises pour exécuter une instance nCore VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	2

> **Remarque :**
>
> Pour l'utilisation en production de l'instance NetScaler VPX, Citrix recommande de définir la priorité du processeur (dans les propriétés de la machine virtuelle) au niveau le plus élevé, afin d'améliorer le comportement de planification et la latence du réseau.

Configuration système requise pour XenCenter

XenCenter est une application cliente Windows. Il ne peut pas être exécuté sur la même machine que l'hôte de l'hyperviseur. Pour plus d'informations sur la configuration système minimale requise et l'installation de XenCenter, consultez les documents Hypervisor suivants :

- Configuration système requise
- Installer

Installez les instances NetScaler VPX sur Hypervisor à l'aide de XenCenter

Après avoir installé et configuré Hypervisor et XenCenter, vous pouvez utiliser XenCenter pour installer des dispositifs virtuels sur l'hyperviseur. Le nombre de dispositifs virtuels que vous pouvez installer dépend de la quantité de mémoire disponible sur le matériel qui exécute l'hyperviseur.

Pour installer des instances NetScaler VPX sur Hypervisor à l'aide de XenCenter, procédez comme suit :

1. Démarrez **XenCenter** sur votre poste de travail.
2. Dans le menu **Serveur**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un nouveau serveur**, dans la zone de texte du nom d'hôte, tapez l'adresse IP ou le nom DNS de l'hyperviseur auquel vous souhaitez vous connecter.
4. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur, puis cliquez sur **Se connecter**. Le nom de l'hyperviseur apparaît dans le volet de navigation avec un cercle vert, ce qui indique que l'hyperviseur est connecté.
5. Dans le volet de navigation, cliquez sur le nom de l'hyperviseur sur lequel vous souhaitez installer l'instance NetScaler VPX.
6. Dans le menu **VM**, cliquez sur **Importer**.
7. Dans la boîte de dialogue **Importer**, dans le nom du fichier d'importation, accédez à l'emplacement où vous avez enregistré le fichier image de l'instance `.xva` NetScaler VPX. Assurez-vous que l'option Machine virtuelle exportée est sélectionnée, puis cliquez sur **Suivant**.
8. Sélectionnez l'hyperviseur sur lequel vous souhaitez installer le dispositif virtuel, puis cliquez sur **Suivant**.

9. Sélectionnez le référentiel de stockage local dans lequel stocker le dispositif virtuel, puis cliquez sur Importer pour commencer le processus d'importation.
10. Vous pouvez ajouter, modifier ou supprimer les interfaces réseau virtuelles si nécessaire. Lorsque vous avez terminé, cliquez sur Suivant.
11. Cliquez sur **Terminer** pour terminer le processus d'importation.

    Remarque : Pour afficher l'état du processus d'importation, cliquez sur l'onglet **Journal** .
12. Si vous souhaitez installer un autre dispositif virtuel, répétez les étapes 5 à 11.

> **Remarque :**
>
> Après la configuration initiale de l'instance VPX, si vous souhaitez mettre à niveau l'appliance vers la dernière version logicielle, reportez-vous à la section Mise à niveau ou rétrogradation du logiciel système.

Configurer les instances VPX pour utiliser les interfaces réseau de virtualisation des E/S racine unique (SR-IOV)

May 5, 2023

Après avoir installé et configuré une instance NetScaler VPX sur Citrix Hypervisor, vous pouvez configurer l'appliance virtuelle pour utiliser les interfaces réseau SR-IOV.

Les cartes réseau suivantes sont prises en charge :

- Intel 82599 10 Go
- Intel X710 10 Go
- Intel XL710 40 Go

Limitations

Citrix Hypervisor ne prend pas en charge certaines fonctionnalités des interfaces SR-IOV. Les limitations des cartes réseau Intel 82599, Intel X710 et Intel XL710 sont répertoriées dans les sections suivantes.

Limitations pour la carte réseau Intel 82599

La carte réseau Intel 82599 ne prend pas en charge les fonctionnalités suivantes :

- Commutation de mode L2
- Clustering

- Partitionnement administrateur [mode VLAN partagé]
- Haute disponibilité [Actif - Mode actif]
- Cadres Jumbo
- Protocole IPv6 dans un environnement Cluster

Limitations pour les cartes réseau Intel X710 10G et Intel XL710 40G

Les cartes réseau Intel X710 10G et Intel XL710 40G présentent les limitations suivantes :

- Le mode L2 n'est pas pris en charge.
- Le partitionnement administrateur (mode VLAN partagé) n'est pas pris en charge.
- Dans un cluster, les trames Jumbo ne sont pas prises en charge lorsque la carte réseau XL710 est utilisée comme interface de données.
- La liste d'interfaces est réorganisée lorsque les interfaces sont déconnectées et reconnectées.
- Les configurations des paramètres d'interface telles que la vitesse, le mode duplex et les négociations automatiques ne sont pas prises en charge.
- Pour les cartes réseau Intel X710 10G et Intel XL710 40G, l'interface se présente comme une interface 40/x.
- Seules 16 interfaces Intel X710/XL710 SR-IOV peuvent être prises en charge sur une instance VPX.

> **Remarque :**
>
> Pour que les cartes réseau Intel X710 10G et Intel XL710 40G prennent en charge IPv6, activez le mode de confiance sur les fonctions virtuelles (VF) en tapant la commande suivante sur l'hôte Citrix Hypervisor :
>
> ```
> ## ip link set <PNIC> <VF> trust on
> ```
>
> **Exemple :**
>
> ```
> ## ip link set ens785f1 vf 0 trust on
> ```

Prérequis pour la carte réseau Intel 82599

Sur l'hôte Citrix Hypervisor, assurez-vous de :

- Ajoutez la carte réseau (NIC) Intel 82599 à l'hôte.
- Bloquez la liste du pilote `ixgbevf` en ajoutant l'entrée suivante au fichier **/etc/modprobe.d/blacklist.conf** :

  liste noire ixgbevf
- Activez les fonctions virtuelles (VF) SR-IOV en ajoutant l'entrée suivante au **fichier /etc/modprobe.d/ixgbe** :

  options ixgbe max_vfs =* <number_of_VFs>*

où ** <number_VFs>représente le nombre de VF SR-IOV que vous souhaitez créer.

- Vérifiez que SR-IOV est activé dans le BIOS.

> Remarque :
>
> La version 3.22.3 du pilote IXGBE est recommandée.

Attribuez des vF Intel 82599 SR-IOV à l'instance NetScaler VPX à l'aide de l'hôte Citrix Hypervisor

Pour attribuer un vFS Intel 82599 SR-IOV à une instance NetScaler VPX, procédez comme suit :

1. Sur l'hôte Citrix Hypervisor, utilisez la commande suivante pour attribuer les vF SR-IOV à l'instance NetScaler VPX :

   xe host-call-plugin plugin=iovirt host-uuid=*<Xen host UUID>* **fn=assign_free_vf args:uuid**=*<NetScaler VM UUID>* **args:ethdev**=*<interface name>* **args:mac=***<Mac addr>*

   Où :

   - *<Xen host UUID>* est l'UUID de l'hôte Citrix Hypervisor.
   - ** <NetScaler VM UUID>est l'UUID de l'instance NetScaler VPX.
   - *<interface name>* est l'interface pour les VF SR-IOV.
   - *<MAC address>* est l'adresse MAC du SR-IOV VF.

   > **Remarque**
   >
   > Spécifiez l'adresse MAC que vous souhaitez utiliser dans le paramètre Args:Mac=. S'il n'est pas spécifié, le script `iovirt` génère et attribue une adresse MAC de manière aléatoire. De plus, si vous souhaitez utiliser les VF SR-IOV en mode Agrégation de liens, assurez-vous de spécifier l'adresse MAC 00:00:00:00:00:00.

2. Démarrez l'instance NetScaler VPX.

Annulez l'attribution des vF Intel 82599 SR-IOV à l'instance NetScaler VPX à l'aide de l'hôte Citrix Hypervisor

Si vous avez attribué une VF SR-IOV incorrecte ou si vous souhaitez modifier une VF SR-IOV attribuée, vous devez annuler l'attribution et réattribuer les VF SR-IOV à l'instance NetScaler VPX.

Pour annuler l'attribution de l'interface réseau SR-IOV attribuée à une instance NetScaler VPX, procédez comme suit :

1. Sur l'hôte Citrix Hypervisor, utilisez la commande suivante pour attribuer les vF SR-IOV à l'instance NetScaler VPX et redémarrer l'instance NetScaler VPX :

xe host-call-plugin plugin=iovirt **host-uuid**=<*Xen_host_UUID*> **fn**=unassign_all **args:uuid**=<*Netscaler_VM_U*

Où :

- <*Xen_host_UUID*> - L'UUID de l'hôte Citrix Hypervisor.
- ** <Netscaler_VM_UUID>- L'UUID de l'instance NetScaler VPX

2. Démarrez l'instance NetScaler VPX.

Attribuez des vF Intel X710/XL710 SR-IOV à l'instance NetScaler VPX à l'aide de l'hôte Citrix Hypervisor

Pour attribuer une VF Intel X710/XL710 SR-IOV à l'instance NetScaler VPX, procédez comme suit :

1. Exécutez la commande suivante sur l'hôte Citrix Hypervisor pour créer un réseau.

```
xe network-create name-label=<network-name>
<!--NeedCopy-->
```

Exemple :

```
xe network-create name-label=SR-IOV-NIC-18 8ee59b73-7319-6998-cd69
   -b9fa3e8d7503
<!--NeedCopy-->
```

2. Déterminez l'identifiant unique universel (UUID) PIF de la carte réseau sur laquelle le réseau SR-IOV doit être configuré.

```
xe pif-list

            uuid ( RO)  : e2874343-f1de-1fa7-8fef-98547c348783
            device ( RO): eth18
currently-attached ( RO): true
              VLAN ( RO): -1
      network-uuid ( RO): f865bd85-44dd-b865-ab65-dcd6ae28c16e
<!--NeedCopy-->
```

3. Configurez le réseau en tant que réseau SR-IOV. La commande suivante renvoie également l'UUID du réseau SR-IOV nouvellement créé :

```
xe network-sriov-create network-uuid=<network-uuid> pif-uuid=<
   physical-pif-uuid>
<!--NeedCopy-->
```

Exemple :


```
xe network-sriov-create network-uuid=8ee59b73-7319-6998-cd69-
   b9fa3e8d7503 pif-uuid=e2874343-f1de-1fa7-8fef-98547
   c3487831629b44f-832a-084e-d67d-5d6d314d5e0f
<!--NeedCopy-->
```

Pour obtenir plus d'informations sur les paramètres réseau SR-IOV, exécutez la commande suivante :

```
[root@citrix-XS82-TOPO ~]# xe network-sriov-param-list uuid=1629
   b44f-832a-084e-d67d-5d6d314d5e0f

               uuid ( RO): 1629b44f-832a-084e-d67d-5d6d314d5e0f
      physical-PIF ( RO): e2874343-f1de-1fa7-8fef-98547c348783
       logical-PIF ( RO): 85d52771-5814-c62d-45fa-f37b536144ff
   requires-reboot ( RO): false
remaining-capacity ( RO): 32
<!--NeedCopy-->
```

4. Créez une interface virtuelle (VIF) et attachez-la à la machine virtuelle cible.

```
xe vif-create device=0 mac=b2:61:fc:ae:00:1d network-uuid=8ee59b73
   -7319-6998-cd69-b9fa3e8d7503 vm-uuid=b507e8a6-f5ca-18eb-561d
   -308218a9dd68
3e1e2e58-b2ad-6dc0-61d4-1d149c9c6466
<!--NeedCopy-->
```

> REMARQUE : Le numéro d'index de carte réseau de la machine virtuelle doit commencer par 0.

Utilisez la commande suivante pour rechercher l'UUID de la machine virtuelle :

```
[root@citrix-XS82-TOPO ~]# xe vm-list
uuid ( RO): b507e8a6-f5ca-18eb-561d-308218a9dd68
 name-label ( RW): sai-vpx-1
power-state ( RO): halted
<!--NeedCopy-->
```

Supprimez les vF Intel X710/XL710 SR-IOV de l'instance NetScaler à l'aide de l'hôte Citrix Hypervisor

Pour supprimer un processeur Intel X710/XL710 SR-IOV VF d'une instance NetScaler VPX, procédez comme suit :

1. Copiez l'UUID du VIF que vous souhaitez détruire.

2. Exécutez la commande suivante sur l'hôte Citrix Hypervisor pour détruire le VIF.

```
xe vif-destroy uuid=<vif-uuid>
<!--NeedCopy-->
```

Exemple :

```
[root@citrix-XS82-TOPO ~]# xe vif-destroy uuid=3e1e2e58-b2ad-6dc0
   -61d4-1d149c9c6466
<!--NeedCopy-->
```

Configuration de l'agrégation de liens sur l'interface SR-IOV

Pour utiliser les fonctions virtuelles (VF) du SR-IOV en mode d'agrégation de liens, vous devez désactiver la vérification des usurpations pour les fonctions virtuelles que vous avez créées.

Sur l'hôte Citrix Hypervisor, utilisez la commande suivante pour désactiver la vérification des usurpations :

ip link set *<interface_name>* **vf** *<VF_id>* **spoofchk** off

Où :

- <interface_name> est le nom de l'interface.
- <VF_id> est l'ID de la fonction virtuelle.

Après avoir désactivé la vérification des usurpations pour toutes les fonctions virtuelles que vous avez créées, redémarrez l'instance NetScaler VPX et configurez l'agrégation de liens. Pour obtenir des instructions, voir Configurer l'agrégation de liens.

> **Important**
>
> Lorsque vous attribuez les VF SR-IOV à l'instance NetScaler VPX, assurez-vous de spécifier l'adresse MAC 00:00:00:00:00:00 pour les VF.

Configurer VLAN sur l'interface SR-IOV

Vous pouvez configurer le VLAN sur les fonctions virtuelles du SR-IOV. Pour obtenir des instructions, consultez la section Configuration d'un VLAN.

> **Important**
>
> Assurez-vous que l'hôte Citrix Hypervisor ne contient pas de paramètres VLAN pour l'interface VF.

Installation d'une instance NetScaler VPX sur VMware ESX

May 5, 2023

Avant d'installer des instances NetScaler VPX sur VMware ESX, assurez-vous que VMware ESX Server est installé sur une machine disposant de ressources système adéquates. Pour installer une instance NetScaler VPX sur VMware ESXi, vous utilisez le client VMware vSphere. Le client ou l'outil doit être installé sur une machine distante pouvant se connecter à VMware ESX via le réseau.

Cette section inclut les rubriques suivantes :

- Composants requis
- Installation d'une instance NetScaler VPX sur VMware ESX

> **Important :**
>
> Vous ne pouvez pas installer VMware Tools standard ni mettre à niveau la version de VMware Tools disponible sur une instance NetScaler VPX. Les outils VMware pour une instance NetScaler VPX sont fournis dans le cadre de la version logicielle NetScaler.

Composants requis

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Installez VMware ESX sur du matériel qui répond à la configuration minimale requise.
- Installez VMware Client sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez un commutateur virtuel et connectez la carte réseau physique au commutateur virtuel.
- Ajoutez un groupe de ports et connectez-le au commutateur virtuel.
- Attachez le groupe de ports à la machine virtuelle.
- Obtenir des fichiers de licence VPX. Pour plus d'informations sur les licences d'instance NetScaler VPX, consultez la section Vue d'ensemble des licences.

Configuration matérielle requise pour VMware ESX

Le tableau suivant décrit la configuration système minimale requise pour les serveurs VMware ESX exécutant l'appliance virtuelle NetScaler VPX nCore.

Tableau 1. Configuration système minimale requise pour un serveur VMware ESX exécutant une instance NetScaler VPX

Composant	Exigences
UC	2 processeurs x86 64 bits ou plus avec assistance à la virtualisation (Intel-VT) activée. Pour exécuter une instance NetScaler VPX, la prise en charge matérielle de la virtualisation doit être activée sur l'hôte VMware ESX. Assurez-vous que l'option BIOS pour la prise en charge de la virtualisation n'est pas désactivée. Pour plus d'informations, consultez la documentation de votre BIOS. À partir de la version 13.1 de NetScaler, l'instance NetScaler VPX sur l'hyperviseur VMware ESXi prend en charge les processeurs AMD.
RAM	2 Go VPX. Pour les déploiements critiques, nous ne recommandons pas 2 Go de RAM pour VPX car le système fonctionne dans un environnement où la mémoire est limitée. Cela peut entraîner des problèmes liés à l'échelle, aux performances ou à la stabilité. 4 Go de RAM ou 8 Go de RAM sont recommandés.
Espace disque	20 Go de plus que la configuration serveur minimale requise par VMware pour configurer ESXi. Consultez la documentation VMware pour connaître la configuration minimale requise pour les serveurs.
Réseau	Une carte réseau (NIC) 1 Gbit/s ; deux cartes réseau 1 Gbit/s recommandées

Pour plus d'informations sur l'installation de VMware ESX, reportez-vous à la section http://www.vmware.com/.

Pour l'interface réseau SR-IOV ou la prise en charge du relais PCI, assurez-vous que les processeurs et paramètres suivants sont activés :

- Processeurs Intel compatibles avec Intel-VT
- Processeurs AMD compatibles avec AMD-V
- L'unité de gestion de la mémoire I/O (IOMMU) ou SR-IOV est activée dans le BIOS

Les cartes réseau suivantes sont prises en charge en mode SR-IOV :

- Carte réseau Mellanox ConnectX-4, à partir de la version 13.1-42.x de NetScaler
- Carte réseau Intel 82599

Le tableau suivant répertorie les ressources informatiques virtuelles que le serveur VMware ESX doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 2 Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
Mémoire	4 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans ESX, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> **Remarque :**
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production du dispositif virtuel VPX, l'allocation de mémoire complète doit être réservée. Des cycles de processeur (en MHz) égaux au moins à la vitesse d'un cœur de processeur de l'ESX doivent être réservés.

Configuration système requise pour VMware vSphere Client

VMware vSphere est une application cliente qui peut s'exécuter sur les systèmes d'exploitation Windows et Linux. Il ne peut pas être exécuté sur la même machine que le serveur VMware ESX. Le tableau suivant décrit la configuration minimale requise.

Tableau 3. Configuration système minimale requise pour l'installation de VMware vSphere Client

Composant	Exigences
OS	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « Matrices de compatibilité vSphere » à l'adresse http://kb.vmware.com/.

Composant	Exigences
UC	750 MHz ; 1 gigahertz (GHz) ou plus rapide recommandé
RAM	1 Go. 2 Go recommandés
NIC (NIC)	Carte réseau 100 Mbit/s ou plus rapide

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Il ne peut pas être exécuté sur la même machine que le serveur VMware ESX. Le tableau suivant décrit la configuration minimale requise.

Tableau 4. Configuration minimale requise pour l'installation d'outils OVF

Composant	Exigences
OS	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
NIC (NIC)	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.

Téléchargement des fichiers de configuration de NetScaler VPX

Le package de configuration de l'instance NetScaler VPX pour VMware ESX respecte la norme de format Open Virtual Machine (OVF). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous ne possédez pas de compte Citrix, accédez à la page d'accueil à l'adresse http://www.citrix.com, cliquez sur le **lien Nouveaux utilisateurs** et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

Citrix.com > **Téléchargements > NetScaler > Appliances virtuelles.**

Copiez les fichiers suivants sur une station de travail située sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (par exemple, NSVPX-ESX-13.0-71.44_nc_64-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (par exemple, NSVPX-ESX-13.0-71.44_nc_64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (par exemple, NSVPX-ESX-13.0-71.44_nc_64.mf)

Installation d'une instance NetScaler VPX sur VMware ESX

Après avoir installé et configuré VMware ESX, vous pouvez utiliser le client VMware vSphere pour installer des dispositifs virtuels sur le serveur VMware ESX. Le nombre de dispositifs virtuels que vous pouvez installer dépend de la quantité de mémoire disponible sur le matériel qui exécute VMware ESX.

Pour installer des instances NetScaler VPX sur VMware ESX à l'aide de VMware vSphere Client, procédez comme suit :

1. Démarrez le client VMware vSphere sur votre station de travail.
2. Dans la zone de texte **Adresse IP/Nom**, tapez l'adresse IP du serveur VMware ESX auquel vous souhaitez vous connecter.
3. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur Connexion.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
5. **Dans la boîte de dialogue**Déployer le modèle OVF**, dans**Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers de configuration de l'instance NetScaler VPX, sélectionnez le fichier .ovf et cliquez sur Suivant.**
6. Mappez les réseaux affichés dans le modèle OVF du dispositif virtuel aux réseaux que vous avez configurés sur l'hôte ESX. Cliquez sur **Suivant** pour commencer à installer un dispositif virtuel sur VMware ESX. Une fois l'installation terminée, une fenêtre contextuelle vous informe de la réussite de l'installation.
7. Vous êtes maintenant prêt à démarrer l'instance NetScaler VPX. **Dans le volet de navigation, sélectionnez l'instance NetScaler VPX que vous avez installée et, dans le menu contextuel, sélectionnez Power On.**
8. Une fois la machine virtuelle démarrée, à partir de la console, configurez les adresses IP, Netmask et Gateway de NetScaler. Lorsque vous avez terminé la configuration, sélectionnez l'option **Enregistrer et quitter** dans la console.
9. Pour installer un autre dispositif virtuel, répétez les étapes 6 à 8.

> **Remarque :**
>
> Par défaut, l'instance NetScaler VPX utilise les interfaces réseau E1000.

> Après l'installation, vous pouvez utiliser le client vSphere ou vSphere Web Client pour gérer les dispositifs virtuels sur VMware ESX.
>
> Pour que la fonctionnalité de balisage de VLAN fonctionne, sur VMware ESX, définissez l'ID VLAN du groupe de ports sur Tous (4095) sur le vSwitch du serveur VMware ESX. Pour plus d'informations sur la définition d'un ID VLAN sur le vSwitch de VMware ESX server, reportez-vous à la section http://www.vmware.com/pdf/esx3_vlan_wp.pdf.

Migrer une instance NetScaler VPX à l'aide de VMware vMotion

Vous pouvez migrer une instance NetScaler VPX à l'aide de VMware vSphere vMotion.

Suivez ces instructions d'utilisation :

- VMware ne prend pas en charge la fonctionnalité VMotion sur les machines virtuelles configurées avec les interfaces PCI Passthrough et SR-IOV.
- Les interfaces prises en charge sont E1000 et VMXNET3. Pour utiliser vMotion sur votre instance VPX, assurez-vous que l'instance est configurée avec une interface prise en charge.
- Pour plus d'informations sur la façon de migrer une instance à l'aide de VMware VMotion, consultez la documentation VMware.

Configurer une instance NetScaler VPX pour utiliser l'interface réseau VMXNET3

May 5, 2023

Après avoir installé et configuré l'instance NetScaler VPX sur VMware ESX, vous pouvez utiliser le client Web VMware vSphere pour configurer l'appliance virtuelle afin qu'elle utilise les interfaces réseau VMXNET3.

Pour configurer les instances NetScaler VPX afin qu'elles utilisent les interfaces réseau VMXNET3 à l'aide du client Web VMware vSphere :

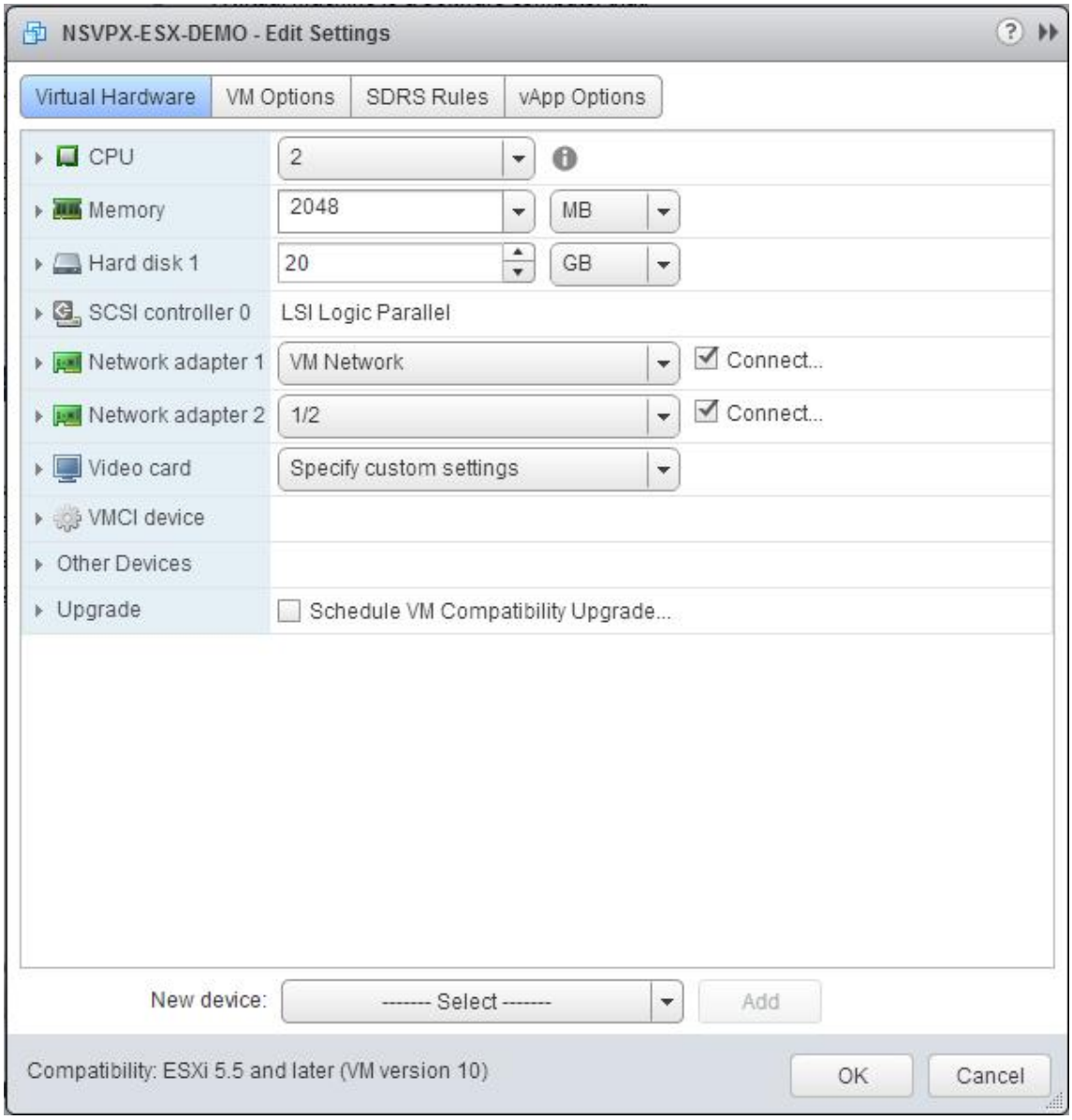
1. Dans vSphere Web Client, sélectionnez Hôtes et clusters.
2. Mettez à niveau le paramètre de compatibilité de l'instance NetScaler VPX vers ESX, comme suit :

   a. Éteignez l'instance NetScaler VPX.

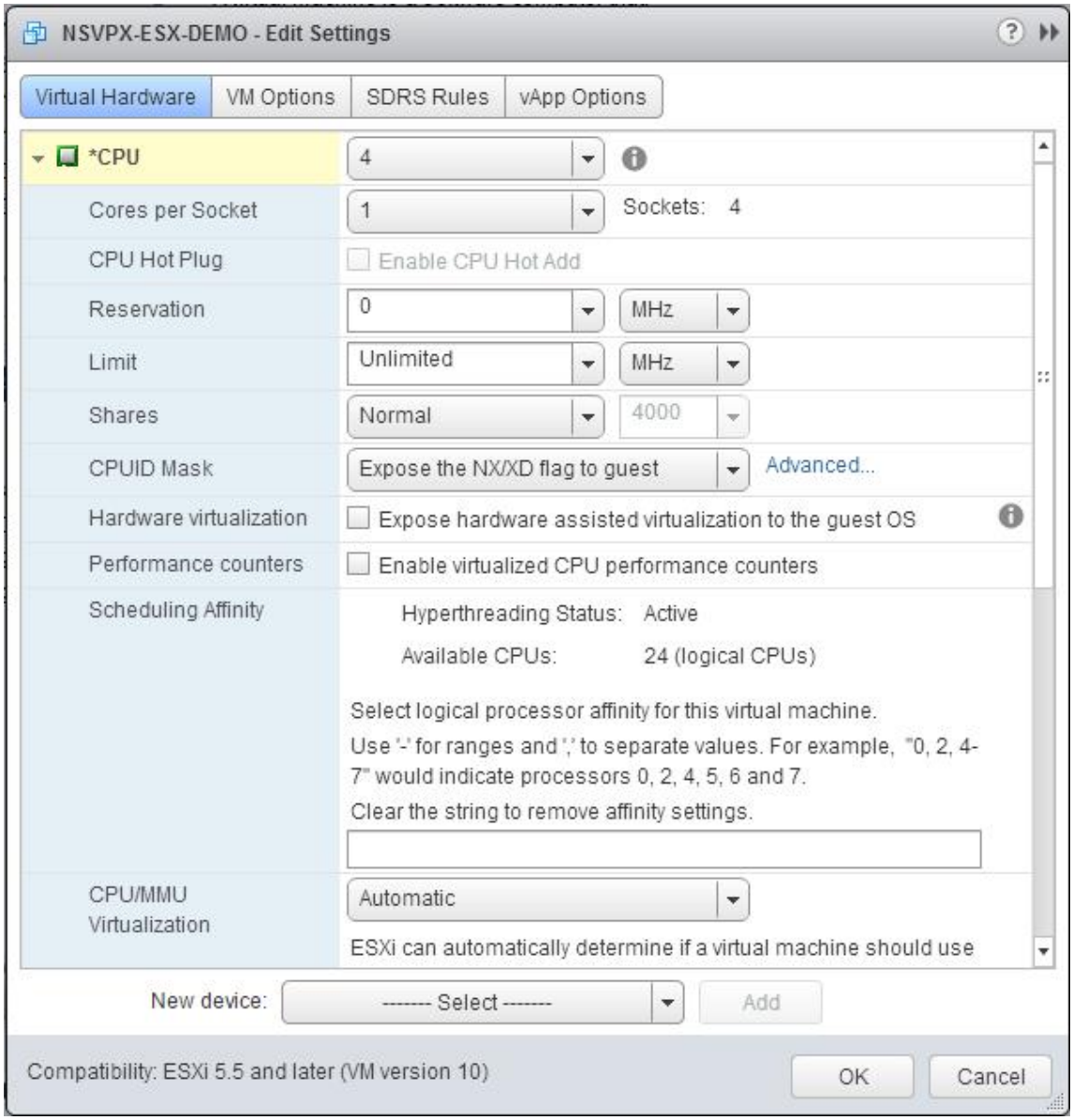
   b. Cliquez avec le bouton droit sur l'instance NetScaler VPX et sélectionnez Compatibilité > Mettre à niveau la compatibilité des machines virtuelles.

   c. Dans la boîte de dialogue Configurer la compatibilité des machines virtuelles, sélectionnez ESXi 5.5 et versions ultérieures dans la liste déroulante Compatible avec, puis cliquez sur OK.

3. Cliquez avec le bouton droit sur l'instance NetScaler VPX et cliquez sur Modifier les paramètres.



4. Dans la boîte de dialogue <virtual_appliance> - Edit Settings, cliquez sur la section CPU.



5. Dans la section CPU, mettez à jour les éléments suivants :

   - Nombre de processeurs
   - Nombre de prises
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

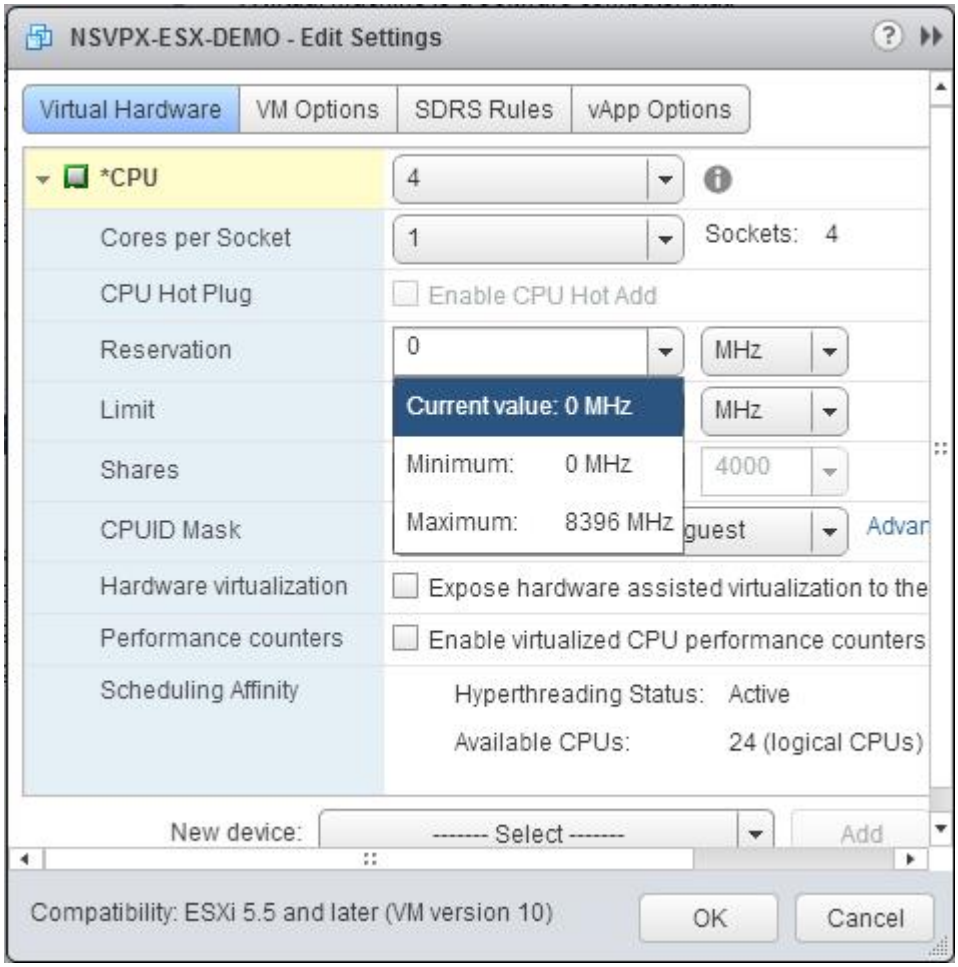
   a. Dans la liste déroulante CPU, sélectionnez le nombre de CPU à attribuer à l'appliance virtuelle.

   b. Dans la liste déroulante Cores par socket, sélectionnez le nombre de sockets.

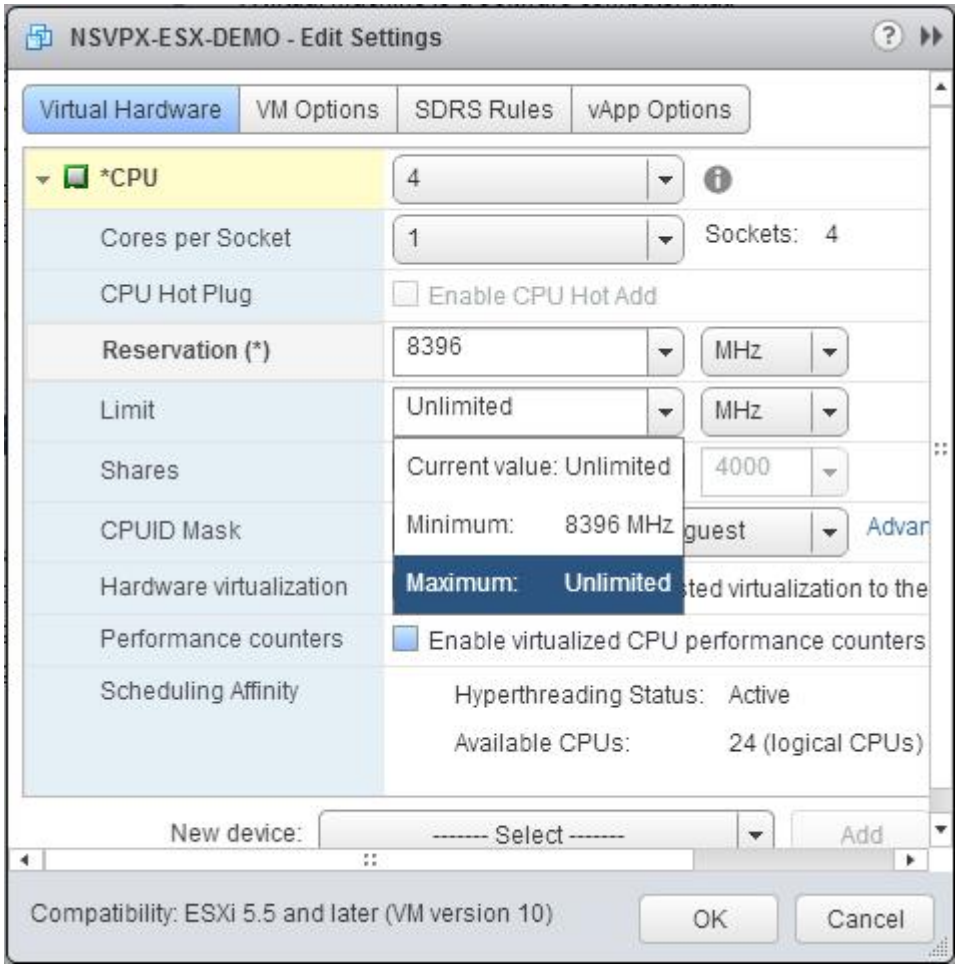
c. (Facultatif) Dans le champ CPU Hot Plug, activez ou désactivez la case à cocher Activer l'ajout à chaud du processeur.

Remarque : Citrix recommande d'accepter la valeur par défaut (désactivée).

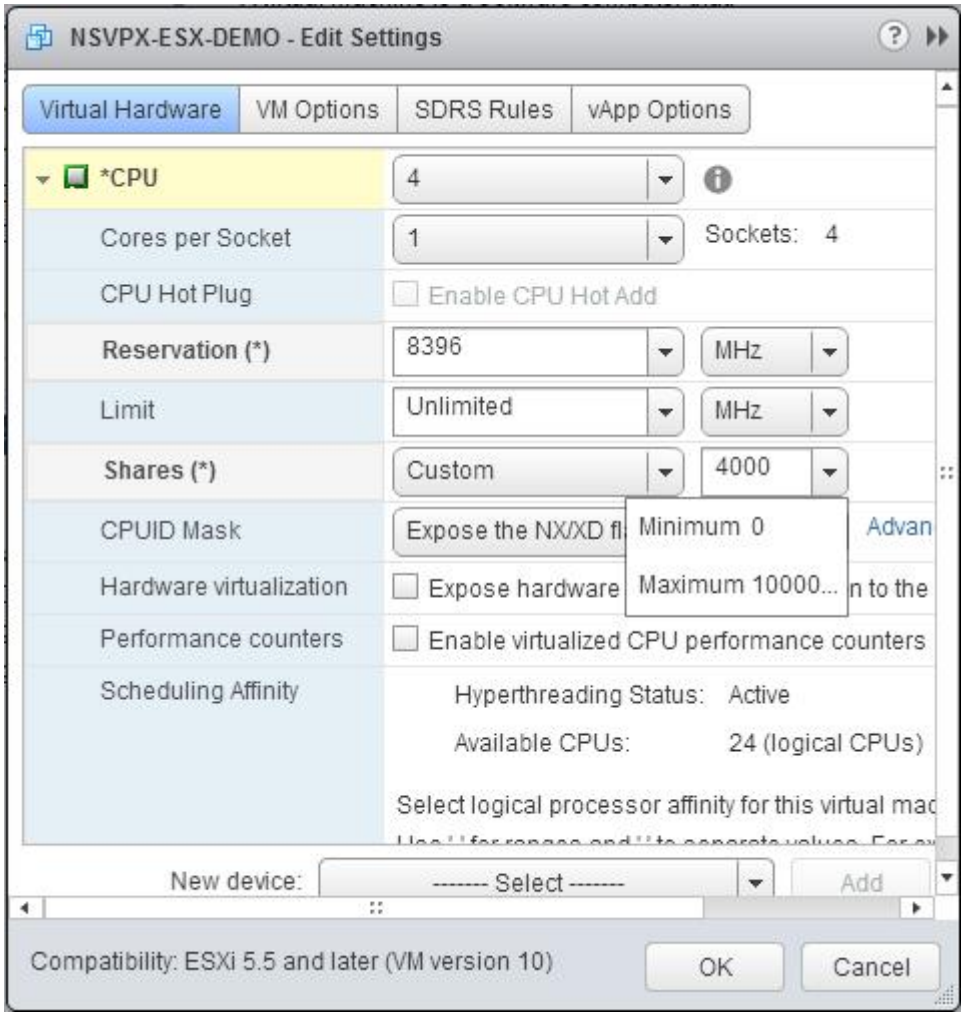
d. Dans la liste déroulante Réservation, sélectionnez le nombre qui est affiché comme valeur maximale.



e. Dans la liste déroulante Limite, sélectionnez le nombre affiché comme valeur maximale.



f. Dans les listes déroulantes Parts, sélectionnez Personnalisé et le nombre affiché comme valeur maximale.



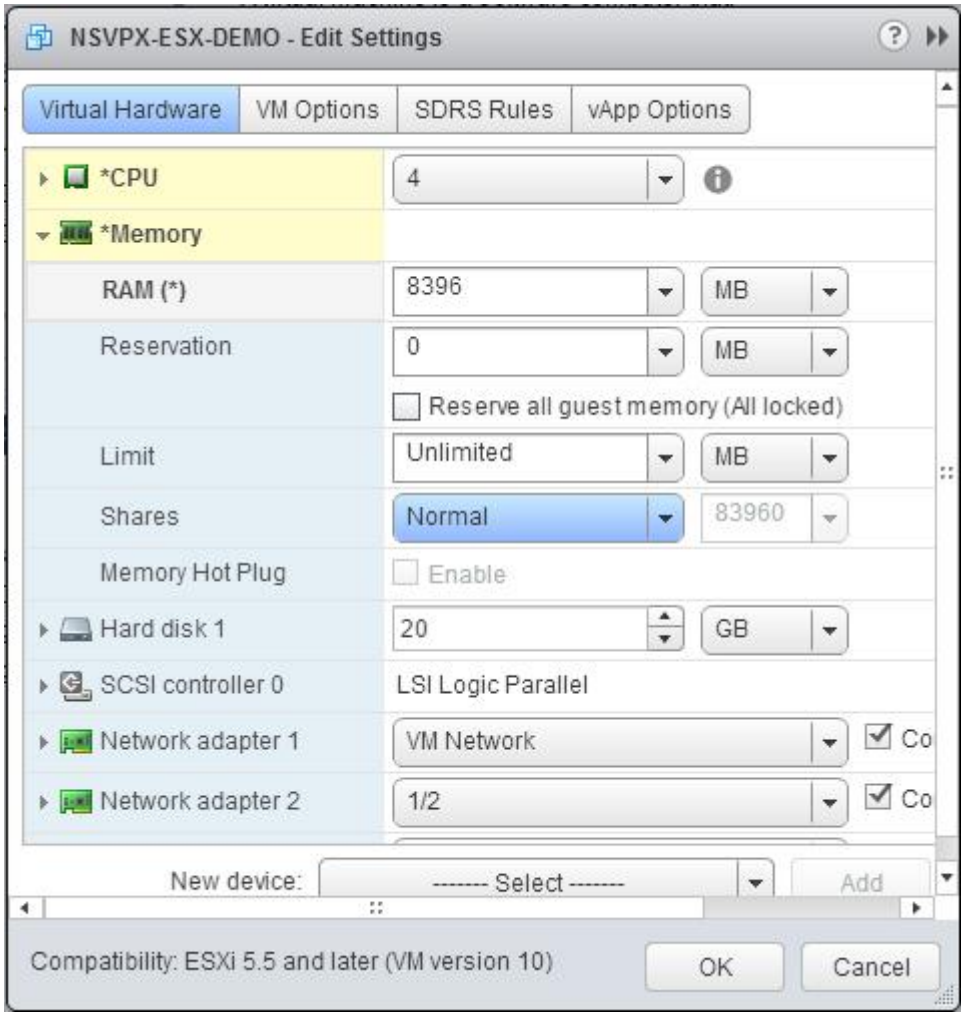
6. Dans la section Mémoire, mettez à jour les éléments suivants :

   - Taille de la mémoire vive
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

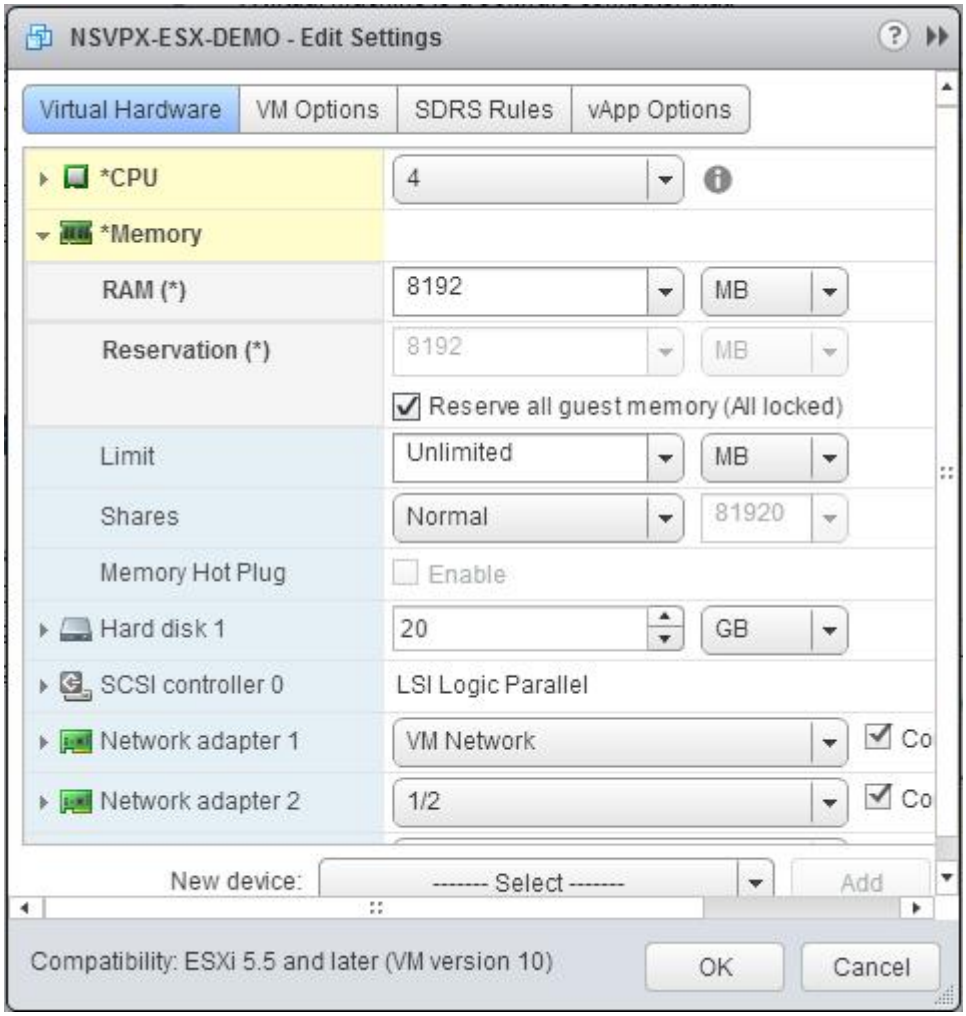
   a. Dans la liste déroulante RAM, sélectionnez la taille de la RAM. Il doit s'agir du nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de processeurs virtuels est de 4, la RAM doit être de 4 x 2 Go = 8 Go.

   Remarque : Pour une édition avancée ou Premium de l'appliance NetScaler VPX, assurez-vous d'allouer 4 Go de RAM à chaque processeur virtuel. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.

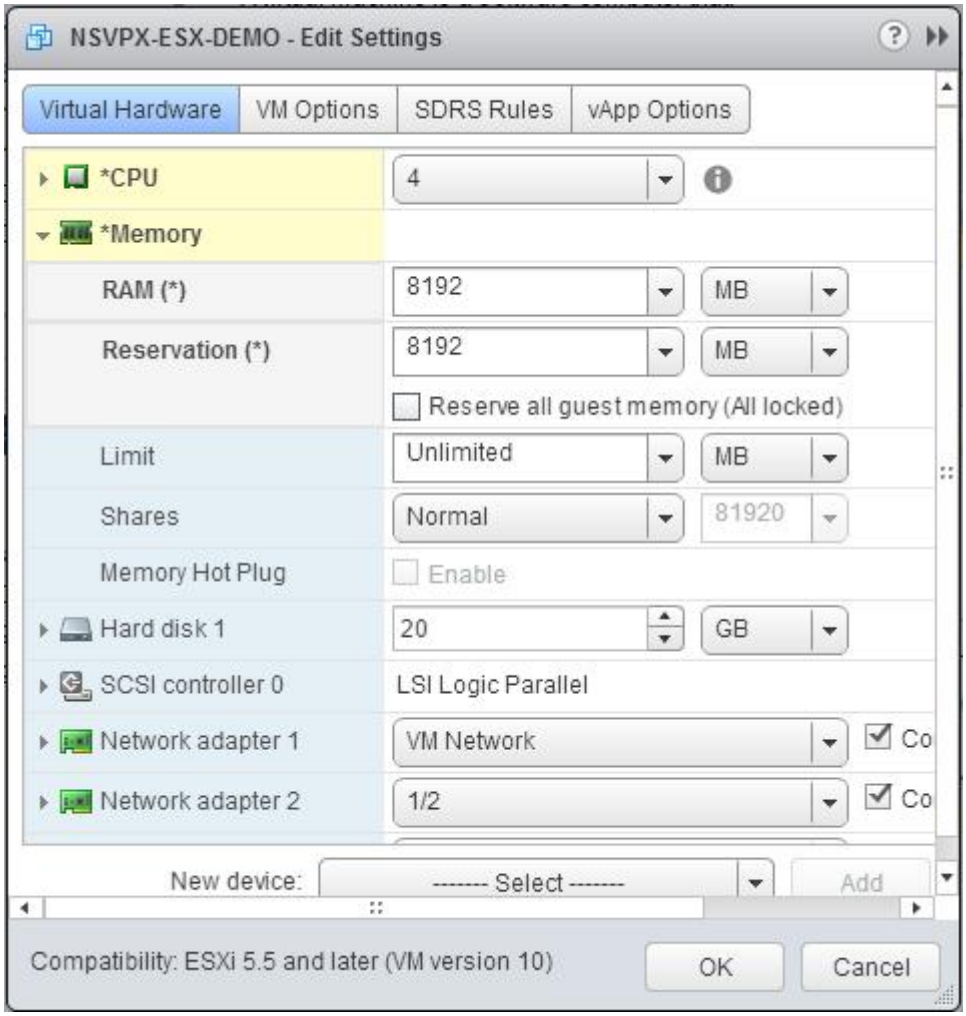


b. Dans la liste déroulante Réservation, entrez la valeur de la réservation mémoire et activez la case à cocher Réserver toute la mémoire invitée (Tout verrouillé). La réservation de mémoire doit correspondre au nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de processeurs virtuels est de 4, la réservation de mémoire doit être de 4 x 2 Go = 8 Go.

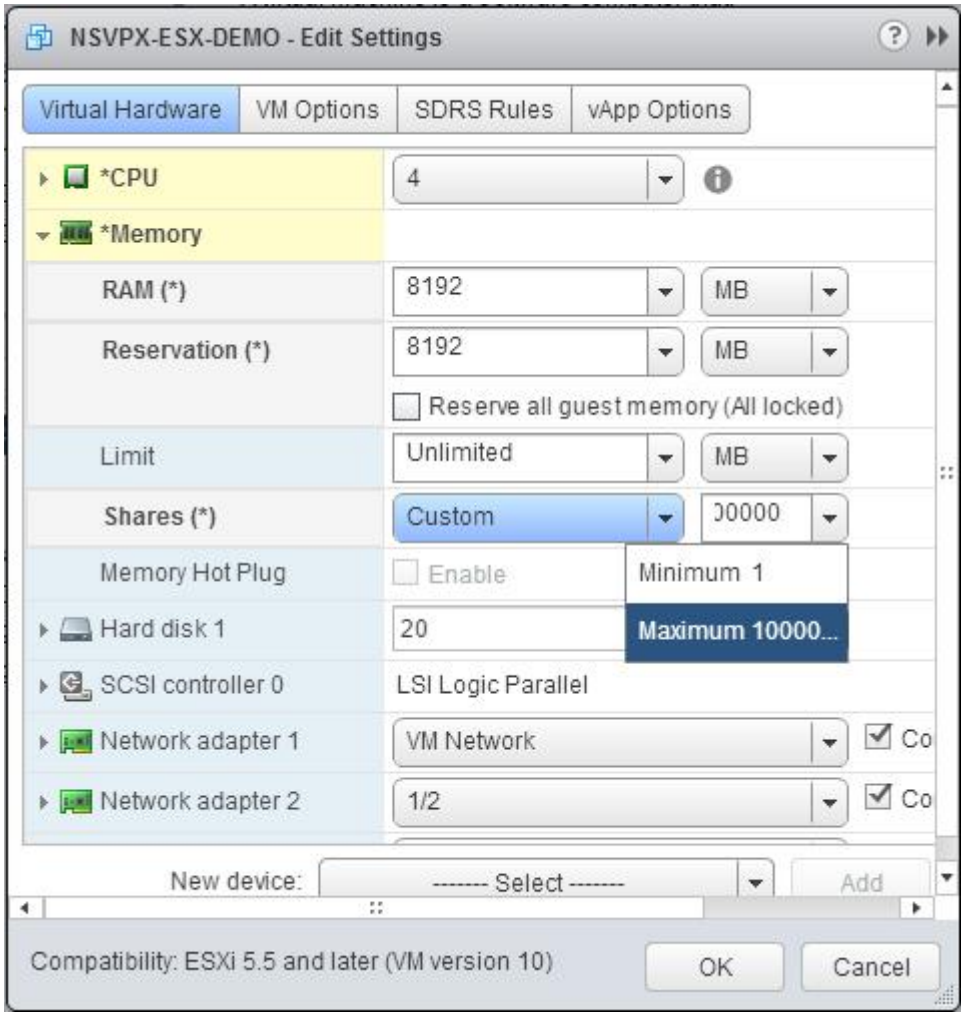
Remarque : Pour une édition avancée ou Premium de l'appliance NetScaler VPX, assurez-vous d'allouer 4 Go de RAM à chaque processeur virtuel. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.



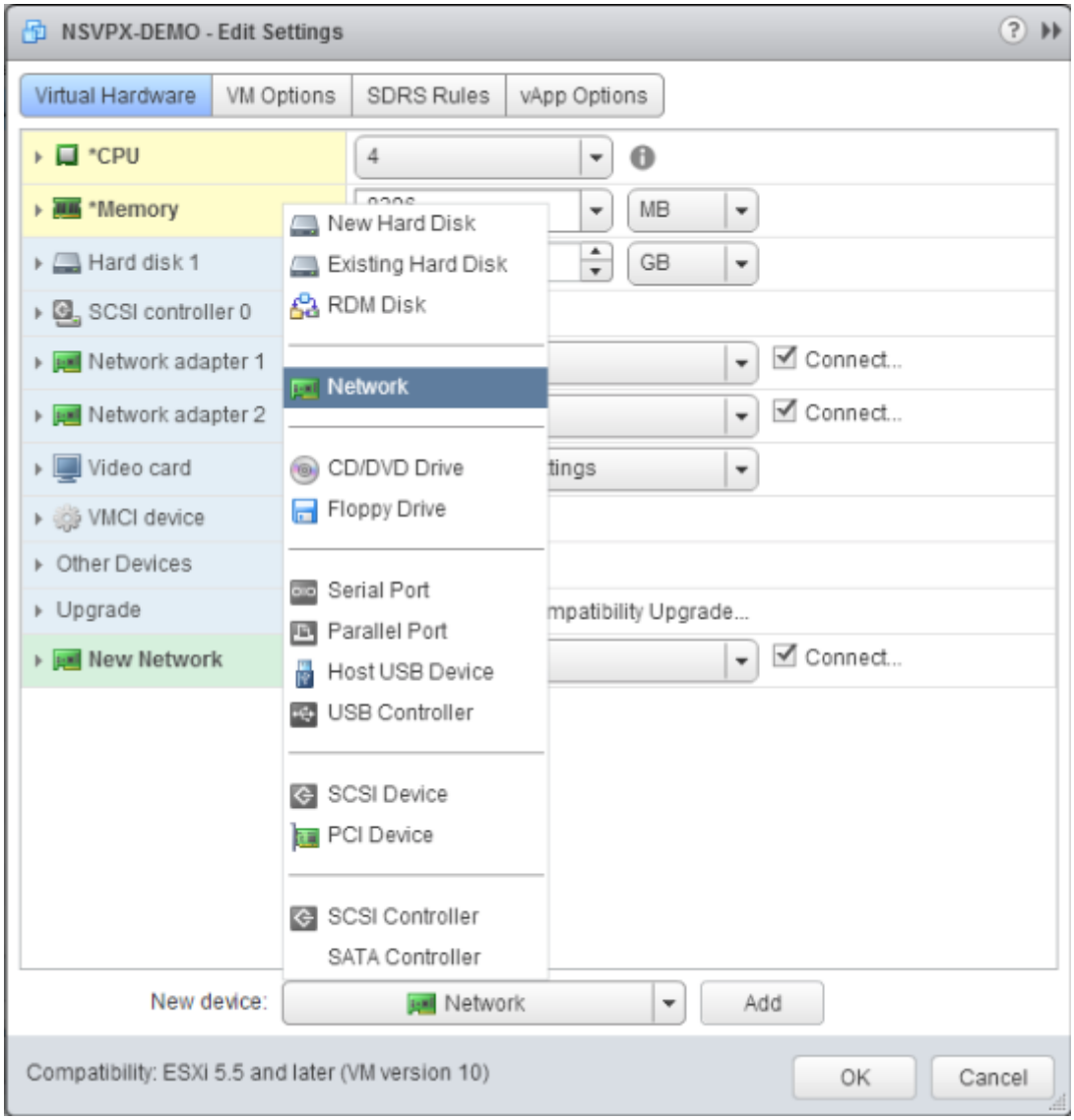
c. Dans la liste déroulante Limite, sélectionnez le nombre affiché comme valeur maximale.



d. Dans les listes déroulantes Partages, sélectionnez Personnalisé et le nombre qui s'affiche comme valeur maximale.



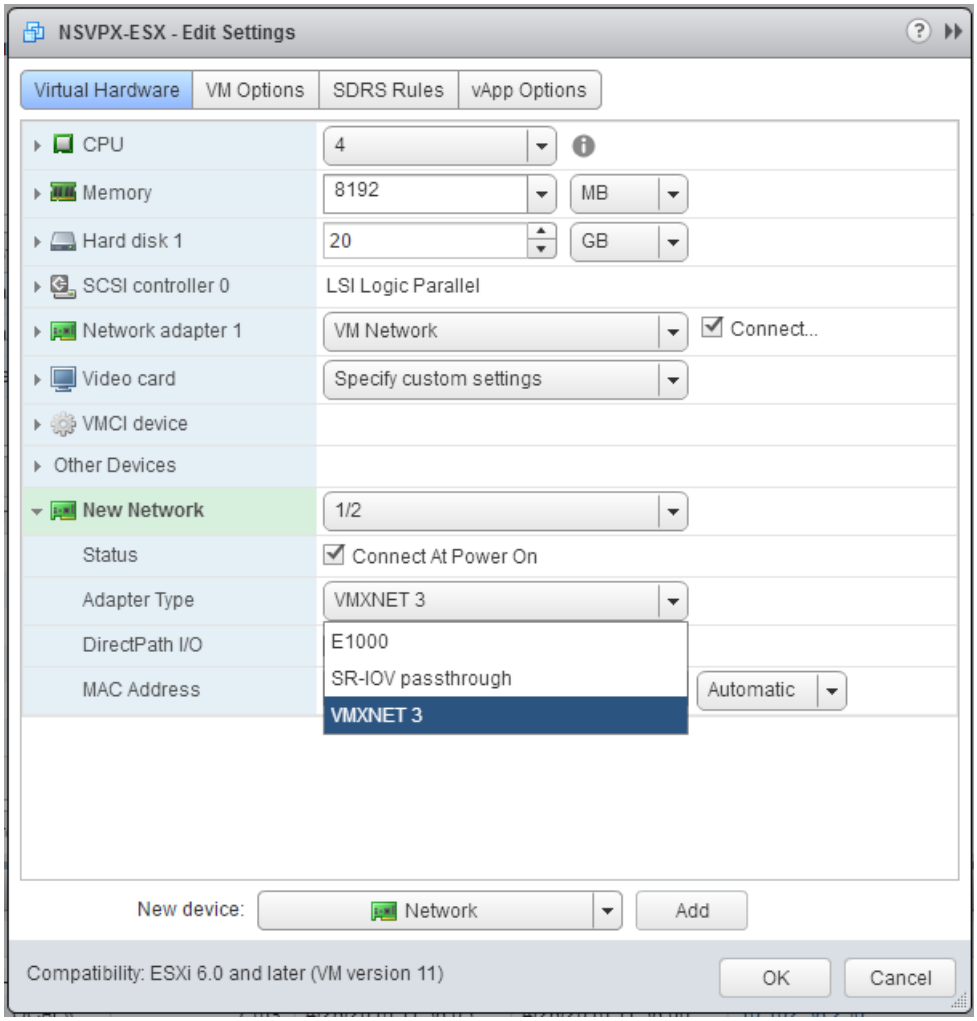
7. Ajoutez une interface réseau VMXNET3. Dans la liste déroulante Nouvel appareil, sélectionnez Réseau, puis cliquez sur Ajouter.



8. Dans la section Nouveau réseau, dans la liste déroulante, sélectionnez l'interface réseau et procédez comme suit :

   a. Dans la liste déroulante Type d'adaptateur, sélectionnez VMXNET3.

   > **Important**
   >
   > L'interface réseau E1000 par défaut et VMXNET3 ne peuvent pas coexister, assurez-vous de supprimer l'interface réseau E1000 et d'utiliser VMXNET3 (0/1) comme interface de gestion.



9. Cliquez sur OK.
10. Allumez l'instance NetScaler VPX.
11. Une fois que l'instance NetScaler VPX est activée, vous pouvez utiliser la commande suivante pour vérifier la configuration :

    > Afficher le résumé de l'interface

La sortie doit afficher toutes les interfaces que vous avez configurées :

```
> show interface summary
-------------------------------------------------------------------------------

      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------------

1     0/1        1500       00:0c:29:89:1d:0e  NetScaler Vir...rface,
    VMXNET3
```



```
6  2     1/1        9000       00:0c:29:89:1d:18    NetScaler Vir...rface,
       VMXNET3
7  3     1/2        9000       00:0c:29:89:1d:22    NetScaler Vir...rface,
       VMXNET3
8  4     LO/1       9000       00:0c:29:89:1d:0e    Netscaler Loopback
      interface
```

> **Remarque**
>
> Après avoir ajouté une interface VMXNET3 et redémarré l'appliance NetScaler VPX, l'hyperviseur VMware ESX peut modifier l'ordre dans lequel la carte réseau est présentée à l'appliance VPX. Par conséquent, la carte réseau 1 peut ne pas toujours rester 0/1, ce qui entraîne une perte de connectivité de gestion à l'appliance VPX. Pour éviter ce problème, modifiez le réseau virtuel de la carte réseau en conséquence.
>
> Il s'agit d'une limitation de l'hyperviseur VMware ESX.

Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV

May 5, 2023

Après avoir installé et configuré l'instance NetScaler VPX sur VMware ESX, vous pouvez utiliser le client Web VMware vSphere pour configurer l'appliance virtuelle afin qu'elle utilise des interfaces réseau d'E/S à racine unique et de virtualisation (SR-IOV).

Limitations

Un NetScaler VPX configuré avec l'interface réseau SR-IOV présente les limites suivantes :

- Les fonctionnalités suivantes ne sont pas prises en charge sur les interfaces SR-IOV utilisant la carte réseau Intel 82599 10G sur ESX VPX :
  - Commutation de mode L2
  - Agrégation de liens statiques et LACP
  - Clustering
  - Partitionnement administrateur [mode VLAN partagé]
  - Haute disponibilité [Actif - Mode actif]
  - Cadres Jumbo
  - IPv6
- Les fonctionnalités suivantes ne sont pas prises en charge sur l'interface SR-IOV avec une carte réseau Intel 82599 10G sur KVM VPX :

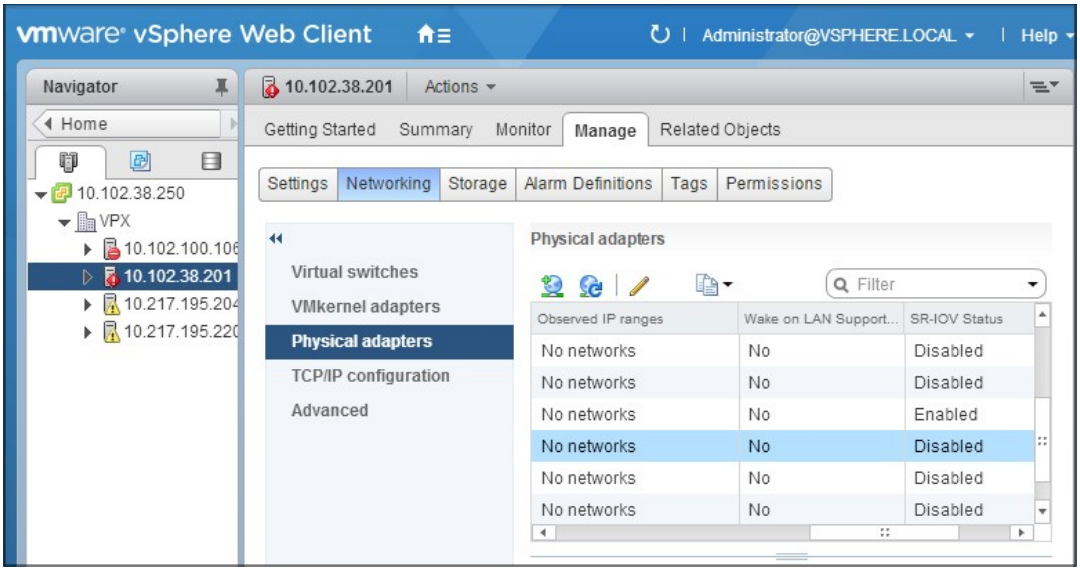
- Agrégation de liens statiques et LACP
- Commutation de mode L2
- Clustering
- Partitionnement administrateur [mode VLAN partagé]
- Haute disponibilité [Mode actif — Actif]
- Cadres Jumbo
- IPv6
- La configuration VLAN sur l'interface Hypervisor for SR-IOV VF via `ip link` commande n'est pas prise en charge

Conditions préalables

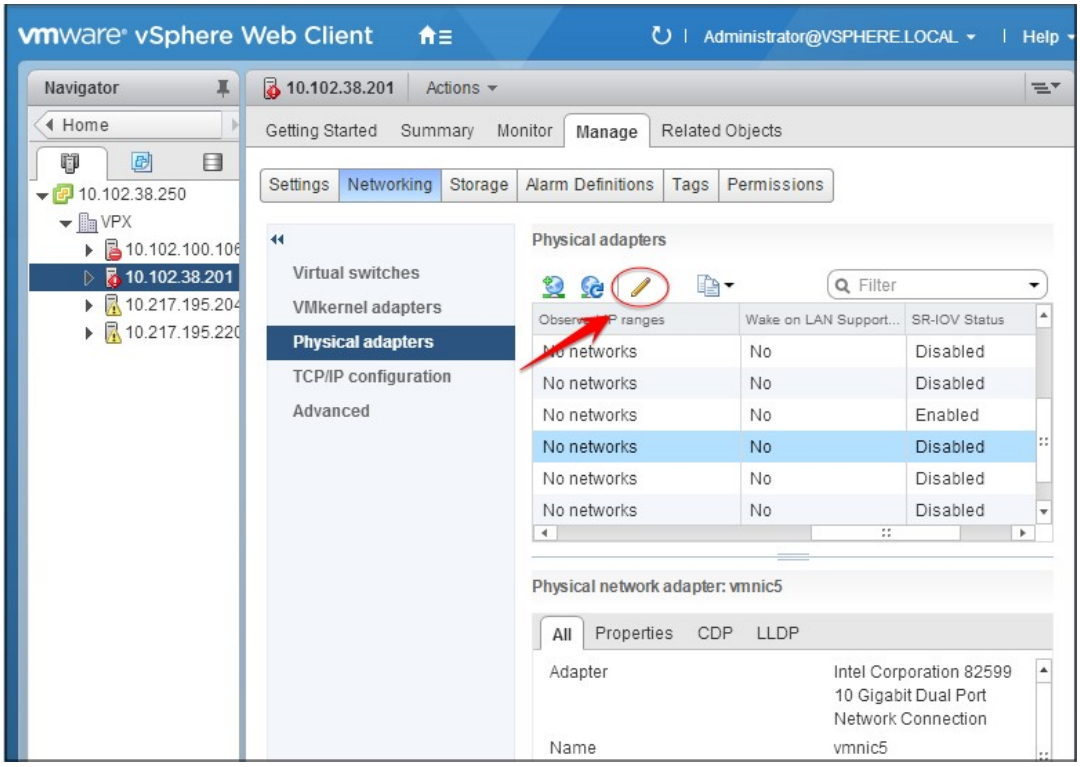
- Assurez-vous d'ajouter l'une des cartes réseau suivantes à l'hôte ESX :
  - Carte réseau Intel 82599, pilote IXGBE version 3.7.13.7.14iov ou ultérieure est recommandée.
  - Carte réseau Mellanox ConnectX-4
- Activez SR-IOV sur l'adaptateur physique de l'hôte.

  Suivez cette procédure pour activer SR-IOV sur l'adaptateur physique hôte :

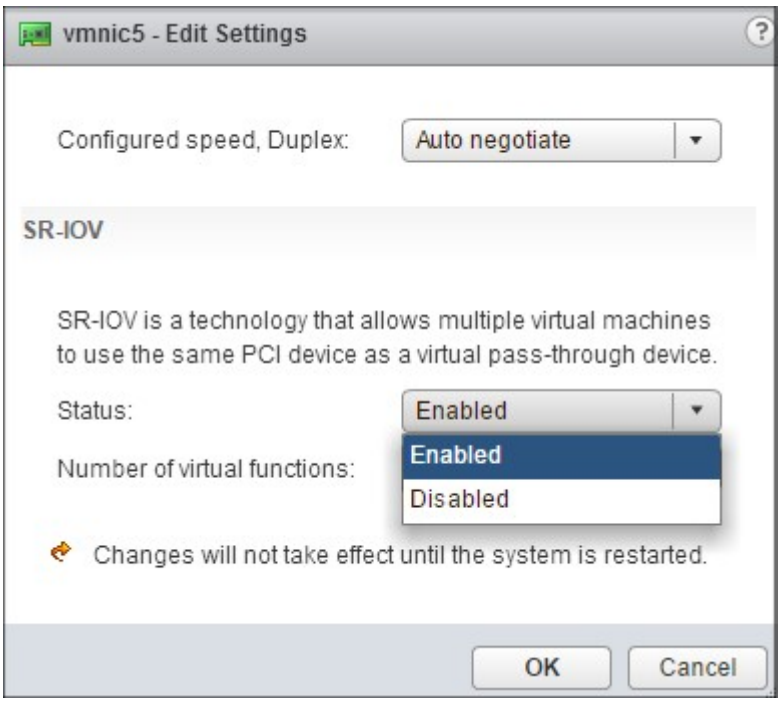
  1. Dans vSphere Web Client, accédez à l'hôte.
  2. Dans l'onglet **Gérer > Réseau**, sélectionnez **Adaptateurs physiques**. Le champ Statut SR-IOV indique si une carte physique prend en charge SR-IOV.



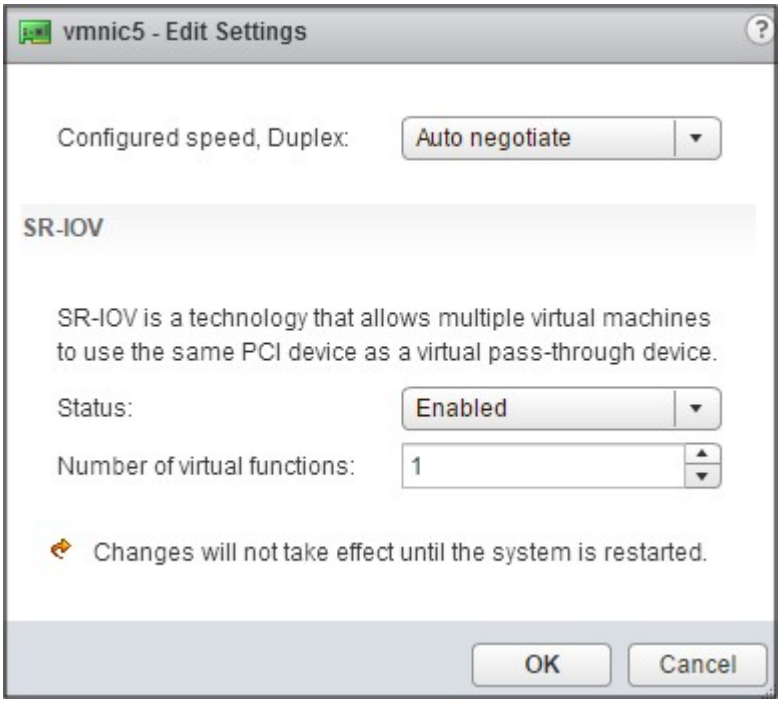
  3. Sélectionnez l'adaptateur physique, puis cliquez sur l'icône en forme de crayon pour ouvrir la boîte de dialogue **Modifier les paramètres** .



4. Sous SR-IOV, sélectionnez **Activé** dans la liste déroulante **Statut** .



5. Dans le champ **Nombre de fonctions virtuelles**, entrez le nombre de fonctions virtuelles que vous souhaitez configurer pour la carte.



6. Cliquez sur **OK**.
7. Redémarrez l'hôte.

- Créez un commutateur virtuel distribué (DVS) et `Portgroups`. Pour obtenir des instructions, reportez-vous à la documentation VMware.

> **Remarque**
>
> Citrix a qualifié la configuration SR-IOV sur DVS et `Portgroups` uniquement.

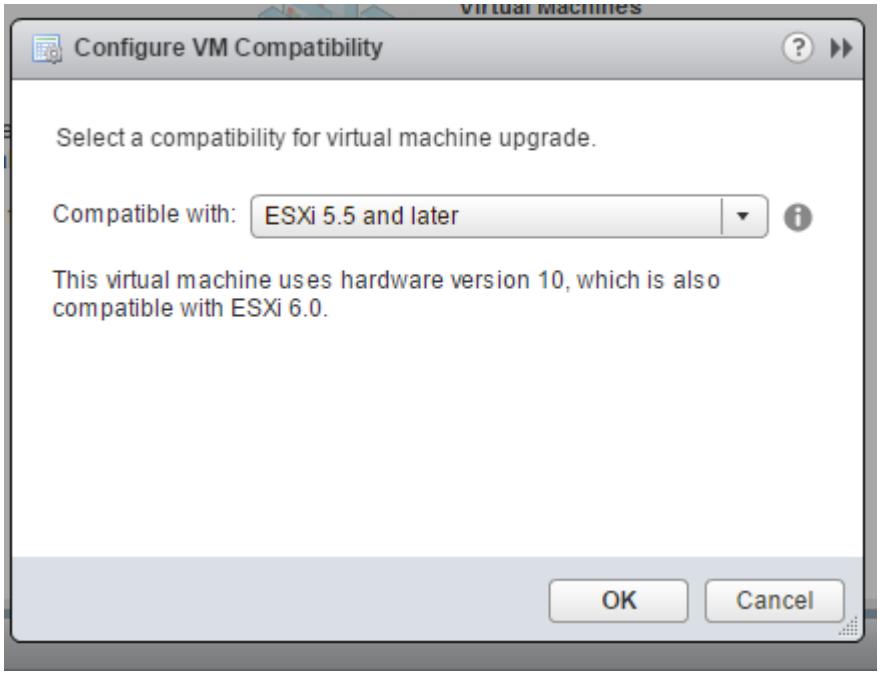
Pour configurer les instances NetScaler VPX afin qu'elles utilisent l'interface réseau SR-IOV à l'aide de VMware vSphere Web Client :

1. Dans vSphere Web Client, sélectionnez **Hôtes et clusters**.
2. Mettez à niveau le paramètre de compatibilité de l'instance NetScaler VPX vers ESX 5.5 ou version ultérieure, comme suit :

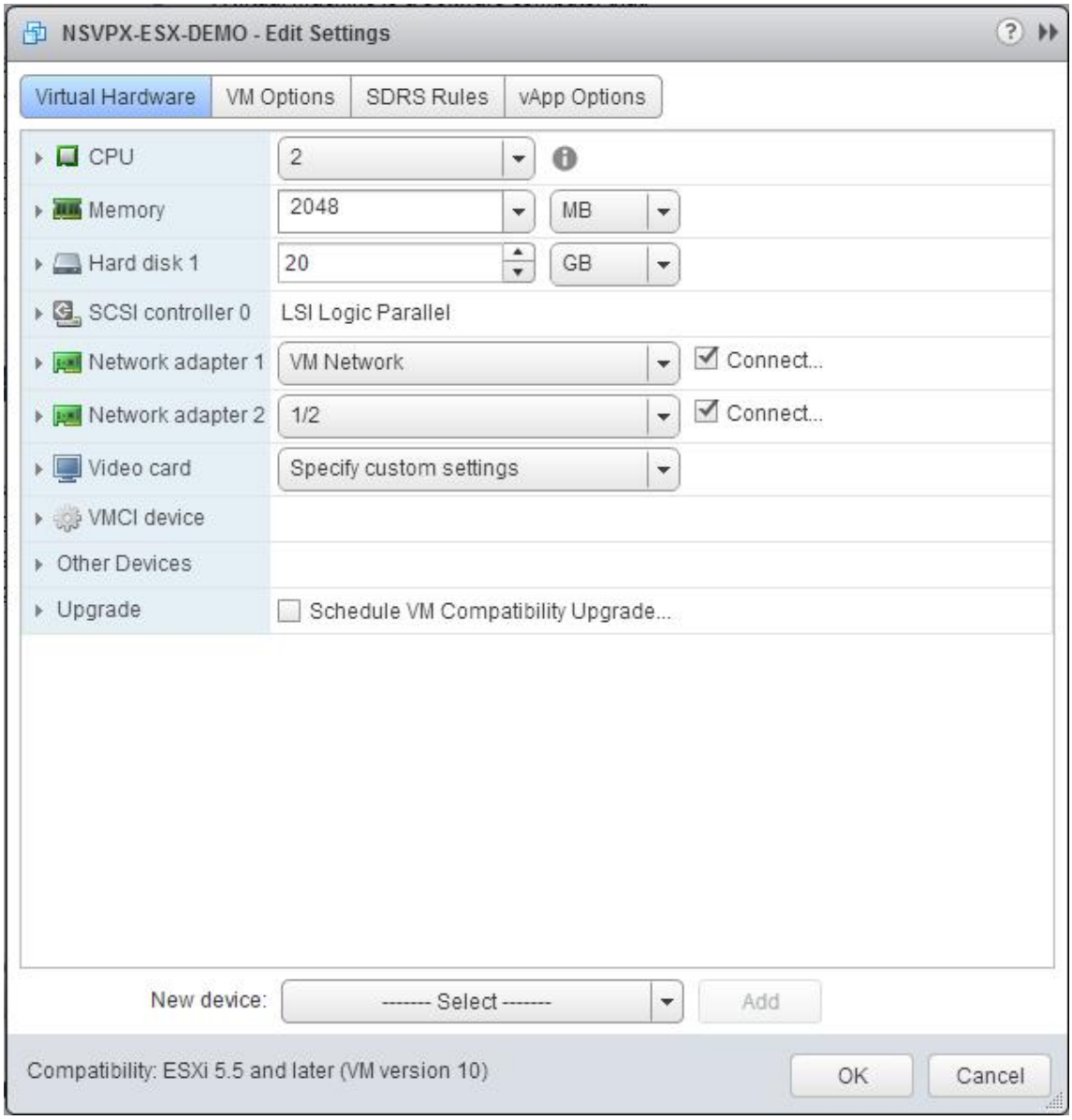
   a. Éteignez l'instance NetScaler VPX.

   b. Cliquez avec le bouton droit sur l'instance NetScaler VPX et sélectionnez **Compatibilité > Mettre à niveau la compatibilité**des machines virtuelles.

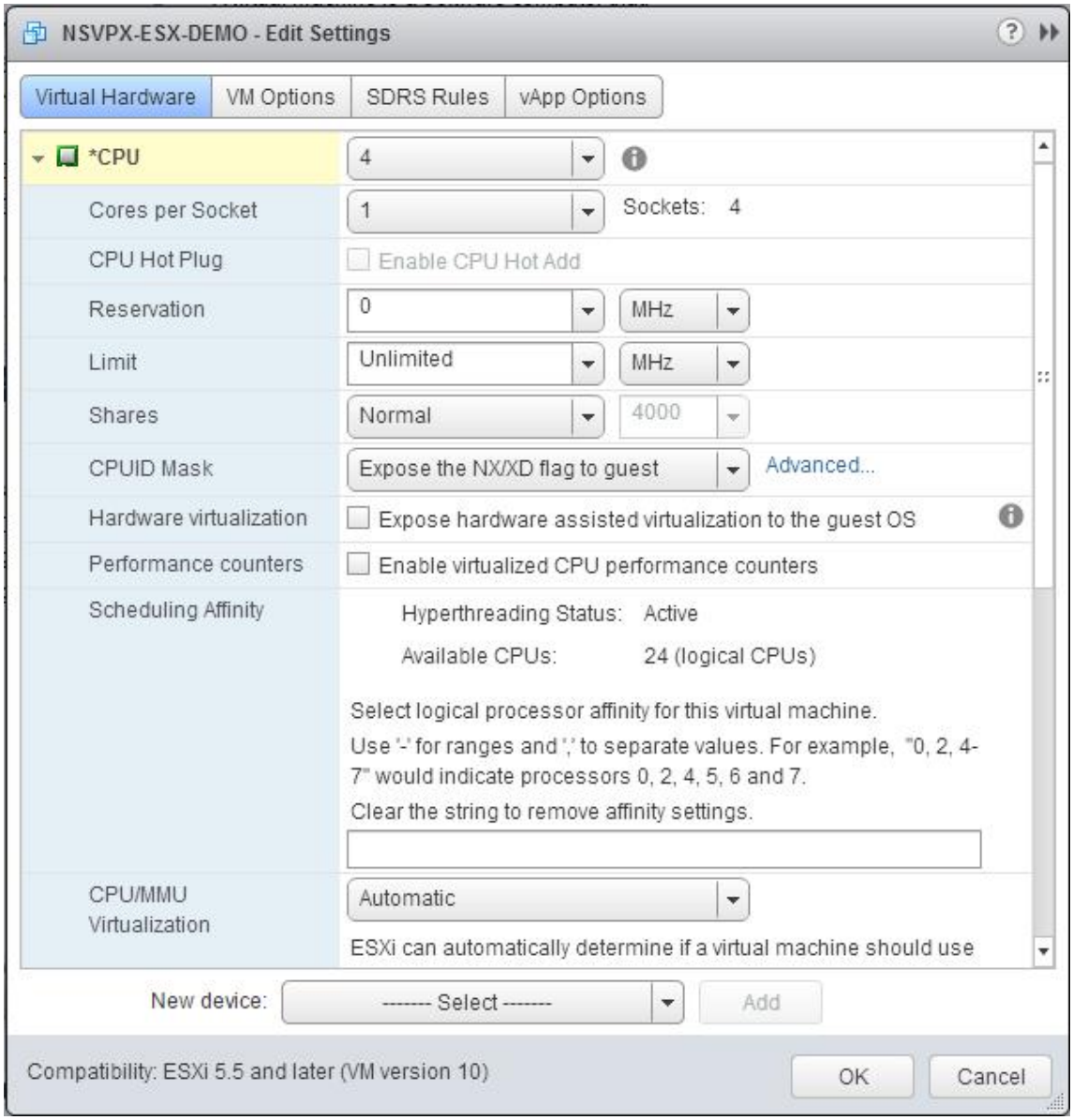
   c. Dans la boîte de dialogue **Configurer la compatibilité des machines virtuelles**, sélectionnez **ESXi 5.5 et versions ultérieures** dans la liste déroulante **Compatible avec**, puis cliquez sur **OK**.



3. **Cliquez avec le bouton droit sur l'instance NetScaler VPX et cliquez sur Modifier les paramètres.**



4. Dans la <virtual_appliance>boîte de dialogue **- Modifier les paramètres**, cliquez sur la section **CPU** .



5. Dans la section **CPU**, mettez à jour les paramètres suivants :

   - Nombre de processeurs
   - Nombre de prises
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

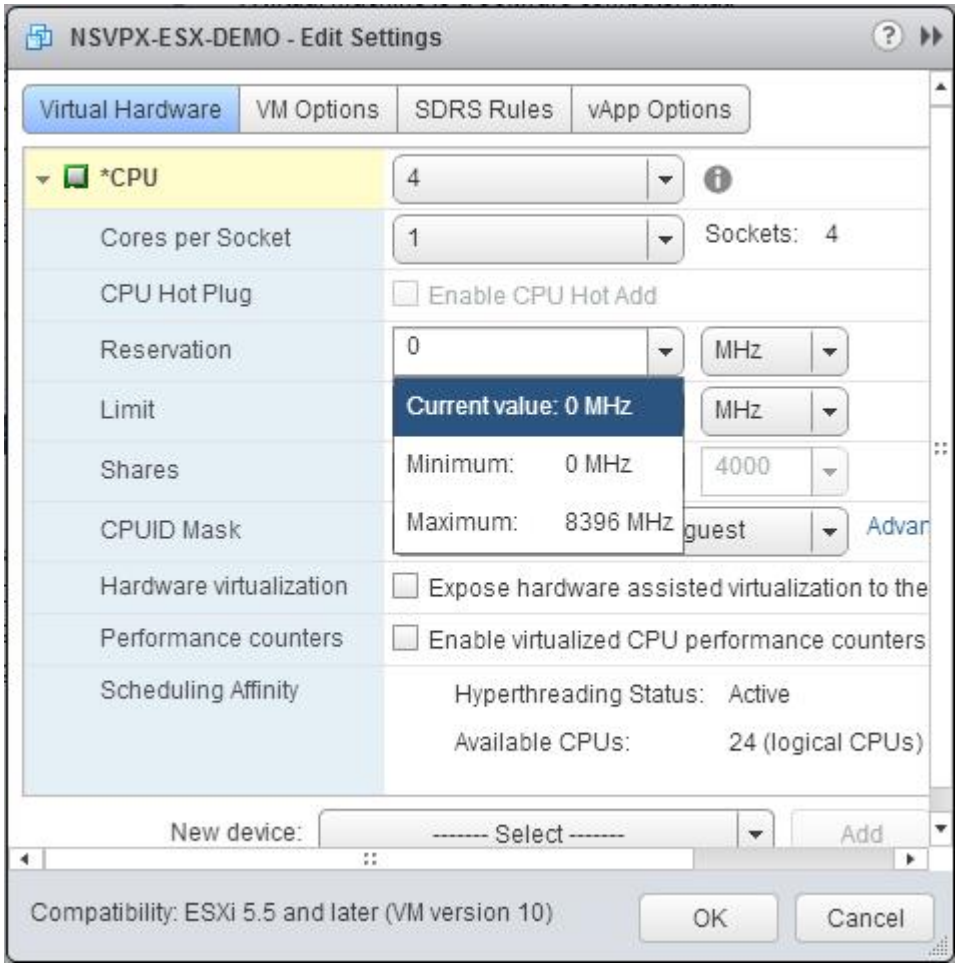
   a. Dans la liste déroulante **CPU**, sélectionnez le nombre de CPU à attribuer à l'appliance virtuelle.

   b. Dans la liste déroulante **Cores par socket**, sélectionnez le nombre de sockets.

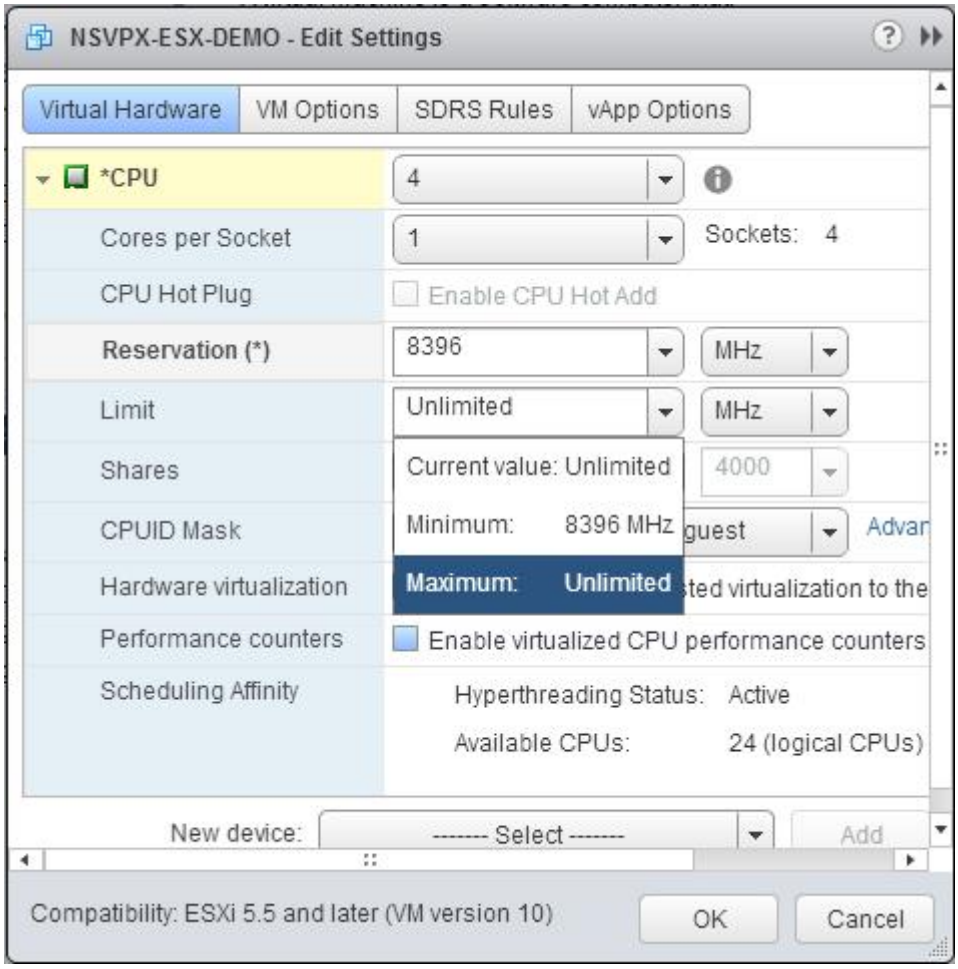
c. (Facultatif) Dans le champ **CPU Hot Plug**, cochez ou décochez la case **Activer l'ajout à chaud du processeur** .

Remarque : Citrix recommande d'accepter la valeur par défaut (désactivée).

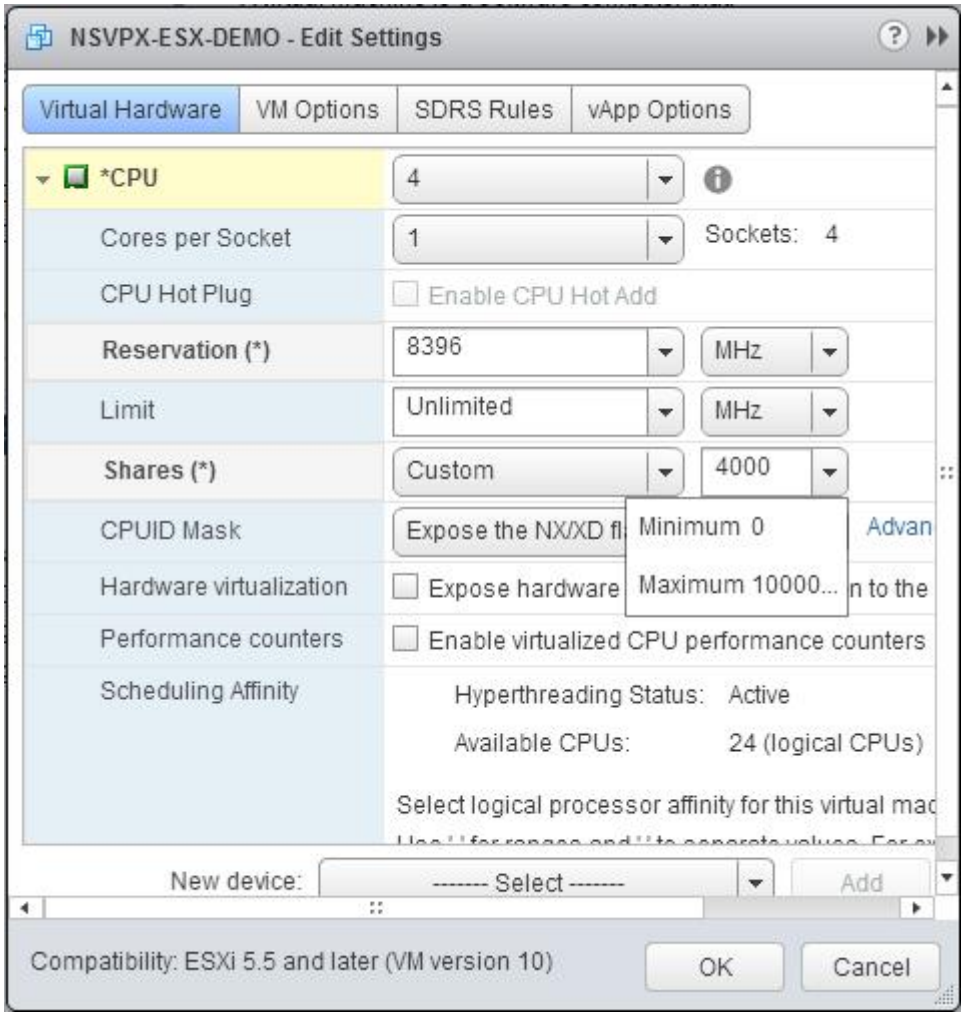
d. Dans la liste déroulante **Réservation**, sélectionnez le nombre affiché comme valeur maximale.



e. Dans la liste déroulante **Limite**, sélectionnez le nombre affiché comme valeur maximale.



f. Dans les listes déroulantes **Partages**, sélectionnez **Personnalisé** et le nombre affiché comme valeur maximale.



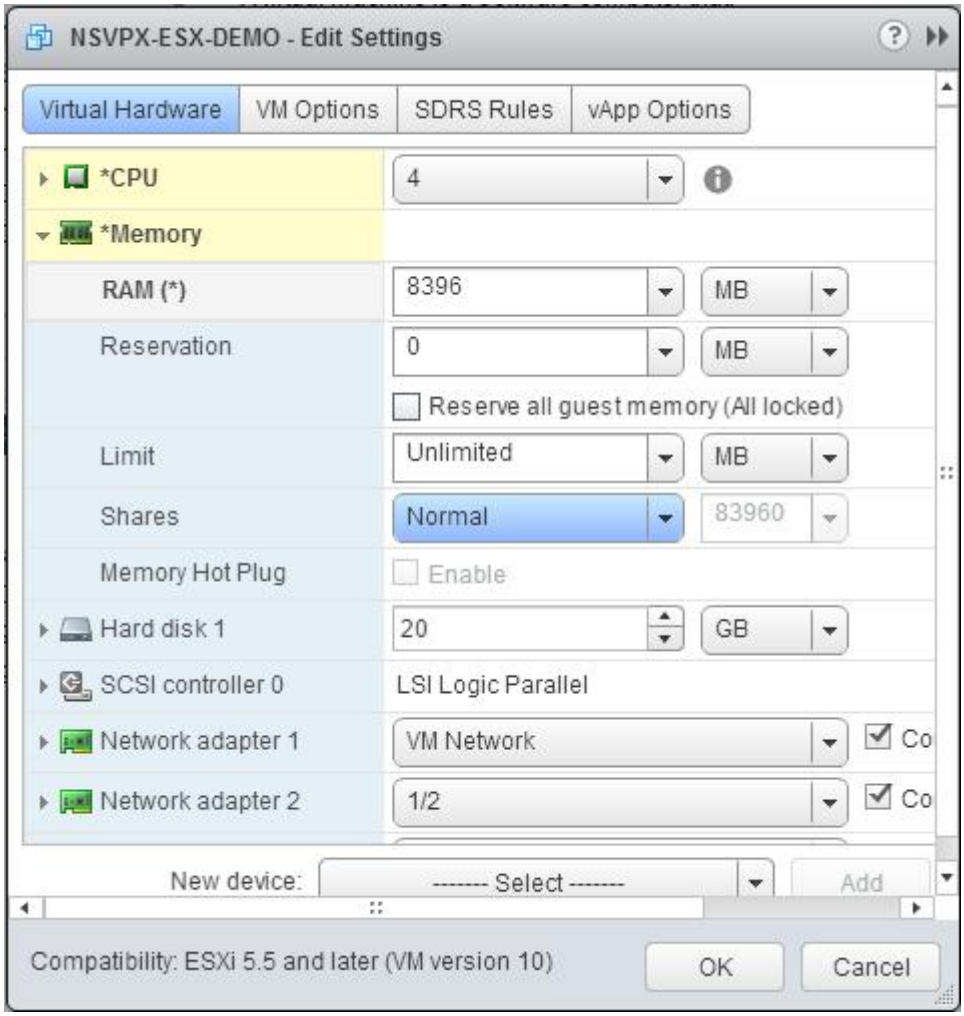
6. Dans la section **Mémoire**, mettez à jour les paramètres suivants :

   - Taille de la mémoire vive
   - Réservations
   - Limite
   - Actions

   Définissez les valeurs comme suit :

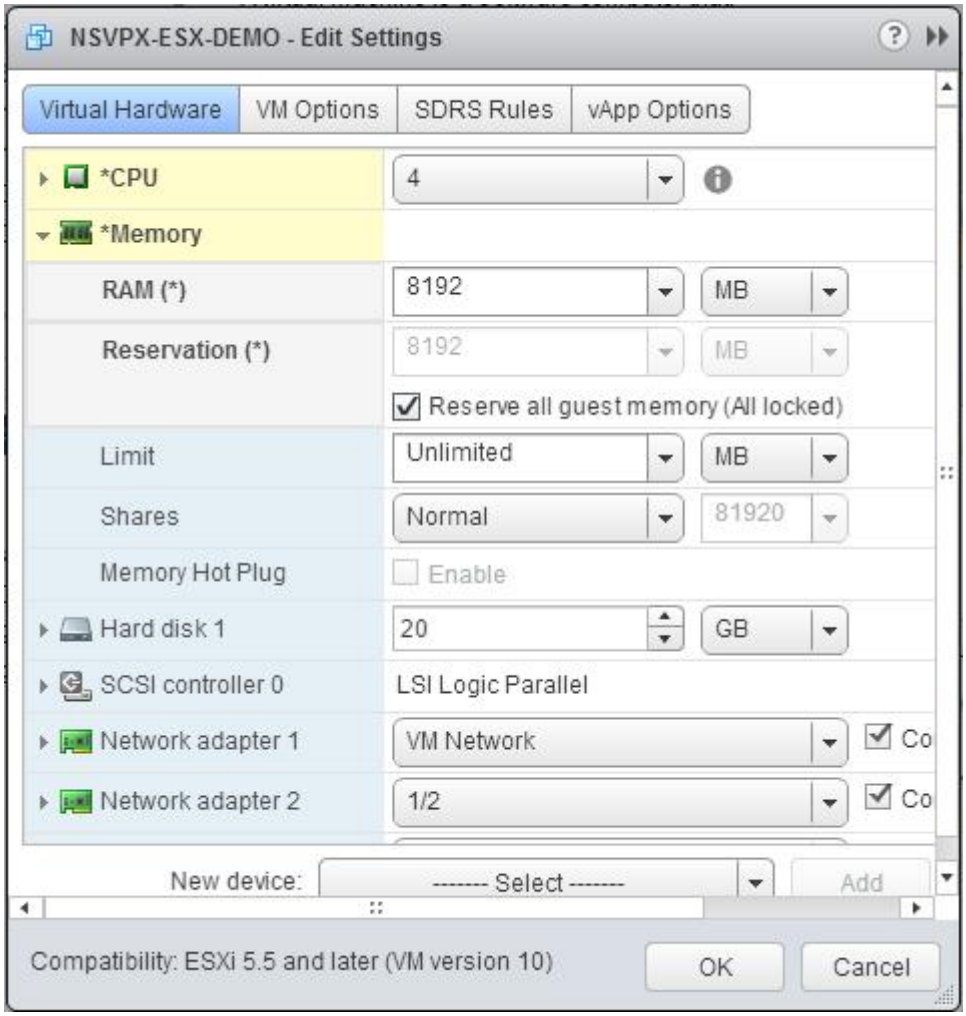
   a. Dans la liste déroulante **RAM**, sélectionnez la taille de la RAM. Il doit s'agir du nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 2 Go = 8 Go.

   Remarque : Pour les éditions Advanced ou Premium de l'appliance NetScaler VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.

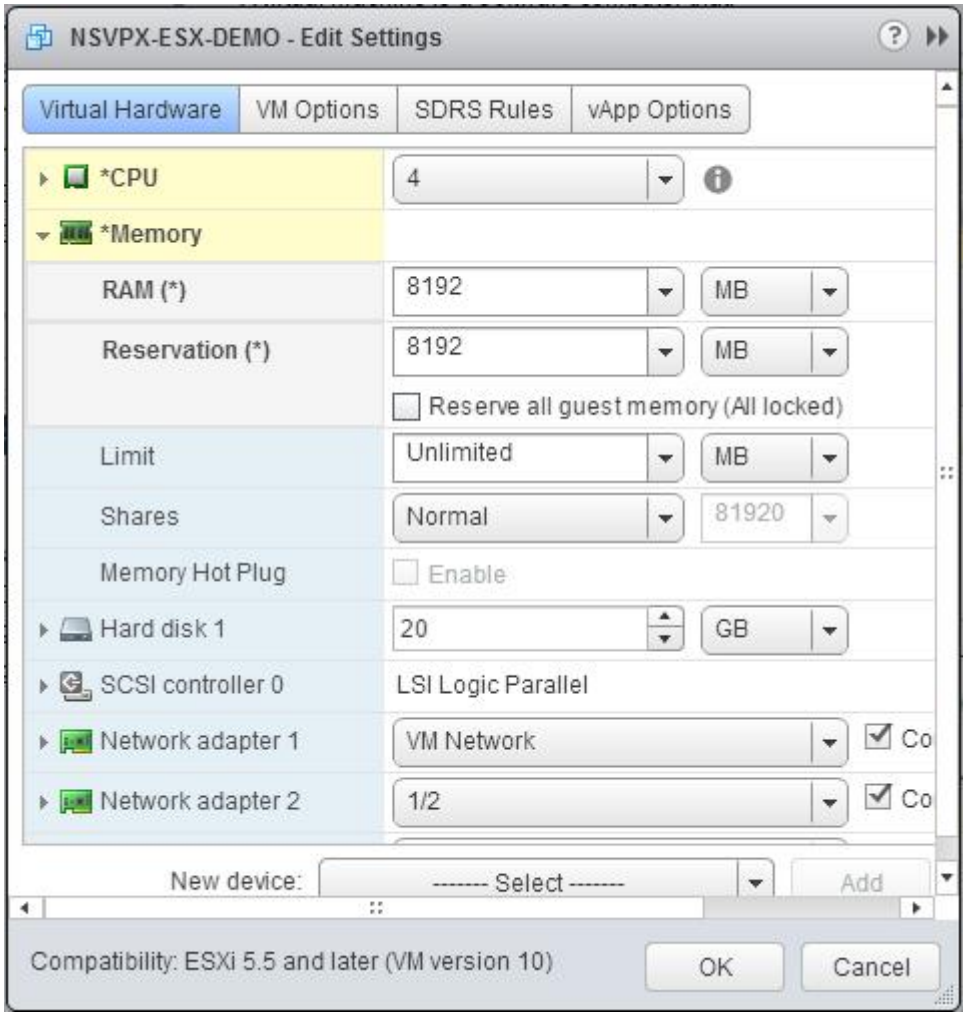


b. Dans la liste déroulante **Réservation**, entrez la valeur de la réservation de mémoire et cochez la case **Réserver toute la mémoire client (Tout est verrouillé)** . La réservation de mémoire doit correspondre au nombre de processeurs virtuels x 2 Go. Par exemple, si le nombre de processeurs virtuels est de 4, la réservation de mémoire doit être de 4 x 2 Go = 8 Go.

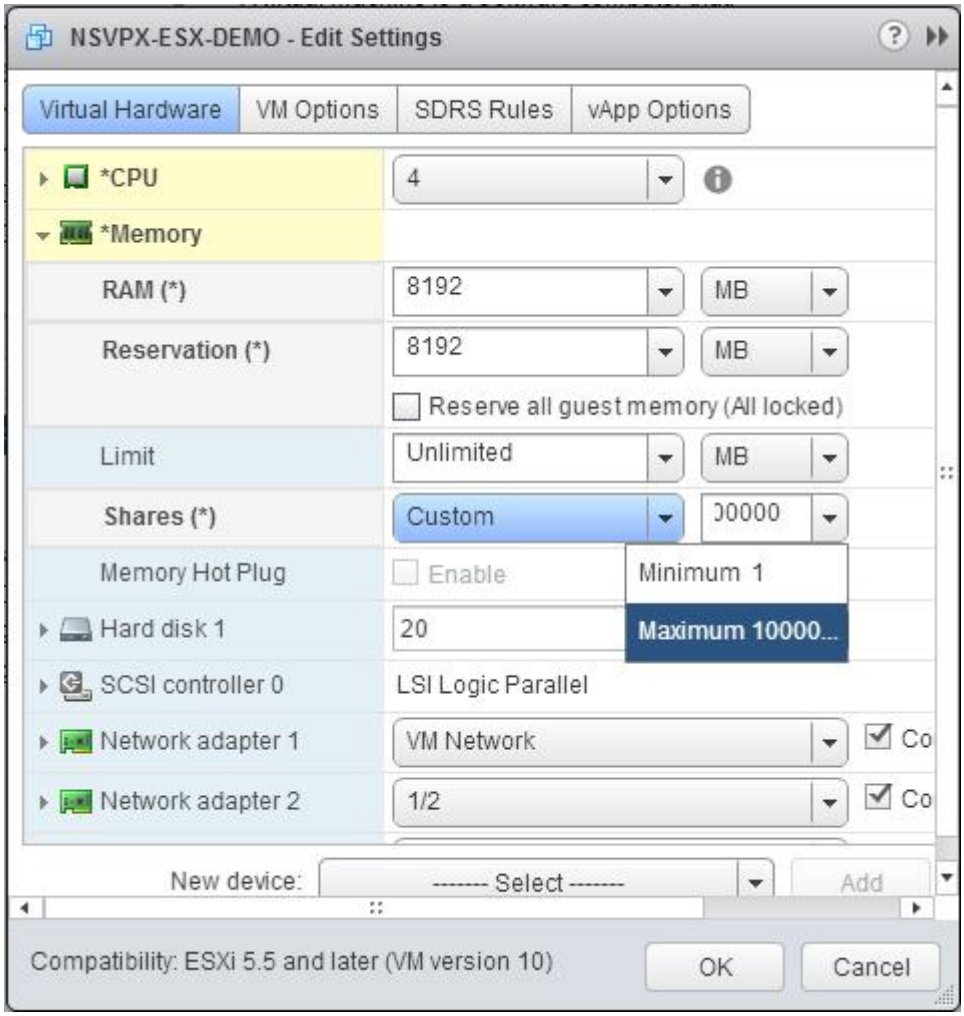
Remarque : Pour les éditions Advanced ou Premium de l'appliance NetScaler VPX, assurez-vous d'allouer 4 Go de RAM à chaque vCPU. Par exemple, si le nombre de vCPU est 4 alors RAM = 4 x 4 Go = 16 Go.



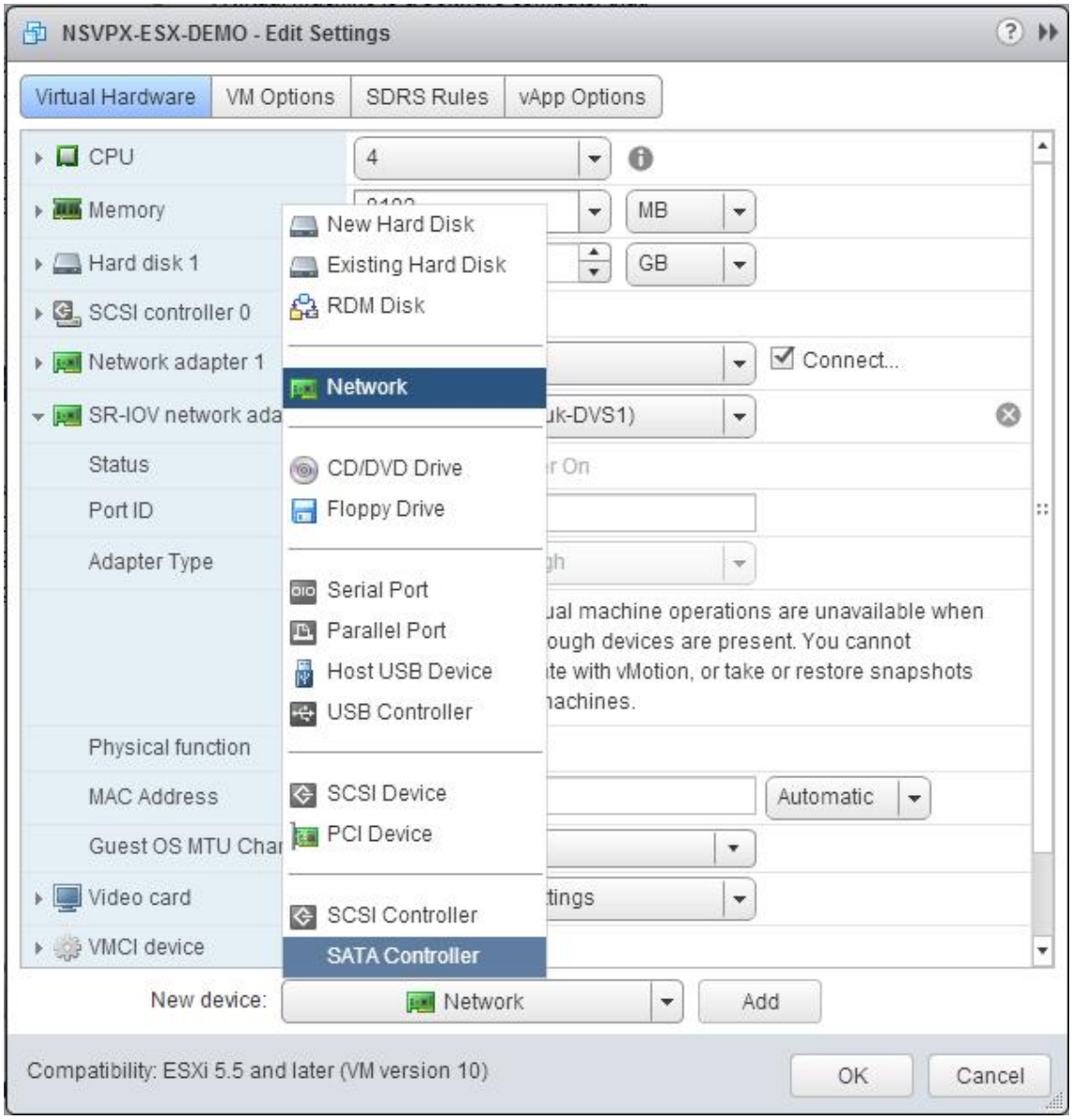
c. Dans la liste déroulante **Limite**, sélectionnez le nombre affiché comme valeur maximale.



d. Dans les listes déroulantes **Parts**, sélectionnez **Personnalisé**, puis sélectionnez le nombre affiché comme valeur maximale.

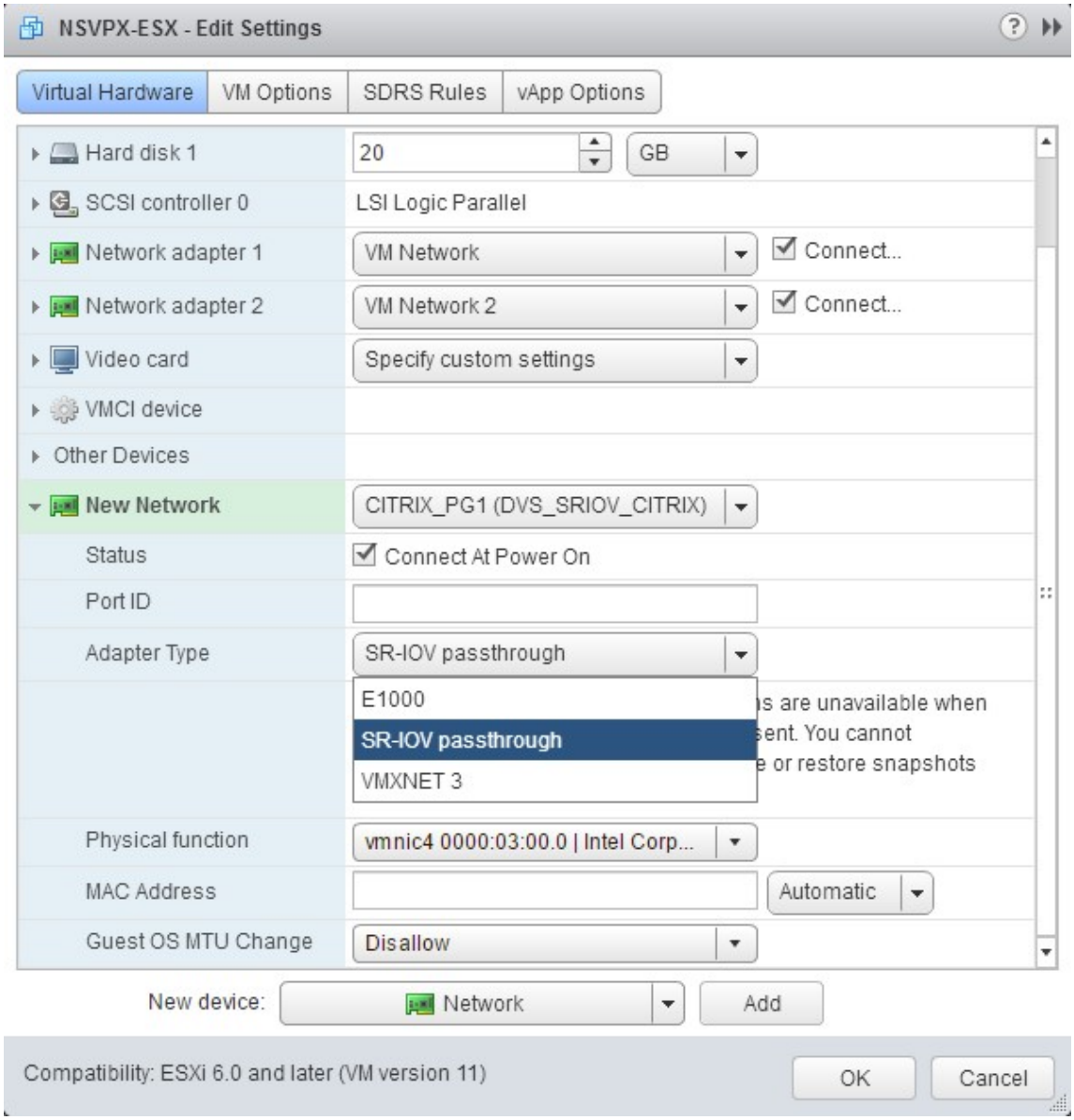


7. Ajouter une interface réseau SR-IOV. Dans la liste déroulante **Nouvel appareil**, sélectionnez **Réseau**, puis cliquez sur **Ajouter**.

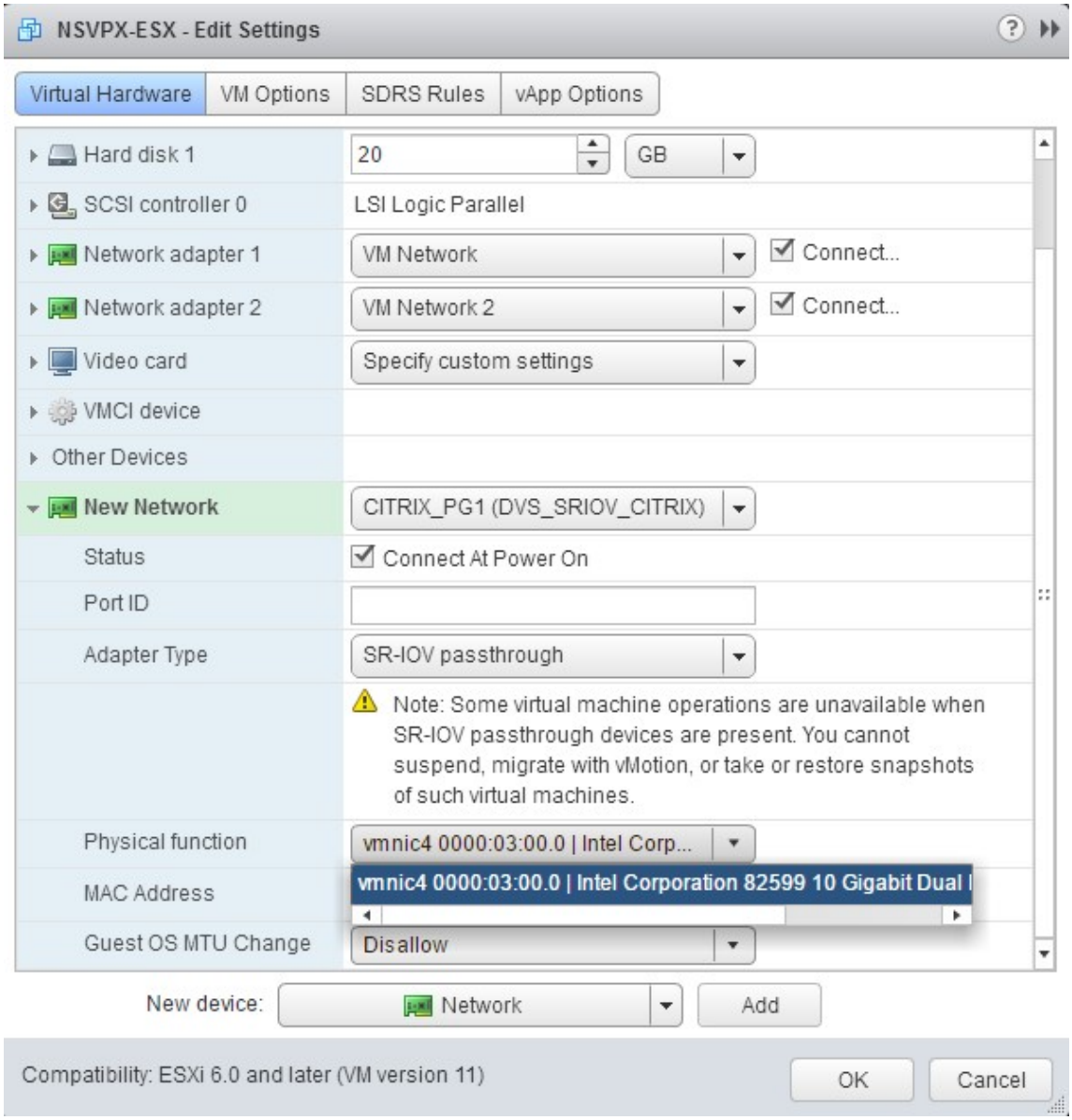


8. Dans la section **Nouveau réseau**. Dans la liste déroulante, sélectionnez celui `Portgroup` que vous avez créé, puis procédez comme suit :

   a. Dans la liste déroulante **Type d'adaptateur**, sélectionnez **Passthrough SR-IOV** .

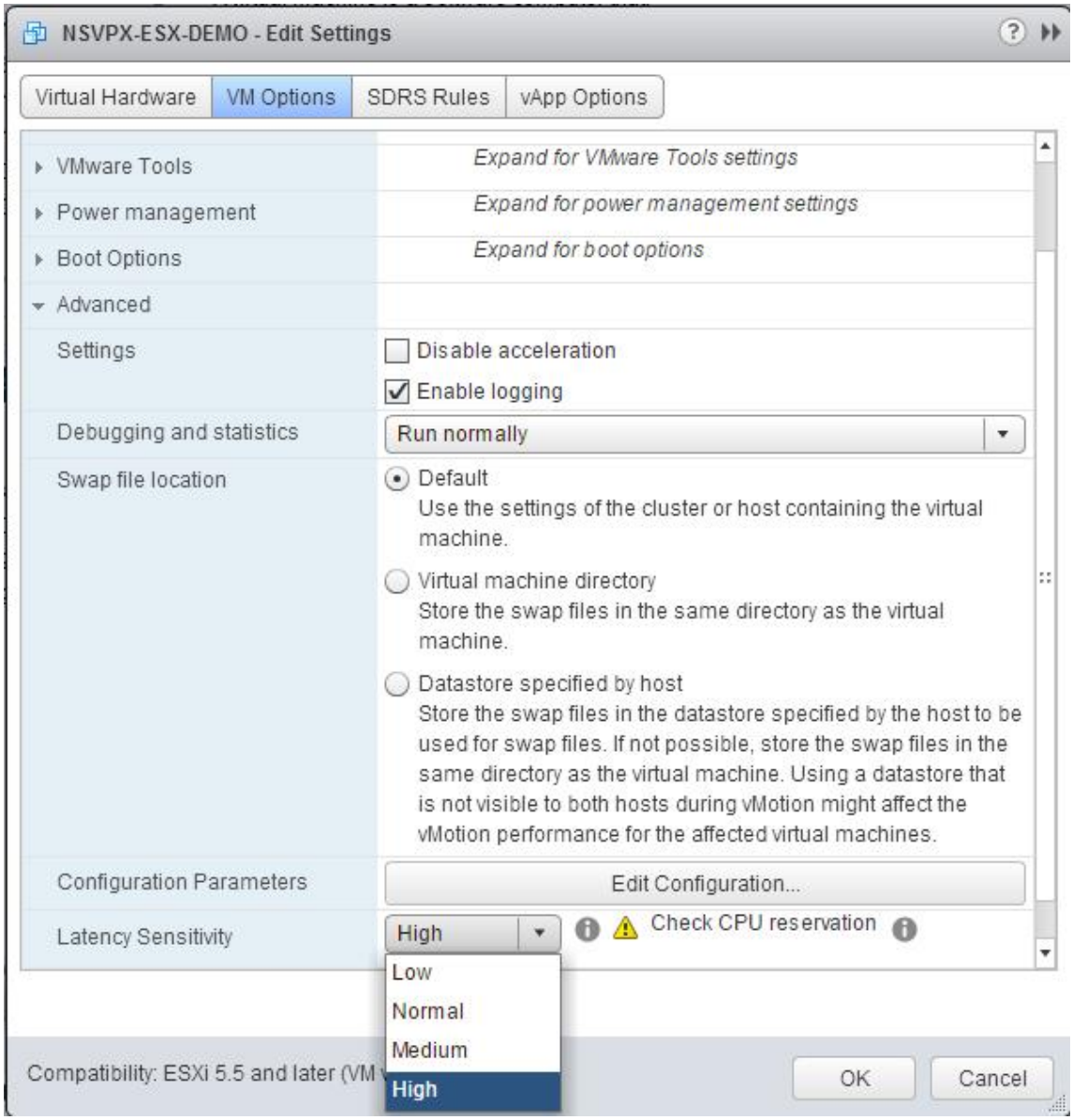


b. Dans la liste déroulante **Fonction physique**, sélectionnez l'adaptateur physique mappé avec le `Portgroup`.



c. Dans la liste déroulante **Guest OS MTU Change**, sélectionnez Interdire **.**

9. Dans la <virtual_appliance>boîte de dialogue **- Modifier les paramètres**, cliquez sur l'onglet **Options de la machine virtuelle** .
10. Dans l'onglet **Options de la machine virtuelle**, sélectionnez la section **Avancé** . Dans la liste déroulante **Sensibilité à la latence**, sélectionnez **Élevé** .



11. Cliquez sur **OK**.
12. Allumez l'instance NetScaler VPX.
13. Une fois que l'instance NetScaler VPX est activée, vous pouvez utiliser la commande suivante pour vérifier la configuration :

    > Afficher le résumé de l'interface

La sortie doit afficher toutes les interfaces que vous avez configurées :

```
1 > show interface summary
2 ---------------------------------------------------------------------------

3       Interface  MTU        MAC                Suffix
```



```
4  ----------------------------------------------------------------------------

5  1     0/1        1500       00:0c:29:1b:81:0b    NetScaler Virtual
       Interface
6  2     10/1       1500       00:50:56:9f:0c:6f    Intel 82599 10G VF
       Interface
7  3     10/2       1500       00:50:56:9f:5c:1e    Intel 82599 10G VF
       Interface
8  4     10/3       1500       00:50:56:9f:02:1b    Intel 82599 10G VF
       Interface
9  5     10/4       1500       00:50:56:9f:5a:1d    Intel 82599 10G VF
       Interface
10 6     10/5       1500       00:50:56:9f:4e:0b    Intel 82599 10G VF
       Interface
11 7     LO/1       1500       00:0c:29:1b:81:0b    Netscaler Loopback
       interface
12  Done
13 > show inter 10/1
14 1)      Interface 10/1 (Intel 82599 10G VF Interface) #1
15         flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
16         MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0
               h21m53s
17         Actual: media FIBER, speed 10000, duplex FULL, fctl NONE,
               throughput 10000
18         LLDP Mode: NONE,                LR Priority: 1024
19
20         RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
               Stalls(0)
21         TX: Pkts(838149954) Bytes(860895860507) Errs(0) Drops(0) Stalls
               (0)
22         NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
23         Bandwidth thresholds are not set.
24  Done
```

Migration du NetScaler VPX de l'E1000 vers les interfaces réseau SR-IOV ou VMXNET3

May 5, 2023

24 mai 2018

Vous pouvez configurer vos instances NetScaler VPX existantes qui utilisent les interfaces réseau E1000

pour utiliser les interfaces réseau SR-IOV ou VMXNET3.

Pour configurer une instance NetScaler VPX existante pour utiliser les interfaces réseau SR-IOV, voir Configurer une instance NetScalerVPX pour utiliser l'interface réseau SR-IOV.

Pour configurer une instance NetScaler VPX existante afin qu'elle utilise les interfaces réseau VMXNET3, voir Configurer une instance NetScaler VPX pour utiliser l'interface réseau VMXNET3.

Configurer une instance NetScaler VPX pour utiliser l'interface réseau PCI passthrough

May 5, 2023

Vue d'ensemble

Après avoir installé et configuré une instance NetScaler VPX sur VMware ESX Server, vous pouvez utiliser vSphere Web Client pour configurer l'appliance virtuelle afin qu'elle utilise des interfaces réseau PCI passthrough.

La fonction PCI Passthrough permet à une machine virtuelle cliente d'accéder directement aux périphériques PCI et PCIe physiques connectés à un hôte.

Composants requis

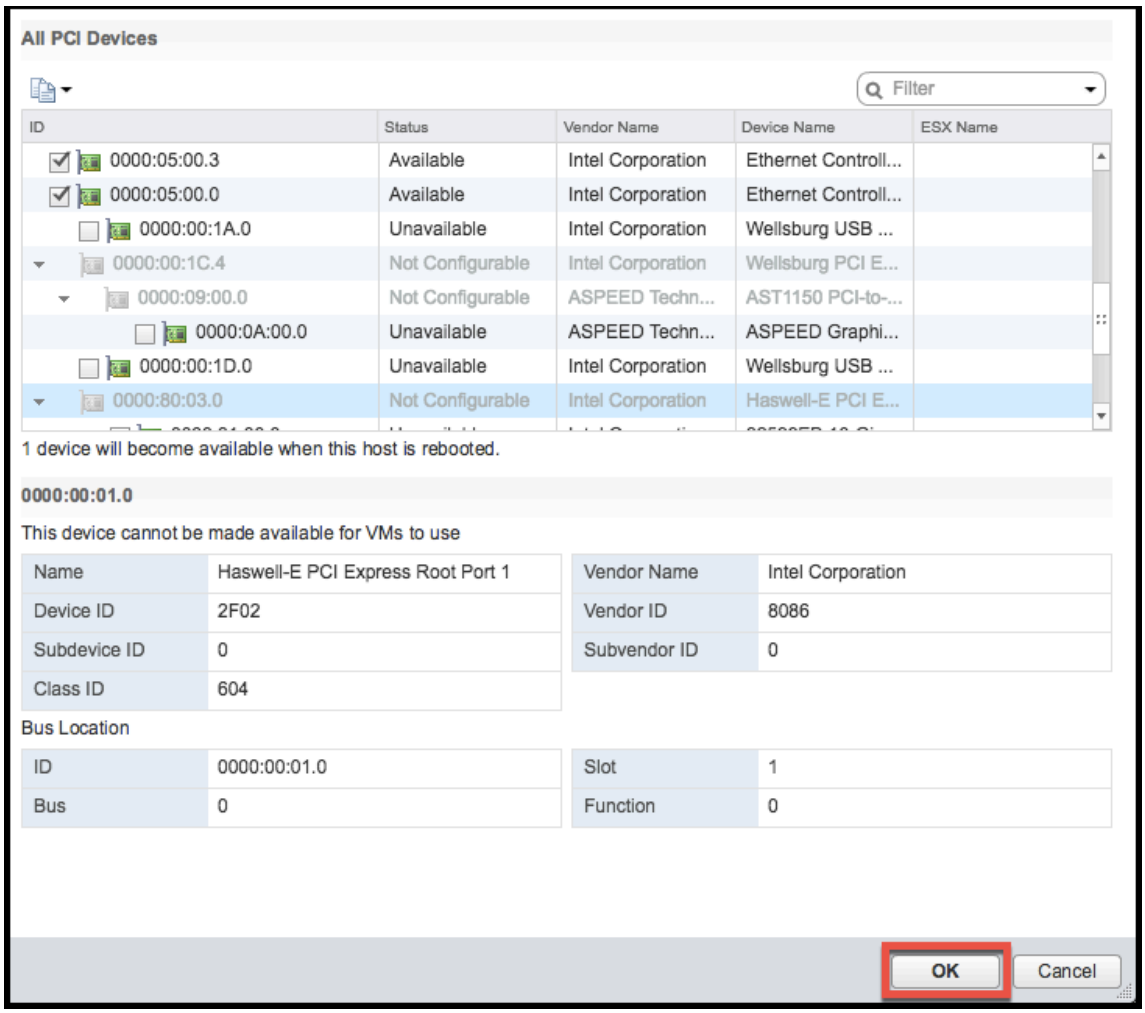
- La version du microprogramme de la carte réseau Intel XL710 installée sur l'hôte est 5.04.
- Un périphérique PCI relais connecté et configuré sur l'hôte
- NIC prises en charge :
  - Carte réseau Intel X710 10G
  - Carte réseau 40G Intel XL710 à double port
  - Carte réseau 40G Intel XL710 à port unique

Configurer les périphériques passthrough sur un hôte

Avant de configurer un périphérique PCI passthrough sur une machine virtuelle, vous devez le configurer sur la machine hôte. Procédez comme suit pour configurer les périphériques passthrough sur un hôte.

1. Sélectionnez l'hôte dans le panneau du navigateur de vSphere Web Client.
2. Cliquez sur **Gérer** > **Paramètres** > **Appareils PCI.** Tous les appareils relais disponibles s'affichent.

3. Cliquez avec le bouton droit sur l'appareil que vous souhaitez configurer, puis cliquez sur **Modifier**.
4. La fenêtre **Modifier la disponibilité du périphérique PCI** s'affiche.
5. Sélectionnez les périphériques à utiliser pour la transmission, puis cliquez sur **OK**.

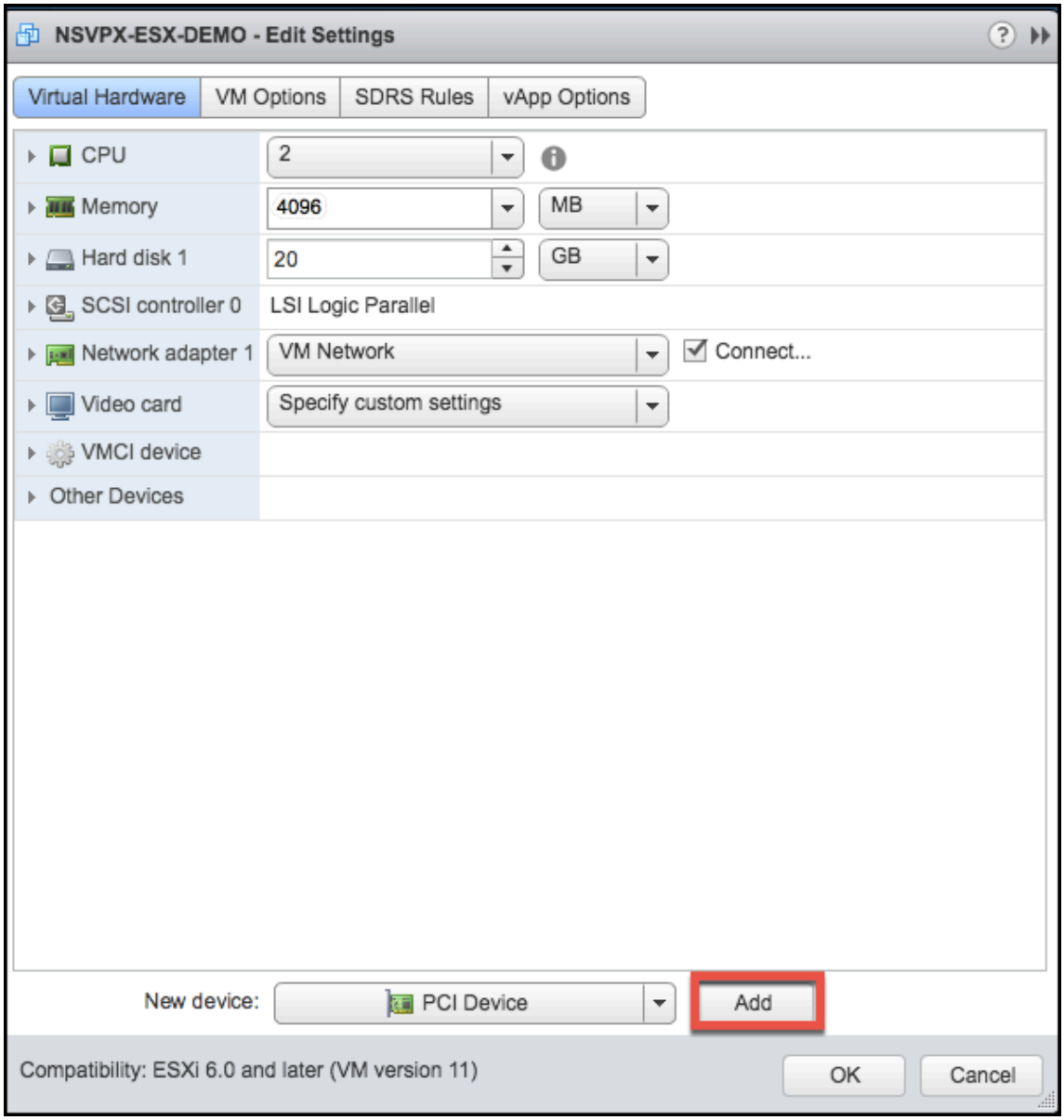


6. Redémarrez la machine hôte.

Configurer des appareils relais sur une instance NetScaler VPX

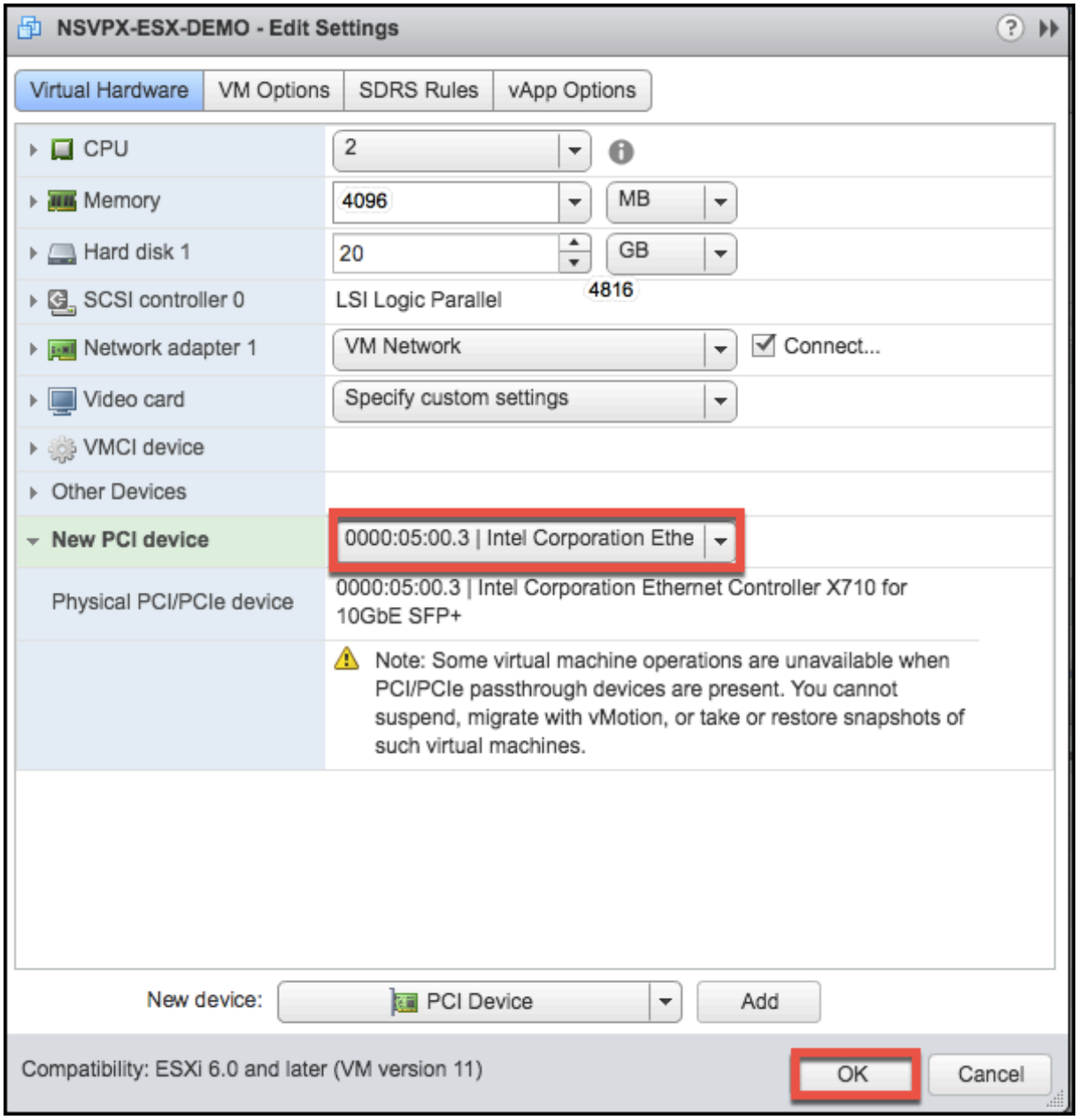
Suivez ces étapes pour configurer un périphérique PCI relais sur une instance NetScaler VPX.

1. Éteignez la machine virtuelle.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Sous l'onglet **Matériel virtuel**, sélectionnez **Périphérique PCI** dans le menu déroulant **Nouveau périphérique**, puis cliquez sur **Ajouter** .



4. Développez **Nouveau périphérique PCI** et sélectionnez le périphérique de transmission à connecter à la machine virtuelle dans la liste déroulante, puis cliquez sur **OK** .

> **Remarque**
>
> L'interface réseau VMXNET3 et l'interface réseau PCI ne peuvent pas coexister.



1. Mettez sous tension la machine virtuelle invitée.

Vous avez terminé les étapes de configuration de NetScaler VPX pour utiliser les interfaces réseau PCI passthrough.

Appliquez les configurations NetScaler VPX au premier démarrage de l'appliance NetScaler sur l'hyperviseur VMware ESX

May 5, 2023

Vous pouvez appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler sur l'hyperviseur VMware ESX. Par conséquent, dans certains cas, une configuration spécifique ou une instance VPX est mise en place en beaucoup moins de temps.

Pour plus d'informations sur les données utilisateur avant le démarrage et leur format, voir Appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler dans le cloud.

> **Remarque :**
>
> Pour amorcer à l'aide des données utilisateur de pré-démarrage dans ESX, la configuration de la passerelle par défaut doit être transmise dans <NS-CONFIG> la section. Pour plus d'informations sur le contenu de la <NS-CONFIG> balise, voir [Sample-<NS-CONFIG>-section] (apply-preboot-userdata-on-esx-vpx.html #sample -<ns-config>-section).

Section <NS-CONFIG> échantillon :

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0  10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP> 10.102.38.216 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Comment fournir des données utilisateur avant le démarrage sur un hyperviseur ESX

Vous pouvez fournir des données utilisateur avant le démarrage sur l'hyperviseur ESX à partir d'un client Web ou d'un client vSphere des deux manières suivantes :

- Utilisation de CD/DVD ISO
- Utiliser la propriété OVF

Fournir les données utilisateur à l'aide de CD/DVD ISO

Vous pouvez utiliser le client VMware vSphere pour injecter des données utilisateur dans la machine virtuelle sous forme d'image ISO à l'aide du lecteur de CD/DVD.

Pour fournir des données utilisateur à l'aide de l'ISO du CD/DVD, procédez comme suit :

1. Créez un fichier dont le nom contient `userdata` le contenu des données utilisateur avant le démarrage. Pour plus d'informations sur le contenu de la `<NS-CONFIG>` balise, consultez la `<NS-CONFIG>` section Exemple.

   > Remarque : Le nom de fichier doit être strictement utilisé comme `userdata`.

2. Stockez le fichier `userdata` dans un dossier et créez une image ISO à l'aide de ce dossier.

   Vous pouvez créer une image ISO avec un fichier `userdata` en utilisant les deux méthodes suivantes :

   - En utilisant n'importe quel outil de traitement d'image tel que PowerISO.
   - Utilisation de la commande `mkisofs` sous Linux.

   L'exemple de configuration suivant montre comment générer une image ISO à l'aide de la commande `mkisofs` sous Linux.

```
root@ubuntu:~/sai/14jul2021# ls -l total 4
drwxr-xr-x 2 root root 4096 Jul 14 12:32 esx_preboot_userdata
root@ubuntu:~/sai/14jul2021#
root@ubuntu:~/sai/14jul2021# ls -l esx_preboot_userdata/total 4
-rw-r--r-- 1 root root 3016 Jul 14 12:32 userdata
root@ubuntu:~/sai/14jul2021# mkisofs -o esx_preboot_userdata.iso
    ./esx_preboot_userdata
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)
root@ubuntu:~/sai/14jul2021# ls -lh
total 356K
drwxr-xr-x 2 root root 4.0K Jul 14 12:32 esx_preboot_userdata
-rw-r--r-- 1 root root 352K Jul 14 12:34 esx_preboot_userdata.iso

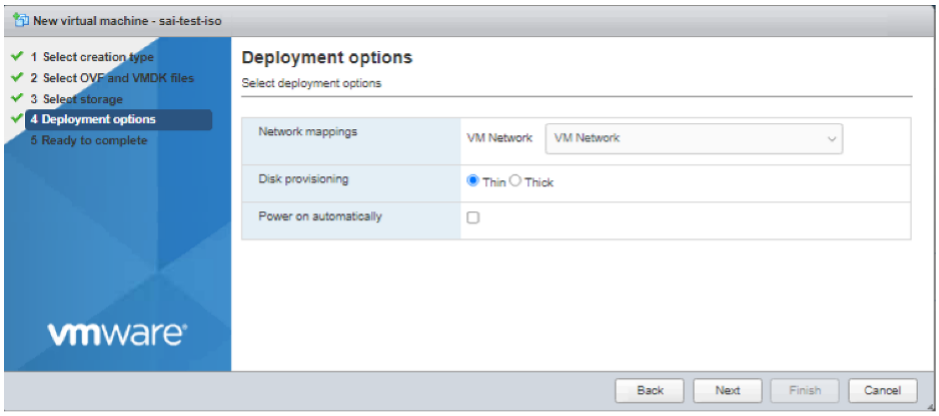
root@ubuntu:~/sai# ls preboot_userdata_155_193 userdata
root@ubuntu:~/sai# mkisofs -o preboot_userdata_155_193.iso ./
    preboot_userdata_155_193
```



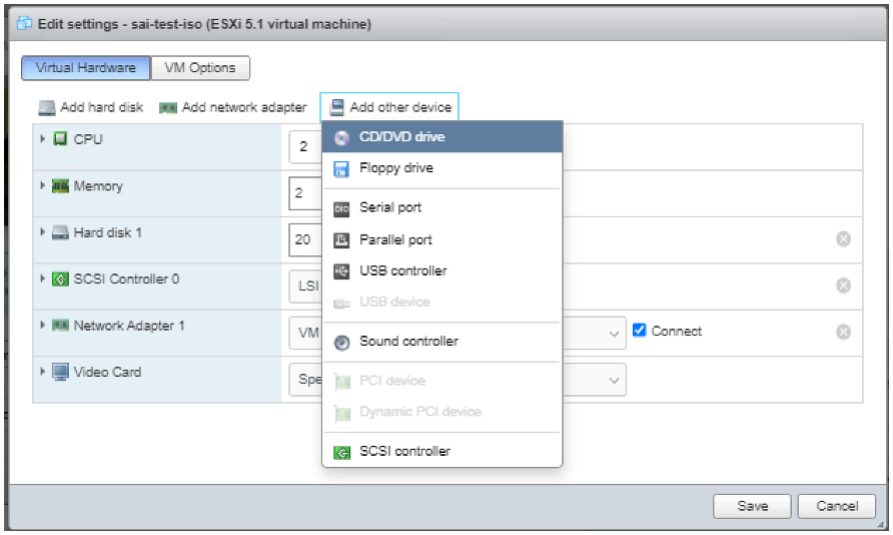
```
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)

<!--NeedCopy-->
```

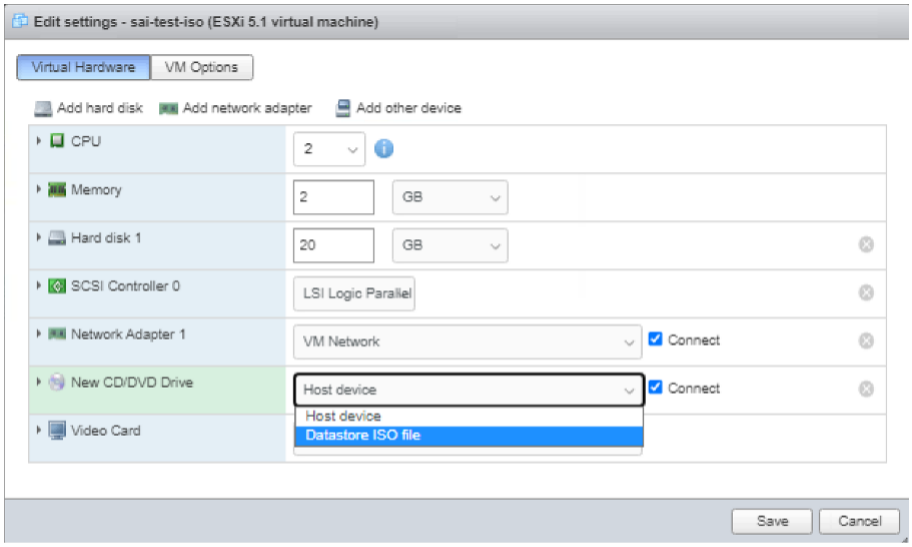
3. Provisionnez l'instance NetScaler VPX à l'aide du processus de déploiement standard pour créer la machine virtuelle. Mais n'allumez pas automatiquement la machine virtuelle.



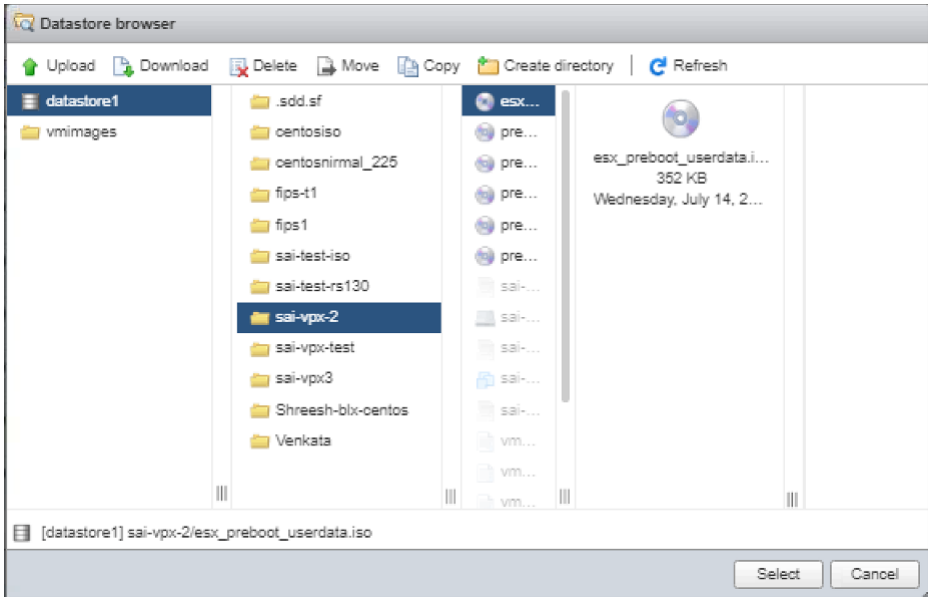
4. Une fois la machine virtuelle créée avec succès, joignez le fichier ISO en tant que lecteur de CD/DVD à la machine virtuelle.



5. Accédez à **Nouveau lecteur de CD/DVD** et choisissez **Fichier ISO de la banque** de données dans le menu déroulant.



6. Sélectionnez une banque de données dans vSphere Client.



7. Allumez la machine virtuelle.

Fourniture de données utilisateur à l'aide de la propriété OVF du client Web ESX

Suivez ces étapes pour fournir des données utilisateur à l'aide de la propriété OVF.

1. Créez un fichier contenant le contenu des données utilisateur.


```
root@ubuntu:~/sai/14jul2021# cat esx_userdata.xml
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0 10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP>    10.102.38.219 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

2. Codez le contenu des données utilisateur avec un codage Base64. Vous pouvez effectuer le codage Base64 à l'aide des deux méthodes suivantes :

   - Sous Linux, utilisez la commande suivante :

     ```
     base64 <userdata-filename>  >   <outuput-file>
     <!--NeedCopy-->
     ```

     Exemple :

     ```
     base64 esx_userdata.xml  > esx_userdata_b64
     <!--NeedCopy-->
     ```

     ```
     root@ubuntu:~/sai/14jul2021# base64 esx_userdata.xml > esx_userdata_b64
     root@ubuntu:~/sai/14jul2021#
     root@ubuntu:~/sai/14jul2021# cat esx_userdata_b64
     PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw
     LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQPgog
     ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U
     U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT
     VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
     ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
     RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
     ```

   - Utilisez des outils en ligne pour coder le contenu des données utilisateur, par exemple, Encodage et décodage Base64.

3. Incluez une section **Produit** dans le modèle OVF d'une instance NetScaler VPX sur l'hyperviseur ESX.

   Section de produit échantillon :

   ```
   <ProductSection>

   ```



```
3    <Info>Information about the installed software</Info>
4    <Product>NSVPX-VSK Template</Product>
5    <Vendor>Citrix</Vendor>
6    <VendorUrl>www.citrix.com</VendorUrl>
7    <Category> Preboot Userdata </Category>
8
9    <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
        userConfigurable="true" ovf:value="">
10
11     <Label>Userdata</Label>
12     <Description> Userdata for ESX VPX </Description>
13   </Property>
14
15 </ProductSection>
16 <!--NeedCopy-->
```

4. Fournissez les données utilisateur codées en base64 en tant que `guestinfo.userdata` propriété `ovf:value` for dans la section Produit.

```
1  <ProductSection>
2
3    <Info>Information about the installed software</Info>
4    <Product>NSVPX-VSK Template</Product>
5    <Vendor>Citrix</Vendor>
6    <VendorUrl>www.citrix.com</VendorUrl>
7    <Category> Preboot Userdata </Category>
8    <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
        userConfigurable="true"
9      ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
          CglhZGQgcm91dGUgMC4wLjAuMCAw
10     LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQ

11     ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1C

12     U1RSQVA+
          CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT

13     VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAg

14     ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAg

15     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5F

16     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
          CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
```



```
17      RS1DT05GSUc+
            CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg
            ==">
18
19      <Label>Userdata</Label>
20      <Description> Userdata for ESX VPX </Description>
21    </Property>
22
23  </ProductSection>
24  <!--NeedCopy-->
```

5. Utilisez le modèle OVF modifié avec la section Produit pour le déploiement de la machine virtuelle.

```
Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
 Done
> sh ns ver
        NetScaler NS13.0: Build 83.9005.nc, Date: Jul 13 2021, 02:56:05   (64-bit)
 Done
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  S
tate
        ---------        --------------  ----             ----     ---      ----     -------  -
-----
1)      10.102.38.219    0               NetScaler IP     Active   Enabled  Enabled  NA       E
nabled
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.102.38.1      0       UP      0               STATI
C
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMA
NENT
3)      10.102.38.0      255.255.255.0    10.102.38.219    0       UP      0               DIREC
T
 Done
```

Fourniture de données utilisateur à l'aide de la propriété OVF du client ESX vSphere

Suivez ces étapes pour fournir des données utilisateur à l'aide de la propriété OVF du client ESX vSphere.

1. Créez un fichier contenant le contenu des données utilisateur.


```
root@ubuntu:~/sai/14jul2021# cat esx_userdata.xml
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0 10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP>    10.102.38.219 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

2. Codez le contenu des données utilisateur avec un codage Base64. Vous pouvez effectuer le codage Base64 à l'aide des deux méthodes suivantes :

   - Sous Linux, utilisez la commande suivante :

     ```
     base64 <userdata-filename>  >   <outuput-file>
     <!--NeedCopy-->
     ```

     Exemple :

     ```
     base64 esx_userdata.xml  > esx_userdata_b64
     <!--NeedCopy-->
     ```

     ```
     root@ubuntu:~/sai/14jul2021# base64 esx_userdata.xml > esx_userdata_b64
     root@ubuntu:~/sai/14jul2021#
     root@ubuntu:~/sai/14jul2021# cat esx_userdata_b64
     PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw
     LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQPgog
     ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U
     U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT
     VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
     ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
     RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
     ```

   - Utilisez des outils en ligne pour coder le contenu des données utilisateur, par exemple, Encodage et décodage Base64.

3. Incluez une section **Produit** dans le modèle OVF d'une instance NetScaler VPX sur l'hyperviseur ESX.

   Section de produit échantillon :

   ```
   <ProductSection>

   ```



```
3    <Info>Information about the installed software</Info>
4    <Product>NSVPX-VSK Template</Product>
5    <Vendor>Citrix</Vendor>
6    <VendorUrl>www.citrix.com</VendorUrl>
7    <Category> Preboot Userdata </Category>
8
9    <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
        userConfigurable="true" ovf:value="">
10
11     <Label>Userdata</Label>
12     <Description> Userdata for ESX VPX </Description>
13   </Property>
14
15 </ProductSection>
16 <!--NeedCopy-->
```

4. Fournissez les données utilisateur codées en base64 en tant que `guestinfo.userdata` propriété `ovf:value` for dans la section Produit.

```
1  <ProductSection>
2
3    <Info>Information about the installed software</Info>
4    <Product>NSVPX-VSK Template</Product>
5    <Vendor>Citrix</Vendor>
6    <VendorUrl>www.Citrix.com</VendorUrl>
7    <Category> Preboot Userdata </Category>
8    <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
        userConfigurable="true"
9      ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
          CglhZGQgcm91dGUgMC4wLjAuMCAw
10     LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQ

11     ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1C

12     U1RSQVA+
          CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT

13     VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAg

14     ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAg

15     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5F

16     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
          CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
```



```
      RS1DT05GSUc+
          CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg
          ==">

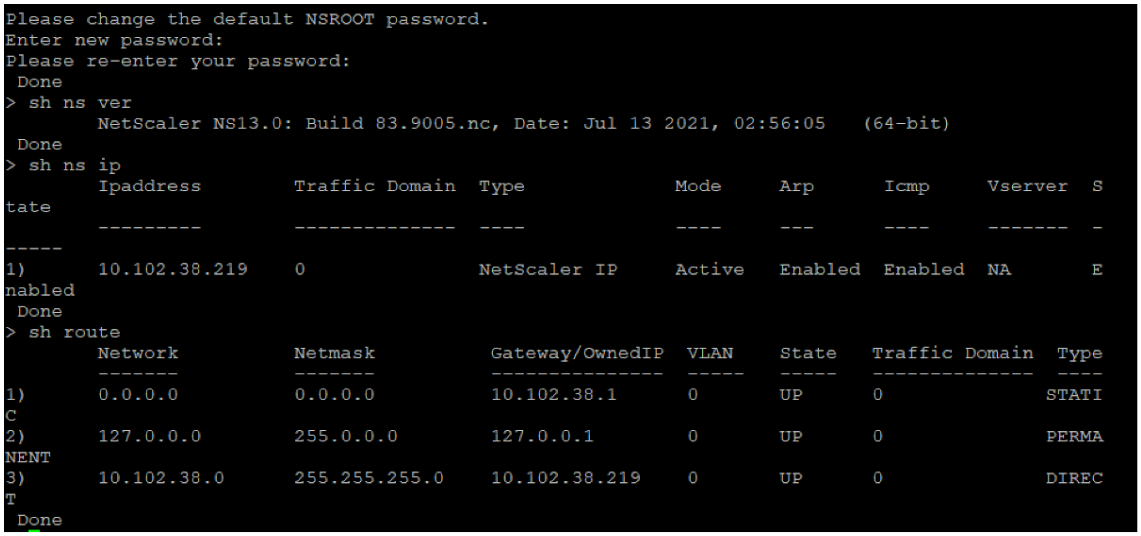
      <Label>Userdata</Label>
      <Description> Userdata for ESX VPX </Description>
    </Property>

</ProductSection>
<!--NeedCopy-->
```

5. Ajoutez la propriété `ovf:transport="com.vmware.guestInfo"` à VirtualHardwareSection comme suit :

```
<VirtualHardwareSection  ovf:transport="com.vmware.guestInfo">
<!--NeedCopy-->
```

6. Utilisez le modèle OVF modifié avec la section Produit pour le déploiement de la machine virtuelle.



Installation d'une instance NetScaler VPX sur le cloud VMware sur AWS

May 5, 2023

Le VMware Cloud (VMC) sur AWS vous permet de créer des centres de données définis par logiciel (SDDC) dans le cloud sur AWS avec le nombre d'hôtes ESX souhaité. La VMC sur AWS prend en charge les déploiements NetScaler VPX. VMC fournit une interface utilisateur identique à vCenter sur site. Il fonctionne de la même manière que les déploiements NetScaler VPX basés sur ESX.

Composants requis

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Un SDDC VMware doit être présent avec au moins un hôte.
- Téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments de réseau appropriés sur VMware SDDC auxquels les machines virtuelles se connectent.
- Obtenir des fichiers de licence VPX. Pour plus d'informations sur les licences d'instance NetScaler VPX, consultez le Guide des licences *NetScaler* VPX à l'adresse. http://support.citrix.com/article/ctx131110

Configuration matérielle du cloud VMware

Le tableau suivant répertorie les ressources informatiques virtuelles que le SDDC VMware doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 1. Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans VMware SDDC, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> Remarque
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production de l'appliance virtuelle VPX, l'allocation complète de mémoire doit être réservée.

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Le tableau suivant décrit la configuration minimale requise.

Tableau 2 Configuration minimale requise pour l'installation d'outils OVF

Composant	Exigences
OS	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
Carte d'interface réseau	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.

Téléchargement des fichiers de configuration de NetScaler VPX

Le package de configuration de l'instance NetScaler VPX pour VMware ESX respecte la norme de format Open Virtual Machine (OVF). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l' adresse http://www.citrix.com. Cliquez sur le **lien Nouveaux utilisateurs**et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

Citrix.com > **Téléchargements > NetScaler > Appliances virtuelles.**

Copiez les fichiers suivants sur une station de travail située sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (for example, NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (for example, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (for example, NSVPX-ESX-13.0-79.64.mf)

Installation d'une instance NetScaler VPX sur le cloud VMware

Après avoir installé et configuré VMware SDDC, vous pouvez utiliser le SDDC pour installer des dispositifs virtuels sur le cloud VMware. Le nombre d'appliances virtuelles que vous pouvez installer dépend de la quantité de mémoire disponible sur le SDDC.

Pour installer des instances NetScaler VPX sur le cloud VMware, procédez comme suit :

1. Ouvrez VMware SDDC sur votre poste de travail.
2. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur Connexion.
3. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
4. **Dans la boîte de dialogue**Déployer le modèle OVF**, dans**Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers de configuration de l'instance NetScaler VPX, sélectionnez le fichier .ovf et cliquez sur Suivant.**

   > **Remarque :** Par défaut, l'instance NetScaler VPX utilise les interfaces réseau E1000. Pour déployer ADC avec l'interface VMXNET3, modifiez l'OVF pour utiliser l'interface VMXNET3 au lieu de l'E1000.

5. Mappez les réseaux affichés dans le modèle OVF de l'appliance virtuelle aux réseaux que vous avez configurés sur VMware SDDC. Cliquez sur **Suivant** pour commencer à installer un dispositif virtuel sur VMware SDDC.
6. Vous êtes maintenant prêt à démarrer l'instance NetScaler VPX. **Dans le volet de navigation, sélectionnez l'instance NetScaler VPX que vous avez installée et, dans le menu contextuel, sélectionnez Power On.** Cliquez sur l'onglet **Console** pour émuler un port de console.
7. Si vous souhaitez installer un autre dispositif virtuel, répétez l'étape 6.
8. Spécifiez l'adresse IP de gestion du même segment que celui sélectionné pour être le réseau de gestion. Le même sous-réseau est utilisé pour la passerelle.
9. Le SDDC VMware exige que les règles NAT et pare-feu soient créées explicitement pour toutes les adresses IP privées appartenant à des segments réseau.

Installation d'une instance NetScaler VPX sur un serveur Microsoft Hyper-V

May 5, 2023

Pour installer des instances NetScaler VPX sur Microsoft Windows Server, vous devez d'abord installer Windows Server avec le rôle Hyper-V activé, sur un ordinateur disposant des ressources système adéquates. Lors de l'installation du rôle Hyper-V, assurez-vous de spécifier les cartes d'interface réseau sur le serveur qui sera utilisé par Hyper-V pour créer les réseaux virtuels. Vous pouvez réserver certaines cartes d'interface réseau pour l'hôte. Utilisez le gestionnaire Hyper-V pour effectuer l'installation de l'instance NetScaler VPX.

L'instance NetScaler VPX pour Hyper-V est fournie au format de disque dur virtuel (VHD). Il inclut la configuration par défaut pour des éléments tels que le CPU, les interfaces réseau, ainsi que la taille

et le format du disque dur. Après avoir installé l'instance NetScaler VPX, vous pouvez configurer les adaptateurs réseau sur une appliance virtuelle, ajouter des cartes réseau virtuelles, puis attribuer l'adresse IP NetScaler, le masque de sous-réseau et la passerelle, et terminer la configuration de base de l'appliance virtuelle.

Après la configuration initiale de l'instance VPX, si vous souhaitez mettre à niveau l'appliance vers la dernière version logicielle, voir Mettre à niveau une appliance autonome NetScalerVPX

> **Remarque**
>
> Le protocole ISIS (Intermediate System-to-Intermediate System) n'est pas pris en charge sur l'appliance virtuelle NetScaler VPX hébergée sur la plateforme HyperV-2012.

Conditions préalables à l'installation de l'instance NetScaler VPX sur des serveurs Microsoft

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Activez le rôle Hyper-V sur les serveurs Windows. Pour plus d'informations, veuillez consulter http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx.
- Téléchargez les fichiers de configuration de l'appliance virtuelle.
- Obtenez les fichiers de licence des instances NetScaler VPX. Pour plus d'informations sur les licences d'instance NetScaler VPX, consultez le Guide des licences *NetScaler* VPX à l'adresse. http://support.citrix.com/article/ctx131110

Configuration matérielle requise pour les serveurs Microsoft

Le tableau suivant décrit la configuration minimale requise pour les serveurs Microsoft.

Tableau 1. Configuration minimale requise pour les serveurs Microsoft

Composant	Exigences
UC	Processeur 64 bits 1,4 GHz
RAM	8 Go
Disk Space	32 Go ou plus

Le tableau suivant répertorie les ressources informatiques virtuelles pour chaque instance de NetScaler VPX.

Tableau 2 Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
RAM	4 Go
CPU virtuel	2
Disk Space	20 Go
Interfaces réseau virtuelles	1

Téléchargez les fichiers de configuration de NetScaler VPX

L'instance NetScaler VPX pour Hyper-V est fournie au format de disque dur virtuel (VHD). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l' adresse http://www.citrix.com, cliquez sur **Connexion > Mon compte > Créer un compte Citrix**, puis suivez les instructions pour créer un compte Citrix.

Pour télécharger les fichiers de configuration de l'instance NetScaler VPX, procédez comme suit :

1. Depuis un navigateur Web, accédez à http://www.citrix.com/.
2. Connectez-vous avec votre nom d'utilisateur et votre mot de passe.
3. Cliquez sur **Téléchargements**.
4. Dans le menu déroulant **Sélectionner un produit**, sélectionnez **NetScaler (NetScaler**ADC).
5. Sous **NetScaler Release X.X > Appliances virtuelles**, cliquez sur **NetScaler**VPX Release X.X
6. Téléchargez le fichier compressé sur votre serveur.

Installation de l'instance NetScaler VPX sur les serveurs Microsoft

Après avoir activé le rôle Hyper-V sur Microsoft Server et extrait les fichiers du dispositif virtuel, vous pouvez utiliser le gestionnaire Hyper-V pour installer l'instance NetScaler VPX. Après avoir importé la machine virtuelle, vous devez configurer les cartes réseau virtuelles en les associant aux réseaux virtuels créés par Hyper-V.

Vous pouvez configurer un maximum de huit cartes réseau virtuelles. Même si la carte réseau physique est hors service, l'appliance virtuelle suppose que la carte réseau virtuelle est active, car elle peut toujours communiquer avec les autres dispositifs virtuels sur le même hôte (serveur).

> **Remarque**
>
> Vous ne pouvez modifier aucun paramètre pendant que l'appliance virtuelle est en cours d'exécution. Arrêtez l'appliance virtuelle, puis apportez des modifications.

Pour installer une instance NetScaler VPX sur Microsoft Server à l'aide du gestionnaire Hyper-V :

1. Pour démarrer Hyper-V Manager, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **Gestionnaire Hyper-V**.
2. Dans le volet de navigation, sous **Hyper-V Manage**r, sélectionnez le serveur sur lequel vous souhaitez installer l'instance NetScaler VPX.
3. Dans le menu **Action**, cliquez sur **Importer une machine virtuelle**.
4. Dans la boîte de dialogue **Importer une machine virtuelle**, dans **Emplacement**, spécifiez le chemin du dossier qui contient les fichiers du logiciel de l'instance NetScaler VPX, puis sélectionnez **Copier la machine virtuelle (créer un nouvel identifiant unique**). Ce dossier est le dossier parent qui contient les dossiers Snapshots, Virtual Hard Disks et Virtual Machines.
5. Remarque : Si vous avez reçu un fichier compressé, assurez-vous de l'extraire dans un dossier avant de spécifier le chemin d'accès au dossier.
6. Cliquez sur **Importer**.
7. Vérifiez que le dispositif virtuel que vous avez importé est répertorié sous **Machines virtuelles**.
8. Pour installer un autre dispositif virtuel, répétez les étapes **2** à **6**.

> **Important**
>
> Assurez-vous d'extraire les fichiers vers un autre dossier à l'étape **4**.

Provisionner automatiquement une instance NetScaler VPX sur Hyper-V

Le provisionnement automatique de l'instance NetScaler VPX est facultatif. Si le provisionnement automatique n'est pas effectué, l'appliance virtuelle propose une option permettant de configurer l'adresse IP, etc.

Pour provisionner automatiquement une instance NetScaler VPX sur Hyper-V, procédez comme suit.

1. Créez une image ISO conforme à la norme ISO9660 à l'aide du fichier XML, comme illustré dans l'exemple. Assurez-vous que le nom du fichier XML est **userdata**.

   Vous pouvez créer un fichier ISO à partir d'un fichier XML en utilisant :

   • Tout outil de traitement d'image tel que PowerISO.

   • `mkisofs` commande sous Linux.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<Environment xmlns:oe=`"http://schemas.dmtf.org/ovf/environment/1`
    "

xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"

oe:id=""
```



```
8
9  xmlns=`"http://schemas.dmtf.org/ovf/environment/1`">
10
11 <PlatformSection>
12
13 <Kind>HYPER-V</Kind>
14
15 <Version>2013.1</Version>
16
17 <Vendor>CITRIX</Vendor>
18
19 <Locale>en</Locale>
20
21 </PlatformSection>
22
23 <PropertySection>
24
25 <Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"
      />
26
27 <Property oe:key="com.citrix.netscaler.platform" oe:value="NS1000V
      "/>
28
29 <Property oe:key="com.citrix.netscaler.orch_env" oe:value="cisco-
      orch-env"/>
30
31 <Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="
      10.102.100.122"/>
32
33 <Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
      255.255.255.128"/>
34
35 <Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
      10.102.100.67"/></PropertySection>
36
37 </Environment>
38 <!--NeedCopy-->
```

2. Copiez l'image ISO sur le serveur Hyper-V.
3. Sélectionnez l'appliance virtuelle que vous avez importée, puis dans le menu **Action**, sélectionnez **Paramètres**. Vous pouvez également sélectionner l'appliance virtuelle, puis cliquer avec le bouton droit de la souris et sélectionner **Paramètres**. La fenêtre **Paramètres** de l'appliance virtuelle sélectionnée s'affiche.

4. Dans la fenêtre **Paramètres**, sous la section Matériel, cliquez sur **Contrôleur IDE**.
5. Dans le volet de droite, sélectionnez **Lecteur DVD** et cliquez sur **Ajouter**. Le lecteur DVD est ajouté dans la section **IDE Controller** dans le volet gauche de la fenêtre.
6. Sélectionnez le **lecteur DVD** ajouté à l'étape 5. Dans le volet droit de la fenêtre, sélectionnez le bouton **radio Fichier image**, cliquez sur **Parcourir** et sélectionnez l'image ISO que vous avez copiée sur le serveur Hyper-V, à l'étape 2.
7. Cliquez sur **Appliquer**.

> **Remarque**
>
> L'instance d'appliance virtuelle apparaît à l'adresse IP par défaut, lorsque :
>
> - Le lecteur de DVD est joint et le fichier ISO n'est pas fourni.
> - Le fichier ISO n'inclut pas le fichier de données utilisateur.
> - Le nom ou le format du fichier de données utilisateur n'est pas correct.

Pour configurer des cartes réseau virtuelles sur l'instance NetScaler VPX, procédez comme suit :

1. Sélectionnez l'appliance virtuelle que vous avez importée, puis dans le menu **Action**, sélectionnez **Paramètres**.
2. Dans la <virtual appliance name>boîte de dialogue **Paramètres pour**, cliquez sur **Ajouter du matériel** dans le volet de gauche.
3. Dans le volet droit, dans la liste des appareils, sélectionnez **Adaptateur réseau**.
4. Cliquez sur **Ajouter**.
5. Vérifiez que **l'adaptateur réseau (non connecté)** apparaît dans le volet de gauche.
6. Sélectionnez l'adaptateur réseau dans le volet de gauche.
7. Dans le volet droit, dans le menu **Réseau**, sélectionnez le réseau virtuel auquel connecter l'adaptateur.
8. Pour sélectionner le réseau virtuel pour les autres adaptateurs réseau que vous souhaitez utiliser, répétez les étapes **6** et **7**.
9. Cliquez sur **Appliquer**, puis sur **OK**.

Pour configurer l'instance NetScaler VPX :

1. Cliquez avec le bouton droit sur l'appliance virtuelle que vous avez précédemment installée, puis sélectionnez **Démarrer**.
2. Accédez à la console en double-cliquant sur l'appliance virtuelle.
3. Tapez l'adresse IP NetScaler, le masque de sous-réseau et la passerelle de votre appliance virtuelle.

Vous avez terminé la configuration de base de votre appliance virtuelle. Entrez l'adresse IP dans un navigateur Web pour accéder à l'appliance virtuelle.

> **Remarque**
>
> Vous pouvez également utiliser un modèle de machine virtuelle (VM) pour provisionner une instance NetScaler VPX à l'aide de SCVMM.
>
> Si vous utilisez la solution d'association de cartes réseau Microsoft Hyper-V avec des instances NetScaler VPX, consultez l'article CTX224494 pour plus d'informations.

Installation d'une instance NetScaler VPX sur la plateforme Linux-KVM

May 5, 2023

Pour configurer un NetScaler VPX pour la plate-forme Linux-KVM, vous pouvez utiliser l'application graphique Virtual Machine Manager (Virtual Manager). Si vous préférez la ligne de commande Linux-KVM, vous pouvez utiliser le `virsh` programme.

Le système d'exploitation Linux hôte doit être installé sur du matériel approprié à l'aide d'outils de virtualisation tels que le module KVM et QEMU. Le nombre de machines virtuelles pouvant être déployées sur l'Hypervisor dépend des besoins de l'application et du matériel choisi.

Après avoir provisionné une instance NetScaler VPX, vous pouvez ajouter d'autres interfaces.

Limitations et directives d'utilisation

Recommandations générales

Pour éviter tout comportement imprévisible, appliquez les recommandations suivantes :

- Ne modifiez pas le MTU de l'interface VNet associée à la machine virtuelle VPX. Arrêtez la machine virtuelle VPX avant de modifier les paramètres de configuration, tels que les modes d'interface ou le processeur.
- Ne forcez pas l'arrêt de la machine virtuelle VPX. C'est-à-dire qu'il ne faut pas utiliser la commande **Forcer off** .
- Toutes les configurations effectuées sur le Linux hôte peuvent être persistantes ou non, selon les paramètres de votre distribution Linux. Vous pouvez choisir de rendre ces configurations persistantes pour garantir un comportement cohérent lors des redémarrages du système d'exploitation Linux hôte.
- Le package NetScaler doit être unique pour chacune des instances NetScaler VPX provisionnées.

Limitations

- La migration en direct d'une instance VPX exécutée sur KVM n'est pas prise en charge.

Conditions préalables à l'installation d'une instance NetScaler VPX sur une plateforme Linux-KVM

May 5, 2023

Vérifiez la configuration minimale requise pour un serveur Linux-KVM s'exécutant sur une instance NetScaler VPX.

Exigence du processeur :

- Processeurs x86 64 bits dotés de la fonctionnalité de virtualisation matérielle incluse dans les processeurs Intel VT-X.

Pour vérifier si votre processeur prend en charge l'hôte Linux, entrez la commande suivante à l'invite de commandes Linux de l'hôte :

```
\*.egrep '^flags.\*(vmx|svm)' /proc/cpuinfo*
<!--NeedCopy-->
```

Si les paramètres du **BIOS** de l'extension précédente sont désactivés, vous devez les activer dans le BIOS.

- Fournir au moins 2 cœurs CPU à Host Linux.
- Il n'y a pas de recommandation spécifique concernant la vitesse du processeur, mais plus la vitesse est élevée, meilleures sont les performances de l'application de machine virtuelle.

Mémoire (RAM) requise :

Minimum 4 Go pour le noyau Linux hôte. Ajoutez davantage de mémoire selon les besoins des machines virtuelles.

Disque dur requis :

Calculez l'espace requis pour le noyau Host Linux et les machines virtuelles. Une seule machine virtuelle NetScaler VPX nécessite 20 Go d'espace disque.

Configuration logicielle requise

Le noyau hôte utilisé doit être un noyau Linux 64 bits, version 2.6.20 ou ultérieure, avec tous les outils de virtualisation. Citrix recommande des noyaux plus récents, tels que 3.6.11-4 et versions ultérieures.

De nombreuses distributions Linux telles que Red Hat, CentOS et Fedora ont testé les versions du noyau et les outils de virtualisation associés.

Configuration matérielle requise pour les machines virtuelles invitées

NetScaler VPX prend en charge les types de disque dur IDE et VirtIO. Le type de disque dur a été configuré dans le fichier XML, qui fait partie du package NetScaler.

Exigences de mise en réseau

NetScaler VPX prend en charge les interfaces réseau VirtIO para-virtualisées, SR-IOV et PCI Passthrough.

Pour plus d'informations sur les interfaces réseau prises en charge, consultez :

- Provisionnez l'instance NetScaler VPX à l'aide du Virtual Machine Manager
- Configurer une instance NetScaler VPX pour utiliser les interfaces réseau SR-IOV
- Configurer une instance NetScaler VPX pour utiliser des interfaces réseau PCI passthrough

Interface source et modes

Le type de périphérique source peut être Bridge ou MacVTap. Dans MacVTAP, quatre modes sont possibles : VEPA, Bridge, Private et Pass-Through. Vérifiez les types d'interfaces que vous pouvez utiliser et les types de trafic pris en charge, comme suit :

Pont :

- Pont Linux.
- `Ebtables` et `iptables` les paramètres sur l'hôte Linux peuvent filtrer le trafic sur le pont si vous ne choisissez pas le bon paramètre ou si vous ne désactivez pas les `IPtable` services.

MacVTap (mode VEPA) :

- Des performances supérieures à celles d'un pont.
- Les interfaces du même périphérique inférieur peuvent être partagées entre les machines virtuelles.
- Communication inter-VM utilisant la même
- l'appareil inférieur n'est possible que si le commutateur en amont ou en aval prend en charge le mode VEPA.

MacVTap (mode privé) :

- Des performances supérieures à celles d'un pont.
- Les interfaces du même périphérique inférieur peuvent être partagées entre les machines virtuelles.
- La communication entre machines virtuelles utilisant le même périphérique inférieur n'est pas possible.

MacVtap (mode pont) :

- Meilleur comparativement au pont.
- Les interfaces situées sur le même appareil inférieur peuvent être partagées entre les machines virtuelles.
- La communication entre machines virtuelles utilisant le même périphérique inférieur est possible si la liaison inférieure du périphérique est UP.

MacVTap (mode Pass-through) :

- Meilleur comparativement au pont.
- Les interfaces hors du même appareil inférieur ne peuvent pas être partagées entre les machines virtuelles.
- Une seule machine virtuelle peut utiliser le périphérique inférieur.

> Remarque : Pour obtenir les meilleures performances de l'instance VPX, assurez-vous que les `lro` fonctionnalités `gro` et sont désactivées sur les interfaces source.

Propriétés des interfaces source

Assurez-vous de désactiver les fonctions generic-receve-offload (`gro`) et large receve-offload (`lro`) des interfaces source. Pour désactiver les `lro` fonctionnalités `gro` et, exécutez les commandes suivantes à l'invite du shell Linux hôte.

```
ethtool -K eth6 gro off
ethool -K eth6 lro off
```

Exemple :

```
1     [root@localhost ~]# ethtool -K eth6
2
3                   Offload parameters for eth6:
4
5                                       rx-checksumming: on
6
7                                       tx-checksumming: on
8
9                   scatter-gather: on
10
11                  tcp-segmentation-offload: on
12
13                  udp-fragmentation-offload: off
14
15                  generic-segmentation-offload: on
16
17                  generic-receive-offload: off
18
```



```
                    large-receive-offload: off

                    rx-vlan-offload: on

                    tx-vlan-offload: on

                    ntuple-filters: off

                    receive-hashing: on

    [root@localhost ~]#
<!--NeedCopy-->
```

Exemple :

Si le pont Linux hôte est utilisé comme périphérique source, comme dans l'exemple suivant, et que les `lro` fonctionnalités doivent être désactivées sur les interfaces VNet, qui sont les interfaces virtuelles connectant l'hôte aux machines virtuelles invitées.

```
    [root@localhost ~]# brctl show eth6_br

    bridge name     bridge  id               STP enabled interfaces

    eth6_br         8000.00e0ed1861ae          no         eth6

                                                          vnet0

                                                          vnet2

    [root@localhost ~]#
<!--NeedCopy-->
```

Dans l'exemple précédent, les deux interfaces virtuelles sont dérivées de eth6_br et sont représentées par vnet0 et vnet2. Exécutez les commandes suivantes pour désactiver `gro` et désactiver `lro` les fonctionnalités de ces interfaces.

```
    ethtool -K vnet0 gro off
            ethtool -K vnet2 gro off
            ethtool -K vnet0 lro off
                    ethtool -K vnet2 lro off
<!--NeedCopy-->
```


Mode promiscuité

Le mode promiscuous doit être activé pour que les fonctionnalités suivantes fonctionnent :

- Mode L2
- Traitement du trafic de multidiffusion
- Diffuser
- Trafic IPV6
- MAC virtuel
- Routage dynamique

Utilisez la commande suivante pour activer le mode promiscuité.

```
[root@localhost ~]# ifconfig eth6 promisc
[root@localhost ~]# ifconfig eth6
eth6       Link encap:Ethernet  HWaddr 78:2b:cb:51:54:a3
            inet6 addr: fe80::7a2b:cbff:fe51:54a3/64 Scope:Link
            UP BROADCAST RUNNING PROMISC MULTICAST  MTU:9000  Metric:1
            RX packets:142961 errors:0 dropped:0 overruns:0 frame:0
            TX packets:2895843 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:14330008 (14.3 MB)  TX bytes:1019416071 (1.0 GB)

[root@localhost ~]#
<!--NeedCopy-->
```

Module requis

Pour de meilleures performances réseau, assurez-vous que le module vhost_net est présent sur l'hôte Linux. Pour vérifier l'existence du module vhost_net, exécutez la commande suivante sur l'hôte Linux :

```
lsmod | grep "vhost_net"
<!--NeedCopy-->
```

Si vhost_net n'est pas encore en cours d'exécution, entrez la commande suivante pour l'exécuter :

```
modprobe vhost_net
<!--NeedCopy-->
```

Provisionner l'instance NetScaler VPX à l'aide d'OpenStack

May 8, 2023

Vous pouvez provisionner une instance NetScaler VPX dans un environnement OpenStack à l'aide de la commande **Nova boot** (OpenStack CLI) ou d'Horizon (tableau de bord OpenStack).

Le provisioning d'une instance VPX implique éventuellement l'utilisation de données provenant du lecteur de configuration. Le lecteur de configuration est un lecteur de configuration spécial qui se connecte à l'instance en tant que lecteur de CD-ROM lors de son démarrage. Ce lecteur de configuration peut être utilisé pour transmettre des configurations réseau telles que l'adresse IP de gestion, le masque réseau, la passerelle par défaut et pour injecter des scripts client.

Dans une appliance NetScaler, le mécanisme d'authentification par défaut est basé sur un mot de passe. Le mécanisme d'authentification par paire de clés SSH est désormais pris en charge pour les instances NetScaler VPX dans l'environnement OpenStack.

La paire de clés (clé publique et clé privée) est générée avant d'utiliser le mécanisme de cryptographie à clé publique. Vous pouvez utiliser différents mécanismes, tels que Horizon, Puttygen.exe pour Windows et `ssh-keygen` pour l'environnement Linux, pour générer la paire de clés. Reportez-vous à la documentation en ligne des mécanismes respectifs pour plus d'informations sur la génération de paires de clés.

Une fois qu'une paire de clés est disponible, copiez la clé privée dans un emplacement sécurisé auquel les personnes autorisées ont accès. Dans OpenStack, la clé publique peut être déployée sur une instance VPX à l'aide de la commande Horizon ou Nova boot. Lorsqu'une instance VPX est provisionnée à l'aide d'OpenStack, elle détecte d'abord que l'instance démarre dans un environnement OpenStack en lisant une chaîne BIOS spécifique. Cette chaîne est « OpenStack Foundation » et pour les distributions Red Hat Linux, elle est stockée dans /etc/nova/release. Il s'agit d'un mécanisme standard disponible dans toutes les implémentations OpenStack basées sur la plateforme d'hyperviseur KVM. Le disque doit comporter une étiquette OpenStack spécifique.

Si le lecteur de configuration est détecté, l'instance tente de lire la configuration réseau, les scripts personnalisés et la paire de clés SSH si elle est fournie.

Fichier de données utilisateur

L'instance NetScaler VPX utilise un fichier OVF personnalisé, également appelé fichier de données utilisateur, pour injecter la configuration réseau et des scripts personnalisés. Ce fichier est fourni dans le cadre du lecteur de configuration. Voici un exemple de fichier OVF personnalisé.

```
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1"
xmlns:cs="http://schemas.citrix.com/openstack">
```

 
```

```
<PlatformSection>
<Kind></Kind>
<Version>2016.1</Version>
<Vendor>VPX</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
<Property oe:key="com.citrix.netscaler.orch_env" oe:value="openstack-
   orch-env"/>
<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
   255.255.255.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1
   "/>
</PropertySection>
 <cs:ScriptSection>
   <cs:Version>1.0</cs:Version>
     <ScriptSettingSection xmlns="http://schemas.citrix.com/openstack"
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
         <Scripts>
           <Script>
                 <Type>shell</Type>
                 <Parameter>X Y</Parameter>
                <Parameter>Z</Parameter>
                <BootScript>before</BootScript>
                  <Text>
                        #!/bin/bash
                        echo "Hi, how are you" $1 $2 >> /var/sample.txt
                  </Text>
           </Script>
           <Script>
                 <Type>python</Type>
                 <BootScript>after</BootScript>
                  <Text>
                       #!/bin/python
print("Hello");
                  </Text>
           </Script>
   <Script>
                 <Type>perl</Type>
                 <BootScript>before</BootScript>
                  <Text>
                       !/usr/bin/perl
```



```
49  my $name = "VPX";
50  print "Hello, World $name !\n" ;
51                      </Text>
52              </Script>
53              <Script>
54                   <Type>nscli</Type>
55                   <BootScript>after</BootScript>
56                   <Text>
57                    add vlan 33
58  bind vlan 33 -ifnum 1/2
59                   </Text>
60              </Script>
61            </Scripts>
62        </ScriptSettingSection>
63   </cs:ScriptSection>
64 </Environment>
65 <!--NeedCopy--> ```
```

Dans le fichier OVF qui précède, « PropertySection » est utilisé pour la configuration réseau de NetScaler tandis que \ <cs:ScriptSection> est utilisé pour inclure tous les scripts. Les balises <Scripts> \ \ </Scripts> sont utilisées pour regrouper tous les scripts. Chaque script est défini entre des balises <Script> \ \ </Script>. Chaque balise de script comporte les champs/balises suivants :

a) \ <Type> : Spécifie la valeur du type de script. Valeurs possibles : Shell/Perl/Python/NSLCI (pour les scripts NetScaler CLI)

b) \ <Parameter> : Fournit des paramètres au script. Chaque script peut comporter plusieurs \ <Parameter> tags.

c) \ <BootScript> : Spécifie le point d'exécution du script. Valeurs possibles pour cette balise : avant/après. « avant » indique que le script est exécuté avant l'apparition de PE. « after » indique que le script sera exécuté après l'arrivée de PE.

d) \ <Text> : Colle le contenu d'un script.

> **Remarque**
>
> Actuellement, l'instance VPX ne prend pas en charge la désinfection des scripts. En tant qu'administrateur, vous devez vérifier la validité du script.
>
> Toutes les sections ne doivent pas être présentes. Utilisez une « PropertySection » vide pour définir uniquement les scripts à exécuter au premier démarrage ou une fenêtre vide pour définir uniquement la configuration réseau.
>
> Une fois que les sections requises du fichier OVF (fichier de données utilisateur) sont remplies, utilisez ce fichier pour provisionner l'instance VPX.

Configuration réseau

Dans le cadre de la configuration réseau, l'instance VPX lit :

- Adresse IP de gestion
- Masque réseau
- passerelle par défaut

Une fois les paramètres correctement lus, ils sont renseignés dans la configuration de NetScaler, afin de permettre la gestion de l'instance à distance. Si les paramètres ne sont pas lus correctement ou si le lecteur de configuration n'est pas disponible, l'instance passe au comportement par défaut, qui est le suivant :

- L'instance tente de récupérer les informations d'adresse IP à partir de DHCP.
- Si DHCP échoue ou s'arrête, l'instance présente la configuration réseau par défaut (192.168.100.1/16).

Script client

L'instance VPX permet d'exécuter un script personnalisé pendant le provisionnement initial. L'appliance prend en charge les scripts de type Shell, Perl, Python et les commandes CLI NetScaler.

Authentification par paire de clés SSH

L'instance VPX copie la clé publique, disponible dans le lecteur de configuration en tant que partie des métadonnées de l'instance, dans son fichier « authorized_keys ». Cela permet à l'utilisateur d'accéder à l'instance à l'aide d'une clé privée.

> **Remarque**
>
> Lorsqu'une clé SSH est fournie, les informations d'identification par défaut (nsroot/nsroot) ne fonctionnent plus. Si un accès par mot de passe est nécessaire, ouvrez une session avec la clé privée SSH respective et définissez manuellement un mot de passe.

Avant de commencer

Avant de provisionner une instance VPX sur un environnement OpenStack, extrayez le `.qcow2` fichier du fichier .tgz et générez

Une image OpenStack de l'image qcow2. Procédez comme suit :

1. Extrayez le `.qcow2` fichier du `.tqz` fichier en tapant la commande suivante

```
tar xvzf <TAR file>
tar xvzf <NSVPX-KVM-12.0-26.2_nc.tgz>
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
```


2. Créez une image OpenStack à l'aide du `.qcoz2` fichier extrait à l'étape 1 en tapant la commande suivante.

```
openstack image create --container-format bare --property
    hw_disk_bus=ide --disk-format qcow2 --file <path to qcow2 file>
     --public <name of the OpenStack image>

glance image-create --name="NS-VPX-12-0-26-2" --property
    hw_disk_bus=ide --ispublic=
true --container-format=bare --disk-format=qcow2< NSVPX-KVM
    -12.0-26.2_nc.qcow2
```

Figure 1 : L'illustration suivante fournit un exemple de sortie pour la commande glance image-create.

```
+------------------+--------------------------------------------------------+
| Field            | Value                                                  |
+------------------+--------------------------------------------------------+
| checksum         | 154ade3fc7dca7d1706b1d03d7d97552                       |
| container_format | bare                                                   |
| created_at       | 2017-03-13T08:52:31Z                                   |
| disk_format      | qcow2                                                  |
| file             | /v2/images/322c1e0f-cce8-4b7b-b53e-bd8152c388ed/file   |
| id               | 322c1e0f-cce8-4b7b-b53e-bd8152c388ed                   |
| min_disk         | 0                                                      |
| min_ram          | 0                                                      |
| name             | VPX-KVM-12.0-26.2
| owner            | 58d17d81df5d4406afbb4fdab3a58d79                       |
| properties       | hw_disk_bus='ide'                                      |
| protected        | False                                                  |
| schema           | /v2/schemas/image                                      |
| size             | 784338944                                              |
| status           | active                                                 |
| updated_at       | 2017-03-13T08:52:43Z                                   |
| virtual_size     | None                                                   |
| visibility       | public                                                 |
+------------------+--------------------------------------------------------+
```

Provisionnement de l'instance VPX

Vous pouvez provisionner une instance VPX de deux manières en utilisant l'une des options suivantes :

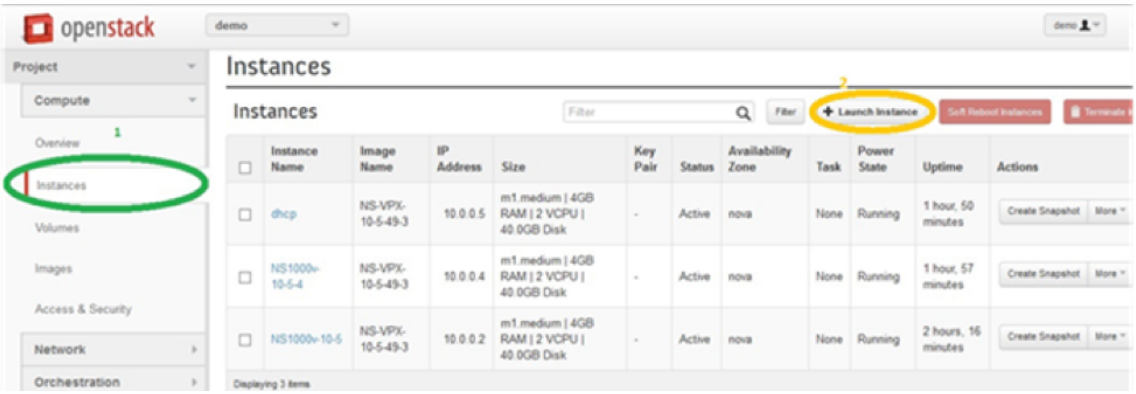
- Horizon (tableau de bord OpenStack)
- Commande de démarrage Nova (CLI OpenStack)

Provisionner une instance VPX à l'aide du tableau de bord OpenStack

Suivez ces étapes pour provisionner l'instance VPX à l'aide d'Horizon :

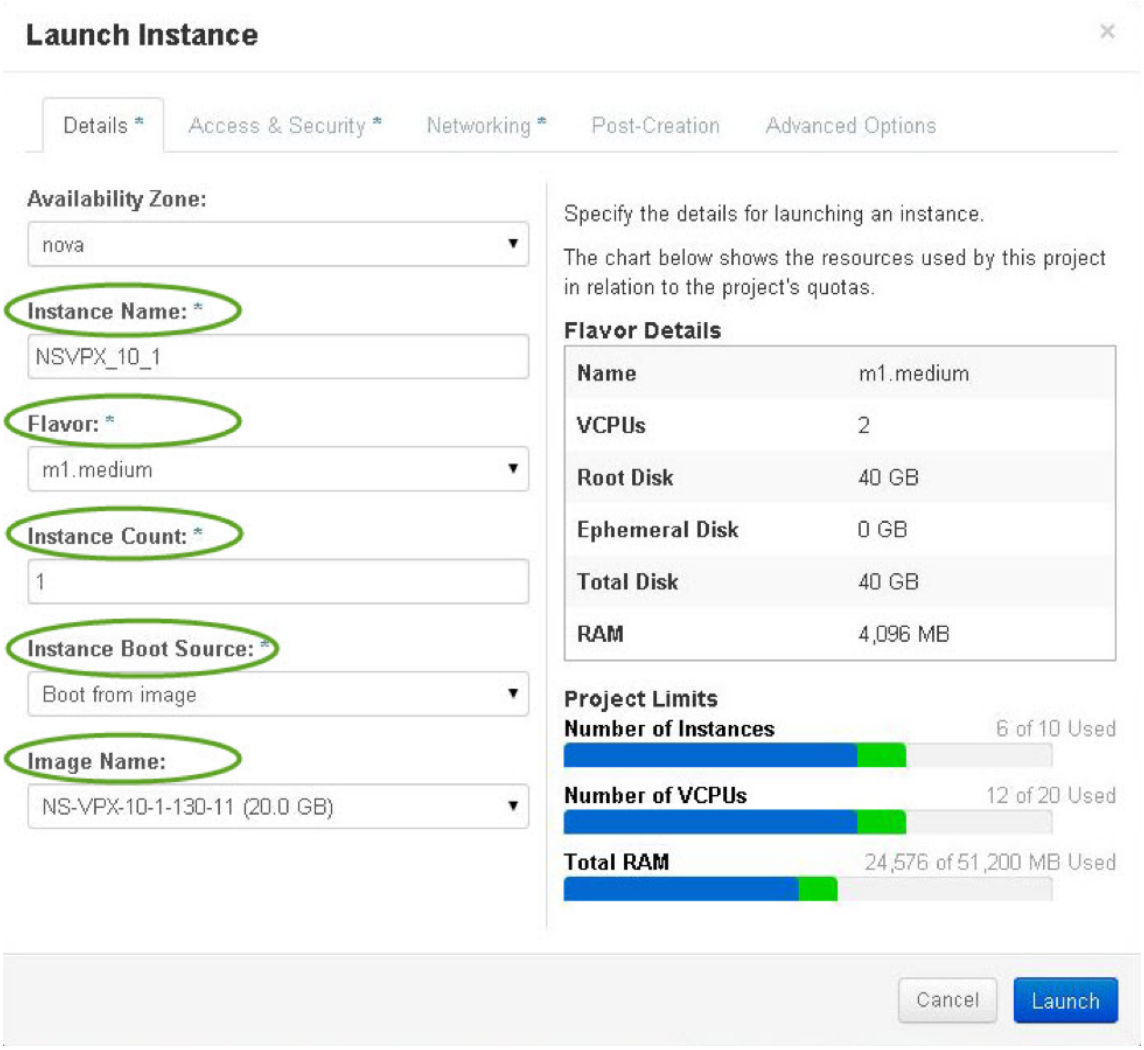
1. Connectez-vous au tableau de bord OpenStack.
2. Dans le panneau Projet sur le côté gauche du tableau de bord, sélectionnez **Instances**.

3. Dans le panneau Instances, cliquez sur **Lancer une instance** pour ouvrir l'Assistant Lancement d'instance.



4. Dans l'assistant de lancement d'instance, entrez les détails, tels que :

   a) Nom de l'instance
   b) Saveur d'instance
   c) Nombre d'instances
   d) Source de démarrage de l'instance
   e) Nom de l'image



5. Déployez une nouvelle paire de clés ou une paire de clés existante via Horizon en procédant comme suit :

   a) Si vous n'avez pas de paire de clés existante, créez-la à l'aide des mécanismes existants. Si vous possédez déjà une clé, ignorez cette étape.

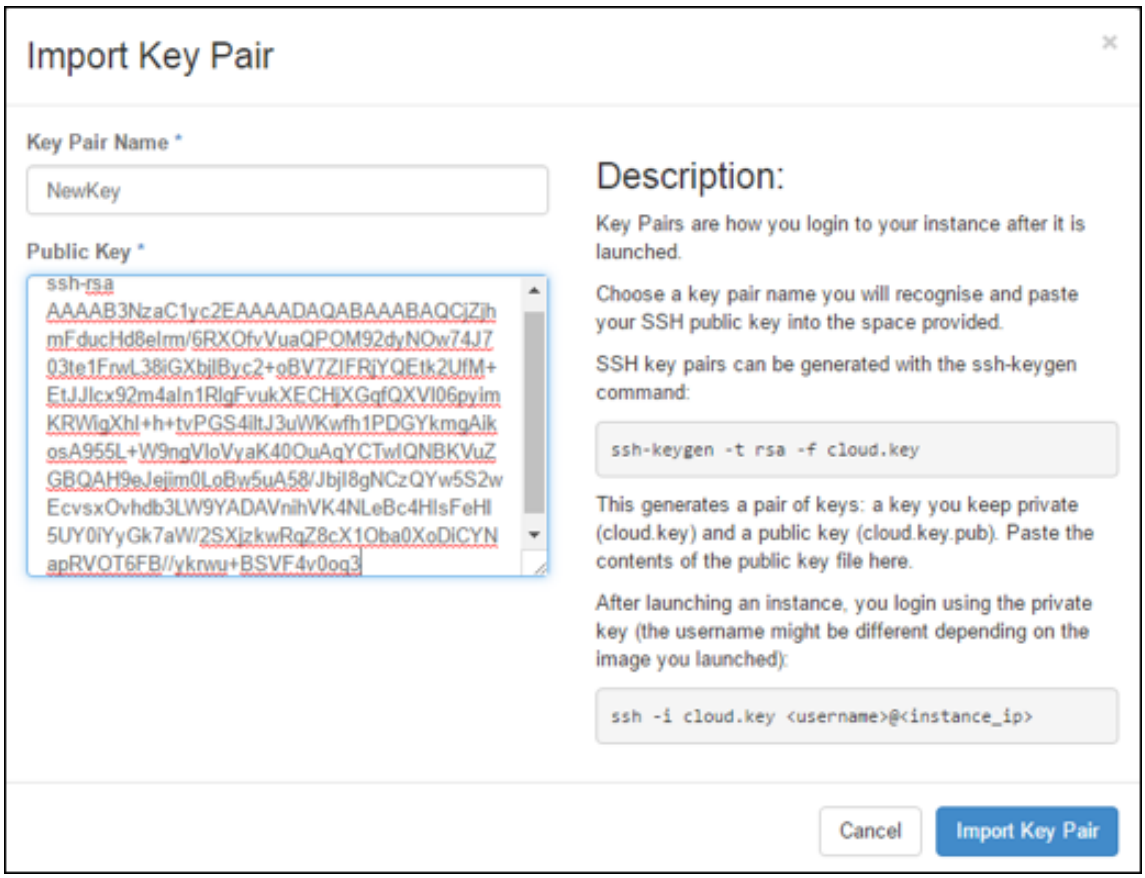
   b) Copiez le contenu de la clé publique.

   c) Accédez à **Horizon > Instances > Créer de nouvelles instances**.

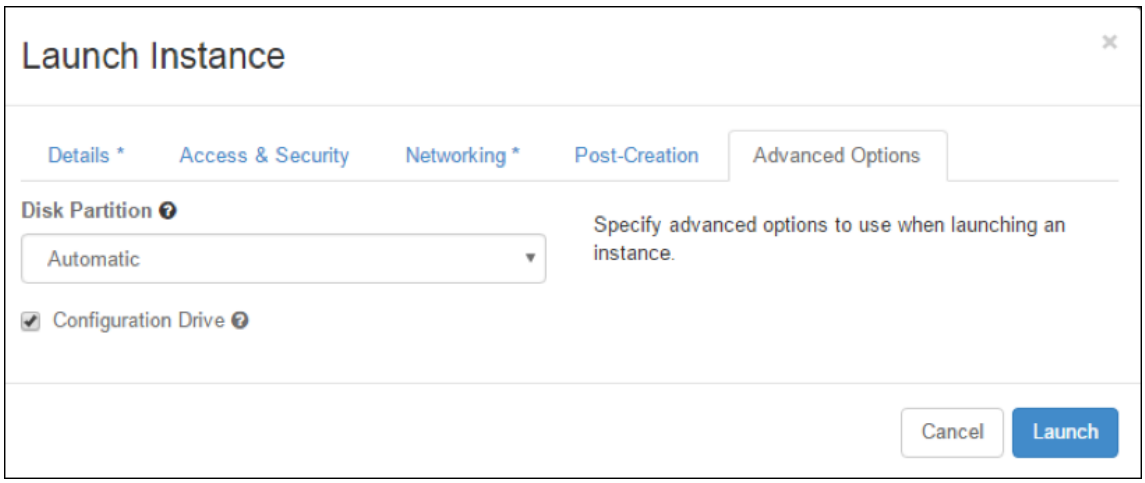
   d) Cliquez sur **Accès et sécurité**.

   e) Cliquez sur le signe + à côté du menu déroulant **Key Pair** et fournissez des valeurs pour les paramètres affichés.

   f) Collez le contenu de la *clé publique dans la zone Clé publique*, donnez un nom à la clé et cliquez sur **Importer la paire de clés** .



6. Cliquez sur l'onglet **Création de publications** dans l'Assistant. Dans le script de personnalisation, ajoutez le contenu du fichier de données utilisateur. Le fichier de données utilisateur contient l'adresse IP, les détails du masque réseau et de la passerelle, ainsi que les scripts client de l'instance VPX.
7. Une fois qu'une paire de clés est sélectionnée ou importée, cochez l'option config-drive et cliquez sur **Launch**.



Provisionner l'instance VPX à l'aide de l'interface de ligne de commande OpenStack

Suivez ces étapes pour provisionner une instance VPX à l'aide de l'interface de ligne de commande OpenStack.

1. Pour créer une image à partir de qcow2, tapez la commande suivante :

   ```
   openstack image create --container-format bare --property hw_disk_bus=
   ide --diskformat qcow2 --file NSVPX-OpenStack.qcow2 --public VPX-ToT-
   Image
   ```

2. Pour sélectionner une image afin de créer une instance, tapez la commande suivante :

   ```
   openstack image list | more
   ```

3. Pour créer une instance d'une saveur particulière, tapez la commande suivante pour choisir un identifiant/un nom de saveur parmi une liste :

   ```
   openstack flavor list
   ```

4. Pour connecter une carte réseau à un réseau particulier, tapez la commande suivante pour choisir un ID réseau dans une liste de réseaux :

   ```
   openstack network list
   ```

5. Pour créer une instance, tapez la commande suivante :

   ```
   1 openstack server create --flavor FLAVOR_ID --image IMAGE_ID --key-
       name KEY_NAME
   2 --user-data USER_DATA_FILE_PATH --config-drive True --nic net-id=
       net-uuid
   3 INSTANCE_NAME
   4 openstack server create --image VPX-ToT-Image --flavor m1.medium
       --user-data
   5 ovf.xml --config-drive True --nic net-id=2734911b-ee2b-48d0-a1b6-3
       efd44b761b9
   6 VPX-ToT
   ```

Figure 2 : L'illustration suivante fournit un exemple de sortie.

Field	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	None
OS-EXT-SRV-ATTR:hypervisor_hostname	None
OS-EXT-SRV-ATTR:instance_name	instance-000001c2
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	None
OS-SRV-USG:terminated_at	None
accessIPv4	
accessIPv6	
addresses	
adminPass	pFVvMtq7N8Z6
config_drive	True
created	2017-03-13T10:32:59Z
flavor	m1.medium (3)
hostId	
id	a1fe991e-3604-43a0-9dd6-59fa0f3749df
image	VPX-ToT-Image (f0c2f9d1-08f2-4b2e-9943-2ee6bc2edbc7)
key_name	None
name	VPX-ToT
os-extended-volumes:volumes_attached	[]
progress	0
project_id	58d17d81df5d4406afbb4fdab3a58d79
properties	
security_groups	[{u'name': u'default'}]
status	BUILD
updated	2017-03-13T10:33:00Z
user_id	a6347b33916b4eb1b1f76360a9c8f935

Provisionnez l’instance NetScaler VPX à l’aide du Virtual Machine Manager

May 5, 2023

Le Virtual Machine Manager est un outil de bureau permettant de gérer les hôtes des machines virtuelles. Il vous permet de créer de nouveaux hôtes de machines virtuelles et différents types de stockage, et de gérer des réseaux virtuels. Vous pouvez accéder à la console graphique des hôtes des machines virtuelles à l’aide du visualiseur VNC intégré et consulter les statistiques de performances, localement ou à distance.

Après avoir installé votre distribution Linux préférée, avec la virtualisation KVM activée, vous pouvez procéder au provisionnement des machines virtuelles.

Lorsque vous utilisez le Virtual Machine Manager pour provisionner une instance NetScaler VPX, deux options s’offrent à vous :

- Entrez manuellement l’adresse IP, la passerelle et le masque de réseau
- Attribuez automatiquement l’adresse IP, la passerelle et le masque de réseau (provisionnement automatique)

Vous pouvez utiliser deux types d’images pour provisionner une instance NetScaler VPX :

- CRU

- QCOW2

Vous pouvez convertir une image RAW NetScaler VPX en image QCOW2 et provisionner l'instance NetScaler VPX. Pour convertir l'image RAW en image QCOW2, tapez la commande suivante :

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow
```

Par exemple :

```
qemu-img convert -O qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5_nc
.qcow
```

Un déploiement standard de NetScaler VPX sur KVM comprend les étapes suivantes :

- Vérification des prérequis pour le Provisioning automatique d'une instance NetScaler VPX
- Provisioning de l'instance NetScaler VPX à l'aide d'une image RAW
- Provisioning de l'instance NetScaler VPX à l'aide d'une image QCOW2
- Ajouter des interfaces supplémentaires à une instance VPX à l'aide de Virtual Machine Manager

Vérifiez les conditions requises pour le provisionnement automatique d'une instance NetScaler VPX

Le provisionnement automatique est une fonctionnalité optionnelle qui implique l'utilisation des données du lecteur de CD-ROM. Si cette fonctionnalité est activée, il n'est pas nécessaire de saisir l'adresse IP de gestion, le masque réseau et la passerelle par défaut de l'instance NetScaler VPX lors de la configuration initiale.

Vous devez effectuer les tâches suivantes avant de pouvoir provisionner automatiquement une instance VPX :

1. Créez un fichier XML OVF (Open Virtualization Format) personnalisé ou un fichier de données utilisateur.
2. Convertissez le fichier OVF en image ISO à l'aide d'une application en ligne (par exemple PowerISO).
3. Montez l'image ISO sur l'hôte KVM à l'aide de n'importe quel outil SCP (Secure Copy).

Exemple de fichier XML OVF :

Voici un exemple de contenu d'un fichier XML OVF, que vous pouvez utiliser comme exemple pour créer votre fichier.

```
1 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2
3 <Environment xmlns:oe="`http://schemas.dmtf.org/ovf/environment/1"`
4
5 xmlns:xsi="`http://www.w3.org/2001/XMLSchema-instance"`
6
```



```
oe:id=""

xmlns="`http://schemas.dmtf.org/ovf/environment/1"`

xmlns:cs="`http://schemas.citrix.com/openstack">`

<PlatformSection>

<Kind></Kind>

<Version>2016.1</Version>

<Vendor>VPX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>

<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>

<Property oe:key="com.citrix.netscaler.orch_env" oe:value="KVM"/>

<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>

<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
   255.255.255.0"/>

<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1
   "/>

</PropertySection>

</Environment>
<!--NeedCopy-->
```

Dans le fichier XML OVF précédent, « PropertySection » est utilisé pour la configuration réseau NetScaler. Lorsque vous créez le fichier, spécifiez les valeurs des paramètres qui sont mis en surbrillance à la fin de l'exemple :

- Adresse IP de gestion
- Masque réseau

- Gateway

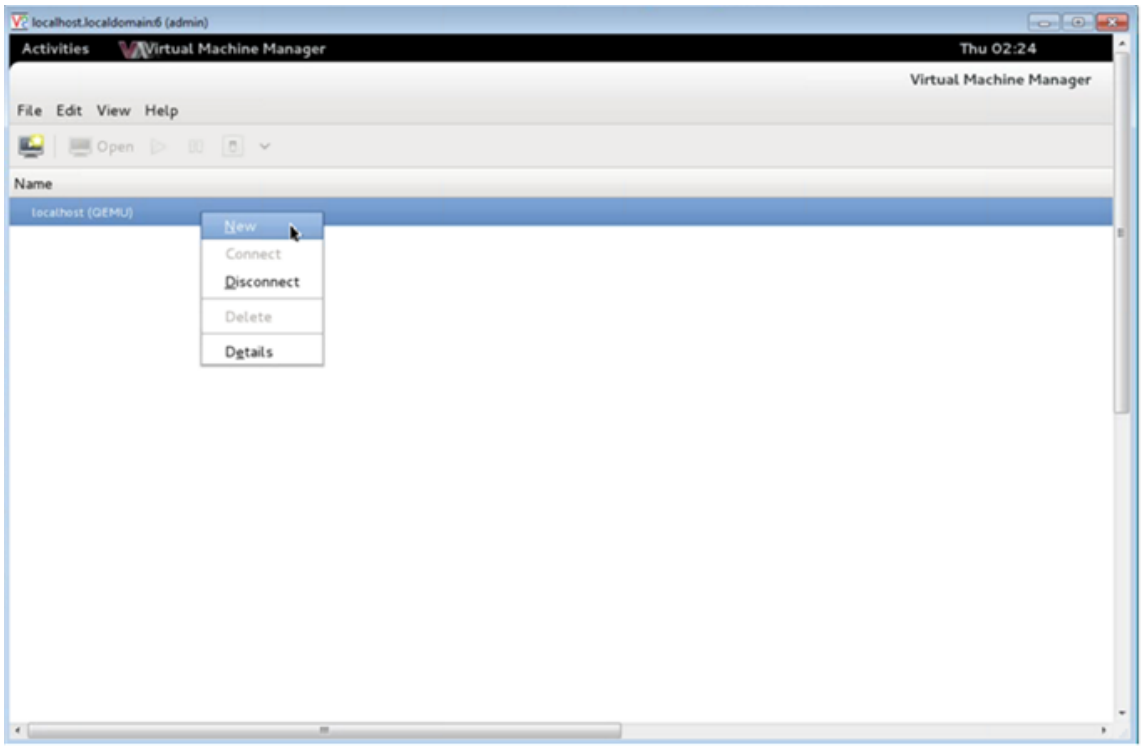
> **Important**
>
> Si le fichier OVF n'est pas correctement formaté au format XML, l'instance VPX se voit attribuer la configuration réseau par défaut, et non les valeurs spécifiées dans le fichier.

Provisionnez l'instance NetScaler VPX à l'aide d'une image RAW

Le Virtual Machine Manager vous permet de provisionner une instance NetScaler VPX à l'aide d'une image RAW.

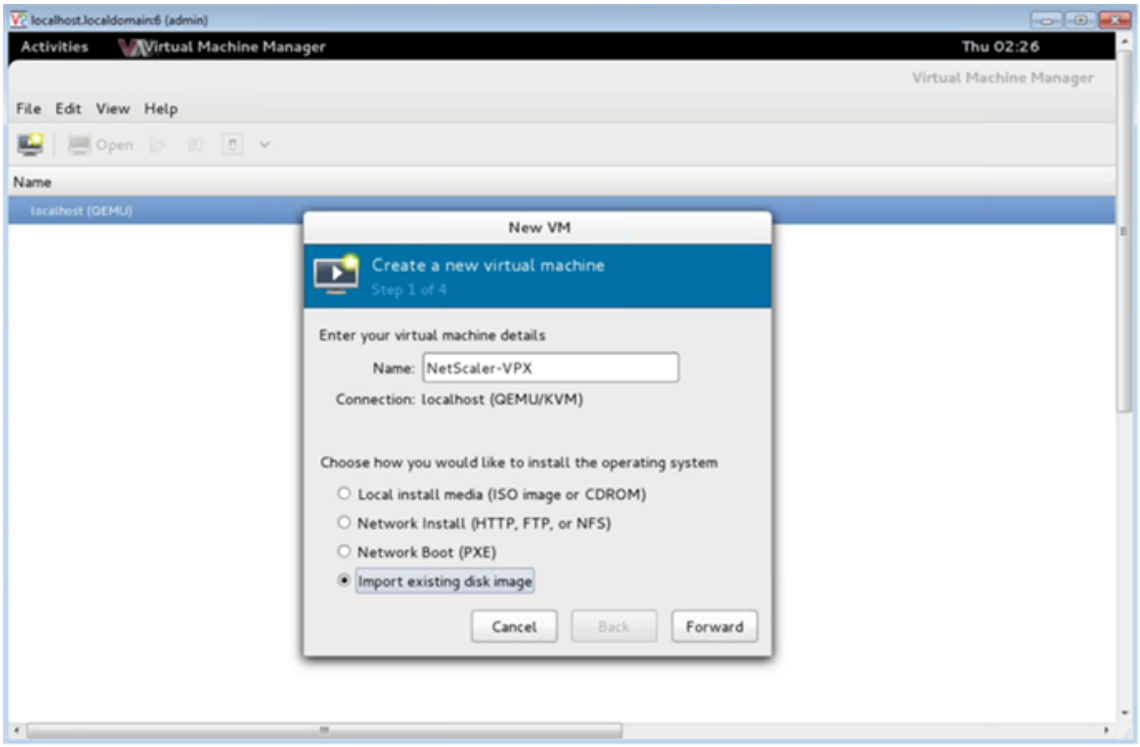
Pour provisionner une instance NetScaler VPX à l'aide du Virtual Machine Manager, procédez comme suit :

1. Ouvrez Virtual Machine Manager (**Application** > **Outils système** > **Virtual Machine Manager**) et entrez les informations d'identification d'ouverture de session dans la fenêtre **Authentifier** .
2. Cliquez sur l'icône  ou cliquez avec le bouton droit sur **localhost (QEMU)** pour créer une nouvelle instance NetScaler VPX.

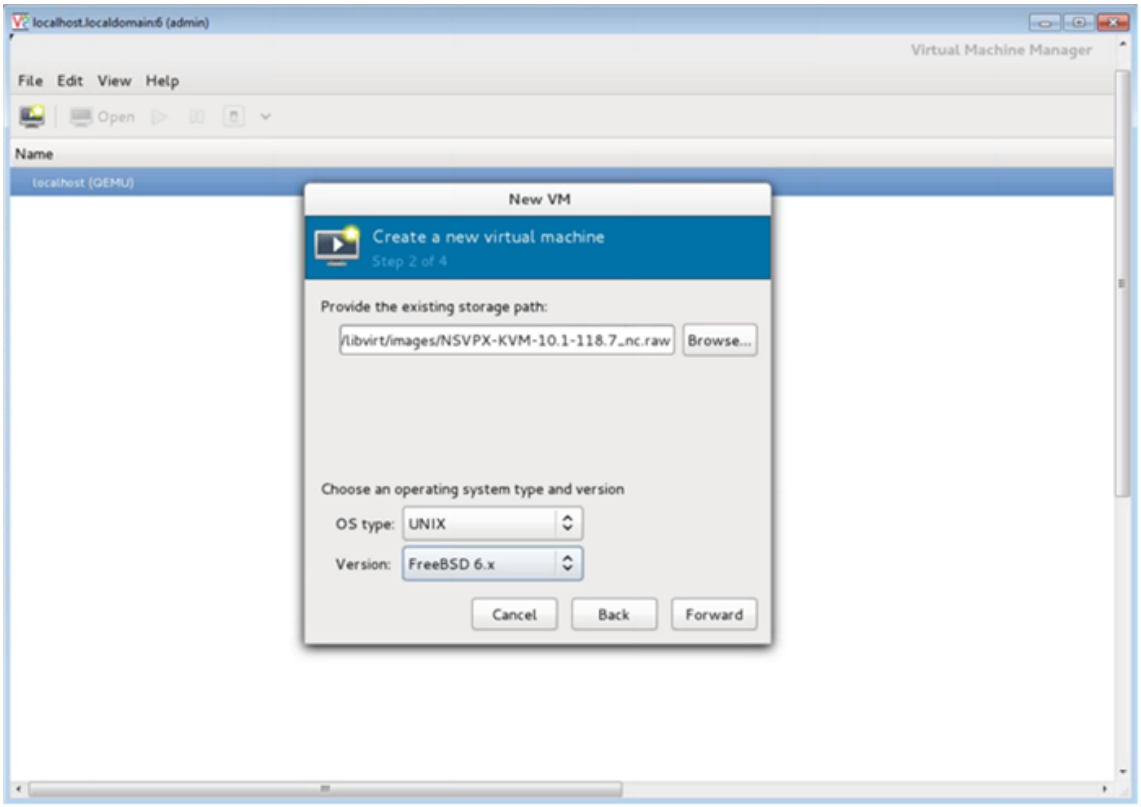


3. Dans la zone de texte **Nom**, entrez le nom de la nouvelle machine virtuelle (par exemple, Netscaler-VPX).
4. Dans la fenêtre **Nouvelle machine virtuelle**, sous « Choisissez la manière dont vous souhaitez installer le système d'exploitation », sélectionnez **Importer une image disque existante**, puis

cliquez sur **Suivant**.

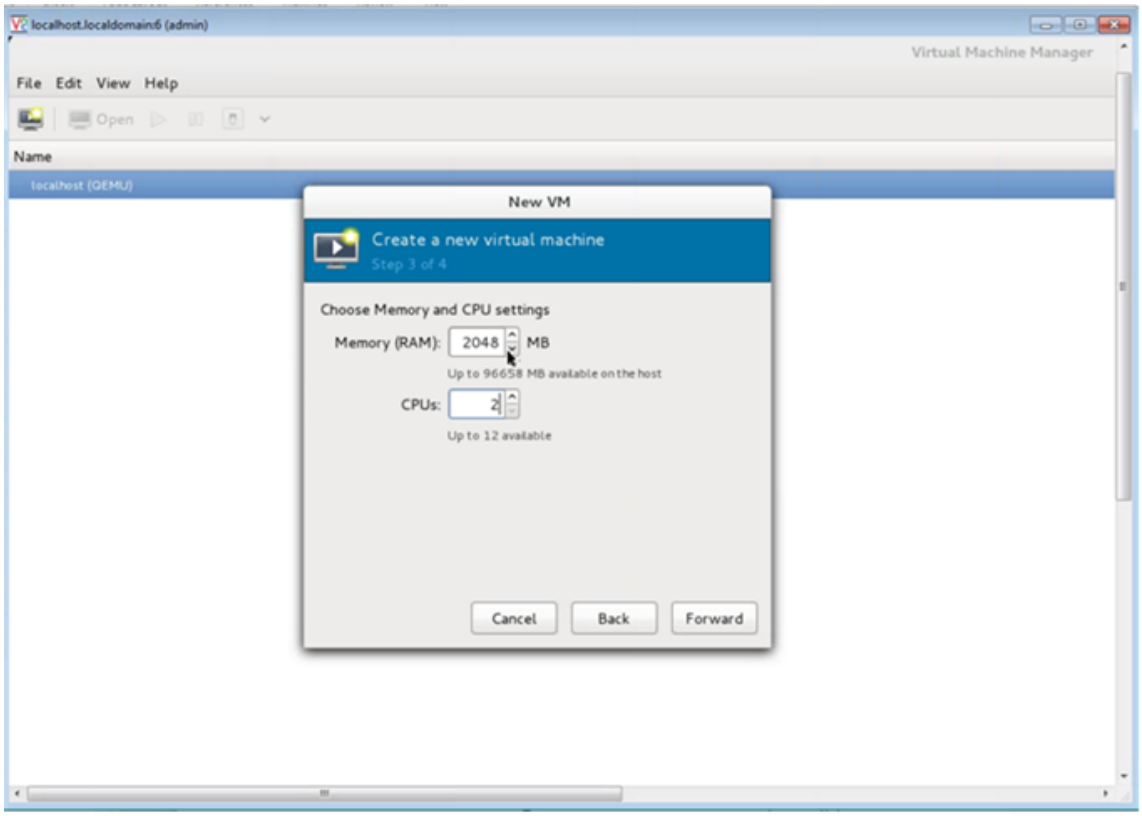


5. Dans le champ **Fournir le chemin de stockage existant**, parcourez le chemin d'accès à l'image. Choisissez le type de système d'exploitation UNIX et la version FreeBSD 6.x. Cliquez ensuite sur **Suivant**.

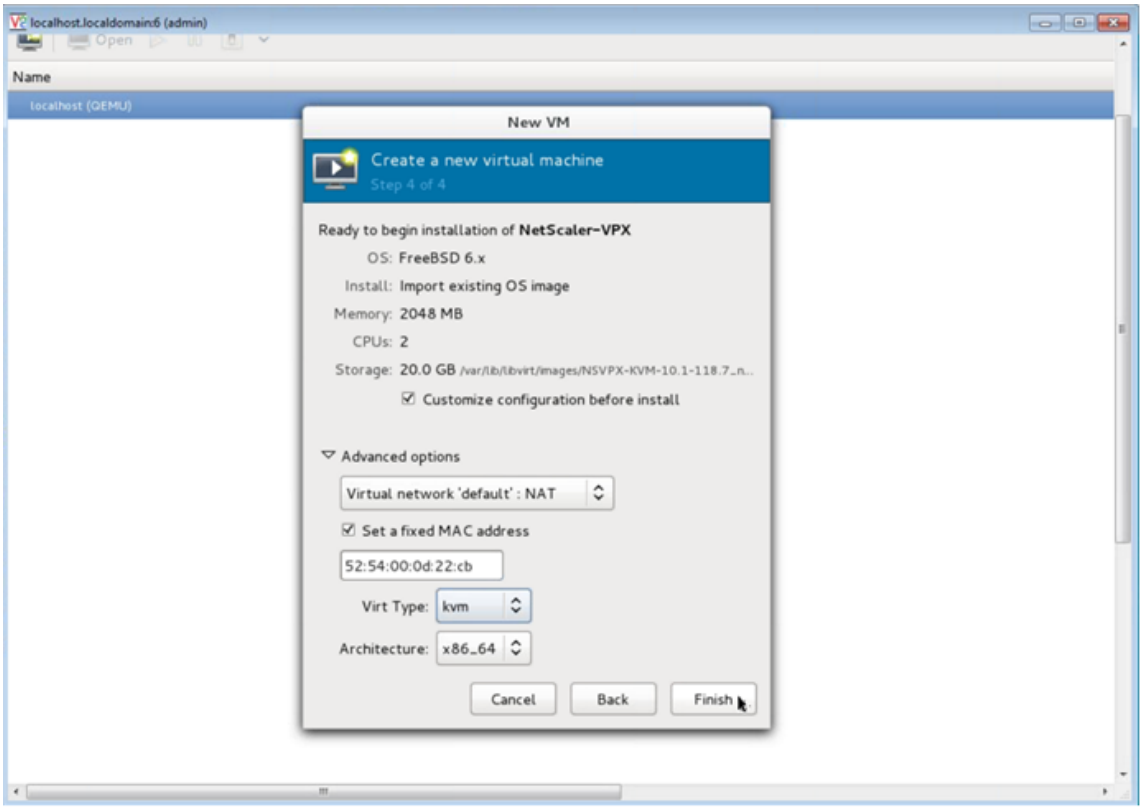


6. Sous **Choisir les paramètres de mémoire et de processeur**, sélectionnez les paramètres suivants, puis cliquez sur **Suivant** :

   - Mémoire (RAM) — 2048 Mo
   - Processeurs : 2

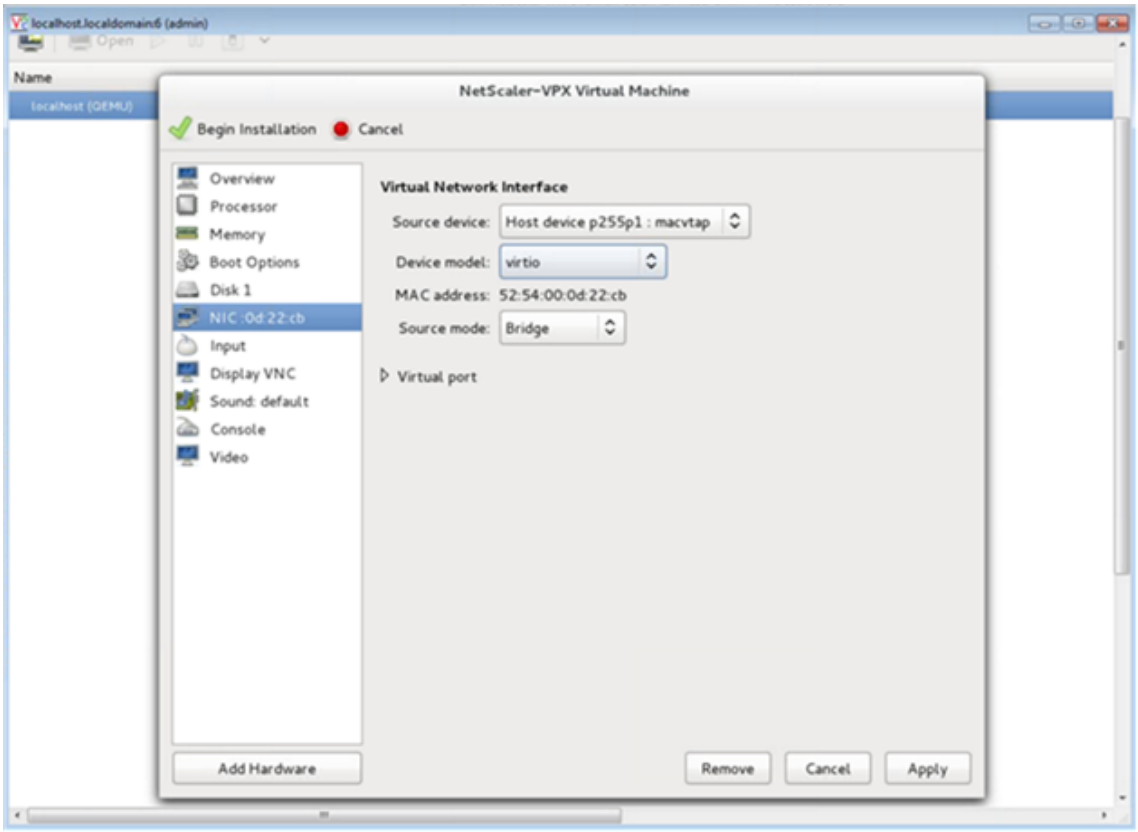


7. Activez la case à cocher **Personnaliser la configuration avant l'installation** . Le cas échéant, sous **Options avancées**, vous pouvez personnaliser l'adresse MAC. Assurez-vous que le **type Virt** sélectionné est KVM et que l'architecture sélectionnée est x86_64. Cliquez sur **Finish**.



8. Sélectionnez une carte réseau et fournissez la configuration suivante :

   - Périphérique source `ethX macvtap` ou Bridge
   - Modèle d'appareil— `virtio`
   - Mode source : Bridge



9. Cliquez sur **Appliquer**.
10. Si vous souhaitez provisionner automatiquement l'instance VPX, consultez la section **Activer le Provisioning automatique en attachant un lecteur de CD-ROM** dans ce document. Sinon, cliquez sur **Commencer l'installation**. Après avoir configuré le NetScaler VPX sur KVM, vous pouvez ajouter d'autres interfaces.

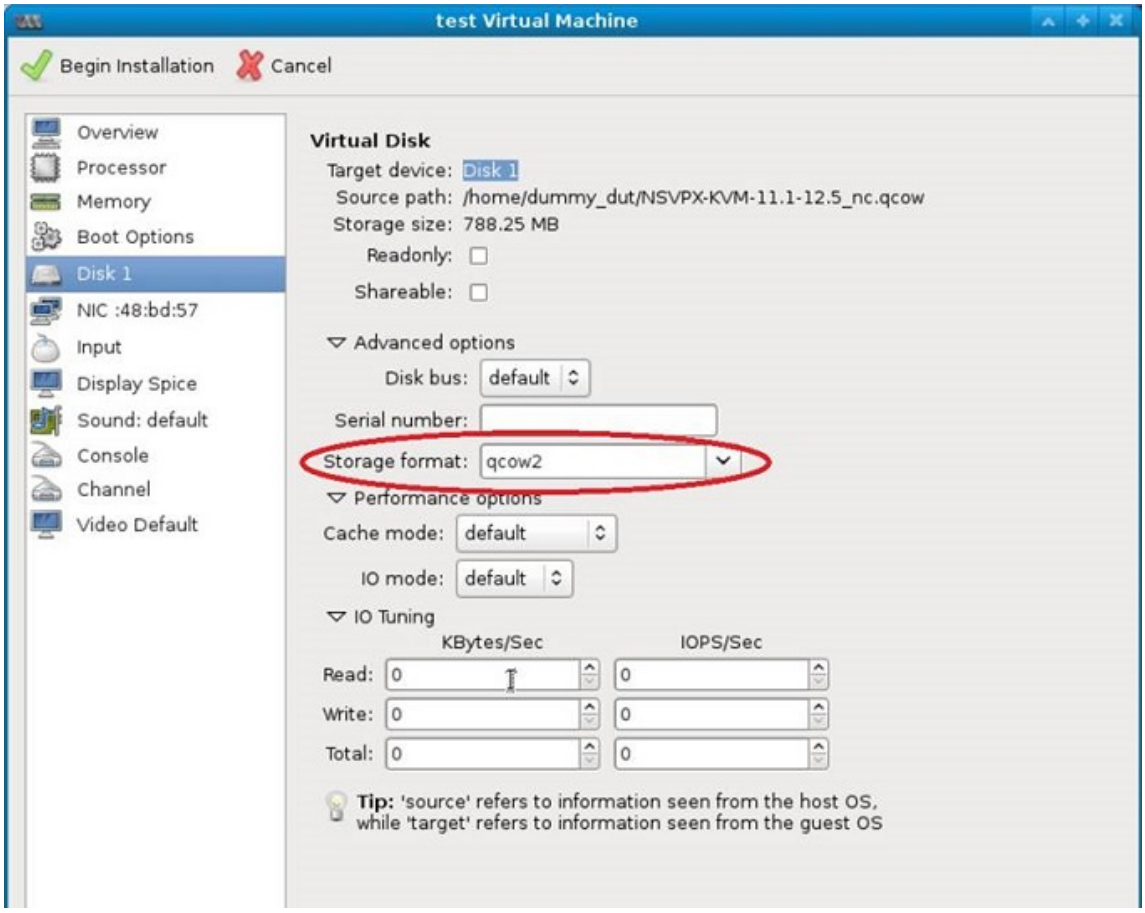
Provisionnez l'instance NetScaler VPX à l'aide d'une image QCOW2

À l'aide du Virtual Machine Manager, vous pouvez provisionner l'instance NetScaler VPX à l'aide d'une image QCOW2.

Pour provisionner une instance NetScaler VPX à l'aide d'une image QCOW2, procédez comme suit :

1. Suivez les **étapes 1** à **8 de la section Provisionner**l'instance NetScaler VPX à l'aide d'uneimage RAW.

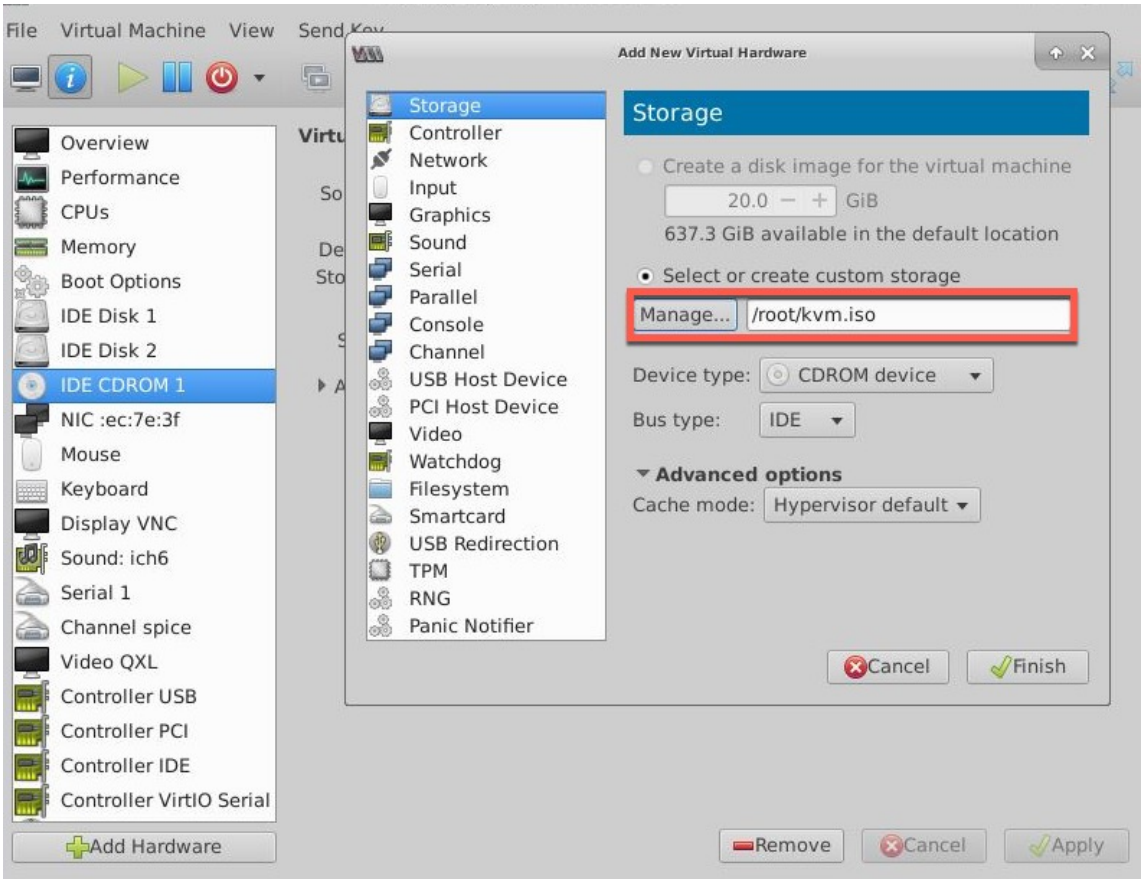
   Remarque : Assurez-vous de sélectionner l'image **qcow2**à l'**étape 5**.
2. Sélectionnez **le disque 1** et cliquez sur **Options avancées**.
3. Sélectionnez **qcow2** dans la liste déroulante Format de stockage.



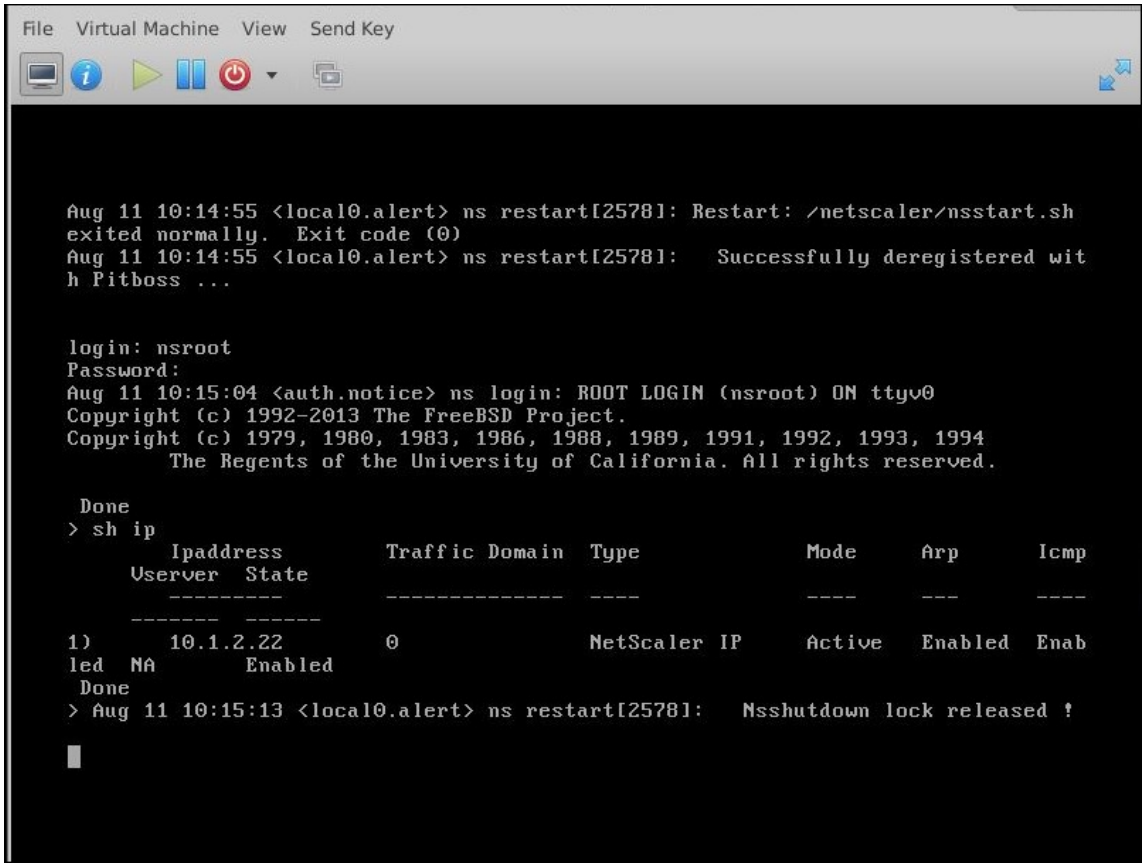
4. Cliquez sur **Appliquer**, puis sur **Commencer l'installation**. Après avoir configuré le NetScaler VPX sur KVM, vous pouvez ajouter d'autres interfaces.

Activer le provisioning automatique en attachant un lecteur de CD-ROM

1. Cliquez sur Ajouter **du matériel > Stockage > Type de périphérique > Lecteur de CD-ROM**.
2. **Cliquez sur**Gérer**et sélectionnez le fichier ISO approprié que vous avez monté dans la section « Conditions requises pour le Provisioning automatique d'une instance NetScaler VPX », puis cliquez sur Terminer.** Un nouveau CDROM est créé sous Ressources sur votre instance NetScaler VPX.



3. Mettez l'instance VPX sous tension, et il provisionnera automatiquement avec la configuration réseau fournie dans le fichier OVF, comme indiqué dans l'exemple de capture d'écran.



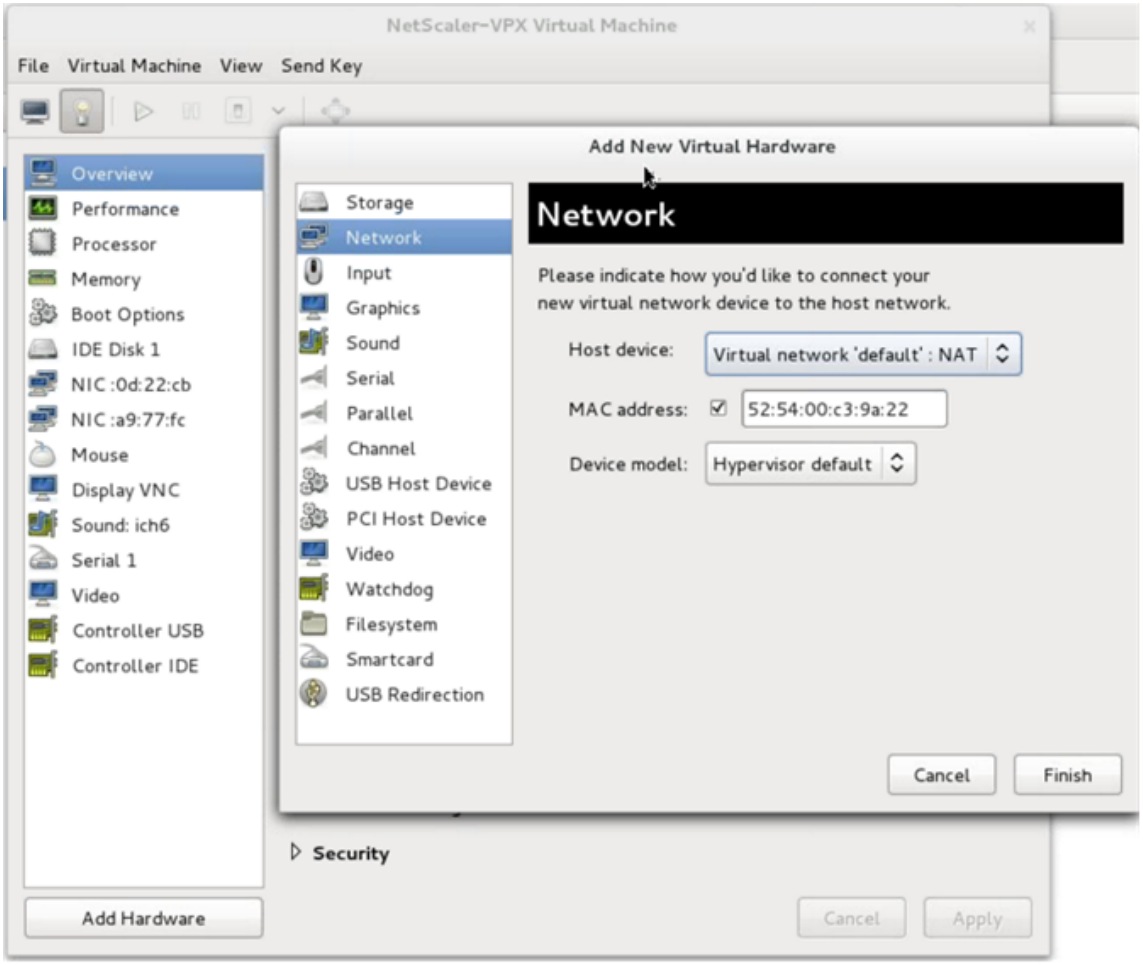
4. Si la mise en service automatique échoue, l'instance affiche l'adresse IP par défaut (192.168.100.1). Dans ce cas, vous devez terminer la configuration initiale manuellement. Pour plus d'informations, voir Configurer l'ADC pour la première fois.

Ajoutez d'autres interfaces à l'instance NetScaler VPX à l'aide du Virtual Machine Manager

Après avoir provisionné l'instance NetScaler VPX sur KVM, vous pouvez ajouter des interfaces supplémentaires.

Pour ajouter d'autres interfaces, procédez comme suit.

1. Arrêtez l'instance NetScaler VPX exécutée sur le KVM.
2. Cliquez avec le bouton droit sur l'instance VPX et choisissez **Ouvrir** dans le menu contextuel.
3. Cliquez sur l'icône de  dans l'en-tête pour afficher les détails du matériel virtuel.
4. Cliquez sur **Ajouter du matériel**. Dans la **fenêtre Ajouter un nouveau matériel virtuel**, sélectionnez **Réseau** dans le menu de navigation.



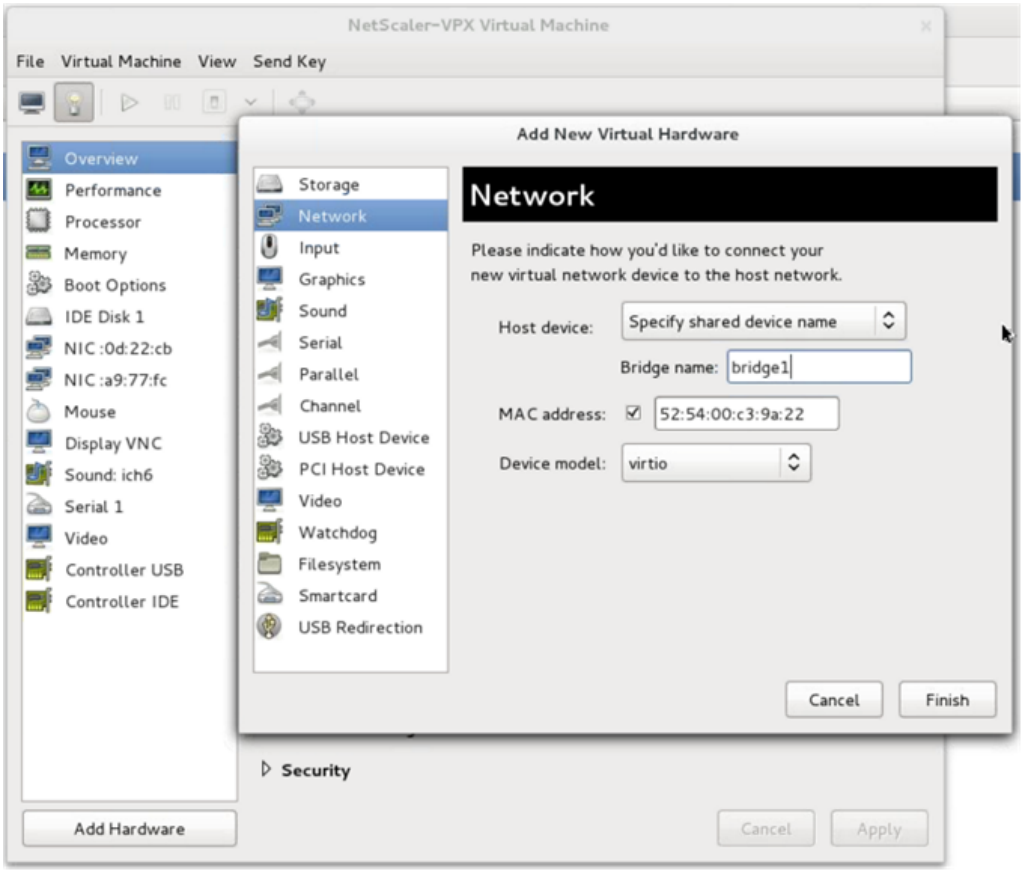
5. Dans le champ **Appareil hôte**, sélectionnez le type d'interface physique. Le type de périphérique hôte peut être Bridge ou MacVTap. Dans le cas d'un MacVTAP, quatre modes possibles sont VEPA, Bridge, Private et Pass-Through.

    a) Pour Bridge

        i. Appareil hôte : sélectionnez l'option « Spécifier le nom de l'appareil partagé ».

        ii. Indiquez le nom du pont configuré sur l'hôte KVM.

        Remarque : Assurez-vous que vous avez configuré un pont Linux sur l'hôte KVM, que vous avez lié l'interface physique au pont et que vous avez mis le pont à l'état UP.



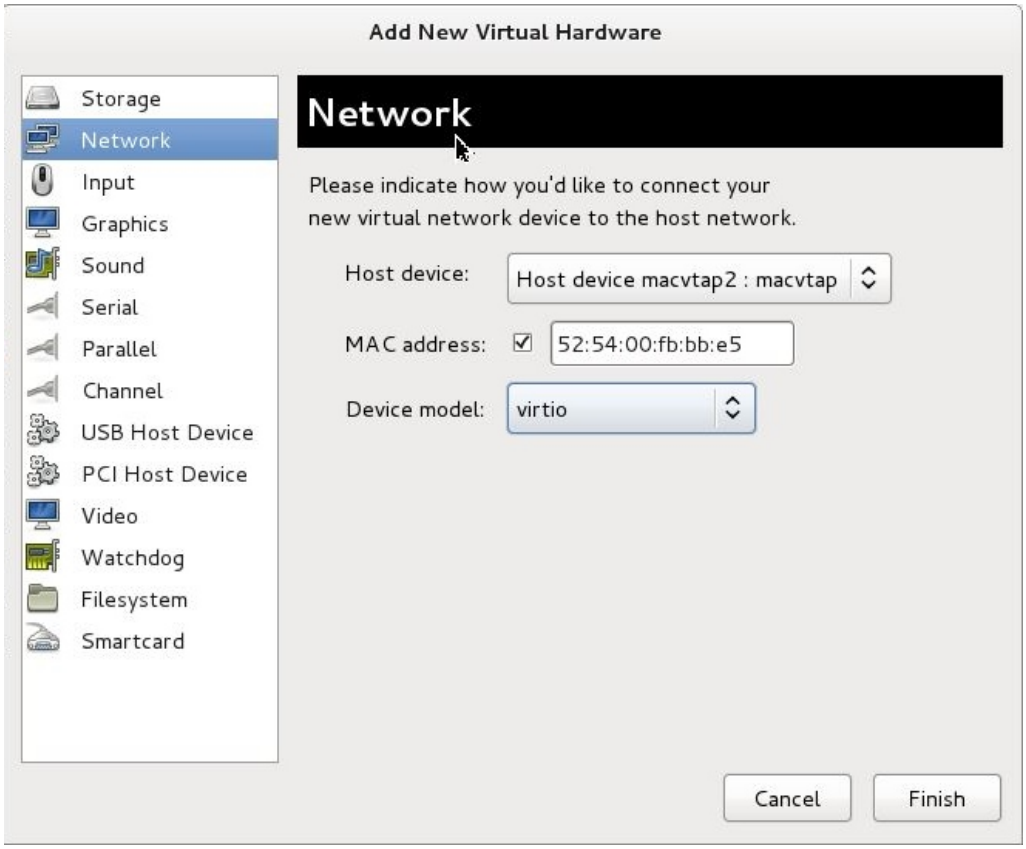
iii. Modèle d'appareil—`virtio`.

iv. Cliquez sur Finish.

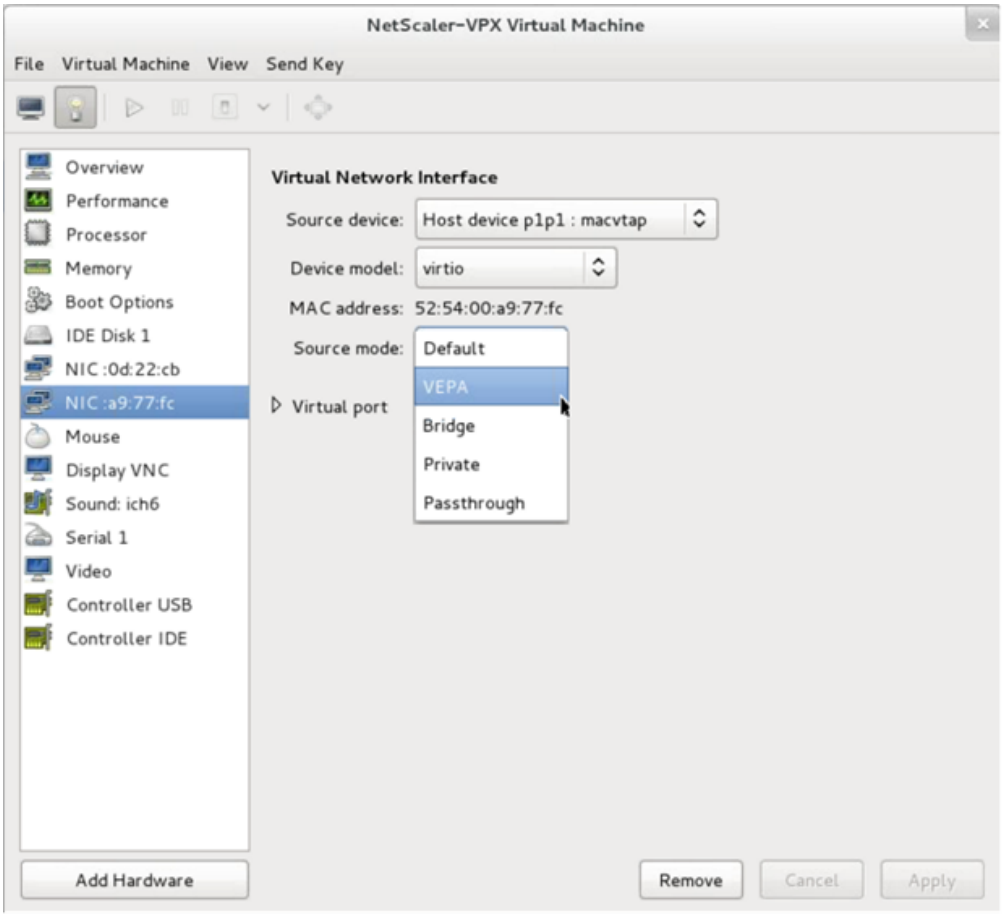
b) Pour MacVTap

i. Périphérique hôte : sélectionnez l'interface physique dans le menu.

ii. Modèle d'appareil—`virtio`.



iii. Cliquez sur Finish. Vous pouvez afficher la carte réseau récemment ajoutée dans le volet de navigation.



iv. Sélectionnez la carte réseau récemment ajoutée et sélectionnez le mode source pour cette carte réseau. Les modes disponibles sont VEPA, Bridge, Private et Passthrough. Pour plus de détails sur l'interface et les modes, voir Interface source et modes.

v. Cliquez sur Appliquer.

6. Si vous souhaitez provisionner automatiquement l'instance VPX, consultez la section « Ajouter un lecteur de configuration pour activer le Provisioning automatique » de ce document. Sinon, allumez l'instance VPX pour terminer la configuration initiale manuellement.

> **Important**
>
> Les configurations de paramètres d'interface telles que la vitesse, le duplex et la négociation automatique ne sont pas prises en charge.

Configurer une instance NetScaler VPX pour utiliser les interfaces réseau SR-IOV

May 5, 2023

Vous pouvez configurer une instance NetScaler VPX exécutée sur la plate-forme Linux-KVM à l'aide de la virtualisation des E/S à racine unique (SR-IOV) avec les cartes réseau suivantes :

- Intel 82599 10 Go
- Intel X710 10 Go
- Intel XL710 40 Go
- Intel X722 10G

Cette section explique comment :

- Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV
- Configuration du LA/LACP statique sur l'interface SR-IOV
- Configurer le VLAN sur l'interface SR-IOV

Limitations

Tenez compte des limites lorsque vous utilisez des cartes réseau Intel 82599, X710, XL710 et X722. Les fonctionnalités suivantes ne sont pas prises en charge.

Limitations de la carte réseau Intel 82599 :

- Commutation du mode L2.
- Partitionnement administratif (mode VLAN partagé).
- Haute disponibilité (mode actif-actif).
- Cadres Jumbo.
- IPv6 : Vous ne pouvez configurer que 30 adresses IPv6 uniques dans une instance VPX si vous disposez d'au moins une interface SR-IOV.
- La configuration VLAN sur l'interface Hypervisor for SRIOV VF via `ip link` commande n'est pas prise en charge.
- Les configurations de paramètres d'interface telles que la vitesse, le duplex et les négociations automatiques ne sont pas prises en charge.

Limitations pour les cartes réseau Intel X710 10G, Intel XL710 40G et Intel X72210G :

- Commutation du mode L2.
- Partitionnement administratif (mode VLAN partagé).
- Dans un cluster, les trames Jumbo ne sont pas prises en charge lorsque la carte réseau XL710 est utilisée comme interface de données.
- La liste d'interfaces est réorganisée lorsque les interfaces sont déconnectées et reconnectées.
- Les configurations des paramètres d'interface telles que la vitesse, le mode duplex et les négociations automatiques ne sont pas prises en charge.
- Le nom de l'interface est 40/X pour les cartes réseau Intel X710 10G, Intel XL710 40G et Intel X722 10G

- Jusqu'à 16 interfaces relais Intel XL710/X710/X722 SRIOV ou PCI peuvent être prises en charge sur une instance VPX.

> **Remarque :** pour que les cartes réseau Intel X710 10G, Intel XL710 40G et Intel X722 10G prennent en charge le protocole IPv6, vous devez activer le mode confiance sur les fonctions virtuelles (VF) en saisissant la commande suivante sur l'hôte KVM :
>
> ```
> ## ip link set <PNIC> <VF> trust on
> ```
>
> Exemple :
>
> ```
> ## ip link set ens785f1 vf 0 trust on
> ```

Composants requis

Avant de configurer une instance NetScaler VPX pour utiliser les interfaces réseau SR-IOV, effectuez les tâches préalables suivantes. Consultez la colonne NIC pour plus de détails sur la façon d'effectuer les tâches correspondantes.

Tâche	Carte réseau Intel 82599	Cartes réseau Intel X710, XL710 et X722
1. Ajoutez la carte réseau à l'hôte KVM.	-	-
2. Téléchargez et installez le dernier pilote Intel.	pilote IXGBE	pilote I40E
3. Liste de blocage du pilote sur l'hôte KVM.	Ajoutez l'entrée suivante dans le fichier /etc/mod-probe.d/blacklist.conf : `blacklist ixgbevf`. Utilisez la version 4.3.15 du pilote IXGBE (recommandée).	Ajoutez l'entrée suivante dans le fichier /etc/mod-probe.d/blacklist.conf : `blacklist i40evf`. Utilisez la version 2.0.26 du pilote i40e (recommandée).

Tâche	Carte réseau Intel 82599	Cartes réseau Intel X710, XL710 et X722
4. Activez les fonctions virtuelles (VF) SR-IOV sur l'hôte KVM. Dans les deux commandes des deux colonnes suivantes : `number_of_VFs` = le nombre de VF virtuels que vous souhaitez créer. `device_name` = le nom de l'interface.	Si vous utilisez une version antérieure du noyau 3.8, ajoutez l'entrée suivante au fichier /etc/modprobe.d/ixgbe et redémarrez l'hôte KVM : `options ixgbe max_vfs =<number_of_VFs>`. Si vous utilisez la version 3.8 du noyau ou une version ultérieure, créez des VF à l'aide de la commande suivante : `echo <number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`. Voir l'exemple de la figure 1.	Si vous utilisez une version antérieure du noyau 3.8, ajoutez l'entrée suivante au fichier /etc/modprobe.d/i40e.conf et redémarrez l'hôte KVM :. `options i40e max_vfs=<number_of_VFs>` Si vous utilisez la version 3.8 du noyau ou une version ultérieure, créez des VF à l'aide de la commande suivante : `echo<number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`. Voir l'exemple de la figure 2.
5. Rendez les fichiers VF persistants en ajoutant les commandes que vous avez utilisées pour créer des fichiers VF au fichier rc.local.	Voir l'exemple de la figure 3.	Voir l'exemple de la figure 3.

> **Important**
>
> Lorsque vous créez les VF SR-IOV, veillez à ne pas leur attribuer d'adresses MAC.

Figure 1 : Activez les vF SR-IOV sur l'hôte KVM pour la carte réseau Intel 82599 10G.

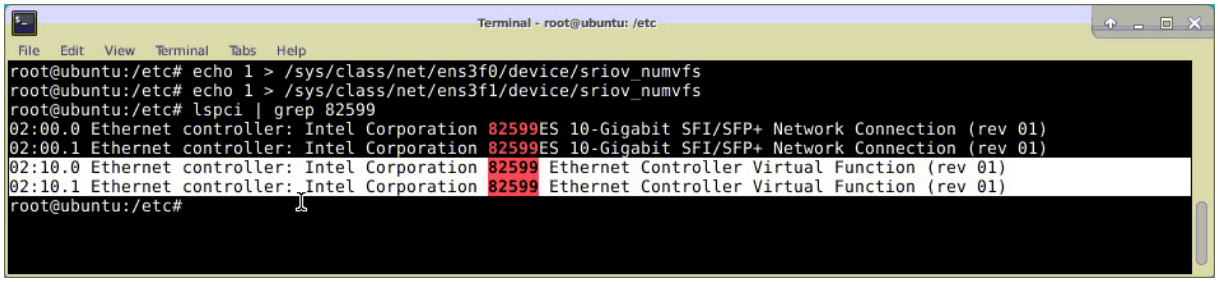


Figure 2 : Activez les vF SR-IOV sur l'hôte KVM pour les cartes réseau Intel X710 10G et XL710 40G.

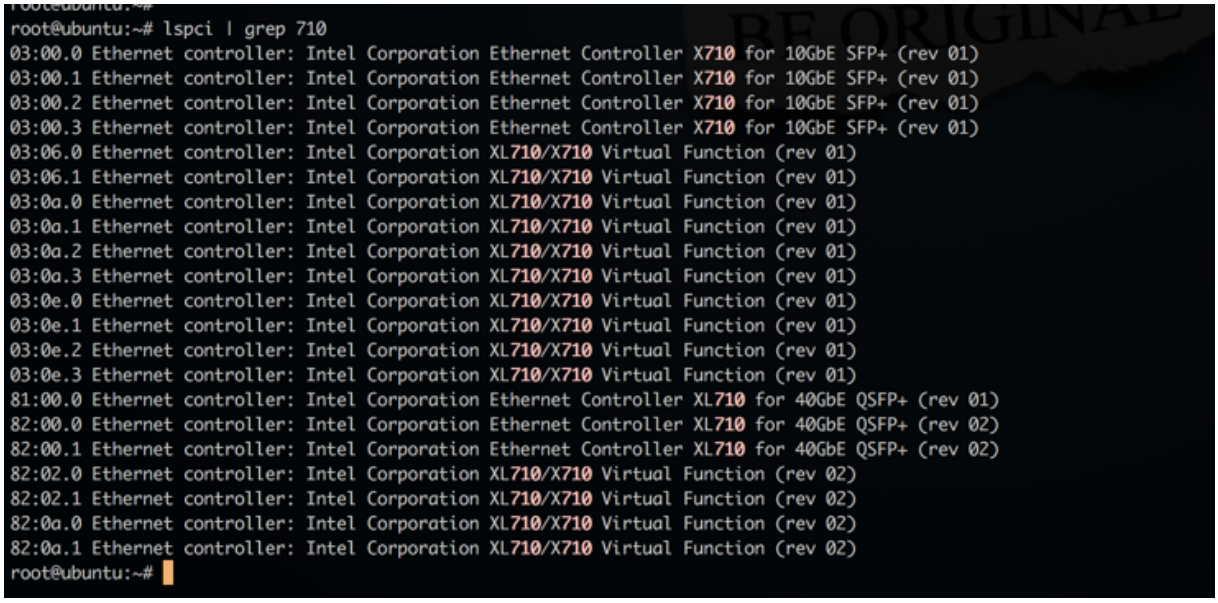


Figure 3 : Activez les vF SR-IOV sur l'hôte KVM pour la carte réseau Intel X722 10G.

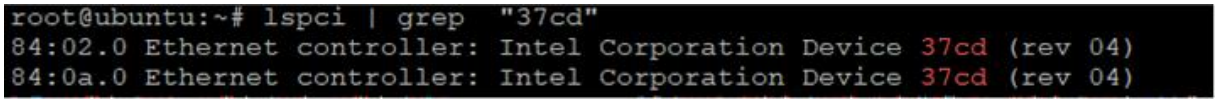
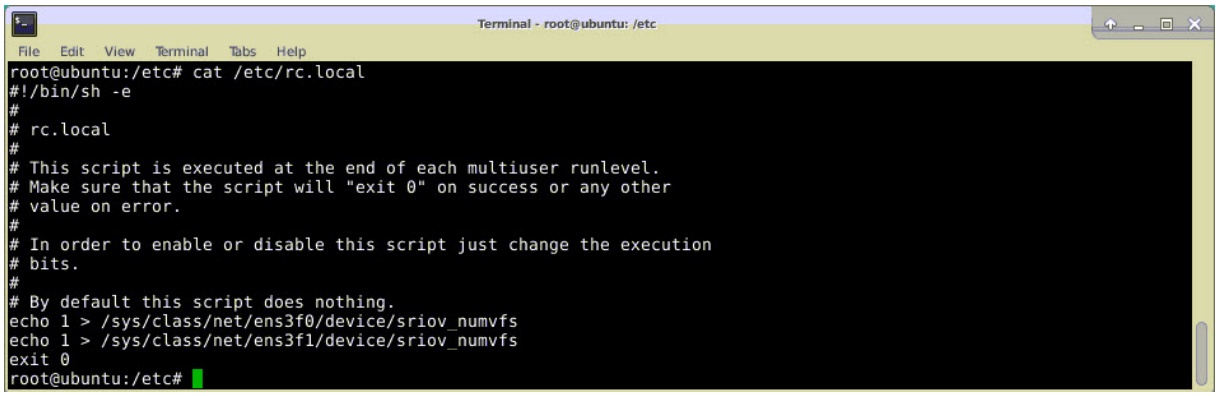


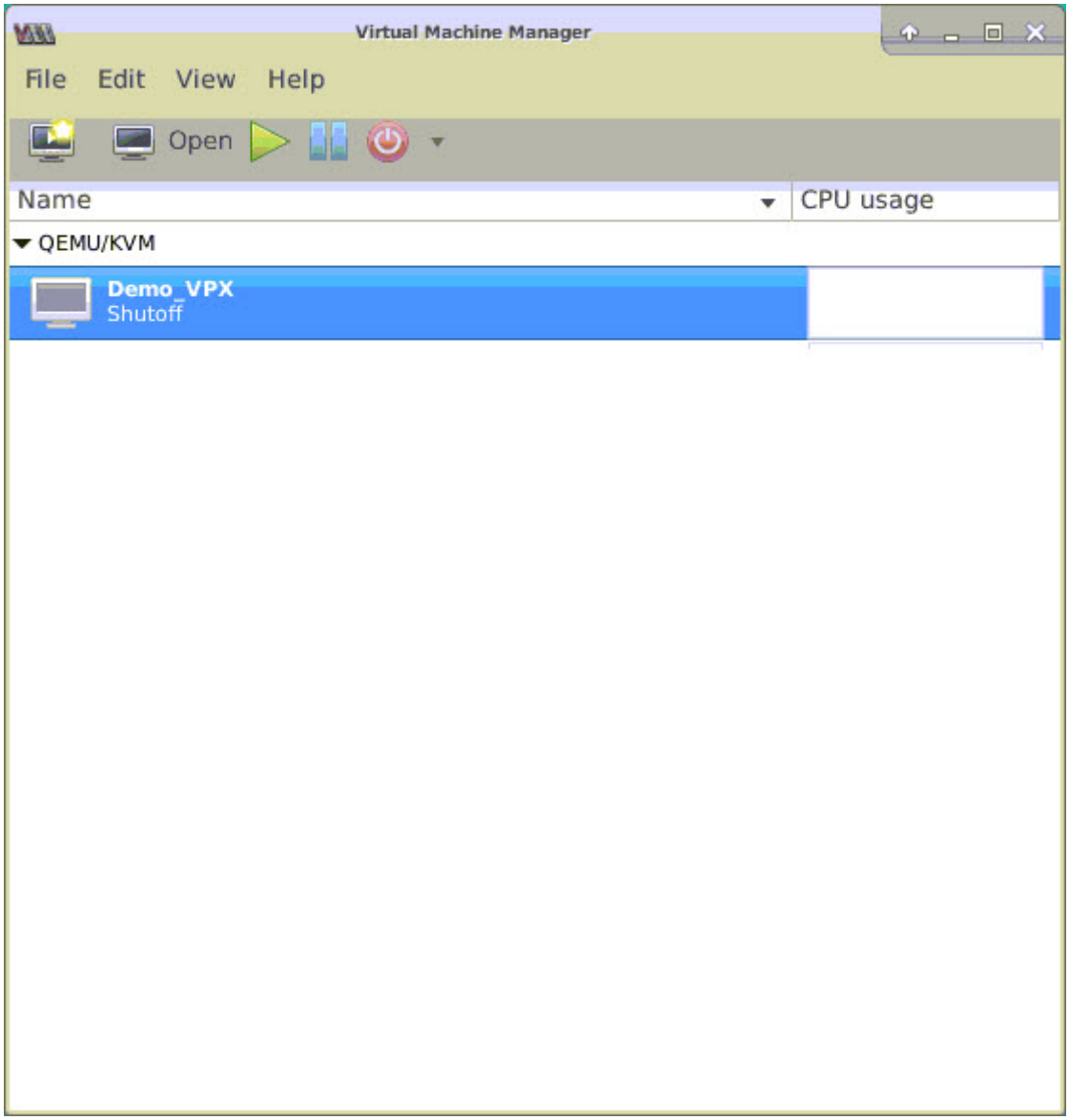
Figure 4 : Rendre les VF persistants.



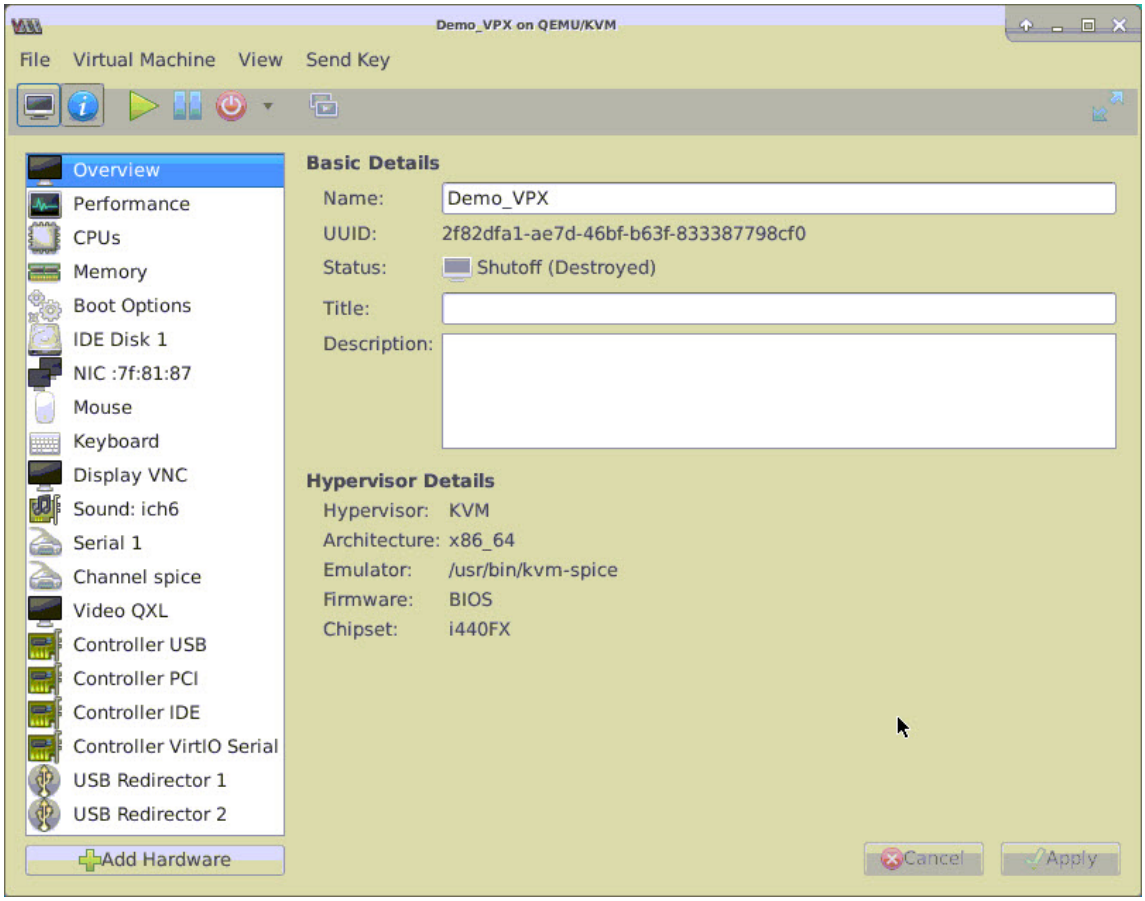
Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV

Pour configurer l'instance NetScaler VPX afin qu'elle utilise l'interface réseau SR-IOV à l'aide de Virtual Machine Manager, procédez comme suit :

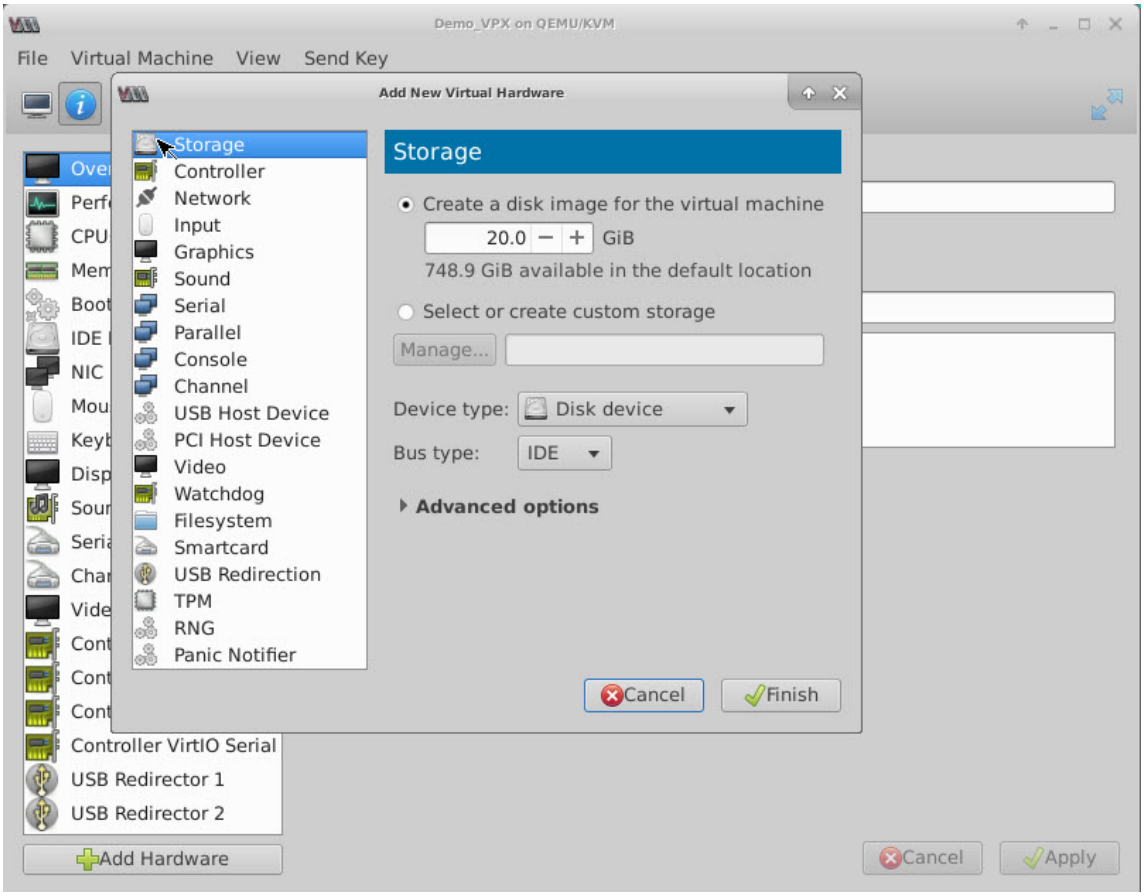
1. Éteignez l'instance NetScaler VPX.
2. Sélectionnez l'instance NetScaler VPX, puis sélectionnez Ouvrir.



3. Dans la <virtual machine on KVM>fenêtre, sélectionnez l'icône **i** .



4. Sélectionnez **Ajouter du matériel**.



5. Dans la boîte de dialogue **Ajouter un nouveau matériel virtuel**, procédez comme suit :

   a) Sélectionnez le périphérique hôte PCI.

   b) Dans la section Appareil hôte, sélectionnez le VF que vous avez créé et cliquez sur Terminer.

Figure 4 : VF pour carte réseau Intel 82599 10G

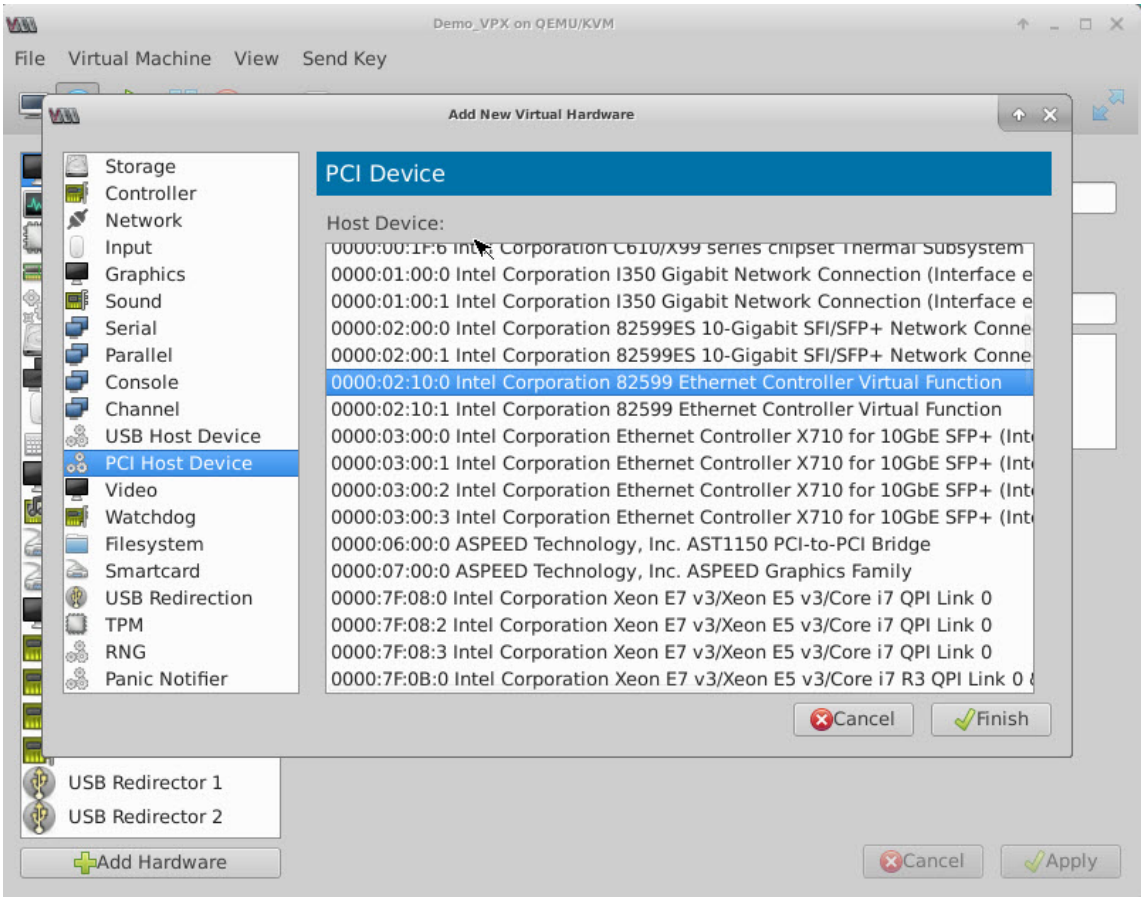


Figure 5 : VF pour carte réseau Intel XL710 40G

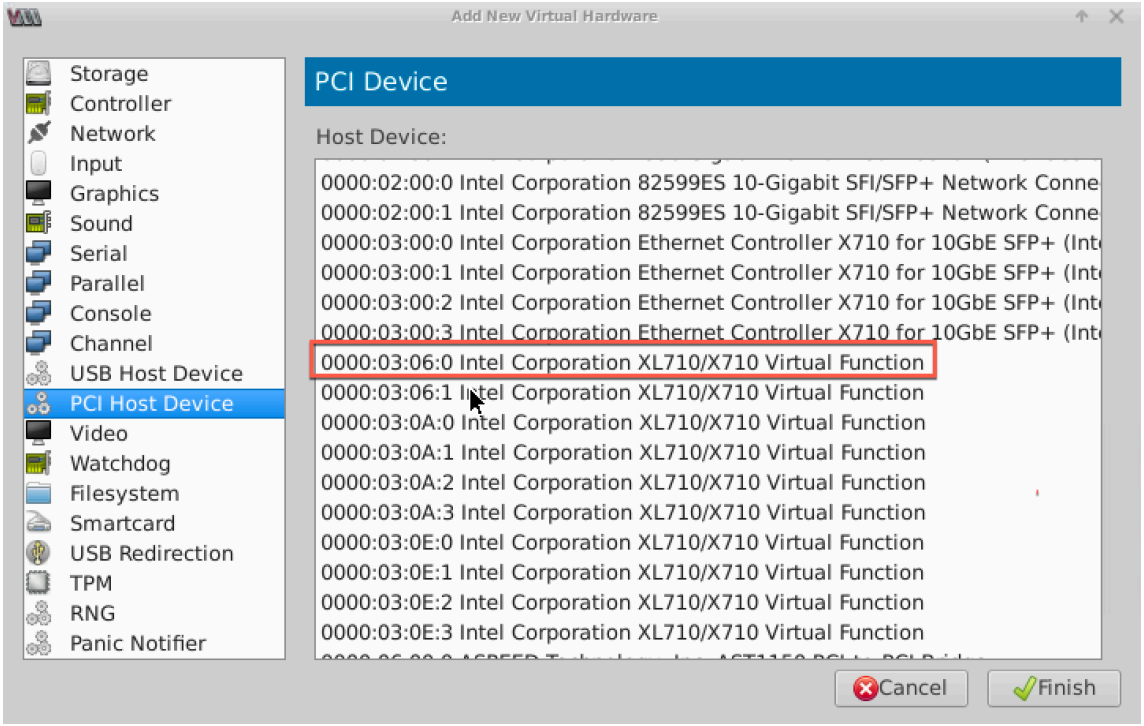
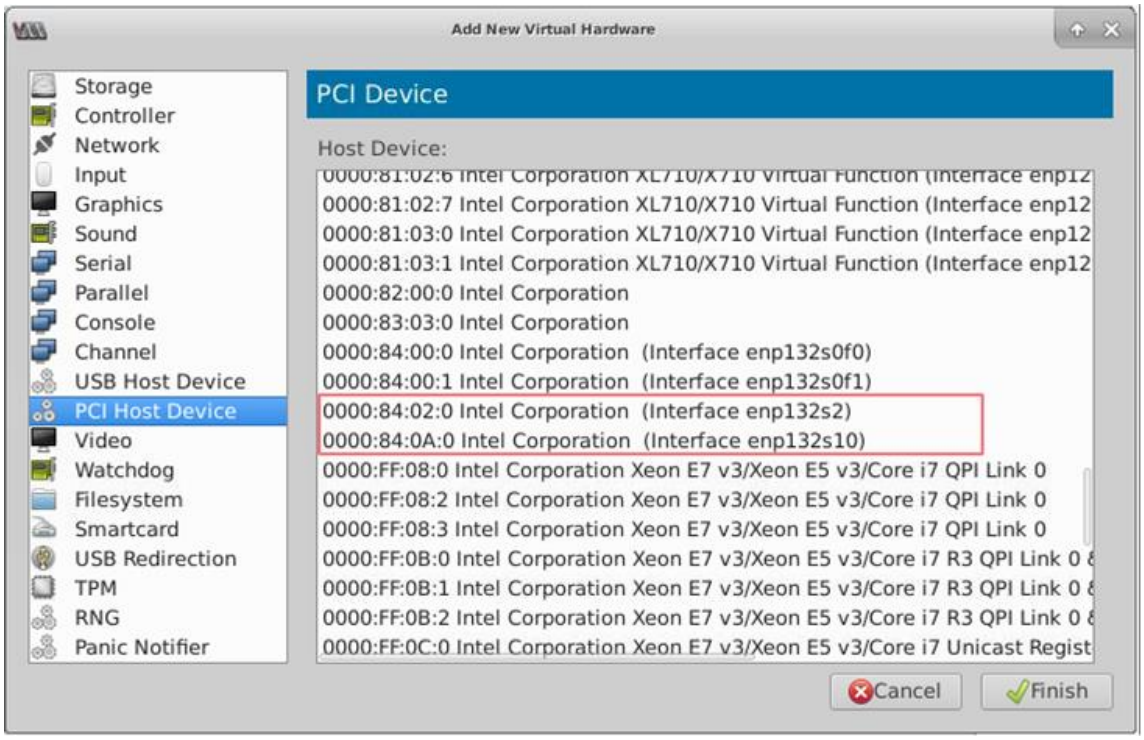


Figure 6 : VF pour carte réseau Intel X722 10G



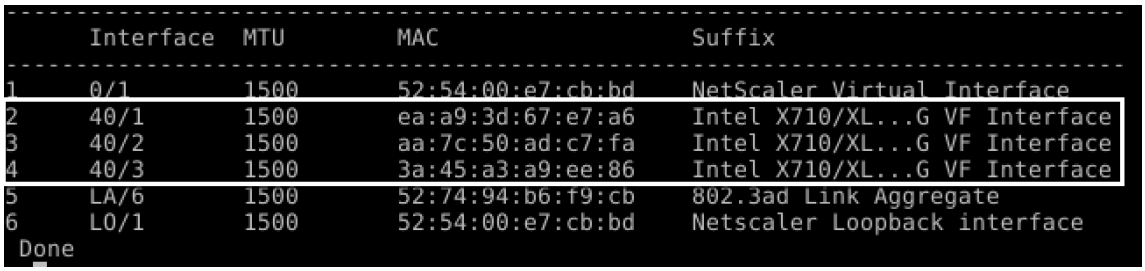
6. Répétez les étapes 4 et 5 pour ajouter les fichiers VF que vous avez créés.
7. Allumez l'instance NetScaler VPX.
8. Une fois l'instance NetScaler VPX activée, utilisez la commande suivante pour vérifier la configuration :

```
1 show interface summary
2 <!--NeedCopy-->
```

La sortie affiche toutes les interfaces que vous avez configurées.

Figure 6 : résumé des sorties pour la carte réseau Intel 82599.

Figure 7. Résumé des résultats pour les cartes réseau Intel X710 et XL710.



Configurer le LA/LACP statique sur l'interface SR-IOV

> **Important**
>
> Lorsque vous créez les VF SR-IOV, veillez à ne pas leur attribuer d'adresses MAC.

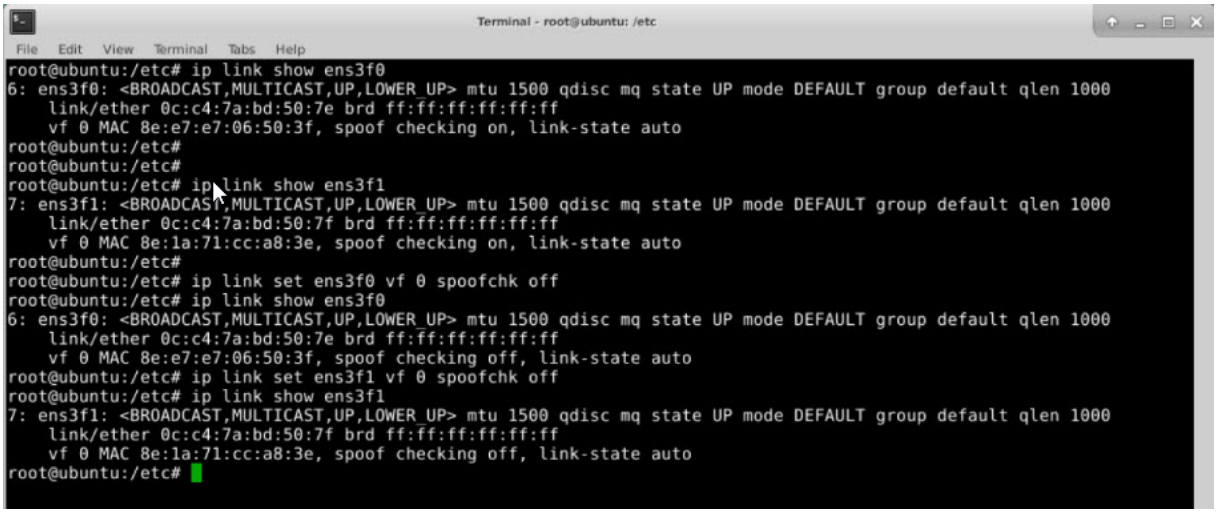
Pour utiliser les VF SR-IOV en mode agrégation de liens, désactivez la vérification des usurpations pour les VF que vous avez créées. Sur l'hôte KVM, utilisez la commande suivante pour désactiver la vérification des usurpations :

```
*ip link set \<interface\\_name\> vf \<VF\\_id\> spoofchk off*
```

Où :

- Interface_name — est le nom de l'interface.
- VF_ID — est l'identifiant de la fonction virtuelle.

Exemple :



Après avoir désactivé la vérification des usurpations pour toutes les VF que vous avez créées. Redémarrez l'instance NetScaler VPX et configurez l'agrégation de liens. Pour obtenir des instructions détaillées, voir Configuration de l'agrégation de liens.

Configuration du VLAN sur l'interface SR-IOV

Vous pouvez configurer VLAN sur les VF SR-IOV. Pour obtenir des instructions détaillées, reportez-vous à la section Configuration d'un VLAN.

> **Important**
>
> Assurez-vous que l'hôte KVM ne contient pas de paramètres VLAN pour l'interface VF.

Configurer une instance NetScaler VPX pour utiliser des interfaces réseau PCI passthrough

May 5, 2023

Après avoir installé et configuré une instance NetScaler VPX sur la plate-forme Linux-KVM, vous pouvez utiliser le Virtual Machine Manager pour configurer l'appliance virtuelle afin qu'elle utilise des interfaces réseau PCI passthrough.

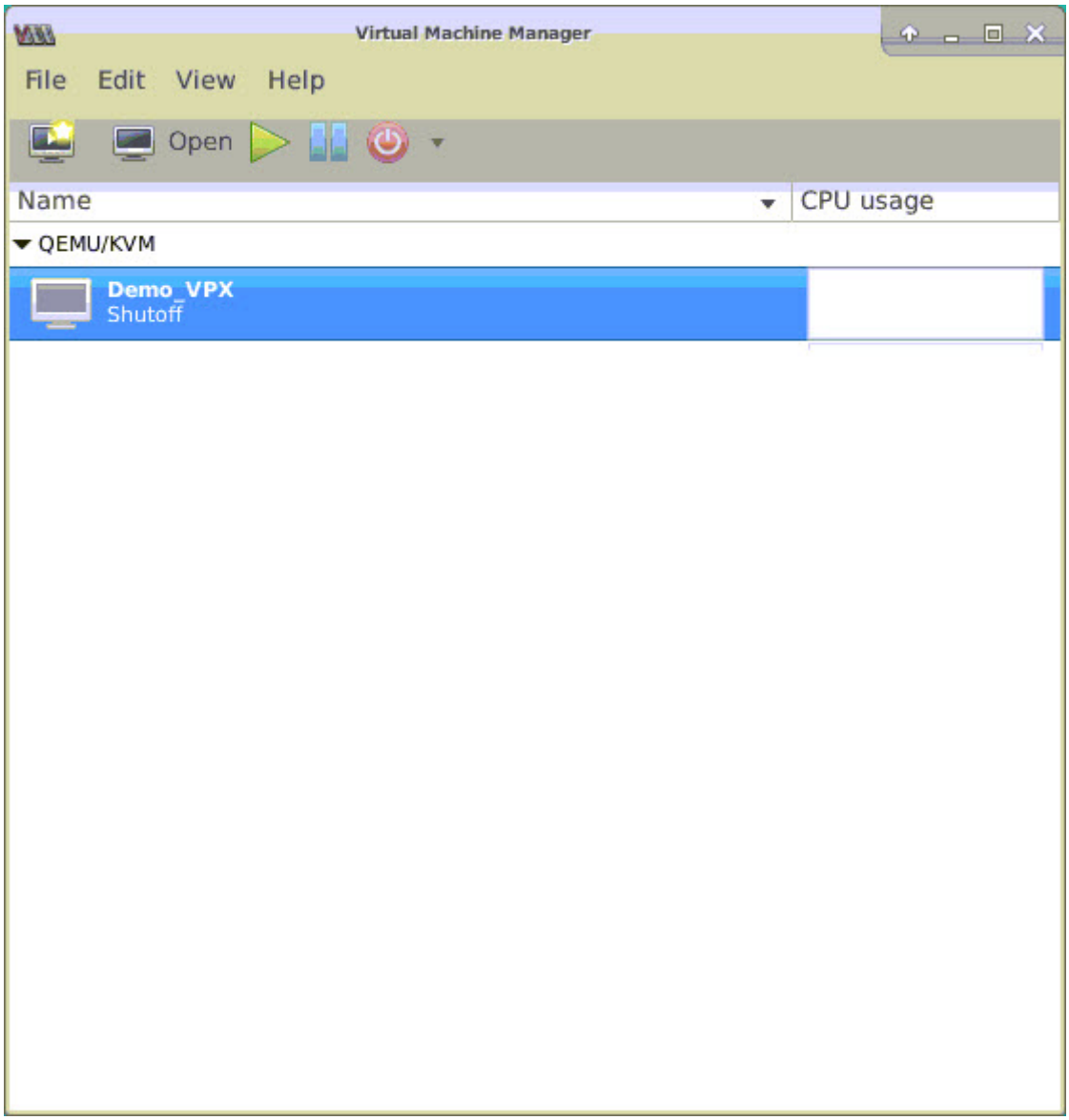
Composants requis

- La version du microprogramme de la carte réseau (NIC) Intel XL710 sur l'hôte KVM est 5.04.
- L'hôte KVM prend en charge l'unité de gestion de la mémoire d'entrée-sortie (IOMMU) et Intel VT-d, et ils sont activés dans le BIOS de l'hôte KVM. Sur l'hôte KVM, pour activer IOMMU, ajoutez l'entrée suivante au fichier **/boot/grub2/grub.cfg**:**intel_iommu=1**

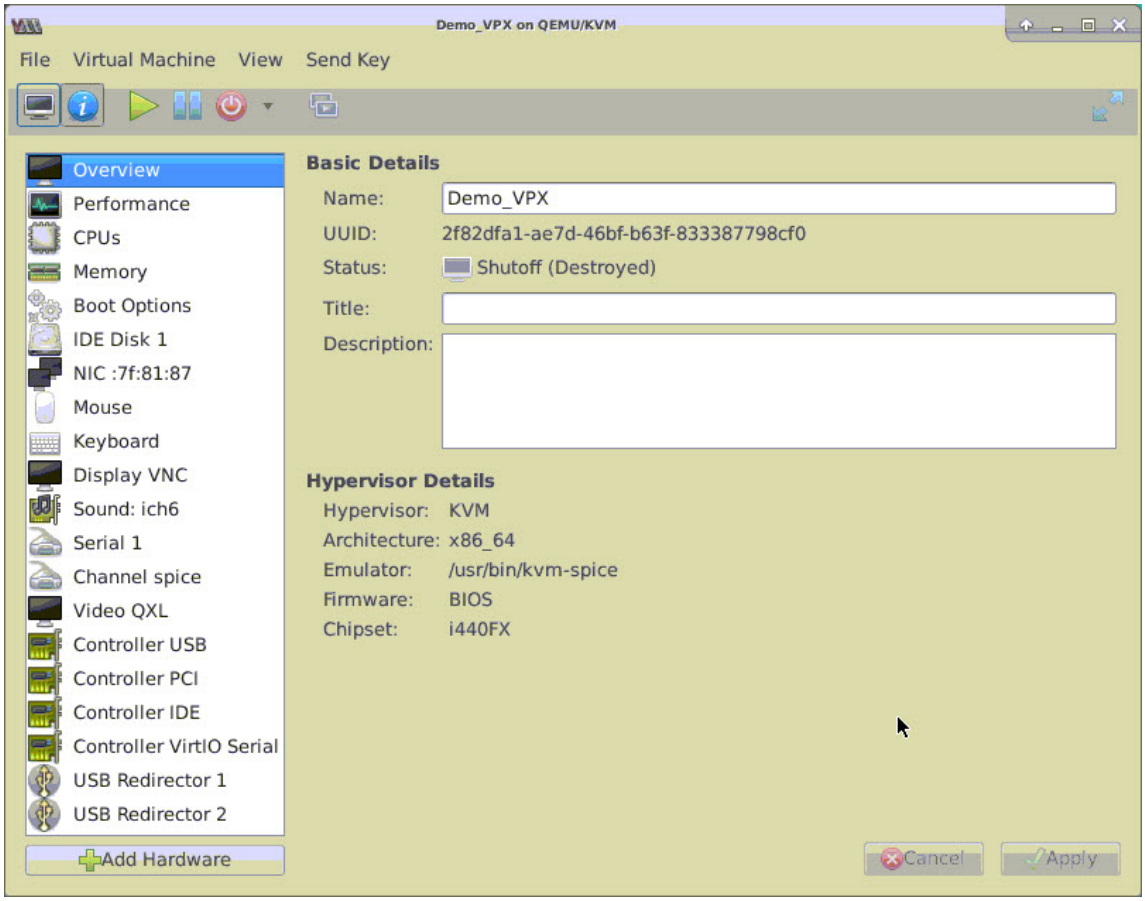
- Exécutez la commande suivante et redémarrez l'hôte KVM : **GRUB2-MKConfig —o /boot/-grub2/grub.cfg**

Pour configurer les instances NetScaler VPX afin qu'elles utilisent des interfaces réseau passthrough PCI à l'aide du Virtual Machine Manager :

1. Éteignez l'instance NetScaler VPX.
2. **Sélectionnez l'instance NetScaler VPX et cliquez sur Ouvrir.**



3. Dans la fenêtre **Virtual_machine sur KVM**, cliquez sur l'icône **i.**

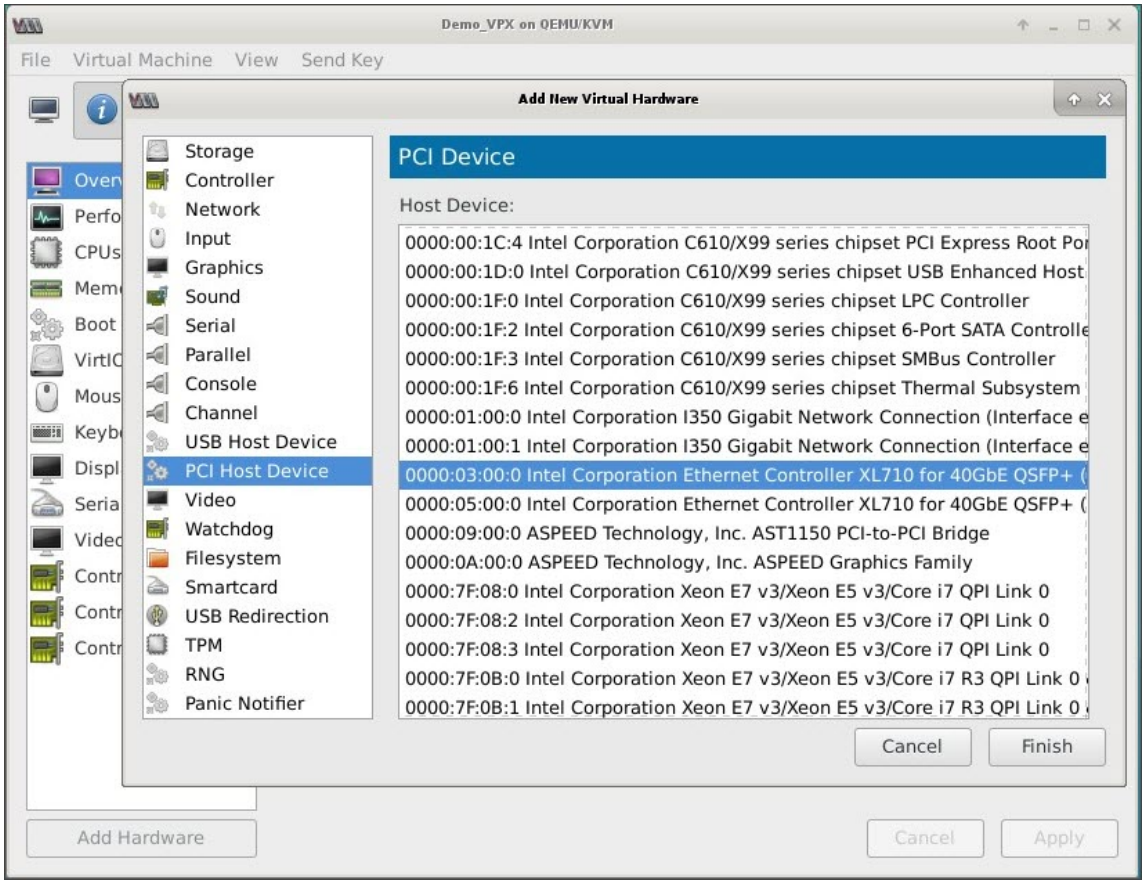


4. Cliquez sur **Ajouter du matériel**.
5. Dans la boîte de dialogue **Ajouter un nouveau matériel virtuel**, procédez comme suit :

   a. Sélectionnez le **périphérique hôte PCI**.

   b. Dans la section **Appareil hôte**, sélectionnez la fonction physique du processeur Intel XL710.

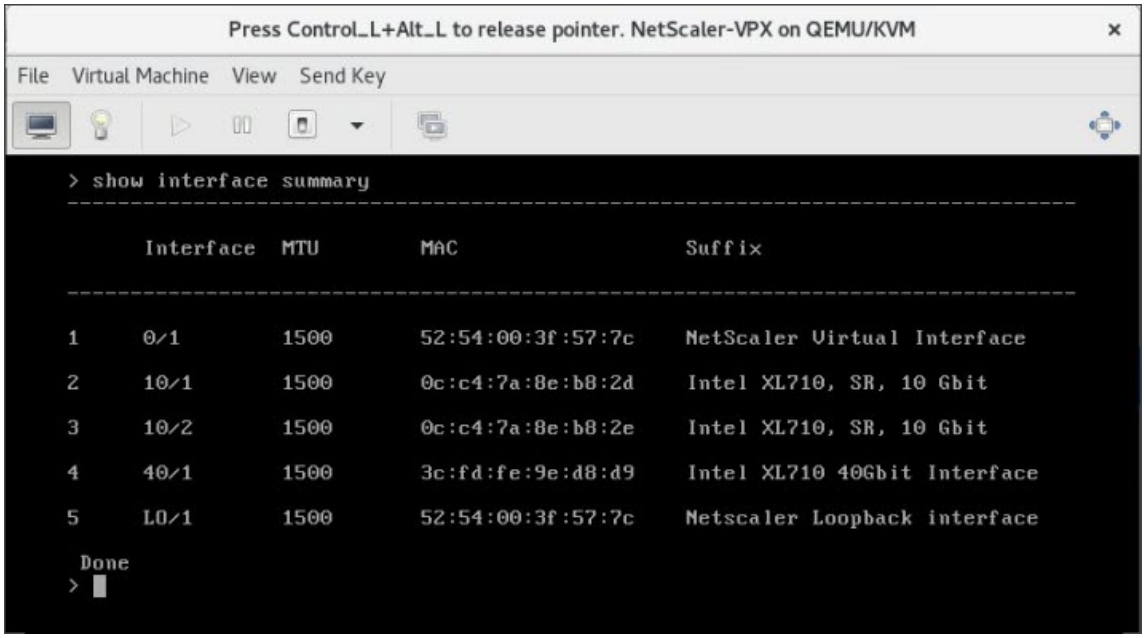
   c. Cliquez sur **Finish**.



6. Répétez les étapes **4** et **5** pour ajouter d'autres fonctions physiques Intel XL710.
7. Allumez l'instance NetScaler VPX.
8. Une fois que l'instance NetScaler VPX est activée, vous pouvez utiliser la commande suivante pour vérifier la configuration :

   ```
   COMMAND
   > show interface summary
   ```

   La sortie doit afficher toutes les interfaces que vous avez configurées :



Provisionnez l'instance NetScaler VPX à l'aide du programme virsh

May 8, 2023

Le `virsh` programme est un outil de ligne de commande permettant de gérer les invités de machines virtuelles. Sa fonctionnalité est similaire à celle de Virtual Machine Manager. Il vous permet de modifier l'état d'un invité VM (démarrage, arrêt, pause, etc.), de configurer de nouveaux invités et appareils et de modifier les configurations existantes. Le `virsh` programme est également utile pour le script des opérations de gestion des invités de machines virtuelles.

Pour provisionner NetScaler VPX à l'aide du `virsh` programme, procédez comme suit :

1. Utilisez la commande tar pour décompresser le package NetScaler VPX. Le package NSVPX-KVM-*_NC.tgz contient les composants suivants :

   - Fichier XML de domaine spécifiant les attributs VPX [NSVPX-KVM-*_NC.xml]
   - Vérifiez la somme des images de disque NS-VM [Checksum.txt]
   - Image de disque NS-VM [NSVPX-KVM-*_NC.raw]

   Exemple :

```
tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
NSVPX-KVM-10.1-117_nc.xml
NSVPX-KVM-10.1-117_nc.raw
checksum.txt
<!--NeedCopy-->
```


2. <DomainName>Copiez le fichier XML NSVPX-KVM- \ * \ _nc.xml dans un fichier nommé \-NSVPX-KVM- \ * _nc.xml. Le \ <DomainName> est également le nom de la machine virtuelle. Exemple :

```
cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc.
   xml
<!--NeedCopy-->
```

3. Modifiez le fichier \-NSVPX-KVM <DomainName>- \ * \ _nc.xml pour spécifier les paramètres suivants :

   - name (name) : spécifiez le nom.
   - Mac : spécifiez l'adresse MAC.
     Remarque : Le nom de domaine et l'adresse MAC doivent être uniques.
   - fichier source : spécifiez le chemin absolu de la source de l'image disque. Le chemin du fichier doit être absolu. Vous pouvez spécifier le chemin du fichier image RAW ou d'un fichier image QCOW2.

     Si vous souhaitez spécifier un fichier image RAW, spécifiez le chemin source de l'image disque comme indiqué dans l'exemple suivant :

     Exemple :

```
<name>NetScaler-VPX</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
<!--NeedCopy-->
```

     Spécifiez le chemin source absolu de l'image disque QCOW2 et définissez le type de pilote comme **qcow2**, comme indiqué dans l'exemple suivant :

     Exemple :

```
<name>NetScaler-VPX</name>
<mac address='52:54:00:29:74:b3'/>
<driver name ='qemu' type='qcow2'/>
<source file='/root/NSVPX-KVM-10.1-117_nc.qcow'/>*
<!--NeedCopy-->
```

4. Modifiez le fichier \-NSVPX-KVM <DomainName>- \ * \ _nc.xml pour configurer les détails du réseau :

   - source dev : spécifiez l'interface.
   - mode : spécifiez le mode. L'interface par défaut est **Macvtap Bridge**.

   Exemple : Mode : MacVTap Bridge Définissez l'interface cible comme `ethx` et le mode comme pont Type de modèle comme `virtio`


```
  <interface type='direct'>
      <mac address='52:54:00:29:74:b3'/>
      <source dev='eth0' mode='bridge'/>
      <target dev='macvtap0'/>
      <model type='virtio'/>
      <alias name='net0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
         function='0x0'/>
    </interface>
<!--NeedCopy-->
```

Ici, eth0 est l'interface physique attachée à la machine virtuelle.

5. <DomainName>Définissez les attributs de la machine virtuelle dans le <DomainName> fichier \-NSVPX-KVM- \ * \ _nc.xml à l'aide de la commande suivante : define `virsh` \-NSVPX-KVM- \ * _nc.xml Exemple :

```
virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
<!--NeedCopy-->
```

6. Démarrez la machine virtuelle en saisissant la commande suivante : `virsh` start \ [\ <DomainName> | \ <DomainUUID> \] Exemple :

```
virsh start NetScaler-VPX
<!--NeedCopy-->
```

7. Connectez la machine virtuelle cliente via la `virsh` console \ [\ <DomainName> | \ <DomainUUID> | \ <DomainID> \] Exemple :

```
virsh console NetScaler-VPX
<!--NeedCopy-->
```

Ajouter d'autres interfaces à l'instance NetScaler VPX à l'aide du programme `virsh`

Après avoir configuré le NetScaler VPX sur KVM, vous pouvez ajouter des interfaces supplémentaires.

Pour ajouter d'autres interfaces, procédez comme suit :

1. Arrêtez l'instance NetScaler VPX exécutée sur le KVM.
2. <DomainName> <DomainUUID>Modifiez le <DomainName> fichier \-NSVPX-KVM- \ * \ _nc.xml à l'aide de la commande suivante : edit `virsh` \ [\ | \ \]
3. Dans le fichier \-NSVPX-KVM <DomainName>- \ * \ _nc.xml, ajoutez les paramètres suivants :
   a) **Pour MacVTap**

- Type d'interface : spécifiez le type d'interface comme « direct ».
- Adresse MAC : spécifiez l'adresse MAC et assurez-vous que l'adresse MAC est unique sur toutes les interfaces.
- source dev : spécifiez le nom de l'interface.
- mode : spécifiez le mode. Les modes pris en charge sont : Bridge, VEPA, Private et Pass-Through
- type de modèle : spécifiez le type de modèle comme `virtio`

Exemple :

Mode : Pass-through MacVTap

Définissez l'interface cible comme
`ethx`, le mode comme
pont et le type de modèle comme
`virtio`

```
<interface type='direct'>
      <mac address='52:54:00:29:74:b3'/>
      <source dev='eth1' mode='passthrough'/>
      <model type='virtio'/>
 </interface>
<!--NeedCopy-->
```

Ici eth1 est l'interface physique attachée à la machine virtuelle.

b) **Pour le mode Bridge**

Remarque : Assurez-vous que vous avez configuré un pont Linux sur l'hôte KVM, que vous avez lié l'interface physique au pont et que vous avez mis le pont à l'état UP.

- Type d'interface : spécifiez le type d'interface comme « pont ».
- Adresse MAC : spécifiez l'adresse MAC et assurez-vous que l'adresse MAC est unique sur toutes les interfaces.
- pont source : spécifiez le nom du pont.
- type de modèle : spécifiez le type de modèle comme `virtio`

Exemple : Mode Pont

```
<interface type='bridge'>
      <mac address='52:54:00:2d:43:a4'/>
      <source bridge='br0'/>
      <model type='virtio'/>
 </interface>
<!--NeedCopy-->
```


Gérer les machines virtuelles clientes NetScaler VPX

May 8, 2023

Vous pouvez utiliser Virtual Machine Manager et le `virsh` programme pour effectuer des tâches de gestion telles que le démarrage ou l'arrêt d'un invité de machine virtuelle, la configuration de nouveaux invités et de nouveaux périphériques, la modification de configurations existantes et la connexion à la console graphique via Virtual Network Computing (VNC).

Gérer les machines virtuelles invitées VPX à l'aide de Virtual Machine Manager

- Lister les invités de la machine virtuelle

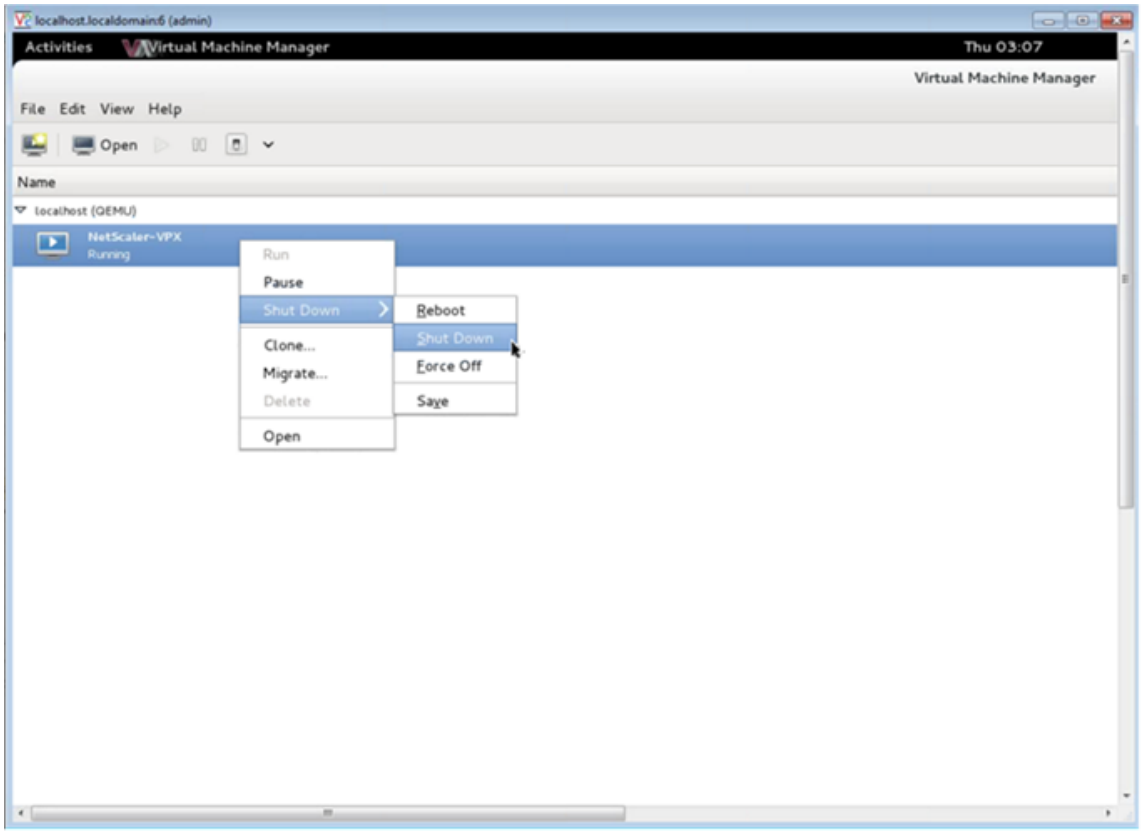
  La fenêtre principale du Virtual Machine Manager affiche une liste de tous les invités de machine virtuelle pour chaque serveur hôte de machine virtuelle auquel il est connecté. Chaque entrée Invité de machine virtuelle contient le nom de la machine virtuelle, ainsi que son état (en cours d'exécution, pause ou arrêt) affiché comme dans l'icône.

- Ouvrir une console graphique

  L'ouverture d'une console graphique à une machine virtuelle invitée vous permet d'interagir avec la machine comme vous le feriez avec un hôte physique via une connexion VNC. Pour ouvrir la console graphique dans Virtual Machine Manager, cliquez avec le bouton droit sur l'entrée VM Guest et sélectionnez l'option Ouvrir dans le menu contextuel.

- Démarrage et arrêt d'un invité

  Vous pouvez démarrer ou arrêter un invité de machine virtuelle à partir du Virtual Machine Manager. Pour modifier l'état de la machine virtuelle, cliquez avec le bouton droit sur l'entrée VM Guest et sélectionnez Exécuter ou l'une des options d'arrêt dans le menu contextuel.



- Redémarrer un invité

  Vous pouvez redémarrer une machine virtuelle invitée à partir du Virtual Machine Manager. Pour redémarrer la machine virtuelle, cliquez avec le bouton droit sur l'entrée VM Guest, puis sélectionnez Arrêter > Redémarrer dans le menu contextuel.

- Supprimer un invité

  La suppression d'un invité de machine virtuelle entraîne la suppression de sa configuration XML par défaut. Vous pouvez également supprimer les fichiers de stockage d'un invité. Cela efface complètement l'invité.

  1. Dans le Virtual Machine Manager, cliquez avec le bouton droit sur l'entrée VM Guest.
  2. Sélectionnez Supprimer dans le menu contextuel. Une fenêtre de confirmation s'ouvre. Remarque : L'option Supprimer est activée uniquement lorsque la machine virtuelle invitée est arrêtée.
  3. Cliquez sur Delete.
  4. Pour effacer complètement l'invité, supprimez le fichier .raw associé en cochant la case Supprimer les fichiers de stockage associés.

Gérez les machines virtuelles clientes NetScaler VPX à l'aide du programme `virsh`

- Répertorier les invités VM et leurs états actuels.

Pour utiliser `virsh` pour afficher des informations sur les invités

```
virsh list --all
```

La sortie de la commande affiche tous les domaines avec leurs états. Exemple de sortie :

```
Id Name                 State
----------------------------------
  0 Domain-0           running
  1 Domain-1           paused
  2 Domain-2           inactive
  3 Domain-3           crashed
<!--NeedCopy-->
```

- Ouvrez une console `virsh`.

  Connectez la machine virtuelle invitée via la console

  ```
  virsh console [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Exemple :

  ```
  virsh console NetScaler-VPX
  ```

- Démarrez et arrêtez un invité.

  Les invités peuvent être créés à l'aide du nom de domaine ou de l'UUID du domaine.

  ```
  virsh start [<DomainName> | <DomainUUID>]
  ```

  Exemple :

  ```
  virsh start NetScaler-VPX
  ```

  Pour arrêter un invité :

  ```
  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Exemple :

  ```
  virsh shutdown NetScaler-VPX
  ```

- Redémarrer un invité

  ```
  virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Exemple :

  ```
  virsh reboot NetScaler-VPX
  ```

  Supprimer un invité

  Pour supprimer une machine virtuelle cliente, vous devez arrêter l'hôte et annuler la définition du fichier \-NSVPX-KVM <DomainName>- \ * \ _nc.xml avant d'exécuter la commande de suppression.


```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
virsh undefine [<DomainName> | <DomainUUID>]
<!--NeedCopy-->
```

Exemple :

```
virsh shutdown NetScaler-VPX
virsh undefine NetScaler-VPX
<!--NeedCopy-->
```

> Remarque : La commande delete ne supprime pas le fichier image disque qui doit être supprimé manuellement.

Provisionner l'instance NetScaler VPX avec SR-IOV, sur OpenStack

May 8, 2023

Vous pouvez déployer des instances NetScaler VPX hautes performances qui utilisent la technologie de virtualisation des E/S à racine unique (SR-IOV) sur OpenStack.

Vous pouvez déployer une instance NetScaler VPX qui utilise la technologie SR-IOV, sur OpenStack, en trois étapes :

- Activez les fonctions virtuelles (VF) SR-IOV sur l'hôte.
- Configurez et mettez les fichiers VF à la disposition d'OpenStack.
- Provisionnez le NetScaler VPX sur OpenStack.

Composants requis

Assurez-vous que vous :

- Ajoutez la carte réseau (NIC) Intel 82599 à l'hôte.
- Téléchargez et installez le dernier pilote IXGBE d'Intel.
- Liste de blocage du pilote IXGBEVF sur l'hôte. Ajoutez l'entrée suivante dans le fichier /etc/modprobe.d/blacklist.conf : Liste des blocs `ixgbevf`

> **Remarque**
>
> La version du `ixgbe` pilote doit être minimale 5.0.4.

Activer les VF SR-IOV sur l'hôte

Procédez de l'une des manières suivantes pour activer les VF SR-IOV :

- Si vous utilisez une version du noyau antérieure à 3.8, ajoutez l'entrée suivante au fichier /etc/-modprobe.d/ixgbe et redémarrez l'hôte : options ixgbe max_vfs= <number_of_VFs>
- Si vous utilisez la version 3.8 du noyau ou une version ultérieure, créez des fichiers VF à l'aide de la commande suivante :

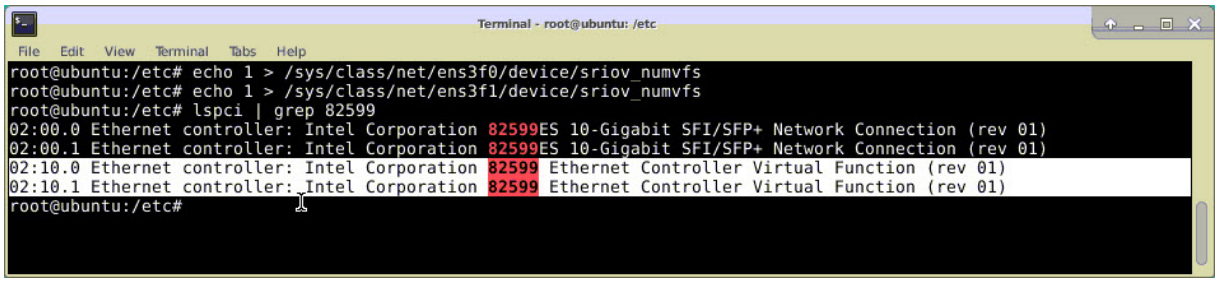
```
1     echo <number_of_VFs> > /sys/class/net/<device_name>/device/
         sriov_numvfs
2 <!--NeedCopy-->
```

Où :

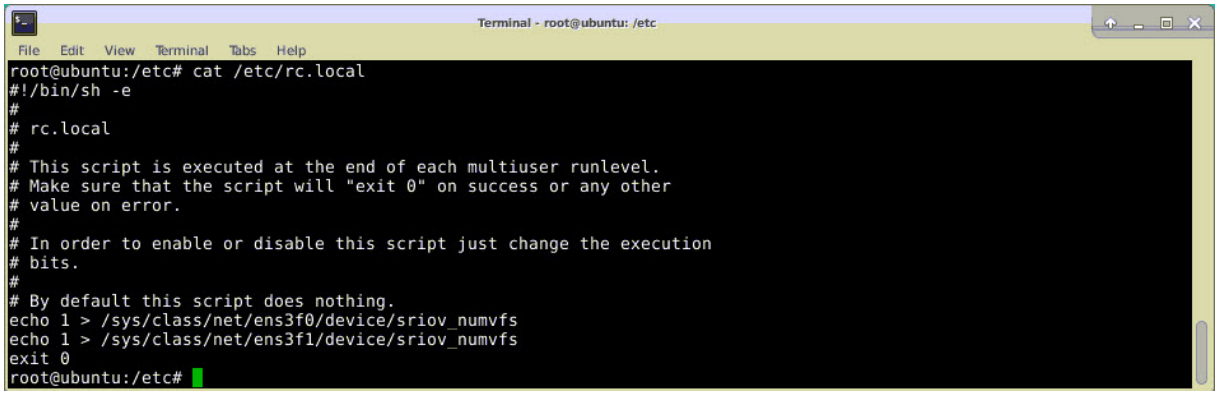
- Number_of_VFS est le nombre de fonctions virtuelles que vous souhaitez créer.
- device_name est le nom de l'interface.

> **Important**
>
> Lorsque vous créez les VF SR-IOV, veillez à ne pas leur attribuer d'adresses MAC.

Voici un exemple de quatre VF en cours de création.



Rendez les VFS persistants, ajoutez les commandes que vous avez utilisées pour créer des VFS au fichier **rc.local** . Voici un exemple montrant le contenu du fichier rc.local.



Pour plus d'informations, consultez ce guide de configuration Intel SR-IOV.

Configurer et rendre les VFS disponibles pour OpenStack

Suivez les étapes indiquées sur le lien ci-dessous pour configurer SR-IOV sur OpenStack : https://wiki.openstack.org/wiki/SR-IOV-Passthrough-For-Networking

Provisionner l'instance NetScaler VPX sur OpenStack

Vous pouvez provisionner une instance NetScaler VPX dans un environnement OpenStack à l'aide de l'interface de ligne de commande OpenStack.

Le provisioning d'une instance VPX implique éventuellement l'utilisation de données provenant du lecteur de configuration. Le lecteur de configuration est un lecteur de configuration spécial qui se fixe à l'instance lors du démarrage. Ce lecteur de configuration peut être utilisé pour transmettre des informations de configuration réseau telles que l'adresse IP de gestion, le masque réseau et la passerelle par défaut, etc., à l'instance avant de configurer les paramètres réseau de l'instance.

Lorsque OpenStack provisionnera une instance VPX, il détecte d'abord que l'instance démarre dans un environnement OpenStack, en lisant une chaîne de BIOS spécifique (OpenStack Foundation) qui indique OpenStack. Pour les distributions Red Hat Linux, la chaîne est stockée dans /etc/nova/release. Il s'agit d'un mécanisme standard disponible dans toutes les implémentations OpenStack basées sur la plate-forme hyper-viseur KVM. Le disque doit comporter une étiquette OpenStack spécifique. Si le lecteur de configuration est détecté, l'instance tente de lire les informations suivantes à partir du nom de fichier spécifié dans la commande de `nova` démarrage. Dans les procédures ci-dessous, le fichier est appelé « userdata.txt ».

- Adresse IP de gestion
- Masque réseau
- passerelle par défaut

Une fois les paramètres correctement lus, ils sont renseignés dans la pile NetScaler. Cela permet de gérer l'instance à distance. Si les paramètres ne sont pas lus correctement ou si le lecteur de configuration n'est pas disponible, l'instance passe au comportement par défaut, qui est le suivant :

- L'instance tente de récupérer les informations d'adresse IP à partir de DHCP.
- En cas d'échec ou d'expiration du protocole DHCP, l'instance définit la configuration réseau par défaut (192.168.100.1/16).

Provisionner l'instance NetScaler VPX sur OpenStack via l'interface de ligne de commande

Vous pouvez provisionner une instance VPX dans un environnement OpenStack à l'aide de l'interface de ligne de commande OpenStack. Voici le résumé des étapes à suivre pour provisionner une instance NetScaler VPX sur OpenStack :

1. Extraction du `.qcow2` fichier du fichier .tgz

2. Création d'une image OpenStack à partir de l'image qcow2
3. Provisioning une instance VPX

Pour provisionner une instance VPX dans un environnement OpenStack, procédez comme suit.

1. Extrayez le. `qcow2` fichier à partir du `.tqz` fichier en tapant la commande :

```
tar xvzf <TAR file>
tar xvzf NSVPX-KVM-12.0-26.2_nc.tgz
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```

2. Créez une image OpenStack à l'aide du `.qcoz2` fichier extrait à l'étape 1 en tapant la commande suivante :

```
glance image-create --name="<name of the OpenStack image>" --
    property hw_disk_bus=ide --is-public=true --container-format=
    bare --disk-format=qcow2< <name of the qcow2 file>

glance image-create --name="NS-VPX-12-0-26-2" --property
    hw_disk_bus=ide --is-public= true --container-format=bare --
    disk-format=qcow2< NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```

L'illustration suivante fournit un exemple de sortie pour la commande glance image-create.

Property	Value
checksum	735dae4ea6e46e39ed3f0acfba02e755
container_format	bare
created_at	2017-02-16T10:03:29Z
disk_format	qcow2
hw_disk_bus	ide
id	aeaa13e9-b49b-411c-ab54-c61820a8e2f3
min_disk	0
min_ram	0
name	NSVPX-KVM-12.0-26.2
owner	06c41a73b32f4b48af55359fd7d3502c
protected	False
size	717946880
status	active
tags	[]
updated_at	2017-02-16T10:03:38Z
virtual_size	None
visibility	private

3. Une fois qu'une image OpenStack est créée, provisionnez l'instance NetScaler VPX.

```
nova boot --image NSVPX-KVM-12.0-26.2 --config-drive=true --
   userdata
./userdata.txt --flavor m1. medium --nic net-id=3b258725-eaae-
455e-a5de-371d6d1f349f --nic port-id=218ba819-9f55-4991-adb6-
02086a6bdee2 NSVPX-10
<!--NeedCopy-->
```

Dans la commande précédente, userdata.txt est le fichier qui contient les détails tels que l'adresse IP, le masque de réseau et la passerelle par défaut de l'instance VPX. Le fichier de données utilisateur est un fichier personnalisable par l'utilisateur. NSVPX-KVM-12.0-26.2 est le nom de l'appliance virtuelle que vous souhaitez provisionner. —NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2 est le VF OpenStack.

L'illustration suivante donne un exemple de sortie de la commande nova boot.

Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	instance-0000003c
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	
accessIPv6	
adminPass	43EjPdM5shLz
config_drive	True
created	2017-02-20T11:53:37Z
flavor	m1.medium (3)
hostId	
id	6b9f6968-aab9-463c-b619-d58c73db3187
image	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
key_name	-
metadata	{}
name	NSVPX-10
os-extended-volumes:volumes_attached	[]
progress	0
security_groups	default
status	BUILD
tenant_id	06c41a73b32f4b48af55359fd7d3502c
updated	2017-02-20T11:53:38Z
user_id	418524f7101b4f0389ecbb36da9916b5

L'illustration suivante montre un exemple du fichier userdata.txt. Les valeurs contenues dans les balises <PropertySection> \ \ </PropertySection> sont celles qui sont configurables par l'utilisateur et contiennent des informations telles que l'adresse IP, le masque réseau et la passerelle par défaut.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1">
<PlatformSection>
<Kind>NOVA</Kind>
<Version>2013.1</Version>
<Vendor>Openstack</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"
   />
<Property oe:key="com.citrix.netscaler.platform" oe:value="vpx"/>
citrix.com 4
<Property oe:key="com.citrix.netscaler.orch_env"
oe:value="openstack-orch-env"/>
```



```
<Property oe:key="com.citrix.netscaler.mgmt.ip"
oe:value="10.1.0.100"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.0.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway"
oe:value="10.1.0.1"/>
</PropertySection>
</Environment>
<!--NeedCopy-->
```

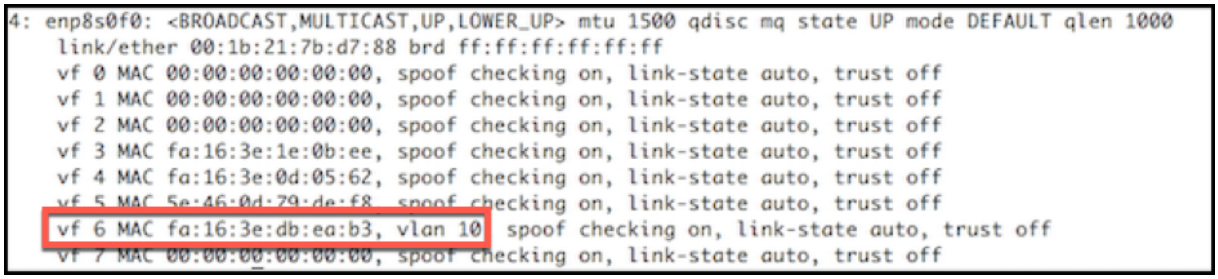
Configurations supplémentaires prises en charge : création et suppression de VLAN sur des VF SR-IOV de l'hôte

Tapez la commande suivante pour créer un VLAN sur le VF SR-IOV :

```
ip link show enp8s0f0 vf 6 vlan 10
```

Dans la commande précédente, « enp8s0f0" est le nom de la fonction physique.

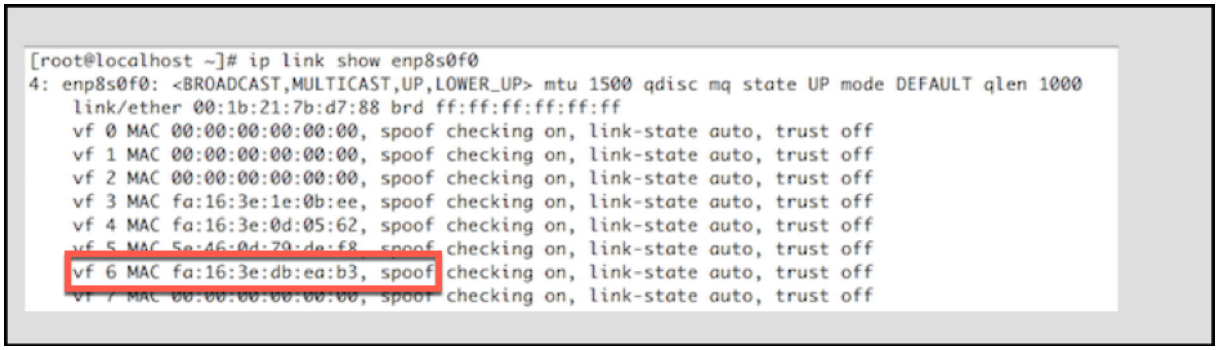
Exemple : VLAN 10, créé sur vf 6



Tapez la commande suivante pour supprimer un VLAN sur le VF SR-IOV :

```
ip link show enp8s0f0 vf 6 vlan 0
```

Exemple : VLAN 10, supprimé de vf 6



Ces étapes complètent la procédure de déploiement d'une instance NetScaler VPX qui utilise la technologie SRIOV sur OpenStack.

Configurer une instance NetScaler VPX sur KVM pour utiliser les interfaces hôtes basées sur OVS DPDK

May 5, 2023

Vous pouvez configurer une instance NetScaler VPX exécutée sur KVM (Fedora et RHOS) pour utiliser Open vSwitch (OVS) avec le kit de développement Data Plane (DPDK) afin d'améliorer les performances du réseau. Ce document explique comment configurer l'instance NetScaler VPX pour qu'elle fonctionne sur les `vhost-user` ports exposés par OVS-DPDK sur l'hôte KVM.

OVS est un commutateur virtuel multicouche sous licence Apache 2.0 open source. DPDK est un ensemble de bibliothèques et de pilotes permettant un traitement rapide des paquets.

Les versions suivantes de Fedora, RHOS, OVS et DPDK sont qualifiées pour configurer une instance NetScaler VPX :

Fedora	RHOS
Fedora 25	ENCORE 7,4
OS 2.7.0	VERSION 2.6.1
DPDK 16.11.12	DPDK 16.11.12

Composants requis

Avant d'installer DPDK, assurez-vous que l'hôte dispose de pages gigantesques de 1 Go.

Pour plus d'informations, consultez cette documentation relative à la configuration système requise pour DPDK. Voici un résumé des étapes requises pour configurer une instance NetScaler VPX sur KVM afin d'utiliser des interfaces hôtes basées sur OVS DPDK :

- Installez DPDK.
- Créez et installez OVS.
- Créez un pont OVS.
- Attachez une interface physique au pont OVS.
- Connectez des `vhost-user` ports au chemin de données OVS.
- Provisionnez un KVM-VPX avec des `vhost-user` ports OVS-DPDK.

Installer DPDK

Pour installer DPDK, suivez les instructions données dans ce document Open vSwitch with DPDK .

Construire et installer OVS

Téléchargez OVS depuis la page de téléchargementd'OVS. Ensuite, créez et installez OVS à l'aide d'un chemin de données DPDK. Suivez les instructions fournies dans le document Installer Open vSwitch .

Pour plus d'informations, consultez DPDK Getting Started Guide for Linux.

Créer un pont OVS

Selon vos besoins, tapez la commande Fedora ou RHOS pour créer un pont OVS :

Commande Fedora :

```
> $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
    datapath_type=netdev
<!--NeedCopy-->
```

Commande RHOS :

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
<!--NeedCopy-->
```

Raccorder l'interface physique au pont OVS

Liez les ports à DPDK, puis connectez-les au pont OVS en saisissant les commandes Fedora ou RHOS suivantes :

Commande Fedora :

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface
    dpdk0 type=dpdk  options:dpdk-devargs=0000:03:00.0

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface
    dpdk1 type=dpdk  options:dpdk-devargs=0000:03:00.1
<!--NeedCopy-->
```

Commande RHOS :

```
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
    options:dpdk-devargs=0000:03:00.0


ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dpdk
    options:dpdk-devargs=0000:03:00.1
<!--NeedCopy-->
```


Le `dpdk-devargs` indiqué dans les options spécifie le BDF PCI de la carte réseau physique respective.

Connectez des `vhost-user` ports au chemin de données OVS

Tapez les commandes Fedora ou RHOS suivantes pour attacher des `vhost-user` ports au chemin de données OVS :

Commande Fedora :

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000

chmod g+w  /usr/local/var/run/openvswitch/vhost*
<!--NeedCopy-->
```

Commande RHOS :

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000

ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000

chmod g+w /var/run/openvswitch/vhost*
<!--NeedCopy-->
```

Provisionner un KVM-VPX avec des `vhost-user` ports OVS-DPDK

Vous pouvez provisionner une instance VPX sur Fedora KVM avec des `vhost-user` ports OVS-DPDK uniquement à partir de l'interface de ligne de commande à l'aide des commandes QEMU suivantes : **commande Fedora** :

```
qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \

-object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages,share=on -numa node,memdev=mem \

-mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-disc-image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-format> \
```



```
-device ide-drive,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,
    bootindex=1 \

-netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \

-device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,
    bus=pci.0,addr=0x3 \

-chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-
    user1> \

-netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
    virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \

-chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-
    user2> \

-netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
    virtio-net

pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \

--nographic
<!--NeedCopy-->
```

Pour RHOS, utilisez l'exemple de fichier XML suivant pour provisionner l'instance NetScaler VPX, en utilisant. `virsh`

```
<domain type='kvm'>

  <name>dpdk-vpx1</name>

  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

  <memory unit='KiB'>16777216</memory>

  <currentMemory unit='KiB'>16777216</currentMemory>

  <memoryBacking>

    <hugepages>

      <page size='1048576' unit='KiB'/>

```



```
17      </hugepages>
18
19    </memoryBacking>
20
21    <vcpu placement='static'>6</vcpu>
22
23    <cputune>
24
25      <shares>4096</shares>
26
27      <vcpupin vcpu='0' cpuset='0'/>
28
29      <vcpupin vcpu='1' cpuset='2'/>
30
31      <vcpupin vcpu='2' cpuset='4'/>
32
33      <vcpupin vcpu='3' cpuset='6'/>
34
35      <emulatorpin cpuset='0,2,4,6'/>
36
37    </cputune>
38
39    <numatune>
40
41      <memory mode='strict' nodeset='0'/>
42
43    </numatune>
44
45    <resource>
46
47      <partition>/machine</partition>
48
49    </resource>
50
51    <os>
52
53      <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
54
55      <boot dev='hd'/>
56
57    </os>
58
59    <features>
60
61      <acpi/>
```



```
62
63      <apic/>
64
65    </features>
66
67    <cpu mode='custom' match='minimum' check='full'>
68
69      <model fallback='allow'>Haswell-noTSX</model>
70
71      <vendor>Intel</vendor>
72
73      <topology sockets='1' cores='6' threads='1'/>
74
75      <feature policy='require' name='ss'/>
76
77      <feature policy='require' name='pcid'/>
78
79      <feature policy='require' name='hypervisor'/>
80
81      <feature policy='require' name='arat'/>
82
83  <domain type='kvm'>
84
85    <name>dpdk-vpx1</name>
86
87    <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
88
89    <memory unit='KiB'>16777216</memory>
90
91    <currentMemory unit='KiB'>16777216</currentMemory>
92
93    <memoryBacking>
94
95      <hugepages>
96
97        <page size='1048576' unit='KiB'/>
98
99      </hugepages>
100
101   </memoryBacking>
102
103   <vcpu placement='static'>6</vcpu>
104
105   <cputune>
106
```



```
    <shares>4096</shares>

    <vcpupin vcpu='0' cpuset='0'/>

    <vcpupin vcpu='1' cpuset='2'/>

    <vcpupin vcpu='2' cpuset='4'/>

    <vcpupin vcpu='3' cpuset='6'/>

    <emulatorpin cpuset='0,2,4,6'/>

  </cputune>

  <numatune>

    <memory mode='strict' nodeset='0'/>

  </numatune>

  <resource>

    <partition>/machine</partition>

  </resource>

  <os>

    <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>

    <boot dev='hd'/>

  </os>

  <features>

    <acpi/>

    <apic/>

  </features>

  <cpu mode='custom' match='minimum' check='full'>

    <model fallback='allow'>Haswell-noTSX</model>
```



```
152
153     <vendor>Intel</vendor>
154
155     <topology sockets='1' cores='6' threads='1'/>
156
157     <feature policy='require' name='ss'/>
158
159     <feature policy='require' name='pcid'/>
160
161     <feature policy='require' name='hypervisor'/>
162
163     <feature policy='require' name='arat'/>
164
165     <feature policy='require' name='tsc_adjust'/>
166
167     <feature policy='require' name='xsaveopt'/>
168
169     <feature policy='require' name='pdpe1gb'/>
170
171     <numa>
172
173       <cell id='0' cpus='0-5' memory='16777216' unit='KiB' memAccess='
             shared'/>
174
175     </numa>
176
177   </cpu>
178
179   <clock offset='utc'/>
180
181   <on_poweroff>destroy</on_poweroff>
182
183   <on_reboot>restart</on_reboot>
184
185   <on_crash>destroy</on_crash>
186
187   <devices>
188
189     <emulator>/usr/libexec/qemu-kvm</emulator>
190
191     <disk type='file' device='disk'>
192
193       <driver name='qemu' type='qcow2' cache='none'/>
194
195       <source file='/home/NSVPX-KVM-12.0-52.18_nc.qcow2'/>
```



```
196
197         <target dev='vda' bus='virtio'/>
198
199         <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
               function='0x0'/>
200
201       </disk>
202
203       <controller type='ide' index='0'>
204
205         <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
               function='0x1'/>
206
207       </controller>
208
209       <controller type='usb' index='0' model='piix3-uhci'>
210
211         <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
               function='0x2'/>
212
213       </controller>
214
215       <controller type='pci' index='0' model='pci-root'/>
216
217       <interface type='direct'>
218
219         <mac address='52:54:00:bb:ac:05'/>
220
221         <source dev='enp129s0f0' mode='bridge'/>
222
223         <model type='virtio'/>
224
225         <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
               function='0x0'/>
226
227       </interface>
228
229       <interface type='vhostuser'>
230
231         <mac address='52:54:00:55:55:56'/>
232
233         <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
               'client'/>
234
235         <model type='virtio'/>
```



```
236
237         <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
               function='0x0'/>
238
239       </interface>
240
241       <interface type='vhostuser'>
242
243         <mac address='52:54:00:2a:32:64'/>
244
245         <source type='unix' path='/var/run/openvswitch/vhost-user2' mode=
               'client'/>
246
247         <model type='virtio'/>
248
249         <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
               function='0x0'/>
250
251       </interface>
252
253       <interface type='vhostuser'>
254
255         <mac address='52:54:00:2a:32:74'/>
256
257         <source type='unix' path='/var/run/openvswitch/vhost-user3' mode=
               'client'/>
258
259         <model type='virtio'/>
260
261         <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
               function='0x0'/>
262
263       </interface>
264
265       <interface type='vhostuser'>
266
267         <mac address='52:54:00:2a:32:84'/>
268
269         <source type='unix' path='/var/run/openvswitch/vhost-user4' mode=
               'client'/>
270
271        <model type='virtio'/>
272
273         <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
               function='0x0'/>
```



```
274
275      </interface>
276
277      <serial type='pty'>
278
279        <target port='0'/>
280
281      </serial>
282
283      <console type='pty'>
284
285        <target type='serial' port='0'/>
286
287      </console>
288
289      <input type='mouse' bus='ps2'/>
290
291      <input type='keyboard' bus='ps2'/>
292
293      <graphics type='vnc' port='-1' autoport='yes'>
294
295        <listen type='address'/>
296
297      </graphics>
298
299      <video>
300
301        <model type='cirrus' vram='16384' heads='1' primary='yes'/>
302
303        <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
             function='0x0'/>
304
305      </video>
306
307      <memballoon model='virtio'>
308
309        <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
             function='0x0'/>
310
311      </memballoon>
312
313    </devices>
314
315  </domain
316  <!--NeedCopy-->
```


Points à noter

Dans le fichier XML, la hugepage taille doit être de 1 Go, comme indiqué dans le fichier exemple.

```
<memoryBacking>

    <hugepages>

      <page size='1048576' unit='KiB'/>

    </hugepages>
<!--NeedCopy-->
```

En outre, dans le fichier exemple, vhost-user1 est le port vhost utilisateur lié à ovs-br0.

```
<interface type='vhostuser'>

      <mac address='52:54:00:55:55:56'/>

      <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
         'client'/>

      <model type='virtio'/>

      <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
         function='0x0'/>

    </interface>
<!--NeedCopy-->
```

Pour faire apparaître l'instance NetScaler VPX, commencez à utiliser la commande. virsh

Appliquez les configurations NetScaler VPX au premier démarrage de l'appliance NetScaler sur l'hyperviseur KVM

May 5, 2023

Vous pouvez appliquer les configurations NetScaler VPX sur l'hyperviseur KVM lors du premier démarrage de l'appliance NetScaler. Par conséquent, une configuration client sur une instance VPX peut être configurée en beaucoup moins de temps.

Pour plus d'informations sur les données utilisateur avant le lancement et leur format, voir Appliquer les configurations NetScaler VPX lors du premier démarrage de l'appliance NetScaler dans le cloud.

> Remarque :
>
> Pour amorcer à l'aide des données utilisateur avant le démarrage dans l'hyperviseur KVM, la configuration de passerelle par défaut doit être transmise dans la section <NS-CONFIG>. Pour plus d'informations sur le contenu de la balise <NS-CONFIG>, reportez-vous à la section <NS-CONFIG > Exemple suivante.

Section <NS-CONFIG> échantillon :

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0  10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP> 10.102.38.216 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Comment fournir des données utilisateur avant le démarrage sur l'hyperviseur KVM

Vous pouvez fournir des données utilisateur avant le démarrage sur l'hyperviseur KVM via un fichier ISO, qui est joint à l'aide d'un périphérique CDROM.

Fournir des données utilisateur à l'aide du fichier ISO du CD-ROM

Vous pouvez utiliser Virtual Machine Manager (VMM) pour injecter des données utilisateur dans la machine virtuelle (VM) en tant qu'image ISO à l'aide du périphérique CDROM. KVM prend en charge les CD-ROM dans VM Guest, soit en accédant directement à un lecteur physique sur le serveur hôte de la machine virtuelle, soit en accédant aux images ISO.

Les étapes suivantes vous permettent de fournir des données utilisateur à l'aide du fichier ISO du CD-ROM :

1. Créez un fichier dont le nom de fichier `userdata` contient le contenu des données utilisateur avant le démarrage.

   > Remarque : Le nom de fichier doit être strictement utilisé comme `userdata`.

2. Stockez le fichier `userdata` dans un dossier et créez une image ISO à l'aide de ce dossier.

   Vous pouvez créer une image ISO avec un fichier `userdata` en utilisant les deux méthodes suivantes :

   - En utilisant n'importe quel outil de traitement d'image tel que PowerISO.
   - Utilisation de la commande `mkisofs` sous Linux.

   L'exemple de configuration suivant montre comment générer une image ISO à l'aide de la commande `mkisofs` sous Linux.

```
root@ubuntu:~/sai/19oct# ls -lh
total 4.0K
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata
I: -input-charset not specified, using utf-8 (detected in locale
   settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
175 extents written (0 MB)
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# ls -lh
total 356K
-rw-r--r-- 1 root root 350K Oct 19 16:25 kvm-userdata.iso
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
<!--NeedCopy-->
```

3. Provisionnez l'instance NetScaler VPX à l'aide du processus de déploiement standard pour créer la machine virtuelle. Mais n'allumez pas automatiquement la machine virtuelle.
4. Ajoutez un lecteur de CD-ROM avec Virtual Machine Manager en suivant les étapes suivantes :
   a) Double-cliquez sur une entrée d'invité de machine virtuelle dans Virtual Machine Manager pour ouvrir sa console, puis passez à la vue Détails avec **Afficher > Détails**.
   b) Cliquez sur **Ajouter un matériel > Stockage > Type de périphérique > Périphérique de CD-ROM**.

c) Cliquez sur **Gérer** et sélectionnez le bon fichier ISO, puis cliquez sur **Terminer**. Un nouveau CDROM est créé sous **Ressources** sur votre instance NetScaler VPX.

5. Allumez la machine virtuelle.

NetScaler VPX sur AWS

July 7, 2023

Vous pouvez lancer une instance NetScaler VPX sur Amazon Web Services (AWS). L'appliance NetScaler VPX est disponible sous forme d'Amazon Machine Image (AMI) sur AWS Marketplace. Une instance NetScaler VPX sur AWS vous permet d'utiliser les fonctionnalités de cloud computing d'AWS et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic de NetScaler pour répondre à leurs besoins commerciaux. L'instance VPX prend en charge toutes les fonctionnalités de gestion du trafic d'une appliance NetScaler physique et peut être déployée en tant qu'instances autonomes ou en paires HA. Pour plus d'informations sur les fonctionnalités de VPX, consultez la fiche technique VPX.

Mise en route

Avant de commencer votre déploiement VPX, vous devez connaître les informations suivantes :

- Terminologie AWS
- Matrice de prise en charge AWS-VPX
- Limitations et directives d'utilisation
- Composants requis
- Comment fonctionne une instance NetScaler VPX sur AWS

Déployer une instance NetScaler VPX sur AWS

Dans AWS, les types de déploiement suivants sont pris en charge pour les instances VPX :

- Autonome
- Haute disponibilité (actif-passif)
  - Haute disponibilité dans la même zone
  - Haute disponibilité dans différentes zones grâce à Elastic IP
  - Haute disponibilité dans différentes zones grâce à une adresse IP privée
- GSLB actif-actif
- Mise à l'échelle automatique (actif-actif) à l'aide d'ADM

Déploiements hybrides

- Déployer NetScaler dans AWS Outpost
- Déployer NetScaler dans VMC dans AWS

Gestion des licences

Une instance NetScaler VPX sur AWS nécessite une licence. Les options de licence suivantes sont disponibles pour les instances NetScaler VPX exécutées sur AWS :

- Gratuit (illimité)
- Horaire
- Annuel
- BYOL
- Essai gratuit (toutes les offres d'abonnement NetScaler VPX-AWS pendant 21 jours gratuits sur AWS Marketplace.)

Automatisation

- NetScaler ADM : déploiement intelligent
- AWS Quick Starts : NetScaler VPX pour les applications Web sur AWS
- GitHub CFT : modèles et scripts NetScaler pour le déploiement d'AWS
- GitHub Ansible : modèles et scripts NetScaler pour le déploiement d'AWS
- GitHub Terraform : modèles et scripts NetScaler pour le déploiement d'AWS
- Bibliothèque de modèles AWS (PL) : NetScaler VPX

Blogs

- Comment NetScaler sur AWS aide les clients à fournir des applications en toute sécurité
- Livraison d'applications dans un cloud hybride avec NetScaler et AWS
- Citrix est un partenaire de compétence réseau AWS
- NetScaler : toujours prêt pour les clouds publics
- Évoluez ou évoluez facilement dans les clouds publics grâce à NetScaler
- Citrix élargit le choix de déploiement ADC avec AWS Outposts
- Utilisation de NetScaler avec le routage d'entrée Amazon VPC
- Citrix offre un choix, des performances et un déploiement simplifié dans AWS

- La sécurité du pare-feu NetScaler Web App, désormais disponible sur AWS Marketplace
- Comment Aria Systems utilise le pare-feu NetScaler Web App sur AWS

Mes vidéos

- Simplification des déploiements NetScaler dans le cloud public grâce à ADM
- Provisioning et configuration de NetScaler VPX dans AWS à l'aide de scripts Terraform prêts à l'emploi
- Déployer NetScaler HA dans AWS à l'aide du modèle CloudFormation
- Déployez NetScaler HA dans les zones de disponibilité à l'aide d'AWS QuickStart
- Comment déployer NetScaler dans AWS
- NetScaler Autoscale à l'aide d'ADM
- NetScaler prend en charge le dimensionnement automatique du serveur principal dans AWS ou dans le groupe AWS Autoscaling

Études de cas clients

- Solution technologique - Xenit AB
- Une meilleure façon de faire des affaires avec Citrix et le cloud AWS — Aria
- Découvrez les avantages de NetScaler et d'AWS
- Rain for Rent - Témoignage client

Solutions

- Déployez une plateforme de publicité numérique sur AWS avec NetScaler
- Améliorer l'analyse du flux de clics dans AWS à l'aide de NetScaler

Assistance

- Ouvrir un dossier de support
- Pour l'offre d'abonnement NetScaler, consultez Résoudre les problèmes liés à une instance VPXsur AWS. Pour déposer une demande d'assistance, recherchez votre numéro de compte AWS et votre code PIN d'assistance, puis appelez le support NetScaler.
- Pour l'offre NetScaler Customer Licensed ou BYOL, assurez-vous que vous disposez d'un contrat de support et de maintenance valide. Si vous n'avez pas conclu d'accord, contactez votre représentant NetScaler.

Références supplémentaires

- Webinaire à la demande AWS - NetScaler sur AWS
- Guides de déploiement pour NetScaler VPX sur AWS
- Création d'une Amazon Machine Image (AMI) VPX dans SC2S/région secrète
- NetScaler sur AWS
- Fiche technique de NetScaler VPX
- NetScaler sur AWS Marketplace
- NetScaler fait partie des solutions de mise en réseau des partenaires AWS (équilibreurs de charge)
- NetScaler pour le cloud VMware sur AWS
- FAQ AWS

Terminologie AWS

August 20, 2021

Cette section décrit la liste des termes et expressions AWS couramment utilisés. Pour plus d'informations, consultez AWS Glossary.

Terme	Définition
Image machine Amazon (AMI)	Image de machine, qui fournit les informations nécessaires au lancement d'une instance, qui est un serveur virtuel dans le cloud.
Elastic Block Store	Fournit des volumes de stockage en blocs persistants à utiliser avec des instances Amazon EC2 dans le cloud AWS.
Service de stockage simple (S3)	Stockage pour Internet. Il est conçu pour faciliter l'informatique à l'échelle du Web pour les développeurs.
Elastic Compute Cloud (EC2)	Service Web qui fournit une capacité de calcul sécurisée et redimensionnable dans le cloud. Il est conçu pour faciliter l'informatique en nuage à l'échelle du Web pour les développeurs.

Terme	Définition
Équilibrage de charge élastique (ELB)	Répartit le trafic d'application entrant sur plusieurs instances EC2, dans plusieurs zones de disponibilité. Cela augmente la tolérance aux pannes de vos applications.
Interface réseau élastique (ENI)	Interface réseau virtuelle que vous pouvez attacher à une instance dans un Virtual Private Cloud (VPC).
Adresse IP élastique (EIP)	Adresse IPv4 publique statique que vous avez allouée dans Amazon EC2 ou Amazon VPC, puis attachée à une instance. Les adresses IP Elastic sont associées à votre compte, et non à une instance spécifique. Ils sont élastiques car vous pouvez facilement les allouer, les attacher, les détacher et les libérer au fur et à mesure que vos besoins changent.
Type d'instance	Amazon EC2 propose un large choix de types d'instance optimisés pour s'adapter à différents cas d'utilisation. Les types d'instance comprennent diverses combinaisons de CPU, de mémoire, de stockage et de capacité réseau et vous offrent la flexibilité nécessaire pour choisir la combinaison appropriée de ressources pour vos applications.
Identity and Access Management (IAM)	Identité AWS avec des stratégies d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dans AWS. Vous pouvez utiliser un rôle IAM pour permettre aux applications exécutées sur une instance EC2 d'accéder en toute sécurité à vos ressources AWS. Le rôle IAM est requis pour déployer des instances VPX dans une configuration haute disponibilité.
Passerelle Internet	Connecte un réseau à Internet. Vous pouvez acheminer le trafic pour les adresses IP en dehors de votre VPC vers la Gateway Internet.

Terme	Définition
Paire de clés	Ensemble d'informations d'identification de sécurité que vous utilisez pour prouver votre identité par voie électronique. Une paire de clés se compose d'une clé privée et d'une clé publique.
Tables de routage	Ensemble de règles de routage qui contrôle le trafic quittant tout sous-réseau associé à la table de routage. Vous pouvez associer plusieurs sous-réseaux à une seule table de routage, mais un sous-réseau ne peut être associé qu'à une seule table de routage à la fois.
Groupes de sécurité	Ensemble nommé de connexions réseau entrantes autorisées pour une instance.
Sous-réseaux	Segment de la plage d'adresses IP d'un VPC auquel les instances EC2 peuvent être attachées. Vous pouvez créer des sous-réseaux pour regrouper des instances en fonction des besoins opérationnels et de sécurité.
Virtual Private Cloud (VPC)	Service Web permettant de Provisioning une section logiquement isolée du cloud AWS dans laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez.
Mise à l'échelle automatique	Service Web permettant de lancer ou de mettre fin à des instances Amazon EC2 automatiquement en fonction de stratégies, de calendriers et de vérifications de l'état définies par l'utilisateur.
CloudFormation	Service d'écriture ou de modification de modèles qui créent et suppriment ensemble des ressources AWS associées en tant qu'unité.

Matrice de prise en charge AWS-VPX

May 5, 2023

Les tableaux suivants répertorient le modèle VPX et les régions AWS, les types d'instance et les services pris en charge.

Tableau 1 : modèles VPX pris en charge sur AWS

Modèle VPX pris en charge
NetScaler VPX Édition Standard/Avancée/Premium - 200 Mbit/s
NetScaler VPX Édition Standard/Avancée/Premium - 1000 Mbit/s
NetScaler VPX Édition Standard/Avancée/Premium - 3 Gbit/s
NetScaler VPX Édition Standard/Avancée/Premium - 5 Gbit/s
NetScaler VPX Standard/Avancé/Premium - 10 Mbit/s
NetScaler VPX Express - 20 Mbit/s
NetScaler VPX - Licence client
NetScaler (anciennement NetScaler) VPX FIPS - Licence client

Tableau : 2 régions AWS prises en charge

régions AWS prises en charge
Ouest des États-Unis (Oregon)
USA West (Californie du Nord)
Est des États-Unis (Ohio)
USA Est (Virginie du Nord)
Asie-Pacifique (Mumbai)
Asie-Pacifique (Séoul)
Asie-Pacifique (Singapour)
Asie-Pacifique (Sydney)
Asie-Pacifique (Tokyo)
Asie-Pacifique (Hong Kong)
Asie-Pacifique (Osaka)

régions AWS prises en charge
Canada (Centre)
Chine (Pékin)
Chine (Ningxia)
UE (Francfort)
UE (Irlande)
UE (Londres)
UE (Paris)
UE (Milan)
Amérique du Sud (São Paulo)
AWS GovCloud (États-Unis et Est)
AWS GovCloud (USA Ouest)
Très secret d'AWS (C2S)
Moyen-Orient (Bahreïn)
Afrique (Le Cap)
C2S

Tableau 3 : types d'instance AWS pris en charge

Types d'instance AWS pris en charge
t2.medium, t2.large, t2.xlarge, t2.2xlarge
m3.large, m3.xlarge, m3.2xlarge
c4.large, c4.xlarge, c4.2xlarge, c4.4xlarge, c4.8xlarge
m4.large, m4.xlarge, m4.2xlarge, m4.4xlarge, m4.10xlarge, m4.16xlarge
m5.large, m5.xlarge, m5.2xlarge, m5.4xlarge, m5.12xlarge, m5.24xlarge
c5.large, c5.xlarge, c5.2xlarge, c5.4xlarge, c5.9xlarge, c5.18xlarge, c5.24xlarge
c5n.large, c5n.xlarge, c5n.2xlarge, c5n.4xlarge, c5n.9xlarge, c5n.18xlarge
D2.xlarge, D2.2xlarge, D2.4xlarge, D2.8xlarge
m5a.large, m5a.xlarge, m5a.2xlarge, m5a.8xlarge, m5a.12xlarge, m5a.16xlarge, m5a.24xlarge
t3a.medium, t3a.large, t3a.xlarge, t3a.2xlarge

Tableau 4 : Services AWS pris en charge

Services AWS pris en charge
EC2 : lance des instances ADC.
Lambda : invoque les API NetScaler VPX NITRO lors du provisionnement d'instances NetScaler VPX depuis CFT.
Routage d'entrée VPC et VPC : Le VPC crée des réseaux isolés dans lesquels l'ADC peut être lancé. Le routage d'entrée VPC est utilisé dans la solution d'équilibrage de charge du pare-feu.
Route53 : distribue le trafic sur tous les nœuds NetScaler VPX de la solution NetScaler Autoscale.
ELB : distribue le trafic sur tous les nœuds NetScaler VPX de la solution NetScaler Autoscale.
Cloudwatch : surveille les performances et les paramètres système de l'instance NetScaler VPX.
AWS Autoscaling : utilisé pour la mise à l'échelle automatique du serveur principal.
Formation dans le cloud : les modèles CloudFormation sont utilisés pour déployer des instances NetScaler VPX.
Service de file d'attente simple (SQS) : surveille les événements de mise à l'échelle et de réduction de la taille dans l'autoscaling principal.
Simple Notification Service (SNS) : surveille les événements de mise à l'échelle et de réduction de l'échelle dans l'autoscaling principal.
Gestion des identités et des accès (IAM) : permet d'accéder aux services et aux ressources AWS.
AWS Outposts : provisionne des instances NetScaler VPX dans AWS Outposts.

Citrix recommande les types d'instance AWS suivants :

- Séries M5 et C5n pour les éditions Marketplace ou les licences de pool basées sur la bande passante.
- Série C5n pour les licences de pool basées sur VCPU.

Offre VPX sur AWS Marketplace	Recommandation d'instance AWS
VPX 10, VPX Express 20, VPX 200	M5.xLarge
VPX 1000, VPX 3 G, VPX 5 G	M5.2xLarge

Citrix recommande les types d'instance AWS suivants en fonction du débit.

VPX avec licences groupées (licences de bande passante)	Recommandation d'instance AWS
VPX 8 G	C5n.4xLarge
VPX 10 G, VPX 15 G, VPX 25 G	C5n.9xLarge

> Remarque :
>
> L'offre VPX 25G ne donne pas le débit 25G souhaité dans AWS, mais peut donner un taux de transactions SSL plus élevé.

Pour atteindre un débit supérieur à la 5G, procédez comme suit :

- Choisissez l'offre **NetScaler VPX - Customer Licensed (BYOL)** sur AWS Marketplace.
- Sélectionnez Licences **groupées (licences de bande passante)** dans l'interface graphique ou l'interface de ligne de commande NetScaler.

Pour déterminer votre instance en fonction de différentes métriques telles que les paquets par seconde, le taux de transactions SSL, contactez votre contact Citrix pour obtenir des conseils. Pour obtenir des conseils sur les licences et le dimensionnement des pools basés sur des processeurs virtuels, contactez le support NetScaler.

Limitations et directives d'utilisation

May 5, 2023

Les limites et directives d'utilisation suivantes s'appliquent lors du déploiement d'une instance NetScaler VPX sur AWS :

- Avant de commencer, lisez la section sur la terminologie AWS dans Déployer une instance NetScaler VPXsur AWS.
- La fonctionnalité de clustering n'est pas prise en charge pour VPX.
- Pour que la configuration haute disponibilité fonctionne efficacement, associez un périphérique NAT dédié à l'interface de gestion ou associez EIP à NSIP. Pour plus d'informations sur NAT, dans la documentation AWS, consultez Instances NAT.
- Le trafic de données et le trafic de gestion doivent être séparés par les ENIs appartenant à différents sous-réseaux.
- Seule l'adresse NSIP doit être présente sur l'ENI de gestion.
- Si une instance NAT est utilisée pour la sécurité au lieu d'affecter un EIP au NSIP, des modifications appropriées de routage au niveau du VPC sont requises. Pour obtenir des instructions sur

la modification du routage au niveau du VPC, dans la documentation AWS, voir Scénario 2 : VPC with Public and Private Subnets.

- Une instance VPX peut être déplacée d'un type d'instance EC2 à un autre (par exemple, de m3.large à m3.xlarge).
- Pour les options de stockage pour VPX sur AWS, Citrix recommande EBS, car il est durable et les données sont disponibles même après leur détachement de l'instance.
- L'ajout dynamique d'ENI à VPX n'est pas pris en charge. Redémarrez l'instance VPX pour appliquer la mise à jour. Citrix vous recommande d'arrêter l'instance autonome ou HA, de joindre la nouvelle ENI, puis de redémarrer l'instance.
- Vous pouvez attribuer plusieurs adresses IP à un ENI. Le nombre maximal d'adresses IP par ENI est déterminé par le type d'instance EC2, voir la section « Adresses IP par interface réseau par type d'instance » dans Elastic Network Interfaces. Vous devez allouer les adresses IP dans AWS avant de les affecter à des ENI. Pour plus d'informations, voir Interfaces réseau Elastic.
- Citrix vous recommande d'éviter d'utiliser les commandes d'interface d'activation et de désactivation sur les interfaces NetScaler VPX.
- NetScaler `set ha node \<NODE\_ID\> -haStatus STAYPRIMARY` et `set ha node \<NODE\_ID\> -haStatus STAYSECONDARY` les commandes sont désactivés par défaut.
- IPv6 n'est pas pris en charge pour VPX.
- En raison des limitations AWS, ces fonctionnalités ne sont pas prises en charge :
  - Gratuitous ARP (GARP)
  - Mode L2
  - VLAN balisé
  - Routage dynamique
  - MAC virtuel
- Pour que RNAT fonctionne, assurez-vous que la **vérification source/destination** est désactivée. Pour plus d'informations, voir « Modification de la vérification source/destination » dans Elastic Network Interfaces.
- Lors d'un déploiement NetScaler VPX sur AWS, dans certaines régions AWS, l'infrastructure AWS peut ne pas être en mesure de résoudre les appels d'API AWS. Cela se produit si les appels d'API sont émis via une interface non administrative sur l'instance NetScaler VPX.
  Comme solution de contournement, limitez les appels d'API à l'interface de gestion uniquement. Pour ce faire, créez un NSVLAN sur l'instance VPX et liez l'interface de gestion au NSVLAN à l'aide de la commande appropriée.
  Par exemple :

```
set ns config -nsvlan <vlan id> -ifnum 1/1 -tagged NO
save config
```


Redémarrez l'instance VPX à l'invite. Pour plus d'informations sur la configuration `nsvlan`, reportez-vous à la section Configuration de NSVLAN.

- Dans la console AWS, l'utilisation du processeur virtuel indiquée pour une instance VPX sous l'onglet **Surveillance** peut être élevée (jusqu'à 100 %), même si l'utilisation réelle est bien inférieure. Pour connaître l'utilisation réelle du processeur virtuel, accédez à **Afficher toutes les métriques CloudWatch**. Pour plus d'informations, voir Surveillance de vos instances à l'aide d'Amazon CloudWatch.

Composants requis

June 20, 2023

Avant de tenter de créer une instance VPX dans AWS, assurez-vous de disposer des éléments suivants :

- **Un compte AWS** : pour lancer une AMI NetScaler VPX dans un cloud privé virtuel (VPC) AWS. Vous pouvez créer un compte AWS gratuitement sur www.aws.amazon.com.
- **Un compte d'utilisateur AWS Identity and Access Management (IAM)** : pour contrôler en toute sécurité l'accès aux services et ressources AWS pour vos utilisateurs. Pour plus d'informations sur la façon de créer un compte d'utilisateur IAM, consultez Création d'utilisateurs IAM (console). Un rôle IAM est obligatoire pour les déploiements autonomes et haute disponibilité.

  Le rôle IAM associé à votre compte AWS doit disposer des autorisations IAM suivantes pour différents scénarios.

  Paire HA avec des adresses IPv4 dans la même zone AWS :

```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

  Paire HA avec des adresses IPv6 dans la même zone AWS :

```
"ec2:DescribeInstances",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```


Couplage HA avec des adresses IPv4 et IPv6 dans la même zone AWS :

```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Paire HA avec des adresses IP élastiques dans différentes zones AWS :

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Paire HA avec des adresses IP privées dans différentes zones AWS :

```
"ec2:DescribeInstances",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Couplage HA avec des adresses IP privées et des adresses IP élastiques dans différentes zones AWS :

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```


Autoscaling du backend AWS :

```
"ec2:DescribeInstances",
"autoscaling:*",
"sns:CreateTopic",
"sns:DeleteTopic",
"sns:ListTopics",
"sns:Subscribe",
"sqs:CreateQueue",
"sqs:ListQueues",
"sqs:DeleteMessage",
"sqs:GetQueueAttributes",
"sqs:SetQueueAttributes",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
<!--NeedCopy-->
```

> Remarque :
>
> - Si vous utilisez une combinaison des fonctionnalités précédentes, utilisez la combinaison d'autorisations IAM pour chacune des fonctionnalités.
> - Si vous utilisez le modèle Citrix CloudFormation, le rôle IAM est automatiquement créé. Le modèle ne permet pas de sélectionner un rôle IAM déjà créé.
> - Lorsque vous vous connectez à l'instance VPX par le biais de l'interface graphique, une invite vous demandant de configurer les privilèges requis pour le rôle IAM s'affiche. Ignorez l'invite si vous avez déjà configuré les privilèges.

- **CLI AWS** : Pour utiliser toutes les fonctionnalités fournies par AWS Management Console à partir de votre programme terminal. Pour plus d'informations, consultez le guide de l'utilisateur de l'AWS CLI. Vous avez également besoin de l'interface de ligne de commande AWS pour changer le type d'interface réseau en SR-IOV.
- **Elastic Network Adapter (ENA)** : pour le type d'instance activé par le pilote ENA, par exemple les instances M5, C5, la version du microprogramme doit être 13.0 et supérieure.
- Vous devez configurer le service de métadonnées d'instance (IMDS) sur l'instance EC2 pour NetScaler VPX. IMDSv1 et IMDSv2 sont deux modes disponibles pour accéder aux métadonnées d'instance à partir d'une instance AWS EC2 en cours d'exécution. L'IMDSv2 est plus sécurisé que l'IMDSv1. Vous pouvez configurer l'instance pour utiliser les deux méthodes (option par défaut) ou uniquement le mode IMDSv2 (en désactivant IMDSv1). Citrix ADC VPX prend en charge le mode IMDSv2 uniquement à partir de la version 13.1.48.x de NetScaler VPX.

Configurer les rôles AWS IAM sur une instance NetScaler VPX

May 5, 2023

Les applications qui s'exécutent sur une instance Amazon EC2 doivent inclure des informations d'identification AWS dans les demandes d'API AWS. Vous pouvez stocker les informations d'identification AWS directement dans l'instance Amazon EC2 et autoriser les applications de cette instance à utiliser ces informations d'identification. Mais vous devez ensuite gérer les informations d'identification et vous assurer qu'elles sont transmises en toute sécurité à chaque instance et mettre à jour chaque instance Amazon EC2 au moment de la rotation des informations d'identification. Cela représente beaucoup de travail supplémentaire.

Vous pouvez et devez plutôt utiliser un rôle de gestion des identités et des accès (IAM) pour gérer les informations d'identification temporaires pour les applications exécutées sur une instance Amazon EC2. Lorsque vous utilisez un rôle, vous n'avez pas besoin de distribuer des informations d'identification à long terme (telles qu'un nom d'utilisateur et un mot de passe ou des clés d'accès) à une instance Amazon EC2. Le rôle fournit plutôt des autorisations temporaires que les applications peuvent utiliser lorsqu'elles effectuent des appels vers d'autres ressources AWS. Lorsque vous lancez une instance Amazon EC2, vous spécifiez un rôle IAM à associer à l'instance. Les applications qui s'exécutent sur l'instance peuvent ensuite utiliser les informations d'identification temporaires fournies par le rôle pour signer les demandes d'API.

Le rôle IAM associé à votre compte AWS doit disposer des autorisations IAM suivantes pour différents scénarios.

Paire HA avec des adresses IPv4 dans la même zone AWS :

```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Paire HA avec des adresses IPv6 dans la même zone AWS :

```
"ec2:DescribeInstances",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Couplage HA avec des adresses IPv4 et IPv6 dans la même zone AWS :


```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Paire HA avec des adresses IP élastiques dans différentes zones AWS :

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Paire HA avec des adresses IP privées dans différentes zones AWS :

```
"ec2:DescribeInstances",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Couplage HA avec des adresses IP privées et des adresses IP élastiques dans différentes zones AWS :

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```


Autoscaling du backend AWS :

```
"ec2:DescribeInstances",
"autoscaling:*",
"sns:CreateTopic",
"sns:DeleteTopic",
"sns:ListTopics",
"sns:Subscribe",
"sqs:CreateQueue",
"sqs:ListQueues",
"sqs:DeleteMessage",
"sqs:GetQueueAttributes",
"sqs:SetQueueAttributes",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Points à noter :

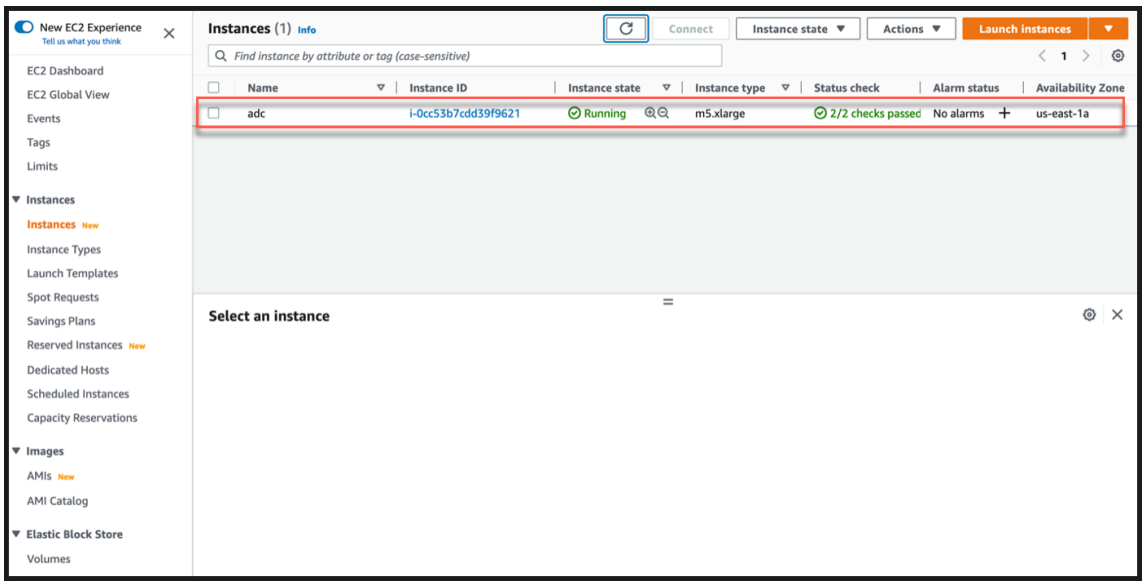
- Si vous utilisez une combinaison des fonctionnalités précédentes, utilisez la combinaison d'autorisations IAM pour chacune des fonctionnalités.
- Si vous utilisez le modèle Citrix CloudFormation, le rôle IAM est automatiquement créé. Le modèle ne permet pas de sélectionner un rôle IAM déjà créé.
- Lorsque vous vous connectez à l'instance VPX par le biais de l'interface graphique, une invite vous demandant de configurer les privilèges requis pour le rôle IAM s'affiche. Ignorez l'invite si vous avez déjà configuré les privilèges.
- Un rôle IAM est obligatoire pour les déploiements autonomes et haute disponibilité.

Créer un rôle IAM

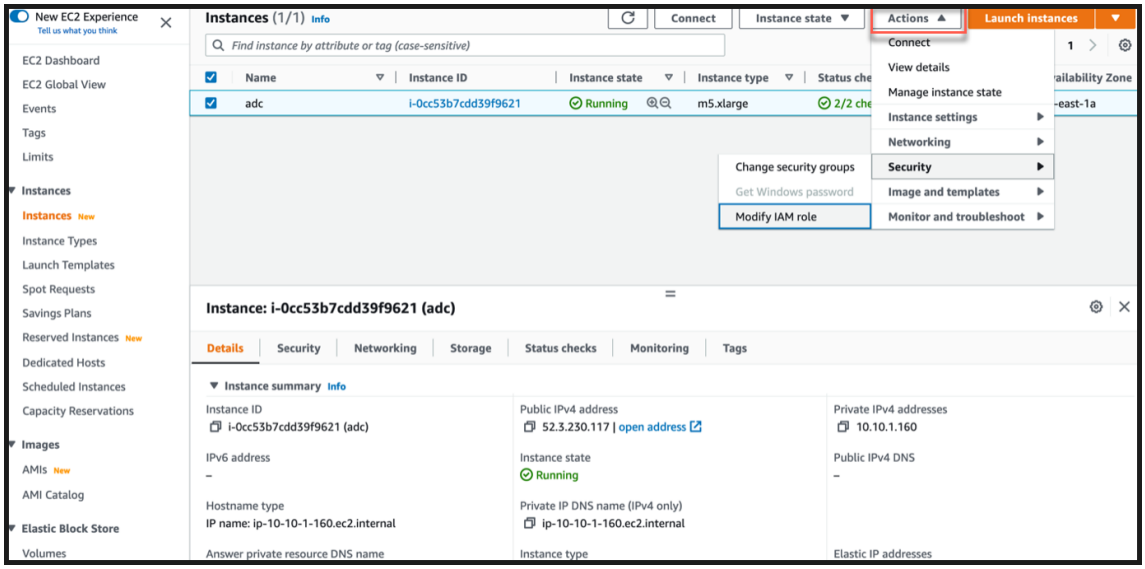
Cette procédure explique comment créer un rôle IAM pour la fonctionnalité de dimensionnement automatique du back-end d'AWS.

> **Remarque :**
>
> Vous pouvez suivre la même procédure pour créer tous les rôles IAM correspondant à d'autres fonctionnalités.

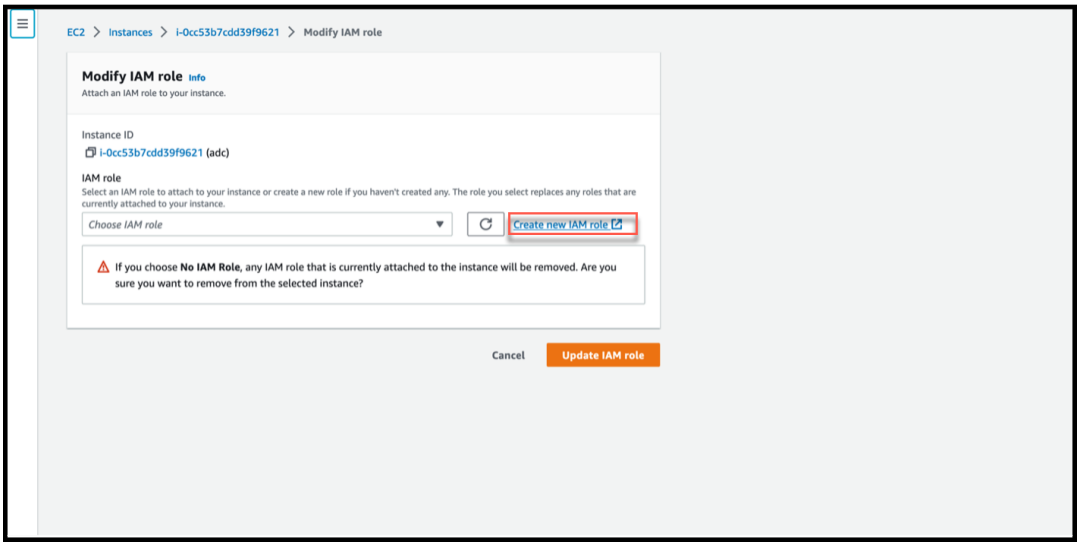
1. Connectez-vous à la console de gestion AWS pour EC2.
2. Accédez à la page de l'instance EC2 et sélectionnez votre instance ADC.



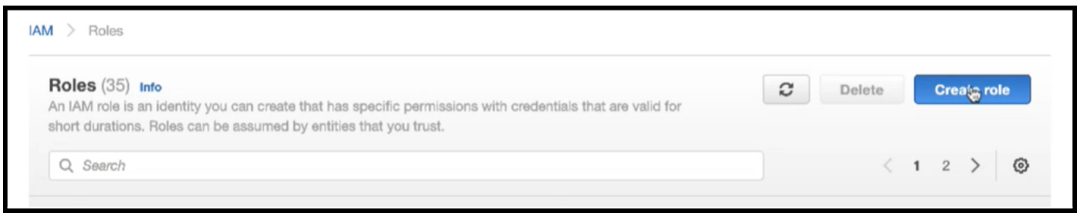
3. Accédez à **Actions > Sécurité > Modifier le rôle IAM**.



4. Sur la page **Modifier le rôle IAM**, vous pouvez choisir un rôle IAM existant ou créer un rôle IAM.
5. Pour créer un rôle IAM, procédez comme suit :
    a) Sur la page **Modifier le rôle IAM**, cliquez sur **Créer un nouveau rôle IAM**.



b) Sur la page **Rôles**, cliquez sur **Créer un rôle**.



c) Sélectionnez le **service AWS** sous **Type d'entité de confiance** et **EC2** sous **Cas d'utilisation courants**, puis cliquez sur **Suivant**.

d) Sur la page **Ajouter des autorisations**, cliquez sur **Créer une politique**.

e) Cliquez sur l'onglet **JSON** pour ouvrir l'éditeur JSON.

f) Dans l'éditeur JSON, supprimez tout et collez les autorisations IAM pour la fonctionnalité que vous souhaitez utiliser.

Par exemple, collez les autorisations IAM suivantes pour la fonctionnalité de mise à l'échelle automatique du back-end d'AWS :

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "autoscaling:\*",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:ListTopics",
                "sns:Subscribe",
                "sqs:CreateQueue",
                "sqs:ListQueues",
                "sqs:DeleteMessage",
                "sqs:GetQueueAttributes",
                "sqs:SetQueueAttributes",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "\*"
         }
```

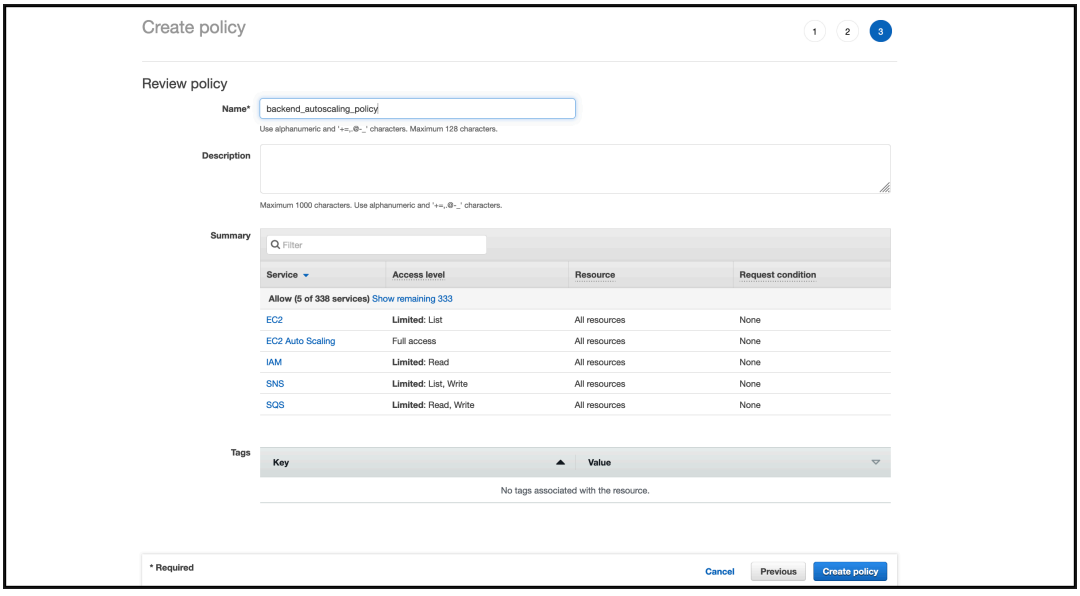


```
26
27        ]
28    }
29
30
31  <!--NeedCopy-->
```

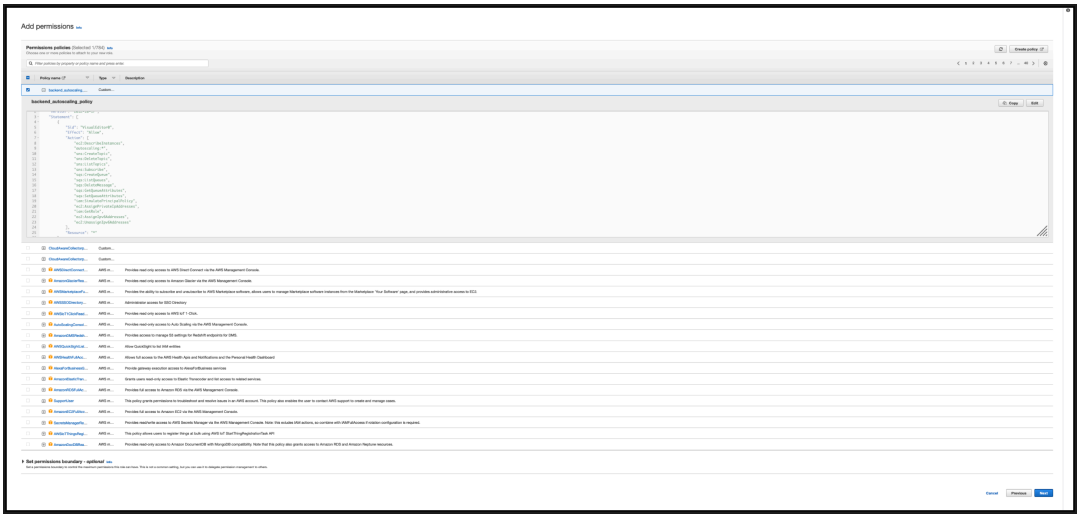
Assurez-vous que la paire clé-valeur « Version » que vous fournissez est identique à celle générée automatiquement par AWS.

g) Cliquez sur **Suivant : Réviser**.

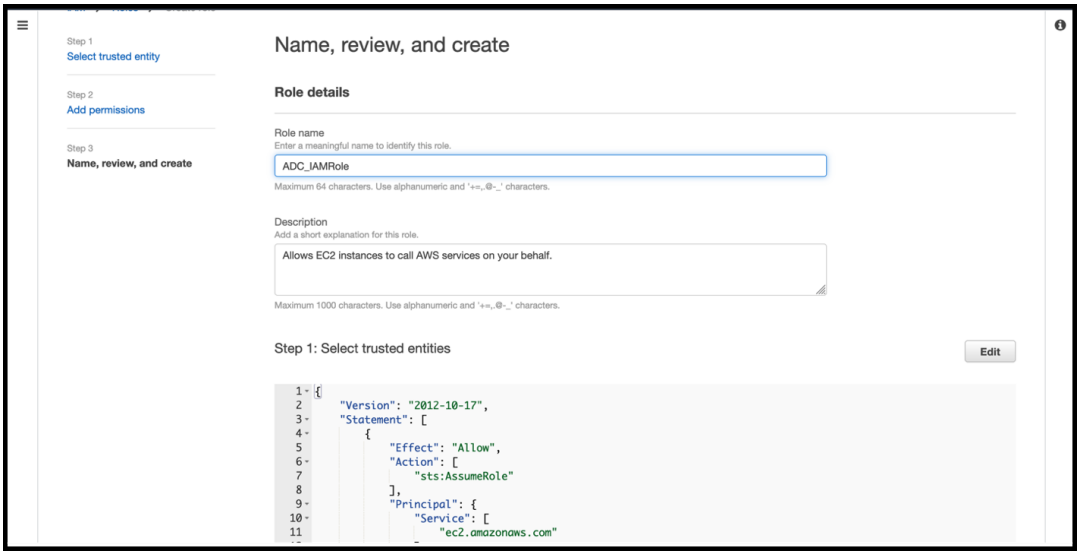
h) Dans l'onglet **Révision de la politique**, donnez un nom valide à la politique, puis cliquez sur **Créer une politique**.



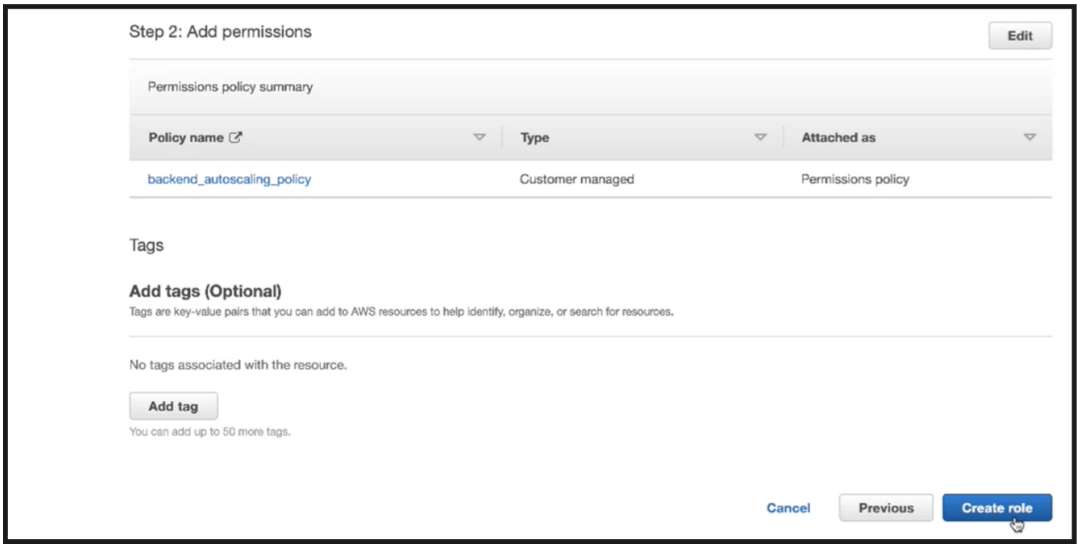
i) Sur la page **Identity Access Management**, cliquez sur le nom de la politique que vous avez créée. Développez la politique pour vérifier l'intégralité du JSON, puis cliquez sur **Suivant**.



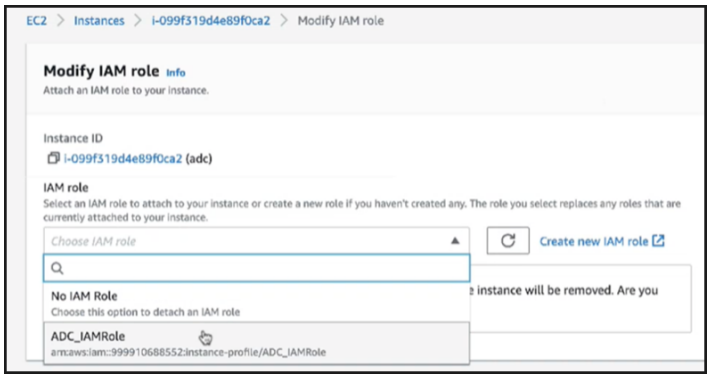
j) Dans la page **Nom, révision et création**, attribuez un nom valide au rôle.



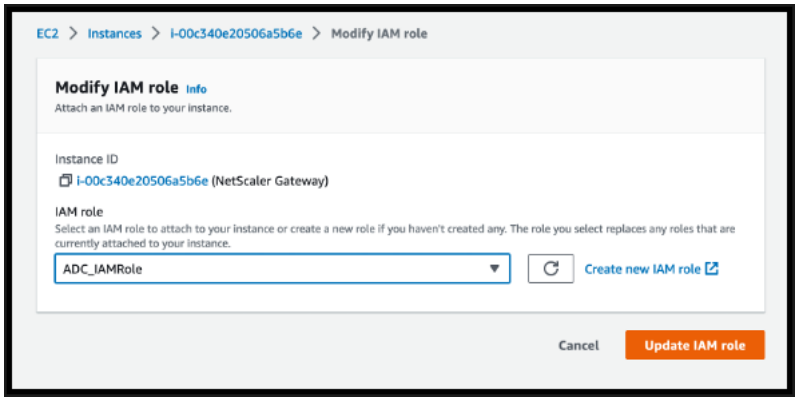
k) Cliquez sur **Créer un rôle**.



6. Répétez les étapes 1, 2 et 3. Cliquez sur le bouton **Actualiser** et sélectionnez le menu déroulant pour voir le rôle que vous avez créé.



7. Cliquez sur **Mettre à jour le rôle IAM**.

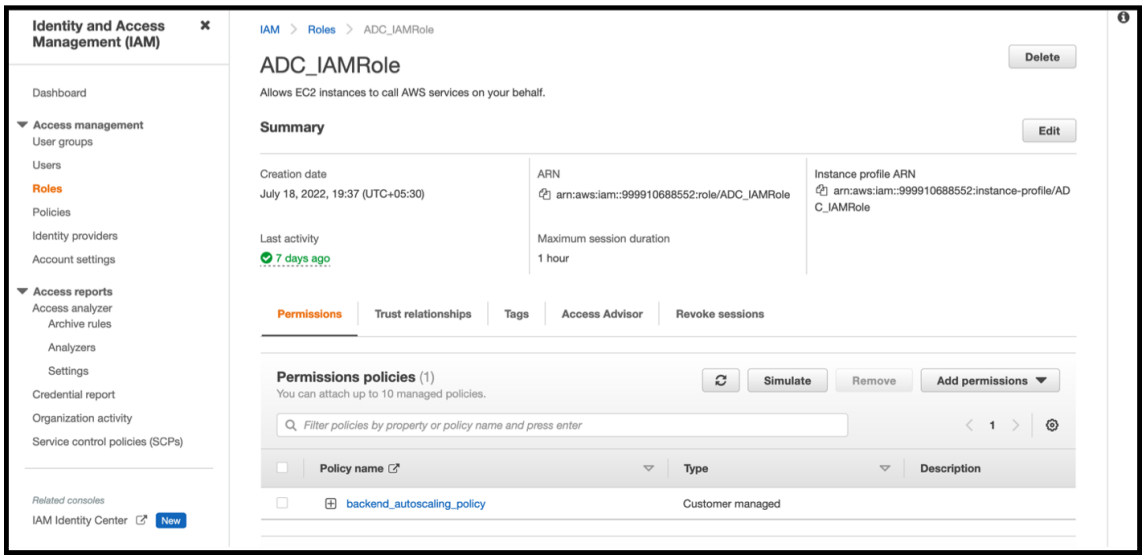


Testez les politiques IAM avec le simulateur de politiques IAM

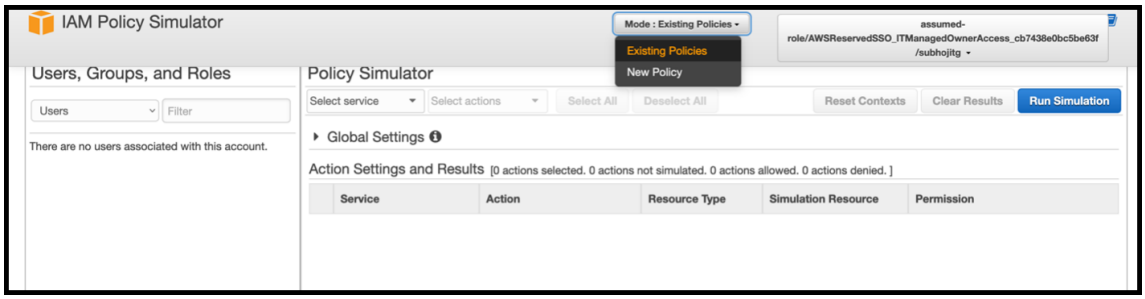
Le simulateur de politiques IAM est un outil qui vous permet de tester les effets des politiques de contrôle d'accès IAM avant de les mettre en production. Il est plus facile de vérifier et de résoudre les

problèmes liés aux autorisations.

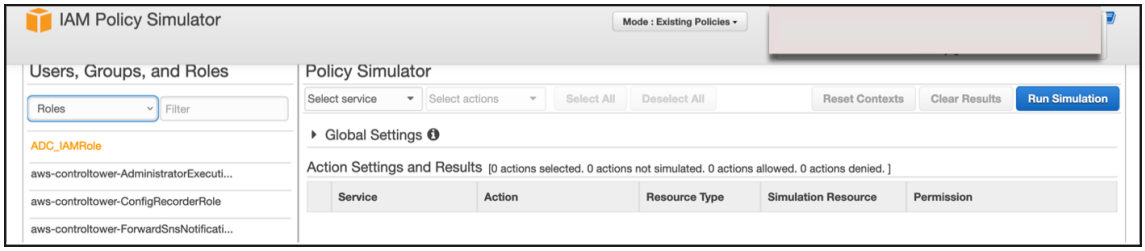
1. **Sur la page**IAM**, sélectionnez le rôle IAM que vous souhaitez tester, puis cliquez sur Simuler.** Dans l'exemple suivant, « ADC_IAMRole » est le rôle IAM.



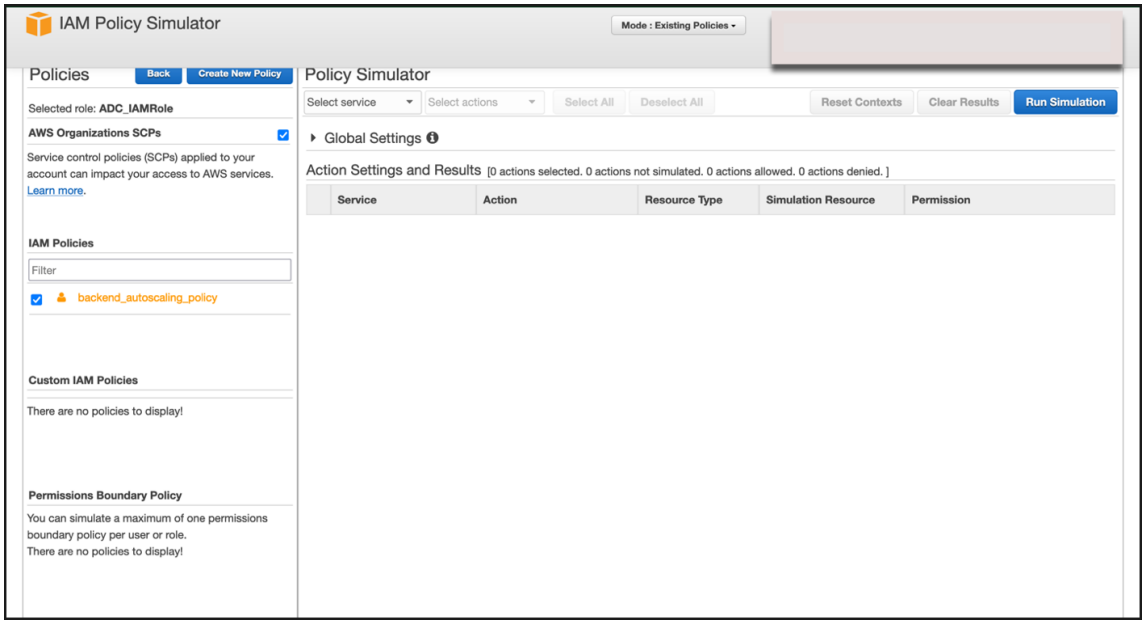
2. Dans la console du **simulateur de politiques IAM**, sélectionnez **Politiques existantes** comme **mode.**



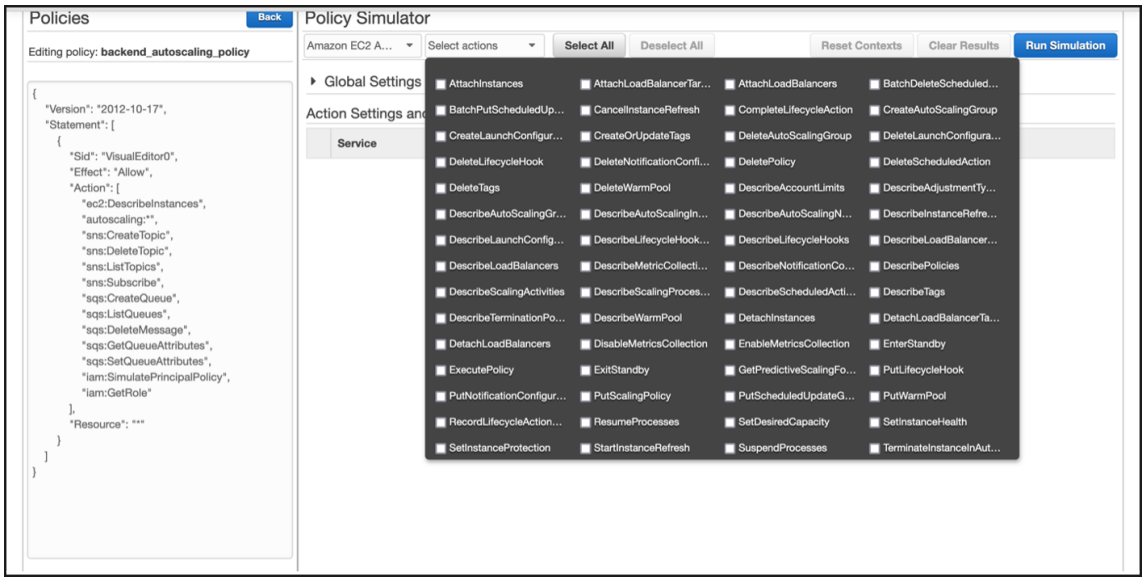
3. Dans l'onglet **Utilisateurs, groupes et rôles**, sélectionnez **Rôles** dans le menu déroulant et choisissez un rôle existant.



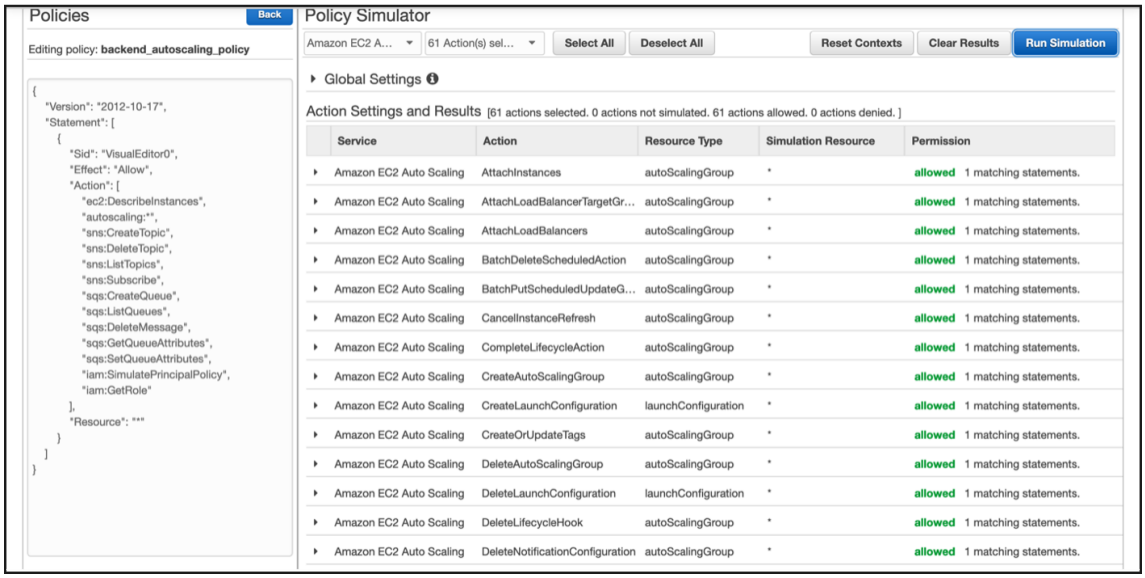
4. Après avoir sélectionné le rôle existant, sélectionnez la politique existante en dessous de celui-ci.



5. Après avoir sélectionné la politique, vous pouvez voir le JSON exact sur le côté gauche de l'écran. Sélectionnez les actions souhaitées dans le menu déroulant **Sélectionner les actions** .



6. Cliquez sur **Exécuter la simulation**.



Pour des informations détaillées, consultez la documentation AWS IAM.

Autres références

Utilisation d'un rôle IAM pour accorder des autorisations aux applications exécutées sur des instances Amazon EC2

Comment fonctionne une instance NetScaler VPX sur AWS

May 5, 2023

L'instance NetScaler VPX est disponible en tant qu'AMI sur AWS Marketplace et peut être lancée en tant qu'instance EC2 au sein d'un AWS VPC. L'instance AMI NetScaler VPX nécessite au moins 2 processeurs virtuels et 2 Go de mémoire. Une instance EC2 lancée dans un VPC AWS peut également fournir les multiples interfaces, plusieurs adresses IP par interface et les adresses IP publiques et privées nécessaires à la configuration VPX. Chaque instance VPX nécessite au moins trois sous-réseaux IP :

- Un sous-réseau de gestion
- Un sous-réseau orienté client (VIP)
- Un sous-réseau orienté vers le serveur principal (SNIP, MIP, etc.)

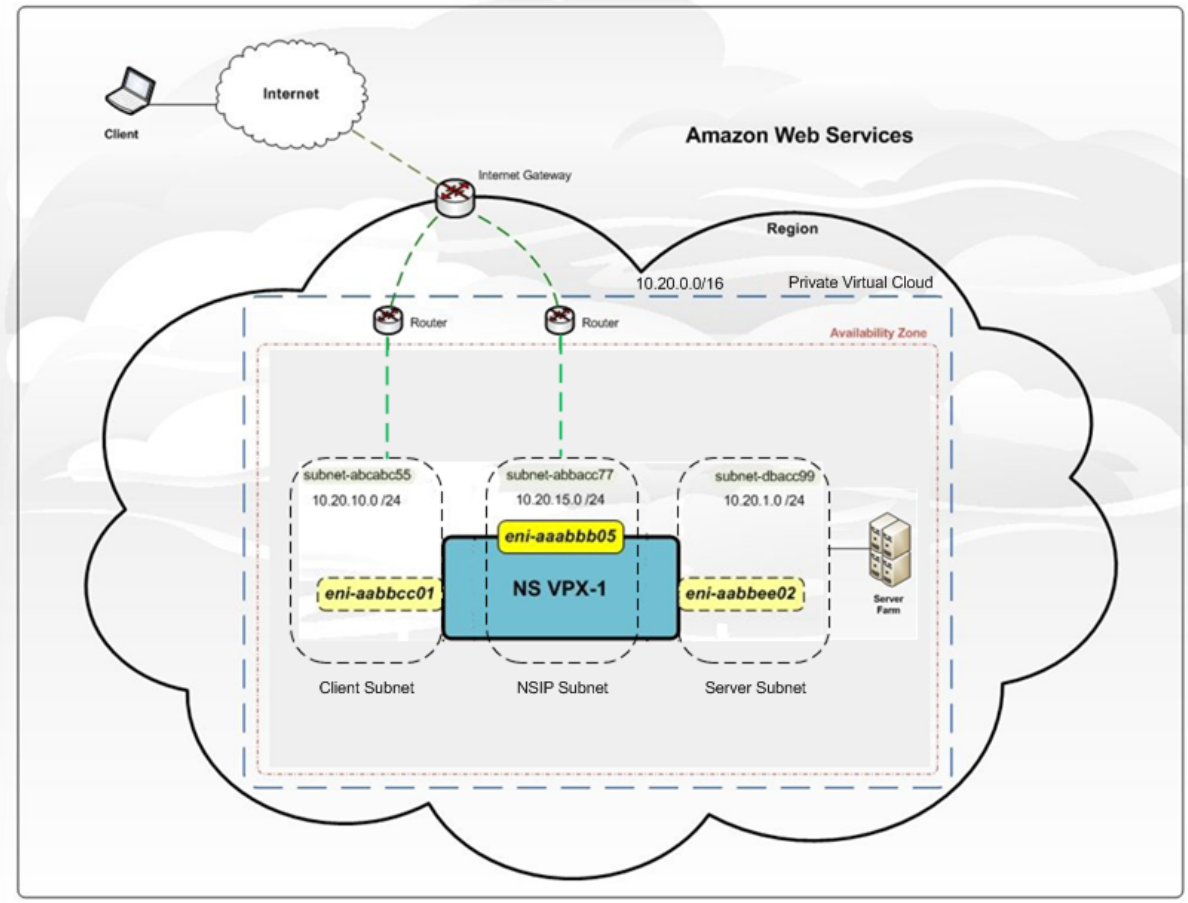
Citrix recommande trois interfaces réseau pour une instance VPX standard sur l'installation AWS.

AWS met actuellement la fonctionnalité multi-IP à la disposition des instances s'exécutant au sein d'un VPC AWS uniquement. Une instance VPX dans un VPC peut être utilisée pour équilibrer la charge des serveurs exécutant dans des instances EC2. Un Amazon VPC vous permet de créer et de contrôler

un environnement réseau virtuel, y compris votre propre plage d'adresses IP, vos sous-réseaux, vos tables de routage et vos passerelles réseau.

Remarque : Par défaut, vous pouvez créer jusqu'à 5 instances VPC par région AWS pour chaque compte AWS. Vous pouvez demander des limites de VPC plus élevées en soumettant le formulaire http://aws.amazon.com/contact-us/vpc-requestde demande d'Amazon.

Figure 1. Exemple de déploiement d'une instance NetScaler VPX sur l'architecture AWS



La figure 1 montre une topologie simple d'un VPC AWS avec un déploiement NetScaler VPX. Le VPC AWS comprend :

1. Une passerelle Internet unique pour acheminer le trafic entrant et sortant du VPC.
2. Connectivité réseau entre la passerelle Internet et Internet.
3. Trois sous-réseaux, un pour la gestion, un pour le client et un pour le serveur.
4. Connectivité réseau entre la passerelle Internet et les deux sous-réseaux (gestion et client).
5. Une instance NetScaler VPX autonome déployée au sein du VPC. L'instance VPX a trois ENI, un attaché à chaque sous-réseau.

Déployer une instance autonome NetScaler VPX sur AWS

May 8, 2023

Vous pouvez déployer une instance autonome NetScaler VPX sur AWS à l'aide des options suivantes :

- console Web AWS
- Modèle CloudFormation créé par Citrix
- CLI AWS

Cette rubrique décrit la procédure de déploiement d'une instance NetScaler VPX sur AWS.

Avant de commencer votre déploiement, lisez les rubriques suivantes :

- Composants requis
- Directives de limitation et d'utilisation

Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS

Vous pouvez déployer une instance NetScaler VPX sur AWS via la console Web AWS. Le processus de déploiement comprend les étapes suivantes :

1. Créer une paire de clés
2. Créer un cloud privé virtuel (VPC)
3. Ajouter d'autres sous-réseaux
4. Créer des groupes de sécurité et des règles de sécurité
5. Ajouter des tables de routage
6. Créer une passerelle Internet
7. Création d'une instance NetScaler VPX
8. Créez et connectez d'autres interfaces réseau
9. Attachez des adresses IP élastiques à la carte réseau de gestion
10. Se connecter à l'instance VPX

Étape 1 : Créez une paire de clés.

Amazon EC2 utilise une paire de clés pour chiffrer et déchiffrer les informations de connexion. Pour vous connecter à votre instance, vous devez créer une paire de clés, spécifier le nom de la paire de clés lorsque vous lancez l'instance et fournir la clé privée lorsque vous vous connectez à l'instance.

Lorsque vous consultez et lancez une instance à l'aide de l'assistant AWS Launch Instance, vous êtes invité à utiliser une paire de clés existante ou à créer une nouvelle paire de clés. Pour plus d'informations sur la création d'une paire de clés, consultez Paires de clés Amazon EC2.

Étape 2 : Créer un VPC.

Une instance NetScaler VPC est déployée au sein d'un VPC AWS. Un VPC vous permet de définir le réseau virtuel dédié à votre compte AWS. Pour plus d'informations sur AWS VPC, voir Démarrage avec Amazon VPC.

Lors de la création d'un VPC pour votre instance NetScaler VPX, tenez compte des points suivants.

- Utilisez l'option VPC avec un seul sous-réseau public uniquement pour créer un VPC AWS dans une zone de disponibilité AWS.
- Citrix vous recommande de créer au moins **trois sous-réseaux**, des types suivants :
  - Un sous-réseau pour le trafic de gestion. Vous placez l'adresse IP de gestion (NSIP) sur ce sous-réseau. Par défaut, l'interface réseau élastique (ENI) eth0 est utilisée pour l'adresse IP de gestion.
  - Un ou plusieurs sous-réseaux pour le trafic d'accès client (utilisateur vers NetScaler VPX), via lesquels les clients se connectent à une ou plusieurs adresses IP virtuelles (VIP) attribuées aux serveurs virtuels d'équilibrage de charge NetScaler.
  - Un ou plusieurs sous-réseaux pour le trafic d'accès au serveur (VPX vers serveur), via lesquels vos serveurs se connectent aux adresses IP des sous-réseaux appartenant à VPX (SNIP). Pour plus d'informations sur l'équilibrage de charge NetScaler et les serveurs virtuels, les adresses IP virtuelles (VIP) et les adresses IP de sous-réseau (SNIP), consultez :
  - Tous les sous-réseaux doivent se trouver dans la même zone de disponibilité.

Étape 3 : Ajoutez des sous-réseaux.

Lorsque vous avez utilisé l'assistant VPC, un seul sous-réseau a été créé. Selon vos besoins, vous pouvez créer d'autres sous-réseaux. Pour plus d'informations sur la création d'autres sous-réseaux, voir Ajout d'un sous-réseau à votre VPC.

Étape 4 : Créer des groupes de sécurité et des règles de sécurité.

Pour contrôler le trafic entrant et sortant, créez des groupes de sécurité et ajoutez des règles aux groupes. Pour plus d'informations sur la création de groupes et l'ajout de règles, voir Groupes de sécurité pour votre VPC.

Pour les instances NetScaler VPX, l'assistant EC2 fournit des groupes de sécurité par défaut, qui sont générés par AWS Marketplace et sont basés sur les paramètres recommandés par Citrix. Vous pouvez toutefois créer d'autres groupes de sécurité en fonction de vos besoins.

> **Remarque**
>
> Les ports 22, 80 et 443 doivent être ouverts sur le groupe de sécurité pour les accès SSH, HTTP et HTTPS respectivement.

Étape 5 : Ajoutez des tables de routage.

La table de routage contient un ensemble de règles, appelées routes, qui sont utilisées pour déterminer où le trafic réseau est dirigé. Chaque sous-réseau de votre VPC doit être associé à une table de routage. Pour plus d'informations sur la création d'une table de routage, consultez Tables de routage.

Étape 6 : Créer une Gateway Internet.

Une passerelle Internet a deux objectifs : fournir une cible dans les tables de routage de votre VPC pour le trafic routable sur Internet et effectuer la traduction d'adresses réseau (NAT) pour les instances auxquelles des adresses IPv4 publiques ont été attribuées.

Créez une Gateway Internet pour le trafic Internet. Pour plus d'informations sur la création d'une passerelle Internet, reportez-vous à la section Attachement d'une passerelle Internet.

Étape 7 : Créez une instance NetScaler VPX à l'aide du service AWS EC2.

Pour créer une instance NetScaler VPX à l'aide du service AWS EC2, procédez comme suit.

1. Dans le tableau de bord AWS, accédez à **Calcul > EC2 > Launch Instance > AWS Marketplace**.

   Avant de cliquer sur **Launch Instance**, assurez-vous que votre région est correcte en consultant la note qui apparaît sous **Launch Instance**.

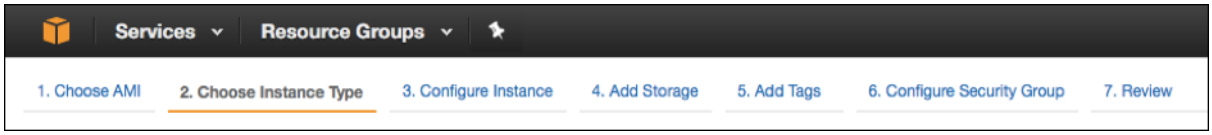
   

2. Dans la barre de recherche sur AWS Marketplace, effectuez une recherche à l'aide du mot clé NetScaler VPX.
3. Sélectionnez la version à déployer, puis cliquez sur **Sélectionner**. Pour la version NetScaler VPX, vous disposez des options suivantes :

   - Une version sous licence
   - Appliance NetScaler VPX Express (Il s'agit d'une appliance virtuelle gratuite, disponible depuis NetScaler 12.0 56.20.)
   - Apportez votre propre appareil

L'assistant de lancement d'instance démarre. Suivez l'assistant pour créer une instance. L'assistant vous invite à :

- Choisir le type d'instance
- Configurer l'instance
- Ajouter un espace de stockage
- Ajouter des balises
- Configurer le groupe de sécurité
- Critique



Étape 8 : Créez et connectez d'autres interfaces réseau.

Créez deux interfaces réseau supplémentaires pour VIP et SNIP. Pour plus d'informations sur la création d'autres interfaces réseau, reportez-vous à la section Création d'une interface réseau .

Après avoir créé les interfaces réseau, vous devez les attacher à l'instance VPX. Avant de joindre l'interface, arrêtez l'instance VPX, connectez l'interface et mettez l'instance sous tension. Pour plus d'informations sur la connexion d'interfaces réseau, consultez la section Attachement d'une interface réseau lors du lancement d'une instance .

Étape 9 : Allouer et associer des IP élastiques.

Si vous attribuez une adresse IP publique à une instance EC2, elle reste attribuée uniquement jusqu'à ce que l'instance soit arrêtée. Après cela, l'adresse est libérée dans le pool. Lorsque vous redémarrez l'instance, une nouvelle adresse IP publique est attribuée.

En revanche, une adresse IP élastique (EIP) reste affectée jusqu'à ce que l'adresse soit dissociée d'une instance.

Allouer et associer une IP élastique pour la carte réseau de gestion. Pour plus d'informations sur la façon d'allouer et d'associer des adresses IP élastiques, consultez les rubriques suivantes :

- Allocation d'une adresse IP élastique
- Associer une adresse IP Elastic à une instance en cours d'exécution

Ces étapes complètent la procédure de création d'une instance NetScaler VPX sur AWS. Cela peut prendre quelques minutes avant que l'instance soit prête. Vérifiez que votre instance a passé avec succès ses contrôles d'état. Vous pouvez consulter ces informations dans la colonne **Contrôles d'état** de la page Instances.

Étape 10 : Connectez-vous à l'instance VPX.

Après avoir créé l'instance VPX, vous connectez l'instance à l'aide de l'interface graphique et d'un client SSH.

- GUI

Les informations d'identification d'administrateur par défaut pour accéder à une instance NetScaler VPX sont les suivantes :

Nom d'utilisateur : `nsroot`

Mot de passe : le mot de passe par défaut du compte root ns est défini sur l'ID d'instance AWS de l'instance NetScaler VPX. Lors de votre première connexion, vous êtes invité à modifier le mot de passe

pour des raisons de sécurité. Après avoir modifié le mot de passe, vous devez enregistrer la configuration. Si la configuration n'est pas enregistrée et que l'instance redémarre, vous devez vous connecter avec le mot de passe par défaut. Modifiez à nouveau le mot de passe lorsque vous y êtes invité.

- Client SSH

Dans la console de gestion AWS, sélectionnez l'instance NetScaler VPX et cliquez sur Connect. Suivez les instructions données sur la page **Connexion à votre instance** .

Pour plus d'informations sur le déploiement d'une instance autonome NetScaler VPX sur AWS à l'aide de la console Web AWS, consultez :

- Scénario : instance autonome
- Comment configurer une instance NetScaler VPX sur AWS à l'aide du modèle Citrix CloudFormation

Configurer une instance NetScaler VPX à l'aide du modèle Citrix CloudFormation

Vous pouvez utiliser le modèle CloudFormation fourni par Citrix pour automatiser le lancement d'une instance VPX. Le modèle fournit des fonctionnalités permettant de lancer une seule instance NetScaler VPX ou de créer un environnement de haute disponibilité avec deux instances NetScaler VPX.

Vous pouvez lancer le modèle depuis AWS Marketplace ou GitHub.

Le modèle CloudFormation nécessite un environnement VPC existant et lance une instance VPX avec trois interfaces réseau élastiques (ENI). Avant de démarrer le modèle CloudFormation, assurez-vous de remplir les conditions suivantes :

- Un cloud privé virtuel (VPC) AWS
- Trois sous-réseaux au sein du VPC : un pour la gestion, un pour le trafic client et un pour les serveurs principaux
- Une paire de clés EC2 pour activer l'accès SSH à l'instance
- Un groupe de sécurité avec des ports UDP 3003, TCP 3009—3010, HTTP et SSH ouverts

Consultez la section « Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS » ou la documentation AWS pour plus d'informations sur la manière de remplir les conditions préalables.

Regardez cette vidéo pour découvrir comment configurer et lancer une instance autonome NetScaler VPX à l'aide du modèle Citrix CloudFormation disponible sur AWS Marketplace.

En outre, vous configurez et lancez une instance autonome NetScaler VPX Express à l'aide du modèle Citrix CloudFormation disponible sur GitHub :

https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/

Un rôle IAM n'est pas obligatoire pour un déploiement autonome. Citrix vous recommande toutefois de créer et d'associer un rôle IAM doté des privilèges requis à l'instance, en cas de besoin futur. Le

rôle IAM garantit que l'instance autonome est facilement convertie en nœud haute disponibilité avec SR-IOV, si nécessaire.

Pour plus d'informations sur les privilèges requis, consultez la section Configuration des instances NetScaler VPX pour utiliser l'interface réseau SR-IOV.

> Remarque
> Si vous déployez une instance NetScaler VPX sur AWS à l'aide de la console Web AWS, le service CloudWatch est activé par défaut. Si vous déployez une instance NetScaler VPX à l'aide du modèle Citrix CloudFormation, l'option par défaut est « Oui ». Si vous souhaitez désactiver le service CloudWatch, sélectionnez « Non ». Pour plus d'informations, voir Surveillance de vos instances à l'aide d'Amazon CloudWatch.

Configurer une instance NetScaler VPX à l'aide de l'AWS CLI

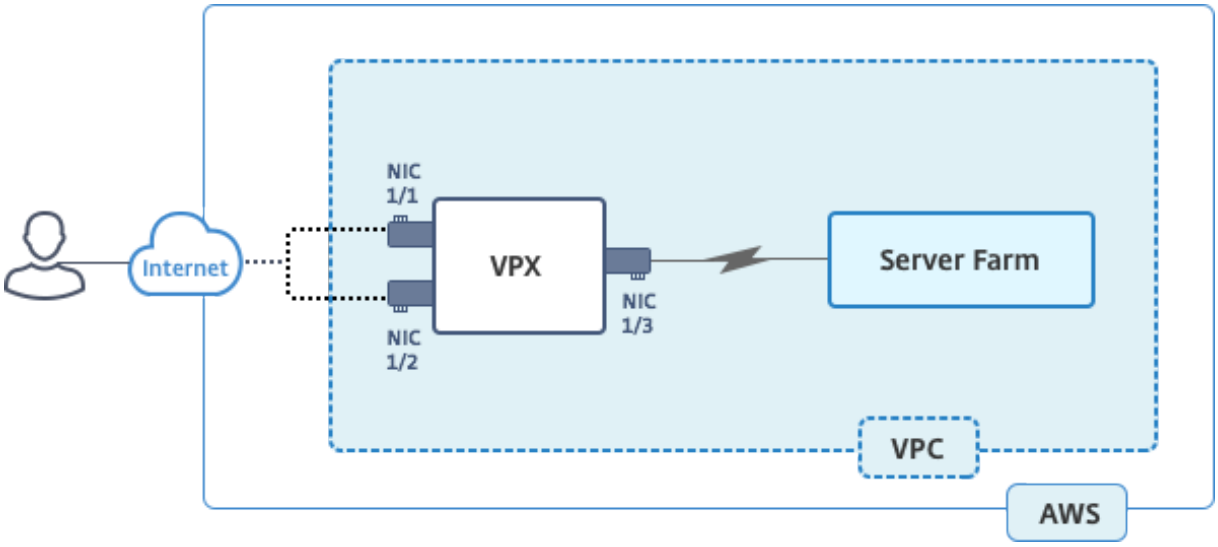
Vous pouvez utiliser l'interface de ligne de commande AWS pour lancer des instances. Pour plus d'informations, consultez la documentation de l'interface de ligne de commande AWS.

Scénario : instance autonome

May 8, 2023

Ce scénario montre comment déployer une instance EC2 autonome NetScaler VPX dans AWS à l'aide de l'interface graphique AWS. Créez une instance VPX autonome avec trois cartes réseau. L'instance, qui est configurée comme un serveur virtuel d'équilibrage de charge, communique avec les serveurs principaux (le parc de serveurs). Pour cette configuration, configurez les routes de communication requises entre l'instance et les serveurs dorsaux, et entre l'instance et les hôtes externes sur Internet public.

Pour plus de détails sur la procédure de déploiement d'une instance VPX, consultez Déployer une instance autonome NetScaler VPXsur AWS.

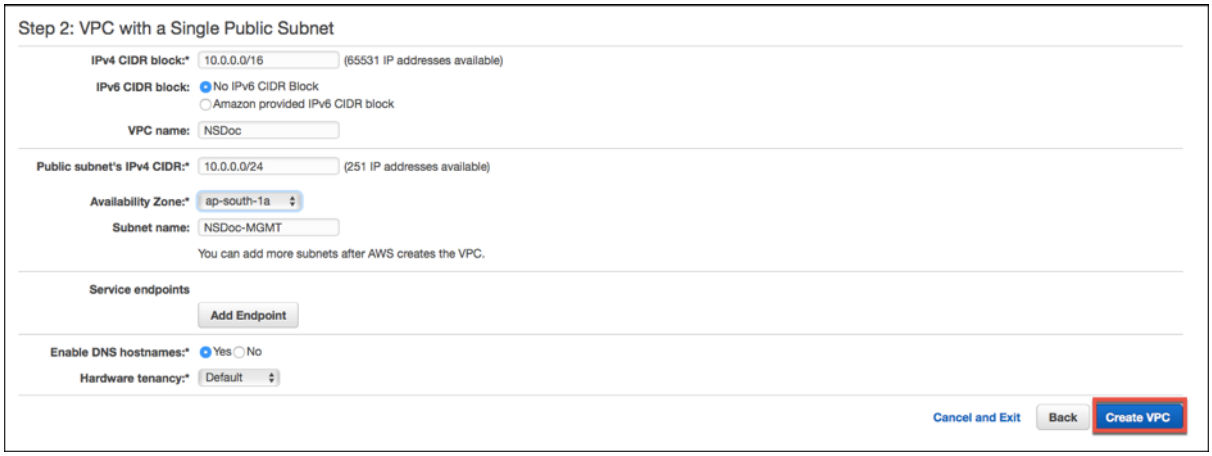


Créez trois cartes réseau. Chaque carte réseau peut être configurée avec une paire d'adresses IP (publique et privée). Les cartes réseau répondent aux objectifs suivants.

Carte d'interface réseau	Motif	Associé à
eth0	Sert le trafic de gestion (NSIP)	Une adresse IP publique et une adresse IP privée
eth1	Sert le trafic côté client (VIP)	Une adresse IP publique et une adresse IP privée
eth2	Communication avec les serveurs back-end (SNIP)	Une adresse IP publique (l'adresse IP privée n'est pas obligatoire)

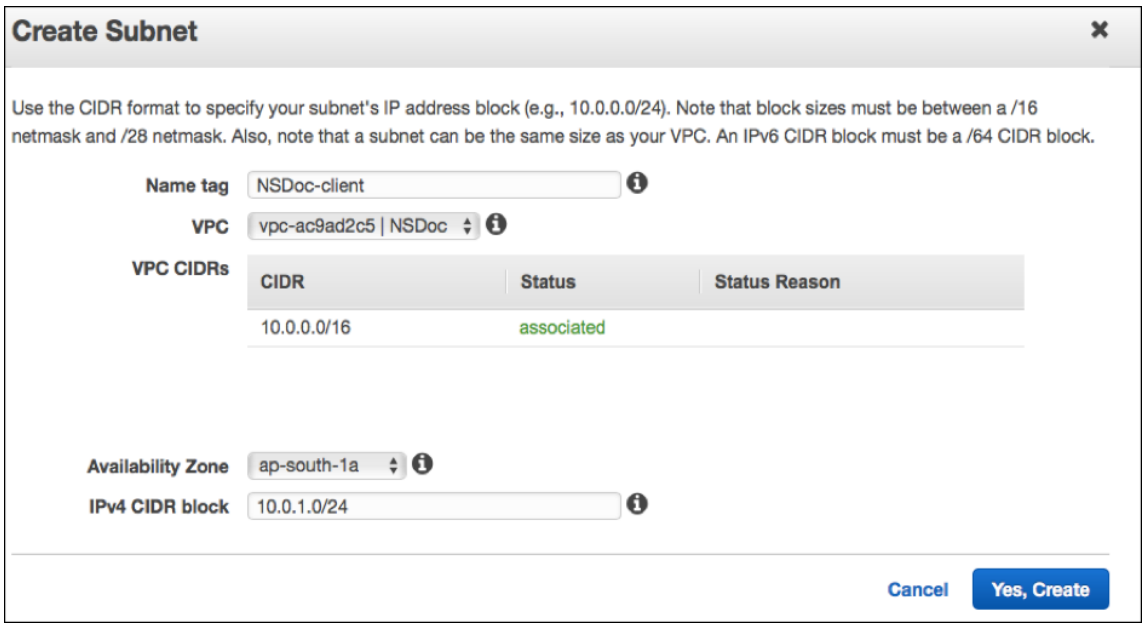
Étape 1 : Créer un VPC.

1. Connectez-vous à la console Web AWS et accédez à **Networking & Content Delivery** > **VPC.** Cliquez sur **Démarrer l'assistant VPC**.
2. **Sélectionnez**VPC avec un seul sous-réseau public**et cliquez sur Sélectionner.**
3. Définissez le bloc d'adresse IP sur 10.0.0.0/16, pour ce scénario.
4. Donnez un nom au VPC.
5. Définissez le sous-réseau public sur 10.0.0.0/24. (Il s'agit du réseau de gestion).
6. Sélectionnez une zone de disponibilité.
7. Donnez un nom au sous-réseau.
8. Cliquez sur Créer un **VPC**.

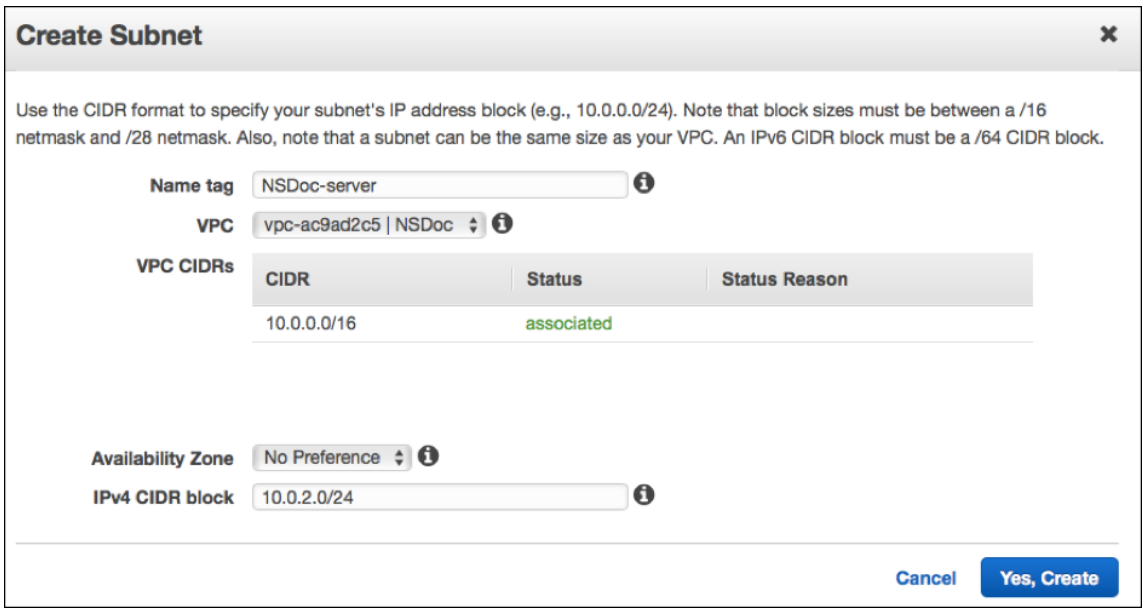


Étape 2 : Création de sous-réseaux supplémentaires

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Subnets, Create Subnet après avoir saisi les informations suivantes.
   - Balise nominative : donnez un nom à votre sous-réseau.
   - VPC : choisissez le VPC pour lequel vous créez le sous-réseau.
   - Zone de disponibilité : choisissez la zone de disponibilité dans laquelle vous avez créé le VPC à l'étape 1.
   - Bloc d'adresse CIDR IPv4 : Spécifiez un bloc d'adresse CIDR IPv4 pour votre sous-réseau. Pour ce scénario, choisissez 10.0.1.0/24.

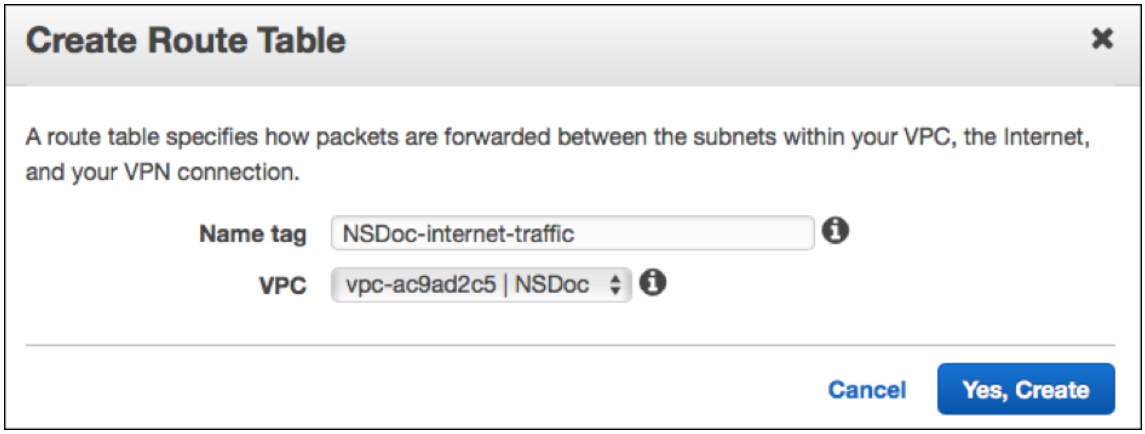


3. Répétez les étapes pour créer un sous-réseau supplémentaire pour les serveurs principaux.



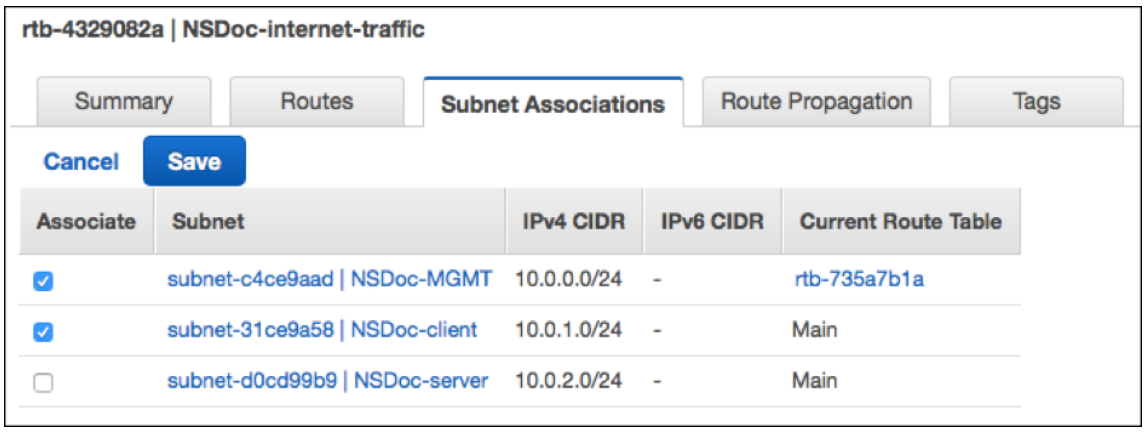
Étape 3 : Création d'une table de routage

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez **Tables de routage** > **Créer une table de routage.**
3. Dans la fenêtre Créer une table de routage, ajoutez un nom et sélectionnez le VPC que vous avez créé à l'étape 1.
4. Cliquez sur **Yes, Create**.



   La table de routage est affectée à tous les sous-réseaux que vous avez créés pour ce VPC, de sorte que le routage du trafic à partir d'une instance d'un sous-réseau peut atteindre une instance d'un autre sous-réseau.

5. Cliquez sur Associations de sous-réseau, puis sur Modifier.
6. Cliquez sur le sous-réseau client et de gestion, puis sur Enregistrer. Cela crée une table de routage pour le trafic Internet uniquement.



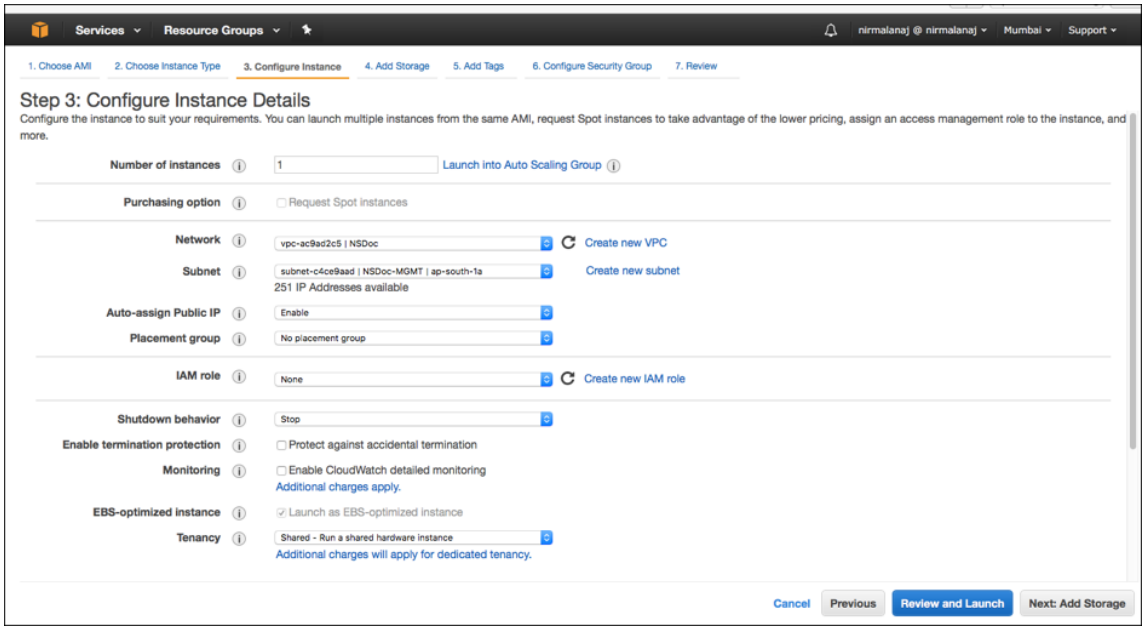
7. Cliquez sur **Itinéraires > Modifier > Ajouter un autre itinéraire**.
8. Dans le champ Destination, ajoutez 0.0.0.0/0, puis cliquez sur le champ Cible pour sélectionner igw- \ <xxxx> la passerelle Internet créée automatiquement par l'assistant VPC.
9. Cliquez sur Enregistrer.

10. Suivez les étapes pour créer une table de routage pour le trafic côté serveur.

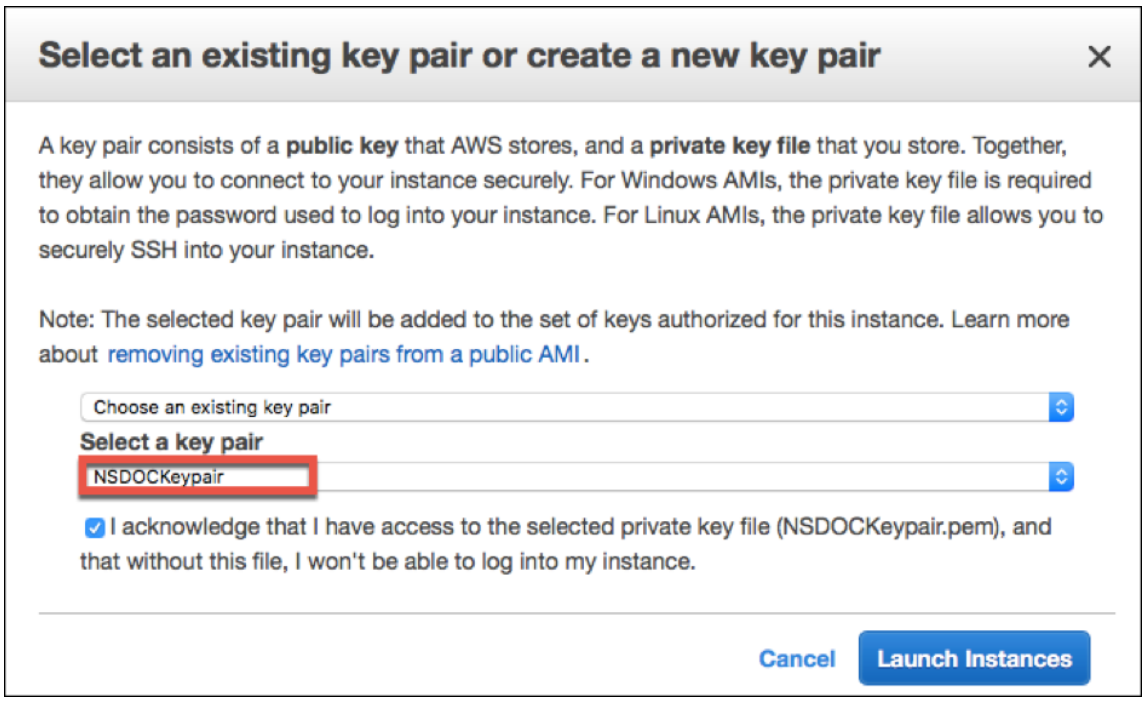
Étape 4 : Création d'une instance NetScaler VPX

1. Connectez-vous à la console de gestion AWS et cliquez sur **EC2** sous **Compute**.
2. Cliquez sur AWS Marketplace. Dans la barre de recherche sur AWS Marketplace, tapez NetScaler VPX et appuyez sur Entrée. Les éditions NetScaler VPX disponibles s'affichent.
3. Cliquez sur **Sélectionner** pour choisir l'édition NetScaler VPX souhaitée. L'assistant d'instance EC2 démarre.
4. Sur la page **Choisir le type d'instance**, sélectionnez **m4. Xlarge** (recommandé) et cliquez sur **Suivant : Configurer les détails de l'instance**.
5. Sur la page Configurer les détails de l'instance, sélectionnez les options suivantes, puis cliquez sur Suivant : Ajouter du stockage.

- Nombre d'instances : 1
- Réseau : le VPC créé à l'étape 1
- Sous-réseau : le sous-réseau de gestion
- Attribuer automatiquement une adresse IP publique : activer



6. Sur la page Ajouter du stockage, sélectionnez l'option par défaut, puis cliquez sur Suivant : Ajouter des balises.
7. Sur la page Ajouter des balises, ajoutez un nom pour l'instance, puis cliquez sur Suivant : Configurer le groupe de sécurité.
8. Sur la page Configurer le groupe de sécurité, sélectionnez l'option par défaut (générée par AWS Marketplace et basée sur les paramètres recommandés par Citrix Systems), puis cliquez sur **Vérifier et lancer > Lancer**.
9. Vous êtes invité à sélectionner une paire de clés existante ou à créer une nouvelle paire de clés. Dans la liste déroulante Sélectionner une paire de clés, sélectionnez la paire de clés que vous avez créée comme condition préalable (voir la section Prérequis).
10. Cochez la case pour accuser réception de la paire de clés et cliquez sur Launch Instances.



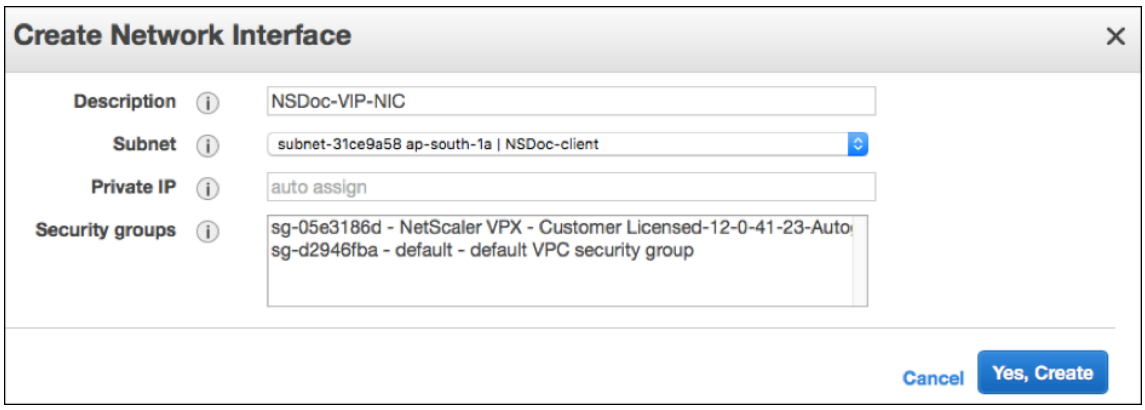
L'assistant de lancement de l'instance affiche l'état du lancement et l'instance apparaît dans la liste des instances lorsqu'elle est complètement lancée.

Pour vérifier l'instance, accédez à la console AWS et cliquez sur EC2 > Instances en cours d'exécution. Sélectionnez l'instance et ajoutez un nom. Assurez-vous que l'état de l'instance est en cours d'exécution et que les contrôles d'état sont terminés.

Étape 5 : Créez et connectez d'autres interfaces réseau.

Lorsque vous avez créé le VPC, une seule interface réseau lui était associée. Ajoutez maintenant deux interfaces réseau supplémentaires au VPC, pour le VIP et le SNIP.

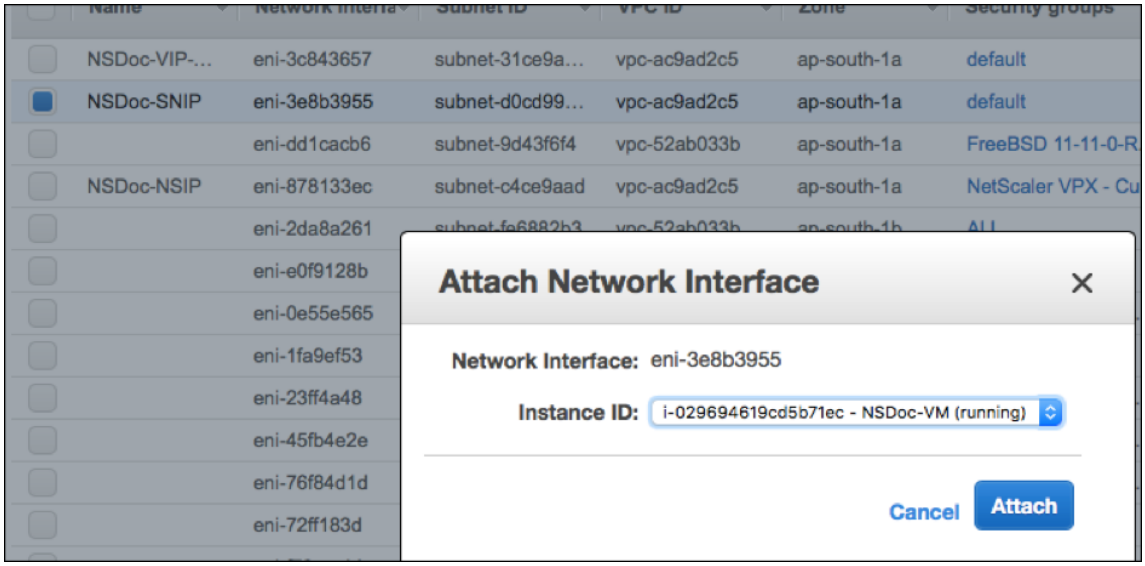
1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Interfaces réseau.
3. Choisissez Create Network Interface.
4. Dans Description, entrez un nom descriptif.
5. Pour Sous-réseau, sélectionnez le sous-réseau que vous avez créé précédemment pour le VIP.
6. Pour Private IP, conservez l'option par défaut.
7. Pour les groupes de sécurité, sélectionnez le groupe.
8. Cliquez sur **Yes, Create**.



9. Une fois l'interface réseau créée, attribuez-lui un nom.
10. Répétez les étapes pour créer une interface réseau pour le trafic côté serveur.

Connectez les interfaces réseau :

1. Dans le volet de navigation, choisissez Interfaces réseau.
2. Sélectionnez l'interface réseau et choisissez Attacher.
3. Dans la boîte de dialogue Attacher une interface réseau, sélectionnez l'instance et choisissez Attacher.



Étape 6 : attachez une adresse IP élastique au NSIP.

1. Depuis la console de gestion AWS, accédez à **RÉSEAU ET SÉCURITÉ > Elastic IPs**.
2. Vérifiez s'il existe un EIP gratuit à joindre. Si ce n'est pas le cas, cliquez sur **Attribuer une nouvelle adresse**.
3. Sélectionnez l'adresse IP nouvellement attribuée et choisissez **Actions > Adresse associée**.
4. Cliquez sur le bouton radio de **l'interface réseau** .

5. Dans la liste déroulante Interface réseau, sélectionnez la carte réseau de gestion.
6. Dans le menu déroulant **Private IP**, sélectionnez l'adresse IP générée par AWS.
7. Cochez la case **Réassociation** .
8. Cliquez sur **Associer**.

Accédez à l'instance VPX :

Après avoir configuré une instance NetScaler VPX autonome avec trois cartes réseau, connectez-vous à l'instance VPX pour terminer la configuration côté NetScaler. Utilisation des options suivantes :

- GUI : saisissez l'adresse IP publique de la carte réseau de gestion dans le navigateur. Ouvrez une session en utilisant `nsroot` comme nom d'utilisateur et l'ID d'instance (i-0c1ffe1d987817522) comme mot de passe.

> Remarque
>
> Lors de votre première connexion, vous êtes invité à modifier le mot de passe pour des raisons de sécurité. Après avoir modifié le mot de passe, vous devez enregistrer la configuration. Si la configuration n'est pas enregistrée et que l'instance redémarre, vous devez vous connecter avec le mot de passe par défaut. Modifiez à nouveau le mot de passe à l'invite et enregistrez la configuration.

- SSH : ouvrez un client SSH et tapez :

```
ssh -i \<location of your private key\> ns root@\<public DNS of the instance \>
```

Pour trouver le DNS public, cliquez sur l'instance, puis sur **Connect**.

Informations connexes :

- Pour configurer les adresses IP appartenant à NetScaler (NSIP, VIP et SNIP), consultez la section Configuration des adresses IP appartenant à NetScaler.
- Vous avez configuré une version BYOL de l'appliance NetScaler VPX. Pour plus d'informations, consultez le Guide des licences VPX à l'adresse http://support.citrix.com/article/CTX122426

Télécharger une licence NetScaler VPX

July 31, 2023

Après le lancement de l'instance sous licence NetScaler VPX-Customer depuis la place de marché AWS, une licence est requise. Pour plus d'informations sur les licences VPX, reportez-vous à la section Présentation des licences.

Vous devez :

1. Utilisez le portail de licences sur le site Web Citrix pour générer une licence valide.
2. Télécharger la licence sur l'instance.

S'il s'agit d'une instance de marketplace **payante**, vous n'avez pas besoin d'installer une licence. Le jeu de fonctionnalités et les performances corrects s'activent automatiquement.

Si vous utilisez une instance NetScaler VPX dont le numéro de modèle est supérieur à VPX 5000, le débit réseau peut ne pas être le même que celui spécifié par la licence de l'instance. Toutefois, d'autres fonctionnalités, telles que le débit SSL et les transactions SSL par seconde, peuvent s'améliorer.

La bande passante réseau de 5 Gbit/s est observée dans le type d' `c4.8xlarge` instance.

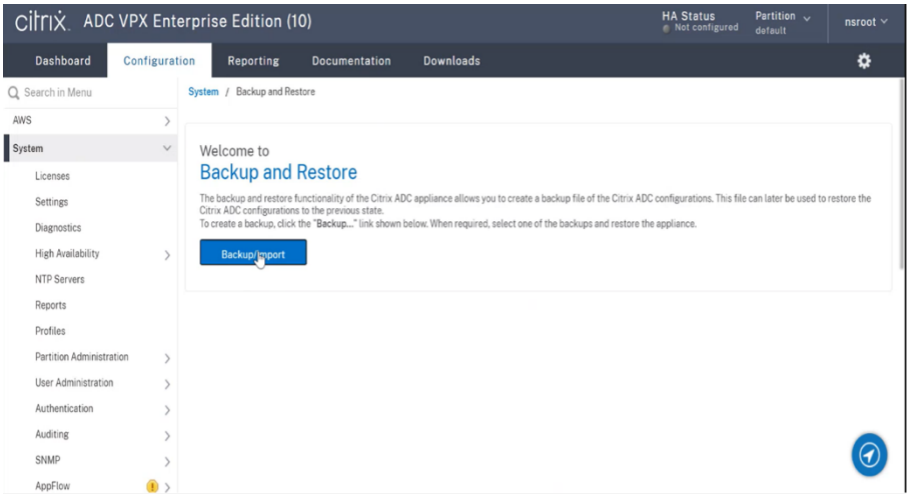
Comment migrer l'abonnement AWS vers BYOL

Cette section décrit la procédure de migration de l'abonnement AWS vers Bring your own license (BYOL), et inversement.

Procédez comme suit pour migrer un abonnement AWS vers BYOL :

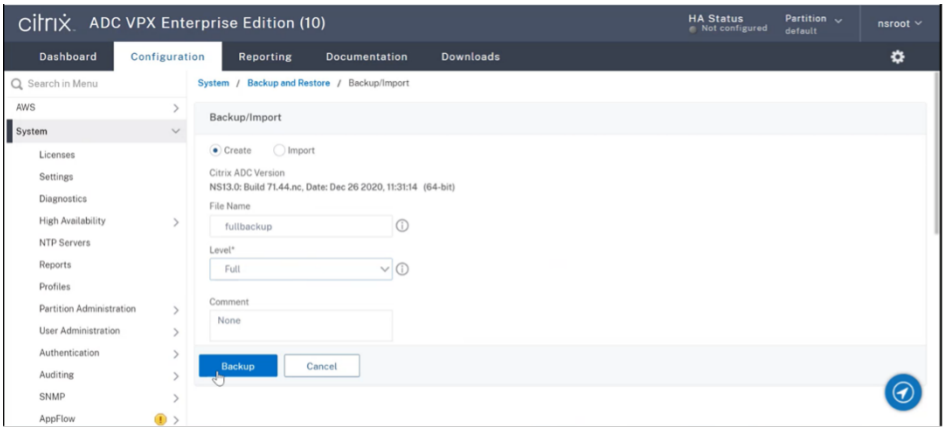
> Remarque
>
> Les **étapes 2** et **3** sont effectuées sur l'instance NetScaler VPX, et toutes les autres étapes sont effectuées sur le portail AWS.

1. Créez une instance BYOL EC2 à l'aide de NetScaler VPX - Customer Licensed dans la même zone de disponibilité que l'ancienne instance EC2 qui possède le même groupe de sécurité, le même rôle IAM et le même sous-réseau. La nouvelle instance EC2 ne doit avoir qu'une seule interface ENI.
2. Pour sauvegarder les données de l'ancienne instance EC2 à l'aide de l'interface graphique NetScaler, procédez comme suit.
   a) Accédez à **Système > Sauvegarde et restauration**.
   b) Dans la page **Bienvenue**, cliquez sur **Sauvegarde/Importation** pour démarrer le processus.

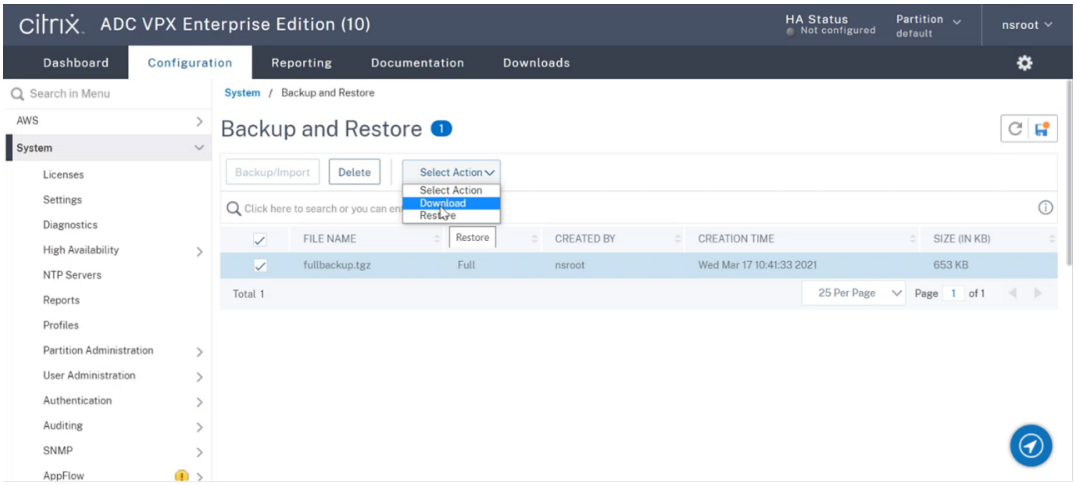


c) Dans la page **Sauvegarde/Importation**, renseignez les informations suivantes :

- **Nom** : nom du fichier de sauvegarde.
- **Niveau** : sélectionnez le niveau de sauvegarde **complet**.
- **Commentaire** : fournissez une brève description de la sauvegarde.



d) Cliquez sur **Sauvegarde**. Une fois la sauvegarde terminée, vous pouvez sélectionner le fichier et le télécharger sur votre machine locale.

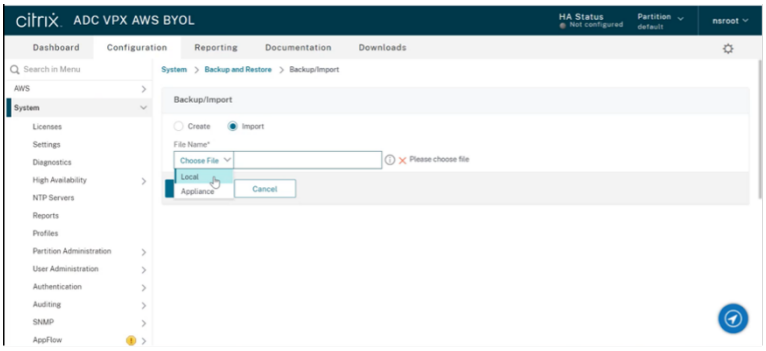


3. Pour restaurer les données sur la nouvelle instance EC2 à l'aide de l'interface graphique NetScaler, procédez comme suit :

   a) Accédez à **Système > Sauvegarde et restauration**.

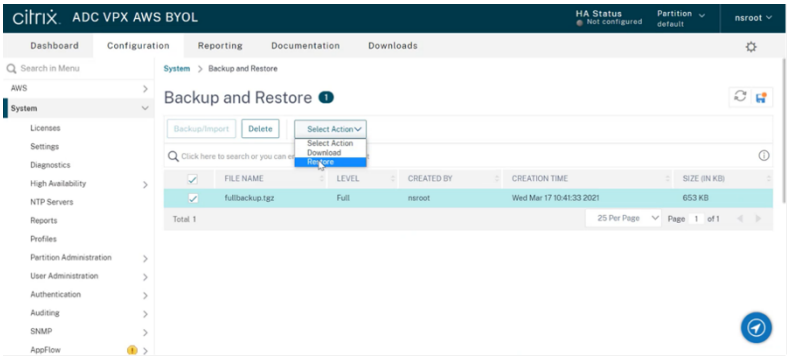
   b) Cliquez sur **Sauvegarde/Importer** pour démarrer le processus.

   c) Sélectionnez l'option **Importer** et téléchargez le fichier de sauvegarde.

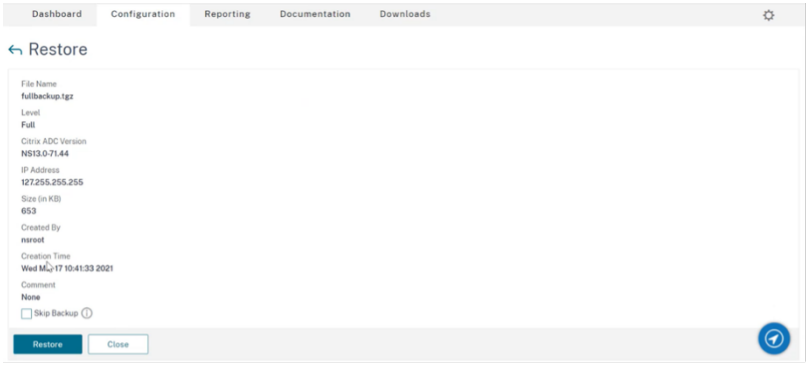


   d) Sélectionnez le fichier.

   e) **Dans le menu déroulant Sélectionner une action**, sélectionnez **Restaurer**.



   f) Sur la page **Restaurer**, vérifiez les détails du fichier, puis cliquez sur **Restaurer**.



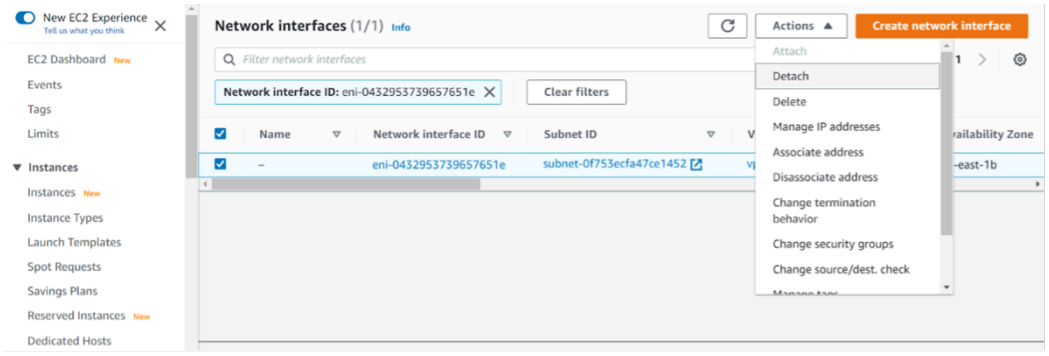
g) Après la restauration, redémarrez l'instance EC2.

4. Déplacez toutes les interfaces (à l'exception de l'interface de gestion à laquelle l'adresse NSIP est liée) de l'ancienne instance EC2 vers la nouvelle instance EC2. Pour déplacer une interface réseau d'une instance EC2 à une autre, procédez comme suit :

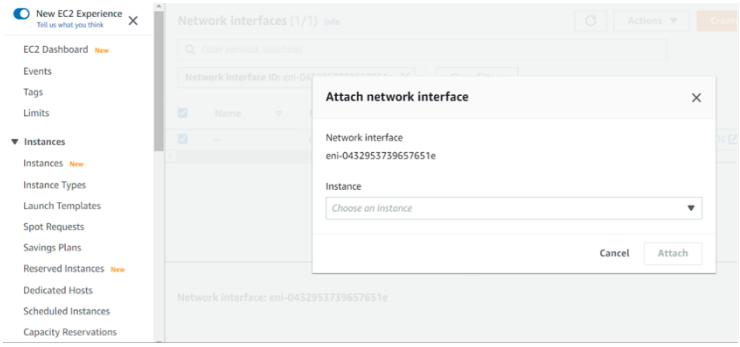
   a) Dans le **portail AWS**, arrêtez les anciennes et nouvelles instances EC2.

   b) Accédez à **Interfaces réseau**et sélectionnez l'interface réseau attachée à l'ancienne instance EC2.

   c) Détachez l'instance EC2 en cliquant sur **Actions > Détacher**.



   d) Connectez l'interface réseau à la nouvelle instance EC2 en cliquant sur **Actions > Attacher**. Entrez le nom de l'instance EC2 auquel l'interface réseau doit être connectée.



   e) Faites les **étapes 1** à **4** pour toutes les autres interfaces connectées. Assurez-vous de suivre la séquence et de conserver l'ordre de l'interface. C'est-à-dire, détachez d'abord l'interface

2 et attachez-la, puis détachez l'interface 3 et attachez-la, etc.

5. Vous ne pouvez pas détacher l'interface de gestion d'une ancienne instance EC2. Déplacez donc toutes les adresses IP secondaires (le cas échéant) de l'interface de gestion (interface réseau principale) de l'ancienne instance EC2 vers la nouvelle instance EC2. Pour déplacer une adresse IP d'une interface à une autre, procédez comme suit :

   a) Dans le **portail AWS**, assurez-vous que les anciennes et nouvelles instances EC2 sont à l'état **Stop** .

   b) Accédez à **Interfaces réseau**et sélectionnez l'interface réseau de gestion attachée à l'ancienne instance EC2.

   c) Cliquez sur **Actions > Gérer l'adresse IP**et notez toutes les adresses IP secondaires attribuées (le cas échéant).

   d) Accédez à l'interface réseau de gestion ou à l'interface principale de la nouvelle instance EC2.

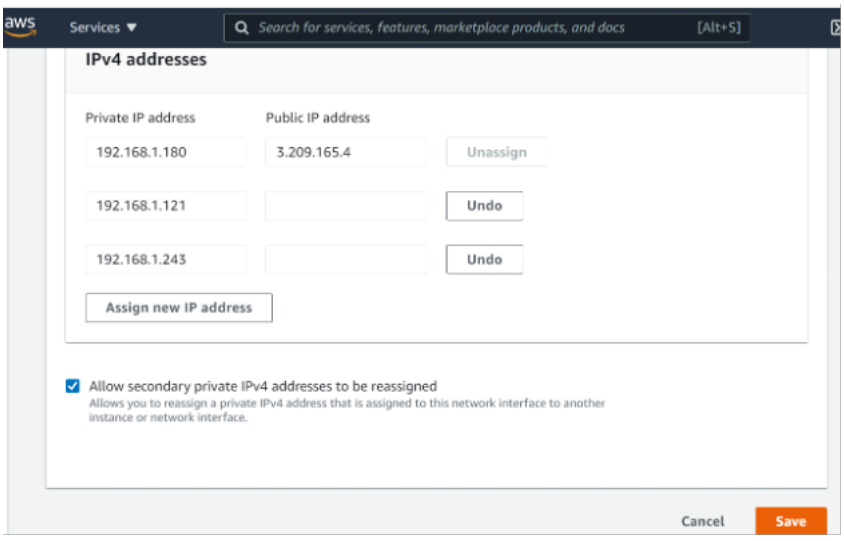
   e) Cliquez sur **Actions > Gérer les adresses IP**.

   f) Sous **Adresses IPv4**, cliquez sur **Attribuer une nouvelle adresse IP**.

   g) Saisissez les adresses IP indiquées à l' **étape 3**.

   h) Activez la case à cocher **Autoriser la réaffectation des adresses IP privées secondaires** .

   i) Cliquez sur **Enregistrer**.



6. Démarrez la nouvelle instance EC2 et vérifiez la configuration. Une fois que toute la configuration est déplacée, vous pouvez supprimer ou conserver l'ancienne instance EC2 selon vos besoins.

7. Si une adresse EIP est attachée à l'adresse NSIP de l'ancienne instance EC2, déplacez l'adresse NSIP de l'ancienne instance vers la nouvelle adresse NSIP de l'instance.
8. Si vous souhaitez revenir à l'ancienne instance, suivez les mêmes étapes de la manière opposée entre l'ancienne et la nouvelle instance.
9. Une fois que vous passez d'une instance d'abonnement à une instance BYOL, une licence est requise. Pour installer une licence, procédez comme suit :
    - Utilisez le portail de licences sur le site Web Citrix pour générer une licence valide.
    - Télécharger la licence sur l'instance. Pour plus d'informations, voir VPX ADC - Installer une nouvelle licence.

> Remarque
>
> Lorsque vous déplacez une instance BYOL vers une instance d'abonnement (instance de marché payante), vous n'avez pas besoin d'installer la licence. Le jeu de fonctionnalités et les performances corrects sont automatiquement activés.

Limitations

L'interface de gestion ne peut pas être déplacée vers la nouvelle instance EC2. Citrix vous recommande donc de configurer manuellement l'interface de gestion. Pour plus d'informations, reportez-vous à l' **étape 5** de la procédure précédente. Une nouvelle instance EC2 est créée avec le réplica exact de l'ancienne instance EC2, mais seule l'adresse NSIP possède une nouvelle adresse IP.

Serveurs d'équilibrage de charge dans différentes zones de disponibilité

May 5, 2023

Une instance VPX peut être utilisée pour équilibrer la charge des serveurs s'exécutant dans la même zone de disponibilité ou dans :

- Une zone de disponibilité (AZ) différente dans le même AWS VPC
- Une région AWS différente
- AWS EC2 dans un VPC

Pour permettre à une instance VPX d'équilibrer la charge des serveurs s'exécutant en dehors du VPC AWS dans lequel se trouve l'instance
VPX, configurez l'instance pour qu'elle utilise des EIP pour acheminer le trafic via la passerelle Internet, comme suit :

1. Configurez un SNIP sur l'instance NetScaler VPX à l'aide de la CLI NetScaler ou de l'interface graphique.

2. Permettez au trafic d'être acheminé hors de la zone de disponibilité en créant un sous-réseau public pour le trafic côté serveur.
3. Ajoutez une route de Gateway Internet à la table de routage, à l'aide de la console AWS GUI.
4. Associez la table de routage que vous avez mise à jour au sous-réseau côté serveur.
5. Associez un EIP à l'adresse IP privée côté serveur mappée à une adresse SNIP NetScaler.

Comment fonctionne la haute disponibilité sur AWS

May 5, 2023

Vous pouvez configurer deux instances NetScaler VPX sur AWS sous la forme d'une paire active-passive à haute disponibilité (HA). Lorsque vous configurez une instance en tant que nœud principal et l'autre en tant que nœud secondaire, le nœud principal accepte les connexions et gère les serveurs. Le nœud secondaire surveille le principal. Si, pour une raison quelconque, le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Dans AWS, les types de déploiement suivants sont pris en charge pour les instances VPX :

- Haute disponibilité dans la même zone
- Haute disponibilité dans différentes zones

> **Remarque**
>
> Pour que la haute disponibilité fonctionne, assurez-vous que les deux instances NetScaler VPX sont associées à des rôles IAM et que l'adresse IP Elastic (EIP) est attribuée au NSIP. Vous n'avez pas besoin d'attribuer un EIP au NSIP si le NSIP peut accéder à Internet via l'instance NAT.

Haute disponibilité dans les mêmes zones

Dans un déploiement haute disponibilité dans les mêmes zones, les deux instances VPX doivent avoir des configurations réseau similaires.

Suivez ces deux règles :

Règle 1. Toute carte réseau d'une instance VPX doit se trouver dans le même sous-réseau que la carte réseau correspondante de l'autre VPX. Les deux instances doivent avoir :

- Interface de gestion sur le même sous-réseau (appelé sous-réseau de gestion)
- Interface client sur le même sous-réseau (appelé sous-réseau client)
- Interface serveur sur le même sous-réseau (appelé sous-réseau du serveur)

Article 2. La séquence de carte réseau de gestion, de carte réseau client et de carte réseau serveur sur les deux instances doit être la même.
Par exemple, le scénario suivant n'est pas pris en charge.

Instance VPX 1

Carte réseau 0 :
carte réseau de gestion 1 :
carte réseau client 2 : serveur

Instance VPX 2

NIC 0 : gestion

NIC 1 : serveur

Carte réseau 2 : client

Dans ce scénario, la carte réseau 1 de l'instance 1 est dans le sous-réseau client tandis que la carte réseau 1 de l'instance 2 est dans le sous-réseau du serveur. Pour que HA fonctionne, la carte réseau 1 des deux instances doit être soit dans le sous-réseau client, soit dans le sous-réseau du serveur.

À partir de 13.0 41.xx, la haute disponibilité peut être obtenue en migrant des adresses IP privées secondaires attachées aux cartes réseau (cartes réseau client et côté serveur) du nœud HA principal vers le nœud HA secondaire après le basculement. Dans ce déploiement :

- Les deux instances VPX ont le même nombre de cartes réseau et de mappage de sous-réseau selon l'énumération de carte réseau.
- Chaque carte réseau VPX possède une adresse IP privée supplémentaire, à l'exception de la première carte réseau, qui correspond à l'adresse IP de gestion. L'adresse IP privée supplémentaire apparaît comme l'adresse IP privée principale dans la console Web AWS. Dans notre document, nous appelons cette adresse IP supplémentaire l'adresse IP fictive).
- Les adresses IP fictives ne doivent pas être configurées sur l'instance NetScaler en tant que VIP et SNIP.
- D'autres adresses IP privées secondaires doivent être créées, selon les besoins, et configurées en tant que VIP et SNIP.
- Lors du basculement, le nouveau nœud principal recherche les SNIP et les VIP configurés et les déplace des cartes réseau attachées à la précédente principale vers les cartes réseau correspondantes sur la nouvelle interface principale.
- Les instances NetScaler nécessitent des autorisations IAM pour que HA fonctionne. Ajoutez les privilèges IAM suivants à la stratégie IAM ajoutée à chaque instance.

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeNetworkInterfaces"
"ec2:AssignPrivateIpAddresses"
```


> Remarque : n'`unassignPrivateIpAddress` est pas obligatoire.

Cette méthode est plus rapide que l'ancienne méthode. Dans l'ancienne méthode, HA dépend de la migration des interfaces réseau élastiques AWS du nœud principal vers le nœud secondaire.

Pour une méthode héritée, les stratégies suivantes sont requises :

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeAddresses"
"ec2:AssociateAddress"
"ec2:DisassociateAddress"
```

Pour plus d'informations, voir Déployer une paire haute disponibilité sur AWS.

Haute disponibilité dans différentes zones

Vous pouvez configurer deux instances NetScaler VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes, sous la forme d'une paire active-passive à haute disponibilité en mode Independent Network Configuration (INC). Lors du basculement, l'EIP (Elastic IP) du VIP de l'instance principale migre vers le secondaire, qui prend le relais en tant que nouveau principal. Dans le processus de basculement, l'API AWS :

- Vérifie les serveurs virtuels qui y sont `IPSets` connectés.
- Recherche l'adresse IP qui a une adresse IP publique associée, à partir des deux adresses IP sur lesquelles le serveur virtuel écoute. L'un qui est directement connecté au serveur virtuel et l'autre qui est connecté via l'ensemble d'adresses IP.
- Réassocie l'adresse IP publique (EIP) à l'adresse IP privée appartenant au nouveau VIP principal.

Pour les HA dans différentes zones, les stratégies suivantes sont requises :

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeAddresses"
"ec2:AssociateAddress"
"ec2:DisassociateAddress"
```

Pour plus d'informations, consultez la section Haute disponibilité dans les zones de disponibilité AWS.

Avant de commencer votre déploiement

Avant de commencer un déploiement HA sur AWS, lisez le document suivant :

- Composants requis
- Limitations et directives d'utilisation

- Déployer une instance NetScaler VPX sur AWS
- Haute disponibilité

Dépannage

Pour résoudre toute défaillance lors d'un basculement en mode HA d'une instance NetScaler VPX sur le cloud AWS, consultez le `cloud-ha-daemon.log` fichier stocké à cet emplacement. `/var/log/`

Déployer une paire HA VPX dans la même zone de disponibilité AWS

May 5, 2023

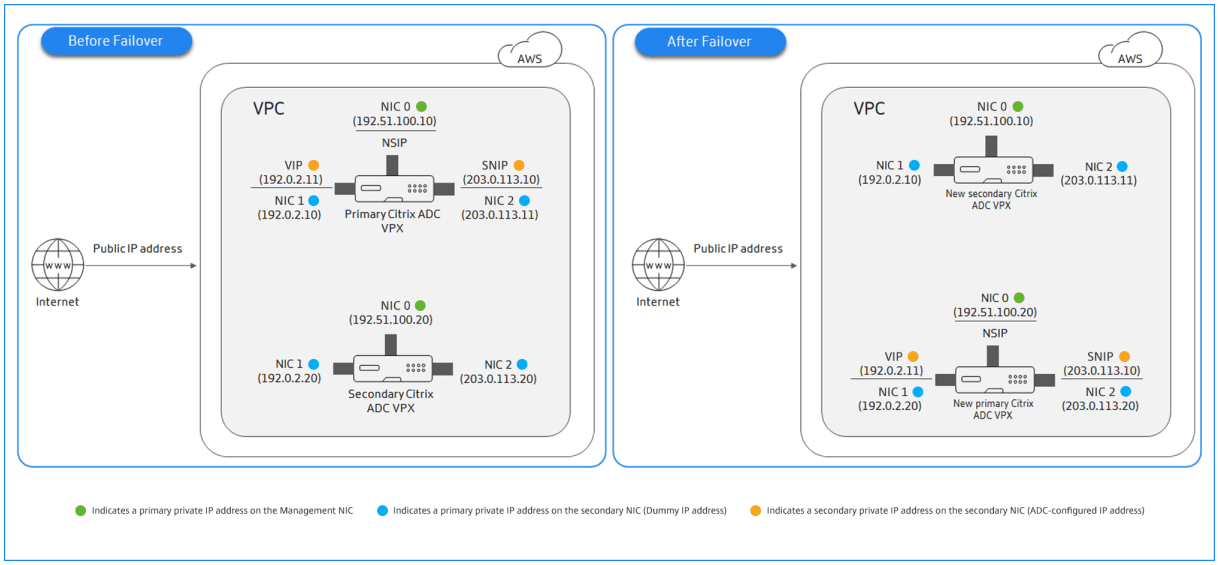
> **Remarque :**
>
> À partir de la version 13.1 build 27.x de NetScaler, la paire VPX HA située dans la même zone de disponibilité AWS prend en charge les adresses IPv6.

Vous pouvez configurer deux instances NetScaler VPX sur AWS en tant que paire HA, dans la même zone AWS où les deux instances VPX se trouvent sur le même sous-réseau. La haute disponibilité est obtenue en migrant les adresses IP privées secondaires attachées aux cartes réseau (cartes réseau côté client et côté serveur) du nœud HA principal vers le nœud HA secondaire après basculement. Toutes les adresses IP Elastic associées aux adresses IP privées secondaires sont également migrées.

La paire NetScaler VPX HA prend en charge les adresses IPv4 et IPv6 dans la même zone de disponibilité AWS.

L'illustration suivante illustre un scénario de basculement HA par migration d'adresses IP privées secondaires.

Figure 1. Une paire NetScaler VPX HA sur AWS, à l'aide d'une migration IP privée



Avant de commencer votre document, lisez les documents suivants :

- Composants requis
- Limitations et directives d'utilisation
- Déployer une instance NetScaler VPX sur AWS
- Haute disponibilité

Comment déployer une paire VPX HA dans la même zone

Voici le résumé des étapes pour déployer une paire VPX HA dans la même zone :

1. Créez deux instances VPX sur AWS, chacune avec trois cartes réseau
2. Affectez l'adresse IP privée secondaire AWS à VIP et SNIP du nœud principal
3. Configurez VIP et SNIP sur le nœud principal à l'aide des adresses IP privées secondaires AWS
4. Configurer la haute disponibilité sur les deux nœuds

Étape 1. Créez deux instances VPX (nœuds primaires et secondaires) à l'aide du même VPC, chacune avec trois cartes réseau (Ethernet 0, Ethernet 1, Ethernet 2)

Suivez les étapes décrites dans Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS.

Étape 2. Sur le nœud principal, attribuez des adresses IP privées pour Ethernet 1 (IP client ou VIP) et Ethernet 2 (IP du serveur principal ou SNIP)

La console AWS attribue automatiquement des adresses IP privées principales aux cartes réseau configurées. Affectez davantage d'adresses IP privées à VIP et SNIP, appelées adresses IP privées secondaires.

Pour attribuer une adresse IP privée à une interface réseau, procédez comme suit :

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez **Network Interfaces**, puis sélectionnez l'interface réseau connectée à l'instance.
3. Choisissez **Actions > Gérer les adresses IP**.
4. Sélectionnez Adresses **IPv4 ou AdressesIPv6 en** fonction de vos besoins.
5. Pour les adresses IPv4 :
   a) Choisissez **Assign new IP**.
   b) Entrez une adresse IPv4 spécifique comprise dans la plage de sous-réseau de l'instance, ou laissez le champ vide pour permettre à Amazon de sélectionner une adresse IP pour vous.
   c) (Facultatif) Choisissez **Autoriser la réaffectation** pour autoriser la réaffectation de l'adresse IP privée secondaire si elle est déjà attribuée à une autre interface réseau.
6. Pour les adresses IPv6 :
   a) Choisissez **Assign new IP**.
   b) Entrez une adresse IPv6 spécifique comprise dans la plage de sous-réseaux de l'instance, ou laissez le champ vide pour permettre à Amazon de sélectionner une adresse IP pour vous.
   c) (Facultatif) Choisissez **Autoriser la réaffectation** pour autoriser la réaffectation de l'adresse IP privée principale ou secondaire si elle est déjà attribuée à une autre interface réseau.
7. Choisissez **Oui > Mettre à jour**.

Sous la **description de l'instance**, les adresses IP privées attribuées apparaissent.

> **Remarque :**
>
> Dans un déploiement de paires HA IPv4, vous pouvez attribuer uniquement les adresses IPv4 secondaires sur l'interface et les utiliser comme adresses VIP et SNIP. Mais dans un déploiement de paires HA IPv6, vous pouvez attribuer les adresses IPv6 principales ou IPv6 secondaires sur l'interface et les utiliser comme adresses VIP et SNIP.

Étape 3. Configurez VIP et SNIP sur le nœud principal, à l'aide d'adresses IP privées secondaires

Accédez au nœud principal via SSH. Ouvrez un client SSH et tapez :

```
ssh -i <location of your private key> nsroot@<public DNS of the
    instance>
<!--NeedCopy-->
```

Ensuite, configurez VIP et SNIP.

Pour les VIP, tapez :

```
1 add ns ip <IPAddress> <netmask> -type <type>
2 <!--NeedCopy-->
```

Pour SNIP, tapez :

```
1 add ns ip <IPAddress> <netmask> -type SNIP
2 <!--NeedCopy-->
```

Tapez `save config` pour enregistrer.

Pour voir les adresses IP configurées, tapez la commande suivante :

```
1 show ns ip
2 <!--NeedCopy-->
```

Pour plus d'informations, consultez les rubriques suivantes :

- Configuration et gestion des adresses IP virtuelles (VIP)
- Configuration de l'adresse NSIP

Étape 4 : Configurer la haute disponibilité sur les deux instances

Sur le nœud principal, ouvrez un client Shell et tapez la commande suivante :

```
1 add ha node <id> <private IP address of the management NIC of the
     secondary node>
2 <!--NeedCopy-->
```

Sur le nœud secondaire, tapez la commande suivante :

```
1 add ha node <id> < private IP address of the management NIC of the
     primary node >
2 <!--NeedCopy-->
```

Tapez `save config` pour enregistrer la configuration.

Pour voir les nœuds HA configurés, tapez `show ha node`.

Lors du basculement, les adresses IP privées secondaires configurées en tant que VIP et SNIP sur le nœud principal précédent sont migrées vers le nouveau nœud principal.

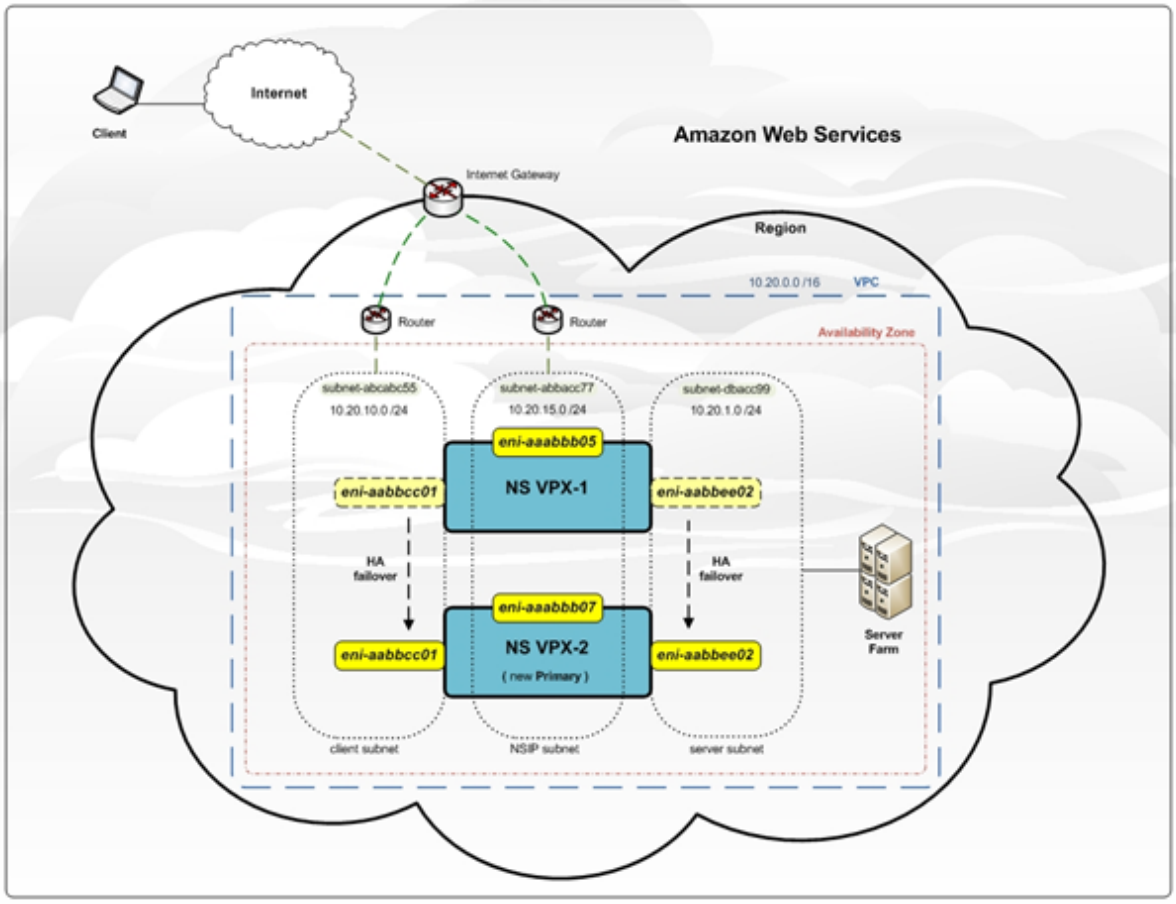
Pour forcer un basculement sur incident sur un nœud, tapez `force HA`Basculement.

Méthode héritée pour déployer une paire VPX HA

Avant la version 13.0 41.x, la haute disponibilité au sein de la même zone était réalisée via la migration AWS Elastic Network Interface (ENI). Cependant, cette méthode est lentement déconseillée.

La figure suivante montre un exemple d'architecture de déploiement HA pour les instances NetScaler VPX sur AWS.

Figure 1. Une paire NetScaler VPX HA sur AWS, à l'aide de la migration ENI



Vous pouvez déployer deux instances VPX sur AWS en tant que paire HA à l'aide de l'une des options suivantes :

- Créez les instances avec le rôle IAM manuellement à l'aide d'AWS Management Console, puis configurez HA dessus.
- Ou automatisez le déploiement haute disponibilité à l'aide du modèle Citrix CloudFormation.

Le modèle CloudFormation réduit considérablement le nombre d'étapes nécessaires à la création d'une paire HA, et il crée automatiquement un rôle IAM. Cette section explique comment déployer une paire NetScaler VPX HA (actif-passif) à l'aide du modèle Citrix CloudFormation.

Gardez les points suivants à l'esprit lorsque vous déployez deux instances NetScaler VPX en tant que

paire HA.

Points à noter

- HA sur AWS exige que le nœud principal dispose d'au moins deux ENI (l'un pour la gestion et l'autre pour le trafic de données) et que le nœud secondaire dispose d'un ENI de gestion. Toutefois, pour des raisons de sécurité, créez trois ENI sur le nœud principal, car cette configuration vous permet de séparer le réseau privé et public (recommandé).
- Le nœud secondaire a toujours une interface ENI (pour la gestion) et le nœud principal peut avoir jusqu'à quatre ENI.
- Les adresses NSIP de chaque instance VPX d'une paire haute disponibilité doivent être configurées sur l'ENI par défaut de l'instance.
- Amazon n'autorise aucun paquet de diffusion/multidiffusion dans AWS. Par conséquent, dans une configuration HA, les ENIS de plan de données sont migrés de l'instance VPX principale vers l'instance VPX secondaire lorsque l'instance VPX principale échoue.
- Étant donné que l'ENI par défaut (gestion) ne peut pas être déplacé vers une autre instance VPX, n'utilisez pas l'ENI par défaut pour le trafic client et serveur (trafic de plan de données).
- Le message de réussite 0 d'AWSCONFIG IOCTL NSAPI_HOTPLUG_INTF dans le fichier /var/log/ns.log indique que les deux ENI de données se sont correctement attachés à l'instance secondaire (la nouvelle instance principale).
- Le basculement peut prendre jusqu'à 20 secondes en raison du mécanisme ENI de détachement/attachement AWS.
- Lors du basculement, l'instance défaillante redémarre toujours.
- Les paquets de pulsation sont reçus uniquement sur l'interface de gestion.
- Le fichier de configuration des instances VPX principale et secondaire est synchronisé, y compris le mot de passe `nsroot`. Le`nsroot` mot de passe du nœud secondaire est défini sur celui du nœud principal après la synchronisation de la configuration HA.
- Pour avoir accès aux serveurs API AWS, soit l'instance VPX doit avoir une adresse IP publique attribuée, soit le routage doit être configuré correctement au niveau du sous-réseau VPC pointant vers la passerelle Internet du VPC.
- Les serveurs de noms et les serveurs DNS sont configurés au niveau du VPC à l'aide des options DHCP.
- Le modèle Citrix CloudFormation ne crée pas de configuration HA entre différentes zones de disponibilité.
- Le modèle Citrix CloudFormation ne crée pas de mode INC.
- Les messages de débogage AWS sont disponibles dans le fichier journal, /var/log/ns.log, sur l'instance VPX.

Déployer une paire haute disponibilité à l'aide du modèle Citrix CloudFormation

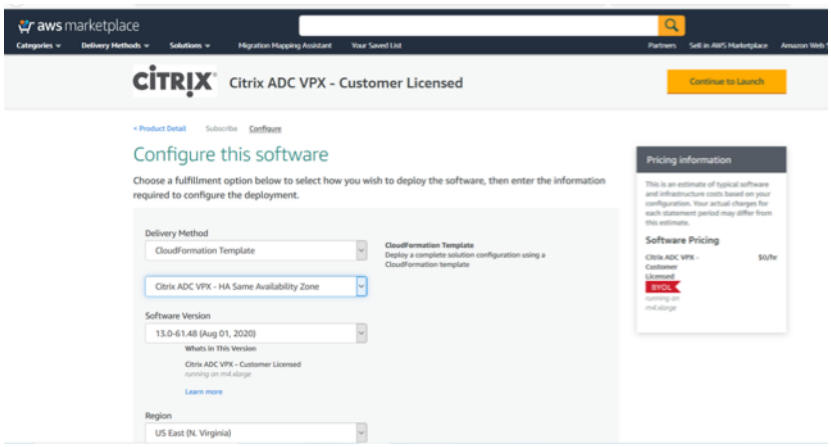
Avant de démarrer le modèle CloudFormation, assurez-vous de répondre aux exigences suivantes :

- Un VPC
- Trois sous-réseaux au sein du VPC
- Un groupe de sécurité avec des ports UDP 3003, TCP 3009—3010, HTTP et SSH ouverts
- Une paire de clés
- Créer une passerelle Internet
- Modifier les tables de routage pour les réseaux de clients et de gestion afin qu'ils pointent vers la passerelle Internet

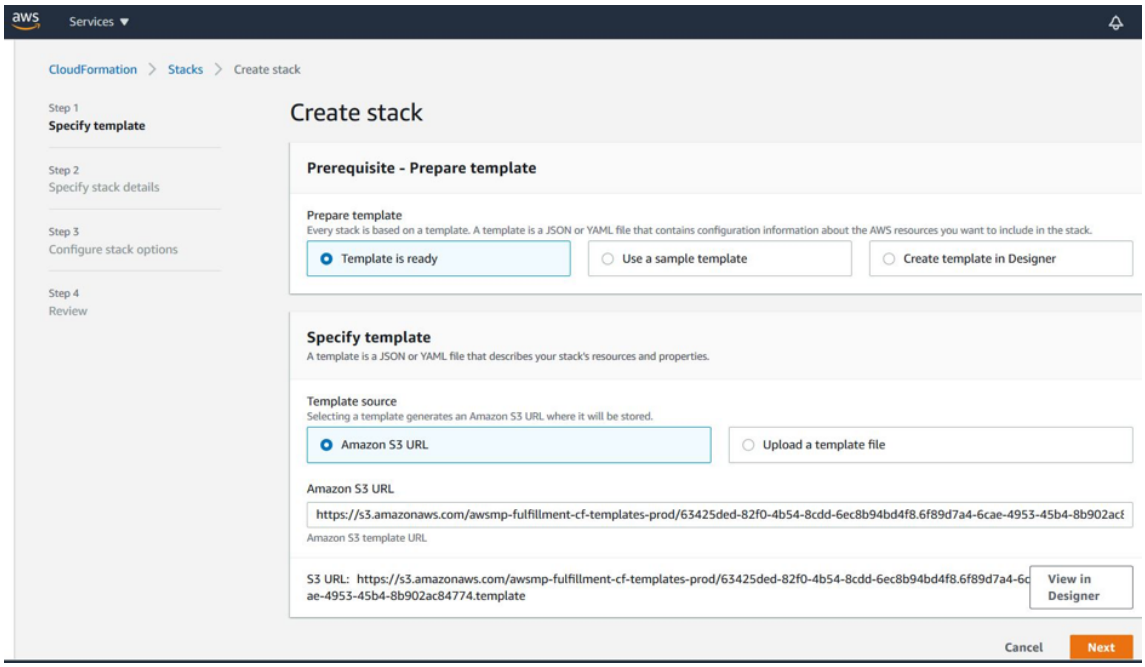
> **Remarque**
>
> Le modèle Citrix CloudFormation crée automatiquement un rôle IAM. Les rôles IAM existants n'apparaissent pas dans le modèle.

Pour lancer le modèle Citrix CloudFormation :

1. Connectez-vous à AWS Marketplace en utilisant vos informations d'identification AWS.
2. **Dans le champ de recherche, tapez**NetScaler VPX**pour rechercher l'AMI NetScaler, puis cliquez sur OK.**
3. Sur la page des résultats de recherche, cliquez sur l'offre NetScaler VPX souhaitée.
4. Cliquez sur l'onglet **Tarification**, pour accéder à **Informations sur la tarification** .
5. Sélectionnez la région et l' **option d'expédition** comme **NetScaler VPX — Customer Licensed**.
6. Cliquez sur **Continuer pour vous abonner**.
7. Consultez les détails sur la page **S'abonner** et cliquez sur **Continuer vers la configuration**.
8. Sélectionnez **Méthode de livraison** comme **modèle CloudFormation**.
9. Sélectionnez le modèle CloudFormation requis.
10. Sélectionnez **Version et**région**du logiciel**, puis cliquez sur **Continuer vers le lancement**.



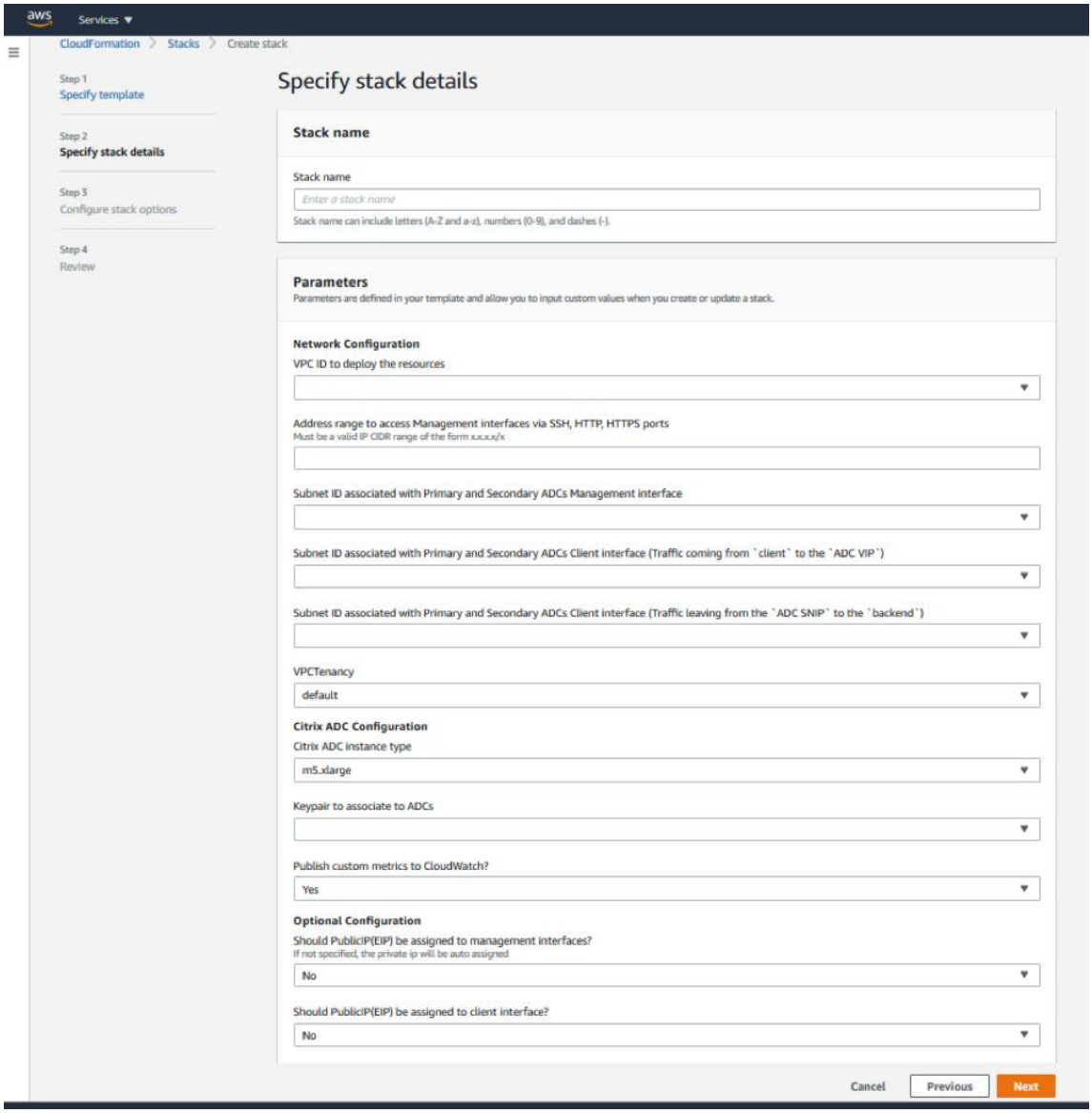
11. Sous **Choisir une action**, sélectionnez **Lancer CloudFormation**, puis cliquez sur **Lancer**. La page **Créer une pile** s'affiche.
12. Cliquez sur **Next**.



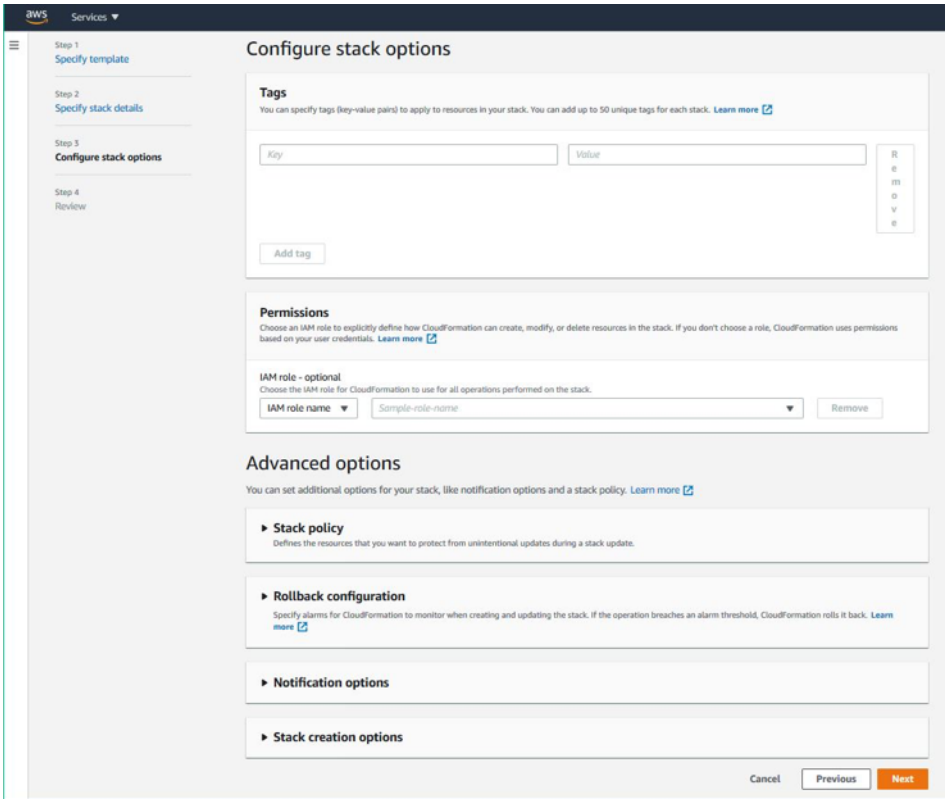
13. La page **Spécifier les détails de la pile** apparaît. Entrez les détails suivants.
    - Saisissez un **nom de pile**. Le nom doit contenir 25 caractères.
    - Sous **Configuration réseau**, effectuez les opérations suivantes :
      - Sélectionnez **Sous-réseau de gestion**, **Sous-réseau client**et **Sous-réseau de serveur**. Assurez-vous de sélectionner les sous-réseaux appropriés que vous avez créés dans le VPC que vous avez sélectionné sous ID du VPC.
      - Ajoutez l' **adresse IP de gestion principale**, l' **adresse IP de gestion secondaire**, l' **adresse IP client**et l' **adresse IP du serveur** Les adresses IP doivent appartenir aux mêmes sous-réseaux des sous-réseaux respectifs. Vous pouvez également laisser le modèle attribuer automatiquement les adresses IP.
      - Sélectionnez **par défaut** pour **VPCTenancy**.
    - Sous **Configuration de NetScaler**, effectuez les opérations suivantes :
      - Sélectionnez **m5.xlarge** pour le **type d'instance**.
      - Sélectionnez la paire de clés que vous avez déjà créée dans le menu de **Paire de clés**.
      - Par défaut, la fonction **Publier des mesures personnalisées sur CloudWatch ?** est définie sur **Oui**. Si vous souhaitez désactiver cette option, sélectionnez **Non**.
        Pour plus d'informations sur les mesures CloudWatch, voir Surveillance de vos instances à l'aide d'Amazon CloudWatch.
    - Sous **Configuration facultative**, procédez comme suit :
      - Par défaut, le champ **Should publicIP(EIP) be assigned to management interfaces?**

est défini sur **Non**.

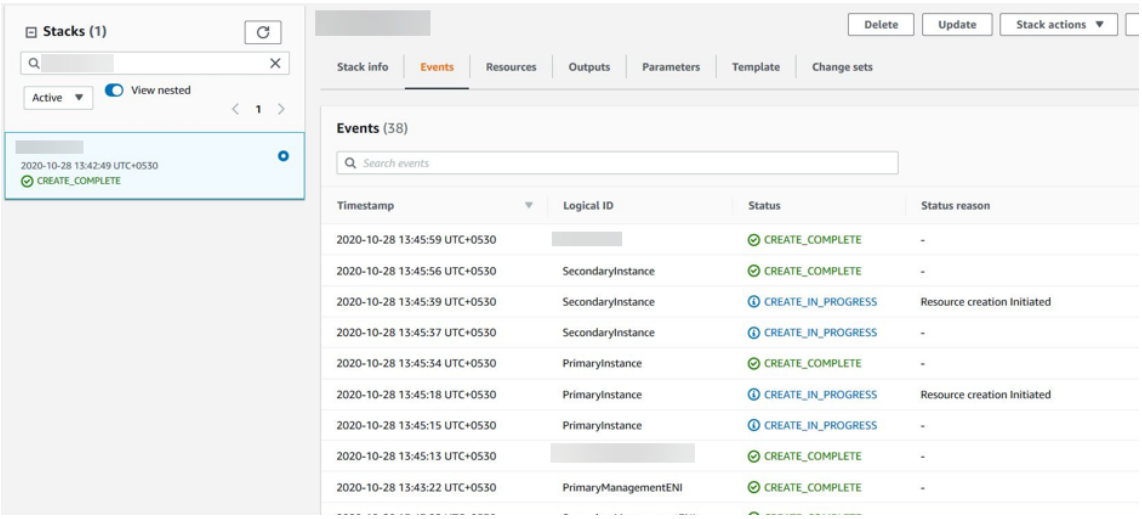
- Par défaut, la fonction **Should publicIP(EIP) be assigned to client interface?** est définie sur **Non**.



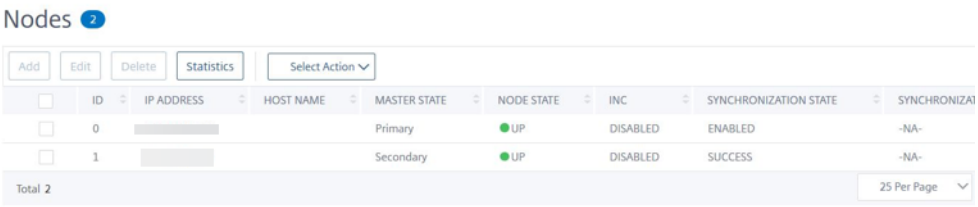
14. Cliquez sur **Next**.
15. La page **Configurer les options de la pile** apparaît. Il s'agit d'une page facultative.



16. Cliquez sur **Next**.
17. La page **Options** s'affiche. (Cette page est facultative.). Cliquez sur **Next**.
18. La page **Révision** s'affiche. Prenez quelques instants pour revoir les paramètres et apporter des modifications éventuelles, si nécessaire.
19. Sélectionnez la case **Je reconnais qu'AWS CloudFormation peut créer des ressources IAM.** , puis cliquez sur **Créer une pile**.
20. Le statut **CREATE-IN-PROGRESS** apparaît. Attendez que le statut soit **CREATE-COMPLETE**. Si le statut ne passe pas à **COMPLETE**, vérifiez la raison de l'échec dans l'onglet **Événements** et recréez l'instance avec les configurations appropriées.



21. Une fois qu'une ressource IAM est créée, accédez à **EC2 Management Console > Instances**. Vous trouvez deux instances VPX créées avec le rôle IAM. Les nœuds principaux et secondaires sont créés chacun avec trois adresses IP privées et trois interfaces réseau.
22. Ouvrez une session sur le nœud principal avec le nom d'utilisateur`nsroot` et l'ID d'instance comme mot de passe. Depuis l'interface graphique, accédez à **Système > Haute disponibilité > Nœuds**. Le NetScaler VPX est déjà configuré en paire HA par le modèle CloudFormation.
23. La paire NetScaler VPX HA s'affiche.



Surveillez vos instances à l'aide d'Amazon CloudWatch

Vous pouvez utiliser le service Amazon CloudWatch pour surveiller un ensemble de mesures NetScaler VPX, telles que l'utilisation du processeur et de la mémoire, ainsi que le débit. CloudWatch surveille les ressources et les applications qui s'exécutent sur AWS, en temps réel. Vous pouvez accéder au tableau de bord Amazon CloudWatch à l'aide de la console AWS Management. Pour plus d'informations, consultez Amazon CloudWatch.

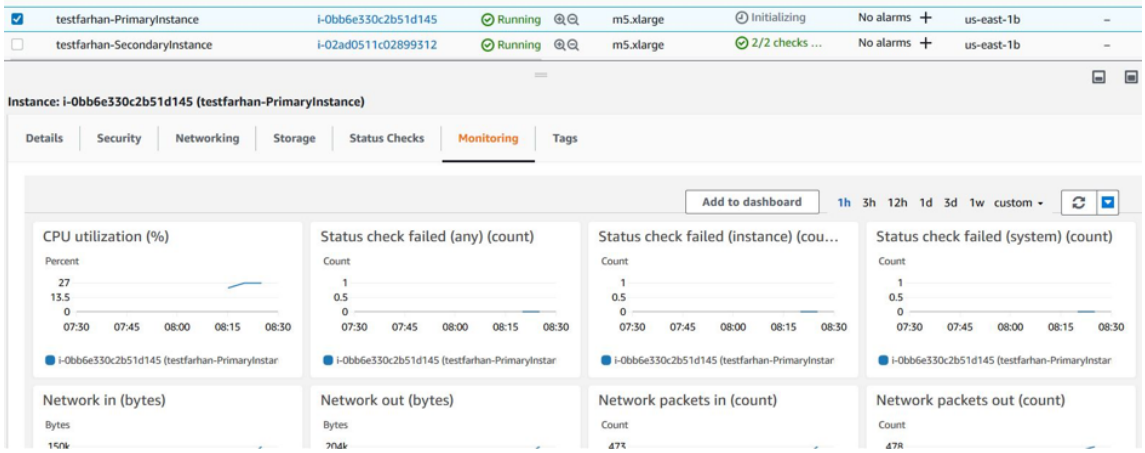
Points à noter

- Si vous déployez une instance NetScaler VPX sur AWS à l'aide de la console Web AWS, le service CloudWatch est activé par défaut.
- Si vous déployez une instance NetScaler VPX à l'aide du modèle Citrix CloudFormation, l'option par défaut est « Oui ». « Si vous souhaitez désactiver le service CloudWatch, sélectionnez « Non. »
- Les métriques sont disponibles pour le processeur (gestion et utilisation du processeur par paquets), la mémoire et le débit (entrant et sortant).

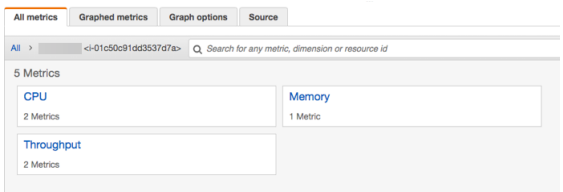
Comment afficher les métriques CloudWatch

Pour afficher les métriques CloudWatch pour votre instance, procédez comme suit :

1. Ouvrez une session sur **AWS Management Console > EC2 > Instances**.
2. Sélectionnez l'instance.
3. Cliquez sur **Surveillance**.
4. Cliquez sur **Afficher toutes les métriques CloudWatch**.

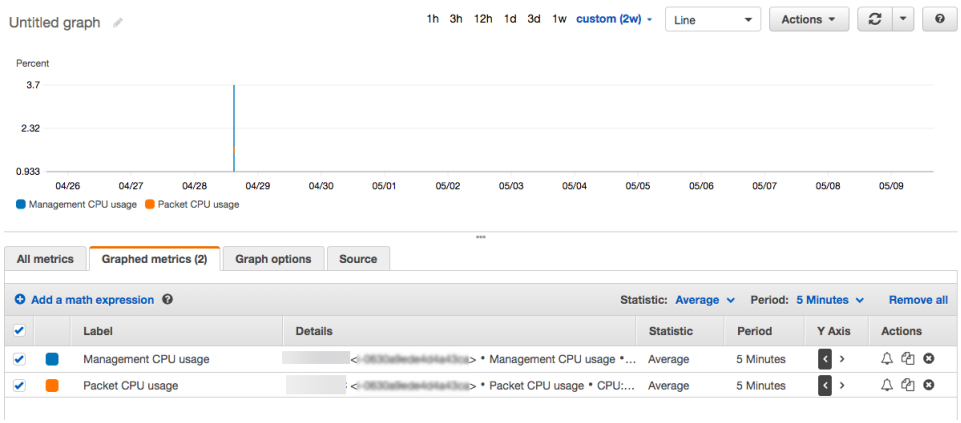


5. Sous Toutes les mesures, cliquez sur votre ID d'instance.



6. Cliquez sur les mesures que vous souhaitez afficher, définissez la durée (en minutes, heures, jours, semaines, mois).
7. Cliquez sur **Mesures graphiques** pour afficher les statistiques d'utilisation. Utilisez les **options de graphique** pour personnaliser votre graphique.

Chiffre. Mesures graphiques pour l'utilisation du processeur



Configuration de SR-IOV sur une configuration haute disponibilité

La prise en charge des interfaces SR-IOV dans une configuration haute disponibilité est disponible à partir de NetScaler version 12.0 57.19. Pour plus d'informations sur la configuration de SR-IOV, consultez Configuration des instances NetScaler VPXpour utiliser l'interface réseau SR-IOV.

Ressources connexes

Comment fonctionne la haute disponibilité sur AWS

Haute disponibilité dans différentes zones de disponibilité AWS

May 5, 2023

Vous pouvez configurer deux instances NetScaler VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes, sous la forme d'une paire active-passive à haute disponibilité en mode Independent Network Configuration (INC). Si, pour une raison quelconque, le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Pour plus d'informations sur INC, voir Configuration de nœuds haute disponibilité dans différents sous-réseaux.

Points à noter

- Lisez les documents suivants avant de commencer votre déploiement :
  - Terminologie AWS
  - Composants requis

  - Limitations et directives d'utilisation
- La paire haute disponibilité VPX peut résider dans la même zone de disponibilité dans un sous-réseau différent ou dans deux zones de disponibilité AWS différentes.
- Citrix vous recommande d'utiliser différents sous-réseaux pour la gestion (NSIP), le trafic client (VIP) et le serveur principal (SNIP).
- La haute disponibilité doit être définie en mode de configuration réseau indépendante (INC) pour qu'un basculement fonctionne.
- Le port 3003 des deux instances doit être ouvert pour le trafic UDP, car il est utilisé pour les pulsations cardiaques.
- Les sous-réseaux de gestion des deux nœuds doivent avoir accès à Internet ou au serveur API AWS via NAT interne afin que les autres API soient fonctionnelles.
- Le rôle IAM doit posséder l'autorisation E2 pour la migration IP publique ou Elastic IP (EIP) et les autorisations de table de routage EC2 pour la migration IP privée.

Vous pouvez déployer la haute disponibilité dans les zones de disponibilité AWS de la manière suivante :

- Utilisation d'adresses IP Elastic
- Utilisation d'adresses IP privées

Références supplémentaires

Pour plus d'informations sur NetScaler Application Delivery Management (ADM) pour AWS, voir Installer l'agent NetScalerADM sur AWS.

Déployer une paire VPX haute disponibilité avec des adresses IP élastiques dans différentes zones AWS

May 5, 2023

Vous pouvez configurer deux instances NetScaler VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes à l'aide d'adresses IP élastiques (EIP) en mode INC.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Pour plus d'informations sur INC, voir Configuration de nœuds haute disponibilité dans différents sous-réseaux.

Comment fonctionne la haute disponibilité avec des adresses EIP dans différentes zones AWS

Lors du basculement, l'EIP du VIP de l'instance principale migre vers l'instance secondaire, qui prend le relais en tant que nouveau serveur principal. Dans le processus de basculement, l'API AWS :

1. Vérifie les serveurs virtuels qui y sont `IPSets` connectés.
2. Recherche l'adresse IP qui a une adresse IP publique associée, à partir des deux adresses IP sur lesquelles le serveur virtuel écoute. L'un qui est directement connecté au serveur virtuel et celui qui est connecté via l'ensemble d'adresses IP.
3. Réassocie l'adresse IP publique (EIP) à l'adresse IP privée appartenant au nouveau VIP principal.

> **Remarque**
>
> Pour protéger votre réseau contre les attaques telles que le déni de service (DoS), lorsque vous utilisez un EIP, vous pouvez créer des groupes de sécurité dans AWS pour restreindre l'accès IP. Pour une haute disponibilité, vous pouvez passer d'EIP à une solution de déplacement IP privée selon vos déploiements.

Comment déployer une paire VPX haute disponibilité avec des adresses IP élastiques dans différentes zones AWS

Voici le résumé des étapes à suivre pour déployer une paire VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes.

1. Créez un cloud privé virtuel Amazon.
2. Déployez deux instances VPX dans deux zones de disponibilité différentes ou dans la même zone mais dans des sous-réseaux différents.
3. Configurer la haute disponibilité
   a) Configurez la haute disponibilité en mode INC dans les deux instances.
   b) Ajoutez un ensemble d'adresses IP dans les deux instances.
   c) Liez l'ensemble d'adresses IP dans les deux instances au VIP.
   d) Ajoutez un serveur virtuel dans l'instance principale.

Pour les étapes 1 et 2, utilisez la console AWS. Pour les étapes 3, utilisez l'interface graphique NetScaler VPX ou la CLI.

Étape 1. Créez un cloud privé virtuel (VPC) Amazon.

Étape 2. Déployez deux instances VPX dans deux zones de disponibilité différentes ou dans la même zone mais dans des sous-réseaux différents. Attachez un EIP au VIP du VPX principal.

Pour plus d'informations sur la création d'un VPC et le déploiement d'une instance VPX sur AWS, consultez [Déployer une instance autonome NetScaler VPX sur AWS et Scénario : instance autonome](/fr-fr/citrix-adc/current-release/deploying-vpx/deploy-aws)

Étape 3. Configurez la haute disponibilité. Vous pouvez utiliser l'interface de ligne de commande NetScaler VPX ou l'interface graphique pour configurer la haute disponibilité.

Configuration de la haute disponibilité à l'aide de la CLI

1. Configurez la haute disponibilité en mode INC dans les deux instances.

   Sur le nœud principal :

   ```
   add ha node 1 <sec_ip> -inc ENABLED
   ```

   Sur le nœud secondaire :

   ```
   add ha node 1 <prim_ip> -inc ENABLED
   ```

   <sec_ip> fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire

   <prim_ip> fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal

2. Ajoutez le jeu d'adresses IP dans les deux instances.

   Tapez la commande suivante sur les deux instances.

   ```
   add ipset <ipsetname>
   ```

3. Liez l'ensemble d'adresses IP à l'ensemble d'adresses IP virtuelles sur les deux instances.

   Tapez la commande suivante sur les deux instances :

   ```
   add ns ip <secondary vip> <subnet> -type VIP
   ```

   ```
   bind ipset <ipsetname> <secondary VIP>
   ```

   > **Remarque**
   >
   > Vous pouvez lier l'ensemble d'adresses IP au VIP principal ou au VIP secondaire. Toutefois, si vous liez l'ensemble d'adresses IP au VIP principal, utilisez l'adresse IP virtuelle secondaire pour l'ajouter au serveur virtuel, et inversement.

4. Ajoutez un serveur virtuel sur l'instance principale.

   Exécutez la commande suivante :

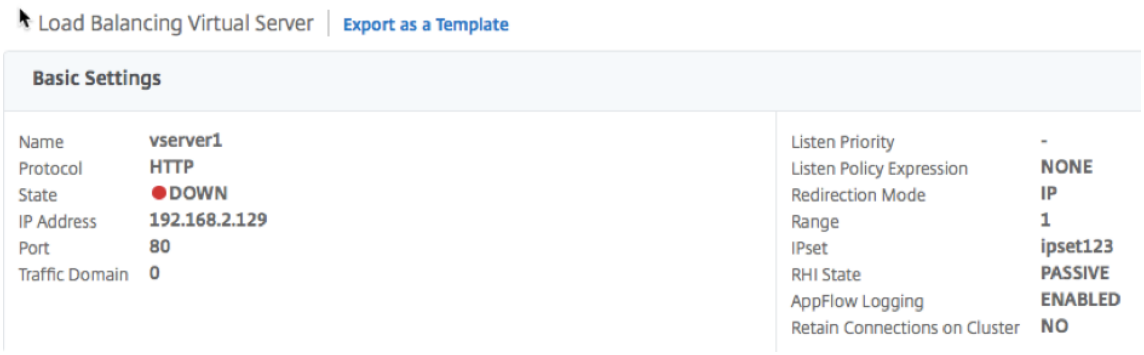
   ```
   add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
   > -ipset \<ipset_name>
   ```

Configurer la haute disponibilité à l'aide de l'interface graphique

1. Configuration de la haute disponibilité en mode INC sur les deux instances
2. Ouvrez une session sur le nœud principal avec le nom d'utilisateur `nsroot` et l'ID d'instance comme mot de passe.
3. Dans l'interface graphique, accédez à **Configuration** > **Système** > **Haute disponibilité**. Cliquez sur **Ajouter**.

4. Dans le champ **Adresse IP du nœud distant**, ajoutez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
5. Sélectionnez **Activer le mode NIC (Independent Network Configuration)** sur le nœud automatique.
6. Sous **Informations d'identification de connexion au système distant**, ajoutez le nom d'utilisateur et le mot de passe du nœud secondaire, puis cliquez sur **Créer**.
7. Répétez les étapes dans le nœud secondaire.
8. Ajoutez l'ensemble d'adresses IP et liez l'ensemble d'adresses IP au jeu d'adresses IP virtuelles sur les deux instances.
9. Dans l'interface graphique, accédez à **Système** > **Réseau** > **IP** > **Ajouter**.
10. Ajoutez les valeurs requises pour l'adresse IP, le masque de réseau, le type d'IP (adresse IP virtuelle) et cliquez sur **Créer**.
11. Accédez à **Système** > **Réseau** > **Ensembles d'adresses IP** > **Ajouter**. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
12. Sur la page IPv4, sélectionnez l'adresse IP virtuelle et cliquez sur **Insérer**. Cliquez sur **Créer** pour créer le jeu d'adresses IP.
13. Ajouter un serveur virtuel dans l'instance principale

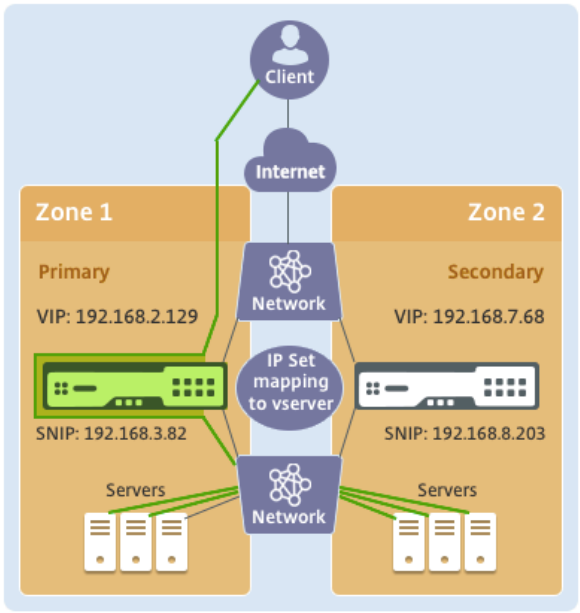
    Dans l'interface graphique, accédez à **Configuration** > **Gestion du trafic** > **Serveurs virtuels** > **Ajouter**.



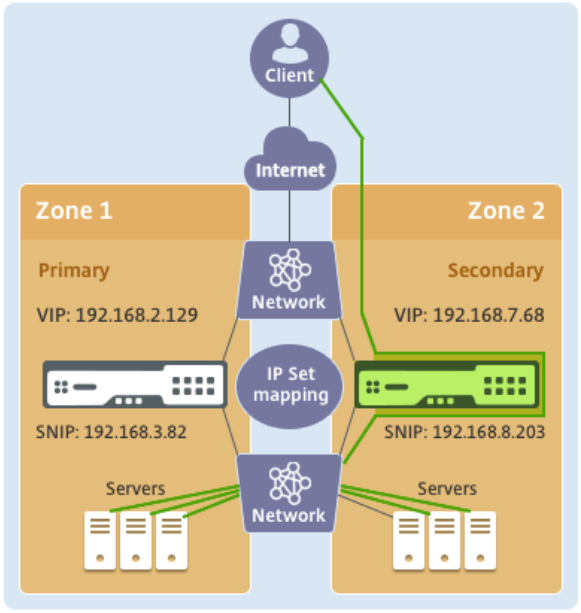
Scénario

Dans ce scénario, un seul VPC est créé. Dans ce VPC, deux instances VPX sont créées dans deux zones de disponibilité. Chaque instance comporte trois sous-réseaux : un pour la gestion, un pour le client et un pour le serveur principal. Un EIP est attaché à l'adresse IP virtuelle du nœud principal.

Schéma : Ce schéma illustre la configuration de haute disponibilité de NetScaler VPX en mode INC, sur AWS



Before failover



After failover

Pour ce scénario, utilisez l'interface de ligne de commande pour configurer la haute disponibilité.

1. Configurez la haute disponibilité en mode INC sur les deux instances.

   Tapez les commandes suivantes sur les nœuds principal et secondaire.

   Sur le primaire :

   ```
   add ha node 1 192.168.6.82 -inc enabled
   ```

   Ici, 192.168.6.82 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire.

   Au secondaire :

   ```
   add ha node 1 192.168.1.108 -inc enabled
   ```

   Ici, 192.168.1.108 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal.

2. Ajoutez un ensemble d'adresses IP et liez l'ensemble d'adresses IP au VIP sur les deux instances

   Au primaire :

   ```
   add ipset ipset123
   ```

   ```
   add ns ip 192.168.7.68 255.255.255.0 -type VIP
   ```

   ```
   bindipset ipset123 192.168.7.68
   ```

   Au secondaire :

   ```
   add ipset ipset123
   ```



```
add ns ip 192.168.7.68 255.255.255.0 -type VIP

bind ipset ipset123 192.168.7.68
```

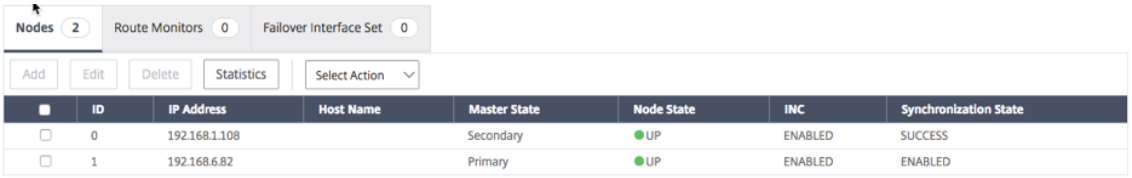
3. Ajoutez un serveur virtuel sur l'instance principale.

   La commande suivante :

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. Enregistrez la configuration.

5. Après un basculement forcé, le secondaire devient le nouveau principal.



Déployez une paire VPX haute disponibilité avec des adresses IP privées dans différentes zones AWS

May 5, 2023

Vous pouvez configurer deux instances NetScaler VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes à l'aide d'adresses IP privées en mode INC. Cette solution peut être facilement intégrée à la paire haute disponibilité VPX multizone existante avec des adresses IP Elastic. Par conséquent, vous pouvez utiliser les deux solutions ensemble.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité. Pour plus d'informations sur INC, voir Configuration de nœuds haute disponibilité dans différents sous-réseaux.

> **Remarque :**
>
> Ce déploiement est pris en charge à partir de la version 13.0 de NetScaler build 67.39. Ce déploiement est compatible avec AWS Transit Gateway.

Paire haute disponibilité avec des adresses IP privées à l'aide d'un VPC non partagé AWS

Composants requis

Assurez-vous que le rôle IAM associé à votre compte AWS dispose des autorisations IAM suivantes :

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
         }

    ]
 }


<!--NeedCopy-->
```

Déployer une paire HA VPX avec des adresses IP privées à l'aide d'un VPC non partagé AWS

Voici un résumé des étapes de déploiement d'une paire VPX sur deux sous-réseaux différents ou deux zones de disponibilité AWS différentes à l'aide d'adresses IP privées.

1. Créez un cloud privé virtuel Amazon.
2. Déployez deux instances VPX dans deux zones de disponibilité différentes.
3. Configurer la haute disponibilité
    a) Configurez la haute disponibilité en mode INC dans les deux instances.

b) Ajoutez les tables de routage respectives dans le VPC qui pointe vers l'interface client.
c) Ajoutez un serveur virtuel dans l'instance principale.

Pour les étapes 1, 2 et 3b, utilisez la console AWS. Pour les étapes 3a et 3c, utilisez l'interface graphique NetScaler VPX ou la CLI.

Étape 1. Créez un cloud privé virtuel (VPC) Amazon.

Étape 2. Déployez deux instances VPX dans deux zones de disponibilité différentes avec le même nombre d'interface réseau (ENI).

Pour plus d'informations sur la création d'un VPC et le déploiement d'une instance VPX sur AWS, consultez [Déployer une instance autonome NetScaler VPX sur AWS et Scénario : instance autonome](/fr-fr/citrix-adc/current-release/deploying-vpx/deploy-aws)

Étape 3. Configurez les adresses VIP ADC en choisissant un sous-réseau qui ne chevauche pas les sous-réseaux Amazon VPC. Si votre VPC est 192.168.0.0/16, pour configurer les adresses VIP ADC, vous pouvez choisir n'importe quel sous-réseau parmi les plages d'adresses IP suivantes :

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

Dans cet exemple, le sous-réseau 10.10.10.0/24 choisi et créé des VIP dans ce sous-réseau. Vous pouvez choisir n'importe quel sous-réseau autre que le sous-réseau VPC (192.168.0.0/16).

Étape 4. Ajoutez une route qui pointe vers l'interface client (VIP) du nœud principal à partir de la table de routage du VPC.

À partir de l'interface de ligne de commande AWS, tapez la commande suivante :

```
1 aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-
     block 10.10.10.0/24 --gateway-id <eni-client-primary>
2 <!--NeedCopy-->
```

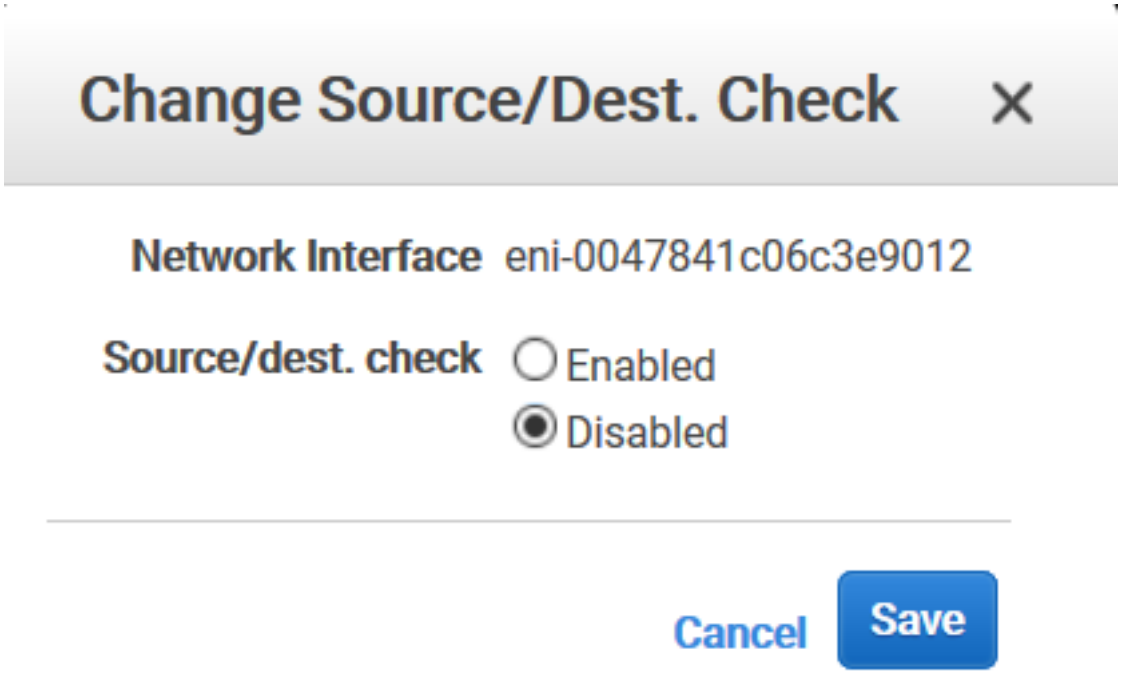
À partir de l'interface graphique AWS, effectuez les étapes suivantes pour ajouter un itinéraire :

1. Ouvrez la console Amazon EC2.
2. Dans le volet de navigation, choisissez **Tables de routage**et sélectionnez la table de routage.
3. Choisissez **Actions**, puis cliquez sur **Modifier les itinéraires**.
4. Pour ajouter un itinéraire, choisissez **Ajouter un itinéraire**. Pour **Destination**, entrez le bloc CIDR de destination, une adresse IP unique ou l'ID d'une liste de préfixes. Pour ID de passerelle, sélectionnez l'ENI d'une interface client du nœud principal.

> **Remarque :**
>
> Vous devez désactiver la **vérification source/dest** sur l'ENI client de l'instance principale.

Pour désactiver la vérification source/destination d'une interface réseau à l'aide de la console, effectuez les opérations suivantes :

1. Ouvrez la console Amazon EC2.
2. Dans le volet de navigation, choisissez **Interfaces réseau**.
3. Sélectionnez l'interface réseau d'une interface client principale, puis choisissez **Actions**, puis cliquez sur **Modifier la source/Dest. Vérifie**.
4. Dans la boîte de dialogue, choisissez **Désactivé**, puis cliquez sur **Enregistrer**.



Étape 5. Configurez la haute disponibilité. Vous pouvez utiliser l'interface de ligne de commande NetScaler VPX ou l'interface graphique pour configurer la haute disponibilité.

Configuration de la haute disponibilité à l'aide de la CLI

1. Configurez la haute disponibilité en mode INC dans les deux instances.

   Sur le nœud principal :

   ```
   1 add ha node 1 <sec_ip> -inc ENABLED
   2 <!--NeedCopy-->
   ```

   Sur le nœud secondaire :

   ```
   1 add ha node 1 <prim_ip> -inc ENABLED
   2 <!--NeedCopy-->
   ```

   <sec_ip>fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire.

   <prim_ip>fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal.

2. Ajoutez un serveur virtuel sur l'instance principale. Vous devez l'ajouter à partir du sous-réseau choisi, par exemple 10.10.10.0/24.

   Exécutez la commande suivante :

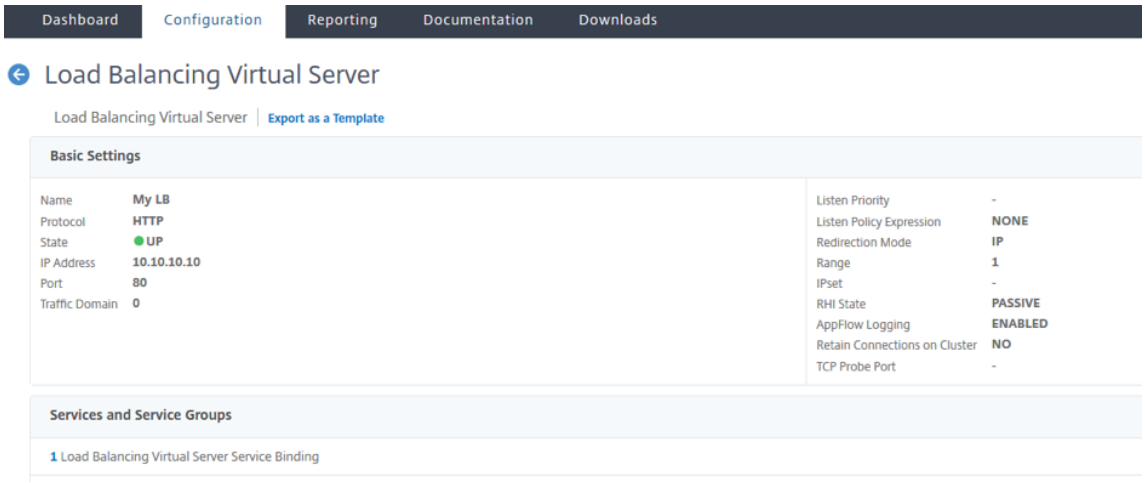
   ```
   1 add \<server\_type\> vserver \<vserver\_name\> \<protocol\> \<
       primary\_vip\> \<port\>
   2 <!--NeedCopy-->
   ```

Configurer la haute disponibilité à l'aide de l'interface graphique

1. Configuration de la haute disponibilité en mode INC sur les deux instances
2. Ouvrez une session sur le nœud principal avec le nom d'utilisateur `nsroot` et l'ID d'instance comme mot de passe.
3. Accédez à **Configuration** > **Système** > **Haute disponibilité**, puis cliquez sur **Ajouter**.
4. Dans le champ **Adresse IP du nœud distant**, ajoutez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
5. Sélectionnez **Activer le mode NIC (Independent Network Configuration)** sur le nœud automatique.
6. Sous **Informations d'identification de connexion au système distant**, ajoutez le nom d'utilisateur et le mot de passe du nœud secondaire, puis cliquez sur **Créer**.

7. Répétez les étapes dans le nœud secondaire.
8. Ajouter un serveur virtuel dans l'instance principale

   Accédez à **Configuration** > **Gestion du trafic** > **Serveurs virtuels** > **Ajouter**.



Déployer une paire HA VPX avec des adresses IP privées à l'aide d'un VPC partagé AWS

Dans un modèle de VPC partagé AWS, le compte propriétaire du VPC (propriétaire) partage un ou plusieurs sous-réseaux avec d'autres comptes (participants). Par conséquent, vous disposez d'un compte propriétaire d'un VPC et d'un compte de participant. Une fois qu'un sous-réseau est partagé, les participants peuvent afficher, créer, modifier et supprimer leurs ressources d'application dans les sous-réseaux partagés avec eux. Les participants ne peuvent pas afficher, modifier ou supprimer des ressources appartenant à d'autres participants ou au propriétaire du VPC.

Pour plus d'informations sur le VPC partagé AWS, consultez la documentation AWS.

> **Remarque :**
>
> Les étapes de configuration pour déployer une paire HA VPX avec des adresses IP privées à l'aide d'un VPC partagé AWS sont identiques à celles de Déployer une paire HA VPX avec des adresses IP privées à l'aide d'un VPC non partagé AWS, à l'exception suivante :
>
> - Les tables de routage du VPC qui pointe vers l'interface client doivent être ajoutées à partir du *compte propriétaire du VPC*.

Composants requis

- Assurez-vous que le rôle IAM associé à l'instance NetScaler VPX dans le compte du participant AWS possède les autorisations IAM suivantes :

```
1  "Version": "2012-10-17",
2      "Statement": [
```



```
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DisassociateAddress",
                "iam:GetRole",
                "iam:SimulatePrincipalPolicy",
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                 “ec2:AssociateAddress” ,
                "sts:AssumeRole"
        ],
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

> Remarque :
>
> Le **rôle AssumeRole** permet à l'instance NetScaler VPX d'assumer le rôle IAM multicompte, qui est créé par le compte propriétaire du VPC.

- Assurez-vous que le compte propriétaire du VPC fournit les autorisations IAM suivantes au compte du participant à l'aide du rôle IAM entre comptes :

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

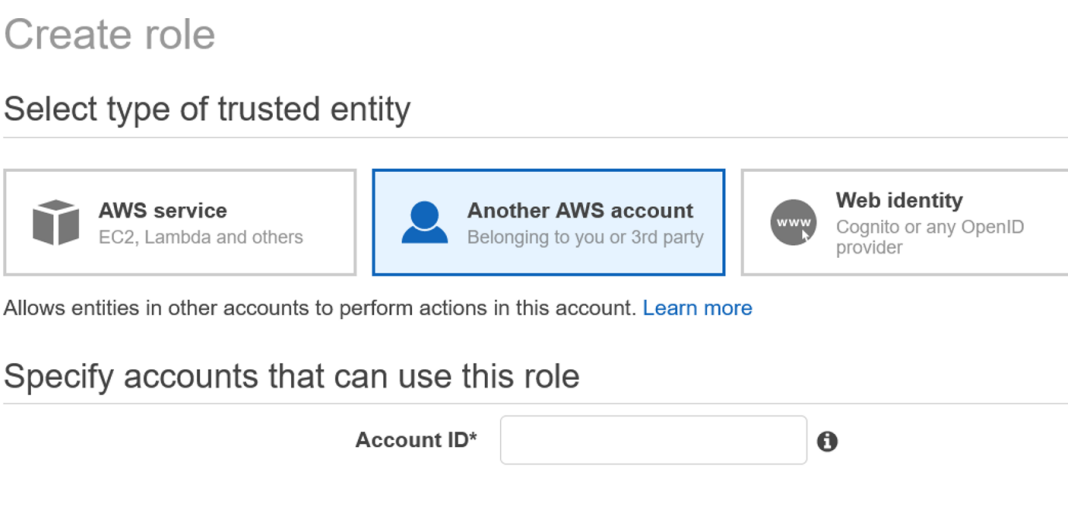
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeRouteTables"
            ],
            "Resource": "*"
         }
```



```
16
17        ]
18     }
19
20  <!--NeedCopy-->
```

Créer un rôle IAM entre comptes

1. Connectez-vous à la console Web AWS.
2. Dans l'onglet **IAM**, accédez à **Roles,** puis choisissez **Create Role**.
3. Choisissez **un autre compte AWS**.



4. Entrez le numéro d'identification de compte à 12 chiffres du compte du participant auquel vous souhaitez accorder l'accès administrateur.

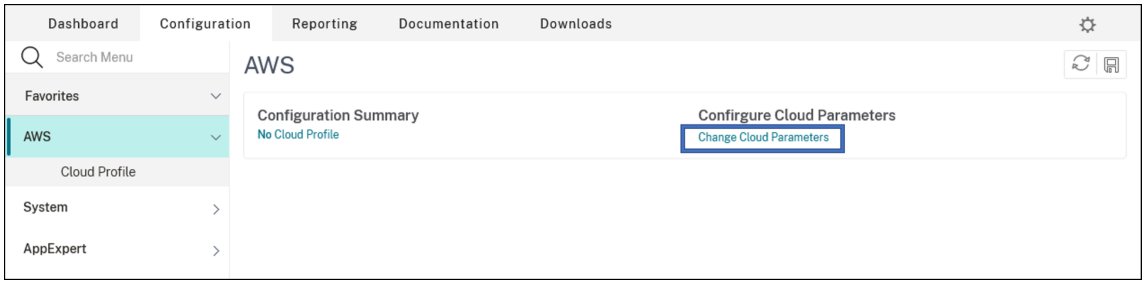
Définissez le rôle IAM multicompte à l'aide de l'interface de ligne de commande NetScaler

La commande suivante permet à l'instance NetScaler VPX d'assumer le rôle IAM intercomptes qui existe dans le compte propriétaire du VPC.

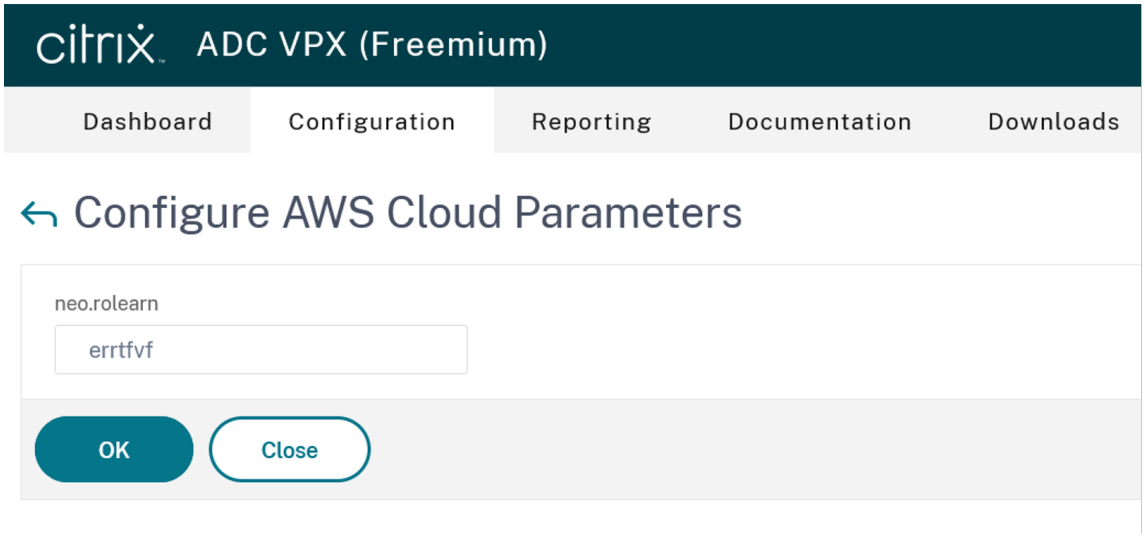
```
1  set cloud awsParam -roleARN <string>
2  <!--NeedCopy-->
```

Définissez le rôle IAM multicompte à l'aide de l'interface graphique NetScaler

1. Connectez-vous à l'appliance NetScaler et accédez à **Configuration > AWS > Modifier les paramètres du cloud**.



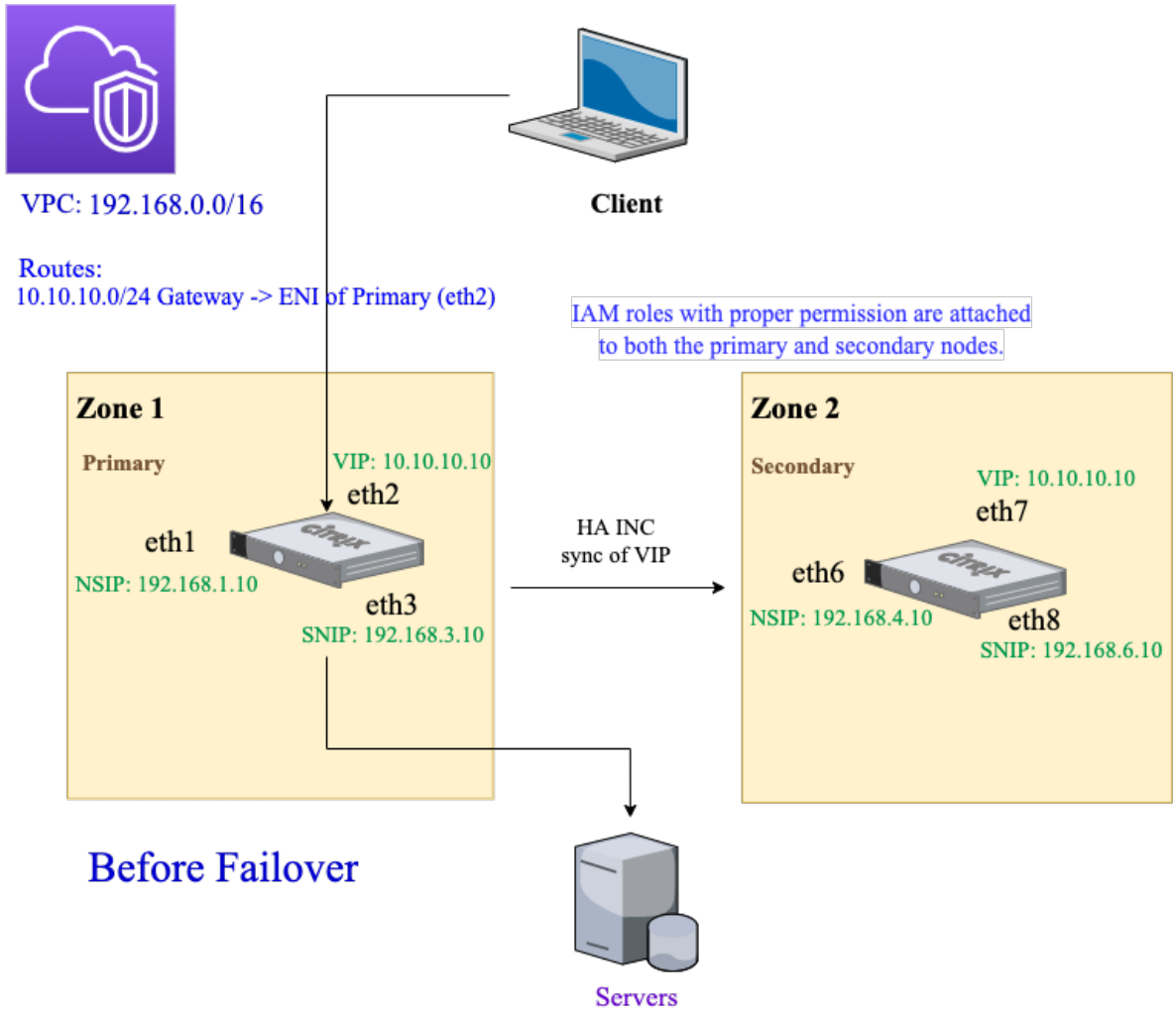
2. Sur la page **Configurer les paramètres du cloud AWS**, saisissez une valeur pour le champ **RoleARN**.

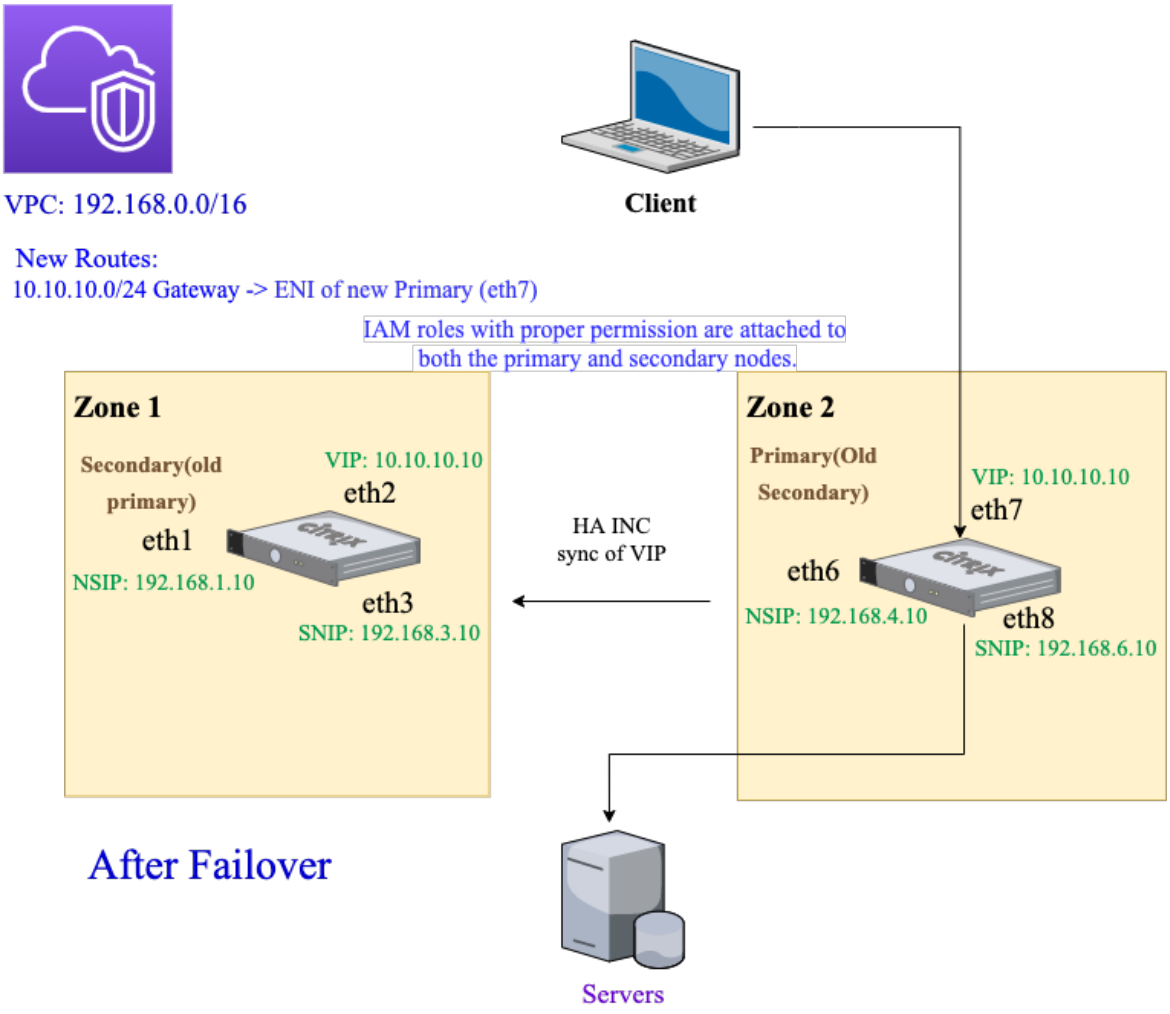


Scénario

Dans ce scénario, un seul VPC est créé. Dans ce VPC, deux instances VPX sont créées dans deux zones de disponibilité. Chaque instance comporte trois sous-réseaux : un pour la gestion, un pour le client et un pour le serveur principal.

Les diagrammes suivants illustrent la configuration de haute disponibilité de NetScaler VPX en mode INC, sur AWS. Le sous-réseau 10.10.10.10 personnalisé, qui ne fait pas partie du VPC, est utilisé comme VIP. Par conséquent, le sous-réseau 10.10.10.10 peut être utilisé dans toutes les zones de disponibilité.





Pour ce scénario, utilisez l'interface de ligne de commande pour configurer la haute disponibilité.

1. Configurez la haute disponibilité en mode INC sur les deux instances.

   Tapez les commandes suivantes sur les nœuds principal et secondaire.

   Sur le nœud principal :

   ```
   add ha node 1 192.168.4.10 -inc enabled
   <!--NeedCopy-->
   ```

   Ici, 192.168.4.10 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud secondaire.

   Sur le nœud secondaire :

   ```
   add ha node 1 192.168.1.10 -inc enabled
   <!--NeedCopy-->
   ```


Ici, 192.168.1.10 fait référence à l'adresse IP privée de la carte réseau de gestion du nœud principal.

2. Ajoutez un serveur virtuel sur l'instance principale.

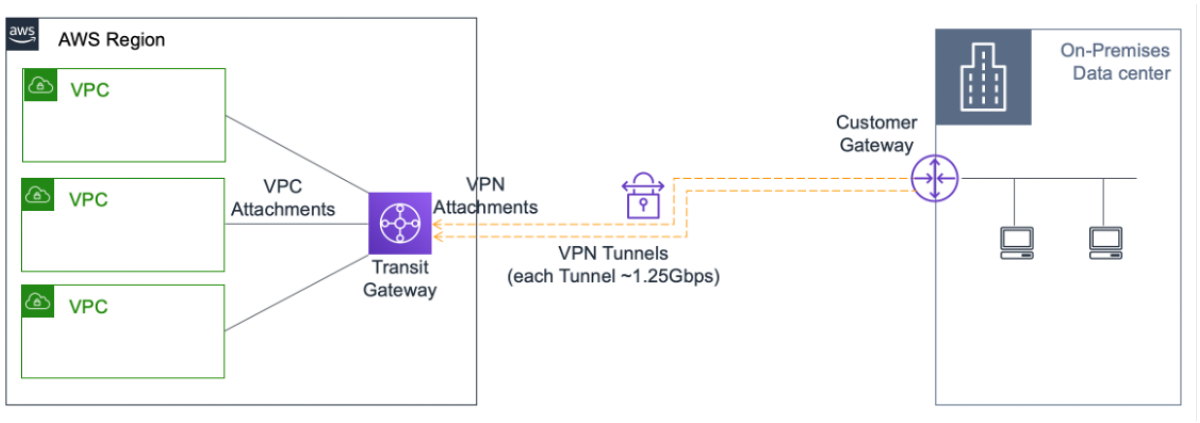
   Exécutez la commande suivante :

```
add lbvserver vserver1 http 10.10.10.10 80
<!--NeedCopy-->
```

3. Enregistrez la configuration.
4. Après un basculement forcé :
   - L'instance secondaire devient la nouvelle instance principale.
   - La route du VPC pointant vers l'ENI principale migre vers l'ENI du client secondaire.
   - Le trafic client reprend vers la nouvelle instance principale.

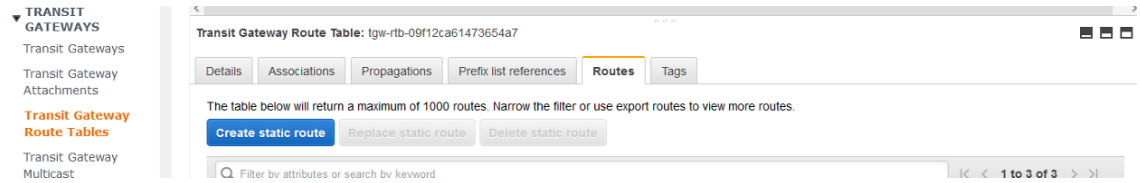
Configuration d'AWS Transit Gateway pour la solution IP privée HA

Vous avez besoin d'AWS Transit Gateway pour que le sous-réseau VIP privé soit routable au sein du réseau interne, sur les VPC AWS, les régions et les réseaux locaux. Le VPC doit se connecter à AWS Transit Gateway. Une route statique pour le sous-réseau VIP ou le pool IP à l'intérieur de la table de routage AWS Transit Gateway est créée et pointée vers le VPC.

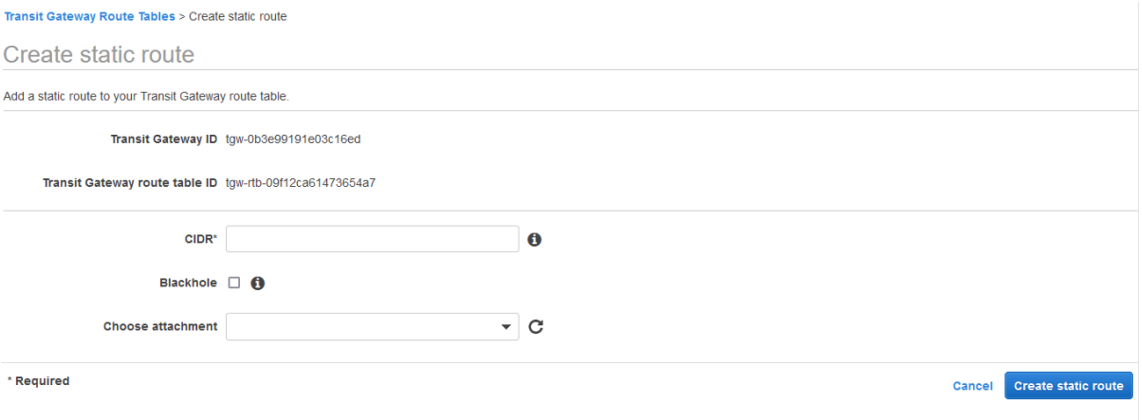


Pour configurer AWS Transit Gateway, procédez comme suit :

1. Ouvrez la console Amazon VPC.
2. Dans le volet de navigation, sélectionnez **Tables de routage Transit Gateway**.
3. Sélectionnez l'onglet **Itinéraires**, puis cliquez sur **Créer un itinéraire statique**.



4. Créez un itinéraire statique où le CIDR pointe vers votre sous-réseau VIPS privé et des points de rattachement vers le VPC doté de NetScaler VPX.



5. Cliquez sur **Créer un itinéraire statique**, puis choisissez **Fermer**.

Dépannage

Si vous rencontrez des problèmes lors de la configuration d'une solution IP privée HA sur une haute disponibilité multizone, vérifiez les points clés suivants pour résoudre les problèmes :

- Les nœuds principal et secondaire disposent du même ensemble d'autorisations IAM.
- Le mode INC est activé à la fois sur les nœuds principal et secondaire.
- Les nœuds principaux et secondaires possèdent le même nombre d'interfaces.
- Lors de la création d'une instance, suivez le même ordre d'attachement des interfaces sur les deux nœuds. Sur un nœud principal, si l'interface client est connectée en premier et l'interface serveur en second lieu. Ensuite, suivez également le même ordre sur le nœud secondaire. En cas de discordance, détachez et reconnectez les interfaces dans le bon ordre.
- Si le trafic ne circule pas, assurez-vous que « Source/DEST ». Check » est désactivé pour la première fois sur l'interface client du nœud principal.
- Assurez-vous que la commande cloudhadaemon (`ps -aux | grep cloudha`) est exécutée dans Shell.
- Assurez-vous que la version du microprogramme NetScaler est 13.0 build 70.x ou ultérieure.
- Pour tout problème lié au processus de basculement, consultez le fichier journal disponible à l'adresse suivante : /var/log/cloud-ha-daemon.log

Déployer une instance NetScaler VPX sur AWS Outposts

May 5, 2023

AWS Outposts est un pool de capacités de calcul et de stockage AWS déployées sur votre site. Outposts fournit l'infrastructure et les services AWS sur site. AWS exploite, surveille et gère cette capacité dans le cadre d'une région AWS. Vous pouvez utiliser les mêmes instances NetScaler VPX, les mêmes API AWS, les mêmes outils et la même infrastructure sur site et dans le cloud AWS pour bénéficier d'une expérience hybride cohérente.

Vous pouvez créer des sous-réseaux sur vos Outposts et les spécifier lorsque vous créez des ressources AWS telles que des instances EC2, des volumes EBS, des clusters ECS et des instances RDS. Les instances des sous-réseaux Outposts communiquent avec d'autres instances de la région AWS à l'aide d'adresses IP privées, toutes au sein du même Amazon Virtual Private Cloud (VPC).

Pour plus d'informations, consultez le guide de l'utilisateur AWS Outposts.

Fonctionnement de AWS Outposts

AWS Outposts est conçu pour fonctionner avec une connexion constante et cohérente entre vos Outposts et une région AWS. Pour établir cette connexion à la région et aux charges de travail locales de votre environnement sur site, vous devez connecter votre Outpost à votre réseau local. Votre réseau local doit fournir un accès WAN à la région et à Internet. Internet doit également fournir un accès LAN ou WAN au réseau local sur lequel résident vos charges de travail ou applications sur site.

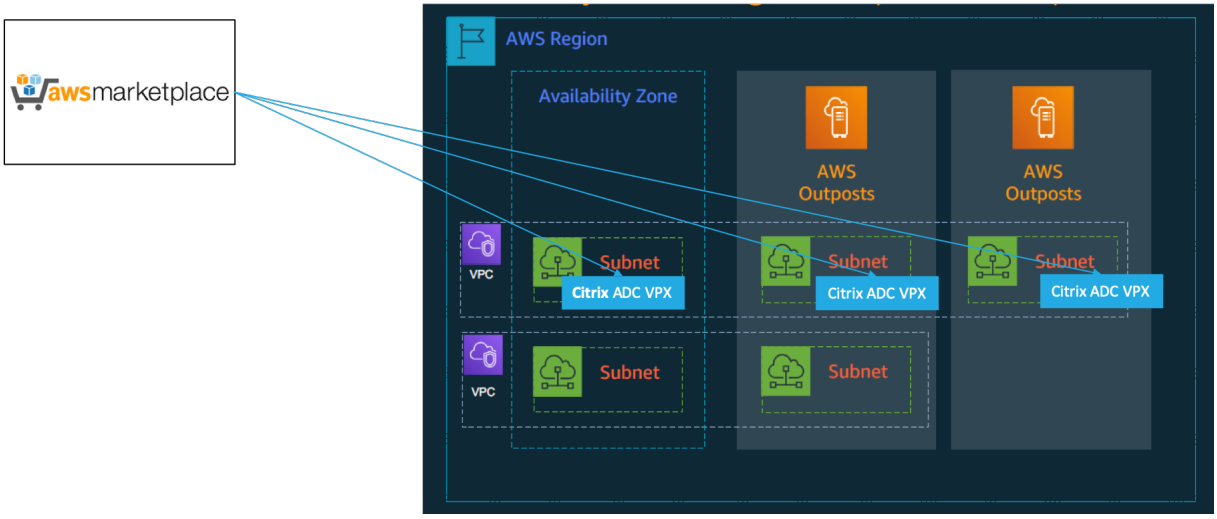
Conditions préalables

- Vous devez installer AWS Outposts sur votre site.
- La capacité de calcul et de stockage d'AWS Outposts doit être disponible pour être utilisée.

Pour plus d'informations sur la manière de passer une commande pour AWS Outposts, consultez la documentation AWS suivante :
https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/

Déployez une instance NetScaler VPX sur AWS Outposts à l'aide de la console Web AWS

La figure suivante décrit un déploiement simple d'instances NetScaler VPX sur les Outposts. L'AMI NetScaler présente sur AWS Marketplace est également déployée dans les Outposts.



Connectez-vous à la console Web AWS et effectuez les étapes suivantes pour déployer des instances NetScaler VPX EC2 sur vos AWS Outposts.

1. Créez une paire de clés.
2. Créez un cloud privé virtuel (VPC).
3. Ajoutez d'autres sous-réseaux.
4. Créez des groupes de sécurité et des règles de sécurité.
5. Ajoutez des tables de routage.
6. Créez une passerelle Internet.
7. Créez une instance NetScaler VPX à l'aide du service AWS EC2.
   Depuis le tableau de bord AWS, accédez à **Compute > EC2 > Launch Instance > AWS Marketplace**.
8. Créez et connectez davantage d'interfaces réseau.
9. Attachez des adresses IP élastiques à la carte réseau de gestion.
10. Connectez-vous à l'instance VPX.

Pour obtenir des instructions détaillées sur chacune des étapes, voir Déployer une instance NetScaler VPX sur AWS à l'aide de la console Web AWS.

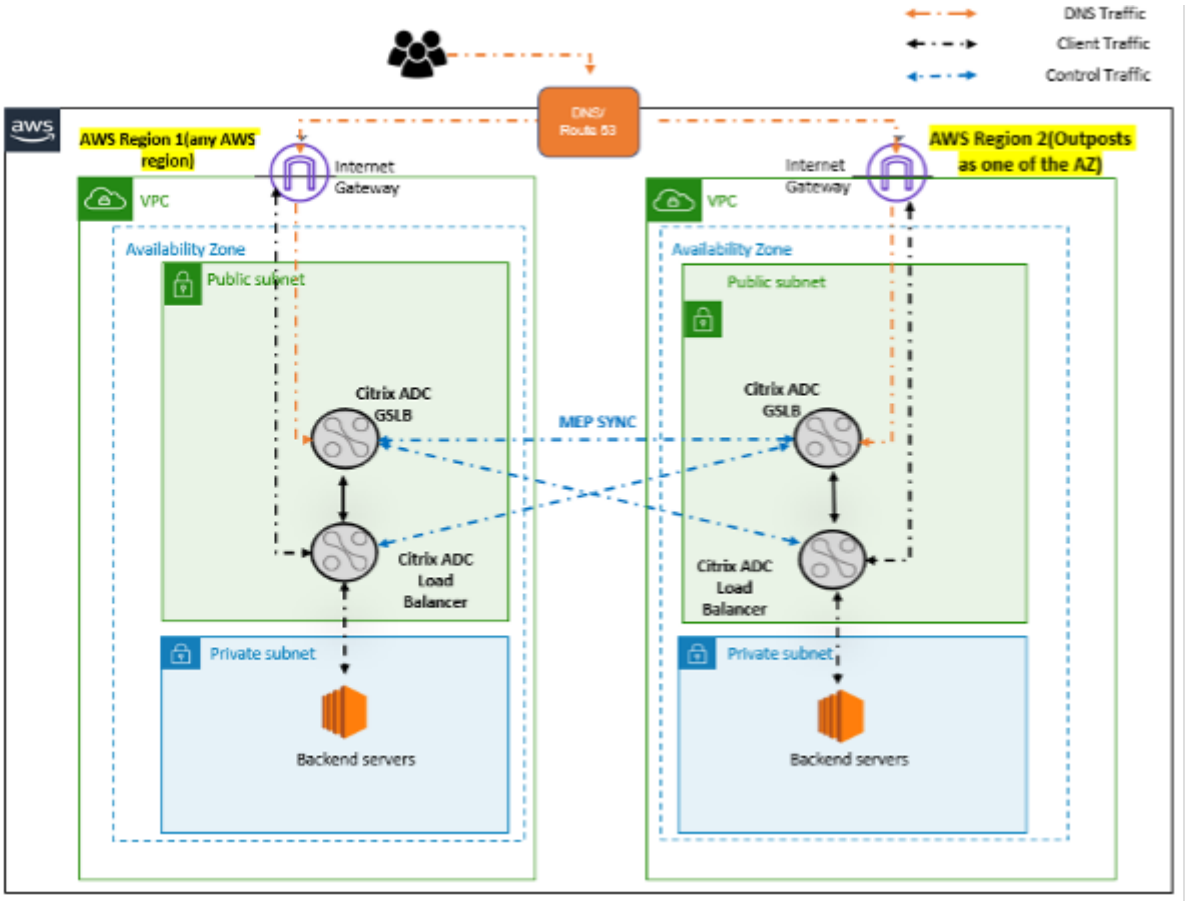
Pour connaître la haute disponibilité dans le cadre du déploiement de la même zone de disponibilité, voir Déployer une paire haute disponibilité sur AWS.

Déployez une instance NetScaler VPX sur un cloud hybride avec AWS Outposts

Vous pouvez déployer une instance NetScaler VPX sur un cloud hybride dans un environnement AWS qui contient des avant-postes AWS. Vous pouvez simplifier le mécanisme de diffusion des applications à l'aide de la solution d'équilibrage de charge globale des serveurs (GSLB) de NetScaler. La solution GSLB distribue le trafic des applications entre plusieurs centres de données dans des clouds hybrides conçus à l'aide des régions AWS et de l'infrastructure AWS Outposts.

NetScaler GSLB prend en charge les types de déploiement actif-actif et actif-passif pour répondre à différents cas d'utilisation. Outre ces options de déploiement flexibles et ces mécanismes de fourniture d'applications, NetScaler sécurise l'ensemble du réseau et du portefeuille d'applications, que les applications soient déployées de manière native sur AWS Cloud ou AWS Outposts.

Le schéma suivant illustre la mise à disposition d'une application avec l'appliance NetScaler dans un cloud hybride avec AWS.



Dans un déploiement actif-actif, NetScaler dirige le trafic à l'échelle mondiale dans un environnement distribué. Tous les sites de l'environnement échangent des mesures concernant la disponibilité et l'état de santé des ressources via le Metrics Exchange Protocol (MEP). L'appliance NetScaler utilise ces informations pour équilibrer la charge du trafic entre les sites et envoie les demandes des clients au site GSLB le plus approprié, selon la méthode définie (round robin, connexion minimale et proximité statique) spécifiée dans la configuration GSLB.

Vous pouvez utiliser le déploiement GSLB actif-actif pour :

- Optimisez l'utilisation des ressources avec tous les nœuds actifs.
- Améliorez l'expérience utilisateur en dirigeant les demandes vers le site le plus proche de chaque utilisateur.
- Migrez les applications vers le cloud à un rythme défini par l'utilisateur.

Vous pouvez utiliser le déploiement GSLB actif-passif pour :

- Récupération d'urgence
- Explosion de nuages

Références

- Déployer une instance NetScaler VPX sur AWS
- Déployez une instance NetScaler VPX sur AWS Outposts à l'aide de la console Web AWS
- Configurer GSLB sur des instances NetScaler VPX

Protégez AWS API Gateway à l'aide du pare-feu NetScaler Web App Firewall

May 5, 2023

Vous pouvez déployer une appliance NetScaler devant votre AWS API Gateway et sécuriser la passerelle d'API contre les menaces externes. NetScaler Web App Firewall (WAF) peut protéger votre API contre les 10 principales menaces de l'OWASP et les attaques de type « jour zéro ». NetScaler Web App Firewall utilise une base de code unique pour tous les formats ADC. Par conséquent, vous pouvez appliquer et appliquer des politiques de sécurité de manière cohérente dans n'importe quel environnement. NetScaler Web App Firewall est facile à déployer et est disponible sous forme de licence unique. Le pare-feu NetScaler Web App fournit les fonctionnalités suivantes :

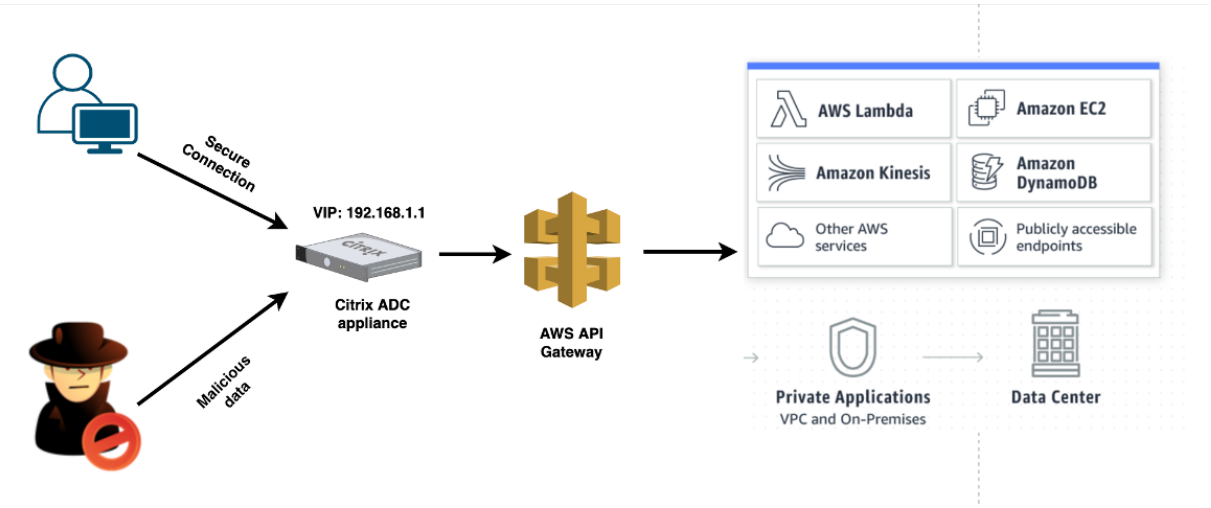
- Configuration simplifiée
- Gestion des robots
- Visibilité holistique
- Rassemblez des données provenant de plusieurs sources et affichez les données sur un écran unifié

Outre la protection de la passerelle d'API, vous pouvez également utiliser les autres fonctionnalités de NetScaler. Pour plus d'informations, consultez la documentation de NetScaler. En plus d'éviter les basculements du centre de données et de minimiser le temps d'arrêt, vous pouvez placer ADC en haute disponibilité au sein ou entre les zones de disponibilité. Vous pouvez également utiliser ou configurer le clustering avec la fonction Autoscale.

Auparavant, AWS API Gateway ne prenait pas en charge les protections nécessaires pour sécuriser les applications sous-jacentes. Sans les protections du Web Application Firewall (WAF), les API étaient sujettes à des menaces de sécurité.

Déployez l'appliance NetScaler devant la passerelle d'API AWS

Dans l'exemple suivant, une appliance NetScaler est déployée devant la passerelle d'API AWS.



Supposons qu'il existe une véritable demande d'API pour le service AWS Lambda. Cette demande peut concerner n'importe lequel des services d'API mentionnés dans la documentation Amazon API Gateway. Comme le montre le schéma précédent, le flux de trafic est le suivant :

1. Le client envoie une demande à la fonction AWS Lambda (XYZ). Cette demande du client est envoyée au serveur virtuel NetScaler (192.168.1.1).
2. Le serveur virtuel inspecte le paquet et recherche tout contenu malveillant.
3. L'appliance NetScaler déclenche une politique de réécriture pour modifier le nom d'hôte et l'URL dans une demande client. Par exemple, vous souhaitez changer `https://restapi.citrix.com/default/LamdaFunctionXYZ` sur `https://citrix.execute-api.<region>.amazonaws.com/default/LambdaFunctionXYZ`.
4. L'appliance NetScaler transmet cette demande à la passerelle d'API AWS.
5. AWS API Gateway envoie ensuite la demande au service Lambda et appelle la fonction Lambda « XYZ ».
6. Dans le même temps, si un attaquant envoie une demande d'API contenant du contenu malveillant, la demande malveillante atterrit sur l'appliance NetScaler.
7. L'appliance NetScaler inspecte les paquets et les supprime en fonction de l'action configurée.

Configurer l'appliance NetScaler avec WAF activé

Pour activer WAF sur une appliance NetScaler, procédez comme suit :

1. Ajoutez un commutateur de contenu ou un serveur virtuel d'équilibrage de charge. Supposons que l'adresse IP du serveur virtuel soit 192.168.1.1, qui se résout en un nom de domaine (restapi.citrix.com).

2. Activez la politique WAF sur le serveur virtuel NetScaler. Pour plus d'informations, consultez Configuration du Web App Firewall.
3. Activez la stratégie de réécriture pour modifier le nom de domaine. Supposons que vous souhaitiez modifier la demande entrante de l'équilibreur de charge sur le nom de domaine « restapi.citrix.com » afin qu'elle soit réécrite sur le serveur principal AWS API Gateway à l'adresse « citrix.execute-api.<region>Nom de domaine .amazonaws ».
4. Activez le mode L3 sur l'appliance NetScaler pour qu'elle agisse en tant que proxy. Utilisez la commande suivante :

```
enable ns mode L3
<!--NeedCopy-->
```

À l'étape 3 de l'exemple précédent, supposons que l'administrateur du site Web souhaite que l'appliance NetScaler remplace le nom de domaine « restapi.citrix.com » par « citrix.execute-api ».<region>.amazonaws.com » et l'URL avec « Default/Lambda/xyz ».

La procédure suivante explique comment modifier le nom d'hôte et l'URL dans une demande client à l'aide de la fonction de réécriture :

1. Connectez-vous à l'appliance NetScaler via SSH.
2. Ajoutez des actions de réécriture.

```
add rewrite action rewrite_host_hdr_act replace "HTTP.REQ.HEADER("
    Host")" ""citrix.execute-api.<region>.amazonaws.com""

add rewrite action rewrite_url_act replace HTTP.REQ.URL.
    PATH_AND_QUERY ""/default/lambda/XYZ""
<!--NeedCopy-->
```

3. Ajoutez des stratégies de réécriture pour les actions de réécriture.

```
add rewrite policy rewrite_host_hdr_pol "HTTP.REQ.HEADER("Host").
    CONTAINS("restapi.citrix.com") "rewrite_host_hdr_act

add rewrite policy rewrite_url_pol "HTTP.REQ.HEADER("Host").
    CONTAINS("restapi.citrix.com") "rewrite_url_act
<!--NeedCopy-->
```

4. Liez les stratégies de réécriture à un serveur virtuel.

```
bind lb vserver LB_API_Gateway -policyName rewrite_host_hdr_pol -
    priority 10 -gotoPriorityExpression 20 -type REQUEST

```



```
3 bind lb vserver LB_API_Gateway -policyName rewrite_url_pol -
     priority 20 -gotoPriorityExpression END -type REQUEST
4 <!--NeedCopy-->
```

Pour plus d'informations, voir Configurer la réécriture pour modifier le nom d'hôte et l'URL dans la demande du client sur l'appliance NetScaler.

Fonctionnalités et fonctionnalités de NetScaler

Outre la sécurisation du déploiement, l'appliance NetScaler peut également améliorer la demande en fonction des besoins de l'utilisateur. L'appliance NetScaler fournit les fonctionnalités clés suivantes.

- **Équilibrage de la charge de la passerelle d'API :** si vous possédez plusieurs passerelles d'API, vous pouvez équilibrer la charge de plusieurs passerelles d'API à l'aide de l'appliance NetScaler et définir le comportement de la demande d'API.
  - Différentes méthodes d'équilibrage de charge sont disponibles. Par exemple, la méthode de connexion Least évite de surcharger la limite API Gateway, la méthode de chargement personnalisé conserve une charge spécifique sur une passerelle API particulière, etc. Pour plus d'informations, consultez Algorithmes d'équilibragede charge
  - Le déchargement SSL est configuré sans interrompre le trafic.
  - Le mode Use Source IP (USIP) est activé pour conserver l'adresse IP du client.
  - Paramètres SSL définis par l'utilisateur : vous pouvez disposer de votre propre serveur virtuel SSL avec vos propres certificats et algorithmes signés.
  - Serveur virtuel de sauvegarde : si la passerelle API n'est pas accessible, vous pouvez envoyer la demande à un serveur virtuel de sauvegarde pour d'autres actions.
  - De nombreuses autres fonctionnalités d'équilibrage de charge sont disponibles. Pour plus d'informations, consultez la section Trafic d'équilibrage de charge sur une appliance NetScaler.
- **Authentification, autorisation et audit :** vous pouvez définir vos propres méthodes d'authentification telles que LDAP, SAML, RADIUS, et autoriser et auditer les demandes d'API.
- **Répondeur :** vous pouvez rediriger les demandes d'API vers une autre API Gateway pendant le temps d'arrêt.
- **Limitation du débit :** vous pouvez configurer la fonctionnalité de limitation de débit pour éviter la surcharge d'une passerelle API.
- **Meilleure disponibilité :** vous pouvez configurer une appliance NetScaler dans une configuration haute disponibilité ou une configuration en cluster pour améliorer la disponibilité de vos trafics d'API AWS.

- **API REST :** prend en charge l'API REST, qui peut être utilisée pour automatiser le travail dans les environnements de production cloud.
- **Surveiller les données :** Surveille et enregistre les données pour référence.

L'appliance NetScaler fournit de nombreuses fonctionnalités supplémentaires, qui peuvent être intégrées à la passerelle d'API AWS. Pour plus d'informations, consultez la documentation de NetScaler.

Ajouter le service principal AWS Autoscaling

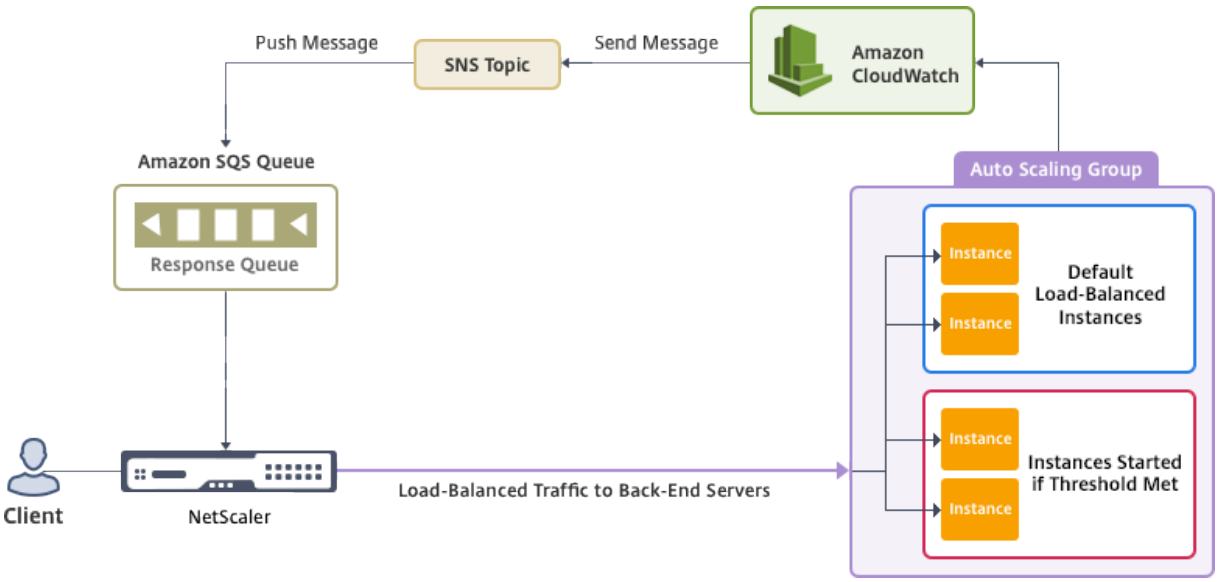
May 5, 2023

L'hébergement efficace des applications dans un cloud implique une gestion aisée et économique des ressources en fonction de la demande des applications. Pour répondre à la demande croissante, vous devez augmenter les ressources réseau. Si la demande diminue, vous devez réduire vos effectifs pour éviter les coûts inutiles liés à des ressources inutilisées. Pour minimiser les coûts d'exécution de l'application en ne déployant que le nombre d'instances nécessaires à un moment donné, vous devez constamment surveiller le trafic, la mémoire et l'utilisation du processeur, etc. Toutefois, la surveillance manuelle du trafic est fastidieuse. Pour que l'environnement d'application évolue de manière dynamique, vous devez automatiser les processus de surveillance du trafic et de mise à l'échelle des ressources lorsque cela est nécessaire.

Intégrée au service AWS Auto Scaling, l'instance NetScaler VPX offre les avantages suivants :

- **Équilibre de charge et gestion** : configure automatiquement les serveurs pour qu'ils augmentent et diminuent, en fonction de la demande. L'instance VPX détecte automatiquement les groupes Autoscale dans le sous-réseau principal et permet à l'utilisateur de sélectionner les groupes Autoscale pour équilibrer la charge. Tout cela se fait en configurant automatiquement les adresses IP virtuelles et de sous-réseau sur l'instance VPX.
- **Haute disponibilité** : détecte les groupes Autoscale qui couvrent plusieurs zones de disponibilité et serveurs d'équilibrage de charge.
- **Meilleure disponibilité du réseau** : l'instance VPX prend en charge :
  - Serveurs dorsaux sur différents VPC, en utilisant le peering VPC
  - Serveurs principaux situés dans les mêmes groupes de placement
  - Serveurs dorsaux situés dans différentes zones de disponibilité
- **Résiliation progressive de la connexion** : supprime les serveurs Autoscale de manière harmonieuse, évitant ainsi la perte de connexions client en cas de réduction de capacité, à l'aide de la fonction Graceful Timeout.

Schéma : service AWS Autoscaling avec une instance NetScaler VPX



Ce schéma montre comment le service AWS Autoscaling est compatible avec une instance NetScaler VPX (serveur virtuel d'équilibrage de charge). Pour plus d'informations, consultez les rubriques AWS suivantes.

- Groupes de mise à l'échelle automatique
- CloudWatch
- Service de notification simple (SNS)
- Service de file d'attente simple (Amazon SQS)

Avant de commencer

Avant de commencer à utiliser Autoscaling avec votre instance NetScaler VPX, vous devez effectuer les tâches suivantes.

1. Lisez les rubriques suivantes :
    - Composants requis
    - Directives de limitation et d'utilisation
2. Créez une instance NetScaler VPX sur AWS selon vos besoins.
    - Pour plus d'informations sur la création d'une instance autonome NetScaler VPX, consultez [Déployer une instance autonome NetScaler VPX sur AWS et Scénario : instance autonome](/fr-fr/citrix-adc/current-release/deploying-vpx/deploy-aws/launch-vpx-for-aws-ami.html)
    - Pour plus d'informations sur le déploiement d'instances VPX en mode HA, voir Déployer une paire haute disponibilité sur AWS.

> **Remarque :**
>
> Citrix recommande le modèle CloudFormation pour créer des instances NetScaler VPX sur AWS.
>
> Citrix vous recommande de créer trois interfaces : une pour la gestion (NSIP), une pour le serveur virtuel LB (VIP) orienté client et une pour l'adresse IP du sous-réseau (NSIP).

3. Créez un groupe AWS Autoscale. Si vous ne disposez pas d'une configuration Autoscaling existante, vous devez :

   a) Création d'une configuration de lancement

   b) Création d'un groupe Autoscaling

   c) Vérifiez le groupe Autoscaling

   Pour plus d'informations, veuillez consulter http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html.

4. Dans le groupe AWS Autoscale, vous devez spécifier au moins une politique de réduction d'échelle. L'instance NetScaler VPX prend uniquement en charge la politique de dimensionnement par étapes. La politique de dimensionnement simple et la politique de dimensionnement de Target Tracking ne sont pas prises en charge pour le groupe Autoscale.

Ajouter le service AWS Autoscaling à une instance NetScaler VPX

Vous pouvez ajouter le service Autoscaling à une instance VPX en un seul clic à l'aide de l'interface graphique. Procédez comme suit pour ajouter le service Autoscaling à l'instance VPX :

1. Connectez-vous à l'instance VPX à l'aide de vos informations d'identification pour `nsroot`.
2. Lorsque vous vous connectez à l'instance NetScaler VPX pour la première fois, la page Cloud Profile par défaut s'affiche. Sélectionnez le groupe AWS Autoscaling dans le menu déroulant et cliquez sur **Créer** pour créer un profil cloud. Cliquez sur **Ignorer** si vous souhaitez créer le profil cloud ultérieurement.

   Points à garder à l'esprit lors de la création d'un profil cloud : par défaut, le modèle CloudFormation crée et attache le rôle IAM ci-dessous.

```
{


    "Version": "2012-10-17",
    "Statement": [

     {

```



```
 9
10              "Action": [
11
12                  "ec2:DescribeInstances",
13                  "ec2:DescribeNetworkInterfaces",
14                  "ec2:DetachNetworkInterface",
15                  "ec2:AttachNetworkInterface",
16                  "ec2:StartInstances",
17                  "ec2:StopInstances",
18                  "ec2:RebootInstances",
19                  "autoscaling:\*",
20                  "sns:\*",
21                  "sqs:*"
22
23                  “iam: SimulatePrincipalPolicy”
24                  “iam: GetRole”
25
26              ],
27
28              "Resource": "*",
29              "Effect": "Allow"
30
31          }
32
33
34      ]
35
36   }
37
38  <!--NeedCopy-->
```

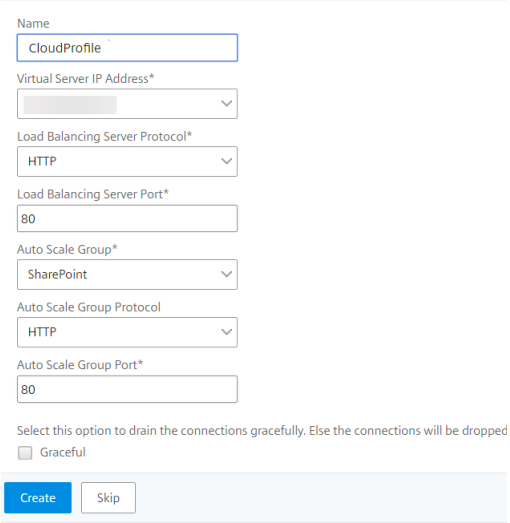
Assurez-vous que le rôle IAM d’une instance dispose des autorisations appropriées.

- L’adresse IP du serveur virtuel est automatiquement renseignée à partir de l’adresse IP libre disponible pour l’instance VPX. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html#ManageMultipleIP
- Le groupe Autoscale est prérempli à partir du groupe Autoscale configuré sur votre compte AWS. http://docs.aws.amazon.com/autoscaling/latest/userguide/AutoScalingGroup.html.
- Lorsque vous sélectionnez le protocole et le port du groupe Autoscaling, assurez-vous que vos serveurs écoutent ces protocoles et ports, et que vous liez le moniteur approprié au groupe de services. Par défaut, le moniteur TCP est utilisé.
- Pour le protocole SSL Autoscaling, une fois le profil cloud créé, le serveur virtuel ou le groupe de services d’équilibrage de charge est en panne en raison d’un certificat man-

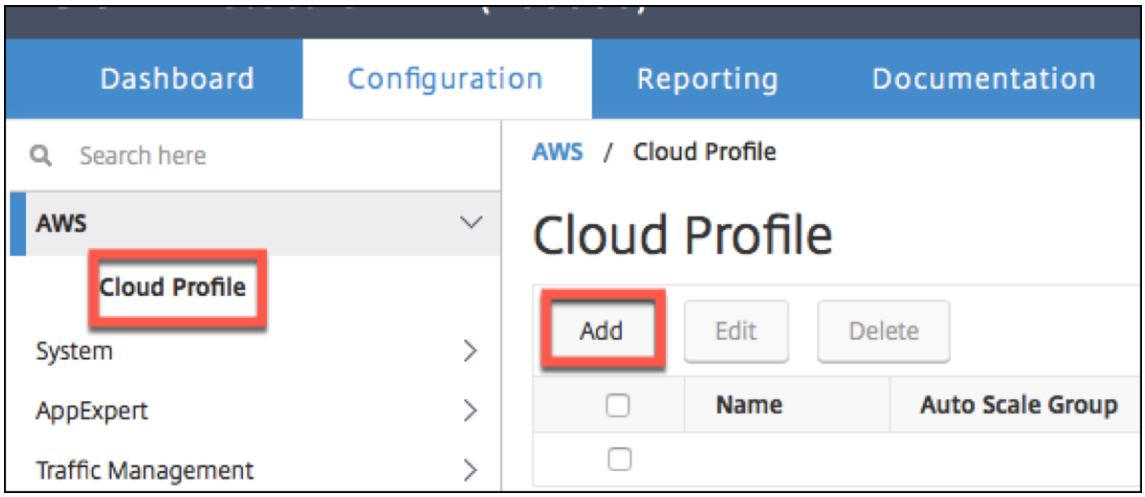
quant. Vous pouvez lier manuellement le certificat au serveur virtuel ou au groupe de services.

- Sélectionnez l'option Graceful Timeout pour supprimer les serveurs Autoscale correctement. Si cette option n'est pas sélectionnée, le serveur est le groupe Autoscale supprimé immédiatement après la fin de la charge, ce qui peut entraîner une interruption de service pour les clients connectés existants. Sélectionnez Graceful et attribuez un délai d'attente en cas de réduction de la taille. L'instance VPX ne supprime pas le serveur immédiatement mais marque l'un des serveurs pour une suppression progressive. Pendant cette période, l'instance n'autorise pas de nouvelles connexions à ce serveur. La connexion existante est servie jusqu'à ce que le délai d'expiration se produise, et après un délai d'expiration, l'instance VPX supprime le serveur.

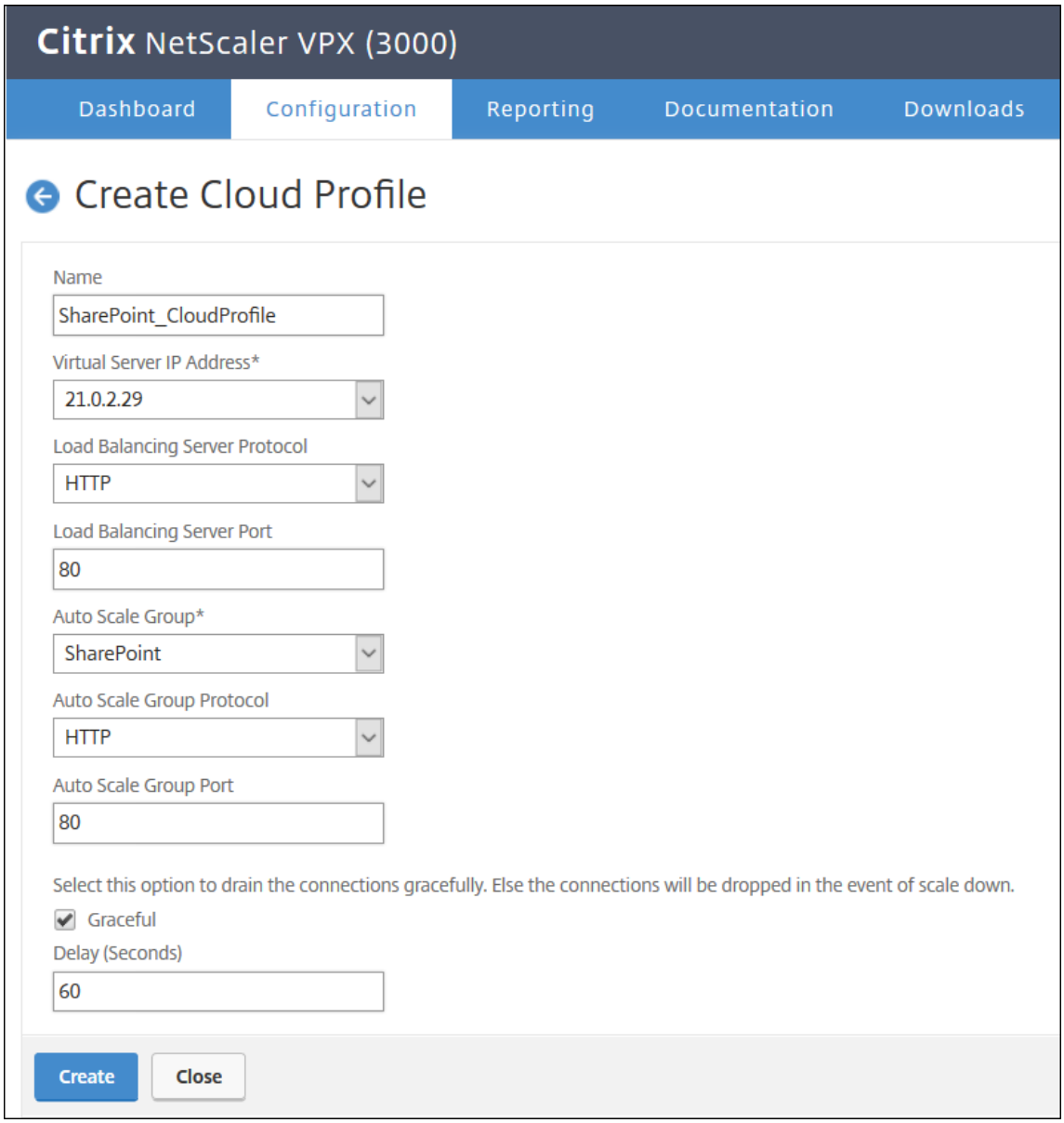
Figure : page Profil cloud par défaut



3. Après la première connexion, si vous souhaitez créer un profil cloud, dans l'interface graphique, accédez à **Système > AWS > Profil cloud** et cliquez sur **Ajouter**.

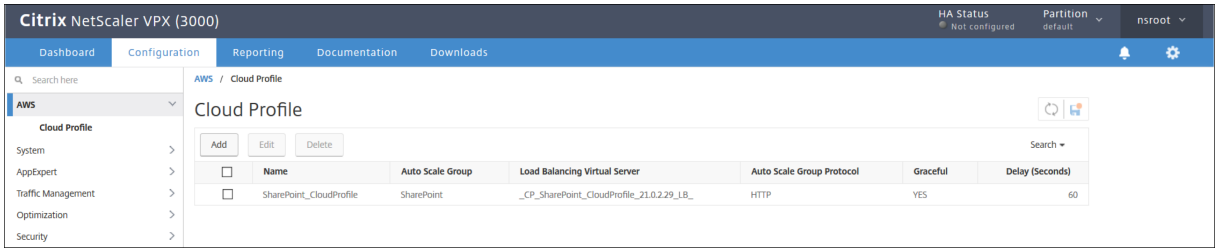


La page de configuration de **Create Cloud Profile** s'affiche.



Cloud Profile crée un serveur virtuel d'équilibrage de charge NetScaler et un groupe de services dont les membres sont les serveurs du groupe Autoscaling. Vos serveurs back-end doivent être accessibles via le SNIP configuré sur l'instance VPX.

> **Remarque :**
>
> À partir de la version 13.1-42.x de NetScaler, vous pouvez créer différents profils cloud pour différents services (en utilisant différents ports) avec le même groupe Autoscaling (ASG) dans AWS. Ainsi, l'instance NetScaler VPX prend en charge plusieurs services avec le même groupe Autoscaling dans le cloud public.



> **Remarque**
>
> Pour consulter les informations relatives à AutoScale dans la console AWS, accédez à **EC2** > **Tableau de bord** > **Auto Scaling** > **Auto Scaling Group**.

Configurer une instance NetScaler VPX pour utiliser l'interface réseau SR-IOV

May 5, 2023

> **Remarque**
>
> La prise en charge des interfaces SR-IOV dans une configuration haute disponibilité est disponible à partir de NetScaler version 12.0 57.19.

Après avoir créé une instance NetScaler VPX sur AWS, vous pouvez configurer l'appliance virtuelle pour qu'elle utilise les interfaces réseau SR-IOV à l'aide de l'interface de ligne de commande AWS.

Dans tous les modèles NetScaler VPX, à l'exception des éditions NetScaler VPX AWS Marketplace 3G et 5G, le SR-IOV n'est pas activé dans la configuration par défaut d'une interface réseau.

Avant de commencer la configuration, lisez les rubriques suivantes :

- Composants requis
- Limitations et directives d'utilisation

Cette section inclut les rubriques suivantes :

- Changez le type d'interface en SR-IOV
- Configurer SR-IOV sur une configuration à haute disponibilité

Changez le type d'interface en SR-IOV

Vous pouvez exécuter la commande show interface summary pour vérifier la configuration par défaut d'une interface réseau.

Exemple 1 : La capture d'écran CLI suivante montre la configuration d'une interface réseau dans laquelle le SR-IOV est activé par défaut sur les éditions 3G et 5G de NetScaler VPX AWS Marketplace.


```
> show interface summary
-------------------------------------------------------------------------------
     Interface  MTU       MAC                Suffix
-------------------------------------------------------------------------------
1      1/1      1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2      LO/1     1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
 Done
```

Exemple 2 : La capture d'écran CLI suivante montre la configuration par défaut d'une interface réseau où SR-IOV n'est pas activée.

```
 Done
> sh int s
-------------------------------------------------------------------------------
     Interface  MTU       MAC                Suffix
-------------------------------------------------------------------------------
1      1/1      1500      12:fc:04:c5:d0:12  NetScaler Virtual Interface
2      LO/1     1500      12:fc:04:c5:d0:12  Netscaler Loopback interface
 Done
>
```

Pour plus d'informations sur la modification du type d'interface en SR-IOV, voir http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html

Pour modifier le type d'interface en SR-IOV

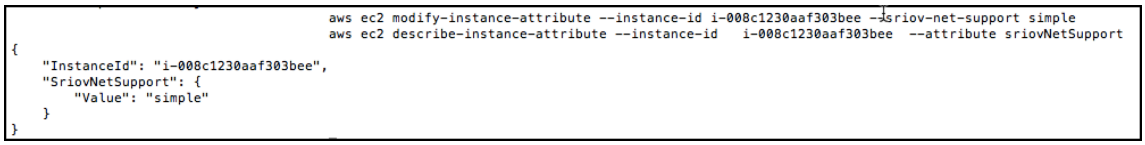
1. Arrêtez l'instance NetScaler VPX exécutée sur AWS.
2. Pour activer SR-IOV sur l'interface réseau, tapez la commande suivante dans l'interface de ligne de commande AWS.

   ```
   $ aws ec2 modify-instance-attribute --instance-id \<instance\\_id\> --sriov-net-support simple
   ```

3. Pour vérifier si SR-IOV a été activé, tapez la commande suivante dans l'interface de ligne de commande AWS.

   ```
   $ aws ec2 describe-instance-attribute --instance-id \<instance\\_id\> --attribute sriovNetSupport
   ```

   Exemple 3 : Le type d'interface réseau est passé à SR-IOV, à l'aide de l'interface de ligne de commande AWS.

   Si SR-IOV n'est pas activé, la valeur de SriovNetSupport est absente.

Exemple 4 : Dans l'exemple suivant, la prise en charge SR-IOV n'est pas activée.

```
{
    "InstanceId": "i-0c3e84cfa65b04cc8",
    "SriovNetSupport": {}
}
```

4. Mettez l'instance VPX sous tension. Pour voir le statut modifié de l'interface réseau, tapez « show interface summary » dans l'interface de ligne de commande.

   Exemple 5 : La capture d'écran suivante montre les interfaces réseau avec SR-IOV activée. Les interfaces 10/1, 10/2, 10/3 sont activées SR-IOV.

```
> show interface summary
-------------------------------------------------------------------------
      Interface  MTU       MAC                Suffix
-------------------------------------------------------------------------
1     10/1       1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2     10/2       1500      0a:df:17:0a:fe:83  Intel 82599 10G VF Interface
3     10/3       1500      0a:de:5d:31:bf:c3  Intel 82599 10G VF Interface
4     LO/1       1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
 Done
```

Ces étapes complètent la procédure de configuration des instances VPX pour utiliser les interfaces réseau SR-IOV.

Configurer SR-IOV sur une configuration à haute disponibilité

La haute disponibilité est prise en charge par les interfaces SR-IOV à partir de NetScaler version 12.0 build 57.19.

Si la configuration haute disponibilité a été déployée manuellement ou à l'aide du modèle Citrix CloudFormation pour NetScaler version 12.0 56.20 et versions antérieures, le rôle IAM associé à la configuration haute disponibilité doit disposer des privilèges suivants :

- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- autoscaling:*
- SNS : *
- sqs:*

- IAM : Simuler la politique principale
- Je suis : Get Role

Par défaut, le modèle Citrix CloudFormation pour NetScaler version 12.0 57.19 ajoute automatiquement les privilèges requis au rôle IAM.

> **Remarque**
>
> Une configuration haute disponibilité avec interfaces SR-IOV prend environ 100 secondes d'arrêt.

Ressources connexes :

Pour plus d'informations sur les rôles IAM, consultez la documentation AWS.

Configurer une instance NetScaler VPX pour utiliser la mise en réseau améliorée avec AWS ENA

May 5, 2023

Après avoir créé une instance NetScaler VPX sur AWS, vous pouvez configurer l'appliance virtuelle pour utiliser la mise en réseau améliorée avec AWS Elastic Network Adapter (ENA), à l'aide de l'interface de ligne de commande AWS.

Associé à AWS ENA, la mise en réseau améliorée offre une bande passante plus élevée, des performances PPS (paquet par seconde) plus élevées et des latences inter-instances toujours plus faibles.

Avant de commencer la configuration, lisez les rubriques suivantes :

- Composants requis
- Limitations et directives d'utilisation

Les configurations HA suivantes sont prises en charge pour les instances compatibles ENA :

- Les adresses IP privées peuvent être déplacées au sein de la même zone de disponibilité.
- Les adresses IP élastiques peuvent être déplacées entre les zones de disponibilité.

Mettre à niveau une instance NetScaler VPX sur AWS

May 5, 2023

Vous pouvez mettre à niveau le type d'instance EC2, le débit, l'édition logicielle et le logiciel système d'un NetScaler VPX s'exécutant sur AWS. Pour certains types de mises à niveau, Citrix recommande d'utiliser la méthode de configuration haute disponibilité afin de minimiser les temps d'arrêt.

> Remarque :
>
> - La version 10.1.e-124.1308.e ou ultérieure du logiciel NetScaler pour une AMI NetScaler VPX (y compris la licence utilitaire et la licence client) ne prend pas en charge les familles d'instances M1 et M2.
> - En raison des modifications apportées à la prise en charge des instances VPX, la rétrogradation de la version 10.1.e-124 ou d'une version ultérieure vers la version 10.1.123.x ou une version antérieure n'est pas prise en charge.
> - La plupart des mises à niveau ne nécessitent pas le lancement d'une nouvelle AMI et la mise à niveau peut être effectuée sur l'instance NetScaler AMI actuelle. Si vous souhaitez effectuer une mise à niveau vers une nouvelle instance NetScaler AMI, utilisez la méthode de configuration haute disponibilité.

Modifier le type d'instance EC2 d'une instance NetScaler VPX sur AWS

Si vos instances NetScaler VPX exécutent la version 10.1.e-124.1308.e ou ultérieure, vous pouvez modifier le type d'instance EC2 depuis la console AWS comme suit :

1. Arrêtez l'instance VPX.
2. Modifiez le type d'instance EC2 depuis la console AWS.
3. Démarrez l'instance.

Vous pouvez également utiliser la procédure ci-dessus pour modifier le type d'instance EC2 pour une version antérieure à 10.1.e-124.1308.e, sauf si vous souhaitez modifier le type d'instance en M3. Dans ce cas, vous devez d'abord suivre la procédure de mise à niveau standard de NetScaler, à l'adresse, pour mettre à niveau le logiciel NetScaler vers la version 10.1.e-124 ou une version ultérieure, puis suivre les étapes ci-dessus.

Mettre à niveau le débit ou l'édition logicielle d'une instance NetScaler VPX sur AWS

Pour mettre à niveau l'édition logicielle (par exemple, pour passer de l'édition Standard à Premium) ou le débit (par exemple, pour passer de 200 Mbps à 1000 Mbps), la méthode dépend de la licence de l'instance.

Utilisation d'une licence client (Bring-Your-Own-License)

Si vous utilisez une licence client, vous pouvez acheter et télécharger la nouvelle licence sur le site Web de Citrix, puis installer la licence sur l'instance VPX. Pour plus d'informations sur le téléchargement et l'installation d'une licence depuis le site Web de Citrix, consultez le Guide des licences VPX.

Utilisation d'une licence utilitaire (licence utilitaire avec tarif horaire)

AWS ne prend pas en charge les mises à niveau directes pour les instances payantes. Pour mettre à niveau l'édition logicielle ou le débit d'une instance NetScaler VPX payante, lancez une nouvelle AMI avec la licence et la capacité souhaitées et migrez l'ancienne configuration d'instance vers la nouvelle instance. Cela peut être réalisé en utilisant une configuration de haute disponibilité NetScaler, comme décrit dans la section Mettre à niveau vers une nouvelle instance NetScaler AMI en utilisant une sous-section de configuration de haute disponibilité NetScaler sur cette page.

Mettre à niveau le logiciel système d'une instance NetScaler VPX sur AWS

Si vous devez mettre à niveau une instance VPX exécutant la version 10.1.e-124.1308.e ou une version ultérieure, suivez la procédure de mise à niveau standard de NetScaler dans la section Mettre à niveau et rétrograder une appliance NetScaler.

Si vous devez mettre à niveau une instance VPX exécutant une version antérieure à 10.1.e-124.1308.e vers 10.1.e-124.1308.e ou une version ultérieure, mettez d'abord à niveau le logiciel système, puis modifiez le type d'instance en M3 comme suit :

1. Arrêtez l'instance VPX.
2. Modifiez le type d'instance EC2 depuis la console AWS.
3. Démarrez l'instance.

Effectuez une mise à niveau vers une nouvelle instance NetScaler AMI à l'aide d'une configuration NetScaler haute disponibilité

Pour utiliser la méthode de haute disponibilité de mise à niveau vers une nouvelle instance NetScaler AMI, effectuez les tâches suivantes :

- Créez une nouvelle instance avec le type d'instance EC2, l'édition logicielle, le débit ou la version logicielle souhaités sur AWS Marketplace.
- Configurez la haute disponibilité entre l'ancienne instance (à mettre à niveau) et la nouvelle instance. Une fois la haute disponibilité configurée entre l'ancienne et la nouvelle instance, la configuration de l'ancienne instance est synchronisée avec la nouvelle instance.
- Forcez un basculement HA de l'ancienne instance vers la nouvelle instance. Par conséquent, la nouvelle instance devient principale et commence à recevoir du trafic.
- Arrêtez, reconfigurez ou supprimez l'ancienne instance d'AWS.

Prérequis et points à prendre en compte

- Assurez-vous de comprendre comment fonctionne la haute disponibilité entre deux instances NetScaler VPX sur AWS. Pour plus d'informations sur la configuration de haute disponibilité en-

tre deux instances NetScaler VPX sur AWS, consultez Déployer une paire de haute disponibilitésur AWS.

- Vous devez créer la nouvelle instance dans la même zone de disponibilité que l'ancienne instance, avec exactement le même groupe de sécurité et sous-réseau.
- La configuration de haute disponibilité nécessite un accès et des clés secrètes associées au compte AWS Identity and Access Management (IAM) de l'utilisateur pour les deux instances. Si les informations de clé correctes ne sont pas utilisées lors de la création d'instances VPX, la configuration HA échoue. Pour plus d'informations sur la création d'un compte IAM pour une instance VPX, consultez Prérequis.
  - Vous devez utiliser la console EC2 pour créer la nouvelle instance. Vous ne pouvez pas utiliser le lancement d'AWS 1-Click, car il n'accepte pas les clés d'accès et les clés secrètes comme entrée.
  - La nouvelle instance ne doit avoir qu'une seule interface ENI.

Pour mettre à niveau une instance NetScaler VPX à l'aide d'une configuration haute disponibilité, procédez comme suit :

1. Configurez la haute disponibilité entre l'ancienne et la nouvelle instance. Pour configurer la haute disponibilité entre deux instances NetScaler VPX, à l'invite de commande de chaque instance, tapez :

   - `add ha node <nodeID> <IPaddress of the node to be added>`
   - `save config`

   Exemple :

   À l'invite de commande de l'ancienne instance, tapez :

   ```
   1 add ha node 30 192.0.2.30
   2 Done
   3 <!--NeedCopy-->
   ```

   À l'invite de commande de la nouvelle instance, tapez :

   ```
   1 add ha node 10 192.0.2.10
   2 Done
   3 <!--NeedCopy-->
   ```

   Tenez compte de ce qui suit :

   - Dans la configuration HA, l'ancienne instance est le nœud principal et la nouvelle instance est le nœud secondaire.
   - L'adresse IP NSIP n'est pas copiée de l'ancienne instance vers la nouvelle instance. Par conséquent, après la mise à niveau, votre nouvelle instance a une adresse IP de gestion différente de la précédente.

- Le mot de passe du `nsroot` compte de la nouvelle instance est défini sur celui de l'ancienne instance après la synchronisation HA.

Pour plus d'informations sur la configuration de haute disponibilité entre deux instances NetScaler VPX sur AWS, consultez Déployer une paire de haute disponibilitésur AWS.

2. Forcer un basculement HA. Pour forcer un basculement dans une configuration haute disponibilité, à l'invite de commande de l'une des instances, tapez :

```
1 force HA failover
2 <!--NeedCopy-->
```

À la suite du basculement forcé, les ENI de l'ancienne instance sont migrés vers la nouvelle instance et le trafic passe par la nouvelle instance (le nouveau nœud principal). L'ancienne instance (le nouveau nœud secondaire) redémarre.

Si le message d'avertissement suivant s'affiche, tapez N pour annuler l'opération :

```
1 [WARNING]:Force Failover may cause configuration loss, peer health
      not optimum. Reason(s):
2 HA version mismatch
3 HA heartbeats not seen on some interfaces
4 Please confirm whether you want force-failover (Y/N)?
5 <!--NeedCopy-->
```

Le message d'avertissement s'affiche car le logiciel système des deux instances VPX n'est pas compatible HA. Par conséquent, la configuration de l'ancienne instance ne peut pas être automatiquement synchronisée avec la nouvelle instance lors d'un basculement forcé.

Voici la solution à ce problème :

a) À l'invite du shell NetScaler de l'ancienne instance, tapez la commande suivante pour créer une sauvegarde du fichier de configuration (ns.conf) :

```
copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp
```

b) Supprimez la ligne suivante du fichier de configuration de sauvegarde (ns.conf.bkp) :

- `set ns config -IPAddress <IP> -netmask <MASK>`

Par exemple, `set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0`

c) Copiez le fichier de configuration de sauvegarde de l'ancienne instance (ns.conf.bkp) dans le répertoire /nsconfig de la nouvelle instance.

d) À l'invite du shell NetScaler de la nouvelle instance, tapez la commande suivante pour charger le fichier de configuration de l'ancienne instance (ns.conf.bkp) sur la nouvelle instance :

- batch -f /nsconfig/ns.conf.bkp

e) Enregistrez la configuration sur la nouvelle instance.

- save conifg

f) À l'invite de commandes de l'un des nœuds, tapez la commande suivante pour forcer un basculement, puis tapez Y pour le message d'avertissement pour confirmer l'opération de basculement forcé :

- force ha failover

Exemple :

```
1          > force ha failover
2
3  WARNING]:Force Failover may cause configuration loss, peer health
       not optimum.
4          Reason(s):
5          HA version mismatch
6          HA heartbeats not seen on some interfaces
7          Please confirm whether you want force-failover (Y/N)? Y
8  <!--NeedCopy-->
```

3. Supprimez la configuration HA, de sorte que les deux instances ne figurent plus dans une configuration HA. Supprimez d'abord la configuration HA du nœud secondaire, puis supprimez la configuration HA du nœud principal.

   Pour supprimer une configuration HA entre deux instances NetScaler VPX, à l'invite de commande de chaque instance, tapez :

```
1      > remove ha node \<nodeID\>
2      >  save config
3  <!--NeedCopy-->
```

   Pour plus d'informations sur la configuration haute disponibilité entre deux instances VPX sur AWS, voir Déployer une paire haute disponibilité sur AWS.

   Exemple :

À l'invite de commande de l'ancienne instance (nouveau nœud secondaire), tapez :

```
1          > remove ha node 30
2            Done
3          > save config
4            Done
5  <!--NeedCopy-->
```


À l'invite de commande de la nouvelle instance (nouveau nœud principal), tapez :

```
> remove ha node 10
  Done
> save config
  Done
<!--NeedCopy-->
```

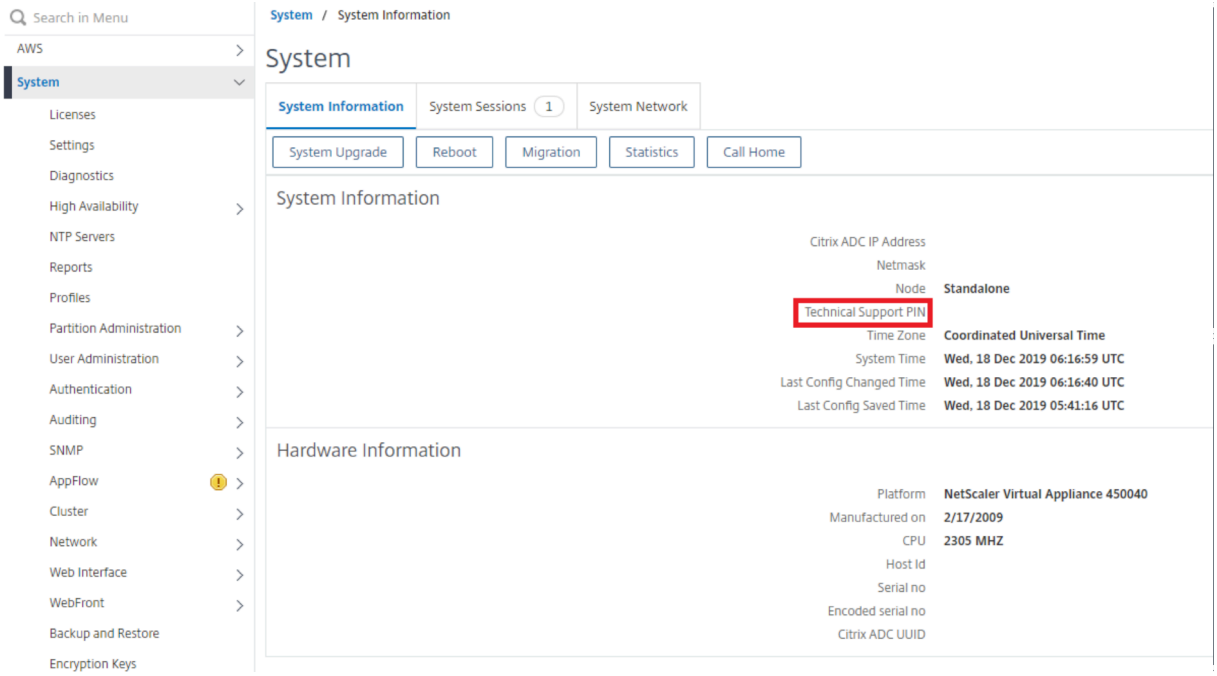
Dépannage d'une instance VPX sur AWS

May 5, 2023

Amazon ne fournit pas d'accès console à une instance NetScaler VPX. Pour résoudre le problème, vous devez utiliser l'interface graphique AWS pour afficher le journal d'activité. Vous ne pouvez déboguer que si le réseau est connecté. Pour afficher le journal système d'une instance, cliquez avec le bouton droit sur l'instance et sélectionnez Journal système.

NetScaler fournit un support pour les instances NetScaler VPX sous licence AWS Marketplace (licence utilitaire avec frais horaires) sur AWS. Pour déposer une demande d'assistance, recherchez votre numéro de compte AWS et votre code PIN d'assistance, puis appelez le support NetScaler. Il vous sera également demandé votre nom et votre adresse e-mail. Pour trouver le code PIN d'assistance, connectez-vous à l'interface graphique VPX et accédez à la page Système.

Voici un exemple de page système montrant le code PIN de support.



FAQ AWS

May 5, 2023

- **Une instance NetScaler VPX prend-elle en charge les volumes chiffrés dans AWS ?**

  Le chiffrement et le déchiffrement s'effectuent au niveau de l'hyperviseur et fonctionnent donc parfaitement avec n'importe quelle instance. Pour plus d'informations sur les volumes chiffrés, consultez le document AWS suivant :

  https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

- **Quel est le meilleur moyen de provisionner une instance NetScaler VPX sur AWS ?**

  Vous pouvez mettre en service une instance NetScaler VPX sur AWS de l'une des manières suivantes :

  - Modèle AWS CloudFormation (CFT) sur AWS Marketplace
  - NetScaler ADM
  - Démarrages rapides AWS
  - CFT Citrix AWS dans GitHub
  - Scripts Citrix Terraform dans GitHub
  - Playbooks Citrix Ansible dans GitHub
  - Workflow de lancement AWS EC2

  Vous pouvez choisir l'une des options répertoriées en fonction de l'outil d'automatisation que vous utilisez.

  Pour plus de détails sur les options, consultez NetScaler VPXsur AWS.

- **Comment mettre à niveau une instance NetScaler VPX dans AWS ?**

  Pour mettre à niveau l'instance NetScaler VPX dans AWS, vous pouvez mettre à niveau le logiciel système ou effectuer une mise à niveau vers une nouvelle Amazon Machine Image (AMI) NetScaler VPX en suivant la procédure décrite dans Mettre à niveau uneinstance NetScaler VPX sur AWS.

  La méthode recommandée pour mettre à niveau une instance NetScaler VPX consiste à utiliser le service ADM en suivant la procédure décrite dans Utiliser des tâches pourmettre à niveau les instances NetScaler.

- **Quel est le délai de basculement en mode HA pour NetScaler VPX dans AWS ?**

  - Le basculement en mode HA de NetScaler VPX dans la zone de disponibilité AWS prend environ 3 secondes.
  - Le basculement en mode HA de NetScaler VPX entre les zones de disponibilité AWS prend environ 5 secondes.

- **Quel niveau de support est fourni aux clients abonnés à NetScaler VPX Marketplace qui fournissent le code PIN du support technique ?**

  Par défaut, le service « Sélectionner pour le logiciel » est fourni aux clients qui fournissent le code PIN du support technique.

- **Dans la haute disponibilité dans différentes zones utilisant le déploiement Elastic IP, devons-nous créer plusieurs IPsets pour chaque application ?**

  Oui. S'il existe plusieurs applications avec plusieurs VIP mappés à plusieurs adresses IP, plusieurs IPsets sont nécessaires. Par conséquent, pendant le basculement HA, tous les mappages VIP principaux des EIP sont remplacés par des VIP secondaires (nouveaux VIP principaux).

- **Pourquoi le mode INC est-il activé en haute disponibilité dans différents déploiements de zones ?**

  Les paires HA dans toutes les zones de disponibilité se trouvent dans différents réseaux. Pour la synchronisation HA, la configuration réseau ne doit pas être synchronisée. Ceci est obtenu en activant le mode INC sur la paire HA.

- **Le nœud HA d'une zone de disponibilité peut-il communiquer avec les serveurs principaux d'une autre zone de disponibilité, à condition que ces zones de disponibilité se trouvent dans le même VPC ?**

  Oui, les sous-réseaux situés dans différentes zones de disponibilité du même VPC sont accessibles en ajoutant un itinéraire supplémentaire pointant vers le sous-réseau du serveur principal via SNIP. Par exemple, si le sous-réseau SNIP d'ADC dans AZ1 est 192.168.3.0/24 et que le sous-réseau du serveur principal dans AZ2 est 192.168.6.0/24, une route doit être ajoutée dans l'appliance NetScaler présente dans AZ1 sous la forme 192.168.6.0 255.255.255.0 192.168.3.1.

- **La haute disponibilité dans différentes zones utilisant Elastic IP et la haute disponibilité dans différentes zones utilisant des déploiements Private IP peut-elle fonctionner ensemble ?**

  Oui, les deux configurations peuvent être appliquées sur la même paire HA.

- **Dans Haute disponibilité dans différentes zones utilisant le déploiement Private IP, s'il existe plusieurs sous-réseaux avec plusieurs tables de routage dans un VPC, comment un nœud secondaire de la paire HA connaît-il la table de routage à vérifier pendant le basculement HA ?**

  Le nœud secondaire connaît les cartes réseau principales et effectue des recherches dans toutes les tables de routage d'un VPC.

- **Quelle est la taille de la `/var` partition lorsque vous utilisez l'image par défaut pour VPX sur AWS ? Comment augmenter l'espace disque ?**

La taille du disque racine est limitée à 20 Go pour garder l'image disque petite.

Si vous souhaitez augmenter l'espace `/var/core/` ou l'espace de `/var/crash/` répertoire, attachez un disque supplémentaire. Pour augmenter la `/var` taille, vous devez actuellement attacher un disque supplémentaire et créer un lien symbolique vers `/var`, après avoir copié le contenu critique sur le nouveau disque.

- **Combien de moteurs de paquets sont activés et alloués aux processeurs virtuels ?**

  Les moteurs de paquets (PE) sont limités par le nombre de processeurs virtuels sous licence. Les démons NetScaler ne sont liés à aucun processeur virtuel en particulier et peuvent s'exécuter sur n'importe quel processeur virtuel autre que PE. Selon AWS, le C5.9XLarge est une instance de 36 processeurs virtuels avec 72 Go de mémoire. Avec les licences groupées, l'instance NetScaler VPX se déploie avec le nombre maximum de PE. Dans ce cas, 19 PE fonctionnent sur les cœurs 1 à 19. Toutefois, les processus de gestion ADC s'exécutent à partir des processeurs 20 à 31.

- **Comment décider de la bonne instance AWS pour ADC ?**

  1. Comprenez votre cas d'utilisation et vos exigences telles que le débit, le PPS, les exigences SSL et la taille moyenne des paquets.
  2. Choisissez l'offre ADC et les licences appropriées qui répondent à vos exigences, telles que les offres de bande passante VPX ou les licences basées sur des processeurs virtuels.
  3. En fonction de l'offre choisie, décidez de l'instance AWS.

  Exemple :

  Une licence de 5 Gbit/s permet 5 moteurs de paquets de données. Par conséquent, l'exigence du processeur virtuel est de 6 (5+1 pour la gestion). Mais l'instance 6 vCPU n'est pas disponible. Un processeur virtuel 8 est donc suffisant pour atteindre ce débit à condition que vous choisissiez un réseau qui prend en charge la bande passante de 5 Gbps. Par exemple, vous devez choisir m5.2xlarge pour une licence de bande passante de 5 Gbps afin d'activer l'allocation PE maximale pour une licence de 5 Gbps. Mais si vous utilisez une licence vCPU qui n'est pas limitée par le débit, vous pouvez obtenir un débit de 5 Gbit/s à l'aide de l'instance m5.xlarge elle-même.

Instance Size	vCPU	Memory (GiB)	Instance Storage (GiB)	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
m5.large	2	8	EBS-Only	Up to 10	Up to 4,750
m5.xlarge	4	16	EBS-Only	Up to 10	Up to 4,750
m5.2xlarge	8	32	EBS-Only	Up to 10	Up to 4,750
m5.4xlarge	16	64	EBS-Only	Up to 10	4,750

- **Le déploiement de trois sous-réseaux NIC et trois sous-réseaux est-il obligatoire pour ADC dans AWS** ?

  `Three NICs-three subnets` est le déploiement recommandé, où chacun est destiné à la

gestion, au réseau client et serveur. Ce déploiement offre une meilleure isolation du trafic et des performances VPX. Deux sous-réseaux NIC, deux et un sous-réseau NIC-One sont les autres options disponibles. Citrix ne recommande pas plusieurs cartes réseau partageant un sous-réseau dans AWS, par exemple deux cartes réseau, un déploiement de sous-réseau. Parce que cela peut entraîner des problèmes de réseau tels que le routage asymétrique. Pour plus d'informations, voir Meilleures pratiques de configuration des interfaces réseau dans AWS.

Déployer une instance NetScaler VPX sur Microsoft Azure

May 5, 2023

Lorsque vous déployez une instance NetScaler VPX sur Microsoft Azure Resource Manager (ARM), vous pouvez utiliser les deux ensembles de fonctionnalités suivants pour répondre aux besoins de votre entreprise :

- Fonctionnalités de cloud computing Azure
- Fonctionnalités d'équilibrage de charge et de gestion du trafic de NetScaler

Vous pouvez déployer des instances NetScaler VPX sur ARM en tant qu'instances autonomes ou en tant que paires haute disponibilité en modes de veille active.

Vous pouvez déployer une instance NetScaler VPX sur Microsoft Azure de deux manières :

- via la Place de marché Azure. L'appliance virtuelle NetScaler VPX est disponible sous forme d'image sur Microsoft Azure Marketplace.
- À l'aide du modèle json NetScaler Azure Resource Manager (ARM) disponible sur GitHub. Pour plus d'informations, consultez le référentiel GitHub pour les modèles de solutions NetScaler.

La pile Microsoft Azure est une plateforme intégrée de matériel et de logiciels qui fournit les services de cloud public Microsoft Azure dans un centre de données local pour permettre aux organisations de construire des clouds hybrides. Vous pouvez désormais déployer les instances NetScaler VPX sur la pile Microsoft Azure.

Conditions préalables

Vous devez disposer de certaines connaissances préalables avant de déployer une instance NetScaler VPX sur Azure.

- Familiarité avec la terminologie Azure et les détails du réseau. Pour plus d'informations, voir Terminologie Azure.
- Connaissance d'une appliance NetScaler. Pour des informations détaillées sur l'appliance NetScaler, voir NetScaler

- Connaissance du réseau NetScaler. Consultez la rubrique Mise en réseau .

Fonctionnement d'une instance NetScaler VPX sur Azure

Dans un déploiement sur site, une instance NetScaler VPX nécessite au moins trois adresses IP :

- Adresse IP de gestion, appelée adresse NSIP
- Adresse IP du sous-réseau (SNIP) pour communiquer avec la batterie de serveurs
- Adresse IP du serveur virtuel (VIP) pour accepter les demandes des clients

Pour plus d'informations, consultez Architecture réseau pour les instances NetScaler VPX sur Microsoft Azure.

> **Remarque**
>
> L'instance NetScaler VPX prend en charge les processeurs Intel et AMD. Les appliances virtuelles VPX peuvent être déployées sur n'importe quel type d'instance doté d'au moins deux cœurs virtualisés et de plus de 2 Go de mémoire. Pour plus d'informations sur la configuration système requise, consultez la fiche technique de NetScaler VPX.

Dans un déploiement Azure, vous pouvez provisionner une instance NetScaler VPX sur Azure de trois manières :

- Architecture multi-NIC Multi-IP
- Architecture multi-IP de carte réseau unique
- Carte d'interface réseau unique, IP unique

En fonction de vos besoins, vous pouvez utiliser n'importe lequel de ces types d'architecture pris en charge.

Architecture multi-NIC Multi-IP

Dans ce type de déploiement, plusieurs interfaces réseau (NIC) peuvent être attachées à une instance VPX. Toute carte réseau peut avoir une ou plusieurs configurations IP (adresses IP publiques et privées statiques ou dynamiques) qui lui sont attribuées.

Pour plus d'informations, consultez les cas d'utilisation suivants :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau
- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell

> Remarque
>
> Pour éviter les déplacements du MAC et les désactivations d'interface dans les environnements Azure, Citrix vous recommande de créer un VLAN par interface de données (sans balise) de

> l'instance NetScaler VPX et de lier l'adresse IP principale de la carte réseau dans Azure. Pour plus d'informations, consultez l'article CTX224626 .

Architecture multi-IP de carte réseau unique

Dans ce type de déploiement, une interface réseau (NIC) associée à plusieurs configurations IP - adresses IP publiques et privées statiques ou dynamiques qui lui sont attribuées.
Pour plus d'informations, consultez les cas d'utilisation suivants :

- Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX
- Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX à l'aide des commandes PowerShell

Carte d'interface réseau unique, IP unique

Dans ce type de déploiement, une interface réseau (NIC) associée à une seule adresse IP, qui est utilisée pour exécuter les fonctions NSIP, SNIP et VIP.

Pour plus d'informations, consultez le cas d'utilisation suivant :

- Configurer une instance autonome NetScaler VPX

> **Remarque**
>
> Le mode IP unique est disponible uniquement dans les déploiements Azure. Ce mode n'est pas disponible pour une instance NetScaler VPX sur site, sur AWS ou dans un autre type de déploiement.

Licence NetScaler VPX

Une instance NetScaler VPX sur Azure nécessite une licence. Les options de licence suivantes sont disponibles pour les instances NetScaler VPX exécutées sur Azure.

- **Licences basées sur un abonnement** : les appliances NetScaler VPX sont disponibles sous forme d'instances payantes sur Azure Marketplace. Les licences par abonnement sont une option de paiement à l'utilisation. Les utilisateurs sont facturés à l'heure.

  > **Remarque**
  >
  > Pour les instances de licence par abonnement, la facturation de votre abonnement s'applique tout au long de la période de licence pour un modèle de licence particulier. En raison des restrictions liées au cloud, Azure ne prend pas en charge la modification ou la suppression du modèle de licence applicable à votre abonnement. Pour modifier ou

> supprimer une licence d'abonnement, supprimez la machine virtuelle ADC existante et recréez une nouvelle machine virtuelle ADC avec la licence souhaitée.

NetScaler fournit un support technique pour les instances de licence par abonnement. Pour déposer un dossier de support, consultez Support pour NetScaler sur Azure — Licence d'abonnement avec prix horaire.

- **Apportez votre propre licence (BYOL)** : Si vous apportez votre propre licence (BYOL), consultez le guide des licences VPX à l'adresse http://support.citrix.com/article/CTX122426. Vous devez :
  - Utilisez le portail de licences du site Web Citrix pour générer une licence valide.
  - Télécharger la licence sur l'instance.

  > **Remarque**
  >
  > Dans un environnement Azure Stack, **BYOL** est la seule option de licence disponible.

- Licence**NetScaler VPX Check-In/Check-Out : pour plus d'informations, consultez la section Licences NetScaler VPX Check-In/Check-Out**.

  À partir de la version 12.0 56.20 de NetScaler, NetScaler VPX Express pour les déploiements sur site et dans le cloud ne nécessite pas de fichier de licence. Pour plus d'informations sur NetScaler VPX Express, consultez la section « Licence NetScaler VPX Express » dans la vue d'ensemble des licences NetScaler.

Les modèles et types de licence VPX suivants sont disponibles sur la Azure Marketplace.

Modèle VPX	Type de licence	Instance recommandée		
		VPX 1 carte réseau/2 cartes réseau	**VPX 3 cartes réseau**	**VPX jusqu'à 8 cartes réseau**
VPX10	Standard, Avancé, Premium	Standard_D2s_v4	Standard_DS3_v2	Standard_DS4_v2
VPX200	Standard, Avancé, Premium	Standard_D2s_v4	Standard_DS3_v2	Standard_DS4_v2
VPX1000	Standard, Avancé, Premium	Standard_D4s_v4	Standard_DS3_v2	Standard_DS4_v2
VPX3000	Standard, Avancé, Premium	Standard_D4s_v4	Standard_D8s_v4	Standard_DS4_v2

Modèle VPX	Type de licence	Instance recommandée		
VPX5000	Standard, Avancé, Premium	Standard_D8s_v4	Standard_D8s_v4	Standard_DS4_v2
VPX8000	Standard, Avancé, Premium	Standard_D8s_v4	Standard_D8s_v4	Standard_DS4_v2
VPX10000	Standard, Avancé, Premium	Standard_D16s_v4	Standard_D16s_v4	Standard_D16s_v4

Points à noter :

- Vous devez activer la mise en réseau accélérée Azure sur les instances NetScaler VPX pour obtenir des performances optimales sur les modèles VPX suivants :
  - VPX1000
  - VPX3000
  - VPX5000
  - VPX8000
  - VPX10000

  Pour plus d'informations sur la configuration de la mise en réseau accélérée, consultez la section Configurer une instance NetScaler VPX pour utiliser la mise en réseau accélérée Azure.
- Les licences VPX8000 et VPX10000 sont disponibles uniquement en tant que BYOL.
- Quelle que soit la licence horaire basée sur un abonnement achetée sur Azure Marketplace, dans de rares cas, l'instance NetScaler VPX déployée sur Azure peut proposer une licence NetScaler par défaut. Cela est dû à des problèmes avec Azure Instance Metadata Service (IMDS).
- Redémarrez à chaud avant de modifier la configuration de l'instance NetScaler VPX pour activer la licence NetScaler VPX appropriée.

Support IPv6 pour l'instance NetScaler VPX dans Azure

À partir de la version 13.1-21.x, l'instance autonome NetScaler VPX prend en charge les adresses IPv6 dans Azure. Vous pouvez configurer les adresses IPv6 en tant qu'adresses VIP et SNIP sur l'instance autonome NetScaler VPX dans le cloud Azure.

Pour plus d'informations sur la façon d'activer IPv6 sur Azure, consultez la documentation Azure suivante :

- Qu'est-ce que IPv6 pour le réseau virtuel Azure ?
- Ajouter IPv6 à une application IPv4 dans le réseau virtuel Azure - Azure CLI
- Types d'adresses

Pour plus d'informations sur la manière dont l'appliance NetScaler prend en charge le protocole IPv6, consultez la version 6 du protocole Internet.

Limites d'IPv6 :

- Les déploiements IPv6 dans NetScaler ne prennent actuellement pas en charge le dimensionnement automatique du backend Azure.
- IPv6 n'est pas pris en charge pour le déploiement de NetScaler VPX HA.

Limitations

L'exécution de la solution d'équilibrage de charge NetScaler VPX sur ARM impose les limites suivantes :

- L'architecture Azure ne prend pas en charge les fonctionnalités NetScaler suivantes :
  - ARP gratuit (GARP)
  - Mode L2
  - VLAN balisé
  - Routage dynamique
  - MAC virtuel
  - USIP
  - Mise en cluster

  > **Remarque :**
  >
  > Grâce à la fonctionnalité Autoscale de NetScaler Application Delivery Management (ADM) (déploiement dans le cloud), les instances ADC prennent en charge le clustering sur toutes les licences. Pour plus d'informations, consultez la section Mise à l'échelle automatique de NetScaler VPX dans Microsoft Azureà l'aide de NetScaler ADM.

- Si vous pensez devoir arrêter et désallouer temporairement la machine virtuelle NetScaler VPX à tout moment, attribuez une adresse IP interne statique lors de la création de la machine virtuelle. Si vous n'attribuez pas d'adresse IP interne statique, Azure peut attribuer à la machine virtuelle une adresse IP différente chaque fois qu'elle redémarre, et la machine virtuelle risque de devenir inaccessible.
- Dans un déploiement Azure, seuls les modèles NetScaler VPX suivants sont pris en charge : VPX 10, VPX 200, VPX 1000, VPX 3000 et VPX 5000. Pour plus d'informations, consultez la fiche technique de NetScaler VPX.

  Si vous utilisez une instance NetScaler VPX dont le numéro de modèle est supérieur à VPX 3000, le débit réseau peut ne pas être le même que celui spécifié par la licence de l'instance. Cepen-

dant, d'autres fonctionnalités telles que le débit SSL et les transactions SSL par seconde peuvent s'améliorer.

- L'ID de déploiement généré par Azure lors du provisionnement de la machine virtuelle n'est pas visible par l'utilisateur dans ARM. Vous ne pouvez pas utiliser l'ID de déploiement pour déployer l'appliance NetScaler VPX sur ARM.
- L'instance NetScaler VPX prend en charge un débit de 20 Mbit/s et des fonctionnalités d'édition standard lors de son initialisation.
- Les instances NetScaler VPX sur Azure avec la mise en réseau accélérée activée offrent de meilleures performances. La mise en réseau accélérée Azure est prise en charge sur les instances NetScaler VPX à partir de la version 13.0 build 76.x. Pour activer la mise en réseau accélérée sur NetScaler VPX, Citrix vous recommande d'utiliser un type d'instance Azure qui prend en charge la mise en réseau accélérée.
- Pour le déploiement de Citrix Virtual Apps and Desktops, un serveur virtuel VPN sur une instance VPX peut être configuré dans les modes suivants :
  - Mode de base, où le paramètre du serveur virtuel `ICAOnly` VPN est défini sur ON. Le mode Basic fonctionne pleinement sur une instance NetScaler VPX sans licence.
  - Mode SmartAccess, où le paramètre du serveur virtuel `ICAOnly` VPN est défini sur OFF. Le mode SmartAccess ne fonctionne que pour cinq utilisateurs de session NetScaler AAA sur une instance NetScaler VPX sans licence.

> **Remarque :**
>
> Pour configurer la fonctionnalité SmartControl, vous devez appliquer une licence Premium à l'instance NetScaler VPX.

Terminologie Azure

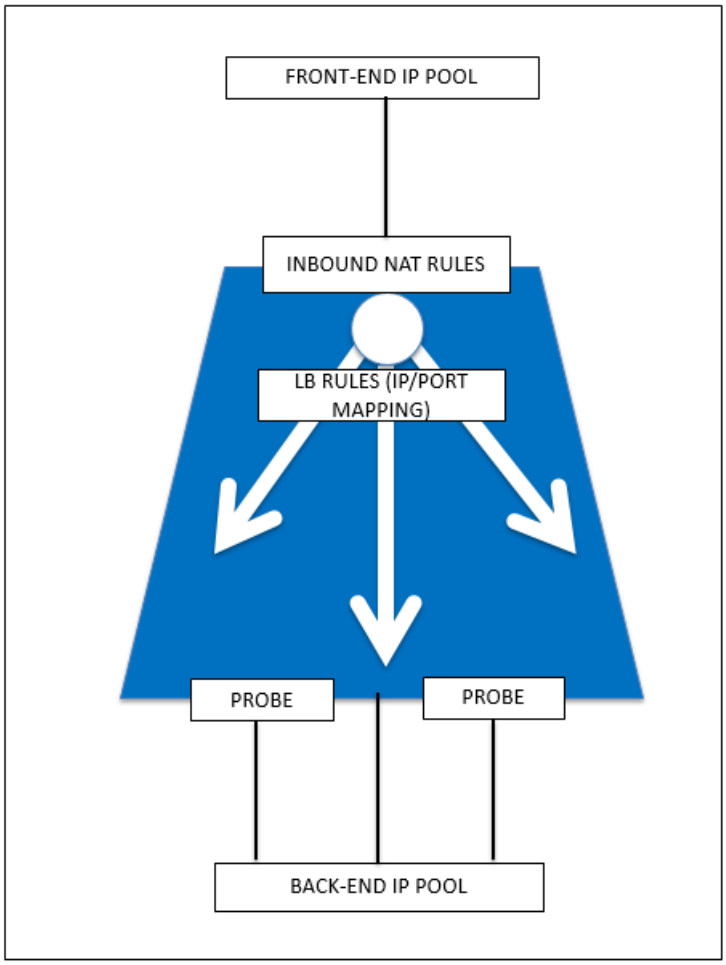
May 5, 2023

Certains des termes Azure utilisés dans la documentation Azure de NetScaler VPX sont répertoriés ci-dessous.

1. Azure Load Balancer — L'équilibreur de charge Azure est une ressource qui distribue le trafic entrant entre les ordinateurs d'un réseau. Le trafic est réparti entre les machines virtuelles définies dans un ensemble d'équilibreurs de charge. Un équilibreur de charge peut être externe ou connecté à Internet, ou il peut être interne.
2. Azure Resource Manager (ARM) — ARM est le nouveau framework de gestion des services dans Azure. Azure Load Balancer est géré à l'aide d'API et d'outils ARM.

3. Pool d'adresses back-end : il s'agit d'adresses IP associées à la carte réseau (NIC) de la machine virtuelle vers laquelle la charge sera distribuée.
4. BLOB - Binary Large Object — Tout objet binaire tel qu'un fichier ou une image qui peut être stocké dans le stockage Azure.
5. Configuration IP frontale : un équilibreur de charge Azure peut inclure une ou plusieurs adresses IP frontales, également appelées adresses IP virtuelles (VIP). Ces adresses IP servent d'entrée pour le trafic.
6. IP publique au niveau de l'instance (ILPIP) : une ILPIP est une adresse IP publique que vous pouvez attribuer directement à votre machine virtuelle ou à votre instance de rôle, plutôt qu'au service cloud dans lequel réside votre machine virtuelle ou votre instance de rôle. Cela ne remplace pas le VIP (IP virtuelle) attribué à votre service cloud. Il s'agit plutôt d'une adresse IP supplémentaire que vous pouvez utiliser pour vous connecter directement à votre machine virtuelle ou instance de rôle.

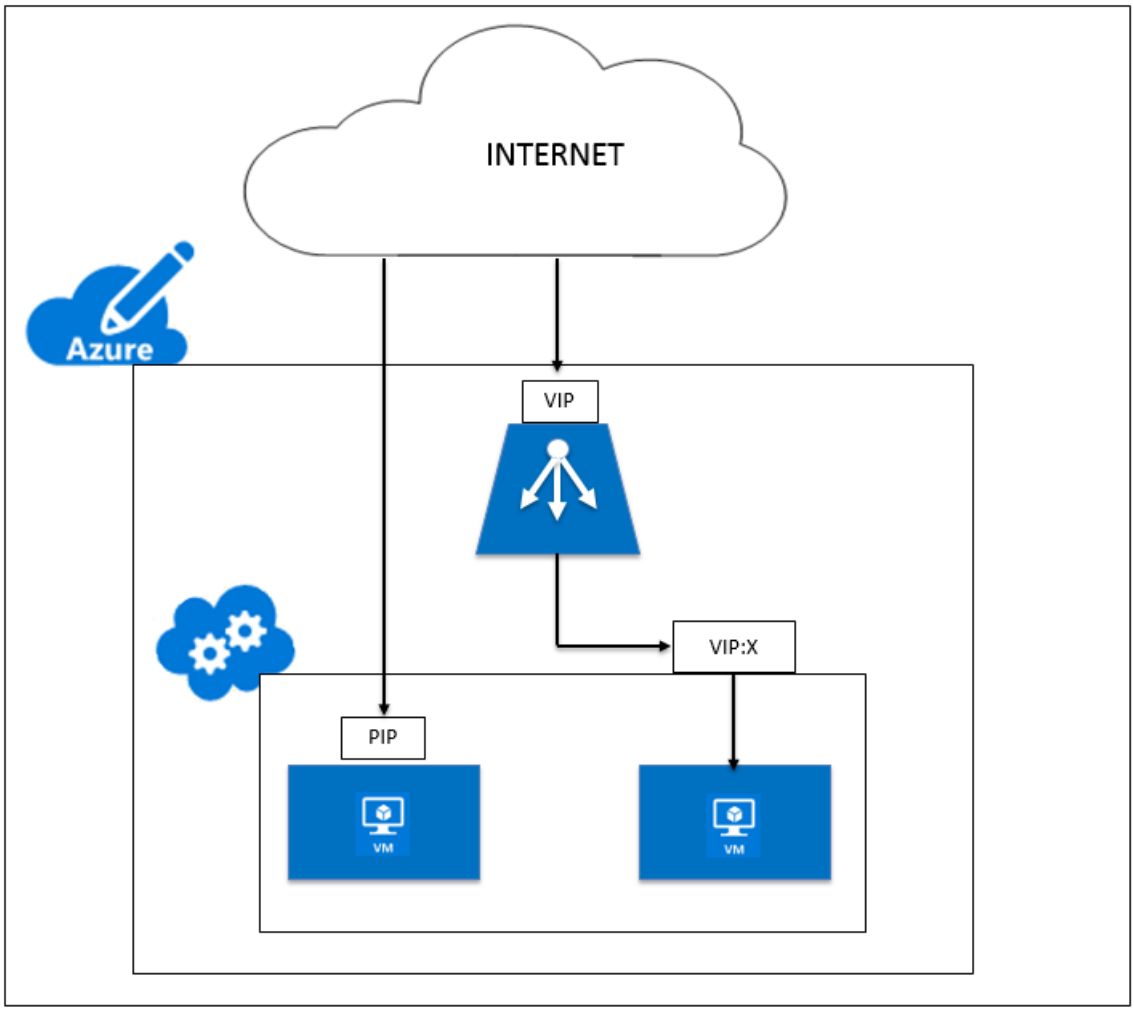
   Note : Dans le passé, unILPIP était appelé PIP, qui signifie PI publique.
7. Règles NAT entrantes : elles contiennent des règles mappant un port public sur l'équilibreur de charge à un port pour une machine virtuelle spécifique dans le pool d'adresses principal.
8. IP-Config - Il peut être défini comme une paire d'adresses IP (IP publique et IP privée) associée à une carte réseau individuelle. Dans une configuration IP, l'adresse IP publique peut être NULL. Chaque carte réseau peut être associée à plusieurs configurations IP, qui peuvent atteindre 255.
9. Règles d'équilibrage de charge : propriété de règle qui mappe une combinaison IP et port frontaux donnée à un ensemble d'adresses IP et de combinaisons de ports back-end. Avec une définition unique d'une ressource d'équilibrage de charge, vous pouvez définir plusieurs règles d'équilibrage de charge, chaque règle reflétant une combinaison d'une adresse IP et d'un port frontaux et d'une adresse IP principale et d'un port associés aux machines virtuelles.



10. Groupe de sécurité réseau : contient une liste de règles de liste de contrôle d'accès (ACL) qui autorisent ou refusent le trafic réseau vers vos instances de machine virtuelle dans un réseau virtuel. Les NSG peuvent être associés à des sous-réseaux ou à des instances de machine virtuelle individuelles au sein de ce sous-réseau. Lorsqu'un groupe de sécurité réseau est associé à un sous-réseau, les règles ACL s'appliquent à toutes les instances de machines virtuelles de ce sous-réseau. En outre, le trafic vers une machine virtuelle individuelle peut être restreint davantage en associant un groupe de sécurité réseau directement à cette machine virtuelle.
11. Adresses IP privées — Utilisées pour la communication au sein d'un réseau virtuel Azure et de votre réseau local lorsque vous utilisez une Gateway VPN pour étendre votre réseau à Azure. Les adresses IP privées permettent aux ressources Azure de communiquer avec d'autres ressources dans un réseau virtuel ou un réseau local via une Gateway VPN ou un circuit ExpressRoute, sans utiliser d'adresse IP accessible par Internet. Dans le modèle de déploiement Azure Resource Manager, une adresse IP privée est associée aux types de ressources Azure suivants : machines virtuelles, équilibreurs de charge internes (ILB) et passerelles d'application.
12. Sondes : elles contiennent des sondes d'intégrité utilisées pour vérifier la disponibilité des in-

stances de machines virtuelles dans le pool d'adresses principal. Si une machine virtuelle particulière ne répond pas aux sondes d'intégrité pendant un certain temps, elle est retirée du service de trafic. Les sondes vous permettent de suivre l'état de santé des instances virtuelles. En cas d'échec d'une sonde de santé, l'instance virtuelle sera automatiquement retirée de la rotation.

13. Adresses IP publiques (PIP) : PIP est utilisé pour la communication avec Internet, y compris les services publics Azure et est associé aux machines virtuelles, aux équilibreurs de charge connectés à Internet, aux passerelles VPN et aux passerelles d'application.
14. Région - Zone au sein d'une géographie qui ne franchit pas les frontières nationales et qui contient un ou plusieurs centres de données. Les tarifs, les services régionaux et les types d'offres sont exposés au niveau régional. Une région est généralement associée à une autre région, qui peut être distante de plusieurs centaines de kilomètres, pour former une paire régionale. Les paires régionales peuvent être utilisées comme mécanisme pour les scénarios de reprise après sinistre et de haute disponibilité. Aussi appelé généralement lieu.
15. Groupe de ressources : un conteneur du Gestionnaire de ressources contient les ressources associées à une application. Le groupe de ressources peut inclure toutes les ressources d'une application ou uniquement les ressources qui sont regroupées de manière logique
16. Compte de stockage : un compte de stockage Azure vous donne accès au blob, à la file d'attente, à la table et aux services de fichiers Azure dans Azure Storage. Votre compte de stockage fournit l'espace de noms unique pour vos objets de données de stockage Azure.
17. Machine virtuelle : implémentation logicielle d'un ordinateur physique qui exécute un système d'exploitation. Plusieurs machines virtuelles peuvent s'exécuter simultanément sur le même matériel. Dans Azure, les machines virtuelles sont disponibles dans différentes tailles.
18. Réseau virtuel : un réseau virtuel Azure est une représentation de votre propre réseau dans le cloud. Il s'agit d'une isolation logique du cloud Azure dédié à votre abonnement. Vous pouvez contrôler entièrement les blocs d'adresses IP, les paramètres DNS, les politiques de sécurité et les tables de routage au sein de ce réseau. Vous pouvez également segmenter davantage votre réseau virtuel en sous-réseaux et lancer des machines virtuelles Azure IaaS et des services cloud (instances de rôle PaaS). En outre, vous pouvez connecter le réseau virtuel à votre réseau local à l'aide de l'une des options de connectivité disponibles dans Azure. Essentiellement, vous pouvez étendre votre réseau à Azure, avec un contrôle complet sur les blocs d'adresses IP avec l'avantage d'Azure à l'échelle de l'entreprise.



Architecture réseau pour les instances NetScaler VPX sur Microsoft Azure

May 5, 2023

Dans Azure Resource Manager (ARM), une machine virtuelle (VM) NetScaler VPX réside dans un réseau virtuel. Une interface réseau unique peut être créée dans un sous-réseau donné du réseau virtuel et peut être attachée à l'instance VPX. Vous pouvez filtrer le trafic réseau à destination et en provenance d'une instance VPX dans un réseau virtuel Azure avec un groupe de sécurité réseau. Un groupe de sécurité réseau contient des règles de sécurité qui autorisent ou refusent le trafic réseau entrant vers ou le trafic réseau sortant à partir d'une instance VPX. Pour plus d'informations, voir Groupes de sécurité.

Le groupe de sécurité réseau filtre les demandes adressées à l'instance NetScaler VPX, qui les envoie aux serveurs. La réponse d'un serveur suit le même chemin à l'envers. Le groupe de sécurité

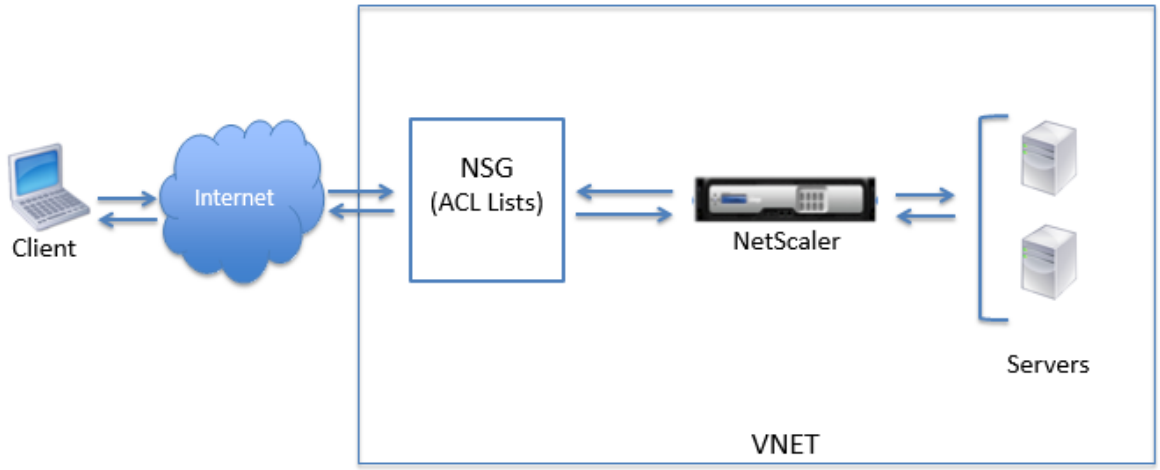
réseau peut être configuré pour filtrer une seule machine virtuelle VPX ou, avec des sous-réseaux et des réseaux virtuels, pour filtrer le trafic lors du déploiement de plusieurs instances VPX.

La carte réseau contient des détails de configuration réseau tels que le réseau virtuel, les sous-réseaux, l'adresse IP interne et l'adresse IP publique.

Sur ARM, il est bon de connaître les adresses IP suivantes qui sont utilisées pour accéder aux machines virtuelles déployées avec une seule carte réseau et une seule adresse IP :

- L'adresse IP publique (PIP) est l'adresse IP connectée à Internet configurée directement sur la carte réseau virtuelle de la machine virtuelle NetScaler. Cela vous permet d'accéder directement à une machine virtuelle à partir du réseau externe.
- L'adresse IP NetScaler (également appelée NSIP) est l'adresse IP interne configurée sur la machine virtuelle. Il n'est pas routable.
- L'adresse IP virtuelle (VIP) est configurée à l'aide du NSIP et d'un numéro de port. Les clients accèdent aux services NetScaler via l'adresse PIP, et lorsque la demande parvient à la carte réseau de la machine virtuelle NetScaler VPX ou à l'équilibreur de charge Azure, le VIP est traduit en adresse IP interne (NSIP) et en numéro de port interne.
- L'adresse IP interne est l'adresse IP interne privée de la machine virtuelle issue du pool d'espaces d'adressage du réseau virtuel. Cette adresse IP ne peut pas être atteinte à partir du réseau externe. Cette adresse IP est dynamique par défaut, sauf si vous la définissez sur statique. Le trafic d'Internet est acheminé vers cette adresse selon les règles créées sur le groupe de sécurité réseau. Le groupe de sécurité réseau s'intègre à la carte réseau pour envoyer de manière sélective le bon type de trafic vers le bon port de la carte réseau, qui dépend des services configurés sur la machine virtuelle.

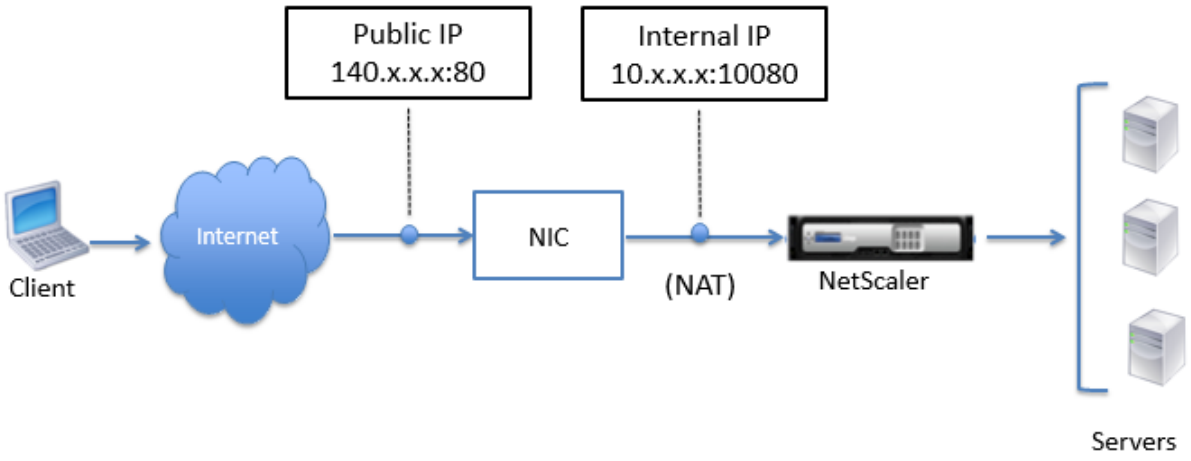
La figure suivante montre comment le trafic circule d'un client vers un serveur via une instance NetScaler VPX provisionnée dans ARM.



Flux de trafic via la traduction d'adresses réseau

Vous pouvez également demander une adresse IP publique (PIP) pour votre instance NetScaler VPX (niveau instance). Si vous utilisez ce PIP direct au niveau de la machine virtuelle, il n'est pas nécessaire de définir des règles entrantes et sortantes pour intercepter le trafic réseau. La demande entrante provenant d'Internet est reçue directement sur la machine virtuelle. Azure effectue la traduction d'adresses réseau (NAT) et transfère le trafic vers l'adresse IP interne de l'instance VPX.

La figure suivante montre comment Azure effectue la traduction des adresses réseau pour mapper l'adresse IP interne de NetScaler.



Dans cet exemple, l'adresse IP publique attribuée au groupe de sécurité réseau est 140.x.x.x et l'adresse IP interne est 10.x.x.x. Lorsque les règles entrantes et sortantes sont définies, le port HTTP public 80 est défini comme le port sur lequel les demandes du client sont reçues, et le port privé correspondant, 10080, est défini comme le port sur lequel l'instance NetScaler VPX écoute. La demande du client est reçue sur l'adresse IP publique (140.x.x.x). Azure effectue la traduction des adresses réseau pour mapper le PIP à l'adresse IP interne 10.x.x.x sur le port 10080 et transmet la demande du client.

> **Remarque**
>
> Les machines virtuelles NetScaler VPX en haute disponibilité sont contrôlées par des équilibreurs de charge externes ou internes sur lesquels des règles entrantes sont définies pour contrôler le trafic d'équilibrage de charge. Le trafic externe est d'abord intercepté par ces équilibreurs de charge et le trafic est détourné conformément aux règles d'équilibrage de charge configurées, qui comportent des pools dorsaux, des règles NAT et des sondes de santé définis sur les équilibreurs de charge.

Instructions relatives à l'utilisation des ports

Vous pouvez configurer davantage de règles entrantes et sortantes dans un groupe de sécurité réseau lors de la création de l'instance NetScaler VPX ou après le provisionnement de la machine virtuelle. Chaque règle entrante et sortante est associée à un port public et à un port privé.

Avant de configurer les règles de groupe de sécurité réseau, notez les instructions suivantes concernant les numéros de port que vous pouvez utiliser :

1. L'instance NetScaler VPX réserve les ports suivants. Vous ne pouvez pas les définir comme des ports privés lorsque vous utilisez l'adresse IP publique pour des requêtes provenant d'Internet.

   Ports 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   Toutefois, si vous souhaitez que les services Internet tels que le VIP utilisent un port standard (par exemple, le port 443), vous devez créer un mappage de ports à l'aide du groupe de sécurité réseau. Le port standard est ensuite mappé à un autre port configuré sur NetScaler pour ce service VIP.

   Par exemple, un service VIP peut s'exécuter sur le port 8443 sur l'instance VPX mais être mappé sur le port public 443. Ainsi, lorsque l'utilisateur accède au port 443 via l'IP publique, la requête est dirigée vers le port privé 8443.
2. L'adresse IP publique ne prend pas en charge les protocoles dans lesquels le mappage des ports est ouvert de manière dynamique, tels que le FTP passif ou l'ALG.
3. La haute disponibilité ne fonctionne pas pour le trafic qui utilise une adresse IP publique (PIP) associée à une instance VPX, au lieu d'un PIP configuré sur l'équilibreur de charge Azure.

> **Remarque**
>
> Dans Azure Resource Manager, une instance NetScaler VPX est associée à deux adresses IP : une adresse IP publique (PIP) et une adresse IP interne. Pendant que le trafic externe se connecte au PIP, l'adresse IP interne ou le NSIP n'est pas routable. Pour configurer VIP dans VPX, utilisez l'adresse IP interne et l'un des ports libres disponibles. N'utilisez pas le PIP pour configurer VIP.

Configurer une instance autonome NetScaler VPX

May 8, 2023

Vous pouvez provisionner une seule instance NetScaler VPX dans le portail Azure Resource Manager (ARM) en mode autonome en créant la machine virtuelle et en configurant d'autres ressources.

Avant de commencer

Assurez-vous que vous disposez des éléments suivants :

- Un compte d'utilisateur Microsoft Azure
- Accès au Gestionnaire de ressources Microsoft Azure
- Kit de développement logiciel Microsoft Azure
- Microsoft Azure PowerShell

Sur la page Microsoft Azure Portal, connectez-vous au portail Azure Resource Manager en fournissant votre nom d'utilisateur et votre mot de passe.

> **Remarque**
>
> Dans le portail ARM, le fait de cliquer sur une option dans un volet ouvre un nouveau volet sur la droite. Naviguez d'un volet à l'autre pour configurer votre appareil.

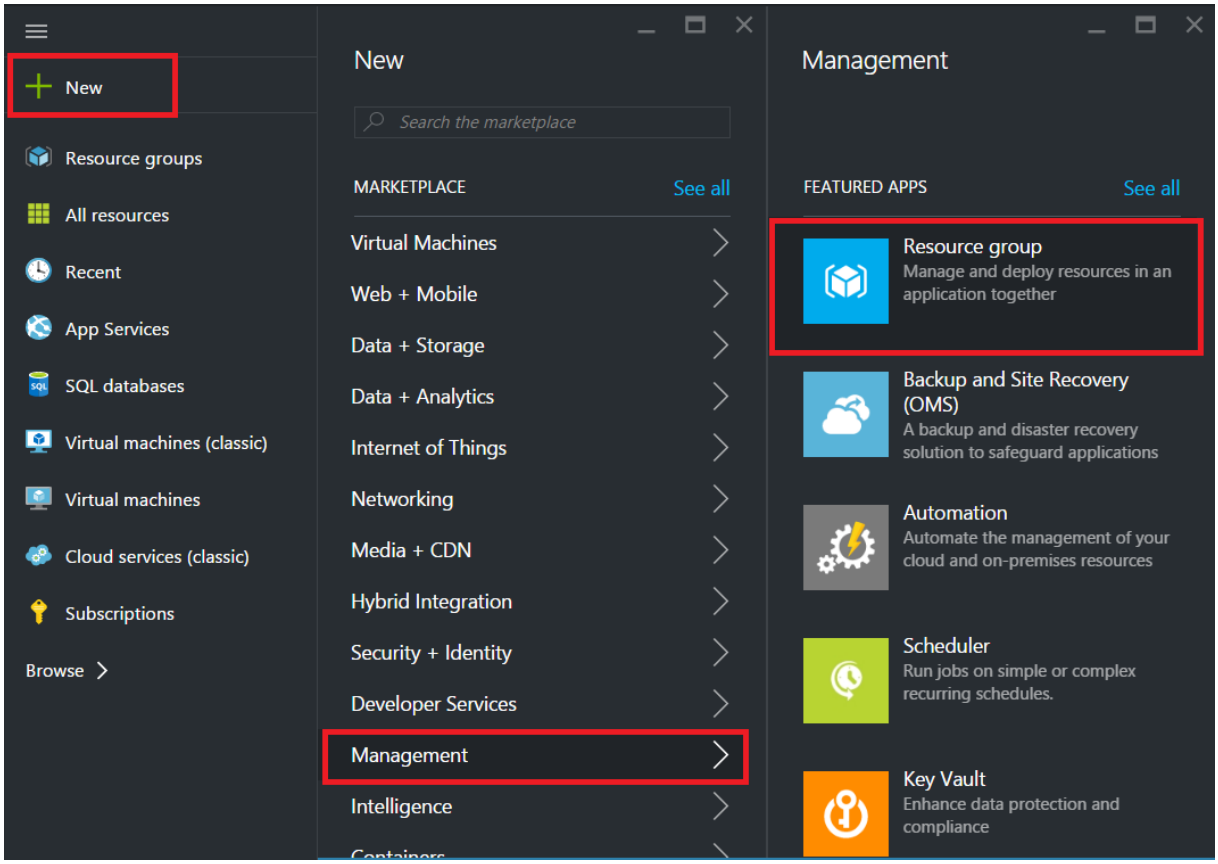
Résumé des étapes de configuration

1. Configuration d'un groupe de ressources
2. Configurer un groupe de sécurité réseau
3. Configuration du réseau virtuel et de ses sous-réseaux
4. Configurer un compte de stockage
5. Configurer un jeu de disponibilité
6. Configurez une instance NetScaler VPX.

Configuration d'un groupe de ressources

Créez un nouveau groupe de ressources qui est un conteneur pour toutes vos ressources. Utilisez le groupe de ressources pour déployer, gérer et surveiller vos ressources en tant que groupe.

1. Cliquez sur **Nouveau** > **Gestion** > **Groupe de ressources**.
2. Dans le volet **Groupe de ressources**, entrez les informations suivantes :
    - Nom du groupe de ressources
    - Emplacement du groupe de ressources
3. Cliquez sur **Create**.

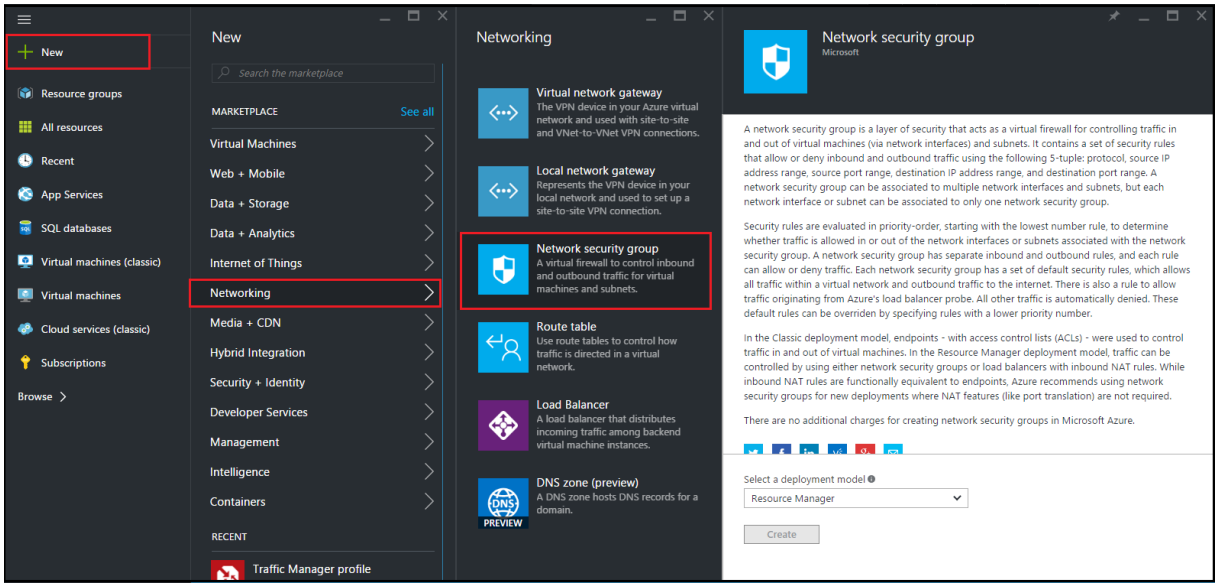


Configurer un groupe de sécurité réseau

Créez un groupe de sécurité réseau pour affecter des règles entrantes et sortantes pour contrôler le trafic entrant et sortant au sein du réseau virtuel. Le groupe de sécurité réseau vous permet de définir des règles de sécurité pour une seule machine virtuelle et de définir des règles de sécurité pour un sous-réseau virtuel.

1. Cliquez sur **Nouveau** > **Mise enréseau > Groupe de sécurité réseau** .
2. Dans le volet **Créer un groupe de sécurité réseau**, entrez les informations suivantes, puis cliquez sur **Créer**.
    - Nom : entrez le nom du groupe de sécurité
    - Groupe de ressources : sélectionnez le groupe de ressources dans la liste déroulante

> **Remarque**
>
> Assurez-vous d'avoir sélectionné le bon emplacement. La liste des ressources qui apparaissent dans la liste déroulante est différente selon les emplacements.

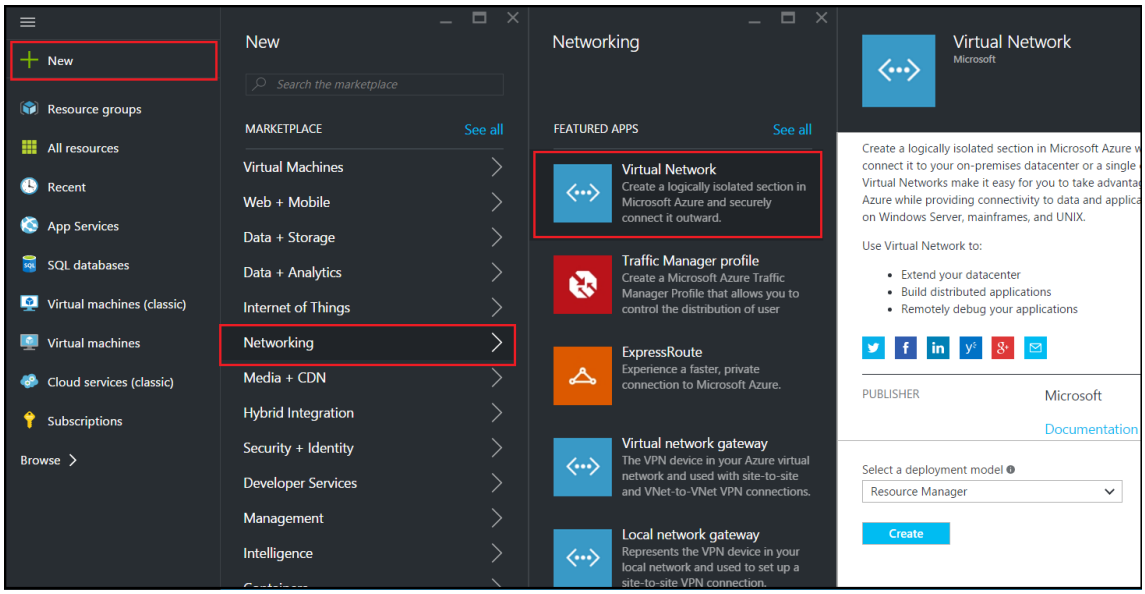


Configurer un réseau virtuel et des sous-réseaux

Les réseaux virtuels d'ARM fournissent un niveau de sécurité et d'isolation à vos services. Les machines virtuelles et les services qui font partie du même réseau virtuel peuvent accéder les uns aux autres.

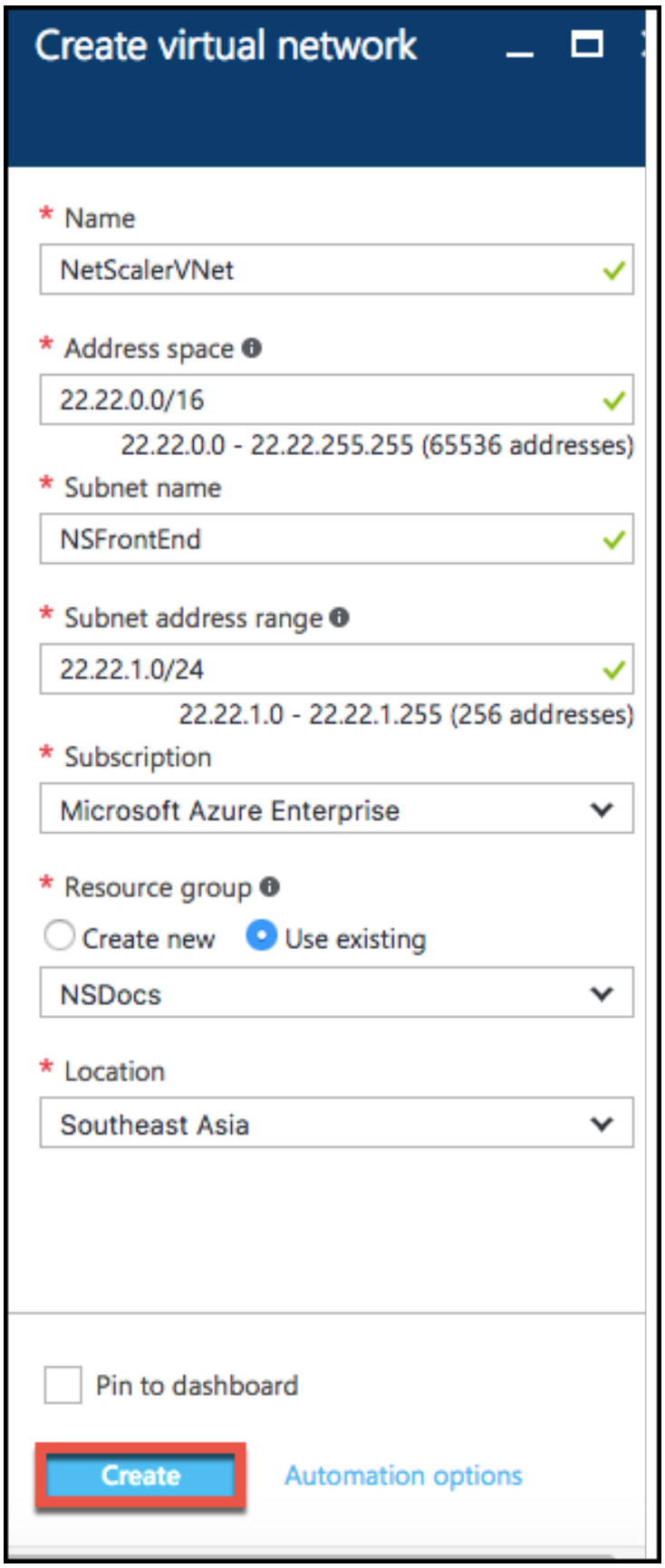
Pour suivre ces étapes pour créer un réseau virtuel et des sous-réseaux.

1. Cliquez sur **Nouveau** > **Réseau** > **Réseau virtuel**.
2. Dans le volet **Réseau virtuel**, assurez-vous que le mode de déploiement est **Gestionnaire de ressources** et cliquez sur **Créer**.



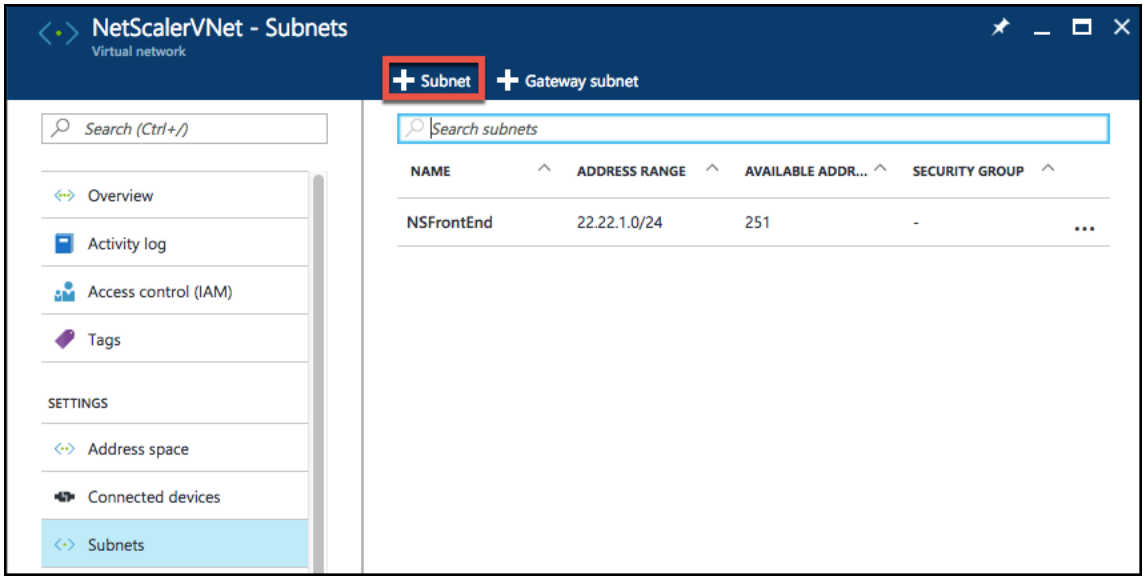
3. Dans le volet **Créer un réseau virtuel**, entrez les valeurs suivantes, puis cliquez sur **Créer** .

- Nom du réseau virtuel
- Espace d'adressage : saisissez le bloc d'adresses IP réservé pour le réseau virtuel
- Sous-réseau : saisissez le nom du premier sous-réseau (vous créerez le second sous-réseau plus tard dans cette étape)
- Plage d'adresses de sous-réseau : saisissez le bloc d'adresses IP réservé du sous-réseau
- Groupe de ressources : sélectionnez le groupe de ressources créé précédemment dans la liste déroulante

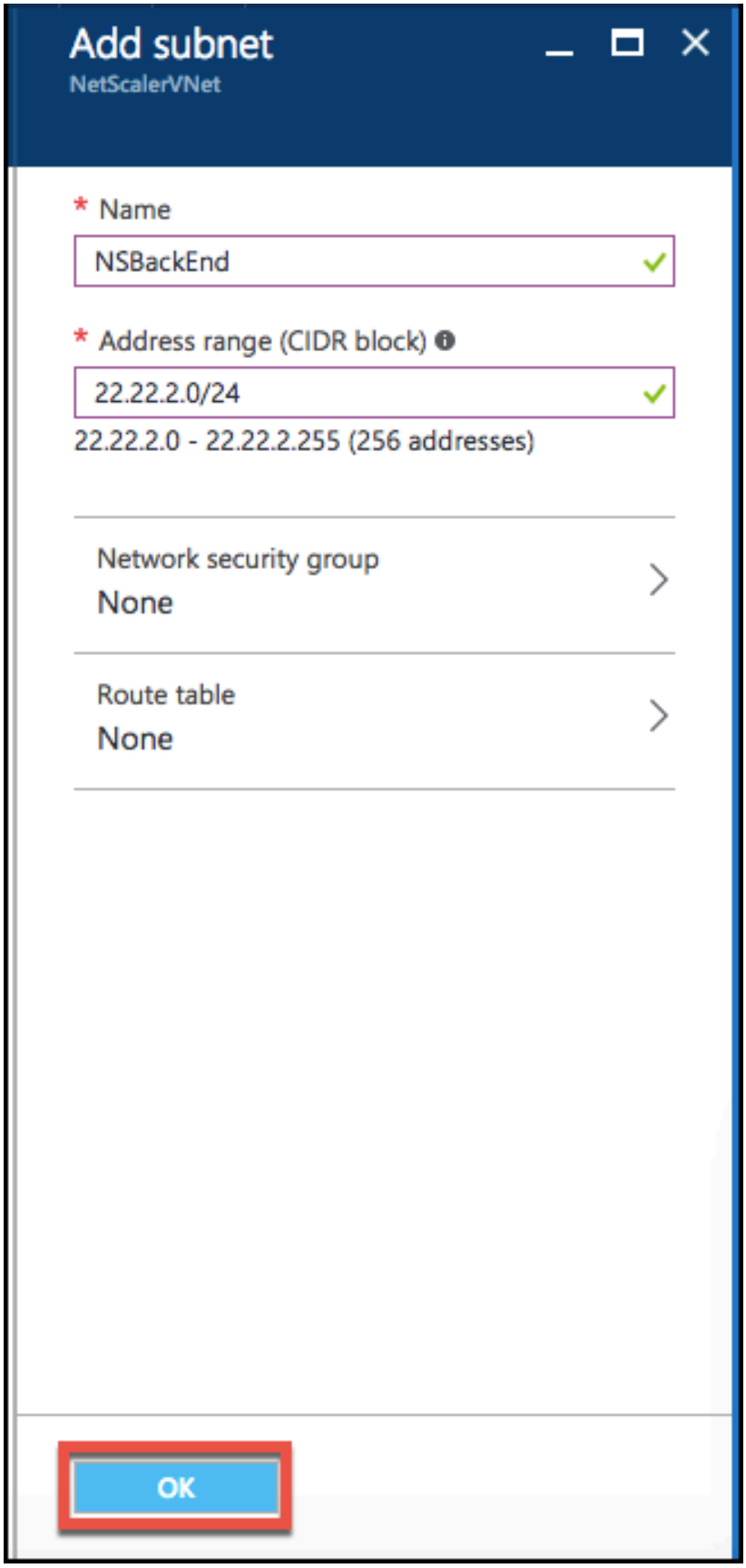


Configurer le deuxième sous-réseau

1. Sélectionnez le réseau virtuel nouvellement créé dans le volet **Toutes les ressources** et dans le volet **Paramètres**, cliquez sur **Sous-réseaux** .



2. Cliquez sur **+ Sous-réseau** et créez le second sous-réseau en entrant les détails suivants.
   - Nom du deuxième sous-réseau
   - Plage d'adresses - tapez le bloc d'adresse IP réservé du deuxième sous-réseau
   - Groupe de sécurité réseau : sélectionnez le groupe de sécurité réseau dans la liste déroulante.
3. Cliquez sur **Create**.

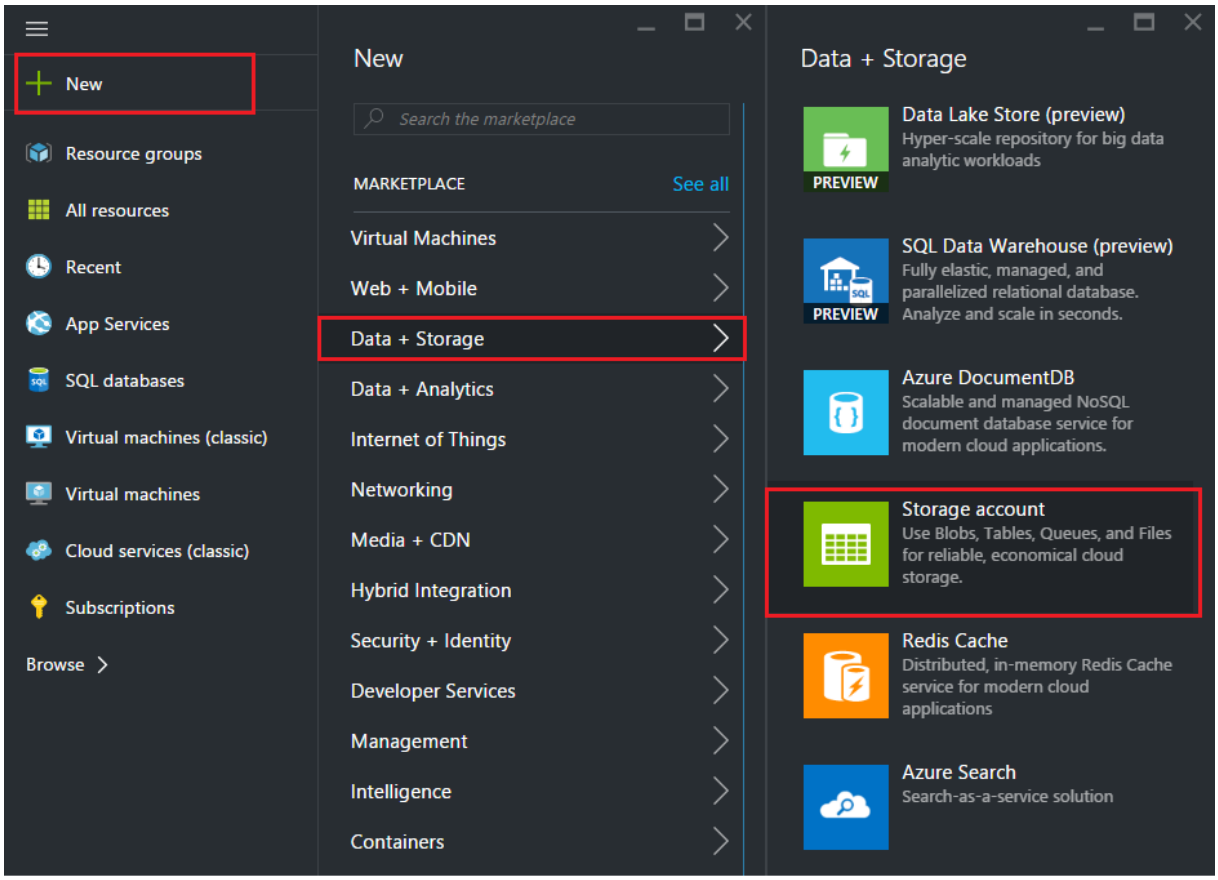


Configurer un compte de stockage

L'infrastructure de stockage ARM IaaS inclut tous les services dans lesquels nous pouvons stocker des données sous forme de blobs, de tables, de files d'attente et de fichiers. Vous pouvez également créer des applications à l'aide de ces formes de données de stockage dans ARM.

Créez un compte de stockage pour stocker toutes vos données.

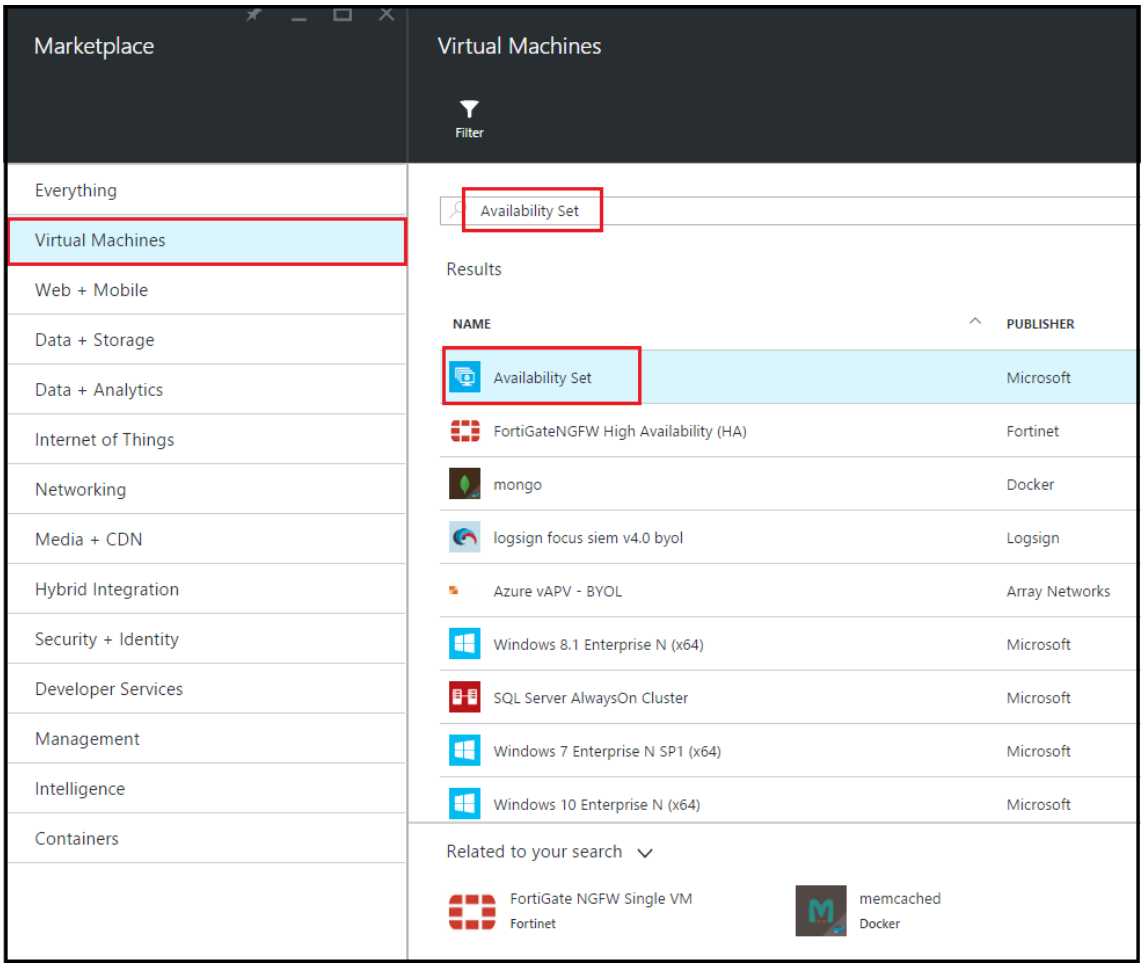
1. Cliquez sur **+Nouveau** > **Données + Stockage** > **Compte de stockage.**
2. Dans le volet **Créer un compte de stockage**, entrez les informations suivantes :
    - Nom du compte
    - Mode de déploiement : assurez-vous de sélectionner **Resource Manager**
    - Type de compte : sélectionnez **Usage général** dans la liste déroulante
    - Réplication : sélectionnez **Stockage localement redondant** dans la liste déroulante
    - Groupe de ressources : sélectionnez le groupe de ressources nouvellement créé dans la liste déroulante
3. Cliquez sur **Create**.



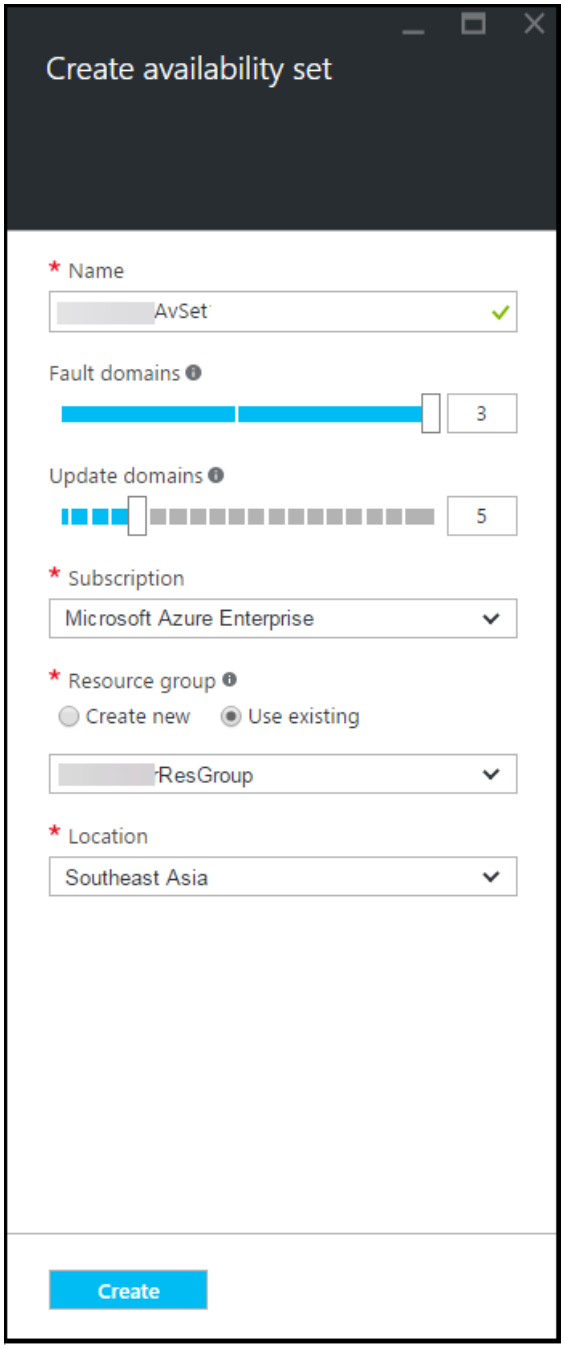
Configurer un jeu de disponibilité

Un ensemble de disponibilité garantit qu'au moins une machine virtuelle reste opérationnelle en cas de maintenance planifiée ou imprévue. Deux machines virtuelles ou plus appartenant au même « ensemble de disponibilité » sont placées sur des domaines de défaillance différents pour fournir des services redondants.

1. Cliquez sur **+Nouveau**.
2. Cliquez sur **Tout afficher** dans le volet MARKETPLACE, puis sur **Machines virtuelles**.
3. Recherchez le jeu de disponibilité, puis sélectionnez Entité de **jeu de disponibilité** dans la liste affichée.



4. Cliquez sur **Créer et,** dans le volet **Créer un jeu de disponibilité**, entrez les détails suivants :
   - Nom du set
   - Groupe de ressources : sélectionnez le groupe de ressources nouvellement créé dans la liste déroulante
5. Cliquez sur **Create**.



Configuration d'une instance NetScaler VPX

Créez une instance de NetScaler VPX dans le réseau virtuel. Obtenez l'image NetScaler VPX sur Azure Marketplace, puis utilisez le portail Azure Resource Manager pour créer une instance NetScaler VPX.

Avant de commencer à créer l'instance NetScaler VPX, assurez-vous d'avoir créé un réseau virtuel avec les sous-réseaux requis dans lesquels l'instance réside. Vous pouvez créer des réseaux virtuels pendant le provisioning de machines virtuelles, mais sans la possibilité de créer différents sous-réseaux.

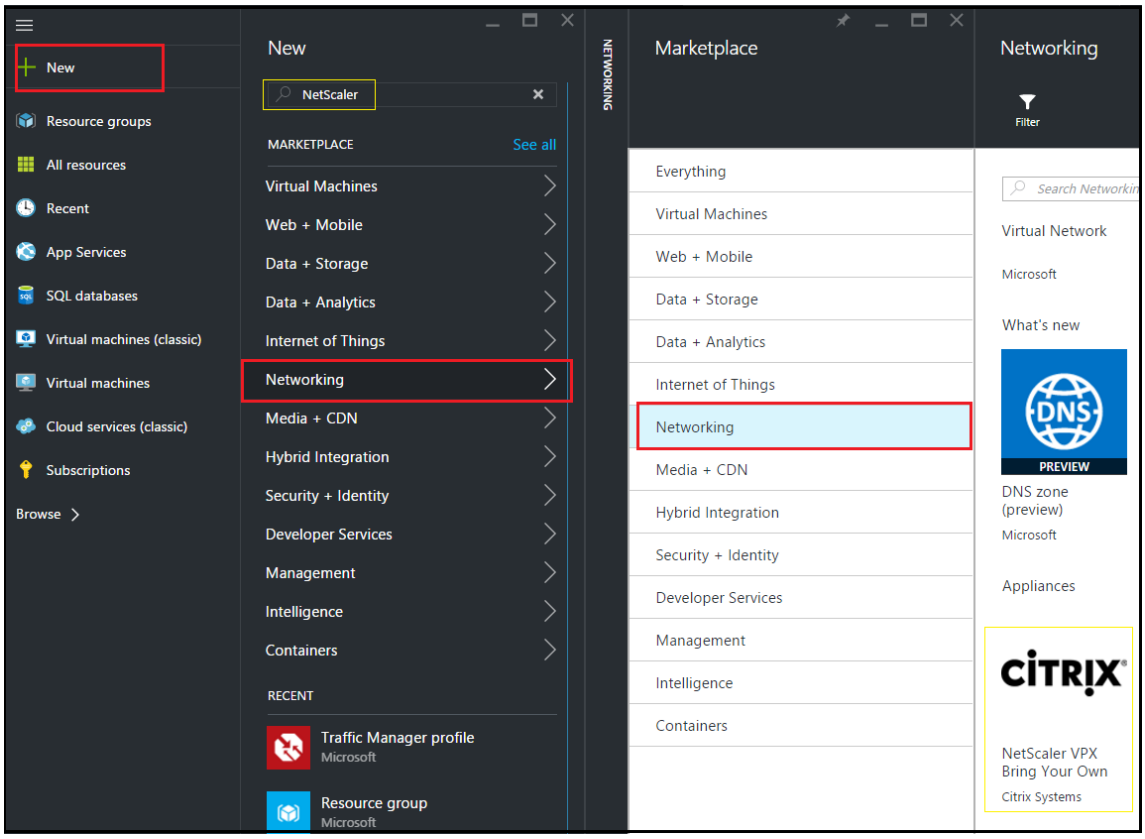
Pour plus d'informations sur la création de réseaux virtuels, consultez http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/.

Configurez éventuellement la connectivité du serveur DNS et du VPN pour permettre à une machine virtuelle d'accéder aux ressources Internet.

> **Remarque**
>
> Citrix vous recommande de créer un groupe de ressources, un groupe de sécurité réseau, un réseau virtuel et d'autres entités avant de provisionner la machine virtuelle NetScaler VPX, afin que les informations réseau soient disponibles lors du provisionnement.

1. Cliquez sur **+Nouveau** > **Réseau**.
2. Cliquez sur **Afficher tout** et dans le volet Réseau, cliquez sur **NetScaler 13.0.**
3. Sélectionnez **NetScaler 13.0 VPX Bring Your Own License** dans la liste des offres logicielles.

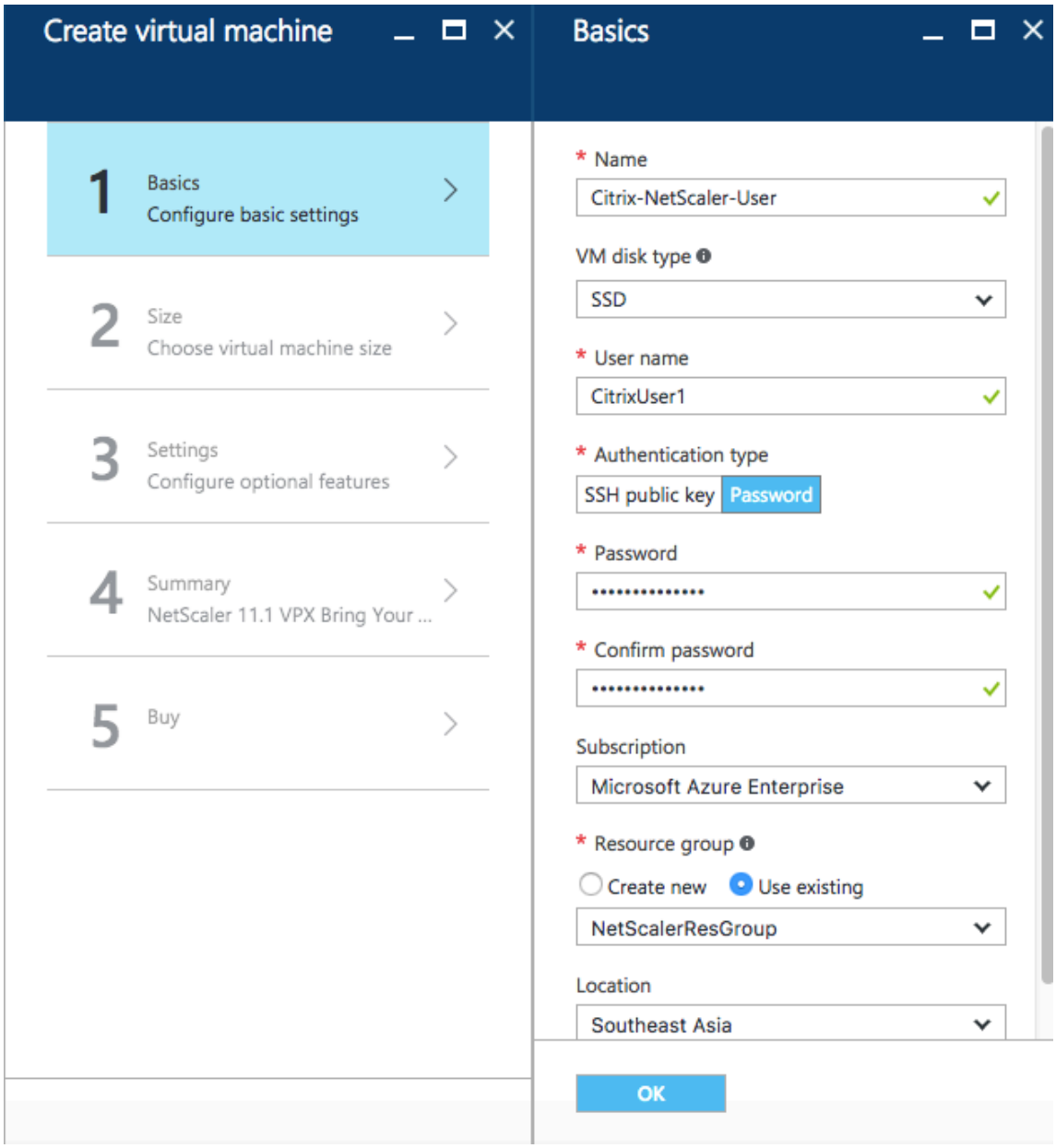
   Pour trouver rapidement une entité sur le portail ARM, vous pouvez également taper le nom de l'entité dans le champ de recherche Azure Marketplace et appuyer sur \ <Enter>. Tapez NetScaler dans la zone de recherche pour trouver les images NetScaler.



> **Remarque**
>
> Assurez-vous de sélectionner la dernière image. Le numéro de version de votre image

> NetScaler figure peut-être dans le nom.

4. **Sur la page**NetScaler VPX Bring Your Own License**, dans la liste déroulante, sélectionnez**Resource Manager**et cliquez sur Créer.**



5. Dans le volet **Créer une machine virtuelle**, spécifiez les valeurs requises dans chaque section pour créer une machine virtuelle. Cliquez sur **OK** dans chaque section pour enregistrer votre configuration.

Basique :

- Nom : spécifiez un nom pour l'instance NetScaler VPX
- Type de disque de machine virtuelle : sélectionnez SSD (valeur par défaut) ou HDD dans le menu

déroulant
- Nom d'utilisateur et mot de passe : spécifiez un nom d'utilisateur et un mot de passe pour accéder aux ressources du groupe de ressources que vous avez créé
- Type d'authentification : sélectionnez la clé publique ou le mot de passe SSH
- Groupe de ressources : sélectionnez le groupe de ressources que vous avez créé dans la liste déroulante

Vous pouvez créer un groupe de ressources ici, mais Citrix vous recommande de créer un groupe de ressources à partir des groupes de ressources dans Azure Resource Manager, puis de sélectionner le groupe dans la liste déroulante.

> **Remarque**
>
> Dans un environnement Azure Stack, en plus des paramètres de base, spécifiez les paramètres suivants :
>
> - Domaine Azure Stack
> - Client Azure Stack (facultatif)
> - Client Azure (facultatif)
> - Secret du client Azure (facultatif)

Taille :

Selon le type de disque de machine virtuelle, SDD ou HDD que vous avez sélectionné dans les paramètres de base, les tailles de disque sont affichées.

- Sélectionnez une taille de disque en fonction de vos besoins et cliquez sur **Sélectionner**.

Paramètres :

- Sélectionnez le type de disque par défaut (Standard)
- Compte de stockage : sélectionnez le compte de stockage
- Réseau virtuel : sélectionnez le réseau virtuel
- Sous-réseau : définissez l'adresse du sous-réseau
- Adresse IP publique : sélectionnez le type d'attribution d'adresse IP
- Groupe de sécurité réseau : sélectionnez le groupe de sécurité que vous avez créé. Assurez-vous que les règles entrantes et sortantes sont configurées dans le groupe de sécurité.
- Ensemble de disponibilité : sélectionnez le jeu de disponibilité dans le menu déroulant

Résumé :

Les paramètres de configuration sont validés et la page Résumé affiche le résultat de la validation. Si la validation échoue, la page Résumé affiche la raison de l'échec. Retournez à la section particulière et apportez les modifications nécessaires. Si la validation réussit, cliquez sur **OK**.

Acheter :

Consultez les détails de l'offre et les conditions légales sur la page d'achat, puis cliquez sur **Acheter**.

Pour un déploiement à haute disponibilité, créez deux instances indépendantes de NetScaler VPX dans le même ensemble de disponibilité et dans le même groupe de ressources pour les déployer dans une configuration de veille active.

Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX

May 5, 2023

Cette section explique comment configurer une instance NetScaler VPX autonome avec plusieurs adresses IP, dans Azure Resource Manager (ARM). Une ou plusieurs cartes réseau peuvent être associées à l'instance VPX, et une ou plusieurs adresses IP publiques et privées statiques ou dynamiques peuvent lui être attribuées à chaque carte réseau. Vous pouvez attribuer plusieurs adresses IP en tant que NSIP, VIP, SNIP, etc.

Pour plus d'informations, consultez la documentation Azure Attribuer plusieurs adresses IP à des machines virtuelles à l'aide du portail Azure.

Si vous souhaitez utiliser les commandes PowerShell, consultez la section Configuration de plusieurs adresses IP pour une instance NetScaler VPX en mode autonome àl'aide des commandes PowerShell.

Cas d'utilisation

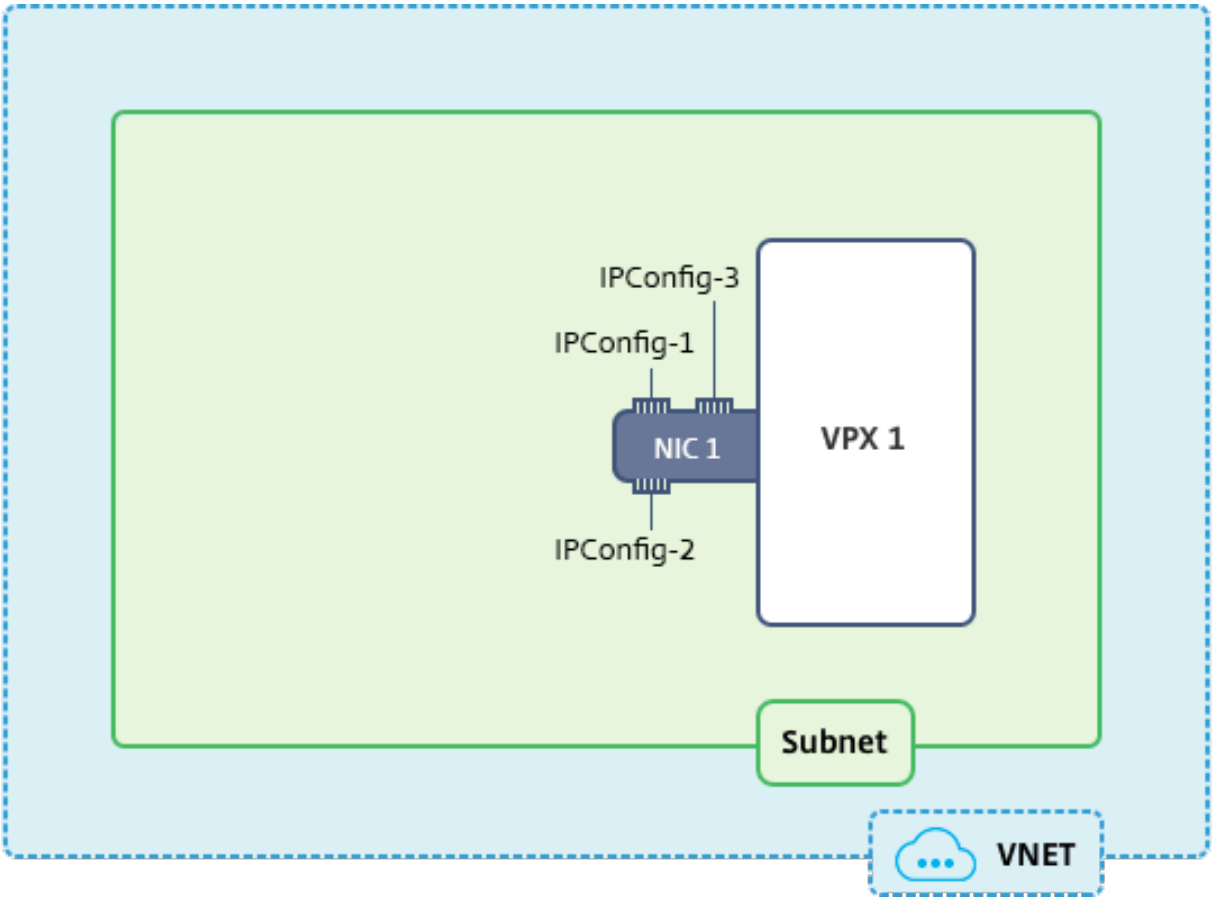
Dans ce cas d'utilisation, une appliance NetScaler VPX autonome est configurée avec une seule carte réseau connectée à un réseau virtuel (VNET). La carte réseau est associée à trois configurations IP (ipconfig), chaque serveur ayant une fonction différente, comme le montre le tableau.

Configuration IP	Associé à	Motif
ipconfig1	Adresse IP publique statique ; adresse IP privée statique	Sert le trafic de gestion
ipconfig2	Adresse IP publique statique ; adresse privée statique	Sert le trafic côté client
ipconfig3	Adresse IP privée statique	Communication avec les serveurs back-end

> **Remarque**
>
> `IPConfig-3` n'est associé à aucune adresse IP publique.

Diagramme : Topologie

Voici la représentation visuelle du cas d'utilisation.



> **Remarque**
>
> Dans un déploiement Azure NetScaler VPX multi-NIC et multi-IP, l'adresse IP privée associée à la principale (première) `IPConfig` de la carte réseau principale (première) est automatiquement ajoutée en tant que NSIP de gestion de l'appliance. Les adresses IP privées restantes associées `IPConfigs` doivent être ajoutées dans l'instance VPX en tant que VIP ou SNIP à l'aide de la `add ns ip` commande, selon vos besoins.

Avant de commencer

Avant de commencer, créez une instance VPX en suivant les étapes indiquées sur ce lien :

Configurer une instance autonome NetScaler VPX

Dans ce cas d'utilisation, l'instance VPX NSDoc0330vm est créée.

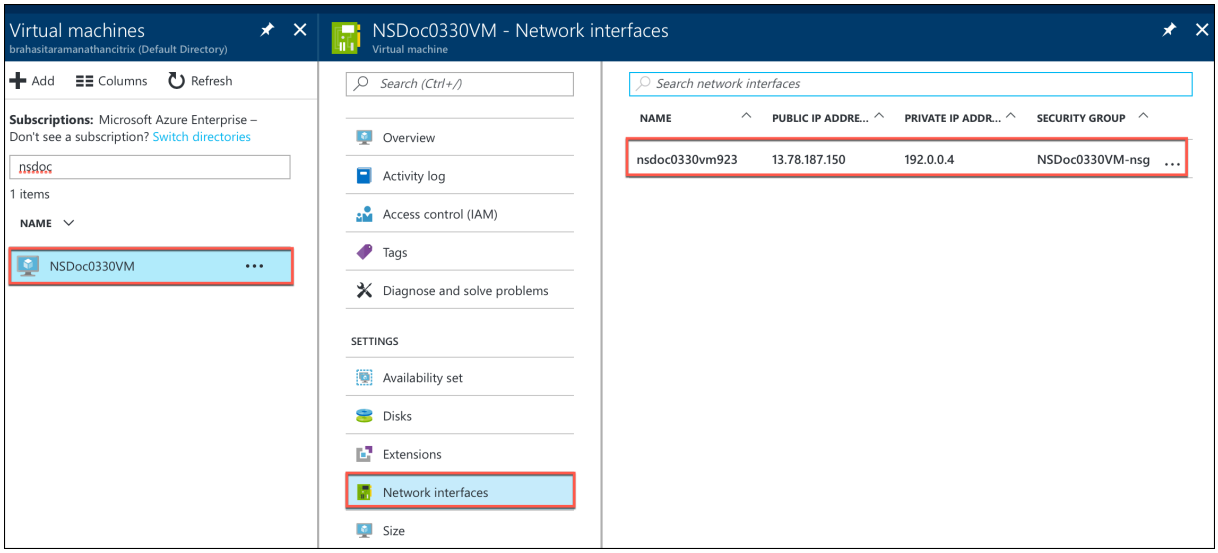
Procédure de configuration de plusieurs adresses IP pour une instance NetScaler VPX en mode autonome.

Pour configurer plusieurs adresses IP pour une appliance NetScaler VPX en mode autonome :

1. Ajouter des adresses IP à la machine virtuelle
2. Configurer les adresses IP appartenant à NetScaler

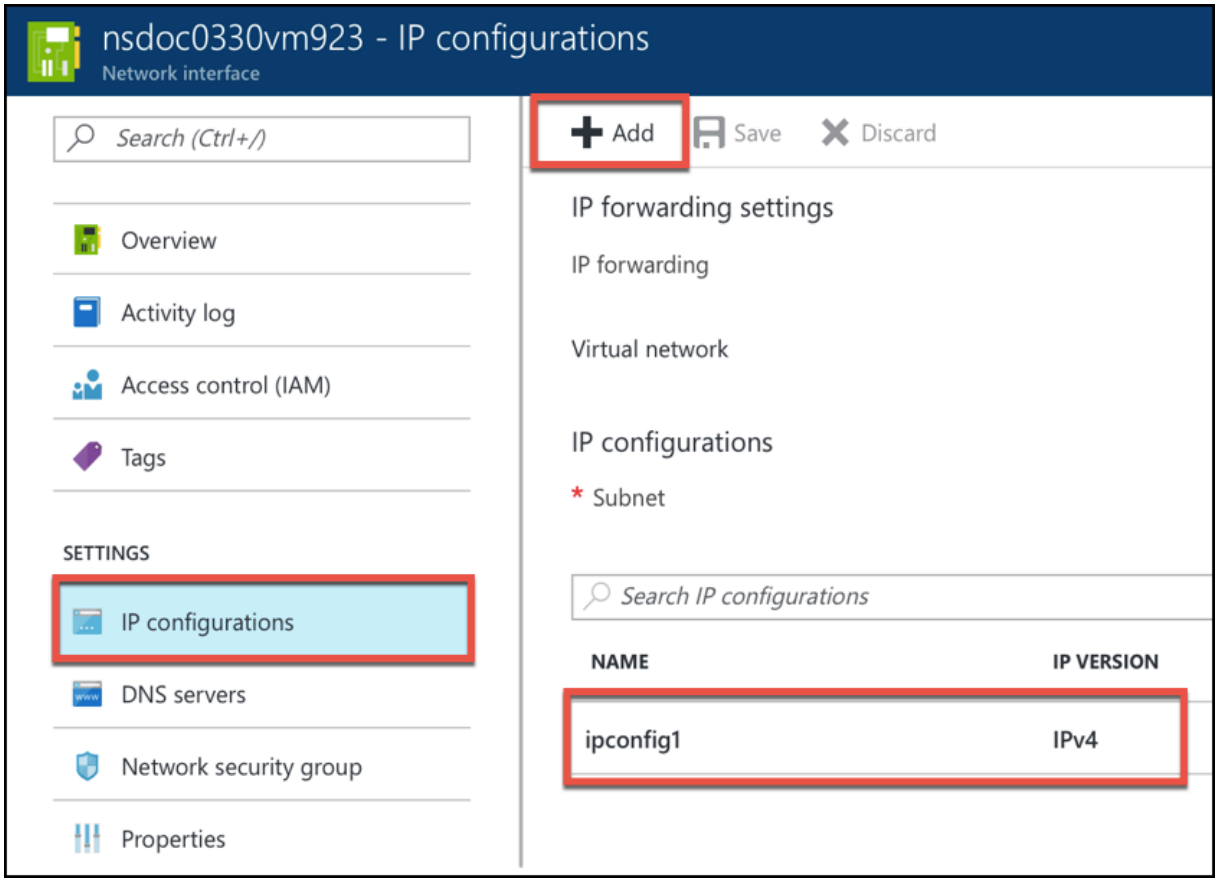
Étape 1 : ajouter des adresses IP à la machine virtuelle

1. Dans le portail, cliquez sur **Plus de services > tapez machines virtuelles** dans la zone de filtre, puis cliquez sur **Machines virtuelles**.
2. Dans le **volet Machines virtuelles**, cliquez sur la machine virtuelle à laquelle vous souhaitez ajouter des adresses IP. Cliquez sur **Interfaces réseau** dans la lame de machine virtuelle qui apparaît, puis sélectionnez l'interface réseau.



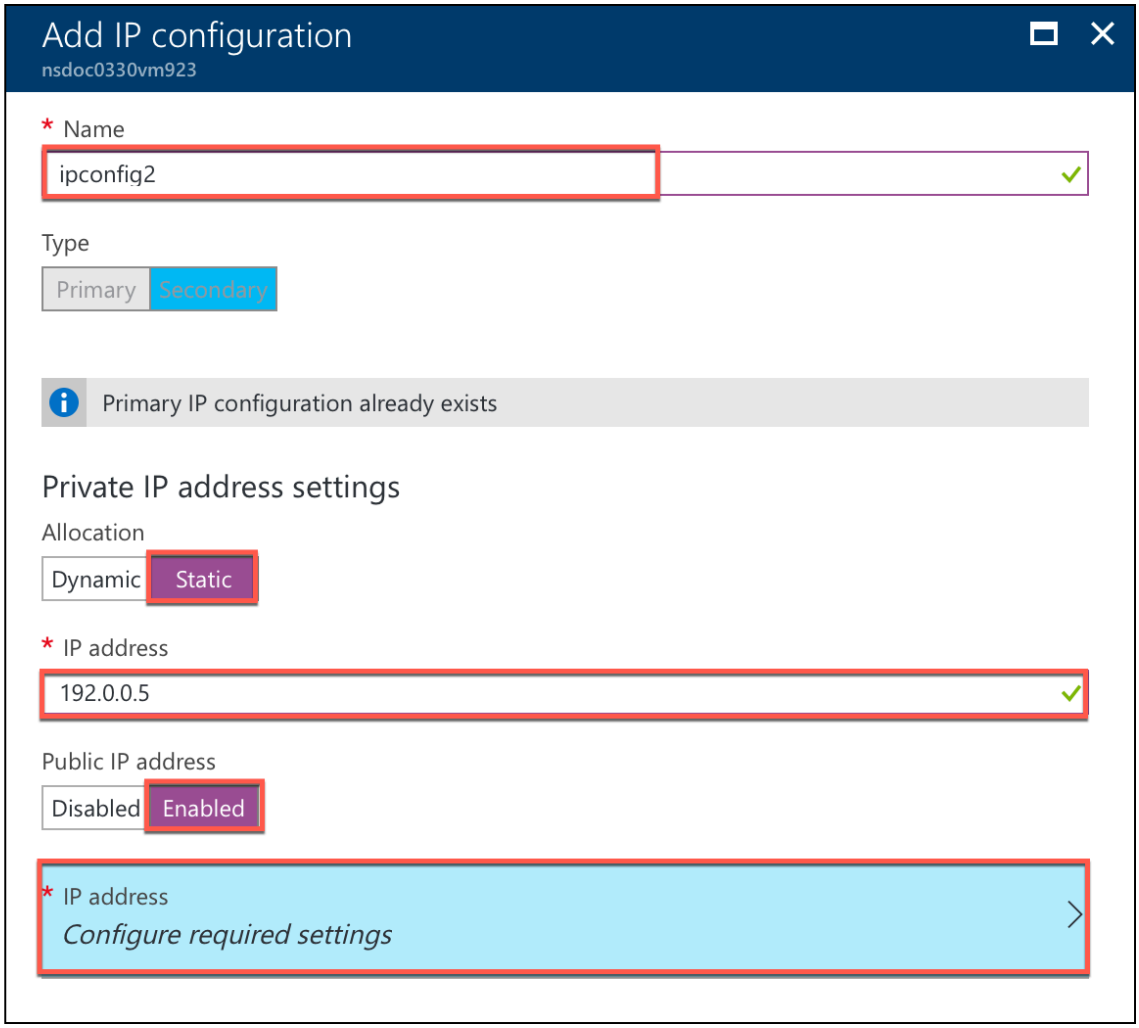
Dans la lame qui apparaît pour la carte réseau sélectionnée, cliquez sur **Configurations IP**. La configuration IP existante qui a été attribuée lors de la création de la machine virtuelle, **ipconfig1**, s'affiche. Dans ce cas d'utilisation, assurez-vous que les adresses IP associées à ipconfig1 sont statiques. Ensuite, créez deux configurations IP supplémentaires : ipconfig2 (VIP) et ipconfig3 (SNIP).

Pour en créer plus `ipconfigs`, créez **Ajouter**.



Dans la fenêtre **Ajouter une configuration IP**, entrez un **nom**, spécifiez la méthode d'allocation comme **statique**, entrez une adresse IP (192.0.0.5 pour ce cas d'utilisation) et activez **l'adresse IP publique** .

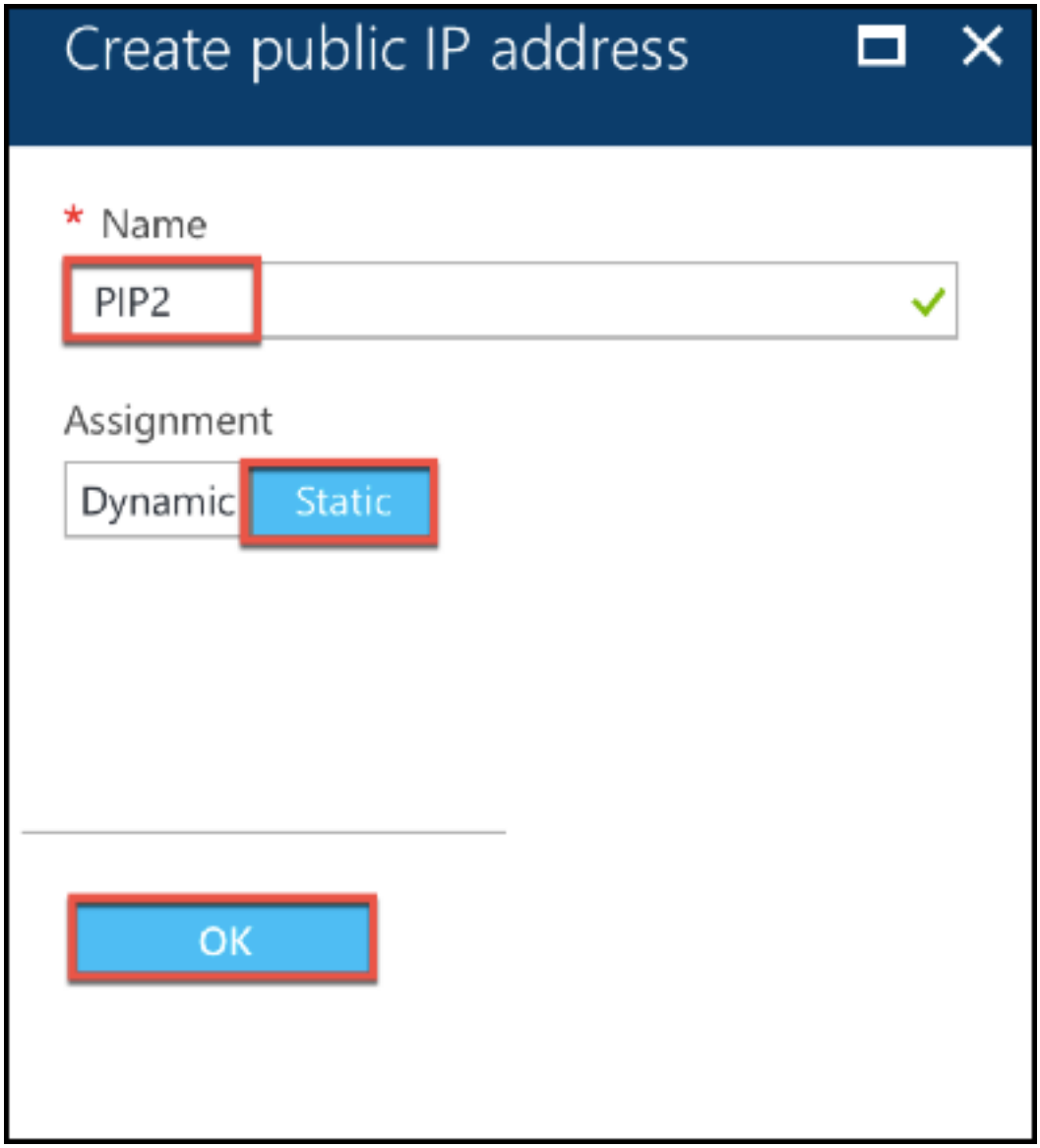
> **Remarque**
>
> Avant d'ajouter une adresse IP privée statique, vérifiez la disponibilité de l'adresse IP et assurez-vous que l'adresse IP appartient au même sous-réseau auquel la carte réseau est attachée.



Ensuite, cliquez sur **Configurer les paramètres requis** pour créer une adresse IP publique statique pour ipconfig2.

Par défaut, les adresses IP publiques sont dynamiques. Pour vous assurer que la machine virtuelle utilise toujours la même adresse IP publique, créez une adresse IP publique statique.

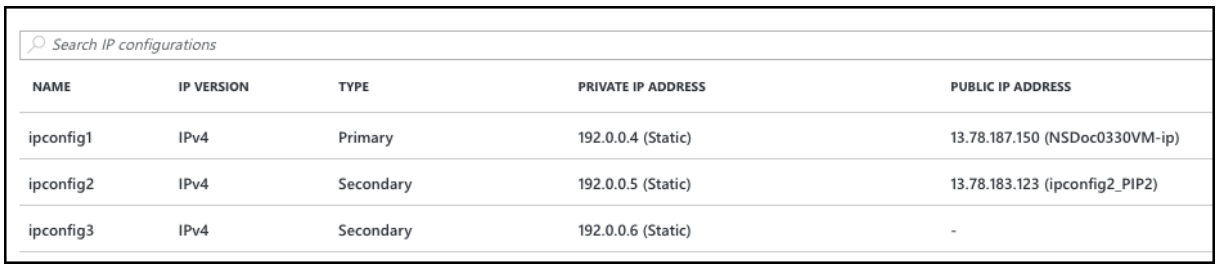
Dans le volet Créer une adresse IP publique, ajoutez un nom. Sous Attribution, cliquez sur **Statique**. Puis cliquez sur **OK**.



Remarque

Même lorsque vous définissez la méthode d'allocation sur statique, vous ne pouvez pas spécifier l'adresse IP réelle attribuée à la ressource IP publique. Elle est plutôt allouée à partir d'un pool d'adresses IP disponibles dans l'emplacement Azure où la ressource est créée.

Suivez les étapes pour ajouter une configuration IP supplémentaire pour ipconfig3. La propriété intellectuelle publique n'est pas obligatoire.



Étape 2 : Configuration des adresses IP appartenant à NetScaler

Configurez les adresses IP appartenant à NetScaler à l'aide de l'interface graphique ou de la commande. `add ns ip` Pour plus d'informations, consultez la section Configuration des adresses IP appartenant à NetScaler.

Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau

May 5, 2023

Dans un déploiement Microsoft Azure, une configuration à haute disponibilité de deux instances NetScaler VPX est obtenue à l'aide de l'Azure Load Balancer (ALB). Pour ce faire, vous pouvez configurer une sonde de santé sur ALB, qui surveille chaque instance VPX en envoyant une sonde de santé toutes les 5 secondes aux instances principales et secondaires.

Dans cette configuration, seul le nœud principal répond aux sondes de santé et le nœud secondaire ne le fait pas. Une fois que le principal envoie la réponse à la sonde d'intégrité, l'ALB commence à envoyer le trafic de données à l'instance. Si l'instance principale rate deux tests d'intégrité consécutifs, ALB ne redirige pas le trafic vers cette instance. Lors du basculement, la nouvelle base commence à répondre aux sondes d'intégrité et l'ALB redirige le trafic vers elle. Le temps de basculement standard VPX haute disponibilité est de trois secondes. Le temps total de basculement que peut prendre le changement de trafic peut être de 13 secondes maximum.

Vous pouvez déployer deux instances NetScaler VPX avec plusieurs cartes réseau dans une configuration de haute disponibilité (HA) active-passive sur Azure. Chaque carte réseau peut contenir plusieurs adresses IP.

Les options suivantes sont disponibles pour un déploiement de haute disponibilité multi-cartes réseau :

- Haute disponibilité à l'aide du jeu de disponibilité Azure
- Haute disponibilité à l'aide des zones de disponibilité Azure

Pour plus d'informations sur Azure Availability Set et Availability Zones, consultez la documentation Azure Gérer la disponibilité des machines virtuelles Linux.

Haute disponibilité en utilisant le jeu de disponibilité

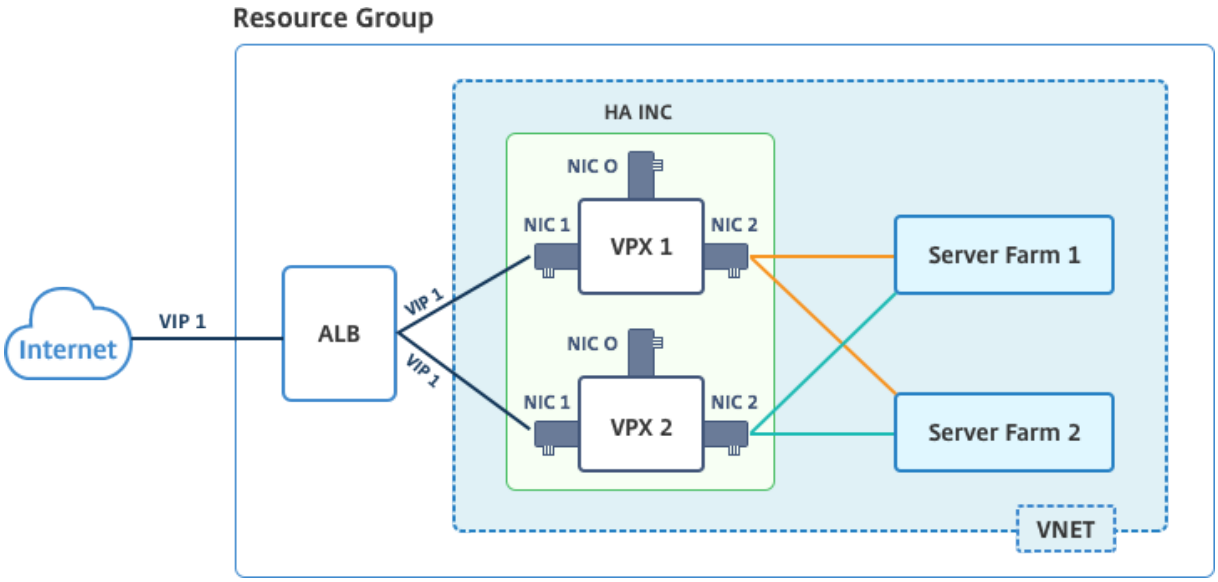
Une configuration haute disponibilité utilisant un jeu de disponibilité doit répondre aux exigences suivantes :

- Configuration INC (Independent Network Configuration) de haute disponibilité
- L'Azure Load Balancer (ALB) en mode Direct Server Return (DSR)

Tout le trafic passe par le nœud principal. Le nœud secondaire reste en mode veille jusqu'à ce que le nœud principal tombe en panne.

> **Remarque**
>
> Pour qu'un déploiement de haute disponibilité de NetScaler VPX sur le cloud Azure fonctionne, vous avez besoin d'une adresse IP publique flottante (PIP) qui peut être déplacée entre les deux nœuds VPX. L'équilibrage de charge Azure (ALB) fournit ce PIP flottant, qui est déplacé automatiquement vers le deuxième nœud en cas de basculement.

Schéma : Exemple d'architecture de déploiement à haute disponibilité utilisant Azure Availability Set



Dans un déploiement actif-passif, les adresses IP publiques frontales (PIP) ALB sont ajoutées en tant qu'adresses VIP dans chaque nœud VPX. Dans la configuration HA-INC, les adresses VIP sont flottantes et les adresses SNIP sont spécifiques à l'instance.

Vous pouvez déployer une paire VPX en mode haute disponibilité actif-passif de deux manières en utilisant :

- **Modèle de haute disponibilité standard NetScaler VPX** : utilisez cette option pour configurer une paire HA avec l'option par défaut de trois sous-réseaux et six cartes réseau.
- **Commandes Windows PowerShell** : utilisez cette option pour configurer une paire HA en fonction des exigences de votre sous-réseau et de votre carte réseau.

Cette rubrique décrit comment déployer une paire VPX dans une configuration HA actif-passif à l'aide du modèle Citrix. Si vous souhaitez utiliser des commandes PowerShell, reportez-vous à la section Configuration d'une configuration HA avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell.

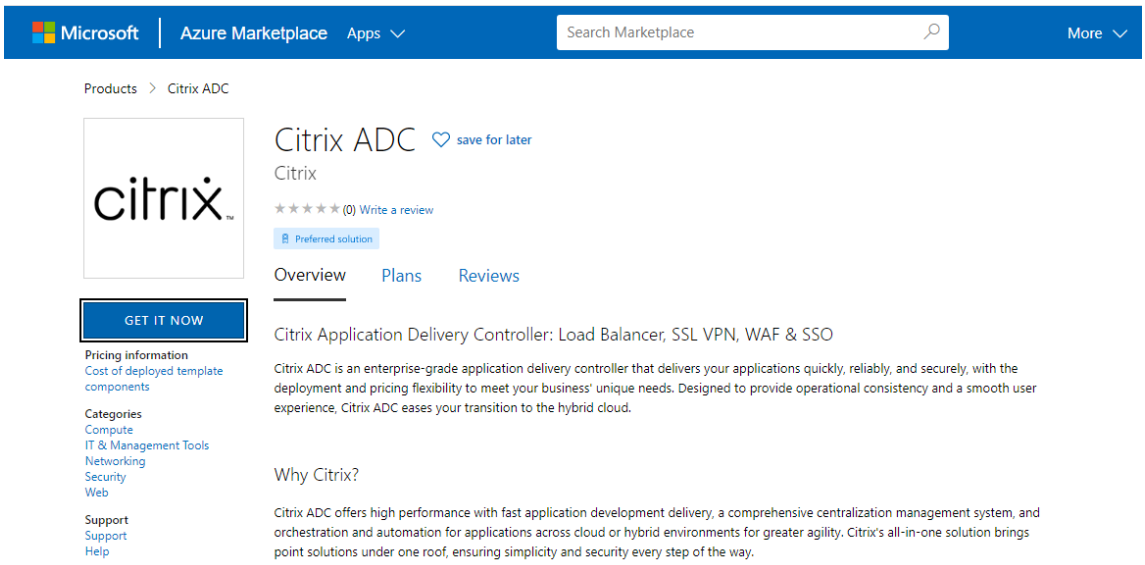
Configurer les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaler

Vous pouvez déployer rapidement et efficacement une paire d'instances VPX en mode HA-INC à l'aide du modèle standard. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés au trafic de gestion, client et côté serveur, et chaque sous-réseau dispose de deux cartes réseau pour les deux instances VPX.

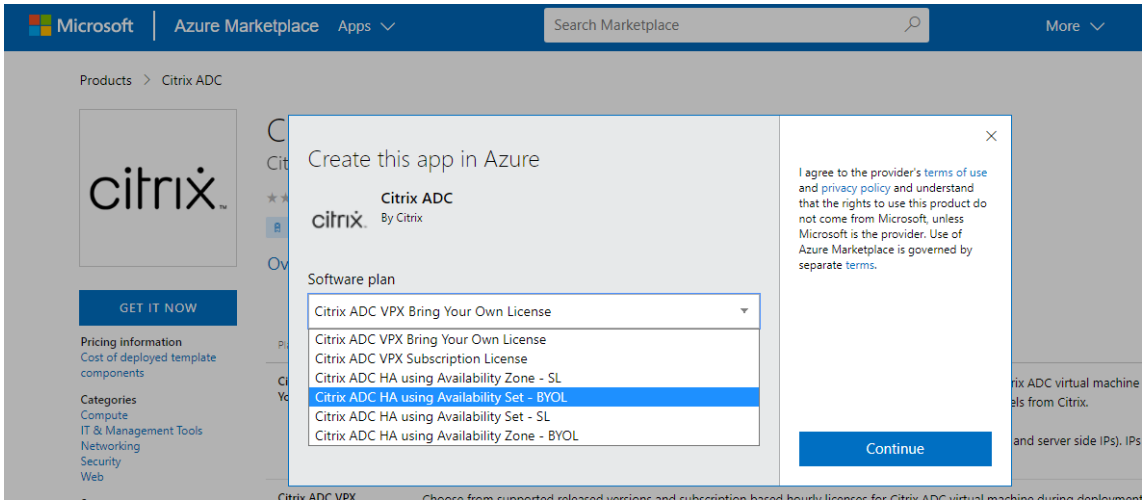
Vous pouvez obtenir le modèle NetScaler HA Pair sur AzureMarketplace.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité, à l'aide des jeux de disponibilité Azure.

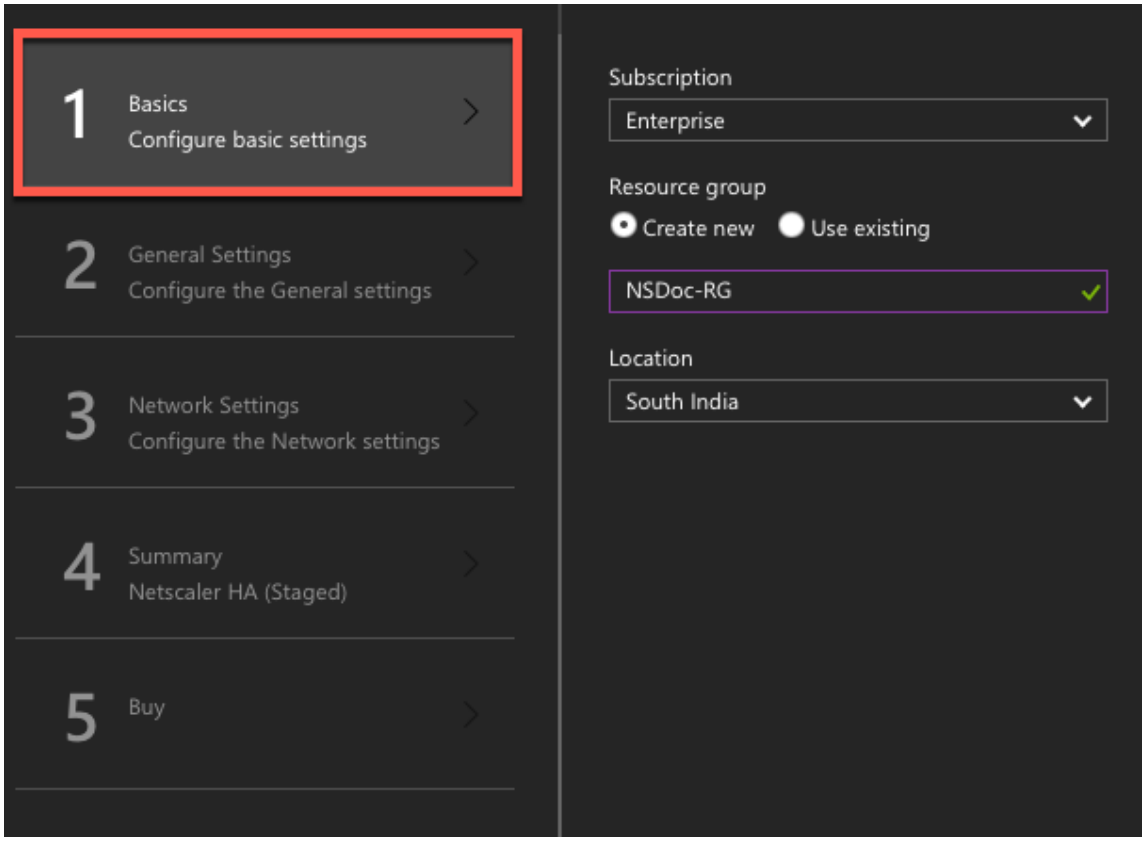
1. Sur Azure Marketplace, recherchez **NetScaler**.



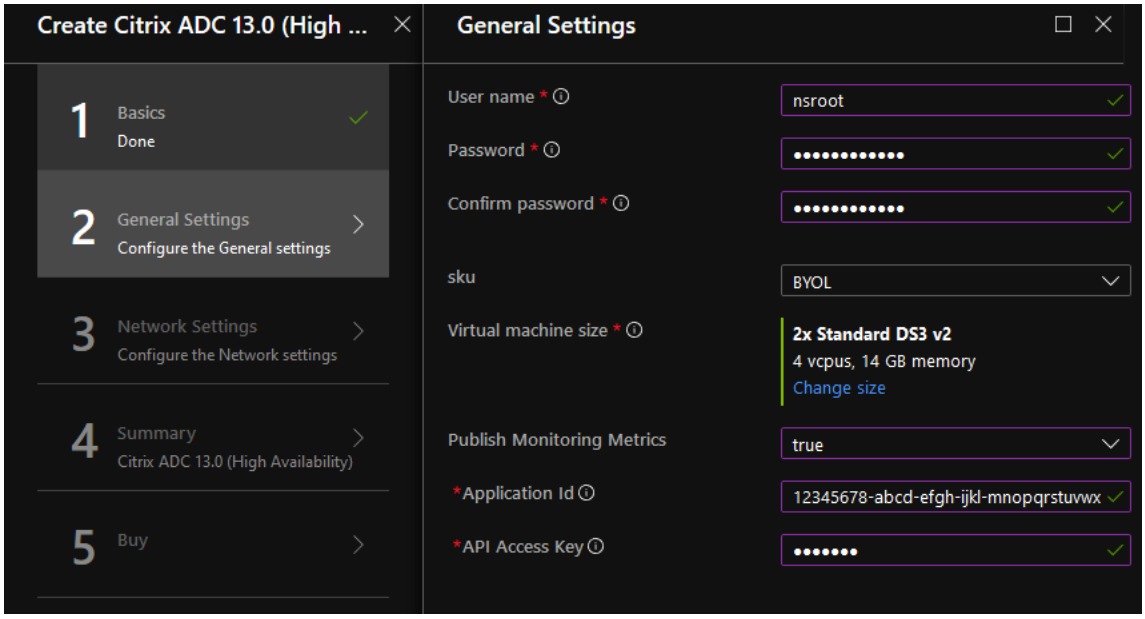
2. Cliquez sur **GET IT NOW**.
3. Sélectionnez le déploiement HA requis ainsi que la licence, puis cliquez sur **Continuer**.



4. La page **Principes** de base s'affiche. Créez un groupe de ressources et sélectionnez **OK**.

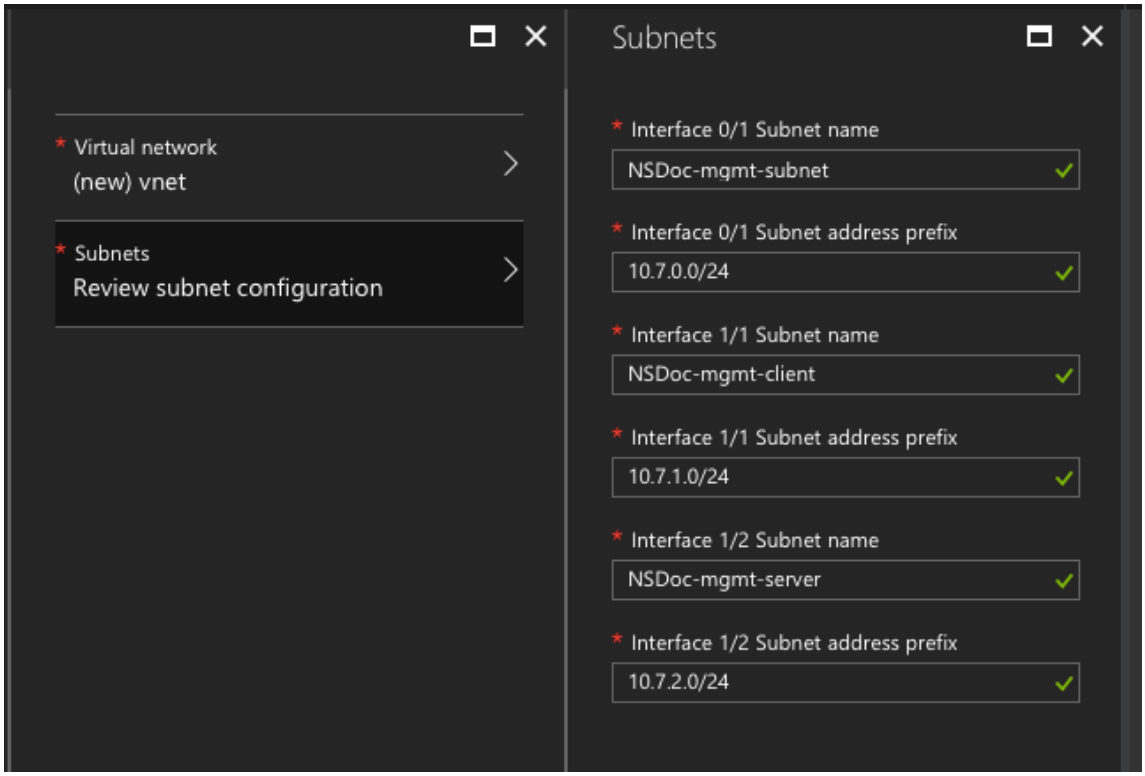


5. La page **Paramètres généraux** s'affiche. Entrez les détails et sélectionnez **OK**.



> Remarque :
>
> Par défaut, l'option **Publishing Monitoring Metrics** est définie sur **false**. Si vous souhaitez activer cette option, sélectionnez **vrai**.
> Créez une application Azure Active Directory (ADD) et un principal de service pouvant accéder aux ressources. Attribuez un rôle de contributeur à l'application AAD nouvellement créée. Pour plus d'informations, voir Utiliser le portail pour créer une application Azure Active Directory et un principal de service pouvant accéder aux ressources.

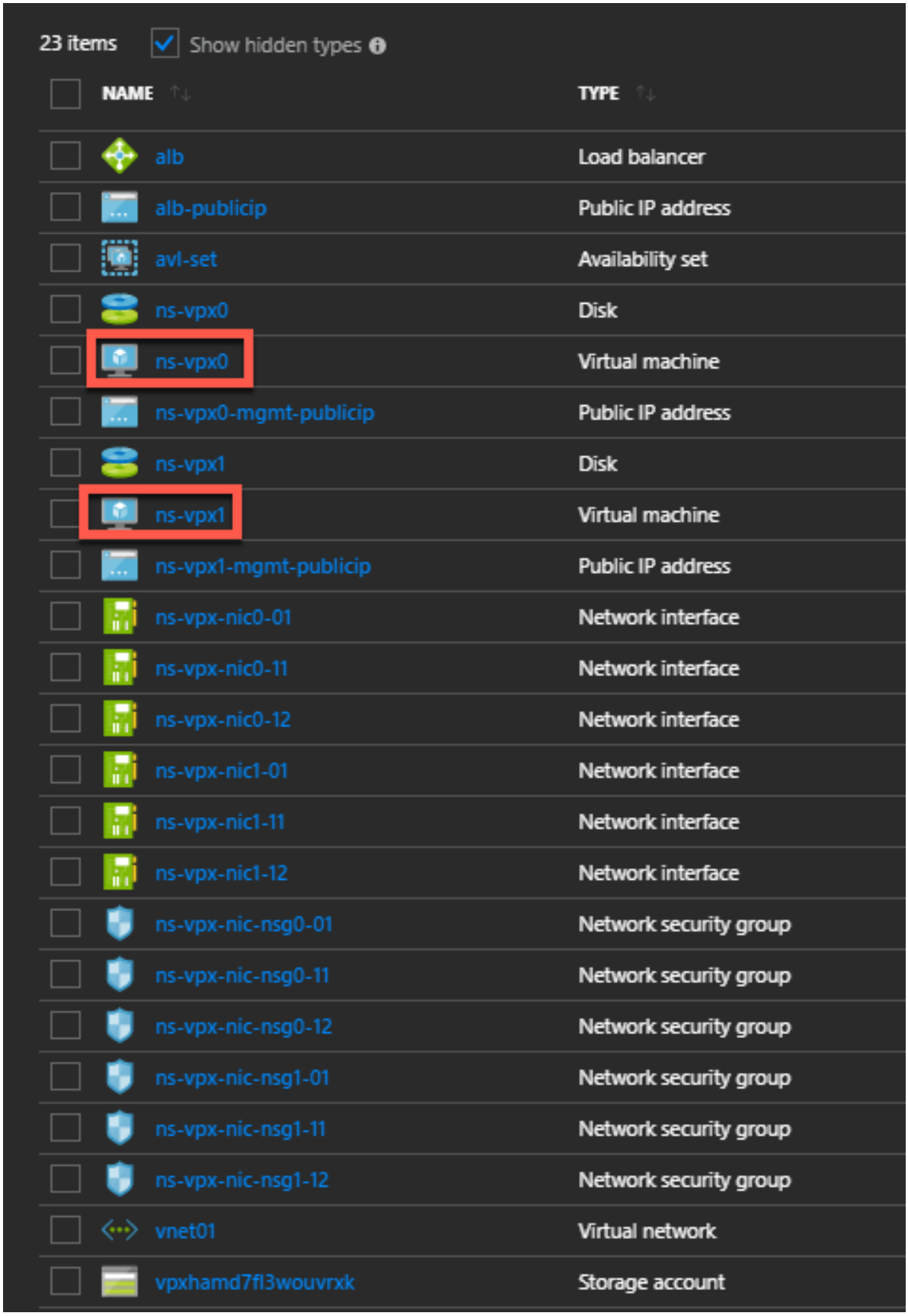
6. La page **Paramètres réseau** s'affiche. Vérifiez les configurations du réseau virtuel et du sous-réseau, modifiez les paramètres requis et sélectionnez **OK**.



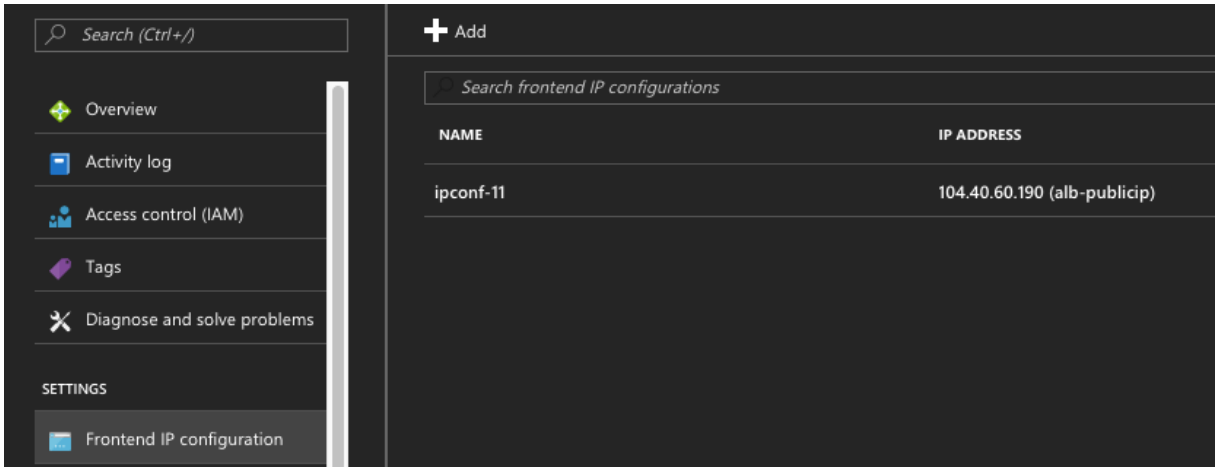
7. La page **Résumé** s'affiche. Vérifiez la configuration et modifiez-la en conséquence. Sélectionnez **OK** pour confirmer.
8. La page **Acheter** s'affiche. Sélectionnez **Acheter** pour terminer le déploiement.

Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois terminé, sélectionnez le **groupe de ressources** sur le portail Azure pour afficher les détails de configuration, tels que les règles LB, les pools dorsaux et les sondes de santé. La paire haute disponibilité apparaît sous la forme ns-vpx0 et ns-vpx1.

Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.



Ensuite, vous devez configurer le serveur virtuel d'équilibrage de charge avec l' **adresse IP publique (PIP) de l'ALB**, sur le nœud principal. Pour trouver le PIP ALB, sélectionnez ALB > Configuration IP du **frontend**.



Consultez la section **Ressources** pour plus d'informations sur la façon de configurer le serveur virtuel d'équilibrage de charge.

Ressources :

Les liens suivants fournissent des informations supplémentaires relatives au déploiement haute disponibilité et à la configuration du serveur virtuel :

- Configuration de nœuds haute disponibilité dans différents sous-réseaux
- Configurer l'équilibrage de charge de base

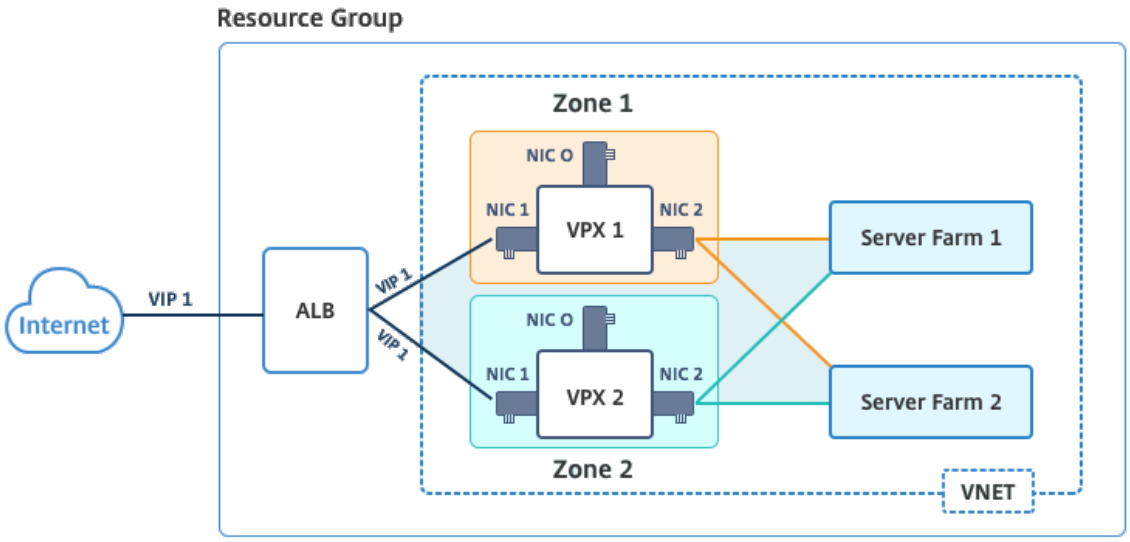
Ressources connexes :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell
- Configuration de GSLB sur un déploiement HA actif de secours sur Azure

Haute disponibilité grâce aux zones de disponibilité

Les zones de disponibilité Azure sont des emplacements isolés de pannes dans une région Azure, fournissant une alimentation, un refroidissement et une mise en réseau redondantes et augmentant la résilience. Seules les régions Azure spécifiques prennent en charge les zones de disponibilité. Pour plus d'informations, consultez la documentation Azure [Qu'est-ce que les zones de disponibilité dans Azure ?

Diagramme : Exemple d'architecture de déploiement haute disponibilité, à l'aide de zones de disponibilité Azure



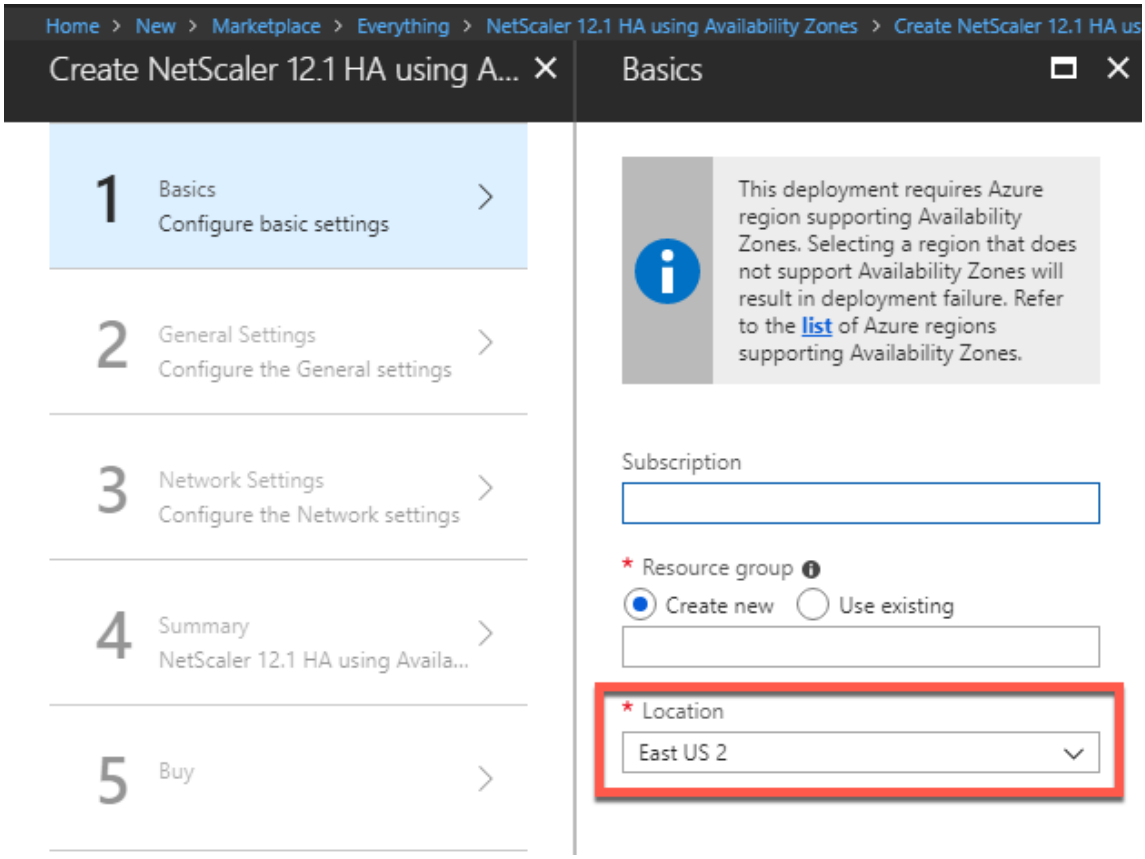
Vous pouvez déployer une paire VPX en mode haute disponibilité à l'aide du modèle intitulé « NetScaler 13.0 HA using Availability Zones », disponible sur Azure Marketplace.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité, à l'aide des zones de disponibilité Azure.

1. À partir de la Place de marché Azure, sélectionnez et lancez le modèle de solution Citrix.

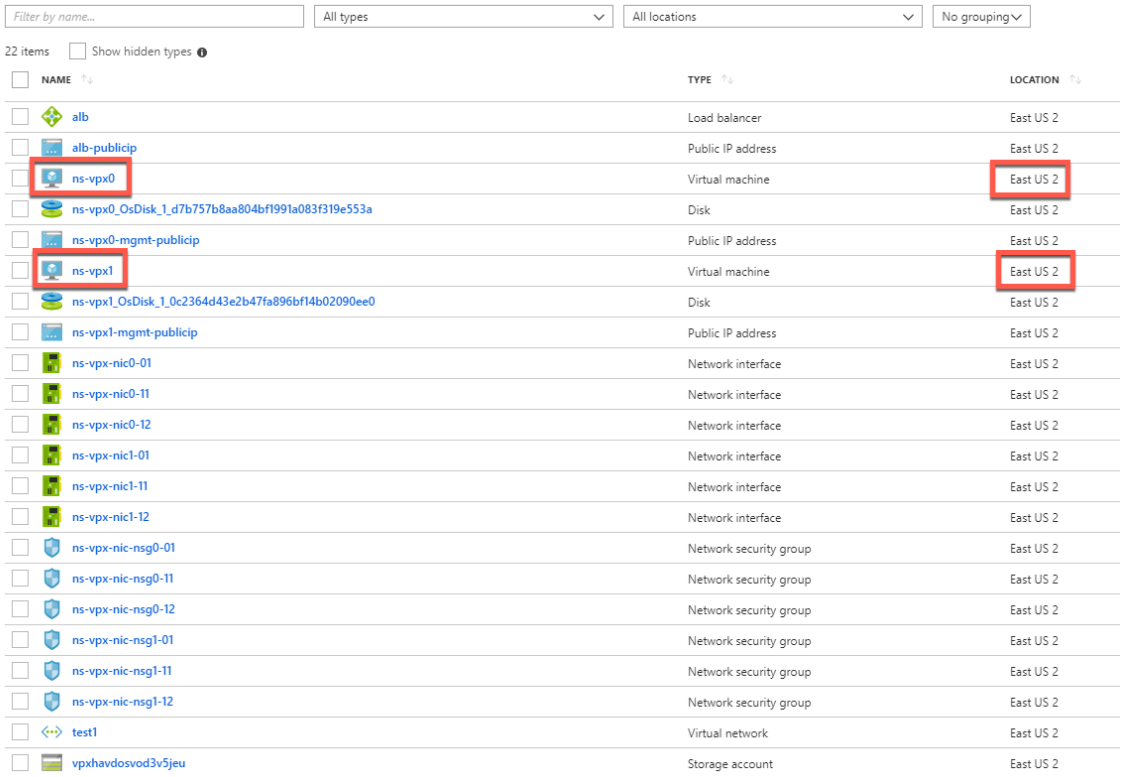
2. Assurez-vous que le type de déploiement est Resource Manager et sélectionnez **Créer**.
3. La page **Principes** de base s'affiche. Entrez les détails et cliquez sur **OK**.

> Remarque : Assurez-vous de sélectionner une région Azure qui prend en charge les zones de disponibilité. Pour plus d'informations sur les régions prenant en charge les zones de disponibilité, consultez la documentation Azure Qu'est-ce que les zones de disponibilité dans Azure ?



4. La page **Paramètres généraux** s'affiche. Entrez les détails et sélectionnez **OK**.
5. La page **Paramètres réseau** s'affiche. Vérifiez les configurations du réseau virtuel et du sous-réseau, modifiez les paramètres requis et sélectionnez **OK**.
6. La page **Résumé** s'affiche. Vérifiez la configuration et modifiez-la en conséquence. Sélectionnez **OK** pour confirmer.
7. La page **Acheter** s'affiche. Sélectionnez **Acheter** pour terminer le déploiement.

   Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois l'opération terminée, sélectionnez le **groupe de ressources** pour voir les détails de configuration, tels que les règles LB, les pools principaux, les sondes de santé, etc., sur le portail Azure. La paire haute disponibilité apparaît sous la forme ns-vpx0 et ns-vpx1. Vous pouvez également voir l'emplacement dans la colonne **Emplacement** .



Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.

Surveillez vos instances à l'aide de mesures dans Azure Monitor

Vous pouvez utiliser les métriques de la plateforme de données Azure Monitor pour surveiller un ensemble de ressources NetScaler VPX telles que le processeur, l'utilisation de la mémoire et le débit. Le service Metrics surveille les ressources NetScaler VPX qui s'exécutent sur Azure, en temps réel. Vous pouvez utiliser **Metrics Explorer** pour accéder aux données collectées. Pour plus d'informations, reportez-vous à la section Présentation des mesures Azure Monitor.

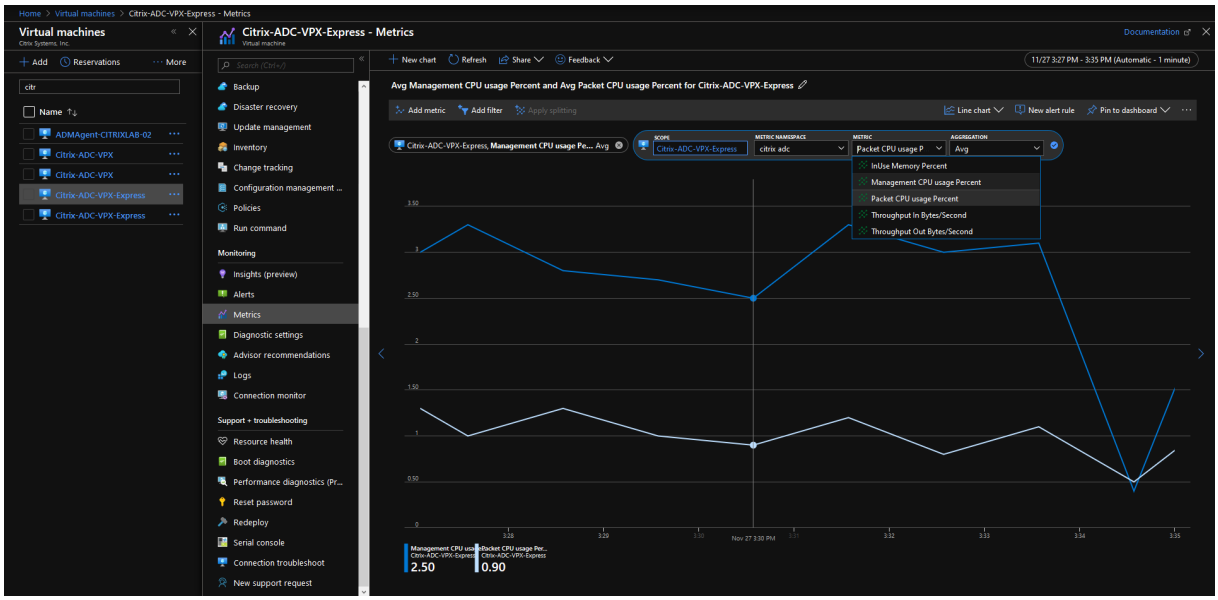
Points à noter

- Si vous déployez une instance NetScaler VPX sur Azure à l'aide de l'offre Azure Marketplace, le service Metrics est désactivé par défaut.
- Le service Metrics n'est pas pris en charge dans Azure CLI.
- Les métriques sont disponibles pour le processeur (gestion et utilisation du processeur par paquets), la mémoire et le débit (entrant et sortant).

Comment afficher les mesures dans Azure Monitor

Pour afficher les mesures dans Azure Monitor pour votre instance, effectuez les opérations suivantes :

1. Connectez-vous à **Azure Portal > Machines virtuelles**.
2. Sélectionnez la machine virtuelle qui est le nœud principal.
3. Dans la section **Surveillance**, cliquez sur **Métriques**.
4. Dans le menu déroulant **Metric Namespace**, cliquez sur **NetScaler**.
5. Dans le menu déroulant **Toutes les**mesures** dans le menu déroulant Mesures, cliquez sur les mesures que vous souhaitez afficher.
6. Cliquez sur **Ajouter une mesure** pour afficher une autre mesure sur le même graphique. Utilisez les options du graphique pour personnaliser votre graphique.



Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell

May 5, 2023

Vous pouvez déployer deux instances NetScaler VPX avec plusieurs cartes réseau dans une configuration de haute disponibilité (HA) active-passive sur Azure. Chaque carte réseau peut contenir plusieurs adresses IP.

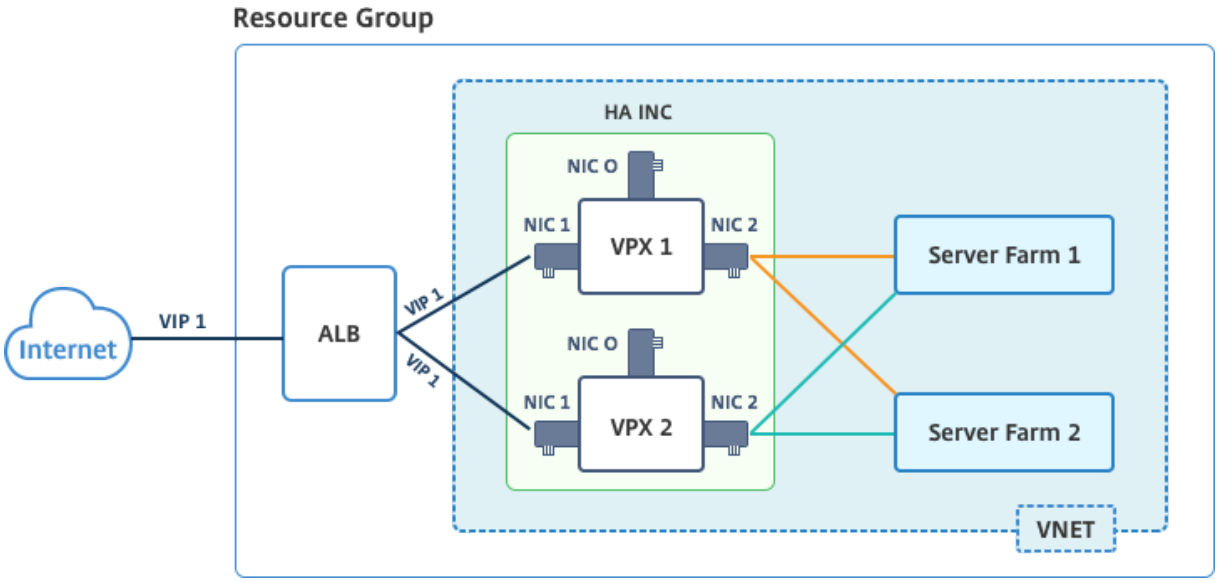
Un déploiement actif-passif nécessite :

- Configuration INC (Independent Network Configuration) de haute disponibilité
- L'Azure Load Balancer (ALB) en mode Direct Server Return (DSR)

Tout le trafic passe par le nœud principal. Le nœud secondaire reste en mode veille jusqu'à ce que le nœud principal tombe en panne.

> **Remarque**
>
> Pour qu'un déploiement de haute disponibilité de NetScaler VPX sur un cloud Azure fonctionne, vous avez besoin d'une adresse IP publique flottante (PIP) qui peut être déplacée entre les deux nœuds de haute disponibilité. L'équilibrage de charge Azure (ALB) fournit ce PIP flottant, qui est déplacé automatiquement vers le deuxième nœud en cas de basculement.

Schéma : Exemple d'architecture de déploiement actif-passif



Dans un déploiement actif-passif, les adresses IP publiques flottantes (PIP) ALB sont ajoutées en tant qu'adresses VIP dans chaque nœud VPX. Dans la configuration HA-INC, les adresses VIP sont flottantes et les adresses SNIP sont spécifiques à l'instance.

ALB surveille chaque instance VPX en envoyant une sonde de santé toutes les 5 secondes et redirige le trafic vers cette instance uniquement qui envoie la réponse des sondes de santé à intervalles réguliers. Ainsi, dans une configuration HA, le nœud principal répond aux sondes d'intégrité et le nœud secondaire ne le fait pas. Si les instances principales manquent deux sondes de santé consécutives, ALB ne redirige pas le trafic vers cette instance. Lors du basculement, la nouvelle base commence à répondre aux sondes d'intégrité et l'ALB redirige le trafic vers elle. Le temps de basculement standard VPX haute disponibilité est de trois secondes. Le temps de basculement total que peut prendre la commutation du trafic peut être de 13 secondes au maximum.

Vous pouvez déployer une paire VPX dans une configuration HA active-passive de deux manières en utilisant :

- **Modèle de haute disponibilité standard NetScaler VPX** : utilisez cette option pour configurer une paire HA avec l'option par défaut de trois sous-réseaux et six cartes réseau.

- **Commandes Windows PowerShell** : utilisez cette option pour configurer une paire HA en fonction des exigences de votre sous-réseau et de votre carte réseau.

Cette rubrique décrit comment déployer une paire VPX dans une configuration HA active-passive à l'aide des commandes PowerShell. Si vous souhaitez utiliser le modèle NetScaler VPX Standard HA, reportez-vous à la section Configuration d'une configuration HA avec plusieurs adresses IPet cartes réseau.

Configurer les nœuds HA-INC à l'aide des commandes PowerShell

Scénario : déploiement PowerShell HA-INC

Dans ce scénario, vous déployez une paire NetScaler VPX en utilisant la topologie indiquée dans le tableau. Chaque instance VPX contient trois cartes réseau, chaque carte réseau étant déployée dans un sous-réseau différent. Une configuration IP est attribuée à chaque carte réseau.

ALB	VPX1	VPX2
ALB est associé à l'adresse IP publique 3 (pip3)	L'IP de gestion est configurée avec IPConfig1, qui inclut une adresse IP publique (pip1) et une adresse IP privée (12.5.2.24) ; nic1 ; Mgmtsubnet=12.5.2.0/24	L'IP de gestion est configurée avec IPConfig5, qui inclut une adresse IP publique (pip3) et une adresse IP privée (12.5.2.26) ; nic4 ; Mgmtsubnet=12.5.2.0/24
Les règles LB et le port configurés sont HTTP (80), SSL (443), Health Probe (9000)	L'adresse IP côté client est configurée avec IPConfig3, qui inclut une adresse IP privée (12.5.1.27) ; nic2 ; FrontendSubet=12.5.1.0/24	L'adresse IP côté client est configurée avec IPConfig7, qui inclut une adresse IP privée (12.5.1.28) ; nic5 ; FrontendSubet=12.5.1.0/24
-	L'adresse IP côté serveur est configurée avec IPConfig4, qui inclut une adresse IP privée (12.5.3.24) ; nic3 ; backendSubnet=12.5.3.0/24	L'adresse IP côté serveur est configurée avec IPConfig8, qui inclut une adresse IP privée (12.5.3.28) ; nic6 ; backendSubnet=12.5.3.0/24
-	Les règles et les ports pour NSG sont SSH (22), HTTP (80), HTTPS (443)	-

Réglages des paramètres

Les paramètres suivants sont utilisés dans ce scénario.

$locName= « Asie du Sud-Est »

$rgname = « RG multi-tip-multinique-rg »

$nicName1= “VM1-NIC1”

$nicName2 = “VM1-NIC2”

$nicName3= “VM1-NIC3”

$nicName4 = “VM2-NIC1”

$nicName5= “VM2-NIC2”

$nicName6 = “VM2-NIC3”

$vNetName = « Azure-MultiIP-alb-VNet »

$vNetAddressRange= « 12.5.0.0/16”

$FrontendSubnetName= « FrontendSubnet »

$frontendSubnetRange= « 12,5.1.0/24 »

$MGMTSubnetName= « MgmtSubnet »

$mgmtSubnetRange= « 12,5.2.0/24 »

$backendSubnetName = « BackendSubnet »

$backendSubnetRange = « 12,5.3.0/24”

$prmStorageAccountName = « stockage multiipmultinicbstorage »

$avSetName = « Plusieurs AVSet »

$vmSize= “Standard_DS4_V2”

$publisher = « Citrix »

$offer = “netscalervpx-120”

$sku = « netscalerbyol »

$version=”dernière »

$pubIPName1=”VPX1MGMT”

$pubIPName2=”VPX2MGMT”

$pubIPName3=”ALBPIP”

$domName1=”vpx1dns”

$domName2=”vpx2dns”

$domName3=”vpxalbdns”

$vmNamePrefix=”VPXMultiIPAlb »

$osDiskSuffix1=”osmultiipalbdiskdb1”

$osDiskSuffix2=”osmultiipalbdiskdb2”

$LBName= « MultiIPAlb »

$frontendConfigName1 = « frontendIP »

$backendPoolName1 = « BackendPoolHTTP »

$lbrUleName1= « lbrUleHttp »

$healthProbeName= « HealthProbe »

$NSGName=”NSG-MultiIP-Alb »

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

Pour terminer le déploiement, procédez comme suit à l’aide des commandes PowerShell :

1. Création d’un groupe de ressources, d’un compte de stockage et d’un ensemble de disponibilité
2. Création d’un groupe de sécurité réseau et ajout de règles
3. Création d’un réseau virtuel et de trois sous-réseaux
4. Création d’adresses IP publiques
5. Création de configurations IP pour VPX1
6. Création de configurations IP pour VPX2
7. Création de cartes réseau pour VPX1
8. Création de cartes réseau pour VPX2
9. Créer VPX1
10. Créer VPX2
11. Créer un ALB

Créez un groupe de ressources, un compte de stockage et un jeu de disponibilité.

```
1 New-AzureRmResourceGroup -Name $rgName -Location $locName
2
3
4 $prmStorageAccount=New-AzureRMStorageAccount -Name
     $prmStorageAccountName -ResourceGroupName $rgName -Type Standard_LRS
      -Location $locName
5
```



```
6
7 $avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
     $rgName -Location $locName
```

Créez un groupe de sécurité réseau et ajoutez des règles.

```
1 $rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
     Description "Allow HTTP" -Access Allow -Protocol Tcp -Direction
     Inbound -Priority 101
2
3
4 -SourceAddressPrefix Internet -SourcePortRange * -
     DestinationAddressPrefix * -DestinationPortRange 80
5
6
7 $rule2 = New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
     Description "Allow HTTPS" -Access Allow -Protocol Tcp -Direction
     Inbound -Priority 110
8
9
10 -SourceAddressPrefix Internet -SourcePortRange * -
     DestinationAddressPrefix * -DestinationPortRange 443
11
12
13 $rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
     Description "Allow SSH" -Access Allow -Protocol Tcp -Direction
     Inbound -Priority 120
14
15
16 -SourceAddressPrefix Internet -SourcePortRange * -
     DestinationAddressPrefix * -DestinationPortRange 22
17
18
19 $nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
     Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

Créez un réseau virtuel et trois sous-réseaux.

```
1 $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
     $frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this
     parameter value should be as per your requirement)
2
3
4 $mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $mgmtSubnetName
      -AddressPrefix $mgmtSubnetRange
```



```
5
6
7  $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       $backEndSubnetName -AddressPrefix $backEndSubnetRange
8
9
10 $vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
       $rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
       $frontendSubnet,$backendSubnet, $mgmtSubnet
11
12
13 $subnetName ="frontEndSubnet"
14
15
16 $subnet1=$vnet.Subnets|?{
17  $_.Name -eq $subnetName }
18
19
20
21 $subnetName="backEndSubnet"
22
23
24 $subnet2=$vnet.Subnets|?{
25  $_.Name -eq $subnetName }
26
27
28
29 $subnetName="mgmtSubnet"
30
31
32 $subnet3=$vnet.Subnets|?{
33  $_.Name -eq $subnetName }
```

Créez des adresses IP publiques.

```
1  $pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
       $rgName -DomainNameLabel $domName1 -Location $locName -
       AllocationMethod Dynamic
2
3  $pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
       $rgName -DomainNameLabel $domName2 -Location $locName -
       AllocationMethod Dynamic
4
5  $pip3=New-AzureRmPublicIpAddress -Name $pubIPName3 -ResourceGroupName
       $rgName -DomainNameLabel $domName3 -Location $locName -
```



```
    AllocationMethod Dynamic
```

Créez des configurations IP pour VPX1.

```
$IpConfigName1 = "IPConfig1"


$IPAddress = "12.5.2.24"


$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip1
    -Primary


$IPConfigName3="IPConfig-3"


$IPAddress="12.5.1.27"


$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary


$IPConfigName4 = "IPConfig-4"


$IPAddress = "12.5.3.24"


$IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Créez des configurations IP pour VPX2.

```
$IpConfigName5 = "IPConfig5"


$IPAddress="12.5.2.26"


$IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip2
    -Primary
```



```
8
9
10 $IPConfigName7="IPConfig-7"
11
12
13 $IPAddress="12.5.1.28"
14
15
16 $IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
       Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19 $IPConfigName8="IPConfig-8"
20
21
22 $IPAddress="12.5.3.28"
23
24
25 $IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
       Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Créez des cartes réseau pour VPX1.

```
1 $nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig1 -
      NetworkSecurityGroupId $nsg.Id
2
3
4 $nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig3 -
      NetworkSecurityGroupId $nsg.Id
5
6
7 $nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig4 -
      NetworkSecurityGroupId $nsg.Id
```

Créez des cartes réseau pour VPX2.

```
1 $nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig5 -
      NetworkSecurityGroupId $nsg.Id
2
3
4 $nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
```



```
    $rgName -Location $locName -IpConfiguration $IpConfig7 -
    NetworkSecurityGroupId $nsg.Id
5
6
7 $nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig8 -
    NetworkSecurityGroupId $nsg.Id
```

Créez VPX1.

Cette étape comprend les sous-étapes suivantes :

- Créer un objet de configuration de machine virtuelle
- Définissez les informations d'identification, le système d'exploitation et l'image
- Ajouter des cartes réseau
- Spécifier le disque du système d'exploitation et créer une machine virtuelle

```
1  $suffixNumber = 1
2
3  $vmName=$vmNamePrefix + $suffixNumber
4
5  $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
       AvailabilitySetId $avSet.Id
6
7  $cred=Get-Credential -Message "Type the name and password for VPX
       login."
8
9  $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
       ComputerName $vmName -Credential $cred
10
11 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
       $publisher -Offer $offer -Skus $sku -Version $version
12
13 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.
       Id -Primary
14
15 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.
       Id
16
17 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.
       Id
18
19 $osDiskName=$vmName + "-" + $osDiskSuffix1
20
```



```
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/" + $osDiskName + ".vhd"

$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri $osVhdUri -CreateOption fromImage

Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -Name $sku

New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location $locName
```

Créez VPX2.

```
```
$suffixNumber=2

$vmName=$vmNamePrefix + $suffixNumber

$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avSet.Id

$cred=Get-Credential -Message "Type the name and password for VPX login."

$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName $vmName -Credential $cred

$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher -Offer $offer -Skus $sku -Version $version

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -Primary

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
```

 
```

```
27
28
29 $osDiskName=$vmName + "-" + $osDiskSuffix2
30
31
32 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/"
       + $osDiskName + ".vhd"
33
34
35 $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
      $osVhdUri -CreateOption fromImage
36
37
38 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
      Name $sku
39
40
41 New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
      $locName
42 <!--NeedCopy--> ```
```

Pour afficher les adresses IP privées et publiques affectées aux cartes réseau, tapez les commandes suivantes :

```
1 ```
2 $nic1.IPConfig
3
4
5 $nic2.IPConfig
6
7
8 $nic3.IPConfig
9
10
11 $nic4.IPConfig
12
13
14 $nic5.IPConfig
15
16
17 $nic6.IPConfig
18 <!--NeedCopy--> ```
```

Créer un équilibrage de charge Azure (ALB).

Cette étape comprend les sous-étapes suivantes :

- Création d'une configuration IP frontale
- Créer une sonde de santé
- Créer un pool d'adresses back-end
- Créer des règles d'équilibrage de charge (HTTP et SSL)
- Créer un ALB avec la configuration IP frontale, le pool d'adresses backend et la règle LB
- Associer la configuration IP à des pools dorsaux

```
$frontEndIP1=New-AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName1
 -PublicIpAddress $pip3

$healthProbe=New-AzureRmLoadBalancerProbeConfig -Name $healthProbeName
-Protocol Tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2

$beAddressPool1=New-AzureRmLoadBalancerBackendAddressPoolConfig -Name
$backendPoolName1

$lbRule1=New-AzureRmLoadBalancerRuleConfig -Name $lbRuleName1 -FrontendIpConfigur
 $frontEndIP1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe -
Protocol Tcp -FrontendPort 80 -BackendPort 80 -EnableFloatingIP

$lb=New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name $lbName -
Location $locName -FrontendIpConfiguration $frontEndIP1 -LoadBalancingRule
 $lbRule1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe

$nic2.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$nic5.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$lb=$lb |Set-AzureRmLoadBalancer

$nic2=$nic2 | Set-AzureRmNetworkInterface

$nic5=$nic5 | Set-AzureRmNetworkInterface
```

Une fois que vous avez déployé avec succès la paire NetScaler VPX, connectez-vous à chaque instance VPX pour configurer les adresses HA-INC, SNIP et VIP.

1. Tapez la commande suivante pour ajouter des nœuds HA.

   ```
   add ha node 1 PeerNodeNSIP -inc Enabled
   ```

2. Ajouter des adresses IP privées de cartes réseau côté client en tant que SNIP pour VPX1 (NIC2) et VPX2 (NIC5)


```
add nsip privateIPofNIC2 255.255.255.0 -type SNIP
add nsip privateIPofNIC5 255.255.255.0 -type SNIP
```

3. Ajoutez un serveur virtuel d'équilibrage de charge sur le nœud principal avec l'adresse IP frontale (IP publique) d'ALB.

```
add lb virtual server v1 HTTP FrontEndIPofALB 80
```

Ressources connexes :

Configuration de GSLB sur un déploiement HA actif de secours sur Azure

Déployez une paire de haute disponibilité NetScaler sur Azure avec ALB en mode IP flottant désactivé

May 5, 2023

Vous pouvez déployer deux instances NetScaler VPX avec plusieurs cartes réseau dans une configuration de haute disponibilité (HA) active-passive sur Azure. Chaque carte réseau peut contenir de nombreuses adresses IP.

Un déploiement actif-passif nécessite :

- Configuration INC (Independent Network Configuration) de haute disponibilité
- L'Azure Load Balancer (ALB) avec :
  - Mode adresse IP flottante ou mode Direct Server Return (DSR)
  - Mode adresse IP flottante désactivé

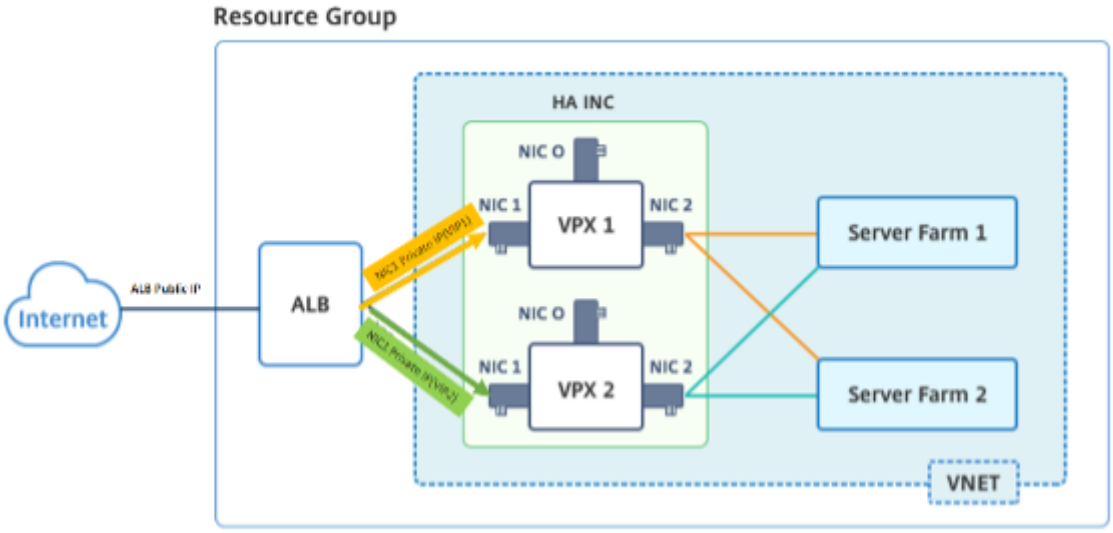
Pour plus d'informations sur les options IP flottantes ALB, consultez la documentation Azure.

Si vous souhaitez déployer une paire VPX dans une configuration HA active-passive sur Azure avec IP flottante ALB activée, consultez Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell.

Architecture de déploiement HA avec ALB en mode adresse IP flottante désactivé

Dans un déploiement actif-passif, les adresses IP privées de l'interface client de chaque instance sont ajoutées en tant qu'adresses VIP dans chaque instance VPX. Configurez en mode HA-INC avec des adresses VIP partagées à l'aide d'IPSet et des adresses SNIP spécifiques à une instance. L'ensemble du trafic passe par l'instance principale. L'instance secondaire est en mode veille jusqu'à ce que l'instance principale tombe en panne.

Schéma : Exemple d'architecture de déploiement actif-passif



Composants requis

Vous devez connaître les informations suivantes avant de déployer une instance NetScaler VPX sur Azure.

- Terminologie Azure et détails réseau. Pour plus d'informations, consultez la section Terminologie Azure.
- Fonctionnement d'une appliance NetScaler. Pour plus d'informations, consultez la documentation de NetScaler.
- Réseau NetScaler. Pour plus d'informations, consultez la section Réseau ADC.
- Configuration de l'équilibreur de charge Azure et des règles d'équilibrage de charge. Pour plus d'informations, consultez la documentation Azure ALB.

Comment déployer une paire VPX HA sur Azure avec l'IP flottante ALB désactivée

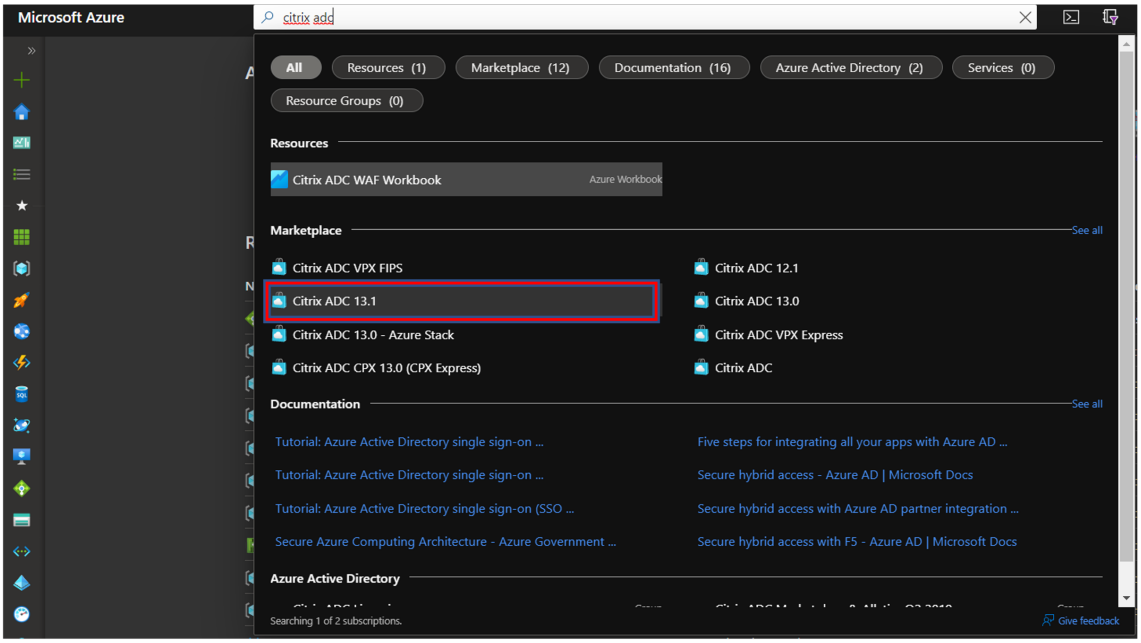
Voici un résumé des étapes de déploiement HA et ALB :

1. Déployez deux instances VPX (instances principales et secondaires) sur Azure.
2. Ajoutez une carte réseau client et serveur sur les deux instances.
3. Déployez un ALB avec une règle d'équilibrage de charge dont le mode adresse IP flottante est désactivé.
4. Configurez les paramètres HA sur les deux instances à l'aide de l'interface graphique NetScaler.

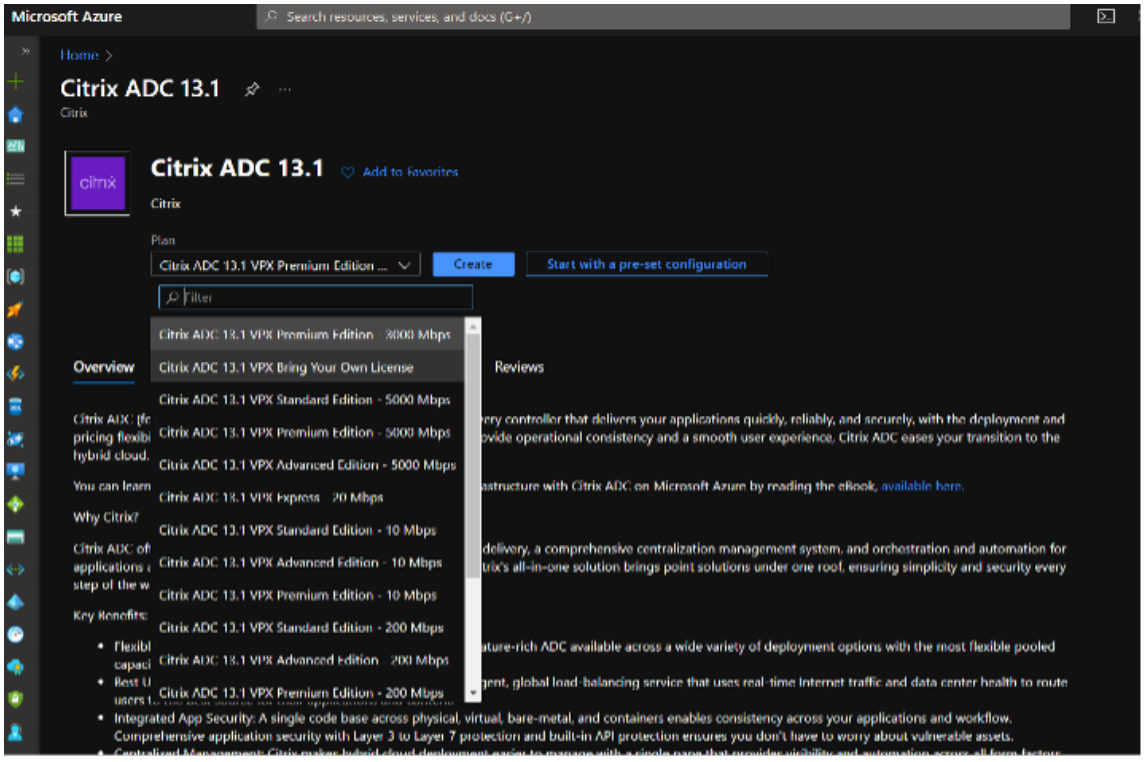
Étape 1. Déployez deux instances VPX sur Azure.

Créez deux instances VPX en suivant ces étapes :

1. Sélectionnez la version de NetScaler sur Azure Marketplace (dans cet exemple, la version 13.1 de NetScaler est utilisée).

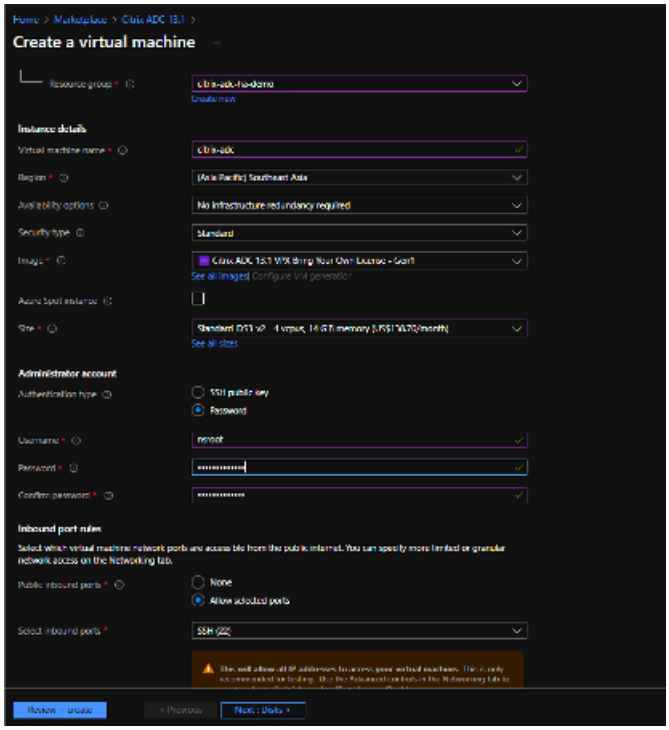


2. Sélectionnez le mode de licence ADC requis, puis cliquez sur **Créer**.



La page **Créer une machine virtuelle** s'ouvre.

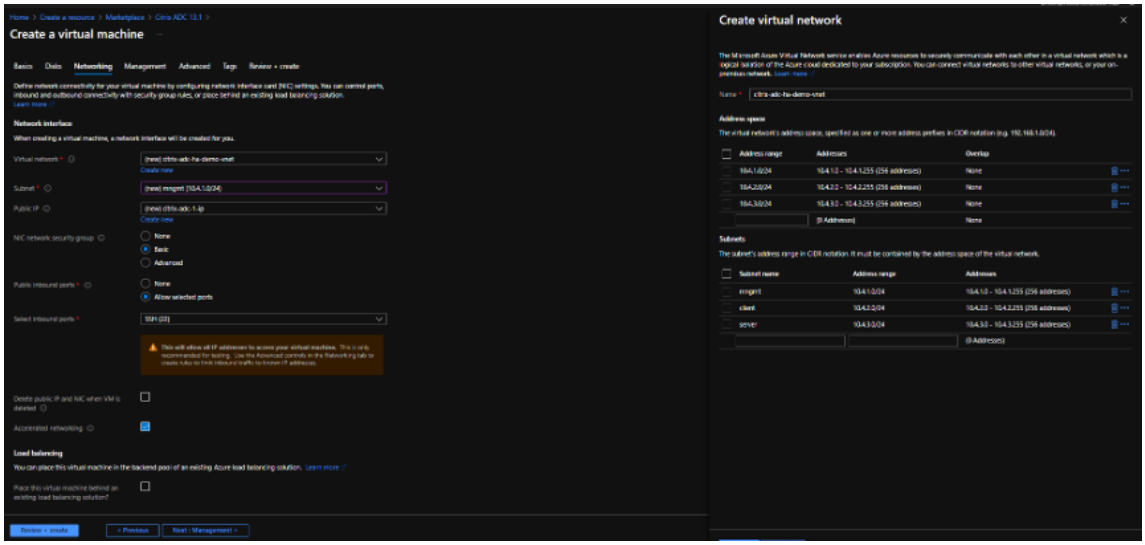
3. Renseignez les informations requises dans chaque onglet pour un déploiement réussi.



4. Dans l'onglet **Mise en réseau**, créez un nouveau réseau virtuel avec 3 sous-réseaux, un pour chacun : les cartes réseau de gestion, de client et de serveur. Sinon, vous pouvez également utiliser un réseau virtuel existant. La carte réseau de gestion est créée lors du déploiement de la VM. Les cartes réseau client et serveur sont créées et attachées après la création de la machine virtuelle. Pour le groupe de sécurité réseau de la carte réseau, vous pouvez effectuer l'une des opérations suivantes :

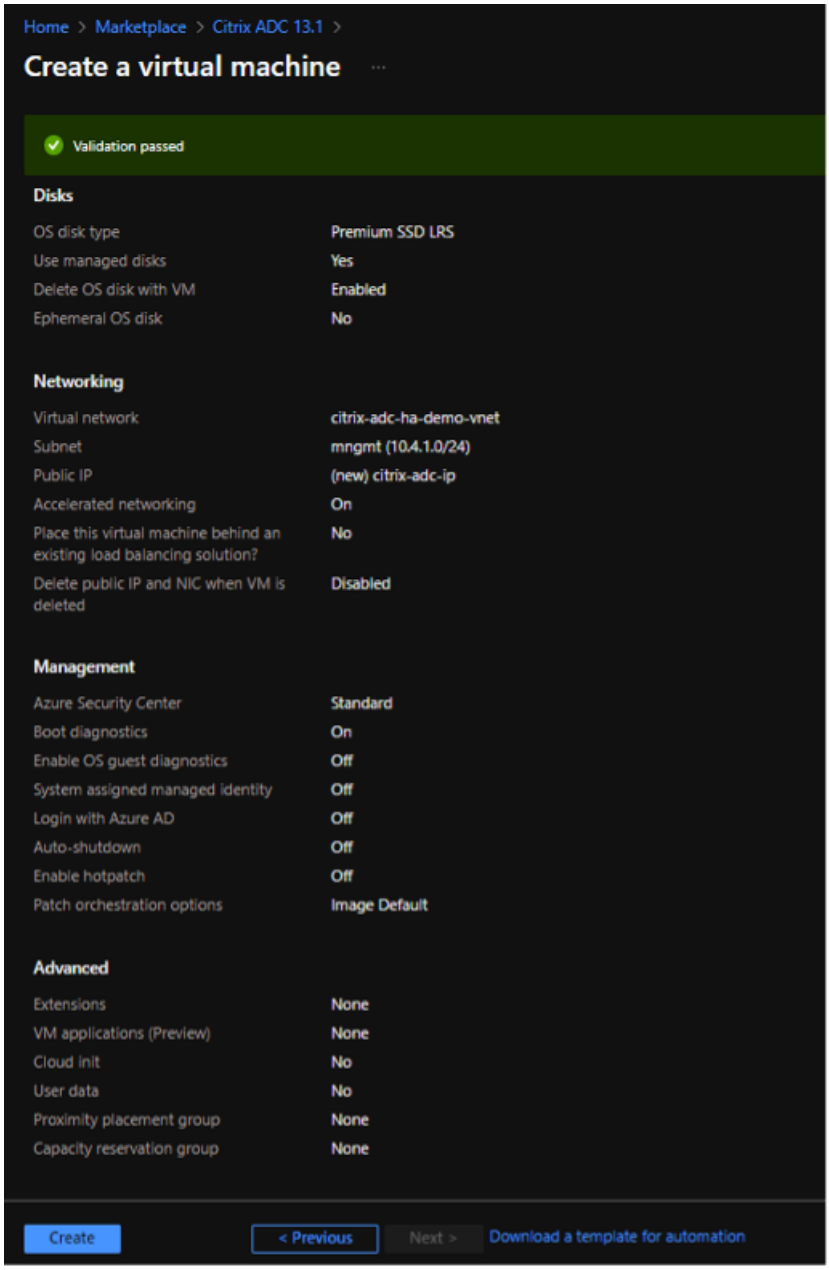
   - Sélectionnez **Avancé** et utilisez un groupe de sécurité réseau existant qui répond à vos besoins.
   - Sélectionnez **Basic** et sélectionnez les ports requis.

   > **Remarque :**
   >
   > Vous pouvez également modifier les paramètres du groupe de sécurité réseau une fois le déploiement de la machine virtuelle terminé.

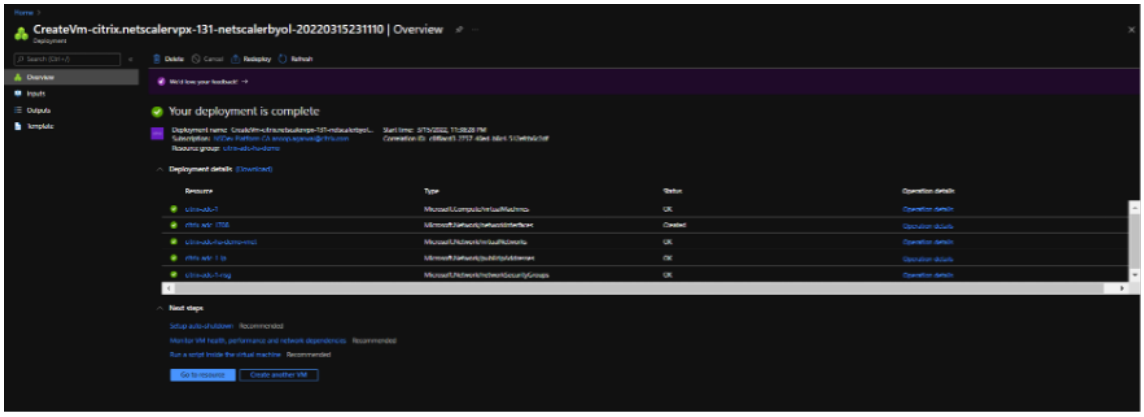


5. Cliquez sur Suivant : **Réviser + créer**.

   Une fois la validation réussie, passez en revue les paramètres de base, les configurations de machines virtuelles, le réseau et les paramètres supplémentaires, puis cliquez sur **Créer**.



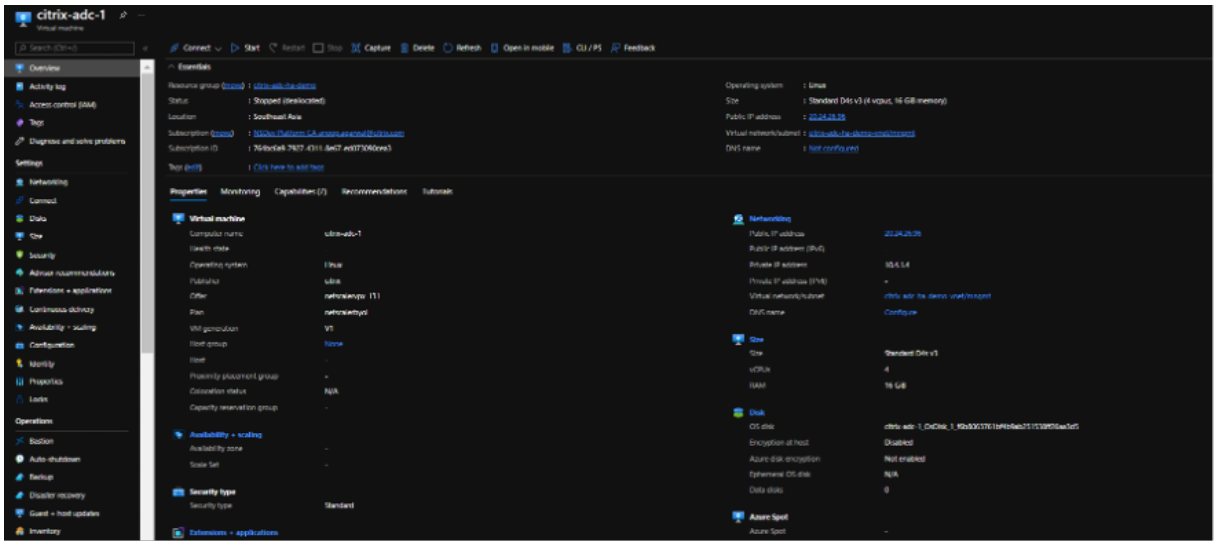
6. Une fois le déploiement terminé, cliquez sur **Go to Resource** pour voir les détails de configuration.



De même, déployez une seconde instance NetScaler VPX.

Étape 2. Ajoutez des cartes réseau client et serveur sur les deux instances.

> **Remarque :**
>
> Pour associer davantage de cartes réseau, vous devez d'abord arrêter la machine virtuelle. Dans le portail Azure, sélectionnez la machine virtuelle que vous souhaitez arrêter. Dans l'onglet **Aperçu**, cliquez sur **Arrêter**. Attendez que Status indique **Stopped**.

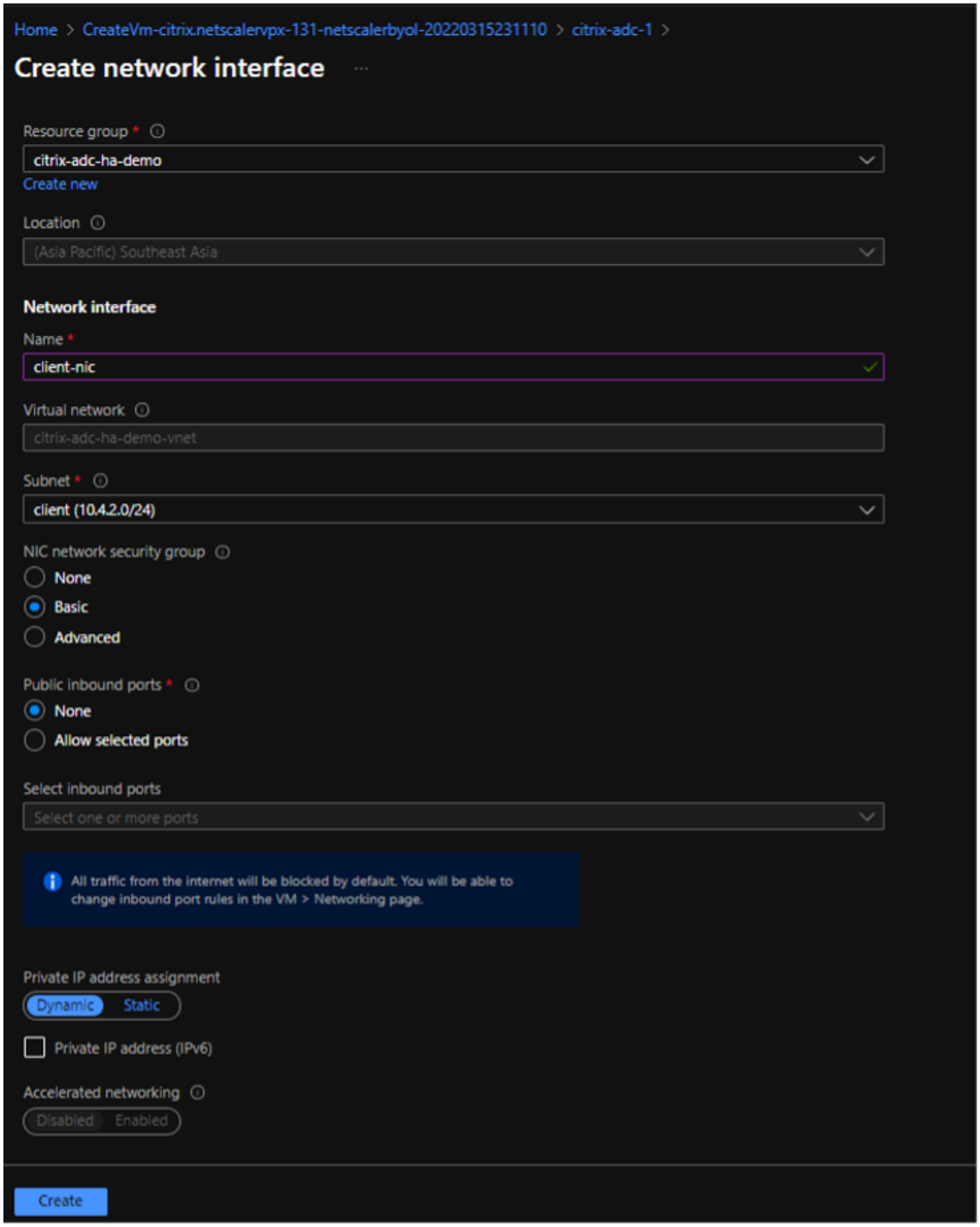


Pour ajouter une carte réseau cliente sur l'instance principale, procédez comme suit :

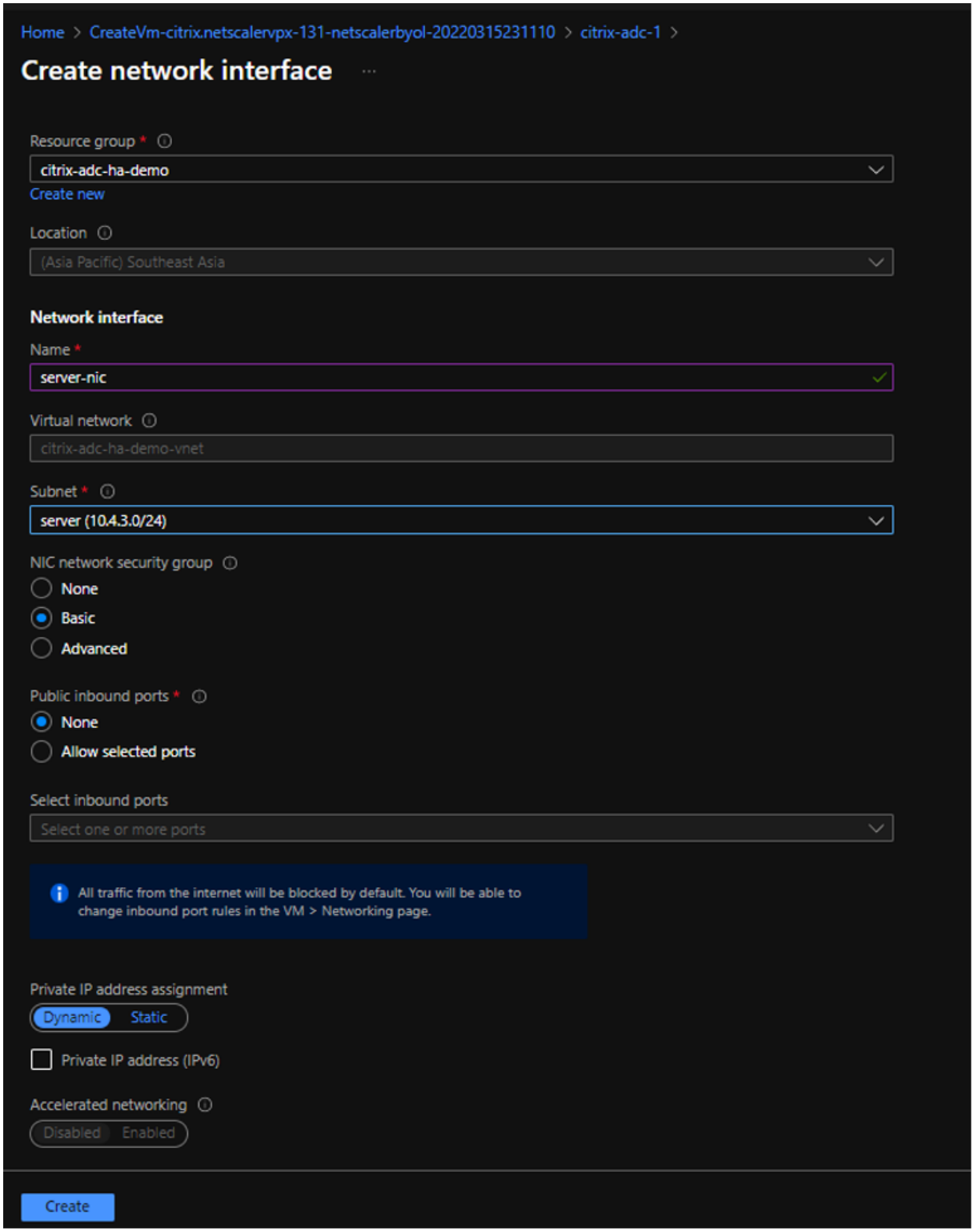
1. Accédez à **Mise en réseau > Connecter une interface réseau**.

   Vous pouvez sélectionner une carte réseau existante ou créer et associer une nouvelle interface.

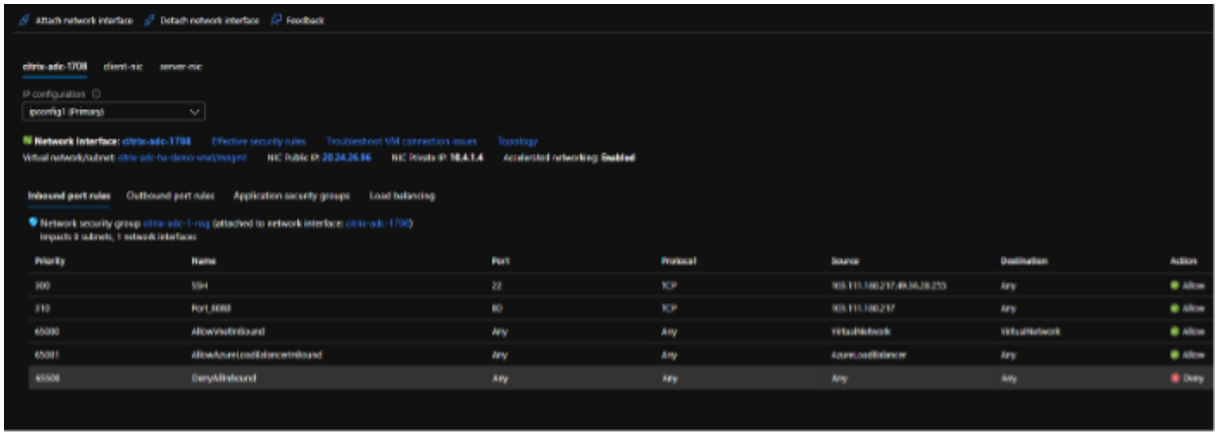
2. Pour le groupe de sécurité réseau de la carte réseau, vous pouvez utiliser un groupe de sécurité réseau existant en sélectionnant **Avancé** ou en créer un en sélectionnant **Basic**.



Pour ajouter une carte réseau de serveur, suivez les mêmes étapes que pour ajouter une carte réseau client.



Les trois cartes réseau (carte réseau de gestion, carte réseau client et carte réseau serveur) sont connectées à l'instance NetScaler VPX.

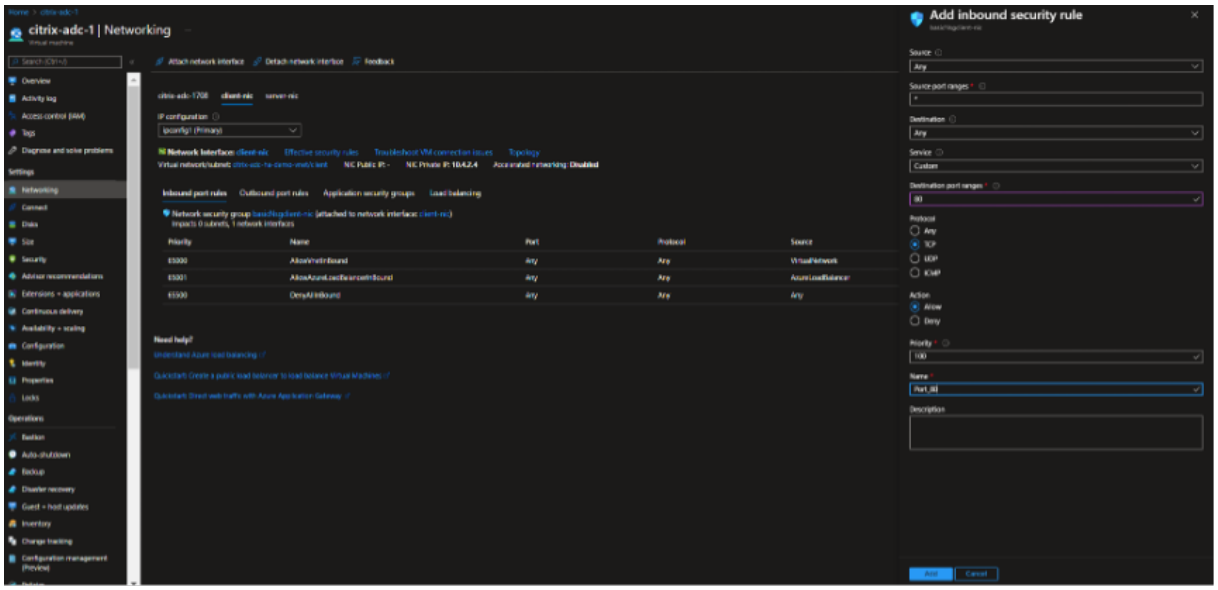


Répétez les étapes précédentes pour ajouter des cartes réseau sur l'instance secondaire.

Après avoir créé et attaché des cartes réseau sur les deux instances, redémarrez-les en accédant à **Overview > Start**.

> **Remarque :**
>
> Vous devez autoriser le trafic via le port dans la règle entrante de la carte réseau cliente, qui sera utilisée ultérieurement pour créer un serveur virtuel d'équilibrage de charge lors de la configuration de l'instance NetScaler VPX.

Dans l'exemple suivant, un port HTTP 80 est ajouté à la règle de sécurité entrante.

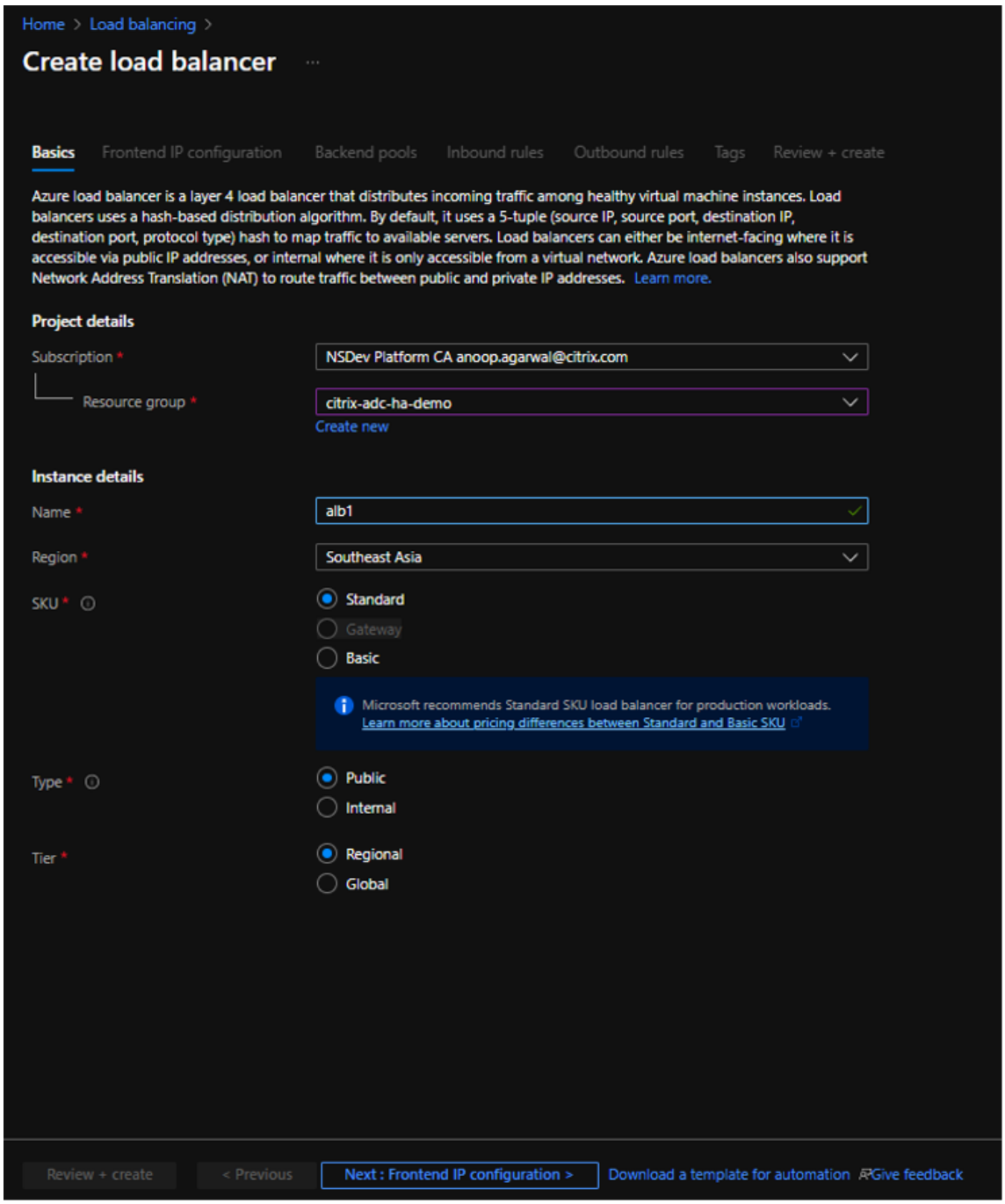


Étape 3. Déployez un ALB avec une règle d'équilibrage de charge dont le mode adresse IP flottante est désactivé.

Pour démarrer la configuration d'ALB, procédez comme suit :

1. Accédez à la page **Load Balancers** et cliquez sur **Create**.
2. Sur la page **Créer un équilibreur** de charge, fournissez les détails nécessaires.

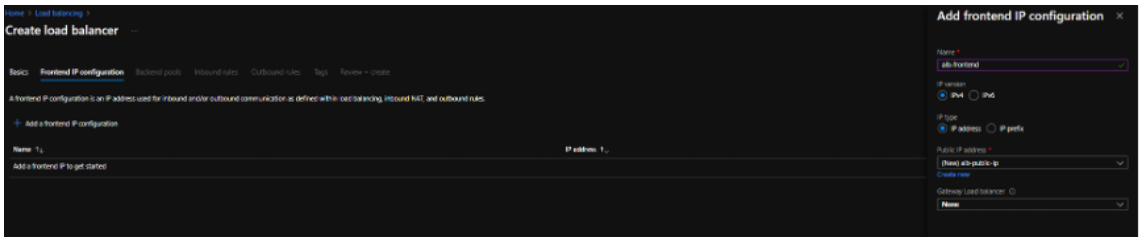
Dans l'exemple suivant, nous déployons un équilibreur de charge public régional de SKU standard.



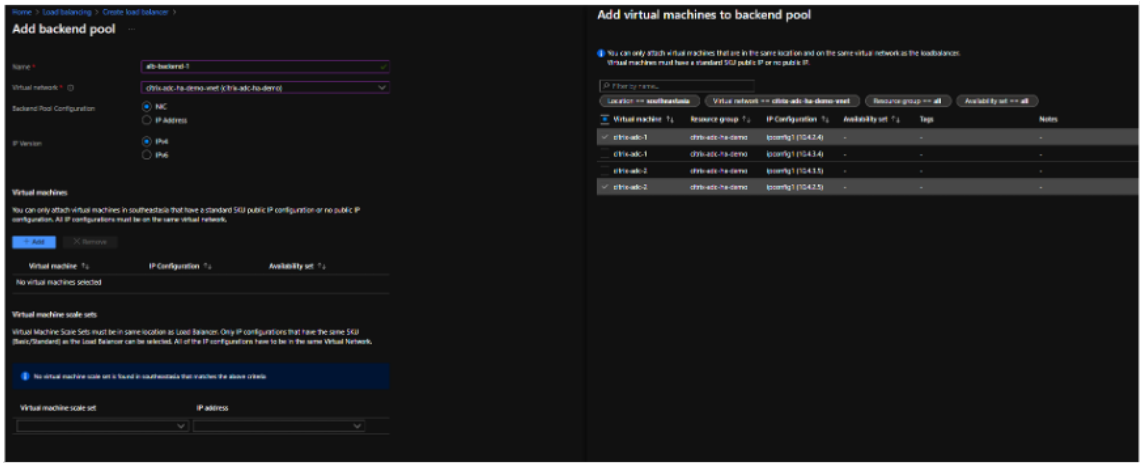
> **Remarque :**
>
> Toutes les adresses IP publiques associées aux machines virtuelles NetScaler doivent avoir le même SKU que celui d'ALB. Pour plus d'informations sur les SKU ALB, consultez la documentation des SKU de l'équilibreur de charge Azure.

3. Dans l'onglet **Configuration IP Frontend**, créez une adresse IP ou utilisez une adresse IP exis-

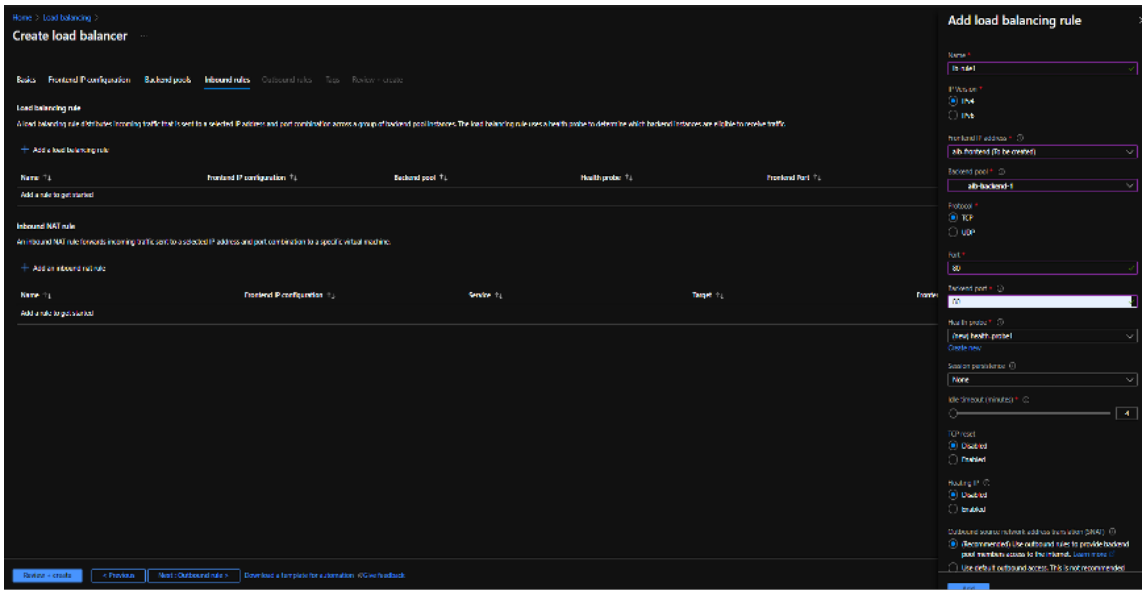
tante.



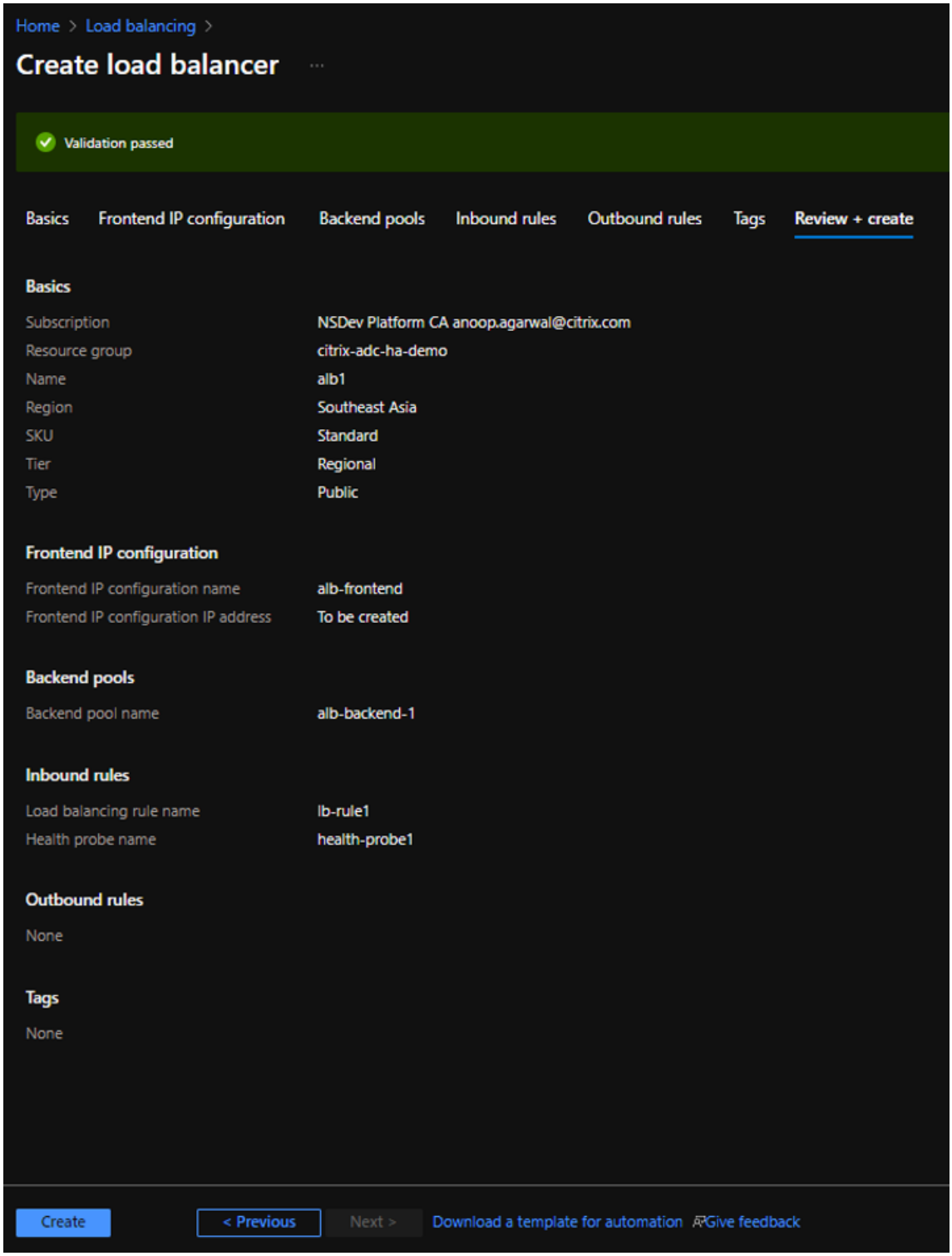
4. Dans l'onglet **Pools de backend**, sélectionnez la configuration du pool de backend basée sur les cartes réseau et ajoutez les cartes réseau clientes des deux machines virtuelles NetScaler.



5. Dans l'onglet **Inbound rules (Règles entrantes**), cliquez sur **Add a Load balancing rule (Ajouter une**règle d'équilibrage de charge) et indiquez l'adresse IP du frontend et le pool backend créés au Sélectionnez le protocole et le port en fonction de vos besoins. Créez ou utilisez une sonde d'intégrité existante. L'option IP flottante doit être définie sur **Désactivé**.



6. Cliquez sur **Réviser + Créer**. Une fois la validation passée, cliquez sur **Créer**.



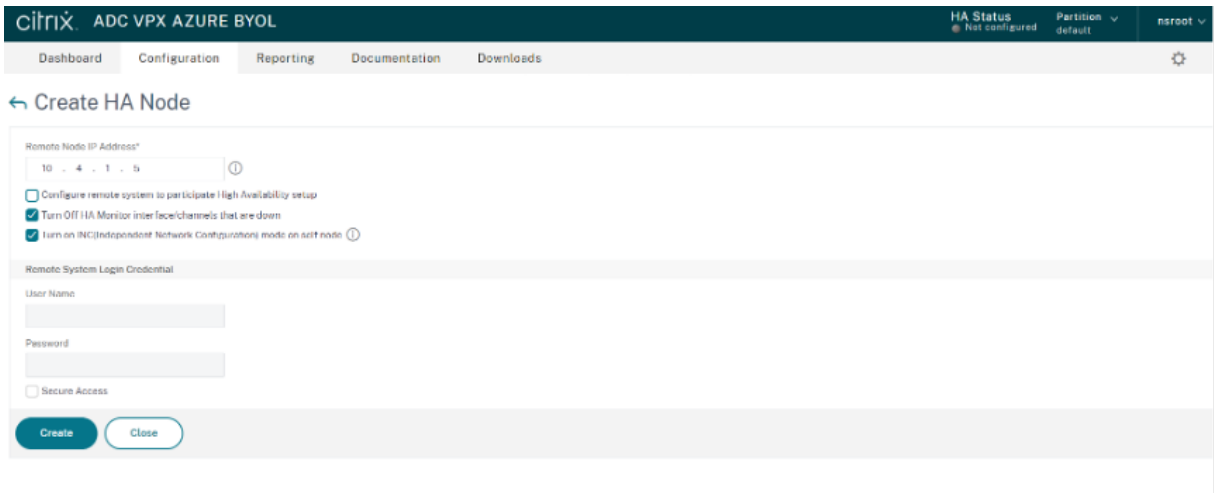
Étape 4. Configurez les paramètres HA sur les deux instances de NetScaler VPX à l'aide de l'interface graphique de NetScaler.

Après avoir créé les instances NetScaler VPX sur Azure, vous pouvez configurer HA à l'aide de l'interface graphique NetScaler.

Étape 1. Configurez la haute disponibilité en mode INC sur les deux instances.

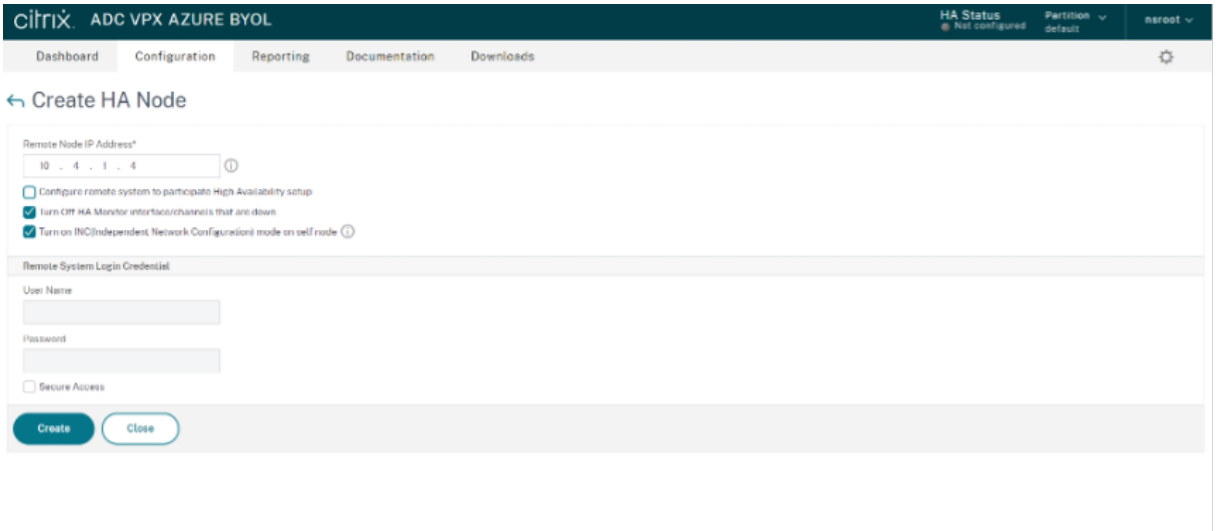
Sur l'instance principale, effectuez les étapes suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et le mot de passe fournis lors du déploiement de l'instance.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion de l'instance secondaire, par exemple : 10.4.1.5.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.



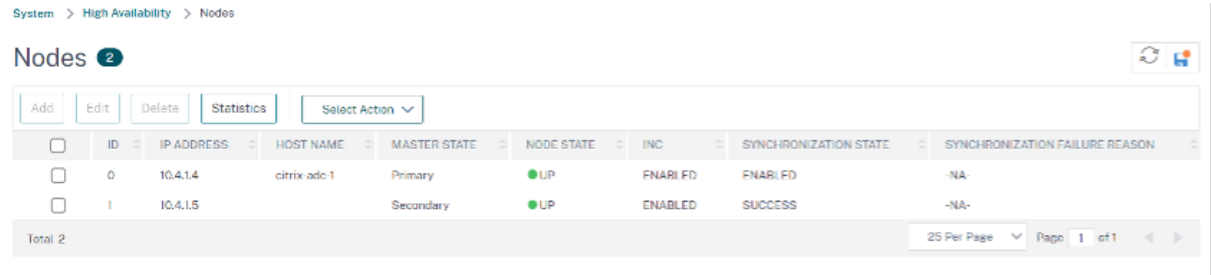
Sur l'instance secondaire, effectuez les étapes suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et le mot de passe fournis lors du déploiement de l'instance.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion de l'instance principale, par exemple : 10.4.1.4.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.



Avant de poursuivre, assurez-vous que l' **état de synchronisation de l'** instance secondaire est indiqué comme **SUCCESS** sur la page **Nodes** .

> **Remarque :**
>
> L'instance secondaire possède désormais les mêmes informations d'identification de connexion que l'instance principale.



Étape 2. Ajoutez une adresse IP virtuelle et une adresse IP de sous-réseau sur les deux instances.

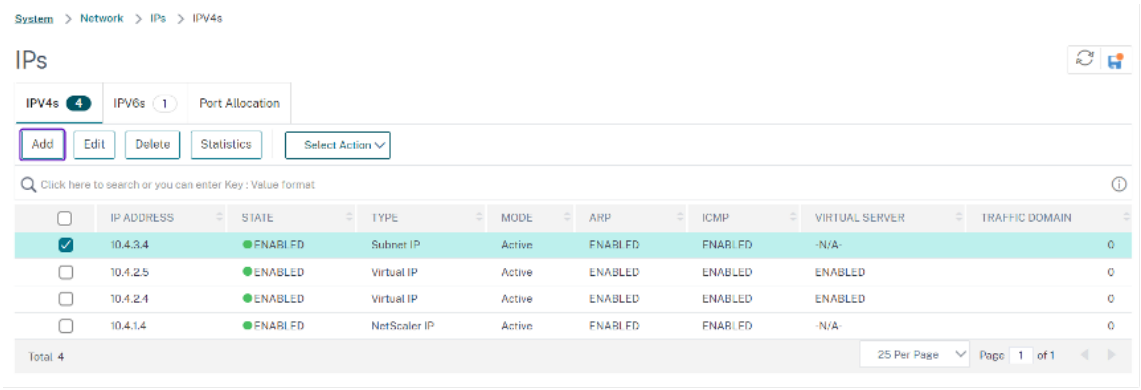
Sur l'instance principale, effectuez les étapes suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Ajoutez une adresse VIP principale en procédant comme suit :
    a) Entrez l'adresse IP privée de la carte réseau client de l'instance principale et le masque de réseau configuré pour le sous-réseau client dans l'instance de VM.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
    c) Cliquez sur **Create**.
3. Ajoutez une adresse SNIP principale en procédant comme suit :
    a) Entrez l'adresse IP interne de la carte réseau du serveur de l'instance principale et le masque de réseau configuré pour le sous-réseau du serveur dans l'instance principale.

b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Create**.

4. Ajoutez une adresse VIP secondaire en procédant comme suit :

a) Entrez l'adresse IP interne de la carte réseau client de l'instance secondaire et le masque de réseau configuré pour le sous-réseau client dans l'instance de VM.
b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
c) Cliquez sur **Create**.



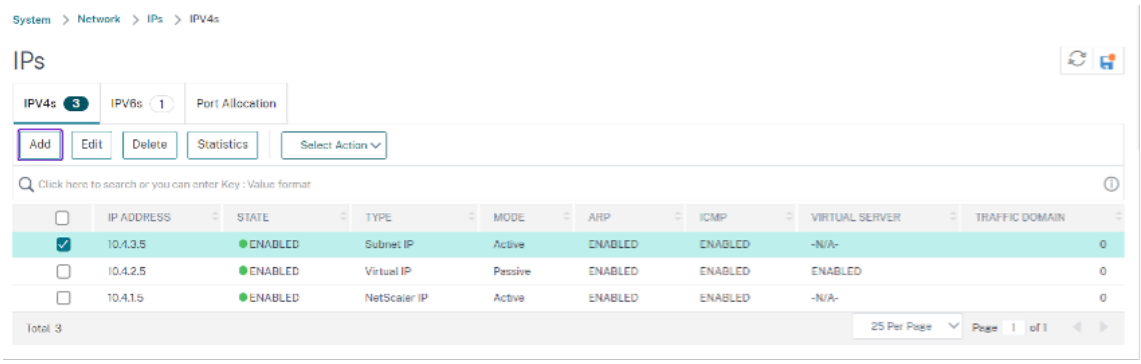
Sur l'instance secondaire, effectuez les étapes suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Ajoutez une adresse VIP secondaire en procédant comme suit :

a) Entrez l'adresse IP interne de la carte réseau client de l'instance secondaire et le masque de réseau configuré pour le sous-réseau client dans l'instance de VM.
b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.

3. Ajoutez une adresse SNIP secondaire en procédant comme suit :

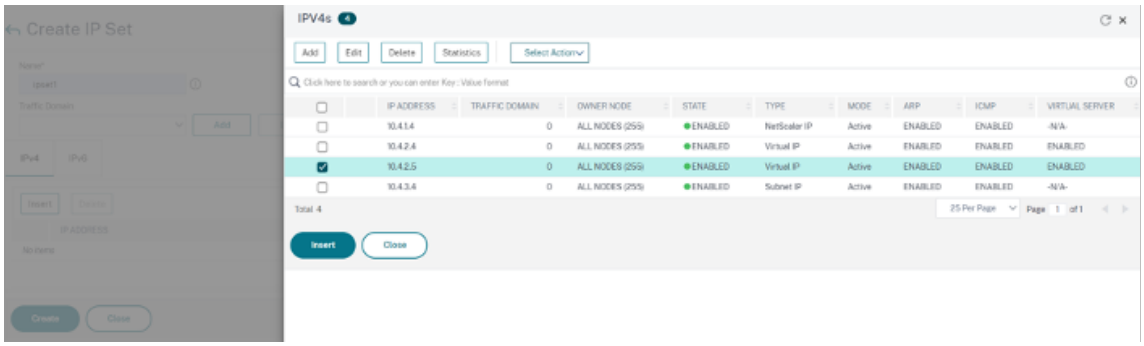
a) Entrez l'adresse IP interne de la carte réseau du serveur de l'instance secondaire et le masque de réseau configuré pour le sous-réseau du serveur dans l'instance secondaire.
b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Create**.



Étape 3. Ajoutez un ensemble d'adresses IP et liez le jeu d'adresses IP au VIP secondaire sur les deux instances.

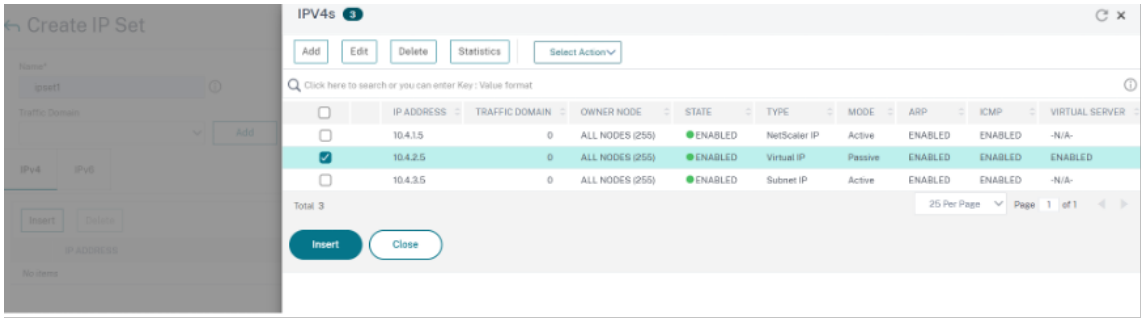
Sur l'instance principale, effectuez les étapes suivantes :

1. Accédez à **Système > Réseau > Ensembles d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.
4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.



Sur l'instance secondaire, effectuez les étapes suivantes :

1. Accédez à **Système > Réseau > Ensembles d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'adresse IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.
4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.

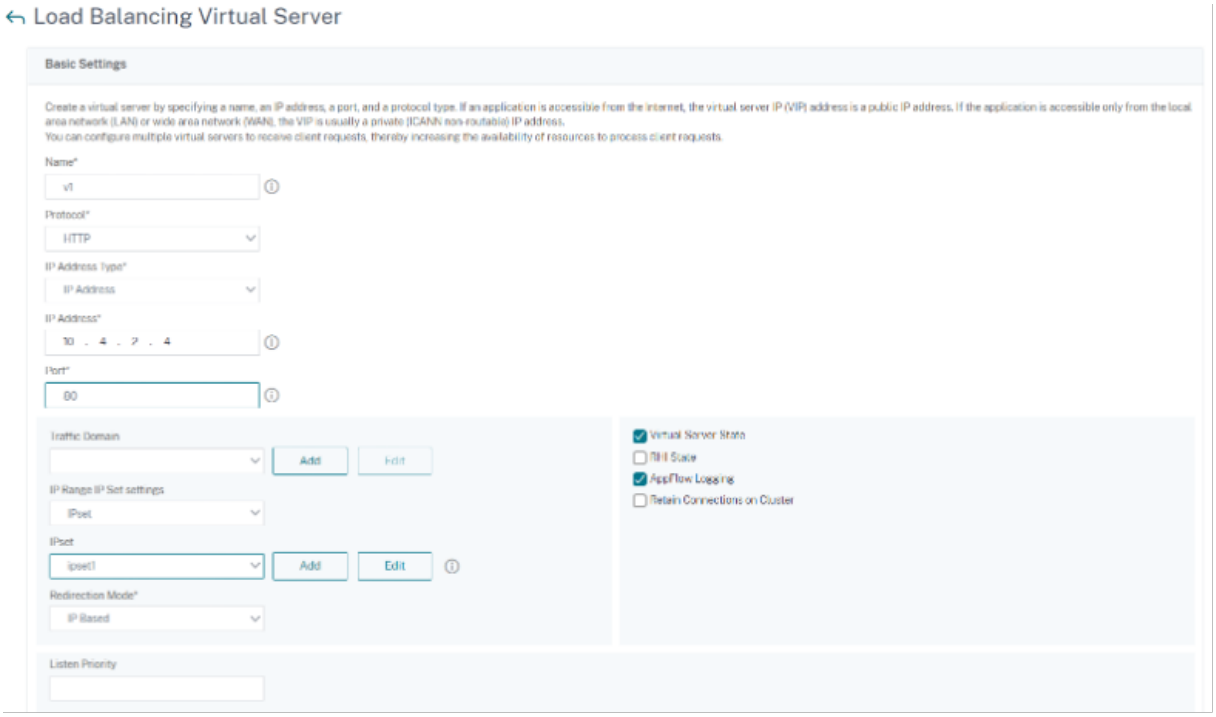


> **Remarque :**
>
> Le nom de l'ensemble d'adresses IP doit être identique sur les instances principale et secondaire.

Étape 4. Ajoutez un serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.
2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (VIP principale) et le port.

3. Cliquez sur **Plus**. Accédez à **Paramètres du jeu d'adresses IP de plage IP**, sélectionnez **IPset** dans le menu déroulant et indiquez l'IPSet créé à l' **étape 3**.
4. Cliquez sur **OK** pour créer le serveur virtuel d'équilibrage de charge.

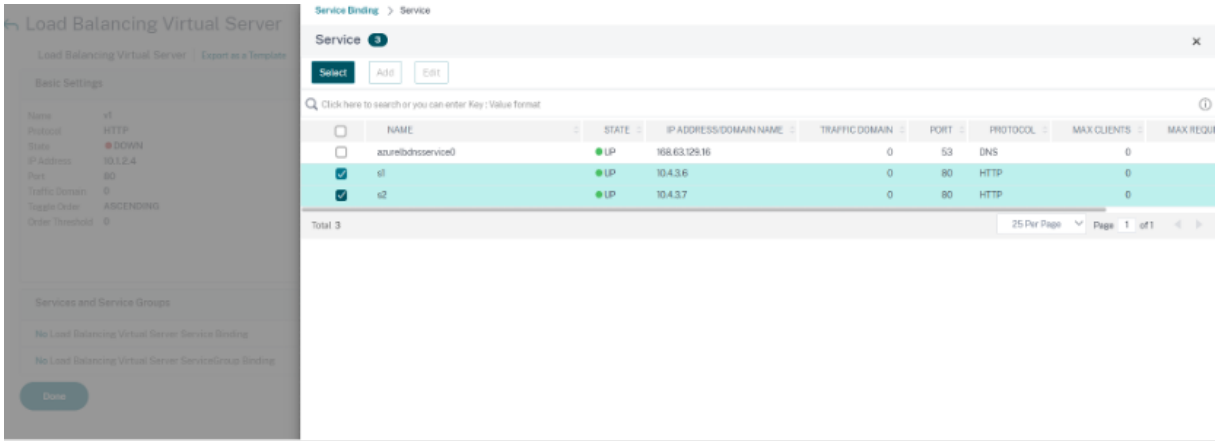


Étape 5. Ajoutez un service ou un groupe de services sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 6. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 4**, puis cliquez sur **Modifier**.
3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l' **étape 5**, puis cliquez sur **Lier**.



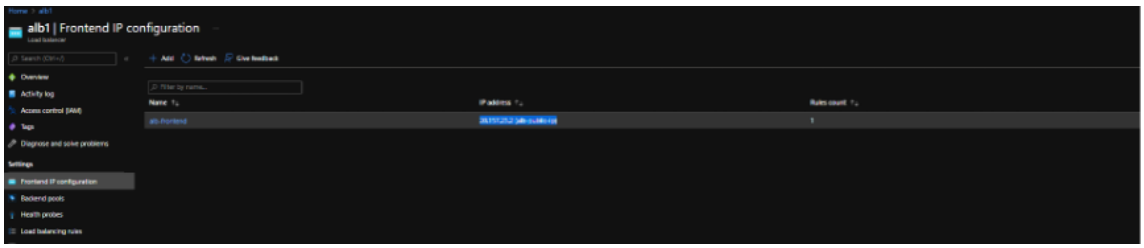
Étape 7. Enregistrez la configuration.

Sinon, toute la configuration est perdue après un redémarrage ou s'il y a un redémarrage instantané.

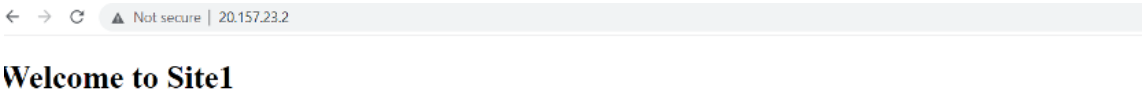
Étape 8. Vérifiez la configuration.

Assurez-vous que l'adresse IP du frontend ALB est accessible après un basculement.

1. Copiez l'adresse IP de l'interface ALB.



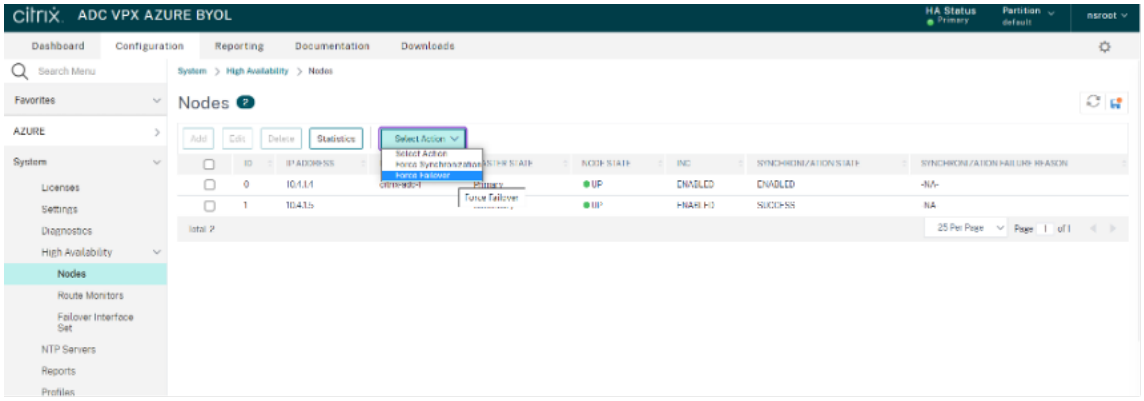
2. Collez l'adresse IP dans le navigateur et assurez-vous que les serveurs principaux sont accessibles.



Welcome to Site1

3. Sur l'instance principale, effectuez un basculement :

   Depuis l'interface graphique de NetScaler, accédez à **Configuration > Système > Haute disponibilité > Action > Forcer**le basculement.



4. Assurez-vous que les serveurs back-end sont accessibles après le basculement via l'IP frontend ALB utilisée précédemment.

Configurer une instance NetScaler VPX pour utiliser le réseau accéléré Azure

May 5, 2023

La mise en réseau accélérée permet la carte réseau (VF) à fonction virtuelle (SR-IOV) de virtualisation d'E/S à racine unique sur une machine virtuelle, ce qui améliore les performances réseau. Vous pouvez utiliser cette fonctionnalité avec des charges de travail lourdes qui doivent envoyer ou recevoir des données à un débit supérieur avec un streaming fiable et une utilisation réduite du processeur. Lorsqu'une carte réseau est activée avec une mise en réseau accélérée, Azure associe l'interface para virtualisée (PV) existante de la carte réseau à une interface VF SR-IOV. La prise en charge de l'interface SR-IOV VF active et améliore le débit de l'instance NetScaler VPX.

La mise en réseau accélérée offre les avantages suivants :

- Latence inférieure
- Performances supérieures des paquets par seconde (pps)
- Débit amélioré
- gigue réduite
- Utilisation réduite du processeur

> Remarque
>
> La mise en réseau accélérée Azure est prise en charge sur les instances NetScaler VPX à partir de la version 13.0 build 76.29.

Composants requis

- Assurez-vous que la taille de votre machine virtuelle correspond aux exigences relatives à la mise en réseau accélérée Azure.
- Arrêtez les machines virtuelles (individuelles ou dans un jeu de disponibilité) avant d'activer la mise en réseau accélérée sur n'importe quelle carte réseau.

Limitations

La mise en réseau accélérée peut être activée uniquement sur certains types d'instances. Pour plus d'informations, voir Types d'instances pris en charge.

cartes réseau prises en charge pour une mise en réseau accélérée

Azure fournit des cartes réseau Mellanox ConnectX3 et ConnectX4 en mode SR-IOV pour une mise en réseau accélérée.

Lorsque la mise en réseau accélérée est activée sur une interface NetScaler VPX, Azure associe l'interface ConnectX3 ou ConnectX4 à l'interface PV existante d'une appliance NetScaler VPX.

Pour plus d'informations sur l'activation d'une mise en réseau accélérée avant d'attacher une interface à une machine virtuelle, voir Créer une interface réseau avec une mise en réseau accélérée.

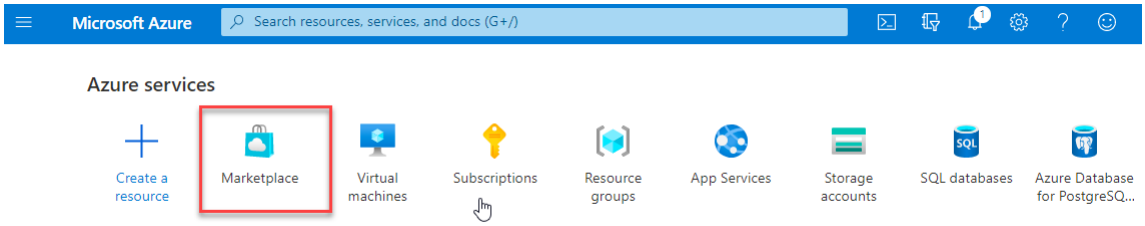
Pour plus d'informations sur l'activation d'une mise en réseau accélérée sur une interface existante sur une machine virtuelle, voir Activer les interfaces existantes sur une machine virtuelle.

Comment activer la mise en réseau accélérée sur une instance NetScaler VPX à l'aide de la console Azure

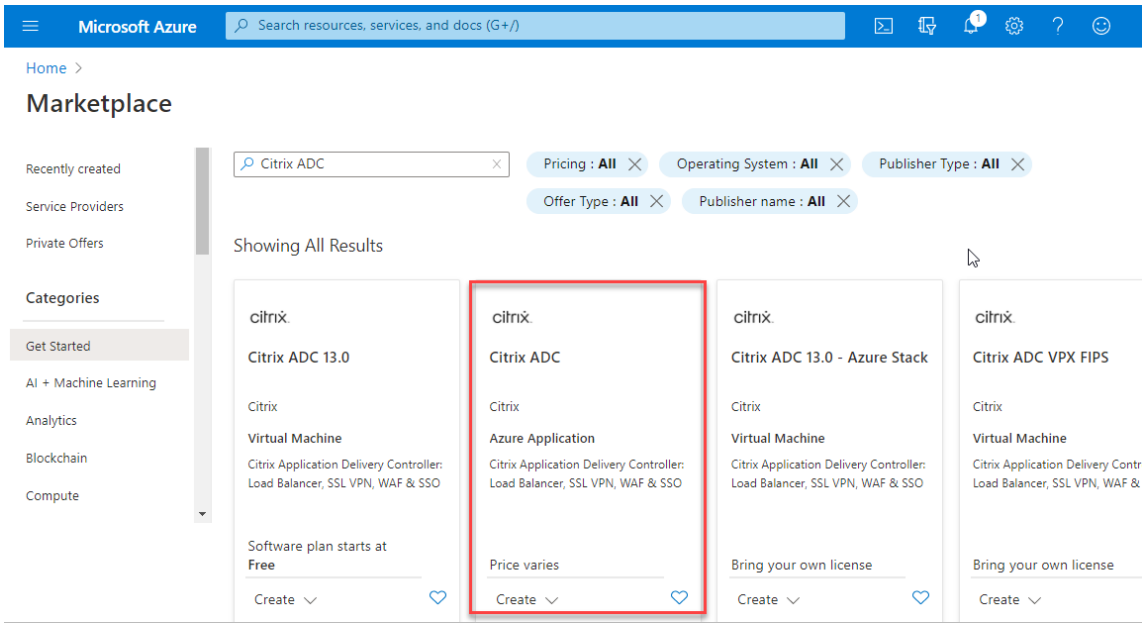
Vous pouvez activer la mise en réseau accélérée sur une interface spécifique à l'aide de la console Azure ou d'Azure PowerShell.

Procédez comme suit pour activer la mise en réseau accélérée à l'aide de jeux de disponibilité ou de zones de disponibilité Azure.

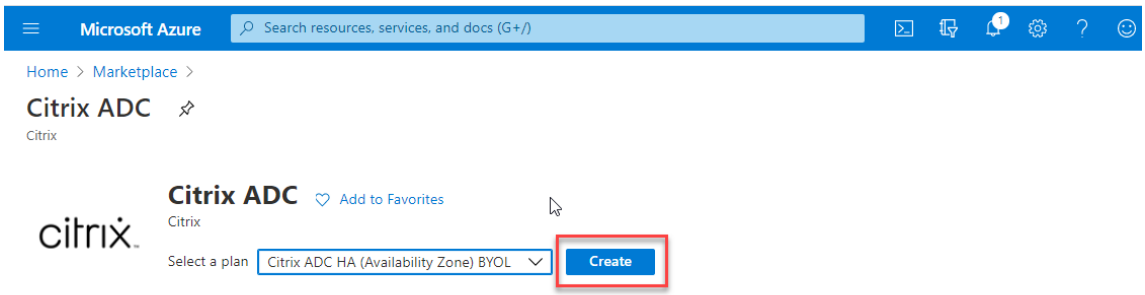
1. Connectez-vous au portail Azureet accédez à **Azure Marketplace**.



2. Sur **Azure Marketplace**, recherchez **NetScaler**.

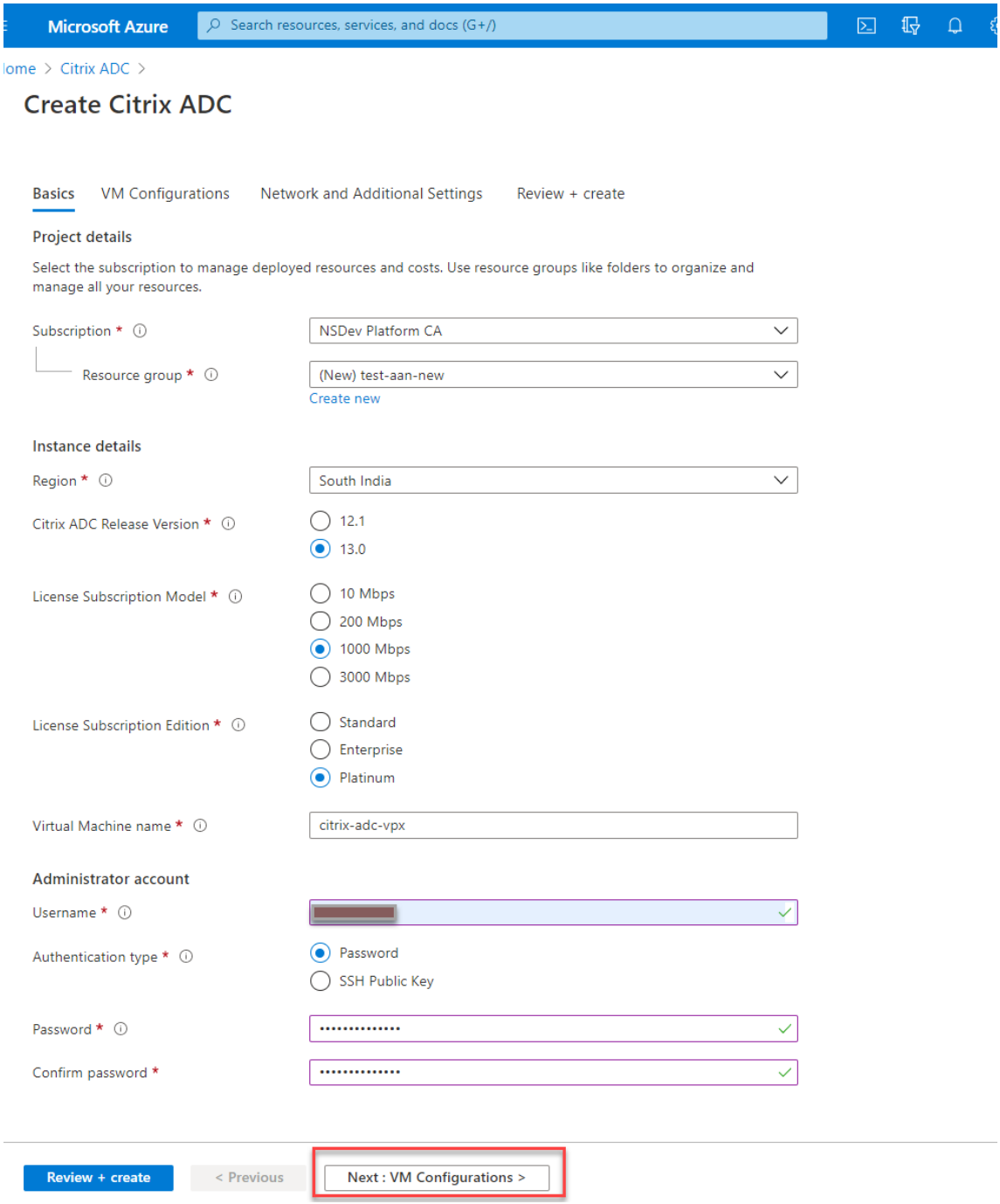


3. **Sélectionnez un plan NetScaler non FIPS ainsi qu'une licence, puis cliquez sur Créer.**



La page **Créer un NetScaler** s'affiche.

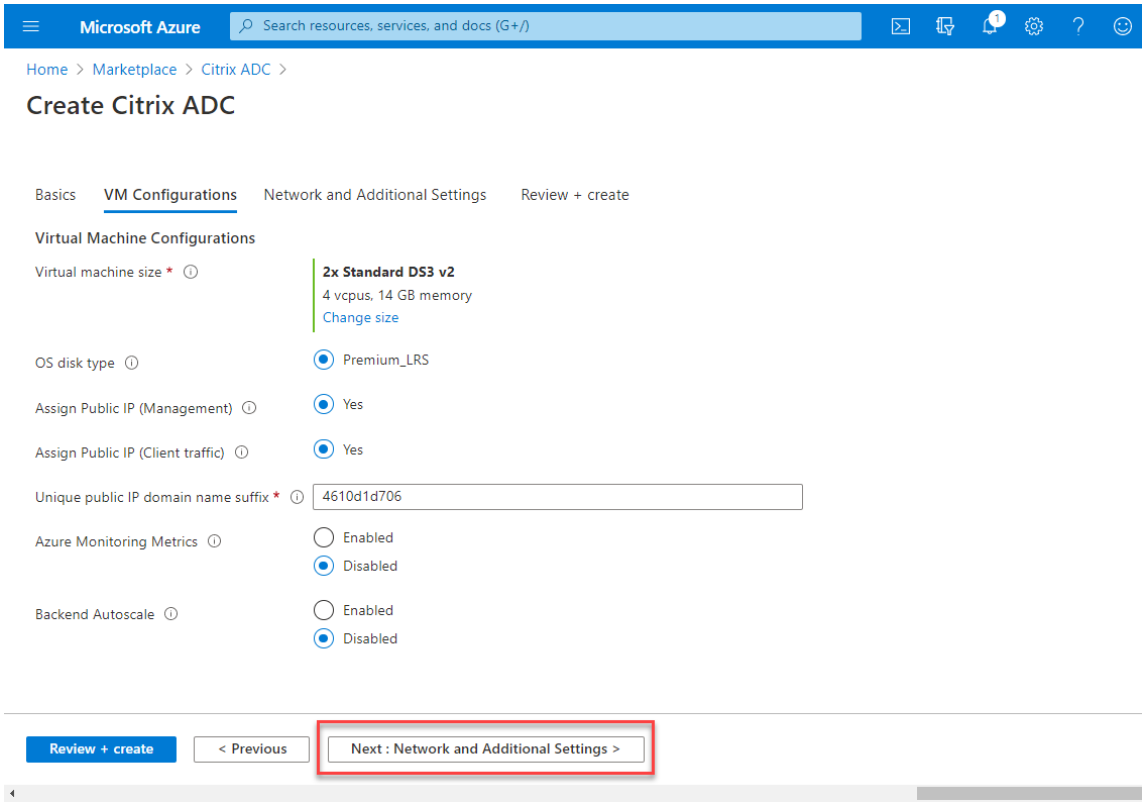
4. Dans l'onglet Notions de **base**, créez un groupe de ressources. Sous l'onglet **Paramètres**, saisissez les détails des champs Région, Nom d'utilisateur Admin, Mot de passe administrateur, type de licence (SKU VM) et d'autres champs.



5. Cliquez sur **Suivant : Configurations de machines virtuelles**.

   Sur la page **Configurations de machines virtuelles**, effectuez les opérations suivantes :

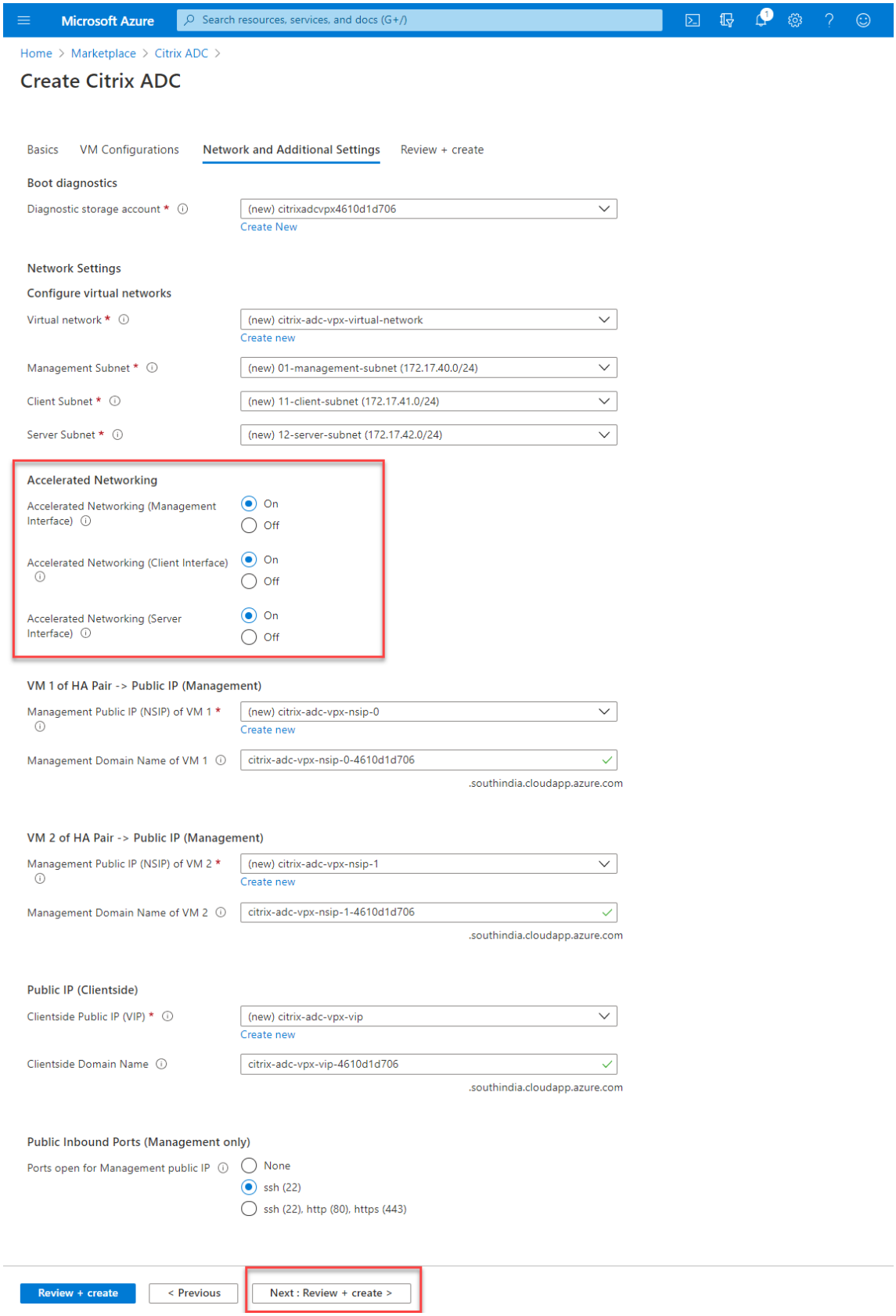
   a) Configurez le suffixe du nom de domaine IP public.
   b) Activez ou désactivez **Azure Monitoring Metrics**.
   c) Activez ou désactivez **Backend Autoscale**.



6. Cliquez sur **Suivant : Paramètres réseau et supplémentaires**.

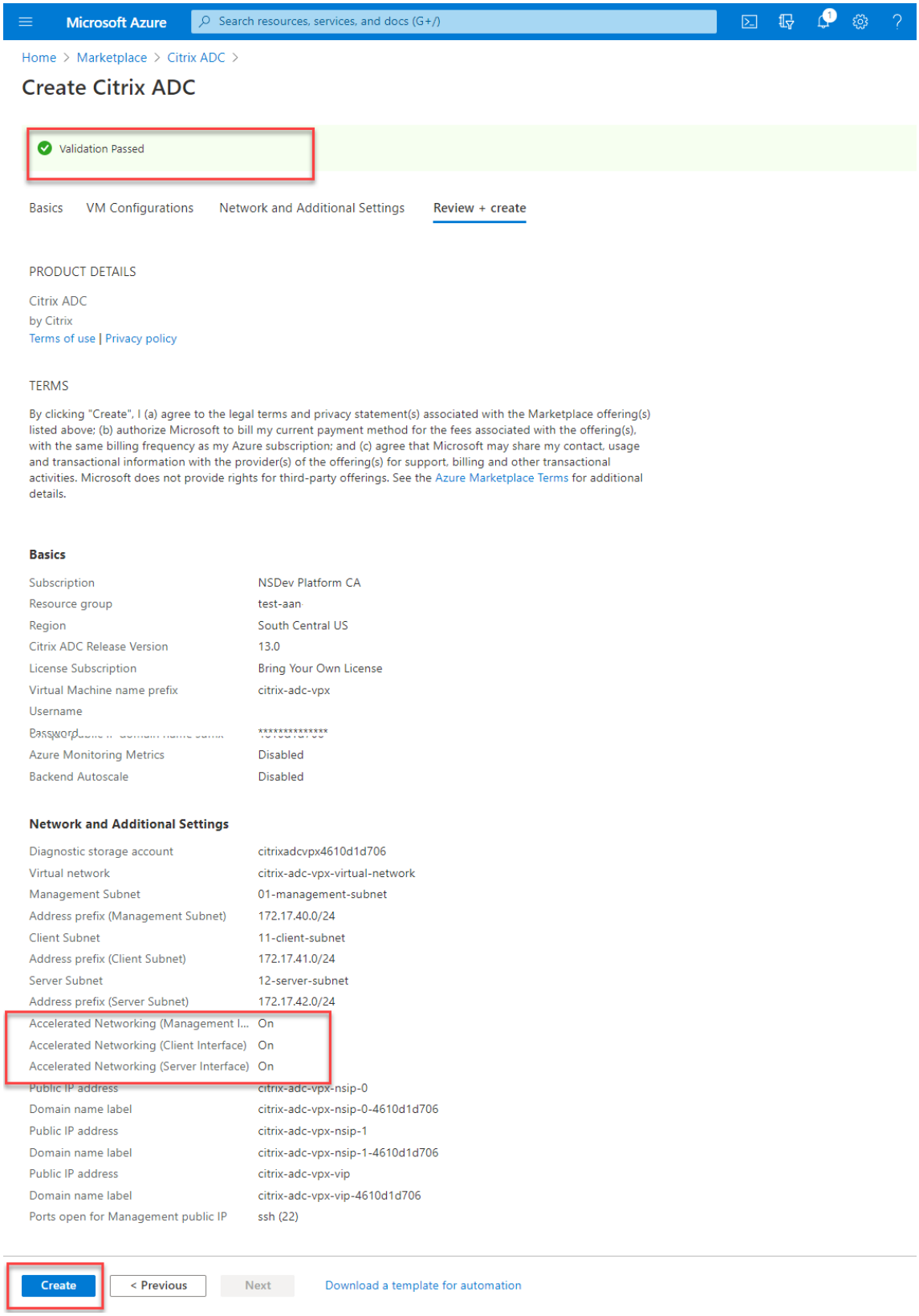
   Sur la page **Network and Additional Settings**, créez un compte de diagnostic de démarrage et configurez les paramètres réseau.

   Dans la section **Accelerated Networking**, vous avez la possibilité d'activer ou de désactiver la mise en réseau accélérée séparément pour l'interface de gestion, l'interface client et l'interface serveur.



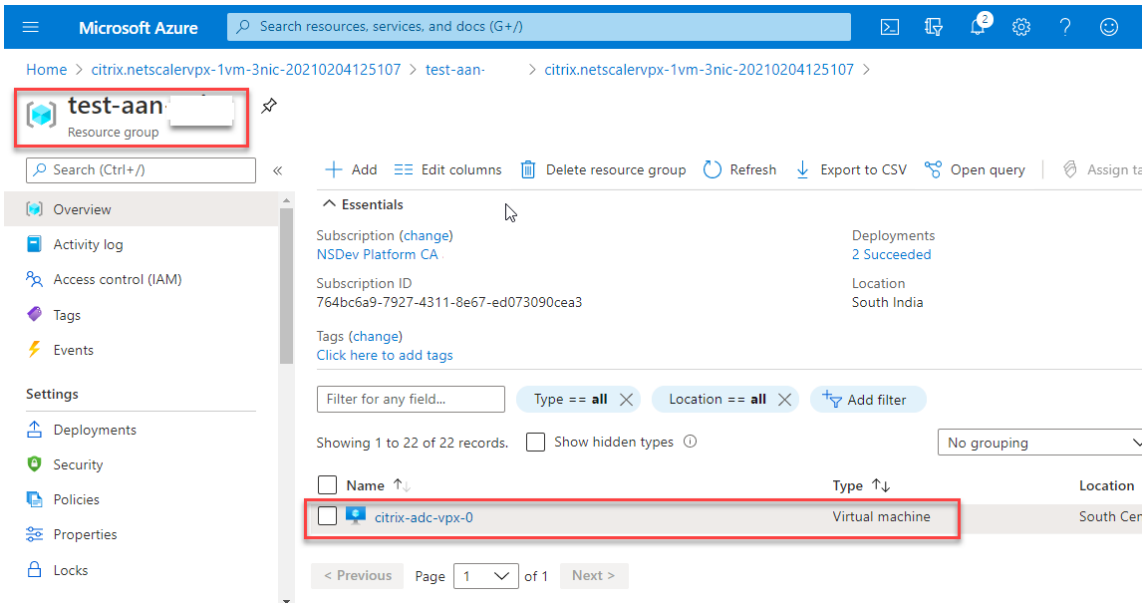
7. Cliquez sur **Suivant : Consulter et créer**.

   Une fois la validation réussie, passez en revue les paramètres de base, les configurations de machines virtuelles, le réseau et les paramètres supplémentaires, puis cliquez sur **Créer**. La création du groupe de ressources Azure avec les configurations requises peut prendre un certain temps.

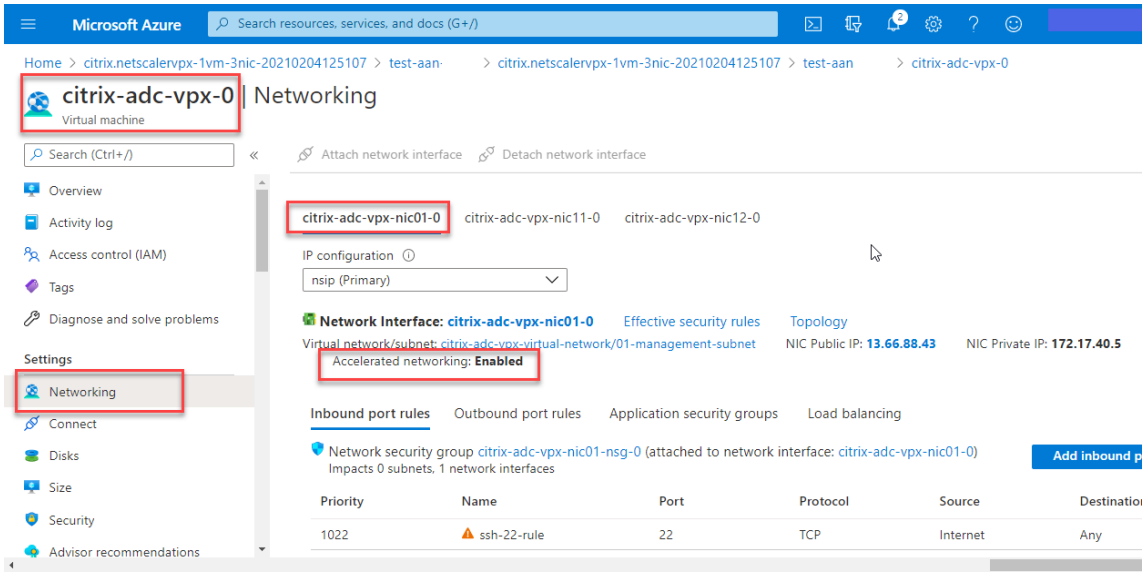


8. Une fois le déploiement terminé, sélectionnez le **groupe de ressources** pour voir les détails de

la configuration.



9. Pour vérifier les configurations Accelerated Networking, sélectionnez **Machine virtuelle > Mise en réseau**. L'état Accelerated Networking s'affiche sous la forme **Activé** ou **Désactivé** pour chaque carte réseau.



Activer la mise en réseau accélérée avec Azure PowerShell

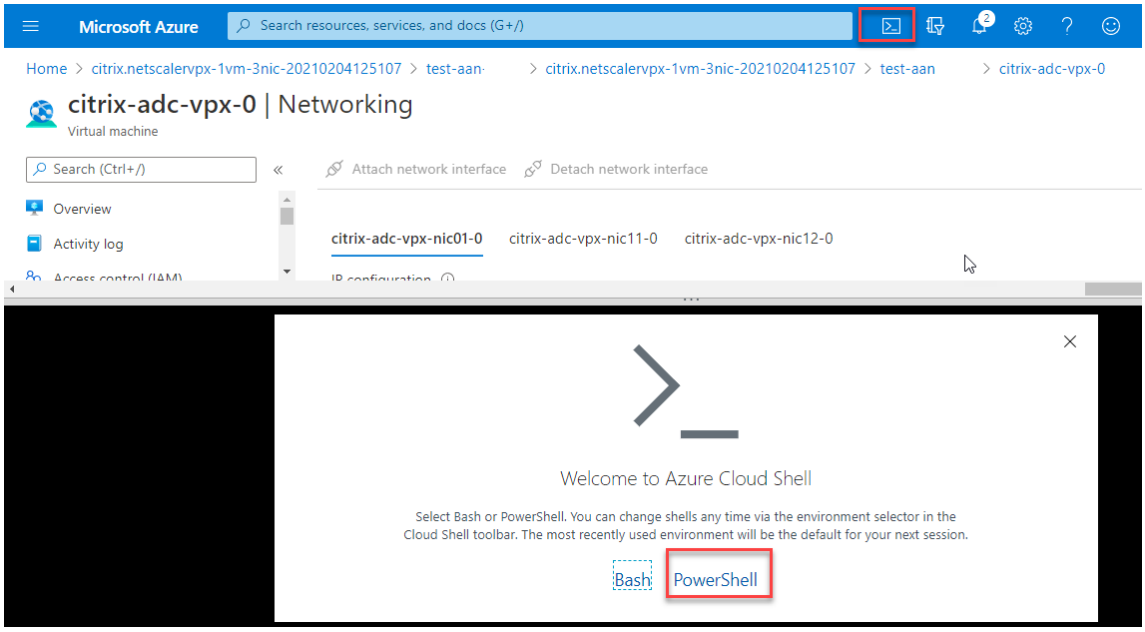
Si vous devez activer la mise en réseau accélérée après la création de la machine virtuelle, vous pouvez le faire à l'aide d'Azure PowerShell.

> Remarque :
>
> Assurez-vous d'arrêter la machine virtuelle avant d'activer Accelerated Networking à l'aide d'Azure PowerShell.

Effectuez les étapes suivantes pour activer la mise en réseau accélérée à l'aide d'Azure PowerShell.

1. Accédez au **portail Azure**, cliquez sur l'icône **PowerShell** dans le coin supérieur droit.

   > Remarque :
   >
   > Si vous êtes en mode Bash, passez au mode PowerShell.



2. À l'invite de commandes, exécutez la commande suivante :

```
az network nic update --name <nic-name> --accelerated-networking [true | false] --resource-group <resourcegroup-name>
<!--NeedCopy-->
```

   Le paramètre de mise en réseau accéléré accepte l'une des valeurs suivantes :

   - **Vrai :** active la mise en réseau accélérée sur la carte réseau spécifiée.
   - **Faux :** désactive la mise en réseau accélérée sur la carte réseau spécifiée.

   Pour activer la mise en réseau accélérée sur une carte réseau spécifique :

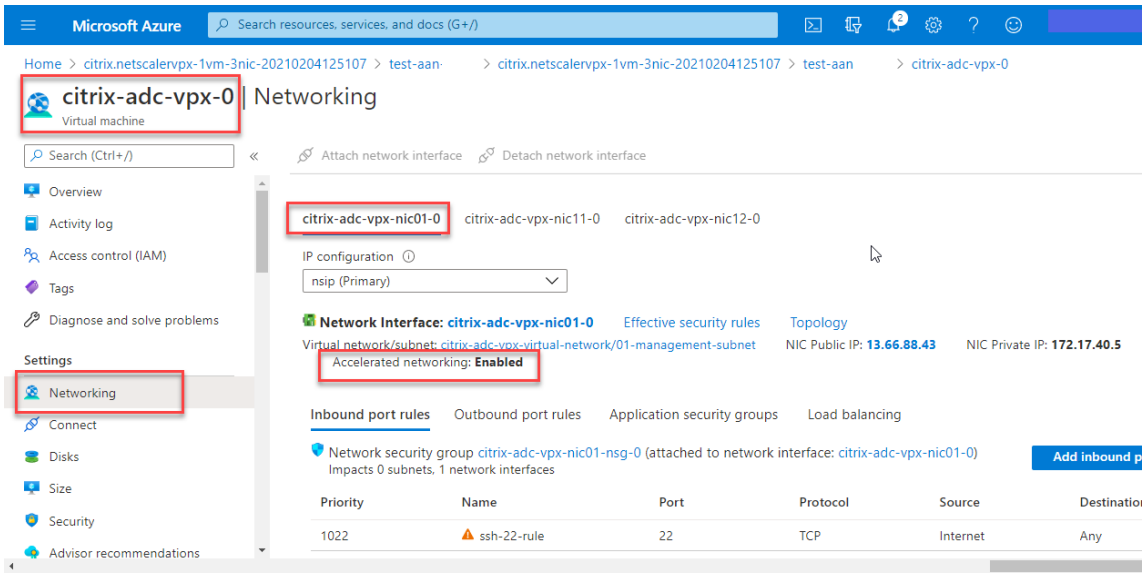
```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking true --resource-group rsgp1-aan
<!--NeedCopy-->
```

   Pour désactiver la mise en réseau accélérée sur une carte réseau spécifique :

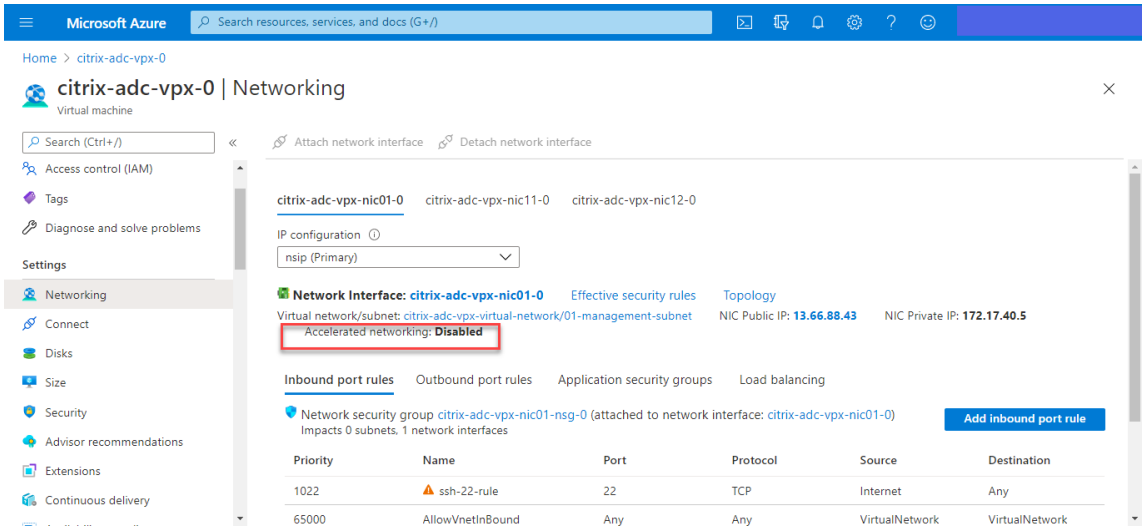

```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking false --resource-group rsgp1-aan
<!--NeedCopy-->
```

3. Pour vérifier que l'état de la mise en réseau accélérée une fois le déploiement terminé, accédez à **VM > Mise en réseau**.

   Dans l'exemple suivant, vous pouvez voir que la mise en réseau accélérée est **activée**.



   Dans l'exemple suivant, vous pouvez voir que la mise en réseau accélérée est **désactivée**.



Pour vérifier l'accélération de la mise en réseau sur une interface à l'aide de FreeBSD Shell de NetScaler

Vous pouvez vous connecter au shell FreeBSD de NetScaler et exécuter les commandes suivantes pour vérifier l'état accéléré du réseau.

Exemple de carte réseau ConnectX3 :

L'exemple suivant montre la sortie de la commande « ifconfig » de la carte réseau Mellanox ConnectX3. Le « 50/n » indique les interfaces VF des cartes réseau Mellanox ConnectX3. 0/1 et 1/1 indiquent les interfaces PV de l'instance NetScaler VPX. Vous pouvez observer que l'interface PV (1/1) et l'interface VF CX3 (50/1) ont les mêmes adresses MAC (00:22:48:1 c : 99:3 e). Cela indique que les deux interfaces sont regroupées ensemble.

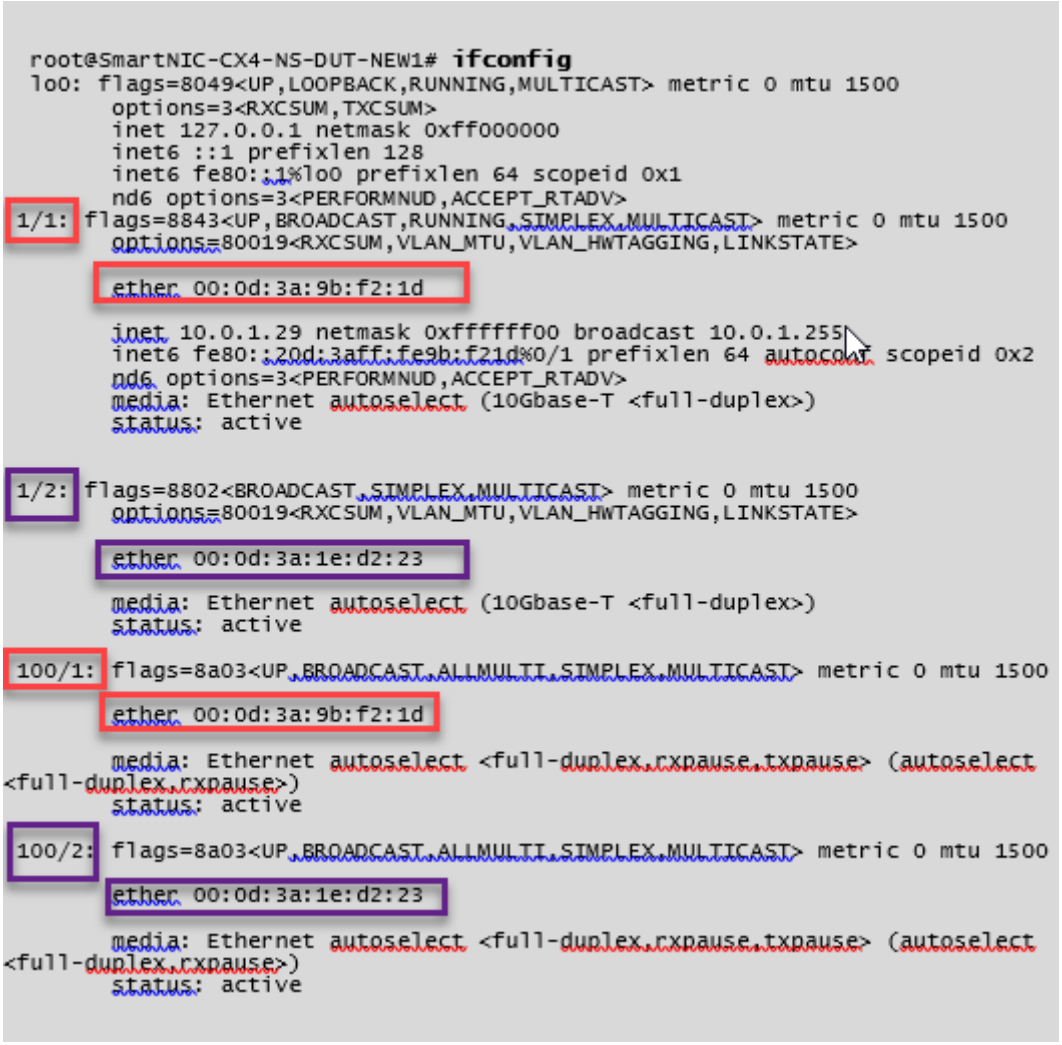

```
root@nvr-us-cx3# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
0/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:98:71:be
        inet 172.16.27.11 netmask 0xffffff00 broadcast 172.16.27.255
        inet6 fe80::20d:3aff:fe98:71be%0/1 prefixlen 64 autoconf scopeid 0x2
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
1/1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
50/1: flags=8842<BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500

options=900b8<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,VLAN_HWFILTER,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (<unknown subtype>)
        status: active
```

Exemple de carte réseau ConnectX4 :

L'exemple suivant montre la sortie de la commande « ifconfig » de la carte réseau Mellanox ConnectX4. Le « 100/n » indique les interfaces VF des cartes réseau Mellanox ConnectX4. 0/1, 1/1 et 1/2 indiquent les interfaces PV de l'instance NetScaler VPX.

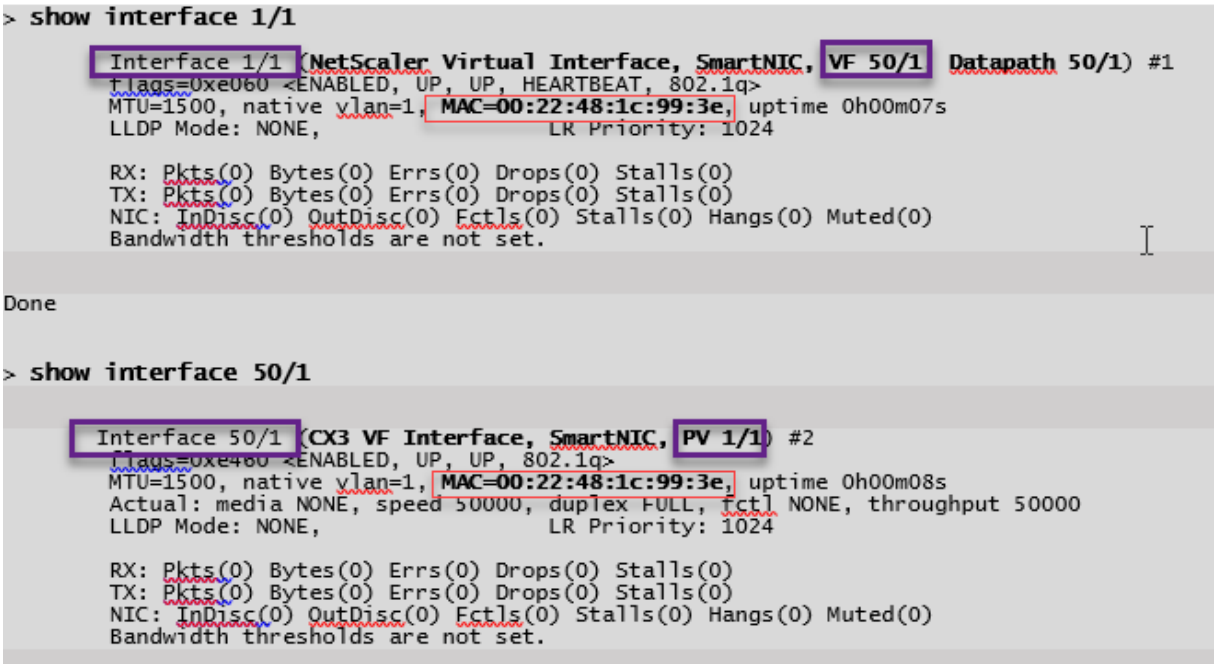
Vous pouvez observer que les interfaces PV (1/1) et CX4 VF (100/1) ont les mêmes adresses MAC (00:0 d:3a:9b:f 2:1 d). Cela indique que les deux interfaces sont regroupées ensemble. De même, l'interface PV (1/2) et l'interface VF CX4 (100/2) ont les mêmes adresses MAC (00:0 d:3a:1e:d 2:23).



Pour vérifier l'accélération de la mise en réseau sur une interface à l'aide d'ADC CLI

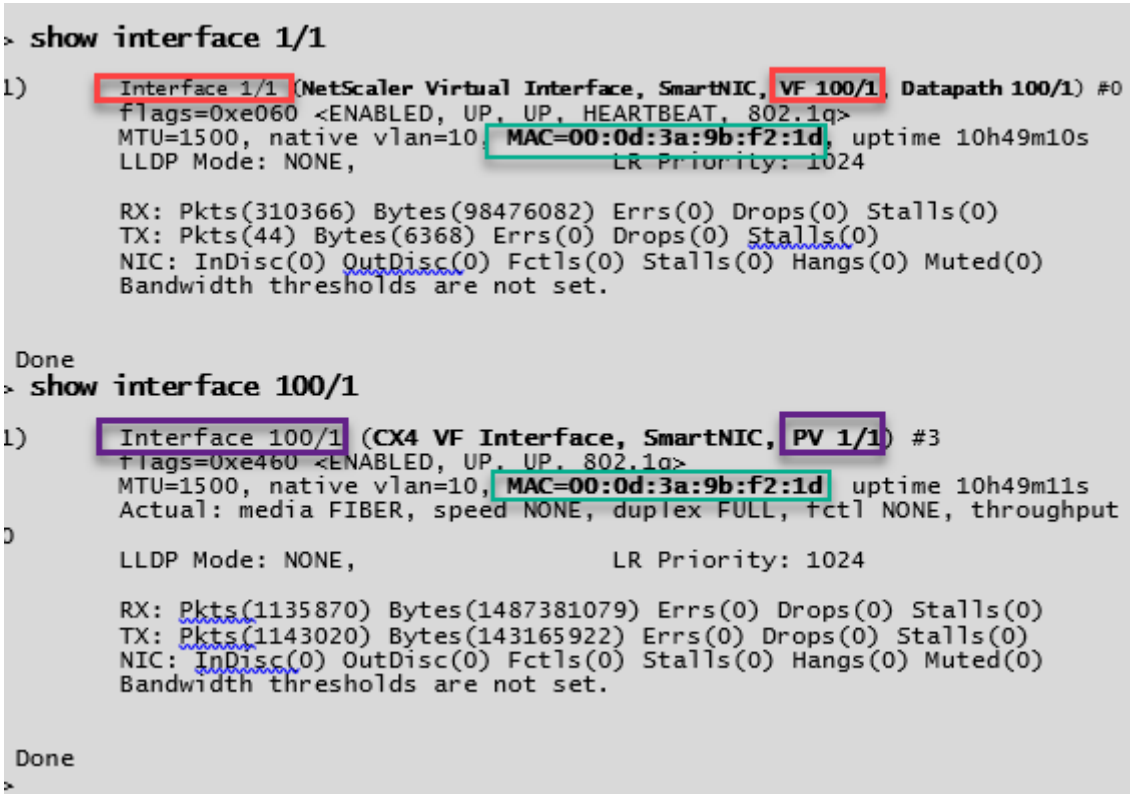
Exemple de carte réseau ConnectX3 :

La sortie de commande show interface suivante indique que l'interface PV 1/1 est fournie avec la fonction virtuelle 50/1, qui est une carte réseau VF SR-IOV. Les adresses MAC des cartes réseau 1/1 et 50/1 sont les mêmes. Une fois la mise en réseau accélérée activée, les données de l'interface 1/1 sont envoyées via le chemin de données de l'interface 50/1, qui est une interface ConnectX3. Vous pouvez voir que la sortie « show interface » de l'interface PV (1/1) pointe vers le VF (50/1). De même, la sortie « show interface » de l'interface VF (50/1) pointe vers l'interface photovoltaïque (1/1).



Exemple de carte réseau ConnectX4 :

La sortie de commande show interface suivante indique que l'interface PV 1/1 est fournie avec la fonction virtuelle 100/1, qui est une carte réseau VF SR-IOV. Les adresses MAC des cartes réseau 1/1 et 100/1 sont les mêmes. Une fois la mise en réseau accélérée activée, les données de l'interface 1/1 sont envoyées via le chemin de données de l'interface 100/1, qui est une interface ConnectX4. Vous pouvez voir que la sortie « show interface » de l'interface photovoltaïque (1/1) pointe vers le VF (100/1). De même, la sortie « show interface » de l'interface VF (100/1) pointe vers l'interface photovoltaïque (1/1).



Points à noter dans NetScaler

- L'interface photovoltaïque est considérée comme l'interface principale ou principale pour toutes les opérations nécessaires. Les configurations doivent être effectuées uniquement sur des interfaces photovoltaïques.
- Toutes les opérations « set » sur une interface VF sont bloquées à l'exception des opérations suivantes :
  - interface d'activation
  - interface de désactivation
  - interface de réinitialisation
  - statistiques claires

  > Remarque :
  >
  > Citrix recommande de ne pas effectuer d'opérations sur l'interface VF.

- Vous pouvez vérifier la liaison de l'interface PV avec l'interface VF à l'aide de la `show interface` commande.
- À partir de la version 13.1-33.x de NetScaler, une instance NetScaler VPX peut gérer de manière fluide les suppressions dynamiques et le rattachement des cartes réseau supprimées dans le réseau accéléré Azure. Azure peut supprimer la carte réseau VF SR-IOV de la mise en réseau

accélérée pour ses activités de maintenance d'hôtes. Chaque fois qu'une carte réseau est supprimée d'une machine virtuelle Azure, l'instance NetScaler VPX affiche l'état de l'interface comme « Link Down » et le trafic passe uniquement par l'interface virtuelle. Une fois la carte réseau supprimée reconnectée, les instances VPX utilisent la carte réseau VF SR-IOV reconnectée. Ce processus se déroule sans problème et ne nécessite aucune configuration.

Configurer un VLAN sur une interface PV

Lorsqu'une interface PV est liée à un VLAN, l'interface VF accélérée associée est également liée au même VLAN que l'interface PV. Dans cet exemple, l'interface PV (1/1) est liée au VLAN (20). L'interface VF (100/1) fournie avec l'interface PV (1/1) est également liée au VLAN 20.

Exemple :

1. Créez un VLAN.

```
add vlan 20
<!--NeedCopy-->
```

2. Liez un VLAN à l'interface PV.

```
bind vlan 20  - ifnum 1/1

show vlan

1)  VLAN ID: 1
    Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
    Interfaces : LO/1

2)  VLAN ID: 10     VLAN Alias Name:
    Interfaces : 0/1 100/1
    IPs : 10.0.1.29  Mask: 255.255.255.0

3)  VLAN ID: 20     VLAN Alias Name:
    Interfaces :  1/1 100/2

<!--NeedCopy-->
```

> Remarque
>
> L'opération de liaison VLAN n'est pas autorisée sur une interface VF accélérée.

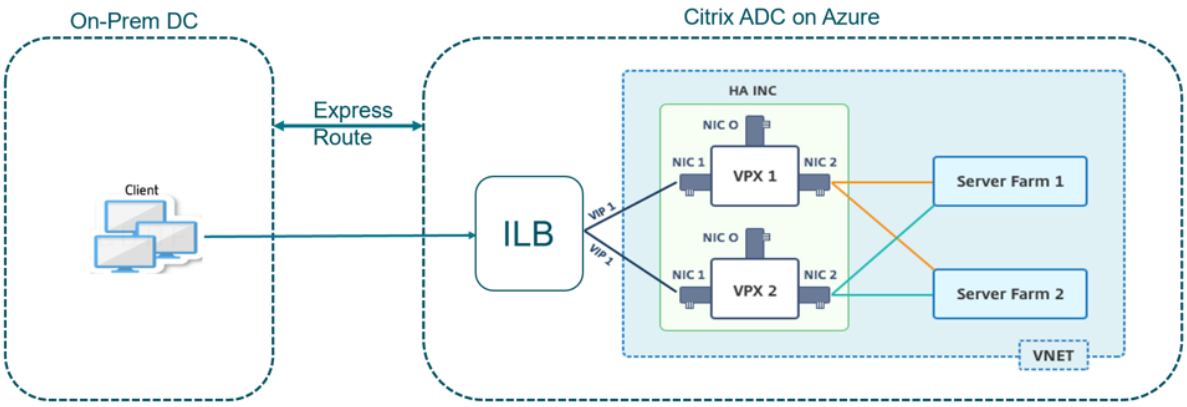
```
bind vlan 1 -ifnum 100/1
ERROR: Operation not permitted
<!--NeedCopy-->
```


Configurez les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaler avec Azure ILB

May 5, 2023

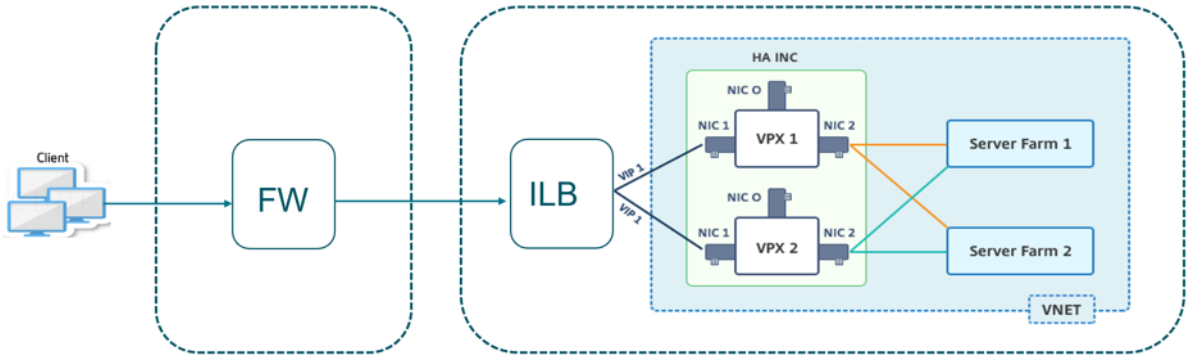
Vous pouvez déployer rapidement et efficacement une paire d'instances VPX en mode HA-INC à l'aide du modèle standard pour les applications intranet. L'équilibreur de charge interne (ILB) Azure utilise une adresse IP interne ou privée pour le frontal, comme illustré à la Figure 1. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés à la gestion, au trafic côté client et côté serveur, chaque sous-réseau appartenant à une carte réseau différente sur chaque périphérique.

Figure 1 : paire NetScaler HA pour les clients d'un réseau interne



Vous pouvez également utiliser ce déploiement lorsque la paire NetScaler HA se trouve derrière un pare-feu, comme le montre la Figure 2. L'adresse IP publique appartient au pare-feu et est NAT à l'adresse IP frontale de l'ILB.

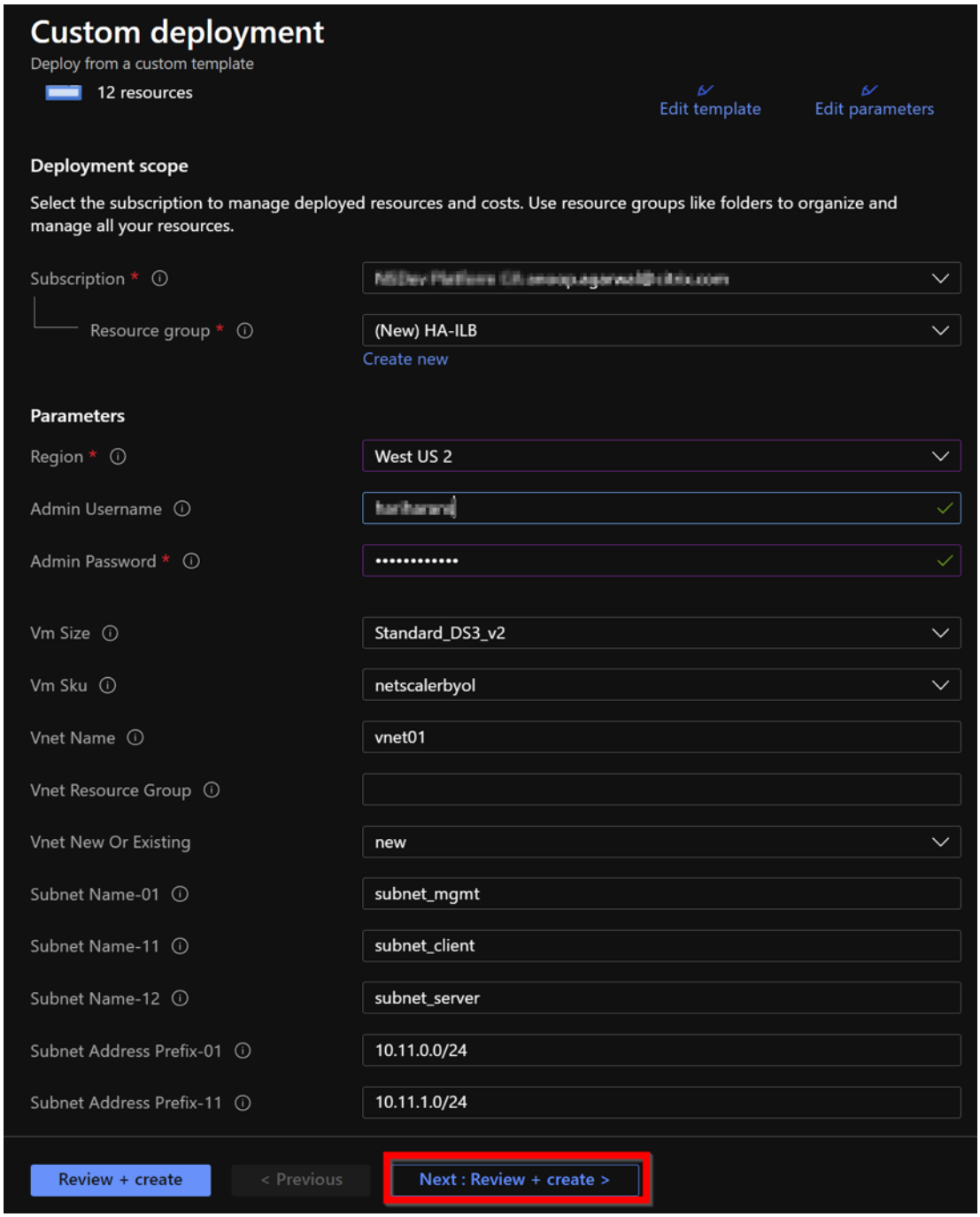
Figure 2 : paire NetScaler HA avec un pare-feu doté d'une adresse IP publique



Vous pouvez obtenir le modèle de paire NetScaler HA pour les applications intranet sur le portail Azure

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité à l'aide des jeux de disponibilité Azure.

1. Sur le portail Azure, accédez à la page **Déploiement personnalisé** .
2. La page **Principes** de base s'affiche. Créez un groupe de ressources. Sous l'onglet **Paramètres**, entrez les détails de la région, du nom d'utilisateur administrateur, du mot de passe administrateur, du type de licence (`VM sku`) et d'autres champs.

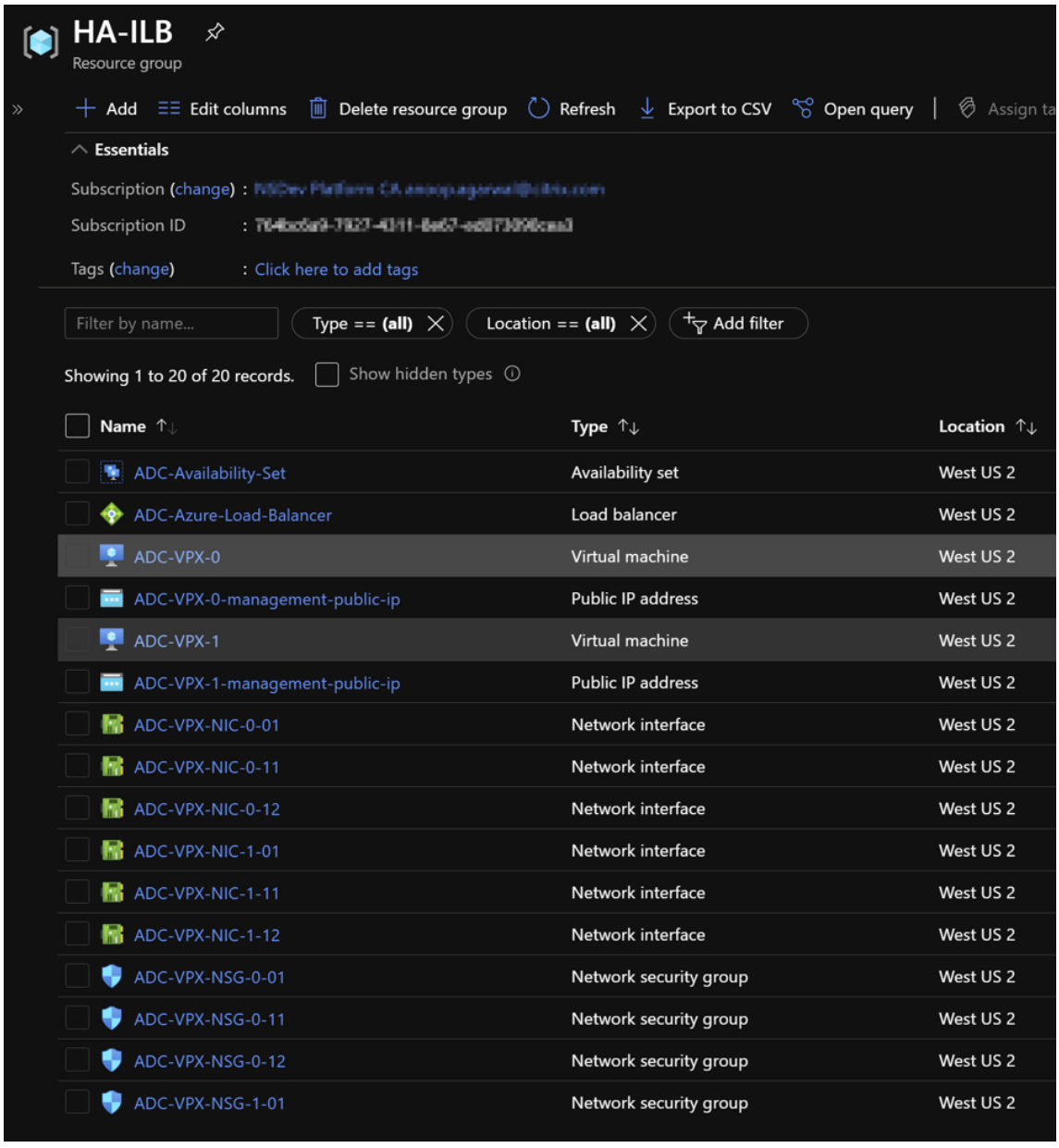


3. Cliquez sur **Next : Review + create >**.

Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois terminé, sélectionnez le groupe de ressources sur le portail Azure pour afficher les détails de configuration, tels que les règles LB, les pools dorsaux et les sondes de santé. La paire haute disponibilité s'affiche sous la forme ADC-VPX-0 et ADC-VPX-1.

Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.

Une fois la configuration requise terminée, les ressources suivantes sont créées.

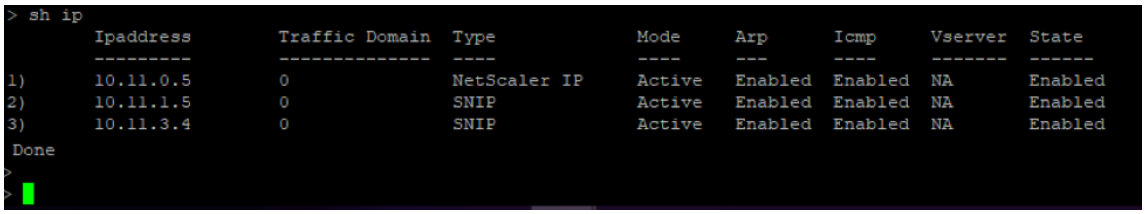


4. Ouvrez une session sur les nœuds **ADC-VPX-0** et **ADC-VPX-1** pour valider la configuration suivante :

- Les adresses NSIP des deux nœuds doivent se trouver dans le sous-réseau de gestion.
- Sur les nœuds principal (ADC-VPX-0) et secondaire (ADC-VPX-1), vous devez voir deux adresses SNIP. Un SNIP (sous-réseau client) est utilisé pour répondre aux sondes ILB et l'autre SNIP (sous-réseau serveur) est utilisé pour la communication avec le serveur principal.

> Remarque
>
> En mode HA-INC, l'adresse SNIP des machines virtuelles ADC-VPX-0 et ADC-VPX-1 est différente dans le même sous-réseau, contrairement au déploiement ADC HA local classique où les deux sont identiques.
> Pour prendre en charge les déploiements lorsque le SNIP de la paire VPX se trouve dans des sous-réseaux différents ou chaque fois que le VIP ne se trouve pas dans le même sous-réseau qu'un SNIP, vous devez soit activer le transfert basé sur Mac (MBF), soit ajouter une route hôte statique pour chaque VIP à chaque nœud VPX.

Sur le nœud principal (ADC-VPX-0)




```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.5 (ADC-VPX-0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:20:26 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.4
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

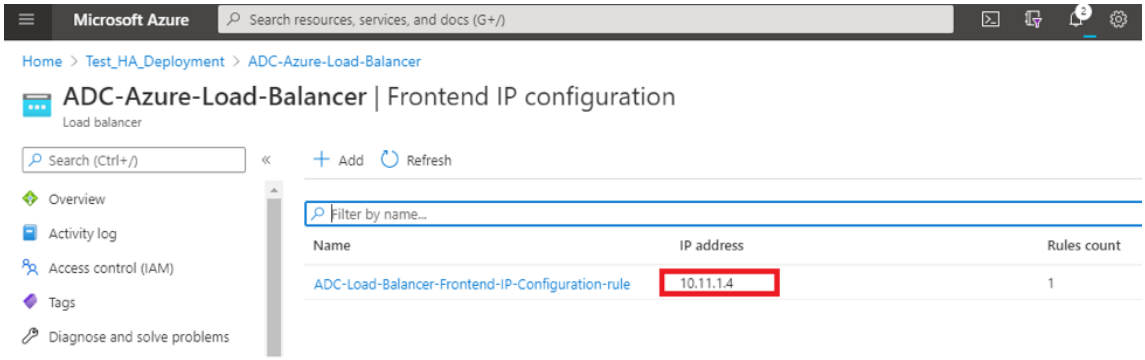
Sur le nœud secondaire (ADC-VPX-1)

```
> sh ip
       Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
       ---------        --------------  ----            ----     ---      ----     -------  ------
1)     10.11.0.4        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)     10.11.1.6        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)     10.11.3.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```

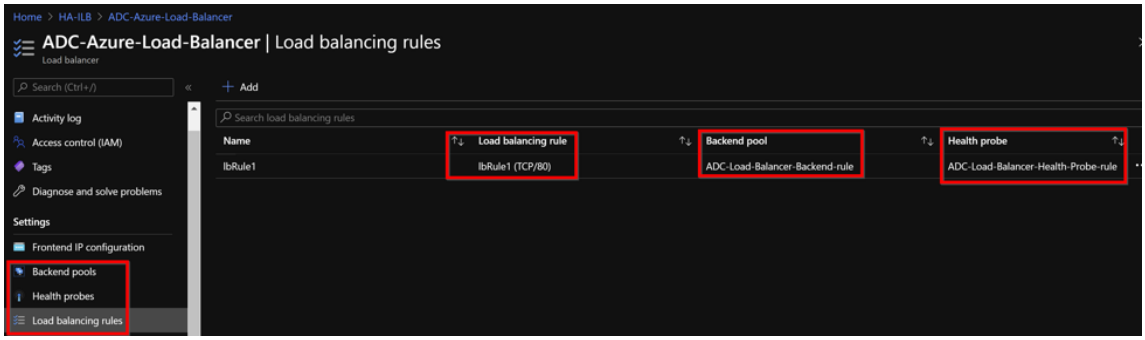


```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.4 (ADC-VPX-1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:24:18 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.5
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

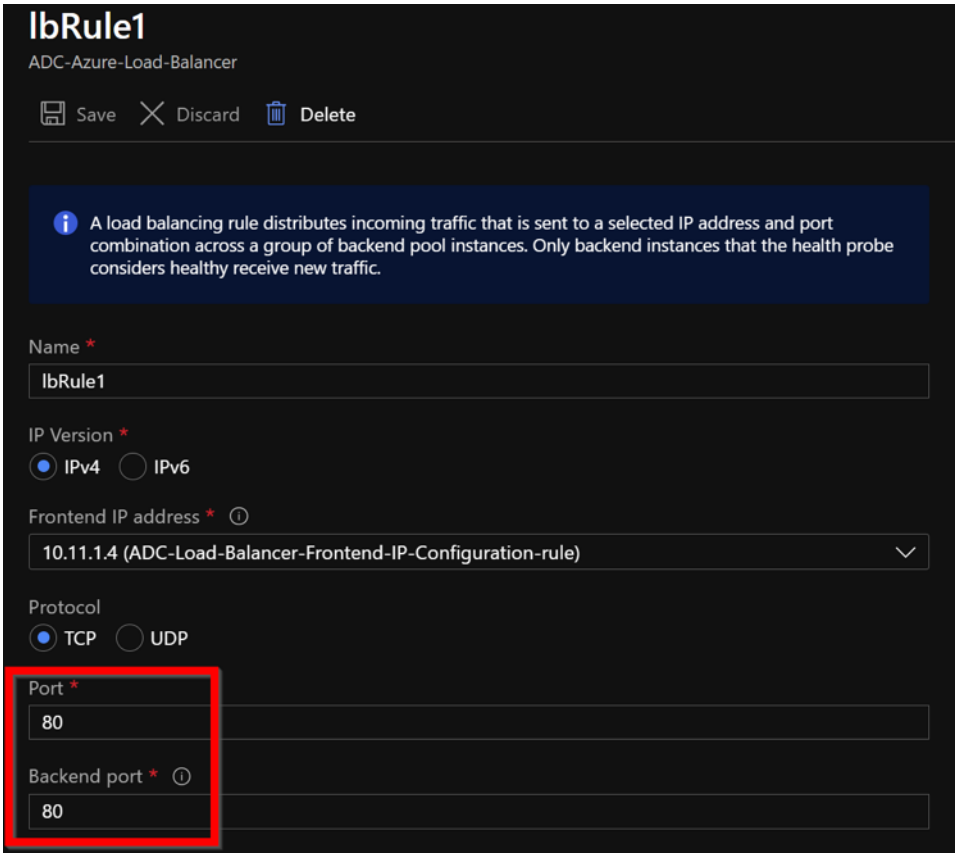
5. Une fois que les nœuds principal et secondaire sont UP et que l'état de synchronisation est **SUCCESS**, vous devez configurer le serveur virtuel d'équilibrage de charge ou le serveur virtuel de passerelle sur le nœud principal (ADC-VPX-0) avec l'adresse IP flottante privée (FIP) de l'équilibreur de charge ADC Azure. Pour plus d'informations, consultez la section Exemple de configuration .
6. Pour rechercher l'adresse IP privée de l'équilibreur de charge ADC Azure, accédez au **portail Azure > AdC Azure Load Balancer > Configuration IP frontend**.



7. Dans la page de configuration de l' **Azure Load Balancer**, le déploiement du modèle ARM permet de créer la règle d'équilibrage de charge, les pools principaux et les sondes d'état.

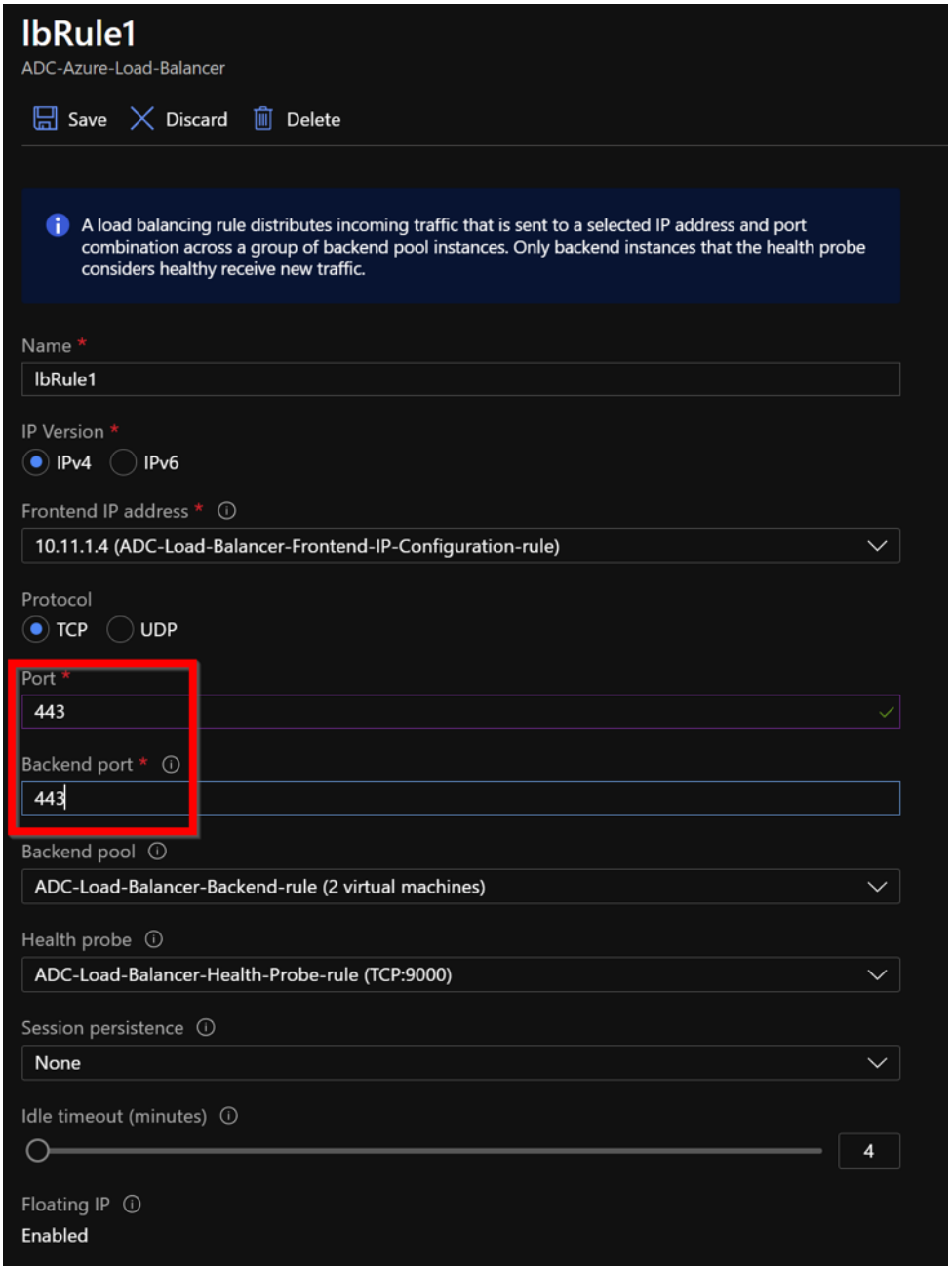


   - La règle d'équilibrage de la charge de travail (LBrule1) utilise le port 80, par défaut.



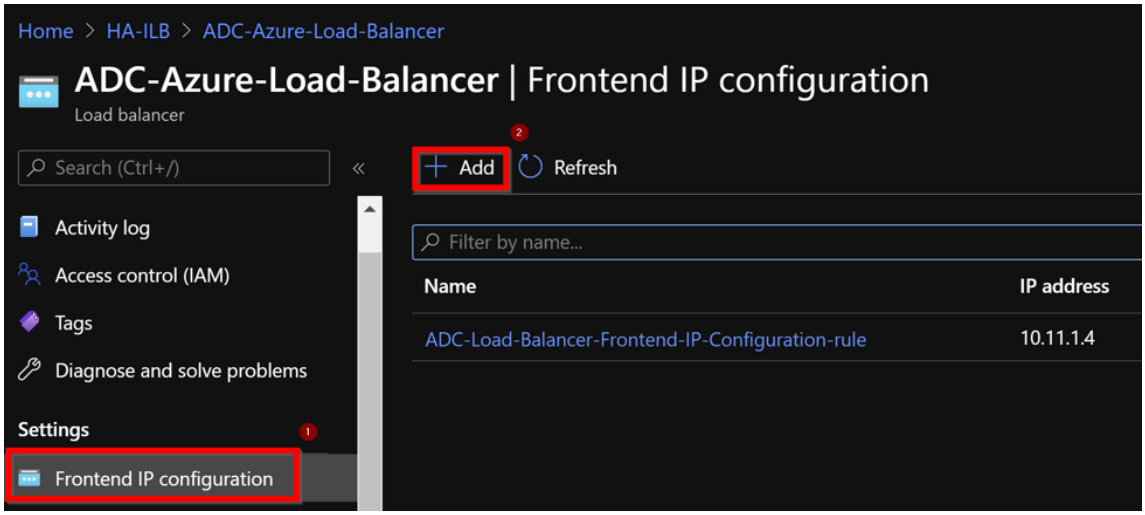
- Modifiez la règle pour utiliser le port 443 et enregistrez les modifications.

> Remarque
>
> Pour une sécurité renforcée, Citrix vous recommande d'utiliser le port SSL 443 pour le serveur virtuel LB ou le serveur virtuel Gateway.

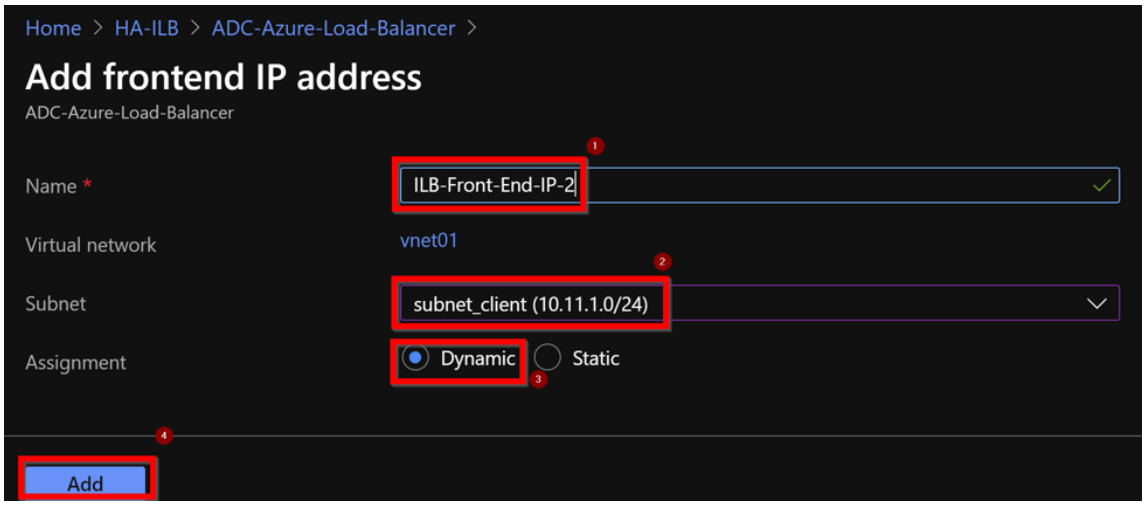


Pour ajouter d'autres adresses VIP sur l'ADC, effectuez les opérations suivantes :

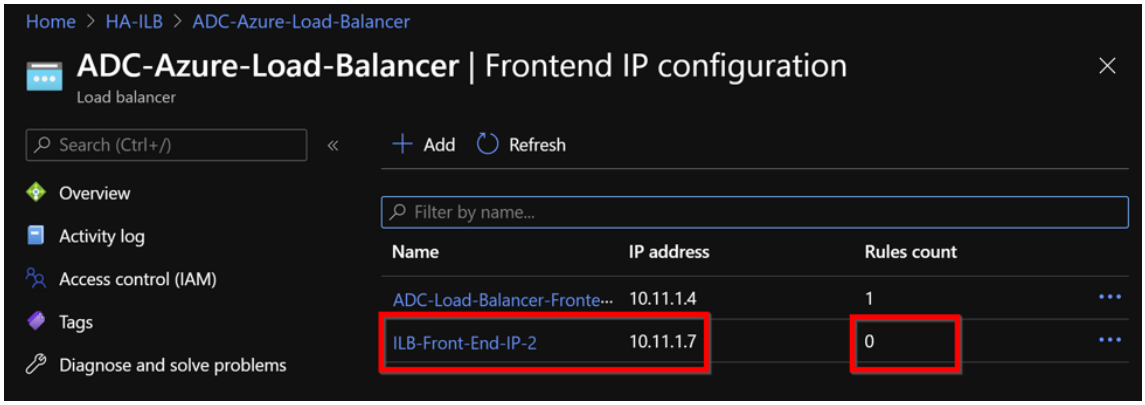
1. Accédez à **Azure Load Balancer > Configuration IP frontend**, puis cliquez sur **Ajouter** pour créer une nouvelle adresse IP d'équilibrage de charge interne.



2. Dans la page **Ajouter une adresse IP frontale**, saisissez un nom, choisissez le sous-réseau client, attribuez une adresse IP dynamique ou statique, puis cliquez sur **Ajouter**.

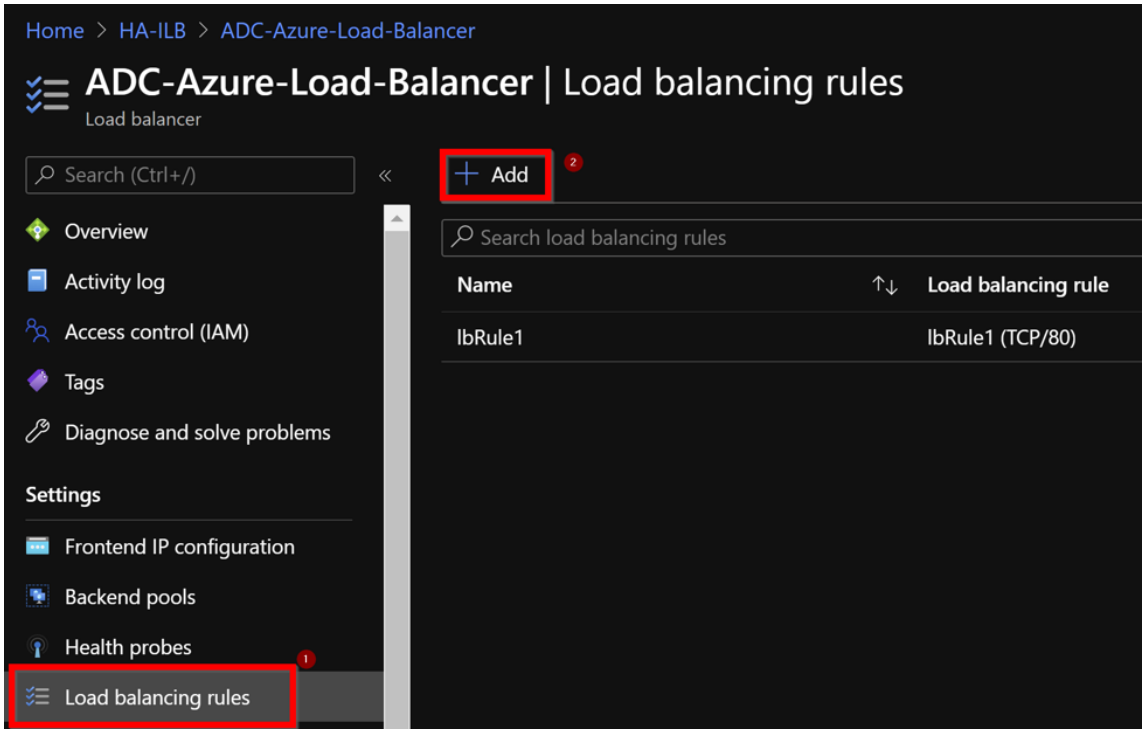


3. L'adresse IP frontale est créée mais aucune règle d'équilibrage de charge n'est associée. Créez une nouvelle règle d'équilibrage de charge et associez-la à l'adresse IP frontale.

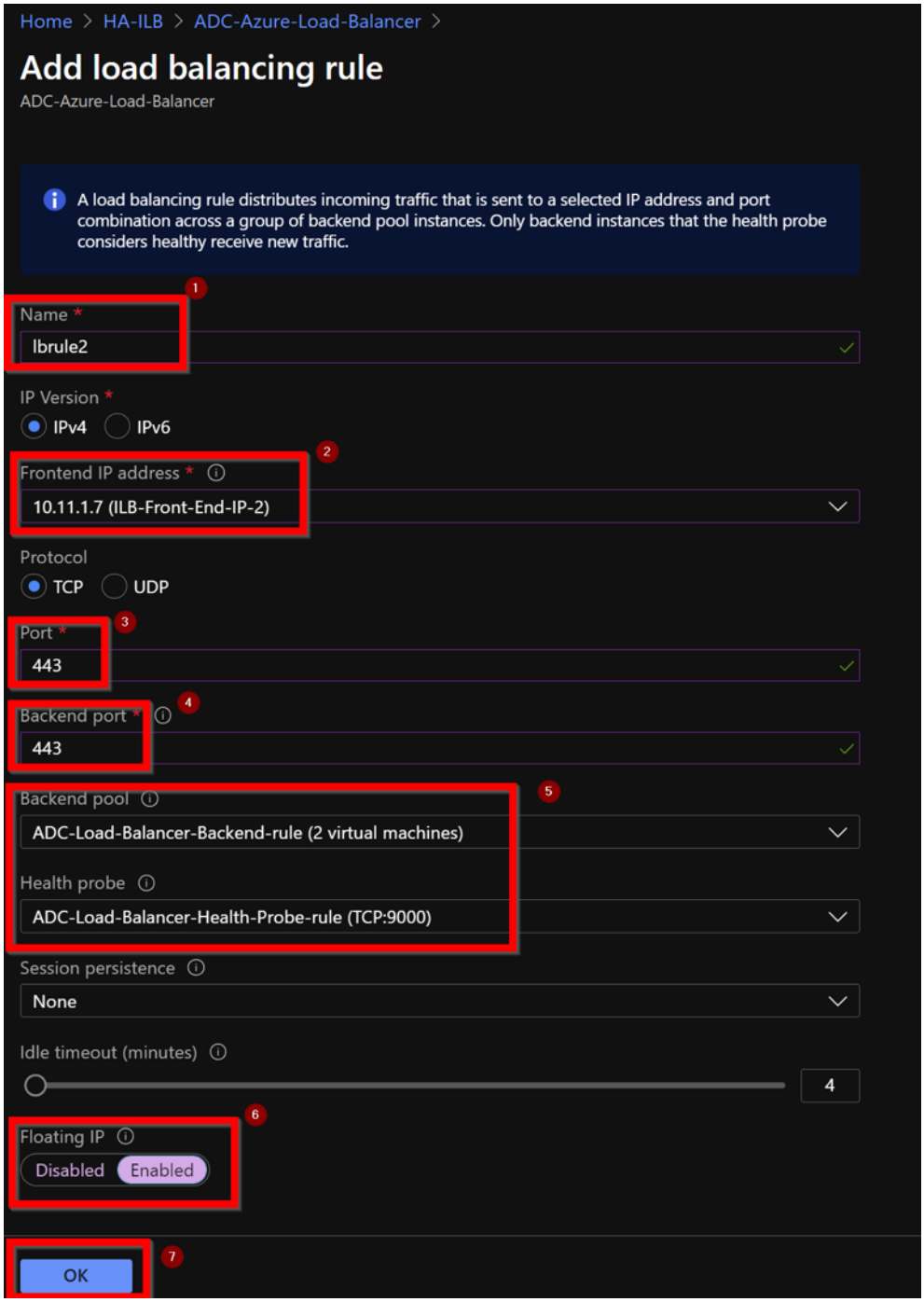


4. Sur la page **Azure Load Balancer**, sélectionnez **Règles d'équilibrage**de charge, puis cliquez

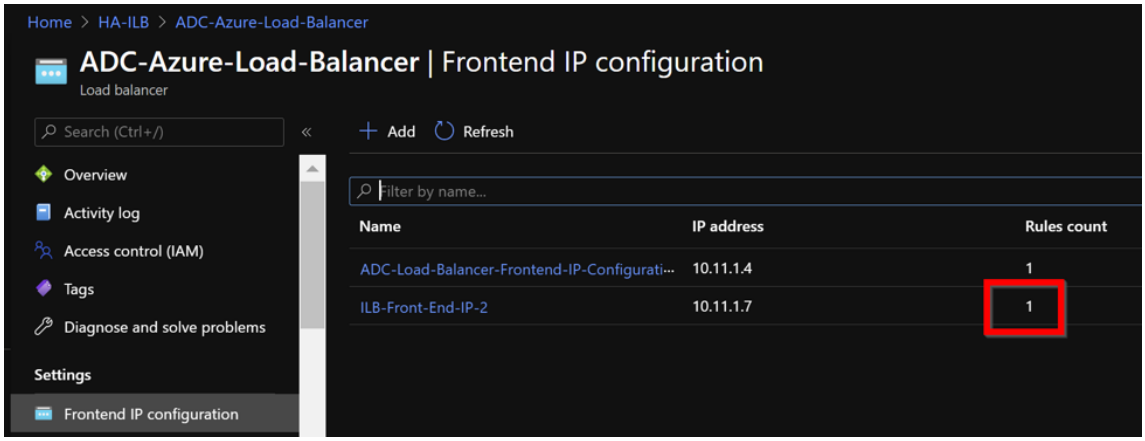
sur **Ajouter**.



5. Créez une nouvelle règle d'équilibrage de la charge de travail en choisissant la nouvelle adresse IP frontale et le port. Le champ**IP flottant** doit être défini sur **Activé**.



6. Maintenant, la **configuration IP du frontend** affiche la règle d'équilibrage de charge appliquée.



Exemple de configuration

Pour configurer un serveur virtuel VPN de passerelle et un serveur virtuel d'équilibrage de charge, exécutez les commandes suivantes sur le nœud principal (ADC-VPX-0). La configuration se synchronise automatiquement avec le nœud secondaire (ADC-VPX-1).

Exemple de configuration de passerelle

```
enable feature aaa LB SSL SSLVPN
enable ns mode MBF
add vpn vserver vpn_ssl SSL 10.11.1.4 443
add ssl certKey ckp -cert wild-cgwsanity.cer -key wild-cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Exemple de configuration d'équilibrage de charge

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 10.11.1.7 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Vous pouvez désormais accéder à l'équilibrage de charge ou au serveur virtuel VPN à l'aide du nom de domaine complet (FQDN) associé à l'adresse IP interne de l'ILB.

Consultez la section **Ressources** pour plus d'informations sur la façon de configurer le serveur virtuel d'équilibrage de charge.

Ressources :

Les liens suivants fournissent des informations supplémentaires relatives au déploiement haute disponibilité et à la configuration du serveur virtuel :

- Configuration de nœuds haute disponibilité dans différents sous-réseaux
- Configurer l'équilibrage de charge de base

Ressources connexes :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell
- Configuration de GSLB sur un déploiement HA actif de secours sur Azure

Configurez les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaler pour les applications connectées à Internet

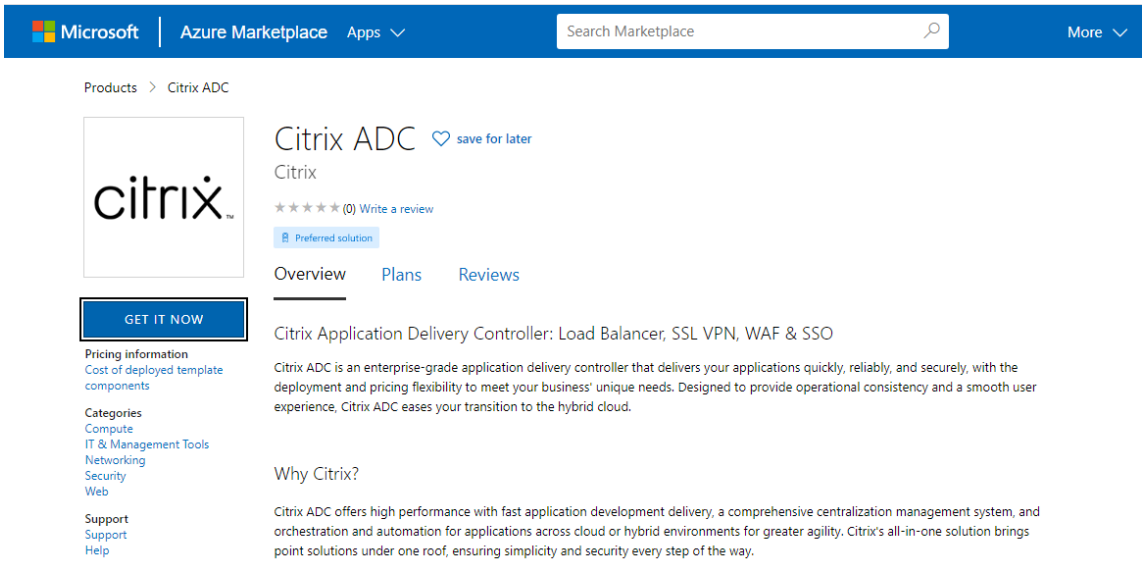
May 5, 2023

Vous pouvez déployer rapidement et efficacement deux instances VPX en mode HA-INC en utilisant le modèle standard pour les applications connectées à Internet. L'équilibreur de charge Azure (ALB) utilise une adresse IP publique pour le front-end. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés à la gestion, au trafic côté client et côté serveur. Chaque sous-réseau possède deux cartes réseau pour les deux instances VPX.

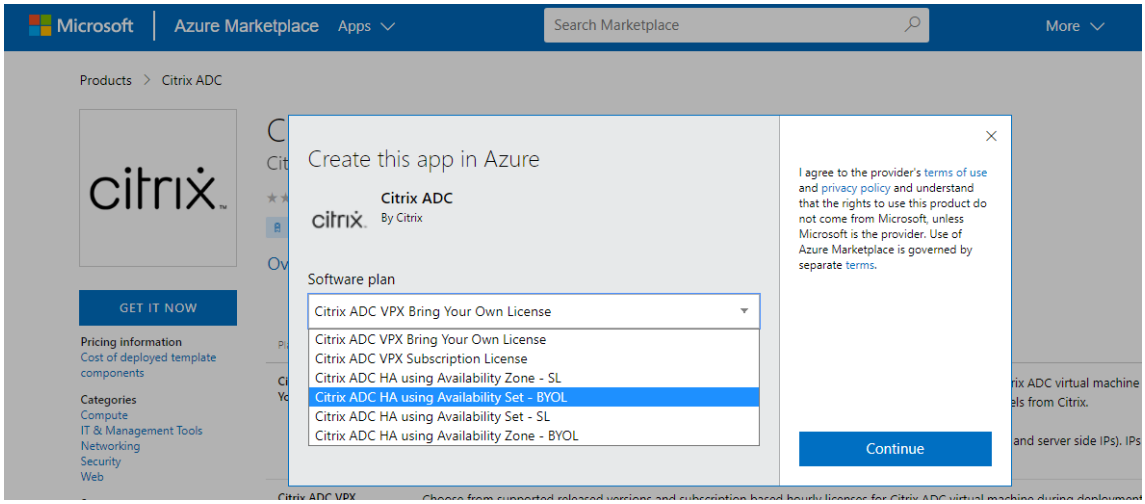
Vous pouvez obtenir le modèle de paire NetScaler HA pour les applications connectées à Internet sur Azure Marketplace.

Procédez comme suit pour lancer le modèle et déployer une paire VPX haute disponibilité à l'aide de jeux de disponibilité Azure ou d'une zone de disponibilité.

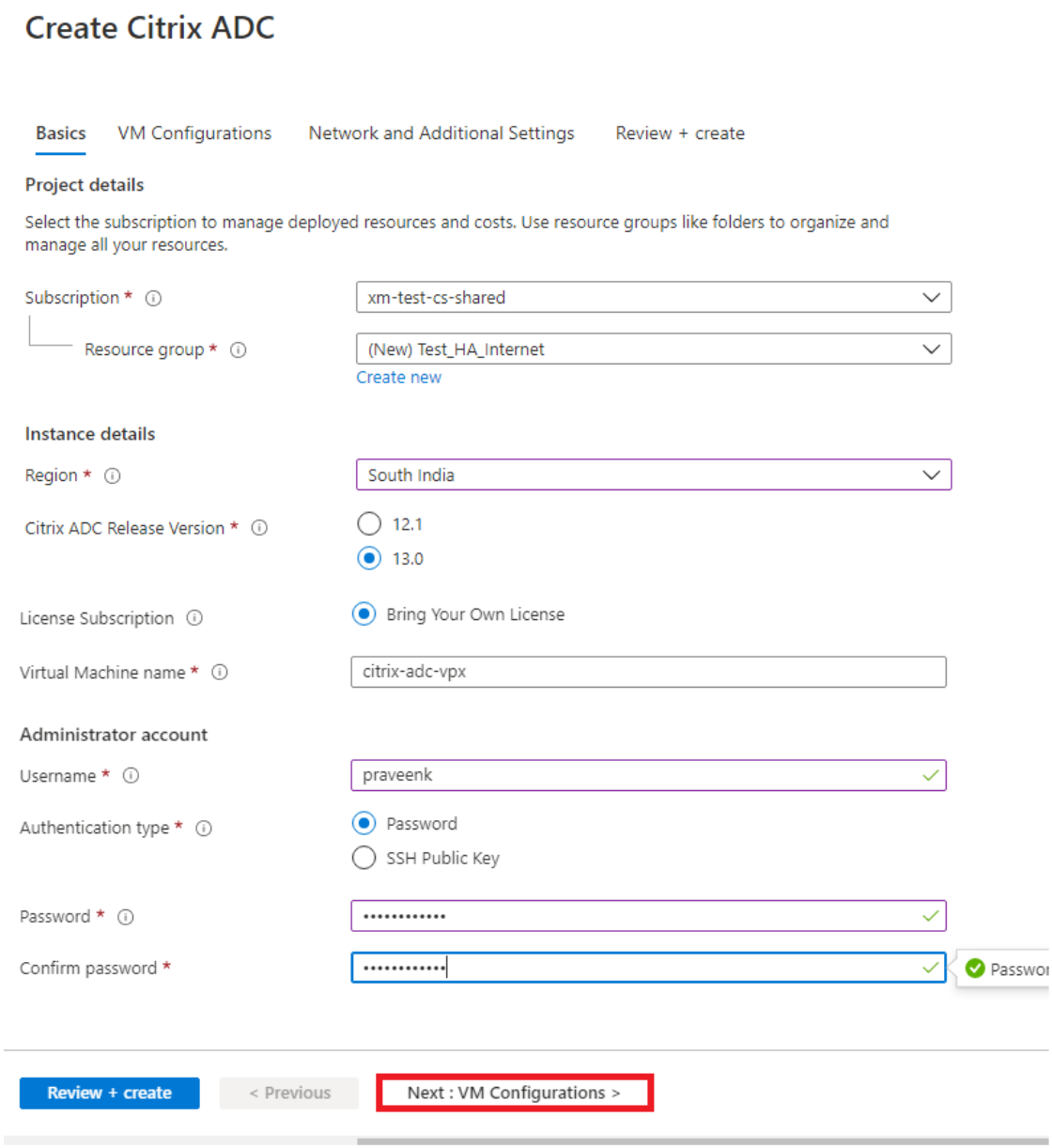
1. Sur Azure Marketplace, recherchez **NetScaler**.
2. Cliquez sur **GET IT NOW**.



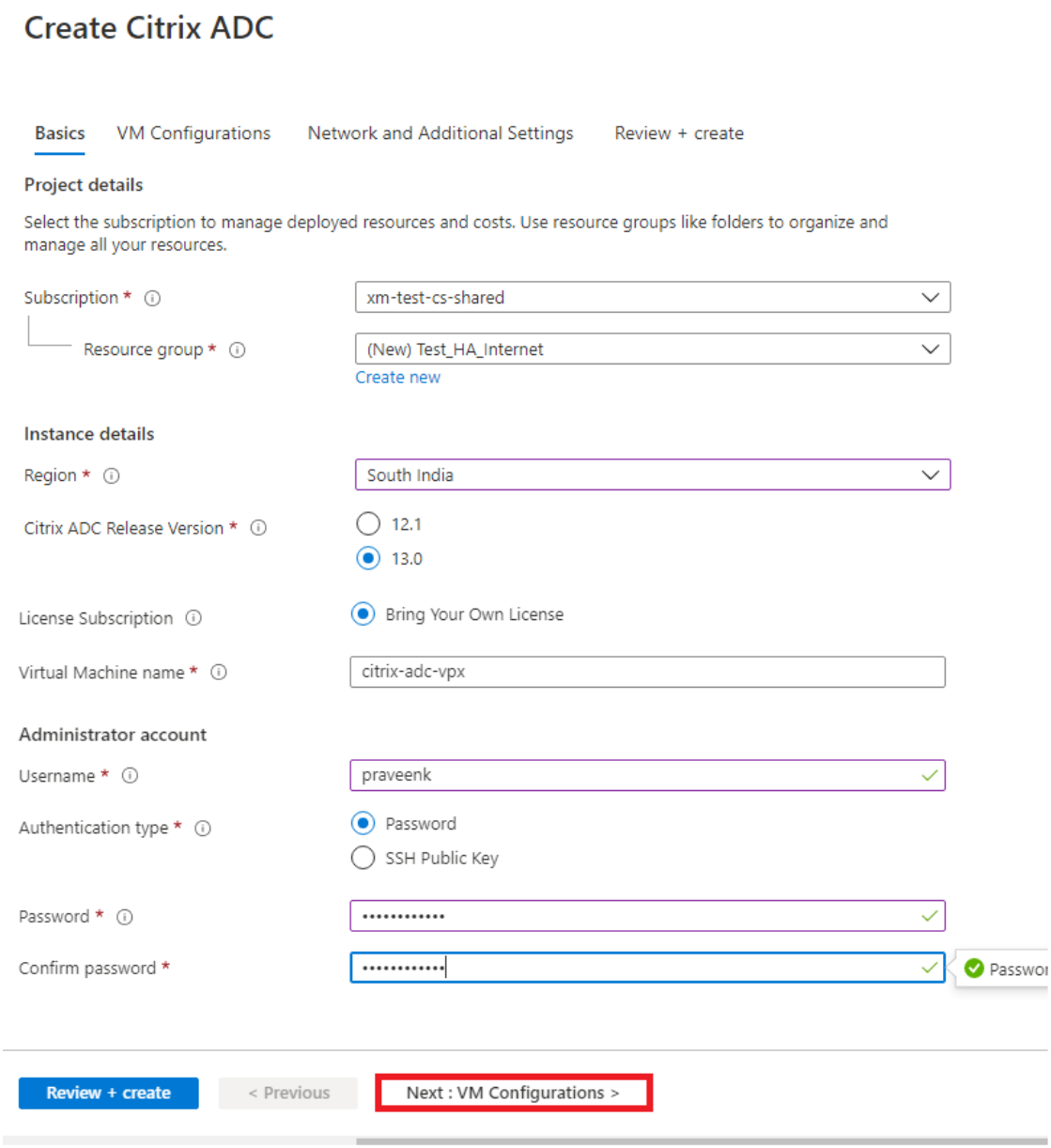
3. Sélectionnez le déploiement HA requis ainsi que la licence, puis cliquez sur **Continuer**.



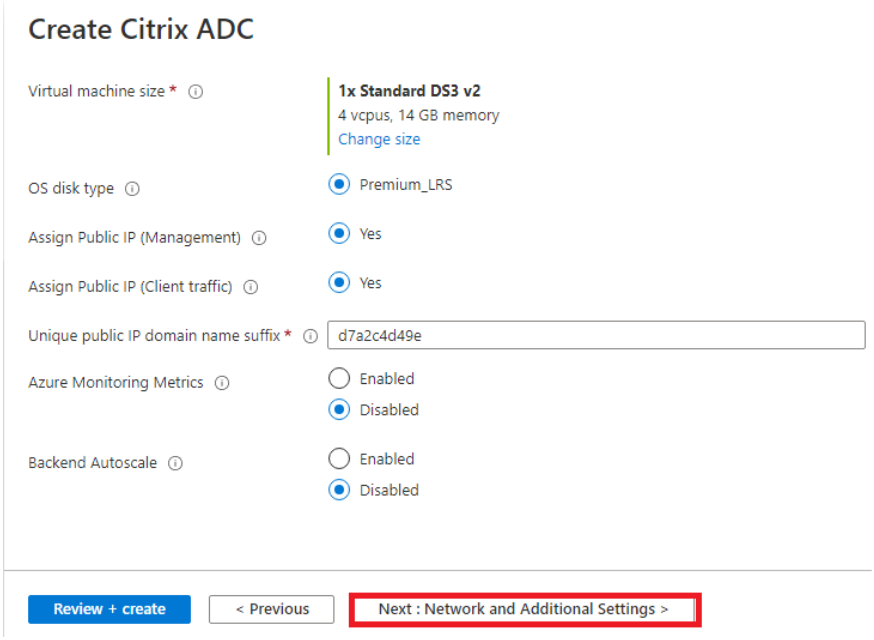
4. La page **Principes** de base s'affiche. Créez un groupe de ressources. Sous l'onglet **Paramètres**, saisissez les détails des champs Région, Nom d'utilisateur Admin, Mot de passe administrateur, type de licence (SKU VM) et d'autres champs.



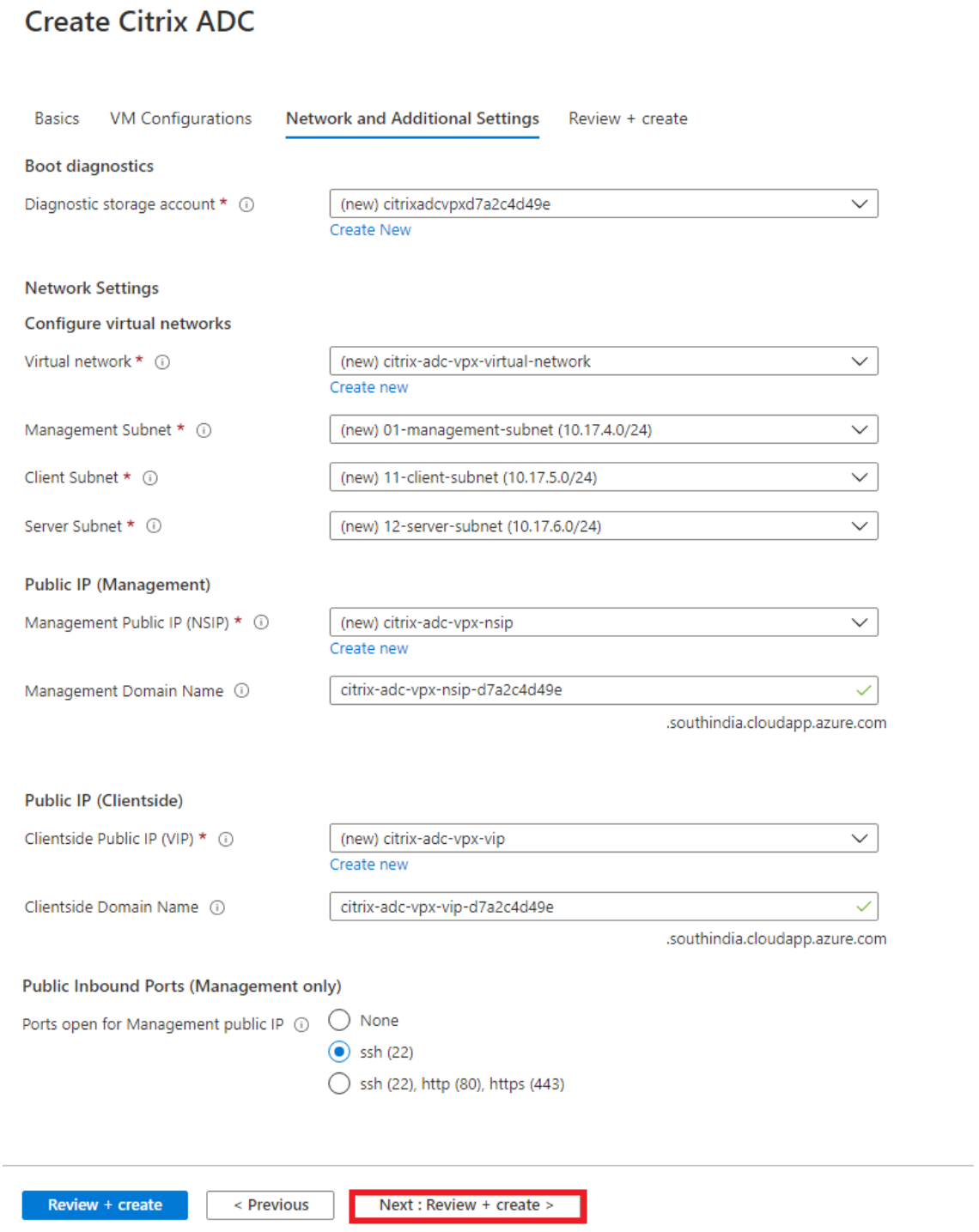
5. Cliquez sur **Suivant : Configurations de machines virtuelles**.



6. Sur la page **Configurations de machines virtuelles**, effectuez les opérations suivantes :
   - Configurer le suffixe du nom de domaine IP public
   - Activer ou désactiver **Azure Monitoring Metrics**
   - Activer ou désactiver **Backend Autoscale**
7. Cliquez sur **Suivant : Réseau et paramètres supplémentaires**



8. Sur la page **Paramètres réseau et supplémentaires**, créez un compte Boot Diagnostics et configurez les paramètres réseau.

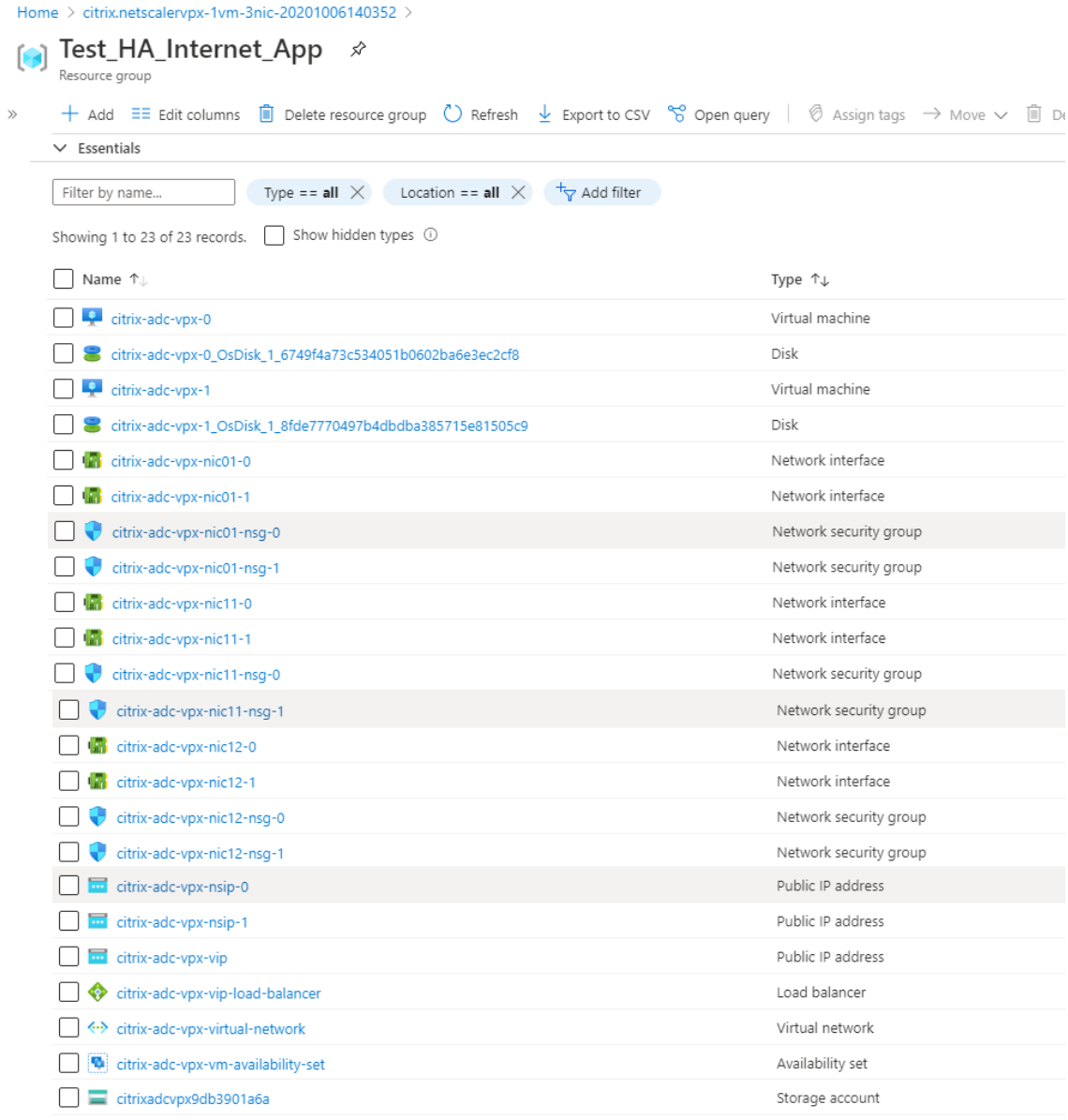


9. Cliquez sur **Suivant : Consulter et créer**.
10. Passez en revue les paramètres de base, la configuration de la machine virtuelle, le réseau et les paramètres supplémentaires, puis cliquez sur **Créer**.

Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois l'opération terminée, sélectionnez le groupe de ressources sur le portail Azure pour voir les détails de configuration, tels que les règles LB, les pools dorsaux et les sondes de santé. La paire haute disponibilité apparaît sous les **formes citrix-adc-vpx-0** et **citrix-adc-vpx-1**.

Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.

Une fois la configuration requise terminée, les ressources suivantes sont créées.



11. Vous devez vous connecter aux nœuds **citrix-adc-vpx-0** et **citrix-adc-vpx-1** pour valider la configuration suivante :

- Les adresses NSIP des deux nœuds doivent se trouver dans le sous-réseau de gestion.
- Sur les nœuds principal (citrix-adc-vpx-0) et secondaire (citrix-adc-vpx-1), vous devez voir deux adresses SNIP. Un SNIP (sous-réseau client) est utilisé pour répondre aux sondes ALB et l'autre SNIP (sous-réseau serveur) est utilisé pour la communication avec le serveur principal.

> Remarque
>
> En mode HA-INC, les adresses SNIP des machines virtuelles citrix-adc-vpx-0 et citrix-adc-vpx-1 sont différentes, contrairement au déploiement classique de haute disponibilité ADC sur site où les deux sont identiques.

Sur le nœud principal (citrix-adc-vpx-0)

```
> sh ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.4        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.4 (ns-vpx0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:34:21 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.5
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
```

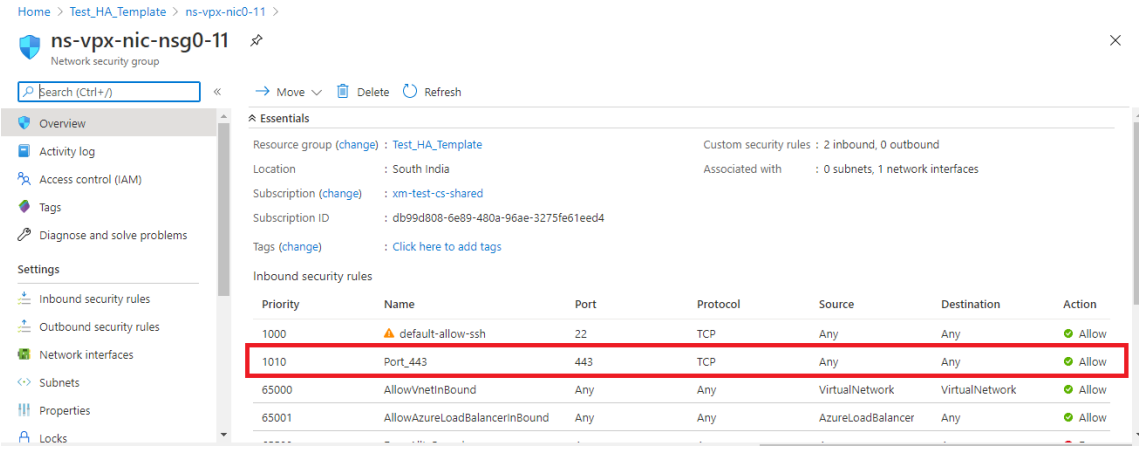
Sur le nœud secondaire (citrix-adc-vpx-1)

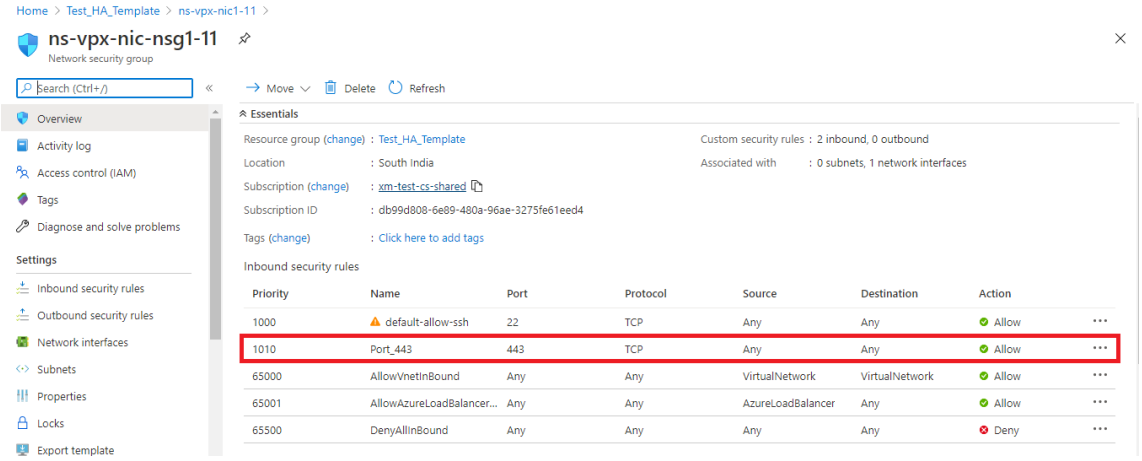

```
> show ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.5        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.5 (ns-vpx1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:23:51 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.4
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

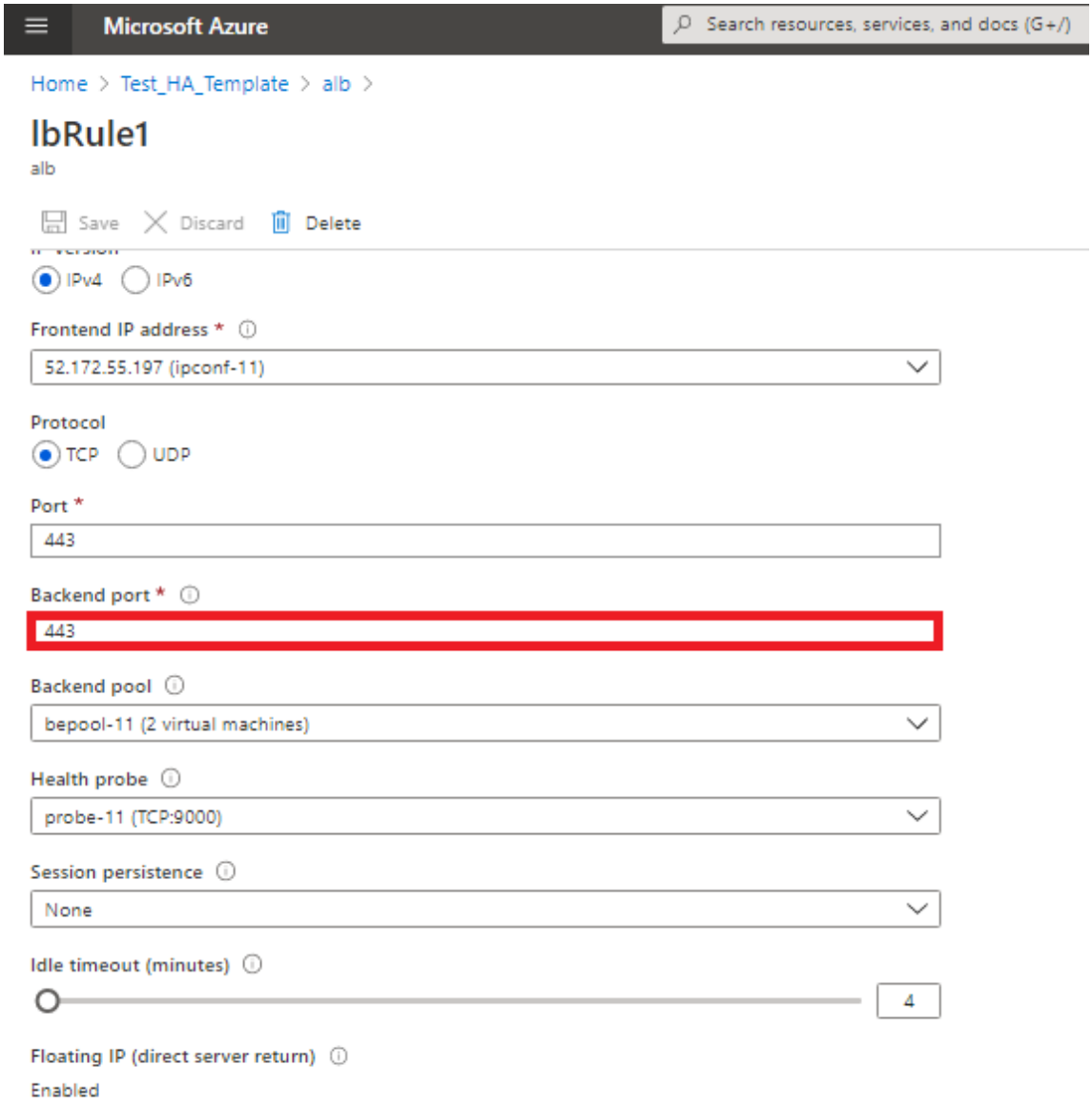
12. Une fois que les nœuds principal et secondaire sont UP et que l'état Synchronisation est **SUCCESS**, vous devez configurer le serveur virtuel d'équilibrage de charge ou le serveur virtuel de passerelle sur le nœud principal (citrix-adc-vpx-0) avec l'adresse IP publique du serveur virtuel ALB. Pour plus d'informations, consultez la section Exemple de configuration .
13. Pour rechercher l'adresse IP publique du serveur virtuel ALB, accédez au **portail Azure > Équilibreur de charge Azure > Configuration IP frontend**.

14. Ajoutez la règle de sécurité entrante pour le port 443 du serveur virtuel dans le groupe de sécurité réseau des deux interfaces clientes.

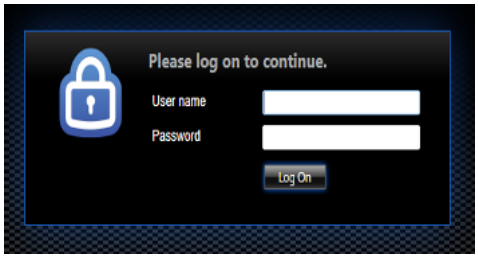




15. Configurez le port ALB auquel vous souhaitez accéder et créez une règle de sécurité entrante pour le port spécifié. Le port principal est le port de votre serveur virtuel d'équilibrage de charge ou le port du serveur virtuel VPN.



16. Vous pouvez désormais accéder au serveur virtuel d'équilibrage de charge ou au serveur virtuel VPN à l'aide du nom de domaine complet (FQDN) associé à l'adresse IP publique ALB.



Exemple de configuration

Pour configurer un serveur virtuel VPN de passerelle et un serveur virtuel d'équilibrage de charge, exécutez les commandes suivantes sur le nœud principal (ADC-VPX-0). La configuration se synchronise automatiquement avec le nœud secondaire (ADC-VPX-1).

Exemple de configuration de passerelle

```
enable feature aaa LB SSL SSLVPN
add ip 52.172.55.197 255.255.255.0 -type VIP
add vpn vserver vpn_ssl SSL 52.172.55.197 443
add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Exemple de configuration d'équilibrage de charge

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 52.172.55.197 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Vous pouvez désormais accéder à l'équilibrage de charge ou au serveur virtuel VPN à l'aide du FQDN associé à l'adresse IP publique d'ALB.

Consultez la section **Ressources** pour plus d'informations sur la configuration du serveur virtuel d'équilibrage de charge.

Ressources :

Les liens suivants fournissent des informations supplémentaires relatives au déploiement haute disponibilité et à la configuration du serveur virtuel :

- Créer des serveurs virtuels
- Configurer l'équilibrage de charge de base

Configurer une configuration haute disponibilité avec des équilibreurs de charge externes et internes Azure simultanément

May 5, 2023

La paire haute disponibilité sur Azure prend en charge simultanément les équilibreurs de charge externes et internes.

Vous disposez des deux options suivantes pour configurer une paire haute disponibilité à l'aide d'équilibreurs de charge externes et internes Azure :

- Utilisation de deux serveurs virtuels LB sur l'appliance NetScaler.
- Utilisation d'un serveur virtuel LB et d'un ensemble d'adresses IP. Le serveur virtuel LB unique sert le trafic vers plusieurs adresses IP définies par l'IPSet.

Effectuez les étapes suivantes pour configurer une paire haute disponibilité sur Azure en utilisant simultanément les équilibreurs de charge externes et internes :

Pour les étapes 1 et 2, utilisez le portail Azure. Pour les étapes 3 et 4, utilisez l'interface graphique NetScaler VPX ou la CLI.

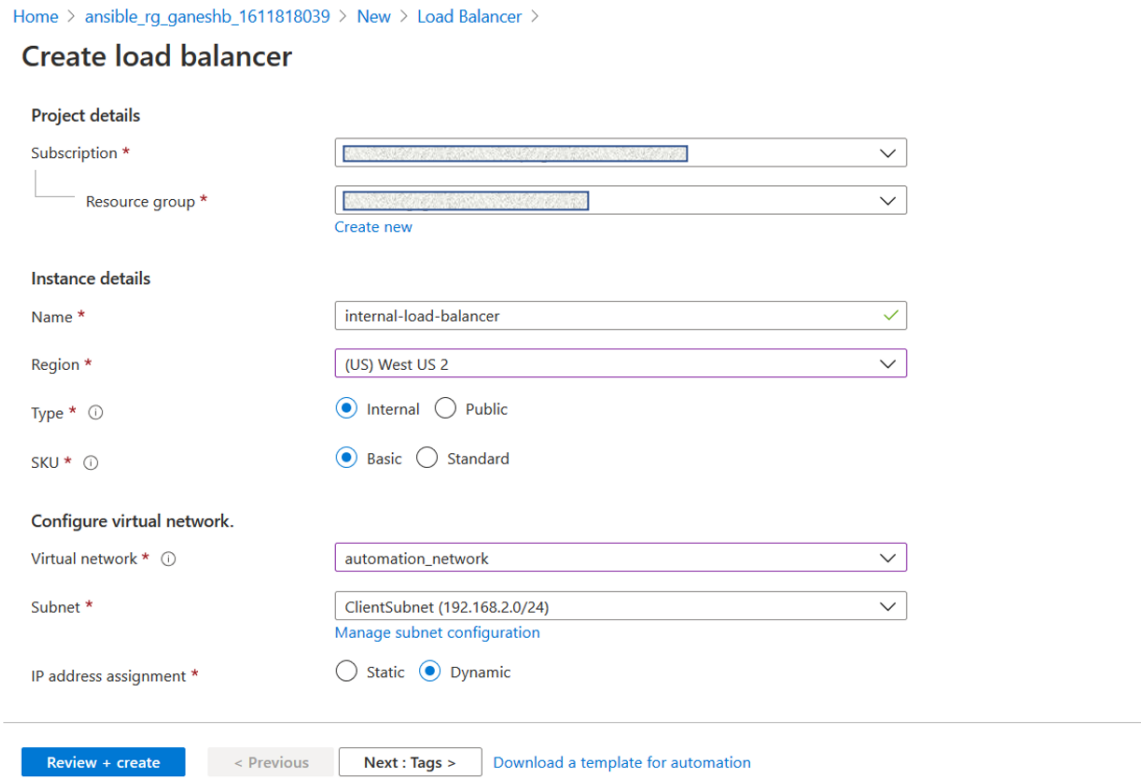
Étape 1. Configurez un équilibreur de charge Azure, soit un équilibreur de charge externe, soit un équilibreur de charge interne.

Pour plus d'informations sur la configuration de la configuration haute disponibilité avec des équilibreurs de charge externes Azure, voir Configurer une configuration haute disponibilité avec plusieurs adresses IP et carte réseau.

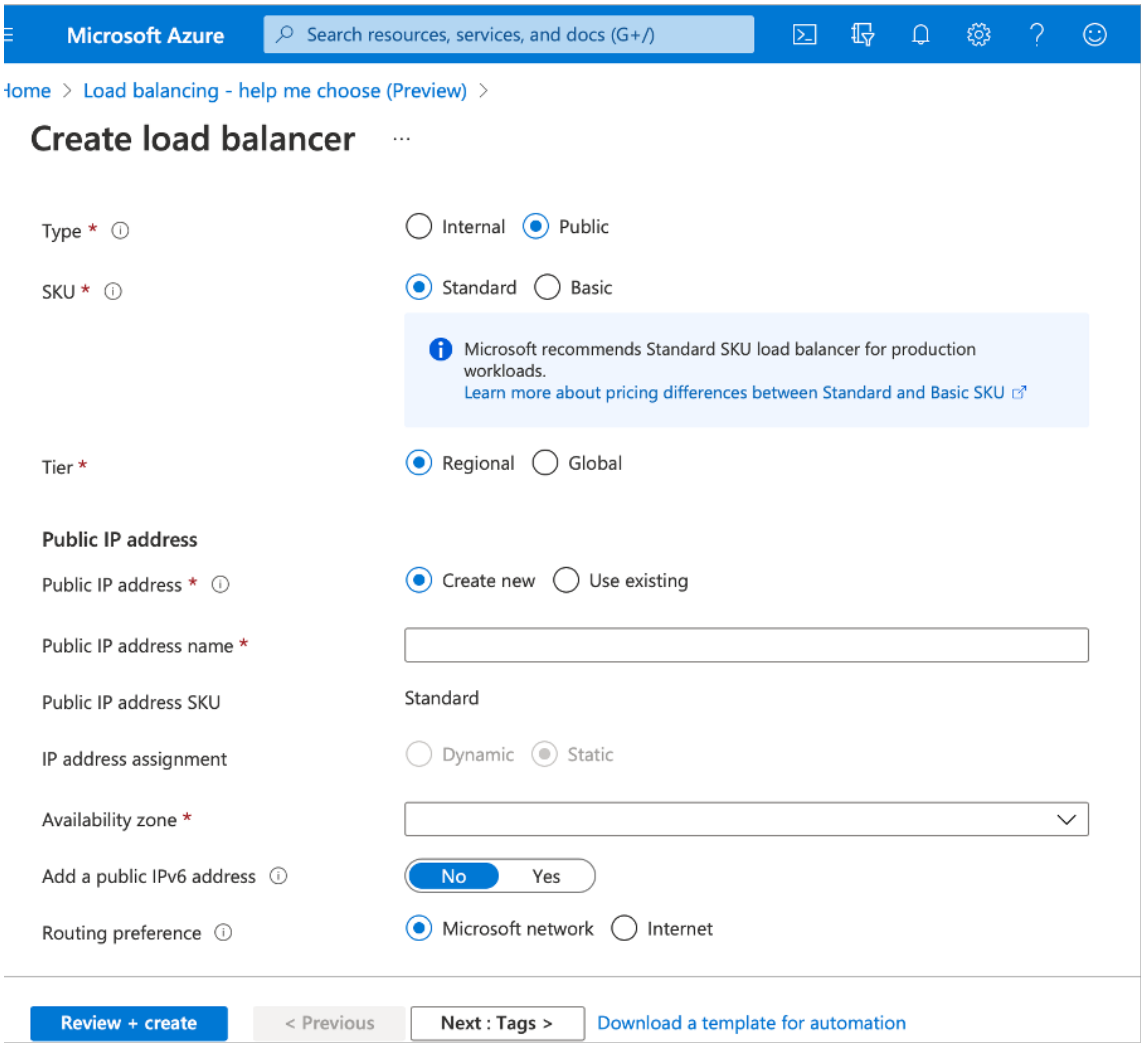
Pour plus d'informations sur la configuration de la haute disponibilité avec les équilibreurs de charge internes Azure, consultez la section Configurer les nœuds HA-INC à l'aide du modèle de haute disponibilité NetScaleravec Azure ILB.

Étape 2. Créez un équilibreur de charge supplémentaire (ILB) dans votre groupe de ressources. À l'étape 1, si vous avez créé un équilibreur de charge externe, vous créez maintenant un équilibreur de charge interne et inversement.

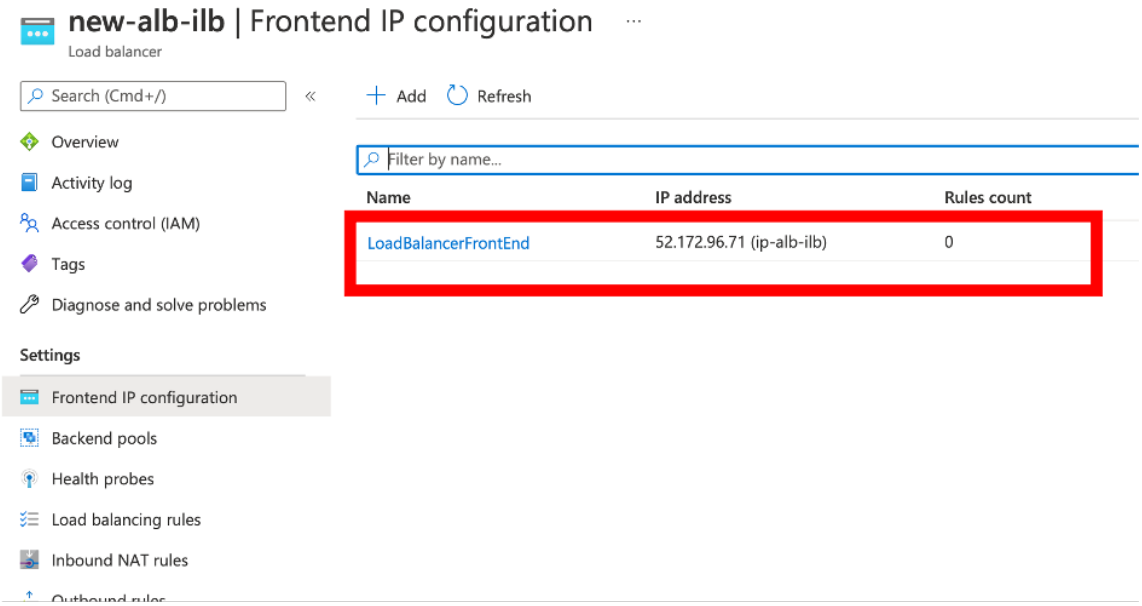
- Pour créer un équilibreur de charge interne, choisissez le type d'équilibreur de charge comme **Interne**. Pour le champ **Sous-réseau**, vous devez choisir le sous-réseau de votre client NetScaler. Vous pouvez choisir de fournir une adresse IP statique dans ce sous-réseau, à condition qu'il n'y ait pas de conflit. Sinon, choisissez l'adresse IP dynamique.



- Pour créer un équilibreur de charge externe, choisissez le type d'équilibreur de charge comme étant **Public** et créez l'adresse IP publique ici.



1. Après avoir créé Azure Load Balancer, accédez à la **configuration IP frontend** et notez l'adresse IP affichée ici. Vous devez utiliser cette adresse IP lors de la création du serveur virtuel d'équilibrage de charge ADC, comme à l'étape 3.



2. Sur la page de **configuration d'Azure Load Balancer**, le déploiement du modèle ARM permet de créer la règle LB, les pools principaux et les sondes de santé.
3. Ajoutez les cartes réseau client de la paire haute disponibilité au pool principal de l'ILB.
4. Créer une sonde de santé (TCP, port 9000)
5. Créez deux règles d'équilibrage de charge :
    - Une règle LB pour le trafic HTTP (cas d'utilisation de l'application Web) sur le port 80. La règle doit également utiliser le port principal 80. Sélectionnez le pool de backend créé et la sonde de santé. L'adresse IP flottante doit être activée.
    - Une autre règle LB pour le trafic HTTPS ou CVAD sur le port 443. Le processus est le même que le trafic HTTP.

Étape 3. Sur le nœud principal de l'appliance NetScaler, créez un serveur virtuel d'équilibrage de charge pour ILB.

1. Ajoutez un serveur virtuel d'équilibrage de charge.

```
add lb vserver <name> <serviceType> [<ILB Frontend IP address>] [<
    port>]
<!--NeedCopy-->
```

Exemple :

```
add lb vserver vserver_name HTTP 52.172.96.71 80
<!--NeedCopy-->
```


> Remarque :
>
> Utilisez l'adresse IP frontale de l'équilibreur de charge, associée à l'équilibreur de charge supplémentaire que vous créez à l'étape 2.

2. Liez un service à un serveur virtuel d'équilibrage de charge.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour plus d'informations, voir Configurer l'équilibrage de charge de base.

Étape 4 : Au lieu de l'étape 3, vous pouvez créer un serveur virtuel d'équilibrage de charge pour ILB à l'aide d'IPsets.

1. Ajoutez une adresse IP de type IP de serveur virtuel (VIP).

```
add nsip <ILB Frontend IP address> -type <type>
<!--NeedCopy-->
```

Exemple :

```
add nsip 52.172.96.71 -type vip
<!--NeedCopy-->
```

2. Ajoutez un IPSet sur les nœuds principaux et secondaires.

```
add ipset <name>
<!--NeedCopy-->
```

Exemple :

```
add ipset ipset1
<!--NeedCopy-->
```

3. Liez les adresses IP au jeu d'adresses IP.

```
bind ipset <name> <ILB Frontend IP address>
<!--NeedCopy-->
```

Exemple :


```
bind ipset ipset1 52.172.96.71
<!--NeedCopy-->
```

4. Définissez le serveur virtuel LB existant pour qu'il utilise IPSet.

```
set lb vserver <vserver name> -ipset <ipset name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vserver_name -ipset ipset1
<!--NeedCopy-->
```

Pour plus d'informations, voir Configurer un serveur virtuel multi-IP.

Installation d'une instance NetScaler VPX sur la solution Azure VMware

May 5, 2023

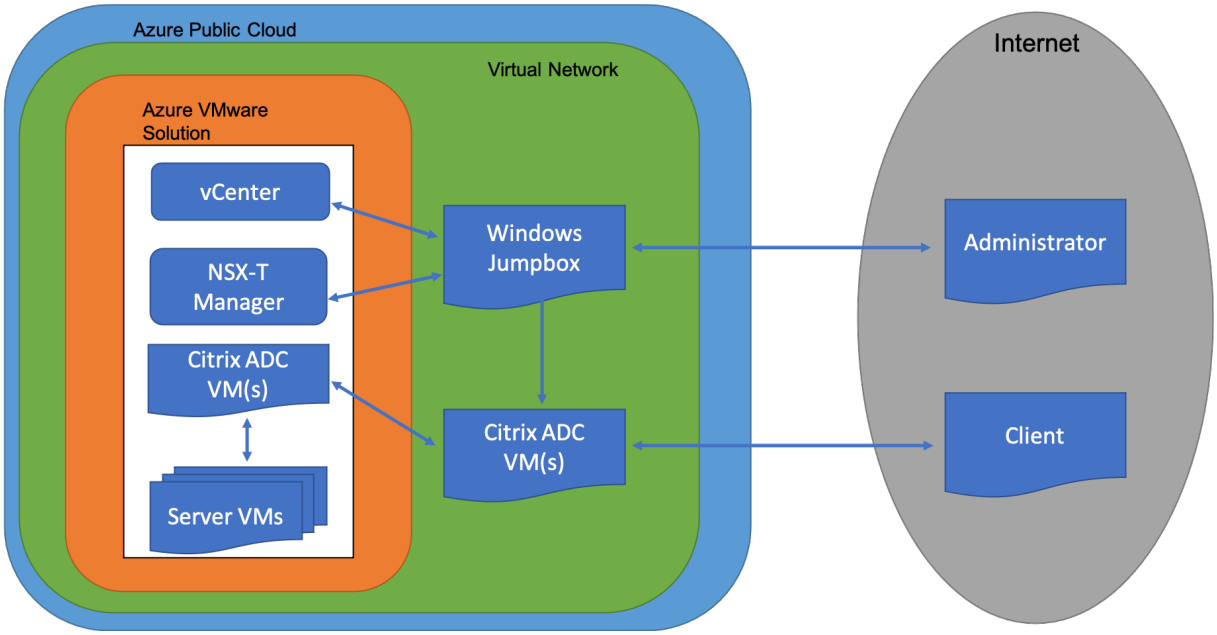
La solution Azure VMware (AVS) vous fournit des clouds privés contenant des clusters vSphere, construits à partir d'une infrastructure Azure dédiée. Le déploiement initial minimum est de trois hôtes, mais des hôtes supplémentaires peuvent être ajoutés un à la fois, jusqu'à 16 hôtes maximum par cluster. Tous les clouds privés provisionnés sont dotés de vCenter Server, vSAN, vSphere et NSX-T.

VMware Cloud (VMC) on Azure vous permet de créer des centres de données définis par logiciel (SDDC) dans le cloud sur Azure avec le nombre d'hôtes ESX que vous souhaitez. La VMC sur Azure prend en charge les déploiements NetScaler VPX. VMC fournit une interface utilisateur identique à vCenter sur site. Il fonctionne de la même manière que les déploiements NetScaler VPX basés sur ESX.

Le diagramme suivant montre la solution Azure VMware sur le cloud public Azure à laquelle un administrateur ou un client peut accéder via Internet. Un administrateur peut créer, gérer et configurer des machines virtuelles de charge de travail ou de serveur à l'aide de la solution Azure VMware. L'administrateur peut accéder au vCenter Web et au gestionnaire NSX-T de l'AVS à partir d'une boîte de dialogue Windows. Vous pouvez créer les instances NetScaler VPX (paire autonome ou haute disponibilité) et les machines virtuelles de serveur au sein de la solution Azure VMware à l'aide de vCenter, et gérer le réseau correspondant à l'aide de NSX-T manager. L'instance NetScaler VPX sur AVS fonctionne de la même manière que le cluster d'hôtes VMware sur site. AVS est géré à partir d'une Jumpbox Windows créée sur le même réseau virtuel.

Un client ne peut accéder au service AVS qu'en se connectant au VIP d'ADC. Une autre instance NetScaler VPX en dehors de la solution Azure VMware mais située dans le même réseau virtuel

Azure permet d'ajouter le VIP de l'instance NetScaler VPX dans la solution Azure VMware en tant que service. Selon vos besoins, vous pouvez configurer l'instance NetScaler VPX pour fournir un service via Internet.



Composants requis

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Pour plus d'informations sur la solution Azure VMware et ses conditions préalables, consultez la documentation de la solution Azure VMware.
- Pour plus d'informations sur le déploiement de la solution Azure VMware, voir Déployer un cloud privé Azure VMware Solution.
- Pour plus d'informations sur la création d'une machine virtuelle Windows Jump Box pour accéder à la solution Azure VMware et la gérer, consultez Access an Azure VMware Solution Private Cloud.
- Dans la machine virtuelle Windows Jump Box, téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments réseau NSX-T appropriés sur VMware SDDC auxquels les machines virtuelles se connectent. Pour plus d'informations, voir Ajouter un segment réseau dans Azure VMware Solution.
- Obtenir des fichiers de licence VPX.
- Les machines virtuelles (VM) créées ou migrées vers le cloud privé Azure VMware Solution doivent être attachées à un segment réseau.

Configuration matérielle du cloud VMware

Le tableau suivant répertorie les ressources informatiques virtuelles que le SDDC VMware doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 1. Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans VMware SDDC, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> Remarque
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production de l'appliance virtuelle VPX, l'allocation complète de mémoire doit être réservée.

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Le tableau suivant décrit la configuration système requise pour l'installation de l'outil OVF.

Tableau 2 Configuration système requise pour l'installation d'outils OVF

Composant	Exigences
OS	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés

Composant	Exigences
Carte d'interface réseau	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.

Téléchargement des fichiers de configuration de NetScaler VPX

Le package de configuration de l'instance NetScaler VPX pour VMware ESX respecte la norme de format Open Virtual Machine (OVF). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l' adresse http://www.citrix.com. Cliquez sur le **lien Nouveaux utilisateurs**et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

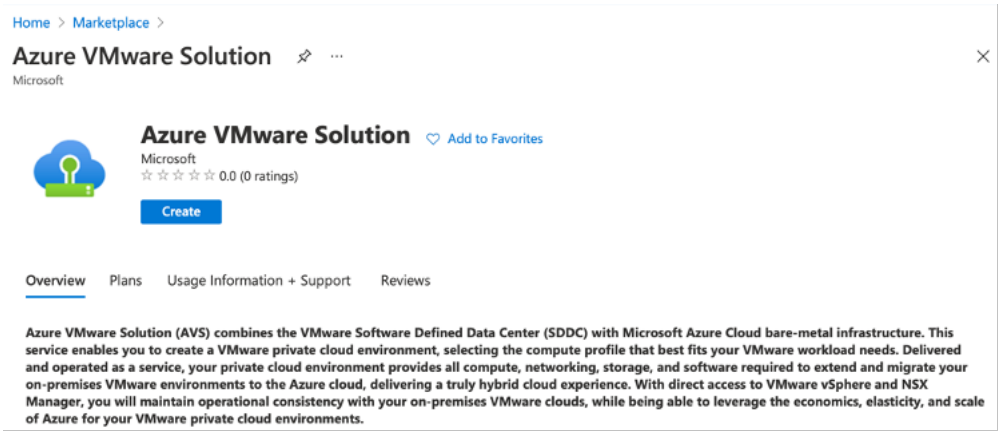
Citrix.com > **Téléchargements > NetScaler > Appliances virtuelles.**

Copiez les fichiers suivants sur une station de travail située sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

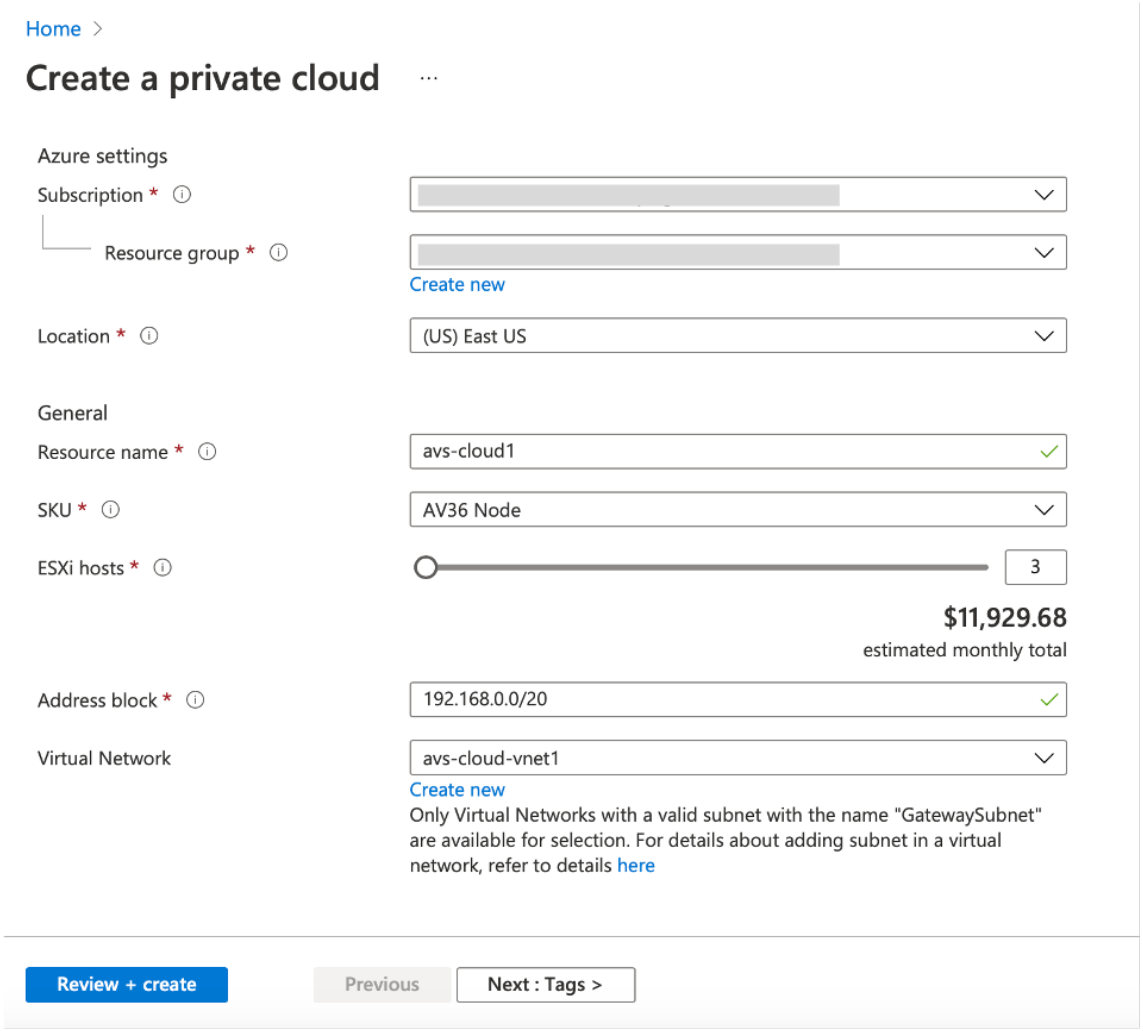
- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (for example, NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (for example, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (for example, NSVPX-ESX-13.0-79.64.mf)

Déploiement de la solution Azure VMware

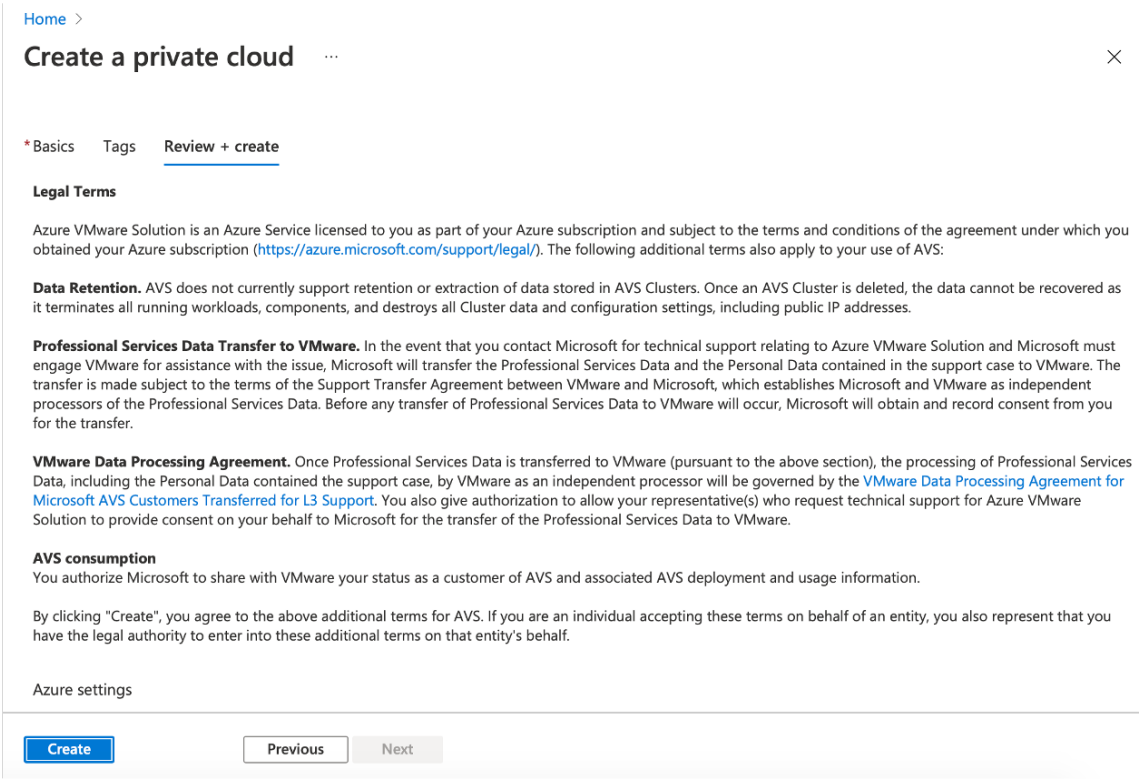
1. Connectez-vous à votre portail Microsoft Azureet accédez à **Azure Marketplace**.
2. Depuis **Azure Marketplace**, recherchez la **solution Azure VMware** et cliquez sur **Créer**.



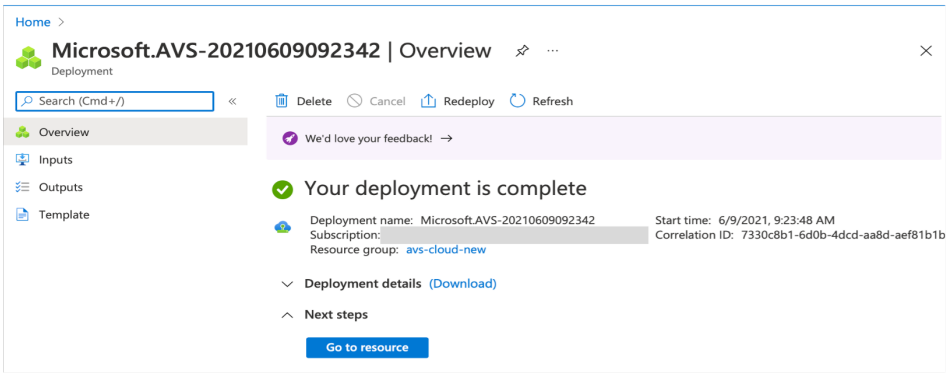
3. Sur la page **Créer un cloud privé**, entrez les informations suivantes :
   - Sélectionnez au moins 3 hôtes ESXi pour créer le cluster par défaut de votre cloud privé.
   - Pour le champ **Bloc d'adresse**, utilisez l'espace d'adressage **/22** .
   - Pour le **réseau virtuel**, assurez-vous que la plage CIDR ne chevauche aucun de vos sous-réseaux locaux ou autres sous-réseaux Azure (réseaux virtuels) ou avec le sous-réseau de passerelle.
   - Le sous-réseau Gateway est utilisé pour exprimer le routage de la connexion avec le cloud privé.



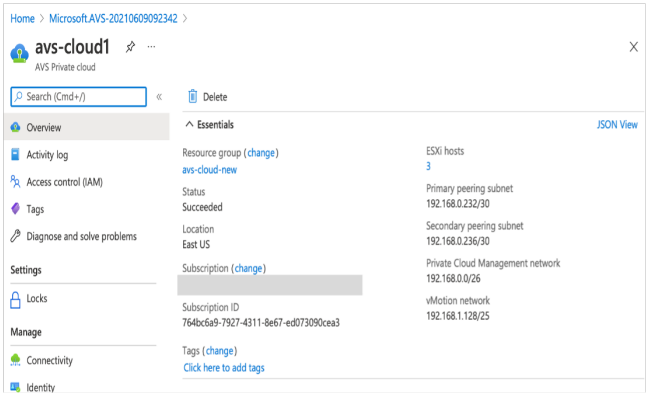
4. Cliquez sur **Réviser + Créer**.
5. Vérifiez les paramètres. Si vous devez modifier des paramètres, cliquez sur **Précédent**.



6. Cliquez sur **Create**. Le processus de provisionnement du cloud privé démarre. Le provisionnement du cloud privé peut prendre jusqu'à deux heures.



7. Cliquez sur **Aller à la ressource**pour vérifier le cloud privé créé.



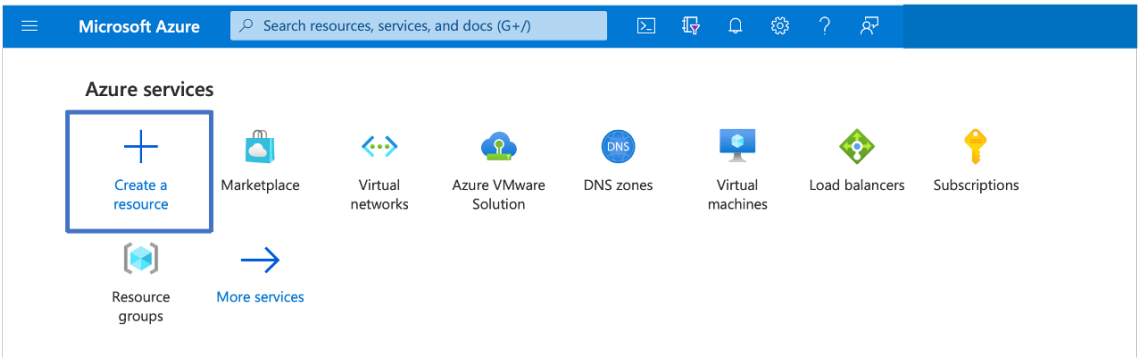
> Remarque
>
> Pour accéder à cette ressource, vous devez disposer d'une machine virtuelle sous Windows qui agit comme une boîte de dialogue Jump.

Connexion à une machine virtuelle Azure exécutant Windows

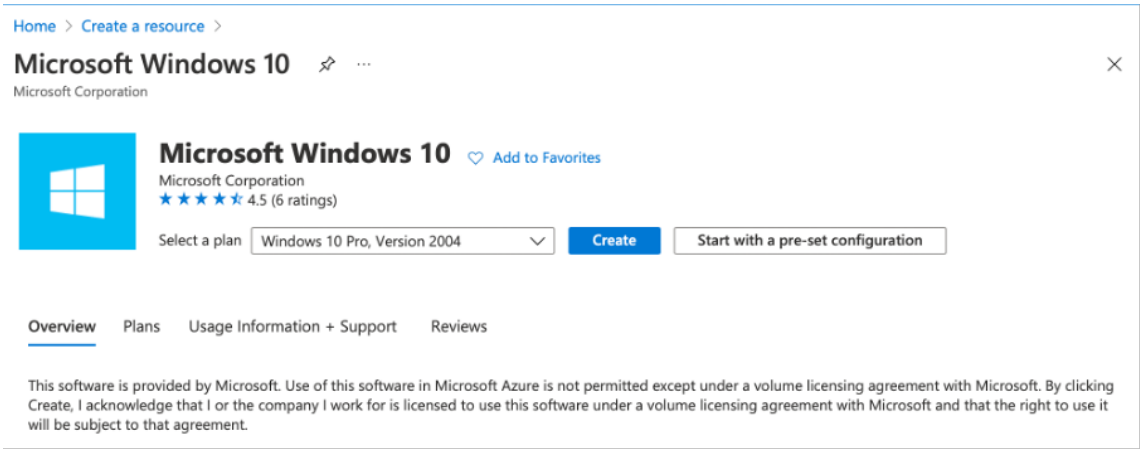
Cette procédure explique comment utiliser le portail Azure pour déployer une machine virtuelle (VM) dans Azure qui exécute Windows Server 2019. Pour voir votre machine virtuelle en action, vous devez ensuite effectuer un RDP sur la machine virtuelle et installer le serveur Web IIS.

Pour accéder au cloud privé que vous avez créé, vous devez créer un Jump Box Windows au sein du même réseau virtuel.

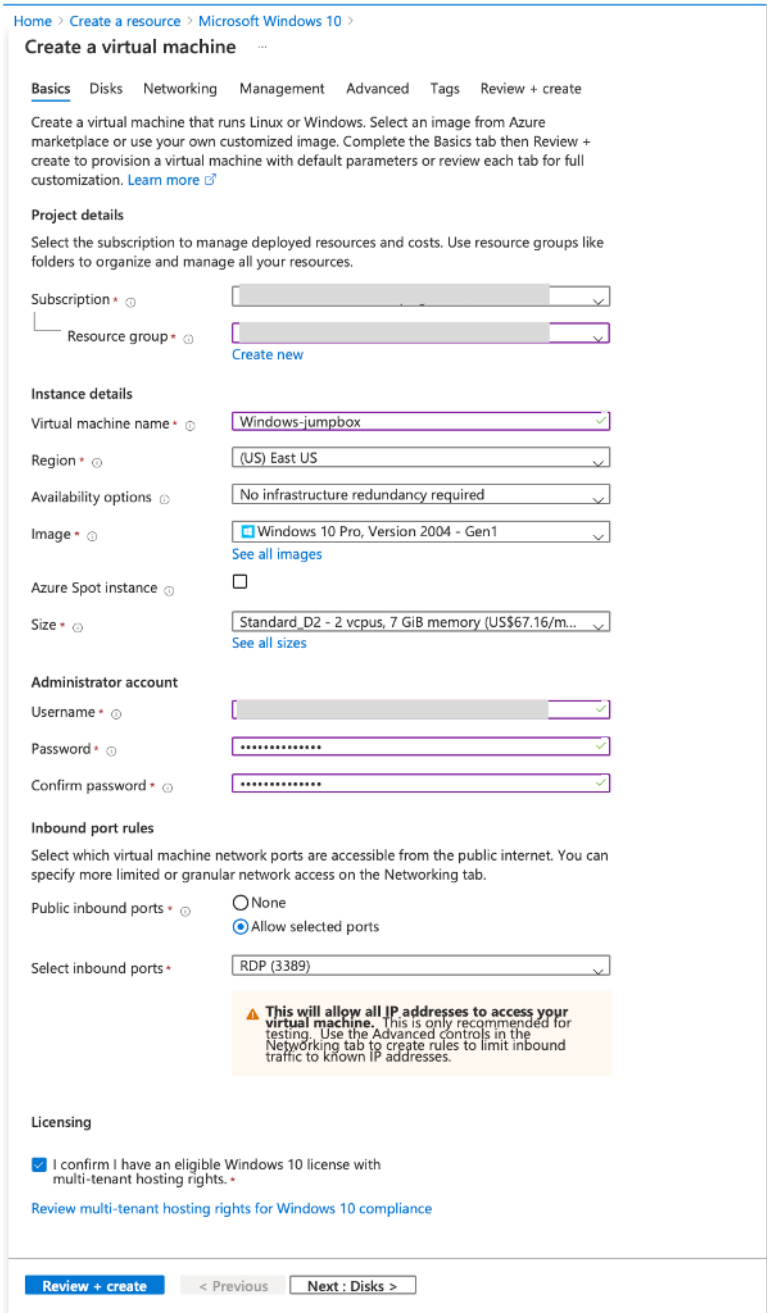
1. Accédez au **portail Azure**, puis cliquez sur **Créer une ressource**.



2. Recherchez **Microsoft Windows 10**, puis cliquez sur **Créer**.



3. Créez une machine virtuelle (VM) qui exécute Windows Server 2019. La page **Créer une machine virtuelle** apparaît. Saisissez tous les détails dans l'onglet **Principes** de base, puis cochez la case **Licences** . Laissez les valeurs par défaut restantes, puis cliquez **sur le bouton Réviser + créer** au bas de la page.



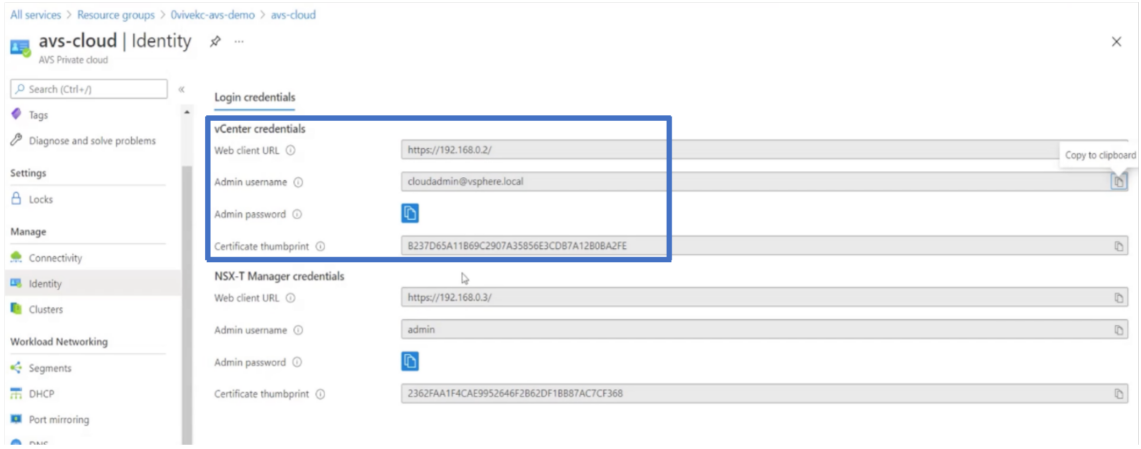
4. Une fois la validation exécutée, cliquez sur le bouton **Créer** en bas de la page.
5. Une fois le déploiement terminé, sélectionnez **Aller à la ressource**.
6. Accédez à la machine virtuelle Windows que vous avez créée. Utilisez l'adresse IP publique de la machine virtuelle Windows et connectez-vous à l'aide de RDP.

   Utilisez le bouton **Connexion** du portail Azure pour démarrer une session Bureau à distance (RDP) à partir d'un poste de travail Windows. Vous vous connectez d'abord à la machine virtuelle, puis vous vous connectez.

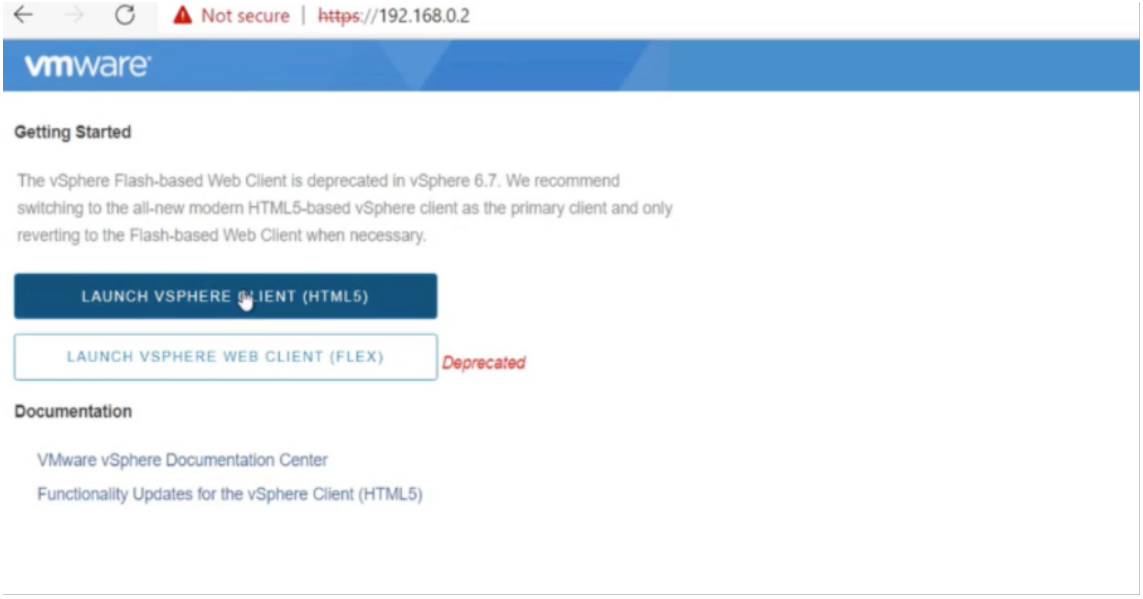
Pour vous connecter à une machine virtuelle Windows à partir d'un Mac, vous devez installer un client RDP pour Mac tel que Microsoft Remote Desktop. Pour plus d'informations, voir Comment se connecter et se connecter à une machine virtuelle Azure exécutant Windows.

Accédez à votre portail Private Cloud vCenter

1. Dans votre cloud privé Azure VMware Solution, sous **Gérer**, sélectionnez **Identité**. Notez les informations d'identification de vCenter.

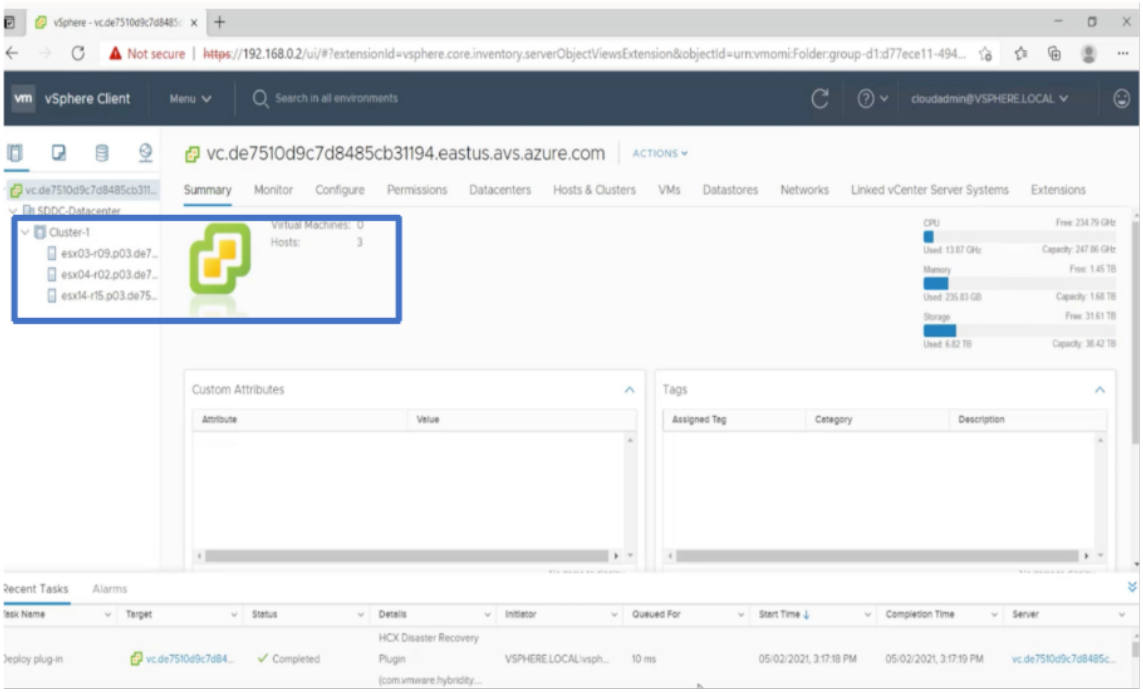


2. Lancez vSphere client en saisissant l'URL du client Web vCenter.



3. Connectez-vous à VMware vSphere à l'aide des informations d'identification vCenter de votre cloud privé Azure VMware Solution.

4. Dans vSphere Client, vous pouvez vérifier les hôtes ESXi que vous avez créés dans le portail Azure.



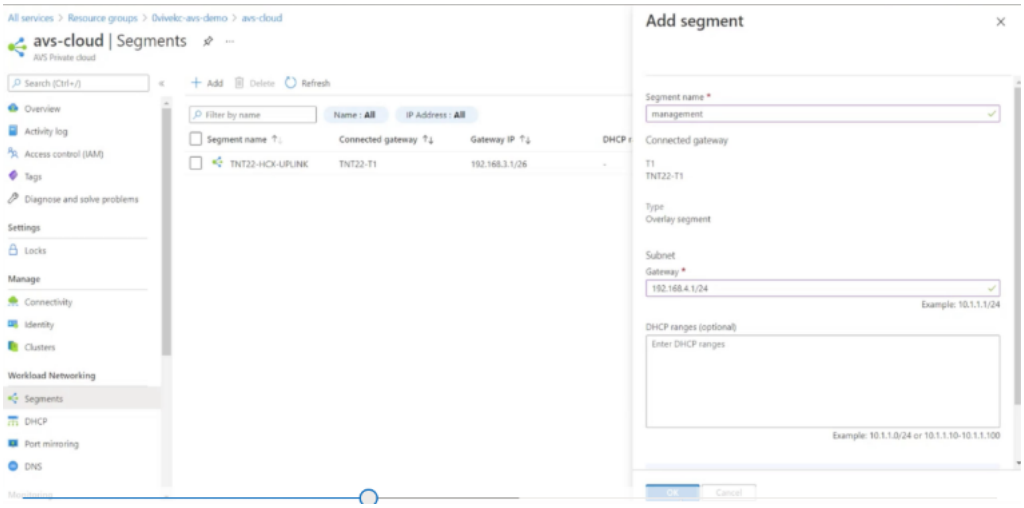
Pour plus d'informations, voir Accès à votre portail Private Cloud vCenter.

Création d'un segment NSX-T dans le portail Azure

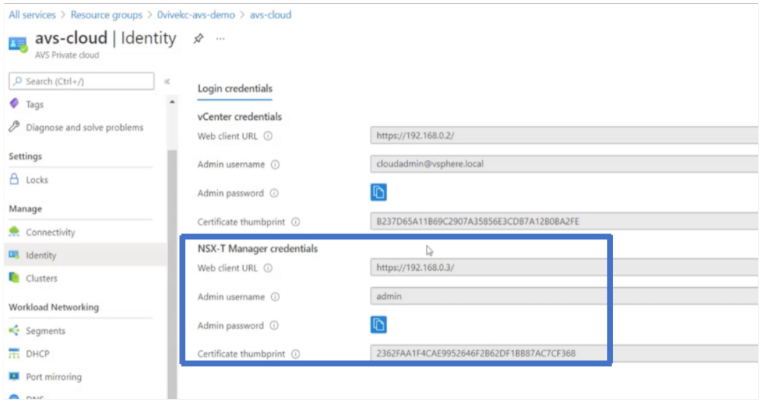
Vous pouvez créer et configurer un segment NSX-T à partir de la console Azure VMware Solution dans le portail Azure. Ces segments sont connectés à la passerelle de niveau 1 par défaut, et les charges

de travail de ces segments sont connectées Est-Ouest et Nord-Sud. Une fois que vous avez créé le segment, il s'affiche dans NSX-T Manager et vCenter.

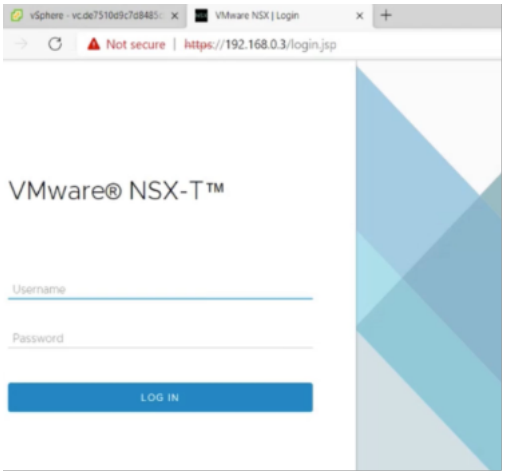
1. Dans votre cloud privé Azure VMware Solution, sous **Workload Networking**, sélectionnez **Segments > Ajouter**. Fournissez les détails du nouveau segment logique et sélectionnez **OK**. Vous pouvez créer trois segments distincts pour les interfaces Client, Management et Server.



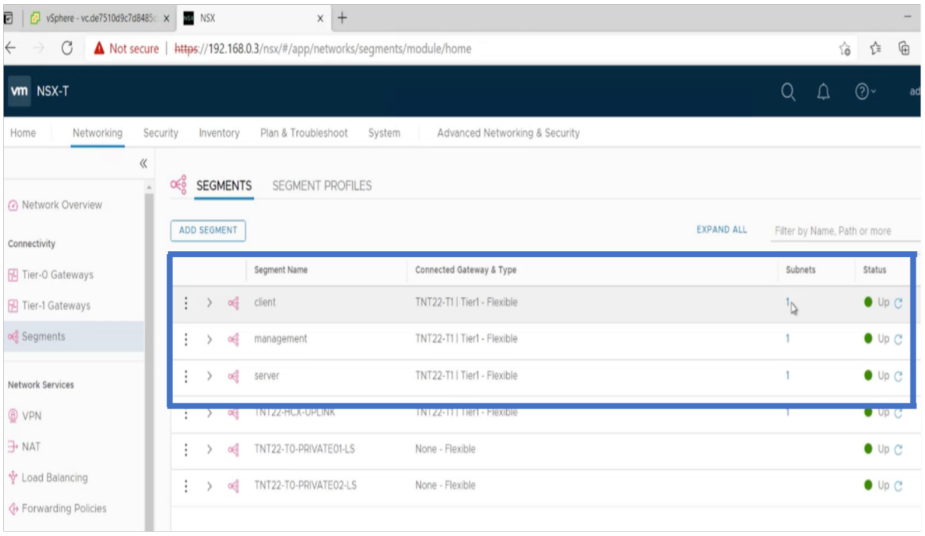
2. Dans votre cloud privé Azure VMware Solution, sous **Gérer**, sélectionnez **Identité**. Notez les informations d'identification NSX-T Manager.



3. Lancez VMware NSX-T Manager en saisissant l'URL du client Web NSX-T.



4. Dans le gestionnaire NSX-T, sous **Mise en réseau > Segments**, vous pouvez voir tous les segments que vous avez créés. Vous pouvez également vérifier les sous-réseaux.



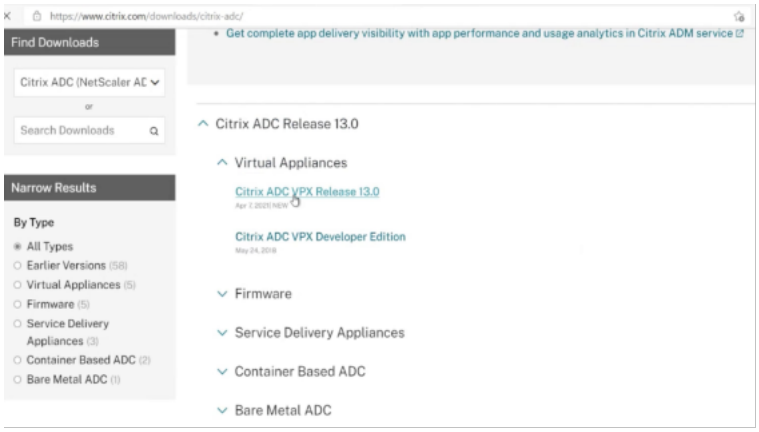
Pour plus d'informations, voir Créer un segment NSX-T dans le portail Azure.

Installation d'une instance NetScaler VPX sur le cloud VMware

Après avoir installé et configuré VMware Software-Defined Data Center (SDDC), vous pouvez utiliser le SDDC pour installer des appliances virtuelles sur le cloud VMware. Le nombre d'appliances virtuelles que vous pouvez installer dépend de la quantité de mémoire disponible sur le SDDC.

Pour installer des instances NetScaler VPX sur le cloud VMware, effectuez ces étapes dans la machine virtuelle Windows Jumpbox :

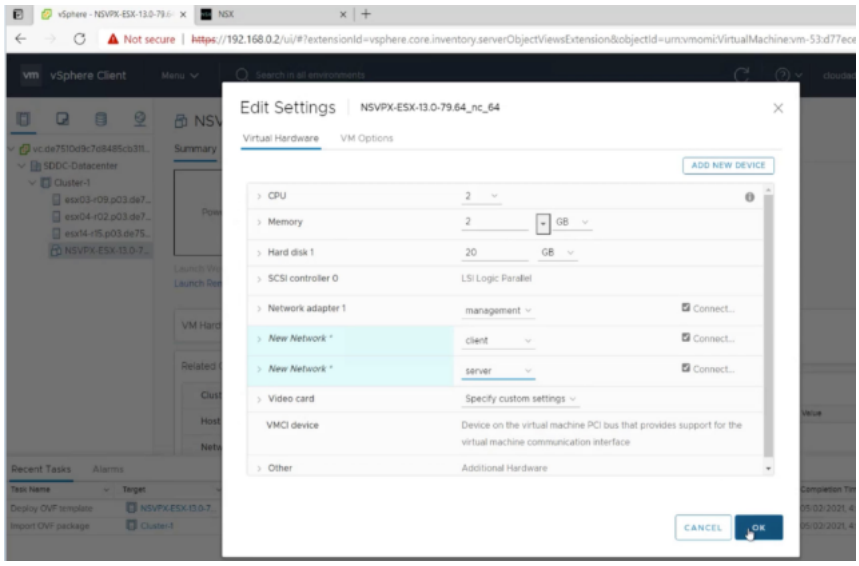
1. Téléchargez les fichiers de configuration de l'instance NetScaler VPX pour l'hôte ESXi depuis le site de téléchargement de NetScaler.



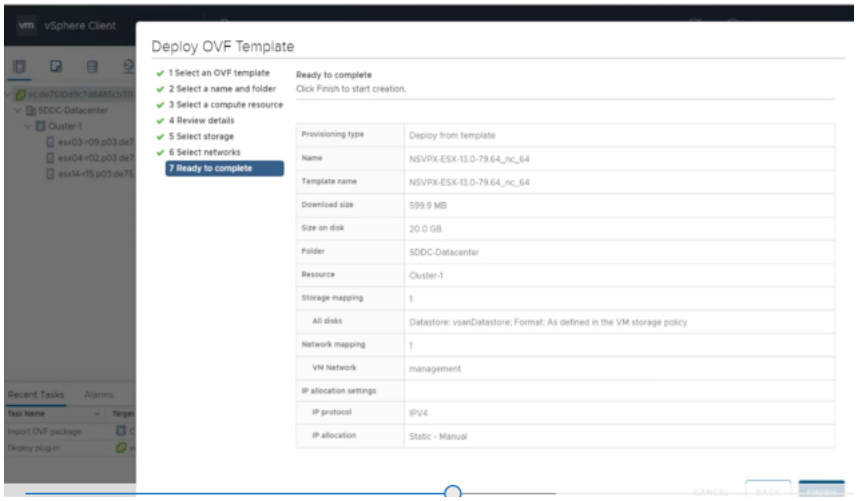
2. Ouvrez le SDDC VMware dans la Jumpbox Windows.
3. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur **Connexion**.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
5. **Dans la boîte de dialogue**Déployer le modèle OVF**, dans le champ**Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers de configuration de l'instance NetScaler VPX, sélectionnez le fichier .ovf et cliquez sur Suivant.**

   > REMARQUE
   >
   > Par défaut, l'instance NetScaler VPX utilise les interfaces réseau E1000. Pour déployer ADC avec l'interface VMXNET3, modifiez l'OVF pour utiliser l'interface VMXNET3 au lieu de l'E1000. La disponibilité de l'interface VMXNET3 est limitée par l'infrastructure Azure et peut ne pas être disponible dans Azure VMware Solution.

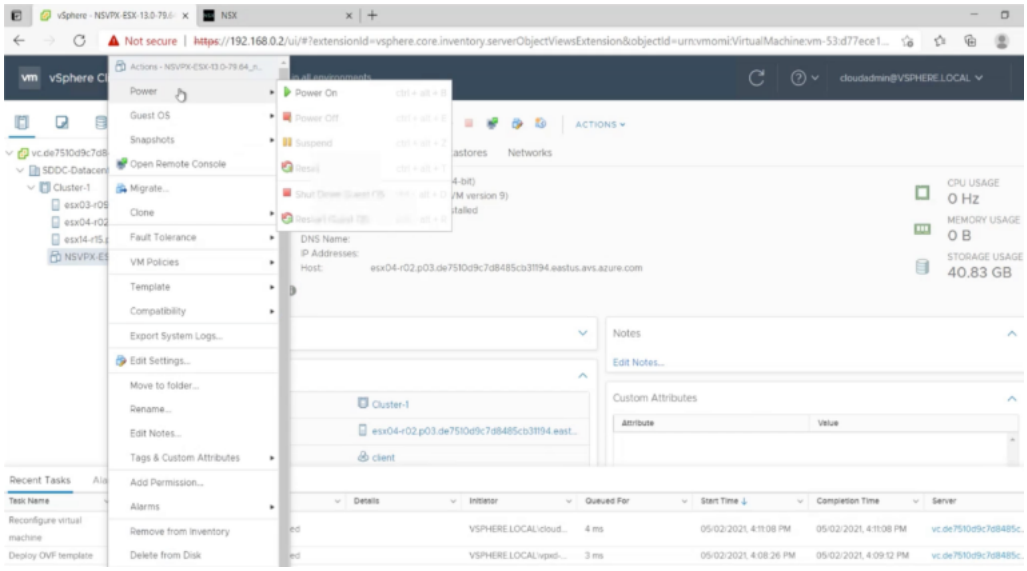
6. Mappez les réseaux affichés dans le modèle OVF de l'appliance virtuelle aux réseaux que vous avez configurés sur VMware SDDC. Cliquez sur **OK**.



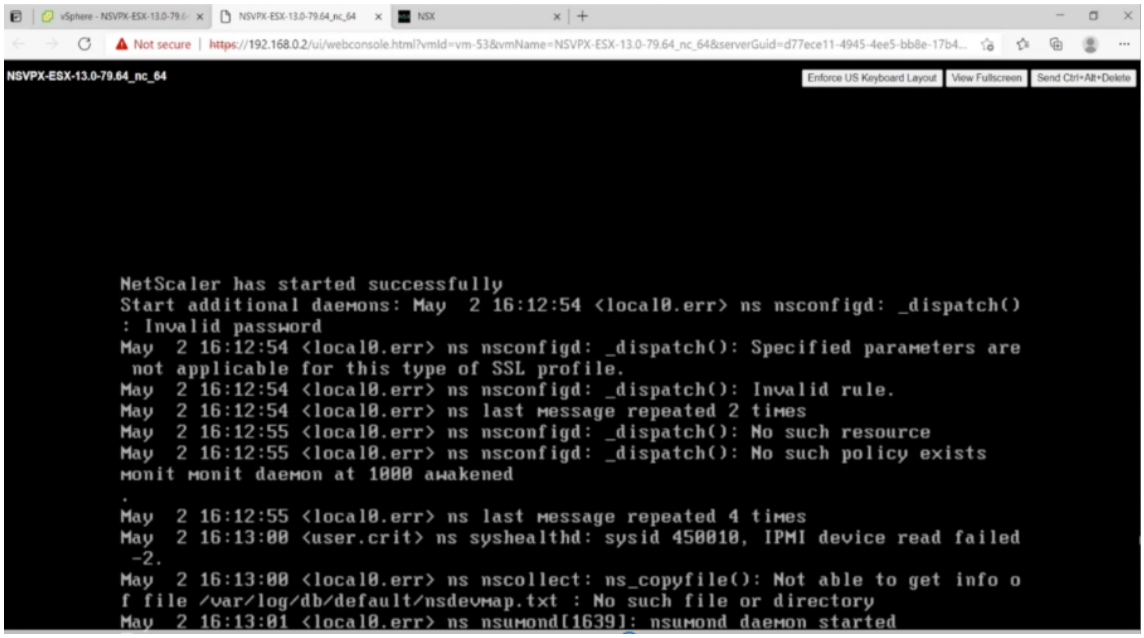
7. Cliquez sur **Terminer** pour commencer l'installation d'une appliance virtuelle sur VMware SDDC.



8. Vous êtes maintenant prêt à démarrer l'instance NetScaler VPX. **Dans le volet de navigation, sélectionnez l'instance NetScaler VPX que vous avez installée et, dans le menu contextuel, sélectionnez Power On.** Cliquez sur l'onglet **Console** pour émuler un port de console.



9. Vous êtes désormais connecté à la machine virtuelle NetScaler depuis le client vSphere.



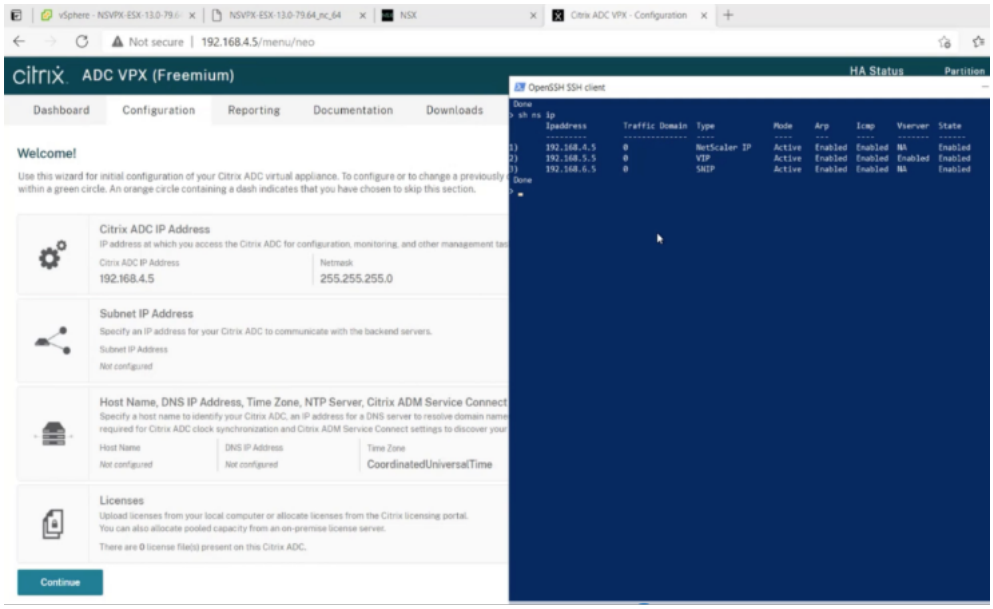
10. Pour accéder à l'appliance NetScaler à l'aide des clés SSH, tapez la commande suivante dans l'interface de ligne de commande :

```
ssh nsroot@<management IP address>
<!--NeedCopy-->
```

Exemple :

```
ssh nsroot@192.168.4.5
<!--NeedCopy-->
```

11. Vous pouvez vérifier la configuration ADC à l'aide de la `show ns ip` commande.

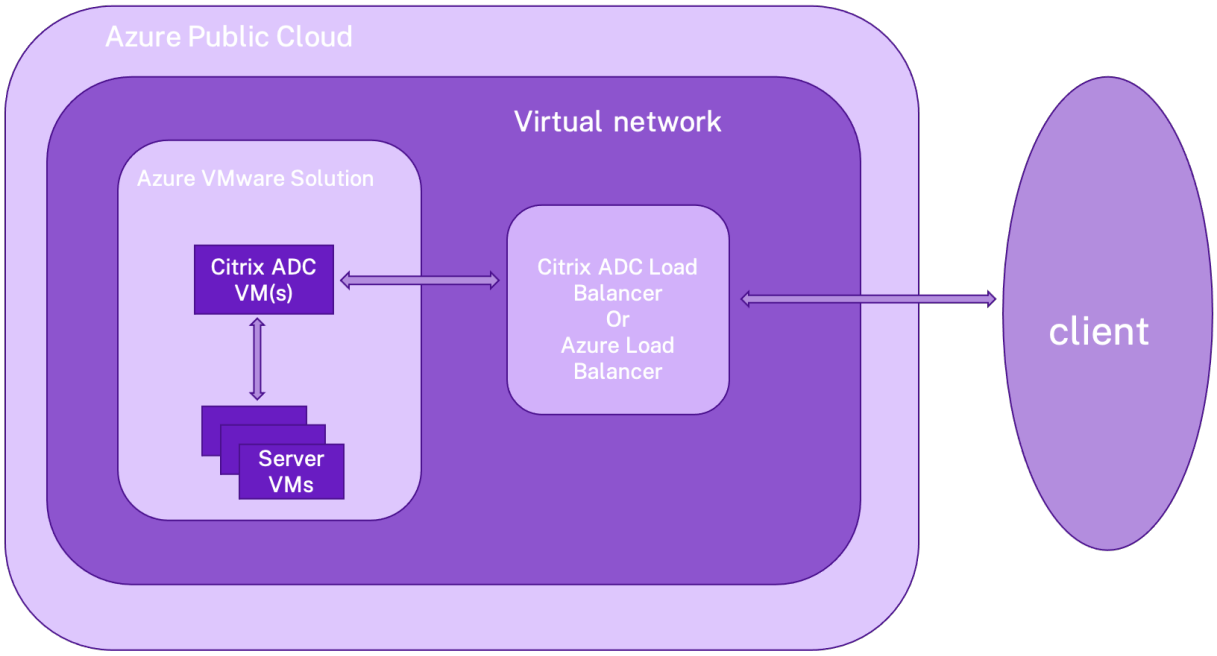


Configurer une instance autonome NetScaler VPX sur la solution Azure VMware

May 5, 2023

Vous pouvez configurer une instance autonome NetScaler VPX sur la solution Azure VMware (AVS) pour les applications connectées à Internet.

Le schéma suivant montre l'instance autonome NetScaler VPX sur la solution Azure VMware. Un client peut accéder au service AVS en se connectant à l'adresse IP virtuelle (VIP) de NetScaler au sein de l'AVS. Vous pouvez y parvenir en provisionnant un équilibreur de charge NetScaler ou l'instance d'équilibreur de charge Azure en dehors d'AVS mais dans le même réseau virtuel Azure. Configurez l'équilibreur de charge pour accéder au VIP de l'instance NetScaler VPX au sein du service AVS.



Composants requis

Avant de commencer à installer un dispositif virtuel, lisez les conditions préalables Azure suivantes :

- Pour plus d'informations sur la solution Azure VMware et ses conditions préalables, consultez la documentation de la solution Azure VMware.
- Pour plus d'informations sur le déploiement de la solution Azure VMware, voir Déployer un cloud privé Azure VMware Solution.
- Pour plus d'informations sur la création d'une machine virtuelle Windows Jump Box pour accéder à la solution Azure VMware et la gérer, voir Accéder à un cloud privé Azure VMware Solution.

- Dans la machine virtuelle Windows Jump Box, téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments réseau NSX-T appropriés sur VMware SDDC auxquels les machines virtuelles se connectent. Pour plus d'informations, voir Ajouter un segment réseau dans Azure VMware Solution.
- Pour plus d'informations sur l'installation d'une instance NetScaler VPX sur le cloud VMware, voir Installer une instance NetScaler VPXsur le cloud VMware.

Configurer une instance autonome NetScaler VPX sur AVS à l'aide de l'équilibreur de charge NetScaler

Suivez ces étapes pour configurer l'instance autonome NetScaler VPX sur AVS pour les applications connectées à Internet à l'aide de l'équilibreur de charge NetScaler.

1. Déployez une instance NetScaler VPX sur le cloud Azure. Pour plus d'informations, consultez la section Configurer une instance autonome NetScaler VPX.

   > Remarque :
   >
   > Assurez-vous qu'il est déployé sur le même réseau virtuel que le cloud Azure VMware.

2. Configurez l'instance NetScaler VPX pour accéder à l'adresse VIP de NetScaler VPX déployé sur AVS.

   a) Ajoutez un serveur virtuel d'équilibrage de charge.

   ```
   add lb vserver <name> <serviceType> [<vip>] [<port>]
   <!--NeedCopy-->
   ```

   Exemple :

   ```
   add lb vserver lb1 HTTPS 172.31.0.6 443
   <!--NeedCopy-->
   ```

   b) Ajoutez un service qui se connecte au VIP de NetScaler VPX déployé sur AVS.

   ```
   add service <name> <ip> <serviceType> <port>
   <!--NeedCopy-->
   ```

   Exemple :

   ```
   add service webserver1 192.168.4.10 HTTP 80
   <!--NeedCopy-->
   ```

   c) Liez un service au serveur virtuel d'équilibrage de charge.


```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb1 webserver1
<!--NeedCopy-->
```

Configurer l'instance autonome NetScaler VPX sur AVS à l'aide de l'équilibreur de charge Azure

Suivez ces étapes pour configurer l'instance autonome NetScaler VPX sur AVS pour les applications connectées à Internet à l'aide de l'équilibreur de charge Azure.

1. Configurez une instance d'Azure Load Balancer de charge Azure sur le cloud Azure. Pour plus d'informations, consultez la documentation Azure sur la création d'un équilibreurde charge.
2. Ajoutez l'adresse VIP de l'instance NetScaler VPX déployée sur AVS au pool principal.

   La commande Azure suivante ajoute une adresse IP principale dans le pool d'adresses principal d'équilibrage de charge.

```
az network lb address-pool address add
                                    --resource-group <Azure VMC
                                       Resource Group>
                                    --lb-name <LB Name>
                                    --pool-name <Backend pool name
                                       >
                                    --vnet <Azure VMC Vnet>
                                    --name <IP Address name>
                                    --ip-address <VIP of ADC in
                                       VMC>
<!--NeedCopy-->
```

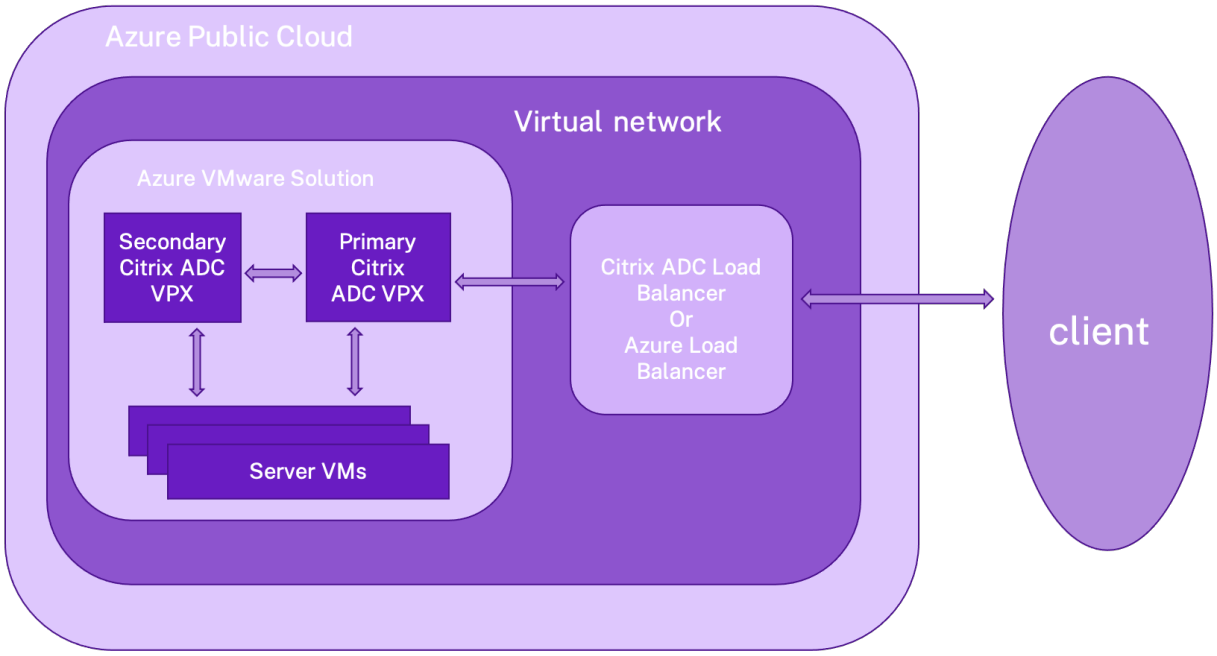
> Remarque :
>
> Assurez-vous que l'équilibreur de charge Azure est déployé sur le même réseau virtuel que le cloud Azure VMware.

Configurer une configuration de haute disponibilité NetScaler VPX sur la solution Azure VMware

May 5, 2023

Vous pouvez configurer une configuration NetScaler VPX HA sur la solution Azure VMware (AVS) pour les applications connectées à Internet.

Le schéma suivant montre la paire NetScaler VPX HA sur AVS. Un client peut accéder au service AVS en se connectant au VIP du nœud ADC principal à l'intérieur de l'AVS. Vous pouvez y parvenir en provisionnant un équilibreur de charge NetScaler ou l'instance d'équilibreur de charge Azure en dehors d'AVS mais dans le même réseau virtuel Azure. Configurez l'équilibreur de charge pour accéder à l'adresse IP virtuelle du nœud ADC principal dans le service AVS.



Composants requis

Avant de commencer à installer un dispositif virtuel, lisez les conditions préalables Azure suivantes :

- Pour plus d'informations sur la solution Azure VMware et ses conditions préalables, consultez la documentation de la solution Azure VMware.
- Pour plus d'informations sur le déploiement de la solution Azure VMware, voir Déployer un cloud privé Azure VMware Solution.
- Pour plus d'informations sur la création d'une machine virtuelle Windows Jump Box pour accéder à la solution Azure VMware et la gérer, voir Accéder à un cloud privé Azure VMware Solution.

- Dans la machine virtuelle Windows Jump Box, téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments réseau NSX-T appropriés sur VMware SDDC auxquels les machines virtuelles se connectent. Pour plus d'informations, consultez Ajouter un segment réseau dans la solution Azure VMware.

Étapes de configuration

Suivez ces étapes pour configurer la configuration de haute disponibilité de NetScaler VPX dans AVS pour les applications connectées à Internet.

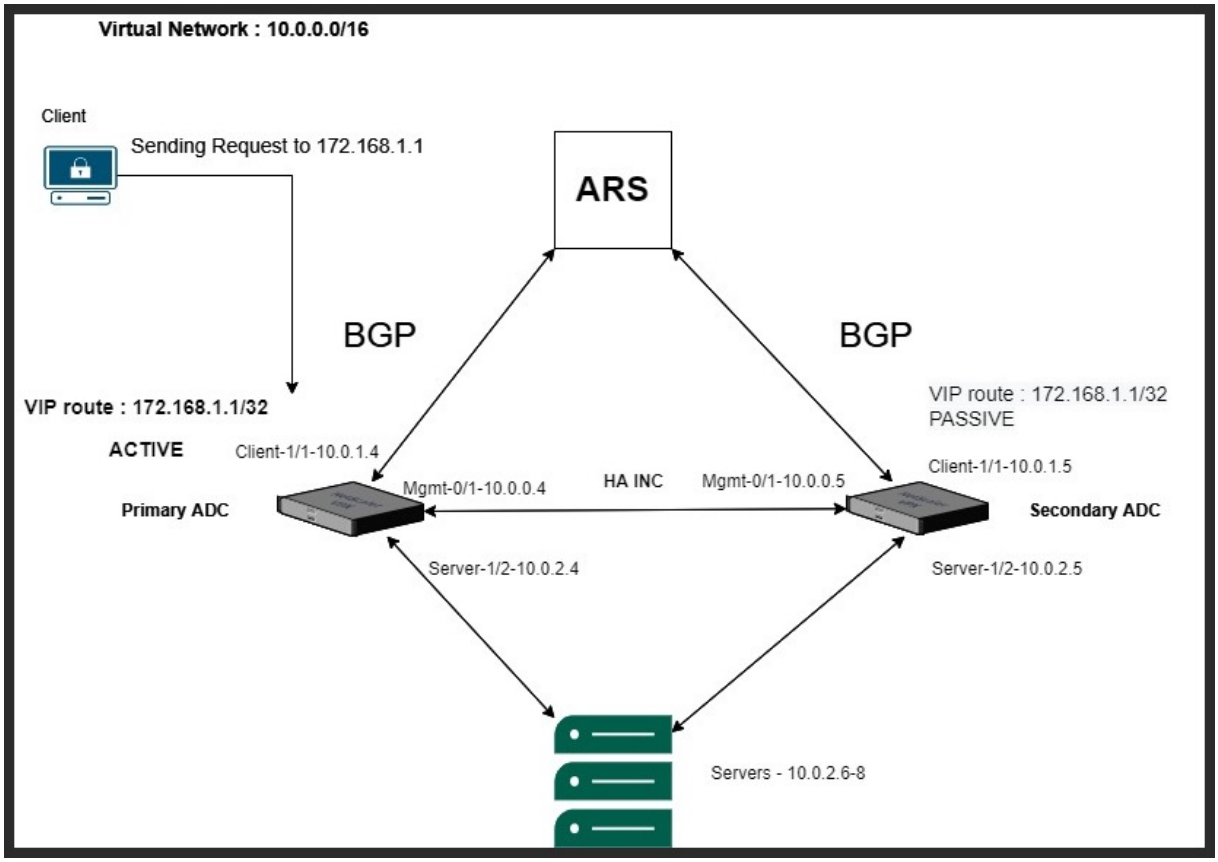
1. Créez deux instances NetScaler VPX sur le cloud VMware. Pour plus d'informations, consultez Installer une instance NetScaler VPX sur le cloud VMware.
2. Configurez la configuration de NetScaler HA. Pour plus d'informations, voir Configuration de la haute disponibilité.
3. Configurez la configuration NetScaler HA pour qu'elle soit accessible aux applications connectées à Internet.
    - Pour configurer l'instance NetScaler VPX à l'aide de l'équilibreur de charge NetScaler, voir Configurer une instance autonome NetScaler VPX sur AVS à l'aide de l'équilibreur de charge NetScaler.
    - Pour configurer l'instance NetScaler VPX à l'aide de l'équilibreur de charge Azure, voir Configurer l'instance autonome NetScaler VPXsur AVS à l'aide de l'équilibreur de charge Azure.

Configurer le serveur de routage Azure avec la paire NetScaler VPX HA

May 5, 2023

Vous pouvez configurer le serveur de route Azure avec l'instance NetScaler VPX pour échanger les itinéraires VIP configurés avec le réseau virtuel à l'aide du protocole BGP. Le NetScaler peut être déployé en mode autonome ou en mode HA-INC, puis configuré avec BGP. Ce déploiement ne nécessite pas d'équilibreur de charge Azure (ALB) devant la paire ADC HA.

Le diagramme suivant montre comment une topologie VPX HA est intégrée au serveur de routage Azure. Chacune des instances ADC possède 3 interfaces : une pour la gestion, une pour le trafic client et une pour le trafic serveur.



Le diagramme topologique utilise les adresses IP suivantes.

Exemple de configuration IP pour l'instance ADC principale :

```
NSIP: 10.0.0.4/24
SNIP on 1/1: 10.0.1.4/24
SNIP on 1/2: 10.0.2.4/24
VIP: 172.168.1.1/32
<!--NeedCopy-->
```

Exemple de configuration IP pour l'instance ADC secondaire :

```
NSIP: 10.0.0.5/24
SNIP on 1/1: 10.0.1.5/24
SNIP on 1/2: 10.0.2.5/24
VIP: 172.168.1.1/32
<!--NeedCopy-->
```

Composants requis

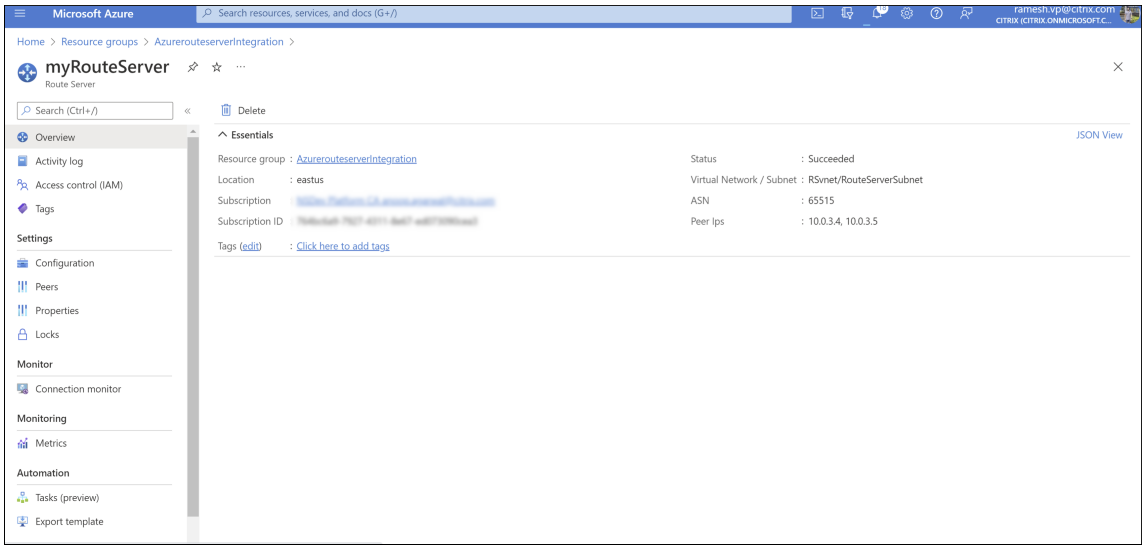
Vous devez connaître les informations suivantes avant de déployer une instance NetScaler VPX sur Azure.

- Terminologie Azure et détails réseau. Pour plus d'informations, consultez la section Terminologie Azure.
- Présentation d'Azure Route Server. Pour plus d'informations, consultez Qu'est-ce qu'Azure Route Server ?.
- Fonctionnement d'une appliance NetScaler. Pour plus d'informations, consultez la documentation de NetScaler.
- Réseau NetScaler. Pour plus d'informations, consultez la section Réseau ADC.

Comment configurer un serveur de routage Azure avec la paire NetScaler VPX HA

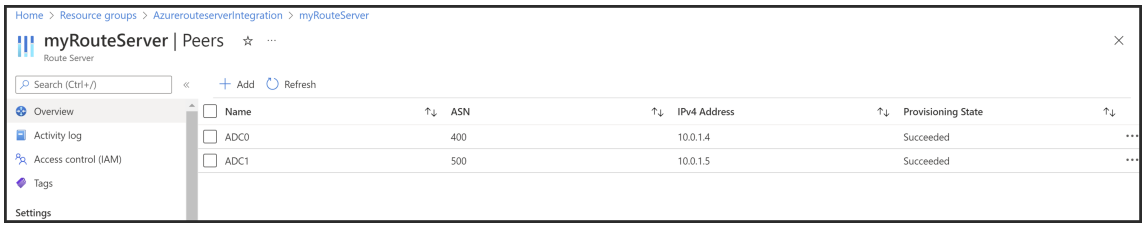
1. Créez un serveur de routage sur le portail Azure. Pour plus d'informations, consultez Créer et configurer un serveur de routage à l'aide du portail Azure.

   Dans l'exemple suivant, le sous-réseau 10.0.3.0/24 est utilisé pour déployer le serveur Azure. Une fois le serveur de routage créé, récupérez les adresses IP du serveur de routage, par exemple : 10.0.3.4, 10.0.3.5.



2. Configurez l'appairage avec l'appliance virtuelle réseau (NVA) dans le portail Azure. Ajoutez votre instance NetScaler VPX en tant que NVA. Pour plus d'informations, consultez la section Configuration de l'appairage avec NVA.

   Dans l'exemple suivant, le SNIP ADC sur les interfaces 1/1 : 10.0.1.4 et 10.0.1.5, et l'ASN : 400 et 500, sont utilisés lors de l'ajout de l'homologue.



3. Ajoutez deux instances NetScaler VPX pour la configuration HA.

   Effectuez les étapes suivantes :

   a) Déployez deux instances VPX (instances principales et secondaires) sur Azure.
   b) Ajoutez une carte réseau client et serveur sur les deux instances.
   c) Configurez les paramètres HA sur les deux instances à l'aide de l'interface graphique NetScaler.

4. Configurez le routage dynamique dans l'instance ADC principale.

   Exemple de configuration :

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -dynamicRouting
    ENABLED
VTYSH
configure terminal
router BGP 400
timers bgp 1 3
neighbor 10.0.3.4 remote-as 65515
neighbor 10.0.3.4 advertisement-interval 3
neighbor 10.0.3.4 fall-over  bfd
neighbor 10.0.3.5 remote-as 65515
neighbor 10.0.3.5 advertisement-interval 3
neighbor 10.0.3.5 fall-over  bfd
address-family ipv4
redistribute kernel
redistribute static
<!--NeedCopy-->
```

5. Configurez le routage dynamique dans l'instance ADC secondaire.

   Exemple de configuration :

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
add ns ip 10.0.1.5 255.255.255.0 -vServer DISABLED -dynamicRouting
    ENABLED
VTYSH
configure terminal
router BGP 500
timers bgp 1 3
neighbor 10.0.3.4 remote-as 65515
neighbor 10.0.3.4 advertisement-interval 3
neighbor 10.0.3.4 fall-over  bfd
```



```
neighbor 10.0.3.5 remote-as 65515
neighbor 10.0.3.5 advertisement-interval 3
neighbor 10.0.3.5 fall-over  bfd
address-family ipv4
redistribute kernel
redistribute static
<!--NeedCopy-->
```

6. Vérifiez les homologues BGP établis à l'aide des commandes BGP dans l'interface shell VTY. Pour plus d'informations, consultez la section Vérification de la configuration BGP.

```
show ip bgp neighbors
<!--NeedCopy-->
```

7. Configurez le serveur virtuel LB dans l'instance ADC principale.

   Exemple de configuration :

```
add ns ip 172.16.1.1 255.255.255.255 -type VIP -hostRoute ENABLED
add lbvserver v1 HTTP 172.16.1.1 80
add service s1 10.0.2.6 HTTP 80
bind lbvserver v1 s1
enable ns feature lb
<!--NeedCopy-->
```

   Un client du même réseau virtuel que celui de l'instance NetScaler VPX peut désormais accéder au serveur virtuel LB. Dans ce cas, l'instance NetScaler VPX annonce l'itinéraire VIP vers le serveur de routage Azure.

Ajouter des paramètres Azure Autoscale

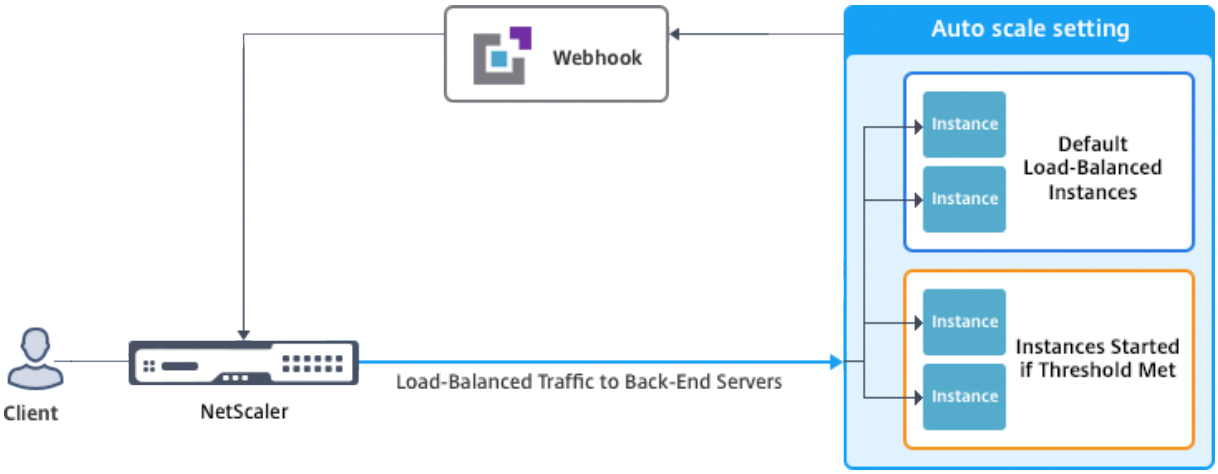
May 5, 2023

L'hébergement efficace des applications dans un cloud implique une gestion aisée et économique des ressources en fonction de la demande des applications. Pour répondre à la demande croissante, vous devez augmenter les ressources réseau. Que la demande diminue, vous devez réduire la demande afin d'éviter le coût inutile des ressources inutilisées. Pour minimiser le coût d'exécution de l'application, vous devez surveiller en permanence le trafic, la mémoire et l'utilisation du processeur, etc. Toutefois, la surveillance manuelle du trafic est fastidieuse. Pour que l'environnement d'application évolue de manière dynamique, vous devez automatiser les processus de surveillance du trafic et de mise à l'échelle des ressources lorsque cela est nécessaire.

Vous pouvez utiliser Autoscale avec des jeux d'échelle de machines virtuelles Azure (VMSS) pour le déploiement autonome et haute disponibilité VPX Multi-IP sur Azure.

Intégrée aux fonctionnalités Azure VMSS et Autoscale, l'instance NetScaler VPX offre les avantages suivants :

- Équilibre de charge et gestion : configure automatiquement les serveurs pour qu'ils augmentent et diminuent, en fonction de la demande. L'instance NetScaler VPX détecte automatiquement le paramètre VMSS Autoscale dans le même réseau virtuel que celui où l'instance VPX est déployée, ou dans les réseaux virtuels homologues qui font partie du même abonnement Azure. Vous pouvez sélectionner le paramètre VMSS Autoscale pour équilibrer la charge. Cela se fait en configurant automatiquement l'adresse IP virtuelle NetScaler et l'adresse IP du sous-réseau sur l'instance VPX.
- Haute disponibilité : détecte les groupes Autoscale et équilibre la charge des serveurs.
- Meilleure disponibilité du réseau : l'instance VPX prend en charge les serveurs back-end sur différents réseaux virtuels (VNET).



Pour plus d'informations, consultez la rubrique Azure suivante

- Documentation sur les jeux d'échelle de machine virtuelle
- Présentation d'Autoscale dans les machines virtuelles Microsoft Azure, les services cloud et les applications Web

Avant de commencer

1. Lisez les instructions d'utilisation relatives à Azure. Pour plus d'informations, consultez Déployer une instance NetScaler VPX sur Microsoft Azure.
2. Créez une ou plusieurs instances NetScaler VPX avec trois interfaces réseau sur Azure en fonction de vos besoins (déploiement autonome ou haute disponibilité).
3. Ouvrez le port TCP 9001 sur le groupe de sécurité réseau de l'interface 0/1 de l'instance VPX. L'instance VPX utilise ce port pour recevoir la notification de scale-out et de scale-in.

4. Créez un Azure VMSS dans le même réseau virtuel que celui où l'instance NetScaler VPX est déployée. Si les instances VMSS et NetScaler VPX sont déployées dans différents réseaux virtuels Azure, les conditions suivantes doivent être remplies :

   - Les deux réseaux virtuels doivent appartenir au même abonnement Azure.
   - Les deux réseaux virtuels doivent être connectés à l'aide de la fonctionnalité d'appairage de réseaux virtuels d'Azure.

   Si vous n'avez pas de configuration VMSS existante, effectuez les tâches suivantes :

   a) Créer un VMSS

   b) Activer Autoscale sur VMSS

   c) Créer une stratégie évolutive et évolutive dans le paramètre VMSS Autoscale

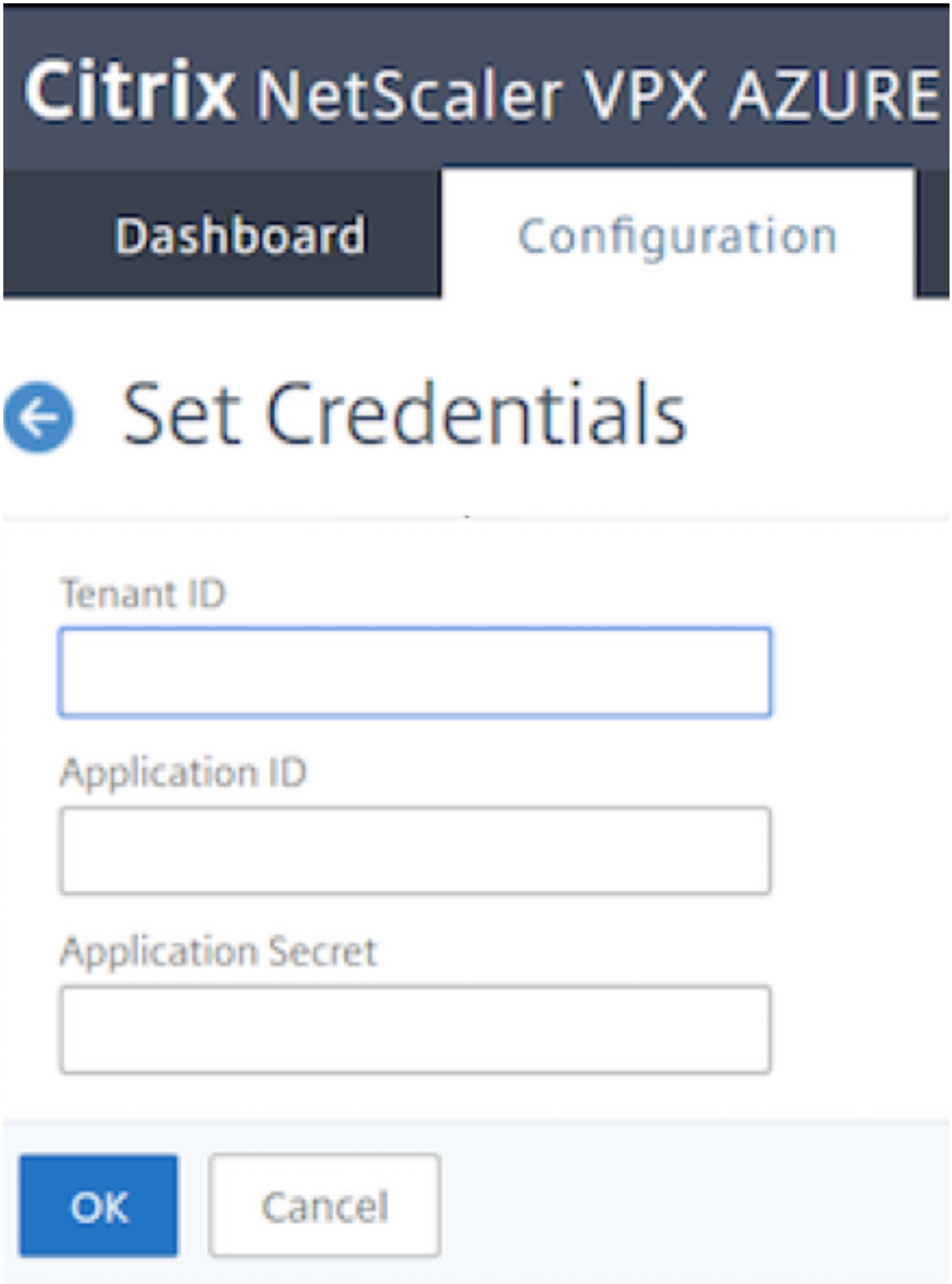
   Pour plus d'informations, voir Vue d'ensemble des jeux d'échelle de machines virtuelles Azure Autoscale with Azure.

5. Créez une application Azure Active Directory (ADD) et un principal de service pouvant accéder aux ressources. Attribuez un rôle de contributeur à l'application AAD nouvellement créée. Pour plus d'informations, voir Utiliser le portail pour créer une application Azure Active Directory et un principal de service pouvant accéder aux ressources.

Ajouter VMSS à une instance NetScaler VPX

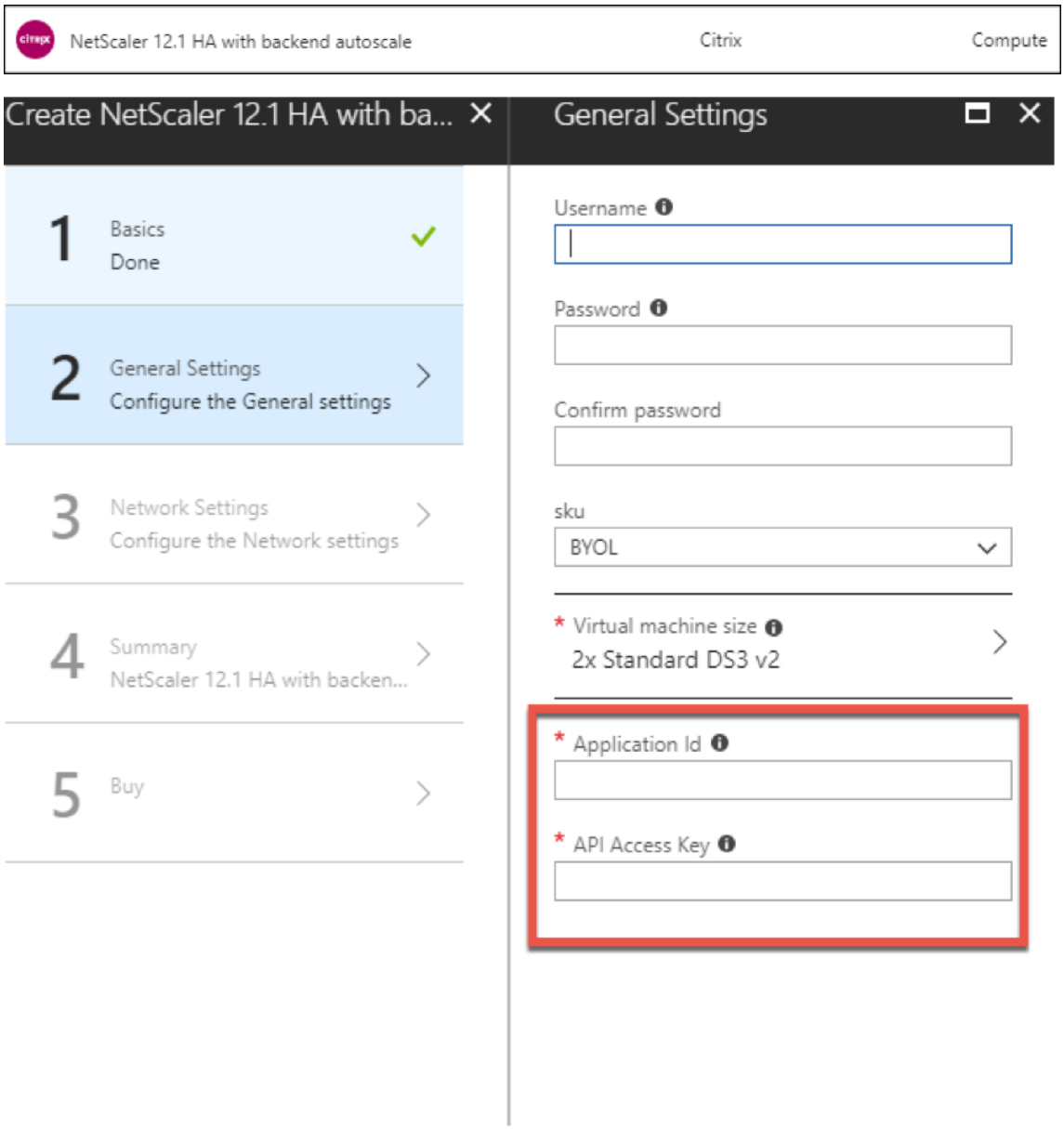
Vous pouvez ajouter le paramètre Autoscale à une instance VPX en un seul clic à l'aide de l'interface graphique. Procédez comme suit pour ajouter le paramètre Autoscale à l'instance VPX :

1. Ouvrez une session sur l'instance VPX.
2. Lorsque vous vous connectez à l'instance NetScaler VPX pour la première fois, la page Définir les informations d'identification s'affiche. Ajoutez les informations d'identification Azure requises pour que la fonctionnalité Autoscale fonctionne.



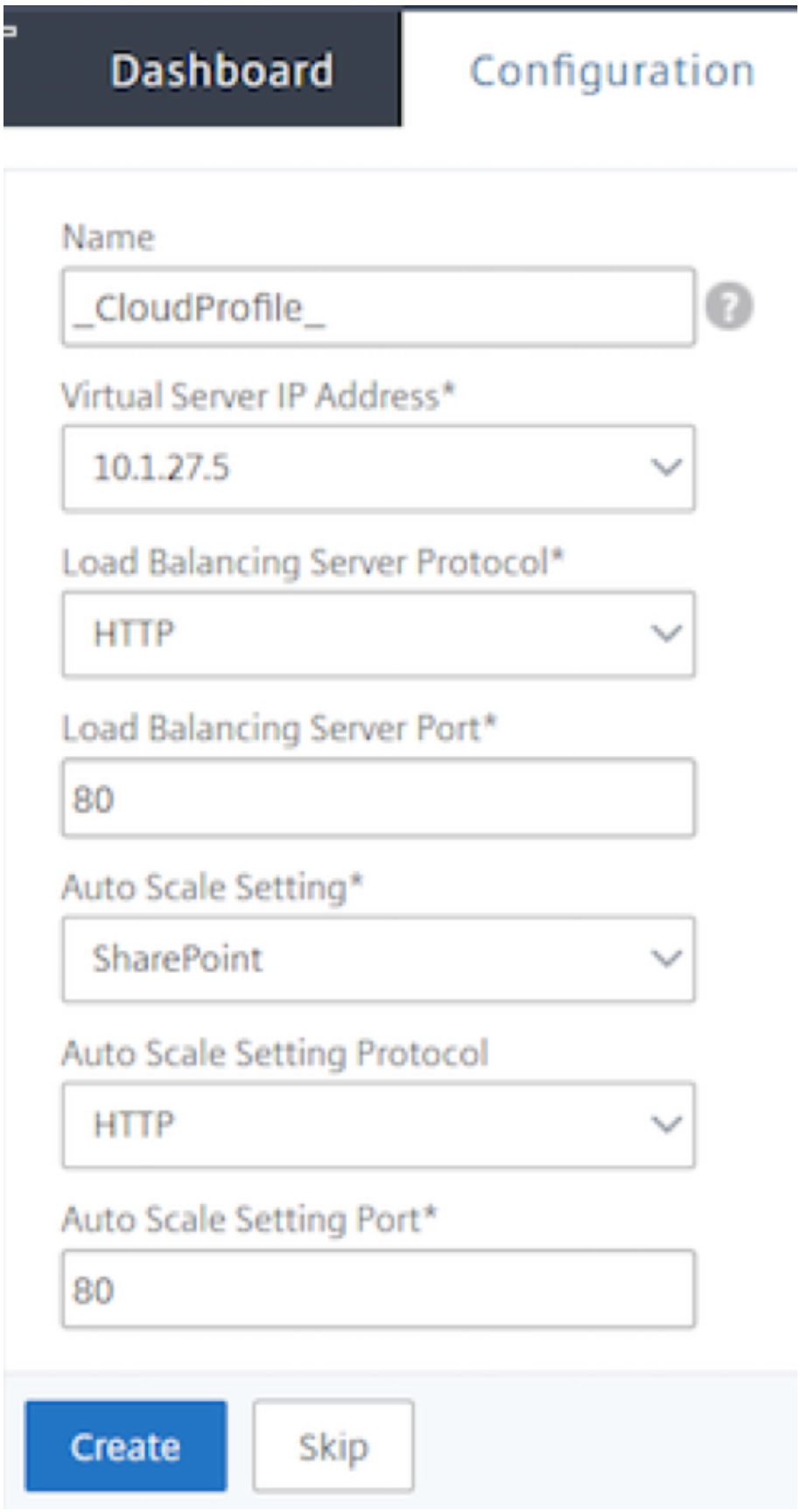
La page Définir les informations d'identification s'affiche uniquement lorsque l'ID d'application et la clé d'accès API ne sont pas définis ou que l'ID d'application et les clés d'accès API corrects (identiques au secret de l'application) ne sont pas définis dans le portail Azure.

Lorsque vous déployez l'offre « NetScaler 12.1 HA avec Autoscale principal » depuis Azure Marketplace, le portail Azure demande les informations d'identification principale du service Azure (ID d'application et clé d'accès API).



Pour plus d'informations sur la création d'un ID d'application, reportez-vous à la section Ajout d'une application et pour créer une clé d'accès ou un secret d'application, voir Configurer une application cliente pour accéder aux API Web.

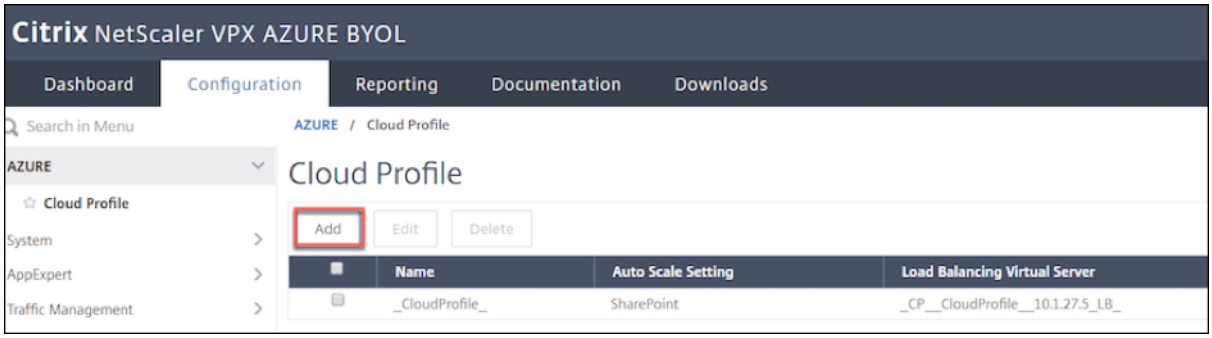
3. Dans la page de profil de cloud par défaut, entrez les détails, comme illustré dans l'exemple suivant, puis cliquez sur Créer.



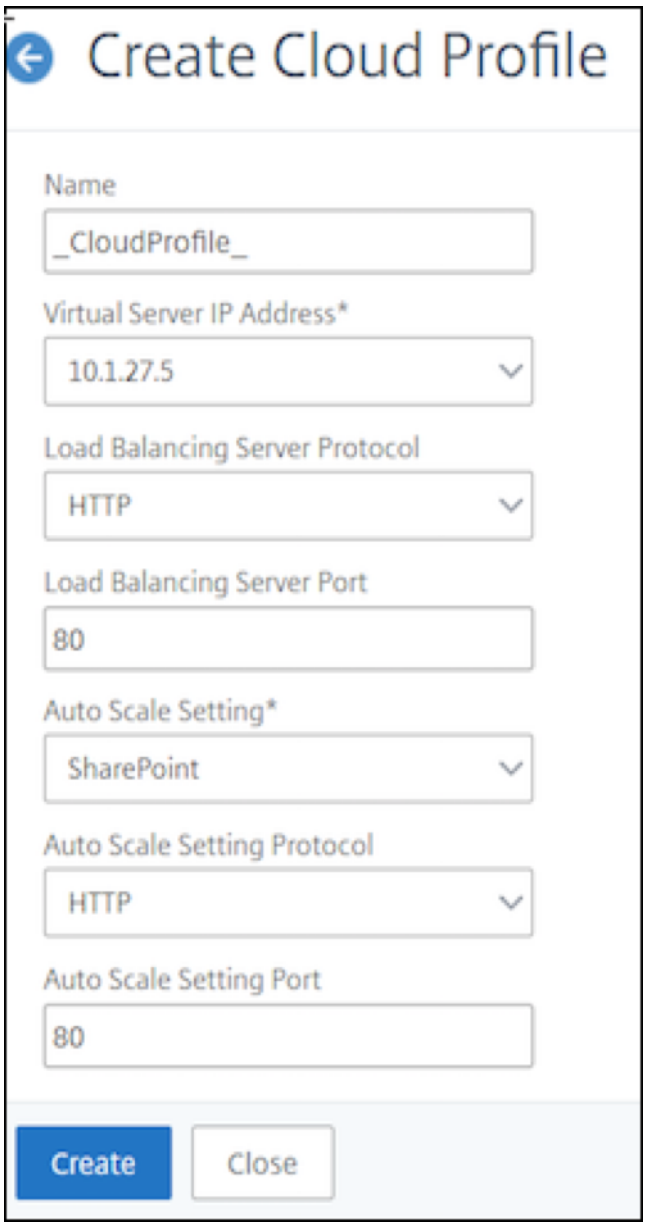
Points à garder à l'esprit lors de la création d'un profil cloud

- L'adresse IP du serveur virtuel est renseignée automatiquement à partir de l'adresse IP libre disponible pour l'instance VPX. Pour plus d'informations, voir Attribuer plusieurs adresses IP à des machines virtuelles à l'aide du portail Azure.
- Le paramètre Autoscale est prérempli à partir de l'instance VMSS connectée à l'instance NetScaler VPX sur le même réseau virtuel ou sur des réseaux virtuels homologues. Pour plus d'informations, voir Vue d'ensemble des jeux d'échelle de machines virtuelles Azure Autoscale with Azure.
- Lors de la sélection du protocole et du port du groupe Auto Scaling, assurez-vous que vos serveurs écoutent les protocoles et les ports et que vous liez le moniteur approprié dans le groupe de services. Par défaut, le moniteur TCP est utilisé.
- Pour le type de protocole SSL Autos Scaling, après avoir créé le profil Cloud, le serveur virtuel d'équilibrage de charge ou le groupe de services est hors service en raison d'un certificat manquant. Vous pouvez lier manuellement le certificat au serveur virtuel ou au groupe de services.

Après la première connexion, si vous souhaitez créer un profil cloud, accédez à **Système > Azure > Profil cloud dans** l'interface utilisateur graphique et cliquez sur **Ajouter**.



La page de configuration de Create Cloud Profile s'affiche.



Cloud Profile crée un serveur virtuel d'équilibrage de charge NetScaler et un groupe de services dont les membres (serveurs) sont les serveurs du groupe Auto Scaling. Vos serveurs back-end doivent être accessibles via le SNIP configuré sur l'instance VPX.

> **Remarque :**
>
> À partir de la version 13.1-42.x de NetScaler, vous pouvez créer différents profils cloud pour différents services (en utilisant différents ports) avec le même VMSS dans Azure. Ainsi, l'instance NetScaler VPX prend en charge plusieurs services avec le même groupe Autoscaling dans le cloud public.

Pour afficher les informations relatives à la mise à l'échelle automatique dans le portail Azure, accédez à **Tous les services > Ensemble d'échelles de machines virtuelles > Sélectionner un ensemble**

d'échelles de machines virtuelles > Mise à l'échelle.

Balises Azure pour le déploiement de NetScaler VPX

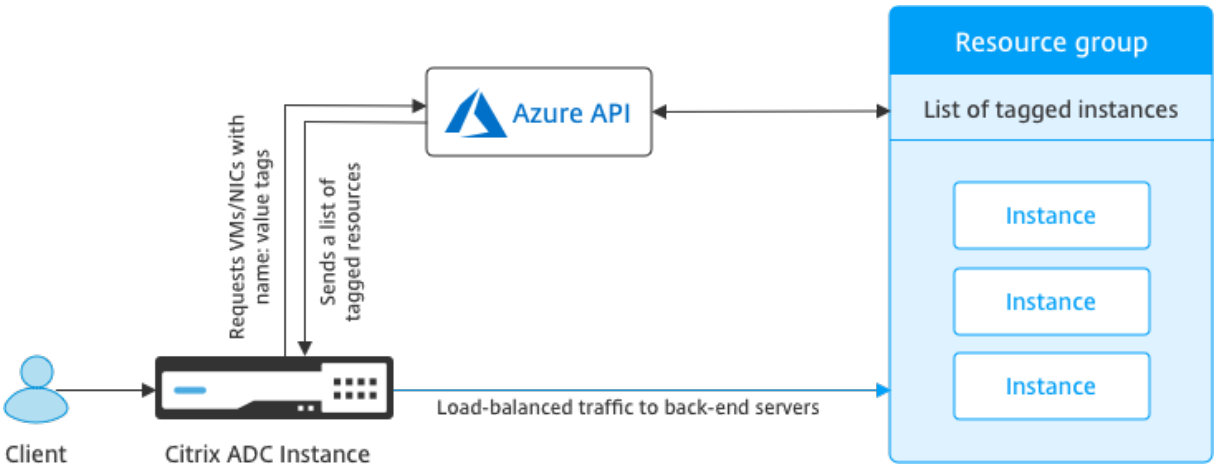
May 5, 2023

Dans le portail cloud Azure, vous pouvez baliser les ressources avec un nom : paire de valeurs (comme Dept : Finance) pour catégoriser et afficher les ressources entre les groupes de ressources et, au sein du portail, sur tous les abonnements. Le balisage est utile lorsque vous avez besoin d'organiser des ressources pour la facturation, la gestion ou l'automatisation.

Comment fonctionne la balise Azure pour le déploiement VPX

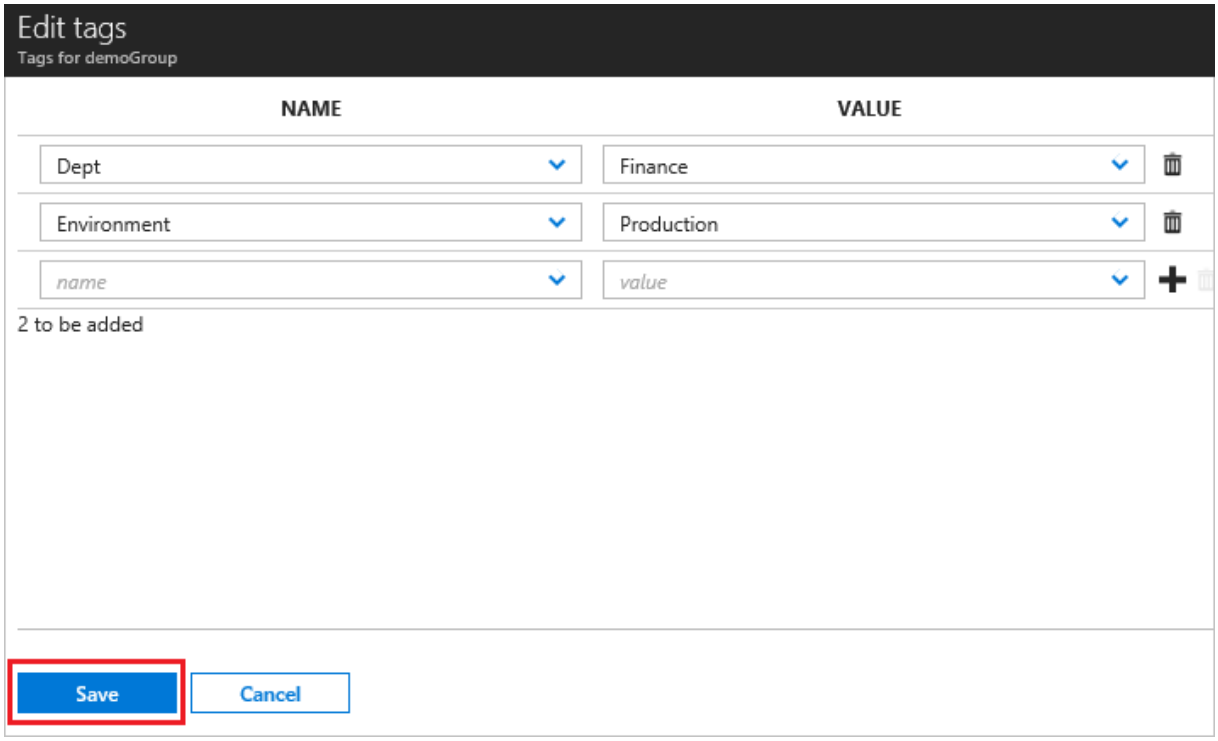
Pour les instances autonomes et à haute disponibilité NetScaler VPX déployées sur Azure Cloud, vous pouvez désormais créer des groupes de services d'équilibrage de charge associés à une balise Azure. L'instance VPX surveille constamment les machines virtuelles Azure (serveurs back-end) et les interfaces réseau (NIC), ou les deux, avec la balise respective et met à jour le groupe de services en conséquence.

L'instance VPX crée le groupe de services qui équilibre la charge des serveurs back-end à l'aide de balises. L'instance interroge l'API Azure pour toutes les ressources qui sont balisées avec un nom de balise et une valeur de balise particuliers. En fonction de la période d'interrogation attribuée (60 secondes par défaut), l'instance VPX interroge régulièrement l'API Azure et récupère les ressources disponibles avec le nom et les valeurs de balise attribués dans l'interface graphique VPX. Chaque fois qu'une machine virtuelle ou une carte réseau avec le tag approprié est ajoutée ou supprimée, l'ADC détecte la modification correspondante et ajoute ou supprime automatiquement l'adresse IP de la machine virtuelle ou de la carte réseau du groupe de services.



Avant de commencer

Avant de créer des groupes de services d'équilibrage de charge NetScaler, ajoutez une balise aux serveurs dans Azure. Vous pouvez affecter la balise à la machine virtuelle ou à la carte réseau.



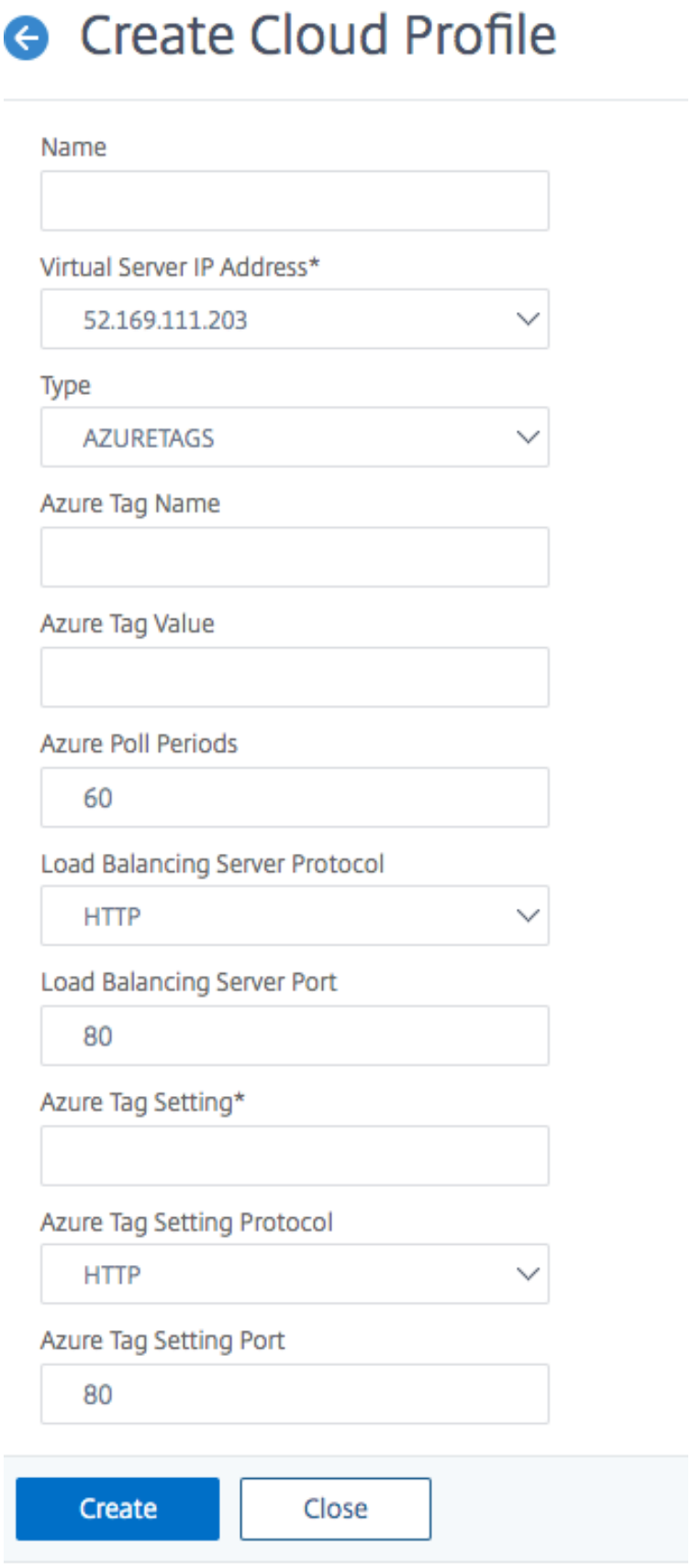
Pour plus d'informations sur l'ajout de balises Azure, consultez le document Microsoft Utiliser des balises pour organiser vos ressources Azure.

> Remarque Les commandes de l'interface de ligne de commande
> ADC pour ajouter des paramètres de balise Azure prennent en charge les noms de balise et les valeurs de balise qui commencent uniquement par des chiffres ou des alphabets et non par d'autres caractères du clavier.

Comment ajouter des paramètres de balise Azure à l'aide de l'interface graphique VPX

Vous pouvez ajouter le profil de cloud de balises Azure à une instance VPX à l'aide de l'interface graphique VPX afin que l'instance puisse équilibrer la charge des serveurs principaux à l'aide de la balise spécifiée. Procédez comme suit :

1. À partir de l'interface graphique VPX, accédez à **Configuration > Azure > Cloud Profile**.
2. Cliquez sur Ajouter pour créer un profil cloud. La fenêtre du profil cloud s'ouvre.



1. Entrez des valeurs pour les champs suivants :
   - Nom : Ajoutez un nom à votre profil
   - Adresse IP du serveur virtuel : l'adresse IP du serveur virtuel est renseignée automatiquement à partir de l'adresse IP libre disponible pour l'instance VPX. Pour plus d'informations, voir Attribuer plusieurs adresses IP à des machines virtuelles à l'aide du portail Azure.
   - Type : Dans le menu, sélectionnez AZURETAGS.
   - Nom de balise Azure : entrez le nom que vous avez attribué aux machines virtuelles ou aux cartes réseau dans le portail Azure.
   - Valeur de balise Azure : entrez la valeur que vous avez attribuée aux machines virtuelles ou aux cartes réseau dans le portail Azure.
   - Périodes de sondage Azure : par défaut, la période de sondage est de 60 secondes, ce qui est la valeur minimale. Vous pouvez le modifier selon vos besoins.
   - Protocole du serveur d'équilibrage de charge : sélectionnez le protocole que votre équilibreur de charge écoute.
   - Port du serveur d'équilibrage de charge : sélectionnez le port sur lequel votre équilibreur de charge écoute.
   - Paramètre de balise Azure : nom du groupe de services qui sera créé pour ce profil cloud.
   - Protocole de réglage des balises Azure : sélectionnez le protocole que vos serveurs principaux écoutent.
   - Port de réglage des balises Azure : sélectionnez le port sur lequel vos serveurs principaux écoutent.
2. Cliquez sur **Create**.

Un serveur virtuel d'équilibrage de charge et un groupe de services sont créés pour les machines virtuelles ou les cartes réseau balisées. Pour voir le serveur virtuel d'équilibrage de charge, à partir de l'interface graphique VPX, accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

Comment ajouter des paramètres de balise Azure à l'aide de l'interface de ligne de commande VPX

Tapez la commande suivante sur l'interface de ligne de commande NetScaler pour créer un profil cloud pour les balises Azure.

```
1 add cloud profile `<profile name>` -type azuretags -vServerName `<
    vserver name>` -serviceType HTTP -IPAddress `<vserver IP address>` -
    port 80 -serviceGroupName `<service group name>` -
    boundServiceGroupSvcType HTTP -vsvrbindsvcport 80 -azureTagName `<
    Azure tag specified on Azure portal>` -azureTagValue `<Azure value
    specified on the Azure portal>` -azurePollPeriod 60
2
3 <!--NeedCopy-->
```


> Important
> Vous devez enregistrer toutes les configurations ; sinon, elles seront perdues après le redémarrage de l'instance. Tapez `save config`.

Exemple 1 : Voici un exemple de commande pour un profil cloud pour le trafic HTTP de toutes les machines virtuelles/cartes réseau Azure étiquetées avec la paire « MyTagName/MyTagValue » :

```
add cloud profile MyTagCloudProfile -type azuretags -vServerName
    MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 -
    serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP -
    vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue myTagValue
     -azurePollPeriod 60
Done
<!--NeedCopy-->
```

Pour afficher le profil de cloud, tapez `show cloudprofile`.

Exemple 2 : la commande CLI suivante imprime des informations sur le profil de nuage nouvellement ajouté dans l'exemple 1.

```
show cloudprofile
1)    Name:  MyTagCloudProfile Type:  azuretags         VServerName:
    MyTagVServer ServiceType:  HTTP       IPAddress:  52.178.209.133
    Port:  80               ServiceGroupName:  MyTagsServiceGroup
    BoundServiceGroupSvcType:  HTTP
       Vsvrbindsvcport:  80     AzureTagName:  myTagName AzureTagValue:
           myTagValue AzurePollPeriod:  60     GraceFul:  NO
          Delay:  60
<!--NeedCopy-->
```

Pour supprimer un profil cloud, tapez profil cloud rm <`cloud profile name`>

Exemple 3 : La commande suivante supprime le profil de nuage créé dans l'exemple 1.

```
> rm cloudprofile MyTagCloudProfile
  Done
<!--NeedCopy-->
```

Dépannage

Problème : Dans de très rares cas, la commande CLI « profil cloud rm » peut ne pas supprimer le groupe de services et les serveurs associés au profil cloud supprimé. Cela se produit lorsque la commande est émise secondes avant l'expiration de la période d'interrogation du profil de nuage en cours de suppression.

Solution : supprimez manuellement les groupes de services restants en saisissant la commande CLI suivante pour chacun des groupes de services restants :

```
#> rm servicegroup <serviceGroupName>

<!--NeedCopy-->
```

Supprimez également chacun des serveurs restants en entrant la commande CLI suivante pour chacun des serveurs restants :

```
#> rm server <name>
<!--NeedCopy-->
```

Problème : Si vous ajoutez un paramètre de balise Azure à une instance VPX à l'aide de l'interface de ligne de commande, le processus rain_tags continue de s'exécuter sur un nœud de paire HA après un redémarrage chaud.

Solution : Terminer manuellement le processus sur le nœud secondaire après un redémarrage à chaud. À partir de l'interface de ligne de commande du nœud HA secondaire, sortez de l'invite de commandes :

```
#> shell

<!--NeedCopy-->
```

Utilisez la commande suivante pour tuer le processus rain_tags :

```
# PID=`ps -aux | grep rain_tags | awk '{
 print $2 }
 '`; kill -9 $PID

<!--NeedCopy-->
```

Problème : les serveurs back-end peuvent ne pas être accessibles et signalés comme DOWN par l'instance VPX, bien qu'ils soient en bonne santé.
Solution : Assurez-vous que l'instance VPX peut atteindre l'adresse IP balisée correspondant au serveur principal. Pour une carte réseau balisée, il s'agit de l'adresse IP de la carte réseau ; alors que pour une machine virtuelle balisée, il s'agit de l'adresse IP principale de la machine virtuelle. Si la VM/NIC réside sur un autre réseau virtuel Azure, assurez-vous que l'appairage de VNet est activé.

Configurer GSLB sur des instances NetScaler VPX

May 5, 2023

Les appliances NetScaler configurées pour l'équilibrage global de la charge des serveurs (GSLB) assurent la reprise après sinistre et la disponibilité continue des applications en les protégeant contre les points de défaillance d'un réseau étendu. GSLB peut équilibrer la charge entre les centres de données en dirigeant les demandes des clients vers le centre de données le plus proche ou le plus performant, ou vers les centres de données survivants en cas de panne.

Cette section décrit comment activer GSLB sur des instances VPX sur deux sites dans un environnement Microsoft Azure, à l'aide des commandes Windows PowerShell.

> **Remarque**
>
> Pour plus d'informations sur GSLB, consultez Global Server Load Balancing.

Vous pouvez configurer GSLB sur une instance NetScaler VPX sur Azure, en deux étapes :

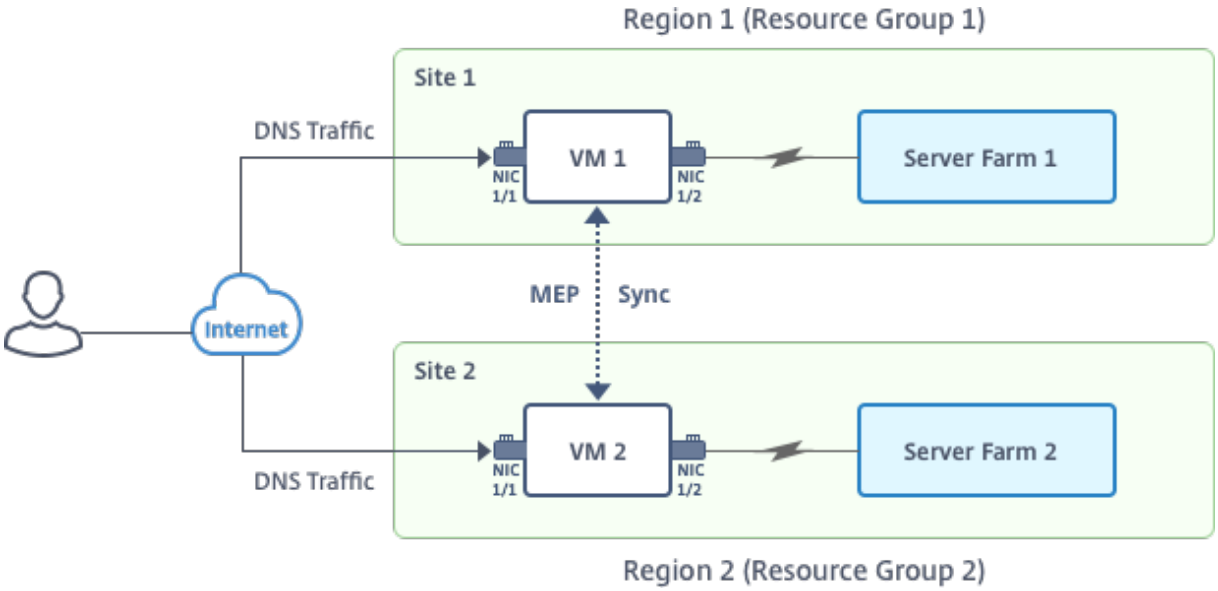
1. Créez une instance VPX avec plusieurs cartes réseau et plusieurs adresses IP, sur chaque site.
2. Activez GSLB sur les instances VPX.

> **Remarque**
>
> Pour plus d'informations sur la configuration de plusieurs cartes réseau et adresses IP, voir : Configurer plusieurs adresses IP pour une instance NetScaler VPX en mode autonome àl'aide des commandes PowerShell

Scénario

Ce scénario inclut deux sites : le site 1 et le site 2. Chaque site possède une machine virtuelle (VM1 et VM2) configurée avec plusieurs cartes réseau, plusieurs adresses IP et GSLB.

Chiffre. Mise en place de la GSLB sur deux sites - le site 1 et le site 2.



Dans ce scénario, chaque machine virtuelle dispose de trois cartes réseau - NIC 0/1, 1/1 et 1/2. Chaque carte réseau peut avoir plusieurs adresses IP privées et publiques. Les cartes réseau sont configurées aux fins suivantes.

- Carte réseau 0/1 : pour le trafic de gestion
- Carte réseau 1/1 : pour servir le trafic côté client
- NIC 1/2 : pour communiquer avec les serveurs back-end

Pour plus d'informations sur les adresses IP configurées sur chaque carte réseau dans ce scénario, reportez-vous à la section Détails de la configuration IP .

Paramètres

Voici des exemples de paramètres de paramètres pour ce scénario dans ce document. Vous pouvez utiliser différents paramètres si vous le souhaitez.

```
$location="West Central US"

$vnetName="NSVPX-vnet"

$RGName="multiIP-RG"

$prmStorageAccountName="multiipstorageaccnt"

$avSetName="MultiIP-avset"

$vmSize="Standard_DS3_V2"

<!--NeedCopy-->
```

Remarque : La configuration minimale requise pour une instance VPX est de 2 processeurs virtuels et de 2 Go de RAM.

```
$publisher="citrix"

$offer="netscalervpx111"

$sku="netscalerbyol"

$version="latest"

$vmNamePrefix="MultiIPVPX"

$nicNamePrefix="MultiipVPX"

```



```
$osDiskSuffix="osdiskdb"

$numberOfVMs=1

$ipAddressPrefix="10.0.0."

$ipAddressPrefix1="10.0.1."

$ipAddressPrefix2="10.0.2."

$pubIPName1="MultiIP-pip1"

$pubIPName2="MultiIP-pip2"

$IpConfigName1="IPConfig1"

$IPConfigName2="IPConfig-2"

$IPConfigName3="IPConfig-3"

$IPConfigName4="IPConfig-4"

$frontendSubnetName="default"

$backendSubnetName1="subnet_1"

$backendSubnetName2="subnet_2"

$suffixNumber=10
<!--NeedCopy-->
```

Créer une machine virtuelle

Suivez les étapes 1 à 10 pour créer VM1 avec plusieurs cartes réseau et plusieurs adresses IP, à l'aide des commandes PowerShell :

1. Créer un groupe de ressources
2. Créer un compte de stockage
3. Créer un ensemble de disponibilités
4. Création d'un réseau virtuel
5. Créer une adresse IP publique
6. Créer des cartes réseau

7. Créer un objet de configuration de machine virtuelle
8. Obtenir des informations d'identification et définir les propriétés du système d'exploitation pour la machine virtuelle
9. Ajouter des cartes réseau
10. Spécifier le disque du système d'exploitation et créer une machine virtuelle

Après avoir effectué toutes les étapes et commandes nécessaires à la création de VM1, répétez ces étapes pour créer une VM2 avec les paramètres qui lui sont spécifiques.

Créer un groupe de ressources

```
New-AzureRMResourceGroup -Name $RGName -Location $location
<!--NeedCopy-->
```

Créer un compte de stockage

```
$prmStorageAccount=New-AzureRMStorageAccount -Name
    $prmStorageAccountName -ResourceGroupName $RGName -Type Standard_LRS
     -Location $location
<!--NeedCopy-->
```

Créer un ensemble de disponibilités

```
$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
    $RGName -Location $location
<!--NeedCopy-->
```

Création d'un réseau virtuel

1. Ajoutez des sous-réseaux.

```
$subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontendSubnetName -AddressPrefix "10.0.0.0/24"
$subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName1 -AddressPrefix "10.0.1.0/24"
$subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName2 -AddressPrefix "10.0.2.0/24"
<!--NeedCopy-->
```


2. Ajoutez un objet réseau virtuel.

```
$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
    $RGName -Location $location -AddressPrefix 10.0.0.0/16 -Subnet
    $subnet1, $subnet2, $subnet3
<!--NeedCopy-->
```

3. Récupérez des sous-réseaux.

```
$frontendSubnet=$vnet.Subnets|?{
 $\_.Name -eq $frontendSubnetName }

$backendSubnet1=$vnet.Subnets|?{
 $\_.Name -eq $backendSubnetName1 }

$backendSubnet2=$vnet.Subnets|?{
 $_.Name -eq $backendSubnetName2 }

<!--NeedCopy-->
```

Créer une adresse IP publique

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
<!--NeedCopy-->
```

Créer des cartes réseau

Créer une carte réseau 0/1

```
$nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"
$ipAddress1=$ipAddressPrefix + $suffixNumber
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    SubnetId $frontendSubnet.Id -PublicIpAddress $pip1 -PrivateIpAddress
     $ipAddress1 -Primary
$nic1=New-AzureRMNetworkInterface -Name $nic1Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig1
<!--NeedCopy-->
```

Créer une carte réseau 1/1


```
$nic2Name $nicNamePrefix + $suffixNumber + "-frontend"
$ipAddress2=$ipAddressPrefix1 + ($suffixNumber)
$ipAddress3=$ipAddressPrefix1 + ($suffixNumber + 1)
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    PublicIpAddress $pip2 -SubnetId $backendSubnet1.Id  -
    PrivateIpAddress $ipAddress2  -Primary
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    SubnetId $backendSubnet1.Id  -PrivateIpAddress $ipAddress3
nic2=New-AzureRMNetworkInterface -Name $nic2Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig2, $IpConfig3
<!--NeedCopy-->
```

Créer une carte réseau 1/2

```
$nic3Name=$nicNamePrefix + $suffixNumber + "-backend"
$ipAddress4=$ipAddressPrefix2 + ($suffixNumber)
$IPConfig4=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    SubnetId $backendSubnet2.Id -PrivateIpAddress $ipAddress4 -Primary
$nic3=New-AzureRMNetworkInterface -Name $nic3Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig4
<!--NeedCopy-->
```

Créer un objet de configuration de machine virtuelle

```
$vmName=$vmNamePrefix
$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avSet.Id
<!--NeedCopy-->
```

Obtenir des informations d'identification et définir les propriétés du système d'exploitation

```
$cred=Get-Credential -Message "Type the name and password for VPX login
    ."
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
<!--NeedCopy-->
```

Ajouter des cartes réseau


```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
    Primary
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id
<!--NeedCopy-->
```

Spécifier le disque du système d'exploitation et créer une machine virtuelle

```
$osDiskName=$vmName + "-" + $osDiskSuffix
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/"
     +$osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
    $osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
    Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location
    $location
<!--NeedCopy-->
```

> **Remarque**
>
> Répétez les étapes 1 à 10 répertoriées dans « Créer des machines virtuelles multi-cartes réseau à l'aide des commandes PowerShell » pour créer VM2 avec des paramètres spécifiques à VM2.

Détails de la configuration IP

Les adresses IP suivantes sont utilisées.

Tableau 1 Adresses IP utilisées dans VM1

Carte d'interface réseau	IP privée	Adresse IP publique (PIP)	Description
0/1	10.0.0.10	PIP1	Configuré en tant que NSIP (IP de gestion)
1/1	10.0.1.10	PIP2	Configuré en tant qu'adresse IP du site SNIP/GSLB

Carte d'interface réseau	IP privée	Adresse IP publique (PIP)	Description
-	10.0.1.11	-	Configuré en tant qu'adresse IP du serveur LB. L'adresse IP publique n'est pas obligatoire
1/2	10.0.2.10	-	Configuration en tant que SNIP pour l'envoi de sondes de moniteur aux services ; une IP publique n'est pas obligatoire

Tableau 2 Adresses IP utilisées dans VM2

Carte d'interface réseau	IP interne	Adresse IP publique (PIP)	Description
0/1	20.0.0.10	PIP4	Configuré en tant que NSIP (IP de gestion)
1/1	20.0.1.10	PIP5	Configuré en tant qu'adresse IP du site SNIP/GSLB
-	20.0.1.11	-	Configuré en tant qu'adresse IP du serveur LB. L'adresse IP publique n'est pas obligatoire
1/2	20.0.2.10	-	Configuration en tant que SNIP pour l'envoi de sondes de moniteur aux services ; une IP publique n'est pas obligatoire

Voici des exemples de configurations pour ce scénario, montrant les adresses IP et les configurations LB initiales créées via l'interface de ligne de commande NetScaler VPX pour VM1 et VM2.

Voici un exemple de configuration sur VM1.

```
add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED
Add nsip 10.0.2.10 255.255.255.0
add service svc1 10.0.1.10 ADNS 53
add lb vserver v1 HTTP 10.0.1.11 80
add service s1 10.0.2.120 http 80
Add service s2 10.0.2.121 http 80
Bind lb vs v1 s[1-2]
<!--NeedCopy-->
```

Voici un exemple de configuration sur VM2.

```
add ns ip 20.0.1.10 255.255.255.0  -mgmtAccess ENABLED
Add nsip 20.0.2.10 255.255.255.0
add service svc1 20.0.1.10 ADNS 53
add lb vserver v1 HTTP 20.0.1.11 80
Add service s1 20.0.2.90 http 80
Add service s2 20.0.2.91 http 80
Bind lb vs v1 s[1-2]
<!--NeedCopy-->
```

Configurer les sites GSLB et d'autres paramètres

Effectuez les tâches décrites dans la rubrique suivante pour configurer les deux sites GSLB et les autres paramètres nécessaires :

Équilibrage de charge de serveur global

Pour plus d'informations, consultez cet article de support :https://support.citrix.com/article/CTX110348

Voici un exemple de configuration GSLB sur VM1 et VM2.

```
enable ns feature LB GSLB
add gslb site site1 10.0.1.10 -publicIP PIP2
add gslb site site2 20.0.1.10 -publicIP PIP5
add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP PIP3
    -publicPort 80 -siteName site1
add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP PIP6
    -publicPort 80 -siteName site2
add gslb vserver gslb_http_vip1 HTTP
bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
<!--NeedCopy-->
```


Vous avez configuré GSLB sur des instances NetScaler VPX exécutées sur Azure.

Récupération d'urgence

La catastrophe est une perturbation soudaine des fonctions commerciales causée par des catastrophes naturelles ou des événements d'origine humaine. Les catastrophes affectent les opérations des centres de données, après quoi les ressources et les données perdues sur le site du sinistre doivent être entièrement reconstruites et restaurées. La perte de données ou les temps d'arrêt dans le datacenter sont critiques et réduit la continuité de l'activité.

L'un des défis auxquels les clients sont confrontés aujourd'hui est de décider où placer leur site de reprise après sinistre. Les entreprises recherchent la cohérence et les performances indépendamment des défaillances de l'infrastructure sous-jacente ou du réseau.

Les raisons possibles pour lesquelles de nombreuses entreprises décident de migrer vers le cloud sont les suivantes :

- Disposer d'un centre de données sur site coûte très cher. En utilisant le cloud, les entreprises peuvent libérer du temps et des ressources pour étendre leurs propres systèmes.
- La plupart des orchestrations automatisées permettent une restauration plus rapide
- Répliquez les données en fournissant une protection continue des données ou des instantanés continus pour vous prémunir contre toute panne ou attaque.
- Prenez en charge les cas d'utilisation dans lesquels les clients ont besoin de différents types de contrôles de conformité et de sécurité déjà présents sur les clouds publics. Ils leur permettent d'atteindre plus facilement la conformité dont ils ont besoin plutôt que de créer leur propre solution.

Un NetScaler configuré pour GSLB transfère le trafic vers le centre de données le moins chargé ou le plus performant. Cette configuration, appelée configuration active-active, améliore non seulement les performances, mais assure également une reprise après sinistre immédiate en acheminant le trafic vers d'autres centres de données si un centre de données faisant partie de la configuration est en panne. NetScaler permet ainsi aux clients d'économiser du temps et de l'argent.

Déploiement de plusieurs cartes réseau et de plusieurs adresses IP (trois cartes réseau) pour la reprise après sinistre

Les clients peuvent déployer à l'aide d'un déploiement à trois cartes réseau s'ils effectuent un déploiement dans un environnement de production où la sécurité, la redondance, la disponibilité, la capacité et l'évolutivité sont essentielles. Avec cette méthode de déploiement, la complexité et la facilité de gestion ne sont pas des préoccupations critiques pour les utilisateurs.

Déploiement d'une seule carte réseau et de plusieurs adresses IP (une carte réseau) pour la reprise après sinistre

Les clients sont susceptibles de procéder à un déploiement à l'aide d'une seule carte réseau s'ils le déploient dans un environnement hors production pour les raisons suivantes :

- Ils configurent l'environnement à des fins de test, ou ils mettent en place un nouvel environnement avant le déploiement en production.
- Déploiement rapide et efficace directement dans le cloud.
- Tout en recherchant la simplicité d'une configuration de sous-réseau unique.

Configurer GSLB sur une configuration haute disponibilité active-veille

May 5, 2023

Vous pouvez configurer l'équilibrage de charge globale du serveur (GSLB) sur un déploiement HA actif-standby sur Azure en trois étapes :

1. Créez une paire HA VPX sur chaque site GSLB. Consultez Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau pour plus d'informations sur la création d'une paire HA.
2. Configurez l'équilibreur de charge Azure (ALB) avec l'adresse IP frontale et les règles pour autoriser le trafic GSLB et DNS.

   Cette étape implique les sous-étapes suivantes. Reportez-vous au scénario de cette section pour connaître les commandes PowerShell utilisées pour effectuer ces sous-étapes.

   a. Créez un site frontal `IPconfig` pour GSLB.

   b. Créez un pool d'adresses back-end avec l'adresse IP de la carte réseau 1/1 des nœuds en HA.

   c. Créez des règles d'équilibrage de charge pour les éléments suivants :

   ```
   TCP/3009 - gslb communication
   TCP/3008 - gslb communication
   UDP/53 - DNS communication
   ```

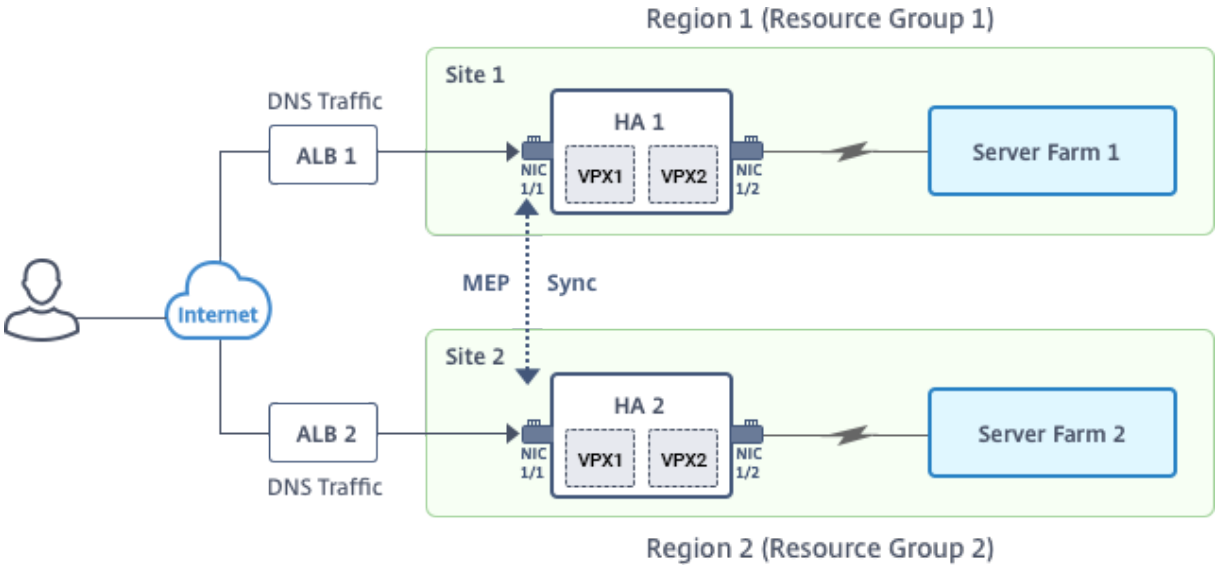
   d. Associer le pool d'adresses back-end aux règles LB créées à l'étape c.

   e. Mettez à jour le groupe de sécurité réseau de la carte réseau 1/1 des nœuds dans la paire HA pour autoriser le trafic pour les ports TCP 3008, TCP 3009 et UDP 53.
3. Activez GSLB sur chaque paire HA.

Scénario

Ce scénario inclut deux sites : le site 1 et le site 2. Chaque site possède une paire HA (HA1 et HA2) configurée avec plusieurs cartes réseau, plusieurs adresses IP et GSLB.

Figure : GLSB sur un déploiement HA active-Standy sur Azure



Dans ce scénario, chaque machine virtuelle dispose de trois cartes réseau - NIC 0/1, 1/1 et 1/2. Les cartes réseau sont configurées aux fins suivantes.

Carte réseau 0/1 : pour le trafic de gestion

Carte réseau 1/1 : pour servir le trafic côté client

NIC 1/2 : pour communiquer avec les serveurs back-end

Réglages des paramètres

Vous trouverez ci-dessous des exemples de paramètres pour l'ALB. Vous pouvez utiliser différents paramètres si vous le souhaitez.

```
$locName="South east Asia"

$rgName="MulitIP-MultiNIC-RG"

$pubIPName4="PIPFORGSLB1"

$domName4="vpxgslbdns"

$lbName="MultiIPALB"

$frontEndConfigName2="FrontEndIP2"
```



```
12
13 $backendPoolName1="BackendPoolHttp"
14
15 $lbRuleName2="LBRuleGSLB1"
16
17 $lbRuleName3="LBRuleGSLB2"
18
19 $lbRuleName4="LBRuleDNS"
20
21 $healthProbeName="HealthProbe"
```

Configurer ALB avec l'adresse IP frontale et les règles pour autoriser le trafic GSLB et DNS

Étape 1. **Créer une adresse IP publique pour l'adresse IP du site GSLB**

```
1 $pip4=New-AzureRmPublicIpAddress -Name $pubIPName4 -ResourceGroupName
    $rgName -DomainNameLabel $domName4 -Location $locName -
    AllocationMethod Dynamic
2
3
4 Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName | Add-
    AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName2 -
    PublicIpAddress $pip4 | Set-AzureRmLoadBalancer
```

Étape 2. **Créez des règles LB et mettez à jour l'ALB existant**.

```
1 $alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName
2
3
4 $frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
    LoadBalancer $alb -Name $frontEndConfigName2
5
6
7 $backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
    LoadBalancer $alb -Name $backendPoolName1
8
9
10 $healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
    Name $healthProbeName
11
12
13 $alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName2 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
```



```
    $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3009 -BackendPort
    3009 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
14
15
16  $alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName3 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3008 -BackendPort
    3008 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
17
18
19  $alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName4 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Udp" -FrontendPort 53 -BackendPort 53
    -Probe $healthprobe -EnableFloatingIP  | Set-AzureRmLoadBalancer
```

Activer GSLB sur chaque paire haute disponibilité

Vous avez maintenant deux adresses IP frontales pour chaque ALB : ALB 1 et ALB 2. Une adresse IP est destinée au serveur virtuel LB et l'autre à l'adresse IP du site GSLB.

HA 1 possède les adresses IP frontales suivantes :

- FrontEndIPofALB1 (pour serveur virtuel LB)
- PIPFORGSLB1 (IP GSLB)

HA 2 possède les adresses IP frontales suivantes :

- FrontEndIPofALB2 (pour serveur virtuel LB)
- PIPFORGSLB2 (IP GSLB)

Les commandes suivantes sont utilisées pour ce scénario.

```
1  enable ns feature LB GSLB
2
3  add service dnssvc PIPFORGSLB1 ADNS 53
4
5  add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1
6
7  add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2
8
9  add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -
   publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1
10
```



```
add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -
    publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2

add gslb vserver gslb_http_vip1 HTTP

bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Ressources connexes :

Configurer GSLB sur des instances NetScaler VPX

Équilibrage de charge de serveur global

Déployez NetScaler GSLB et le back-end des services basés sur des domaines avec un équilibreur de charge cloud

May 5, 2023

L'équilibrage de charge globale des serveurs (GSLB) est énorme pour bon nombre de nos clients. Ces entreprises disposent d'un centre de données sur site au service des clients régionaux, mais compte tenu de la demande croissante pour leur activité, elles souhaitent désormais étendre et déployer leur présence à l'échelle mondiale sur AWS et Azure tout en maintenant leur présence sur site pour les clients régionaux. Les clients souhaitent également réaliser tout cela avec des configurations automatisées. Ils sont donc à la recherche d'une solution capable de s'adapter rapidement à l'évolution des besoins de l'entreprise ou à l'évolution du marché mondial.

NetScaler étant du côté de l'administrateur réseau, les clients peuvent utiliser le GSLB StyleBook pour configurer des applications à la fois sur site et dans le cloud, et cette même configuration peut être transférée vers le cloud avec NetScaler ADM. Les utilisateurs peuvent accéder aux ressources sur site ou dans le cloud en fonction de la proximité avec GSLB. Cela permet une expérience fluide, peu importe où se trouvent les utilisateurs dans le monde.

Présentation de DBS

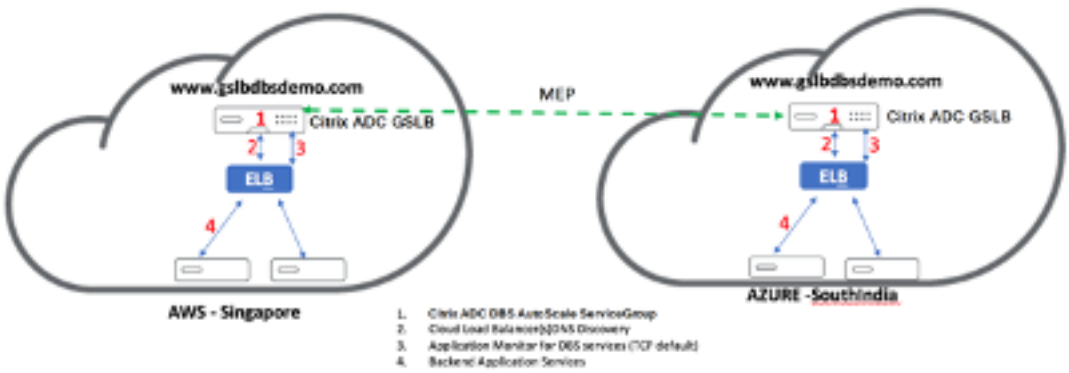
NetScaler GSLB prend en charge l'utilisation de services basés sur le domaine (DBS) pour les équilibreurs de charge dans le cloud. Cela permet la découverte automatique des services cloud dynamiques à l'aide d'une solution d'équilibreur de charge cloud. Cette configuration permet à

NetScaler d'implémenter GSLB DBS dans un environnement Active-Active. DBS permet de dimensionner les ressources dorsales dans les environnements Microsoft Azure à partir de la découverte DNS. Cette section traite de l'intégration entre NetScalers dans l'environnement Azure Autoscale.

Services basés sur des noms de domaine utilisant Azure Load Balancer (ALB)

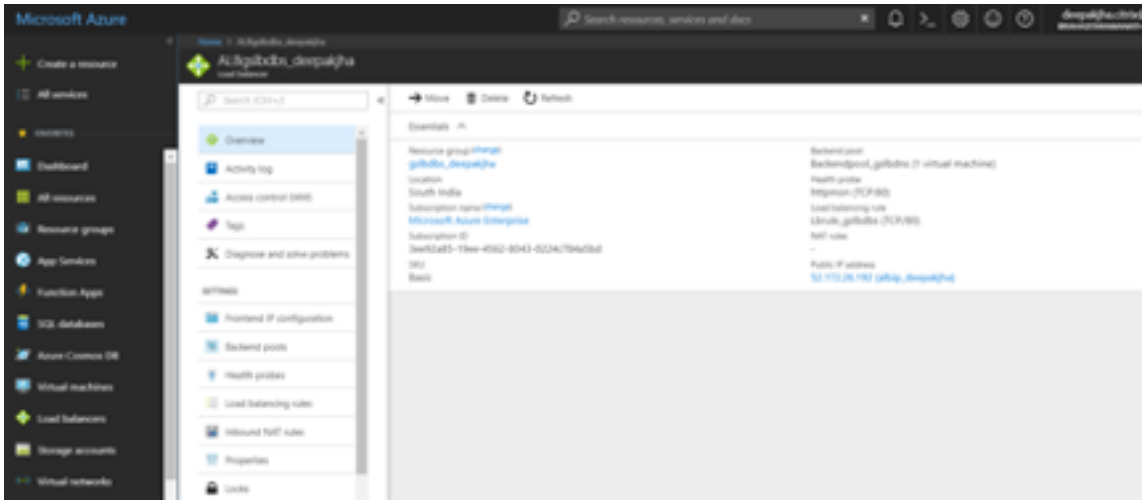
GLSB DBS utilise le nom de domaine complet de l'utilisateur ALB pour mettre à jour dynamiquement les groupes de services GSLB afin d'inclure les serveurs principaux créés et supprimés dans Azure. Pour configurer cette fonctionnalité, l'utilisateur pointe NetScaler vers son ALB pour un routage dynamique vers différents serveurs dans Azure. Ils peuvent le faire sans avoir à mettre à jour manuellement NetScaler chaque fois qu'une instance est créée et supprimée dans Azure. La fonctionnalité NetScaler DBS pour les groupes de services GSLB utilise la découverte de services compatible DNS pour déterminer les ressources des services membres de l'espace de noms DBS identifié dans le groupe autoscale.

L'image suivante décrit les composants de mise à l'échelle automatique NetScaler GSLB DBS avec des équilibreurs de charge cloud :

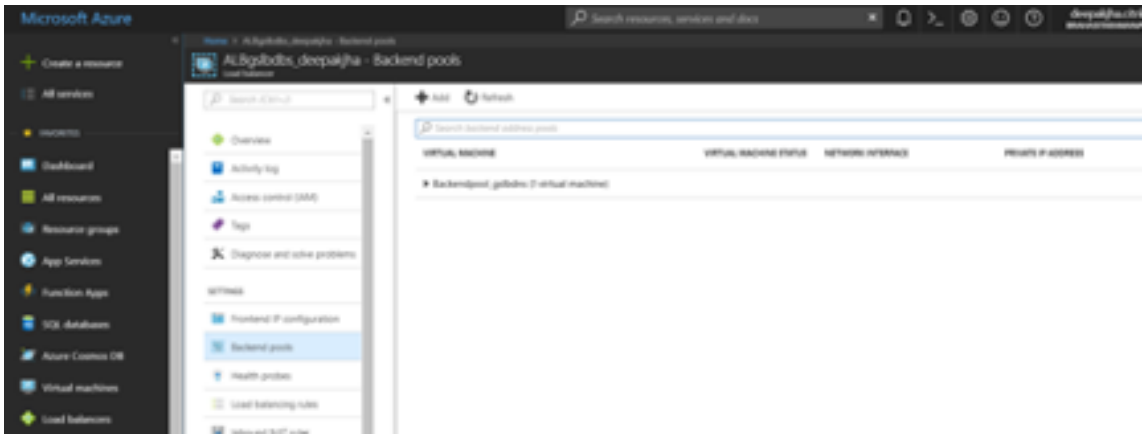


Configuration des composants Azure

1. Connectez-vous à l'utilisateur Azure Portal et créez une nouvelle machine virtuelle à partir d'un modèle NetScaler.
2. Créez un équilibreur de charge Azure.



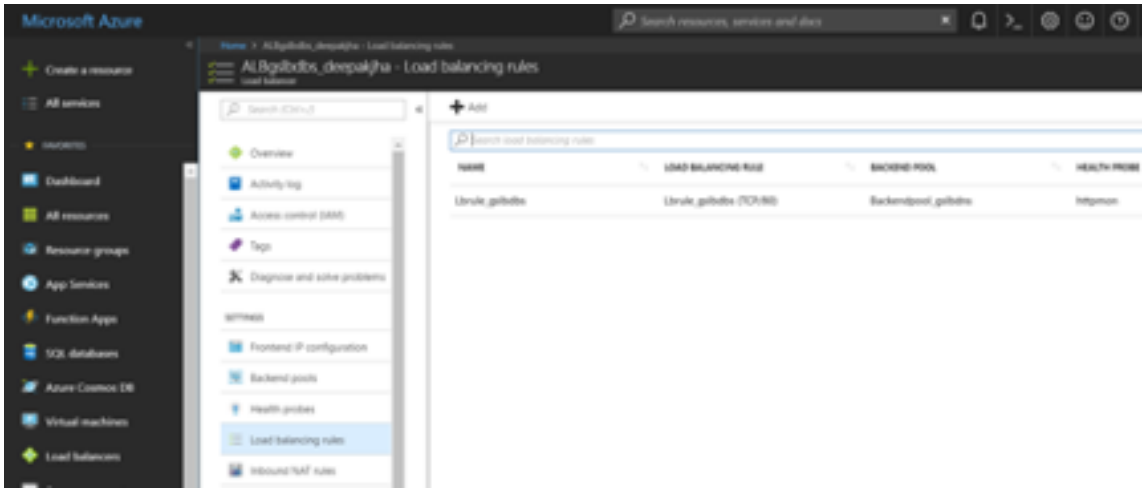
3. Ajoutez les pools principaux NetScaler créés.



4. Créez une analyse de santé pour le port 80.

   Créez une règle d'équilibrage de charge à l'aide de l'adresse IP frontale créée à partir de l'équilibreur de charge.

   - Protocole : TCP
   - Port principal : 80
   - Pool principal : NetScaler créé à l'étape 1
   - Analyse de santé : créée à l'étape 4
   - Persistance de la session : Aucun



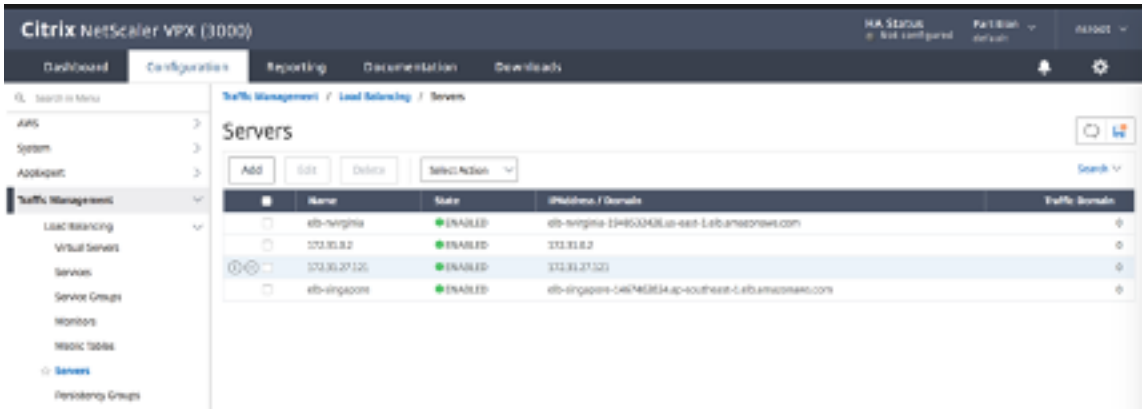
Configurer le service basé sur le domaine NetScaler GSLB

Les configurations suivantes résument ce qui est nécessaire pour activer les services basés sur le domaine pour la mise à l'échelle automatique des ADC dans un environnement compatible GSLB.

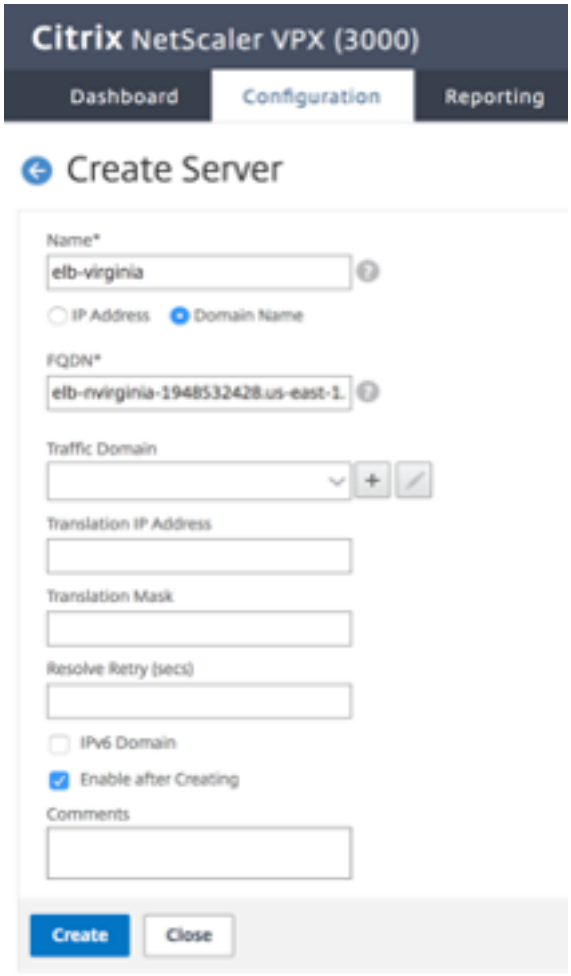
Configurations de gestion du trafic

> **Remarque :**
>
> Il est nécessaire de configurer NetScaler avec un serveur de noms ou un serveur virtuel DNS via lequel les domaines ELB /ALB sont résolus pour les groupes de services DBS. Pour plus d'informations sur les serveurs de noms ou les serveurs virtuels DNS, voir : DNS NameServer

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs**.



2. Cliquez sur **Ajouter** pour créer un serveur, fournir un nom et un FQDN correspondant à l'enregistrement A (nom de domaine) dans Azure pour l'ALB.



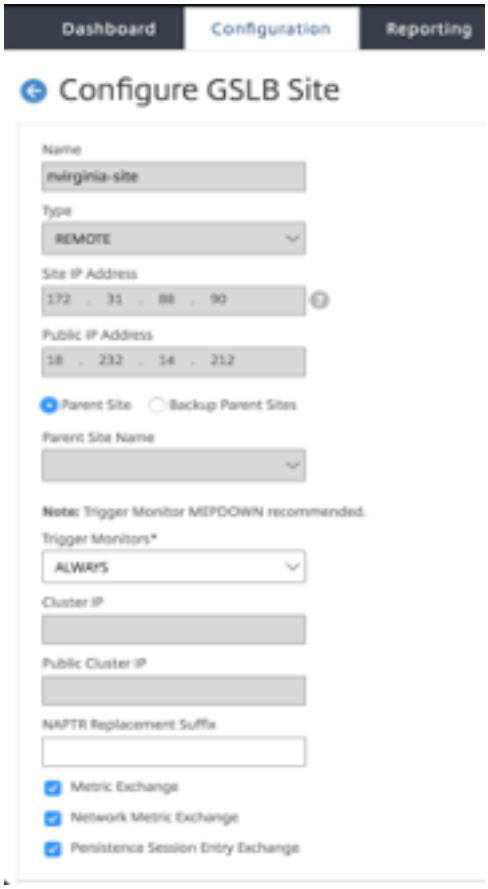
3. Répétez l'étape 2 pour ajouter le deuxième ALB à partir de la deuxième ressource dans Azure.

Configurations GSLB

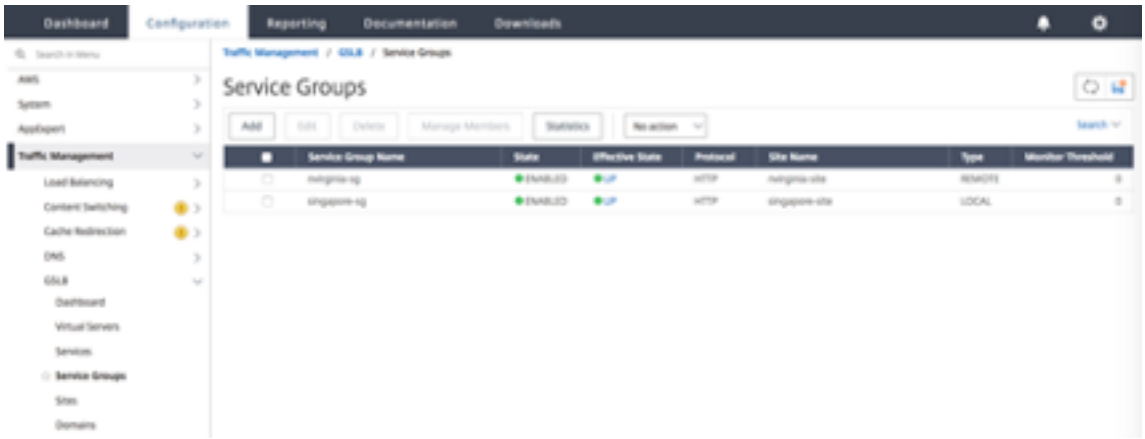
1. Cliquez sur le bouton **Ajouter** pour configurer un site GSLB.
2. Donnez un nom au site.

   Le type est configuré comme distant ou local en fonction de la configuration du site par les utilisateurs de NetScaler. L'adresse IP du site est l'adresse IP du site GSLB. Le site GSLB utilise cette adresse IP pour communiquer avec les autres sites GSLB. L'adresse IP publique est requise lors de l'utilisation d'un service cloud où une adresse IP particulière est hébergée sur un pare-feu externe ou un périphérique NAT. Assurez-vous que le site est configuré en tant que site parent. Assurez-vous que les moniteurs de déclenchement sont réglés sur TOUJOURS. Veillez également à cocher les trois cases en bas pour l'échange de métriques, l'échange de métriques réseau et l'échange d'entrées de session de persistance.

   Nous vous recommandons de définir le paramètre Trigger monitor sur MEPDOWN, voir :Configurer un groupe de services GSLB.

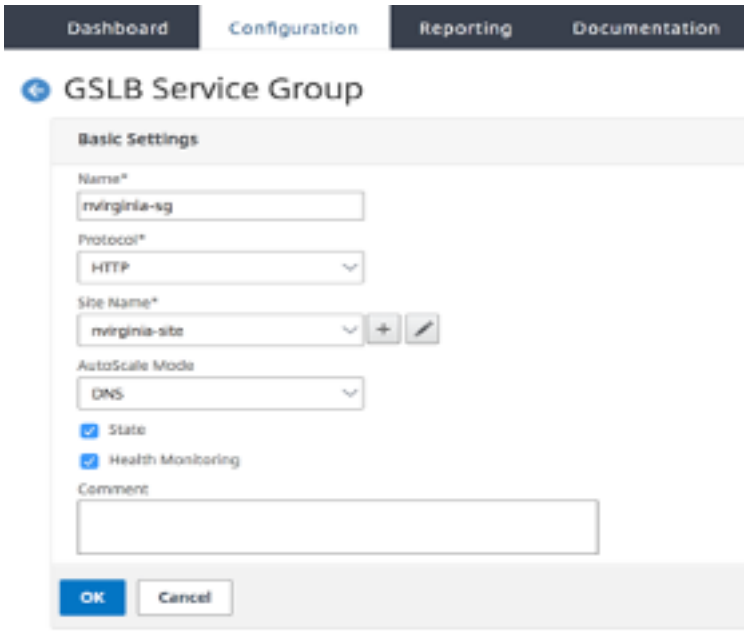


3. Cliquez sur**Créer**, répétez les étapes 3 et 4 pour configurer le site GSLB pour l'autre emplacement de ressources dans Azure (cela peut être configuré sur le même NetScaler).
4. Accédez à **Gestion du trafic > GSLB > Groupes de services**.

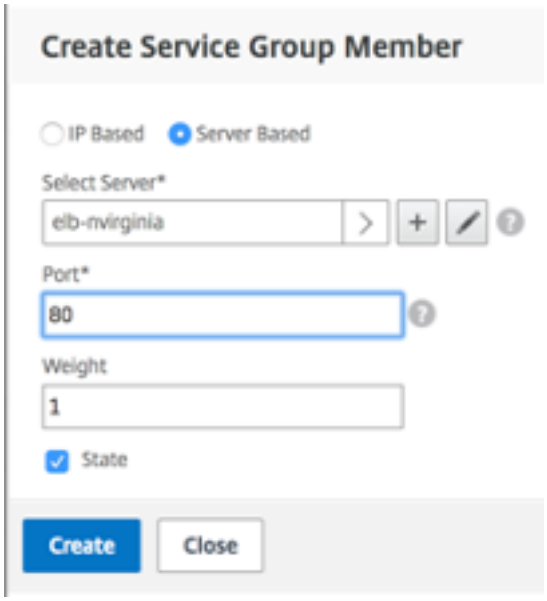


Cliquez sur **Ajouter** pour ajouter un groupe de services. Choisissez le site correspondant qui a été créé lors des étapes précédentes pour Nommer le groupe de services, utilisez le protocole HTTP, puis sous Nom du site. Assurez-vous de configurer le mode Autoscale en tant que DNS et de cocher les cases correspondant à la surveillance de l'état et de l'état de santé. Cliquez sur

OK pour créer le groupe de services.

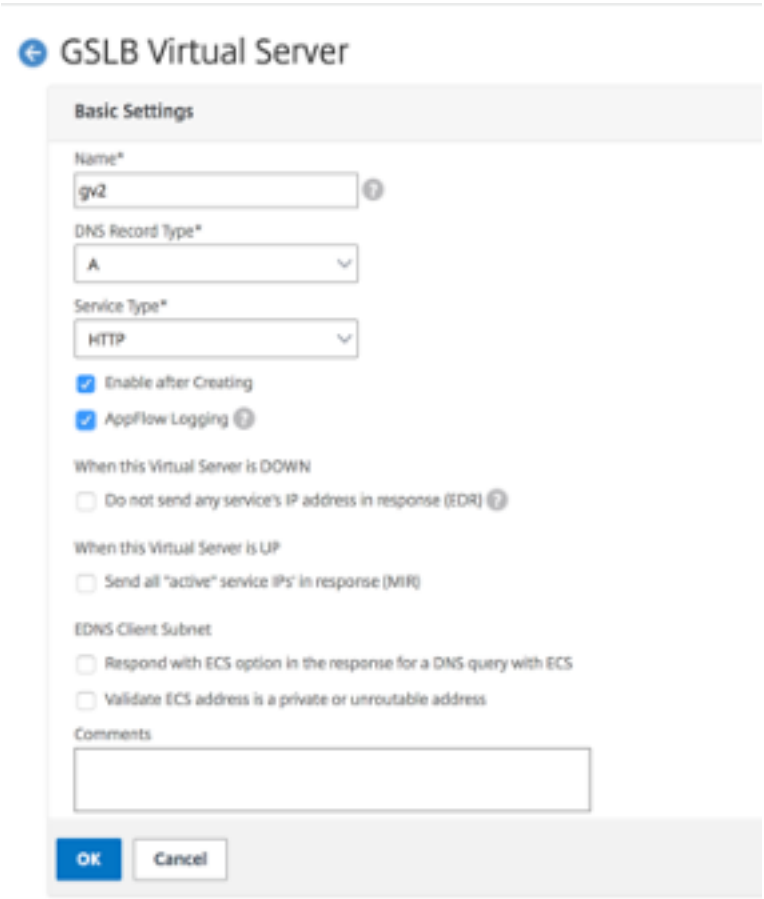


5. Cliquez sur **Membres du groupe de services** et sélectionnez **Basé sur un serveur**. Sélectionnez le serveur Elastic Load Balancing correspondant qui a été configuré au début du guide d'exécution. Configurez le trafic pour passer par le port 80. Cliquez sur**Créer**.

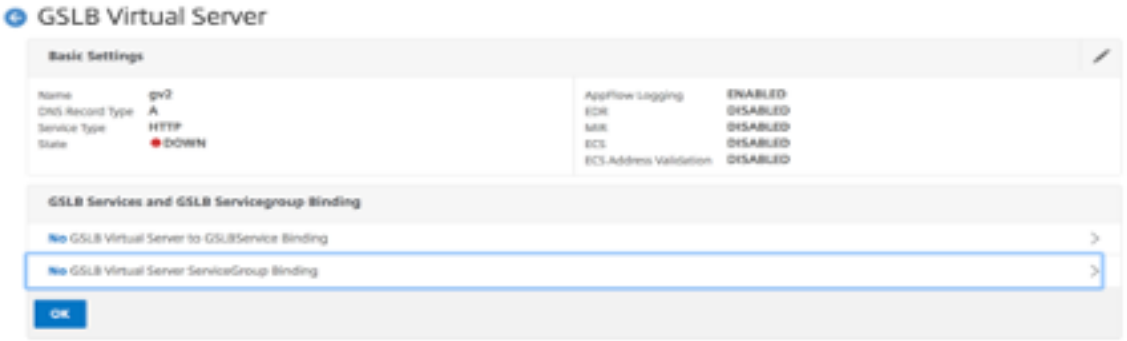


6. La liaison entre les membres du groupe de services doit être remplie de deux instances qu'elle reçoit de l'équilibreur de charge élastique.

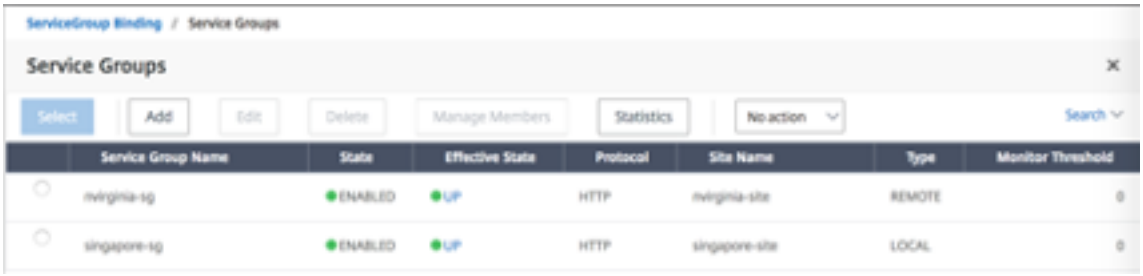
7. Répétez les étapes 5 et 6 pour configurer le groupe de services pour le deuxième emplacement de ressources dans Azure. (Cela peut être fait à partir de la même interface graphique NetScaler).
8. La dernière étape consiste à configurer un serveur virtuel GSLB. Accédez à **Gestion du trafic > GSLB > Serveurs virtuels**.
9. Cliquez sur **Ajouter** pour créer le serveur virtuel. Nommez le serveur, le type d'enregistrement DNS est défini comme A, le type de service est défini comme HTTP et cochez les cases Activer après la création et la journalisation AppFlow. Cliquez sur **OK** pour créer le serveur virtuel GSLB.



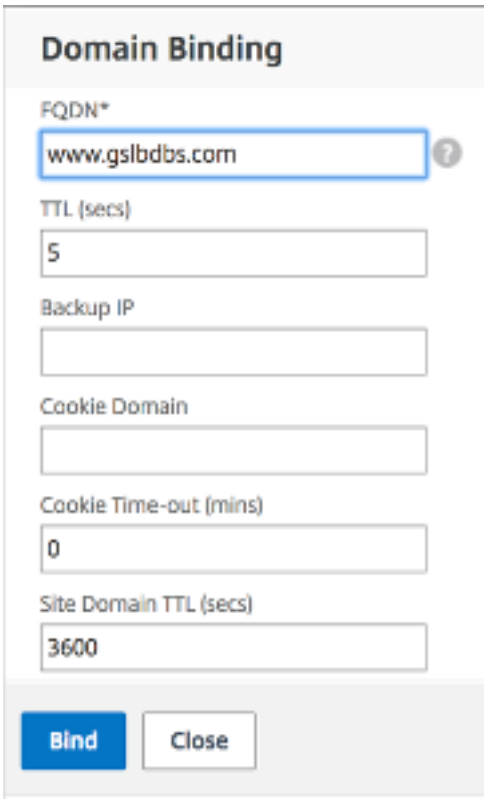
10. Une fois le serveur virtuel GSLB créé, cliquez sur **No GSLB Virtual Server ServiceGroup Binding**.



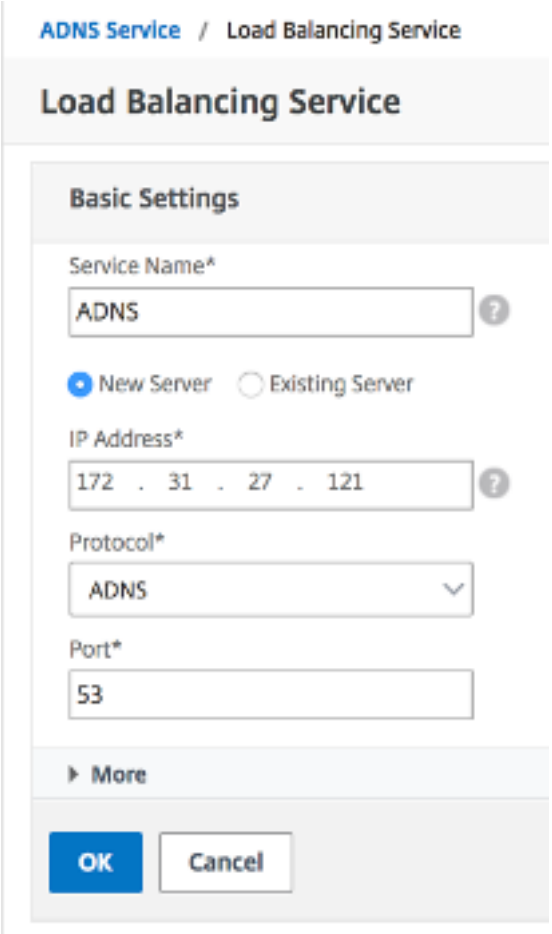
11. Sous ServiceGroup Binding, utilisez Select pour **sélectionner** et ajouter les groupes de services créés lors des étapes précédentes.



12. Configurez la liaison de domaine du serveur virtuel GSLB en cliquant sur **Aucune liaison de domaine du serveur virtuel GSLB**. Configurez le FQDN et Bind. Les autres paramètres peuvent être conservés par défaut.



13. Configurez le service ADNS en cliquant sur **Aucun service**. Ajoutez un **nom de service**, cliquez sur **Nouveau serveur** et entrez l' **adresse IP** du serveur ADNS. Si l'ADNS utilisateur est déjà configuré, les utilisateurs peuvent sélectionner le **serveur existant**, puis choisir l'ADNS utilisateur dans le menu déroulant. Assurez-vous que le protocole est ADNS et que le trafic est configuré pour passer par le port 53.



14. Configurez la méthode en tant que **connexion minimale** et la méthode de sauvegarde en tant que méthode **Round Robin**.

15. Cliquez sur **Terminé** et vérifiez que le serveur virtuel GSLB de l'utilisateur est affiché comme étant actif.

Prérequis pour Azure GSLB

Les prérequis pour les groupes de services NetScaler GSLB incluent un environnement Microsoft Azure fonctionnel doté des connaissances et de la capacité nécessaires pour configurer des groupes de sécurité, des serveurs Web Linux, des appliances NetScaler au sein d'AWS, des adresses IP élastiques et des équilibreurs de charge Elastic.

- L'intégration du service GSLB DBS nécessite NetScaler version 12.0.57 pour les instances d'équilibreur de charge Microsoft Azure.
- Entité du groupe de services GSLB : NetScaler version 12.0.57.
- Le groupe de services GSLB est introduit. Il prend en charge la mise à l'échelle automatique à l'aide de la découverte dynamique DBS.
- Les composants fonctionnels DBS (service basé sur le domaine) doivent être liés au groupe de services GSLB.

Exemple :

```
1 ```
2  > add server sydney_server LB-Sydney-xxxxxxxxxx.ap-southeast-2.elb.
     amazonaws.com
3  > add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName sydney
4  > bind gslb serviceGroup sydney_sg sydney_server 80
5 <!--NeedCopy--> ```
```

Autres ressources

Équilibrage de charge global NetScaler pour les déploiements hybrides et multicloud

Configurer les pools d'adresses IP de l'intranet pour une appliance NetScaler Gateway

May 5, 2023

Dans certains cas, les utilisateurs qui se connectent à l'aide du plug-in NetScaler Gateway ont besoin d'une adresse IP unique pour un dispositif NetScaler Gateway. Lorsque vous activez des pools d'adresses (également appelés pool d'adresses IP) pour un groupe, l'appliance NetScaler Gateway peut attribuer un alias d'adresse IP unique à chaque utilisateur. Vous configurez des pools d'adresses à l'aide d'adresses IP intranet (IIP).

Vous pouvez configurer des pools d'adresses sur une appliance NetScaler Gateway déployée sur Azure en suivant cette procédure en deux étapes :

- Enregistrement des adresses IP privées utilisées dans le pool d'adresses, dans Azure
- Configuration des pools d'adresses dans l'appliance NetScaler Gateway

Enregistrer une adresse IP privée dans le portail Azure

Dans Azure, vous pouvez déployer une instance NetScaler VPX avec plusieurs adresses IP. Vous pouvez ajouter des adresses IP à une instance VPX de deux manières :

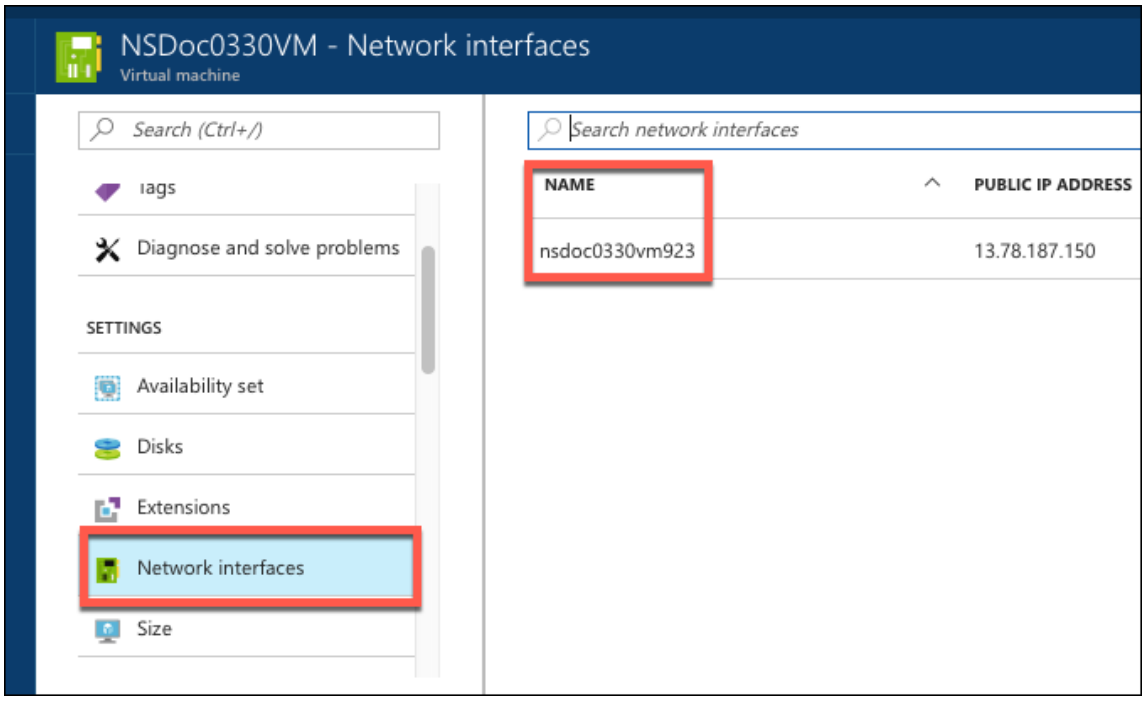
a. Lors du Provisioning d'une instance VPX

Pour plus d'informations sur la façon d'ajouter plusieurs adresses IP lors du provisionnement d'une instance VPX, consultez Configurer plusieurs adresses IP pour une instance autonome NetScaler. Pour ajouter des adresses IP à l'aide des commandes PowerShell lors du provisionnement d'une instance VPX, voir Configurer plusieurs adresses IP pour une instance NetScaler VPX en mode autonome àl'aide des commandes PowerShell.

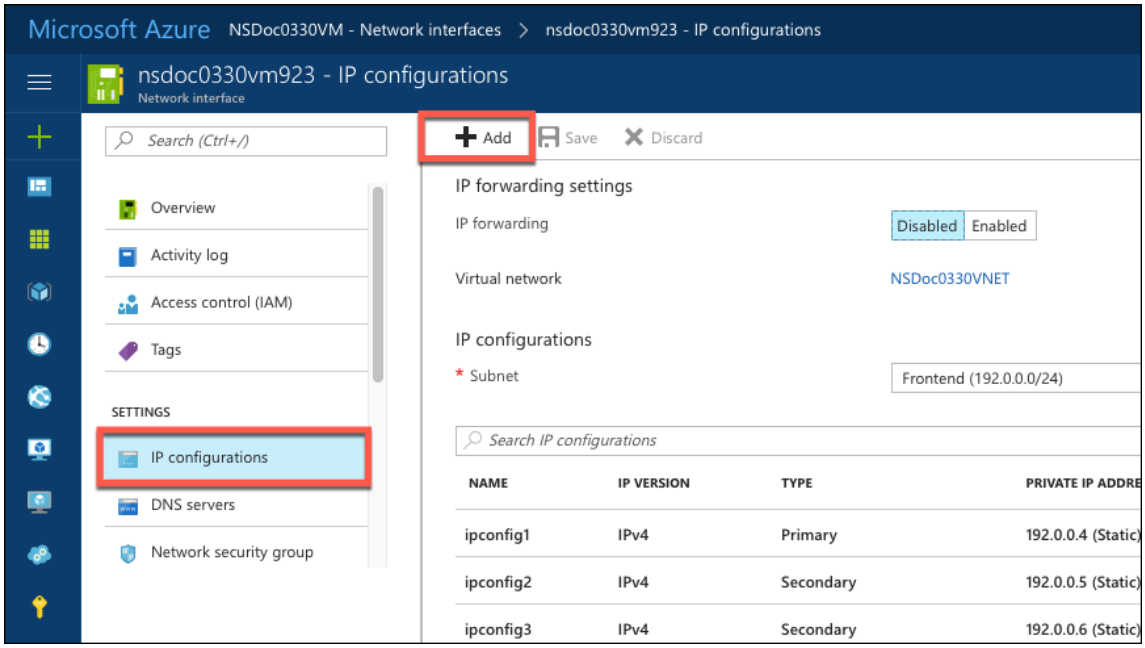
b. Après avoir Provisioning une instance VPX

Après avoir provisionné une instance VPX, procédez comme suit pour enregistrer une adresse IP privée sur le portail Azure, que vous configurez en tant que pool d'adresses dans l'appliance NetScaler Gateway.

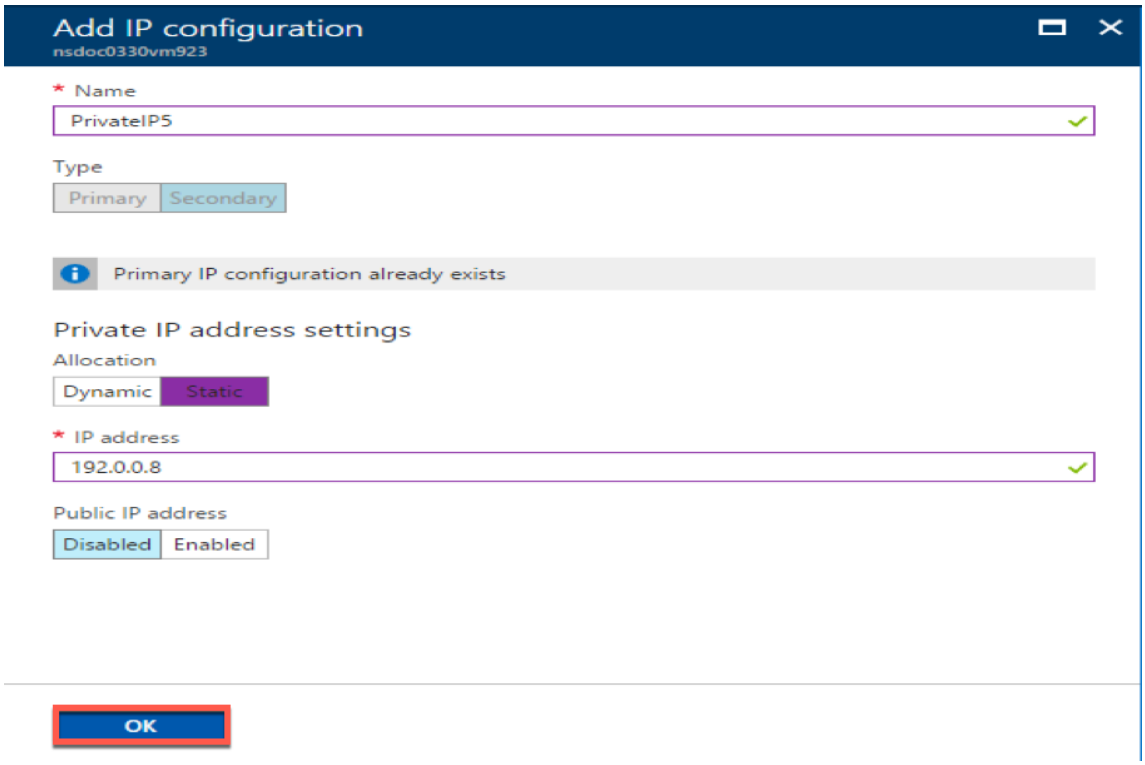
1. **Dans Azure Resource Manager (ARM), accédez à l'instance NetScaler VPX déjà créée > Interfaces réseau.** Choisissez l'interface réseau qui est liée à un sous-réseau auquel appartient l'IIP que vous souhaitez enregistrer.



2. Cliquez sur **Configurations IP**, puis sur **Ajouter**.



3. Fournissez les détails requis comme indiqué dans l'exemple ci-dessous et cliquez sur **OK**.



Configurer les pools d'adresses dans l'appliance NetScaler Gateway

Pour plus d'informations sur la configuration des pools d'adresses sur NetScaler Gateway, consultez cette rubrique Configuration des pools d'adresses.

Limitation : Vous ne pouvez pas lier une plage d'adresses IP à des utilisateurs. Chaque adresse IIP utilisée dans un pool d'adresses doit être enregistrée.

Configurer plusieurs adresses IP pour une instance autonome NetScaler VPX à l'aide des commandes PowerShell

May 5, 2023

Dans un environnement Azure, une appliance virtuelle NetScaler VPX peut être déployée avec plusieurs cartes réseau. Chaque carte réseau peut avoir plusieurs adresses IP. Cette section explique comment déployer une instance NetScaler VPX avec une seule carte réseau et plusieurs adresses IP, à l'aide des commandes PowerShell. Vous pouvez utiliser le même script pour un déploiement multi-NIC et multi-IP.

> **Remarque**
>
> Dans ce document, IP-Config fait référence à une paire d'adresses IP, IP publique et IP privée, associées à une carte réseau individuelle. Pour plus d'informations, consultez la section Terminologie Azure .

Cas d'utilisation

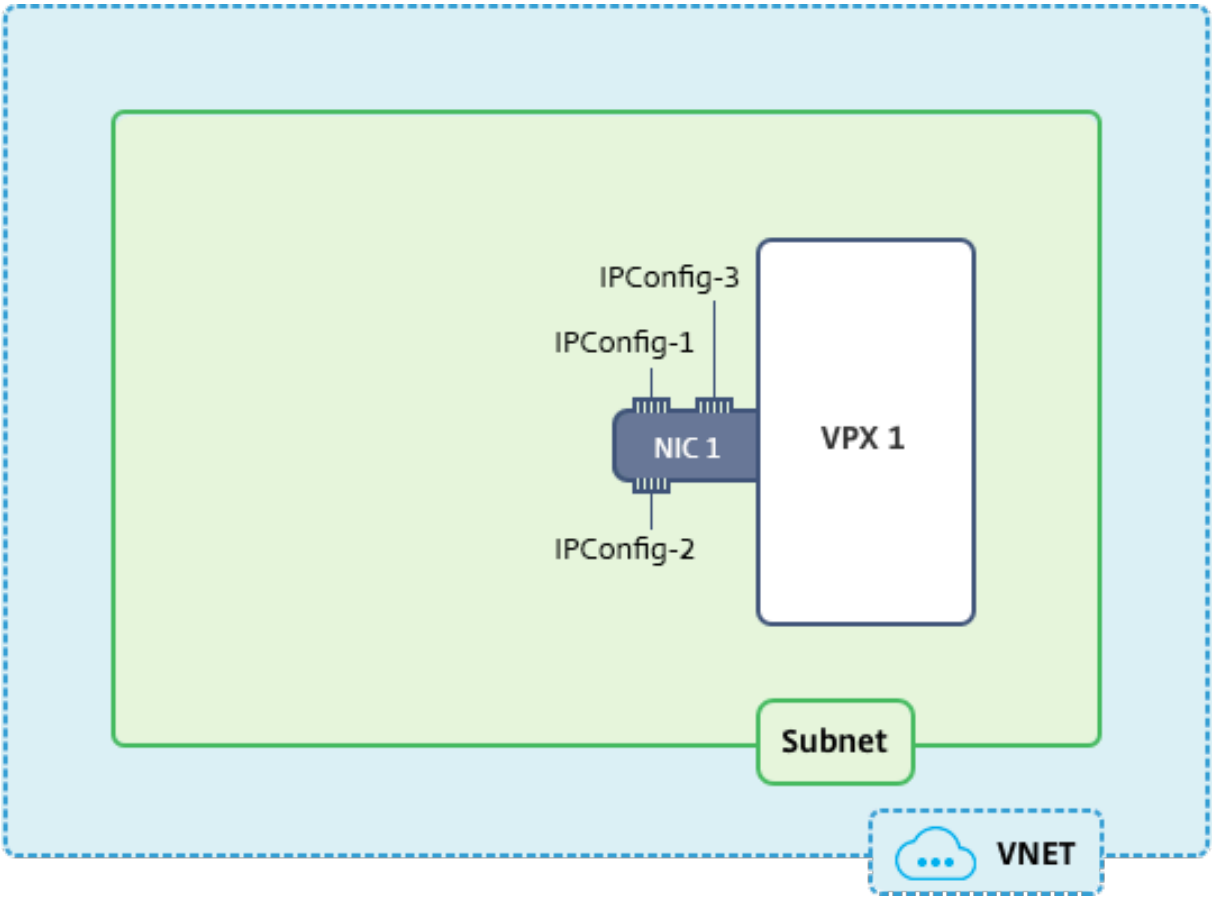
Dans ce cas d'utilisation, une seule carte réseau est connectée à un réseau virtuel (VNET). La carte réseau est associée à trois configurations IP, comme indiqué dans le tableau suivant.

Configuration IP	Associé à
IPConfig-1	Adresse IP publique statique ; adresse IP privée statique
IPConfig-2	Adresse IP publique statique ; adresse privée statique
IPConfig-3	Adresse IP privée statique

> **Remarque**
>
> IPConfig-3 n'est associé à aucune adresse IP publique.

Diagramme : Topologie

Voici la représentation visuelle du cas d'utilisation.



> **Remarque**
>
> Dans un déploiement Azure NetScaler VPX multi-NIC et multi-IP, l'adresse IP privée associée à la principale (première) `IPConfig` de la (première) carte réseau principale est automatiquement ajoutée en tant qu'adresse NSIP de gestion de l'appliance. Les adresses IP privées restantes associées `IPConfigs` doivent être ajoutées dans l'instance VPX en tant que VIP ou SNIP à l'aide de la `add ns ip` commande, comme déterminé par vos besoins.

Voici le résumé des étapes requises pour configurer plusieurs adresses IP pour une appliance virtuelle NetScaler VPX en mode autonome :

1. Créer un groupe de ressources
2. Créer un compte de stockage
3. Créer un jeu de disponibilité
4. Créer un groupe de services réseau
5. Créer un réseau virtuel
6. Créer une adresse IP publique
7. Attribuer une configuration IP
8. Créer une carte réseau
9. Création d'une instance NetScaler VPX

10. Vérifier les configurations de carte réseau
11. Vérifier les configurations côté VPX

Script

Paramètres

Voici des exemples de paramètres pour le cas d'utilisation dans ce document. Vous pouvez utiliser différents paramètres si vous le souhaitez.

$locName="westcentralus"

$rgname="Azure-MultiIP »

$nicName1="VM1-NIC1"

$VNetName="Azure-MultiIP-VNet »

$vNetAddressRange="11.6.0.0/16"

$FrontendSubnetName= « FrontendSubnet »

$frontEndSubnetRange="11.6.1.0/24"

$prmStorageAccountName="MultiIPStorage »

$avSetName="multiip-avSet"

$VMSize="Standard_DS4_v2" (Ce paramètre crée une machine virtuelle comportant jusqu'à quatre cartes réseau.)

Remarque : La configuration minimale requise pour une instance VPX est de 2 processeurs virtuels et de 2 Go de RAM.

$publisher = « Citrix »

$offer="netscalervpx110-6531" (Vous pouvez utiliser différentes offres.)

$sku="netscalerbyol » (Selon votre offre, le SKU peut être différent.)

$version="dernière »

$pubIPName1="PIP1"

$pubIPName2="PIP2"

$domName1="multiipvpx1"

$domName2="multiipvpx2"

$vmNamePrefix="VPXMultiIP »

$osDiskSuffix="osmultiipalbdiskdb1"

Informations relatives au groupe de sécurité réseau (NSG) :

$NSGName=”NSG-MultiIP »

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

$IpConfigName1=”IPConfig1”

$IPConfigName2=”IPConfig-2”

$IPConfigName3=”IPConfig-3”

1. Créer un groupe de ressources

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Créer un compte de stockage

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName
 -ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

3. Créer un jeu de disponibilité

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
$rgName -Location $locName
```

4. Créer un groupe de sécurité réseau

1. Ajoutez des règles. Vous devez ajouter une règle au groupe de sécurité réseau pour n’importe quel port desservant le trafic.

   ```
   $rule1=New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -Description
    "Allow HTTP"-Access Allow -Protocol Tcp -Direction Inbound -Priority
   101 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 80
   $rule2=New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -Description
    "Allow HTTPS"-Access Allow -Protocol Tcp -Direction Inbound -Priority
   110 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 443
   ```



```
$rule3=New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -Description
 "Allow SSH"-Access Allow -Protocol Tcp -Direction Inbound -Priority
120 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
 * -DestinationPortRange 22
```

2. Créez un objet de groupe de sécurité réseau.

```
$nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

5. Créer un réseau virtuel

1. Ajoutez des sous-réseaux.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $frontEndSubnetName
 -AddressPrefix $frontEndSubnetRange
```

2. Ajoutez un objet réseau virtuel.

```
$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
$frontendSubnet
```

3. Récupérez des sous-réseaux.

```
$subnetName="frontEndSubnet"
$subnet1=$vnet.Subnets|?{ $_.Name -eq $subnetName }
```

6. Créer une adresse IP publique

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
$rgName -DomainNameLabel $domName1 -Location $locName -AllocationMethod
Static
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
$rgName -DomainNameLabel $domName2 -Location $locName -AllocationMethod
Static
```

> **Remarque**
>
> Vérifiez la disponibilité des noms de domaine avant de les utiliser.
>
> La méthode d'allocation des adresses IP peut être dynamique ou statique.

7. Attribuer une configuration IP

Dans ce cas d'utilisation, tenez compte des points suivants avant d'attribuer des adresses IP :

- IPConfig-1 appartient au sous-réseau 1 de VPX1.
- IPConfig-2 appartient au sous-réseau 1 de VPX1.
- IPConfig-3 appartient au sous-réseau 1 de VPX1.

> **Remarque**
>
> Lorsque vous affectez plusieurs configurations IP à une carte réseau, une configuration doit être affectée comme principale.

```
$IPAddress1="11.6.1.27"
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress $pip1
     -Primary
$IPAddress2="11.6.1.28"
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress $pip2
$IPAddress3="11.6.1.29"
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary
```

Utilisez une adresse IP valide qui répond aux exigences de votre sous-réseau et vérifiez sa disponibilité.

8. Créer une carte réseau

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,$IPConfig3
 -NetworkSecurityGroupId $nsg.Id
```

9. Création d'une instance NetScaler VPX

1. Initialisez les variables.

   ```
   $suffixNumber = 1
   $vmName = $vmNamePrefix + $suffixNumber
   ```

2. Créez un objet de configuration de machine virtuelle.

   ```
   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
    $avSet.Id
   ```

3. Définissez les informations d'identification, le système d'exploitation et l'image.

   ```
   $cred=Get-Credential -Message "Type the name and password for VPX login
   ."
   ```



```
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName
 $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher
 -Offer $offer -Skus $sku -Version $version
```

4. Ajoutez une carte réseau.

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
Primary
```

> **Remarque**
>
> Dans un déploiement VPX multi-NIC, une carte réseau doit être principale. Par conséquent, « -Primary » doit être ajouté lors de l'ajout de cette carte réseau à l'instance VPX.

5. Spécifiez le disque du système d'exploitation et créez une machine virtuelle.

```
$osDiskName=$vmName + "-"+ $osDiskSuffix1
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString()+ "vhds/"+
 $osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
$osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
$locName
```

10. Vérifier les configurations de carte réseau

Une fois l'instance VPX démarrée, vous pouvez vérifier les adresses IP allouées à `IPConfigs` la carte réseau VPX à l'aide de la commande suivante.

```
$nic.IPConfig
```

11. Vérifier les configurations côté VPX

Lorsque l'instance NetScaler VPX démarre, une adresse IP privée associée à la carte réseau principale `IPconfig` est ajoutée en tant qu'adresse NSIP. Les adresses IP privées restantes doivent être ajoutées en tant qu'adresses VIP ou SNIP, selon vos besoins. Utilisez la commande suivante.

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

Vous avez maintenant configuré plusieurs adresses IP pour une instance NetScaler VPX en mode autonome.

Scripts PowerShell supplémentaires pour le déploiement Azure

June 2, 2023

Cette section fournit les applets de commande PowerShell avec lesquels vous pouvez effectuer les configurations suivantes dans Azure PowerShell :

- Provisionner une instance autonome NetScaler VPX
- Provisionner une paire NetScaler VPX dans une configuration haute disponibilité avec un équilibreur de charge externe Azure
- Provisionner une paire NetScaler VPX dans une configuration haute disponibilité avec l'équilibreur de charge interne Azure

Consultez également les rubriques suivantes pour les configurations que vous pouvez effectuer à l'aide des commandes PowerShell :

- Configurer une configuration haute disponibilité avec plusieurs adresses IP et cartes réseau à l'aide des commandes PowerShell
- Configurer GSLB sur des instances NetScaler VPX
- Configurer GSLB sur une configuration de haute disponibilité NetScaler active Standby
- Configurer plusieurs adresses IP pour une instance NetScaler VPX en mode autonome à l'aide des commandes PowerShell
- Configurer plusieurs VIP Azure pour une instance VPX autonome

Provisionner une instance autonome NetScaler VPX

1. **Création d'un groupe de ressources**

   Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous souhaitez gérer en tant que groupe. L'emplacement spécifié ici est l'emplacement par défaut des ressources de ce groupe de ressources. Assurez-vous que toutes les commandes permettant de créer un équilibreur de charge utilisent le même groupe de ressources.

   ```
   $rgName="<resource group name>"
   $locName="<location name, such as West US>
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Par exemple :

   ```
   $rgName = "ARM-VPX"
   $locName = "West US"
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```


2. **Créer un compte de stockage**

   Choisissez un nom unique pour votre compte de stockage qui ne contient que des lettres minuscules et des chiffres.

   ```
   $saName="<storage account name>"
   $saType="<storage account type>", spécifiez-en une : Standard_LRSStandard_GRS,
   Standard_RAGRS, ou Premium_LRS
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -
   Type $saType -Location $locName
   ```

   Par exemple :

   ```
   1 $saName="vpxstorage"
   2 $saType="Standard_LRS"
   3 New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
         -Type $saType -Location $locName
   4 <!--NeedCopy-->
   ```

3. **Création d'un ensemble de disponibilité**

   L'ensemble de disponibilité permet de maintenir vos machines virtuelles disponibles pendant les temps d'arrêt, par exemple pendant la maintenance. Un équilibreur de charge configuré avec un ensemble de disponibilité garantit que votre application est toujours disponible.

   ```
   $avName="<availability set name>"

   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -
   Location $locName
   ```

4. **Créer un réseau virtuel**

   Ajoutez un nouveau réseau virtuel avec au moins un sous-réseau, si le sous-réseau n'a pas été créé précédemment.

   ```
   $FrontendAddressPrefix="10.0.1.0/24"
   $BackendAddressPrefix="10.0.2.0/24"
   $vnetAddressPrefix="10.0.0.0/16"
   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet
    -AddressPrefix $FrontendAddressPrefix
   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet
    -AddressPrefix $BackendAddressPrefix
   New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName -
   Location $locName -AddressPrefix $vnetAddressPrefix -Subnet $frontendSubnet
   ,$backendSubnet
   ```

   Par exemple :


```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix

$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix

New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName
     -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
    $frontendSubnet,$backendSubnet
<!--NeedCopy-->
```

5. **Création d'une carte réseau**

   Créez une carte réseau et associez-la à l'instance NetScaler VPX. Le sous-réseau frontal créé dans la procédure ci-dessus est indexé à 0 et le sous-réseau principal est indexé à 1. Créez maintenant une carte réseau de l'une des trois manières suivantes :

   a) *NIC avec adresse IP publique*

   ```
   $nicName="<name of the NIC of the VM>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -Location $locName -AllocationMethod Dynamic

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
   $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
   PublicIpAddressId $pip.Id
   ```

   b) Carte *réseau avec adresse IP publique et étiquette DNS*

   ```
   $nicName="<name of the NIC of the VM>"

   $domName="<domain name label>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -DomainNameLabel $domName -Location $locName -AllocationMethod
   Dynamic
   ```

   Avant d'attribuer $DOMName, vérifiez qu'il est disponible ou non en utilisant la commande :

   ```
   Test-AzureRmDnsAvailability -DomainQualifiedName $domName -Location
   $locName

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
   $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
   PublicIpAddressId $pip.Id
   ```

   Par exemple :


```
$nicName="frontendNIC"

$domName="vpxazure"

$pip = New-AzureRmPublicIpAddress -Name $nicName -
    ResourceGroupName $rgName -DomainNameLabel $domName -Location
    $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -SubnetId $vnet.
    Subnets[0].Id -PublicIpAddressId $pip.Id
<!--NeedCopy-->
```

c) *Carte réseau avec adresse publique dynamique et adresse IP privée statique*

Assurez-vous que l'adresse IP privée (statique) que vous ajoutez à la machine virtuelle doit correspondre à celle du sous-réseau spécifié.

```
$nicName="<name of the NIC of the VM>"

$staticIP="<available static IP address on the subnet>"

$pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
$rgName -Location $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
PublicIpAddressId $pip.Id -PrivateIpAddress $staticIP
```

6. **Créer un objet virtuel**

```
$vmName="<VM name>"

$vmSize="<VM size string>"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName

$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
 $avset.Id
```

7. **Obtenir l'image NetScaler VPX**

```
$pubName="<Image publisher name>"

$offerName="<Image offer name>"

$skuName="<Image SKU name>"
```



```
$cred=Get-Credential -Message "Type the name and password of the local administrator account."
```

Fournissez vos informations d'identification utilisées pour vous connecter à VPX

```
$vm=Set-AzureRmVMOperatingSystem -VM $vm -Linux -ComputerName $vmName -Credential $cred -Verbose

$vm=Set-AzureRmVMSourceImage -VM $vm -PublisherName $pubName -Offer $offerName -Skus $skuName -Version "latest"

$vm=Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id
```

Par exemple :

```
$pubName="citrix"
```

La commande suivante est utilisée pour afficher toutes les offres de Citrix :

```
Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
    Select Offer

$offerName="netscalervpx110-6531"
<!--NeedCopy-->
```

La commande suivante permet de connaître le SKU proposé par l'éditeur pour un nom d'offre spécifique :

```
Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -Offer $offerName | Select Skus
```

8. **Créer une machine virtuelle**

```
$diskName="<name identifier for the disk in Azure storage, such as OSDisk>"
```

Par exemple :

```
$diskName="dynamic"

$pubName="citrix"

$offerName="netscalervpx110-6531"

$skuName="netscalerbyol"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

```



```
$osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/"
    + $diskName  + ".vhd"

$vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri $osDiskUri
     -CreateOption fromImage
<!--NeedCopy-->
```

Lorsque vous créez une machine virtuelle à partir d'images présentes sur Marketplace, utilisez la commande suivante pour spécifier le plan de machine virtuelle :

```
Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName -Name
 $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Provisionner une paire NetScaler VPX dans une configuration haute disponibilité avec un équilibreur de charge externe Azure

Connectez-vous à AzureRMAccount à l'aide de vos informations d'identification utilisateur Azure.

1. **Création d'un groupe de ressources**

   L'emplacement spécifié ici est l'emplacement par défaut des ressources de ce groupe de ressources. Assurez-vous que toutes les commandes utilisées pour créer un équilibreur de charge utilisent le même groupe de ressources.

   ```
   $rgName="<resource group name>"

   $locName="<location name, such as West US>"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Par exemple :

   ```
   $rgName = "ARM-LB-NS"

   $locName = "West US"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```

2. **Créer un compte de stockage**

   Choisissez un nom unique pour votre compte de stockage qui ne contient que des lettres minuscules et des chiffres.

   ```
   $saName="<storage account name>"
   ```


`$saType="<storage account type>"`, spécifiez-en une : `Standard_LRSStandard_GRS`, `Standard_RAGRS`, ou `Premium_LRS`

```
New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -
Type $saType -Location $locName
```

Par exemple :

```
$saName="vpxstorage"

$saType="Standard_LRS"

New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
    -Type $saType -Location $locName
<!--NeedCopy-->
```

3. **Création d'un ensemble de disponibilité**

   Un équilibreur de charge configuré avec un ensemble de disponibilité garantit que votre application est toujours disponible.

   `$avName="<availability set name>"`

   ```
   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -
   Location $locName
   ```

4. **Créer un réseau virtuel**

   Ajoutez un nouveau réseau virtuel avec au moins un sous-réseau, si le sous-réseau n'a pas été créé précédemment.

   ```
   $vnetName = "LBVnet"

   $FrontendAddressPrefix="10.0.1.0/24"

   $BackendAddressPrefix="10.0.2.0/24"

   $vnetAddressPrefix="10.0.0.0/16"

   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       frontendSubnet -AddressPrefix $FrontendAddressPrefix

   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       backendSubnet -AddressPrefix $BackendAddressPrefix

   $vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
        $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
       Subnet $frontendSubnet,$backendSubnet
   ```



```
<!--NeedCopy-->
```

Remarque : Choisissez la valeur du paramètre AddressPrefix selon vos besoins.

Affectez des sous-réseaux frontaux et back-end au réseau virtuel que vous avez créé précédemment au cours de cette étape.

Si le sous-réseau frontal est le premier élément du réseau virtuel de tableau, SubnetID doit être $VNet.Subnets [0] .Id.

Si le sous-réseau frontal est le deuxième élément du tableau, l'ID de sous-réseau doit être $VNet.Subnets [1] .Id, etc.

5. **Configurer l'adresse IP frontale et créer un pool d'adresses back-end**

   Configurez une adresse IP frontale pour le trafic réseau d'équilibrage de charge entrant et créez un pool d'adresses principal pour recevoir le trafic d'équilibrage de charge.

```
$pubName="PublicIp1"

$publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
    ResourceGroupName $rgName -Location $locName -AllocationMethod
    Static -DomainNameLabel nsvpx
<!--NeedCopy-->
```

   Remarque : Vérifiez la disponibilité de la valeur pour DomainNameLabel.

```
$FIPName = "ELBFIP"

$frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -Name
    $FIPName -PublicIpAddress $publicIP1

$BEPool = "LB-backend-Pool"

$beaddresspool1= New-AzureRmLoadBalancerBackendAddressPoolConfig -
    Name $BEPool
<!--NeedCopy-->
```

6. **Créez une sonde de santé**

   Créez une sonde de santé TCP avec le port 9000 et un intervalle de 5 secondes.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name
    HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
<!--NeedCopy-->
```


7. **Création d'une règle d'équilibrage de charge**

   Créez une règle LB pour chaque service pour lequel vous équilibrez la charge.

   Par exemple :

   Vous pouvez utiliser l'exemple suivant pour équilibrer la charge du service HTTP.

```
$lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
    FrontendIpConfiguration $frontendIP1 -BackendAddressPool
    $beAddressPool1 -Probe $healthProbe -Protocol Tcp -FrontendPort
     80 -BackendPort 80
<!--NeedCopy-->
```

8. **Création de règles NAT entrantes**

   Créez des règles NAT pour les services dont vous n'équilibrez pas la charge.

   Par exemple, lors de la création d'un accès SSH à une instance NetScaler VPX.

   Remarque : Le triplet Protocol-FrontEndPort-BackendPort ne doit pas être le même pour deux règles NAT.

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH1     -FrontendIpConfiguration $frontendIP1 -Protocol
    TCP -FrontendPort 22 -BackendPort 22

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH2 -FrontendIpConfiguration $frontendIP1 -Protocol TCP -
    FrontendPort 10022 -BackendPort 22
<!--NeedCopy-->
```

9. **Créer une entité d'équilibrage de charge**

   Créez l'équilibreur de charge en ajoutant tous les objets (règles NAT, règles de l'équilibreur de charge, configurations de sonde).

```
$lbName="ELB"

$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name
    $lbName -Location $locName -InboundNatRule $inboundNATRule1,
    $inboundNATRule2 -FrontendIpConfiguration $frontendIP1 -
    LoadBalancingRule $lbrule1 -BackendAddressPool $beAddressPool1
    -Probe $healthProbe
<!--NeedCopy-->
```

10. **Création d'une carte réseau**

    Créez deux cartes réseau et associez chaque carte réseau à chaque instance VPX

a) NIC1 avec VPX1

Par exemple :

```
$nicName="NIC1"

$lbName="ELB"

$bePoolIndex=0

* Rule indexes starts from 0.

$natRuleIndex=0

$subnetIndex=0

* Frontend subnet index

$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName

$nic1=New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
    BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
    $lb.InboundNatRules[$natRuleIndex]
<!--NeedCopy-->
```

b) NIC2 avec VPX2

Par exemple :

```
$nicName="NIC2"

$lbName="ELB"

$bePoolIndex=0

$natRuleIndex=1

* Second Inbound NAT (SSH) rule we need to use

`$subnetIndex=0

* Frontend subnet index

```



```
$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
    $rgName

$nic2=New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
    BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
    $lb.InboundNatRules[$natRuleIndex]
<!--NeedCopy-->
```

11. **Création d'instances NetScaler VPX**

    Créez deux instances NetScaler VPX faisant partie du même groupe de ressources et du même ensemble de disponibilité, puis associez-les à l'équilibreur de charge externe.

    a) Instance 1 de NetScaler VPX

    Par exemple :

```
$vmName="VPX1"

$vmSize="Standard_A3"

$pubName="citrix"

$offerName="netscalervpx110-6531"

$skuName="netscalerbyol"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
     $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be used
     to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id

```



```
$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
    " + $diskName  + ".vhd"

$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
     -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm1
<!--NeedCopy-->
```

b) Instance 2 de NetScaler VPX

Par exemple :

```
$vmName="VPX2"

$vmSize="Standard_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
     $rgName

$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message " Type Credentials which will be
    used to login to VPX instance "

$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id

$diskName="dynamic"

```



```
$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/
    " + $diskName  + ".vhd"

$vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
     -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm2
<!--NeedCopy-->
```

12. **Configuration des machines virtuelles**

    Lorsque les deux instances NetScaler VPX démarrent, connectez-vous aux deux instances NetScaler VPX à l'aide du protocole SSH pour configurer les machines virtuelles.

    a) Active-Active : exécutez le même ensemble de commandes de configuration sur la ligne de commande des deux instances de NetScaler VPX.

    b) Actif-Passif : exécutez cette commande sur la ligne de commande des deux instances NetScaler VPX.

    ```
    add ha node ##nodeID <nsip of other NetScaler VPX>
    ```

    En mode actif-passif, exécutez uniquement les commandes de configuration sur le nœud principal.

Provisionner une paire NetScaler VPX dans une configuration haute disponibilité avec l'équilibreur de charge interne Azure

Connectez-vous à AzureRMAccount à l'aide de vos informations d'identification utilisateur Azure.

1. **Création d'un groupe de ressources**

   L'emplacement spécifié ici est l'emplacement par défaut des ressources de ce groupe de ressources. Assurez-vous que toutes les commandes permettant de créer un équilibreur de charge utilisent le même groupe de ressources.

   ```
   $rgName="\<resource group name\>"

   $locName="\<location name, such as West US\>"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```


Par exemple :

```
$rgName = "ARM-LB-NS"

$locName = "West US"

New-AzureRmResourceGroup -Name $rgName -Location $locName
<!--NeedCopy-->
```

2. **Créer un compte de stockage**

   Choisissez un nom unique pour votre compte de stockage qui ne contient que des lettres minuscules et des chiffres.

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`, spécifiez-en une : `Standard_LRSStandard_GRS`, `Standard_RAGRS`, ou `Premium_LRS`

   `New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName`

   Par exemple :

   ```
   $saName="vpxstorage"

   $saType="Standard_LRS"

   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
       -Type $saType -Location $locName
   <!--NeedCopy-->
   ```

3. **Création d'un ensemble de disponibilité**

   Un équilibreur de charge configuré avec un ensemble de disponibilité garantit que votre application est toujours disponible.

   `$avName="<availability set name>"`

   `New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName`

4. **Créer un réseau virtuel**

   Ajoutez un nouveau réseau virtuel avec au moins un sous-réseau, si le sous-réseau n'a pas été créé précédemment.

   ```
   $vnetName = "LBVnet"

   ```



```
$vnetAddressPrefix="10.0.0.0/16"

$FrontendAddressPrefix="10.0.1.0/24"

$BackendAddressPrefix="10.0.2.0/24"

$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
    $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
   Subnet $frontendSubnet,$backendSubnet`

$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   frontendSubnet -AddressPrefix $FrontendAddressPrefix

$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   backendSubnet -AddressPrefix $BackendAddressPrefix
<!--NeedCopy-->
```

Remarque : Choisissez la valeur du paramètre AddressPrefix selon vos besoins.

Affectez des sous-réseaux frontaux et back-end au réseau virtuel que vous avez créé précédemment au cours de cette étape.

Si le sous-réseau frontal est le premier élément du réseau virtuel de tableau, SubnetID doit être $VNet.Subnets [0] .Id.

Si le sous-réseau frontal est le deuxième élément du tableau, l'ID de sous-réseau doit être $VNet.Subnets [1] .Id, etc.

5. **Créer un pool d'adresses backend**

```
$beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -Name "
LB-backend"
```

6. **Création de règles NAT**

Créez des règles NAT pour les services dont vous n'équilibrez pas la charge.

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
   Name "Inboundnatrule1" -FrontendIpConfiguration $frontendIP -
   Protocol TCP -FrontendPort 3441 -BackendPort 3389

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
   Name "RDP2" -FrontendIpConfiguration $frontendIP -Protocol TCP
   -FrontendPort 3442 -BackendPort 3389
<!--NeedCopy-->
```

Utilisez les ports frontaux et dorsaux selon vos besoins.

7. **Créez une sonde de santé**

   Créez une sonde de santé TCP avec le port 9000 et un intervalle de 5 secondes.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "
    HealthProbe"  " -Protocol tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
<!--NeedCopy-->
```

8. **Création d'une règle d'équilibrage de charge**

   Créez une règle LB pour chaque service pour lequel vous équilibrez la charge.

   Par exemple :

   Vous pouvez utiliser l'exemple suivant pour équilibrer la charge du service HTTP.

```
$lbrule = New-AzureRmLoadBalancerRuleConfig -Name "lbrule1" -
    FrontendIpConfiguration $frontendIP -BackendAddressPool
    $beAddressPool -Probe $healthProbe -Protocol Tcp -FrontendPort
    80 -BackendPort 80
<!--NeedCopy-->
```

   Utilisez les ports frontaux et dorsaux selon vos besoins.

9. **Créer une entité d'équilibrage de charge**

   Créez l'équilibreur de charge en ajoutant tous les objets (règles NAT, règles de l'équilibreur de charge, configurations de sonde).

```
$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -Name
    "InternalLB" -Location $locName -FrontendIpConfiguration
    $frontendIP -InboundNatRule $inboundNATRule1,$inboundNatRule2 -
    LoadBalancingRule $lbrule -BackendAddressPool $beAddressPool -
    Probe $healthProbe
<!--NeedCopy-->
```

10. **Création d'une carte réseau**

    Créez deux cartes réseau et associez chaque carte réseau à chaque instance NetScaler VPX

```
$backendnic1= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic1-be -Location $locName -PrivateIpAddress
    10.0.2.6 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
     $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
    $nrplb.InboundNatRules[0]
<!--NeedCopy-->
```


Cette carte réseau est destinée à NetScaler VPX 1. L'IP privée doit se trouver dans le même sous-réseau que celui du sous-réseau ajouté.

```
$backendnic2= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic2-be -Location $locName -PrivateIpAddress
    10.0.2.7 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
     $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
    $nrplb.InboundNatRules[1].
<!--NeedCopy-->
```

Cette carte réseau est destinée à NetScaler VPX 2. Le paramètre `Private IPAddress` peut avoir n'importe quelle adresse IP privée selon vos besoins.

11. **Création d'instances NetScaler VPX**

    Créez deux instances VPX faisant partie du même groupe de ressources et du même ensemble de disponibilité, et associez-les à l'équilibreur de charge interne.

    a) Instance 1 de NetScaler VPX

    Par exemple :

```
$vmName="VPX1"

$vmSize="Standard_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
     $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be used
     to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName
```



```
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
      " + $diskName  + ".vhd"
22
23 $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
      $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
       -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
      $vm1
28 <!--NeedCopy-->
```

b) Instance 2 de NetScaler VPX

Par exemple :

```
1  $vmName="VPX2"
2
3  $vmSize="Standard_A3"
4
5  $avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
       $rgName
6
7  $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
      AvailabilitySetId $avset.Id
8
9  $cred=Get-Credential -Message " Type Credentials which will be
      used to login to VPX instance "
10
11 $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
      $vmName -Credential $cred -Verbose
12
13 $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
      Offer $offerName -Skus $skuName -Version "latest"
14
15 $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id
16
17 $diskName="dynamic"
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
      Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/
```



```
      " + $diskName  + ".vhd"
22
23 $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
      $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
       -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
      $vm2
28 <!--NeedCopy-->
```

12. **Configuration des machines virtuelles**

    Lorsque les deux instances NetScaler VPX démarrent, connectez-vous aux deux instances NetScaler VPX à l'aide du protocole SSH pour configurer les machines virtuelles.

    a) Active-Active : exécutez le même ensemble de commandes de configuration sur la ligne de commande des deux instances de NetScaler VPX.

    b) Actif-Passif : exécutez cette commande sur la ligne de commande des deux instances NetScaler VPX.

    ```
    add ha node ##nodeID <nsip of other NetScaler VPX>
    ```

    En mode actif-passif, exécutez uniquement les commandes de configuration sur le nœud principal.

FAQ Azure

May 5, 2023

- **La procédure de mise à niveau de l'instance NetScaler VPX installée depuis Azure Marketplace est-elle différente de la procédure de mise à niveau locale ?**

  Non. Vous pouvez mettre à niveau votre instance NetScaler VPX dans le cloud Microsoft Azure vers NetScaler VPX version 11.1 ou ultérieure, à l'aide des procédures de mise à niveau standard de NetScaler VPX. Vous pouvez effectuer la mise à niveau à l'aide de procédures GUI ou CLI. Pour toute nouvelle installation, utilisez l'image NetScaler VPX pour le cloud Microsoft Azure.

  Pour télécharger les versions de mise à niveau de NetScaler VPX, accédez à Téléchargements de NetScaler > Micrologiciel **NetScaler.**

- **Comment corriger les mouvements MAC et les désactivations d'interface observées sur les instances NetScaler VPX hébergées sur Azure ?**

Dans un environnement Azure Multi-NIC, par défaut, toutes les interfaces de données peuvent afficher des mouvements MAC et des muettes d'interface. Pour éviter les déplacements du MAC et les désactivations d'interface dans les environnements Azure, Citrix vous recommande de créer un VLAN par interface de données (sans balise) de l'instance NetScaler VPX et de lier l'adresse IP principale de la carte réseau dans Azure.

Pour plus d'informations, consultez l'article CTX224626 .

Déployer une instance NetScaler VPX sur Google Cloud Platform

May 5, 2023

Vous pouvez déployer une instance NetScaler VPX sur Google Cloud Platform (GCP). Une instance VPX dans GCP vous permet de tirer parti des fonctionnalités de cloud computing GCP et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic Citrix pour vos besoins professionnels. Vous pouvez déployer des instances VPX dans GCP en tant qu'instances autonomes. Les configurations à carte réseau unique et à plusieurs cartes réseau sont prises en charge.

Fonctionnalités prises en charge

Toutes les fonctionnalités Premium, Advanced et Standard sont prises en charge sur le GCP en fonction de la licence/du type de version utilisé.

Limitation

- IPv6 n'est pas pris en charge.

Configuration matérielle requise

L'instance VPX dans GCP doit avoir au moins 2 vCPU et 4 Go de RAM.

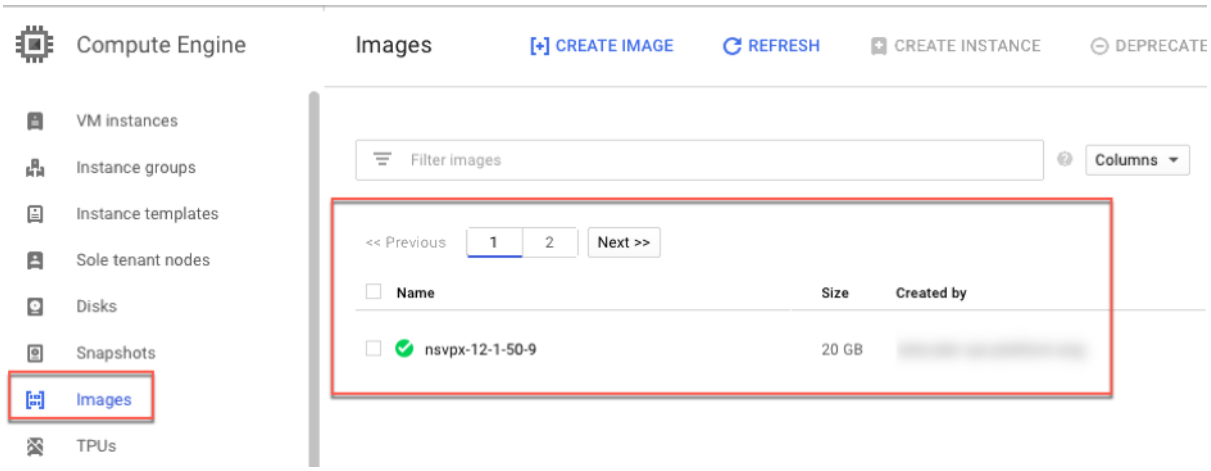
Composants requis

1. Installez l'utilitaire « gcloud » sur votre appareil. Vous pouvez trouver l'utilitaire sur ce lien : https://cloud.google.com/sdk/install
2. Téléchargez l'image NSVPX-GCP depuis le site NetScaler.
3. Téléchargez le fichier (par exemple, NSVPX-GCP-12.1-50.9_NC_64.tar.gz) dans un compartiment de stockage sur Google en suivant les étapes indiquées à l'adresse https://cloud.google.com/storage/docs/uploading-objects.

4. Exécutez la commande suivante sur l'utilitaire gcloud pour créer une image.

```
gcloud compute images create <IMAGE_NAME> --source-uri=gs://<
    STORAGE_BUCKET_NAME>/<FILE_NAME>.tar.gz --guest-os-features=
    MULTI_IP_SUBNET
<!--NeedCopy-->
```

La création de l'image peut prendre un moment. Une fois l'image créée, elle apparaît sous **Compute** > **Compute Engine** dans la console GCP.



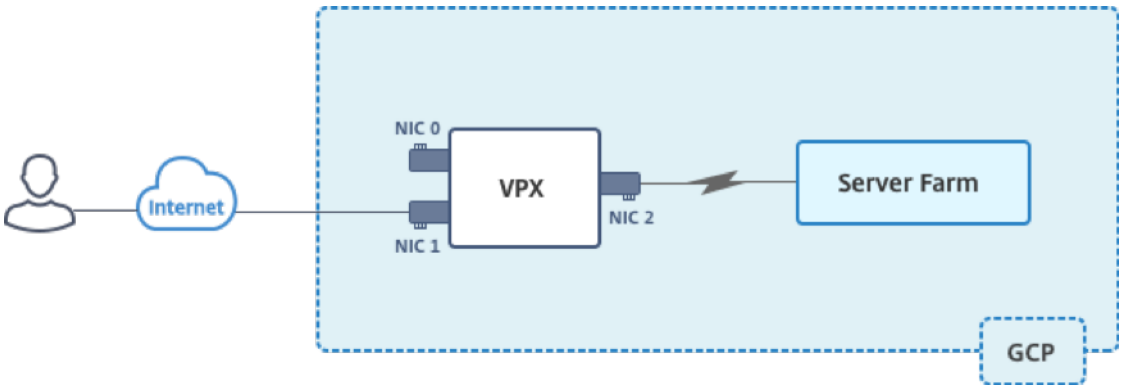
Points à noter

Prenez en compte les points spécifiques au GCP suivants avant de commencer votre déploiement.

- Après avoir créé l'instance, vous ne pouvez ni ajouter ni supprimer d'interfaces réseau.
- Pour un déploiement multi-cartes réseau, créez des réseaux VPC distincts pour chaque carte réseau. Une carte réseau ne peut être associée qu'à un seul réseau.
- Pour une instance à carte réseau unique, la console GCP crée un réseau par défaut.
- Au moins 4 vCPU sont requis pour une instance avec plus de deux interfaces réseau.
- Si le transfert IP est requis, vous devez activer le transfert IP lors de la création de l'instance et de la configuration de la carte réseau.

Scénario : Déployer une instance VPX autonome multi-NIC et multi-IP

Ce scénario montre comment déployer une instance autonome NetScaler VPX dans GCP. Dans ce scénario, vous créez une instance VPX autonome avec de nombreuses cartes réseau. L'instance communique avec les serveurs principaux (la batterie de serveurs).



Créez trois cartes réseau pour atteindre les objectifs suivants.

Carte d'interface réseau	Motif	Associé au réseau VPC
NIC 0	Trafic de gestion des serveurs (NetScaler IP)	Réseau de gestion
CARTE RÉSEAU 1	Sert le trafic côté client (VIP)	Réseau client
NIC 2	Communication avec les serveurs back-end (SNIP)	Réseau de serveurs dorsaux

Configurez les routes de communication requises entre les éléments suivants :

- instance VPX et les serveurs principaux.
- instance VPX et les hôtes externes sur l'Internet public.

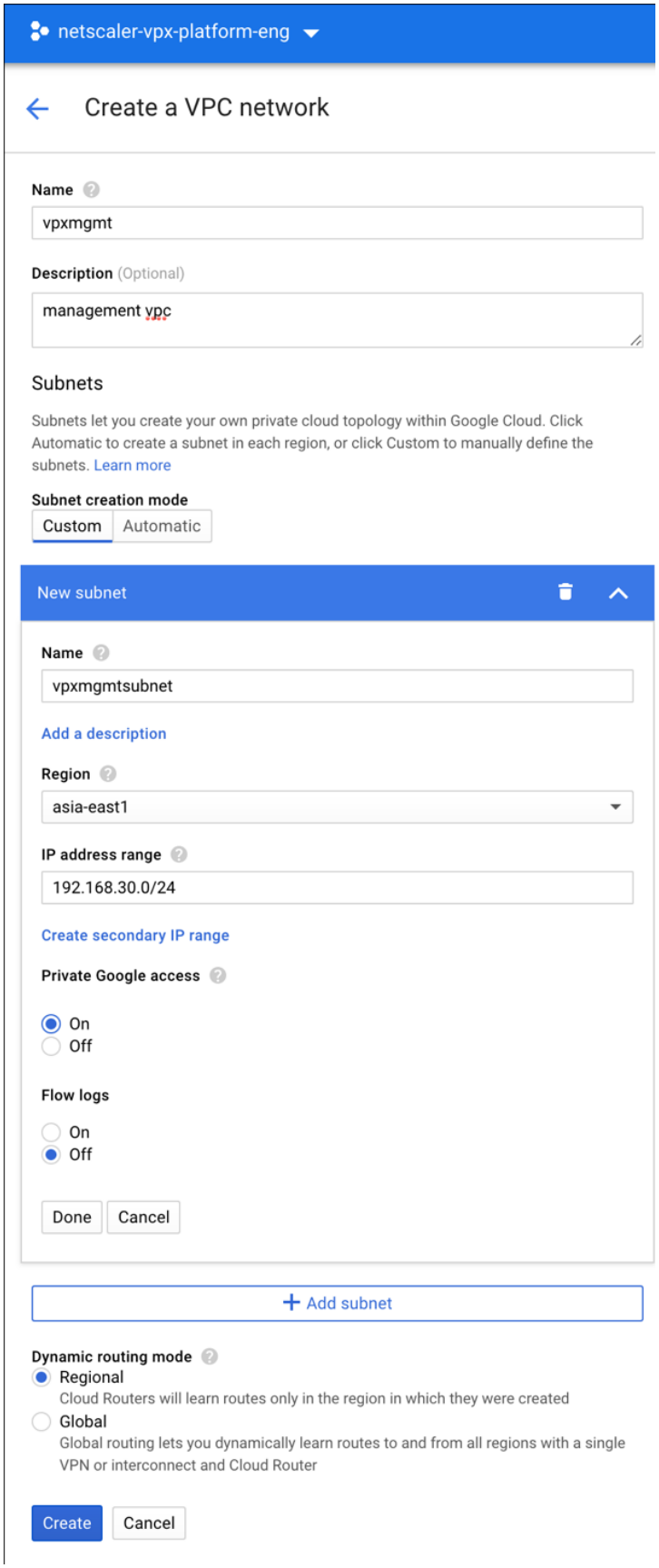
Résumé des étapes de déploiement

1. Créez trois réseaux VPC pour trois cartes réseau différentes.
2. Création de règles de pare-feu pour les ports 22, 80 et 443
3. Créer une instance avec trois cartes réseau

> **Remarque :**
>
> Créez une instance dans la même région que celle où vous avez créé les réseaux VPC.

Étape 1. Créez des réseaux VPC.

Créez trois réseaux VPC associés à la carte réseau de gestion, à la carte réseau cliente et à la carte réseau de serveur. Pour créer un réseau VPC, connectez-vous à **la console Google > Réseau > Réseau VPC > Créer un réseau VPC**. Renseignez les champs obligatoires, comme indiqué dans la capture d'écran, puis cliquez sur **Créer**.

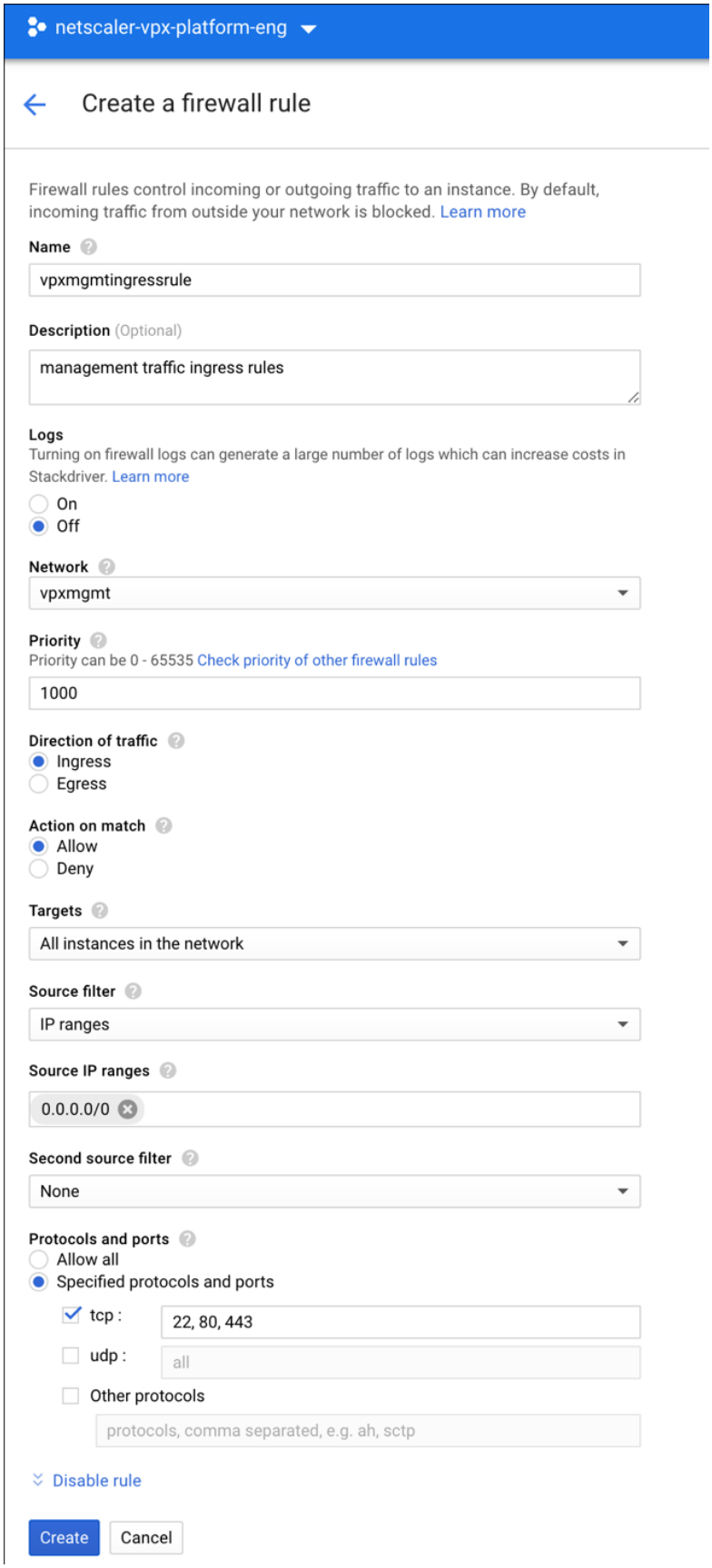


De même, créez des réseaux VPC pour les cartes réseau côté client et côté serveur.

> **Remarque :**
>
> Les trois réseaux VPC doivent se trouver dans la même région, à savoir asia-east1 dans ce scénario.

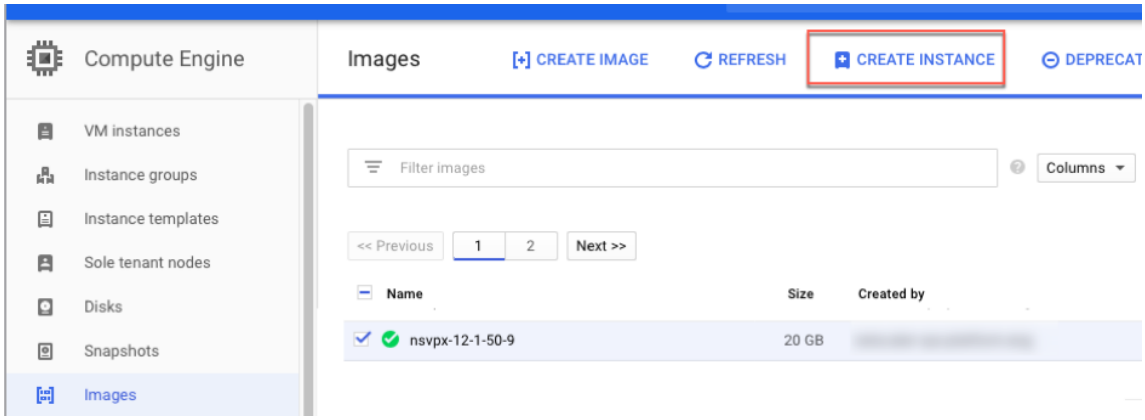
Étape 2. Créez des règles de pare-feu pour les ports 22, 80 et 443.

Créez des règles pour SSH (port 22), HTTP (port 80) et HTTPS (port 443) pour chaque réseau VPC. Pour plus d'informations sur les règles de pare-feu, voir Vue d' ensemble des règles de pare-feu.



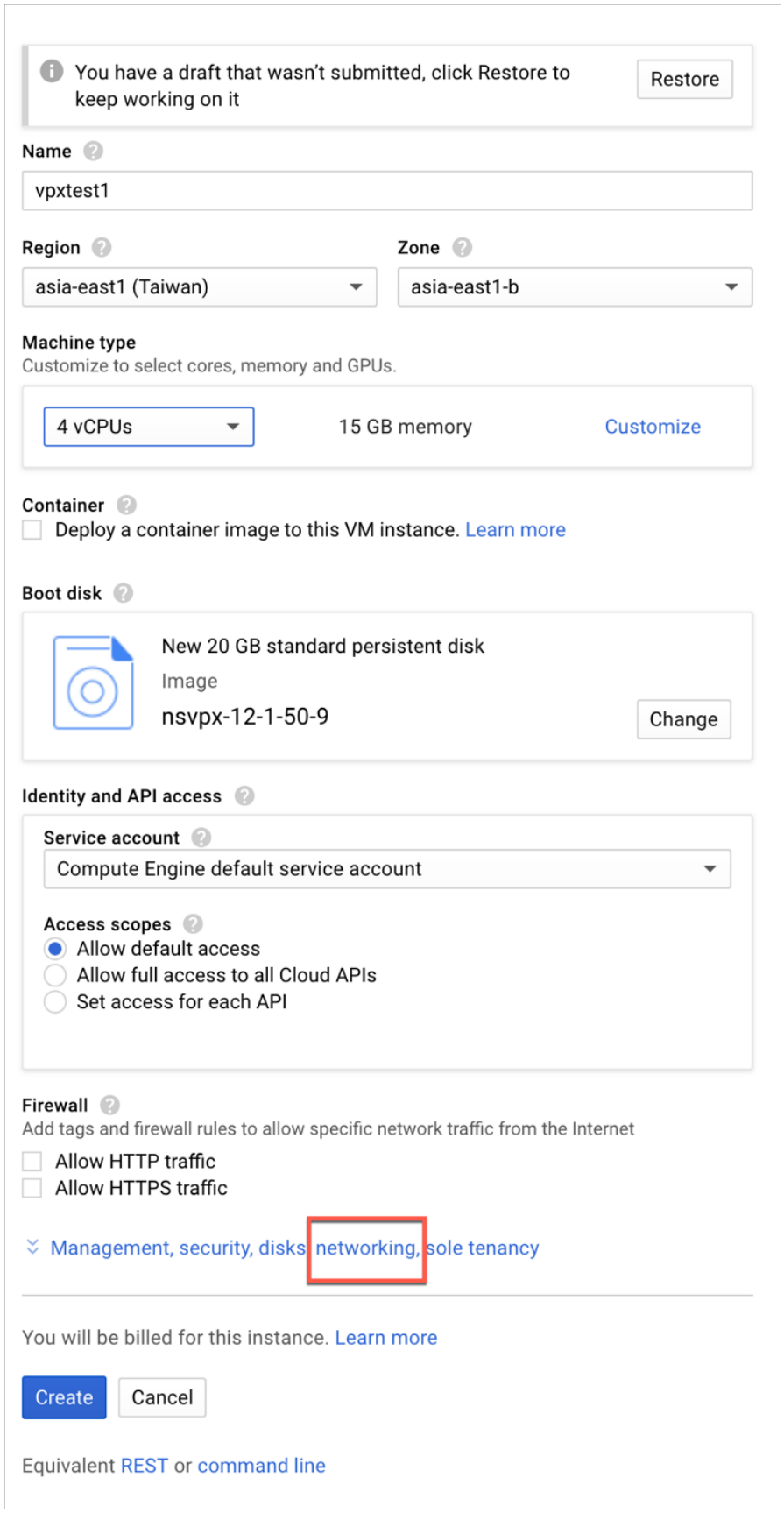
Étape 3. Créez l'instance VPX.

1. Ouvrez une session sur la console GCP.
2. **Sous**Compute**, passez la souris sur Compute Engine, puis sélectionnez Images.**
3. Sélectionnez l'image, puis cliquez sur **Créer une instance**.

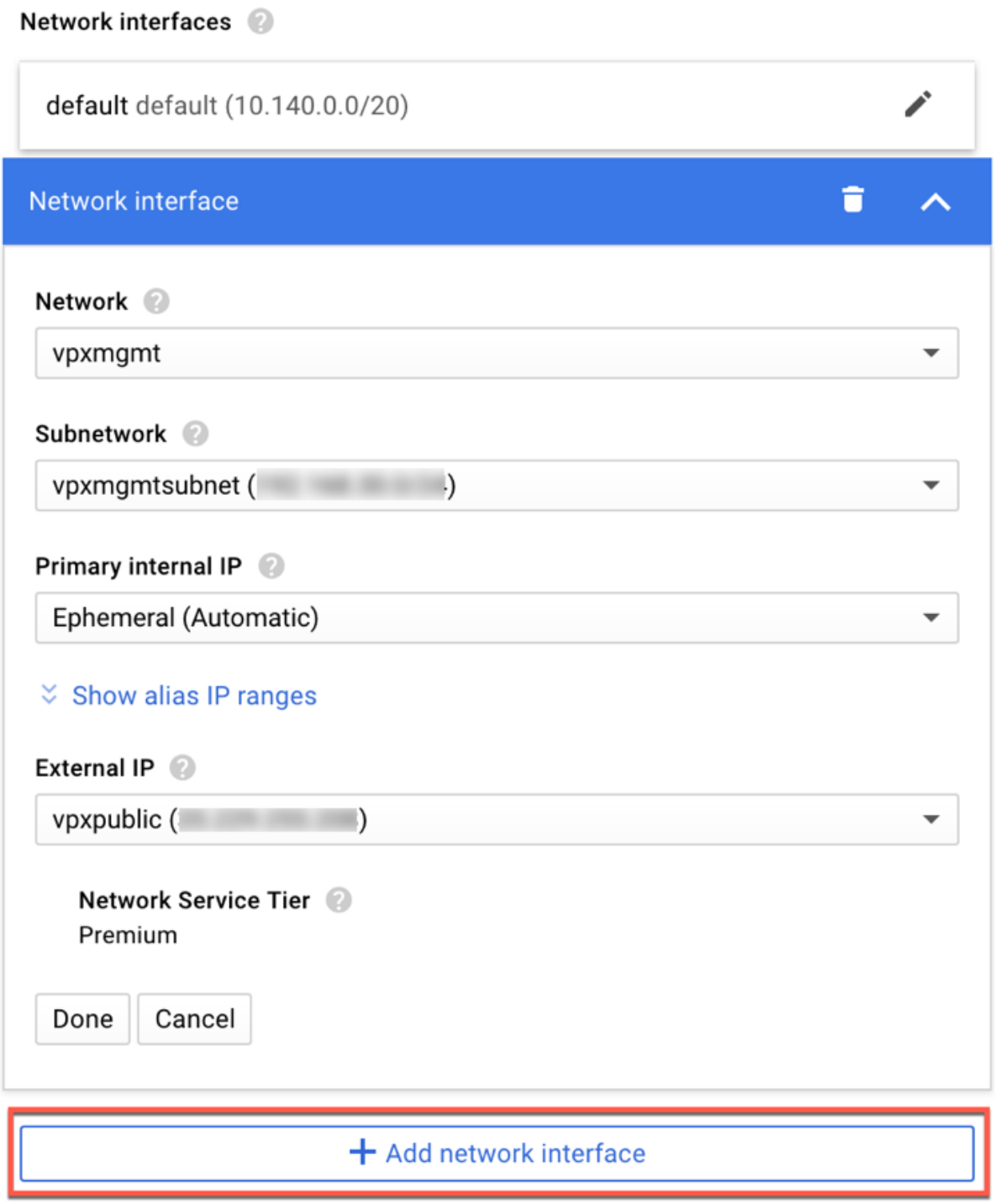


4. Sélectionnez une instance avec 4 vCPU, pour prendre en charge plusieurs cartes réseau.
5. Cliquez sur l'option réseau dans Gestion, sécurité, disques, mise en réseau, location unique pour ajouter les cartes réseau supplémentaires.

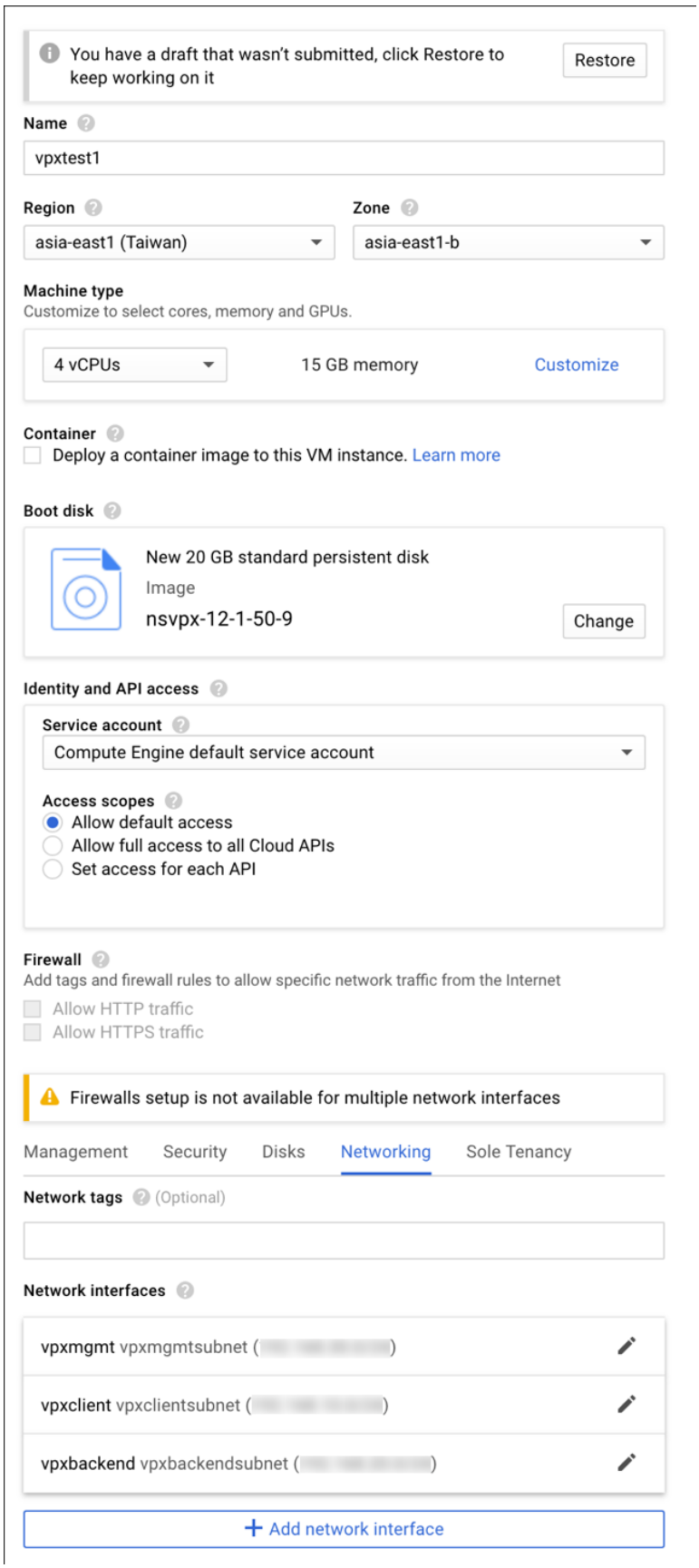
> **Remarque :**
>
> L'image de conteneur n'est pas prise en charge sur les instances VPX sur GCP.



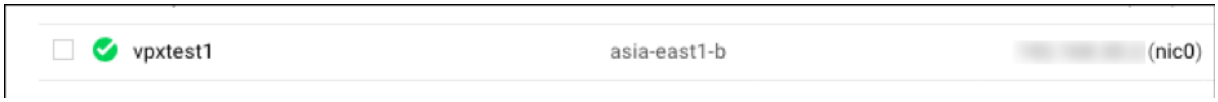
6. Sous **Interfaces réseau**, cliquez sur l'icône Modifier pour modifier la carte réseau par défaut. Cette carte réseau est la carte réseau de gestion.
7. Dans la fenêtre **Interfaces réseau**, sous **Réseau**, sélectionnez le réseau VPC que vous avez créé pour la carte réseau de gestion.
8. Pour la carte réseau de gestion, créez une adresse IP externe statique. Dans la liste des adresses IP externes, cliquez sur **Créer une adresse IP**.
9. Dans la fenêtre **Réserver une nouvelle adresse IP statique**, ajoutez un nom et une description, puis cliquez sur **Réserver**.
10. Cliquez sur **Ajouter une interface réseau** pour créer des cartes réseau pour un trafic côté client et serveur.



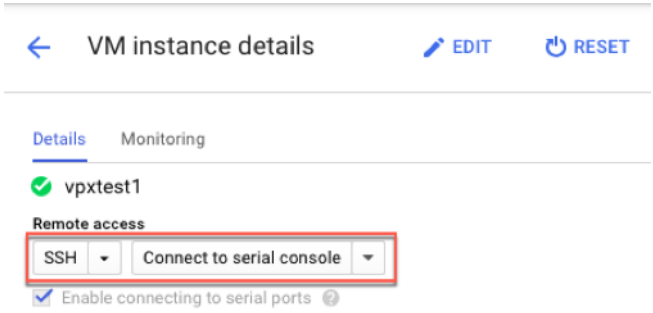
Après avoir créé toutes les cartes réseau, cliquez sur **Créer** pour créer l'instance VPX.



L'instance s'affiche sous **Instances de VM**.

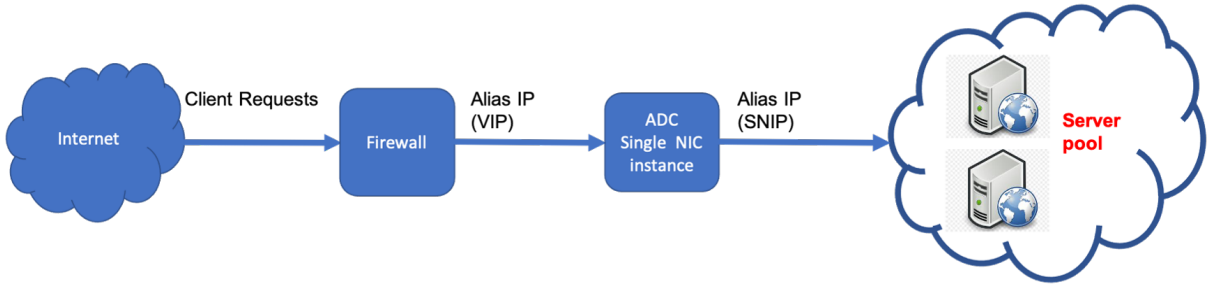


Utilisez le SSH GCP ou la console série pour configurer et gérer l'instance VPX.



Scénario : Déployer une instance VPX autonome à une seule carte réseau

Ce scénario montre comment déployer une instance autonome NetScaler VPX avec une seule carte réseau dans GCP. Les adresses IP d'alias sont utilisées pour réaliser ce déploiement.



Créez une carte réseau unique (NIC0) pour répondre aux objectifs suivants :

- Gérez le trafic de gestion (NetScaler IP) dans le réseau de gestion.
- Gérez le trafic côté client (VIP) dans le réseau client.
- Communiquez avec les serveurs principaux (SNIP) du réseau de serveurs principaux.

Configurez les routes de communication requises entre les éléments suivants :

- L'instance et les serveurs principaux.
- Instance et les hôtes externes sur l'Internet public.

Résumé des étapes de déploiement

1. Créez un réseau VPC pour NIC0.
2. Créez des règles de pare-feu pour les ports 22, 80 et 443.

3. Créez une instance avec une seule carte réseau.
4. Ajoutez des adresses IP d'alias à VPX.
5. Ajoutez VIP et SNIP sur VPX.
6. Ajoutez un serveur virtuel d'équilibrage de charge.
7. Ajoutez un service ou un groupe de services sur l'instance.
8. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur l'instance.

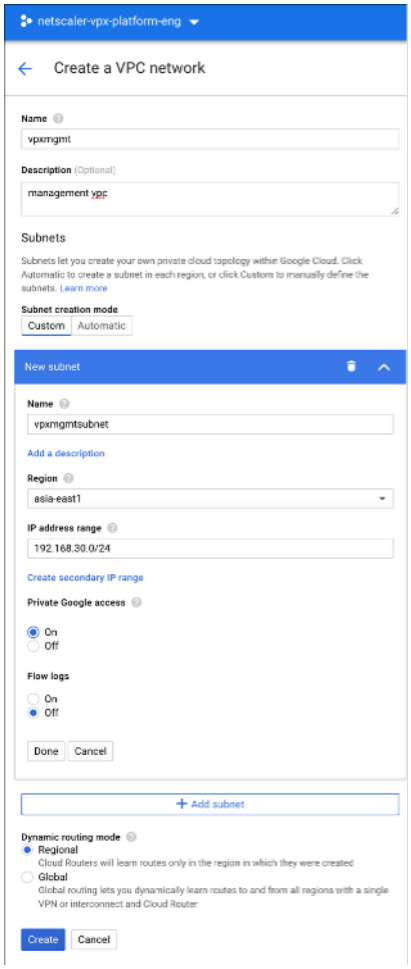
> **Remarque** :
>
> Créez une instance dans la même région que celle où vous avez créé les réseaux VPC.

Étape 1. Créez un réseau VPC.

Créez un réseau VPC à associer à NIC0.

Pour créer un réseau VPC, procédez comme suit :

1. Ouvrez une session sur **la console GCP > Mise en réseau > Réseau VPC > Créer un réseau VPC**
2. Remplissez les champs requis, puis cliquez sur **Créer**.



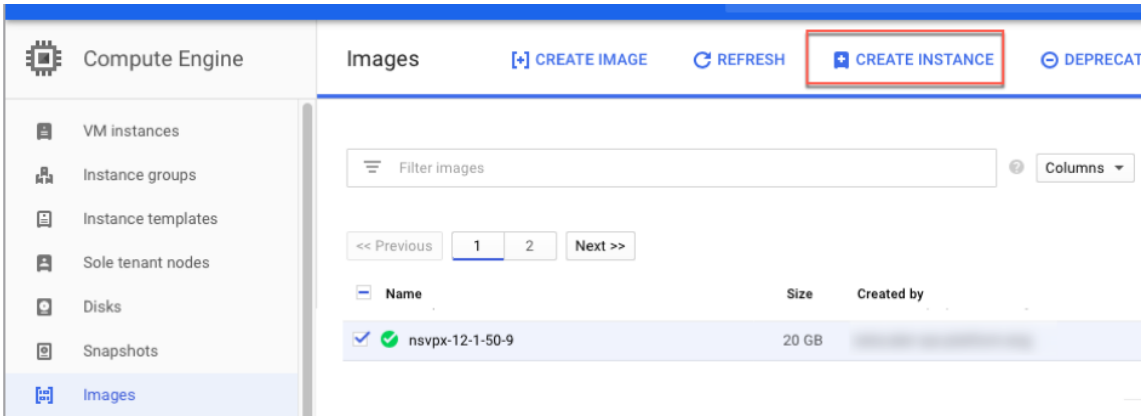
Étape 2. Créez des règles de pare-feu pour les ports 22, 80 et 443.

Créez des règles pour SSH (port 22), HTTP (port 80) et HTTPS (port 443) pour le réseau VPC. Pour plus d'informations sur les règles de pare-feu, voir Vue d' ensemble des règles de pare-feu.

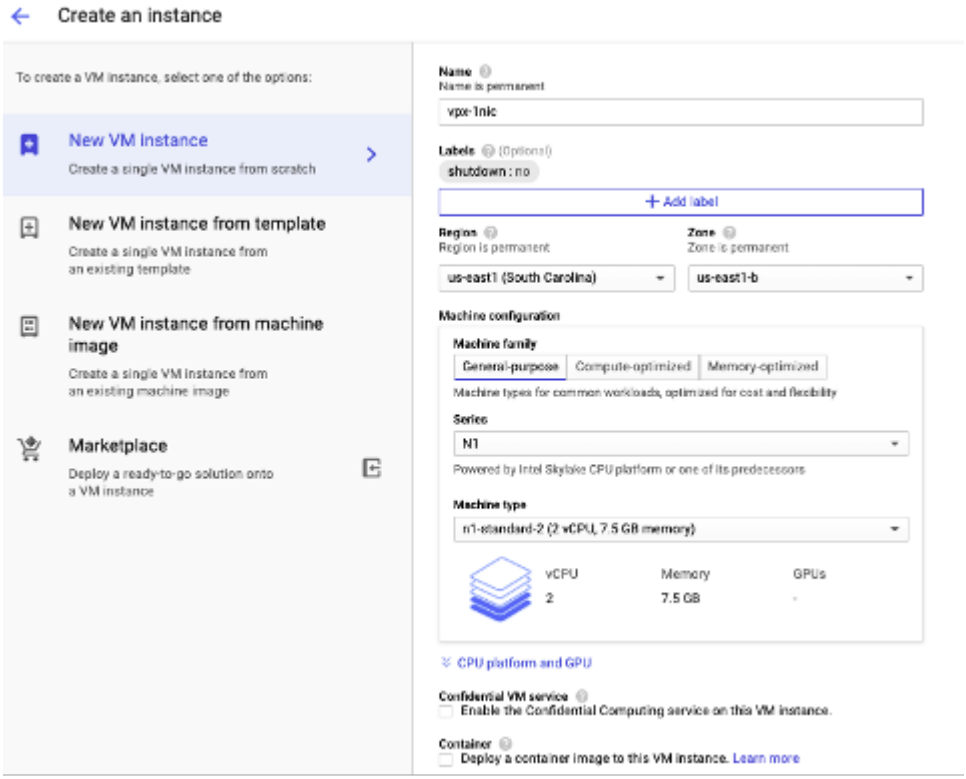
Étape 3. Créez une instance avec une seule carte réseau.

Pour créer une instance avec une seule carte réseau, procédez comme suit :

1. Ouvrez une session sur la **console GCP**.
2. Sous **Compute**, passez la souris sur **Compute Engine**et sélectionnez **Images**.
3. Sélectionnez l'image, puis cliquez sur **Créer une instance**.



4. Sélectionnez un type d'instance avec deux vCPU (configuration minimale pour l'ADC).



5. Cliquez sur l'onglet **Mise en réseau** dans la fenêtre **Gestion, sécurité, disques, mise en réseau** .
6. Sous **Interfaces réseau**, cliquez sur l'icône **Modifier** pour modifier la carte réseau par défaut.
7. Dans la fenêtre **Interfaces réseau**, sous **Réseau**, sélectionnez le réseau VPC que vous avez créé.
8. Vous pouvez créer une adresse IP externe statique. Sous **Adresses IP externes**, cliquez sur **Créer une adresse IP**.
9. Dans la fenêtre **Réserver une adresse statique**, ajoutez un nom et une description, puis cliquez sur **Réserver**.

10. Cliquez sur **Créer** pour créer l'instance VPX.
    La nouvelle instance s'affiche sous Instances de machines virtuelles.

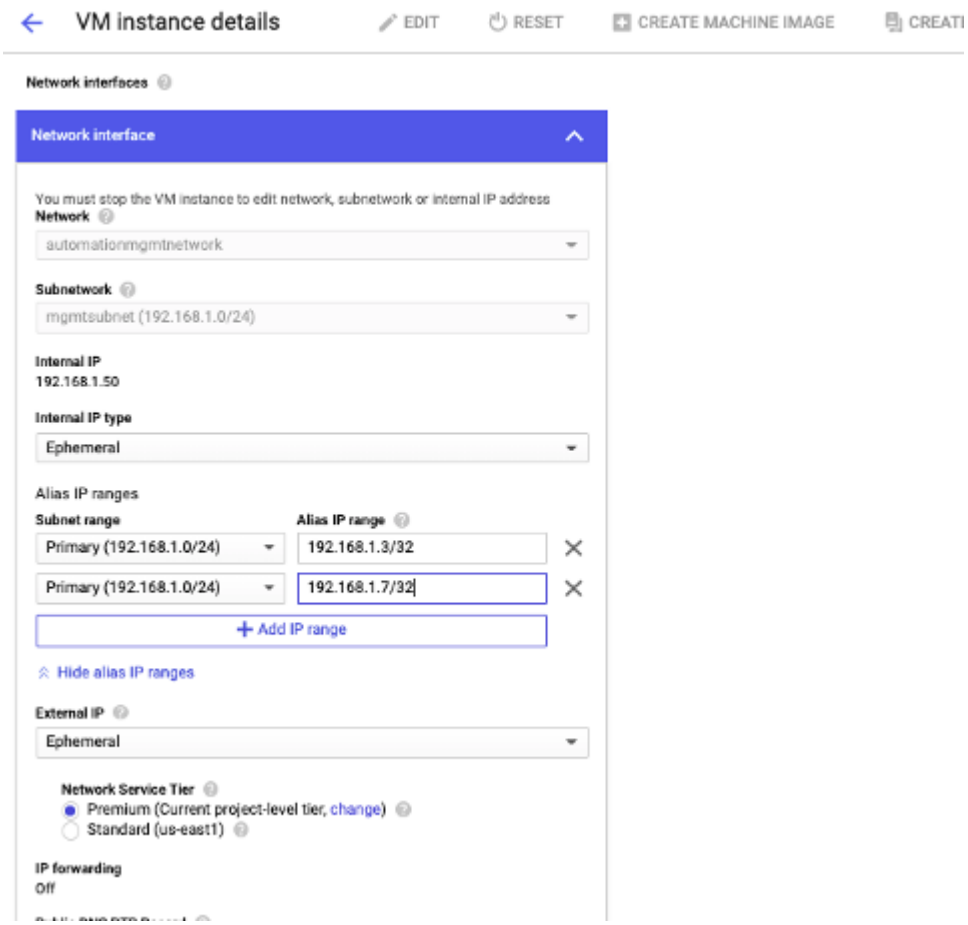
Étape 4. Ajoutez des adresses IP d'alias à l'instance VPX.

Affectez deux adresses IP d'alias à l'instance VPX à utiliser comme adresses VIP et SNIP.

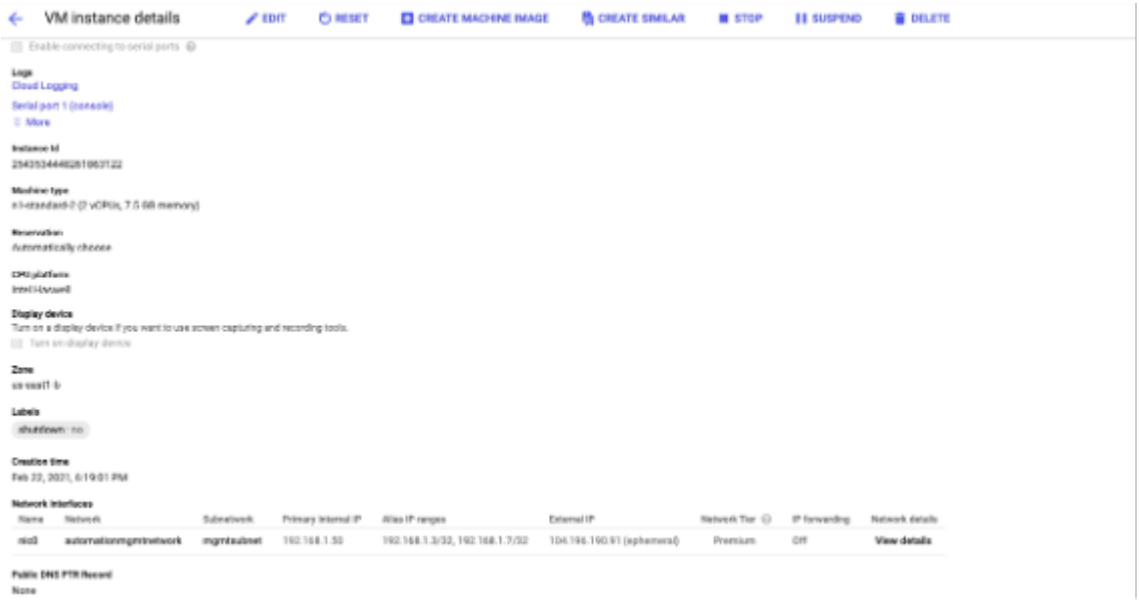
> **Remarque :**
>
> N'utilisez pas l'adresse IP interne principale de l'instance VPX pour configurer l'adresse IP virtuelle ou le SNIP.

Pour créer une adresse IP d'alias, procédez comme suit :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface NIC0.
3. Dans le champ **Plage d'adresses IP d'alias**, saisissez les adresses IP d'alias.



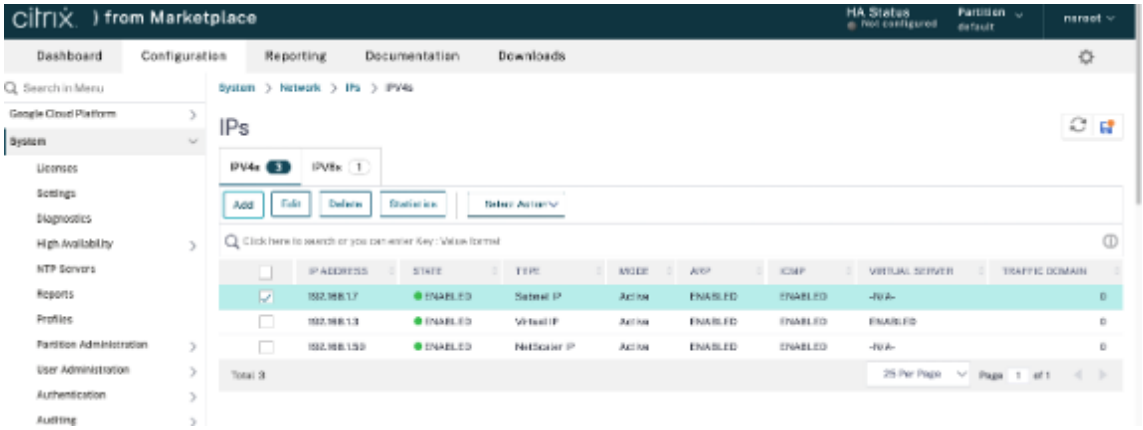
4. Cliquez sur **Terminé**, puis sur **Enregistrer**.
5. Vérifiez les adresses IP d'alias sur la page de **détails de l'instance de machine virtuelle** .



Étape 5. Ajoutez VIP et SNIP sur l'instance VPX.

Sur l'instance VPX, ajoutez l'adresse IP d'alias client et l'adresse IP d'alias de serveur.

1. **Sur l'interface graphique de NetScaler, accédez à**Système > Réseau > IP > IPv4S**, puis cliquez sur Ajouter.**

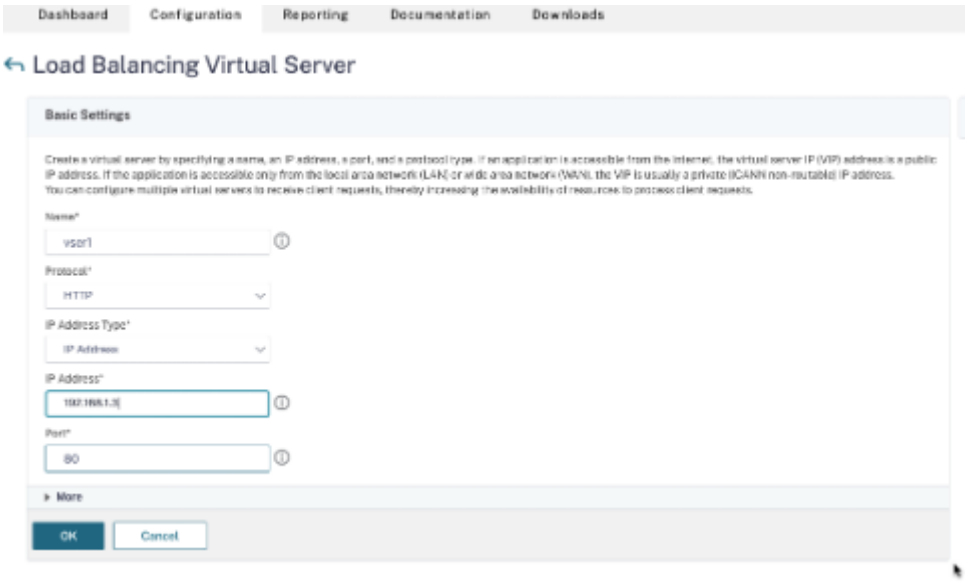


2. Pour créer une adresse IP (VIP) alias client :
   - Entrez l'adresse IP d'alias client et le masque de réseau configurés pour le sous-réseau VPC dans l'instance de machine virtuelle.
   - Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
   - Cliquez sur **Create**.
3. Pour créer une adresse IP d'alias de serveur (SNIP) :
   - Entrez l'adresse IP et le masque de réseau d'alias de serveur configurés pour le sous-réseau VPC dans l'instance de machine virtuelle.
   - Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.

- Cliquez sur **Create**.

Étape 6. Ajoutez un serveur virtuel d'équilibrage de charge.

1. **Sur l'interface graphique de NetScaler, accédez à**Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis cliquez sur Ajouter.**
2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (adresse IP d'alias client) et le port.
3. Cliquez sur **OK** pour créer le serveur virtuel d'équilibrage de charge.



Étape 7. Ajoutez un service ou un groupe de services sur l'instance VPX.

1. **Dans l'interface graphique de NetScaler, accédez à**Configuration > Gestion du trafic > Équilibrage de charge > Services**, puis cliquez sur Ajouter.**
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 8. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance.

1. À partir de l'interface graphique, accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 6**, puis cliquez sur **Modifier**.
3. Dans la fenêtre **Services et groupes de services**, cliquez sur **Liaison de service de serveur virtuel sans équilibrage**de charge.
4. Sélectionnez le service configuré à l' **étape 7**, puis cliquez sur **Lier**.

Points à noter après le déploiement de l'instance VPX sur GCP

- Connectez-vous au VPX avec le nom d'utilisateur `nsroot` et l'ID d'instance comme mot de passe. À l'invite, modifiez le mot de passe et enregistrez la configuration.
- Pour collecter un bundle de support technique, exécutez la commande `shell /netscaler/showtech_cloud.pl` au lieu de la commande habituelle `show techsupport`.
- Après avoir supprimé une machine virtuelle NetScaler de la console GCP, supprimez également l'instance cible interne NetScaler associée. Pour ce faire, accédez à l'interface de ligne de commande gcloud et tapez la commande suivante :

```
1 gcloud compute -q  target-instances delete <instance-name>-
     adcinternal --zone <zone>
2 <!--NeedCopy-->
```

> **Remarque :**
>
> `<instance-name>-adcinternal` est le nom de l'instance cible qui doit être supprimée.

Licence NetScaler VPX

Une instance NetScaler VPX sur GCP nécessite une licence. Les options de licence suivantes sont disponibles pour les instances NetScaler VPX exécutées sur GCP.

- **Licences basées sur un abonnement** : les appliances NetScaler VPX sont disponibles sous forme d'instances payantes sur la place de marché GCP. Les licences par abonnement sont une option de paiement à l'utilisation. Les utilisateurs sont facturés à l'heure. Les modèles VPX et les éditions de licences suivants sont disponibles sur le marché GCP.

Modèle VPX	Éditions sous licence
VPX10, VPX200, VPX1000, VPX3000, VPX5000	Standard, Avancé, Premium

- **Apportez votre propre licence (BYOL)** : Si vous apportez votre propre licence (BYOL), consultez le guide des licences VPX à l'adresse http://support.citrix.com/article/CTX122426. Vous devez :
  - Utilisez le portail de licences sur le site Web Citrix pour générer une licence valide.
  - Télécharger la licence sur l'instance.
- Licence**NetScaler VPX Check-In/Check-Out : pour plus d'informations, consultez la section Licences NetScaler VPX Check-In/Check-Out**.

VPX Express pour les déploiements sur site et dans le cloud ne nécessite pas de fichier de licence. Pour plus d'informations sur NetScaler VPX Express, consultez la section « Licence NetScaler VPX Express »

dans la vue d'ensemble des licences NetScaler.

Modèles GDM pour déployer une instance NetScaler VPX

Vous pouvez utiliser un modèle NetScaler VPX Google Deployment Manager (GDM) pour déployer une instance VPX sur GCP. Pour plus de détails, consultez la section Modèles NetScaler GDM.

Images de NetScaler Marketplace

Vous pouvez utiliser les images des modèles GDM pour faire apparaître l'appliance NetScaler.

Le tableau suivant répertorie les images disponibles sur le marché GCP.

Libérer	Nom de l'image	Emplacement de l'image
13.0	citrix-adc-vpx-10-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-enterprise-13-0-83-29
13.0	citrix-adc-vpx-10-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-platinum-13-0-83-29
13.0	citrix-adc-vpx-10-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-standard-13-0-83-29
13.0	citrix-adc-vpx-200-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-0-83-29
13.0	citrix-adc-vpx-200-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-platinum-13-0-83-29
13.0	citrix-adc-vpx-200-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-standard-13-0-83-29

Libérer	Nom de l'image	Emplacement de l'image
13.0	citrix-adc-vpx-1000-advanced-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-advanced-13-0-83-29
13.0	citrix-adc-vpx-1000-premium-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-premium-13-0-83-29
13.0	citrix-adc-vpx-1000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-standard-13-0-83-29
13.0	citrix-adc-vpx-3000-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-enterprise-13-0-83-29
13.0	citrix-adc-vpx-3000-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-platinum-13-0-83-29
13.0	citrix-adc-vpx-3000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-standard-13-0-83-29
13.0	citrix-adc-vpx-5000-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-enterprise-13-0-83-29
13.0	citrix-adc-vpx-5000-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-0-83-29
13.0	citrix-adc-vpx-5000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-standard-13-0-83-29

Libérer	Nom de l'image	Emplacement de l'image
13.0	citrix-adc-vpx-byol-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-0-83-29
13.0	citrix-adc-vpx-express-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-0-83-29
13.0	citrix-adc-vpx-waf-1000-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-waf-1000-13-0-83-29
13.1	citrix-adc-vpx-10-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-10-enterprise-13-1-9-60
13.1	citrix-adc-vpx-10-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-10-platinum-13-1-9-60
13.1	citrix-adc-vpx-10-standard-13-1-9-60	projects/citrix-master-project/global/imagescitrix-adc-vpx-10-standard-13-1-9-60
13.1	citrix-adc-vpx-200-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-1-9-60
13.1	citrix-adc-vpx-200-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-200-platinum-13-1-9-60
13.1	citrix-adc-vpx-200-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-200-standard-13-1-9-60

Libérer	Nom de l'image	Emplacement de l'image
13.1	citrix-adc-vpx-1000-advanced-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-advanced-13-1-9-60
13.1	citrix-adc-vpx-1000-premium-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-premium-13-1-9-60
13.1	citrix-adc-vpx-1000-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-standard-13-1-9-60
13.1	citrix-adc-vpx-3000-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-enterprise-13-1-9-60
13.1	citrix-adc-vpx-3000-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-platinum-13-1-9-60
13.1	citrix-adc-vpx-3000-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-standard-13-1-9-60
13.1	citrix-adc-vpx-5000-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-enterprise-13-1-9-60
13.1	citrix-adc-vpx-5000-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-1-9-60
13.1	citrix-adc-vpx-5000-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-standard-13-1-9-60

Libérer	Nom de l'image	Emplacement de l'image
13.1	citrix-adc-vpx-byol-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-1-9-60
13.1	citrix-adc-vpx-express-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-1-9-60
13.1	citrix-adc-vpx-waf-1000-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-waf-1000-13-1-9-60

Ressources

- Création d'instances avec plusieurs interfaces réseau
- Création et démarrage d'une instance de machine virtuelle

Informations connexes

- Déployer une paire haute disponibilité VPX sur Google Cloud Platform

Déployer une paire haute disponibilité VPX sur Google Cloud Platform

May 5, 2023

Vous pouvez configurer deux instances NetScaler VPX sur Google Cloud Platform (GCP) en tant que paire active et passive à haute disponibilité (HA). Lorsque vous configurez une instance en tant que nœud principal et l'autre en tant que nœud secondaire, le nœud principal accepte les connexions et gère les serveurs. Le nœud secondaire surveille le principal. Si pour une raison quelconque, si le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Pour plus d'informations sur HA, voir Haute disponibilité.

Les nœuds doivent se trouver dans la même région ; cependant, ils peuvent se trouver soit dans la même zone, soit dans des zones différentes. Pour plus d'informations, voir Régions et zones.

Chaque instance VPX nécessite au moins trois sous-réseaux IP (réseaux Google VPC) :

- Un sous-réseau de gestion
- Un sous-réseau orienté client (VIP)

- Un sous-réseau orienté vers le serveur principal (SNIP, MIP, etc.)

Citrix recommande trois interfaces réseau pour une instance VPX standard.

Vous pouvez déployer une paire VPX à haute disponibilité selon les méthodes suivantes :

- Utilisation d'une adresse IP statique externe
- Utilisation d'une adresse IP privée
- Utilisation de machines virtuelles à carte réseau unique avec adresse IP privée

Modèles GDM pour déployer une paire VPX à haute disponibilité sur GCP

Vous pouvez utiliser un modèle NetScaler Google Deployment Manager (GDM) pour déployer une paire de haute disponibilité VPX sur GCP. Pour plus de détails, consultez la section Modèles NetScaler GDM.

Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP

Vous pouvez déployer une paire VPX haute disponibilité sur le GCP à l'aide de règles de transfert.

Pour plus d'informations sur les règles de transfert, voir Vue d'ensemble des règles de transfert.

Composants requis

- Les règles de transfert doivent se situer dans la même région que les instances VPX.
- Les instances cibles doivent se trouver dans la même zone que l'instance VPX.
- Le nombre d'instances cibles pour les nœuds principal et secondaire doit correspondre.

Exemple :

Vous disposez d'une paire à haute disponibilité dans la `us-east1` région avec un VPX principal dans la `us-east1-b` zone et un VPX secondaire dans la `us-east1-c` zone. Une règle de transfert est configurée pour le VPX principal avec l'instance cible dans la `us-east1-b` zone. Configurez une instance cible pour le VPX secondaire dans la `us-east1-c` zone afin de mettre à jour la règle de transfert en cas de basculement.

Limitations

Seules les règles de transfert configurées avec des instances cibles en arrière-plan sont prises en charge dans le déploiement à haute disponibilité de VPX.

Déployer une paire haute disponibilité VPX avec une adresse IP statique externe sur Google Cloud Platform

May 5, 2023

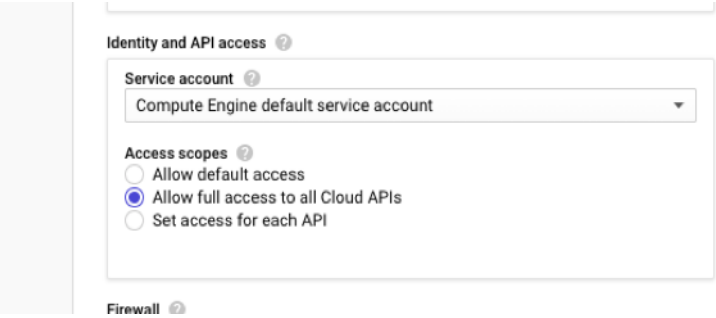
Vous pouvez déployer une paire haute disponibilité VPX sur GCP à l'aide d'une adresse IP statique externe. L'adresse IP du client du nœud principal doit être liée à une adresse IP statique externe. Lors du basculement, l'adresse IP statique externe est déplacée vers le nœud secondaire pour que le trafic reprenne.

Une adresse IP externe statique est une adresse IP externe qui est réservée à votre projet jusqu'à ce que vous décidiez de la publier. Si vous utilisez une adresse IP pour accéder à un service, vous pouvez réserver cette adresse IP afin que seul votre projet puisse l'utiliser. Pour plus d'informations, voir Réserver une adresse IP externe statique.

Pour plus d'informations sur HA, voir Haute disponibilité.

Avant de commencer

- Lisez les limitations, les exigences matérielles et les points à noter mentionnés dans Déployer une instance NetScaler VPX sur GoogleCloud Platform. Ces informations s'appliquent également aux déploiements HA.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



- Assurez-vous que le rôle IAM associé à votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.addresses.use",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata"
```



```
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.instances.get",
"Compute.instances.list",
"compute.networks.useExternalIp",
"compute.subnetworks.useExternalIp",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
<!--NeedCopy-->
```

- Si vous avez configuré des adresses IP d'alias sur une interface autre que l'interface de gestion, assurez-vous que votre compte de service GCP dispose des autorisations IAM supplémentaires suivantes :

```
"compute.instances.updateNetworkInterface"
<!--NeedCopy-->
```

- Si vous avez configuré des règles de transfert GCP sur le nœud principal, lisez les limitations et exigences mentionnées dans Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP pour les mettre à jour vers le nouveau serveur principal lors du basculement.

Comment déployer une paire VPX HA sur Google Cloud Platform

Voici un résumé des étapes de déploiement HA :

1. Créez des réseaux VPC dans la même région. Par exemple, Asie-Est.
2. Créez deux instances VPX (nœuds principal et secondaire) sur la même région. Ils peuvent se trouver dans la même zone ou dans des zones différentes. Par exemple, l'Asie orientale 1a et l'Asie orientale Ib.
3. Configurez les paramètres HA sur les deux instances à l'aide de l'interface graphique NetScaler ou des commandes ADC CLI.

Étape 1. Créer des réseaux VPC

Créez des réseaux VPC en fonction de vos besoins. Citrix vous recommande de créer trois réseaux VPC à associer à une carte réseau de gestion, une carte réseau client et une carte réseau de serveur.

Pour créer un réseau VPC, procédez comme suit :

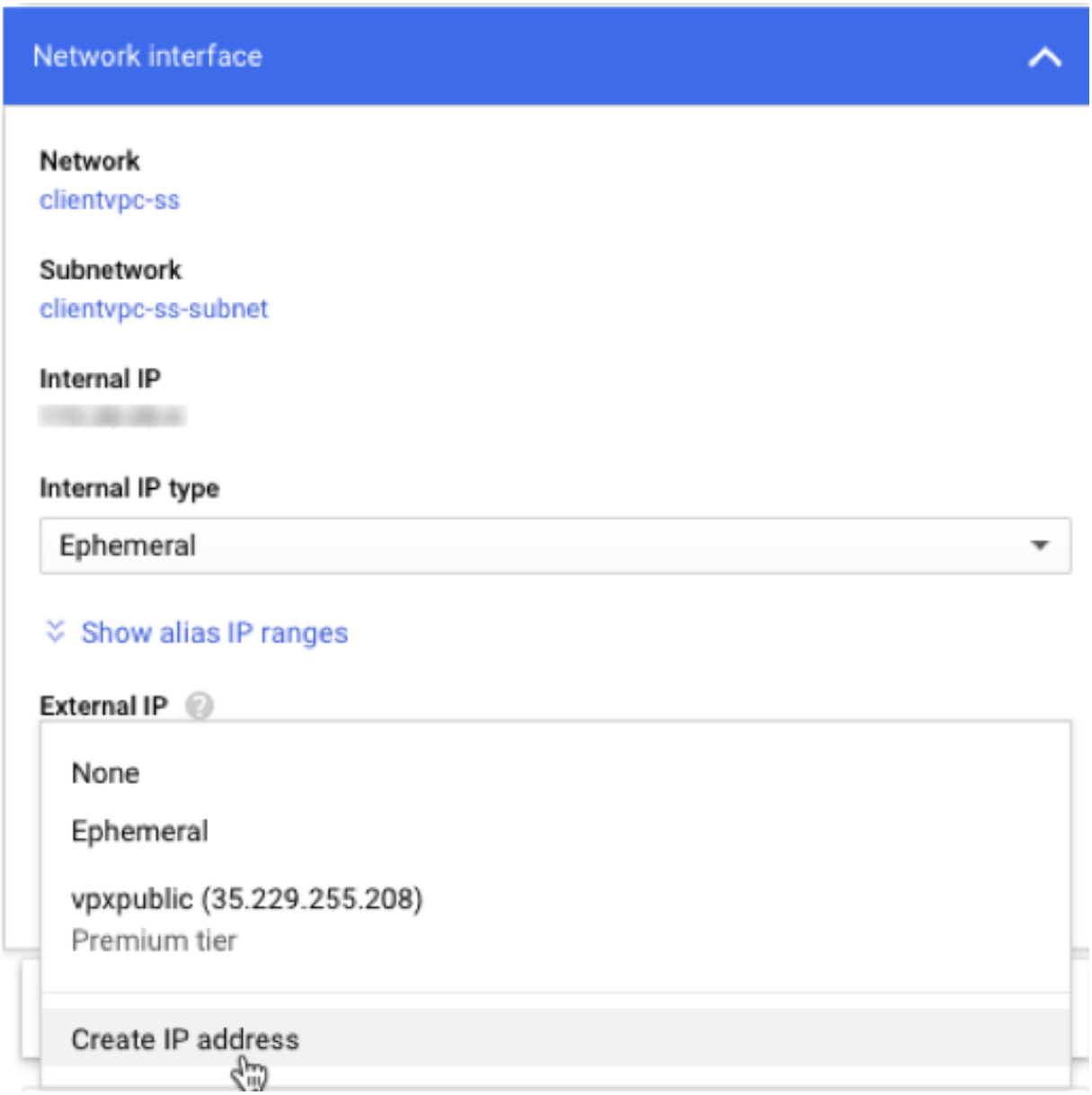
1. Ouvrez une session sur la **console Google > Mise en réseau > Réseau VPC > Créer un réseau VPC**.
2. Remplissez les champs requis, puis cliquez sur **Créer**.

Pour plus d'informations, consultez la section **Créer des réseaux VPC** dans Déployer une instance NetScaler VPX surGoogle Cloud Platform.

Étape 2. Créer deux instances VPX

Créez deux instances VPX en suivant les étapes indiquées dans Scénario : déployer une instance VPX autonome multi-cartes réseau et multi-IP.

> **Important**
>
> Attribuez une adresse IP externe statique à l'adresse IP du client (VIP) du nœud principal. Vous pouvez utiliser une adresse IP réservée existante ou en créer une nouvelle. Pour créer une adresse IP externe statique, accédez à **Interface réseau > IP externe**, cliquez sur **Créer une adresse IP**.



Après le basculement, lorsque l'ancien principal devient le nouveau secondaire, l'adresse IP externe statique se déplace de l'ancien principal et est attachée au nouveau principal. Pour plus d'informations, consultez le document Google Cloud Reserving a Static External IP Address.

Une fois que vous avez configuré les instances VPX, vous pouvez configurer les adresses VIP et SNIP. Pour plus d'informations, consultez la section Configuration des adresses IP appartenant à NetScaler.

Étape 3. Configurer la haute disponibilité

Après avoir créé les instances sur Google Cloud Platform, vous pouvez configurer la haute disponibilité à l'aide de l'interface graphique NetScaler pour CLI.

Configurer HA à l'aide de l'interface graphique

Étape 1. Configurez la haute disponibilité en mode INC sur les deux instances.

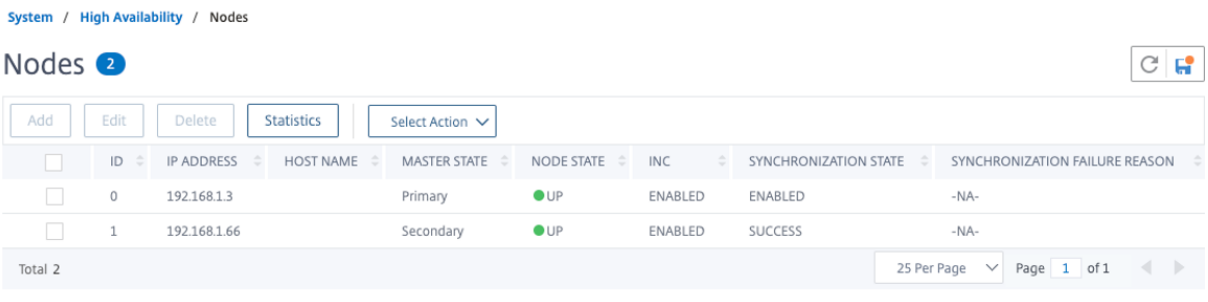
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud principal.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Avant d'aller plus loin, assurez-vous que l'état de synchronisation du nœud secondaire s'affiche comme **SUCCÈS** dans la page **Nœuds** .



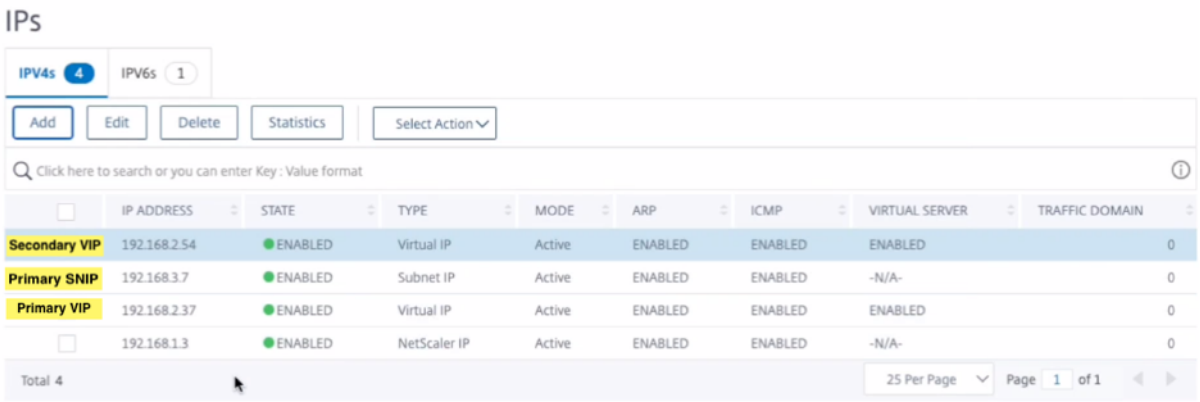
> **Remarque**
>
> Maintenant, le nœud secondaire a les mêmes informations d'identification d'ouverture de session que le nœud principal.

Étape 2 Ajoutez une adresse IP virtuelle et une adresse IP de sous-réseau sur les deux nœuds.

Sur le **nœud principal**, effectuez les opérations suivantes :

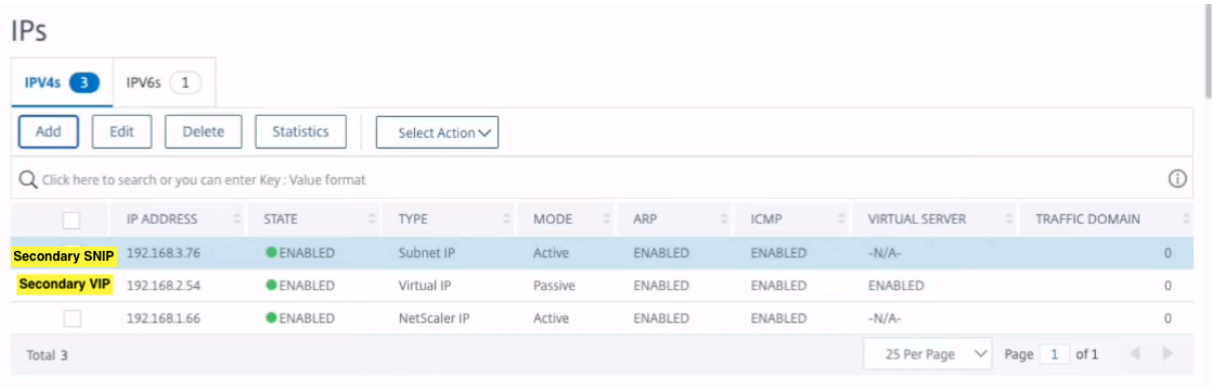
1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.

2. Ajoutez une adresse VIP principale en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée client de l'instance principale et du masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
    c) Cliquez sur **Create**.
3. Ajoutez une adresse SNIP principale en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance principale et du masque de réseau configurés pour le sous-réseau du serveur dans l'instance principale.
    b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
    c) Cliquez sur **Create**.
4. Ajoutez une adresse VIP secondaire en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée client de l'instance secondaire et du masque réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
    c) Cliquez sur **Create**.



Sur le **nœud secondaire**, effectuez les opérations suivantes :

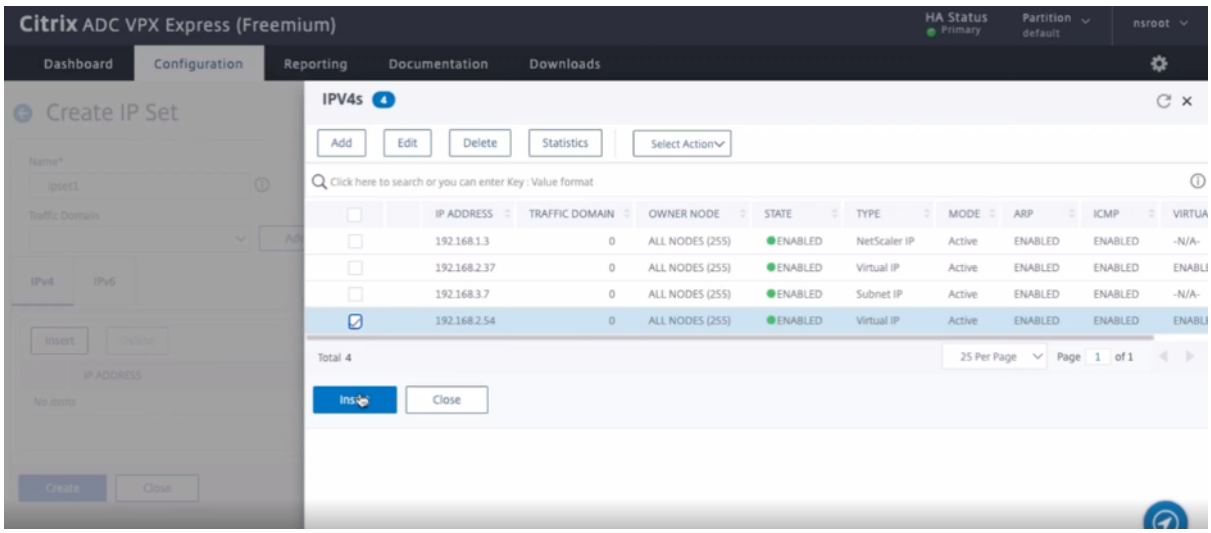
1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Ajoutez une adresse VIP secondaire en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée client de l'instance secondaire et du masque réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
    b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
3. Ajoutez une adresse SNIP secondaire en procédant comme suit :
    a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance secondaire et du masque de réseau configurés pour le sous-réseau du serveur dans l'instance secondaire.
    b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
    c) Cliquez sur **Create**.



Étape 3. Ajoutez un ensemble d'adresses IP et liez le jeu d'adresses IP au VIP secondaire sur les deux instances.

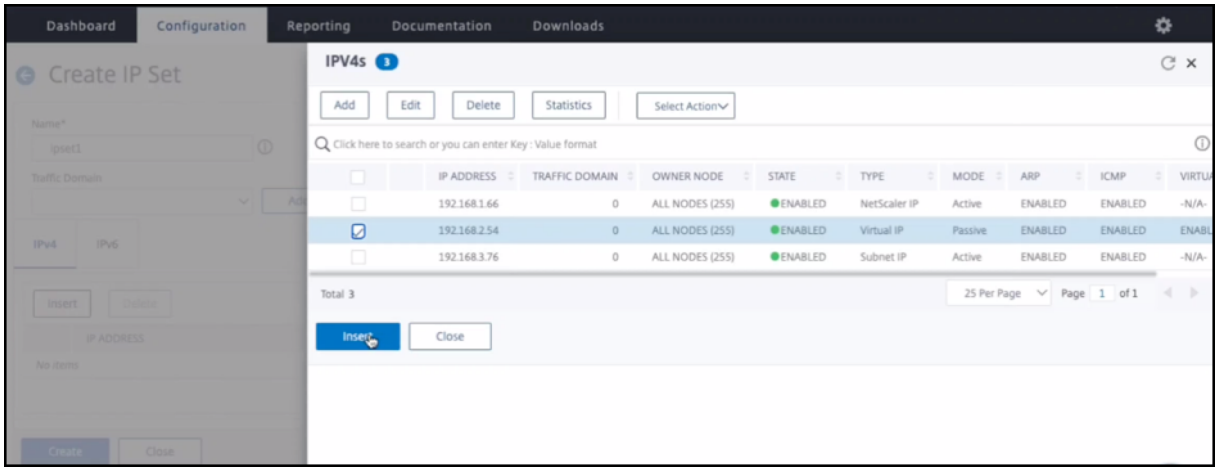
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > Ensembles d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.
4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.



Sur le **nœud secondaire**, effectuez les opérations suivantes :

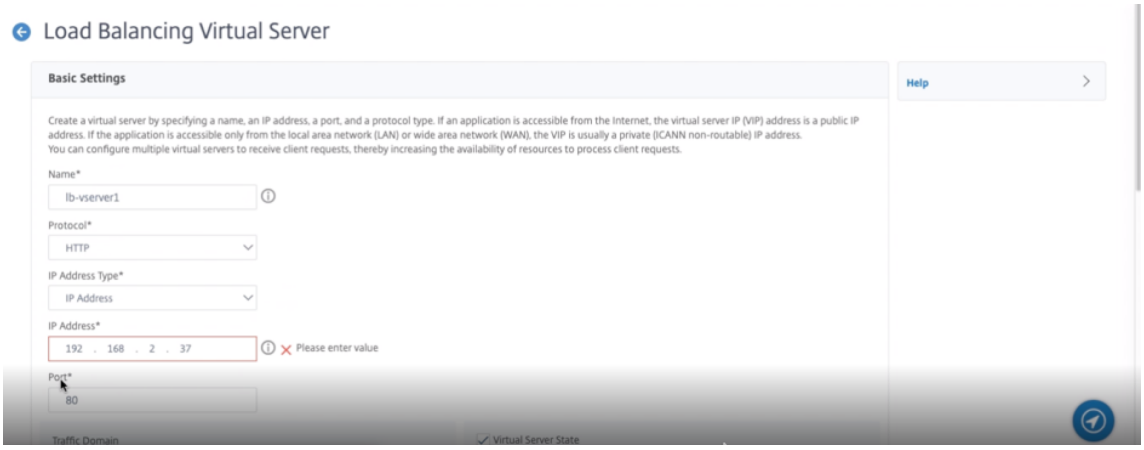
1. Accédez à **Système > Réseau > Ensembles d'adresses IP > Ajouter**.
2. Ajoutez un nom d'ensemble d'adresses IP et cliquez sur **Insérer**.
3. Sur la page **IPv4**, sélectionnez l'IP virtuelle (VIP secondaire) et cliquez sur **Insérer**.
4. Cliquez sur **Créer** pour créer le jeu d'adresses IP.



> **Remarque**
>
> Le nom du jeu d'adresses IP doit être identique sur les deux instances.

Étape 4 Ajoutez un serveur virtuel d'équilibrage de charge sur l'instance principale.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.
2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (VIP principale) et le port.



3. Cliquez sur **Plus**. Accédez à **Paramètres du jeu d'adresses IP de plage IP**, sélectionnez **IPset** dans le menu déroulant et indiquez l'IPSet créé à l' **étape 3**.
4. Cliquez sur **OK** pour créer le serveur virtuel d'équilibrage de charge.

Étape 5. Ajoutez un service ou un groupe de services sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 6. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 4**, puis cliquez sur **Modifier**.
3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l' **étape 5**, puis cliquez sur **Lier**.

Enregistrez la configuration. Après un basculement forcé, le secondaire devient le nouveau principal. L'adresse IP statique externe de l'ancienne VIP principale passe au nouveau VIP secondaire.

Configuration de la haute disponibilité à l'aide de l'interface

Étape 1. Configurez la haute disponibilité en mode INC dans les deux instances.

Sur le nœud principal, tapez la commande suivante.

```
add ha node 1 <sec_ip> -inc ENABLED
<!--NeedCopy-->
```

Sur le nœud secondaire, tapez la commande suivante.

```
add ha node 1 <prim_ip> -inc ENABLED
<!--NeedCopy-->
```

`sec_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud secondaire.

`prim_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud principal.

Étape 2 Ajoutez des IP virtuelles et des adresses IP de sous-réseau sur les deux nœuds.

Sur le nœud principal, tapez la commande suivante.

```
add ns ip <primary_vip> <subnet> -type VIP

add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <primary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

`primary_vip` fait référence à l'adresse IP interne de l'interface orientée client de l'instance principale.

`secondary_vip` fait référence à l'adresse IP interne de l'interface orientée client de l'instance secondaire.

`primary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance principale.

Sur le nœud secondaire, tapez la commande suivante.

```
add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <secondary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

`secondary_vip` fait référence à l'adresse IP interne de l'interface orientée client de l'instance secondaire.

`secondary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance secondaire.

Étape 3. Ajoutez un ensemble d'adresses IP et liez le jeu d'adresses IP à une adresse VIP secondaire sur les deux instances.

Sur le nœud principal, tapez la commande suivante :

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
<!--NeedCopy-->
```

Sur le nœud secondaire, tapez la commande suivante :

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
<!--NeedCopy-->
```

> **Remarque**
>
> Le nom du jeu d'adresses IP doit être identique sur les deux instances.

Étape 4 Ajoutez un serveur virtuel sur l'instance principale.

Exécutez la commande suivante :

```
add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
    > -ipset <ipset_name>
<!--NeedCopy-->
```

Étape 5. Ajoutez un service ou un groupe de services sur l'instance principale.

Exécutez la commande suivante :

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```


Étape 6. Liez le groupe de services/services au serveur virtuel d'équilibrage de charge sur l'instance principale.

Exécutez la commande suivante :

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```

> *Remarque* :
>
> Pour enregistrer votre configuration, tapez la commande `save config`. Sinon, les configurations sont perdues après le redémarrage des instances.

Étape 7. Vérifiez la configuration.

Assurez-vous que l'adresse IP externe attachée à la carte réseau client principale se déplace vers la secondaire lors d'un basculement.

1. Effectuez une requête cURL à l'adresse IP externe et assurez-vous qu'elle est accessible.
2. Sur l'instance principale, effectuez un basculement :

   Depuis l'interface graphique, accédez à **Configuration > Système > Haute disponibilité > Action > Forcer le basculement**.

   À partir de l'interface de ligne de commande, tapez la commande suivante :

   ```
   force ha failover -f
   <!--NeedCopy-->
   ```

   Sur la console GCP, accédez à l'instance secondaire. L'adresse IP externe doit avoir été déplacée vers la carte réseau client de secondaire après basculement.
3. Émettez une requête cURL à l'adresse IP externe et assurez-vous qu'elle est à nouveau accessible.

Déployez une paire de cartes réseau VPX à haute disponibilité unique avec une adresse IP privée sur Google Cloud Platform

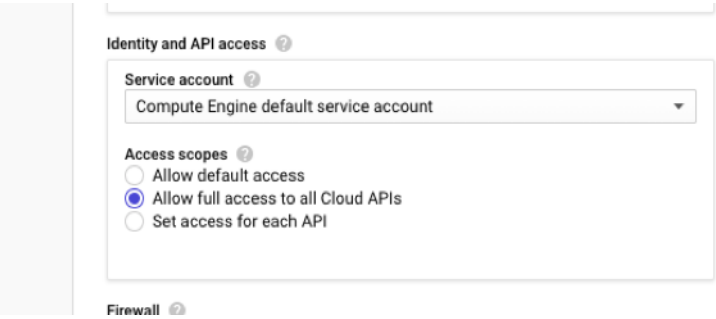
May 5, 2023

Vous pouvez déployer une seule paire de cartes réseau VPX à haute disponibilité sur GCP à l'aide d'une adresse IP privée. L'adresse IP du client (VIP) doit être configurée comme adresse IP d'alias sur le nœud principal. Lors du basculement, l'adresse IP du client est déplacée vers le nœud secondaire, pour que le trafic reprenne. Les adresses IP de sous-réseau (SNiP) de chaque nœud doivent également être configurées en tant que plage d'adresses IP d'alias.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité.

Avant de commencer

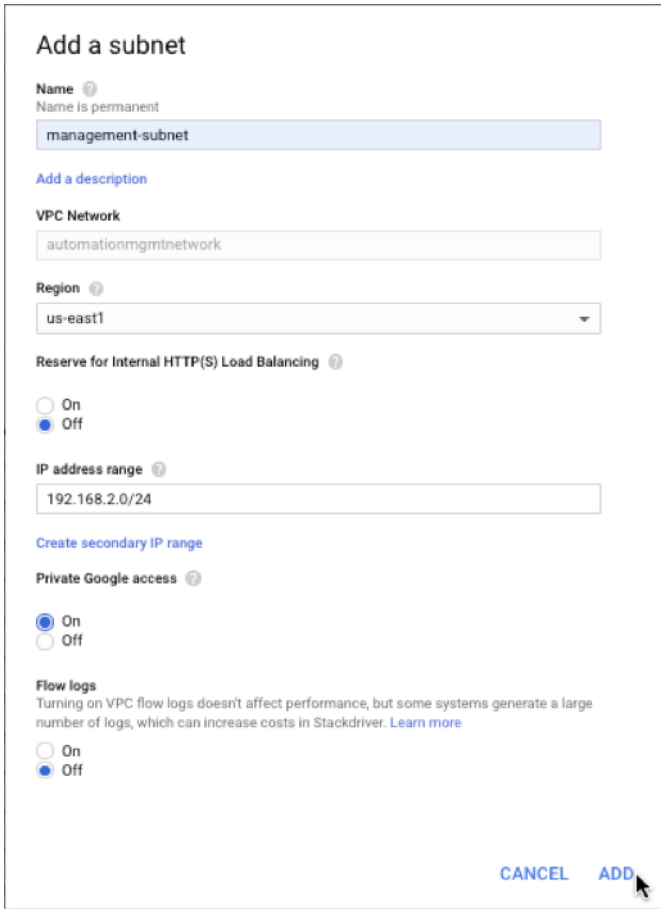
- Lisez les limitations, les exigences matérielles et les points à noter mentionnés dans Déployer une instance NetScaler VPX sur GoogleCloud Platform. Ces informations s'appliquent également aux déploiements haute disponibilité.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
"compute.instances.get",
"compute.instances.list",
"compute.instances.updateNetworkInterface",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
<!--NeedCopy-->
```

- Si vos machines virtuelles n'ont pas accès à Internet, vous devez activer **Private Google Access** sur le sous-réseau VPC.



- Si vous avez configuré des règles de transfert GCP sur le nœud principal, lisez les limitations et exigences mentionnées dans Prise en charge des règles de transfert pour la paire haute disponibilité VPX sur GCP pour les mettre à jour vers le nouveau serveur principal lors du basculement.

Comment déployer une paire haute disponibilité VPX sur Google Cloud Platform

Voici un résumé des étapes à suivre pour déployer une paire HA avec une seule carte réseau :

1. Créez un réseau VPC.
2. Créez deux instances VPX (nœuds principal et secondaire) dans la même région. Ils peuvent se trouver dans la même zone ou dans des zones différentes. Par exemple, l'Asie orientale 1a et l'Asie orientale Ib.
3. Configurez les paramètres HA sur les deux instances à l'aide de l'interface graphique NetScaler ou des commandes ADC CLI.

Étape 1. Création d'un réseau VPC

Pour créer un réseau VPC, procédez comme suit :

1. Connectez-vous à la **console Google > Réseau > Réseau VPC > Créer un réseau VPC**.

2. Remplissez les champs requis, puis cliquez sur **Créer**.

Pour plus d'informations, consultez la section **Créer des réseaux VPC** dans Déployer une instance NetScaler VPX surGoogle Cloud Platform.

Étape 2. Créer deux instances VPX

Créez deux instances VPX en suivant les étapes 1 à 3 décrites dans Scénario : déploiement d'une instance VPX autonome à carte réseau unique.

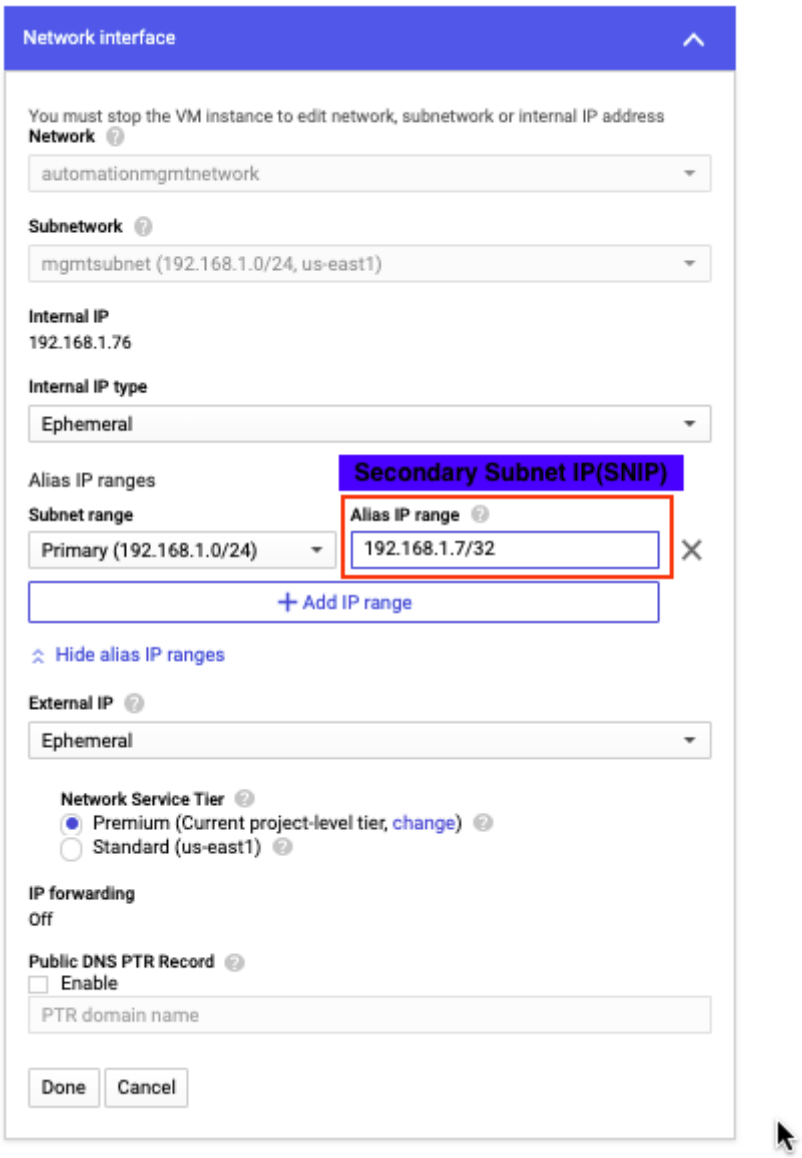
> **Important :**
>
> Attribuez une adresse IP d'alias client uniquement au nœud principal et des adresses IP d'alias de serveur aux nœuds principal et secondaire. N'utilisez pas l'adresse IP interne de l'instance VPX pour configurer le VIP ou le SNIP.

Pour créer des adresses IP d'alias de client et de serveur, effectuez ces étapes sur le nœud principal :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface client (NIC0).
3. Dans le champ **Plage d'adresses IP d'alias**, saisissez l'adresse IP de l'alias du client.
4. Cliquez sur **Ajouter une plage d'adresses IP** et entrez l'adresse IP de l'alias du serveur.

Pour créer une adresse IP d'alias de serveur, effectuez ces étapes sur le nœud secondaire :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface client (NIC0).
3. Dans le champ **Plage d'adresses IP d'alias**, entrez l'adresse IP de l'alias du serveur.



Après le basculement, lorsque l'ancien serveur principal devient le nouveau serveur secondaire, l'adresse IP de l'alias du client est déplacée de l'ancien serveur principal et est associée au nouveau serveur principal.

Une fois que vous avez configuré les instances VPX, vous pouvez configurer les adresses IP virtuelles (VIP) et SNIP (Subnet IP). Pour plus d'informations, consultez la section Configuration des adresses IP appartenant à NetScaler.

Étape 3. Configurer la haute disponibilité

Après avoir créé les instances sur Google Cloud Platform, vous pouvez configurer la haute disponibilité à l'aide de l'interface graphique ou de la CLI de NetScaler.

Configurer la haute disponibilité à l'aide de l'interface graphique

Étape 1. Configurez la haute disponibilité en mode INC Enabled sur les deux nœuds.

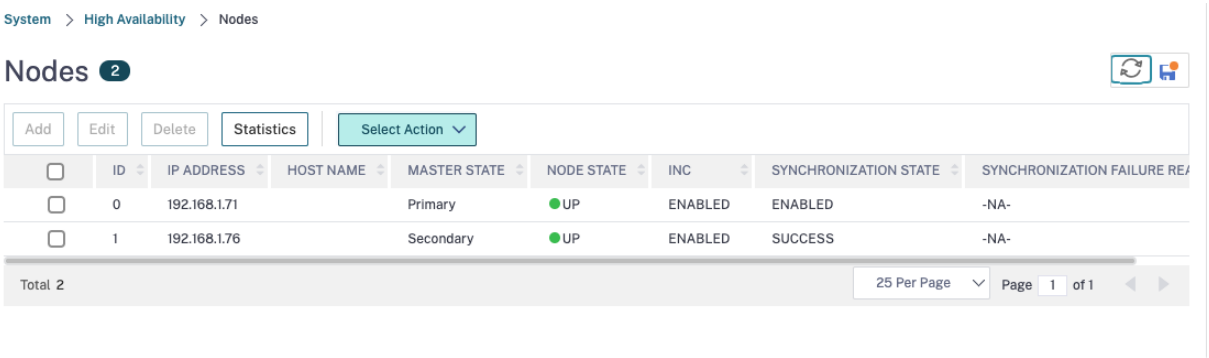
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud principal.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Avant d'aller plus loin, assurez-vous que l'état de synchronisation du nœud secondaire s'affiche comme **SUCCÈS** dans la page **Nœuds** .

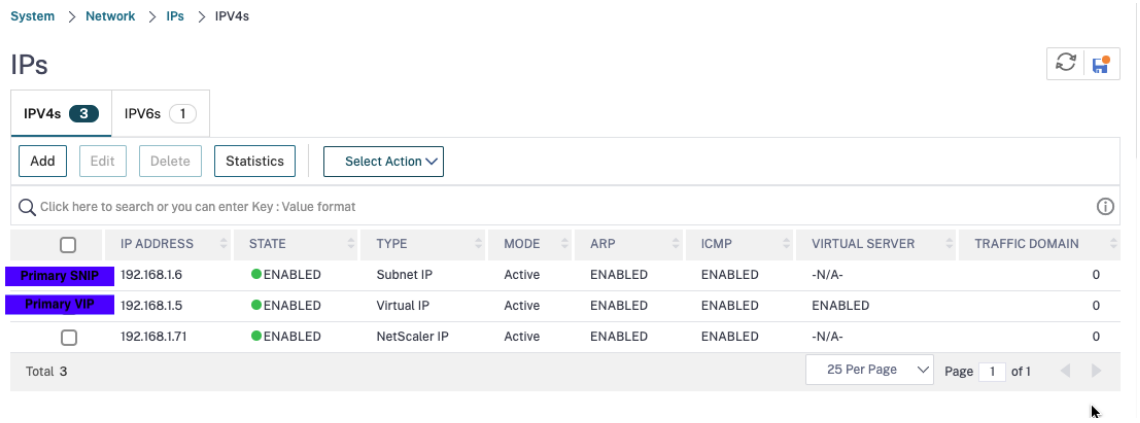


> **Remarque :**
>
> Une fois le nœud secondaire synchronisé avec le nœud principal, le nœud secondaire possède les mêmes informations de connexion que le nœud principal.

Étape 2 Ajoutez une adresse IP virtuelle et une adresse IP de sous-réseau sur les deux nœuds.

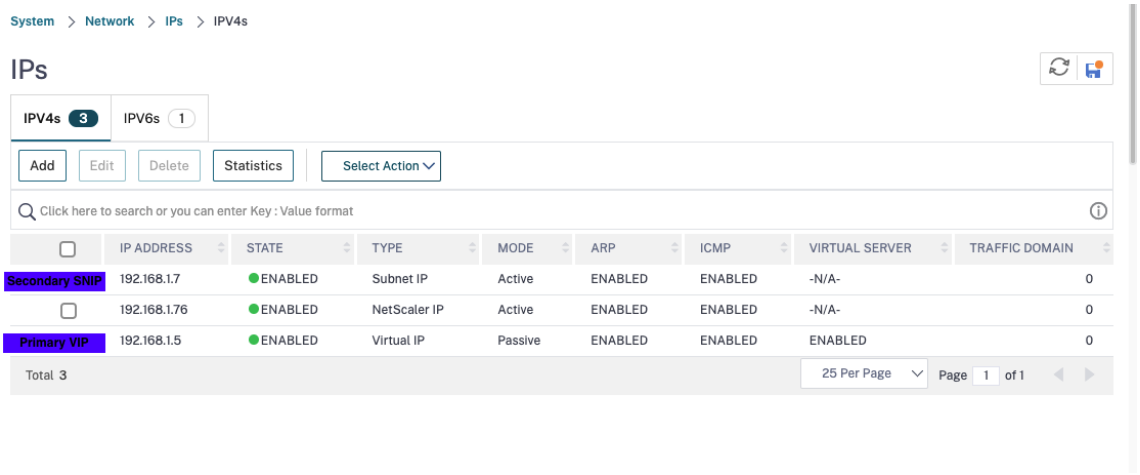
Sur le nœud principal, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :
   a) Entrez l'alias du client, l'adresse IP et le masque de réseau configurés pour le sous-réseau VPC dans l'instance de machine virtuelle principale.
   b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
   c) Cliquez sur **Create**.
3. Pour créer une adresse IP d'alias de serveur (SNIP) :
   a) Entrez l'alias du serveur, l'adresse IP et le masque de réseau configurés pour le sous-réseau VPC dans l'instance de machine virtuelle principale.
   b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
   c) Cliquez sur **Create**.



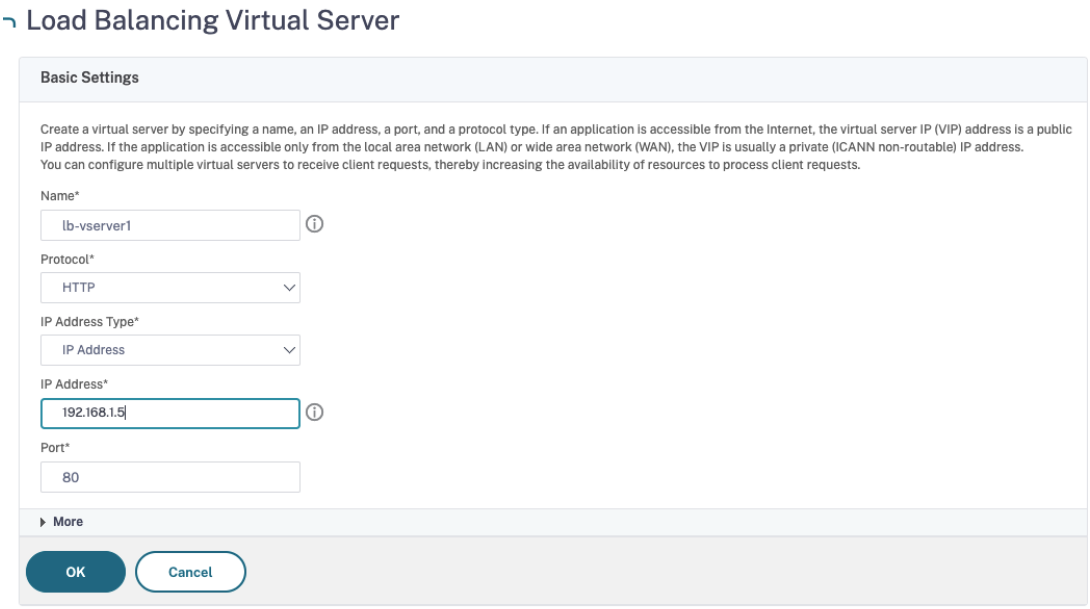
Sur le nœud secondaire, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :
   a) Entrez l'alias du client, l'adresse IP et le masque de réseau configurés pour le sous-réseau VPC de l'instance de machine virtuelle principale.
   b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
   c) Cliquez sur **Create**.
3. Pour créer une adresse IP d'alias de serveur (SNIP) :
   a) Entrez l'alias du serveur, l'adresse IP et le masque de réseau configurés pour le sous-réseau VPC de l'instance de machine virtuelle secondaire.
   b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
   c) Cliquez sur **Create**.



Étape 3. Ajoutez un serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.
2. Ajoutez les valeurs requises pour Nom, Protocole, Type d'adresse IP (adresse IP), Adresse IP (adresse IP de l'alias principal du client) et Port, puis cliquez sur **OK**.



Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 5. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 3**, puis cliquez sur **Modifier**.
3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l'**étape 4**, puis cliquez sur **Lier**.

Étape 6. Enregistrez la configuration.

Après un basculement forcé, le secondaire devient le nouveau principal. L'adresse IP d'alias client (VIP) de l'ancien serveur principal est transférée vers le nouveau serveur principal.

Configuration de la haute disponibilité à l'aide de la CLI

Étape 1. Configurez la haute disponibilité en mode **INC Enabled** dans les deux instances à l'aide de l'interface de ligne de commande NetScaler.

Sur le nœud principal, tapez la commande suivante.

```
1 add ha node 1 <sec_ip> -inc ENABLED
2 <!--NeedCopy-->
```

Sur le nœud secondaire, tapez la commande suivante.

```
1 add ha node 1 <prim_ip> -inc ENABLED
2 <!--NeedCopy-->
```

Le `sec_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud secondaire.

Le `prim_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud principal.

Étape 2 Ajoutez VIP et SNIP sur les nœuds principaux et secondaires.

Tapez les commandes suivantes sur le nœud principal :

```
1 add ns ip <primary_client_alias_ip> <subnet> -type VIP
2
3 <!--NeedCopy-->
```

> **Remarque :**
>
> Entrez l'alias, l'adresse IP et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.

```
1 add ns ip <primary_server_alias_ip> <subnet> -type SNIP
2 <!--NeedCopy-->
```


Tapez les commandes suivantes sur le nœud secondaire :

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
<!--NeedCopy-->
```

> **Remarque :**
>
> Entrez l'alias, l'adresse IP et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.

```
add ns ip <secondary_server_alias_ip> <subnet> -type SNIP
<!--NeedCopy-->
```

> **Remarque :**
>
> Entrez l'alias, l'adresse IP et le masque de réseau configurés pour le sous-réseau du serveur dans l'instance de machine virtuelle.

Étape 3. Ajoutez un serveur virtuel sur le nœud principal.

Exécutez la commande suivante :

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
<!--NeedCopy-->
```

Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal.

Exécutez la commande suivante :

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```

Étape 5. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

Exécutez la commande suivante :

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour enregistrer votre configuration, tapez la commande `save config`. Sinon, les configurations sont perdues après le redémarrage des instances.

Déployer une paire VPX haute disponibilité avec une adresse IP privée sur Google Cloud Platform

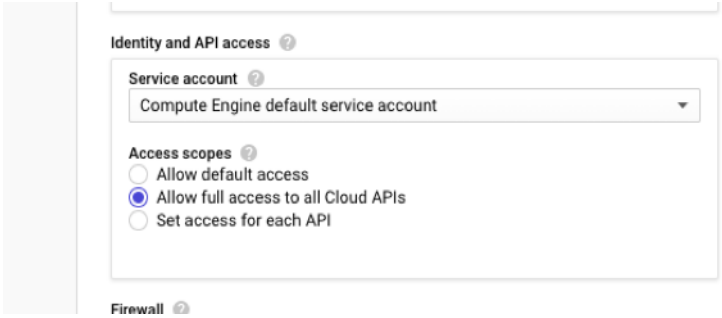
May 5, 2023

Vous pouvez déployer une paire VPX haute disponibilité sur GCP à l'aide d'une adresse IP privée. L'adresse IP du client (VIP) doit être configurée en tant qu'adresse IP alias sur le nœud principal. Lors du basculement, l'adresse IP du client est déplacée vers le nœud secondaire, pour que le trafic reprenne.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité.

Avant de commencer

- Lisez les limitations, les exigences matérielles et les points à noter mentionnés dans Déployer une instance NetScaler VPX sur GoogleCloud Platform. Ces informations s'appliquent également aux déploiements haute disponibilité.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
"compute.instances.get",
"compute.instances.list",
"compute.instances.updateNetworkInterface",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
```

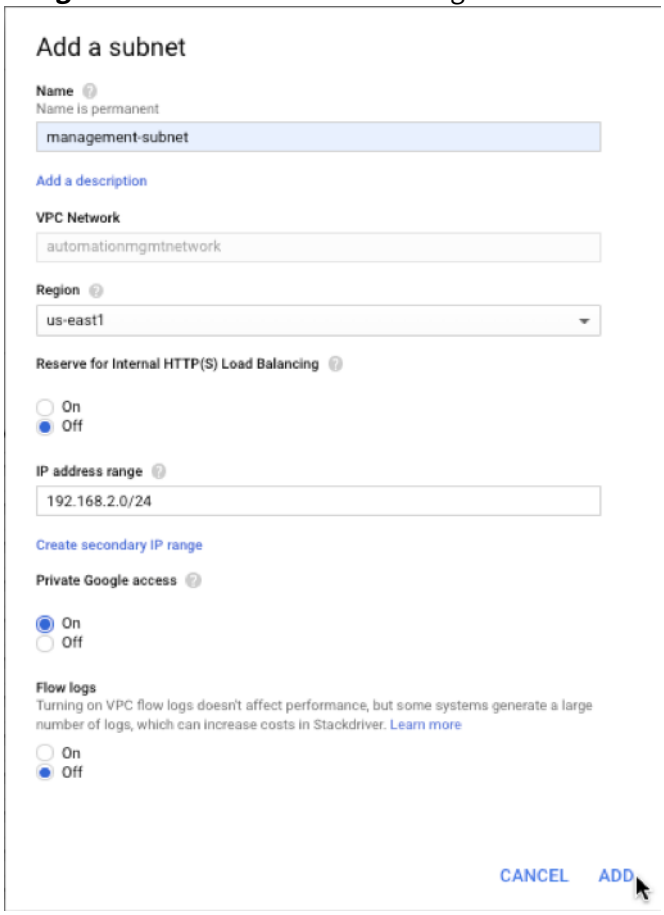


```
13   ]
14   <!--NeedCopy-->
```

- Si vous avez configuré des adresses IP externes sur une interface autre que l'interface de gestion, assurez-vous que votre compte de service GCP dispose des autorisations IAM supplémentaires suivantes :

```
1   REQUIRED_INSTANCE_IAM_PERMS = [
2   "compute.addresses.use"
3   "compute.instances.addAccessConfig",
4   "compute.instances.deleteAccessConfig",
5   "compute.networks.useExternalIp",
6   "compute.subnetworks.useExternalIp",
7   ]
8   <!--NeedCopy-->
```

- Si vos machines virtuelles ne disposent pas d'un accès Internet, vous devez activer **Private Google Access** sur le sous-réseau de gestion.



- Si vous avez configuré des règles de transfert GCP sur le nœud principal, lisez les limitations et exigences mentionnées dans Prise en charge des règles de transfert pour la paire haute disponi-

bilité VPX sur GCP pour les mettre à jour vers le nouveau serveur principal lors du basculement.

Comment déployer une paire haute disponibilité VPX sur Google Cloud Platform

Voici un résumé des étapes de déploiement haute disponibilité :

1. Créez des réseaux VPC dans la même région. Par exemple, Asie-Est.
2. Créez deux instances VPX (nœuds principal et secondaire) sur la même région. Ils peuvent se trouver dans la même zone ou dans des zones différentes. Par exemple, l'Asie orientale 1a et l'Asie orientale Ib.
3. Configurez les paramètres de haute disponibilité sur les deux instances à l'aide de l'interface graphique NetScaler ou des commandes ADC CLI.

Étape 1. Créer des réseaux VPC

Créez des réseaux VPC en fonction de vos besoins. Citrix vous recommande de créer trois réseaux VPC à associer à une carte réseau de gestion, une carte réseau client et une carte réseau de serveur.

Pour créer un réseau VPC, procédez comme suit :

1. Ouvrez une session sur la **console Google > Mise en réseau > Réseau VPC > Créer un réseau VPC**.
2. Remplissez les champs requis, puis cliquez sur **Créer**.

Pour plus d'informations, consultez la section **Créer des réseaux VPC** dans Déployer une instance NetScaler VPX surGoogle Cloud Platform.

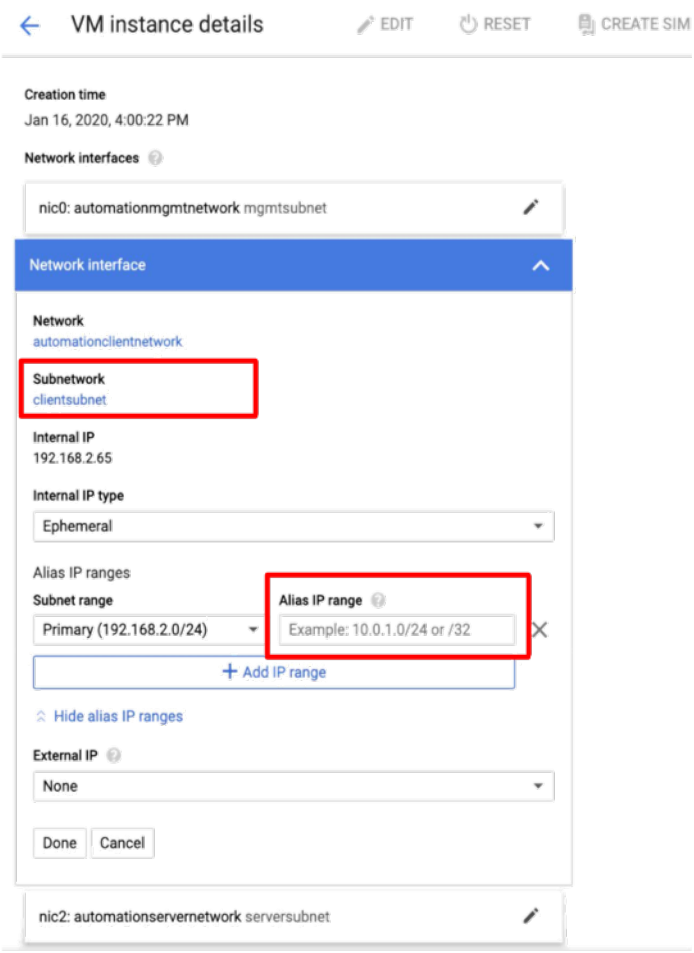
Étape 2. Créer deux instances VPX

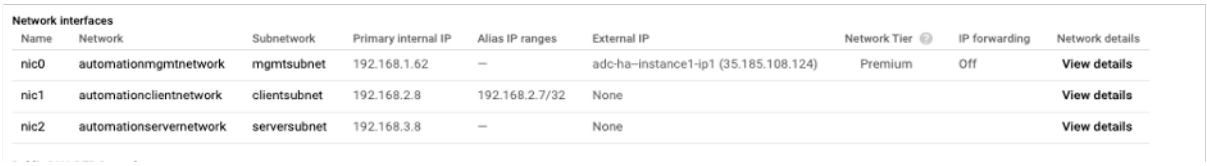
Créez deux instances VPX en suivant les étapes indiquées dans Scénario : déployer une instance VPX autonome multi-cartes réseau et multi-IP.

> **Important :**
>
> Attribuez une adresse IP d'alias client au nœud principal. N'utilisez pas l'adresse IP interne de l'instance VPX pour configurer le VIP.

Pour créer une adresse IP d'alias client, procédez comme suit :

1. Accédez à l'instance de machine virtuelle et cliquez sur **Modifier**.
2. Dans la fenêtre **Interface réseau**, modifiez l'interface client.
3. Dans le champ **Plage d'adresses IP d'alias**, saisissez l'adresse IP de l'alias du client.





Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	automationmgmtnetwork	mgmtsubnet	192.168.1.62	–	adc-ha--instance1-ip1 (35.185.108.124)	Premium	Off	View details
nic1	automationclientnetwork	clientsubnet	192.168.2.8	192.168.2.7/32	None			View details
nic2	automationservernetwork	serversubnet	192.168.3.8	–	None			View details

Après le basculement, lorsque l'ancien principal devient le nouveau secondaire, les adresses IP de l'alias se déplacent de l'ancien principal et sont attachées au nouveau principal.

Une fois que vous avez configuré les instances VPX, vous pouvez configurer les adresses IP virtuelles (VIP) et SNIP (Subnet IP). Pour plus d'informations, consultez la section Configuration des adresses IP appartenant à NetScaler.

Étape 3. Configurer la haute disponibilité

Après avoir créé les instances sur Google Cloud Platform, vous pouvez configurer la haute disponibilité à l'aide de l'interface graphique ou de la CLI de NetScaler.

Configurer la haute disponibilité à l'aide de l'interface graphique

Étape 1. Configurez la haute disponibilité en mode INC Enabled sur les deux nœuds.

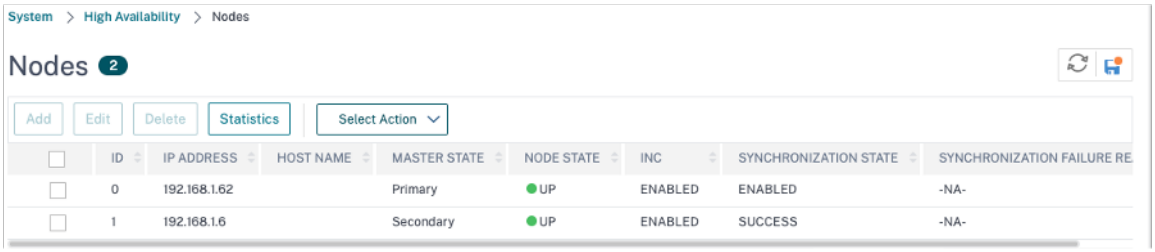
Sur le **nœud principal**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud secondaire.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Sur le **nœud secondaire**, effectuez les opérations suivantes :

1. Connectez-vous à l'instance avec le nom d'utilisateur `nsroot` et l'ID d'instance du nœud depuis la console GCP comme mot de passe.
2. Accédez à **Configuration > Système > Haute disponibilité > Nœuds**, puis cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP du nœud distant**, entrez l'adresse IP privée de la carte réseau de gestion du nœud principal.
4. Activez la case à cocher **Activer le mode INC (Independent Network Configuration) sur auto-nœud**.
5. Cliquez sur **Create**.

Avant d'aller plus loin, assurez-vous que l'état de synchronisation du nœud secondaire s'affiche comme **SUCCÈS** dans la page **Nœuds** .



> **Remarque**
>
> Une fois le nœud secondaire synchronisé avec le nœud principal, le nœud secondaire possède les mêmes informations de connexion que le nœud principal.

Étape 2 Ajoutez une adresse IP virtuelle et une adresse IP de sous-réseau sur les deux nœuds.

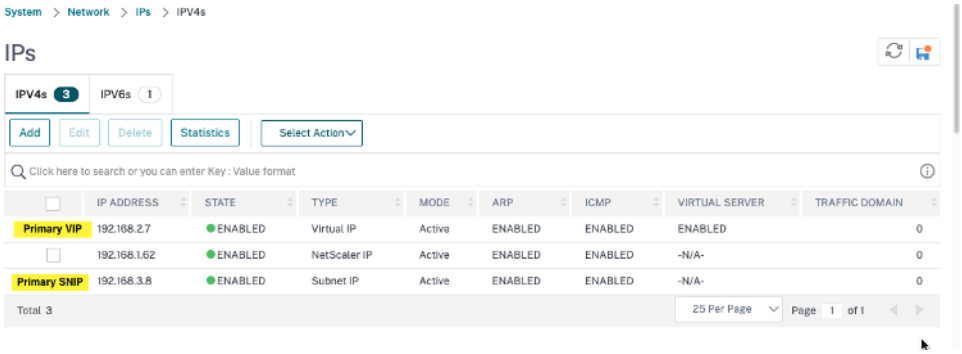
Sur le nœud principal, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :

a) Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.
b) Dans le champ **Type d'IP**, sélectionnez **IP virtuelle** dans le menu déroulant.
c) Cliquez sur **Create**.

3. Pour créer une adresse IP du serveur (SNIP) :

a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance principale et du masque de réseau configurés pour le sous-réseau du serveur.
b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Create**.



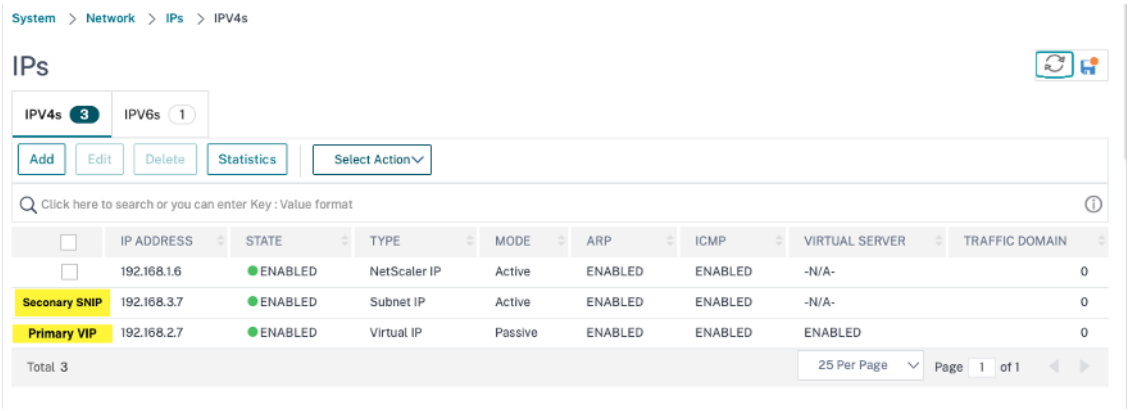
Sur le nœud secondaire, effectuez les opérations suivantes :

1. Accédez à **Système > Réseau > IPs > IPv4**, puis cliquez sur **Ajouter**.
2. Pour créer une adresse IP (VIP) alias client :

a) Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client sur l'instance de machine virtuelle principale.
b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Create**.

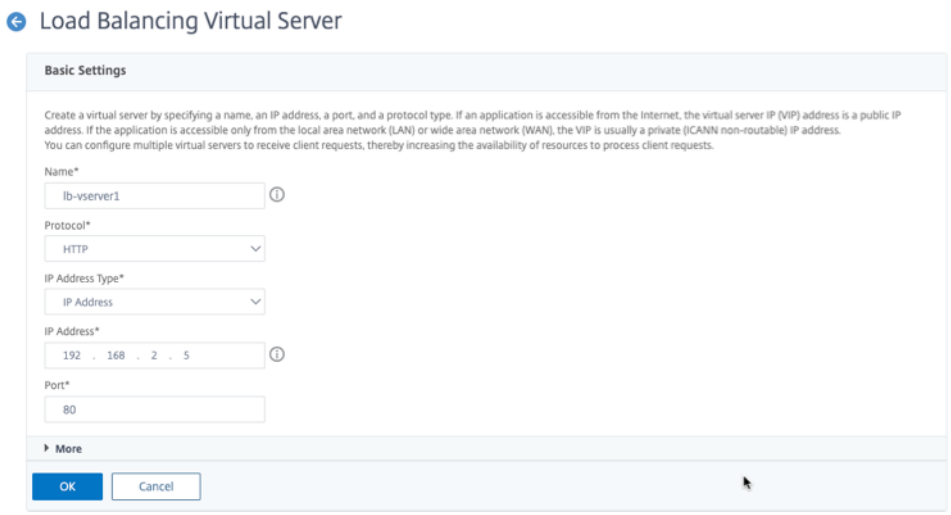
3. Pour créer une adresse IP du serveur (SNIP) :

a) Entrez l'adresse IP interne de l'interface orientée serveur de l'instance secondaire et du masque de réseau configurés pour le sous-réseau du serveur.
b) Dans le champ **Type IP**, sélectionnez **IP du sous-réseau** dans le menu déroulant.
c) Cliquez sur **Create**.



Étape 3. Ajoutez un serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.
2. Ajoutez les valeurs requises pour Nom, Protocole, Type d'adresse IP (adresse IP), Adresse IP (adresse IP de l'alias principal du client) et Port, puis cliquez sur **OK**.



Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

Étape 5. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 3**, puis cliquez sur **Modifier**.

3. Dans l'onglet **Groupes de services et de services**, cliquez sur **Liaison de service Virtual Server sans équilibrage de charge**.
4. Sélectionnez le service configuré à l'**étape 4**, puis cliquez sur **Lier**.

Étape 5. Enregistrez la configuration.

Après un basculement forcé, le secondaire devient le nouveau principal. L'adresse IP de l'alias client (VIP) et l'adresse IP de l'alias de serveur (SNIP) de l'ancien serveur principal sont déplacées vers la nouvelle adresse principale.

Configuration de la haute disponibilité à l'aide de la CLI

Étape 1. Configurez la haute disponibilité en mode **INC Enabled** dans les deux instances à l'aide de l'interface de ligne de commande NetScaler.

Sur le nœud principal, tapez la commande suivante.

```
add ha node 1 <sec_ip> -inc ENABLED
<!--NeedCopy-->
```

Sur le nœud secondaire, tapez la commande suivante.

```
add ha node 1 <prim_ip> -inc ENABLED
<!--NeedCopy-->
```

Le `sec_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud secondaire.

Le `prim_ip` fait référence à l'adresse IP interne de la carte réseau de gestion du nœud principal.

Étape 2 Ajoutez VIP et SNIP sur les deux nœuds.

Tapez les commandes suivantes sur le nœud principal :

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP

<!--NeedCopy-->
```

> **Remarque :**
>
> Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client dans l'instance de machine virtuelle.

```
add ns ip <primary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

Le `primary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance principale.

Tapez les commandes suivantes sur le nœud secondaire :

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
<!--NeedCopy-->
```

> Remarque
>
> Entrez l'adresse IP de l'alias et le masque de réseau configurés pour le sous-réseau client sur l'instance de machine virtuelle principale.

```
add ns ip <secondary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

Le `secondary_snip` fait référence à l'adresse IP interne de l'interface orientée serveur de l'instance secondaire.

> **Remarque :**
>
> Entrez l'adresse IP et le masque de réseau configurés pour le sous-réseau du serveur dans l'instance de machine virtuelle.

Étape 3. Ajoutez un serveur virtuel sur le nœud principal.

Exécutez la commande suivante :

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
<!--NeedCopy-->
```

Étape 4 Ajoutez un service ou un groupe de services sur le nœud principal.

Exécutez la commande suivante :

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```

Étape 5. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge sur le nœud principal.

Exécutez la commande suivante :

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```

> **Remarque :**

> Pour enregistrer votre configuration, tapez la commande `save config`. Sinon, les configurations sont perdues après le redémarrage des instances.

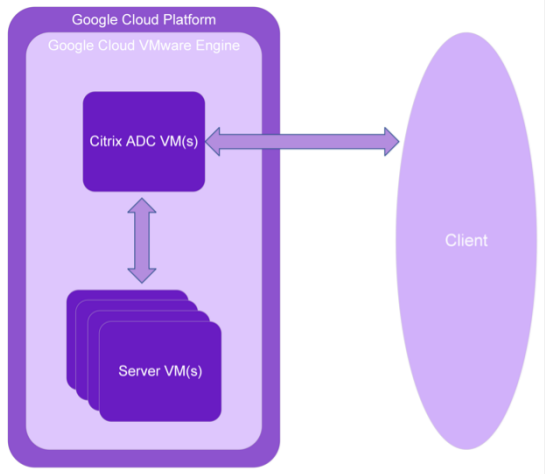
Installation d'une instance NetScaler VPX sur Google Cloud VMware Engine

May 5, 2023

Google Cloud VMware Engine (GCVE) met à votre disposition des clouds privés contenant des clusters vSphere, conçus à partir d'une infrastructure Google Cloud Platform dédiée. Le déploiement initial minimum est de trois hôtes, mais des hôtes supplémentaires peuvent être ajoutés un par un. Tous les clouds privés provisionnés sont dotés de vCenter Server, vSAN, vSphere et NSX-T.

GCVE vous permet de créer des centres de données définis par logiciel (SDDC) dans le cloud sur Google Cloud Platform avec le nombre souhaité d'hôtes ESX. GCVE prend en charge les déploiements NetScaler VPX. GCVE fournit une interface utilisateur identique à celle de vCenter sur site. Il fonctionne de la même manière que les déploiements NetScaler VPX basés sur ESX.

Le schéma suivant montre le GCVE sur la Google Cloud Platform auquel un administrateur ou un client peut accéder via Internet. Un administrateur peut créer, gérer et configurer des machines virtuelles de charge de travail ou de serveur à l'aide de GCVE. L'administrateur peut accéder au vCenter et au NSX-T Manager basés sur le Web du GCVE via une connexion OpenVPN. Vous pouvez créer les instances NetScaler VPX (autonomes ou par paire HA) et les machines virtuelles de serveur au sein de GCVE à l'aide de vCenter, et gérer le réseau correspondant à l'aide de NSX-T manager. L'instance NetScaler VPX sur GCVE fonctionne de la même manière que le cluster d'hôtes VMware sur site. Le GCVE peut être géré à l'aide d'une connexion OpenVPN à l'infrastructure de gestion.



Composants requis

Avant de commencer à installer une appliance virtuelle, procédez comme suit :

- Pour plus d'informations sur Google Cloud VMware Engine et ses prérequis, consultez la documentation Google Cloud VMware Engine.
- Pour plus d'informations sur le déploiement de Google Cloud VMware Engine, voir Déployer un cloud privé Google Cloud VMware Engine.
- Pour plus d'informations sur la connexion à votre cloud privé à l'aide d'une passerelle VPN point à site pour accéder à Google Cloud VMware Engine et le gérer, consultez Accéder à un cloud privé Google Cloud VMware Engine.
- Sur la machine cliente VPN, téléchargez les fichiers de configuration de l'appliance NetScaler VPX.
- Créez des segments réseau NSX-T appropriés sur VMware SDDC auxquels les machines virtuelles se connectent. Pour plus d'informations, voir Ajouter un segment réseau dans Google Cloud VMware Engine.
- Obtenir des fichiers de licence VPX. Pour plus d'informations sur les licences d'instance NetScaler VPX, consultez la section Vue d'ensemble des licences.
- Les machines virtuelles (VM) créées ou migrées vers le cloud privé GCVE doivent être connectées à un segment réseau.

Configuration matérielle du cloud VMware

Le tableau suivant répertorie les ressources informatiques virtuelles que le SDDC VMware doit fournir pour chaque appliance virtuelle VPX nCore.

Tableau 1. Ressources informatiques virtuelles minimales requises pour exécuter une instance NetScaler VPX

Composant	Exigences
Mémoire	2 Go
Processeur virtuel	2
Interfaces réseau virtuelles	Dans VMware SDDC, vous pouvez installer un maximum de 10 interfaces réseau virtuelles si le matériel VPX est mis à niveau vers la version 7 ou supérieure.
Espace disque	20 Go

> Remarque
>
> Ceci s'ajoute à toutes les exigences de disque pour l'Hypervisor.

Pour une utilisation en production de l'appliance virtuelle VPX, l'allocation complète de mémoire doit être réservée.

Configuration système requise pour OVF Tool 1.0

OVF Tool est une application cliente qui peut s'exécuter sur les systèmes Windows et Linux. Le tableau suivant décrit la configuration système minimale requise pour l'installation de l'outil OVF.

Tableau 2 Configuration minimale requise pour l'installation d'outils OVF

Composant	Exigences
OS	Pour connaître les exigences détaillées de VMware, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.
UC	750 MHz minimum, 1 GHz ou plus rapide recommandé
RAM	1 Go minimum, 2 Go recommandés
Carte d'interface réseau	Carte réseau 100 Mbit/s ou plus rapide

Pour plus d'informations sur l'installation d'OVF, recherchez le fichier PDF « OVF Tool User Guide » à l'adresse http://kb.vmware.com/.

Téléchargement des fichiers de configuration de NetScaler VPX

Le package de configuration de l'instance NetScaler VPX pour VMware ESX respecte la norme de format Open Virtual Machine (OVF). Vous pouvez télécharger les fichiers depuis le site Web de Citrix. Vous avez besoin d'un compte Citrix pour vous connecter. Si vous n'avez pas de compte Citrix, accédez à la page d'accueil à l' adresse http://www.citrix.com. Cliquez sur le **lien Nouveaux utilisateurs**et suivez les instructions pour créer un compte Citrix.

Une fois connecté, naviguez dans le chemin suivant à partir de la page d'accueil Citrix :

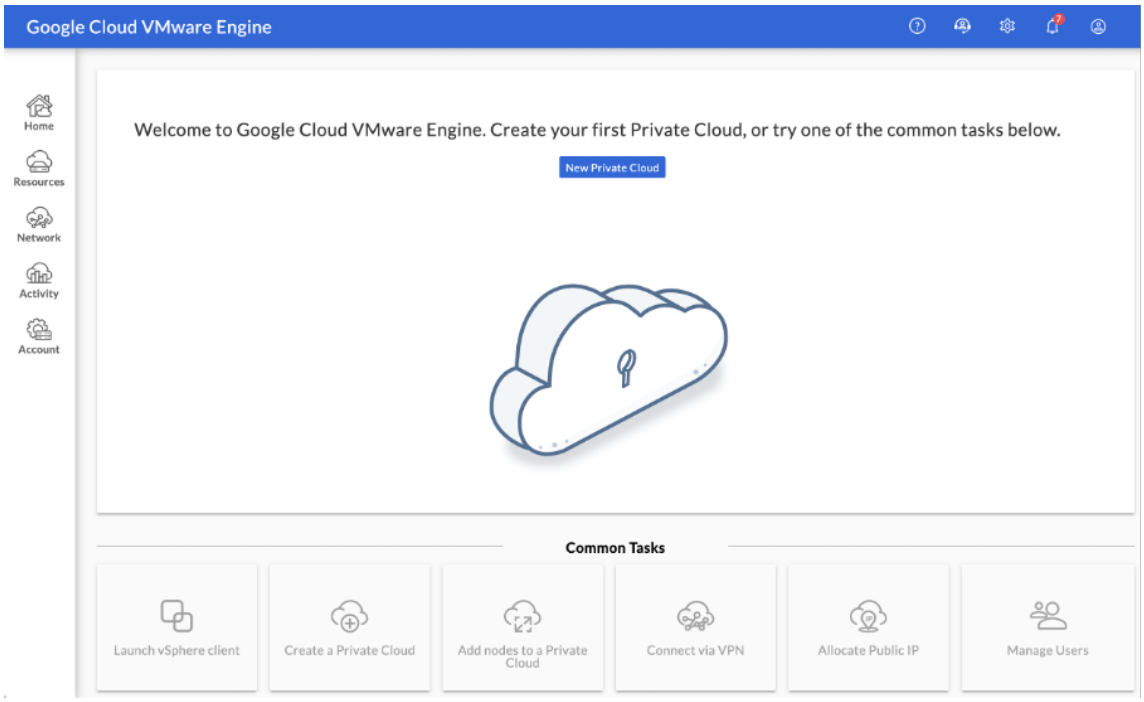
Citrix.com > **Téléchargements > NetScaler > Appliances virtuelles.**

Copiez les fichiers suivants sur une station de travail située sur le même réseau que le serveur ESX. Copiez les trois fichiers dans le même dossier.

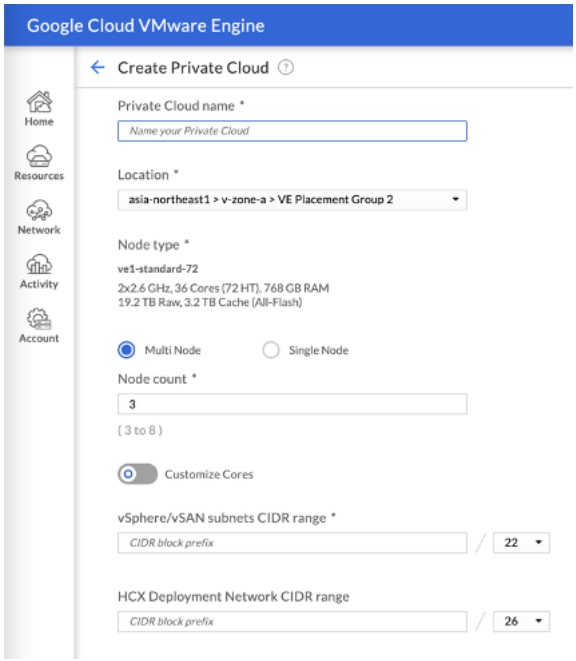
- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (for example, NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (for example, NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (for example, NSVPX-ESX-13.0-79.64.mf)

Déployer Google Cloud VMware Engine

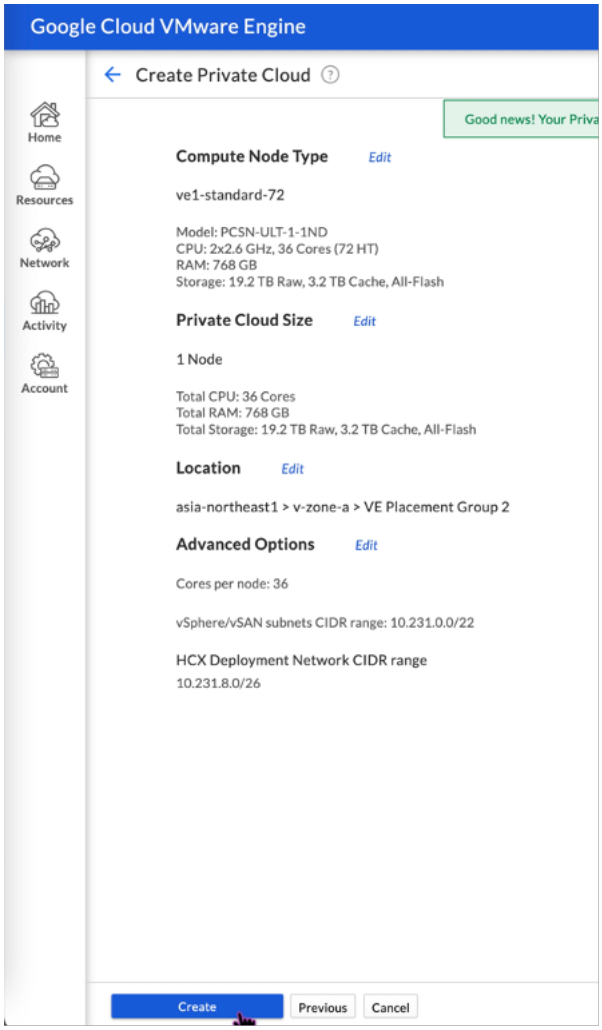
1. Connectez-vous à votre portail GCVEet accédez à la page d' **accueil**.



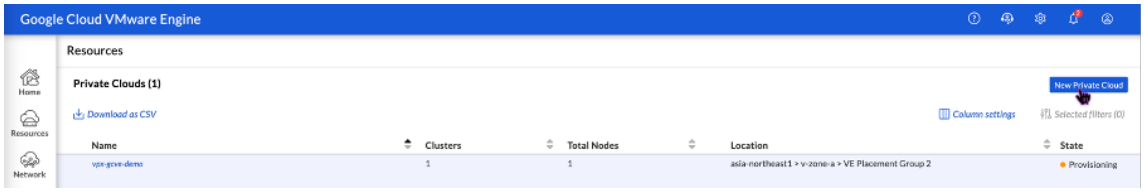
2. Sur la page **Nouveau cloud privé**, entrez les informations suivantes :
   - Sélectionnez au moins 3 hôtes ESXi pour créer le cluster par défaut de votre cloud privé.
   - Pour le champ de **plage d'adresses CIDR du sous-réseau vSphère/vSAN**, utilisez l'espace d'adressage /22.
   - Pour le champ de **plage d'adresses CIDR du réseau de déploiement HCX**, utilisez l'espace d'adressage /26.
   - Pour le réseau virtuel, assurez-vous que la plage CIDR ne chevauche aucun de vos sous-réseaux GCP locaux ou autres (réseaux virtuels).



3. Cliquez sur **Vérifier et créer**.
4. Vérifiez les paramètres. Si vous devez modifier des paramètres, cliquez sur **Précédent**.



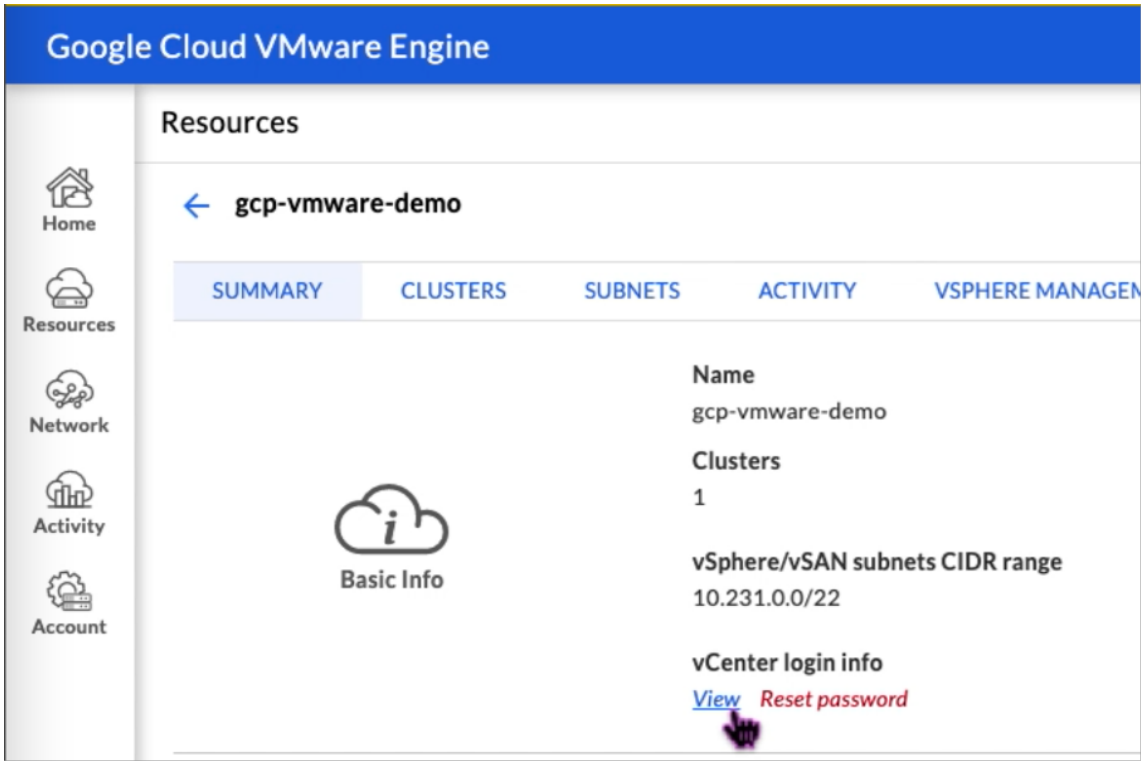
5. Cliquez sur **Create**. Le processus de provisionnement du cloud privé démarre. Le provisionnement du cloud privé peut prendre jusqu'à deux heures.
6. Accédez à **Ressources** pour vérifier le cloud privé créé.



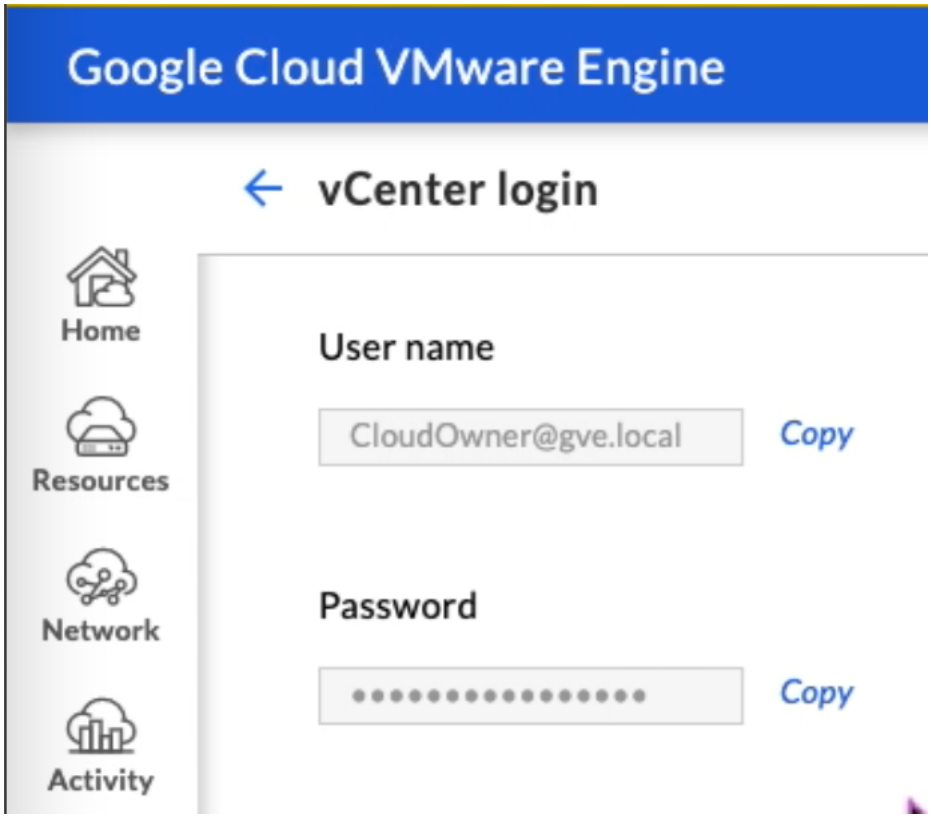
7. Pour accéder à cette ressource, vous devez vous connecter à GCVE à l'aide d'un VPN point à site. Pour plus d'informations, consultez la documentation suivante :
   - Passerelles VPN
   - Connexion via un VPN

Accédez à votre portail Private Cloud vCenter

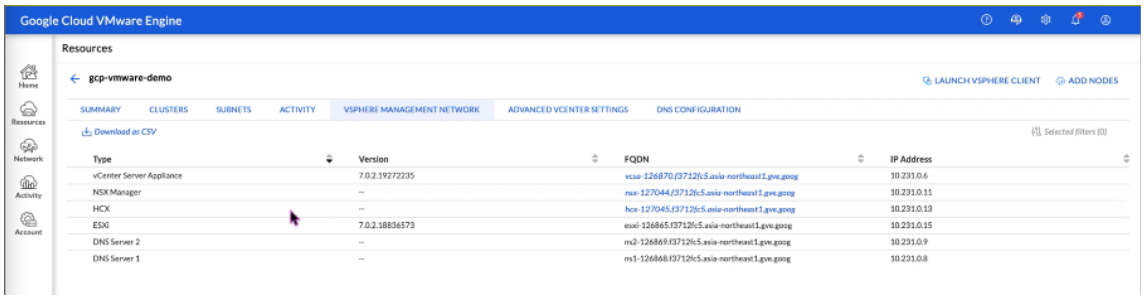
1. Accédez à votre cloud privé Google Cloud VMware Engine. Dans l'onglet **RÉSUMÉ**, sous **Informations de connexion à vCenter**, cliquez sur **Afficher**.



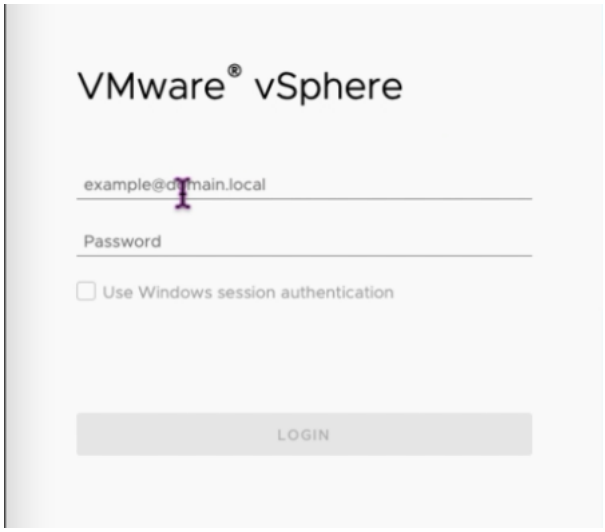
2. Notez les informations d'identification de vCenter.



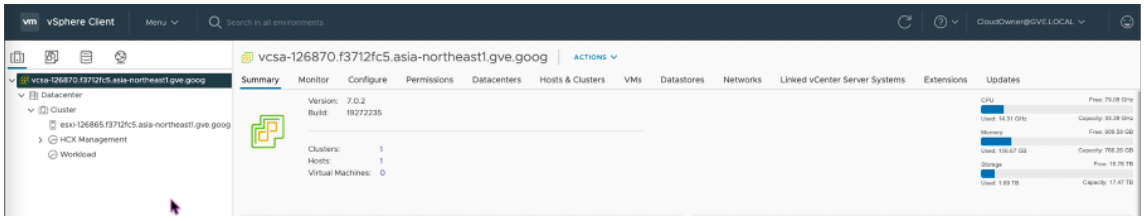
3. Lancez le client vSphere en cliquant sur **LANCER VSPHERE CLIENT** ou accédez à **VSPHERE MANAGEMENT NETWORK** et cliquez sur le nom de domaine complet de **vCenter Server Appliance** .



4. Connectez-vous à VMware vSphere à l'aide des informations d'identification vCenter indiquées à l'étape 2 de cette procédure.



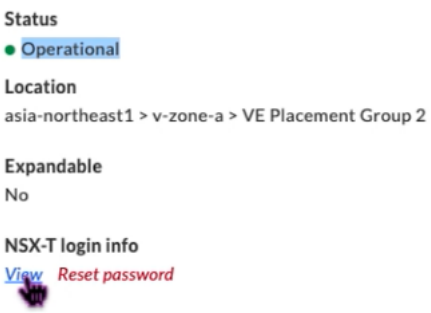
5. Dans le client vSphere, vous pouvez vérifier les hôtes ESXi que vous avez créés sur le portail GCVE.



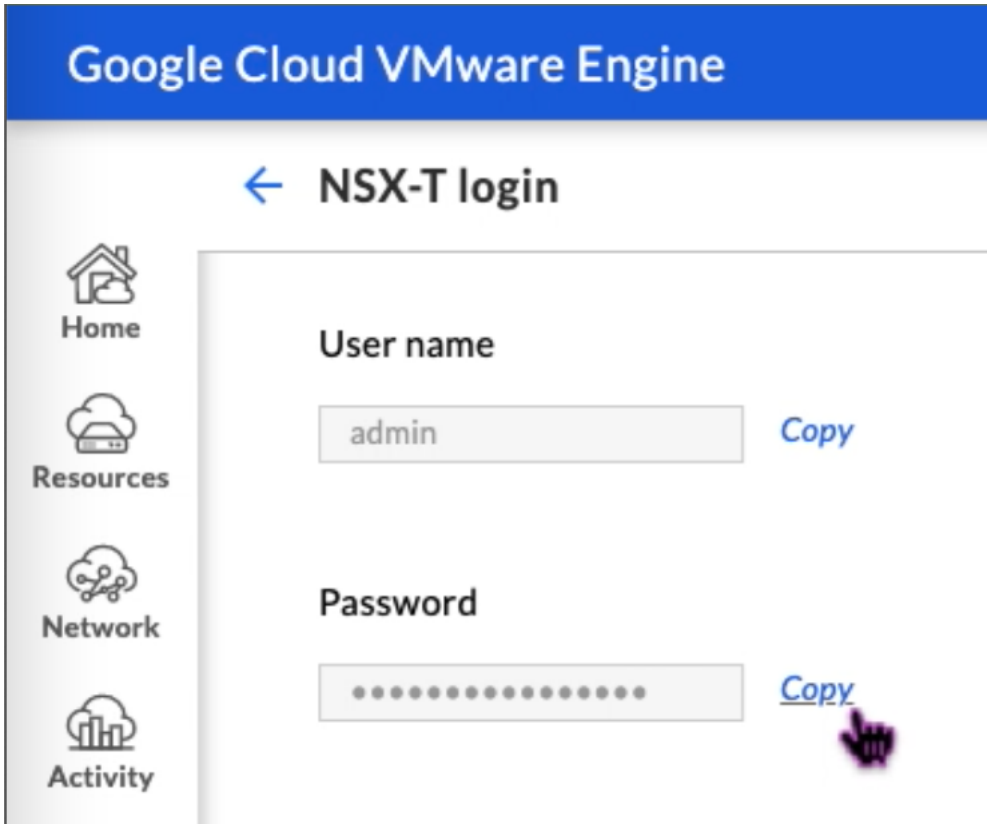
Création d'un segment NSX-T dans le portail GCVE NSX-T

Vous pouvez créer et configurer un segment NSX-T à partir de NSX Manager dans la console Google Cloud VMware Engine. Ces segments sont connectés à la passerelle de niveau 1 par défaut, et les charges de travail de ces segments sont connectées Est-Ouest et Nord-Sud. Une fois que vous avez créé le segment, il s'affiche dans vCenter.

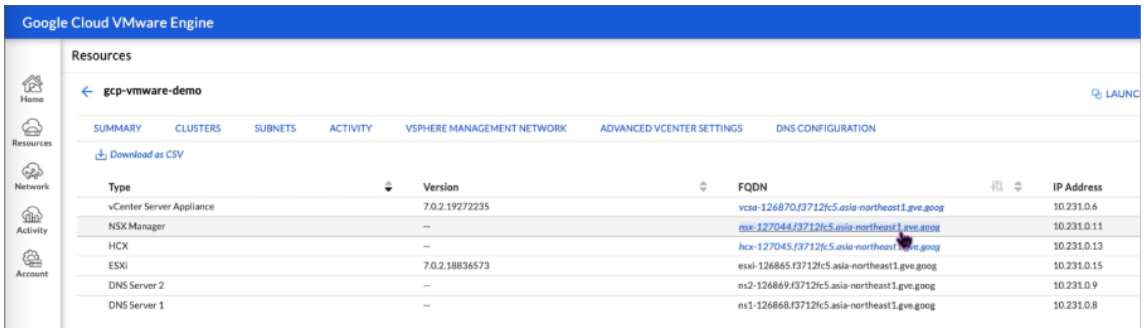
1. Dans votre cloud privé GCVE, sous **Résumé -> Informations de connexion NSX-T**, sélectionnez **Afficher**.



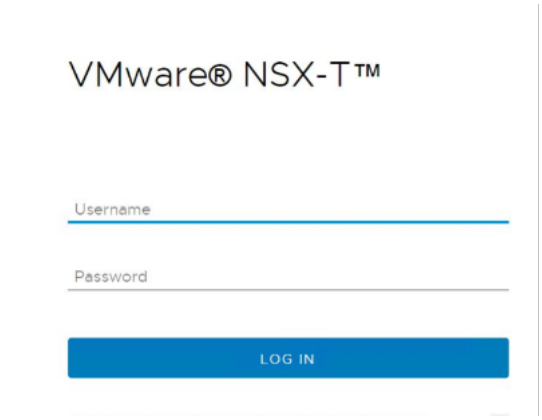
2. Prenez note des informations d'identification de la NSX-T.



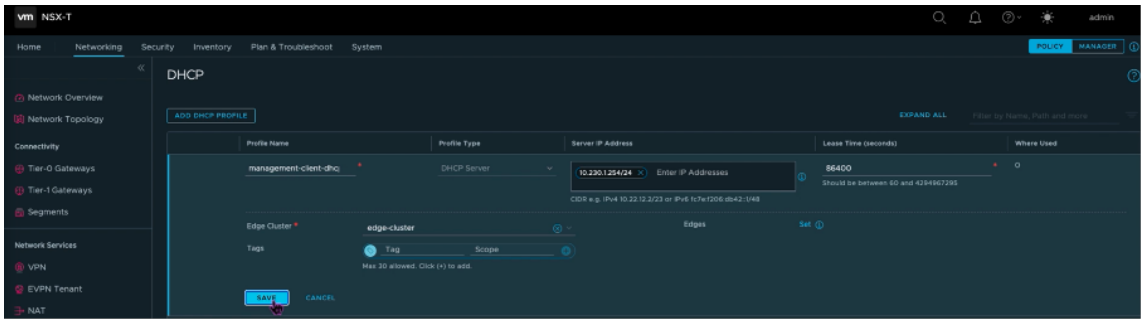
3. Lancez NSX Manager en accédant à **VSPHERE MANAGEMENT NETWORK** et en cliquant sur le nom de domaine complet de **NSX Manager** .



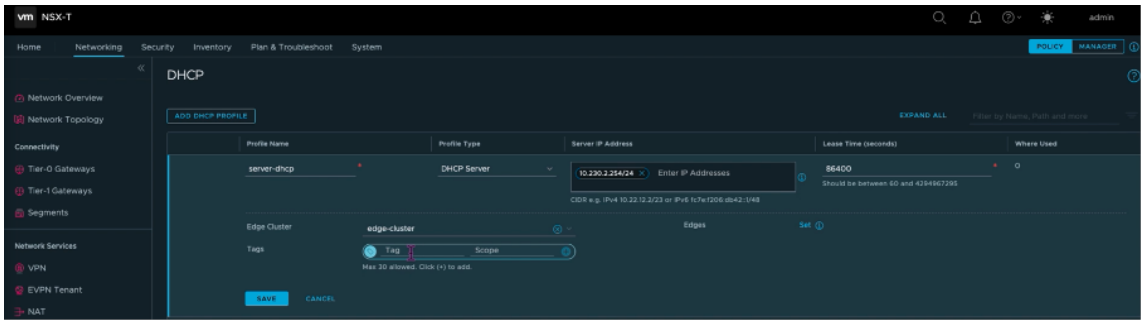
4. Connectez-vous à NSX Manager à l'aide des informations d'identification indiquées à l'étape 2 de cette procédure.



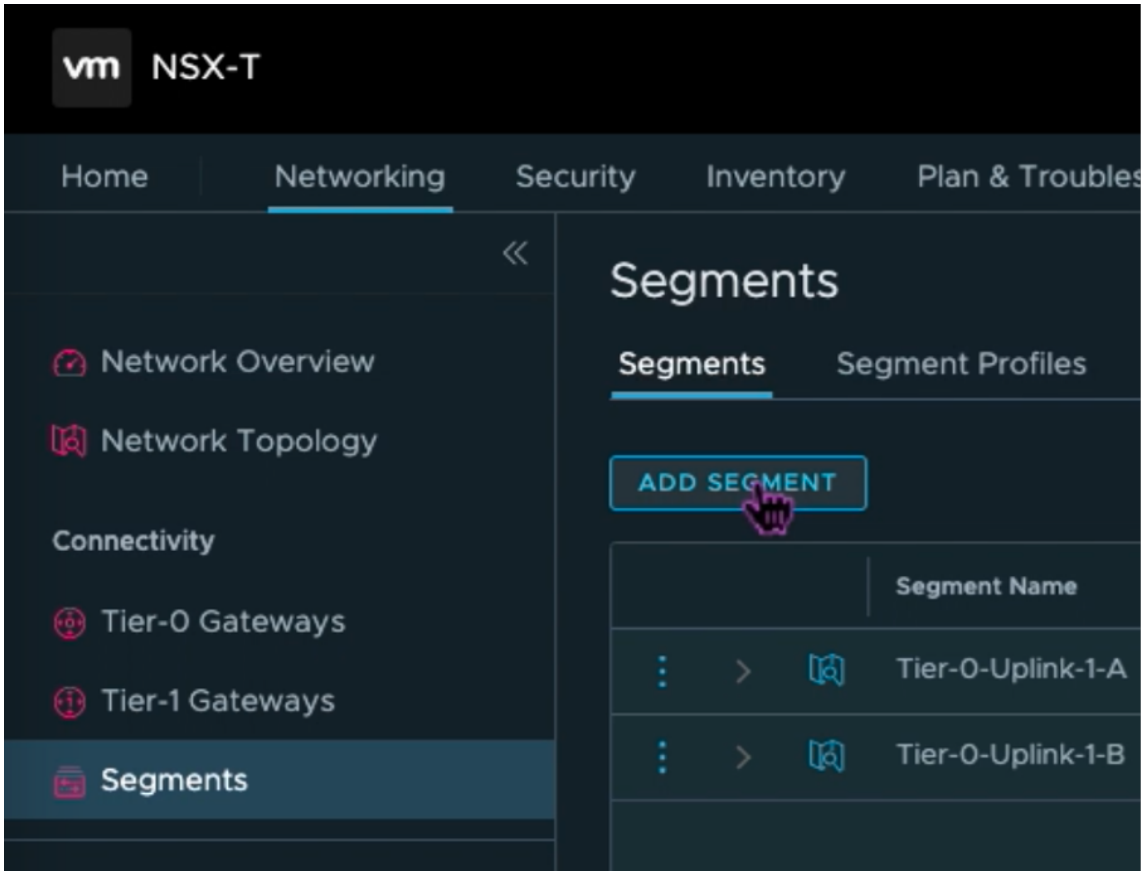
5. Configurez le service DHCP pour les nouveaux segments ou sous-réseaux.
6. Avant de créer un sous-réseau, configurez un service DHCP.
7. Dans NSX-T, accédez à **Réseau > DHCP**. Le tableau de bord réseau indique que le service crée une passerelle de niveau 0 et une passerelle de niveau 1.
8. Pour commencer à approvisionner un serveur DHCP, cliquez sur **Ajouter un profil DHCP**.
9. Dans le champ Nom DHCP, entrez le nom du profil **Client-Management** .
10. Sélectionnez le **serveur DHCP** comme type de profil.
11. Dans la colonne **Adresse IP du serveur**, indiquez une plage d'adresses IP du service DHCP.
12. Sélectionnez votre **Edge Cluster**.
13. Cliquez sur **Enregistrer** pour créer le service DHCP.



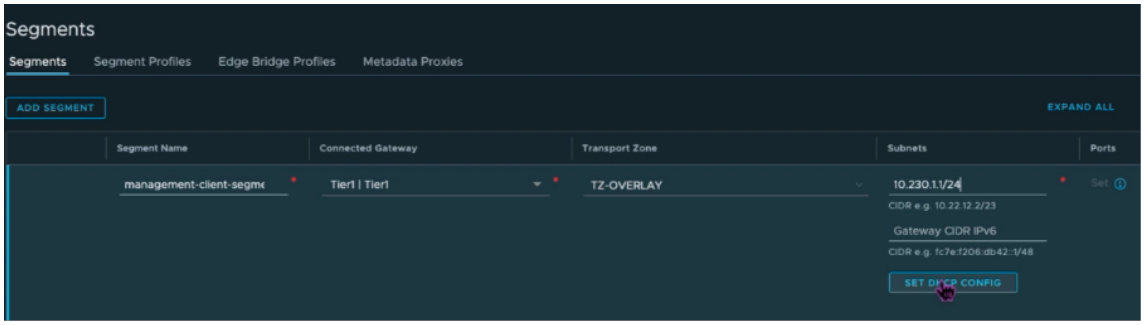
14. Répétez les étapes 6 à 13 pour la plage DHCP du serveur.



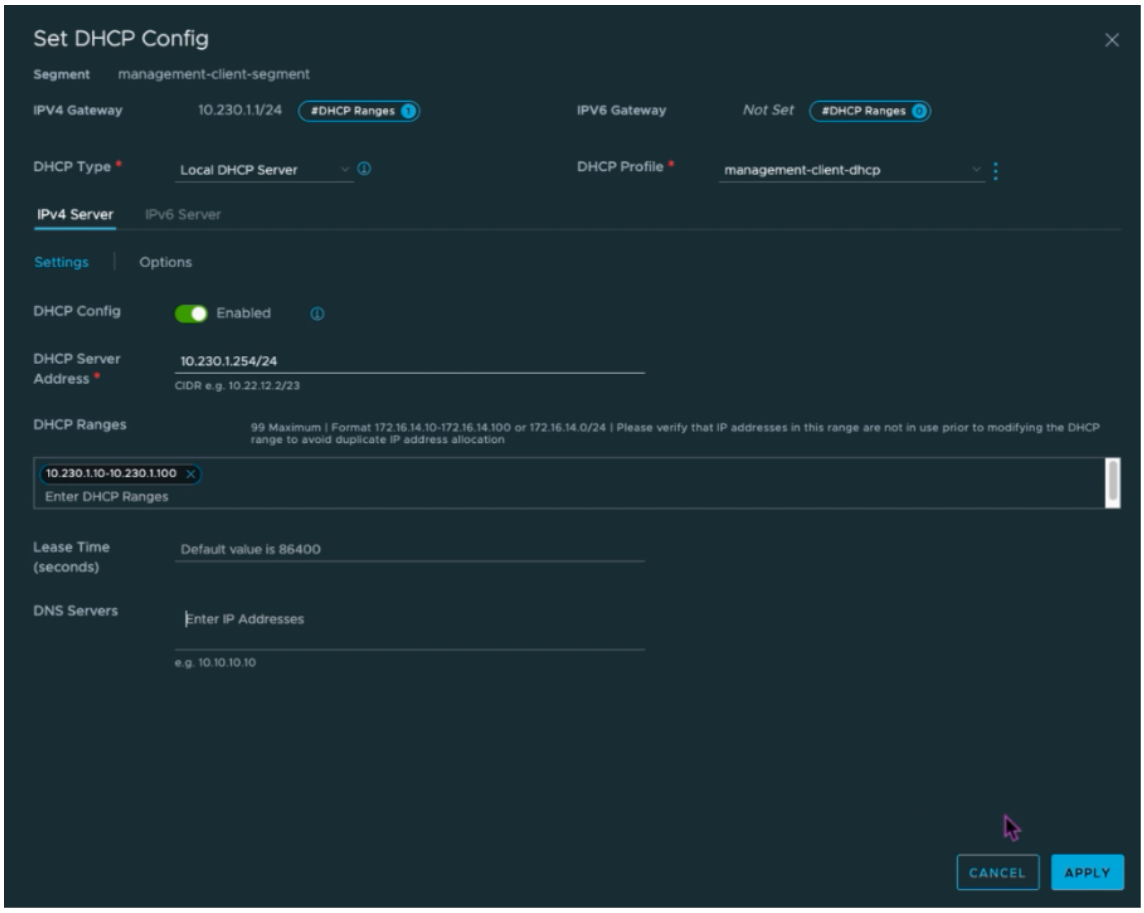
15. Créez deux segments distincts : l'un pour les interfaces client et de gestion, et l'autre pour les interfaces serveur.
16. Dans NSX-T, accédez à **Mise en réseau > Segments**.
17. Cliquez sur **Add Segment**.



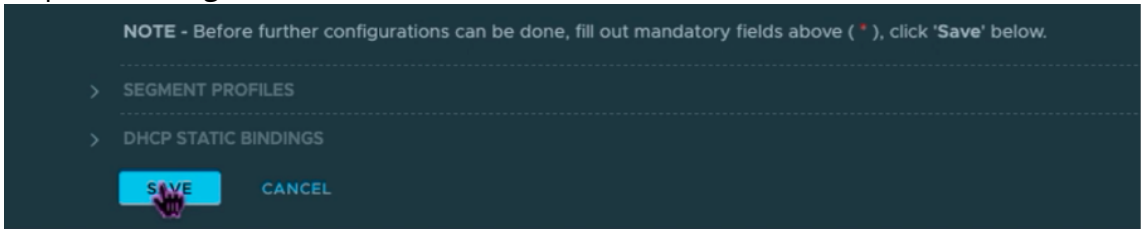
18. Dans le champ **Nom du segment**, entrez le nom de votre segment **Gestion des clients** .
19. Dans la liste des **passerelles connectées**, sélectionnez **Tier1** pour vous connecter à la passerelle de niveau 1.
20. Dans la liste des **zones de transport**, sélectionnez **TZ-OVERLAY | Overlay**.
21. Dans la colonne **Sous-réseaux**, entrez la plage de sous-réseaux. Spécifiez la plage de sous-réseaux avec `.1` comme dernier octet. Par exemple, 10.12.2.1/24.

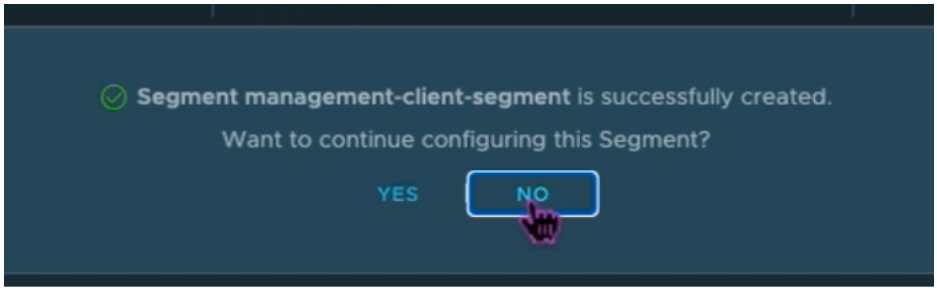


22. Cliquez sur **Définir la configuration DHCP**et entrez des valeurs pour le champ **Plages DHCP** .



23. Cliquez sur **Appliquer** pour enregistrer votre configuration DHCP.
24. Cliquez sur **Enregistrer**.





25. Répétez également les étapes 17 à 24 pour le segment de serveur.
26. Vous pouvez désormais sélectionner ces segments de réseau dans vCenter lors de la création d'une machine virtuelle.

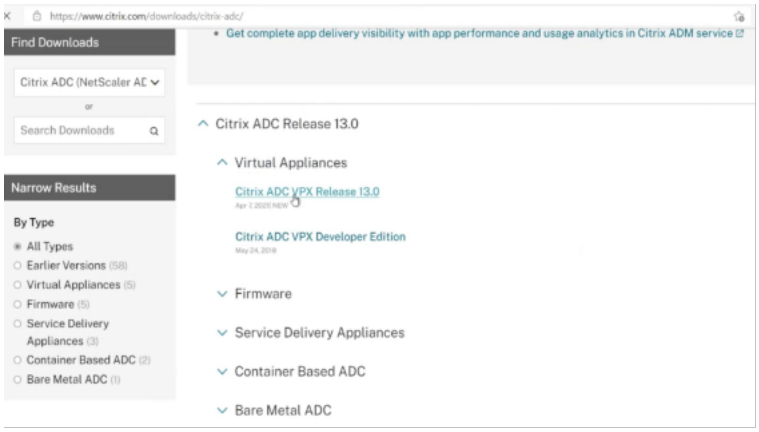
Pour plus d'informations, voir Création de votre premier sous-réseau.

Installation d'une instance NetScaler VPX sur le cloud VMware

Après avoir installé et configuré Private Cloud sur GCVE, vous pouvez utiliser le vCenter pour installer des appliances virtuelles sur VMware Engine. Le nombre d'appliances virtuelles que vous pouvez installer dépend de la quantité de ressources disponibles sur le cloud privé.

Pour installer des instances NetScaler VPX sur un cloud privé, effectuez ces étapes sur un poste de travail connecté à un VPN point à site de cloud privé :

1. Téléchargez les fichiers de configuration de l'instance NetScaler VPX pour l'hôte ESXi depuis le site de téléchargement de NetScaler.

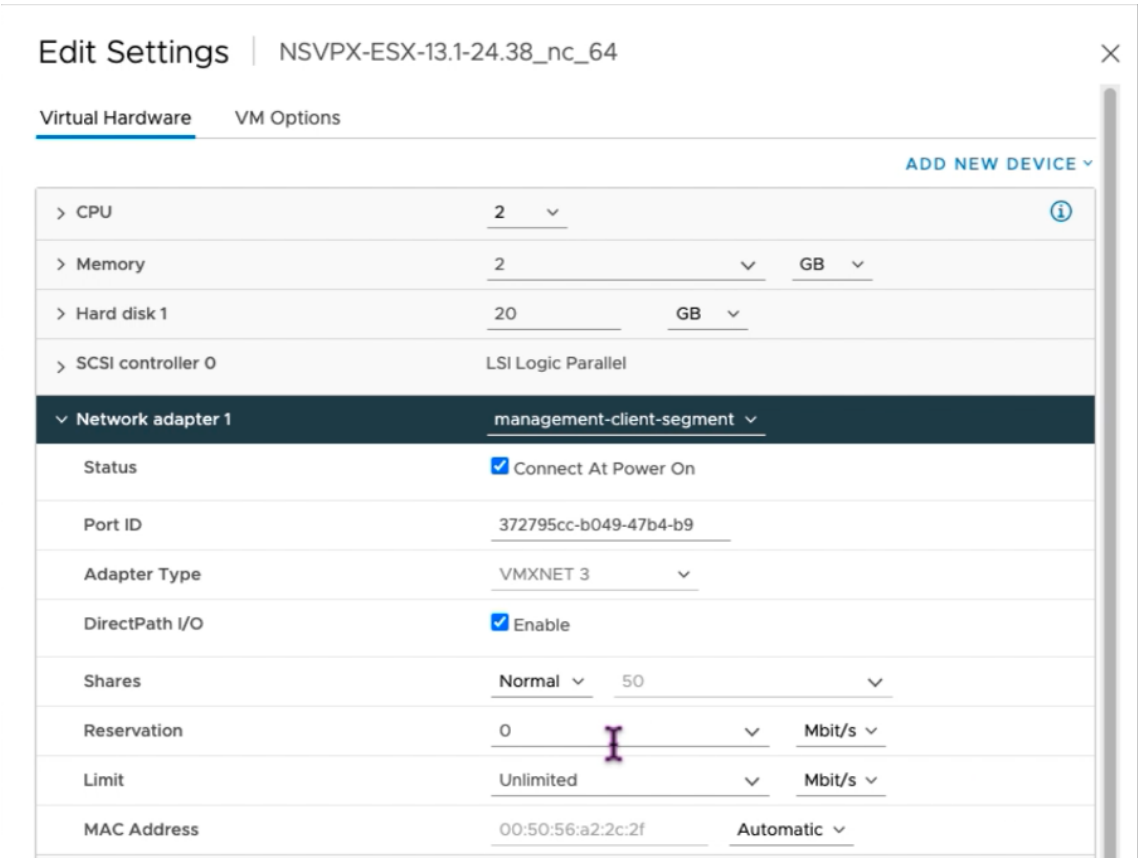


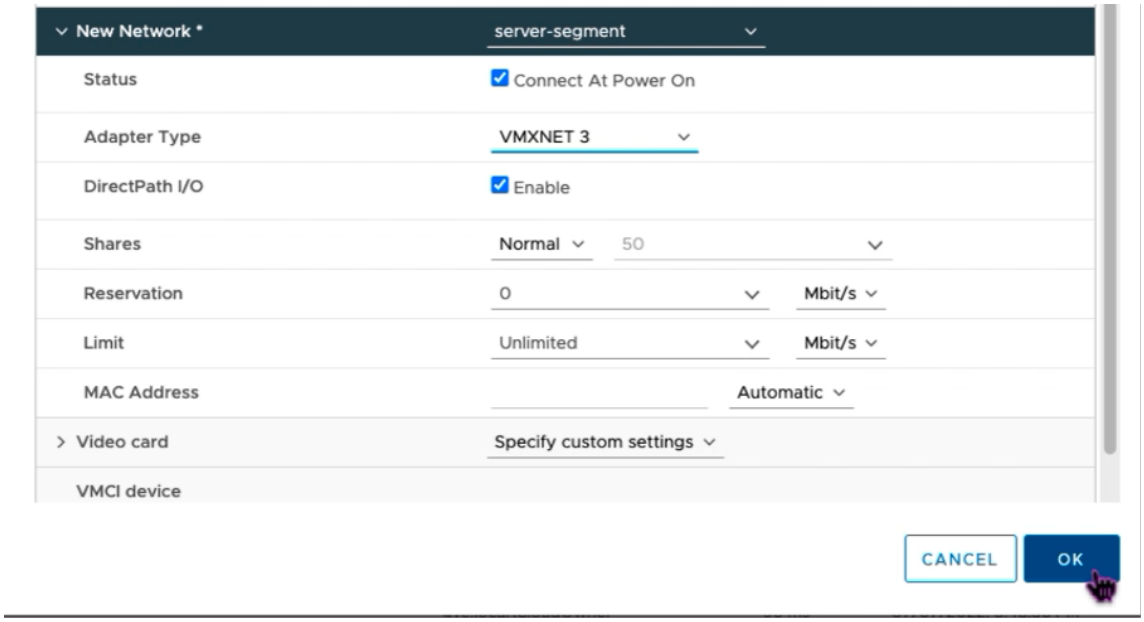
2. Ouvrez VMware vCenter dans un navigateur connecté à votre VPN point à site de cloud privé.
3. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur **Connexion**.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.

5. **Dans la boîte de dialogue**Déployer le modèle OVF**, dans le champ**Déployer à partir d'un fichier**, accédez à l'emplacement où vous avez enregistré les fichiers de configuration de l'instance NetScaler VPX, sélectionnez le fichier .ovf et cliquez sur Suivant.**

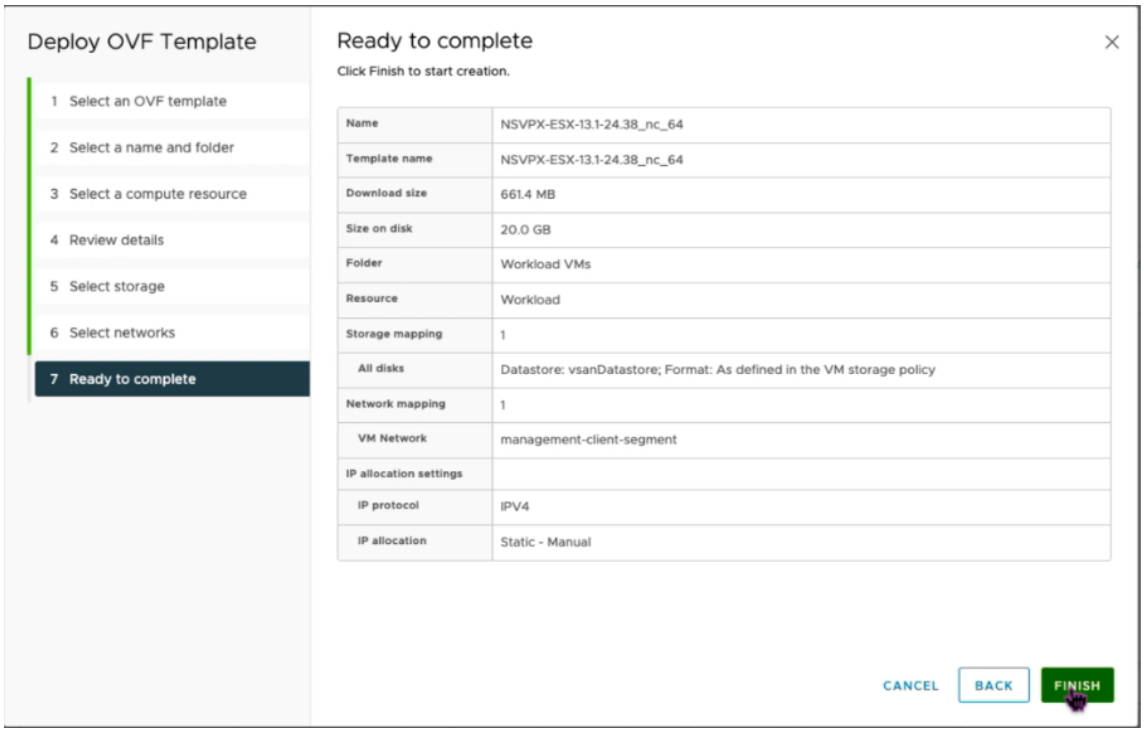
   > REMARQUE
   >
   > Par défaut, l'instance NetScaler VPX utilise les interfaces réseau E1000. Pour déployer ADC avec l'interface VMXNET3, modifiez l'OVF pour utiliser l'interface VMXNET3 au lieu de l'E1000. La disponibilité de l'interface VMXNET3 est limitée par l'infrastructure GCP et peut ne pas être disponible dans Google Cloud VMware Engine.

6. Mappez les réseaux affichés dans le modèle OVF du dispositif virtuel aux réseaux que vous avez configurés sur NSX-T Manager. Cliquez sur **OK**.

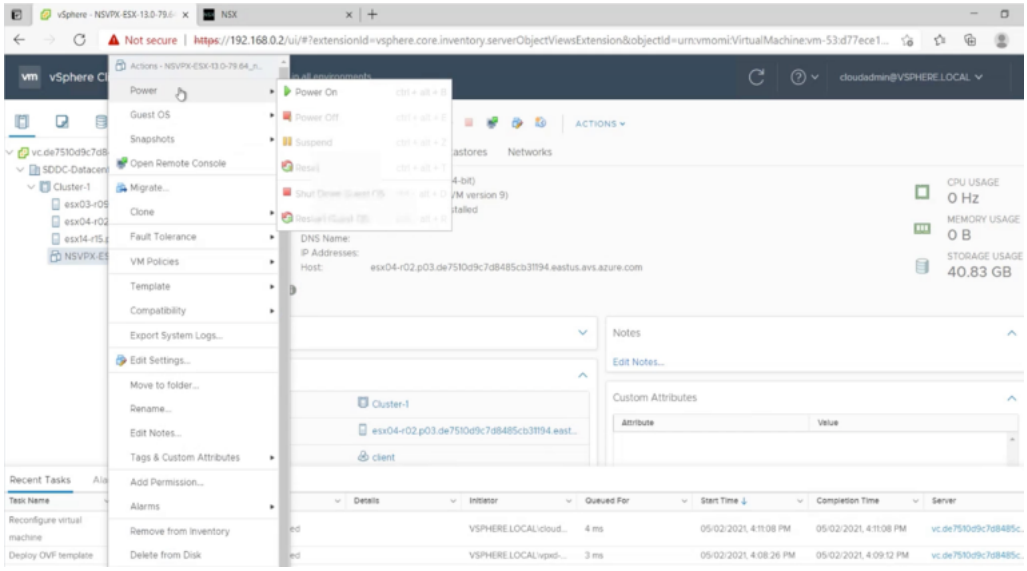




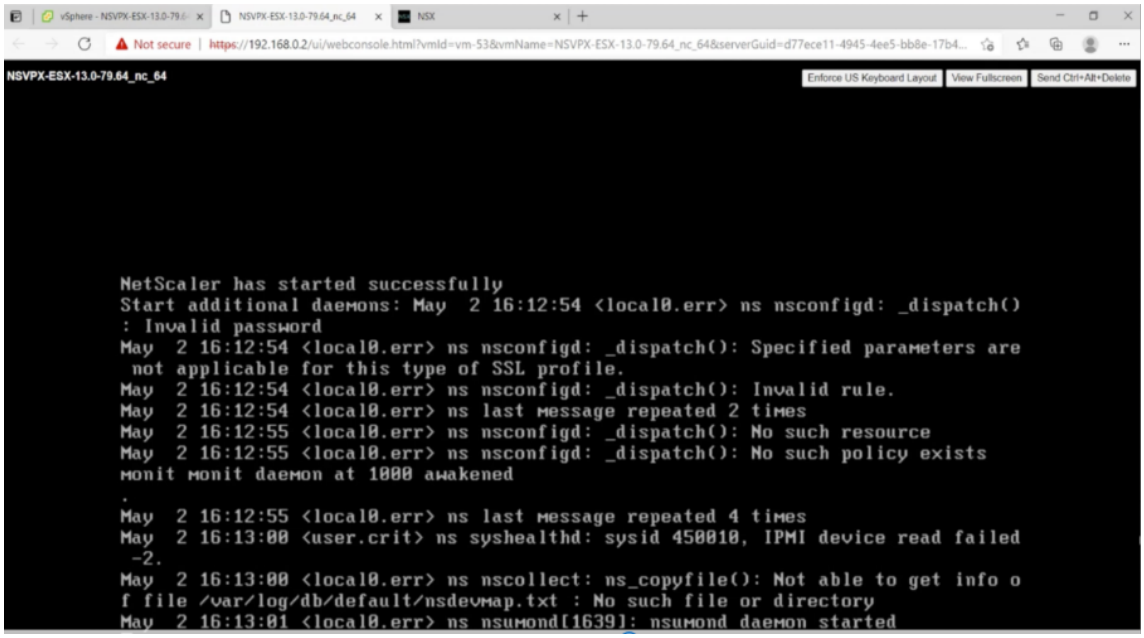
7. Cliquez sur **Terminer** pour commencer à installer une appliance virtuelle sur le cloud VMware.



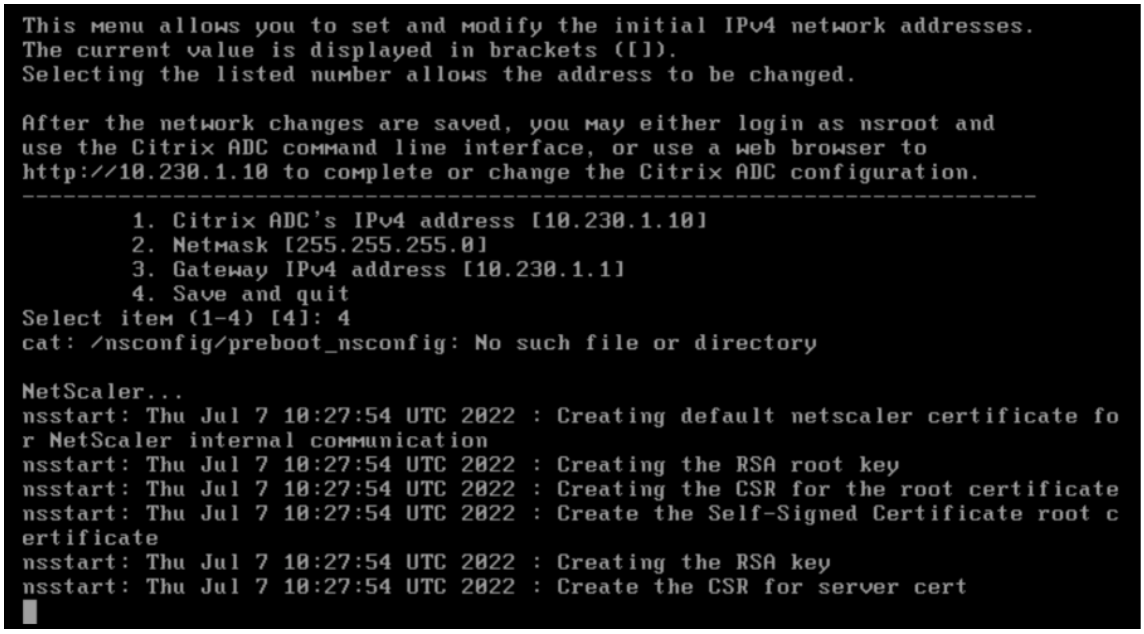
8. Vous êtes maintenant prêt à démarrer l'instance NetScaler VPX. **Dans le volet de navigation, sélectionnez l'instance NetScaler VPX que vous avez installée et, dans le menu contextuel, sélectionnez Power On.** Cliquez sur l'onglet **Lancer la console Web** pour émuler un port de console.



9. Vous êtes désormais connecté à la machine virtuelle NetScaler depuis le client vSphere.



10. Lors du premier démarrage, définissez l'adresse IP de gestion et la passerelle pour l'instance ADC.



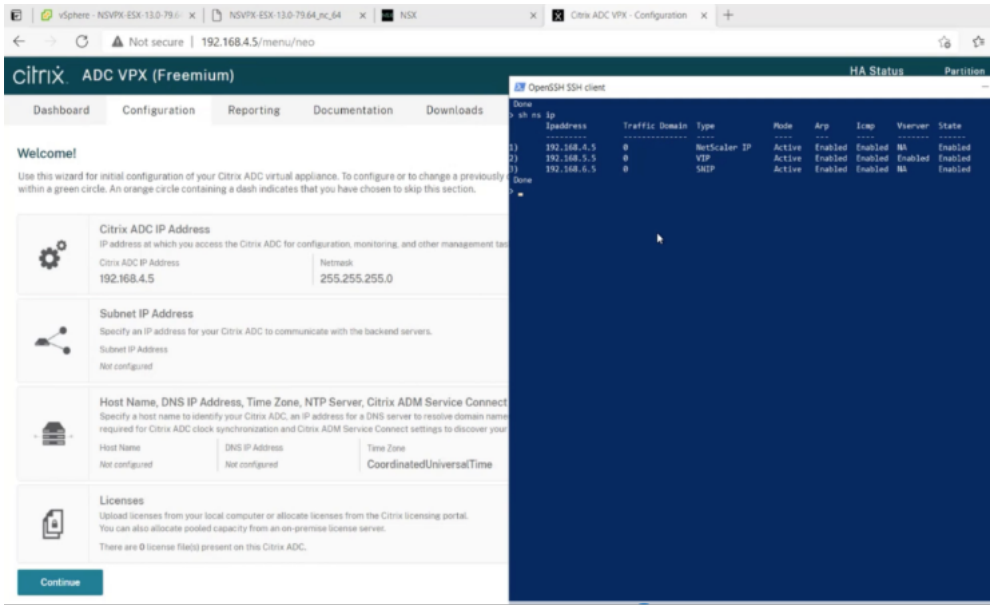
11. Pour accéder à l'appliance NetScaler à l'aide des clés SSH, tapez la commande suivante dans l'interface de ligne de commande :

```
ssh nsroot@<management IP address>
<!--NeedCopy-->
```

Exemple :

```
ssh nsroot@10.230.1.10
<!--NeedCopy-->
```

12. Vous pouvez vérifier la configuration ADC à l'aide de la `show ns ip` commande.

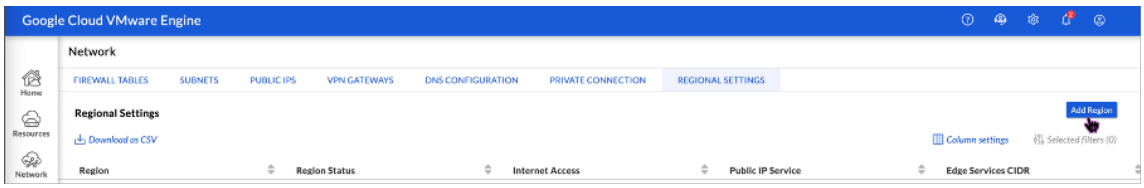


Attribuer une adresse IP publique à une instance NetScaler VPX sur le cloud VMware

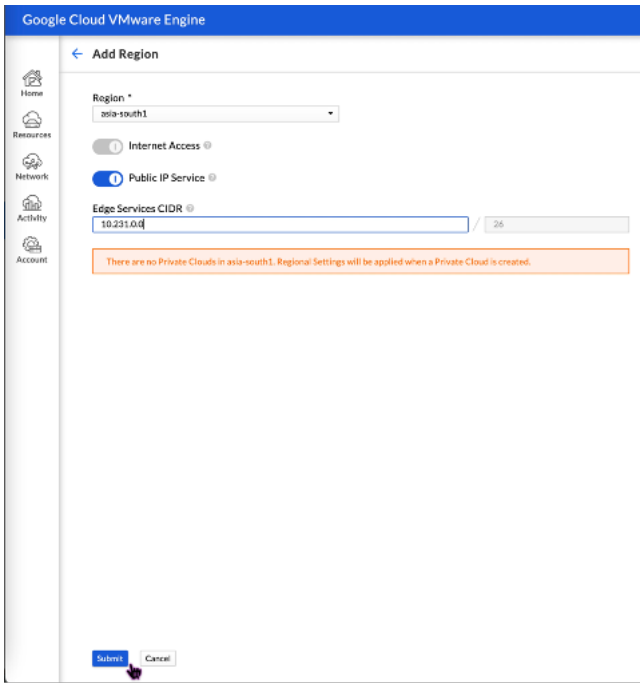
Après avoir installé et configuré l'instance NetScaler VPX sur GCVE, vous devez attribuer une adresse IP publique à l'interface client. Avant d'attribuer des adresses IP publiques à vos machines virtuelles, assurez-vous que le service IP public est activé pour votre région Google Cloud.

Pour activer le service IP public pour une nouvelle région, procédez comme suit :

1. Sur la console GCVE, accédez à **Réseau > PARAMÈTRES RÉGIONAUX > Ajouter une région**.



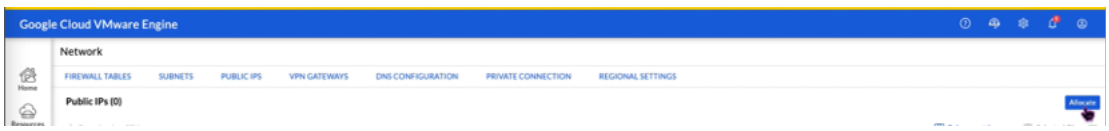
2. Sélectionnez votre région et activez l' **accès à Internet** et le **service IP public**.
3. Attribuez un CIDR Edge Services en vous assurant que la plage d'adresses CIDR ne chevauche aucun de vos sous-réseaux GCP/GCVE locaux ou autres (réseaux virtuels).



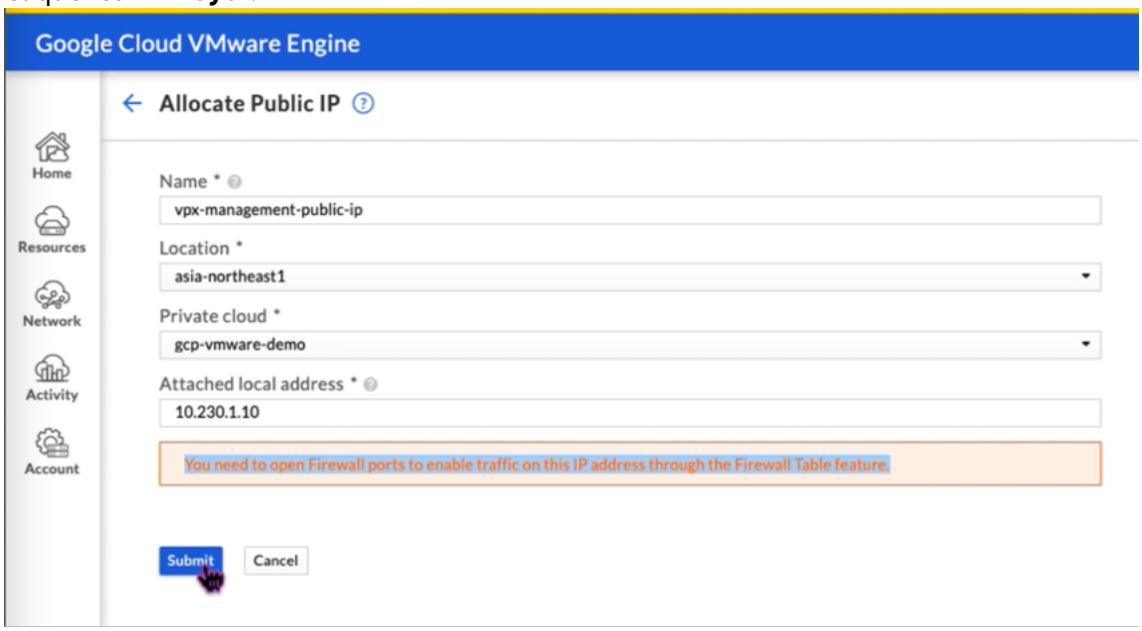
4. Le service IP public sera activé pour la région sélectionnée dans quelques minutes.

Pour attribuer une adresse IP publique à l'interface client sur l'instance NetScaler VPX sur GCVE, effectuez ces étapes sur le portail GCVE :

1. Sur la console GCVE, accédez à **Réseau > IP PUBLIC > Allouer**.



2. Entrez un nom pour l'adresse IP publique. Sélectionnez votre région et sélectionnez le cloud privé dans lequel l'adresse IP sera utilisée.
3. Fournissez l'adresse IP privée de l'interface sur laquelle vous souhaitez que l'adresse IP publique soit mappée. Il s'agira de l' **adresse IP privée** de votre interface **client** .
4. Cliquez sur **Envoyer**.



5. L'adresse IP publique est prête à être utilisée en quelques minutes.
6. Vous devez ajouter des règles de pare-feu pour autoriser l'accès à l'adresse IP publique avant de pouvoir l'utiliser. Pour plus d'informations, consultez la section Règles de pare-feu.

Ajouter un service GCP Autoscaling principal

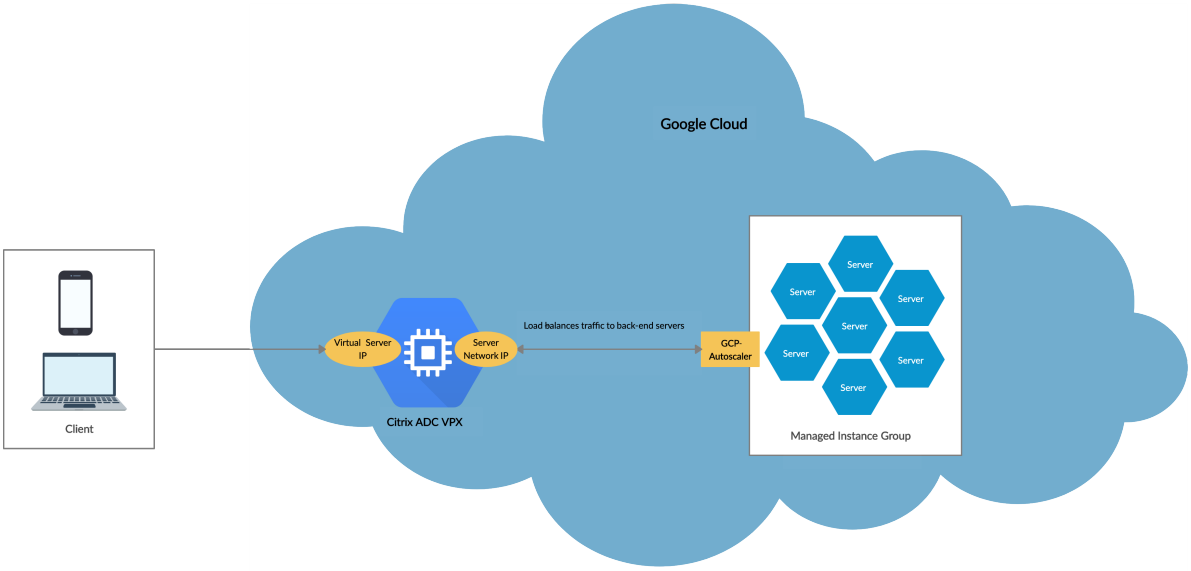
May 5, 2023

L'hébergement efficace des applications dans le cloud nécessite une gestion simple et rentable des ressources, en fonction de la demande des applications. Pour répondre à la demande croissante, vous devez augmenter les ressources du réseau. Lorsque la demande diminue, vous devez réduire vos dépenses pour éviter les coûts inutiles liés à la sous-utilisation des ressources. Pour minimiser le coût d'exécution de l'application, vous devez surveiller en permanence le trafic, la mémoire et l'utilisation du processeur, etc. Toutefois, la surveillance manuelle du trafic est fastidieuse. Pour que l'environnement d'application évolue de manière dynamique, vous devez automatiser les processus de surveillance du trafic et de mise à l'échelle des ressources lorsque cela est nécessaire.

Intégrée au service GCP Autoscaling, l'instance NetScaler VPX offre les avantages suivants :

- **Équilibre de charge et gestion** : configure automatiquement les serveurs pour qu'ils augmentent et diminuent, en fonction de la demande. L'instance VPX détecte automatiquement les groupes d'instances gérés dans le sous-réseau principal et vous permet de sélectionner les groupes d'instances gérés pour équilibrer la charge. Les adresses IP virtuelles et de sous-réseau sont configurées automatiquement sur l'instance VPX.
- **Haute disponibilité** : détecte les groupes d'instances gérés qui couvrent plusieurs zones et les serveurs d'équilibrage de charge.
- **Meilleure disponibilité du réseau** : l'instance VPX prend en charge :
  - Serveurs principaux situés dans les mêmes groupes de placement
  - Serveurs dorsaux sur différentes zones

Ce diagramme illustre le fonctionnement du service GCP Autoscaling dans une instance NetScaler VPX agissant en tant que serveur virtuel d'équilibrage de charge.

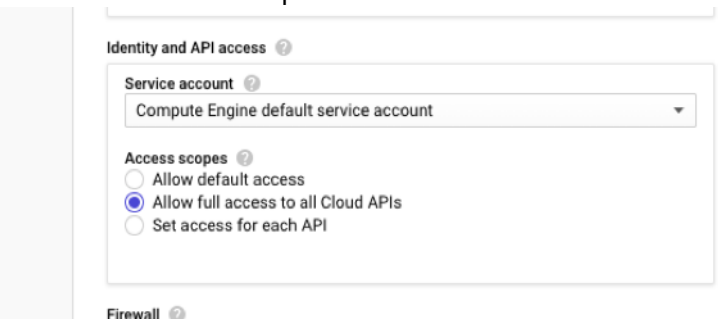


Avant de commencer

Avant de commencer à utiliser Autoscaling avec votre instance NetScaler VPX, vous devez effectuer les tâches suivantes.

- Créez une instance NetScaler VPX sur GCP en fonction de vos besoins.
  - Pour plus d'informations sur la création d'une instance NetScaler VPX, consultez Déployer une instance NetScaler VPXsur Google Cloud Platform.
  - Pour plus d'informations sur le déploiement d'instances VPX en mode HA, voir Déployer une paire haute disponibilité VPX sur Google Cloud Platform.
- Activez l'**API Cloud Resource Manager** pour votre projet GCP.

- Autorisez un accès complet à toutes les API Cloud lors de la création des instances.



- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_INSTANCE_IAM_PERMS = [

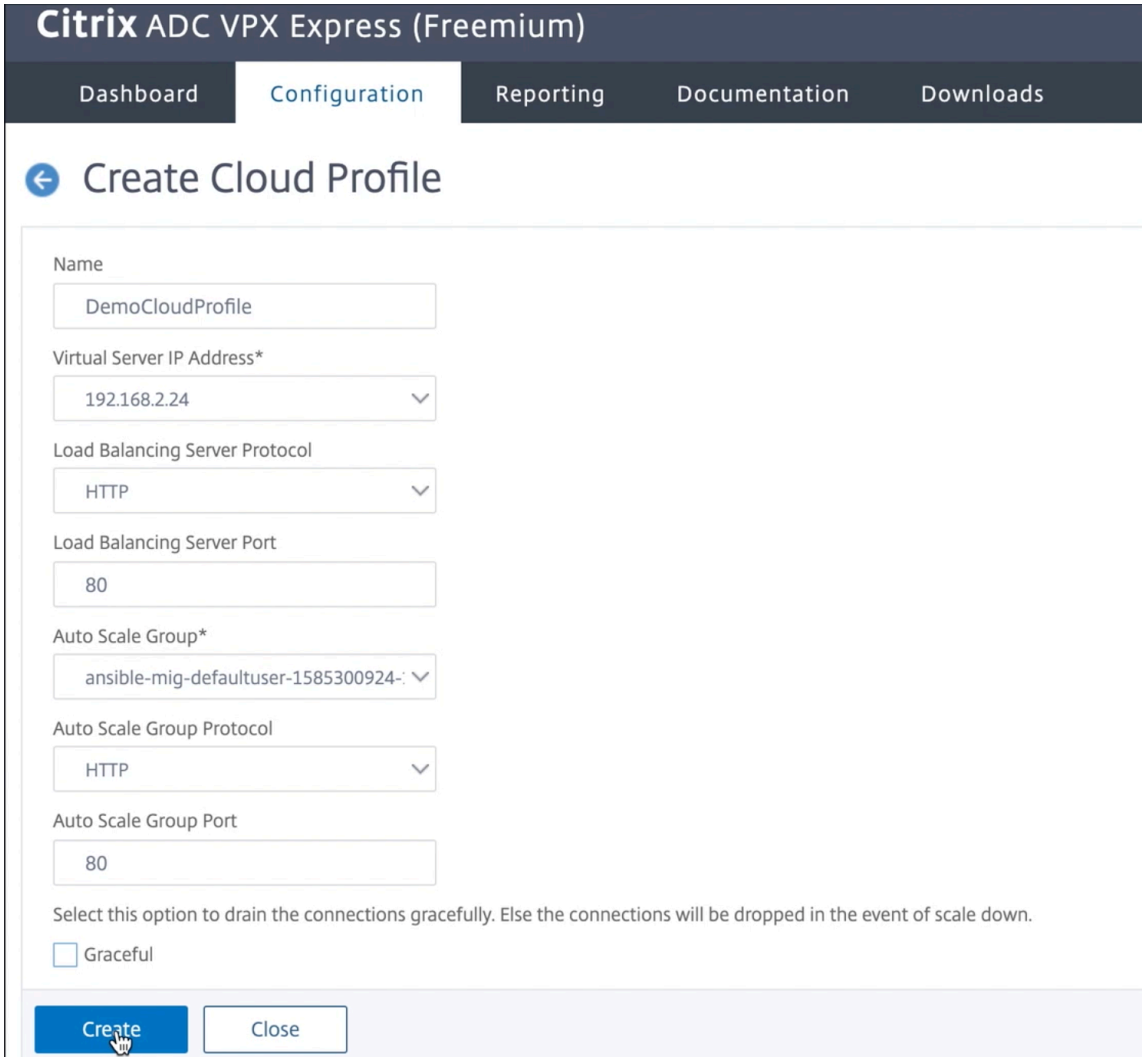
"compute.instances.get",
"compute.zones.list",
"compute.instanceGroupManagers.list",
"compute.instanceGroupManagers.get"
]
<!--NeedCopy-->
```

- Pour configurer Autoscaling, assurez-vous que les éléments suivants sont configurés :
  - Modèle d'instance
  - Groupe d'instances géré
  - Politique de mise à l'échelle automatique

Ajouter le service GCP Autoscaling à une instance NetScaler VPX

Vous pouvez ajouter le service Autoscaling à une instance VPX en un seul clic à l'aide de l'interface graphique. Procédez comme suit pour ajouter le service Autoscaling à l'instance VPX :

1. Connectez-vous à l'instance VPX à l'aide de vos informations d'identification pour `nsroot`.
2. Lorsque vous vous connectez à l'instance NetScaler VPX pour la première fois, la page Cloud Profile par défaut s'affiche. Sélectionnez le groupe d'instances géré par GCP dans le menu déroulant et cliquez sur **Créer** pour créer un profil cloud.

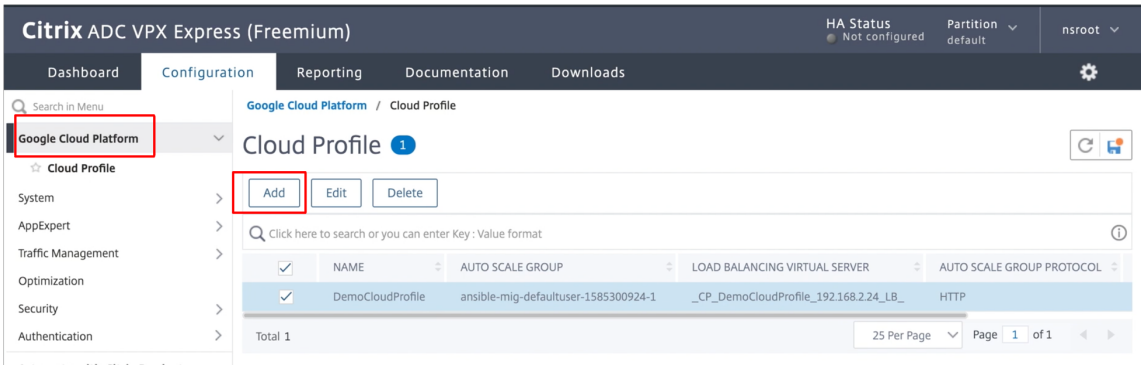


- Le champ **Adresse IP du serveur virtuel** est automatiquement renseigné à partir de toutes les adresses IP associées aux instances.
- Le **groupe Autoscale** est prérempli à partir du groupe d'instances géré configuré sur votre compte GCP.
- Lorsque vous sélectionnez le **protocole de groupe de mise** à l'**échelle automatique et le port de groupe**de mise à l'échelle automatique, assurez-vous que vos serveurs écoutent le protocole et les ports configurés. Liez le moniteur approprié au groupe de services. Par défaut, le moniteur TCP est utilisé.
- Décochez la case **Graceful** car elle n'est pas prise en charge.

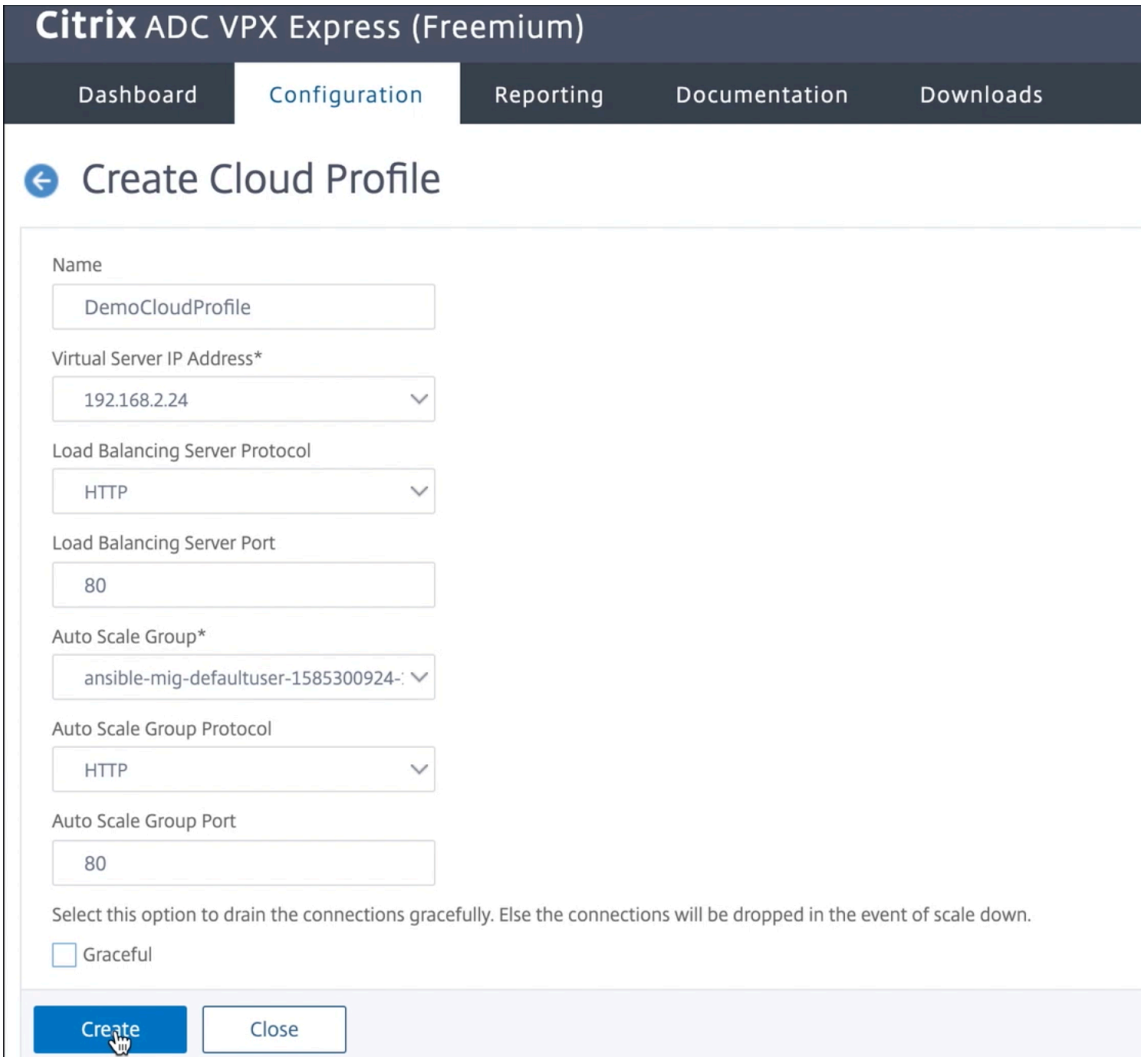
> Remarque :
>
> Pour le protocole SSL Autoscaling, une fois le profil cloud créé, le serveur virtuel ou le groupe de services d'équilibrage de charge est hors service en raison d'un certificat manquant. Vous pouvez lier manuellement le certificat au serveur virtuel ou au groupe de ser-

vices.

3. Après la première connexion, si vous souhaitez créer un profil cloud, dans l'interface graphique, accédez à **Système > Google Cloud Platform > Profil cloud** et cliquez sur **Ajouter**.



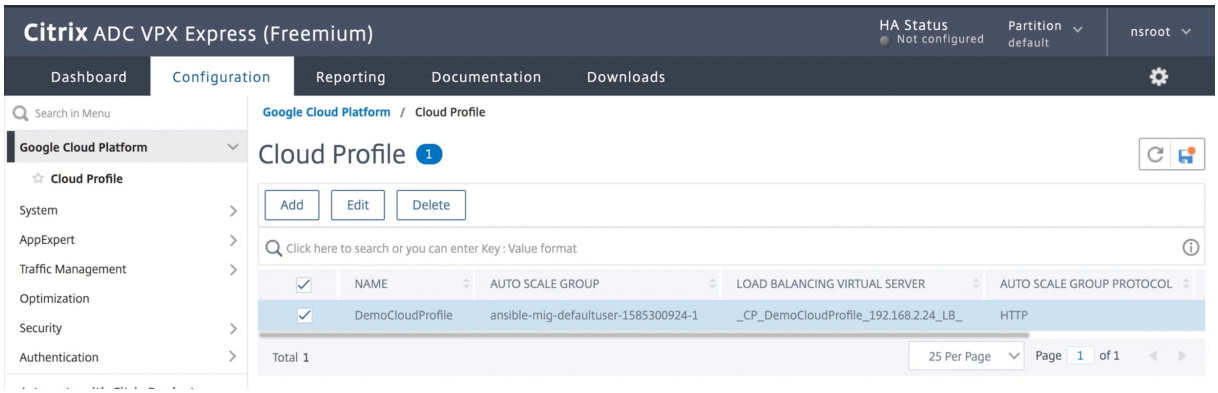
La page de configuration de **Create Cloud Profile** s'affiche.



Cloud Profile crée un serveur virtuel d'équilibrage de charge NetScaler et un groupe de services

dont les membres sont les serveurs du groupe d'instances géré. Vos serveurs back-end doivent être accessibles via le SNIP configuré sur l'instance VPX.

> **Remarque :**
>
> À partir de la version 13.1-42.x de NetScaler, vous pouvez créer différents profils cloud pour différents services (en utilisant différents ports) avec le même groupe d'instances géré dans GCP. Ainsi, l'instance NetScaler VPX prend en charge plusieurs services avec le même groupe Autoscaling dans le cloud public.



Support de dimensionnement VIP pour l'instance NetScaler VPX sur GCP

May 5, 2023

Une appliance NetScaler se trouve entre les clients et les serveurs, de sorte que les demandes des clients et les réponses du serveur passent par elle. Dans une installation classique, les serveurs virtuels configurés sur l'appliance fournissent des points de connexion que les clients utilisent pour accéder aux applications derrière l'appliance. Le nombre d'adresses IP virtuelles (VIP) publiques nécessaires pour un déploiement varie au cas par cas.

L'architecture GCP limite chaque interface de l'instance à connecter à un VPC différent. Un VPC sur GCP est un ensemble de sous-réseaux, et chaque sous-réseau peut s'étendent sur plusieurs zones d'une région. De plus, GCP impose la limitation suivante :

- Il existe un mappage 1:1 du nombre d'adresses IP publiques au nombre de cartes réseau. Une seule adresse IP publique peut être attribuée à une carte réseau.
- Un maximum de 8 cartes réseau peuvent être attachées à un type d'instance de capacité supérieure.

Par exemple, une instance n1-standard-2 ne peut avoir que 2 cartes réseau, et les VIP publics pouvant être ajoutés sont limités à 2. Pour plus d'informations, consultez Quotas de ressources VPC.

Pour obtenir des échelles plus élevées d'adresses IP virtuelles publiques sur une instance NetScaler VPX, vous pouvez configurer les adresses VIP dans le cadre des métadonnées de l'instance. L'instance NetScaler VPX utilise en interne les règles de transfert fournies par le GCP pour réaliser le dimensionnement VIP. L'instance NetScaler VPX fournit également une haute disponibilité aux VIP configurés. Une fois que vous avez configuré les adresses VIP dans le cadre des métadonnées, vous pouvez configurer un serveur virtuel LB à l'aide de la même adresse IP que celle utilisée pour créer les règles de transfert. Ainsi, nous pouvons utiliser des règles de transfert pour atténuer les limites d'échelle liées à l'utilisation d'adresses VIP publiques sur une instance NetScaler VPX sur GCP.

Pour plus d'informations sur les règles de transfert, voir Vue d'ensemble des règles de transfert.

Pour plus d'informations sur HA, voir Haute disponibilité.

Points à noter

- Google facture des frais supplémentaires pour chaque règle de transfert d'adresse IP virtuelle. Le coût réel dépend du nombre d'entrées créées. Le coût associé est disponible dans les documents de tarification de Google.
- Les règles de transfert ne s'appliquent qu'aux VIP publics. Vous pouvez utiliser des adresses IP d'alias lorsque le déploiement a besoin d'adresses IP privées en tant que VIP.
- Vous pouvez créer des règles de transfert uniquement pour les protocoles qui nécessitent le serveur virtuel LB. Les VIP peuvent être créés, mis à jour ou supprimés à la volée. Vous pouvez également ajouter un nouveau serveur virtuel d'équilibrage de charge avec la même adresse VIP, mais avec un protocole différent.

Avant de commencer

- L'instance NetScaler VPX doit être déployée sur GCP.
- L'adresse IP externe doit être réservée. Pour plus d'informations, voir Réservation d'une adresse IP externe statique.
- Assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
```



```
"compute.targetInstances.create"
"compute.targetInstances.get"
"compute.targetInstances.use",
]

<!--NeedCopy-->
```

- Activez l'**API Cloud Resource Manager** pour votre projet GCP.
- Si vous utilisez la mise à l'échelle VIP sur une instance VPX autonome, assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create",
"compute.targetInstances.list",
"compute.targetInstances.use",
]
<!--NeedCopy-->
```

- Si vous utilisez la mise à l'échelle VIP en mode haute disponibilité, assurez-vous que votre compte de service GCP dispose des autorisations IAM suivantes :

```
REQUIRED_IAM_PERMS = [
"compute.addresses.get",
"compute.addresses.list",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.use",
"compute.instances.get",
"compute.instances.list",
"compute.instances.setMetadata",
"compute.subnetworks.use",
```



```
"compute.targetInstances.create",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.zones.list",
]
<!--NeedCopy-->
```

> Remarque :
>
> En mode haute disponibilité, si votre compte de service n'a pas de rôle de propriétaire ou d'éditeur, vous devez ajouter le **rôle d'utilisateur du compte de service** à votre compte de service.

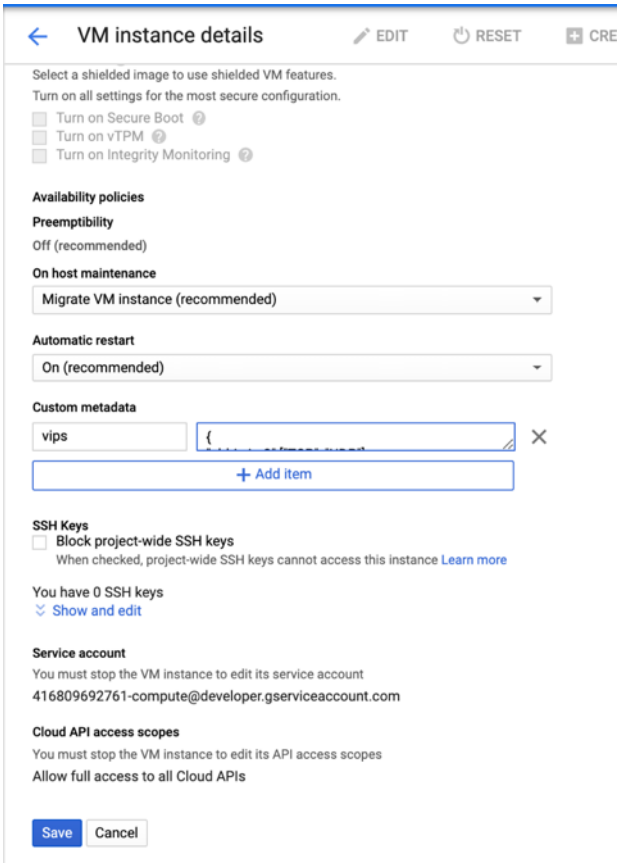
Configurer des adresses IP externes pour le dimensionnement VIP sur une instance NetScaler VPX

1. Dans la console Google Cloud, accédez à la page **Instances de machine virtuelle** .
2. Créez une nouvelle instance de machine virtuelle ou utilisez une instance existante.
3. Cliquez sur le nom de l'instance. Sur la page des **détails de l'instance de machine virtuelle**, cliquez sur **Modifier**.
4. Mettez à jour les **métadonnées personnalisées** en saisissant ce qui suit :
   - Clé = VIP
   - Valeur = Fournir une valeur au format JSON suivant :

     {
     « Nom de l'adresse IP externe réservée » : [liste des protocoles],
     }

   GCP prend en charge les protocoles suivants :

   - AH
   - ESP
   - ICMP
   - SCT
   - TCP
   - UDP



Pour plus d'informations, voir Métadonnées personnalisées.

Exemple de métadonnées personnalisées :

{
"external-ip1-name":["TCP", "UDP"],
"external-ip2-name":["ICMP", "AH"]
}

Dans cet exemple, l'instance NetScaler VPX crée en interne une règle de transfert pour chaque paire de protocoles IP. Les entrées de métadonnées sont mappées aux règles de transfert. Cet exemple vous aide à comprendre le nombre de règles de transfert créées pour une entrée de métadonnées.

Quatre règles de transfert sont créées comme suit :

a) nom-ip1-externe et TCP
b) nom-ip1-externe et UDP
c) nom-ip2 externe et ICMP
d) nom-ip2 externe et AH

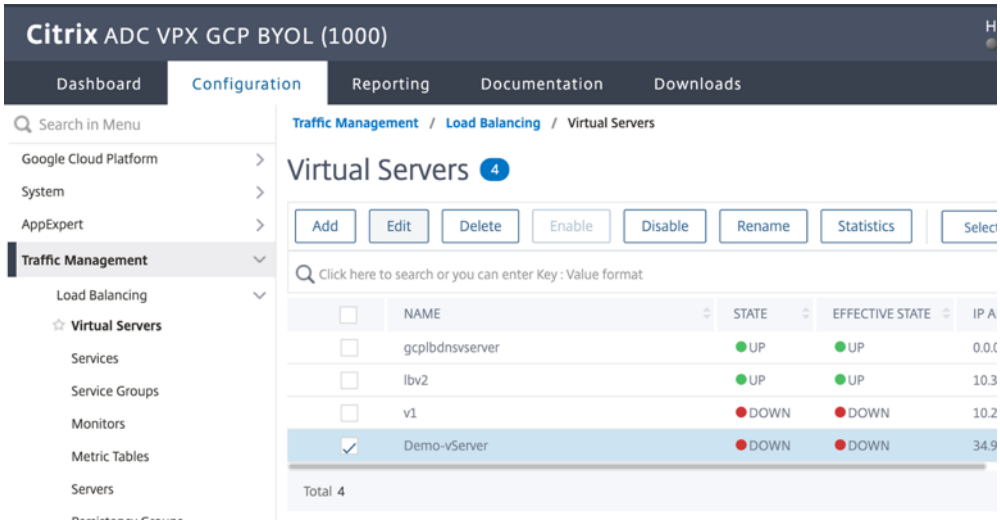
> Remarque :
>
> En mode HA, vous devez ajouter des métadonnées personnalisées uniquement sur l'instance principale. En cas de basculement, les métadonnées personnalisées sont synchronisées avec le nouveau serveur principal.

5. Cliquez sur **Enregistrer**.

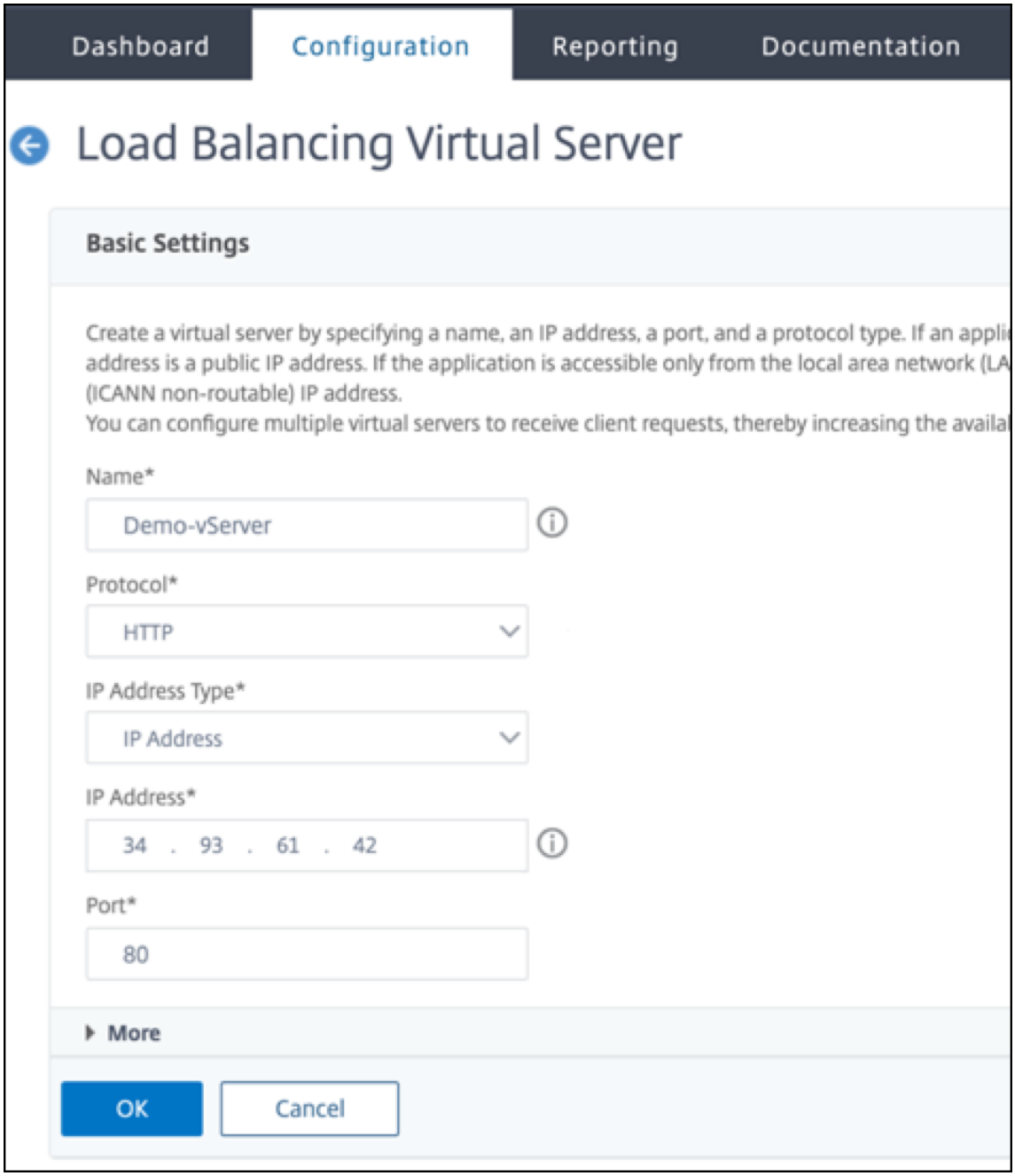
Configuration d'un serveur virtuel d'équilibrage de charge avec adresse IP externe sur une instance NetScaler VPX

Étape 1. Ajoutez un serveur virtuel d'équilibrage de charge.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Ajouter**.

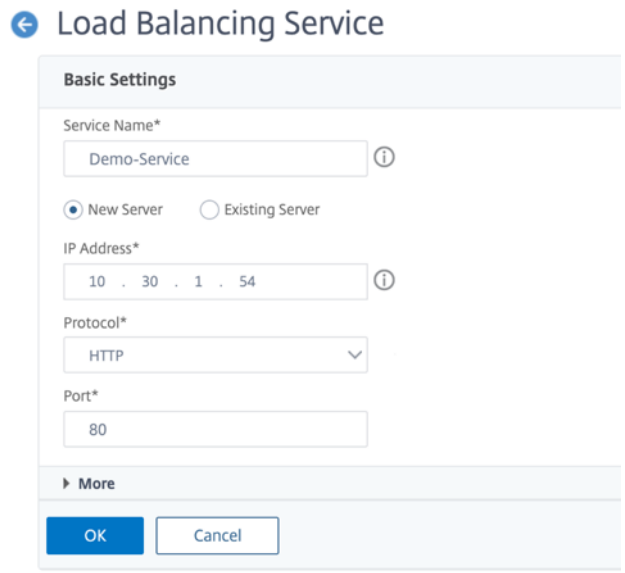


2. Ajoutez les valeurs requises pour le nom, le protocole, le type d'adresse IP (adresse IP), l'adresse IP (adresse IP externe de la règle de transfert ajoutée en tant que VIP sur ADC) et le port, puis cliquez sur **OK**.



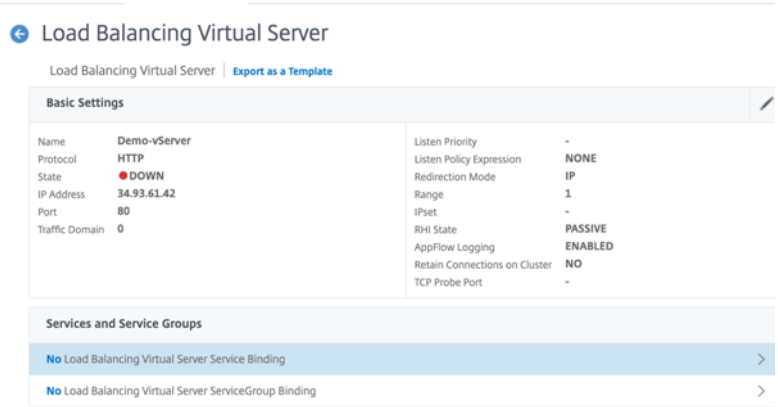
Étape 2 Ajoutez un service ou un groupe de services.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Services > Ajouter**.
2. Ajoutez les valeurs requises pour le nom de service, l'adresse IP, le protocole et le port, puis cliquez sur **OK**.

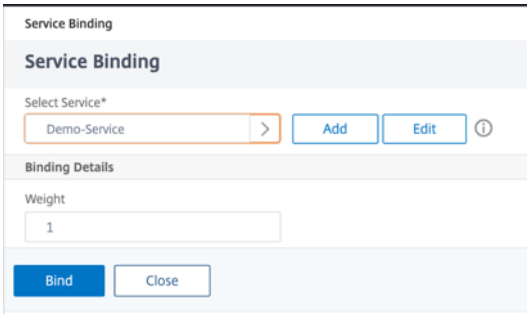


Étape 3. Liez le service ou le groupe de services au serveur virtuel d'équilibrage de charge.

1. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel d'équilibrage de charge configuré à **l'étape 1**, puis cliquez sur **Modifier**.
3. Dans la page **Groupes de services et de services**, cliquez sur **Liaison de service de serveur virtuel sans équilibrage de charge**.



4. Sélectionnez le service configuré à l' **étape 3**, puis cliquez sur **Lier**.



5. Enregistrez la configuration.

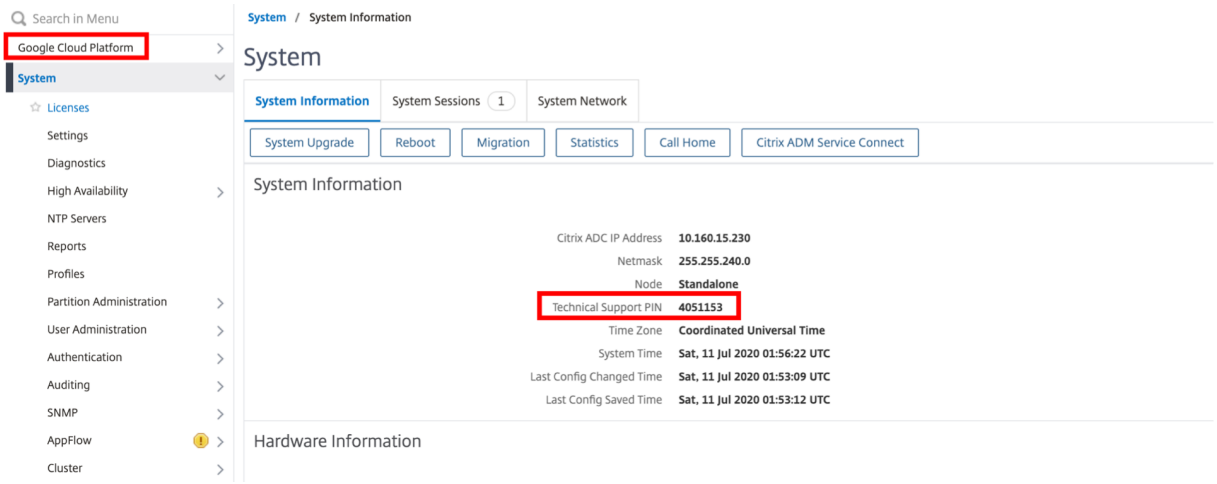
Dépannage d'une instance VPX sur GCP

May 5, 2023

Google Cloud Platform (GCP) fournit un accès console à une instance NetScaler VPX. Vous ne pouvez déboguer que si le réseau est connecté. Pour consulter le journal système d'une instance, accédez à la console et consultez **les fichiers journaux système**.

NetScaler prend en charge les instances NetScaler VPX payantes (licence utilitaire avec tarif horaire) sur GCP. Pour déposer une demande d'assistance, recherchez votre numéro de compte GCP et votre code PIN d'assistance, puis appelez le support NetScaler. Il vous est demandé de fournir votre nom et votre adresse e-mail. Pour trouver le code PIN d'assistance, connectez-vous à l'interface graphique VPX et accédez à la page **Système** .

Voici un exemple de page système montrant le code PIN de support.



Trames Jumbo sur les instances NetScaler VPX

May 5, 2023

Les appliances NetScaler VPX prennent en charge la réception et la transmission de trames jumbo contenant jusqu'à 9 216 octets de données IP. Les trames Jumbo peuvent transférer des fichiers volumineux plus efficacement qu'il n'est possible avec la taille MTU IP standard de 1 500 octets.

Une appliance NetScaler peut utiliser des trames jumbo dans les scénarios de déploiement suivants :

- De Jumbo à Jumbo. L'appliance reçoit les données sous forme de trames Jumbo et les envoie sous forme de trames Jumbo.
- Non-Jumbo vers Jumbo. L'appliance reçoit les données sous forme de trames normales et les envoie sous forme de trames jumbo.
- Jumbo à Non-Jumbo. L'appliance reçoit les données sous forme de trames jumbo et les envoie en tant que trames régulières.

Pour plus d'informations, consultez la sectionConfiguration de la prise en charge des Jumbo Frames sur une appliance NetScaler.

La prise en charge des trames Jumbo est disponible sur les appliances NetScaler VPX exécutées sur les plateformes de virtualisation suivantes :

- VMware ESX
- Plateforme Linux-KVM
- Citrix XenServer
- Amazon Web Services (AWS)

Les trames Jumbo sur les appliances VPX fonctionnent de la même manière que les trames Jumbo sur les appliances MPX. Pour plus d'informations sur les cadres Jumbo et leurs cas d'utilisation, consultez la section Configuration des cadres Jumbo sur des appliances MPX. Les cas d'utilisation des trames jumbo sur les appliances MPX s'appliquent également aux appliances VPX.

Configurer des trames jumbo pour une instance VPX exécutée sur VMware ESX

Effectuez les tâches suivantes pour configurer des trames jumbo sur une appliance NetScaler VPX exécutée sur le serveur VMware ESX :

1. Définissez la MTU de l'interface ou du canal de l'appliance VPX sur une valeur comprise entre 1501—9000. Utilisez l'interface de ligne de commande ou l'interface graphique pour définir la taille de la MTU. Les appliances NetScaler VPX exécutées sur VMware ESX prennent en charge la réception et la transmission de trames jumbo contenant jusqu'à 9 000 octets de données IP.
2. Définissez la même taille MTU sur les interfaces physiques correspondantes du serveur VMware ESX à l'aide de ses applications de gestion. Pour plus d'informations sur la définition de la taille

du MTU sur les interfaces physiques de VMware ESX, voir http://vmware.com/.

Configurer des trames jumbo pour une instance VPX exécutée sur un serveur Linux-KVM

Effectuez les tâches suivantes pour configurer des trames jumbo sur une appliance NetScaler VPX exécutée sur un serveur Linux-KVM :

1. Définissez le MTU de l'interface ou du canal de l'appliance VPX sur une valeur comprise entre 1501 et 9216. Utilisez la CLI ou l'interface graphique NetScaler VPX pour définir la taille de la MTU.
2. Définissez la même taille de MTU sur les interfaces physiques correspondantes d'un serveur Linux-KVM à l'aide de ses applications de gestion. Pour plus d'informations sur la définition de la taille de la MTU sur les interfaces physiques de Linux-KVM, consultez. http://www.linux-kvm.org/

Configurer des trames jumbo pour une instance VPX exécutée sur Citrix XenServer

Effectuez les tâches suivantes pour configurer des trames jumbo sur une appliance NetScaler VPX exécutée sur Citrix XenServer :

1. Connectez-vous au XenServer à l'aide de XenCenter.
2. Arrêtez toutes les instances VPX qui utilisent les réseaux pour lesquels le MTU doit être modifié.
3. Dans l'onglet **Réseau**, sélectionnez le réseau - réseau 0/1/2.
4. Sélectionnez **Propriétés** et modifiez MTU.

Après avoir configuré les trames jumbo sur XenServer, vous pouvez configurer les trames jumbo sur l'appliance ADC. Pour plus d'informations, consultez la sectionConfiguration de la prise en charge des Jumbo Frames sur une appliance NetScaler.

Configurer des trames jumbo pour une instance VPX exécutée sur AWS

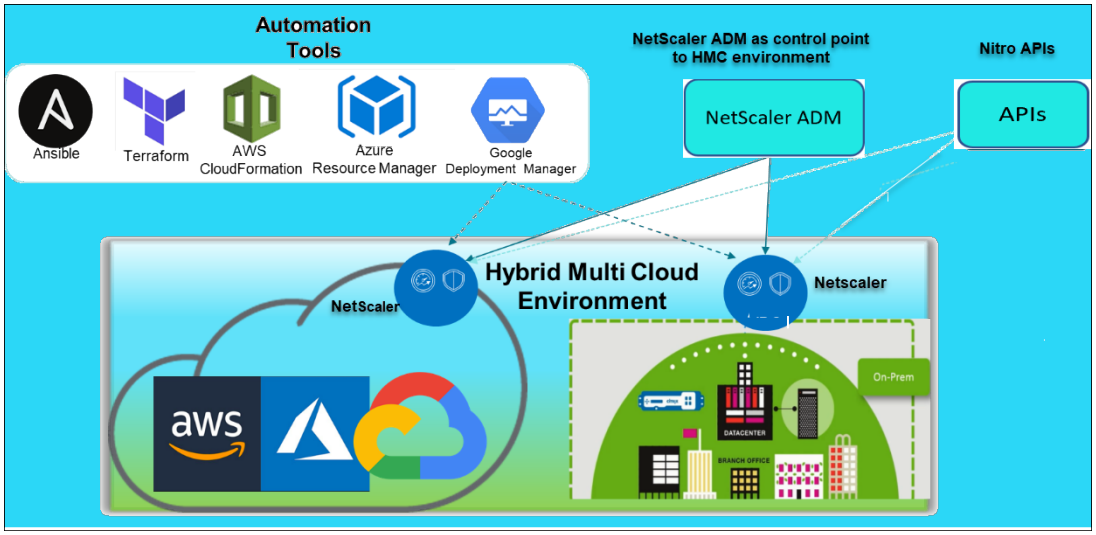
La configuration au niveau de l'hôte n'est pas requise pour VPX sur Azure. Pour configurer les Jumbo Frames sur VPX, suivez les étapes décrites dans Configuration de la prise en charge des Jumbo Frames sur uneappliance NetScaler.

Automatisez le déploiement et les configurations de NetScaler

June 20, 2023

NetScaler fournit plusieurs outils pour automatiser vos déploiements et configurations ADC. Ce document fournit un bref résumé des différents outils d'automatisation et des références aux différentes ressources d'automatisation que vous pouvez utiliser pour gérer les configurations de ADC.

L'illustration suivante fournit une vue d'ensemble de l'automatisation NetScaler dans un environnement hybride multicloud (HMC).



Automatisez NetScaler à l'aide de NetScaler ADM

NetScaler ADM agit comme un point de contrôle d'automatisation pour votre infrastructure ADC distribuée. NetScaler ADM fournit un ensemble complet de fonctionnalités d'automatisation allant du provisionnement des appliances ADC à leur mise à niveau. Voici les principales fonctionnalités d'automatisation d'ADM :

- Provisioning d'instances NetScaler VPX sur AWS
- Provisioning d'instances NetScaler VPX sur Azure
- StyleBooks
- Tâches de configuration
- Audit de configuration
- Mises à niveau ADC
- Gestion des certificats SSL
- Intégrations - Intégrations [GitHub](/fr-fr/citrix-application-delivery-management-service/stylebooks/impor and-synchronizing-stylebooks-from-github-repository.html), [ServiceNow](/fr-fr/citrix-application-delivery-management-service/setting-up/integrate-itsm-adapter-citrix-adm-servicenow.html), notifications d'événements

Blogs et vidéos de NetScaler ADM sur l'automatisation

- Migrations d'applications à l'aide

- Intégrez les configurations ADC avec CI/CD à l'aide des StyleBooks ADM
- Simplification des déploiements NetScaler dans le cloud public grâce à ADM
- 10 manières dont le service NetScaler ADM facilite les mises à niveau de NetScaler

NetScaler ADM fournit également des API pour ses différentes fonctionnalités qui intègrent NetScaler ADM et NetScaler dans le cadre de l'automatisation informatique globale. Pour plus d'informations, consultez la section API du service NetScaler ADM.

Automatisez NetScaler à l'aide de Terraform

Terraform est un outil qui prend l'infrastructure en tant qu'approche de code pour fournir et gérer le cloud, l'infrastructure ou le service. Les ressources NetScaler Terraform sont disponibles sur GitHub pour être utilisées. Consultez GitHub pour obtenir une documentation et une utilisation détaillées.

- Modules NetScaler Terraform pour configurer l'ADC pour divers cas d'utilisation tels que l'équilibrage de charge et le GSLB
- Scripts cloud Terraform pour déployer ADC dans AWS
- Scripts cloud Terraform pour déployer ADC dans Azure
- Scripts cloud Terraform pour déployer ADC dans GCP
- Déploiement bleu-vert à l'aide de pipelines NetScaler VPX et Azure

Blogs et vidéos sur Terraform pour l'automatisation ADC

- Automatisez vos déploiements NetScaler avec Terraform
- Provisionner et configurer ADC dans la configuration HA dans AWS à l'aide de Terraform

Automatisez NetScaler à l'aide de Consul-Terraform-Sync

Le module NetScaler Consul-Terraform-Sync (CTS) permet aux équipes d'applications d'ajouter ou de supprimer automatiquement de nouvelles instances de services dans NetScaler. Il n'est pas nécessaire d'envoyer des tickets manuels aux administrateurs informatiques ou aux équipes réseau pour apporter les modifications nécessaires aux configurations ADC.

- Module NetScaler Consul-Terraform-Sync pour l'automatisation de l'infrastructure réseau
- Webinaire conjoint entre Citrix-HashiCorp : mise en réseau dynamique avec Consul-Terraform-Sync pour Terraform Enterprise et NetScaler

Automatisez NetScaler à l'aide d'Ansible

Ansible est un outil open source de provisionnement de logiciels, de gestion de la configuration et de déploiement d'applications permettant l'infrastructure en tant que code. Les modules NetScaler An-

sible et des exemples de playbooks peuvent être consultés sur GitHub. Consultez GitHub pour obtenir une documentation et une utilisation détaillées.

- Modules Ansible pour configurer l'ADC
- Documentation et guide de référence des modules ADC Ansible
- Modules Ansible pour ADM

Citrix est un partenaire certifié Ansible Automation. Les utilisateurs abonnés à Red Hat Ansible Automation Platform peuvent accéder aux collections NetScaler depuis Red HatAutomation Hub.

Blogs d'automatisation Terraform et Ansible

- Citrix nommé partenaire d'intégration HashiCorp de l'année
- Citrix est désormais un partenaire certifié Red Hat Ansible Automation Platform
- Terraform et Ansible Automation pour la mise à disposition et la sécurité des applications

Modèles de cloud public pour les déploiements ADC

Les modèles de cloud public simplifient le provisionnement de vos déploiements dans les clouds publics. Différents modèles NetScaler sont disponibles pour différents environnements. Pour plus de détails sur l'utilisation, reportez-vous aux référentiels GitHub respectifs.

CFT AWS :

- Les CFT vont provisionner NetScaler VPX sur AWS

Modèles Azure Resource Manager (ARM) :

- Modèles ARM pour provisionner NetScaler VPX sur Azure

Modèles Google Cloud Deployment Manager (GDM) :

- Modèles GDM pour provisionner NetScaler VPX sur Google

Vidéos sur les modèles

- Déployer NetScaler HA dans AWS à l'aide du modèle CloudFormation
- Déployez NetScaler HA dans les zones de disponibilité à l'aide d'AWS QuickStart
- Déploiement de NetScaler HA dans GCP à l'aide de modèles GDM

Démarrages rapides AWS

- Démarrage rapide de NetScaler Web App Firewall
- Démarrage rapide d'AWS pour NetScaler VPX pour les applications Web sur AWS

API NITRO

Le protocole NetScaler NITRO vous permet de configurer et de surveiller par programmation l'appliance NetScaler à l'aide des interfaces REST (Representational State Transfer). Par conséquent, les applications NITRO peuvent être développées dans n'importe quel langage de programmation. Pour les applications qui doivent être développées en Java, .NET ou Python, les API NITRO sont exposées par le biais de bibliothèques pertinentes qui sont empaquetées sous forme de kits de développement logiciel (SDK) distincts.

- Documentation de l'API NITRO
- Référence de l'API NetScaler
- Exemple de configuration de cas d'utilisation d'ADC à NITRO aide de

FAQ

July 31, 2023

La section suivante vous aide à classer les questions fréquentes en fonction de Citrix Application Delivery Controller (ADC) VPX.

- Fonctionnalité et fonctionnalité
- Encryption
- Prix et emballage
- NetScaler VPX Express
- Hyperviseur
- Planification ou dimensionnement des capacités
- Configuration système requise
- Autres FAQ techniques

Fonctionnalité et fonctionnalité

Qu'est-ce que NetScaler VPX ?

NetScaler VPX est une appliance ADC virtuelle qui peut être hébergée sur un hyperviseur installé sur des serveurs conformes aux normes du secteur.

NetScaler VPX inclut-il toutes les fonctionnalités d'optimisation des applications Web sous forme d'appliances ADC ?

Oui. NetScaler VPX inclut toutes les fonctionnalités d'équilibrage de charge, de gestion du trafic, d'accélération des applications, de sécurité des applications (y compris NetScaler Gateway et Citrix Application Firewall) et de déchargement. Pour une présentation complète des fonctionnalités de NetScaler, voir Application Delivery your way.

Le pare-feu d'applications Citrix est-il soumis à des limites lors de son utilisation sur NetScaler VPX ?

Le pare-feu d'applications Citrix sur NetScaler VPX fournit les mêmes protections de sécurité que sur les appliances NetScaler. Les performances ou le débit de Citrix Application Firewall varient selon la plate-forme.

Existe-t-il des différences entre NetScaler Gateway sur NetScaler VPX et NetScaler Gateway sur des appliances NetScaler ?

Sur le plan fonctionnel, ils sont identiques. NetScaler Gateway sur NetScaler VPX prend en charge toutes les fonctionnalités de NetScaler Gateway disponibles dans la version 9.1 du logiciel NetScaler. Toutefois, étant donné que les appliances NetScaler fournissent du matériel d'accélération SSL dédié, elles offrent une évolutivité VPN SSL supérieure à celle d'une instance NetScaler VPX.

Outre la différence évidente liée à la possibilité de s'exécuter sur un hyperviseur, en quoi NetScaler VPX diffère-t-il des appliances physiques NetScaler ?

Il existe deux principaux domaines dans lesquels les clients constatent des différences de comportement. La première est que NetScaler VPX ne peut pas offrir les mêmes performances que de nombreuses appliances NetScaler. La seconde est que si les appliances NetScaler intègrent leurs propres fonctionnalités réseau L2, NetScaler VPX s'appuie sur l'hyperviseur pour ses services réseau L2. En général, cela ne limite pas la manière dont NetScaler VPX peut être déployé. Certaines fonctionnalités L2 configurées sur une appliance NetScaler physique peuvent devoir être configurées sur l'hyperviseur sous-jacent.

Quel est le rôle de NetScaler VPX sur le marché de la diffusion d'applications ?

NetScaler VPX change la donne sur le marché de la fourniture d'applications de la manière suivante :

- En rendant une appliance NetScaler encore plus abordable, NetScaler VPX permet à toute organisation informatique de déployer une appliance NetScaler. Il ne s'agit pas uniquement de leurs applications Web les plus critiques, mais également de toutes leurs applications Web.

- NetScaler VPX permet aux clients de faire davantage converger la mise en réseau et la virtualisation au sein de leurs centres de données. NetScaler VPX ne peut pas uniquement être utilisé pour optimiser les applications Web hébergées sur des serveurs virtualisés. Il permet également à la livraison d'applications Web elle-même de devenir un service virtualisé qui peut être facilement et rapidement déployé n'importe où. Les organisations informatiques utilisent les processus standard du centre de données pour des tâches telles que le provisionnement, l'automatisation et la rétrofacturation pour l'infrastructure de distribution d'applications Web.
- NetScaler VPX ouvre la voie à de nouvelles architectures de déploiement qui ne sont pas pratiques si seules des appliances physiques sont utilisées. Les appliances NetScaler VPX et NetScaler MPX peuvent être utilisées de manière standard, adaptées aux besoins individuels de chaque application respective pour gérer des actions gourmandes en processeur telles que la compression et l'inspection du pare-feu des applications. À la périphérie du datacenter, les appliances NetScaler MPX gèrent des tâches à volume élevé à l'échelle du réseau, telles que la distribution initiale du trafic, le chiffrement ou le déchiffrement SSL, la prévention des attaques par déni de service (DoS) et l'équilibrage de charge global. L'association d'appliances NetScaler MPX hautes performances à une appliance virtuelle NetScaler VPX facile à déployer apporte une flexibilité et des capacités de personnalisation inégalées aux environnements de centres de données modernes à grande échelle, tout en réduisant les coûts globaux des centres de données.

Comment NetScaler VPX s'intègre-t-il à notre stratégie de centre de livraison Citrix ?

Avec la disponibilité de NetScaler VPX, l'ensemble de l'offre du centre de distribution Citrix est disponible sous forme d'offre virtualisée. L'ensemble du centre de mise à disposition Citrix bénéficie des puissantes fonctionnalités de gestion, de provisionnement, de surveillance et de création de rapports disponibles dans Citrix XenCenter. Cela peut être déployé rapidement dans presque n'importe quel environnement et géré de manière centralisée depuis n'importe où. Grâce à une infrastructure intégrée et virtualisée de distribution d'applications, les entreprises peuvent fournir des postes de travail, des applications client-serveur et des applications Web.

Encryption

NetScaler VPX prend-il en charge le déchargement SSL ?

Oui. Toutefois, NetScaler VPX effectue tous les traitements SSL dans le logiciel. NetScaler VPX n'offre donc pas les mêmes performances SSL que les appliances NetScaler. NetScaler VPX peut prendre en charge jusqu'à 750 nouvelles transactions SSL par seconde.

Les cartes SSL tierces installées sur le serveur hébergeant NetScaler VPX accélèrent-elles le chiffrement ou le déchiffrement SSL ?

Non. La prise en charge des cartes SSL tierces ne permet pas d'associer le NetScaler VPX à des implémentations matérielles spécifiques. Cela réduit considérablement la capacité d'une entreprise à héberger NetScaler VPX de manière flexible n'importe où dans le centre de données. Les appliances NetScaler MPX doivent être utilisées lorsqu'un débit SSL supérieur à celui fourni par NetScaler VPX est requis.

NetScaler VPX prend-il en charge les mêmes chiffrements de chiffrement que les appliances NetScaler physiques ?

VPX prend en charge tous les chiffrements de chiffrement en tant qu'appliances NetScaler physiques, à l'exception de l'ECDSA.

Quel est le débit des transactions SSL de NetScaler VPX ?

Consultez la fiche technique de NetScaler VPX pour plus d'informations sur le débit des transactions SSL.

Prix et emballage

Comment est packagé NetScaler VPX ?

La sélection de NetScaler VPX est similaire à la sélection d'appliances NetScaler. Tout d'abord, le client sélectionne l'édition NetScaler en fonction de ses exigences fonctionnelles. Le client sélectionne ensuite le niveau de bande passante NetScaler VPX spécifique en fonction de ses besoins en matière de débit. NetScaler VPX est disponible dans les éditions Standard, Advanced et Premium. NetScaler VPX propose des débits allant de 10 Mbit/s (VPX 10) à 100 Gbit/s (VPX 100G). Vous trouverez plus de détails dans la fiche technique de NetScaler VPX.

Le prix de NetScaler VPX est-il le même pour tous les hyperviseurs ?

Oui.

Les mêmes SKU NetScaler sont-ils utilisés pour VPX sur tous les hyperviseurs ?

Oui.

Une licence NetScaler VPX peut-elle être déplacée d'un hyperviseur à un autre (par exemple de VMware vers Hyper-V) ?

Oui. Les licences NetScaler VPX sont indépendantes de l'hyperviseur sous-jacent. Si vous décidez de déplacer la machine virtuelle NetScaler VPX d'un hyperviseur à un autre, il n'est pas nécessaire d'obtenir une nouvelle licence. Toutefois, il se peut que vous deviez réhéberger la licence NetScaler VPX existante.

Les instances NetScaler VPX peuvent-elles être mises à niveau ?

Oui. Les limites de débit et l'édition de la famille NetScaler peuvent être mises à niveau. Les SKU de mise à niveau pour les deux types de mise à niveau sont disponibles.

Si je souhaite déployer NetScaler VPX dans une paire haute disponibilité, de combien de licences ai-je besoin ?

Comme pour les appliances physiques NetScaler, une configuration haute disponibilité de NetScaler nécessite deux instances actives. Par conséquent, le client doit acheter deux licences.

NetScaler VPX Express et essai gratuit de 90 jours

NetScaler VPX Express inclut-il toutes les fonctionnalités standard de NetScaler ? Inclut-il NetScaler Gateway et l'équilibrage de charge pour l'interface Web Citrix Virtual Apps (anciennement XenApp) et le courtier XML ?

Oui. NetScaler VPX Express inclut toutes les fonctionnalités de NetScaler Standard. À partir des versions 12.0-56.20 de NetScaler, Citrix a modifié le comportement de VPX Express.

NetScaler VPX Express inclut-il toutes les fonctionnalités standard de NetScaler ? Inclut-il NetScaler Gateway et l'équilibrage de charge pour l'interface Web Citrix Virtual Apps et le courtier XML ?

À partir des versions 12.0-56.20 de NetScaler, VPX Express propose l'ensemble des fonctionnalités de NetScaler Standard Edition, à l'exception de la fonctionnalité Gateway. Avant la version 12.0—56.20, VPX Express inclut toutes les fonctionnalités de l'édition standard.

NetScaler VPX Express nécessite-t-il une licence ?

Avec la nouvelle version de NetScaler VPX Express (12.0—56.20 et versions ultérieures), VPX Express est gratuit, ne nécessite aucun fichier de licence pour être installé et est fourni sans engagement. Si vous possédez déjà une licence VPX Express, le comportement VPX Express précédent est conservé. Si

le *fichier de licence* VPX Express est supprimé et que les versions 12.0—56.20 et suivantes sont utilisées, le nouveau comportement VPX Express prend effet.

La licence NetScaler VPX Express expire-t-elle ?

Avec le nouveau VPX Express, non. Il n'y a pas de licence ni de date d'expiration. Si vous possédez déjà une licence VPX Express, celle-ci expire un an après le téléchargement.

NetScaler VPX Express inclut-il les cinq licences simultanées gratuites de NetScaler Gateway ?

Oui, si vous possédez une licence VPX Express.

Le nombre de NetScaler VPX Express qu'un client peut télécharger est-il limité ?

Cinq.

NetScaler VPX Express prend-il en charge les mêmes chiffrements de chiffrement que les appliances NetScaler MPX ?

Pour une disponibilité générale, les mêmes chiffrements de chiffrement puissants pris en charge par les appliances NetScaler sont disponibles sur NetScaler VPX et NetScaler VPX Express. Il est soumis aux mêmes réglementations en matière d'importation ou d'exportation.

Puis-je déposer des dossiers de support technique pour NetScaler VPX Express ?

Non. Une licence NetScaler VPX commerciale telle que VPX-10, VPX-200, VPX-1000, VPX-3000 est requise pour déposer des dossiers de support technique. Toutefois, les utilisateurs de NetScaler VPX Express sont libres d'utiliser à la fois le centre de connaissances NetScaler VPX et de demander de l'aide à la communauté via les forums de discussion Z.

NetScaler VPX Express peut-il être mis à niveau vers une version commerciale ?

Oui. Il vous suffit d'acheter la licence NetScaler VPX commerciale dont vous avez besoin, puis d'appliquer la licence correspondante à l'instance NetScaler VPX Express.

Hyperviseur

Quelles sont les versions de VMware prises en charge par NetScaler VPX ?

NetScaler VPX prend en charge VMware ESX et ESXi pour les versions 3.5 ou ultérieures. Pour plus d'informations, consultez la matrice de support et les directives d'utilisation.

Pour VMware, combien d'interfaces réseau virtuelles pouvez-vous allouer à un VPX ?

Vous pouvez allouer jusqu'à 10 interfaces réseau virtuelles à un NetScaler VPX.

Depuis vSphere, comment accéder à la ligne de commande NetScaler VPX ?

Le client VMware vSphere fournit un accès intégré à la ligne de commande NetScaler VPX via un onglet de console. En outre, vous pouvez utiliser n'importe quel client SSH ou Telnet pour accéder à la ligne de commande. Vous pouvez utiliser l'adresse NSIP du NetScaler VPX dans le client SSH ou Telnet.

Comment accéder à l'interface graphique de NetScaler VPX ?

Pour accéder à l'interface graphique de NetScaler VPX, saisissez le NSIP du NetScaler VPX, par exemple `http://NSIP address` dans le champ d'adresse de n'importe quel navigateur.

Deux instances NetScaler VPX installées sur le même VMware ESX peuvent-elles être configurées dans une configuration haute disponibilité ?

Oui, mais ce n'est pas recommandé. Une panne matérielle affecterait les deux instances de NetScaler VPX.

Deux instances NetScaler VPX exécutées sur deux systèmes VMware ESX différents peuvent-elles être configurées dans une configuration haute disponibilité ?

Oui. Il est recommandé dans une configuration haute disponibilité.

Pour VMware, les événements liés à l'interface sont-ils pris en charge sur NetScaler VPX ?

Non. Les événements liés à l'interface ne sont pas pris en charge.

Pour VMware, les VLAN balisés sont-ils pris en charge sur NetScaler VPX ?

Oui. Les VLAN balisés NetScaler sont pris en charge sur NetScaler VPX à partir de la version 11.0 et des versions ultérieures. Pour plus d'informations, consultez la documentation de NetScaler.

Pour VMware, l'agrégation de liens et le LACP sont-ils pris en charge sur NetScaler VPX ?

Non. L'agrégation de liens et le LACP ne sont pas pris en charge pour NetScaler VPX. L'agrégation de liens doit être configurée au niveau VMware.

Comment accéder à la documentation de NetScaler VPX ?

La documentation est disponible à partir de l'interface graphique de NetScaler VPX. Une fois connecté, sélectionnez l'onglet **Documentation** .

Planification ou dimensionnement des capacités

À quelles performances puis-je m'attendre avec NetScaler VPX ?

NetScaler VPX offre de bonnes performances. Consultez la fiche technique de NetScaler VPX pour connaître le niveau de performance spécifique pouvant être atteint à l'aide de NetScaler VPX.

Étant donné que la puissance du processeur du serveur varie, comment pouvons-nous estimer les performances maximales d'une instance NetScaler ?

L'utilisation d'un processeur plus rapide peut entraîner des performances supérieures (jusqu'au maximum autorisé par la licence), tandis que l'utilisation d'un processeur plus lent peut certainement limiter les performances.

La bande passante ou le débit de NetScaler VPX sont-ils limités au trafic entrant uniquement, ou à la fois au trafic entrant et sortant ?

Les limites de bande passante de NetScaler VPX sont appliquées uniquement au trafic entrant vers NetScaler, qu'il s'agisse du trafic de requête ou du trafic de réponse. Cela indique qu'un NetScaler VPX-1000 (par exemple) peut traiter simultanément 1 Gbit/s de trafic entrant et 1 Gbit/s de trafic sortant. Le trafic entrant et sortant n'est pas le même que le trafic de demande et de réponse. Pour NetScaler, le trafic provenant des points de terminaison (trafic de requêtes) et le trafic provenant des serveurs d'origine (trafic de réponse) sont « entrants » (c'est-à-dire entrant dans NetScaler).

Est-il possible d'exécuter plusieurs instances de NetScaler VPX sur le même serveur ?

Oui. Assurez-vous toutefois que le serveur physique dispose d'une capacité de processeur et d'E/S suffisante pour prendre en charge la charge de travail totale exécutée sur l'hôte, sinon les performances de NetScaler VPX pourraient être affectées.

Si plusieurs instances de NetScaler VPX s'exécutent sur un serveur physique, quelle est la configuration matérielle minimale requise par instance de NetScaler VPX ?

Chaque instance NetScaler VPX doit se voir allouer 2 Go de RAM physique, 20 Go d'espace disque et 2 processeurs virtuels.

> **Remarque :**
>
> Le NetScaler VPX est une appliance virtuelle haute performance sensible à la latence. Pour fournir les performances attendues, le dispositif nécessite la réservation du processeur virtuel, la réservation de la mémoire et l'épinglage du processeur virtuel sur l'hôte. En outre, l'hyper thread doit être désactivé sur l'hôte. Si l'hôte ne répond pas à ces exigences, des problèmes tels que basculement haute disponibilité, pic de processeur dans l'instance VPX, lenteur dans l'accès à l'interface de ligne de commande VPX, plantage du démon pit boss, pertes de paquets et faible débit se produisent.
>
> Assurez-vous que chaque instance VPX répond aux conditions prédéfinies.

Puis-je héberger NetScaler VPX et d'autres applications sur le même serveur ?

Oui. Par exemple, NetScaler VPX, Citrix Virtual Apps Web Interface et Citrix Virtual Apps XML Broker peuvent tous être virtualisés et exécutés sur le même serveur. Pour des performances optimales, assurez-vous que l'hôte physique dispose d'une capacité de processeur et d'E/S suffisante pour prendre en charge toutes les charges de travail en cours d'exécution.

L'ajout de cœurs de processeur à une seule instance NetScaler VPX augmentera-t-il les performances de cette instance ?

Selon la licence, une instance NetScaler VPX peut utiliser jusqu'à 4 processeurs virtuels aujourd'hui. L'ajout d'un processeur supplémentaire à une instance NetScaler VPX qui peut utiliser davantage de processeurs augmente les performances.

Pourquoi NetScaler VPX semble consommer plus de 90 % du processeur alors qu'il est inactif ?

Il s'agit d'un comportement normal et les appliances NetScaler présentent le même comportement. Pour connaître l'étendue réelle de l'utilisation du processeur NetScaler VPX, utilisez la commande stat CPU dans l'interface de ligne de commande NetScaler ou consultez l'utilisation du processeur NetScaler VPX à partir de l'interface graphique de NetScaler. Le moteur de traitement de paquets NetScaler est toujours « à la recherche de travail », même lorsqu'il n'y a rien à faire. Par conséquent, il fait tout pour prendre le contrôle de la CPU et ne pas le libérer. Sur un serveur installé avec NetScaler VPX et rien d'autre, cela donne l'impression (du point de vue de l'hyperviseur) que NetScaler VPX consomme la totalité du processeur. L'examen de l'utilisation du processeur « au sein de NetScaler » (à l'aide de l'interface de ligne de commande ou de l'interface graphique) fournit une image de la capacité du processeur NetScaler VPX utilisée.

Configuration système requise

Quelle est la configuration matérielle minimale requise pour NetScaler VPX ?

Le tableau suivant explique la configuration matérielle minimale requise pour NetScaler VPX.

Type	Exigences
Processeur	Serveur double cœur avec Intel Xeon ou AMD EPYC.
Mémoire	Minimum 2 Go. Cependant, 4 Go sont recommandés.
Disque	Disque dur de 20 Go minimum.
Hyperviseur	Citrix Hypervisor 5.6 ou version ultérieure, VMware ESX/ESXi 3.5 ou version ultérieure, ou Windows Server 2008 R2 avec Hyper-V
Connectivité réseau	100 Mbits/s minimum, mais 1 Gbit/s est recommandé.
Carte d'interface réseau	Une carte réseau compatible avec l'hyperviseur que vous utilisez.

> **Remarque :**
>
> Pour les déploiements critiques, une mémoire de 4 Go est préférable pour NetScaler VPX. Avec une mémoire de 2 Go, NetScaler VPX fonctionne dans un environnement où la mémoire est très limitée. Cela peut entraîner des problèmes liés à l'échelle, aux performances ou à la stabilité.

Pour plus d'informations sur la configuration système requise, consultez la fiche technique de NetScaler VPX.

> **Remarque :**
>
> À partir de la version 13.1 de NetScaler, l'instance NetScaler VPX sur l'hyperviseur VMware ESXi prend en charge les processeurs AMD EPYC.

Qu'est-ce qu'Intel VT-x ?

Ces fonctionnalités, parfois appelées « assistance matérielle » ou « assistance à la virtualisation », interceptent les instructions du processeur sensibles ou privilégiées exécutées par le système d'exploitation invité vers l'hyperviseur. Cela simplifie l'hébergement des systèmes d'exploitation invités (BSD pour un NetScaler VPX) sur l'hyperviseur.

Quelle est la commune de VT-x ?

Pratiquement, tous les serveurs livrés au cours des deux dernières années peuvent prendre en charge VT-x. De nombreux serveurs sont livrés avec l'aide à la virtualisation désactivée dans le BIOS. Avant de supposer que vous ne pouvez pas exécuter NetScaler VPX, vérifiez si vous devez modifier ce paramètre sur le serveur.

Existe-t-il une liste de compatibilité matérielle (HCL) pour NetScaler VPX ?

Tant que le serveur prend en charge la technologie Intel VT-x, NetScaler VPX doit s'exécuter sur n'importe quel serveur compatible avec l'hyperviseur sous-jacent. Consultez la HCL de l'hyperviseur pour obtenir une liste complète des plates-formes prises en charge.

Sur quelle version de NetScaler OS est basé NetScaler VPX ?

NetScaler VPX est basé sur NetScaler 9.1 ou versions ultérieures.

Étant donné que NetScaler VPX fonctionne sous BSD, peut-il être exécuté nativement sur un serveur sur lequel BSD Unix est installé ?

Non. NetScaler VPX nécessite l'hyperviseur pour fonctionner. Les supports détaillés des hyperviseurs sont disponibles dans la fiche technique de NetScaler VPX.

Autres FAQ techniques

L'agrégation de liens sur un serveur physique avec plusieurs cartes réseau fonctionne-t-elle ?

LACP n'est pas pris en charge. Pour Citrix Hypervisor, l'agrégation de liens statiques est prise en charge et est limitée à quatre canaux et sept interfaces virtuelles. Pour VMware, l'agrégation de liens statiques n'est pas prise en charge dans NetScaler VPX, mais elle peut être configurée au niveau de VMware.

Le transfert basé sur MAC (MBF) est-il pris en charge sur VPX ? Y a-t-il eu un changement par rapport à l'implémentation de l'appliance NetScaler ?

Le MBF est pris en charge et se comporte de la même manière qu'avec l'appliance NetScaler. L'hyperviseur fait essentiellement basculer tous les paquets reçus de NetScaler VPX vers l'extérieur et inversement.

Comment s'effectue le processus de mise à niveau de NetScaler VPX ?

Les mises à niveau s'effectuent de la même manière que pour les appliances NetScaler : téléchargez un fichier de noyau et utilisez install ns ou l'utilitaire de mise à niveau dans l'interface graphique.

Comment sont alloués la mémoire flash et l'espace disque ? Pouvons-nous le changer ?

/flash = 965M
/var = 14G
Un minimum de 2 Go de mémoire doit être alloué à chaque instance NetScaler VPX. L'image disque de NetScaler VPX a été dimensionnée à 20 Go pour des raisons de facilité de maintenance, par exemple pour accueillir et stocker jusqu'à 4 Go de dumps principaux et de fichiers journaux et de traçage. Bien qu'il soit possible de générer une image disque plus petite, il n'est pas prévu de le faire actuellement. `/flash` et `/var` se trouvent tous les deux dans la même image disque. Ils sont conservés en tant que systèmes de fichiers distincts à des fins de compatibilité.
Pour des recommandations détaillées en matière d'allocation de mémoire, consultez la fiche technique de NetScaler VPX.

Pouvons-nous ajouter un nouveau disque dur pour augmenter l'espace sur l'instance NetScaler VPX ?

Oui. À partir de la version 13.1 build 21.x de NetScaler, vous avez la possibilité d'augmenter l'espace disque sur l'instance NetScaler VPX en ajoutant un deuxième disque. Lorsque vous connectez le second disque, le répertoire « /var/crash » est automatiquement monté sur ce disque. Le second disque est utilisé pour le stockage des fichiers principaux et la journalisation. Les répertoires existants qui sont utilisés pour stocker les fichiers principaux et les fichiers journaux continuent de fonctionner comme précédemment.

> **Remarque :**
>
> Effectuez une sauvegarde externe lors de la rétrogradation de l'appliance NetScaler pour éviter toute perte de données.

Pour plus d'informations sur la façon de connecter un nouveau disque dur (HDD) à une instance NetScaler VPX sur un cloud, consultez les rubriques suivantes :

- Documentation Azure

  > **Remarque :**
  >
  > Pour associer un disque secondaire à des instances VPX déployées sur Azure, assurez-vous que les machines virtuelles Azure disposent d'un disque temporaire local. Pour plus d'informations, consultez la section Tailles des machines virtuelles Azure sans disque temporaire local.

- Documentation AWS
- Documentation GCP

> **Avertissement :**
>
> Après avoir ajouté un nouveau disque dur à VPX, certains scripts qui fonctionnent sur les fichiers, qui sont déplacés vers le nouveau disque dur, peuvent échouer dans les conditions suivantes :
>
> Si vous utilisez la commande shell « link » pour créer des liens matériels vers les fichiers qui ont été déplacés vers un nouveau disque dur.
>
> Toutes ces commandes doivent être remplacées par « ln -s » pour utiliser un lien symbolique. Modifiez également les scripts défaillants en conséquence.

Que pouvons-nous espérer considérer la numérotation de build NetScaler VPX et l'interopérabilité avec d'autres versions ?

La numérotation des versions de NetScaler VPX est similaire à celle de la version 9.1. Cl (classique) et 9.1. Version de Nc (nCore), par exemple 9.1_97.3.vpx, 9.1_97.3.nc et 9.1_97.3.cl.

Le NetScaler VPX peut-il faire partie d'une configuration de haute disponibilité avec une appliance NetScaler ?

Configuration non prise en charge.

Toutes les interfaces visibles dans NetScaler VPX sont-elles directement liées au nombre d'interfaces sur l'hyperviseur ?

Non. Vous pouvez ajouter jusqu'à sept interfaces (10 pour VMware) via l'utilitaire de configuration NetScaler VPX avec une seule carte réseau physique sur l'hyperviseur.

La migration en direct de Citrix Hypervisor XenMotion, VMware vMotion ou Hyper-V peut-elle être utilisée pour déplacer des instances actives de NetScaler VPX ?

NetScaler VPX ne prend pas en charge la migration en direct de XenMotion ou d'Hyper-V. VMotion est pris en charge à partir de la version NetScaler 12.1. Pour plus d'informations, consultez Notes de publication.

Présentation des licences

June 20, 2023

NetScaler propose une large gamme d'éditions de produits et de modèles de licence pour les appliances MPX et VPX, afin de répondre aux besoins de votre entreprise.

Pour fonctionner correctement, une appliance NetScaler doit disposer de l'une des licences NetScaler Family Edition. La gamme de produits ADC comprend trois éditions familiales :

- Édition Standard

  > **Remarque**
  >
  > L'édition Standard a atteint la fin de commercialisation (EOS) et n'est disponible que pour le renouvellement.

- Édition Advanced
- Édition Premium

Pour plus d'informations, consultez la fiche technique. La fiche technique est disponible sur www.netscaler.com.

Sélectionnez une édition NetScaler. Sélectionnez ensuite une offre de licence MPX ou VPX en fonction des critères suivants :

- Perpétuel et abonnement (abonnement annuel et horaire)
- Processeur virtuel et bande passante
- sur site et dans le cloud

Licence NetScaler VPX Express

VPX Express pour les déploiements sur site et dans le cloud ne nécessite pas de fichier de licence et offre les fonctionnalités suivantes :

- Bande passante 20 Mbps
- Toutes les fonctionnalités de licence standard ADC, à l'exception de NetScaler Gateway et des défenses L4 et L7
- 250 sessions SSL maximum
- Débit SSL de 20 Mbps

Vous pouvez mettre à niveau la licence VPX Express vers les deux options suivantes :

1. Une licence NetScaler VPX autonome.
2. Licence NetScaler Pooled Capacity pour les instances VPX. Pour plus d'informations, consultez NetScaler Pooled Capacity.

> **Important**
>
> Le clustering est disponible dans l'édition Standard pour le cloud public VPX et dans la licence VPX Express.

Licence NetScaler Pooled Capacity

Utilisez NetScaler Application Delivery Management (ADM) pour créer un cadre de licence comprenant une bande passante commune et un pool d'instances. Pour plus d'informations, consultez NetScaler Pooled Capacity.

> **Remarque :**
>
> NetScaler ADM peut héberger à la fois des licences de pool groupées et autogérées. Pour utiliser la licence requise, configurez le serveur de licences sur NetScaler et vérifiez la capacité du pool approprié. Les étapes de configuration de la CLI et de l'interface graphique ADC pour la licence Pooled et Self Managed Pool sont les mêmes.

Licence NetScaler Self Managed Pool

À partir de la version 13.1 build 30.x de NetScaler, les instances NetScaler prennent en charge la licence Self Managed Pool. Cette licence vous permet de simplifier et d'automatiser le téléchargement des fichiers de licence vers un serveur de licences. Utilisez NetScaler ADM pour créer un cadre de licence comprenant une bande passante ou un processeur virtuel et un pool d'instances communs.

Pour utiliser la licence Self Managed Pool, configurez le serveur de `SelfManagedPool` licences en mode licence sur NetScaler et vérifiez la capacité requise. Utilisez la `show ns license` commande après avoir redémarré l'appliance NetScaler pour connaître la licence configurée.

> **Important**
>
> Si votre système est configuré avec une licence Pooled Capacity mais que vous souhaitez migrer vers une licence Self Managed Pool sans affecter le flux de trafic, assurez-vous que le serveur cible dispose de la licence Self Managed Pool requise.
>
> Vous pouvez migrer uniquement entre les licences compatibles suivantes :
>
> - Pooled Capacity to Self Managed Pool, et inversement.
> - vCPU à vCPU auto-géré, et inversement.
>
> Pour migrer la licence, exécutez la commande suivante :
>
> ```
> add ns licenseserver (<licenseServerIP> | <serverName>)-forceUpdateIP -
> licensemode [CICO | Pooled | SelfManagedPool | VCPU | SelfManagedvCPU]
> ```
>
> **Exemple :**
>
> ```
> add licenseserver 192.0.2.246 -forceUpdateIP -licensemode selfManagedvcPU
> ```


Configurer la licence du pool auto-géré à l'aide de l'

Pour ajouter la configuration du serveur de licences à l'appliance NetScaler, exécutez la commande suivante :

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    positive_integer>] -licensemode [CICO | Pooled | SelfManagedPool |
    VCPU | SelfManagedvCPU]
<!--NeedCopy-->
```

Exemple :

```
add ns licenseserver 192.0.2.246 -port 27000 -licensemode
    SelfManagedPool
<!--NeedCopy-->
```

> **Remarque :**
>
> La `show ns licenseserverpool` commande affiche uniquement les licences basées sur le mode de licence spécifié. Par conséquent, les licences sont récupérées plus rapidement. Pour obtenir un inventaire de toutes les licences, exécutez la commande `show ns licenseserverpool -getallLicenses`. Si le mode de licence n'est pas spécifié, les licences de capacité groupée sont affichées par défaut.

Pour modifier la capacité du système, exécutez la commande suivante :

```
set ns capacity ((-bandwidth <positive_integer> -unit ( Gbps | Mbps ))
    | -platform <platform>) [-Edition <Edition>]
<!--NeedCopy-->
```

Exemple :

```
set ns capacity -bandwidth 3 -unit gbps -edition enterprise
<!--NeedCopy-->
```

> Remarque :
>
> La capacité est extraite du pool de licences du serveur de licences.

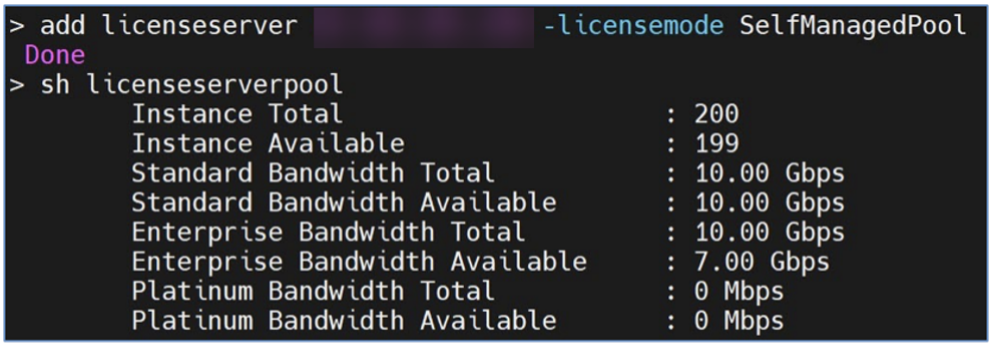
Pour redémarrer l'appliance NetScaler, exécutez la commande suivante :

```
reboot [-warm]
<!--NeedCopy-->
```

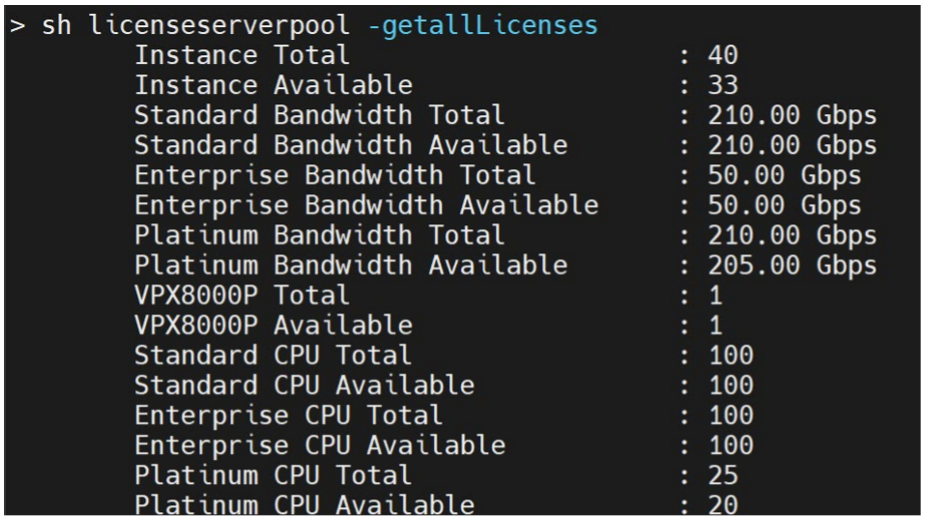
Pour afficher l'état de toutes les fonctionnalités sous licence et du mode de licence configuré, exécutez la commande suivante :


```
show ns license
<!--NeedCopy-->
```

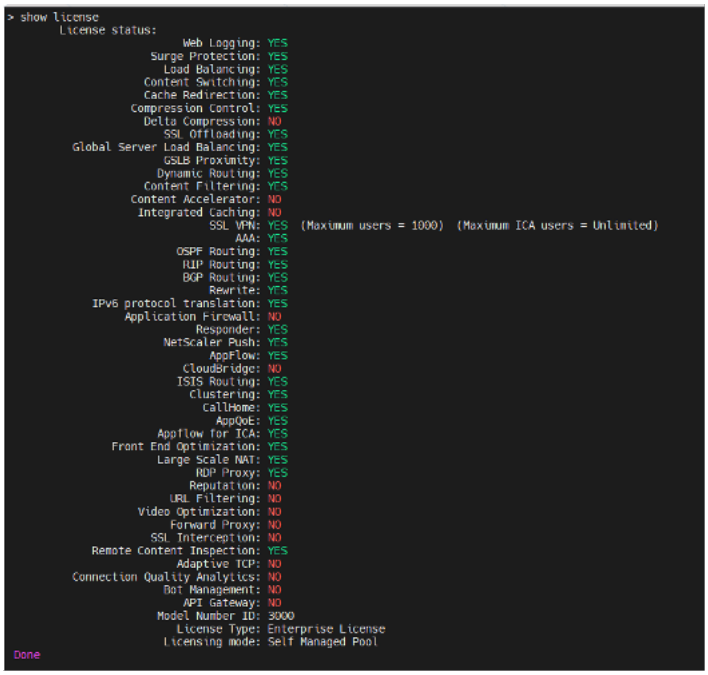
Exemple de sortie de commande `show ns licenseserverpool` :



Exemple de sortie de commande `show ns licenseserverpool -getallLicenses` :



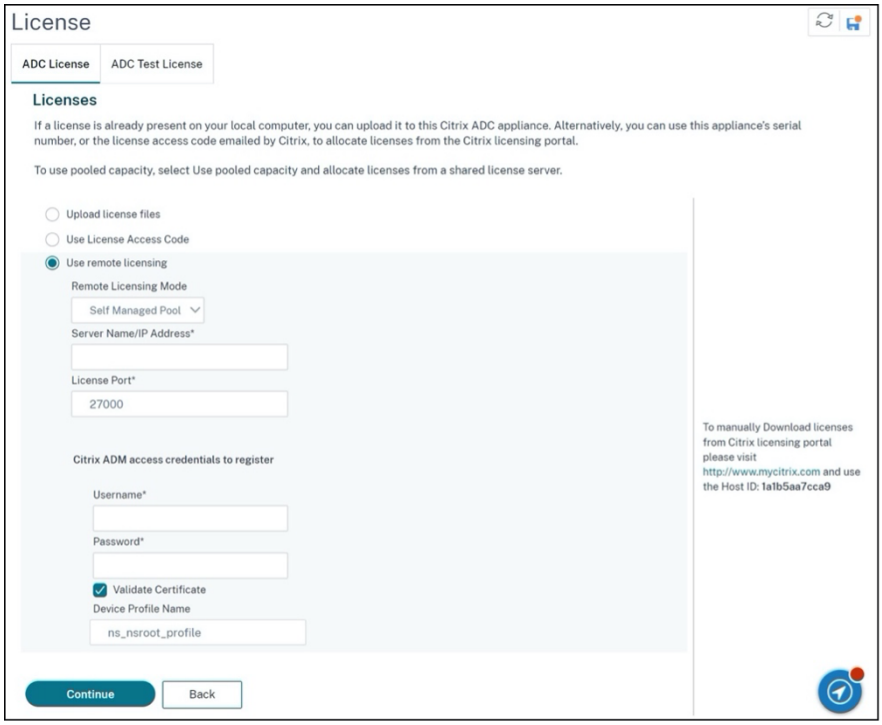
Exemple de sortie de commande `show license` :



Configurer la licence de pool auto-géré à l'aide de l'interface utilisateur

Effectuez les étapes suivantes pour configurer la licence du pool auto-géré :

1. Accédez à **Système > Licences > Licence ADC > Gérer les licences > Ajouter une nouvelle licence**.
2. Sur la page **Licences**, sélectionnez le bouton radio **Use remote licensing**, puis choisissez votre mode de licence dans **Remote Licensing Mode**.
3. Entrez l'adresse IP du serveur et les détails du port de licence.
4. Fournissez les informations d'accès NetScaler ADM.
5. Cliquez sur **Continuer**.



Ressources connexes

Système de licences Citrix

Licence VPX sur le cloud

Le déploiement VPX est pris en charge sur des fournisseurs de cloud public tels qu'Azure, AWS et Google. Pour plus d'informations, consultez les documents suivants :

- Licence VPX-Azure
- Licence VPX-AWS
- Licence VPX-GCP

Attribuer et appliquer une licence

July 31, 2023

Dans l'interface graphique de NetScaler MPX et VPX ADC, vous pouvez utiliser votre numéro de série matériel (HSN) ou votre code d'accès aux licences pour attribuer vos licences. Si une licence est déjà présente sur votre ordinateur local, vous pouvez également la télécharger sur l'appliance.

Pour toutes les autres fonctionnalités, telles que le retour ou la réallocation de votre licence, vous devez utiliser le portail de licences. Le cas échéant, vous pouvez toujours utiliser le portail de licences pour l'allocation de licences. Pour plus d'informations, voir Utiliser la gestion des licences dans My Account sur citrix.com.

Guide de gestion des licences Citrix

Le guide des licences Citrix fournit également des informations sur l'installation de licences dans une appliance NetScaler et sur l'installation de licences dans d'autres produits NetScaler. Pour plus d'informations, consultez Citrix Licensing Guide.

Composants requis

> **Remarque**
>
> Achetez des licences distinctes pour chaque appliance dans une paire haute disponibilité. Assurez-vous que les mêmes types de licences sont installés sur les deux appliances. Par exemple, si vous achetez une licence Premium pour une appliance, vous devez acheter une autre licence Premium pour l'autre appliance.

Pour utiliser le numéro de série du matériel ou le code d'accès de licence pour allouer vos licences :

- Vous devez être en mesure d'accéder aux domaines publics via l'appliance. Par exemple, l'appliance doit pouvoir accéder au site www.citrix.com. Le logiciel d'allocation de licence accède en interne au portail de licences Citrix pour votre licence. Pour accéder à un domaine public :
  - Utilisez un serveur proxy ou configurez un serveur DNS.
  - Configurez une adresse IP NetScaler (NSIP) ou une adresse IP de sous-réseau (SNIP) sur votre appliance NetScaler.
- Votre licence doit être liée à votre matériel ou vous devez disposer d'un code d'accès à la licence valide. Citrix envoie votre code d'accès à la licence par e-mail lorsque vous achetez une licence.

Attribuer une licence à l'aide de l'interface graphique

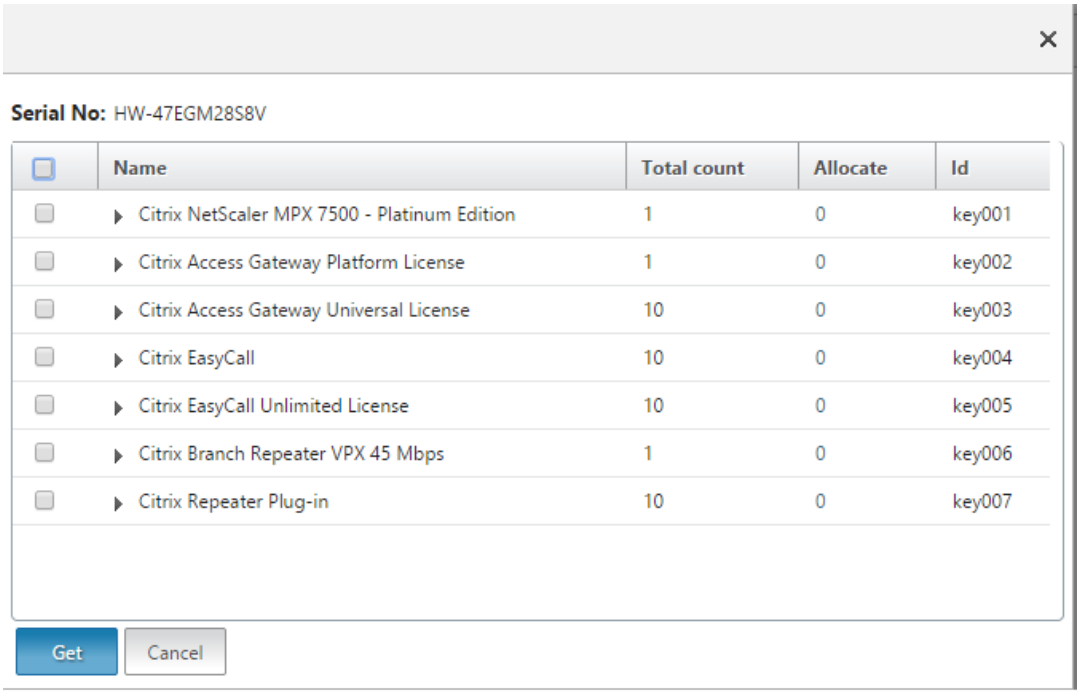
Si votre licence est déjà liée à votre matériel, le processus d'attribution des licences peut utiliser le numéro de série du matériel. Sinon, vous devez entrer le code d'accès à la licence.

Vous pouvez allouer partiellement des licences selon les besoins de votre déploiement. Par exemple, si votre fichier de licences contient 10 licences, mais que vos besoins actuels ne concernent que six licences, vous pouvez allouer six licences maintenant et en attribuer d'autres ultérieurement. Vous ne pouvez pas allouer plus de licences que le nombre total de licences présentes dans votre fichier de licences.

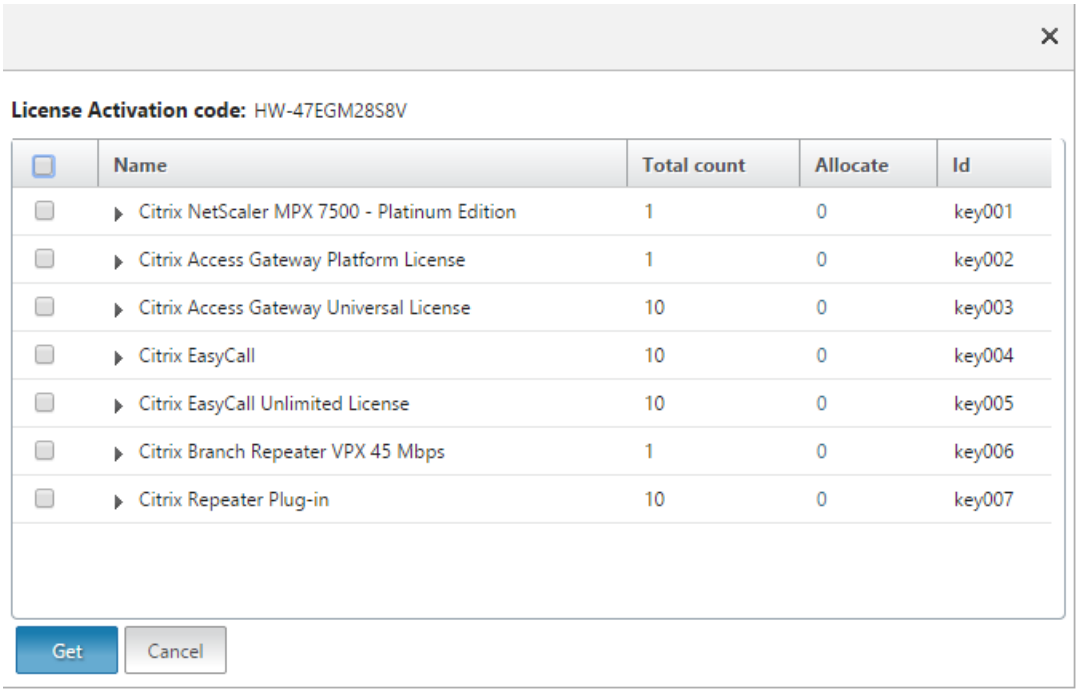
Pour attribuer votre licence

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance NetScaler (par exemple, `http://192.168.100.1`).
2. Dans Nom d'utilisateur et Mot de passe, tapez les informations d'identification de l'administrateur.
3. Sous l'onglet **Configuration**, accédez à **Système > Licences**.
4. Dans le volet d'informations, cliquez sur **Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez l'une des options suivantes :
   - **Utiliser le numéro de série** : Le logiciel récupère en interne le numéro de série de votre appliance et utilise ce numéro pour afficher vos licences.
   - **Utiliser le code d'accès à**la licence : Citrix envoie par e-mail le code d'accès à la licence que vous avez achetée. Entrez le code d'accès à la licence dans la zone de texte.

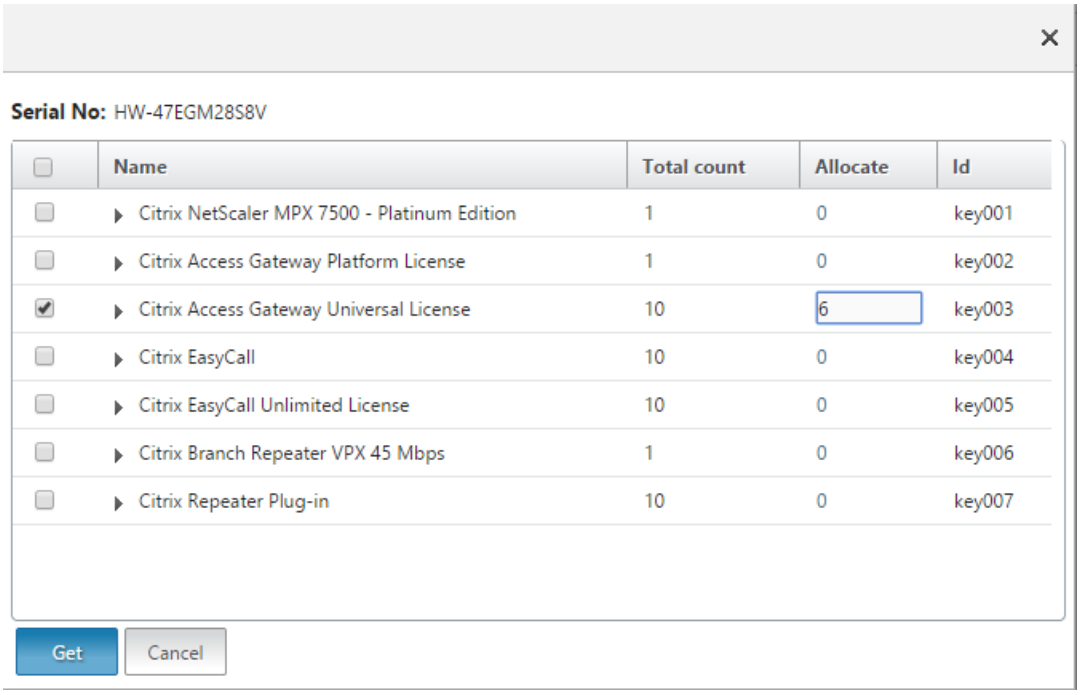
     Si vous ne souhaitez pas configurer la connectivité Internet sur l'appliance NetScaler, vous pouvez utiliser un serveur proxy. Activez la case à cocher **Connect through Proxy Server** et spécifiez l'adresse IP et le port de votre serveur proxy.
5. Cliquez sur **Obtenir licences**. Selon l'option sélectionnée, l'une des boîtes de dialogue suivantes s'affiche.
   - La boîte de dialogue suivante s'affiche si vous avez sélectionné Numéro de série du matériel.



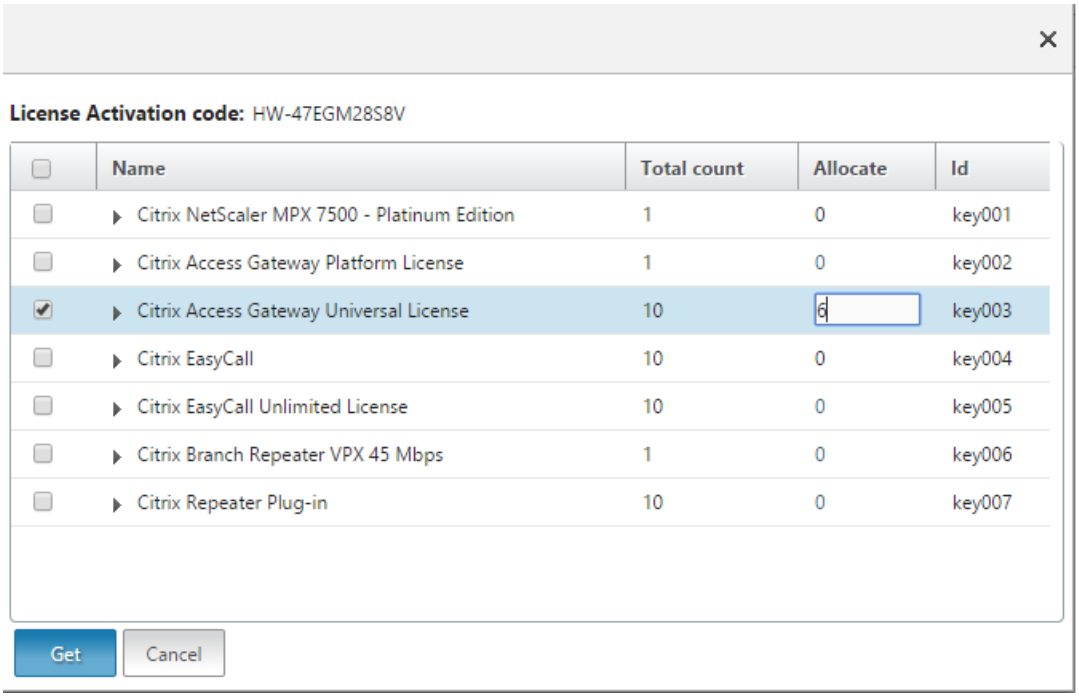
   - La boîte de dialogue suivante apparaît si vous avez sélectionné un code d'accès à la licence.



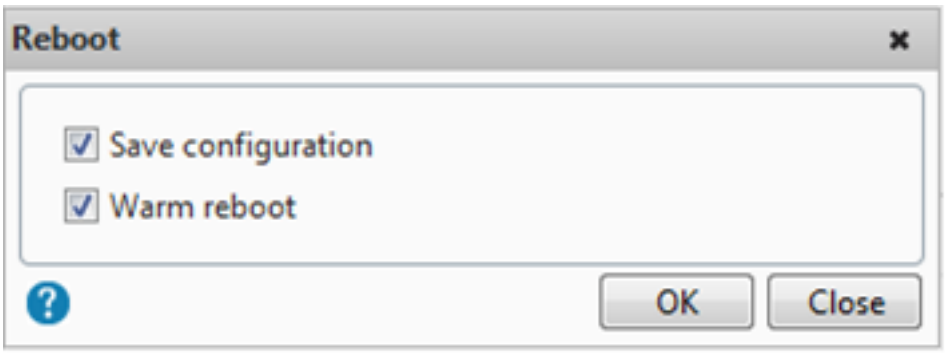
6. Sélectionnez le fichier de licences que vous souhaitez utiliser pour allouer vos licences.
7. Dans la colonne **Allocate**, saisissez le nombre de licences à allouer. Cliquez ensuite sur **Obtenir**.
   - Si vous avez sélectionné **Numéro de série matériel**, saisissez le nombre de licences, comme indiqué dans la capture d'écran suivante.



   - Si vous avez sélectionné le **code d'accès aux licences**, saisissez le nombre de licences, comme indiqué dans la capture d'écran suivante.



8. Cliquez sur Redémarrer pour que la licence soit appliquée.
9. Dans la boîte de dialogue de redémarrage, cliquez sur **OK** pour poursuivre les modifications, ou cliquez sur **Fermer** pour annuler les modifications.



Installer une licence

Si vous avez téléchargé votre fichier de licence sur votre ordinateur local en accédant au portail de licences, vous devez télécharger la licence sur l'appliance.

Pour installer un fichier de licence à l'aide de l'interface graphique

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance NetScaler (par exemple, `http://192.168.100.1`).
2. Dans Nom d'utilisateur et Mot de passe, tapez les informations d'identification de l'administrateur.

3. Dans l'onglet **Configuration**, accédez à Licences système.
4. Dans le volet d'informations, cliquez sur **Gérer les licences**.
5. Cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez **Charger fichier de licences depuis un ordinateur local**.
6. Cliquez sur **Parcourir**. Accédez à l'emplacement des fichiers de licence, sélectionnez le fichier de licences, puis cliquez sur **Ouvrir**.
7. Cliquez sur Redémarrer pour appliquer la licence.
8. Dans la boîte de dialogue de redémarrage, cliquez sur **OK** pour poursuivre les modifications, ou cliquez sur **Fermer** pour annuler les modifications.

Pour installer les licences à l'aide de l'interface de ligne de commande

1. Ouvrez une **connexion SSH** à l'appliance ADC à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur l'appliance ADC à l'aide des informations d'identification de l'administrateur.
3. Passez à l'invite du shell, créez un sous-répertoire de licences dans le `nsconfig` répertoire, s'il n'existe pas, et copiez un ou plusieurs nouveaux fichiers de licences dans ce répertoire.

   Exemple

   ```
   login: nsroot
   Password: nsroot
   Last login: Mon Aug  4 03:37:27 2008 from 10.102.29.9
   Done
   > shell
   Last login: Mon Aug  4 03:51:42 from 10.103.25.64
   root@ns# mkdir /nsconfig/license
   root@ns# cd /nsconfig/license
   <!--NeedCopy-->
   ```

   Copiez un ou plusieurs nouveaux fichiers de licence dans ce répertoire.

   > **Remarque**
   >
   > L'appliance NetScaler ne demande pas d'option de redémarrage lorsque vous utilisez l'interface de ligne de commande pour installer les licences. Exécutez la commande reboot -w pour redémarrer à chaud le système ou exécutez la commande de redémarrage pour redémarrer le système normalement.

Vérifier les fonctionnalités sous licence

Avant d'utiliser une fonctionnalité, assurez-vous que votre licence prend en charge cette fonctionnalité.

Pour vérifier les fonctionnalités sous licence à l'aide de l'interface de ligne de commande

1. Ouvrez une **connexion SSH** à l'appliance ADC à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur l'appliance ADC à l'aide des informations d'identification de l'administrateur.
3. À l'invite de commandes, entrez la commande sh ns license pour afficher les fonctionnalités prises en charge par la licence.

   Exemple

```
sh ns license
        License status:
                            Web Logging: YES
                        Surge Protection: YES
                          .......

                          Responder: YES
 Done
<!--NeedCopy-->
```

Pour vérifier les fonctionnalités sous licence à l'aide de l'interface graphique

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance ADC, par exemple `http://192.168.100.1`.
2. Dans Nom d'utilisateur et Mot de passe, tapez les informations d'identification de l'administrateur.
3. Indiquez le nom d'utilisateur et le mot de passe, puis cliquez sur **Connexion**.
4. Dans le volet de navigation, développez **Système**, puis cliquez sur **Licences**. Une coche verte s'affiche en regard des fonctionnalités sous licence.

Activer ou désactiver une fonctionnalité

Lorsque vous utilisez l'appliance NetScaler pour la première fois, vous devez activer une fonctionnalité avant de pouvoir utiliser ses fonctionnalités. Si vous configurez une fonctionnalité avant qu'elle ne soit activée, un message d'avertissement s'affiche. La configuration est enregistrée, mais elle ne s'applique qu'une fois la fonctionnalité activée.

Pour activer une fonctionnalité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer une fonctionnalité et vérifier la configuration :

- enable feature <FeatureName>

- show feature

Exemple

```
enable feature lb cs
done
 >show feature

        Feature                        Acronym
           Status
        -------                        -------
           ------
 1)     Web Logging                    WL                    OFF
 2)     Surge Protection               SP                    ON
 3)     Load Balancing                 LB                    ON
 4)     Content Switching              CS                    ON
 5)     Cache Redirection              CR                    ON
 .
 .
 .
 24)    NetScaler Push                 push                  OFF
 Done
<!--NeedCopy-->
```

L'exemple montre comment activer l'équilibrage de charge (lb) et la commutation de contenu (cs).

Si la clé de licence n'est pas disponible pour une fonctionnalité particulière, le message d'erreur suivant s'affiche pour cette fonctionnalité :

ERREUR : fonctionnalités non concédées sous licence

Remarque : Pour activer une fonctionnalité facultative, vous devez disposer d'une licence spécifique à cette fonctionnalité. Par exemple, vous avez acheté et installé la licence NetScaler Advanced Edition. Toutefois, pour activer la fonctionnalité de mise en cache intégrée, vous devez acheter et installer la licence AppCache.

Pour désactiver une fonctionnalité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour désactiver une fonctionnalité et vérifier la configuration :

- disable feature <FeatureName>
- show feature

Exemple

L'exemple suivant montre comment désactiver l'équilibrage de charge (LB).

```
> disable feature lb
 Done
> show feature

        Feature                     Acronym
           Status
        -------                     -------
           ------
 1)     Web Logging                 WL                  OFF
 2)     Surge Protection            SP                  ON
 3)     Load Balancing              LB                  OFF
 4)     Content Switching           CS                  ON
 .
 .
 .
 24)    NetScaler Push              push                OFF
 Done
>
<!--NeedCopy-->
```

Configurer les alertes d'expiration des licences NetScaler

Par défaut, une alerte GUI apparaît lorsque la date d'expiration de la licence ADC est inférieure ou égale à 30 jours.

Vous pouvez configurer l'appliance NetScaler pour qu'elle exécute les opérations d'alerte suivantes pendant un nombre de jours spécifié avant l'expiration d'une licence NetScaler :

- Affichez une bannière d'alerte d'expiration de licence sur l'interface graphique de NetScaler.
- Envoyez des traps SNMP contenant les informations d'expiration de licence à intervalles réguliers aux écouteurs de trap configurés si l'alarme SNMP « NS_LICENSE_EXPIRY » est activée.

À l'expiration de la licence, l'appliance NetScaler redémarre automatiquement pour révoquer la licence. Si une appliance NetScaler utilise des licences de fournisseur de services Citrix (CSP), l'appliance ne redémarre pas automatiquement pour révoquer la licence. Toutefois, si l'utilisateur redémarre l'appliance, elle redémarre sans licence.

Pour spécifier le nombre de jours pour les alertes d'expiration des licences NetScaler à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set licenseparameters** [-**licenseexpiryalerttime**]

- **sh licenseparameters**

Exemple :

```
> set licenseparameters -licenseexpiryalerttime 200
Done

> sh licenseparameters
...
    Licenseexpiryalerttime:  200
<!--NeedCopy-->
```

Pour spécifier le nombre de jours pour les alertes d'expiration des licences NetScaler à l'aide de l'interface graphique NetScaler :

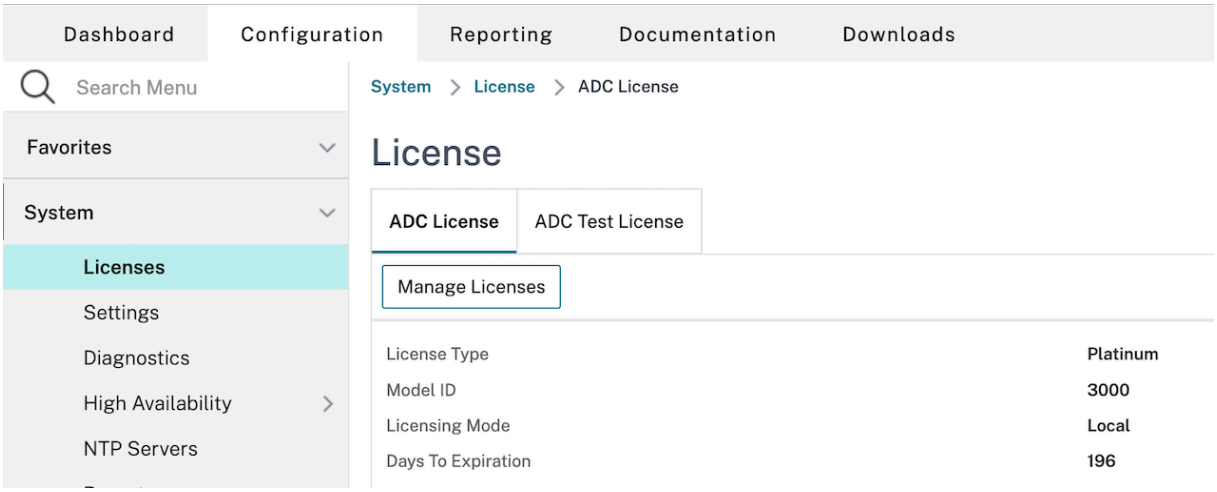
1. Accédez à **Configuration** > **Système** > **Licences** > **Gérer les licences**.
2. Dans **Paramètres de notification**, cliquez sur le bouton Modifier pour spécifier le nombre de jours pour les alertes d'expiration de licence NetScaler.

Vérifier les informations d'expiration de la licence

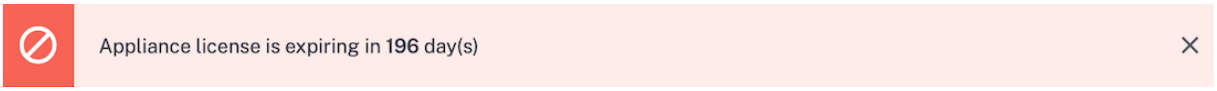
Vous pouvez vérifier les informations d'expiration des licences NetScaler via l'interface graphique ou l'interface de ligne de commande.

Pour vérifier les informations d'expiration des licences NetScaler via l'interface graphique :

Accédez à **Configuration > Système > Licences**.



Une alerte GUI apparaît lorsque la date d'expiration de la licence ADC est inférieure ou égale au nombre de jours spécifié pour l'alerte d'expiration de licence NetScaler.



Pour vérifier les informations d'expiration de la licence via l'interfacede ligne de commande :

Tapez la commande « show ns license ».

```
> sh license
    License status:

    Web Logging: YES
    Surge Protection: YES

    Web Logging: YES
    Surge Protection: YES

    …

Days to expiry: 196

Done
>
<!--NeedCopy-->
```

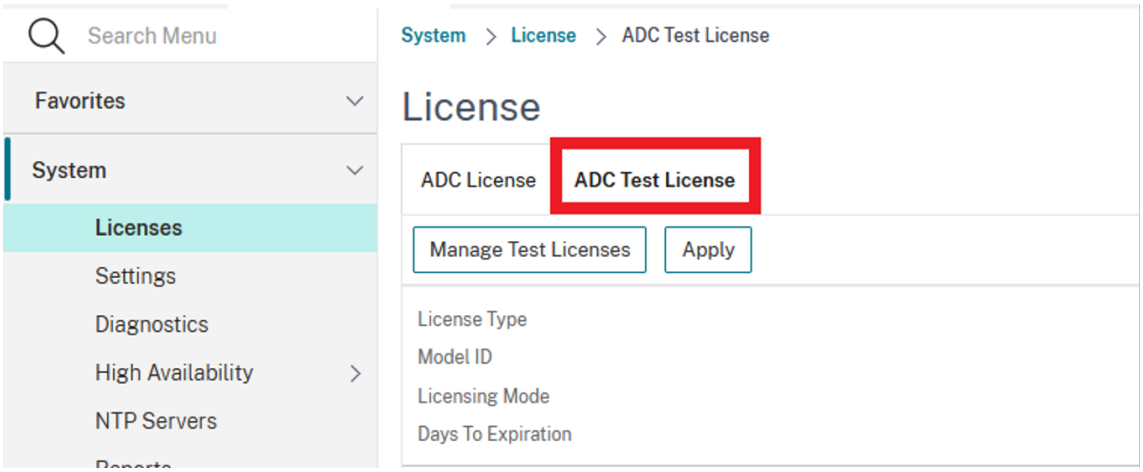
Validez les fichiers de licence sans redémarrer l'appliance NetScaler

Cette fonctionnalité vous permet de tester des licences et de voir toutes les fonctionnalités disponibles dans la licence donnée sans les appliquer à l'appliance NetScaler. Cette option vous permet de tester de nouvelles licences sans redémarrer l'appliance NetScaler.

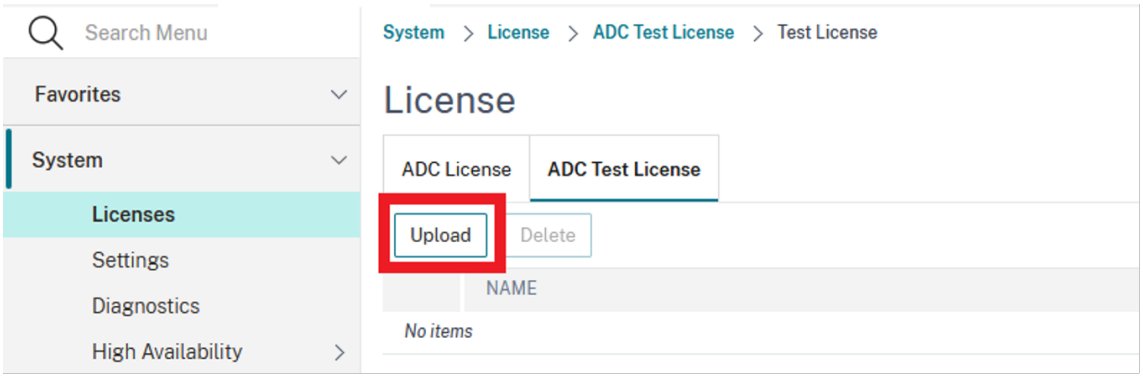
Vous pouvez utiliser cette fonctionnalité à la fois via l'interface graphique et l'interface de ligne de commande.

Valider les fichiers de licence à l'aide de l'interface graphique

1. Accédez à **Système -> Licences**.
2. Dans l'onglet **Licence de test ADC**, cliquez sur **Gérer les licences de test**.

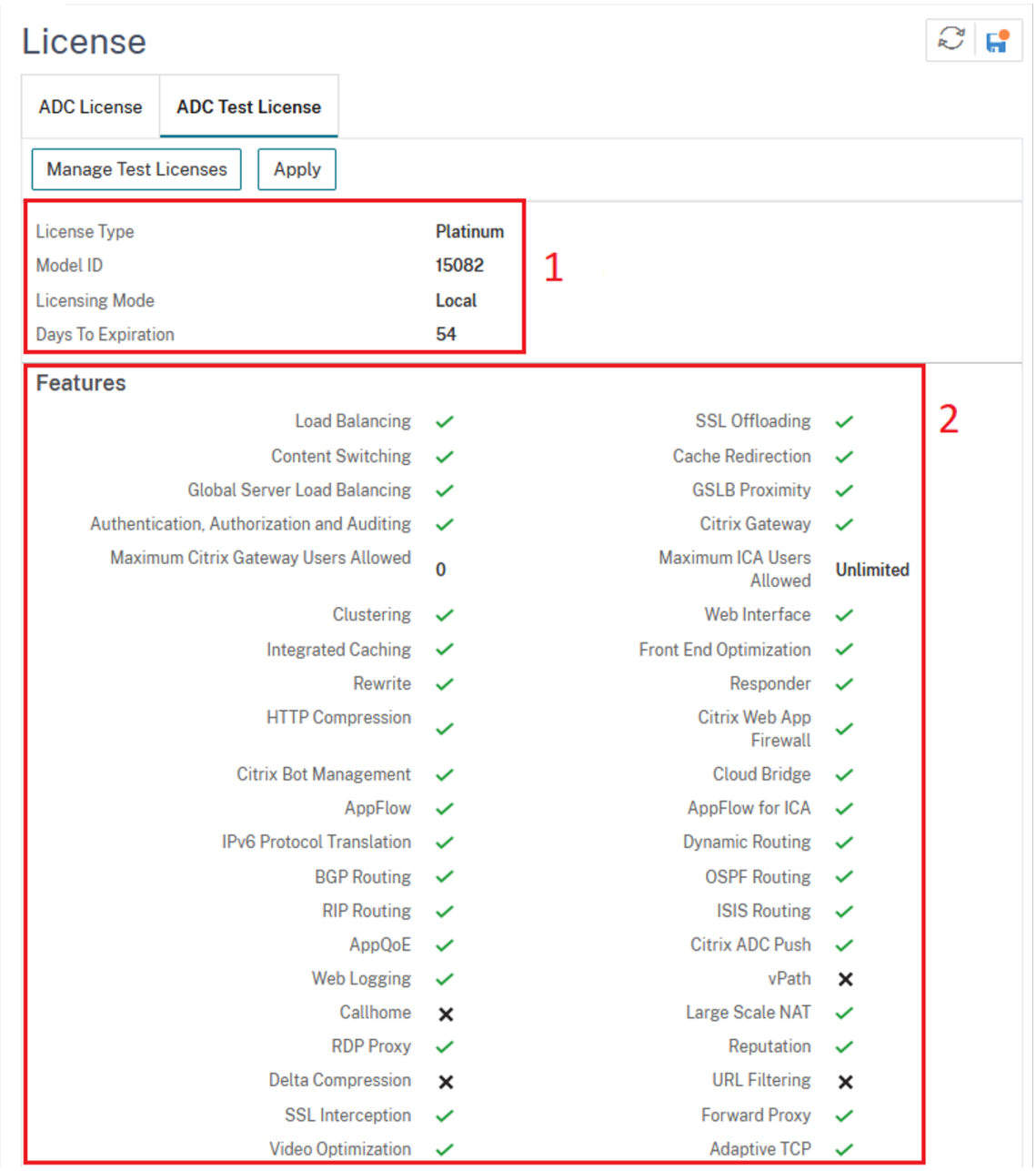


3. Cliquez sur **Charger**, puis chargez un ou plusieurs fichiers de licence. Si plusieurs fichiers de licence sont chargés, l'union de tous les fichiers de licence est calculée.



4. Une fois le téléchargement du fichier de licence terminé, cliquez à nouveau sur **ADC Test License** pour afficher les fonctionnalités sous licence de la licence téléchargée.

   La section 1 présente les informations de licence et la section 2 présente toutes les fonctionnalités incluses dans la licence.



5. Vérifiez les informations affichées et cliquez sur **Appliquer** pour utiliser la licence. Redémarrez (à chaud) l'appliance NetScaler pour que la licence prenne effet. Le redémarrage immédiat n'est pas obligatoire et la licence actuelle est applicable jusqu'au prochain redémarrage.

Validez les fichiers de licence à l'aide de la CLI

1. Copiez le fichier de licence de test sur l'appliance ADC à l'adresse path : `/nsconfig/testlicense`.

   Exemple :


```
scp CNS_15082_SERVER_PLT_Retail.lic nsroot@<ns_ip>:/nsconfig/
   testlicense/
<!--NeedCopy-->
```

2. Vérifiez si le fichier de licence est copié au bon emplacement.

   Exemple :

```
ls /nsconfig/testlicense/  CNS_15082_SERVER_PLT_Retail.lic
<!--NeedCopy-->
```

3. Exécutez la `show ns testlicense` commande pour voir les informations de licence.

```
> sh ns testlicense
    License status:
                        Web Logging: YES
                  Surge Protection: YES
                    Load Balancing: YES
                 Content Switching: YES
                 Cache Redirection: YES
               Compression Control: YES
                 Delta Compression: NO
                    SSL Offloading: YES
      Global Server Load Balancing: YES
                                .....
                        API Gateway: YES
                   Model Number ID: 15082
                      License Type: Platinum License
                    Licensing mode: Local
                Days to expiration: 54
<!--NeedCopy-->
```

4. Vérifiez les informations affichées et exécutez la `apply ns testlicense` commande pour appliquer la licence. Redémarrez (à chaud) l'appliance NetScaler pour que la licence prenne effet.

```
> apply ns testlicense

Warning: The configuration changes will not take effect until the
   system is rebooted
Done
> reboot -w
Are you sure you want to restart NetScaler (Y/N)? [N]:Y
Done
<!--NeedCopy-->
```


Mise à niveau d'une licence

Vous pouvez mettre à niveau une appliance NetScaler d'une édition familiale à une autre et d'une plage de capacités à une autre en achetant une licence de capacité supérieure.

Les mises à niveau sont de deux types :

- Mises à niveau de l'édition : Standard vers Advanced, Standard to Premium et Advanced to Premium. Les mises à niveau de l'édition doivent être à l'intérieur de la même bande passante.
- Mises à niveau de capacité : vous pouvez passer d'une capacité inférieure à une capacité supérieure, à la fois pour le vCPU et la bande passante. Les mises à niveau de capacité ne peuvent être effectuées que sur la même édition (Standard, Advanced ou Premium).

Si vous souhaitez mettre à niveau la capacité et l'édition, commencez par mettre à niveau la capacité, redémarrez l'appliance, puis mettez à niveau l'édition.

Exemple : Pour mettre à niveau une licence VPX 10 Mbps Standard Edition vers VPX 200 Mbps Premium Edition, la mise à niveau doit être effectuée en deux étapes.

- Mise à niveau VPX de 10 Mbps Standard Edition à 200 Mbps Standard Edition.
- Mise à niveau VPX de 200 Mbps Standard Edition à 200 Mbps Premium Edition.

> Remarque
>
> Vous pouvez utiliser NetScaler Application Delivery Management (ADM) pour créer un cadre de licence comprenant une bande passante et un pool d'instances communs. Pour des informations complètes, consultez la section Capacité groupée de NetScaler.

Ressources connexes

- Système de licences Citrix
- Comment allouer des licences NetScaler VPX

Gouvernance des données

May 5, 2023

Qu'est-ce que NetScaler ADM Service Connect ?

La connexion au service NetScaler Application Delivery Management (ADM) est une fonctionnalité qui permet l'intégration fluide des instances NetScaler MPX, SDX et VPX et des appliances NetScaler Gateway au service NetScaler ADM. Cette fonctionnalité permet à l'instance NetScaler ou à l'appliance

NetScaler Gateway de se connecter automatiquement et en toute sécurité au service NetScaler ADM et de lui envoyer des données système, d'utilisation et de télémétrie. Sur la base de ces données, vous obtenez des informations et des recommandations pour votre infrastructure NetScaler sur le service NetScaler ADM.

En utilisant la fonctionnalité de connexion au service NetScaler ADM et en intégrant vos instances NetScaler ou vos appliances NetScaler Gateway au service NetScaler ADM. Vous pouvez également gérer tous vos actifs NetScaler et NetScaler Gateway, que ce soit sur site ou dans le cloud. En outre, vous bénéficiez d'un accès à un ensemble riche de fonctionnalités de visibilité qui aident à identifier rapidement les problèmes de performances, l'utilisation élevée des ressources, les erreurs critiques, etc. Le service NetScaler ADM fournit un large éventail de fonctionnalités pour vos instances et applications NetScaler. Pour plus d'informations sur le service NetScaler ADM, voir NetScalerApplication Delivery Management Service

> **Important**
>
> - L'appliance NetScaler Gateway prend également en charge la fonctionnalité de connexion au service NetScaler ADM. Pour plus de facilité, l'appliance NetScaler Gateway n'est pas appelée explicitement dans les sections consécutives.

Qu'est-ce que le service NetScaler ADM ?

Le service NetScaler ADM est une solution basée sur le cloud qui vous aide à gérer, surveiller, orchestrer, automatiser et dépanner vos instances NetScaler. Il vous fournit également des informations analytiques et des recommandations personnalisées basées sur l'apprentissage automatique concernant les instances NetScaler ainsi que l'état, les performances et la sécurité des applications. Pour plus d'informations, voir Présentation du service NetScaler ADM

Comment la connexion au service NetScaler ADM est-elle activée ?

La connexion au service NetScaler ADM est activée par défaut après l'installation ou la mise à niveau de NetScaler ou Gateway vers la version 13.0 build 61.xx et ultérieure.

Quelles données sont capturées à l'aide de NetScaler ADM Service Connect ?

Les détails suivants sont capturés à l'aide de la connexion au service NetScaler ADM :

- **Détails de NetScaler**
  - ID de série
  - Numéro de série codé
  - ID d'hôte
  - UUID

  - Adresse IP de gestion
  - Nom d'hôte
  - Version
  - Type de construction
  - Créer
  - Type de licence
  - Hyperviseur
  - Type de déploiement (autonome/HA)
  - Type de plateforme
  - Description de la plateforme
  - ID système
  - Modes activés sur ADC
  - Fonctionnalités activées sur ADC

- **Informations sur la licence**
  - Fonctionnalités sous licence NetScaler
  - Numéro de licence

- **Indicateurs d'utilisation clés**
  - Date et heure du système
  - Pourcentage d'utilisation de l'UC
  - Pourcentage de CPU de gestion
  - Débit
  - Nouvelles sessions SSL
  - Débit de cryptage SSL
  - Débit de décryptage SSL
  - Temps de fonctionnement du système

- **Configuration**
  - fichier ns.conf

> **Remarque**
>
> Avant que le service NetScaler ADM ne se connecte au service NetScaler `ns.conf` ADM, il anonymise les mots de passe chiffrés ou hachés depuis l'appliance NetScaler ADM. La connexion au service NetScaler ADM vérifie les `-encrypted-passcrypt` paramètres et remplace la valeur cryptée ou hachée associée par. `XXXX` Le service NetScaler ADM se connecte ensuite au code et compresse le `ns.conf` fichier, puis l'envoie au point de terminaison du service NetScaler ADM.

- **Détails des erreurs critiques**
  - Pannes de disque dur

  - Pannes de carte SSL
  - Défaillances du bloc d'alimentation (PSU)
  - Panne du lecteur flash
  - Redémarrage à chaud
  - Utilisation prolongée de la mémoire supérieure à 90 % ou fuite de mémoire
  - Baisses de limite de taux durables

- **Utilisation des outils d'automatisation NITRO**
  - Utilisation d'outils d'automatisation tels que les SDK Ansible, Terraform ou NITRO.

- **Détails du diagnostic**

  > Remarque :
  >
  > L'outil de diagnostic ADM utilise les informations de diagnostic suivantes. Pour plus d'informations, consultez la rubrique relative à l' outil de diagnostic dans NetScaler ADM.

  - État de l'interface de ligne de commande ADC
  - État du DNS ADC
  - état de la connexion réseau au point de terminaison ADM « adm.cloud.com »
  - état de la connexion réseau au point de terminaison ADM « agent.adm.cloud.com »
  - état de la connexion réseau au service de confiance ADM « trust.citrixnetworkapi.net »
  - état de la connexion réseau au site de téléchargement d'ADM « download.citrixnetworkapi.net »

Comment les données sont-elles utilisées ?

En collectant les données, NetScaler peut vous fournir des informations détaillées et opportunes sur vos installations NetScaler, notamment les suivantes :

- **Principales mesures**. Détails des indicateurs clés concernant le processeur, la mémoire, le débit, le débit SSL et mettant en évidence les comportements anormaux sur les instances NetScaler.
- **Erreurs critiques**. Toute erreur critique qui aurait pu se produire sur vos instances NetScaler.
- **Avis de déploiement**. Identifiez les instances NetScaler qui sont déployées en mode autonome mais qui ont un débit élevé et sont vulnérables à un point de défaillance unique.
- **Outil de diagnostic**. Lorsque vous intégrez une instance ADC à NetScaler ADM, vous pouvez rencontrer quelques problèmes qui empêchent l'intégration réussie de l'instance ADC. Pour résoudre les problèmes, vous pouvez utiliser manuellement l'outil de diagnostic ou consulter les informations de diagnostic dans l'interface graphique d'ADM. Pour plus d'informations, consultez la section Outil de diagnostic.

Combien de temps les données collectées sont-elles conservées ?

Les données collectées ne sont pas conservées plus de 13 mois.

Si vous décidez de mettre fin à l'utilisation du service en désactivant la fonctionnalité de connexion au service NetScaler ADM depuis NetScaler, toutes les données précédemment collectées sont supprimées après une période de 30 jours.

Où les données sont stockées et dans quelle mesure sont-elles sécurisées ?

Toutes les données collectées par NetScaler ADM Service Connect sont stockées dans l'une des trois régions suivantes : États-Unis, Union européenne, Australie et Nouvelle-Zélande (ANZ). Pour plus d'informations, voir Considérations géographiques.

Les données sont stockées en toute sécurité avec une isolation stricte des locataires au niveau de la couche de base de données.

Comment désactiver la connexion au service NetScaler ADM ?

Si vous souhaitez désactiver la collecte de données via la connexion au service NetScaler ADM, consultez Comment activer et désactiver la connexion au service NetScalerADM.

Présentation du service NetScaler ADM Connect pour les appliances NetScaler

May 5, 2023

Le service NetScaler ADM est une solution basée sur le cloud qui vous aide à gérer, surveiller, orchestrer, automatiser et dépanner vos instances NetScaler. Il fournit également des informations analytiques et des recommandations basées sur l'apprentissage automatique pour la santé, les performances et la sécurité de vos applications. Pour plus d'informations, consultez NetScaler Application Delivery Management Service.

La connexion au service NetScaler Application Delivery Management (ADM) est une fonctionnalité qui permet l'intégration fluide des instances NetScaler dans le service NetScaler ADM. Cette fonctionnalité permet aux instances NetScaler et au service NetScaler ADM de fonctionner comme une solution globale, qui offre aux clients de multiples avantages.

La fonction de connexion au service NetScaler ADM permet à l'instance NetScaler de se connecter automatiquement au service NetScaler ADM et de lui envoyer des données système, d'utilisation et de télémétrie. Sur la base de ces données, le service NetScaler ADM vous fournit des informations et des recommandations sur votre infrastructure NetScaler et Gateway, notamment les suivantes :

- Informations sur les conseils de sécurité mettant en évidence vos appliances ADC vulnérables.
- Mise à niveau des informations consultatives mettant en évidence les appliances ADC qui ont atteint ou sont sur le point d'atteindre la fin de la maintenance et la fin de vie.
- Identification rapide des problèmes de performances, de l'utilisation élevée des ressources et des erreurs critiques.

Pour exploiter la puissance du service NetScaler ADM, vous pouvez choisir d'intégrer vos instances NetScaler au service NetScaler ADM. Le processus d'intégration utilise ADM Service Connect et rend l'expérience fluide et plus rapide pour vous.

> **Points à noter**
>
> - La connexion au service NetScaler ADM est désormais disponible sur les instances NetScaler MPX, SDX et VPX et sur les appliances NetScaler Gateway.
> - L'initiative du service NetScaler ADM qui utilise cette fonctionnalité de connexion au service NetScaler ADM est l'intégration low-touch basée sur ADM Service Connect. Pour plus d'informations, consultez la section Intégration simplifiée des instances NetScaler à l'aide de NetScaler ADM Service Connect.
> - Si la connexion au service ADM est activée sur une instance ADC, certains détails de diagnostic sont automatiquement envoyés au service ADM.

Pour plus d'informations, voir Gouvernance des données.

> **Important**
>
> La connexion au service NetScaler ADM ne parvient pas à collecter les données de sonde et ne peut pas aider à intégrer l'appliance ADC au service ADM si les conditions suivantes sont remplies :
>
> - `NSinternal` le compte utilisateur est désactivé.
> - La clé publique SSH n'est pas configurée.
>
> Pour surmonter le scénario précédent, Citrix vous recommande de suivre l'une des opérations suivantes :
>
> - Activez le compte `internaluser` d'utilisateur à l'aide du `set ns param -internaluserlogin ENABLED`.
> - Configurez l'authentification par clé publique. Pour plus d'informations, consultez la section Accès à une appliance NetScaler à l'aide de clés SSH etsans mot de passe.

Comment le service NetScaler ADM relie-t-il le support au service NetScaler ADM ?

Voici un flux de travail de haut niveau expliquant comment la fonctionnalité de connexion au service NetScaler ADM sur NetScaler interagit avec le service NetScaler ADM.

1. La fonctionnalité de connexion au service NetScaler ADM de l'appliance NetScaler se connecte automatiquement au service NetScaler ADM à l'aide d'une demande de sonde périodique.
2. Cette demande contient des données système, d'utilisation et de télémétrie, à l'aide desquelles le service NetScaler ADM vous fournit des informations et des recommandations sur votre infrastructure NetScaler. Par exemple, l'identification rapide des problèmes de performances, une utilisation élevée des ressources et des erreurs critiques.
3. Vous pouvez consulter les informations et les recommandations et décider d'intégrer vos instances ADC au service NetScaler ADM pour commencer à gérer vos instances NetScaler.
4. Lorsque vous décidez de vous intégrer, la fonctionnalité de connexion au service NetScaler ADM vous permet de terminer l'intégration en toute fluidité.

Quelles versions de NetScaler sont compatibles avec NetScaler ADM Service Connect ?

La connexion au service NetScaler ADM est prise en charge sur toutes les plateformes NetScaler et tous les modèles d'appliances (MPX, VPX et SDX). À partir de la version 13.0 build 61.xx de NetScaler, la connexion au service NetScaler ADM est activée par défaut pour les appliances NetScaler.

Comment activer la connexion au service NetScaler ADM ?

Si vous êtes déjà client de NetScaler et que vous effectuez une mise à niveau vers NetScaler version 13.0 build 61.xx, la connexion au service NetScaler ADM est activée par défaut dans le cadre du processus de mise à niveau.

Si vous êtes un nouveau client de NetScaler et que vous installez NetScaler version 13.0 build 61.xx, la connexion au service NetScaler ADM est activée par défaut dans le cadre du processus d'installation.

> **Remarque**
>
> Contrairement aux nouvelles appliances NetScaler, les appliances NetScaler existantes trouvent l'itinéraire via Citrix Insight Service (CIS) ou Call Home.

Comment activer et désactiver la connexion au service NetScaler ADM ?

Vous pouvez activer et désactiver la connexion au service NetScaler ADM à partir de méthodes CLI, GUI ou API NITRO.

Utilisation du CLI

Pour activer le service NetScaler ADM, connectez-vous à l'aide de l'interface de ligne de commande.

À l'invite de commande, tapez :


```
set adm parameter -admserviceconnect ENABLED
```

Pour désactiver le service NetScaler ADM, connectez-vous à l'aide de la CLI

À l'invite de commande, tapez :

```
set adm parameter -admserviceconnect DISABLED
```

> **Important**
>
> Si votre NetScaler utilise la version 13.0 build 61.xx, le nom du paramètre pour activer ou désactiver la connexion au service NetScaler est « autoconnect ». « Par exemple, pour activer la connexion de service, utilisez la commande `set adm parameter - autoconnect ENABLED` .

Utilisation de l'interface graphique

Pour désactiver le service NetScaler ADM, connectez-vous à l'aide de l'interface graphique de NetScaler

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance NetScaler (par exemple, http://192.0.2.10).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Système > Paramètres > Configurer les paramètres ADM**.
4. **Sur la page**Configurer les paramètres ADM**, désactivez la boîte de dialogue**Activer la connexion au service NetScaler ADM**, puis cliquez sur OK.**

Utilisation de l'API NITRO

Vous pouvez désactiver la connexion au service NetScaler ADM à l'aide de la commande NITRO.

- Dans NetScaler version 13.0 build 61.xx, vous pouvez activer ou désactiver la connexion au service NetScaler ADM à l'aide de la commande suivante :

  ```
  - curl -X PUT -H "Content-Type:application/json"http://192.0.2.10/
    nitro/v1/config/admparameter> -d '{ "admparameter":{ "autoconnect
    ":"enabled" } } ' -u nsroot:Test@1
  ```

- À partir de la version 13.0 build 64.xx de NetScaler, le nom du paramètre « autoconnect » est renommé en. `admserviceconnect` Vous pouvez désactiver la connexion au service NetScaler ADM à l'aide de la commande suivante :


```
- curl -X PUT -H "Content-Type:application/json" http://192.0.2.10/
  nitro/v1/config/admparameter -d '{ "admparameter":{ "admserviceconnect
  ":"disabled" } } ' -u nsroot:Test@1
```

Outil de diagnostic

Lorsque vous intégrez une instance ADC à NetScaler ADM, vous pouvez rencontrer quelques problèmes qui empêchent l'intégration réussie de l'instance ADC. Pour résoudre les problèmes, vous pouvez utiliser manuellement l'outil de diagnostic ou consulter les informations de diagnostic dans l'interface graphique d'ADM.

- Pour plus d'informations sur les détails capturés à l'aide de ADM Service Connect, consultez la section Gouvernance des données.
- Pour plus d'informations sur l'outil de diagnostic, reportez-vous à la section Outil de diagnostic.

Comportement de l'agent intégré à NetScaler ADM

À partir de la version 13.0 build 61.xx de NetScaler et des versions ultérieures, l'agent intégré NetScaler ADM disponible sur les instances NetScaler communique avec le service ADM. Il communique sans qu'il soit nécessaire d'initialiser manuellement l'instance ADC correspondante. Une fois la communication avec le service ADM établie, l'agent intégré reste permanent en effectuant une mise à niveau automatique vers la dernière version du logiciel régulièrement.

Auparavant, vous deviez initialiser l'agent intégré sur les instances ADC, à l'aide des commandes `mastools`, pour établir une communication avec le service ADM et pour des mises à niveau automatiques régulières.
Pour plus d'informations, voir Configurer l'agent intégré ADC pour gérer les instances.

Références

Pour plus d'informations sur la connexion au service NetScaler ADM, consultez les rubriques suivantes :

- Gouvernance des données : gouvernance des données.
- Service NetScaler ADM : service de gestion des livraisons d'applications NetScaler.

Mettre à niveau et rétrograder une appliance NetScaler

May 5, 2023

NetScaler 13.1 propose des fonctionnalités nouvelles et mises à jour avec des fonctionnalités améliorées. Une liste complète des améliorations est répertoriée dans les notes de mise à jour accompagnant l'annonce de publication. Lisez les notes de mise à jour avant de mettre à niveau votre logiciel.

Cette section fournit des informations sur la **mise à niveau et la rétrogradation du microprogramme d'une appliance NetScaler** (MPX et VPX) à l' **aide**de l'interface graphique ou de la CLI NetScaler.

Vous pouvez également **utiliser NetScaler ADM pour mettre à niveau une**appliance NetScaler. Pour plus d'informations, consultez :

- 10 manières dont le service NetScaler ADM facilite les mises à niveau de NetScaler
- Utiliser le service NetScaler ADM pour mettre à niveau les instances NetScaler
- Utiliser le logiciel NetScaler ADM pour mettre à niveau les instances NetScaler

Pour plus d'informations sur la **mise à niveau d'une appliance NetScaler SDX**, consultez la section Mise à niveau d'un seul bundle.

> **Remarque**
>
> À partir de la version 13.1 de NetScaler, les fonctions et fonctionnalités classiques obsolètes basées sur des politiques sont supprimées de l'appliance NetScaler. Pour plus d'informations, consultez le tableau FAQ sur la dépréciation des stratégies classiques .

Avant de commencer

June 20, 2023

Avant de commencer le processus de mise à niveau ou de rétrogradation, assurez-vous de vérifier les points suivants :

- Évaluez le contrat de support de votre organisation. Documentez le numéro de série de l'appliance, le contrat de support et les coordonnées de contact pour obtenir de l'assistance auprès du support technique Citrix ou du partenaire agréé Citrix.
- Temps alloué à la mise à niveau des appliances NetScaler. Suivez la procédure de contrôle des modifications de votre organisation. Allouez deux fois plus de temps pour effectuer les mises à niveau. Prévoyez suffisamment de temps pour mettre à niveau chacune des appliances NetScaler.
- Le système de licences NetScaler applique la validation des licences d'adhésion aux Customer Success Services (CSS) pour les appliances NetScaler VPX. Avant de mettre à niveau une appli-

ance NetScaler VPX, assurez-vous que l'appartenance CSS actuelle de l'appliance est valide et qu'elle n'a pas expiré.

Assurez-vous que la date d'expiration actuelle de l'adhésion au CSS est égale ou ultérieure à la date d'éligibilité CSS de la version du produit NetScaler à mettre à niveau.

Si la date d'expiration de l'adhésion à la CSS est antérieure à la date d'éligibilité à la CSS, la licence existante ne fonctionne pas sur la version mise à niveau de l'appliance NetScaler VPX. Cette fonctionnalité peut empêcher l'utilisation non autorisée des licences. Vous devez renouveler l'adhésion à la CSS avant de pouvoir mettre à niveau l'appliance NetScaler VPX.

Pour obtenir la liste des versions de NetScaler VPX et leurs dates d'éligibilité CSS, consultez les dates d'éligibilité des produits NetScaler Customer Success Services.

Pour plus d'informations sur le CSS, consultez Customer Success Services.

- Citrix recommande la mise à niveau d'une version majeure à la fois. Par exemple, si l'appliance NetScaler utilise la version 12.1 et que vous souhaitez effectuer une mise à niveau vers la version 13.1, commencez par la mettre à niveau vers la version 13.0, puis vers la version 13.1.
- Le cadre de licences et les types de licences. Une mise à niveau d'une édition logicielle peut nécessiter de nouvelles licences, telles que :
  - mise à niveau de l'édition standard vers l'édition avancée, ou
  - l'édition standard à l'édition Premium, ou
  - l'édition avancée jusqu'à l'édition Premium.

  Les licences NetScaler existantes continuent de fonctionner lorsque vous effectuez une mise à niveau vers la version 13.1. Pour plus d'informations, voir Licences
- Vérifiez la présence de commandes, de paramètres et d'OID SNMP nouveaux et obsolètes.
- Consultez la matrice de compatibilité matérielle et logicielle de NetScaler MPX.
- Si la page de connexion à NetScaler Gateway est personnalisée, assurez-vous que le thème de l'interface utilisateur est défini par défaut.
- Si vous mettez à niveau LOM, consultez la page Mise à niveau du microprogramme LOM.
- Téléchargez le microprogramme NetScaler depuis les téléchargements de NetScaler. Pour les étapes détaillées du téléchargement du microprogramme NetScaler, consultez la section Télécharger un package de version de NetScaler.
- Sauvegardez les fichiers. Effectuez une sauvegarde du fichier de configuration, du fichier de personnalisation, des certificats, des scripts de surveillance, des fichiers de licence, etc. manuellement ou consultez la documentation suivante pour effectuer une sauvegarde à l'aide de la CLI ou de l'interface graphique NetScaler - Sauvegarde et restauration.
  - Reportez-vous à la liste suivante pour connaître les autres fichiers personnalisés courants à sauvegarder.

    * /nsconfig/monitors/*.pl
    * /nsconfig/rc.netscaler
  - Sauvegardez et supprimez le dossier de personnalisation. C'est généralement sous /var/customizations. Un exemple de personnalisation est une page d'ouverture de session avec un logo. Après avoir copié le dossier de personnalisations, vous devez le supprimer de l'appliance NetScaler avant de procéder à la mise à niveau de l'appliance. La mise à niveau avec personnalisation en place peut entraîner certains problèmes.

> **Important :**
>
> Citrix recommande vivement de consulter les procédures de sauvegarde ci-dessus. Établissez un plan d'action au cas où la mise à jour ne serait pas terminée sur l'appliance NetScaler.

- Vérifiez qu'il y a suffisamment d'espace dans les répertoires /var et /flash pour l'appliance NetScaler avant d'effectuer une mise à niveau. Le fichier /var nécessite 5 Go d'espace libre (1 Go pour le bundle de mise à niveau + 4 Go pour le processus de mise à niveau)
  Le /flash nécessite suffisamment d'espace pour copier sur le nouveau noyau, qui diffère entre 140 Mo et 160 Mo environ, garantissant qu'il y a au moins 250 Mo d'espace libre disponible.
  Pour plus d'informations sur la suppression de l'espace disque dans /var, consultez Comment libérer de l'espace sur le répertoire /var pour la journalisation des problèmes liés à une appliance NetScaler.
  Pour plus d'informations sur la suppression des espaces disque dans /flash, reportez-vous à la section https://support.citrix.com/article/CTX133587.
- Validez l'intégrité de l'appliance NetScaler. Si vous possédez une appliance matérielle NetScaler, Citrix recommande vivement de l'exécuter fsck pour exécuter une vérification du disque et valider l'intégrité du disque dur NetScaler. En cas d'erreur, réinitialisez le disque dur et répétez la commande de vérification du disque. Si le message d'erreur réapparaît, contactez le support NetScaler pour approfondir le problème.
  - Validez l'intégrité du disque dur à l'aide d'une commande fsck. Pour plus d'informations, voir CTX122845.
  - Validez l'intégrité d'une appliance NetScaler à l'aide des fichiers des bundles de diagnostic et en téléchargeant les journaux vers Citrix Insight Service à des fins d'analyse. Pour plus d'informations, voir Comment collecter un pack de support technique.
- Consultez la matrice de support NetScaler VPX etles directives d'utilisation.
- Consultez la section FAQ .
- Vérifiez les procédures de mise à niveau avec un environnement de test.

Pour plus d'informations sur les conditions préalables à la mise à niveau ou à la rétrogradation de l'appliance NetScaler, consultez ces articles de support :

- CTX220371 : Vous devez lire les articles avant et après la mise à niveau de NetScaler

Considérations relatives à la mise à niveau des fichiers de configuration personnalisés du répertoire /etc

May 5, 2023

Les fichiers de configuration suivants peuvent être modifiés dans le répertoire `/etc` :

- `inetd.conf`
- `syslog.conf`
- `newsyslog.conf`
- `ntp.conf`
- `crontab`
- `host.conf`
- `hosts`
- `ttys`
- `sshd_config`
- `httpd.conf`
- `monitrc`
- `rc.conf`
- `ssh_config`
- `localtime`
- `issue`
- `issue.net`
- `ldap.conf`
- `motd`

> **Remarque :**
>
> De nouveaux fichiers peuvent être ajoutés à la liste ci-dessus en fonction de la version NetScaler exécutée sur l'appliance. Vous pouvez afficher une liste de fichiers mise à jour en exécutant la commande shell suivante dans l'interface de ligne de commande NetScaler :
>
> ```
> grep NSETC= /etc/rc
> ```

Si vous avez modifié l'un des fichiers de configuration du `/etc` répertoire et que vous l'avez copié dans le `/nsconfig` répertoire, pour maintenir la persistance, l'appliance NetScaler crée un lien symbolique pointant vers le fichier dans `/etc`. `/nsconfig`

Pa exemple : `/etc/httpd.conf -> /nsconfig /httpd.conf`

Un package de version peut contenir sa propre version des fichiers de configuration du répertoire `/etc`. Ces fichiers de configuration incluent des mises à jour importantes nécessaires au bon fonctionnement de l'appliance NetScaler. La mise à niveau d'un dispositif NetScaler vers une version remplace les fichiers de configuration du `/etc` répertoire par les fichiers de configuration contenant les mises à jour de version.

Prenons l'exemple d'un fichier de configuration personnalisé `example.conf`, présent dans le répertoire `/etc`. Le fichier `example.conf` est copié dans le répertoire `/nsconfig` pour préserver sa persistance. L'appliance NetScaler crée un lien symbolique `/etc` pointant vers le fichier dans : `/nsconfig /etc/example.conf -> / nsconfig /example.conf`

En outre, un package de version inclut sa propre version de `example.conf`, qui contient des mises à jour importantes. Le comportement suivant est observé lorsque vous mettez à niveau l'appliance NetScaler vers la version suivante :

Le lien symbolique `/etc/example.conf` étant déjà présent, l'appliance NetScaler ne place pas la copie du package de version `example.conf` dans le `/etc` répertoire pendant le processus de mise à niveau.

Comme la copie du package de version `example.conf` contient des mises à jour importantes, leur absence dans le `/etc` répertoire peut entraîner la défaillance ou le mauvais fonctionnement de l'appliance NetScaler.

Étapes pour préserver les modifications apportées aux mises à niveau

Pour vous assurer que les mises à jour de version et vos personnalisations ne sont pas perdues, effectuez les opérations suivantes :

- Étapes de pré-mise à niveau
  - Sauvegarder le fichier personnalisé avant la mise à niveau
  - Suppression de la persistance du fichier personnalisé avant la mise à niveau
- Étapes post-mise à niveau :
  - Application de personnalisations au fichier mis à niveau et ajout de persistance après la mise à niveau

> **Important :**
> NE remplacez PAS directement votre fichier personnalisé dans le dossier `/etc`. Le remplacement direct d'un fichier `/etc` par le fichier personnalisé de sauvegarde supprime toutes les mises à jour de version ajoutées au fichier pendant le processus de mise à niveau.

Sauvegarder le fichier personnalisé avant la mise à niveau

Effectuez une sauvegarde des fichiers personnalisés présents dans le répertoire `/nsconfig` avant de mettre à niveau l'appliance.

Créez un répertoire `/var/nsconfig_backup` et déplacez les fichiers personnalisés vers ce répertoire. En d'autres termes, déplacez tous les fichiers que vous avez modifiés dans le répertoire `/etc` et dans lesquels vous avez copié `/nsconfig` en exécutant la commande suivante à l'invite du shell :

```
mv /nsconfig/<filename> /var/nsconfig_backup/
<!--NeedCopy-->
```

Exemple :

```
mv /nsconfig/httpd.conf /var/nsconfig_backup/
<!--NeedCopy-->
```

Suppression de la persistance du fichier personnalisé avant la mise à niveau

Supprimez les liens symboliques `/etc` pointant vers les fichiers `/nsconfig` avant de mettre à niveau l'appliance.

1. Vérifiez les liens symboliques existants dans le répertoire `/etc` en exécutant la commande suivante à l'invite du shell :

   ```
   ls -la /etc
   <!--NeedCopy-->
   ```

2. Supprimez un lien symbolique `/etc` pointant vers un fichier `/nsconfig` en exécutant la commande suivante à l'invite du shell :

   ```
   unlink /etc/<filename>
   <!--NeedCopy-->
   ```

   Exemple :

   ```
   unlink /etc/httpd.conf
   <!--NeedCopy-->
   ```

3. Vérifiez que le lien symbolique est supprimé en exécutant la commande suivante à l'invite du shell :

   ```
   cat /etc/<filename>
   <!--NeedCopy-->
   ```


Exemple :

```
cat /etc/httpd.conf
<!--NeedCopy-->
```

Cette commande n'affiche aucun contenu si le lien symbolique est supprimé.

Application de personnalisations au fichier mis à niveau et ajout de persistance après la mise à niveau

Si vous avez effectué une sauvegarde d'un fichier de configuration `/nsconfig` modifié sur `/var/nsconfig_backup`, procédez comme suit après la mise à niveau de l'appliance :

1. Comparez le fichier présent dans les répertoires `/var/nsconfig_backup` et `/etc`. Ajoutez manuellement les modifications appropriées au fichier `/etc` contenant déjà les mises à jour de version.

   > **Important :**
   >
   > Le remplacement direct du fichier `/etc` par le fichier `/var/nsconfig_backup` supprime toutes les mises à jour de version ajoutées au fichier pendant le processus de mise à niveau. Cette suppression des mises à jour peut entraîner l'échec ou le mauvais fonctionnement des fonctionnalités NetScaler associées.

2. Pour maintenir la persistance, copiez le fichier mis à jour présent dans le répertoire `/etc` dans le répertoire `/nsconfig` en exécutant la commande suivante à l'invite du shell :

   ```
   cp /etc/<filename> /nsconfig/
   <!--NeedCopy-->
   ```

   Exemple :

   ```
   cp /etc/httpd.conf /nsconfig/
   <!--NeedCopy-->
   ```

3. Répétez les deux étapes ci-dessus pour chaque fichier personnalisé présent dans le répertoire `/var/nsconfig_backup`.
4. Redémarrez l'appliance pour que les modifications soient prises en compte.

Remarques sur la mise à niveau - configuration SNMP

May 5, 2023

Le paramètre de délai d'expiration d'une alarme SNMP est une option interne qui n'a aucun impact sur la configuration de l'alarme.

Le paramètre Timeout peut apparaître dans les configurations d'alarme SNMP de la configuration en cours (sh running) et de la configuration enregistrée (ns.conf) même si vous n'avez apporté aucune modification à ces configurations d'alarme SNMP.

Lors de la mise à niveau vers une version contenant le correctif du problème de réglage du délai d'expiration, les configurations SNMP sont réinitialisées par erreur aux valeurs par défaut.

Les alarmes SNMP suivantes (si elles sont configurées) sont affectées lors d'une mise à niveau :

- APPFW-BUFFER-OVERFLOW
- APPFW-COOKIE
- BALISE APPFW-CSRF
- APPFW-DENY-URL
- COHÉRENCE DES CHAMPS APPFW
- FORMAT DE CHAMP APPFW
- APPFW-POLICY-HIT
- EN-TÊTE APPFW-REFERER-HEADER
- COMMERCE ÉLECTRONIQUE SÉCURISÉ PAR APPFW-SAFE
- APPFW-SAFE-OBJECT
- APPFW-SQL
- URL DE DÉMARRAGE APPFW-
- TYPE DE VIOLATION D'APPFW
- PIÈCE JOINTE APPFW-XML
- APPFW-XML-DOS
- APPFW-XML-SCHEMA-COMPILE
- ERREUR APPFW-XML-SOAP-FAULT
- APPFW-XML-SQL
- VALIDATION APPFW-XML
- APPFW-XML-WSI
- APPFW-XML-XSS
- APPFW-XSS
- CLUSTER-BACKPLANE-HB-MANQUANT
- ÉTAT DE SANTÉ DES NŒUDS DU CLUSTER
- QUORUM DE NŒUDS DE CLUSTER
- INCOMPATIBILITÉ ENTRE LES VERSIONS DU CLUSTER
- COMPACT-FLASH-ERRORS
- CHANGEMENT DE CONFIGURATION
- CONFIG-SAVE
- HA-BAD-STATE-SECONDAIRE

- HA-PAS DE BATTEMENTS DE CŒUR
- ÉCHEC DE LA SYNCHRONISATION HA-
- HA-VERSION-DISCORDANCE
- HARD-DISK-DRIVE-ERRORS
- CHANGEMENT D'ÉTAT
- HA-STICKY-PRIMARY
- ÉCHEC DE L'ALLOCATION DE PORT
- SYNFLOOD

Ces configurations d'alarmes SNMP sont affectées lorsque vous mettez à niveau NetScaler vers les versions suivantes :

- Version 11.1 build 61.2 ou ultérieure
- Version 12.0 build 61.0 ou ultérieure
- Version 12.1 build 30.1 ou ultérieure
- Version 13.0 build 51.4 ou ultérieure

Exemple

Prenons un exemple d'alarme SNMP CLUSTER-NODE-HEALTH.

```
CLUSTER-NODE-HEALTH SNMP alarm is set up by using the NetScaler command line:

> set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -severity Major

> save config
<!--NeedCopy-->
```

Cette configuration d'alarme SNMP apparaît dans le fichier de configuration enregistré (`ns.conf`) sous la forme suivante :

```
set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -severity Major -timeout 86400

<!--NeedCopy-->
```

Lors d'une mise à niveau vers l'une des versions mentionnées ci-dessus, l'erreur suivante apparaît dans le fichier ns.log :

```
May 23 09:14:46 <local0.err> ns nsconfigd: __init_config_filter(): (null) line 0: No such argument [-timeout]>> set snmp alarm CLUSTER-
```



```
    NODE-HEALTH -time 111 -state DISABLED -severity Major -timeout
    86400.
<!--NeedCopy-->
```

Après la mise à niveau, les configurations d'alarme SNMP sont réinitialisées aux valeurs par défaut.

Solution

Utilisez l'une des résolutions suivantes :

- Avant la mise à niveau, supprimez le paramètre de délai d'expiration des configurations SNMP dans le fichier de configuration enregistré (ns.conf).
- Après la mise à niveau, reconfigurez les alarmes SNMP sans le paramètre de délai d'expiration.

Télécharger un package de version de NetScaler

May 5, 2023

Procédez comme suit pour télécharger un package de version de NetScaler :

1. Ouvrez la page de téléchargement de NetScaler dans un navigateur Web.
2. Sur la page Téléchargements de NetScaler, développez la version de **NetScaler vers laquelle vous souhaitez effectuer la mise** à jour.
3. Développez l'une des catégories appropriées, puis cliquez sur le lien de création de NetScaler. Par exemple, pour télécharger une version du microprogramme NetScaler, développez le **microprogramme**et cliquez sur la version de NetScaler que vous souhaitez télécharger.
4. Sur la page de build NetScaler sélectionnée, développez la section **Build**, cliquez sur **Télécharger le fichier pour télécharger le package** de build NetScaler.

> **Remarque :**
> La somme de contrôle est fournie pour garantir que vous faites correspondre le package de construction téléchargé avec le package réel qui est hébergé sur le site Web. La somme de contrôle est une vérification importante qui permet de s'assurer que vous disposez des bons bits.

Mettre à niveau une appliance autonome NetScaler

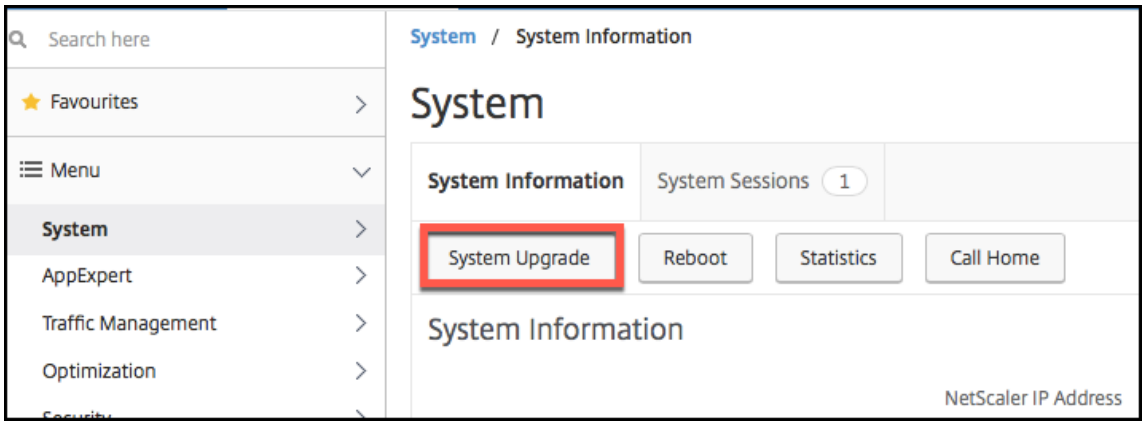
July 31, 2023

Avant de mettre à niveau le logiciel système, assurez-vous de lire la section Avant de commencer et de remplir les conditions préalables, telles que la sauvegarde des fichiers nécessaires et le téléchargement du microprogramme NetScaler.

Mettre à niveau une appliance autonome NetScaler à l'aide de l'interface graphique

Suivez ces étapes pour mettre à niveau un NetScaler autonome vers la version 13.1 à l'aide de l'interface graphique.

1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler, par exemple. `http://10.102.29.50`
2. Dans Nom d'utilisateur et mot de passe, tapez les informations d'identification de l'administrateur (nsroot/nsroot), puis cliquez **sur Connexion**.
3. Dans l'interface graphique, cliquez sur **Mise à niveau du système**.



4. Dans le menu **Choisir un fichier**, choisissez l'option appropriée : **Local** ou **Appliance**. Si vous souhaitez utiliser l'option Appliance, le microprogramme doit d'abord être téléchargé sur NetScaler. Vous pouvez utiliser n'importe quelle méthode de transfert de fichiers, telle que WinSCP, pour télécharger le microprogramme NetScaler sur l'appliance.
5. Sélectionnez le fichier approprié et cliquez sur **Mettre à niveau**.
6. Suivez les instructions pour mettre à niveau le logiciel.
7. Lorsque vous y êtes invité, sélectionnez **Redémarrer**.

Après la mise à niveau, fermez toutes les instances de navigateur et videz le cache de votre ordinateur avant d'accéder à l'appliance.

Mettre à niveau une appliance autonome NetScaler à l'aide de l'interface de ligne de commande

Suivez ces étapes pour mettre à niveau un NetScaler autonome vers la version 13.1 à l'aide de l'interface de ligne de commande :

Dans la procédure suivante, `<release>` et `<releasenumber>` représentent la version de mise à niveau vers laquelle vous effectuez la mise à niveau et `<targetbuildnumber>` le numéro de version vers lequel vous effectuez la mise à niveau. La procédure inclut des étapes facultatives pour éviter de perdre les mises à jour qui sont poussées vers le répertoire /etc pendant la mise à niveau.

1. Utilisez un client SSH, tel que PuTTY, pour ouvrir une connexion SSH vers l'appliance.
2. Connectez-vous à l'appliance à l'aide des informations d'identification de l'administrateur. Enregistrez la configuration en cours d'exécution. À l'invite, tapez :

   ```
   save config
   ```

3. Passez à l'invite du shell en exécutant la commande suivante :

   ```
   shell
   ```

4. Créez une copie du fichier ns.conf. À l'invite shell, tapez :

   - `cd /nsconfig`
   - `cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber>`

   Vous devez sauvegarder le fichier de configuration sur un autre ordinateur.

5. **IMPORTANT :**

   > Il est important que les modifications de mise à niveau et vos personnalisations soient appliquées à une appliance NetScaler mise à niveau. Par conséquent, si vous avez des fichiers de configuration personnalisés dans le répertoire `/etc`, effectuez les **étapes préalables à la mise à niveau** dans Considérations relatives à la mise à niveau pour les fichiers

6. Créez un emplacement pour le package d'installation. À l'invite du shell, tapez :

   - `cd /var/nsinstall`
   - `cd <releasenumber>`

     > **Remarque :**
     >
     > Si le répertoire du numéro de version souhaité n'est pas présent, créez-en un à l'aide de la commande suivante :
     >
     > `mkdir <releasenumber>`
     >
     > **Exemple :**
     >
     > `mkdir 13.1`

- `mkdir build_<targetbuildnumber>`
- `cd build_<targetbuildnumber>`

7. Copiez le microprogramme NetScaler déjà téléchargé dans le répertoire de compilation que vous avez créé à l'étape ci-dessus, en utilisant n'importe quelle méthode de transfert de fichiers telle que WinSCP. Consultez la section Avant de commencer pour plus d'informations sur le téléchargement du microprogramme NetScaler.
8. Extraire le contenu du package d'installation. Exemple :

   ```
   tar -xvzf build-13.1-37.2_nc_64.tgz
   ```

9. Exécutez le script installns pour installer la nouvelle version du logiciel système.

   ```
   ./installns
   ```

10. Lorsque vous y êtes invité, redémarrez NetScaler.
11. **IMPORTANT :**

    Il est important que les modifications de mise à niveau et vos personnalisations soient appliquées à une appliance NetScaler mise à niveau. Par conséquent, si vous avez des fichiers de configuration personnalisés dans le répertoire `/etc`, suivez les **étapes postérieures à la mise à niveau** de la section Considérations relatives à lamise à niveau

Vous trouverez ci-dessous un exemple de mise à niveau du microprogramme NetScaler.

```
login: nsroot

Password: nsroot

Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134

Done

> save config

> shell

Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134

root@NSnnn# cd /var/nsinstall

root@NSnnn# cd 13.1

root@NSnnn# mkdir build_43.1

root@NSnnn# cd build_43.1
```



```
22
23 root@NSnnn# ftp <FTP server IP address>
24
25 ftp> mget build-13.1-41.1_nc.tgz
26
27 ftp> bye
28
29 root@NSnnn# tar xzvf build-13.1-41.1_nc.tgz
30
31 root@NSnnn# ./installns
32
33 installns version (13.1-41.1) kernel (ns-13.1-41.1_nc.gz)
34
35 ...
36
37 Copying ns-13.1-41.1_nc.gz to /flash/ns-13.1-41.1_nc.gz ...
38
39 ...
40
41 Installation has completed.
42
43 Reboot NOW? [Y/N] Y
```

Regardez cette vidéo pour découvrir comment mettre à niveau un dispositif autonome NetScaler à l'aide de l'interface de ligne de commande.

Mettre à niveau une appliance autonome NetScaler à l'aide de l'API NITRO

Pour utiliser l'API NITRO pour mettre à niveau ou rétrograder un NetScaler, voir Automatiser la mise à niveau et la rétrogradation de NetScaleravec une seule API.

Vérifier l'état des entités sur l'appliance NetScaler après la mise à niveau

Une fois l'appliance NetScaler mise à niveau, vérifiez l'état des entités suivantes :

- Les serveurs virtuels sont en état UP
- Les moniteurs sont en état UP
- Les sites GSLB se synchronisent sans problème
- Tous les certificats sont présents sur l'appliance
- Toutes les licences sont présentes sur l'appliance

Vérifiez et installez la mise à jour logicielle NetScaler 13.1

Mettez à jour le logiciel NetScaler lorsqu'une mise à jour est disponible, pour de meilleures performances. Une mise à jour de NetScaler peut inclure des améliorations de fonctionnalités, des corrections de performances ou des améliorations. N'oubliez pas de lire les notes de publication pour voir quels correctifs et améliorations sont disponibles dans la mise à jour. Pour vérifier et installer une mise à jour logicielle, procédez comme suit.

1. Sur la page d'accueil de NetScaler, cliquez sur **Vérifier les mises à jour** dans le menu **nsroot** en haut à droite.
2. Dans la page **Dernières mises à jour logicielles système disponibles**, vérifiez la mise à jour logicielle disponible que vous pouvez installer.
3. Cliquez sur **Télécharger** pour télécharger le package d'installation depuis le site Web de téléchargement de NetScaler .
4. Après avoir téléchargé le package logiciel, installez la mise à jour via la procédure CLI ou GUI.

> **Remarque**
>
> Le lien **Vérifier la mise à jour** n'est accessible que si vous vous connectez à l'interface graphique via le protocole HTTP et non via le protocole HTTPS.

Ressources connexes

Les ressources suivantes fournissent des informations connexes sur la mise à niveau ou la rétrogradation d'une appliance NetScaler :

- Tutoriel vidéo - Comment mettre à niveau votre NetScalerà l'aide de l'interface de ligne de commande

Rétrograder une appliance autonome NetScaler

May 8, 2023

Vous pouvez revenir à n'importe quelle version antérieure sur un NetScaler autonome à l'aide de l'interface de ligne de commande ou de l'interface graphique.

> **Remarque :**
>
> Une perte de configuration peut survenir lors d'une rétrogradation. Comparez les configurations avant et après la rétrogradation, puis saisissez à nouveau manuellement les entrées manquantes.

Rétrograder une appliance NetScaler à l'aide de l'interface de ligne de commande

Suivez les étapes ci-dessous pour rétrograder une appliance autonome NetScaler exécutant la version 13.1 vers une version antérieure.

Dans cette procédure, <release> et <releasenumber> représente la version de mise à niveau vers laquelle vous êtes en train de rétrograder et <targetbuildnumber> représente le numéro de version vers lequel vous procédez à la rétrogradation.

1. Ouvrez une connexion SSH à NetScaler à l'aide d'un client SSH, tel que PuTTY.
2. Connectez-vous à NetScaler à l'aide des informations d'identification de l'administrateur. Enregistrez la configuration en cours d'exécution. À l'invite, tapez :

   enregistrer la configuration
3. Créez une copie du fichier ns.conf. À l'invite shell, tapez :

   a) `cd /nsconfig`
   b) `cp ns.conf ns.conf.NS<currentbuildnumber>`

   Vous devez sauvegarder une copie du fichier de configuration sur un autre ordinateur.
4. <releasenumber>Copiez le <releasenumber> fichier de configuration \ (ns.conf.ns \) vers ns.conf. À l'invite shell, tapez :

```
cp ns.conf.NS<releasenumber> ns.conf
<!--NeedCopy-->
```

> **Remarque :**
>
> ns.conf.NS<releasenumber> est le fichier de configuration de sauvegarde qui est automatiquement créé lorsque le logiciel système est mis à niveau de la version finale <releasenumber> vers la version actuelle.
>
> Il peut y avoir une perte de configuration lors d'une rétrogradation. Après le redémarrage de la solution matérielle-logicielle, comparez la configuration enregistrée à l'étape 3 avec la configuration en cours d'exécution et effectuez les ajustements nécessaires pour les fonctionnalités et entités configurées avant la mise à niveau vers le bas. Enregistrez la configuration en cours d'exécution après avoir effectué les modifications.
>
> **Important :**
>
> Si le routage est activé, effectuez l'étape 5. Sinon, passez directement à l'étape 6.

5. Si le routage est activé, le fichier Zebos.conf contient la configuration. À l'invite shell, tapez :

```
cd /nsconfig
cp ZebOS.conf ZebOS.conf.NS
cp ZebOS.conf.NS<targetreleasenumber> ZebOS.conf
```



```
4  <!--NeedCopy-->
```

6. Changez le `/var/nsinstall/<releasenumber>nsinstall`répertoire ou créez-en un s'il n'existe pas.
7. Changez le `build_<targetbuildnumber>`répertoire ou créez-en un s'il n'existe pas.
8. Téléchargez ou copiez le package d'installation (`build-<release>-<targetbuildnumber>.tgz`) dans ce répertoire et extrayez le contenu du package d'installation.
9. Exécutez le `installns` script pour installer la nouvelle version du logiciel système. Le script met à jour le `/etc` répertoire.

   Si le fichier de configuration de la version vers laquelle vous procédez à la rétrogradation existe sur la solution matérielle-logicielle, vous êtes invité à charger cette configuration :

   Figure 1. Menu rétrograder s'il existe un fichier de configuration


```
 version build       size  last modified  file name
Copied to ns.conf    72545  Jun 18 04:42   ns.conf.NS10.1-112.13
  NS10.1  112.13     72545  Jun 18 04:42   ns.conf.NS10.1
  NS10.1  112.13     72545  Jun 18 04:42   ns.conf.4
  NS10.1  109.1      87219  Jun 18 04:42   ns.conf.NS10.1-109.1
  NS10.1  93.051     74443  Jun 18 04:42   ns.conf.NS10.1-93.051
  NS10.0  29.1.      62849  Jun 18 04:42   ns.conf.NS10.0-29.1.









Listed above are 5 configuration files, found in /nsconfig, that are
appropriate for use with build 112.13.

Use the arrow keys to select an item in the menu above, then type:
  'c' - copy file over ns.conf
  'v' - view file (with vi; type ':q!' to exit vi)
  '>' - more files
  '<' - fewer files
  'd' - done
```


Si l'espace libre disponible sur le lecteur flash est insuffisant pour installer la nouvelle version, NetScaler abandonne l'installation. Nettoyez manuellement le lecteur flash et redémarrez l'installation.

Exemple :

```
login: nsroot

Password: nsroot

Last login: Mon Apr 24 02:06:52 2017 from 10.102.29.9

Done

> save config

> shell

root@NSnnn# cp ns.conf.NS10.5 ns.conf

root@NSnnn# cd /var/nsinstall

root@NSnnn# mkdir 10.5nsinstall

root@NSnnn# cd 10.5nsinstall

root@NSnnn# mkdir build_57

root@NSnnn# cd build_57

root@NSnnn# ftp 10.102.1.1

ftp> mget build-10.5-57_nc.tgz

ftp> bye

root@NSnnn# tar -xzvf build-10.1-125_nc.tgz

root@NSnnn# ./installns

installns version (10.5-57) kernel (ns-10.5-57.gz)

...

...
```



```
40
41 ...
42
43 Copying ns-10.5-57.gz to /flash/ns-10.5-57_nc.gz ...
44
45 Changing /flash/boot/loader.conf for ns-10.5-57 ...
46
47
48
49 Installation has completed.
50
51
52
53 Reboot NOW? [Y/N] Y
54 <!--NeedCopy-->
```

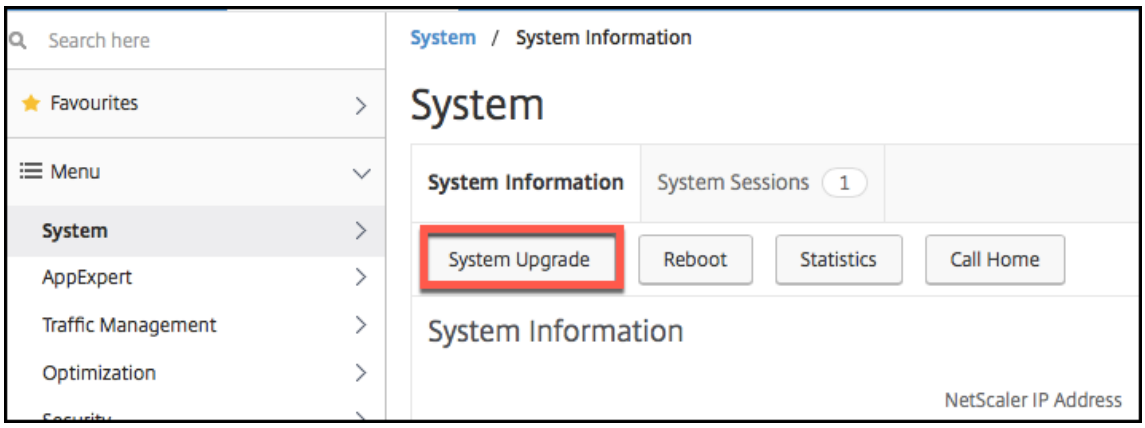
Rétrograder une appliance NetScaler à l'aide de l'interface graphique

Vous pouvez utiliser l'assistant de mise à niveau de l'interface graphique pour rétrograder une appliance NetScaler exécutant la version 13.1 vers une version antérieure.

> **Remarques :**
>
> Vous ne pouvez pas rétrograder une appliance NetScaler exécutant la version 13.1 directement vers la version 10.5 ou une version antérieure à l'aide de l'interface graphique. Citrix recommande d'utiliser l'interface de ligne de commande pour la rétrogradation.
>
> Consultez le site Product Matrix pour plus d'informations sur le cycle de vie des versions de NetScaler.
>
> Il est recommandé de passer à une version majeure à la fois.
>
> Par exemple, si l'appliance NetScaler utilise la version 13.1 et que vous souhaitez passer à la version 12.1, vous devez d'abord rétrograder l'appliance vers la version 13.0, puis vers la version 12.1.

Suivez les étapes ci-dessous pour rétrograder une appliance NetScaler exécutant la version 13.1 vers une version antérieure à l'aide de l'interface graphique.

1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler, par exemple. `http://10.102.29.50`
2. Dans Nom d'utilisateur et mot de passe, tapez les informations d'identification de l'administrateur, puis cliquez **sur Connexion**.
3. Dans l'interface graphique, cliquez sur **Mise à niveau du système**.



4. Dans le menu **Choisir un fichier**, choisissez l'option appropriée : **Local** ou **Appliance**. Si vous souhaitez utiliser l'option Appliance, le microprogramme doit d'abord être téléchargé sur NetScaler. Vous pouvez utiliser n'importe quelle méthode de transfert de fichiers, telle que WinSCP, pour télécharger le microprogramme NetScaler sur l'appliance.
5. Sélectionnez le fichier approprié et cliquez sur **Mettre à niveau**.
6. Suivez les instructions pour rétrograder le logiciel.
7. Lorsque vous y êtes invité, sélectionnez **Redémarrer**.

Après la mise à niveau, fermez toutes les instances de navigateur et effacez le cache de votre ordinateur avant d'accéder à la solution matérielle-logicielle.

Ressources connexes

Les ressources suivantes fournissent des informations connexes sur la mise à niveau ou la rétrogradation d'une appliance NetScaler :

- Tutoriel vidéo - Comment mettre à niveau votre NetScalerà l'aide de l'interface de ligne de commande

Mise à niveau d'une paire haute disponibilité

July 31, 2023

L'une des exigences des appliances NetScaler dans une configuration haute disponibilité est d'installer la même version du logiciel NetScaler sur les deux appliances de la configuration. Par conséquent, lorsque le logiciel d'une appliance est mis à niveau, assurez-vous que le logiciel est mis à niveau sur les deux appliances.

Vous pouvez suivre la même procédure pour mettre à niveau une appliance autonome ou chaque appliance dans une paire haute disponibilité, bien que des considérations supplémentaires s'appliquent à la mise à niveau d'une paire haute disponibilité.

Avant de commencer la mise à niveau du microprogramme NetScaler sur une paire HA, lisez les prérequis mentionnés dans la section Avant de commencer. En outre, vous devez considérer quelques points spécifiques à l'HA.

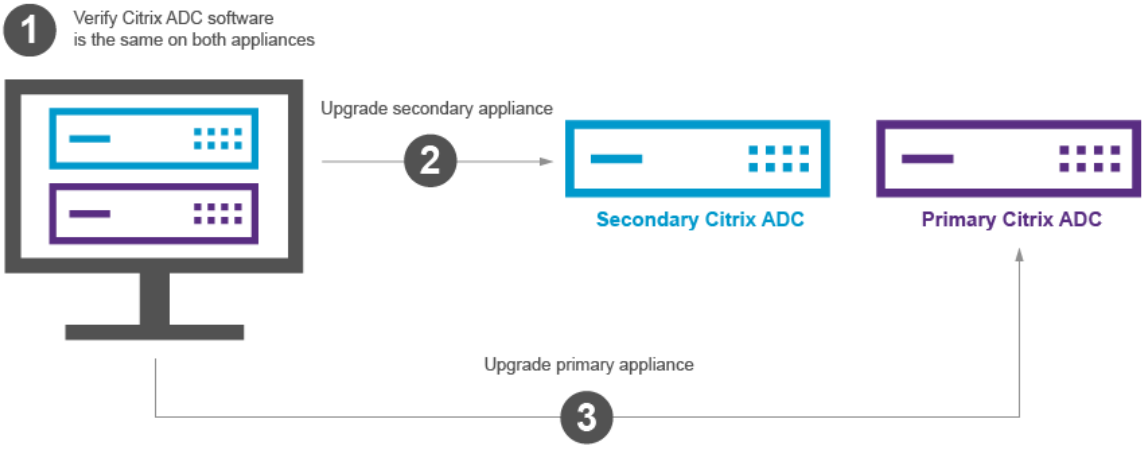
Points à noter

> - **IMPORTANT :**
>
> Il est important que les modifications de mise à niveau et vos personnalisations soient appliquées à une appliance NetScaler mise à niveau. Par conséquent, si vous avez des fichiers de configuration personnalisés dans le répertoire `/etc`, consultez Considérations relatives à la mise à niveau pour les fichiers de configuration personnalisés avant de procéder à la mise à niveau.

- Mettez d'abord à niveau le nœud secondaire, puis le nœud principal. La mise à niveau du logiciel sur l'appliance secondaire avant l'appliance principale garantit que le processus de mise à niveau est terminé sans aucun problème.
- Si les deux nœuds d'une configuration haute disponibilité (HA) exécutent différentes versions du logiciel NetScaler, les fonctionnalités suivantes sont désactivées :
  - Synchronisation de configuration HA
  - Propagation des commandes HA
  - Synchronisation HA des informations sur les services d'états
  - Mise en miroir de connexion (basculement de connexion) des sessions
  - Synchronisation HA des informations sur les sessions de persistance
- Les fonctionnalités mentionnées ci-dessus sont désactivées si les deux nœuds d'une configuration haute disponibilité (HA) exécutent des versions différentes de la même version mais que les deux versions ont des versions HA internes différentes. Les fonctionnalités mentionnées ci-dessus fonctionnent correctement si les deux nœuds d'une configuration haute disponibilité (HA) exécutent des versions différentes de la même version mais que les deux versions ont les mêmes versions HA internes.

  Reportez-vous à la section Nouvelle version HA interne dans les versions NetScaler pour vérifier si la version HA interne a changé dans une version NetScaler.
- La synchronisation des fichiers en mode Tout de la commande Synchroniser les fichiers HA fonctionne correctement si les deux nœuds d'une configuration HA exécutent différentes versions du logiciel NetScaler ou si les deux nœuds exécutent des versions différentes de la même version. Pour plus d'informations, consultez Synchronisation des fichiers de configuration dans la configuration haute disponibilité.

Figurine. Mise à niveau d'une paire haute disponibilité



Vous pouvez effectuer la mise à niveau à l'aide de la CLI ou de l'interface graphique NetScaler.

Nouvelle version HA interne dans les versions de NetScaler

Le tableau suivant répertorie les versions de NetScaler dotées d'une nouvelle version HA interne :

Version 13.1	Version 13	Version 12.1
Build 33.54	Build 87.9	Build 65.21
Build 30.52	Build 86.17	Build 62.27
Build 27.59	Build 85.19	Build 61.19
Build 24.38	Build 84.11	Build 60.19
Build 21.50	Build 82.45	Build 59.16
Build 17.42	Build 79.64	Build 58.15
Build 12.51	Build 76.31	Build 57.18
Build 9.60	Build 71.44	Build 56.22
Build 4.44	Build 67.43	Build 55.24
	Build 64.35	Build 50.31
	Build 61.48	Build 49.37
	Build 58.32	
	Build 52.24	
	Build 41.28	

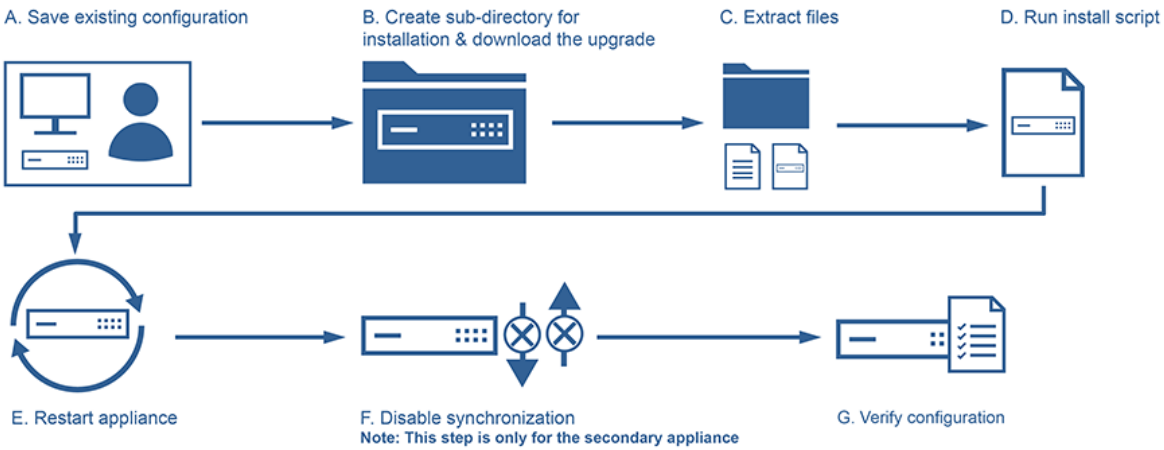
Mettre à niveau une paire haute disponibilité à l'aide de la CLI

Le processus de mise à niveau comprend les étapes suivantes :

1. Mettre à niveau le logiciel sur l'appliance secondaire
2. Mettre à niveau le logiciel sur l'appliance principale
3. Synchroniser l'appliance secondaire

Mettre à niveau le logiciel sur l'appliance secondaire

L'illustration suivante illustre la procédure de mise à niveau du logiciel sur l'appliance secondaire :



1. Connectez-vous à l'appliance secondaire à l'aide d'un utilitaire SSH, tel que PuTTY et en spécifiant l'adresse IP NetScaler (NSIP). Utilisez les `nsroot` informations d'identification pour vous connecter à l'appliance.
2. Dans l'interface de ligne de commande de l'appliance, tapez la commande suivante pour enregistrer la configuration existante :

```
save config
<!--NeedCopy-->
```

3. Passez à l'invite du shell :

```
shell
<!--NeedCopy-->
```

4. Exécutez la commande suivante pour passer au répertoire d'installation par défaut :

```
cd /var/nsinstall
<!--NeedCopy-->
```


5. Exécutez la commande suivante pour créer un sous-répertoire temporaire dans le répertoire `nsinstall`:

```
mkdir x_xnsinstall
<!--NeedCopy-->
```

> **Remarque :**
>
> Le texte x_x est utilisé pour nommer la version de NetScaler pour les configurations futures. Par exemple, le répertoire des fichiers d'installation de NetScaler 13.1 s'appelle 13_1nsinstall. N'utilisez pas de point (.) dans le nom du dossier, cela peut entraîner l'échec des mises à niveau.

6. Accédez au répertoire **x_xnsinstall** .
7. Téléchargez le package d'installation et la documentation nécessaires, tels que « ns-x.0-xx.x-doc.tgz », dans le répertoire temporaire créé à l'étape 4.

> **Remarque :**
>
> Certaines versions n'ont pas de bundle de documentation car il n'est pas nécessaire de l'installer.
>
> Cliquez sur l'onglet **Documentation** de l'interface graphique pour accéder à la documentation.

8. Avant d'exécuter le script d'installation, les fichiers doivent être extraits et placés sur l'appliance. Utilisez la commande suivante pour décompresser le bundle téléchargé à partir du site Web Citrix : `tar -zxvf ns-x.0-xx.x-doc.tgz`. Vous trouverez ci-dessous une brève explication des paramètres utilisés.
   - x - Extraire les fichiers.
   - v - Affiche les noms de fichiers tels qu'ils sont extraits un par un.
   - z - Le fichier est un fichier `gzipped`.
   - f - Utilisez l'archive tar suivante pour l'opération.
9. Exécutez la commande suivante pour installer le logiciel téléchargé :

```
./installns
<!--NeedCopy-->
```

> **Remarque :**
>
> Si l'appliance ne dispose pas de suffisamment d'espace disque pour installer les nouveaux fichiers du noyau, le processus d'installation effectue un nettoyage automatique du lecteur flash.

10. Une fois le processus d'installation terminé, le processus invite à redémarrer l'appliance. Appuyez sur `y` pour redémarrer l'appareil.
11. Connectez-vous à l'interface de ligne de commande de l'appliance à l'aide des informations d'identification `nsroot`.
12. Exécutez la commande suivante depuis pour afficher l'état de l'appliance NetScaler. La sortie de la commande précédente doit indiquer que l'appliance est un nœud secondaire et que la synchronisation est désactivée.

```
show ha node
<!--NeedCopy-->
```

13. Exécutez la commande suivante pour effectuer un basculement forcé et une prise de contrôle en tant qu'appliance principale :

```
force failover
<!--NeedCopy-->
```

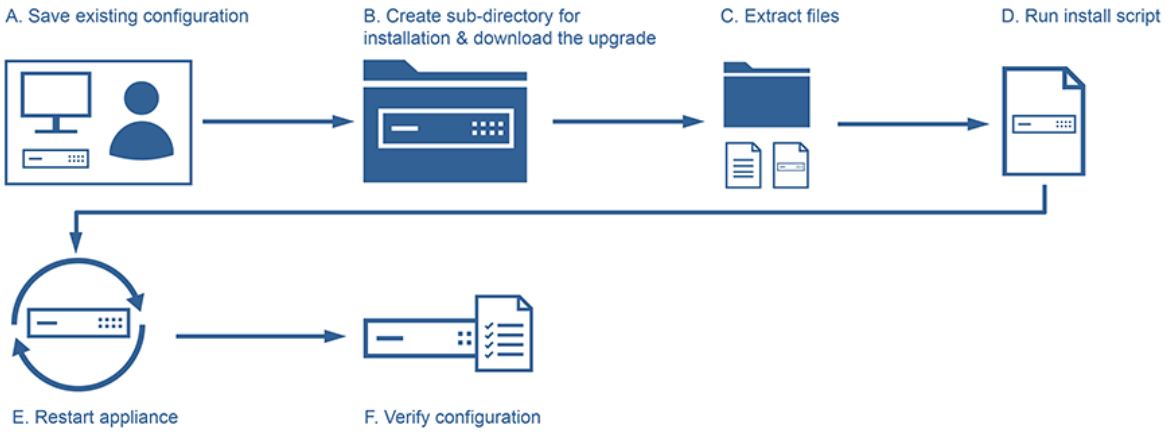
14. Vérifiez que le matériel est désormais un appareil principal.

    Voici un exemple de configuration dans le nouveau nœud principal.

```
login: nsroot
Password: nsroot
Last login: Monday Apr  17 08:37:26 2017 from 10.102.29.9
Done
show ha node
        2 nodes:
1)      Node ID:      0
        IP:        10.0.4.2
        Node State: UP
        Master State: Primary
        ...
        Sync State: AUTO DISABLED
        Propagation: AUTO DISABLED
        ...
Done
<!--NeedCopy-->
```

Mettre à niveau le logiciel sur l'appliance principale

L'illustration suivante illustre la procédure de mise à niveau du logiciel sur l'appliance principale :



> **Remarque :**
>
> Après avoir terminé la procédure « Mettre à niveau le logiciel sur l'appareil secondaire », l'appareil principal d'origine est désormais un appareil secondaire.

1. Ouvrez une session sur le dispositif secondaire à l'aide d'un utilitaire SSH, tel que PuTTY. Utilisez les `nsroot` informations d'identification pour vous connecter à l'appliance. Suivez les mêmes étapes que celles mentionnées dans la section ci-dessus pour terminer le processus d'installation. Nous devons suivre les mêmes étapes que celles mentionnées aux étapes 2 à 9 de la section précédente (Mise à niveau du logiciel de l'appareil secondaire).
2. Une fois le processus d'installation terminé, le processus invite à redémarrer l'appliance. Appuyez sur `y` pour redémarrer l'appareil.
3. Connectez-vous à l'interface de ligne de commande de l'appliance à l'aide des informations d'identification `nsroot`.
4. Exécutez la commande suivante pour afficher l'état du dispositif NetScaler. La sortie de la commande précédente doit indiquer que l'appliance est un nœud secondaire et que l'état de l'état du nœud est marqué comme UP.

```
1 show ha node
2 <!--NeedCopy-->
```

5. Exécutez la commande suivante pour effectuer un basculement forcé afin de vous assurer que l'appliance est un dispositif principal :

```
1 force failover
2 <!--NeedCopy-->
```

6. Vérifiez que le matériel est un appareil principal.

   Voici un exemple de configuration du nouveau nœud principal et du nouveau nœud secondaire.


```
show ha node
    Node ID:      0
    IP:   10.0.4.11
    Node State: UP
    Master State: Primary
    ...
    ...
    INC State: DISABLED
    Sync State: ENABLED
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    ...
    ...
    Local node information
    Critical Interfaces: 1/1
Done

Show ha node
    Node ID:      0
    IP:   10.0.4.2
    Node State: UP
    Master State: Secondary
    ..
    ..
    INC State: DISABLED
    Sync State: SUCCESS
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    . .
    . .
    Local node information:
    Critical Interfaces: 1/1
Done
<!--NeedCopy-->
```

Mettre à niveau une paire haute disponibilité à l'aide de l'interface graphique

Suivez ces étapes pour mettre à niveau une paire NetScaler dans une configuration haute disponibilité, à l'aide de l'interface graphique ADC. Prenons l'exemple d'une configuration à haute disponibilité

des appliances NetScaler CITRIX-ADC-A (principal) et CITRIX-ADC-B (secondaire).

1. **Mettez à niveau le nœud secondaire**. Connectez-vous à l'interface graphique du nœud secondaire à l'aide des informations d'identification de l'administrateur et effectuez la mise à niveau comme décrit dans Mettre à niveau une appliance autonome NetScaler à l'aide de l'interface graphique.
2. **Forcer le basculement**. Effectuez un basculement forcé sur le nœud secondaire à l'aide de l'interface graphique, comme décrit à la section Forcer un nœud à basculer.

   Après l'opération de basculement, le nœud secondaire prend le relais en tant que principal et le nœud principal devient le nouveau nœud secondaire. Après l'opération de basculement dans l'exemple de configuration HA :

   - CITRIX-ADC-B devient le nouveau primaire
   - CITRIX-ADC-A devient le nouveau secondaire
3. **Mettez à niveau le nœud principal d'origine (nouveau nœud secondaire)**. Connectez-vous à la nouvelle interface graphique du nœud secondaire (CITRIX-ADC-A) et effectuez la mise à niveau comme décrit dans Mettre à niveau une appliance autonome NetScaler à l'aide de l'interface graphique.
4. **Forcer le basculement**. Effectuez un basculement forcé sur le nouveau nœud secondaire (CITRIX-ADC-A) à l'aide de l'interface graphique, comme décrit dans la section Forcer un nœud à basculer.

   Après cette deuxième opération de basculement, l'état des deux nœuds revient au même état qu'avant le démarrage de l'opération de mise à niveau HA. Après l'opération de basculement dans l'exemple de configuration HA :

   - CITRIX-ADC-A devient primaire
   - CITRIX-ADC-B devient secondaire
5. **Vérifiez le processus de mise à niveau**. Ouvrez une session sur l'interface graphique des deux nœuds. Accédez à **Système > Haute disponibilité**, sur la page de détails, vérifiez l'état HA des deux nœuds. Vérifiez également les détails de la version mise à niveau affichés dans le volet supérieur de l'interface graphique.

Regardez cette vidéo pour découvrir comment mettre à niveau une configuration de haute disponibilité à l'aide de l'interface graphique.

Prise en charge de la mise à niveau logicielle en service pour une haute disponibilité afin d'effectuer une mise

May 5, 2023

Au cours d'un processus de mise à niveau régulier dans une configuration haute disponibilité, à un moment donné, les deux nœuds exécutent des versions logicielles différentes. Ces deux versions peuvent avoir des numéros de version internes de haute disponibilité identiques ou différents.

Si les deux versions ont des numéros de version haute disponibilité différents, le basculement de connexion (même s'il est activé) pour les connexions de données existantes n'est pas pris en charge. En d'autres termes, toutes les connexions de données existantes sont perdues, ce qui entraîne des temps d'arrêt.

Pour résoudre ce problème, la mise à niveau du logiciel de service (ISSU) peut être utilisée pour les configurations haute disponibilité. ISSU introduit une fonctionnalité de migration, qui remplace l'étape d'opération de basculement forcé dans le processus de mise à niveau. La fonctionnalité de migration s'occupe de respecter les connexions existantes et inclut l'opération de basculement forcé.

Après l'exécution d'une opération de migration, le nouveau nœud principal reçoit toujours le trafic (demande et réponse) lié aux connexions existantes mais les dirige vers l'ancien nœud principal. L'ancien nœud principal traite le trafic de données, puis les envoie directement à la destination.

Comment fonctionne l'ISSU amélioré

Le processus de mise à niveau standard dans une configuration haute disponibilité comprend les étapes suivantes :

1. **Mettez à niveau le nœud secondaire**. Cette étape inclut la mise à niveau logicielle du nœud secondaire et le redémarrage du nœud.
2. **Basculement forcé**. L'exécution du basculement forcé transforme le nœud secondaire mis à niveau en nœud principal et le nœud principal en nœud secondaire.
3. **Mettez à niveau le nouveau nœud secondaire**. Cette étape inclut la mise à niveau logicielle du nouveau nœud secondaire et le redémarrage du nœud.

Au cours de la période entre les étapes 1 et 3, les deux nœuds exécutent des versions logicielles différentes. Ces deux versions peuvent avoir des versions internes haute disponibilité identiques ou différentes.

Si les deux versions ont des numéros de version haute disponibilité différents, le basculement de connexion (même s'il est activé) pour les connexions de données existantes n'est pas pris en charge. En d'autres termes, toutes les connexions de données existantes sont perdues, ce qui entraîne des temps d'arrêt.

Le processus de mise à niveau ISSU dans une configuration haute disponibilité comprend les étapes suivantes :

1. **Mettez à niveau le nœud secondaire**. Cette étape inclut la mise à niveau logicielle du nœud secondaire et le redémarrage du nœud.

2. **Opération de migration ISSU**. L'étape inclut l'opération de basculement forcé et prend en charge les connexions existantes. Après avoir effectué l'opération de migration, le nouveau nœud principal reçoit toujours le trafic (demande et réponse) lié aux connexions existantes, mais les dirige vers l'ancien nœud principal via le VLAN SYNC configuré dans le tunnel GRE. L'ancien nœud principal traite le trafic de données, puis les envoie directement à la destination. L'opération de migration ISSU est terminée lorsque toutes les connexions existantes sont fermées.
3. **Mettez à niveau le nouveau nœud secondaire**. Cette étape inclut la mise à niveau logicielle du nouveau nœud secondaire et le redémarrage du nœud.

Avant de commencer

Avant de commencer à exécuter le processus ISSU dans une configuration à haute disponibilité, passez en revue les prérequis, les limites et les points à noter suivants :

- Assurez-vous que `SYNC VLAN` est configuré sur les deux nœuds de la configuration haute disponibilité. Pour plus d'informations, voir Restriction du trafic de synchronisation haute disponibilité à un VLAN.
- ISSU n'est pas pris en charge sur le cloud Microsoft Azure car Microsoft Azure ne prend pas en charge le tunneling GRE.
- La propagation et la synchronisation de la configuration haute disponibilité ne fonctionnent pas pendant l'ISSU.
- ISSU n'est pas pris en charge pour la configuration haute disponibilité IPv6.
- L'ISSU n'est pas pris en charge pour les sessions suivantes :
  - Cadres Jumbo
  - Sessions IPv6
  - NAT à grande échelle (LSN)
- Dans une configuration HA en mode INC, l'opération de migration ISSU migre uniquement les connexions côté client. La migration des connexions côté serveur n'est pas requise car les deux nœuds HA ont des configurations SNIP indépendantes.

Étapes de configuration

ISSU inclut une fonctionnalité de migration, qui remplace l'opération de basculement forcé dans le processus de mise à niveau standard d'une configuration haute disponibilité. La fonctionnalité de migration s'occupe de respecter les connexions existantes et inclut l'opération de basculement forcé.

Au cours du processus ISSU d'une configuration haute disponibilité, vous exécutez l'opération de migration juste après la mise à niveau du nœud secondaire. Vous pouvez effectuer l'opération de migration à partir de l'un des deux nœuds.

Procédure CLI

Pour effectuer l'opération de migration haute disponibilité à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
start ns migration
<!--NeedCopy-->
```

Procédure GUI

Pour effectuer l'opération de migration haute disponibilité à l'aide de l'interface graphique :

Accédez à **Système**, cliquez sur l'onglet **Informations système**, sur **l'onglet Migration**, puis sur **Démarrer la migration**.

Afficher les statistiques ISSU

Vous pouvez consulter les statistiques ISSU pour surveiller le processus ISSU actuel dans une configuration haute disponibilité. Les statistiques ISSU affichent les informations suivantes :

- État actuel de l'opération de migration ISSU
- Heure de début de l'opération de migration ISSU
- Heure de fin de l'opération de migration ISSU
- Heure de début de l'opération de restauration d'ISSU
- Nombre total de connexions traitées dans le cadre de l'opération de migration ISSU
- Nombre de connexions restantes en cours de traitement dans le cadre de l'opération de migration ISSU

Vous pouvez afficher les statistiques ISSU sur l'un des nœuds haute disponibilité à l'aide de l'interface de ligne de commande ou de l'interface graphique

Procédure CLI

Pour afficher les statistiques ISSU à l'aide de la CLI :

À l'invite de commandes, tapez :


```
show ns migration
<!--NeedCopy-->
```

Procédure GUI

Pour afficher les statistiques ISSU à l'aide de l'interface graphique :

Accédez à **Système**, cliquez sur l'onglet **Informations système**, sur l'**onglet Migration**, puis cliquez sur **Cliquez pour afficher les détails de la migration**.

Afficher les statistiques ISSU - la liste des connexions existantes traitées par l'ancien nœud principal

Vous pouvez afficher la liste des connexions existantes que l'ancien nœud principal dessert actuellement dans le cadre de l'opération de migration ISSU en utilisant l'option `dumpsession` (`Dump Session`) de l'opération `show migration`.

L'opération de migration d'exposition avec l'option `dumpsession` doit être exécutée uniquement sur le nouveau nœud principal pendant l'opération ISSU.

Procédure CLI

Pour afficher la liste des connexions existantes que l'ancien nœud principal traite actuellement à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
show ns migration  - dumpsession YES
<!--NeedCopy-->
```

```
> sh migration -dumpsession yes

Index   remote-IP-port          local-IP-port           idle-time(x 10
    ms)

1       192.0.2.10      22      192.0.2.1       15998       703
2       198.51.100.20   7375    98.51.100.2     22          687
3       203.0.113.30    5506    203.0.113.3     22          687


<!--NeedCopy-->
```


Procédure GUI

Pour afficher la liste des connexions existantes que l'ancien nœud principal est en train de traiter à l'aide de l'interface graphique :

Accédez à **Système**, cliquez sur l'onglet **Informations système**, sur **l'onglet Migration**, puis cliquez sur **Cliquez pour afficher les connexions de migration**.

Annulation du processus ISSU

Les configurations haute disponibilité (HA) prennent désormais en charge la restauration du processus ISSU (In-Service Software Upgrade). La fonction de restauration d'ISSU est utile si vous constatez que la configuration HA pendant l'opération de migration ISSU n'est pas stable ou ne fonctionne pas à un niveau optimal comme prévu.

Le rollback ISSU est applicable lorsque l'opération de migration ISSU est en cours. La restauration d'ISSU ne fonctionne pas si l'opération de migration ISSU est déjà terminée. En d'autres termes, vous devez exécuter l'opération de restauration ISSU lorsque l'opération de migration ISSU est en cours.

Le rollback ISSU fonctionne différemment en fonction de l'état de l'opération de migration ISSU lorsque l'opération de restauration ISSU est déclenchée :

- **Le basculement forcé ne s'est pas encore produit pendant l'opération de migration ISSU**. L'annulation d'ISSU arrête l'opération de migration ISSU et supprime toutes les données internes liées à la migration ISSU stockées dans les deux nœuds. Le nœud principal actuel reste le nœud principal et continue de traiter le trafic de données lié aux connexions existantes et nouvelles.
- **Un basculement forcé s'est produit pendant l'opération de migration ISSU**. Si le basculement haute disponibilité s'est produit pendant l'opération de migration ISSU, le nouveau nœud principal (par exemple N1) traite le trafic lié aux nouvelles connexions. L'ancien nœud principal (nouveau nœud secondaire, disons N2) traite le trafic lié aux anciennes connexions (connexions existantes avant l'opération de migration ISSU).

  Le rollback ISSU arrête l'opération de migration ISSU et déclenche un basculement forcé. Le nouveau nœud principal (N2) commence maintenant à traiter le trafic lié aux nouvelles connexions. Le nouveau nœud principal (N2) continue également à traiter le trafic lié aux anciennes connexions (connexions existantes établies avant l'opération de migration ISSU). En d'autres termes, les connexions existantes établies avant l'opération de migration ISSU ne sont pas perdues.

  Le nouveau nœud secondaire (N1) supprime toutes les connexions existantes (nouvelles connexions créées lors de l'opération de migration ISSU) et ne traite aucun trafic. En d'autres termes, toutes les connexions existantes qui ont été établies après le basculement forcé de l'opération de migration ISSU sont perdues à jamais.

Étapes de configuration

Vous pouvez utiliser la CLI ou l'interface graphique NetScaler pour effectuer l'opération de restauration ISSU.

Procédure CLI

Pour effectuer l'opération de restauration ISSU à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
stop ns migration
<!--NeedCopy-->
```

Procédure GUI

Pour effectuer l'opération de restauration ISSU à l'aide de l'interface graphique :

Accédez à **Système**, cliquez sur l'onglet **Informations système**, sur **l'onglet Migration**, puis sur **Arrêter la migration**.

Interruptions SNMP pour le processus de mise à niveau logicielle en service

Le processus de mise à niveau logicielle en service (ISSU) pour une configuration haute disponibilité prend en charge les messages d'interruption SNMP suivants au début et à la fin de l'opération de migration ISSU.

Interruption SNMP	Description
migrationStarted	Cette interruption SNMP est générée et envoyée aux écouteurs d'interruption SNMP configurés lorsque l'opération de migration ISSU démarre.
migrationComplete	Cette interruption SNMP est générée et envoyée aux écouteurs d'interruption SNMP configurés lorsque l'opération de migration ISSU est terminée.

Le nœud principal (avant le début du processus ISSU) génère toujours ces deux interruptions SNMP et les envoie aux écouteurs d'interruption SNMP configurés.

Aucune alarme SNMP n'est associée aux interruptions SNMP ISSU. En d'autres termes, ces déroute-

ments sont générés quelle que soit l'alarme SNMP. Il suffit de configurer les écouteurs SNMP d'interruption.

Pour plus d'informations sur la configuration des écouteurs d' interruptions SNMP, consultez la section Interruptions SNMPsur NetScaler.

Rétrograder une paire haute disponibilité

May 5, 2023

Vous pouvez passer à n'importe quelle version d'une paire haute disponibilité à l'aide de l'interface de ligne de commande. L'interface graphique ne prend pas en charge le processus de rétrogradation.

Pour rétrograder le logiciel système d'une paire NetScaler dans une paire haute disponibilité, vous devez d'abord rétrograder le logiciel sur le nœud secondaire, puis sur le nœud principal. Pour obtenir des instructions sur la rétrogradation de chaque nœud séparément, consultez la section Rétrograder une appliance autonome NetScaler.

> **Important**
>
> Une perte de configuration peut survenir lors d'une rétrogradation. Vous devez comparer les configurations avant et après la rétrogradation, puis saisir manuellement les entrées manquantes.

Résolution des problèmes liés aux processus d'installation, de mise à niveau et de rétrogradation

May 8, 2023

Si la solution matérielle-logicielle ne fonctionne pas comme prévu une fois le processus d'installation, de mise à niveau ou de mise à niveau antérieure terminé, la première chose à faire est de rechercher les causes les plus courantes du problème.

Ressources pour le dépannage

Pour de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème lié à l'installation, à la mise à niveau ou à la rétrogradation d'un NetScaler :

- Les fichiers de configuration de la solution matérielle-logicielle. Dans le cas d'une paire haute disponibilité, les fichiers de configuration des deux solutions matérielles-logicielles.
- Les fichiers suivants de la ou des solutions matérielle-logicielles :
  - Les fichiers newnslog pertinents.

  - Le fichier ns.log.
  - Le fichier de messages.
- Un diagramme de topologie du réseau.

Problèmes et résolutions

Voici les problèmes d'installation, de mise à niveau et de rétrogradation les plus courants, ainsi que des conseils pour les résoudre :

1. **Problème**

   La mise à niveau d'une appliance NetScaler MPX échoue en raison d'une incompatibilité matérielle et logicielle.

   Résolution

   Consultez la matrice de compatibilité matérielle/logicielle NetScaler MPX et vérifiez si la version logicielle est prise en charge sur le matériel NetScaler MPX.

2. **Problème**

   La mise à niveau d'une appliance NetScaler VPX échoue en raison d'une incompatibilité entre l'appliance NetScaler VPX et l'hyperviseur.

   Résolution

   Consultez la matrice de compatibilité de l'appliance NetScaler VPX et de l'hyperviseur et vérifiez si le modèle d'appliance NetScaler VPX est pris en charge sur l'hyperviseur.

3. **Problème**

   La mise à niveau d'une appliance NetScaler échoue en raison d'erreurs matérielles.

   Résolution

   Validez l'intégrité de l'appliance NetScaler. Si vous possédez une appliance matérielle NetScaler, Citrix recommande de l'exécuter `fsck` pour exécuter une vérification du disque et valider l'intégrité du disque dur NetScaler.

   Pour plus d'informations, consultez Comment vérifier l'intégrité du système de fichiers d'une appliance NetScaler.

4. **Problème**

   Mise à niveau d'une appliance NetScaler à l'aide des stalles de l'interface graphique.

   Résolution

   Actualisez le navigateur pour vérifier si la mise à niveau progresse ou non.

5. **Problème**

   La mise à niveau d'une appliance NetScaler échoue en raison du manque d'espace dans le répertoire /var

   Résolution

   Libérez de l'espace sur le répertoire /var. Pour plus d'informations, reportez-vous à la section Comment libérer de l'espace dans le répertoire /var.

6. **Problème**

   Le NetScaler n'est pas accessible après la rétrogradation du logiciel

   Cause

   Au cours du processus de mise à niveau du logiciel, si le fichier de configuration de la version et de la version existantes ne correspond pas au fichier de configuration de la version et de la version antérieures, l'appliance ne peut pas charger la configuration et l'adresse IP par défaut est attribuée à la solution matérielle-logicielle.

   Résolution

   - Vérifiez que la solution matérielle-logicielle est accessible depuis la console.
   - Vérifiez l'adresse NSIP et les routes sur la solution matérielle-logicielle.
     - Si l'adresse IP est passée à l'adresse IP 192.168.100.1 par défaut, modifiez l'adresse IP si nécessaire.
     - Vérifiez que la solution matérielle-logicielle est accessible.

7. **Problème**

   Au cours d'une mise à niveau, si j'exécute la commande de synchronisation, le message suivant apparaît :

   La commande a échoué sur le nœud secondaire, mais a réussi sur le nœud principal.

   Résolution

   N'exécutez aucune commande dépendante (set /unset /bind /unbind) lorsque la synchronisation haute disponibilité (HA) est en cours.

8. **Problème**

   Au cours d'un processus de mise à niveau, le trafic ne passe pas par le nouveau nœud principal lorsque vous exécutez la commande de basculement forcé.

   Résolution

   - Recherchez les problèmes liés à la topologie du réseau et aux configurations des commutateurs.
   - Exécutez la commande set L2Param -garpreply ENABLED pour activer la réponse GARP.

- Essayez d'utiliser un MAC virtuel s'il n'est pas déjà utilisé.
- Exécutez la commande sendarp —a depuis le nœud principal.

9. **Problème**

   Après la mise à niveau ou la rétrogradation d'une appliance NetScaler, la connexion à l'appliance échoue via SSH.

   Résolution

   Effectuez les opérations suivantes dans l'appliance NetScaler :

   - Supprimez les clés d'hôte anciennes ou non sécurisées à l'adresse `/nsconfig/ssh/ssh_host_*`.
   - Consultez la configuration SSHD personnalisée à l'adresse `/nsconfig/sshd_config` et vérifiez si elle est toujours pertinente et compatible. Renommez ou supprimez la configuration SSHD personnalisée en conséquence.
   - Redémarrage à froid de l'appliance NetScaler

10. **Problème**

    Dans une paire HA, après avoir exécuté la commande Forcer le basculement HA, les périphériques continuent de redémarrer. Le périphérique secondaire n'apparaît pas après une mise à niveau.

    Résolution

    Vérifiez si le répertoire /var est plein. Si c'est le cas, supprimez les anciens fichiers d'installation. Exécutez la commande df —h pour afficher l'espace disque disponible.

11. **Problème**

    Après la mise à niveau d'une paire HA, l'un des nœuds est répertorié comme état UNKNOWN.

    Résolution

    - Vérifiez si les deux nœuds exécutent la même version. Si les versions ne sont pas identiques et que les nœuds HA ne correspondent pas à la version, certains champs sont affichés comme UNKNOWN lorsque vous exécutez la commande show ha node.
    - Vérifiez si la solution matérielle-logicielle secondaire est accessible.

12. **Problème**

    Après la mise à niveau de NetScaler, l'interface indique que la plupart des serveurs et services virtuels d'équilibrage de charge sont hors service.

    Résolution

    Vérifiez que l'adresse SNIP est active sur la solution matérielle-logicielle secondaire. Tapez également la commande show service pour voir si le service est en cours d'exécution.

13. **Problème**

    Après avoir effectué une mise à niveau, tous les serveurs virtuels sont en panne sur le dispositif secondaire.

    Résolution

    Activez l'état HA et la synchronisation HA en exécutant les commandes suivantes :

    - définir le nœud hastate enable
    - activer le mode hasync du nœud

    La désactivation de l'HA n'est pas recommandée.

14. **Problème**

    Après avoir effectué une rétrogradation, NetScaler ne démarre pas correctement.

    Résolution

    Vérifiez si la licence correcte a été installée.

15. **Problème**

    Dans une paire HA, certaines fonctionnalités ne sont pas synchronisées après une mise à niveau.

    Résolution

    Exécutez la commande sync ha file misc pour synchroniser les fichiers de configuration du nœud principal vers le nœud secondaire.

16. **Problème**

    Au cours du redémarrage, le message d'erreur suivant s'affiche :

    Une ou plusieurs commandes dans ns.conf ont échoué. Que dois-je faire ?

    Résolution

    Assurez-vous qu'aucune commande du fichier ns.conf ne dépasse la limite de 255 octets. Dans les commandes qui créent des stratégies trop longues pour la limite de 255 octets, vous pouvez utiliser des jeux de modèles pour raccourcir les stratégies.

    Exemple :

    ```
    1 add cs policy p11 -rule 'HTTP.REQ.URL.ENDSWITH_ANY("
        ctx_file_extensions")'
    2 Done
    3 <!--NeedCopy-->
    ```

    ctx_file_extensions est un jeu de patset par défaut qui couvre un grand nombre d'extensions. En plus des jeux de motifs par défaut, vous pouvez créer des jeux de motifs définis par l'utilisateur. Ajoutez un patset en exécutant la commande suivante :


```
add patset <name>
<!--NeedCopy-->
```

Remarque : Les patsets sont pris en charge uniquement dans la version 9.3 ou ultérieure.

17. **Problème**

    Lors de la mise à niveau d'une appliance NetScaler VPX, on me demande de libérer de l'espace dans /var. Quels fichiers dois-je supprimer ?

    Résolution

    Supprimez les anciens fichiers d'installation du répertoire /var/tmp/. Supprimez également les fichiers indésirables de /flash.

18. **Problème**

    Il n'y a pas de connectivité à l'interface utilisateur graphique (GUI) lorsque vous exécutez la commande forcer le basculement HA sur le dispositif secondaire.

    Résolution

    Ouvrez une session sur l'appliance secondaire à l'aide de l'interface de ligne de commande et activez l'accès à l'interface graphique en exécutant la <IP> commande set ns ip \ -gui enabled.

19. **Problème**

    Après avoir effectué une mise à niveau, et lorsque je clique sur un lien de l'interface graphique qui doit charger une applet Java (Assistant de mise à niveau ou assistant de licence), le message d'erreur suivant apparaît : la version de l' **interface graphique ne correspond pas à la version du noyau. Fermez cette instance, videz le cache du plug-in Java et rouvrez-la**.

    Résolution

    - Connectez-vous à NetScaler à l'aide de l'interface graphique.
    - Accédez à NetScaler Gateway > Paramètres généraux.
    - Cliquez sur Modifier les paramètres globaux sous Paramètres.
    - Dans le volet d'informations, sous Expérience client, sélectionnez Par défaut dans la liste des thèmes de l'interface utilisateur.
    - Cliquez sur OK.

20. **Problème**

    Si la mise à niveau d'une appliance NetScaler échoue pour une raison quelconque, comment restaurer l'appliance à l'aide des fichiers sauvegardés ?

    Résolution

Si la mise à niveau échoue, restaurez l'appliance vers la version précédente de l'appliance NetScaler à l'aide des fichiers sauvegardés. Pour plus d'informations, consultez la section Sauvegarde et restauration d'un dispositif NetScaler.

Pour plus d'informations sur la sauvegarde et la restauration d'une configuration de cluster NetScaler, consultez la section Sauvegarde et restauration d'une configuration de cluster.

21. **Problème**

    Si des licences sont manquantes après l'échec de la mise à niveau d'une appliance NetScaler, comment résoudre le problème ?

    Résolution

    Si une licence est manquante ou si vous souhaitez réallouer les licences, reportez-vous à la rubrique Présentation des licencesci-dessous.

> **Remarque**
>
> Ces étapes de dépannage s'appliquent également aux problèmes de perte de configuration lors de la rétrogradation du logiciel sur plusieurs versions.
>
> Pour tout autre problème, consultez les notes de mise à jour, les articles du centre de connaissances et les FAQ.

FAQ

May 5, 2023

Pour obtenir des réponses aux questions que vous pouvez vous poser concernant la mise à niveau du microprogramme NetScaler, consultez les FAQ sur l' installation, la mise à niveau et la rétrogradation .

Commandes, paramètres et OID SNMP nouveaux et obsolètes

May 5, 2023

Cette section répertorie les commandes, paramètres et OID SNMP nouveaux et obsolètes.

Nouvelles commandes

Le tableau suivant répertorie les nouvelles commandes de la version 13.1.

Groupe de commande	Commande
Cloud	Statistiques du cloud

Nouveaux paramètres

Groupe de commande	Commandes et paramètres

Pare-feu d'application	`add appfw profile [-clientIpExpression <expression>];`
	`set appfw profile [-clientIpExpression <expression>];`
	`show appfw profile [-clientIpExpression <expression>]`

Bot	`add bot profile [-verboseLogLevel ( NONE | HTTP_FULL_HEADER )];`
	`set bot profile [-verboseLogLevel ( NONE | HTTP_FULL_HEADER )];`
	`show bot profile [verbose Log Level ];`
	`set cloud ngsparameter [-csvserverTicketingDecouple ( YES | NO )];`
	`show cloud ngsparameter [-csvserverTicketingDecouple]`

GSLB	`set gslb parameter [-GSLBSyncSaveConfigCommand ( ENABLED | DISABLED )];` `show gslb parameter [GSLBSyncSaveConfigCommand]`
NS	`set ns tcpParam [-delinkClientServerOnRST ( ENABLED | DISABLED )];` `show ns tcpParam [delinkClientServerOnRST]`

Groupe de commande	Commandes et paramètres
RDP	add rdp clientprofile [-rdpValidateClientIP (ENABLE | DISABLE)]; set rdp clientprofile [-rdpValidateClientIP (ENABLE | DISABLE)]; show rdp clientprofile [-rdpValidateClientIP]

Commandes déconseillées

Groupe de commande	Commandes
NS	add ns trafficDomain; rm ns trafficDomain; bind ns trafficDomain; unbind ns trafficDomain; enable ns trafficDomain; disable ns trafficDomain; show ns trafficDomain; stat ns trafficDomain
WI	add wi site; rm wi site; set wi site; bind wi site; unbind wi site; show wi site; install wi **package**; uninstall wi **package**; show wi **package**
WF	install wf **package**; uninstall wf **package**; show wf **package**; add wf site; rm wf site; set wf site; show wf site

Suppression des fonctionnalités dépréciées

Les fonctionnalités obsolètes suivantes ont été supprimées et ne sont plus configurables à partir de la version 13.1 de NetScaler.

- La fonction de filtrage (également connue sous le nom de filtrage de contenu ou CF) : actions,

stratégies et liaison.

- Les fonctionnalités SPDY, Sure Connect (SC), Priority Queuing (PQ), HTTP Denial of Service (DoS) et HTML Injection.
- Stratégies classiques pour SSL, la commutation de contenu, la redirection du cache, la compression et le pare-feu d'application.
- Les paramètres `url` et `domain` dans les stratégies de commutation de contenu.
- Expressions classiques dans les règles de persistance de l'équilibrage de charge.
- Le paramètre `pattern` dans les actions de réécriture.
- Le paramètre `bypassSafetyCheck` dans les actions de réécriture.
- `SYS.EVAL_CLASSIC_EXPR` dans les expressions avancées.
- L'entité `patclass` de configuration.
- La valeur `HTTP.REQ.BODY` sans argument dans les expressions avancées.
- Préfixes Q et S dans les expressions avancées.
- Paramètre `policyType` pour le réglage du paramètre de compression. (commande CLI `set cmp parameter`.)

Vous pouvez utiliser l'outil `nspepi` pour la conversion. Vous devez exécuter l'outil sur une appliance NetScaler version 13.0 ou 12.1.

Pour plus d'informations, consultez la FAQ sur l'obsolescence des stratégies classiques.

De plus, pour utiliser la dernière version des outils pour migrer de la configuration classique vers la configuration avancée, consultez les scripts NetScaler sur GitHub.

Nouveaux OID SNMP

Pour plus d'informations, consultez le guide SNMP OID Reference .

Solutions pour les fournisseurs de services de télécommunication

May 5, 2023

Les technologies de l'information et de la communication (TIC) visent à rapprocher l'internaute des applications et des données. Les technologies de centre de données les plus récentes ont permis de localiser l'utilisateur, les applications et les données n'importe où. Un utilisateur peut accéder aux applications et aux données depuis son bureau ou son domicile, ou depuis un lieu tel qu'un aéroport. Les applications et les données peuvent être situées dans les locaux de l'entreprise, dans un cloud public ou privé, ou sur un hôte hybride. Le résultat n'a été qu'une augmentation de la productivité, mais également une réduction des coûts de propriété et de maintenance.

Les fournisseurs de services offrent l'infrastructure de base nécessaire au transport des applications et des données de l'utilisateur sur le réseau. Étant donné que l'infrastructure de base dessert des

millions d'abonnés et une grande variété d'applications et de données, les exigences en matière d'évolutivité et de prise en charge des protocoles sont très élevées. L'infrastructure de base gère deux principaux types de trafic : le plan de données et le plan de contrôle. Chacun de ces avions a sa propre échelle et ses propres exigences en matière de support protocolaire.

Le plan de données est la partie de l'infrastructure de base qui transporte les applications et les données des utilisateurs de bout en bout, c'est-à-dire entre l'équipement de l'utilisateur final et le serveur d'applications. Le nombre d'utilisateurs accédant à des applications et à des données se chiffre en milliers de millions. Les exigences en matière de débit et d'adressage IP sont donc très élevées. Chaque utilisateur du réseau doit être identifiable de manière unique. Ce n'est qu'alors que le fournisseur de services peut contrôler le trafic, surveiller l'utilisation du réseau, fournir des services spécifiques aux utilisateurs et enregistrer correctement les informations. De nombreux appareils clients et serveurs d'applications actuels prennent en charge le protocole IPv6 de manière native. L'infrastructure de base doit non seulement prendre en charge une combinaison de clients et de serveurs IPv4 et IPv6, mais également fournir les technologies nécessaires à la communication croisée entre IPv4 et IPv6. Enfin, un fournisseur de services est évalué en fonction de la qualité du service (directement liée à l'expérience de l'utilisateur final) et de la disponibilité du service sans interruption. Le plan de données doit être suffisamment résilient pour garantir à la fois qualité et disponibilité.

L'infrastructure du plan de contrôle gère le trafic utilisateur et assure la maintenance des services commerciaux et d'exploitation du réseau. Parmi les nombreux protocoles qui s'exécutent dans ce plan, les plus importants sont Diameter, Radius et SMPP. Diameter est un protocole de base sur lequel plusieurs autres protocoles spécifiques à des fonctions ont été développés. Par exemple :

- Interface Gx entre la fonction d'application des politiques et de facturation (PCEF) et la fonction des règles de politique et de facturation (PCRF)
- Interface entre le système de recharge en ligne (OCS) et la passerelle de réseau de données par paquets Cisco (PGW) /fonction d'application des politiques et de la facturation (PCEF)

Le volume du trafic de l'avion de contrôle est directement proportionnel à l'activité des utilisateurs. Pour gérer le trafic du plan de contrôle, les fournisseurs de services utilisent plusieurs fonctionnalités ADC, telles que l'équilibrage de charge et la commutation de contenu. Ils ont besoin d'un contrôle précis du trafic des avions de contrôle, dont la complexité équivaut à celle du trafic des avions de données.

Les fournisseurs de services doivent respecter des accords de niveau de service (SLA) exigeants et sont soumis à un examen minutieux de la part des régulateurs pour vérifier leur conformité. Pour respecter les exigences tout en gérant les données et en contrôlant le trafic des avions, un fournisseur de services doit maintenir son infrastructure agile, dans les limites du budget, facilement évolutif et flexible. En tant que ADC les plus puissants et les plus avancés du marché actuel, les produits NetScaler sont parfaitement adaptés à l'environnement des fournisseurs de services.

NAT à grande échelle

May 5, 2023

> **Remarque**
>
> Cette fonctionnalité est disponible avec une licence NetScaler Advanced ou Premium.

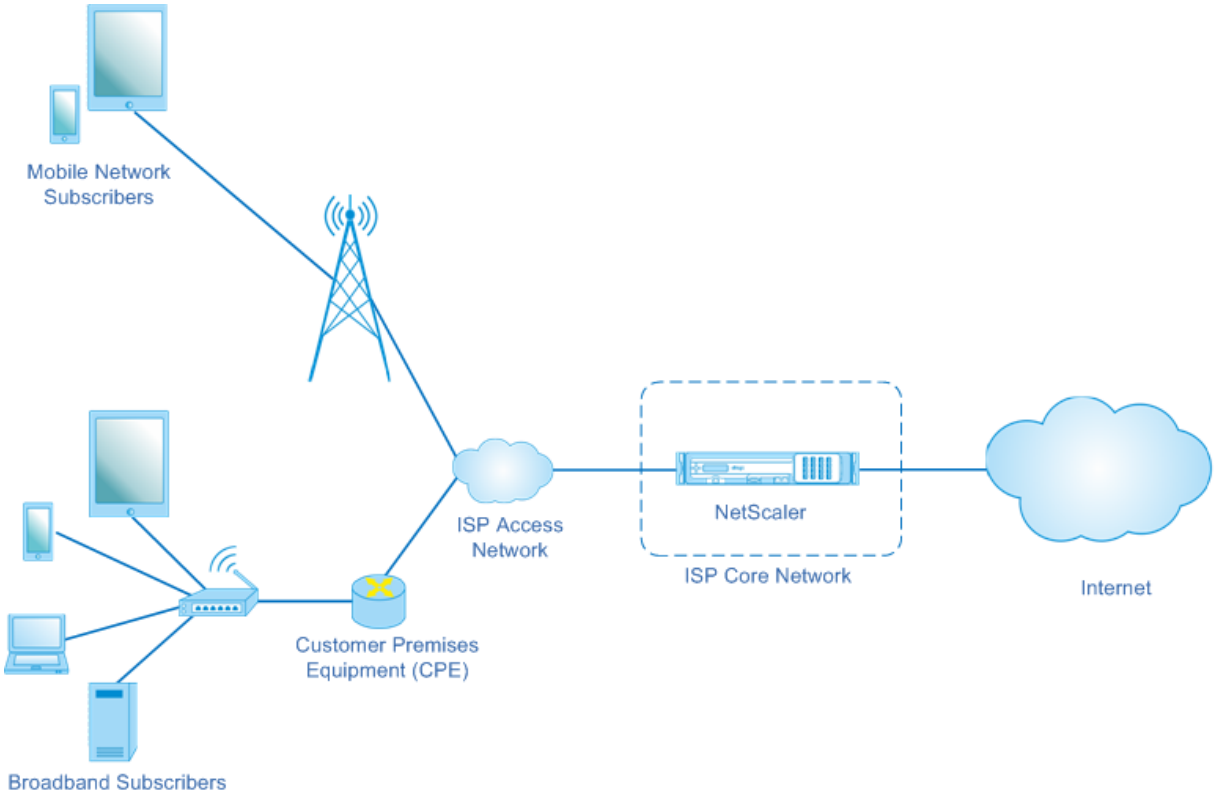
La croissance phénoménale d'Internet a entraîné une pénurie d'adresses IPv4 publiques. Le NAT à grande échelle (LSN/CGNAT) apporte une solution à ce problème en maximisant l'utilisation des adresses IPv4 publiques disponibles en partageant quelques adresses IPv4 publiques entre un large groupe d'utilisateurs Internet.

Le LSN traduit les adresses IPv4 privées en adresses IPv4 publiques. Il inclut des méthodes de traduction des adresses réseau et des ports pour agréger de nombreuses adresses IP privées en un nombre réduit d'adresses IPv4 publiques. Le LSN est conçu pour gérer le NAT à grande échelle. La fonctionnalité NetScaler LSN est très utile pour les fournisseurs de services Internet (ISP) et les opérateurs fournissant des millions de traductions pour prendre en charge un grand nombre d'utilisateurs (abonnés) et à très haut débit.

Architecture LSN

L'architecture LSN d'un fournisseur de services Internet utilisant des produits NetScaler consiste en des abonnés (utilisateurs d'Internet) dans des espaces d'adressage privés accédant à Internet via une appliance NetScaler déployée sur le réseau central du fournisseur de services Internet. Les abonnés sont connectés au FAI via le réseau d'accès du FAI. Habituellement, les abonnés à des fins commerciales d'Internet sont directement connectés au réseau d'accès du fournisseur de services Internet. Pour répondre aux besoins de ces abonnés, il suffit d'un seul niveau de NAT (NAT44).

Toutefois, les abonnés non commerciaux utilisent généralement des équipements sur site client (CPE), tels que des routeurs et des modems, qui implémentent également la NAT. Ces deux niveaux de NAT créent le modèle NAT444. Le déploiement d'une appliance NetScaler sur le réseau central d'un fournisseur de services Internet pour les fonctionnalités LSN est transparent pour les abonnés et ne nécessite aucune modification de configuration des abonnés ou des CPE.



Large Scale NAT

L'appliance NetScaler reçoit tous les paquets d'abonnés destinés à Internet. L'appliance est configurée avec un pool d'adresses IP NAT prédéfinies à utiliser pour le LSN. L'appliance NetScaler utilise sa fonctionnalité LSN pour traduire l'adresse IP source (privée) et le port du paquet vers l'adresse IP NAT (publique) et le port NAT, puis envoie le paquet vers sa destination sur Internet. L'appliance conserve un enregistrement de toutes les sessions actives qui utilisent la fonctionnalité LSN. Ces sessions sont appelées sessions LSN. L'appliance NetScaler gère également les mappages entre l'adresse IP et le port de l'abonné, et l'adresse IP NAT et le port, pour chaque session. Ces mappages sont appelés mappages LSN. À partir des sessions LSN et des mappages LSN, l'appliance NetScaler reconnaît un paquet de réponse (reçu depuis Internet) appartenant à une session particulière. L'appliance traduit l'adresse IP de destination et le port du paquet de réponse de l'adresse IP NAT address:port à l'adresse IP de l'abonné:port, puis envoie le paquet traduit à l'abonné.

Fonctionnalités LSN prises en charge sur l'appliance NetScaler

La section suivante décrit certaines des fonctionnalités LSN prises en charge sur l'appliance NetScaler :

Allocation de ressources NAT

L'appliance NetScaler alloue des adresses IP et des ports NAT, à partir de son pool de ressources NAT prédéfini, aux abonnés afin qu'ils traduisent leurs paquets en vue de leur transmission vers des hôtes externes (Internet). L'appliance NetScaler prend en charge les types suivants d'adresses IP NAT et d'allocation de ports pour les abonnés :

- **Déterministe.** L'appliance NetScaler attribue une adresse IP NAT et un bloc de ports à chaque abonné. L'appliance alloue des ressources NAT de manière séquentielle à ces abonnés. Il attribue le premier bloc de ports de l'adresse IP NAT de début à l'adresse IP de l'abonné de début. La plage de ports suivante est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. À ce stade, le premier bloc de port de l'adresse NAT suivante est attribué à l'abonné, et ainsi de suite.

  L'appliance NetScaler enregistre l'adresse IP NAT allouée et le bloc de ports pour un abonné. Pour une connexion, un abonné peut être identifié uniquement par son adresse IP NAT mappée et son bloc de ports. Pour cette raison, l'appliance NetScaler n'enregistre aucune session LSN créée ou supprimée. Si l'intégralité du bloc de ports est utilisée, l'appliance NetScaler abandonne toute nouvelle connexion de l'abonné.

- **Dynamique.** L'appliance NetScaler alloue une adresse IP NAT aléatoire et un port du pool NAT LSN pour la connexion d'un abonné. Lorsque l'allocation de blocs de ports est activée dans la configuration, l'appliance alloue une adresse IP NAT aléatoire et un bloc de ports à un abonné lorsqu'elle établit une connexion pour la première fois. L'appliance NetScaler attribue ensuite cette adresse IP NAT et l'un des ports du bloc alloué à chaque connexion ultérieure de cet abonné. Si l'intégralité du bloc de ports est utilisée, l'appliance alloue un nouveau bloc de ports aléatoire à l'abonné lorsqu'elle initie une nouvelle connexion. L'un des ports du nouveau bloc de ports est affecté à la nouvelle connexion.

Regroupement d'adresses IP

Les options d'allocation de ressources NAT suivantes sont disponibles pour les sessions suivantes d'un abonné auquel une adresse IP NAT aléatoire et un port ont été attribués pour une session existante.

- **Jumelé.** L'appliance NetScaler alloue la même adresse IP NAT pour toutes les sessions associées au même abonné. Lorsqu'aucun port n'est disponible pour cette adresse, l'appliance abandonne toute nouvelle connexion de l'abonné. Cette option est nécessaire au bon fonctionnement de certaines applications qui nécessitent la création de plusieurs sessions sur la même adresse IP source (par exemple, dans les applications peer-to-peer qui utilisent le protocole RTP ou RTCP).
- **Aléatoire.** L'appliance NetScaler alloue des adresses IP NAT aléatoires, à partir du pool, pour différentes sessions associées au même abonné.

Réutilisation des mappages LSN

L'appliance NetScaler peut réutiliser une carte LSN existante pour les nouvelles connexions provenant de la même adresse IP et du même port d'abonné. La fonctionnalité NetScaler LSN prend en charge les types suivants de réutilisation du mappage LSN :

1. **Indépendant des terminaux.** L'appliance NetScaler réutilise le mappage LSN pour les paquets suivants envoyés depuis la même adresse IP et le même port d'abonné (x:X) vers n'importe quelle adresse IP et port externes. Ce type de réutilisation des cartes LSN est utile au bon fonctionnement des applications VOIP et peer-to-peer.
2. **Dépendant de l'adresse.** L'appliance NetScaler réutilise le mappage LSN pour les paquets suivants envoyés depuis la même adresse IP d'abonné et le même port (x:X) vers la même adresse IP externe (Y), quel que soit le port externe.
3. **Dépendant du port d'adresse.** L'appliance NetScaler réutilise le mappage LSN pour les paquets suivants envoyés depuis la même adresse IP interne et le même port (x:X) vers la même adresse IP externe et le même port (Y:y) alors que le mappage est toujours actif.

Filtrage LSN

L'appliance NetScaler peut filtrer les paquets provenant d'hôtes externes en fonction des sessions LSN actives et des mappages LSN. Prenons un exemple de mappage LSN qui inclut le mappage IP:port (x:X) de l'abonné, IP:port NAT (N:n) et IP:port de l'hôte externe (Y:y). La fonctionnalité NetScaler LSN prend en charge les types de filtrage suivants :

1. **Indépendant des terminaux.** L'appliance NetScaler filtre uniquement les paquets qui ne sont pas destinés à NAT IP:Port (N:N), qui représente l'IP:Port de l'abonné (x:X), quelles que soient l'adresse IP de l'hôte externe et la source du port (Z:z). L'appliance NetScaler transmet tous les paquets destinés à x:X. En d'autres termes, l'envoi de paquets depuis l'abonné vers n'importe quelle adresse IP externe est suffisant pour autoriser les paquets de n'importe quel hôte externe à destination de l'abonné. Ce type de filtrage est utile au bon fonctionnement des applications VOIP et peer-to-peer.
2. **Dépendant de l'adresse.** L'appliance NetScaler filtre les paquets qui ne sont pas destinés à NAT IP:Port (N:n), qui représente l'IP:Port (x:X) de l'abonné. En outre, l'appliance filtre les paquets provenant de l'adresse IP de l'hôte externe et du port (Y:y) destinés à N:n si l'abonné n'a jamais envoyé de paquets à Y:anyPort (indépendant du port externe). En d'autres termes, pour recevoir des paquets d'un hôte externe spécifique, l'abonné doit d'abord envoyer des paquets à l'adresse IP de cet hôte externe spécifique.
3. **Dépendant du port d'adresse.** L'appliance NetScaler filtre les paquets qui ne sont pas destinés à NAT IP:Port (N:n), qui représente l'IP:Port (x:X) de l'abonné. En outre, l'appliance filtre les paquets provenant de l'adresse IP de l'hôte externe et du port (Y:y) destinés à N:n si l'abonné n'a jamais envoyé de paquets à Y:y auparavant. En d'autres termes, pour recevoir des paquets d'un

hôte externe spécifique, l'abonné doit d'abord envoyer des paquets à cette adresse IP externe et à ce port spécifiques.

Quotas

L'appliance NetScaler peut limiter le nombre de ports et de sessions NAT pour chaque abonné afin de garantir une répartition équitable des ressources entre les abonnés. L'appliance NetScaler peut également limiter le nombre de sessions pour un groupe d'abonnés afin de garantir une répartition équitable des ressources entre les différents groupes d'abonnés.

- **Quota de port.** L'appliance NetScaler peut limiter les ports NAT LSN pouvant être utilisés à la fois par chaque abonné pour un protocole spécifié. Par exemple, vous pouvez limiter chaque abonné à un maximum de 500 ports NAT TCP. Lorsque les mappages NAT LSN d'un abonné atteignent la limite, l'appliance NetScaler n'alloue pas de ports NAT supplémentaires du protocole spécifié à cet abonné.
- **Limite de session d'abonné.** Le nombre de sessions simultanées pour un abonné peut être supérieur à son quota de port. L'appliance NetScaler peut limiter les sessions LSN autorisées pour chaque abonné pour un protocole spécifié. Lorsque le nombre de sessions LSN atteint la limite pour un abonné, l'appliance NetScaler n'autorise pas l'abonné à ouvrir des sessions supplémentaires du protocole spécifié.
- **Limite de sessions de groupe.** L'appliance NetScaler peut limiter le nombre total de sessions LSN autorisées pour un groupe d'abonnés pour un protocole spécifié. Lorsque le nombre total de sessions LSN atteint la limite pour un groupe pour un protocole spécifié, l'appliance NetScaler n'autorise aucun abonné du groupe à ouvrir des sessions supplémentaires du protocole spécifié. Par exemple, vous limitez un groupe à un maximum de 10 000 sessions UDP. Lorsque le nombre total de sessions UDP pour ce groupe atteint 10 000, l'appliance NetScaler n'autorise aucun abonné du groupe à ouvrir des sessions UDP supplémentaires.

Passerelles de couche d'application

Pour certains protocoles de couche application, les adresses IP et les numéros de port du protocole sont également communiqués dans la charge utile du paquet. La passerelle de couche d'application d'un protocole analyse la charge utile du paquet et apporte les modifications nécessaires pour garantir que le protocole continue de fonctionner sur LSN.

L'appliance NetScaler prend en charge le protocole ALG pour les protocoles suivants :

- FTP
- ICMP
- TFTP
- PPTP
- SIP

- RTSP

Support en épingle à cheveux

L'appliance NetScaler prend en charge la communication entre les abonnés ou les hôtes internes à l'aide d'adresses IP NAT. Ce type de communication entre deux abonnés utilisant des adresses IP NAT est appelé « hairpin flow ». Le flux en épingle à cheveux est activé par défaut et vous ne pouvez pas le désactiver.

Points à prendre en compte avant de configurer le LSN

May 5, 2023

Tenez compte des points suivants avant de configurer LSN sur une appliance NetScaler :

- Assurez-vous de bien comprendre les différents composants du NAT à grande échelle, décrits dans les RFC 6888, 5382, 5508 et 4787.
- Le mappage indépendant des points de terminaison (EIM) et le filtrage indépendant des points de terminaison (EIF) sont désactivés par défaut. Ces options doivent être activées pour le bon fonctionnement des applications VoIP et peer-to-peer (P2P).
- **Journalisation du LSN** : voici les points à prendre en compte pour la journalisation des informations LSN :
  - Citrix recommande de consigner les informations LSN sur des serveurs de journaux externes plutôt que sur l'appliance NetScaler. La journalisation sur des serveurs externes permet d'optimiser les performances lorsque l'appliance crée un grand nombre d'entrées de journal LSN (de l'ordre de millions).
  - Citrix recommande d'utiliser SYSLOG sur TCP ou NSLOG. Par défaut, SYSLOG utilise le protocole UDP et NSLOG utilise uniquement le protocole TCP pour transférer les informations du journal vers les serveurs de journaux. Le protocole TCP est plus fiable que le protocole UDP pour transférer des données complètes.
  - Les limitations suivantes s'appliquent à SYSLOG via TCP :
    * La solution Syslog over TCP ne fournit pas d'authentification, de contrôle d'intégrité et de confidentialité.
    * L'appliance NetScaler s'appuie sur le protocole TCP pour confirmer la remise des messages SYSLOG à des serveurs de journaux externes.
- **Haute disponibilité** : voici les points à prendre en compte pour la haute disponibilité des appliances NetScaler pour LSN :
  - Citrix recommande de configurer la fonctionnalité LSN dans le cadre d'un déploiement à haute disponibilité de deux appliances NetScaler pour un fonctionnement ininterrompu et fluide de toutes les sessions LSN.

  - Dans le cadre d'un déploiement à haute disponibilité, Citrix recommande :
    * Définition du paramètre SYNC VLAN pour dédier un VLAN à toutes les communications liées à la HA.
    * Synchronisation de la clé RSS symétrique du nœud principal avec le nœud secondaire pour une synchronisation dynamique d'un grand nombre de mappages et de sessions LSN.
    * Liez le sous-réseau d'adresses IP LSN à un VLAN pour éviter une inondation de diffusions GARP sur tous les VLAN après un basculement.
  - Dans un déploiement à haute disponibilité d'appliances NetScaler, les sessions liées à l'ALG ne sont pas reflétées sur l'appliance secondaire.
- **Passerelles de couche application (ALG) : voici**les points à prendre en compte concernant les ALG sur une appliance NetScaler :
  - Les éléments suivants ne sont pas pris en charge pour SIP ALG :
    * Adresses IP de multidiffusion
    * SDP crypté
    * Messages SIP via TLS
    * Traduction du FQDN dans les messages SIP
    * Authentification des messages SIP
    * Domaines de trafic, partitions d'administration et clusters NetScaler.
    * Messages SIP avec corps en plusieurs parties.
  - Les éléments suivants ne sont pas pris en charge pour RTSP ALG :
    * Sessions RTSP multidiffusion
    * Session RTSP via UDP
    * Domaines de trafic NetScaler, partitions d'administration et clusters NetScaler
  - L'appliance NetScaler ne prend pas en charge le protocole ALG pour le protocole IPsec.
- Si vous désactivez la fonctionnalité LSN alors que certaines sessions LSN existent sur l'appliance NetScaler, ces sessions continuent d'exister pendant la durée de l'intervalle de temporisation configuré.
- Le LSN a la priorité sur le RNAT. Si un paquet provenant d'un abonné LSN spécifié correspond également à une règle RNAT, le paquet est traduit conformément à la configuration LSN.
- Le transfert des paquets liés uniquement aux sessions LSN est basé sur la table de routage de l'appliance NetScaler.
- Contrairement aux adresses IP de sous-réseau, la sélection d'une adresse IP NAT LSN pour la connexion d'un abonné n'est pas basée sur l'entrée de routage pour l'adresse IP de destination.
- Pour les paquets entrants, les mappages LSN statiques sont prioritaires par rapport aux mappages LSN dynamiques.
- Pour les paquets sortants, les profils d'application LSN ont la priorité sur le mappage statique.
- Lorsqu'un grand nombre de sessions LSN (> 1 million) existent sur l'appliance NetScaler, Citrix recommande d'afficher les sessions LSN sélectionnées au lieu de toutes. Dans l'interface de

ligne de commande ou dans l'utilitaire de configuration, utilisez les paramètres de sélection pour afficher le fonctionnement de la session LSN.

- Pour réduire la quantité de mémoire active allouée à la fonctionnalité LSN, vous devez redémarrer à chaud l'appliance NetScaler après avoir modifié le paramètre de mémoire configurée. Sans redémarrage à chaud, vous ne pouvez qu'augmenter la quantité de mémoire active.

Étapes de configuration pour LSN

May 5, 2023

La configuration du LSN sur une appliance NetScaler comprend les tâches suivantes :

1. **Définissez les paramètres LSN globaux.** Les paramètres globaux incluent la quantité de mémoire NetScaler réservée à la fonctionnalité LSN et la synchronisation des sessions LSN dans une configuration haute disponibilité.
2. **Créez une entité cliente LSN et liez-y les abonnés.** Une entité cliente LSN est un ensemble d'abonnés sur le trafic desquels vous souhaitez que l'appliance NetScaler exécute le LSN. L'entité cliente inclut des adresses IPv4 et des règles ACL étendues pour identifier les abonnés. Un client LSN ne peut être lié qu'à un seul groupe LSN. L'interface de ligne de commande comporte deux commandes permettant de créer une entité cliente LSN et de lier un abonné à l'entité cliente LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.
3. **Créez un pool LSN et liez-y des adresses IP NAT.** Un pool LSN définit un pool d'adresses IP NAT à utiliser par l'appliance NetScaler pour effectuer le LSN. Des paramètres sont affectés au pool, tels que l'allocation des blocs de ports et le type de NAT (déterministe ou dynamique). Un pool LSN lié à un groupe LSN s'applique à tous les abonnés d'une entité cliente LSN liée au même groupe. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés entre eux. Plusieurs pools LSN peuvent être liés à un groupe LSN. Pour le NAT dynamique, un pool LSN peut être lié à plusieurs groupes LSN. Pour le NAT déterministe, les pools liés à un groupe LSN ne peuvent pas être liés à d'autres groupes LSN. L'interface de ligne de commande comporte deux commandes permettant de créer un pool LSN et de lier des adresses IP NAT au pool LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.
4. **(Facultatif) Créez un profil de transport LSN pour un protocole spécifié.** Un profil de transport LSN définit différents délais et limites, tels que le nombre maximal de sessions LSN et l'utilisation maximale des ports, qu'un abonné peut avoir pour un protocole donné. Vous liez un profil de transport LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil de transport LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP est lié à un groupe LSN lors de sa création. Ce

profil est appelé profil de transport par défaut. Un profil de transport LSN que vous liez à un groupe LSN remplace le profil de transport LSN par défaut pour ce protocole.

5. **(Facultatif) Créez un profil d'application LSN pour un protocole spécifié et liez un ensemble de ports de destination à celui-ci.** Un profil d'application LSN définit les contrôles de mappage LSN et de filtrage LSN d'un groupe pour un protocole donné et pour un ensemble de ports de destination. Pour un ensemble de ports de destination, vous liez un profil LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil d'application LSN lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil d'application LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP pour tous les ports de destination est lié à un groupe LSN lors de sa création. Ce profil est appelé profil d'application par défaut. Lorsque vous liez un profil d'application LSN, avec un ensemble spécifié de ports de destination, à un groupe LSN, le profil lié remplace le profil d'application LSN par défaut pour ce protocole sur cet ensemble de ports de destination. L'interface de ligne de commande comporte deux commandes permettant de créer un profil d'application LSN et de lier un ensemble de ports de destination au profil d'application LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.
6. **Créez un groupe LSN et liez des pools LSN, des profils de transport LSN (facultatifs) et des profils d'application LSN (facultatifs) au groupe LSN.** Un groupe LSN est une entité composée d'un client LSN, d'un ou de plusieurs pools LSN, de profils de transport LSN et de profils d'application LSN. Des paramètres sont affectés à un groupe, tels que la taille du bloc de ports et la journalisation des sessions LSN. Les paramètres s'appliquent à tous les abonnés d'un client LSN lié au groupe LSN. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés entre eux. Plusieurs pools LSN peuvent être liés à un groupe LSN. Pour le NAT dynamique, un pool LSN peut être lié à plusieurs groupes LSN. Pour le NAT déterministe, les pools liés à un groupe LSN ne peuvent pas être liés à d'autres groupes LSN. Une seule entité cliente LSN peut être liée à un groupe LSN, et une entité cliente LSN liée à un groupe LSN ne peut pas être liée à d'autres groupes LSN. L'interface de ligne de commande comporte deux commandes permettant de créer un groupe LSN et de lier des pools LSN, des profils de transport LSN et des profils d'application LSN au groupe LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.

Le tableau suivant répertorie le nombre maximum d'entités LSN et de liaisons différentes pouvant être créées sur une appliance NetScaler. Ces limites dépendent également de la mémoire disponible sur l'appliance NetScaler.

Entités et liaisons LSN	Limite
Clients du réseau LSN	1024
Piscines LSN	128
Groupes LSN	1024

Entités et liaisons LSN	Limite
Réseaux d'abonnés pouvant être liés à un client LSN	64
ACL étendues pouvant être liées à un client LSN	1024
Adresses IP NAT dans un pool	4096
Pools LSN pouvant être liés à un groupe LSN	8
Groupes LSN pouvant utiliser le même pool LSN	16
Profils de transport LSN pouvant être liés à un groupe LSN	3 (un pour chacun des protocoles TCP, UDP et ICMP)
Groupes LSN pouvant utiliser le même profil de transport LSN	8
Profils d'applications LSN pouvant être liés à un groupe LSN	64
Groupes LSN pouvant utiliser le même profil d'application LSN	8
Plages de ports pouvant être liées à un profil d'application LSN	8

Configuration à l'aide de l'interface de ligne de commande

Pour créer un client LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

Pour lier une adresse réseau ou une règle ACL à un client LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn client <clientname> ((-network <ip_addr> [-netmask <netmask>]
    [-td<positive_integer>]) | -aclname <string>)
```



```
2
3 show lsn client
4 <!--NeedCopy-->
```

Pour créer un pool LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add lsn pool <poolname> [-nattype ( DYNAMIC | DETERMINISTIC )] [-
     portblockallocation ( ENABLED | DISABLED )] [-portrealloctimeout <
     secs>] [-maxPortReallocTmq <positive_integer>]
2
3 show lsn pool
4 <!--NeedCopy-->
```

Pour lier une plage d'adresses IP à un pool LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 bind lsn pool <poolname> <lsnip>
2
3 show lsn pool
4 <!--NeedCopy-->
```

Remarque : Pour supprimer les adresses IP LSN d'un pool LSN, utilisez la commande unbind lsn pool.

Pour créer un profil de transport LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add lsn transportprofile <transportprofilename> <transportprotocol> [-
     sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
     positive_integer>] [-sessionquota <positive_integer>] [-
     portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
     ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]
2
3 show lsn transportprofile
4 <!--NeedCopy-->
```

Pour créer un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]

show lsn appsprofile
<!--NeedCopy-->
```

Pour lier une plage de ports de protocole d'application à un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

Pour créer un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
    DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging (
    ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
    sessionSync (ENABLED | DISABLED )] [-snmptraplimit <positive_integer
    >] [-ftp ( ENABLED | DISABLED )]

show lsn group
<!--NeedCopy-->
```

Pour lier des profils LSN et des pools LSN à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -appsprofilename <string>)

show lsn group
<!--NeedCopy-->
```


Configuration à l'aide de l'utilitaire de configuration

Pour configurer un client LSN et lier une adresse réseau IPv4 ou une règle ACL à l'aide de l'utilitaire de configuration

Accédez à **Système** > **NAT à grande échelle** > **Clients**, ajoutez un client, puis liez une adresse réseau IPv4 ou une règle ACL au client.

Pour configurer un pool LSN et lier des adresses IP NAT à l'aide de l'utilitaire de configuration

Accédez à **Système > NAT à grande échelle** > **Pools**, puis ajoutez un pool, puis liez une adresse IP NAT ou une plage d'adresses IP NAT au pool.

Pour configurer un profil de transport LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Système > NAT à grande échelle > Profils**.
2. Dans le volet de détails, cliquez sur l'onglet **Transport**, puis ajoutez un profil de transport.

Pour configurer un profil d'application LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Système > NAT à grande échelle > Profils**.
2. Dans le volet de détails, cliquez sur l'onglet **Application**, puis ajoutez un profil d'application.

Pour configurer un groupe LSN et lier un client LSN, des pools, des profils de transport et des profils d'application à l'aide de l'utilitaire de configuration

Accédez à **Système > NAT à grande échelle > Groupes**, ajoutez un groupe, puis liez un client LSN, des pools, des profils de transport et des profils d'application au groupe.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- ajouter un client lsn
  - clientname

    Nom de l'entité cliente LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du client LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn client1 » ou « lsn client1 »).

    Il s'agit d'un argument obligatoire. Longueur maximale : 127

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- client LSN de Bind

- clientname

  Nom de l'entité cliente LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du client LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn client1 » ou « lsn client1 »).

  Il s'agit d'un argument obligatoire. Longueur maximale : 127

- network

  Adresse (s) IPv4 du ou des abonnés LSN ou du ou des réseaux d'abonnés sur le trafic desquels vous souhaitez que l'appliance NetScaler exécute un NAT à grande échelle.

- masque de réseau

  Masque de sous-réseau pour l'adresse IPv4 spécifiée dans le paramètre Réseau.

  Valeur par défaut : 255.255.255.255

- td

  ID du domaine de trafic auquel appartient cet abonné ou le réseau d'abonnés (tel que spécifié par le paramètre réseau).

  Si vous ne spécifiez pas d'ID, l'abonné ou le réseau d'abonnés fait partie du domaine de trafic par défaut.

  Valeur par défaut : 0

  Valeur minimale : 0

  Valeur maximale : 4094

- nom de l'acl

  Nom (s) de tous les ACL étendus configurés dont l'action est AUTORISER. La condition spécifiée dans la règle ACL étendue identifie le trafic provenant d'un abonné LSN pour lequel l'appliance NetScaler doit effectuer un NAT à grande échelle. Longueur maximale : 127

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- ajouter un pool LSN
  - nom du pool

    Nom du pool LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait

d'union (-). Ne peut pas être modifié après la création du pool LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn pool1 » ou « lsn pool1 »).

Il s'agit d'un argument obligatoire. Longueur maximale : 127

- nattype

  Type d'adresse IP NAT et d'allocation de port (à partir des pools LSN liés à un groupe LSN) pour les abonnés (de l'entité cliente LSN liée au groupe LSN) :

  Les options disponibles fonctionnent comme suit :

  * **Déterministe**—Allouez une adresse IP NAT et un bloc de ports à chaque abonné (du client LSN lié au groupe LSN). L'appliance NetScaler alloue des ressources NAT de manière séquentielle à ces abonnés. L'appliance NetScaler attribue le premier bloc de ports (taille de bloc déterminée par le paramètre de taille de bloc de ports du groupe LSN) de l'adresse IP NAT de début à l'adresse IP de l'abonné de début. La plage de ports suivante est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. Dans ce cas, le premier bloc de port sur l'adresse NAT suivante est utilisé pour l'abonné, et ainsi de suite. Comme chaque abonné reçoit désormais une adresse IP NAT déterministe et un bloc de ports, un abonné peut être identifié sans qu'il soit nécessaire de se connecter. Pour une connexion, un abonné peut être identifié uniquement sur la base de l'adresse IP et du port NAT, ainsi que de l'adresse IP et du port de destination.
  * **Dynamique** : allouez une adresse IP NAT aléatoire et un port à partir du pool NAT LSN pour la connexion d'un abonné. Si l'allocation de blocs de ports est activée (dans le pool LSN) et qu'une taille de bloc de ports est spécifiée (dans le groupe LSN), l'appliance NetScaler alloue une adresse IP NAT aléatoire et un bloc de ports à un abonné lorsqu'elle établit une connexion pour la première fois. L'appliance alloue cette adresse IP NAT et un port (à partir du bloc de ports alloué) pour différentes connexions de cet abonné. Si tous les ports sont alloués (pour différentes connexions d'abonnés) à partir du bloc de ports alloué aux abonnés, l'appliance alloue un nouveau bloc de ports aléatoire à l'abonné. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés entre eux. Plusieurs pools LSN peuvent être liés à un groupe LSN.

    Valeurs possibles : DYNAMIQUE, DÉTERMINISTE

    Valeur par défaut : DYNAMIC

- allocation de blocs de ports

  Allouez un bloc de ports NAT aléatoire, à partir du pool de ports NAT disponible d'une adresse IP NAT, à chaque abonné lorsque l'allocation NAT est définie comme NAT dy-

namique. Pour toute connexion initiée par un abonné, l'appliance NetScaler alloue un port NAT à partir du bloc de ports NAT alloué à l'abonné pour créer la session LSN.

Vous devez définir la taille du bloc de ports dans le groupe LSN lié. Pour un abonné, si tous les ports sont alloués à partir du bloc de ports alloué à l'abonné, l'appliance NetScaler alloue un nouveau bloc de ports aléatoire à l'abonné.

Pour le NAT déterministe, ce paramètre est activé par défaut et vous ne pouvez pas le désactiver.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

- délai d'expiration du délai de réallocation du port

  Le temps d'attente, en secondes, entre la désallocation des ports NAT LSN (lorsqu'un mappage LSN est supprimé) et leur réallocation pour une nouvelle session LSN. Ce paramètre est nécessaire pour éviter les collisions entre les anciens et les nouveaux mappages et sessions. Cela garantit que toutes les sessions établies sont interrompues au lieu d'être redirigées vers un autre abonné. Cela ne s'applique pas aux ports utilisés dans :

  * NAT déterministe
  * Filtrage dépendant de l'adresse et filtrage dépendant du port d'adresse
  * NAT dynamique avec allocation de blocs de ports

  Dans ces cas, les ports sont immédiatement réaffectés.

  Valeur par défaut : 0

  Valeur maximale : 600

- MaxPort RealLocTMQ

  Nombre maximum de ports pour lesquels le délai de réallocation de port s'applique pour chaque adresse IP NAT. En d'autres termes, la taille maximale de la file d'attente de ports désaffectés pour laquelle le délai de réallocation s'applique pour chaque adresse IP NAT.

  Lorsque la taille de la file d'attente est pleine, le port suivant déalloué est immédiatement réalloué pour une nouvelle session LSN.

  Valeur par défaut : 65536

  Valeur maximale : 65536

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- piscine Bind LN

- nom du pool

  Nom du pool LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du pool LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn pool1 » ou « lsn pool1 »).

  Il s'agit d'un argument obligatoire. Longueur maximale : 127

- slnip

  Adresse IPv4 ou plage d'adresses IPv4 à utiliser comme adresses IP NAT pour le LSN.

  Une fois le pool créé, ces adresses IPv4 sont ajoutées à l'appliance NetScaler en tant qu'adresse IP de type LSN appartenant à NetScaler. Une adresse IP LSN associée à un pool LSN ne peut pas être partagée avec d'autres pools LSN. Les adresses IP spécifiées pour ce paramètre ne doivent pas déjà exister sur l'appliance NetScaler comme toutes les adresses IP appartenant à NetScaler. Dans l'interface de ligne de commande, séparez la plage par un trait d'union. Par exemple : 10.102.29.30-10.102.29.189. Vous pouvez ultérieurement supprimer certaines ou toutes les adresses IP LSN du pool et ajouter des adresses IP au pool LSN.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- ajouter un profil de transport lsn

  - nom du profil de transport

    Nom du profil de transport LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du profil de transport LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn transport profile1 » ou « lsn transport profile1 »).

    Il s'agit d'un argument obligatoire. Longueur maximale : 127

  - protocole de transport

    Protocole pour lequel définir les paramètres du profil de transport LSN.

    Il s'agit d'un argument obligatoire.

    Valeurs possibles : TCP, UDP, ICMP

- délai d'expiration de la session

  Délai d'expiration, en secondes, pour une session LSN inactive. Si une session LSN est inactive pendant une durée supérieure à cette valeur, l'appliance NetScaler supprime la session.

  Ce délai ne s'applique pas à une session TCP LSN lorsqu'un message FIN ou RST est reçu de l'un des points de terminaison.

  Valeur par défaut : 120

  Valeur minimale : 60

- finrsttimeout

  Délai d'expiration, en secondes, d'une session TCP LSN après la réception d'un message FIN ou RST de l'un des points de terminaison.

  Si une session TCP LSN est inactive (après que l'appliance NetScaler a reçu un message FIN ou RST) pendant une durée supérieure à cette valeur, l'appliance NetScaler supprime la session.

  Étant donné que la fonctionnalité LSN de l'appliance NetScaler ne conserve pas les informations d'état des sessions TCP LSN, ce délai permet la transmission des messages FIN, RST et ACK depuis l'autre point de terminaison afin que les deux points de terminaison puissent fermer correctement la connexion.

  Valeur par défaut : 30

- quota de port

  Nombre maximum de ports NAT LSN pouvant être utilisés simultanément par chaque abonné pour le protocole spécifié. Par exemple, chaque abonné peut être limité à un maximum de 500 ports NAT TCP. Lorsque les mappages NAT LSN d'un abonné atteignent la limite, l'appliance NetScaler n'alloue pas de ports NAT supplémentaires à cet abonné.

  Valeur par défaut : 0

  Valeur minimale : 0

  Valeur maximale : 65535

- quota de session

  Nombre maximum de sessions LSN simultanées autorisées pour chaque abonné pour le protocole spécifié. Lorsque le nombre de sessions LSN atteint la limite pour un abonné, l'appliance NetScaler n'autorise pas l'abonné à ouvrir des sessions supplémentaires.

  Valeur par défaut : 0

  Valeur minimale : 0

Valeur maximale : 65535

- parité entre les ports

  Activez la parité de port entre le port d'un abonné et son port NAT LSN mappé. Par exemple, si un abonné initie une connexion à partir d'un port numéroté impair, l'appliance NetScaler alloue un port NAT LSN de numéro impair à cette connexion. Vous devez définir ce paramètre pour garantir le bon fonctionnement des protocoles qui exigent que le port source soit pair ou impair, par exemple dans les applications peer-to-peer qui utilisent le protocole RTP ou RTCP.

  Valeurs possibles : ENABLED, DISABLED

  Valeur par défaut : DISABLED

- gamme Port Preserve

  Si un abonné établit une connexion à partir d'un port connu (0-1023), attribuez un port NAT de la plage de ports connue (0-1023) à cette connexion. Par exemple, si un abonné initie une connexion à partir du port 80, l'appliance NetScaler peut allouer le port 100 comme port NAT pour cette connexion.

  Ce paramètre s'applique au NAT dynamique sans allocation de blocs de ports. Cela s'applique également au NAT déterministe si la plage de ports alloués inclut des ports connus.

  Lorsque tous les ports connus de toutes les adresses IP NAT disponibles sont utilisés dans différentes connexions d'abonnés (sessions LSN) et qu'un abonné initie une connexion à partir d'un port connu, l'appliance NetScaler abandonne cette connexion.

  Valeurs possibles : ENABLED, DISABLED

  Valeur par défaut : DISABLED

- syncheck

  Supprimez silencieusement tous les paquets non SYN pour les connexions pour lesquelles aucune session LSN-NAT n'est présente sur l'appliance NetScaler.

  Si vous désactivez ce paramètre, l'appliance NetScaler accepte tous les paquets non SYN et crée une nouvelle entrée de session LSN pour cette connexion.

  Voici quelques raisons pour lesquelles l'appliance NetScaler reçoit de tels paquets :

  * Une session LSN pour une connexion existait mais l'appliance NetScaler a supprimé cette session car la session LSN est restée inactive pendant une durée dépassant le délai d'expiration de session configuré.
  * Ces paquets peuvent faire partie d'une attaque DoS.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- ajouter un profil lsn appsprofile
  - nom du profil des applications

    Nom du profil d'application LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du profil d'application LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn application profile 1 » ou « lsn application profile 1 »).

    Il s'agit d'un argument obligatoire. Longueur maximale : 127
  - protocole de transport

    Nom du protocole auquel s'appliquent les paramètres de ce profil d'application LSN.

    Il s'agit d'un argument obligatoire.

    Valeurs possibles : TCP, UDP, ICMP
  - transfert de propriété intellectuelle

    Options d'allocation d'adresses IP NAT pour les sessions associées au même abonné.

    Les options disponibles fonctionnent comme suit :

    * **Couplé** : l'appliance NetScaler alloue la même adresse IP NAT pour toutes les sessions associées au même abonné. Lorsque tous les ports d'une adresse IP NAT sont utilisés dans des sessions LSN (pour le même ou plusieurs abonnés), l'appliance NetScaler supprime toute nouvelle connexion de l'abonné.
    * **Aléatoire** : l'appliance NetScaler alloue des adresses IP NAT aléatoires, à partir du pool, pour différentes sessions associées au même abonné.

    Ce paramètre s'applique uniquement à l'allocation NAT dynamique.

    Valeurs possibles : PAIRED, RANDOM

    Valeur par défaut : RANDOM
  - cartographie

    Type de mappage LSN à appliquer aux paquets suivants provenant de la même adresse IP et du même port d'abonné.

Prenons un exemple de mappage LSN qui inclut le mappage de l'abonné IP:port (x:X), de l'IP:port du NAT (N:n) et de l'adresse IP:port de l'hôte externe (Y:y).

Les options disponibles fonctionnent comme suit :

* **ENDPOINT-INDEPENDENT**—Réutilisez le mappage LSN pour les paquets suivants envoyés depuis la même adresse IP et le même port d'abonné (x:X) vers n'importe quelle adresse IP et port externes.
* **DÉPENDANT DE L'ADRESSE —Réutilisez**le mappage LSN pour les paquets suivants envoyés depuis la même adresse IP d'abonné et le même port (x:X) vers la même adresse IP externe (Y), quel que soit le port externe.
* **ADDRESS-PORT-DEPENDANT**—Réutilisez le mappage LSN pour les paquets suivants envoyés depuis la même adresse IP interne et le même port (x:X) vers la même adresse IP externe et le même port (Y:y) alors que le mappage est toujours actif.

Valeurs possibles : ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDANT

Valeur par défaut : ADDRESS-PORT-DEPENDENT

– filtrage

Type de filtre à appliquer aux paquets provenant d'hôtes externes.

Prenons un exemple de mappage LSN qui inclut le mappage IP:port (x:X) de l'abonné, IP:port NAT (N:n) et IP:port de l'hôte externe (Y:y).

Les options disponibles fonctionnent comme suit :

* **ENDPOINT INDEPENDENT**—Filtre uniquement les paquets qui ne sont pas destinés à l'adresse IP de l'abonné et au port x:x, quelles que soient l'adresse IP de l'hôte externe et la source du port (Z:z). L'appliance NetScaler transmet tous les paquets destinés à x:X. En d'autres termes, l'envoi de paquets depuis l'abonné vers n'importe quelle adresse IP externe est suffisant pour autoriser les paquets provenant de n'importe quel hôte externe à l'abonné.
* **DÉPENDANT DE L'ADRESSE**—Filtre les paquets qui ne sont pas destinés à l'adresse IP de l'abonné et au port x:X. En outre, l'appliance filtre les paquets provenant de Y:y destinés à l'abonné (x:X) si le client n'a jamais envoyé de paquets à Y:AnyPort (indépendant du port externe). En d'autres termes, pour recevoir des paquets d'un hôte externe spécifique, l'abonné doit d'abord envoyer des paquets à l'adresse IP de cet hôte externe spécifique.
* **ADDRESS PORT DEPENDANT** (valeur par défaut) : filtre les paquets non destinés à l'adresse IP et au port de l'abonné (x:X). En outre, l'appliance NetScaler filtre les paquets de Y:y destinés à l'abonné (x:X) si l'abonné n'a jamais envoyé de paquets à Y:y auparavant. En d'autres termes, pour recevoir des paquets d'un hôte externe spéci-

fique, l'abonné doit d'abord envoyer les paquets à cette adresse IP et à ce port externes.

Valeurs possibles : ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDANT

Valeur par défaut : ADDRESS-PORT-DEPENDENT

- proxy tcp

  Activez le proxy TCP, qui permet à l'appliance NetScaler d'optimiser le trafic TCP à l'aide des fonctionnalités de couche 4.

  Valeurs possibles : ENABLED, DISABLED

  Valeur par défaut : DISABLED

- td

  ID du domaine de trafic via lequel l'appliance NetScaler envoie le trafic sortant après avoir effectué le LSN.

  Si vous ne spécifiez pas d'ID, l'appliance envoie le trafic sortant via le domaine de trafic par défaut, dont l'ID est 0.

  Valeur par défaut : 65535

  Valeur maximale : 65535

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- profil de bind lsn appsprofile
  - nom du profil des applications

    Nom du profil d'application LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du profil d'application LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn application profile 1 » ou « lsn application profile 1 »).

    Il s'agit d'un argument obligatoire. Longueur maximale : 127

  - lsnport

    Numéros de port ou plage de numéros de port à comparer avec le port de destination du paquet entrant provenant d'un abonné. Lorsque le port de destination correspond, le profil d'application LSN est appliqué pour la session LSN. Séparez une plage de ports par un trait d'union. Par exemple, 40-90.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- ajouter un groupe lsn
  - nom du groupe

    Nom du groupe LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du groupe LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn group1 » ou « lsn group1 »).

    Il s'agit d'un argument obligatoire. Longueur maximale : 127
  - clientname

    Nom de l'entité cliente LSN à associer au groupe LSN. Vous ne pouvez associer qu'une seule entité cliente LSN à un groupe LSN. Vous ne pouvez pas supprimer cette association ni la remplacer par une autre entité cliente LSN une fois le groupe LSN créé.

    Il s'agit d'un argument obligatoire. Longueur maximale : 127
  - nattype

    Type d'adresse IP NAT et d'allocation de port (à partir des pools LSN liés) pour les abonnés :

    Les options disponibles fonctionnent comme suit :

    * **Déterministe**—Allouez une adresse IP NAT et un bloc de ports à chaque abonné (du client LSN lié au groupe LSN). L'appliance NetScaler alloue des ressources NAT de manière séquentielle à ces abonnés. L'appliance NetScaler attribue le premier bloc de ports (taille de bloc déterminée par le paramètre de taille de bloc de ports du groupe LSN) de l'adresse IP NAT de début à l'adresse IP de l'abonné de début. La plage de ports suivante est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. Dans ce cas, le premier bloc de port sur l'adresse NAT suivante est utilisé pour l'abonné, et ainsi de suite. Comme chaque abonné reçoit désormais une adresse IP NAT déterministe et un bloc de ports, un abonné peut être identifié sans qu'il soit nécessaire de se connecter. Pour une connexion, un abonné peut être identifié uniquement sur la base de l'adresse IP et du port NAT, ainsi que de l'adresse IP et du port de destination.
    * **Dynamique** : allouez une adresse IP NAT aléatoire et un port du pool NAT LSN pour la connexion d'un abonné. Si l'allocation de blocs de ports est activée (dans le pool LSN) et qu'une taille de bloc de ports est spécifiée (dans le groupe LSN), l'appliance NetScaler alloue une adresse IP NAT aléatoire et un bloc de ports à un abonné lorsqu'elle établit une connexion pour la première fois. L'appliance alloue cette adresse IP NAT et un port (à partir du bloc de ports alloué) pour différentes

connexions de cet abonné. Si tous les ports sont alloués (pour différentes connexions d'abonnés) à partir du bloc de ports alloué aux abonnés, l'appliance alloue un nouveau bloc de ports aléatoire à l'abonné.

Valeurs possibles : DYNAMIQUE, DÉTERMINISTE

Valeur par défaut : DYNAMIC

- taille du bloc de ports

  Taille du bloc de ports NAT à allouer à chaque abonné.

  Pour définir ce paramètre pour le NAT dynamique, vous devez activer le paramètre d'allocation de blocs de ports dans le pool LSN lié. Pour le NAT déterministe, le paramètre d'allocation de blocs de ports est toujours activé et vous ne pouvez pas le désactiver.

  Dans Dynamic NAT, l'appliance NetScaler alloue un bloc de ports NAT aléatoire, à partir du pool de ports NAT disponible d'une adresse IP NAT, pour chaque abonné. Pour un abonné, si tous les ports sont alloués à partir du bloc de ports attribué à l'abonné, l'appliance alloue un nouveau bloc de ports aléatoire à l'abonné.

- enregistrement

  Enregistrez les entrées de mappage et les sessions créées ou supprimées pour ce groupe LSN. L'appliance NetScaler enregistre les sessions LSN pour ce groupe LSN uniquement lorsque les paramètres de journalisation et de journalisation de session sont activés.

  L'appliance utilise son syslog et son framework de journaux d'audit existants pour enregistrer les informations LSN. Vous devez activer la journalisation LSN au niveau global en activant le paramètre LSN dans les entités d'action NSLOG et SYLOG associées. Lorsque le paramètre Logging est activé, l'appliance NetScaler génère des messages de journal relatifs aux mappages LSN et aux sessions LSN de ce groupe LSN. L'appliance envoie ensuite ces messages de journal aux serveurs associés aux entités d'action NSLOG et d'actions SYSLOG.

  Un message de journal pour une entrée de mappage LSN contient les informations suivantes :

  * Adresse NSIP de l'appliance NetScaler
  * Horodatage
  * Type d'entrée (MAPPING ou SESSION)
  * Si l'entrée de mappage LSN est créée ou supprimée
  * Adresse IP, port et ID de domaine de trafic de l'abonné
  * Adresse IP et port NAT
  * Nom du protocole
  * L'adresse IP de destination, le port et l'ID du domaine de trafic peuvent être présents, selon les conditions suivantes :

- L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison
- Seule l'adresse IP de destination (et non le port) est enregistrée pour le mappage dépendant de l'adresse
- L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

– Enregistrement des sessions

Consigner les sessions créées ou supprimées pour le groupe LSN. L'appliance NetScaler enregistre les sessions LSN pour ce groupe LSN uniquement lorsque les paramètres de journalisation et de journalisation de session sont activés.

Un message de journal pour une session LSN contient les informations suivantes :

* Adresse NSIP de l'appliance NetScaler
* Horodatage
* Type d'entrée (MAPPING ou SESSION)
* Si la session LSN est créée ou supprimée
* Adresse IP, port et ID de domaine de trafic de l'abonné
* Adresse IP et port NAT
* Nom du protocole
* Adresse IP de destination, port et ID de domaine de trafic

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

– Synchronisation de session

Dans un déploiement à haute disponibilité (HA), synchronisez les informations de toutes les sessions LSN liées à ce groupe LSN avec le nœud secondaire. Après un basculement, les connexions TCP établies et les flux de paquets UDP restent actifs et reprennent sur le nœud secondaire (nouveau nœud principal).

Pour que ce paramètre fonctionne, vous devez activer le paramètre de synchronisation de session globale.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

– limite snmptrap

Nombre maximum de messages SNMP Trap pouvant être générés pour le groupe LSN en une minute.

Valeur par défaut : 100

Valeur minimale : 0

Valeur maximale : 10000

- ftp

  Activez Application Layer Gateway (ALG) pour le protocole FTP. Pour certains protocoles de couche application, les adresses IP et les numéros de port du protocole sont généralement communiqués dans la charge utile des paquets. Lorsqu'elle agit en tant qu'ALG, l'appliance modifie la charge utile des paquets pour garantir que le protocole continue de fonctionner sur LSN.

  Remarque : L'appliance NetScaler inclut également ALG pour les protocoles ICMP et TFTP. L'ALG pour le protocole ICMP est activé par défaut et aucune disposition ne permet de le désactiver. L'ALG pour le protocole TFTP est désactivé par défaut. ALG est automatiquement activé pour un groupe LSN lorsque vous liez un profil d'application UDP LSN, avec un mappage indépendant du point de terminaison, un filtrage indépendant du point de terminaison et un port de destination 69 (port connu pour TFTP), au groupe LSN.

  Valeurs possibles : ENABLED, DISABLED

  Valeur par défaut : ENABLED

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- groupe Bind LSN
  - nom du groupe

    Nom du groupe LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du groupe LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn group1 » ou « lsn group1 »).

    Il s'agit d'un argument obligatoire. Longueur maximale : 127

  - nom du pool

    Nom du pool LSN à lier au groupe LSN spécifié. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés entre eux. Plusieurs pools LSN peuvent être liés à un groupe LSN.

    Pour le NAT déterministe, les pools liés à un groupe LSN ne peuvent pas être liés à d'autres groupes LSN. Pour le NAT dynamique, les pools liés à un groupe LSN peuvent être liés à plusieurs groupes LSN. Longueur maximale : 127

- nom du profil de transport

  Nom du profil de transport LSN à lier au groupe LSN spécifié. Liez un profil pour chaque protocole pour lequel vous souhaitez spécifier des paramètres.

  Par défaut, un profil de transport LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP est lié à un groupe LSN lors de sa création. Ce profil est appelé transport par défaut.

  Un profil de transport LSN que vous liez à un groupe LSN remplace le profil de transport LSN par défaut pour ce protocole. Longueur maximale : 127

- nom du profil des applications

  Nom du profil d'application LSN à lier au groupe LSN spécifié. Pour chaque ensemble de ports de destination, liez un profil pour chaque protocole pour lequel vous souhaitez spécifier des paramètres.

  Par défaut, un profil d'application LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP pour tous les ports de destination est lié à un groupe LSN lors de sa création. Ce profil est appelé profil d'application par défaut.

  Lorsque vous liez un profil d'application LSN, avec un ensemble spécifié de ports de destination, à un groupe LSN, le profil lié remplace le profil d'application LSN par défaut pour ce protocole sur cet ensemble de ports de destination. Longueur maximale : 127

Exemples de configurations LSN

January 21, 2021

Voici des exemples de configuration de LSN via l'interface de ligne de commande.

Créez une configuration LSN simple avec un réseau abonné unique, une adresse IP NAT LSN unique et des paramètres par défaut :

```
1  add lsn client LSN-CLIENT-1
2
3  Done
4
5  bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-1
10
```



```
Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done
<!--NeedCopy-->
```

Créez une configuration LSN avec une liste ACL étendue pour identifier les abonnés LSN :

```
add ns acl LSN-ACL-2 ALLOW -srcIP 192.0.2.10-192.0.2.20

Done

apply acls

Done

add lsn client LSN-CLIENT-2

Done

bind lsn client LSN-CLIENT-2  -aclname LSN-ACL-2

Done

add lsn pool LSN-POOL-2

Done

bind lsn pool LSN-POOL-2 203.0.113.5-203.0.113.10

Done

add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2

Done

```



```
29 bind lsn group LSN-GROUP-2 -poolname LSN-POOL-2
30
31 Done
32 <!--NeedCopy-->
```

Créez une configuration LSN avec mappage indépendant du point de terminaison pour le protocole HTTP (port 80) et mappage dépendant du port d'adresse pour le protocole SSH (port 22). En outre, limitez chaque abonné à utiliser un maximum de 1000 ports NAT pour le protocole TCP et 100 ports NAT pour le protocole UDP. Restreindre chaque abonné à avoir un maximum de 2000 sessions simultanées pour le protocole TCP. Restreindre le groupe pour qu'il dispose d'un maximum de 30000 sessions simultanées pour le protocole TCP :

```
1  add lsn client LSN-CLIENT-3
2
3  Done
4
5  bind lsn client LSN-CLIENT-3 -network 192.0.3.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-3
10
11 Done
12
13 bind lsn pool LSN-POOL-3 203.0.113.11
14
15 Done
16
17 add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-3
18
19 Done
20
21 bind lsn group LSN-GROUP-3 -poolname LSN-POOL-3
22
23 Done
24
25 add lsn appsprofile LSN-APPS-HTTPPROFILE-3 TCP -mapping ENDPOINT-
      INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile LSN-APPS-HTTPPROFILE-3 80
30
31 Done
```



```
32
33 bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-HTTPPROFILE
       -3
34
35 Done
36
37 add lsn appsprofile LSN-APPS-SSHPROFILE-3 TCP -mapping ADDRESS-PORT-
       DEPENDENT
38
39 Done
40
41 bind lsn appsprofile LSN-APPS-SSHPROFILE-3 22
42
43 Done
44
45 bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-SSHPROFILE
       -3
46
47 Done
48
49 add lsn transportprofile LSN-TRANS-PROFILE-TCP-3 TCP -portquota 1000 -
       sessionquota 2000 -groupSessionLimit 30000
50
51 Done
52
53 bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-TCP
       -3
54
55 Done
56
57 add lsn transportprofile LSN-TRANS-PROFILE-UDP-3 UDP -portquota 100
58
59 Done
60
61 bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-UDP
       -3
62
63 Done
64 <!--NeedCopy-->
```

Créez une configuration LSN pour un grand nombre d'abonnés :

```
1 add lsn client LSN-CLIENT-4
2
3 Done
```



```
4
5  bind lsn client LSN-CLIENT-4 -network 192.0.4.0 -netmask 255.255.255.0
6
7  Done
8
9  bind lsn client LSN-CLIENT-4 -network 192.0.5.0 -netmask 255.255.255.0
10
11 Done
12
13 bind lsn client LSN-CLIENT-4 -network 192.0.6.0 -netmask 255.255.255.0
14
15 Done
16
17 bind lsn client LSN-CLIENT-4 -network 192.0.7.0 -netmask 255.255.255.0
18
19 Done
20
21 bind lsn client LSN-CLIENT-4 -network 192.0.8.0 -netmask 255.255.255.0
22
23 Done
24
25 add lsn pool LSN-POOL-4
26
27 Done
28
29 bind lsn pool LSN-POOL-4 203.0.113.30-203.0.113.40
30
31 Done
32
33 bind lsn pool LSN-POOL-4 203.0.113.45-203.0.113.50
34
35 Done
36
37 bind lsn pool LSN-POOL-4 203.0.113.55-203.0.113.60
38
39 Done
40
41 add lsn group LSN-GROUP-4 -clientname LSN-CLIENT-4
42
43 Done
44
45 bind lsn group LSN-GROUP-4 -poolname LSN-POOL-4
46
47 Done
48
```



```
49 add lsn appsprofile LSN-APPS-WELLKNOWNPROFILE-4 TCP -mapping ENDPOINT-
      INDEPENDENT
50
51 Done
52
53 bind lsn appsprofile LSN-APPS-WELLKNOWN-PORTS-PROFILE-4 1- 1023
54
55 Done
56
57 bind lsn group LSN-GROUP-4 -applicationprofilename LSN-APPS-WELLKNOWN-
      PORTS-PROFILE-4
58
59 Done
60 <!--NeedCopy-->
```

Créez une configuration LSN avec le partage des ressources NAT entre plusieurs groupes LSN. Dans cet exemple, le pool LSN LSN-POOL-5 est partagé avec les groupes LSN LSN-GROUP-5 et LSN-GROUP-6 :

```
1  add lsn client LSN-CLIENT-5
2
3  Done
4
5  bind lsn client LSN-CLIENT-5 -network 192.0.15.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-5
10
11 Done
12
13 bind lsn pool LSN-POOL-5 203.0.113.12-203.0.113.14
14
15 Done
16
17 add lsn group LSN-GROUP-5 -clientname LSN-CLIENT-5
18
19 Done
20
21 bind lsn group LSN-GROUP-5 -poolname LSN-POOL-5
22
23 Done
24
25 add lsn client LSN-CLIENT-6
26
```



```
Done

bind lsn client LSN-CLIENT-6 -network 192.0.16.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-6

Done

bind lsn pool LSN-POOL-6 203.0.113.15-203.0.113.18

Done

add lsn group LSN-GROUP-6 -clientname LSN-CLIENT-6

Done

bind lsn group LSN-GROUP-6 -poolname LSN-POOL-6

Done

bind lsn group LSN-GROUP-6 -poolname LSN-POOL-5

Done
<!--NeedCopy-->
```

Créez une configuration LSN avec une allocation de ressources NAT déterministe :

```
add lsn client LSN-CLIENT-7

Done

bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-7 -nattype DETERMINISTIC

Done

bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23

Done

```



```
add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
   DETERMINISTIC -portblocksize 1024

Done

bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7

Done
<!--NeedCopy-->
```

Créez une configuration LSN avec plusieurs réseaux d'abonnés ayant la même adresse réseau mais chaque réseau appartenant à un domaine de trafic différent. En outre, limitez le trafic sortant lié au protocole HTTP (port 80), en l'envoyant via un domaine de trafic particulier (td 5) :

```
add lsn client LSN-CLIENT-8

Done

bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
    -td 1

Done

bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
    -td 2

Done

bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
    -td 3

Done

add lsn pool LSN-POOL-8

Done

bind lsn pool LSN-POOL-8 203.0.113.80-203.0.113.86

Done

add lsn group LSN-GROUP-8 -clientname LSN-CLIENT-8

```



```
Done

bind lsn group LSN-GROUP-8 -poolname LSN-POOL-8

Done

add lsn appsprofile LSN-APPS-HTTP-PROFILE-8 TCP -td 5

Done

bind lsn appsprofile LSN-APPS-HTTP-PROFILE-8 80

Done

bind lsn group LSN-GROUP-8 -applicationprofilename LSN-APPS-HTTP-
   PROFILE-8

Done
<!--NeedCopy-->
```

Créez une configuration LSN qui limite le trafic sortant d'un protocole spécifique (TCP), en l'envoyant via un domaine de trafic particulier (td 5). Avec le filtrage indépendant du point de terminaison, recevez le trafic entrant lié à ce protocole (TCP) sur n'importe quel domaine de trafic :

```
add lsn client LSN-CLIENT-9

Done

bind lsn client LSN-CLIENT-9 -network 192.0.9.0 -netmask 255.255.255.0
   -td 1

Done

add lsn pool LSN-POOL-9

Done

bind lsn pool LSN-POOL-9 203.0.113.90

Done

add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

```



```
Done

bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done

add lsn appsprofile LSN-APPS-PROFILE-9 TCP -filtering ENDPOINT-
    INDEPENDENT -td 5

Done

bind lsn group LSN-GROUP-9 -approfile LSN-APPS-PROFILE-9

Done
<!--NeedCopy-->
```

Créez une configuration LSN qui limite le trafic HTTP sortant (port 80), en l'envoyant via un domaine de trafic particulier (td 10). Avec le filtrage dépendant de l'adresse, recevez le trafic entrant lié à ce protocole (HTTP) sur le domaine de trafic spécifié (td 10) :

```
add lsn client LSN-CLIENT-10

Done

bind lsn client LSN-CLIENT-10 -network 192.0.10.0 -netmask
    255.255.255.0 -td 1

Done

add lsn pool LSN-POOL-10

Done

bind lsn pool LSN-POOL-10 203.0.113.100

Done

add lsn group LSN-GROUP-10 -clientname LSN-CLIENT-10

Done

bind lsn group LSN-GROUP-10 -poolname LSN-POOL-10

Done

```



```
25 add lsn appsprofile LSN-APPS-PROFILE-10 TCP -mapping ENDPOINT -
      INDEPENDENT -filtering ADDRESS-DEPENDENT -td 10
26
27 Done
28
29 bind lsn appsprofile LSN-APPS-PROFILE-10 80
30
31 Done
32
33 bind lsn group LSN-GROUP-10 -approfile LSN-APPS-PROFILE-10
34
35 Done
36 <!--NeedCopy-->
```

Configuration des mappages LSN statiques

May 5, 2023

L'appliance NetScaler prend en charge la création manuelle d'un mappage LSN biunivoque entre une adresse IP:port d'un abonné et une adresse IP NAT:port. Les mappages LSN statiques sont utiles dans les cas où vous souhaitez vous assurer que les connexions initiées vers un NAT IP:Port correspondent à l'adresse IP:Port de l'abonné. Par exemple, les serveurs Web situés dans le réseau interne.

Pour créer un mappage LSN statique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
     <positive_integer>] [<natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd
      <positive_integer>]]
2 -  show lsn static
3 <!--NeedCopy-->
```

Pour créer un mappage LSN statique à l'aide de l'utilitaire de configuration

Accédez à Système > NAT à grande échelle > Statique, puis ajoutez un nouveau mappage statique.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

ajouter un nom statique lsn

Nom de l'entrée de mappage statique LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du groupe LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « lsn static1 » ou « lsn static1 »). Il s'agit d'un argument obligatoire. Longueur maximale : 127

protocole de transport

Protocole pour l'entrée de mappage LSN. Il s'agit d'un argument obligatoire. Valeurs possibles : TCP, UDP, ICMP

S'abonner

Adresse IPv4 d'un abonné LSN pour l'entrée de mappage LSN. Il s'agit d'un argument obligatoire.

S'abonner au port

Port de l'abonné LSN pour l'entrée de mappage LSN. Il s'agit d'un argument obligatoire. Valeur maximale : 65535

td

ID du domaine de trafic auquel appartient l'abonné. Si vous ne spécifiez pas d'ID, l'abonné est supposé faire partie du domaine de trafic par défaut. Valeur par défaut : 0, valeur minimale : 0, valeur maximale : 4094

NatiP

Adresse IPv4, déjà existante sur l'appliance NetScaler en tant que type LSN, à utiliser comme adresse IP NAT pour cette entrée de mappage.

Port de NAT

Port NAT pour cette entrée de mappage LSN.

DestP

Adresse IP de destination pour l'entrée de mappage LSN.

dsttd

ID du domaine de trafic via lequel l'adresse IP de destination de cette entrée de mappage LSN est accessible depuis l'appliance NetScaler. Si vous ne spécifiez pas d'ID, l'adresse IP de destination est supposée être accessible via le domaine de trafic par défaut, dont l'ID est 0. Valeur par défaut : 0, valeur minimale : 0, valeur maximale : 4094

Cartes statiques des ports Wildcard

Une entrée de mappage statique est généralement un mappage LSN un à un entre une adresse IP d'abonné:port et une adresse IP NAT:port. Une entrée de mappage LSN statique un à un n'expose qu'un seul port de l'abonné à Internet.

Dans certaines situations, il peut être nécessaire d'exposer tous les ports (64 Ko) d'un abonné à Internet (par exemple, un serveur hébergé sur un réseau interne et exécutant un service différent sur chaque port). Pour rendre ces services internes accessibles via Internet, vous devez exposer tous les ports du serveur à Internet.

L'un des moyens de répondre à cette exigence consiste à ajouter 64 000 entrées de mappage statiques individuelles, soit une entrée de mappage pour chaque port. La création de 64 000 entrées est très fastidieuse et constitue une tâche ardue. Ce grand nombre d'entrées de configuration peut également entraîner des problèmes de performances dans l'appliance NetScaler.

Une autre méthode simple consiste à utiliser des ports génériques dans une entrée de mappage statique. Il vous suffit de créer une entrée de mappage statique avec les paramètres du port NAT et du port abonné définis sur le caractère générique (*), et le paramètre de protocole défini sur ALL, pour exposer tous les ports d'un abonné à Internet. Pour les connexions entrantes ou sortantes d'un abonné correspondant à une entrée de mappage statique générique, le port de l'abonné ne change pas après l'opération NAT.

Lorsqu'une connexion à Internet initiée par un abonné correspond à une entrée de mappage statique générique, l'appliance NetScaler attribue un port NAT portant le même numéro que le port d'abonné à partir duquel la connexion est initiée. De même, un hôte Internet se connecte au port d'un abonné en se connectant au port NAT qui porte le même numéro que le port de l'abonné.

Configuration de l'appliance NetScaler pour fournir un accès à tous les ports d'un abonné IPv4

Pour configurer l'appliance NetScaler afin de fournir un accès à tous les ports d'un abonné IPv4, créez une carte statique générique avec les paramètres obligatoires suivants :

- Protocol=Tout
- Port d'abonné = *
- Port NAT = *

Dans une carte statique générique, contrairement à une carte statique un à un, la définition du paramètre IP NAT est obligatoire. De plus, l'adresse IP NAT attribuée à une carte statique générique ne peut être utilisée pour aucun autre abonné.

Pour créer une carte statique avec caractères génériques à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
   positive_integer>] [-destIP <ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Exemple de configuration

Dans l'exemple de configuration suivant d'une carte statique générique, tous les ports d'un abonné dont l'adresse IP est 192.0.2.10 sont rendus accessibles via l'adresse IP NAT 203.0.11.33.

Exemple de configuration :

```
add lsn static NAT44-WILDCARD-STATIC-1 ALL  192.0.2.10 * 203.0.113.33 *

Done
<!--NeedCopy-->
```

Configuration des passerelles de la couche application

May 5, 2023

Pour certains protocoles de couche application, les adresses IP et les numéros de port du protocole sont également communiqués dans la charge utile du paquet. La passerelle de couche d'application

d'un protocole analyse la charge utile du paquet et apporte les modifications nécessaires pour garantir que le protocole continue de fonctionner sur LSN.

L'appliance NetScaler prend en charge le protocole ALG pour les protocoles suivants :

- FTP
- ICMP
- TFTP
- PPTP
- SIP
- RTSP

Passerelle de couche d'application pour les protocoles FTP, ICMP et TFTP

May 5, 2023

Vous pouvez activer ou désactiver ALG pour le protocole FTP d'une configuration LSN en activant ou en désactivant l'option FTP du groupe LSN de la configuration LSN.

L'ALG pour le protocole ICMP est activé par défaut et aucune disposition ne permet de le désactiver.

L'ALG pour le protocole TFTP est désactivé par défaut. L'ALG TFTP est automatiquement activé pour une configuration LSN lorsque vous liez un profil d'application UDP LSN, avec un mappage indépendant du point de terminaison, un filtrage indépendant du point de terminaison et un port de destination 69 (port connu pour TFTP), au groupe LSN.

Exemple de configuration LSN pour FTP ALG :
Dans l'exemple de configuration LSN suivant, FTP ALG est activé pour les abonnés dont l'adresse IP est comprise entre 192.0.2.30 et 192.0.2.100.

```
add ns acl LSN-ACL-1 ALLOW -srcIP 192.0.2.30-192.0.2.100

Done

apply acls

Done

add lsn client LSN-CLIENT-1

Done

```



```
bind lsn client LSN-CLIENT-1  - aclname LSN-ACL

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.10

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -FTP ENABLED

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done
<!--NeedCopy-->
```

Exemple de configuration LSN pour TFTP ALG :

Dans l'exemple de configuration LSN suivant, le mappage indépendant du point de terminaison et le filtrage indépendant du point de terminaison sont activés pour le protocole TFTP (port UDP 69). L'appliance NetScaler active automatiquement l'ALG TFTP pour cette configuration LSN.

```
add lsn client LSN-CLIENT-2

Done

bind lsn client LSN-CLIENT-2 -network 198.51.100.0 -netmask
   255.255.255.0

Done

add lsn pool LSN-POOL-2

Done

bind lsn pool LSN-POOL-2 203.0.113.10-203.0.113.11

Done

add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2
```



```
18
19 Done
20
21 bind lsn group LSN-GROUP-2 -poolname pool1 LSN-POOL-2
22
23 Done
24
25 add lsn appsprofile LSNAPPSPROFILE-TFTP-2 UDP -mapping ENDPOINT-
      INDEPENDENT  - filtering  ENDPOINT-INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile LSNAPPSPROFILE-TFTP-2 69
30
31 Done
32
33 bind lsn group LSN-GROUP-1 -applicationprofilename LSNAPPSPROFILE-TFTP
      -2
34
35 Done
36 <!--NeedCopy-->
```

Passerelle de la couche application pour le protocole PPTP

May 5, 2023

L'appliance NetScaler prend en charge les passerelles ALG (Application Layer Gateway) pour le protocole PPTP (Point-to-Point Tunneling Protocol).

Le PPTP est un protocole réseau qui permet le transfert sécurisé de données d'un client distant vers un serveur d'entreprise en créant un tunnel entre des réseaux de données basés sur TCP/IP. Le protocole PPTP encapsule les paquets PPP dans des paquets IP en vue de leur transmission sur Internet. PPTP établit un tunnel pour chaque paire serveur réseau PPTP (PNS) communiquant - concentrateur d'accès PPTP (PAC). Une fois le tunnel configuré, l'encapsulation de routage générique améliorée (GRE) est utilisée pour échanger des paquets PPP. Un identifiant d'appel dans l'en-tête GRE indique la session à laquelle appartient un paquet PPP particulier.

L'appliance NetScaler reconnaît les paquets PPTP qui arrivent sur le port TCP par défaut, 1723. L'appliance analyse les paquets de contrôle PPTP, traduit l'ID d'appel et attribue une adresse IP NAT. Pour la communication de données bidirectionnelle entre le client et le serveur, l'appliance NetScaler crée une entrée de session LSN basée sur l'ID d'appel du serveur et une session LSN basée

sur l'ID d'appel du client. L'appliance analyse ensuite les paquets de données GRE et traduit les identifiants d'appel sur la base des deux entrées de session LSN.

Pour le protocole PPTP, l'appliance NetScaler inclut également un paramètre de délai d'expiration pour toutes les sessions PPTP LSN inactives. Si une session PPTP LSN est inactive pendant une durée supérieure au paramètre de délai d'expiration, l'appliance NetScaler supprime la session.

Limites :

Les limites de l'ALG PPTP sur une appliance NetScaler sont les suivantes :

- L'ALG PPTP n'est pas pris en charge pour le flux LSN en épingle.
- L'ALG PPTP n'est pas pris en charge pour fonctionner avec n'importe quelle configuration RNAT.
- L'ALG PPTP n'est pas pris en charge dans les clusters NetScaler.

Configuration de PPTP ALG

La configuration de PPTP ALG sur l'appliance NetScaler comprend les tâches suivantes :

- Créez une configuration LSN et activez l'ALG PPTP sur celle-ci. Dans une configuration LSN, le groupe LSN inclut le paramètre ALG PPTP. Pour obtenir des instructions sur la création d'une configuration LSN, voir Étapes de configuration pour LSN.
- (Facultatif) Définissez le délai global pour les sessions LSN PPTP inactives.

Pour activer l'ALG PPTP pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn group <groupname> -clientname <string> [-pptp ( ENABLED |
    DISABLED )]

show lsn group
<!--NeedCopy-->
```

Pour définir le délai d'expiration global pour les sessions PPTP LSN inactives à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set appAlgParam -pptpGreIdleTimeout <positive_integer>

show appAlgParam
<!--NeedCopy-->
```


Exemple :

Dans l'exemple de configuration LSN suivant, l'ALG PPTP est activé pour les abonnés du réseau 192.0.2.0/24.

Le délai d'expiration de la session PPTP LSN inactive est également défini sur 200 secondes.

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -pptp ENABLED

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done

set appAlgParam -pptpGreIdleTimeout 200

Done
<!--NeedCopy-->
```

Passerelle de couche d'application pour le protocole SIP

May 5, 2023

L'utilisation d'un NAT à grande échelle (LSN) avec le protocole SIP (Session Initiation Protocol) est complexe, car les messages SIP contiennent des adresses IP dans les en-têtes SIP ainsi que dans le corps du SIP. Lorsque le LSN est utilisé avec SIP, les en-têtes SIP contiennent des informations sur

l'appelant et le récepteur, et l'appareil traduit ces informations pour les masquer au réseau extérieur. Le corps du SIP contient les informations du protocole SDP (Session Description Protocol), qui incluent les adresses IP et les numéros de port pour la transmission du média.

SIP ALG adhère aux RFC suivants :

- RFC 3261
- RFC 3581
- RFC 456
- RFC 475

> **Remarque**
>
> Le SIP ALG est pris en charge dans une appliance autonome NetScaler, dans une configuration haute disponibilité NetScaler, ainsi que dans une configuration de cluster NetScaler.

Comment fonctionne SIP ALG

La manière dont la traduction des adresses IP est effectuée dépend du type et de la direction du message. Un message peut être l'un des suivants :

- Demande entrante
- Réponse sortante
- Demande sortante
- Réponse entrante

Pour un message sortant, l'adresse IP privée et le numéro de port du client SIP sont remplacés par l'adresse IP publique et le numéro de port appartenant à NetScaler, appelés adresse IP et numéro de port du *pool LSN, spécifiés lors de la configuration*du LSN. Pour un message entrant, l'adresse IP du pool LSN et le numéro de port sont remplacés par l'adresse privée du client. Si le message contient des adresses IP publiques, le NetScaler SIP ALG les conserve. Un sténopé est également créé sur :

- Adresse IP et port du pool LSN pour le compte du client privé, de sorte que les messages qui arrivent à cette adresse IP et à ce port depuis le réseau public sont traités comme des messages SIP.
- Adresse IP et port publics pour le compte des clients publics, de sorte que les messages qui arrivent à cette adresse IP et à ce port depuis le réseau privé sont traités comme des messages SIP.

Lorsqu'un message SIP est envoyé sur le réseau, la passerelle SIP Application Layer Gateway (ALG) collecte des informations à partir du message et traduit les adresses IP des en-têtes suivants en adresses IP du pool LSN :

- Via
- Contacter

- Itinéraire
- Itinéraire record

Dans l'exemple de message de demande SIP suivant, LSN remplace les adresses IP dans les champs d'en-tête pour les masquer au réseau extérieur.

```
1 INVITE adam@10.102.185.156 SIP/2.0 Via: SIP/2.0/UDP 192.170.1.161:62914
      From: eve@10.120.210.3 To: adam@10.102.185.156 Call-ID: a12abcde@10
     .120.210.3 Contact: adam@10.102.185.156 Route: <sip:netscreen@10
     .150.20.3:5060> Record-Route: <sip:netscreen@10.150.20.3:5060>
2 <!--NeedCopy-->
```

Lorsqu'un message contenant des informations SDP arrive, l'ALG SIP collecte des informations à partir du message et traduit les adresses IP des champs suivants en adresses IP et en numéros de port du pool LSN :

- c= (informations de connexion)

  Ce champ peut apparaître au niveau de la session ou du média. Il apparaît dans le format suivant :

  c=<network-type><address-type><connection-address>

  Si l'adresse IP de destination est une adresse IP monodiffusion, l'ALG SIP crée des trous en utilisant l'adresse IP et les numéros de port spécifiés dans le champ m=.

- m= (annonce aux médias)

  Ce champ apparaît au niveau du média et contient la description du média. Il apparaît dans le format suivant :

  m =<media><port><transport><fmt list>

- a = (information about the media field)

  Ce champ peut apparaître au niveau de la session ou du média, au format suivant :

  a =<attribute>

  a =<attribute>:<value>

L'extrait suivant d'un exemple de section SDP montre les champs qui sont traduits pour l'allocation des ressources.

o=user 2344234 55234434 DANS IP4 10.150.20.3

C = dans IP4 10.150.20.3

m=audio 43249 RTP/AVP 0

Le tableau suivant montre comment la charge utile SIP est traduite.

Requête entrante (du public au privé)	par :	Aucun
	À partir de :	Aucun
	ID d'appel :	Aucun
	Par :	Aucun
	URI de requête :	Remplacer l'adresse IP du pool LSN par une adresse IP privée
	Personne à contacter :	Aucun
	Itinéraire record	Aucun
	Parcours :	Aucun
Réponse sortante (du privé vers le public)	par :	Aucun
	À partir de :	Aucun
	ID d'appel :	Aucun
	Par :	Aucun
	URI de requête :	Remplacer l'adresse IP privée par l'adresse IP du pool LSN
	Personne à contacter :	Remplacer l'adresse IP privée par l'adresse IP du pool LSN
	Itinéraire record	Aucun
	Parcours :	Aucun
Requête sortante (du privé vers le public)	par :	Aucun
	À partir de :	Aucun
	ID d'appel :	Aucun
	Par :	Remplacer l'adresse IP privée par l'adresse IP du pool LSN
	URI de requête :	Aucun
	Personne à contacter :	Remplacer l'adresse IP privée par l'adresse IP du pool LSN

	Itinéraire record	Aucun
	Parcours :	Aucun
Réponse entrante (du public au privé)	par :	Aucun
	À partir de :	Aucun
	ID d'appel :	Aucun
	Par :	Remplacer l'adresse IP du pool LSN par une adresse IP privée
	URI de requête :	Aucun
	Personne à contacter :	Conserver l'adresse IP publique, si elle est présente
	Itinéraire record	Aucun
	Parcours :	Aucun

Limites du SIP ALG

Un SIP ALG présente les limites suivantes :

- Seule la charge utile SDP est prise en charge.
- Les éléments suivants ne sont pas pris en charge :
  - Adresses IP de multidiffusion
  - SDP crypté
  - EXPÉDITION TLS
  - Traduction du FQDN
  - Authentification de couche SIP
  - TD/Clotionnement
  - Carrosserie en plusieurs parties
  - Messages SIP sur le réseau IPv6
  - Pliage en ligne

Clients SIP et serveurs proxy testés

Les clients SIP et le serveur proxy suivants ont été testés avec SIP ALG :

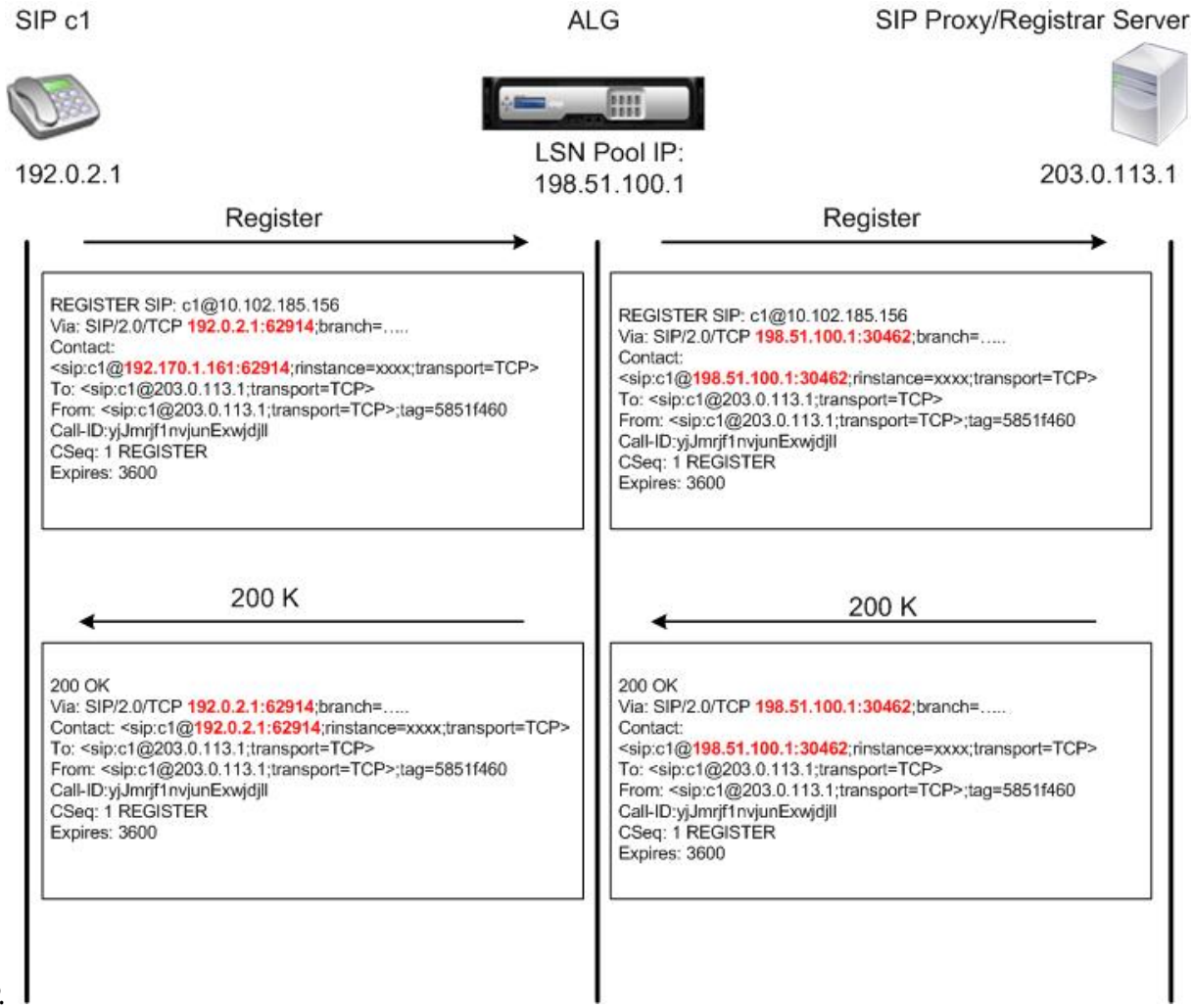
- **Clients SIP :** X-Lite, Zoiper, Ekiga. Avaya

- **Serveur proxy : OpenSIPS**

Scénario LSN SIP : Proxy SIP en dehors du réseau privé (réseau public)

Enregistrement du client SIP

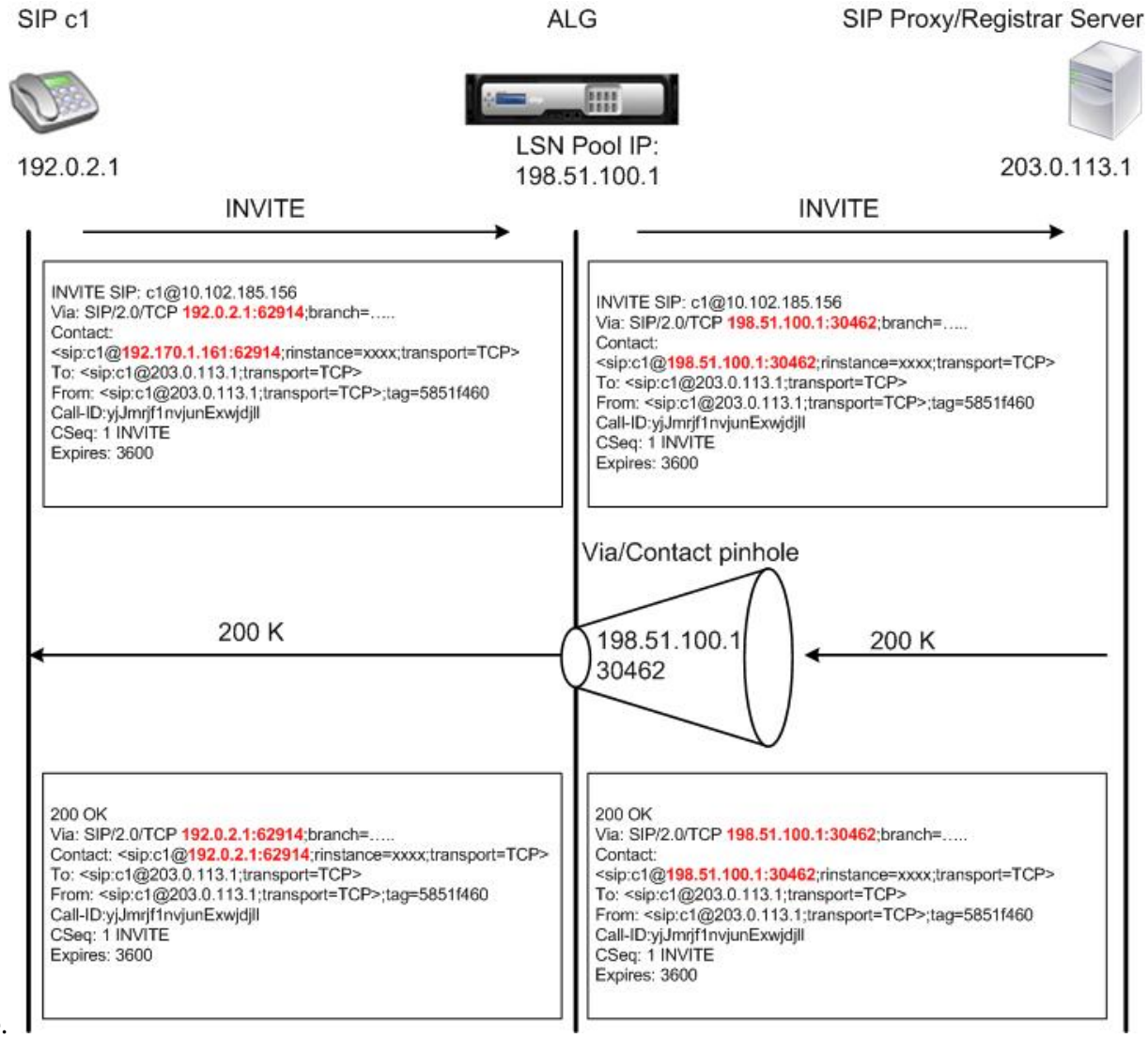
Pour un appel SIP classique, le client SIP doit s'enregistrer auprès du bureau d'enregistrement SIP en composant une demande REGISTER et en l'envoyant au bureau d'enregistrement SIP. L'ALG SIP de l'appliance NetScaler intercepte la demande, remplace l'adresse IP et le numéro de port de la demande par l'adresse IP et le numéro de port du pool LSN fournis dans la configuration LSN, puis transmet la demande au bureau d'enregistrement SIP. L'ALG SIP ouvre ensuite un sténopé dans la configuration de NetScaler pour permettre la poursuite des communications SIP entre le client SIP et le bureau d'enregistrement SIP. Le bureau d'enregistrement SIP envoie une réponse 200 OK au client SIP via l'adresse IP et le numéro de port du pool LSN. L'appliance NetScaler capture cette réponse dans le sténopé, et l'ALG SIP remplace l'en-tête SIP en replaçant les champs SIP Contact, Via, Route et Record-Route d'origine dans le message. L'ALG SIP transmet ensuite le message au client SIP. La figure suivante montre comment SIP ALG utilise le LSN dans un flux d'enregistrement d'appels



SIP.

Appels sortants

Un appel SIP est lancé avec un message SIP INVITE envoyé du réseau interne vers le réseau externe. L'ALG SIP exécute la NAT sur les adresses IP et les numéros de port dans les champs d'en-tête SIP Via, Contact, Route et Record-Route, en les remplaçant par l'adresse IP et le numéro de port du pool LSN. Le LSN stocke ces mappages pour les messages SIP suivants dans l'appel SIP. L'ALG SIP ouvre ensuite des trous séparés dans la configuration de NetScaler pour autoriser le SIP et le multimédia à passer par l'appliance NetScaler sur les ports assignés dynamiquement spécifiés dans les en-têtes SDP et SIP. Lorsqu'un message 200 OK arrive au NetScaler, il est capturé par l'un des trous d'épingle créés. L'ALG SIP remplace l'en-tête SIP en restaurant les champs SIP Contact, Via, Route et Record-Route d'origine, puis transmet le message au client SIP in-

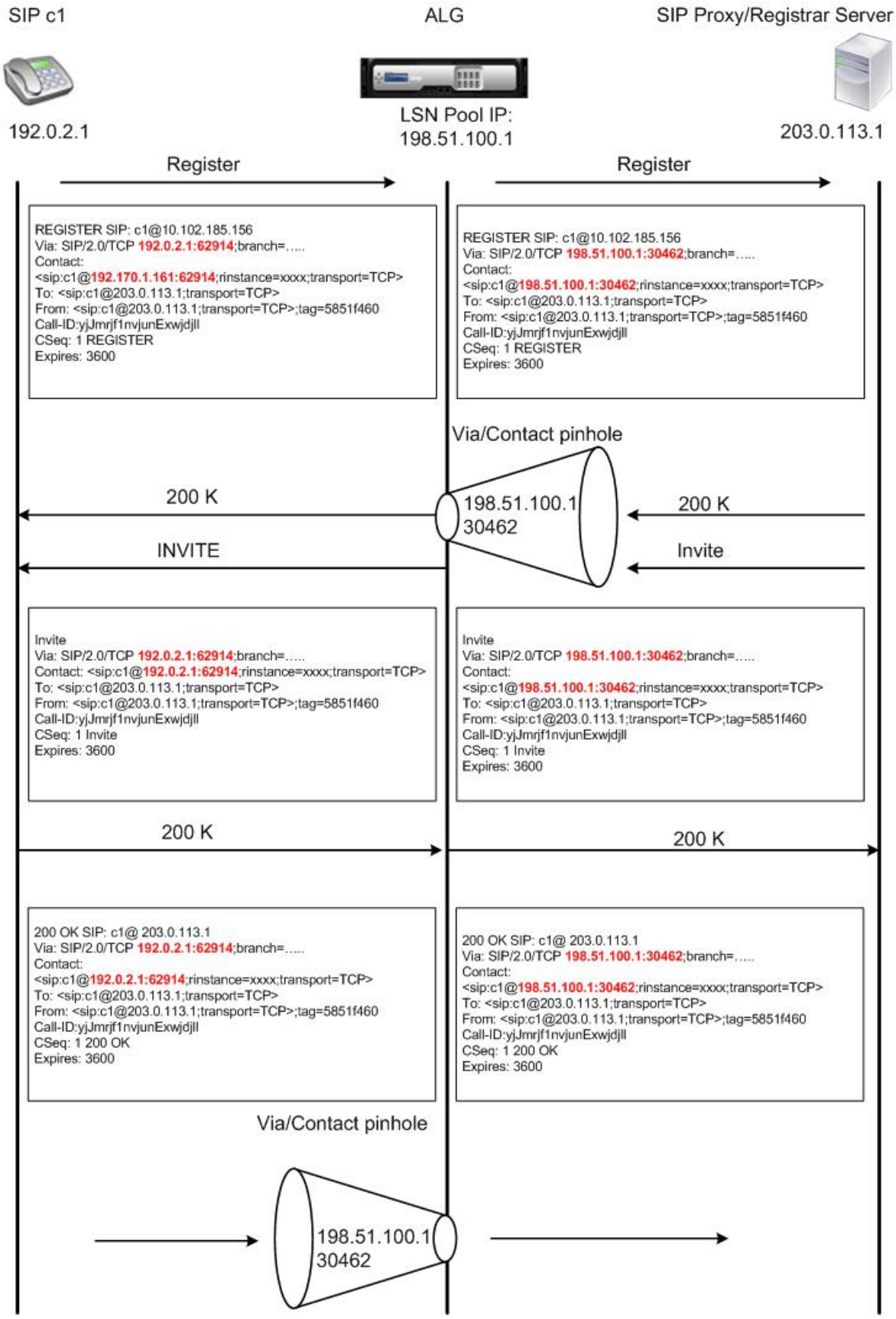


terne.

Appels entrants

Un appel entrant SIP est lancé avec un message SIP INVITE du client externe vers le réseau interne. Le bureau d'enregistrement SIP transmet le message INVITE au client SIP du réseau interne, à l'aide du sténopé créé lors de l'enregistrement du client SIP interne auprès du bureau d'enregistrement SIP.

L'ALG SIP exécute la NAT sur les adresses IP LSN et les numéros de port dans les champs d'en-tête SIP Via, Contact, Route et Record-Route, en les traduisant en adresse IP et en numéro de port du client SIP interne, puis transmet la demande au client SIP. Lorsque le message de réponse 200 OK envoyé par le client SIP interne arrive à l'appliance NetScaler, l'ALG SIP exécute un NAT sur les adresses IP et les numéros de port des champs d'en-tête SIP Via, Contact, Route et Record-Route, les traduit en adresse IP et en numéro de port du pool LSN, transmet le message de réponse au bureau d'enregistrement SIP, puis ouvre un sténopé dans le sens sortant pour poursuivre la communication



SIP.

Fin d'appel

Le message BYE met fin à un appel. Lorsque l'appareil reçoit un message BYE, il traduit les champs d'en-tête du message comme il le fait pour tout autre message. Mais comme le récepteur doit accuser réception d'un message BYE avec un 200 OK, l'ALG retarde le démontage de l'appel de 15 secondes pour laisser le temps de transmettre le 200 OK.

Appel entre clients d'un même réseau

Lorsque le client A et le client B du même réseau lancent un appel, les messages SIP sont routés via le proxy SIP du réseau extérieur. L'ALG SIP traite l'INVITE du client A comme un appel sortant normal. Comme le client B se trouve sur le même réseau, le proxy SIP renvoie l'INIVITE à l'appliance NetScaler. L'ALG SIP examine le message INIVITE, détermine qu'il contient l'adresse IP NAT du client A et remplace cette adresse par l'adresse IP privée du client A avant d'envoyer le message au client B. Une fois l'appel établi entre les clients, NetScaler n'est pas impliqué dans la transmission multimédia entre les clients.

Autres scénarios LSN SIP : Proxy SIP au sein du réseau privé

Si vous souhaitez héberger le serveur proxy SIP sur le réseau privé, Citrix vous recommande d'effectuer l'une des opérations suivantes :

- Configurez un mappage LSN statique pour le proxy SIP privé. Pour plus d'informations, reportez-vous à la section Configuration de cartes LSN statiques. Assurez-vous que le port NAT est le même que celui configuré dans le profil ALG SIP.
- Configurez le serveur proxy SIP dans une zone démilitarisée (DMZ).

Figure 1. Enregistrement des appels SIP

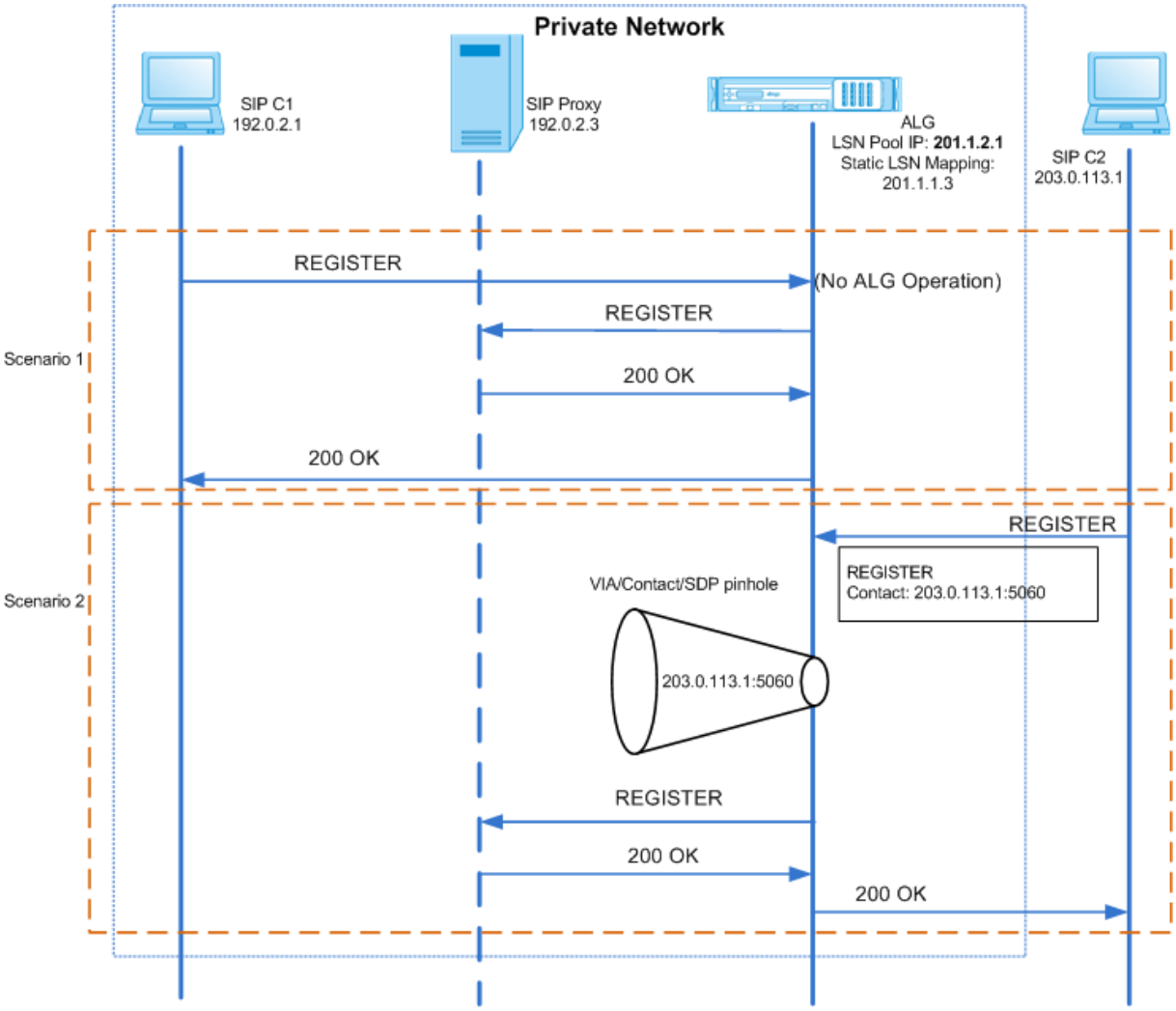
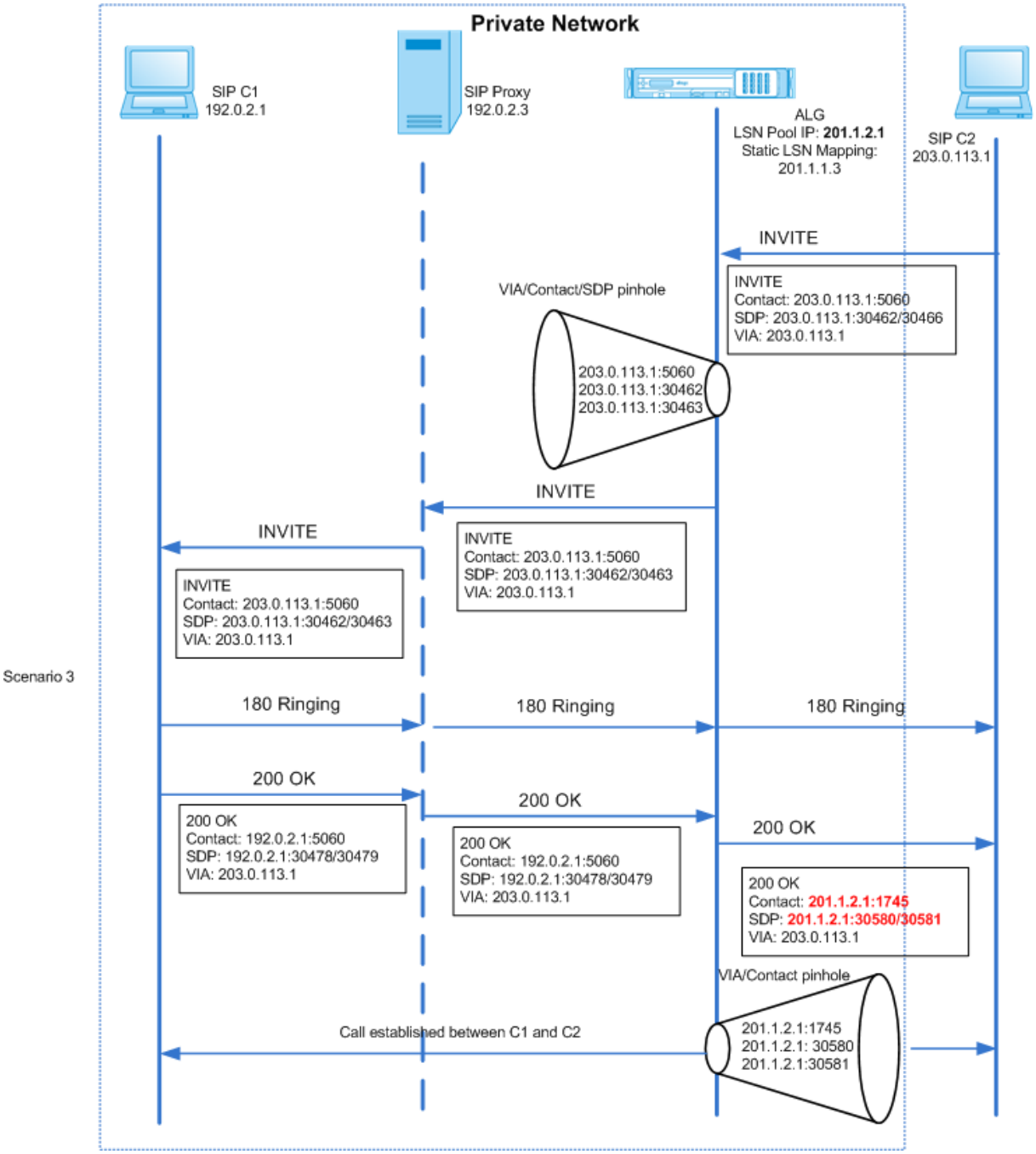


Figure 2. Flux d'appels entrants SIP



Les figures 1 et 2 présentent les scénarios suivants :

- Scénario 1 : Le client SIP du réseau privé s'enregistre auprès du serveur proxy SIP du même réseau. Les opérations ALG ne sont pas effectuées car le client SIP et le serveur proxy SIP se trouvent sur le même réseau.
- Scénario 2 : Le client SIP du réseau public s'enregistre auprès du serveur proxy SIP du réseau privé. Le message REGISTER du client SIP public est envoyé à l'appliance NetScaler à l'aide du mappage LSN statique configuré sur l'appliance, et l'appliance crée un sténopé pour d'autres

opérations SIP.

- Scénario 3 : Flux d'appels entrants SIP. Un appel entrant SIP est lancé avec un message SIP INVITE du réseau externe vers le réseau interne. L'appliance NetScaler reçoit le message INVITE du client SIP C2, qui se trouve sur le réseau externe, via les cartes LSN statiques configurées sur l'appliance NetScaler.
  L'appliance crée un trou d'épingle et transmet le message INVITE au proxy SIP. Le proxy SIP transmet ensuite le message INVITE au client SIP C1 du réseau interne. Le client SIP C1 envoie ensuite 180 et 200 messages OK au proxy SIP, qui à son tour transmet le message au client SIP C2 via l'appliance NetScaler.
  Lorsque le message de réponse 200 OK envoyé par le client SIP interne C1 arrive à NetScaler, l'ALG SIP exécute un NAT sur les adresses IP et les numéros de port dans les champs d'en-tête SIP Via, Contact, Route et Record-Route, et dans les champs SDP, en les remplaçant par l'adresse IP et le numéro de port du pool LSN. L'ALG SIP transmet ensuite le message de réponse au client SIP C2 et ouvre un sténopé dans la direction sortante pour une communication SIP ultérieure.

Support pour les journaux d'audit

Vous pouvez consigner les informations ALG dans le cadre de la journalisation LSN en activant ALG dans la configuration de journalisation d'audit LSN. Pour plus d'informations sur la journalisation LSN, consultez Logging and Monitoring LSN. Un message de journal pour une entrée ALG dans le journal LSN contient les informations suivantes :

- Horodatage
- Type de message SIP (par exemple, demande SIP)
- Adresse IP source et port du client SIP
- Adresse IP de destination et port du proxy SIP
- Adresse IP et port NAT
- Méthode SIP
- Numéro de séquence
- Si le client SIP est enregistré ou non
- Nom d'utilisateur et domaine de l'appelant
- Nom d'utilisateur et domaine du destinataire

Exemple de journal d'audit :

Demande :

```
1 07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
    ALG_SIP_INFO_PACKET_EVENT 169 0 : Infomsg: "SIP request" - Group: g2
     - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. - Transport
    : TCP - Source_IP: 192.169.1.165 - Source_port: 57952 -
    Destination_IP: 10.102.185.156 - Destination_port: 5060 - Natted_IP:
     10.102.185.191 - Natted_port: 10313 - Method: REGISTER -
```



```
    Sequence_Number: 3060 - Register: YES - Content_Type: -
    Caller_user_name: 156_pvt_1 - Callee_user_name: 156_pvt_1 -
    Caller_domain_name: - Callee_domain_name: -
<!--NeedCopy-->
```

Réponse :

```
07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
    ALG_SIP_INFO_PACKET_EVENT 170 0 : Infomsg: "SIP response" - Group:
    g2 - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. -
    Transport: TCP - Response_code 200 - Source_IP: 10.102.185.156 -
    Source_port: 5060 - Destination_IP: 192.169.1.165 - Destination_port
    : 57952 - Natted_IP: 10.102.185.191 - Natted_port: 10313 -
    Sequence_Number: 3060 - Content_Type: - Caller_user_name: 156_pvt_1
    - Callee_user_name: 156_pvt_1 - Caller_domain_name: -
    Callee_domain_name: -
<!--NeedCopy-->
```

Configuration de SIP ALG

Vous devez configurer le SIP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, voir Étapes de configuration pour LSN. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez les paramètres suivants lors de l'ajout du profil d'application LSN :
  - Regroupement d'adresses IP = APPARIÉ
  - Mappage des adresses et des ports = INDÉPENDANT DU POINT DE TERMINAISON
  - Filtrage = INDÉPENDANT DU POINT DE TERMINAISON

Important : pour que l'ALG SIP fonctionne, une configuration NAT à cône complet est obligatoire.

Exemple :

```
add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT
<!--NeedCopy-->
```

- Créez un profil SIP ALG et assurez-vous de définir la plage de ports source ou la plage de ports de destination.

Exemple :

```
add lsn sipalgprofile sipalgprofile_tcp -sipsrcportrange 1-65535 -
    sipdstportrange 5060 -openViaPinhole ENABLED -openRecordRoutePinhole
     ENABLED  - sipTransportProtocol TCP
```



```
<!--NeedCopy-->
```

- Définissez SIP ALG = ENABLED lors de la création du groupe LSN.

Exemple :

```
add lsn group g1 -clientname c1 -sipalg ENABLED
<!--NeedCopy-->
```

- Liez le profil SIP ALG au groupe LSN.

Exemple de configuration SIP ALG :

L'exemple de configuration suivant montre comment créer une configuration LSN simple avec un seul réseau d'abonnés, une adresse IP NAT LSN unique, un paramètre spécifique SIP ALG et configurer SIP ALG :

```
add lsn pool p1

Done

bind lsn pool p1 10.102.185.190

Done

add lsn client c1

Done

bind lsn client c1 -network 192.170.1.0 -netmask 255.255.255.0

Done

add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

add lsn appsprofile app_udp UDP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

bind lsn appsprofile app_tcp 1-65535

Done
```



```
28
29 bind lsn appsprofile app_udp 1-65535
30
31 Done
32
33 add lsn sipalgprofile sipalgprofile_tcp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED  -
      sipTransportProtocol TCP
34
35 Done
36
37 add lsn sipalgprofile sipalgprofile_udp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED -
      sipTransportProtocol UDP
38
39 Done
40
41 add lsn group g1 -clientname c1 -sipalg ENABLED
42
43 Done
44
45 bind lsn group g1 -poolname p1
46
47 Done
48
49 bind lsn group g1 -appsprofilename app_tcp
50
51 Done
52
53 bind lsn group g1 -appsprofilename app_udp
54
55 Done
56
57 bind lsn group g1 -sipalgprofilename sipalgprofile_tcp
58
59 Done
60
61 bind lsn group g1 -sipalgprofilename sipalgprofile_udp
62
63 Done
64 <!--NeedCopy-->
```


Passerelle de couche application pour le protocole RTSP

July 18, 2023

Le protocole RTSP (Real Time Streaming Protocol) est un protocole au niveau de l'application pour le transfert de données multimédia en temps réel. Utilisé pour établir et contrôler des sessions multimédia entre les points de terminaison, le RTSP est un protocole de canal de contrôle entre le client multimédia et le serveur multimédia. La communication classique se fait entre un client et un serveur de streaming multimédia.

La diffusion de contenu multimédia d'un réseau privé vers un réseau public nécessite la traduction des adresses IP et des numéros de port sur le réseau. Les fonctionnalités de NetScaler incluent une passerelle de couche d'application (ALG) pour RTSP, qui peut être utilisée avec un NAT à grande échelle (LSN) pour analyser le flux multimédia et apporter les modifications nécessaires pour garantir que le protocole continue de fonctionner sur le réseau.

La manière dont la traduction des adresses IP est effectuée dépend du type et de la direction du message, ainsi que du type de média pris en charge par le déploiement client-serveur. Les messages sont traduits comme suit :

- Requête sortante : adresse IP privée vers une adresse IP publique appartenant à NetScaler appelée adresse IP du pool LSN.
- Réponse entrante : adresse IP du pool LSN vers adresse IP privée.
- Demande entrante : aucune traduction.
- Réponse sortante : adresse IP privée vers l'adresse IP du pool LSN.

> **Remarque**
>
> L'ALG RTSP est pris en charge dans une appliance autonome NetScaler, dans une configuration haute disponibilité NetScaler, ainsi que dans une configuration de cluster NetScaler.

Limites de RTSP ALG

Le RTSP ALG ne prend pas en charge les éléments suivants :

- Sessions RTSP multidiffusion
- Session RTSP via UDP
- Partitionnement TD/Admin
- Authentification RSTP
- Tunneling HTTP

Scénario RTSP et LSN

Généralement, une demande RTSP SETUP indique comment un seul flux multimédia doit être transporté. La demande contient l'URL du flux multimédia et un spécificateur de transport. Ce spécificateur inclut généralement un port local pour recevoir des données RTP (audio ou vidéo) et un autre pour recevoir des données RTCP (méta-informations). La réponse du serveur confirme généralement les paramètres choisis et complète les parties manquantes, telles que les ports choisis par le serveur. Chaque flux multimédia doit être configuré à l'aide de la commande SETUP avant qu'une demande de lecture agrégée puisse être envoyée.

Dans une communication RTSP classique, le client multimédia du réseau public envoie une demande de configuration au serveur multimédia du réseau privé. RSTP ALG intercepte la demande et, dans le flux multimédia, remplace l'adresse IP publique et le numéro de port par l'adresse IP du pool LSN et le numéro de port LSN.

Le serveur multimédia du réseau privé utilise l'adresse IP du pool LSN et le numéro de port LSN pour envoyer une réponse 200 OK au client multimédia du réseau public. L'ALG NetScaler RTSP intercepte la réponse et remplace l'adresse IP du pool LSN et le numéro de port LSN par l'adresse IP publique et le numéro de port du client multimédia.

Configuration de RTSP ALG

Configurez RTSP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, voir Étapes de configuration pour LSN. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez le **type NAT comme DETERMINSTIC** ou DYNAMIC lors de l'ajout du pool LSN.
- Définissez les paramètres suivants lors de l'ajout du profil d'application LSN :
  - Regroupement d'adresses IP = PAIRED
  - Mappage des adresses et des ports = ENDPOINT-INDEPENDENT
  - Filtrage = INDÉPENDANT DU POINT DE TERMINAISON
- Créez un profil RTSP ALG et liez le profil RTSP ALG au groupe LSN

Exemple de configuration RTSP ALG :

L'exemple de configuration suivant montre comment créer une configuration LSN simple avec un réseau abonné unique, une adresse IP NAT LSN unique et des paramètres ALG RTSP :

```
enable ns feature WL SP LB CS LSN

Done

add lsn pool pool1 -nattype DETERMINISTIC

Done
```



```
8
9  bind lsn pool pool1 10.102.218.246
10
11 Done
12
13 add lsn client client1
14
15 Done
16
17 bind lsn client client1 -network 200.200.200.11 -netmask 255.255.255.0
18
19 Done
20
21 add lsn appsprofile app1 TCP -ippooling PAIRED -mapping ENDPOINT-
      INDEPENDENT -filtering ENDPOINT-INDEPENDENT
22
23 Done
24
25 add lsn appsprofile app2 UDP -ippooling PAIRED -mapping ENDPOINT-
      INDEPENDENT -filtering ENDPOINT-INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile app1 1-65535
30
31 Done
32
33 bind lsn appsprofile app2 1-65535
34
35 Done
36
37 add lsn rtspalgprofile rtspalgprofiledefault -rtspIdleTimeout 1000 -
      rtspportrange 554
38
39 Done
40
41 add lsn group group1 -clientname client1 -nattype DETERMINISTIC -
      portblocksize 512 -rtspalg ENABLED
42
43 Done
44
45 bind lsn group group1 -poolname pool1
46
47 Done
48
```



```
bind lsn group group1 -appsprofilename app1

Done

bind lsn group group1 -appsprofilename app2

Done

bind lsn group group1 -rtspalgprofilename rtspalgprofiledefault

Done
<!--NeedCopy-->
```

Passerelle de la couche application pour le protocole IPsec

May 5, 2023

Si la communication entre deux périphériques réseau (par exemple, client et serveur) utilise le protocole IPsec, le trafic IKE (via UDP) utilise des champs de port, mais pas le trafic ESP (Encapsulating Security Payload). Si un périphérique NAT sur le chemin attribue la même adresse IP NAT (mais des ports différents) à deux clients ou plus situés sur la même destination, le périphérique NAT est incapable de distinguer et d'acheminer correctement le trafic ESP de retour qui ne contient pas d'informations de port. Par conséquent, le trafic IPSec ESP échoue au niveau du périphérique NAT.

Les points de terminaison IPsec compatibles NAT-T détectent la présence d'un périphérique NAT intermédiaire pendant la phase 1 de l'IKE et basculent vers le port UDP 4500 pour tout le trafic IKE et ESP suivant (encapsulation de l'ESP dans UDP). Sans support NAT-T sur les points de terminaison IPsec homologues, le trafic ESP protégé par IPsec est transmis sans aucune encapsulation UDP. Par conséquent, le trafic IPSec ESP échoue au niveau du périphérique NAT.

L'appliance NetScaler prend en charge la fonctionnalité IPSec Application Layer Gateway (ALG) pour les configurations NAT à grande échelle. L'ALG IPsec traite le trafic IPsec ESP et conserve les informations de session afin que le trafic n'échoue pas lorsque les points de terminaison IPsec ne prennent pas en charge le NAT-T (encapsulation UDP du trafic ESP).

Comment fonctionne IPSec ALG

Un ALG IPsec surveille le trafic IKE entre un client et le serveur et n'autorise qu'un seul échange de messages IKE de phase 2 entre le client et le serveur à la fois.

Une fois que les paquets ESP bidirectionnels sont reçus pour un flux particulier, l'ALG IPsec crée une session NAT pour ce flux particulier afin que le trafic ESP suivant puisse circuler sans problème. Le

trafic ESP est identifié par des indices de paramètres de sécurité (SPI), qui sont uniques pour un flux et pour chaque direction. Un ALG IPsec utilise des SPI ESP à la place des ports source et de destination pour effectuer un NAT à grande échelle.

Si une porte ne reçoit aucun trafic, elle expire. Après expiration du délai imparti pour les deux portes, un autre échange IKE de phase 2 est autorisé.

Délais d'expiration d'IPsec ALG

L'ALG IPsec sur une appliance NetScaler possède trois paramètres de délai d'expiration :

- **Délai d'expiration de la porte ESP**. Durée maximale pendant laquelle l'appliance NetScaler bloque une porte ALG IPsec pour un client particulier sur une adresse IP NAT spécifique pour un serveur donné si aucun trafic ESP bidirectionnel n'est échangé entre le client et le serveur.
- **Délai d'expiration de la session IKE.** Durée maximale pendant laquelle l'appliance NetScaler conserve les informations de session IKE avant de les supprimer s'il n'y a pas de trafic IKE pour cette session.
- **Délai d'expiration de la session ESP**. Durée maximale pendant laquelle l'appliance NetScaler conserve les informations de session ESP avant de les supprimer s'il n'y a pas de trafic ESP pour cette session.

Points à prendre en compte avant de configurer IPsec ALG

Avant de commencer à configurer IPsec ALG, tenez compte des points suivants :

- Vous devez comprendre les différents composants du protocole IPsec.
- L'ALG IPsec n'est pas pris en charge pour les configurations DS-Lite et NAT64 à grande échelle.
- L'ALG IPsec n'est pas pris en charge pour le flux LSN en épingle.
- L'ALG IPsec ne fonctionne pas avec les configurations RNAT.
- L'ALG IPsec n'est pas pris en charge dans les clusters NetScaler.

Étapes de configuration

La configuration d'IPsec ALG pour un NAT44 à grande échelle sur une appliance NetScaler comprend les tâches suivantes :

- **Créez un profil d'application LSN et liez-le à la configuration LSN.** Définissez les paramètres suivants lors de la configuration d'un profil d'application :
  - Protocole=UDP
  - Regroupement d'adresses IP = APPARIÉ
  - Port=500

Liez le profil d'application au groupe LSN d'une configuration LSN. Pour obtenir des instructions sur la création d'une configuration LSN, voir Étapes de configuration pour LSN.

- **Créez un profil IPSec ALG**. Un profil IPsec inclut différents délais d'expiration IPsec, tels que le délai d'expiration de session IKE, le délai d'expiration de session ESP et le délai d'expiration de porte ESP. Vous liez un profil ALG IPsec à un groupe LSN. Un profil ALG IPsec possède les paramètres par défaut suivants :
  - Délai d'expiration de la session IKE = 60 minutes
  - Délai d'expiration de la session ESP = 60 minutes
  - Délai d'expiration de la porte ESP = 30 secondes
- **Liez le profil ALG IPsec à la configuration LSN**. L'ALG IPsec est activé pour une configuration LSN lorsque vous liez un profil ALG IPsec à la configuration LSN. Liez le profil ALG IPsec à la configuration LSN en définissant le paramètre de profil ALG IPsec sur le nom du profil créé dans le groupe LSN. Un profil ALG IPsec peut être lié à plusieurs groupes LSN, mais un groupe LSN ne peut avoir qu'un seul profil ALG IPsec.

Pour créer un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn appsprofile <appsprofilename> UDP -ippooling PAIRED

show lsn appsprofile
<!--NeedCopy-->
```

Pour lier le port de destination au profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

Pour lier un profil d'application LSN à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname> -appsprofilename <string>

```



```
show lsn group
<!--NeedCopy-->
```

Pour créer un profil ALG IPsec à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ipsecalg profile <name> [-ikeSessionTimeout <positive_integer>] [-
    espSessionTimeout <positive_integer>] [-espGateTimeout <
    positive_integer>] [-connfailover ( ENABLED | DISABLED)

show ipsecalg profile <name>
<!--NeedCopy-->
```

Pour lier un profil ALG IPsec à une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname> -poolname <string> - ipsecAlgProfile <string
    >

show lsn group <name>
<!--NeedCopy-->
```

Pour créer un profil d'application LSN et le lier à une configuration LSN à l'aide de l'interface graphique

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur l'onglet **Application**, ajoutez un profil d'application LSN et liez-le à un groupe LSN.

Pour créer un profil ALG IPsec à l'aide de l'interface graphique**

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur l'onglet **IPSEC ALG**, puis ajoutez un profil ALG IPsec.

Pour lier un profil ALG IPsec à une configuration LSN à l'aide de l'interface graphique**

1. Accédez à **Système** > **NAT à grande échelle** > **Groupe LSN**, ouvrez le groupe LSN.
2. Dans **Paramètres avancés**, cliquez sur **+ Profil ALG IPSEC pour lier le profil** ALG IPsec créé au groupe LSN.

Exemple de configuration

Dans l'exemple de configuration NAT44 à grande échelle suivant, l'ALG IPsec est activé pour les abonnés du réseau 192.0.2.0/24. Le profil ALG IPsec IPSECALGPROFILE-1 avec différents paramètres de délai d'expiration IPsec est créé et est lié au groupe LSN Groupe LSN -1.

Exemple de configuration :

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.9

Done

add lsn appsprofile LSN-APPSPROFILE-1 UDP -ippooling PAIRED

Done

bind lsn appsprofile LSN-APPSPROFILE-1 500

Done

add ipsecalg profile  IPSECALGPROFILE-1 -ikeSessionTimeout 45  -
   espSessionTimeout 40  - espGateTimeout 20 -connfailover ENABLED

Done

bind lsn group LSN-GROUP-1 -appsprofilename LSN-APPSPROFILE-1

Done

bind lsn group LSN-GROUP-1 -poolname LSN-POOL-1

Done

bind lsn group LSN-GROUP-1 - ipsecAlgProfile IPSECALGPROFILE-1
```



```
38
39 Done
40 <!--NeedCopy-->
```

Enregistrement et surveillance du LSN

May 5, 2023

Vous pouvez enregistrer les informations LSN pour diagnostiquer, résoudre les problèmes et respecter les exigences légales. Vous pouvez surveiller les performances de la fonctionnalité LSN en utilisant les compteurs statistiques LSN et en affichant les sessions LSN en cours.

Journalisation du LSN

L'enregistrement des informations LSN est l'une des fonctions importantes requises par les FAI pour répondre aux exigences légales et pour identifier la source du trafic à tout moment.

Une appliance NetScaler enregistre les entrées de mappage LSN et les sessions LSN créées ou supprimées pour chaque groupe LSN. Vous pouvez contrôler la journalisation des informations LSN pour un groupe LSN à l'aide des paramètres de journalisation et de journalisation de session du groupe LSN. Il s'agit de paramètres au niveau du groupe qui sont désactivés par défaut. L'appliance NetScaler enregistre les sessions LSN pour un groupe LSN uniquement lorsque les paramètres de journalisation et de journalisation de session sont activés.

Le tableau suivant présente le comportement de journalisation d'un groupe LSN pour différents paramètres de journalisation et de journalisation de session.

Journalisation	Journalisation des sessions	Comportement d'enregistrement
Activé	Activé	Consigne les entrées de mappage LSN ainsi que les sessions LSN.
Activé	Désactivé	Consigne les entrées de mappage LSN mais pas les sessions LSN.
Désactivé	Activé	N'enregistre ni les entrées de mappage ni les sessions LSN.

Un message de journal pour une entrée de mappage LSN contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal.
- Horodatage
- Type d'entrée (MAPPING)
- Si l'entrée de mappage LSN a été créée ou supprimée
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole
- L'adresse IP de destination, le port et l'ID du domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session LSN contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal.
- Horodatage
- Type d'entrée (SESSION)
- Si la session LSN est créée ou supprimée
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

L'appliance utilise son syslog et son framework de journaux d'audit existants pour enregistrer les informations LSN. Vous devez activer la journalisation LSN au niveau global en activant le paramètre LSN dans les entités d'action NSLOG et SYLOG associées. Lorsque le paramètre Logging est activé, l'appliance NetScaler génère des messages de journal relatifs aux mappages LSN et aux sessions LSN de ce groupe LSN. L'appliance envoie ensuite ces messages de journal aux serveurs associés aux entités d'action NSLOG et SYSLOG.

Pour enregistrer les informations du LSN, Citrix recommande :

- Enregistrement des informations LSN sur des serveurs de journaux externes plutôt que sur l'appliance NetScaler. La journalisation sur des serveurs externes permet d'optimiser les performances lorsque l'appliance crée de grandes quantités d'entrées de journal LSN (de l'ordre de millions).

- Utilisation de SYSLOG sur TCP ou NSLOG. Par défaut, SYSLOG utilise le protocole UDP et NSLOG utilise uniquement le protocole TCP pour transférer les informations du journal vers les serveurs de journaux. Le protocole TCP est plus fiable que le protocole UDP pour transférer des données complètes.

  Remarque :

  - Le SYSLOG généré sur l'appliance NetScaler est envoyé dynamiquement aux serveurs de journaux externes.
  - Lorsque vous utilisez SYSLOG sur TCP, si la connexion TCP est interrompue ou si le serveur SYSLOG est occupé, les appliances NetScaler stockent les journaux dans la mémoire tampon et envoient les données une fois la connexion active.

Pour plus d'informations sur la configuration de la journalisation, voir Journalisation des audits.

La configuration de la journalisation LSN comporte les tâches suivantes :

- **Configuration de l'appliance NetScaler pour la journalisation.** Cette tâche implique la création et la définition de diverses entités et paramètres de l'appliance NetScaler :
  - **Créez une configuration de journalisation d'audit SYSLOG ou NSLOG.** La création d'une configuration de journalisation des audits implique les tâches suivantes :
    * Créez une action d'audit NSLOG ou SYSLOG et activez le paramètre LSN. Les actions d'audit spécifient les adresses IP des serveurs de journaux.
    * Créez une politique d'audit SYSLOG ou NSLOG et liez l'action d'audit à la politique d'audit. Les actions d'audit spécifient les adresses IP des serveurs de journaux. Vous pouvez éventuellement définir la méthode de transport des messages de journal envoyés aux serveurs de journaux externes. Par défaut, UDP est sélectionné, vous pouvez définir la méthode de transport comme TCP pour un mécanisme de transport fiable. Liez la politique d'audit à l'ensemble du système.
    * Créez une politique d'audit SYSLOG ou NSLOG et liez l'action d'audit à la politique d'audit.
    * Liez la politique d'audit à l'ensemble du système.
      Remarque : Pour une configuration de journalisation d'audit existante, activez simplement le paramètre LSN pour enregistrer les informations LSN sur le serveur spécifié par l'action d'audit.
  - **Activez les paramètres de journalisation et de journalisation de session.** Activez les paramètres de journalisation et de journalisation de session lorsque vous ajoutez des groupes LSN ou après avoir créé les groupes. L'appliance NetScaler génère des messages de journal liés à ces groupes LSN et les envoie au serveur des actions d'audit pour lesquelles le paramètre LSN est activé.
- **Configuration des serveurs de journaux.** Cette tâche implique l'installation des packages SYSLOG ou NSLOG sur les serveurs souhaités. Cette tâche implique également de spécifier l'adresse NSIP de l'appliance NetScaler dans le fichier de configuration de SYSLOG ou NSLOG. La spéci-

fication de l'adresse NSIP permet au serveur d'identifier les informations du journal envoyées par l'appliance NetScaler pour les stocker dans un fichier journal.

Pour plus d'informations sur la configuration de la journalisation, voir Journalisation des audits.

Configuration SYSLOG à l'aide de l'interface de ligne de commande

Pour créer une action de serveur SYSLOG pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
    <logLevel>... [-transport (TCP)] [-lsn ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Pour créer une politique de serveur SYSLOG pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add audit syslogPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Pour lier une politique de serveur SYSLOG à l'ensemble du système pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind system global [<policyName> [-priority <positive_integer>]]
<!--NeedCopy-->
```

Configuration de SYSLOG à l'aide de l'utilitaire de configuration

Pour configurer une action du serveur SYSLOG pour la journalisation LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Systèmes** > **Audit** > **Syslog** et, dans l'onglet Serveurs, ajoutez un nouveau serveur d'audit ou modifiez un serveur existant.
2. Pour activer la journalisation LSN, sélectionnez l'option de **journalisation NAT à grande échelle** .
3. (Facultatif) Pour activer SYSLOG sur TCP, sélectionnez l'option de journalisation **TCP** .

Pour configurer une politique de serveur SYSLOG pour la journalisation LSN à l'aide de l'utilitaire de configuration

Accédez à **Systèmes** > **Audit** > **Syslog** et, dans l'onglet **Politiques**, ajoutez une nouvelle politique ou modifiez une politique existante.

Pour lier une politique de serveur SYSLOG à l'ensemble du système pour la journalisation LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Systèmes** > **Audit** > **Syslog**.
2. Dans l'onglet **Politiques**, dans la liste des **actions**, cliquez sur **Liaisons globales** pour lier les politiques globales d'audit.

Configuration NSLOG à l'aide de l'interface de ligne de commande

Pour créer une action de serveur NSLOG pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
    <logLevel> ... [-lsn ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Pour créer une politique de serveur NSLOG pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add audit nslogPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Pour lier une politique de serveur NSLOG à l'ensemble du système pour la journalisation LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind system global [<policyName>]
<!--NeedCopy-->
```


Configuration NSLOG à l'aide de l'utilitaire de configuration

Pour configurer une action du serveur NSLOG pour la journalisation LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Systèmes** > **Audit** > **Nslog** et, dans l'onglet **Serveurs**, ajoutez un nouveau serveur d'audit ou modifiez un serveur existant.
2. Pour activer la journalisation LSN, sélectionnez l'option de **journalisation NAT à grande échelle** .

Pour configurer une politique de serveur NSLOG pour la journalisation LSN à l'aide de l'utilitaire de configuration

Accédez à **Systèmes** > **Audit** > **Nslog** et, dans l'onglet **Politiques**, ajoutez une nouvelle politique ou modifiez une politique existante.

Pour lier une politique de serveur NSLOG à l'ensemble du système pour la journalisation LSN à l'aide de l'utilitaire de configuration

1. Accédez à **Systèmes** > **Audit** > **Nslog**.
2. Dans l'onglet **Politiques**, dans la liste des **actions**, cliquez sur **Liaisons globales** pour lier les politiques globales d'audit.

Exemple

La configuration suivante spécifie deux serveurs SYSLOG et deux serveurs NSLOG pour stocker les entrées de journal, y compris les journaux LSN. La journalisation LSN est configurée pour les groupes LSN LSN-GROUP-2 et LSN-GROUP-3.

L'appliance NetScaler génère des messages de journal relatifs aux mappages LSN et aux sessions LSN de ces groupes LSN, et les envoie aux serveurs de journaux spécifiés.

```
add audit syslogAction SYS-ACTION-1 198.51.101.10 -logLevel ALL -lsn
    ENABLED
Done
add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
Done
bind system global SYSLOG-POLICY-1
Done

add audit syslogAction SYS-ACTION-2 198.51.101.20 -logLevel ALL -lsn
    ENABLED
Done
add audit syslogPolicy SYSLOG-POLICY-2 ns_true SYS-ACTION-2
```



```
Done
bind system global SYSLOG-POLICY-2
Done

add audit nslogAction NSLOG-ACTION-1 198.51.101.30 -logLevel ALL -lsn
    ENABLED
Done
add audit nslogPolicy NSLOG-POLICY-1 ns_true NSLOG-ACTION-1
Done
bind system global NSLOG-POLICY-1
Done
add audit nslogAction NSLOG-ACTION-2 198.51.101.40 -logLevel ALL -lsn
    ENABLED
Done
add audit nslogPolicy NSLOG-POLICY-2 ns_true NSLOG-ACTION-2
Done
bind system global NSLOG-POLICY-2
Done

add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-2  - logging ENABLED  -
    sessionLogging ENABLED
Done
set lsn group LSN-GROUP-2   - logging ENABLED  - sessionLogging ENABLED
Done
<!--NeedCopy-->
```

La configuration suivante spécifie la configuration SYSLOG pour l'envoi de messages de journal au serveur SYSLOG externe 192.0.2.10 via TCP.

```
add audit syslogAction SYS-ACTION-1 192.0.2.10 -logLevel ALL -transport
    TCP
Done

add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
Done

bind system global SYSLOG-POLICY-1
Done
<!--NeedCopy-->
```

Le tableau suivant présente des exemples d'entrées de journal LSN de chaque type stockées sur les serveurs de journaux configurés. Ces entrées de journal LSN sont générées par une appliance NetScaler dont l'adresse NSIP est 10.102.37.115.

Type d'entrée du journal LSN	Exemple d'entrée dans le journal
Création d'une session LSN	Local4. Informational 10.102.37.115 08/05/2014:09:59:48 GMT 0-PPE-0 : LSN LSN_SESSION 2581750 : SESSION CRÉÉE IP du client : Port:TD 192.0.2.10 : 15136 : 0, IP natif : NATport 203.0.113.6 : 6234, IP de destination : Port : TD 198.51.100.9 : 80:0, Protocole : TCP
Suppression de session LSN	Local 4. Informational 10.102.37.115 08/05/2014 : 10:05:12 GMT 0-PPE-0 : LSN LSN_SESSION 3871790 : SESSION SUPPRIMÉE IP du client : Port : TD 192.0.2.11 : 15130 : 0, IP NAT : Port 203.0.113.6 : 7887, IP de destination : Port : TD 198.51.101. 2:80:0, Protocole : TCP
Création d'un mappage LSN	Local4. Informational 10.102.37.115 08/05/2014:09:59:47 GMT 0-PPE-0 : LSN LSN_MAPPING 2581580 : IP du client EIM CREATED : port 192.0.2.15 : 14567, IP natif : NATport 203.0.113.5 : 8214, protocole : TCP
Suppression du mappage LSN	Local 4. Informational 10.102.37.115 08/05/2014 : 10:05:12 GMT 0-PPE-0 : LSN LSN_MAPPING 3871700 : IP du client EIM SUPPRIMÉ : port 192.0.3.15 : 14565, IP NAT : port 203.0.113.11 : 8217, protocole : TCP

Journalisation minimale

Les configurations LSN déterministes et les configurations LSN dynamiques avec bloc de ports réduisent considérablement le volume des journaux LSN. Pour ces deux types de configuration, l'appliance NetScaler alloue une adresse IP NAT et un bloc de ports à un abonné. L'appliance NetScaler génère un message de journal pour un bloc de ports au moment de l'allocation à un abonné. L'appliance NetScaler génère également un message de journal lorsqu'une adresse IP NAT et un bloc de ports sont libérés. Pour une connexion, un abonné peut être identifié uniquement par son adresse IP NAT mappée et son bloc de ports. Pour cette raison, l'appliance NetScaler n'enregistre aucune session LSN créée ou supprimée. L'appliance ne consigne également aucune entrée de mappage créée pour une session ni lorsque l'entrée de mappage est supprimée.

La fonctionnalité de journalisation minimale pour les configurations LSN déterministes et les configurations LSN dynamiques avec bloc de ports est activée par défaut et aucune disposition ne permet de

la désactiver. En d'autres termes, l'appliance NetScaler effectue automatiquement une journalisation minimale pour les configurations LSN déterministes et les configurations LSN dynamiques avec bloc de ports. Aucune option n'est disponible pour désactiver cette fonctionnalité. L'appliance envoie les messages de journal à tous les serveurs de journaux configurés.

Un message de journal pour chaque bloc de ports contient les informations suivantes :

- Adresse NSIP de l'appliance NetScaler
- Horodatage
- Type d'entrée : DETERMINISTIC ou PORTBLOCK
- Si un bloc de ports est alloué ou libéré
- Adresse IP de l'abonné, adresse IP NAT et bloc de ports attribués
- Nom du protocole

Journalisation minimale pour une configuration LSN déterministe

Prenons l'exemple d'une configuration LSN déterministe simple pour quatre abonnés ayant les adresses IP 192.0.17.1, 192.0.17.2, 192.0.17.3 et 192.0.17.4.

Dans cette configuration LSN, la taille du bloc de ports est définie sur 32768 et le pool d'adresses IP NAT LSN possède des adresses IP comprises entre 203.0.113.19 et 203.0.113.23.

```
1  add lsn client LSN-CLIENT-7
2  Done
3  bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask
       255.255.255.253
4  Done
5  add lsn pool LSN-POOL-7 -nattype DETERMINISTIC
6  Done
7  bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23
8  Done
9  add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
       DETERMINISTIC -portblocksize 32768
10 Done
11 bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7
12 Done
13 <!--NeedCopy-->
```

L'appliance NetScaler préalloue séquentiellement, à partir du pool d'adresses IP NAT LSN et sur la base de la taille de bloc de ports définie, une adresse IP NAT LSN et un bloc de ports à chaque abonné. Il attribue le premier bloc de ports (1024-33791) de l'adresse IP NAT de début (203.0.113.19) à l'adresse IP de l'abonné de début (192.0.17.1). La plage de ports suivante est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné

suivant. À ce stade, le premier bloc de port de l'adresse IP NAT suivante est attribué à l'abonné, et ainsi de suite. L'appliance enregistre l'adresse IP NAT et le bloc de ports alloués à chaque abonné.

L'appliance NetScaler n'enregistre aucune session LSN créée ou supprimée pour ces abonnés. L'appliance génère les messages de journal suivants pour la configuration du LSN.

```
1) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201453 0 :  Dtrstc ALLOC Client 12.0.0.241,
   NatInfo 50.0.0.2:59904 to 60415
2) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201454 0 :  Dtrstc ALLOC Client 12.0.0.242,
   NatInfo 50.0.0.2:60416 to 60927
3) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
   NatInfo 50.0.0.2:60928 to 61439
4) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
   NatInfo 50.0.0.2:60928 to 61439
<!--NeedCopy-->
```

Lorsque vous supprimez la configuration LSN, l'adresse IP NAT et le bloc de ports alloués sont libérés pour chaque abonné. L'appliance enregistre l'adresse IP NAT et le bloc de ports libérés pour chaque abonné. L'appliance génère les messages de journal suivants pour chaque abonné lorsque vous supprimez la configuration LSN.

```
1) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201706 0 :  Dtrstc FREE Client 12.0.0.238,
   NatInfo 50.0.0.2:58368 to 58879
2) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201707 0 :  Dtrstc FREE Client 12.0.0.239,
   NatInfo 50.0.0.2:58880 to 59391
3) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201708 0 :  Dtrstc FREE Client 12.0.0.240,
   NatInfo 50.0.0.2:59392 to 59903
<!--NeedCopy-->
```

Journalisation minimale pour la configuration dynamique du LSN avec bloc de ports

Prenons un exemple de configuration LSN dynamique simple avec un bloc de ports pour tout abonné du réseau 192.0.2.0/24. Dans cette configuration LSN, la taille du bloc de ports est définie sur 1024 et le pool d'adresses IP NAT LSN possède des adresses IP comprises entre 203.0.113.3 et 203.0.113.4.

```
set lsn parameter -memLimit 4000
Done
```



```
add lsn client LSN-CLIENT-1
Done
bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-1
Done
bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done
bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done
<!--NeedCopy-->
```

L'appliance NetScaler alloue une adresse IP NAT aléatoire et un bloc de ports, à partir du pool d'adresses IP NAT LSN et sur la base de la taille de bloc de ports définie, à un abonné lorsqu'il lance une session pour la première fois. NetScaler enregistre l'adresse IP NAT et le bloc de ports alloués à cet abonné. L'appliance n'enregistre aucune session LSN créée ou supprimée pour cet abonné. Si tous les ports sont alloués (pour différentes sessions d'abonné) à partir du bloc de ports alloué à l'abonné, l'appliance alloue une nouvelle adresse IP NAT aléatoire et un nouveau bloc de ports à l'abonné pour des sessions supplémentaires. NetScaler enregistre chaque adresse IP NAT et chaque bloc de port alloués à un abonné.

L'appliance génère le message de journal suivant lorsque l'abonné, dont l'adresse IP est 192.0.2.1, lance une session. Le message du journal indique que l'appliance a alloué l'adresse IP NAT 203.0.113.3 et le bloc de ports 1024-2047 à l'abonné.

```
03/23/2015:00:07:12 GMT  Informational 0-PPE-3 : default LSN
    LSN_PORTBLOCK 106725793 0 :  Portblock ALLOC Client 12.0.2.72,
    NatInfo 203.0.113.3:1024 to 2047, Proto:TCP
<!--NeedCopy-->
```

Une fois qu'il ne reste plus de sessions utilisant l'adresse IP NAT allouée et l'un des ports du bloc de ports alloué, l'adresse IP NAT et le bloc de ports alloués sont libérés de l'abonné. NetScaler enregistre que l'adresse IP NAT et le bloc de ports sont libérés de l'abonné. L'appliance génère les messages de journal suivants pour l'abonné, dont l'adresse IP est 192.0.2.1, lorsqu'il ne reste plus de session utilisant l'adresse IP NAT allouée (203.0.113.3) et un port du bloc de ports alloué (1024-2047). Le message du journal indique que l'adresse IP NAT et le bloc de ports sont libérés de l'abonné.

```
03/23/2015:00:11:09 GMT Informational 0-PPE-3 : default LSN
    LSN_PORTBLOCK 106814342 0 :  Portblock FREE Client 12.0.3.122,
    NatInfo 203.0.113.3: 1024 to 2047, Proto:TC
<!--NeedCopy-->
```


Serveurs SYSLOG d'équilibrage de charge

L'appliance NetScaler envoie ses événements et messages SYSLOG à tous les serveurs de journaux externes configurés. Cela entraîne le stockage de messages redondants et rend la surveillance difficile pour les administrateurs système. Pour résoudre ce problème, l'appliance NetScaler propose des algorithmes d'équilibrage de charge capables d'équilibrer la charge des messages SYSLOG entre les serveurs de journaux externes afin d'améliorer la maintenance et les performances. Les algorithmes d'équilibrage de charge pris en charge incluent RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets et AuditLogHash.

Équilibrage de charge des serveurs SYSLOG à l'aide de l'interface de ligne de commande

Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

```
add service <name>(<IP> | <serverName>) <serviceType (SYSLOGTCP |
    SYSLOGUDP)> <port>
<!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP et la méthode d'équilibrage de charge AUDITLOGHASH.

```
add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
    <AUDITLOGHASH>]
<!--NeedCopy-->
```

Transférez le service au serveur virtuel d'équilibrage de charge.

```
Bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge dont le type de service est SYSLOGTCP ou SYSLOGUDP.

```
add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
     <logLevel>]
<!--NeedCopy-->
```

Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

```
add syslogpolicy <name> <rule> <action>
<!--NeedCopy-->
```

Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.


```
bind system global <policyName>
<!--NeedCopy-->
```

Équilibrage de charge des serveurs SYSLOG à l'aide de l'utilitaire de configuration

1. Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

   Accédez à Gestion du trafic > Services, cliquez sur Ajouter et sélectionnez SYLOGTCP ou SYSLOGUDP comme protocole.

2. Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP et la méthode d'équilibrage de charge AUDITLOGHASH.

   Accédez à Gestion du trafic > Serveurs virtuels, cliquez sur Ajouter et sélectionnez SYLOGTCP ou SYSLOGUDP comme protocole.

3. Transférez le service au serveur virtuel d'équilibrage de charge vers le service.

   Transférez le service au serveur virtuel d'équilibrage de charge.

   Accédez à Gestion du trafic > Serveurs virtuels, sélectionnez un serveur virtuel, puis sélectionnez AuditLogHash dans la méthode d'équilibrage de charge.

4. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge dont le type de service est SYSLOGTCP ou SYSLOGUDP.

   Accédez à Système > Audit, cliquez sur Serveurs et ajoutez un serveur en sélectionnant l'option LB Vserver dans Servers.

5. Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

   Accédez à Système > Syslog, cliquez sur Stratégies et ajoutez une stratégie SYSLOG.

6. Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

   Accédez à Système > Syslog, sélectionnez une stratégie SYSLOG et cliquez sur Action, puis cliquez sur Liaisons globales et liez la stratégie au système global.

Exemple :

La configuration suivante spécifie l'équilibre de charge des messages SYSLOG entre les serveurs de journaux externes à l'aide de la méthode AUDITLOGHASH comme méthode d'équilibrage de charge. L'appliance NetScaler génère des événements et des messages SYSLOG dont la charge est équilibrée entre les services, service1, service2 et service 3.

```
add service service1 192.0.2.10 SYSLOGUDP 514
Done

```



```
add service service2 192.0.2.11 SYSLOGUDP 514
Done

add service service3 192.0.2.11 SYSLOGUDP 514
Done

add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
Done

bind lb vserver lbvserver1 service1
Done

bind lb vserver lbvserver1 service2
Done

bind lb vserver lbvserver1 service3
Done

add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
Done

add syslogpolicy syspol1 ns_true sysaction1
Done

bind system global syspol1
Done
<!--NeedCopy-->
```

Enregistrement des informations d'en-tête HTTP

L'appliance NetScaler peut désormais enregistrer les informations d'en-tête de demande d'une connexion HTTP utilisant la fonctionnalité LSN de NetScaler. Les informations d'en-tête suivantes d'un paquet de requête HTTP peuvent être enregistrées :

- URL à laquelle la requête HTTP est destinée.
- Méthode HTTP spécifiée dans la requête HTTP.
- Version HTTP utilisée dans la requête HTTP.
- Adresse IP de l'abonné qui a envoyé la requête HTTP.

Les journaux d'en-tête HTTP peuvent être utilisés par les FAI pour voir les tendances liées au protocole HTTP parmi un ensemble d'abonnés. Par exemple, un fournisseur de services Internet peut utiliser cette fonctionnalité pour découvrir les sites Web les plus populaires parmi un ensemble d'abonnés.

Un profil de journal d'en-tête HTTP est un ensemble d'attributs d'en-tête HTTP (par exemple, URL et

méthode HTTP) qui peuvent être activés ou désactivés pour la journalisation. Le profil du journal d'en-tête HTTP est ensuite lié à un groupe LSN. L'appliance NetScaler enregistre ensuite les attributs d'en-tête HTTP, qui sont activés dans le profil de journal d'en-tête HTTP lié pour la journalisation, de toutes les requêtes HTTP liées au groupe LSN. L'appliance envoie ensuite les messages de journal aux serveurs de journaux configurés.

Un profil de journal d'en-tête HTTP peut être lié à plusieurs groupes LSN, mais un groupe LSN ne peut avoir qu'un seul profil de journal d'en-tête HTTP.

Pour créer un profil de journal d'en-tête HTTP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

Pour lier un profil de journal d'en-tête HTTP à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Exemple

Dans l'exemple suivant de configuration LSN, le profil de journal d'en-tête HTTP HTTP-Header-Log-1 est lié au groupe LSN LSN-GROUP-1. Le profil de journal contient tous les attributs HTTP (URL, méthode HTTP, version HTTP et adresse IP HOST) activés pour la journalisation afin que tous ces attributs soient enregistrés pour toutes les requêtes HTTP des abonnés (sur le réseau 192.0.2.0/24) liées au groupe LSN.

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done

set lsn parameter -memLimit 4000
```



```
Done

add lsn client LSN-CLIENT-1
Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done

add lsn pool LSN-POOL-1
Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done

bind lsn group  LSN-GROUP-1  -httphdrlogprofilename HTTP-HEADER-LOG-1
Done
<!--NeedCopy-->
```

NetScaler génère le message de journal d'en-tête HTTP suivant lorsque l'un des abonnés appartenant à l'exemple de configuration LSN envoie une requête HTTP.

Le message du journal nous indique qu'un client ayant l'adresse IP 192.0.2.33 envoie une requête HTTP à URL example.com à l'aide de la méthode HTTP GET et de la version HTTP 1.1.

```
03/19/2015:16:24:04 GMT  Informational 0-PPE-1 : default LSN Message 59
     0 :  "LSN Client IP:TD 10.102.37.118:0 URL: example.com Host:
    192.0.2.33 Version: HTTP1.1 Method: GET"
<!--NeedCopy-->
```

Enregistrement des informations MSISDN

Un numéro de répertoire d'abonnés intégré à une station mobile (MSISDN) est un numéro de téléphone identifiant de manière unique un abonné sur plusieurs réseaux mobiles. Le MSISDN est associé à un code de pays et à un code de destination national identifiant l'opérateur de l'abonné.

Vous pouvez configurer une appliance NetScaler pour inclure MsisDNS dans les entrées du journal LSN pour les abonnés des réseaux mobiles. La présence de MSISDNS dans les journaux LSN permet

à l'administrateur de retrouver plus rapidement et précisément un abonné mobile qui a enfreint une politique ou une loi, ou dont les informations sont requises par des agences d'interception légales.

Les exemples d'entrées de journal LSN suivants incluent des informations MSISDN pour une connexion depuis un abonné mobile dans une configuration LSN. Les entrées du journal indiquent qu'un abonné mobile dont le MSISDN est E 164:5556543210 était connecté à l'adresse IP de destination 23.0.0. 1:80 via l'adresse NAT IP:port 203.0.113. 3:45195.

Type d'entrée de journal	Exemple d'entrée dans le journal
Création d'une session LSN	14 octobre 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6 : LSN LSN_SESSION 25012 0 par défaut : SESSION CRÉÉE E 164:5556543210 IP du client : Port:TD 192.0.2. 50:4649:0, Natip:NATPort 203.0.113. 3:45195, IP de destination : Port:Port:23.0.0. 1:0:0, Protocole : TCP
Création d'un mappage LSN	14 octobre 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6 : LSN LSN_ADDR_MAPPING 25013 0 par défaut : ADM CREATED E 164:5556543210 IP du client : Port:TD 192.0.2. 50:4649:0, NatiP:NATPort 203.0.113. 3:45195, IP de destination : Port:TD 23.0.0. 1:0:0, Protocole : TCP
Suppression de session LSN	14 octobre 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6 : LSN LSN_SESSION 25012 0 par défaut : SESSION CRÉÉE E 164:5556543210 IP du client : Port:TD 192.0.2. 50:4649:0, Natip:NATPort 203.0.113. 3:45195, IP de destination : PortTD 23.0.0. 1:0:0, Protocole : TCP
Cartographie LSN	14 octobre 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6 : LSN LSN_ADDR_MAPPING 25013 0 par défaut : ADM CREATED E 164:5556543210 IP du client : Port:TD 192.0.2. 50:4649:00, Natip:NATPort 203.0.113. 3:45195, IP de destination : Port:TD 23.0.0. 1:0:0, Protocole : T CP

Effectuez les tâches suivantes pour inclure les informations MSISDN dans les journaux LSN

- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre ID d'abonné au journal, qui indique s'il faut ou non inclure les informations MSISDN dans les journaux LSN d'une configuration LSN. Activez le paramètre ID d'abonné au journal lors de la création du profil de journal LSN.
- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN**. Liez le profil de journal LSN créé à un groupe LSN d'une configuration LSN en définissant le paramètre nom de profil de journal sur le nom de profil de journal LSN créé. Pour obtenir des instructions sur la configuration du NAT à grande échelle, consultez Étapes de configuration pour LSN.

Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn logprofile <logprofilename -logSubscriberID ( ENABLED |
   DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Pour lier un profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Exemple de configuration :

Dans cet exemple de configuration LSN, le paramètre ID d'abonné au journal est activé pour le profil de journal LSN. Le profil est lié au groupe LSN LSN-GROUP-9. Les informations MSISDN sont incluses dans la session LSN et les journaux de mappage LSN pour les connexions des abonnés mobiles (sur le réseau 192.0.2.0/24).

```
add lsn logprofile  LOG-PROFILE-MSISDN-9   -logSubscriberID ENABLED

Done
add lsn client LSN-CLIENT-9

Done
```



```
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done
add lsn pool LSN-POOL-9

Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done
bind lsn group  LSN-GROUP-9  -logprofilename LOG-PROFILE-MSISDN-9

Done
<!--NeedCopy-->
```

Affichage des sessions LSN en cours

Vous pouvez afficher les sessions LSN en cours pour détecter toute session LSN indésirable ou inefficace sur l'appliance NetScaler. Vous pouvez afficher toutes les sessions LSN ou certaines d'entre elles en fonction des paramètres de sélection.

Remarque : Lorsque plus d'un million de sessions LSN existent sur l'appliance NetScaler, Citrix recommande d'afficher les sessions LSN sélectionnées au lieu de toutes à l'aide des paramètres de sélection.

Configuration à l'aide de l'interface de ligne de commande

Pour afficher toutes les sessions LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show lsn session
<!--NeedCopy-->
```

Pour afficher des sessions LSN sélectives à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
show lsn session [-clientname <string>] [-network <ip_addr> [-netmask <
    netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <
    port>]]
<!--NeedCopy-->
```

Exemple

Pour afficher toutes les sessions LSN existantes sur un NetScaler

```
> show lsn session
        SubscrIP             SubscrPort      SubscrTD              DstIP                        DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10           15136           0             198.51.100.9           80             0       203.0.113.6     6234           TCP     OUT
2.      192.0.2.11           15130           0             198.51.101.2           80             0       203.0.113.6     7887           TCP     OUT
3.      192.0.2.12           16136           0             198.51.100.3           80             0       203.0.113.6     9807           TCP     OUT
4.      192.0.2.13           18148           0             198.51.101.6           80             0       203.0.113.6     4657           TCP     OUT
5.      192.0.2.14           13560           0             198.51.101.7           80             0       203.0.113.7     9341           TCP     OUT
6.      192.0.2.15           14567           0             198.51.100.8           80             0       203.0.113.5     8214           TCP     OUT
7.      192.0.2.15           16890           0             198.51.101.1           80             0       203.0.113.5     8214           TCP     OUT
8.      192.0.2.16           12345           0             198.51.102.9           80             0       203.0.113.5     1678           TCP     OUT
9.      192.0.2.19           19876           0             198.51.103.8           80             0       203.0.113.5     1567           TCP     OUT
10.     192.0.2.20           10989           0             198.51.104.19          80             0       203.0.113.11    1343           TCP     OUT
11.     192.0.3.13           18149           0             198.51.101.61          80             0       203.0.113.11    4653           TCP     OUT
12.     192.0.3.14           13510           0             198.51.101.74          80             0       203.0.113.11    9344           TCP     OUT
13.     192.0.3.15           14565           0             198.51.100.82          80             0       203.0.113.11    8217           TCP     OUT
14.     192.0.3.15           16899           0             198.51.101.12          80             0       203.0.113.11    8219           TCP     OUT
15.     192.0.3.16           12343           0             198.51.102.99          80             0       203.0.113.11    1673           TCP     OUT

Done
```

Pour afficher toutes les sessions LSN associées à une entité cliente LSN LSN-CLIENT-2

```
> show lsn session -clientname LSN-CLIENT-2
        SubscrIP             SubscrPort      SubscrTD              DstIP                        DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10           15136           0             198.51.100.9           80             0       203.0.113.6     6234           TCP     OUT
2.      192.0.2.11           15130           0             198.51.101.2           80             0       203.0.113.6     7887           TCP     OUT
3.      192.0.2.12           16136           0             198.51.100.3           80             0       203.0.113.6     9807           TCP     OUT
4.      192.0.2.13           18148           0             198.51.101.6           80             0       203.0.113.6     4657           TCP     OUT
5.      192.0.2.14           13560           0             198.51.101.7           80             0       203.0.113.7     9341           TCP     OUT
6.      192.0.2.15           14567           0             198.51.100.8           80             0       203.0.113.5     8214           TCP     OUT
7.      192.0.2.15           16890           0             198.51.101.1           80             0       203.0.113.5     8214           TCP     OUT
8.      192.0.2.16           12345           0             198.51.102.9           80             0       203.0.113.5     1678           TCP     OUT
9.      192.0.2.19           19876           0             198.51.103.8           80             0       203.0.113.5     1567           TCP     OUT
10.     192.0.2.20           10989           0             198.51.104.19          80             0       203.0.113.11    1343           TCP     OUT

Done
```

Pour afficher toutes les sessions LSN qui utilisent 203.0.113.5 comme adresse IP NAT

```
> show lsn session –natIP 203.0.113.5
SubscrIP             SubscrPort      SubscrTD        DstIP                  DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.15           14567           0             198.51.100.8           80             0       203.0.113.5     8214           TCP     OUT
2.      192.0.2.15           16890           0             198.51.101.1           80             0       203.0.113.5     8214           TCP     OUT
3.      192.0.2.16           12345           0             198.51.102.9           80             0       203.0.113.5     1678           TCP     OUT
4.      192.0.2.19           19876           0             198.51.103.8           80             0       203.0.113.5     1567           TCP     OUT
Done
```

Configuration à l'aide de l'utilitaire de configuration

Pour afficher toutes les sessions LSN ou certaines d'entre elles à l'aide de l'utilitaire de configuration

1. Accédez à Système > NAT à grande échelle > Sessions, puis cliquez sur l'onglet NAT44.
2. Pour afficher les sessions LSN en fonction des paramètres de sélection, cliquez sur Rechercher.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- Afficher la session LSN
  - clientname

    Nom de l'entité cliente LSN. Longueur maximale : 127
  - network

    Adresse IP ou adresse réseau du ou des abonnés.
  - masque de réseau

    Masque de sous-réseau pour l'adresse IP spécifiée par le paramètre réseau.

    Valeur par défaut : 255.255.255.255
  - td

    ID de domaine de trafic de l'entité cliente LSN.

    Valeur par défaut : 0

    Valeur minimale : 0

    Valeur maximale : 4094
  - NatiP

    Adresse IP NAT mappée utilisée dans les sessions LSN.

Affichage des statistiques LSN

Vous pouvez afficher des statistiques relatives à la fonctionnalité LSN pour évaluer les performances de la fonctionnalité LSN ou pour résoudre des problèmes. Vous pouvez afficher un résumé des statistiques de la fonctionnalité LSN ou d'un groupe LSN particulier. Les compteurs statistiques reflètent les événements survenus depuis le dernier redémarrage de l'appliance NetScaler. Tous ces compteurs sont remis à 0 lorsque l'appliance NetScaler est redémarrée.

Pour afficher toutes les statistiques LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat lsn
<!--NeedCopy-->
```


Pour afficher les statistiques d'un groupe LSN spécifié à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat lsn group [<groupname>]
<!--NeedCopy-->
```

Exemple

```
> stat lsn

Large Scale NAT statistics
                                                    Rate(/s)
                                                       Total
LSN TCP Received Packets                              0
   40
LSN TCP Received Bytes                                0
   3026
LSN TCP Transmitted Packets                           0
   40
LSN TCP Transmitted Bytes                             0
   3026
LSN TCP Dropped Packets                               0
                         0
LSN TCP Current Sessions                              0
                         0
LSN UDP Received Packets                              0
                         0
LSN UDP Received Bytes                                0
                         0
LSN UDP Transmitted Packets                           0
                         0
LSN UDP Transmitted Bytes                             0
                         0
LSN UDP Dropped Packets                               0
                         0
LSN UDP Current Sessions                              0
                         0
LSN ICMP Received Packets                             0
   982
LSN ICMP Received Bytes                               0
   96236
LSN ICMP Transmitted Packets                          0
```



```
                          0
LSN ICMP Transmitted Bytes                          0
                          0
LSN ICMP Dropped Packets                            0
    982
LSN ICMP Current Sessions                           0
                          0
LSN Subscribers                                     0
                          1

Done

> stat lsn group LSN-GROUP-1

LSN Group Statistics
                                                 Rate (/s)
                                                    Total
TCP Translated Pkts                                 0
    40
TCP Translated Bytes                                0
    3026
TCP Dropped Pkts                                    0
                          0
TCP Current Sessions                                0
                          0
UDP Translated Pkts                                 0
                          0
UDP Translated Bytes                                0
                          0
UDP Dropped Pkts                                    0
                          0
UDP Current Sessions                                0
                          0
ICMP Translated Pkts                                0
                          0
ICMP Translated Bytes                               0
                          0
ICMP Dropped Pkts                                   0
                          0
ICMP Current Sessions                               0
                          0
Current Subscribers                                 0
                          1

Done
```



```
<!--NeedCopy-->
```

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- groupe Stat LSN
  - nom du groupe

    Nom du groupe LSN. Longueur maximale : 127
  - détail

    Spécifie la sortie détaillée (y compris davantage de statistiques). La sortie peut être assez volumineuse. Sans cet argument, la sortie affichera uniquement un résumé.
  - Valeurs complètes

    Spécifie que les nombres et les chaînes doivent être affichés dans leur forme complète. Sans cette option, les chaînes longues sont raccourcies et les grands nombres sont abrégés.
  - n fois

    Le nombre de fois, par intervalles de sept secondes, que les statistiques doivent être affichées.

    Valeur par défaut : 1
  - Fichier journal

    Le nom du fichier journal à utiliser comme entrée.
  - statistiques claires

    Effacer les statistiques et les compteurs

    Valeurs possibles : basique, complète

Journalisation compacte

L'enregistrement des informations LSN est l'une des fonctions importantes dont les FAI ont besoin pour répondre aux exigences légales et être en mesure d'identifier la source du trafic à tout moment. Cela se traduit finalement par un énorme volume de données de journalisation, obligeant les FAI à réaliser d'importants investissements pour maintenir l'infrastructure de journalisation.

La journalisation compacte est une technique qui permet de réduire la taille du journal en utilisant un changement de notation impliquant des codes courts pour les noms d'événements et de protocoles. Par exemple, C pour le client, SC pour la session créée et T pour TCP. La journalisation compacte entraîne une réduction moyenne de 40 % de la taille des journaux.

Les exemples suivants d'entrées du journal de création de mappages NAT44 montrent les avantages de la journalisation compacte.

|-|-|
| Format de journalisation par défaut|02/02/ 2016:01:13:01 GMT Informatif 0-PPE-2 : LSN LSN_ADDRPORT_MAPPING 85 0 : A&PDM CREATED ClientIP : Port:TD1.1.1. 1:6500:0, IP natif : NATPort 8.8.8. 8:47902, IP de destination : Port:TD2.2.2. 2:80:00, Protocole : TCP| | Format de journalisation compact|02/02/ 2016:00 1:14:57 GMT Info 0-PE2 : LSN 87 par défaut : A&PDMC | C-1.1.1. 1:6500:0 | N-8.8.8. 9:51066 |D-2.2.2. 2:80:0 |T|

Étapes de configuration

Effectuez les tâches suivantes pour enregistrer les informations LSN au format compact :

- **Créez un profil de journal LSN.** Un profil de journal LSN inclut le paramètre Log Compact, qui indique si les informations doivent être enregistrées au format compact pour une configuration LSN.
- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN.** Liez le profil de journal LSN créé à un groupe LSN d'une configuration LSN en définissant le paramètre Nom du profil de journal sur le nom du profil de journal LSN créé. Toutes les sessions et tous les mappages de ce groupe LSN sont enregistrés au format compact.

Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```

Pour lier un profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Exemple de configuration :


```
add lsn logprofile  LOG-PROFILE-COMPACT-9 -logCompact ENABLED

Done
add lsn client LSN-CLIENT-9
Done
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-9
Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9
Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9
Done
bind lsn group  LSN-GROUP-9  - logProfileName LOG-PROFILE-COMPACT-9
Done
<!--NeedCopy-->
```

Journalisation IPFIX

L'appliance NetScaler prend en charge l'envoi d'informations sur les événements LSN au format IPFIX (Internet Protocol Flow Information Export) vers l'ensemble configuré de collecteurs IPFIX. L'appliance utilise la fonctionnalité AppFlow existante pour envoyer des événements LSN au format IPFIX aux collecteurs IPFIX.

La journalisation basée sur IPFIX est disponible pour les événements à grande échelle suivants liés à NAT44 :

- Création ou suppression d'une session LSN.
- Création ou suppression d'une entrée de mappage LSN.
- Allocation ou désallocation de blocs de ports dans le contexte d'un NAT déterministe.
- Allocation ou désallocation de blocs de ports dans le contexte d'un NAT dynamique.
- Chaque fois que le quota de sessions d'abonnés est dépassé.

Points à prendre en compte avant de configurer la journalisation IPFIX

Avant de commencer à configurer IPsec ALG, tenez compte des points suivants :

- Vous devez configurer la fonctionnalité AppFlow et le ou les collecteurs IPFIX sur l'appliance NetScaler. Pour obtenir des instructions, consultez la rubrique Configuration de la fonctionnalité AppFlow.

Étapes de configuration

Effectuez les tâches suivantes pour enregistrer les informations LSN au format IPFIX :

- **Activez la journalisation LSN dans la configuration AppFlow**. Activez le paramètre de journalisation LSN dans le cadre de la configuration d'AppFlow.
- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre IPFIX qui active ou désactive les informations du journal au format IPFIX.
- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN**. Liez le profil du journal LSN à un ou plusieurs groupes LSN. Les événements liés au groupe LSN lié seront enregistrés au format IPFIX.

Pour activer la journalisation LSN dans la configuration AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set appflow param -lsnLogging ( ENABLED | DISABLED )

show appflow param
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide de la CLI à l'invite de commande

À l'invite de commande, tapez :

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```


Pour créer un profil de journal LSN à l'aide de l'interface graphique

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur l'onglet **Journal**, puis ajoutez un profil de journal.

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface graphique

1. Accédez à **Système** > **NAT à grande échelle** > Groupe **LSN, puis ouvrez le groupeLSN.**
2. Dans **Paramètres avancés,** cliquez sur **+ Profil de journal** pour lier le profil de journal créé au groupe LSN.

Délai d'inactivité TCP SYN

May 5, 2023

Le délai d'inactivité SYN est le délai d'expiration pour établir des connexions TCP utilisant le LSN sur l'appliance NetScaler. Si aucune session TCP n'est établie dans le délai configuré, NetScaler supprime la session. Le délai d'inactivité de SYN est utile pour fournir une protection contre les attaques SYN flood. Dans une configuration LSN, l'entité du groupe LSN inclut le paramètre de délai d'inactivité SYN.

Exemple :

Dans l'exemple de configuration LSN suivant, le délai d'inactivité de SYN est défini à 30 secondes pour les connexions TCP liées aux abonnés du réseau 192.0.2.0/24.

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

```



```
add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  - synidletimeout 30

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done
<!--NeedCopy-->
```

Remplacement de la configuration LSN avec la configuration d'équilibrage de charge

May 5, 2023

Par défaut, une configuration LSN est prioritaire par rapport à toute configuration d'équilibrage de charge. Pour remplacer la configuration du réseau à grande échelle (LSN) par la configuration d'équilibrage de charge pour le trafic correspondant aux deux configurations, créez un profil réseau avec le paramètre Override LSN activé et liez ce profil au serveur virtuel de la configuration d'équilibrage de charge. Les paramètres USNIP ou USIP de la configuration d'équilibrage de charge sont appliqués au trafic, au lieu d'appliquer l'adresse IP LSN de la configuration LSN.

Cette option est utile dans un déploiement LSN qui inclut des appliances NetScaler et des services à valeur ajoutée, tels que des dispositifs de pare-feu et d'optimisation. Dans ce type de déploiement, le trafic entrant sur l'appliance NetScaler doit passer par ces services à valeur ajoutée avant qu'une configuration LSN sur l'appliance ne soit appliquée au trafic. Pour que l'appliance NetScaler envoie le trafic entrant vers un service à valeur ajoutée, une configuration d'équilibrage de charge est créée et le LSN de remplacement est activé sur l'appliance. La configuration d'équilibrage de charge inclut des services à valeur ajoutée, représentés sous forme de services d'équilibrage de charge, liés à un serveur virtuel de type ANY. Le serveur virtuel est configuré avec des politiques d'écoute pour identifier le trafic à envoyer au service à valeur ajoutée.

Pour activer le remplacement de lsn dans un profil réseau à l'aide de l'interface de ligne de commande

Pour activer la fonction override lsn lors de l'ajout d'un profil réseau, à l'invite de commande, tapez

```
add netProfile <name> -overrideLsn ( ENABLED | DISABLED )

show netprofile <name>
```



```
<!--NeedCopy-->
```

Pour activer la fonction override lsn lors de l'ajout d'un profil réseau, à l'invite de commande, tapez

```
set netProfile <name> -overrideLsn ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Pour activer le remplacement de lsn dans un profil réseau à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Profils réseau**.
2. Définissez le paramètre **Override LSN** lors de l'ajout ou de la modification de profils réseau.

Dans l'exemple de configuration suivant, l'option de remplacement LSN du profil réseau NETPROFILE-OVERRIDELSN-1 est activée et est lié au serveur virtuel d'équilibrage de charge LBVS-1.

Exemple de configuration :

```
add netprofile NETPROFILE-OVERRIDELSN-1 -overrideLsn ENABLED

Done

set lb vserver LBVS-1 -netprofile NETPROFILE-OVERRIDELSN-1

Done
<!--NeedCopy-->
```

Effacer les sessions LSN

May 5, 2023

Vous pouvez supprimer toutes les sessions LSN indésirables ou inefficaces de l'appliance NetScaler. L'appliance libère immédiatement les ressources (telles que l'adresse IP NAT, le port et la mémoire) allouées à ces sessions, les rendant ainsi disponibles pour de nouvelles sessions. L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions LSN ou certaines d'entre elles de l'appliance NetScaler.

Pour effacer toutes les sessions LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
flush lsn session

show lsn session
<!--NeedCopy-->
```

Pour effacer des sessions LSN sélectives à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
flush lsn session [-clientname <string>] [-network <ip_addr> [-netmask
    <netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <
    port>]]

show lsn session
<!--NeedCopy-->
```

Exemple

Effacer toutes les sessions LSN existantes sur un NetScaler

```
flush lsn session

Done
<!--NeedCopy-->
```

Efface toutes les sessions LSN liées à l'entité cliente LSN LSN-CLIENT-1

```
flush lsn session -clientname LSN-CLIENT-1

Done
<!--NeedCopy-->
```

Efface toutes les sessions LSN liées à un réseau d'abonnés (192.0.2.0) de l'entité cliente LSN LSN-CLIENT-2 appartenant au domaine de trafic 100

```
flush lsn session -clientname LSN-CLIENT-2 -network 192.0.2.0 -
    netmask 255.255.255.0 -td 100

Done
<!--NeedCopy-->
```


Pour effacer toutes les sessions LSN à l'aide de l'utilitaire de configuration

Accédez à Système > NAT à grande échelle > Sessions, puis cliquez sur Flush Sessions.

Description des paramètres (des commandes répertoriées dans la procédure CLI)

- session Flush LSN
  - clientname

    Nom de l'entité cliente LSN. Longueur maximale : 127
  - network

    Adresse IP ou adresse réseau du ou des abonnés.
  - masque de réseau

    Masque de sous-réseau pour l'adresse IP spécifiée par le paramètre réseau.

    Valeur par défaut : 255.255.255.255
  - td

    ID de domaine de trafic de l'entité cliente LSN.

    Valeur par défaut : 0

    Valeur minimale : 0

    Valeur maximale : 4094
  - NatiP

    Adresse IP NAT mappée utilisée dans les sessions LSN.
  - Port de NAT

    Port NAT mappé utilisé dans les sessions LSN.

Serveurs SYSLOG d'équilibrage de charge

May 5, 2023

L'appliance NetScaler envoie ses événements et messages SYSLOG à tous les serveurs de journaux externes configurés. Cela entraîne le stockage de messages redondants et rend la surveillance difficile pour les administrateurs système. Pour résoudre ce problème, l'appliance NetScaler propose des algorithmes d'équilibrage de charge capables d'équilibrer la charge des messages SYSLOG entre les serveurs de journaux externes afin d'améliorer la maintenance et les performances. Les algorithmes

d'équilibrage de charge pris en charge incluent RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets et AuditLogHash.

Équilibrage de charge des serveurs SYSLOG à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

```
add service <name>(<IP> | <serverName>) <serviceType (SYSLOGTCP |
   SYSLOGUDP)> <port>
<!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP et la méthode d'équilibrage de charge AUDITLOGHASH.

```
add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
   <AUDITLOGHASH>]
<!--NeedCopy-->
```

Liez le service au serveur virtuel d'équilibrage de charge.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

1. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge dont le type de service est SYSLOGTCP ou SYSLOGUDP.

```
add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
<!--NeedCopy-->
```

Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

```
add syslogpolicy <name> <rule> <action>
<!--NeedCopy-->
```

Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

```
bind system global <policyName>
<!--NeedCopy-->
```

Équilibrage de charge des serveurs SYSLOG à l'aide de l'utilitaire de configuration

1. Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

Accédez à Gestion du trafic > Services, cliquez sur Ajouter et sélectionnez SYLOGTCP ou SYSLOGUDP comme protocole.

2. Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP et la méthode d'équilibrage de charge AUDITLOGHASH.

   Accédez à Gestion du trafic > Serveurs virtuels, cliquez sur Ajouter et sélectionnez SYLOGTCP ou SYSLOGUDP comme protocole.

3. Transférez le service au serveur virtuel d'équilibrage de charge vers le service.

   Transférez le service au serveur virtuel d'équilibrage de charge.

   Accédez à Gestion du trafic > Serveurs virtuels, sélectionnez un serveur virtuel, puis sélectionnez AuditLogHash dans la méthode d'équilibrage de charge.

4. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge dont le type de service est SYSLOGTCP ou SYSLOGUDP.

   Accédez à Système > Audit, cliquez sur Serveurs et ajoutez un serveur en sélectionnant l'option LB Vserver dans Servers.

5. Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

   Accédez à Système > Syslog, cliquez sur Stratégies et ajoutez une stratégie SYSLOG.

6. Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

   Accédez à Système > Syslog, sélectionnez une stratégie SYSLOG et cliquez sur Action, puis cliquez sur Liaisons globales et liez la stratégie au système global.

Exemple :

La configuration suivante spécifie l'équilibre de charge des messages SYSLOG entre les serveurs de journaux externes à l'aide de la méthode AUDITLOGHASH comme méthode d'équilibrage de charge. L'appliance NetScaler génère des événements et des messages SYSLOG dont la charge est équilibrée entre les services, service1, service2 et service 3.

```
add service service1 192.0.2.10 SYSLOGUDP 514

add service service2 192.0.2.11 SYSLOGUDP 514

add service service3 192.0.2.11 SYSLOGUDP 514

add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH

bind lb vserver lbvserver1 service1

bind lb vserver lbvserver1 service2

```



```
bind lb vserver lbvserver1 service3

add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All

add syslogpolicy syspol1 ns_true sysaction1

bind system global syspol1
<!--NeedCopy-->
```

Limites :

L'appliance NetScaler ne prend pas en charge un serveur virtuel d'équilibrage de charge externe équilibrant la charge des messages SYSLOG entre les serveurs de journaux.

Protocole de contrôle des ports

May 5, 2023

Les appliances NetScaler prennent désormais en charge le protocole PCP (Port Control Protocol) pour le NAT à grande échelle (LSN). De nombreuses applications réservées aux abonnés d'un fournisseur de services Internet doivent être accessibles depuis Internet (par exemple, les appareils Internet des objets (IoT), tels qu'une caméra IP qui assure la surveillance sur Internet). L'un des moyens de répondre à cette exigence consiste à créer des cartes NAT (LSN) statiques à grande échelle. Mais pour un très grand nombre d'abonnés, la création de cartes NAT LSN statiques n'est pas une solution réalisable.

Le protocole PCP (Port Control Protocol) permet à un abonné de demander des mappages NAT LSN spécifiques pour lui-même et/ou pour d'autres appareils tiers. Le périphérique NAT à grande échelle crée une carte LSN et l'envoie à l'abonné. L'abonné envoie aux appareils distants sur Internet l'adresse IP NAT:port NAT sur lequel ils peuvent se connecter à l'abonné.

Les applications envoient généralement des messages de maintien en activité fréquents au périphérique NAT à grande échelle afin que leurs mappages LSN n'arrivent pas à expiration. Le PCP permet de réduire la fréquence de tels messages de maintien en activité en permettant aux applications de connaître les paramètres de délai d'expiration des mappages LSN. Cela permet de réduire la consommation de bande passante sur le réseau d'accès du FAI et la consommation de batterie sur les appareils mobiles.

Le PCP est un modèle client-serveur qui s'exécute via le protocole de transport UDP. Une appliance NetScaler implémente le composant serveur PCP et est conforme à la RFC 6887.

Étapes de configuration

Effectuez les tâches suivantes pour configurer le PCP :

- (Facultatif) Créez un profil PCP. Un profil PCP inclut des réglages pour les paramètres liés au PCP (par exemple, pour écouter le mappage et les requêtes PCP homologues). Un profil PCP peut être lié à un serveur PCP. Un profil PCP lié à un serveur PCP applique tous ses paramètres au serveur PCP. Un profil PCP peut être lié à plusieurs serveurs PCP. Par défaut, un profil PCP avec des paramètres par défaut est lié à tous les serveurs PCP. Un profil PCP que vous liez à un serveur PCP remplace les paramètres de profil PCP par défaut de ce serveur. Un profil PCP par défaut possède les paramètres suivants :
  - Mappage : activé
  - Homologue : activé
  - Durée de vie minimale de la carte : 120 secondes
  - Durée de vie maximale maximale : 86400 secondes
  - Nombre d'annonces : 10
  - Tierce partie : désactivée
- Créez un serveur PCP et liez-y un profil PCP. Créez un serveur PCP sur l'appliance NetScaler pour écouter les demandes et les messages liés au PCP provenant des abonnés. Une adresse IP de sous-réseau (SNIP) doit être attribuée à un serveur PCP pour y accéder. Par défaut, un serveur PCP écoute sur le port 5351.
- Liez le serveur PCP à un groupe LSN d'une configuration LSN. Liez le serveur PCP créé à un groupe LSN d'une configuration LSN en définissant le paramètre PCP Server pour spécifier le serveur PCP créé. Le serveur PCP créé n'est accessible qu'aux abonnés de ce groupe LSN.

> **Remarque**
>
> Un serveur PCP destiné à une configuration NAT à grande échelle ne répond pas aux demandes des abonnés identifiés à partir des règles ACL.

Pour créer un profil PCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

Pour créer un serveur PCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Exemple de configuration pour NAT44

Dans l'exemple de configuration suivant, le serveur PCP PCP-SERVER-9, avec les paramètres PCP par défaut, est lié au groupe LSN LSN-GROUP-9. PCP-SERVER-9 traite les requêtes PCP des abonnés du réseau 192.0.2.0/24.

Exemple de configuration :

```
add pcp server PCP-SERVER-9 192.0.3.9

Done

add lsn client LSN-CLIENT-9

Done

bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-9

Done

bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done

add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done

bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done

bind lsn group  LSN-GROUP-9  -pcpServer PCP-SERVER-9

```



```
Done
<!--NeedCopy-->
```

LSN44 dans une configuration de cluster

May 5, 2023

Les configurations NAT44 à grande échelle sont prises en charge sur une configuration de cluster NetScaler.

Un cluster NetScaler est un groupe d'appliances NetScaler configurées et gérées comme un seul système. Un cluster NetScaler garantit évolutivité et disponibilité. Chaque appliance NetScaler d'une configuration de cluster agit comme une entité LSN indépendante et est gérée comme un système unique.

La configuration LSN dans une configuration en cluster est identique à celle d'une appliance autonome, sauf qu'un pool spécifique d'adresses IP LSN est détenu par un seul nœud à la fois. En d'autres termes, une entité de pool d'adresses IP LSN est configurée en tant qu'entité repérée dans un nœud particulier. Tous les nœuds d'une configuration de cluster peuvent avoir une entité de pool IP LSN spécifique. Pour s'assurer que les paquets liés à une session LSN sont reçus sur le même nœud de cluster qui a effectué l'opération NAT, le pilotage du backplane basé sur des politiques (PBS) est configuré. PBS dirige les paquets associés reçus d'une session LSN vers le même nœud de cluster.

Exemple de configuration :

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 -ownerNode 1 203.0.113.3

Done

bind lsn pool LSN-POOL-1 -ownerNode 2 203.0.113.3

```



```
Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done

add ns acl b1 ALLOW -srcIP = 192.0.2.0-192.0.2.255 -type DFD -dfdhash
   SIP


Done

apply ns acls -type DFD

Done
<!--NeedCopy-->
```

Dual-Stack Lite

May 5, 2023

En raison de la pénurie d'adresses IPv4 et des avantages d'IPv6 par rapport à IPv4, de nombreux fournisseurs de services Internet ont commencé à passer à l'infrastructure IPv6. Mais pendant la transition, les fournisseurs de services Internet doivent continuer à prendre en charge le protocole IPv4 en même temps que le protocole IPv6, car la majeure partie de l'Internet public utilise toujours uniquement le protocole IPv4 et de nombreux abonnés ne le prennent pas en charge.

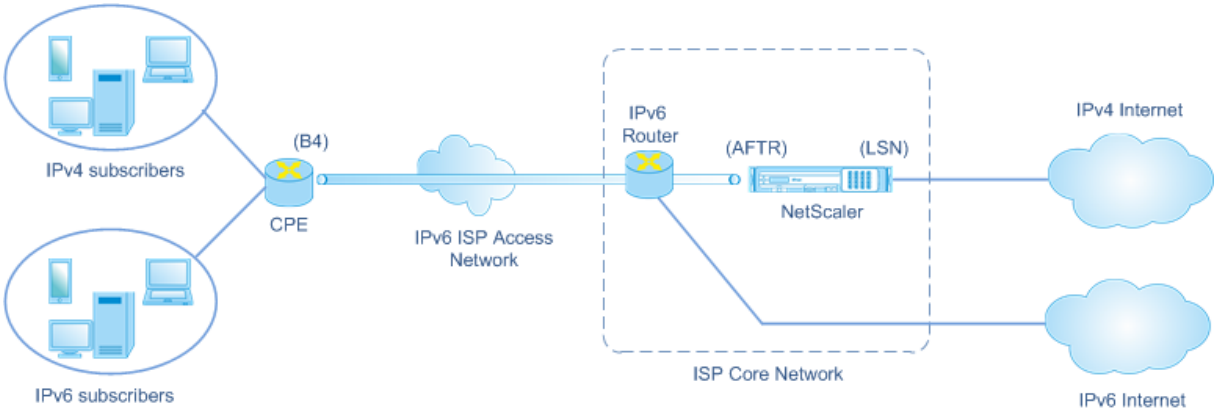
Dual Stack Lite (DS-Lite) est une solution de transition IPv6 destinée aux fournisseurs d'accès Internet dotés d'une infrastructure IPv6 afin de connecter leurs abonnés IPv4 à Internet. DS-Lite utilise le tunneling IPv4-in-IPv6 pour envoyer le paquet IPv4 d'un abonné via un tunnel du réseau d'accès IPv6 vers le fournisseur de services Internet. Le paquet IPv6 est désencapsulé pour récupérer le paquet IPv4 de l'abonné et est ensuite envoyé sur Internet après la traduction de l'adresse NAT et du port et d'autres traitements liés au LSN. Les paquets de réponse empruntent le même chemin jusqu'à l'abonné.

L'appliance NetScaler implémente le composant AFTR d'un déploiement DS-Lite et est conforme à la RFC 6333.

Architecture

L'architecture Dual-Stack Lite pour un fournisseur de services Internet comprend les composants suivants :

- **Haut débit de liaison de base (B4).** Le Basic Bridging Broadband, ou B4, est un appareil ou un composant qui se trouve dans les locaux de l'abonné. Généralement, le B4 est un composant des dispositifs CPE situés dans les locaux de l'abonné. Les abonnés IPv4 sont connectés au réseau d'accès ISP IPv6 uniquement via le périphérique CPE contenant le composant B4. La fonction principale du B4 est d'initier un tunnel IPv6 entre le B4 et un routeur de transition de famille d'adresses (AFTR) afin d'envoyer ou de recevoir des paquets de demande ou de réponse IPv4 d'abonnés via le tunnel. B4 inclut une adresse IPv6 connue sous le nom d'adresse de point de terminaison du tunnel B4. B4 utilise cette adresse pour envoyer des paquets IPv6 à AFTR et recevoir des paquets depuis AFTR.
- **Routeur de transition familiale d'adresses (AFTR).** L'AFTR est un appareil ou un composant résidant dans le réseau central du fournisseur de services Internet. L'AFTR met fin au tunnel IPv6 depuis le périphérique B4. En d'autres termes, le tunnel IPv6 est formé entre B4 dans les locaux de l'abonné et AFTR dans le réseau central du FAI. AFTR désencapsule les paquets IPv6 reçus de B4 pour récupérer les paquets IPv4 d'origine des abonnés. AFTR envoie les paquets IPv4 au périphérique ou au composant LSN. Le LSN achemine les paquets IPv4 vers leur destination après avoir effectué une traduction d'adresse NAT et de port (NAT 44) et d'autres traitements liés au LSN. L'AFTR inclut une adresse IPv6 connue sous le nom d'adresse de point de terminaison du tunnel AFTR. AFTR utilise cette adresse pour envoyer des paquets IPv6 à B4 et pour recevoir des paquets IPv6 de B4. L'appliance NetScaler implémente le composant AFTR.
- **Fil logiciel.** Le tunnel IPv6 créé entre B4 et AFTR s'appelle un fil logiciel.



L'architecture DS-Lite d'un FAI utilisant une appliance NetScaler consiste en des abonnés dans des espaces d'adressage privés accédant à Internet via une appliance NetScaler déployée sur le réseau central du fournisseur de services Internet. Les abonnés IPv4 sont connectés à un appareil CPE qui inclut la fonctionnalité DS-Lite B4. Le dispositif CPE est connecté au réseau central du fournisseur de services Internet via le réseau d'accès IPv6 uniquement du fournisseur de services Internet. L'appliance

NetScaler contient les fonctionnalités DS-Lite AFTR et LSN.

Les abonnés IPv4 connectés au périphérique CPE se voient attribuer des adresses IPv4 privées manuellement ou via un serveur DHCP s'exécutant sur le périphérique CPE. Sur le périphérique CPE, l'adresse du point de terminaison du tunnel AFTR est spécifiée manuellement ou via DHCPv6. La configuration des appareils CPE est spécifique au fournisseur et n'entre donc pas dans le cadre de cette documentation.

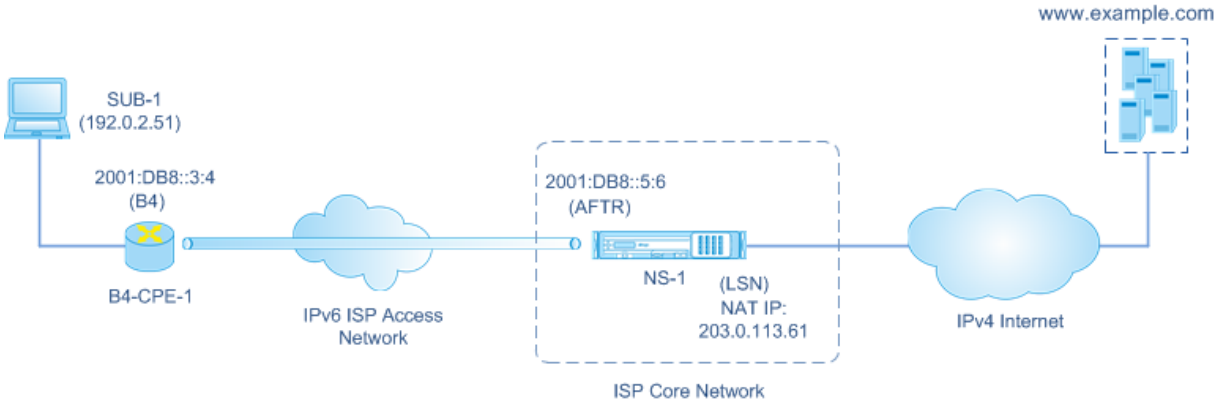
Lors de la réception d'un paquet de demande provenant d'un abonné IPv4 et destiné à un emplacement sur Internet, le composant B4 du dispositif CPE encapsule le paquet IPv4 dans un paquet IPv6 et l'envoie à l'appliance NetScaler sur le réseau central du FAI. La fonctionnalité AFTR de l'appliance NetScaler désencapsule le paquet IPv6 pour récupérer le paquet IPv4 d'origine de l'abonné. La fonctionnalité LSN de l'appliance NetScaler traduit l'adresse IP source et le port du paquet IPv4 en une adresse IP NAT et un port NAT sélectionnés dans le pool NAT configuré, puis envoie le paquet vers sa destination sur Internet.

L'appliance conserve un enregistrement de toutes les sessions actives qui utilisent les fonctionnalités AFTR et LSN. Ces sessions sont appelées sessions DS-Lite. L'appliance NetScaler gère également les mappages entre l'adresse IPv6 B4, l'adresse et le port IPv4 de l'abonné, et l'adresse et le port IPv4 NAT, pour chaque session DS-Lite. Ces mappages sont appelés mappages DSLite LSN. À partir des entrées de session DS-Lite et des entrées de mappage DSLite LSN, l'appliance NetScaler reconnaît qu'un paquet de réponse (reçu depuis Internet) appartient à une session DS-Lite particulière.

Lorsque l'appliance NetScaler reçoit un paquet de réponse appartenant à une session DS-Lite particulière, la fonctionnalité LSN de l'appliance traduit l'adresse IP de destination et le port du paquet de réponse de l'adresse IP et du port NAT vers l'adresse IP et le port de l'abonné. La fonctionnalité AFTR encapsule le paquet résultant dans un paquet IPv6 et l'envoie au périphérique CPE. La fonctionnalité B4 du dispositif CPE désencapsule le paquet IPv6 pour récupérer le paquet de réponse IPv4, puis envoie le paquet IPv4 à l'abonné.

Exemple

Prenons l'exemple d'un déploiement DS-Lite comprenant NetScaler NS-1 dans le réseau central d'un fournisseur de services Internet, le périphérique CPE B4-CPE-1 dans les locaux d'un abonné et un seul abonné IPv4 SUB-1. Le B4-CPE-1 prend en charge la fonctionnalité B4 de la fonction DS-Lite.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Entité	Nom	Détails
Adresse IPv4 de l'abonné SUB-1		192.0.2.51
Adresse IPv6 du point de terminaison logiciel sur le périphérique B4 (B4-CPE-1)		2001:DB8::3:4
Adresse IPv6 du point de terminaison logiciel sur le périphérique AFTR (NS-1)		2001:DB8::5:6

Paramètres de l'appliance NetScaler NS-1 :

Entité	Nom	Détails
Client LSN	LSN-DSLITE-CLIENT-1	Network6 (Identification du trafic provenant des appareils B4) = 2001:DB8 : 3:0 /100
Piscine LSN	LSN-DSLITE-POOL-1	IP LSN (IP NAT) = 203.0.113.61 - 203.0.113.70
Profil IPv6	LSN-DSLITE-PROFILE-1	Type = DS-LITE ; adresse IPv6 (adresse IPv6 AFTR) = L'une des adresses IPv6 appartenant à NetScaler, de type SNIP6 = 2001:DB8 : : 5:6

Entité	Nom	Détails
groupe LSN	LSN-DSLITE-GROUP-1	Client LSN = LSN-DSLITE-CLIENT-1 ; pool LSN = LSN-DSLITE-POOL-1 ; profil IPv6 = LSN-DSLITE-PROFILE-1

Voici le flux de trafic dans cet exemple :

1. L'abonné IPv4 SUB-1 envoie une demande à ()`http://www.example.com/`. Le paquet IPv4 contient :
    - Adresse IP source = 192.0.2.51
    - Port source = 2552
    - Adresse IP de destination = 198.51.100.250
    - Port de destination = 80
2. À la réception du paquet de requête IPv4, B4-CPE-1 l'encapsule dans la charge utile d'un paquet IPv6, puis envoie le paquet IPv6 à NS-1. Le paquet IPv6 contient :
    - Adresse IP source = 2001:DB8 : 3:4
    - Adresse IP de destination = 2001:DB8 : 5:6
3. Lorsque NS-1 reçoit le paquet IPv6, le module AFTR désencapsule le paquet en supprimant les en-têtes IPv6. Le paquet résultant est le paquet de requête IPv4 d'origine de SUB-1.
4. Le module LSN de NS-1 traduit l'adresse IP source et le port du paquet en une adresse IP NAT et un port NAT sélectionnés dans le pool NAT configuré. Le paquet IPv4 traduit contient :
    - Adresse IP source = 203.0.113.61
    - Port source = 3002
    - Adresse IP de destination = 198.51.100.250
    - Port de destination = 80
5. Le module LSN crée également un mappage LSN et une entrée de session pour cette session DS Lite. Le mappage inclut les informations suivantes :
    - Adresse IP source du paquet IPv6 (adresse IPv6 du B4-CPE-1) = 2001:DB8 : : 3:4
    - Adresse IP source du paquet IPv4 (adresse IPv4 du SUB-1) = 192.0.2.51
    - Port source du paquet IPv4 = 2552
    - Adresse IP NAT = 203.0.113.61
    - Port NAT = 3002
6. Le NS-1 envoie le paquet IPv4 résultant vers sa destination sur Internet.

7. Le serveur de www.example.com traite le paquet de demande et envoie un paquet de réponse. Le paquet de réponse IPv4 contient :
   - Adresse IP source = 198.51.100.250
   - Port source = 80
   - Adresse IP de destination = 203.0.113.61
   - Port de destination = 3002
8. À la réception du paquet IPv4, le NS-1 examine le mappage LSN et les entrées de session et constate que le paquet de réponse IPv4 appartient à une session DS Lite. Le module LSN de NS-1 traduit l'adresse IP et le port de destination. Le paquet IPv4 contient désormais :
   - Adresse IP source = 198.51.100.250
   - Port source = 80
   - Adresse IP de destination = 192.0.2.51
   - Port de destination = 2552
9. Le module AFTR du NS-1 encapsule le paquet IPv4 dans un paquet IPv6, puis envoie le paquet IPv6 à B4-CPE-1. Le paquet IPv6 contient :
   - Adresse IP source = 2001:DB8 : 5:6
   - Adresse IP de destination = 2001:DB8 : 3:4
10. À la réception du paquet, B4-CPE-1 décapsule le paquet IPv6 en supprimant les en-têtes IPv6, puis envoie le paquet IPv4 résultant à CL-1.

Points à prendre en compte avant de configurer DS-Lite

May 5, 2023

Tenez compte des points suivants avant de configurer DS-Lite sur une appliance NetScaler :

1. Vous devez comprendre les différents composants de DS-Lite, décrits dans la RFC 6333.
2. Une configuration DS-Lite sur une appliance NetScaler utilise les jeux de commandes LSN. Dans une configuration DS-Lite, l'entité client LSN spécifie l'adresse IPv6 ou l'adresse réseau IPv6 ou les règles ACL6 pour identifier le trafic à partir du périphérique B4. Une configuration DS-Lite inclut également un profil IPv6, qui spécifie le composant AFTR de l'adresse IPv6 sur une appliance NetScaler. Pour plus d'informations sur la fonctionnalité NetScaler LSN, consultez la section NAT à grandeéchelle.
3. Pour une configuration DS-Lite, l'appliance NetScaler prend en charge le LSN pour les paquets IPv4 appartenant uniquement à l'un des protocoles suivants. L'appliance NetScaler supprime les paquets IPv4 appartenant à d'autres protocoles :

- TCP
- UDP
- ICMP

4. L'appliance NetScaler prend en charge les ALG DS-Lite suivants :

   - ICMP
   - FTP
   - TFTP
   - Protocole d'initiation de session (SIP)
   - Protocole de diffusion en temps réel (RTSP)

Configuration de DS-Lite

May 5, 2023

Une configuration DS-Lite sur une appliance NetScaler utilise les jeux de commandes LSN. Dans une configuration DS-Lite, l'entité client LSN spécifie l'adresse IPv6 ou l'adresse réseau IPv6 ou les règles ACL6 pour identifier le trafic à partir du périphérique B4. Pour plus d'informations sur la fonctionnalité NetScaler LSN, consultez la section NAT à grandeéchelle. Une configuration DS-Lite inclut également un profil IPv6, qui spécifie l'adresse IPv6 (de type SNIP6) du composant DS-Lite AFTR sur une appliance NetScaler.

La configuration de DS-Lite sur une appliance NetScaler comprend les tâches suivantes :

- **Définissez les paramètres LSN globaux**. Les paramètres globaux incluent la quantité de mémoire NetScaler réservée à la fonctionnalité LSN et la synchronisation des sessions LSN dans une configuration haute disponibilité.
- **Créez une entité cliente LSN pour identifier le trafic provenant des appareils CPE B4**. L'entité cliente LSN fait référence à un ensemble de périphériques DS-Lite B4. L'entité cliente inclut des adresses IPv6 ou une adresse réseau IPv6 ou des règles ACL6 pour identifier le trafic provenant de ces appareils B4. Un client LSN ne peut être lié qu'à un seul groupe LSN. L'interface de ligne de commande comporte deux commandes permettant de créer une entité cliente LSN et de lier un abonné à l'entité cliente LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.
- **Créez un pool LSN et liez des adresses IP NAT à celui-ci**. Un pool LSN définit un pool d'adresses IP NAT à utiliser par l'appliance NetScaler pour effectuer le LSN. L'interface de ligne de commande comporte deux commandes permettant de créer un pool LSN et de lier des adresses IP NAT au pool LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.

- **Créez un profil IP6 LSN.** Un profil IP6 LSN définit l'adresse IPv6 du composant DS-Lite AFTR sur l'appliance NetScaler. L'adresse IPv6 doit être l'une des adresses IPv6 de type SNIP6 appartenant à NetScaler.
- **(Facultatif) Créez un profil de transport LSN pour un protocole spécifié**. Un profil de transport LSN définit différents délais et limites, tels que le nombre maximal de sessions LSN et l'utilisation maximale des ports qu'un abonné peut avoir pour un protocole donné. Vous liez un profil de transport LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil de transport LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP est lié à un groupe LSN lors de sa création. Ce profil est appelé profil de transport par défaut. Un profil de transport LSN que vous liez à un groupe LSN remplace le profil de transport LSN par défaut pour ce protocole.
- **(Facultatif) Créez un profil d'application LSN pour un protocole spécifié et liez-y un ensemble de ports de destination**. Un profil d'application LSN définit les contrôles de mappage LSN et de filtrage LSN d'un groupe pour un protocole donné et pour un ensemble de ports de destination. Pour un ensemble de ports de destination, vous liez un profil LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil d'application LSN lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil d'application LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP pour tous les ports de destination est lié à un groupe LSN lors de sa création. Ce profil est appelé profil d'application par défaut. Lorsque vous liez un profil d'application LSN, avec un ensemble spécifié de ports de destination, à un groupe LSN, le profil lié remplace le profil d'application LSN par défaut pour ce protocole sur cet ensemble de ports de destination. L'interface de ligne de commande comporte deux commandes permettant de créer un profil d'application LSN et de lier un ensemble de ports de destination au profil d'application LSN. L'utilitaire de configuration combine ces deux opérations sur un seul écran.
- **Créez un groupe LSN et liez des pools LSN, un profil IPv6 LSN, des profils de transport LSN (facultatifs) et des profils d'application LSN (facultatifs) au groupe LSN**. Un groupe LSN est une entité composée d'un client LSN, d'un profil IPv6 LSN, d'un ou de plusieurs pools LSN, d'un ou de plusieurs profils de transport LSN et de profils d'application LSN. Des paramètres sont affectés à un groupe, tels que la taille du bloc de ports et la journalisation des sessions LSN. Les paramètres s'appliquent à tous les abonnés d'un client LSN lié au groupe LSN. Un seul profil IPv6 LSN peut être lié à un groupe LSN, et un profil LSN IPv6 lié à un groupe LSN ne peut pas être lié à d'autres groupes LSN. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés entre eux. Plusieurs pools LSN peuvent être liés à un groupe LSN. Une seule entité cliente LSN peut être liée à un groupe LSN, et une entité cliente LSN liée à un groupe LSN ne peut pas être liée à d'autres groupes LSN. L'interface de ligne de commande comporte deux commandes permettant de créer un groupe LSN et de lier des pools LSN, des profils de transport LSN et des profils d'application LSN au groupe LSN. L'utilitaire de configuration

combine ces deux opérations sur un seul écran.

Configuration à l'aide de la ligne de commande

Pour créer un client LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

Pour lier un réseau IPv6 ou une règle ACL6 à un client LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
    string>)

show lsn client
<!--NeedCopy-->
```

Pour créer un pool LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
add lsn pool <poolname> [-nattype ( DYNAMIC )] [-portblockallocation (
    ENABLED | DISABLED )] [-portrealloctimeout <secs>] [-
    maxPortReallocTmq <positive_integer>]

show lsn pool
<!--NeedCopy-->
```

Pour lier une plage d'adresses IP à un pool LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

Remarque : Pour supprimer les adresses IP LSN d'un pool LSN, utilisez la commande unbind lsn pool.

Pour configurer un profil IPv6 LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
add lsn ip6profile <name>  -type DS-Lite  -network6 < ipv6_addr|*s >

show lsn ip6profile
<!--NeedCopy-->
```

Pour créer un profil de transport LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

Pour créer un profil d'application LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]

show lsn appsprofile
<!--NeedCopy-->
```

Pour lier une plage de ports de protocole d'application à un profil d'application LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

Pour créer un groupe LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC )]
    [-portblocksize <positive_integer>] [-logging (ENABLED | DISABLED )]
```



```
      [-sessionLogging ( ENABLED | DISABLED )][-sessionSync ( ENABLED |
     DISABLED )] [-snmptraplimit<positive_integer>] [-ftp ( ENABLED |
     DISABLED )] [-pptp ( ENABLED |DISABLED )] [-sipalg ( ENABLED |
     DISABLED )] [-rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]
2
3 show lsn group
4 <!--NeedCopy-->
```

Pour lier des profils de protocole LSN et des pools LSN à un groupe LSN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
1 bind lsn group <groupname> (-poolname <string> | -transportprofilename
     <string> | -httphdrlogprofilename <string> | -appsprofilename <
     string> | -sipalgprofilename <string> | rtspalgprofilename <string>)
2
3 show lsn group
4 <!--NeedCopy-->
```

Configuration à l'aide de l'utilitaire de configuration

Pour configurer un client LSN et lier une adresse réseau IPv6 ou une règle ACL6 à l'aide de l'utilitaire de configuration :

Accédez à **Système** > **NAT à grande échelle** > **Clients**, ajoutez un client, puis liez une adresse réseau IPv6 ou une règle ACL6 au client.

Pour configurer un pool LSN et lier des adresses IP NAT à l'aide de l'utilitaire de configuration :

Accédez à **Système** > **NAT à grande échelle** > **Pools**, ajoutez un pool, puis liez une adresse IP NAT ou une plage d'adresses IP NAT au pool.

Pour configurer un profil IPv6 LSN à l'aide de l'utilitaire de configuration :

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur l'onglet **IPv6** et attribuez une adresse IPv6 à DS-Lite AFTR.

Pour configurer un profil de transport LSN à l'aide de l'utilitaire de configuration :

1. Accédez à **Système** > **NAT à grande échelle** > **Profils**.
2. Dans le volet de détails, cliquez sur **Transport**, puis ajoutez un profil de transport.

Pour configurer un profil d'application LSN à l'aide de l'utilitaire de configuration :

1. Accédez à **Système** > **NAT à grande échelle** > **Profils**.
2. Dans le volet de détails, cliquez sur **Application**, puis ajoutez un profil d'application.

Pour configurer un groupe LSN et lier un client LSN, un profil IPv6 LSN, des pools, des profils de transport et des profils d'application à l'aide de l'utilitaire de configuration :

Accédez à **Système** > **NAT à grande échelle** > **Groupes**, puis ajoutez un groupe, puis liez un client LSN, un profil IPv6 LSN, des pools, des profils de transport et des profils d'application au groupe.

```
> add lsn client LSN-DSLITE-CLIENT-1
Done
> bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
Done
> add lsn pool LSN-DSLITE-POOL-1
Done
> bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
> add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6
Done
> add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1
Done
> add lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
Done
```

Journalisation et surveillance de DS-Lite

Vous pouvez enregistrer les informations DS-Lite pour diagnostiquer ou résoudre des problèmes et pour répondre aux exigences légales. L'appliance NetScaler prend en charge toutes les fonctionnalités de journalisation LSN pour la journalisation des informations DS-Lite. Pour configurer la journalisation DS-Lite, utilisez les procédures de configuration de la journalisation LSN, décrites dans Logging and Monitoring LSN.

Un message de journal pour une entrée de mappage DS-Lite LSN contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage
- Type d'entrée (MAPPING)
- Si l'entrée de mappage DSLite LSN a été créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole

- L'adresse IP de destination, le port et l'ID du domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session DS-Lite contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage
- Type d'entrée (SESSION)
- Si la session DS-Lite est créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal DS-Lite de chaque type stockées sur les serveurs de journaux configurés. Ces entrées de journal sont générées par une appliance NetScaler dont l'adresse NSIP est 10.102.37.115. Vous pouvez enregistrer les informations DS-Lite pour diagnostiquer ou résoudre des problèmes et pour répondre aux exigences légales. L'appliance NetScaler prend en charge toutes les fonctionnalités de journalisation LSN pour la journalisation des informations DS-Lite. Pour configurer la journalisation DS-Lite, utilisez les procédures de configuration de la journalisation LSN, décrites dans Logging and Monitoring LSN.

Un message de journal pour une entrée de mappage DS-Lite LSN contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage
- Type d'entrée (MAPPING)
- Si l'entrée de mappage DSLite LSN a été créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole
- L'adresse IP de destination, le port et l'ID du domaine de trafic peuvent être présents, selon les

conditions suivantes :

- L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
- Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
- L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session DS-Lite contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage
- Type d'entrée (SESSION)
- Si la session DS-Lite est créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal DS-Lite de chaque type stockées sur les serveurs de journaux configurés. Ces entrées de journal sont générées par une appliance NetScaler dont l'adresse NSIP est 10.102.37.115.

Type d'entrée du journal LSN	Exemple d'entrée dans le journal
Création d'une session DS-Lite	Local4.Informational 10.102.37.115 14/08/2015:13:35:38 GMT 0-PPE-1 : LSN LSN_SESSION 37647607 0 par défaut : SESSION CRÉÉE 2001:DB8 : 3:4 IP du client : Port:TD 192.0.2. 51:2552:0, Natip:NATPort 203.0.113. 61:3002, IP de destination : Port TD 198.51.100. 250:80:0, Protocole : TTP CP
Suppression de session DS-Lite	Local4.Informational 10.102.37.115 14/08/2015:13:38:22 GMT 0-PPE-1 : LSN LSN_SESSION 37647617 0 par défaut : SESSION SUPPRIMÉE 2001:DB8 : 3:4 IP du client : Port:TD 192.0.2. 51:2552:0, Natip:NATPort 203.0.113. 61:3002, IP de destination : Port TD 198.51.100. 250:80:0, Protocole : TG CP

Création d'un mappage LSN DS-Lite	Local4. Informational 10.102.37.115 14/08/2015:13:35:39 GMT 0-PPE-1 : LSN LSN_EIM_MAPPING 37647610 0 par défaut : EIM CREATED 2001:DB8 : 3:4 IP du client : Port:TD 192.0.2. 51:2552:0, Natip:NATPort 198.51.100. 250:80, Protocole : TCP
Suppression du mappage DSLite LSN	Local 4. Informational 10.102.37.115 14/08/2015:13:38:25 GMT 0-PPE-1 : LSN LSN_EIM_MAPPING 37647618 0 par défaut : EIM DELETED 2001:DB8 : 3:4 IP du client : Port:TD 192.0.2. 51:2552:0, Natip:NATPort 198.51.100. 250:80, Protocole : TCP

Affichage des sessions DS-Lite en cours

Vous pouvez afficher les sessions DS-Lite en cours pour détecter toute session indésirable ou inefficace sur l'appliance NetScaler. Vous pouvez afficher toutes les sessions DS-Lite ou certaines d'entre elles en fonction des paramètres de sélection.

Configuration à l'aide de l'interface de ligne de commande

Pour afficher toutes les sessions DS-Lite à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

Pour afficher les sessions DS-Lite sélectionnées à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
show lsn session -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Exemple :

L'exemple de sortie suivant affiche toutes les sessions DS-Lite existantes sur une appliance NetScaler :


```
show lsn session  - nattype DS-Lite
  B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
     NatPort Proto Dir

1.  2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
    3002 TCP OUT

2.  2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
    52862 TCP OUT

3.  2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
    48116 ICMP OUT

4.  2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
    48305 TCP OUT

Done
<!--NeedCopy-->
```

Configuration à l'aide de l'utilitaire de configuration

Pour afficher toutes les sessions DS-Lite ou certaines d'entre elles à l'aide de l'utilitaire de configuration

1. **Accédez à Système** > **NAT à grande échelle** > **Sessions**, puis cliquez sur l'onglet **DS-Lite** .
2. **Pour afficher les sessions DS-Lite en fonction des paramètres de sélection, cliquez sur Rechercher.**

Effacer des sessions DS-Lite

Vous pouvez supprimer toutes les sessions DS-Lite indésirables ou inefficaces de l'appliance NetScaler. L'appliance libère immédiatement les ressources (telles que l'adresse IP NAT, le port et la mémoire) allouées à ces sessions, les rendant ainsi disponibles pour de nouvelles sessions. L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions DS-Lite ou certaines d'entre elles de l'appliance NetScaler.

Pour effacer toutes les sessions DS-Lite à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
flush lsn session -nattype DS-Lite
show lsn session -nattype DS-Lite
```

Pour effacer les sessions DS-Lite sélectionnées à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
flush lsn session  -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]

show lsn session  -nattype DS-Lite
<!--NeedCopy-->
```

Pour effacer toutes les sessions DS-Lite ou certaines d'entre elles à l'aide de l'utilitaire de configuration :

1. Accédez à **Système** > **NAT à grande échelle** > **Sessions**, puis cliquez sur l'onglet **DS-Lite** .
2. Cliquez sur **Vider les sessions**.

Configuration des cartes statiques DS-Lite

May 5, 2023

L'appliance NetScaler prend en charge la création manuelle de mappages DSLite LSN, qui contiennent le mappage entre les informations suivantes :

- Adresse IP et port de l'abonné, et adresse IPv6 du périphérique ou du composant B4
- Adresse IP et port NAT

Les mappages LSN DS-Lite statiques sont utiles lorsque vous souhaitez vous assurer que les connexions initiées vers une adresse IP et un port NAT correspondent à l'adresse IP et au port de l'abonné via le périphérique B4 spécifié (par exemple, des serveurs Web situés dans le réseau interne).

Remarque : Cette fonctionnalité est prise en charge dans les versions 11.0 build 64.x et ultérieures.

Pour créer un mappage LSN statique DS-Lite à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
    <positive_integer>] [-network6 <B4_ADDR>] [<natIP> [<natPort>]] [-
    destIP<ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```


Descriptions des paramètres

ajouter lsn static

- nom

Nom de l'entrée de mappage statique LSN. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du groupe LSN. L'exigence suivante s'applique uniquement à la CLI : si le nom inclut un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « ds-lite lsn static1 » ou « ds-lite lsn static1 »). Il s'agit d'un argument obligatoire. Longueur maximale : 127

- protocole de transport

Protocole pour l'entrée de mappage DSLite LSN.

- S'abonner

Adresse IPv4 d'un abonné pour l'entrée de mappage DSLite LSN.

- S'abonner au port

Port de l'abonné pour l'entrée de mappage DSLite LSN.

- Network6

Adresse IPv6 du périphérique ou du composant B4.

- td

ID du domaine de trafic auquel appartient le périphérique B4. L'adresse IPv6 du périphérique B4 est spécifiée dans le paramètre network6. Si vous ne spécifiez pas d'ID, le périphérique B4 est supposé faire partie du domaine de trafic par défaut.

- NatiP

Adresse IPv4, déjà existante sur l'appliance NetScaler en tant que type LSN, à utiliser comme adresse IP NAT pour cette entrée de mappage.

- Port de NAT

Port NAT pour cette entrée de mappage DSLite LSN.

- DestP

Adresse IP de destination pour l'entrée de mappage DSLite LSN.

- dsttd

ID du domaine de trafic via lequel l'adresse IP de destination de cette entrée de mappage DSLite LSN est accessible depuis l'appliance NetScaler. Si vous ne spécifiez pas d'ID, l'adresse IP de destination est supposée être accessible via le domaine de trafic par défaut, dont l'ID est 0.

Pour créer un mappage LSN statique DS-Lite à l'aide de l'utilitaire de configuration

Accédez à Système > NAT à grande échelle > Statique et ajoutez un nouveau mappage LSN statique DS-Lite.

Configuration de l'allocation NAT déterministe pour DS-Lite

May 5, 2023

L'allocation NAT déterministe pour les déploiements DSLite LSN est un type d'allocation de ressources NAT dans lequel l'appliance NetScaler préalloue, à partir du pool d'adresses IP NAT LSN et sur la base de la taille de bloc de ports spécifiée, une adresse IP NAT LSN et un bloc de ports à chaque abonné (abonné derrière le périphérique B4).

Remarque : Cette fonctionnalité est prise en charge dans les versions 11.0 build 64.x et ultérieures.

L'appliance alloue des ressources NAT de manière séquentielle à ces abonnés. Il attribue le premier bloc de ports de l'adresse IP NAT de début à l'adresse IP de l'abonné de début. La plage de ports suivante est attribuée à l'abonné suivant, et ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. À ce stade, le premier bloc de port de l'adresse NAT suivante est attribué à l'abonné, et ainsi de suite.

L'appliance NetScaler enregistre l'adresse IP NAT allouée et le bloc de ports pour un abonné. Pour une connexion, un abonné peut être identifié uniquement par son adresse IP NAT mappée et son bloc de ports. Pour cette raison, l'appliance NetScaler ne consigne pas la création ou la suppression d'une session LSN.

Un abonné DS-Lite ne peut disposer que d'un seul bloc de ports déterministe. Si l'intégralité du bloc de ports est utilisée, l'appliance NetScaler abandonne toute nouvelle connexion de l'abonné.

Exemple : DS-Lite déterministe

Dans cet exemple, une configuration DS-Lite déterministe inclut quatre abonnés avec les adresses IP 192.0.17.5, 192.0.17.6, 192.0.17.7 et 192.0.17.8. Ces abonnés IPv4 se trouvent derrière un appareil B4 dont l'adresse IPv6 est 2001:DB8 : : 3:4. Dans cette configuration, la taille du bloc de ports est définie sur 20480 et le pool d'adresses IP NAT LSN possède des adresses IP comprises entre 203.0.113.41 et 203.0.113.42.

L'appliance NetScaler préalloue séquentiellement, à partir du pool d'adresses IP NAT LSN et en fonction de la taille de bloc de ports définie, une adresse IP NAT LSN et un bloc de ports à chaque abonné. Il attribue le premier bloc de ports (1024-21503) de l'adresse IP NAT de début (203.0.113.41) à l'adresse IP de l'abonné de début (192.0.17.5). La plage de ports suivante est attribuée à l'abonné suivant, et

ainsi de suite, jusqu'à ce que l'adresse NAT ne dispose pas de suffisamment de ports pour l'abonné suivant. À ce stade, le premier bloc de port de l'adresse IP NAT suivante est attribué à l'abonné, et ainsi de suite. NetScaler enregistre l'adresse IP NAT et le bloc de ports alloués à chaque abonné.

L'appliance NetScaler n'enregistre aucune session LSN créée ou supprimée pour ces abonnés.

Le tableau suivant répertorie l'adresse IP NAT et les blocs de ports alloués à chaque abonné dans cet exemple :

Adresse IP de l'abonné	Adresse IP NAT allouée	Bloc de ports alloué	Adresse IPv6 de B4
192.0.17.5	203.0.113.41	1024 - 21503	2001:DB8::3:4
192.0.17.6	203.0.113.41	21504 - 41983	2001:DB8::3:4
192.0.17.7	203.0.113.41	41984 - 62463	2001:DB8::3:4
192.0.17.8	203.0.113.42	1024 - 21503	2001:DB8::3:4

Étapes de configuration

Vous devez configurer NAT déterministe dans le cadre de la configuration DS-Lite. Pour obtenir des instructions sur la configuration de DS-Lite, reportez-vous à la section Configuration de DS-Lite.

Lors de la configuration de DS-Lite, assurez-vous que vous :

- Définissez le paramètre NAT Type sur Déterministe lors de l'ajout du pool LSN et du groupe LSN.
- Définissez le paramètre de taille de bloc de port souhaité lors de l'ajout du groupe LSN, sauf si vous pouvez accepter la valeur par défaut.

Points à prendre en compte avant de configurer DS-Lite déterministe

Tenez compte des points suivants avant de configurer DS-Lite déterministe :

- L'adresse IP complète de chaque abonné doit être spécifiée dans une commande client add lsn distincte, en définissant les paramètres Réseau et Masque réseau. (Définissez le masque réseau sur 255.255.255.255.) L'adresse IPv4 du périphérique B4 spécifiée dans le paramètre Network6 doit également être complète (préfixe /128). En d'autres termes, les paramètres Network et Network6 n'acceptent pas d'adresses autres que le masque /32 bits et le préfixe /128, respectivement.
- L'appliance NetScaler supprime les connexions des abonnés qui ne sont spécifiés dans aucune configuration DS-Lite déterministe mais qui se trouvent derrière des appareils B4 spécifiés dans une configuration DS-Lite déterministe.

- L'appliance NetScaler reconnaît les abonnés ayant la même adresse IPv4 comme des abonnés différents s'ils se trouvent derrière des appareils B4 différents. Une combinaison de l'adresse IPv4 de l'abonné et du périphérique B4 définit un abonné unique dans l'entité cliente LSN d'une configuration DS-Lite.

Exemple de configuration déterministe DS-Lite :

La configuration suivante utilise les paramètres répertoriés dans la section Exemple : DETERMINISTIC DS-Lite.

```
add lsn client LSN-DSLITE-CLIENT-10

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.5 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.6 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.7 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.8 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
add lsn pool LSN-DSLITE-POOL-10 -nattype DETERMINISTIC

Done
bind lsn pool LSN-DSLITE-POOL-10  203.0.113.41-203.0.113.42

Done
add lsn ip6profile LSN-DSLITE-PROFILE-10 -type DS-Lite -network6 2001:
    DB8::5:6

Done
add lsn group LSN-DSLITE-GROUP-10 -clientname LSN-DSLITE-CLIENT-10 -
    nattype DETERMINISTIC -portblocksize 20480 -ip6profile LSN-DSLITE-
    PROFILE-10

Done
bind lsn group LSN-DSLITE-GROUP-10 -poolname LSN-DSLITE-POOL-10
```



```
29
30 Done
31 <!--NeedCopy-->
```

Configuration des passerelles de la couche application pour DS-Lite

May 5, 2023

Pour certains protocoles de couche application, les adresses IP et les numéros de port du protocole sont également communiqués dans la charge utile du paquet. La passerelle de couche d'application (AGL) d'un protocole analyse la charge utile du paquet et apporte les modifications nécessaires pour garantir que le protocole continue de fonctionner sur DS-Lite.

L'appliance NetScaler prend en charge le protocole ALG pour les protocoles suivants pour DS-Lite :

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Passerelle de couche d'application pour les protocoles FTP, ICMP et TFTP

January 21, 2021

Vous pouvez activer ou désactiver ALG pour le protocole FTP pour une configuration DS-Lite en activant ou en désactivant l'option ALG FTP du groupe LSN de la configuration.

ALG pour le protocole ICMP est activé par défaut et aucune disposition ne permet de le désactiver.

ALG pour le protocole TFTP est désactivé par défaut. TFTP ALG est activé automatiquement pour une configuration DS-Lite lorsque vous liez un profil d'application UDP LSN, avec mappage indépendant du point de terminaison, filtrage indépendant du point de terminaison et port de destination 69 (port connu pour TFTP), au groupe LSN.

Passerelle de couche d'application pour le protocole SIP

May 5, 2023

L'utilisation de DS-Lite avec le protocole SIP (Session Initiation Protocol) est compliquée, car les messages SIP contiennent des adresses IP dans les en-têtes SIP ainsi que dans le corps du SIP. Lorsque le LSN est utilisé avec SIP, les en-têtes SIP contiennent des informations sur l'appelant et le récepteur, et l'appareil traduit ces informations pour les masquer au réseau extérieur. Le corps du SIP contient les informations du protocole SDP (Session Description Protocol), qui incluent les adresses IP et les numéros de port pour la transmission du média. SIP ALG pour DS-Lite est conforme aux normes RFC 3261, RFC 3581, RFC 4566 et RFC 4475.

> **Remarque**
>
> Le SIP ALG est pris en charge dans une appliance autonome NetScaler, dans une configuration haute disponibilité NetScaler, ainsi que dans une configuration de cluster NetScaler.

Limites du SIP ALG

SIP ALG pour DS-Lite présente les limites suivantes :

- Seule la charge utile SDP est prise en charge.
- Les éléments suivants ne sont pas pris en charge :
  - Adresses IP de multidiffusion
  - SDP crypté
  - EXPÉDITION TLS
  - Traduction du FQDN
  - Authentification de couche SIP
  - Partitions d'administration
  - Carrosserie en plusieurs parties
  - Pliage en ligne

Configuration de SIP ALG

Vous devez configurer le SIP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, reportez-vous à la section Configuration de DS-Lite. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez les paramètres suivants lors de l'ajout d'un profil d'application LSN :
  - Regroupement d'adresses IP = APPARIÉ
  - Mappage des adresses et des ports = INDÉPENDANT DU POINT DE TERMINAISON
  - Filtrage = INDÉPENDANT DU POINT DE TERMINAISON
- Créez un profil SIP ALG et assurez-vous de définir la plage de ports source ou la plage de ports de destination. Liez le profil SIP ALG au groupe LSN
- Activer SIP ALG dans le groupe LSN

Pour activer SIP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn group <groupname> -clientname <string>[-sipalg ( ENABLED |
    DISABLED )]

show lsn group<groupname>
<!--NeedCopy-->
```

Pour activer SIP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn sipalgprofile<sipalgprofilename>[-dataSessionIdleTimeout<
    positive_integer>][-sipSessionTimeout<positive_integer>][-
    registrationTimeout<positive_integer>][-sipsrcportrange<port[-port
    ]>][-sipdstportrange<port[-port]>][-openRegisterPinhole ( ENABLED |
    DISABLED )][-openContactPinhole ( ENABLED | DISABLED )][-
    openViaPinhole ( ENABLED | DISABLED )][-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP )[-
    openRoutePinhole ( ENABLED | DISABLED )][-rport ( ENABLED | DISABLED
     )]

show lsn sipalgprofile<sipalgprofilename>
<!--NeedCopy-->
```

Exemple de configuration

L'exemple de configuration DS-Lite suivant, SIP ALG, est activé pour le trafic TCP provenant de périphériques B4 du réseau 2001:DB8 : : 3:0 /96.

```
add lsn client LSN-DSLITE-CLIENT-1
Done
bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/96
Done
add lsn pool LSN-DSLITE-POOL-1
Done
bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
    DB8::5:6
Done
```



```
add lsn appsprofile LSN-DSLITE-APPS-PROFILE-1 TCP -ippooling PAIRED -
   mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn sipalgprofile SIPALGPROFILE-1  -sipdstportrange 5060 -
   sipTransportProtocol TCP
Done
add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1 -sipalg ENABLED
Done
bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -appsprofilename LSN-DSLITE-APPS-
   PROFILE-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -sipalgprofilename SIPALGPROFILE-1
Done
<!--NeedCopy-->
```

Passerelle de couche application pour le protocole RTSP

May 5, 2023

Le protocole RTSP (Real Time Streaming Protocol) est un protocole au niveau de l'application pour le transfert de données multimédia en temps réel. Utilisé pour établir et contrôler des sessions multimédia entre les points de terminaison, le RTSP est un protocole de canal de contrôle entre le client multimédia et le serveur multimédia. La communication classique se fait entre un client et un serveur de streaming multimédia.

La diffusion de contenu multimédia d'un réseau privé vers un réseau public nécessite la traduction des adresses IP et des numéros de port sur le réseau. Les fonctionnalités de NetScaler incluent une passerelle de couche d'application (ALG) pour RTSP, qui peut être utilisée avec un NAT à grande échelle (LSN) pour analyser le flux multimédia et apporter les modifications nécessaires pour garantir que le protocole continue de fonctionner sur le réseau.

La manière dont la traduction des adresses IP est effectuée dépend du type et de la direction du message, ainsi que du type de média pris en charge par le déploiement client-serveur. Les messages sont traduits comme suit :

- Requête sortante : adresse IP privée vers une adresse IP publique appartenant à NetScaler appelée adresse IP LSN.
- Réponse entrante : adresse IP LSN vers adresse IP privée.
- Demande entrante : aucune traduction.

- Réponse sortante : adresse IP privée vers l'adresse IP du pool LSN.

> **Remarque**
>
> L'ALG RTSP est pris en charge dans une appliance autonome NetScaler, dans une configuration haute disponibilité NetScaler, ainsi que dans une configuration de cluster NetScaler.

Limites de RTSP ALG

Le RTSP ALG ne prend pas en charge les éléments suivants :

- Sessions RTSP multidiffusion
- Session RTSP via UDP
- Partitions d'administration
- Authentification RTSP
- Tunneling HTTP

Configuration de RTSP ALG

Configurez RTSP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration de LSN, reportez-vous à la section Configuration de DS-Lite. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez les paramètres suivants lors de l'ajout d'un profil d'application LSN :
  - Regroupement d'adresses IP = APPARIÉ
  - Mappage des adresses et des ports = INDÉPENDANT DU POINT DE TERMINAISON
  - Filtrage = INDÉPENDANT DU POINT DE TERMINAISON
- Activer RTSP ALG dans le groupe LSN
- Créez un profil RTSP ALG et liez le profil RTSP ALG au groupe LSN

Pour activer RTSP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

Pour activer RTSP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
    positive_integer>] -rtspportrange <port[-port]> [-
    rtspTransportProtocol (TCP|UDP)]

show lsn rtspalgprofile <rtspalgprofilename>
<!--NeedCopy-->
```

Exemple de configuration RTSP ALG

L'exemple de configuration DS-Lite suivant, RTSP ALG, est activé pour le trafic TCP en provenance des appareils B4 du réseau 2001:DB8 : : 4:0 /96.

Exemple de configuration RTSP ALG :

```
add lsn client LSN-DSLITE-CLIENT-5
Done
bind lsn client LSN-DSLITE-CLIENT-5 -network6 2001:DB8::4:0/96
Done
add lsn pool LSN-DSLITE-POOL-5
Done
bind lsn pool LSN-DSLITE-POOL-5 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-5 -type DS-Lite -network6 2001:
    DB8::5:6
Done
add lsn appsprofile LSN-DSLITE-APPS-PROFILE-5 TCP -ippooling PAIRED -
    mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn rtspalgprofile RTSPALGPROFILE-5 -rtspIdleTimeout 1000 -
    rtspportrange 554
Done
add lsn group LSN-DSLITE-GROUP-5 -clientname LSN-DSLITE-CLIENT-5 -
    portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-5 -rtspalg ENABLED
Done
bind lsn group LSN-DSLITE-GROUP-5 -poolname LSN-DSLITE-POOL-5
Done
bind lsn group LSN-DSLITE-GROUP-5 -appsprofilename LSN-DSLITE-APPS-
    PROFILE-5
Done
bind lsn group LSN-DSLITE-GROUP-5 -rtspalgprofilename RTSPALGPROFILE-5
Done
<!--NeedCopy-->
```


Journalisation et surveillance de DS-Lite

May 5, 2023

Vous pouvez enregistrer les informations DS-Lite pour diagnostiquer ou résoudre des problèmes et pour répondre aux exigences légales. L'appliance NetScaler prend en charge toutes les fonctionnalités de journalisation LSN pour la journalisation des informations DS-Lite. Pour configurer la journalisation DS-Lite, utilisez les procédures de configuration de la journalisation LSN, décrites dans Logging and Monitoring LSN.

Un message de journal pour une entrée de mappage DS-Lite LSN contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage
- Type d'entrée (MAPPING)
- Si l'entrée de mappage DSLite LSN a été créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole
- L'adresse IP de destination, le port et l'ID du domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session DS-Lite contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage
- Type d'entrée (SESSION)
- Si la session DS-Lite est créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole

- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal DS-Lite de chaque type stockées sur les serveurs de journaux configurés. Ces entrées de journal sont générées par une appliance NetScaler dont l'adresse NSIP est 10.102.37.115. Vous pouvez enregistrer les informations DS-Lite pour diagnostiquer ou résoudre des problèmes et pour répondre aux exigences légales. L'appliance NetScaler prend en charge toutes les fonctionnalités de journalisation LSN pour la journalisation des informations DS-Lite. Pour configurer la journalisation DS-Lite, utilisez les procédures de configuration de la journalisation LSN, décrites dans Logging and Monitoring LSN.

Un message de journal pour une entrée de mappage DS-Lite LSN contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage
- Type d'entrée (MAPPING)
- Si l'entrée de mappage DSLite LSN a été créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole
- L'adresse IP de destination, le port et l'ID du domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour le mappage dépendant du port d'adresse.

Un message de journal pour une session DS-Lite contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage
- Type d'entrée (SESSION)
- Si la session DS-Lite est créée ou supprimée
- Adresse IPv6 de B4
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal DS-Lite de chaque type stockées sur les serveurs de journaux configurés. Ces entrées de journal sont générées par une appliance NetScaler dont l'adresse NSIP est 10.102.37.115.

Type d'entrée du journal LSN	Exemple d'entrée dans le journal
Création d'une session DS-Lite	Local4.Informational 10.102.37.115 14/08/2015:13:35:38 GMT 0-PPE-1 : LSN LSN_SESSION 37647607 0 par défaut : SESSION CRÉÉE 2001:DB8 : 3:4 IP du client : Port:TD 192.0.2. 51:2552:0, Natip:NATPort 203.0.113. 61:3002, IP de destination : Port TD 198.51.100. 250:80:0, Protocole : TTP CP
Suppression de session DS-Lite	Local4.Informational 10.102.37.115 14/08/2015:13:38:22 GMT 0-PPE-1 : LSN LSN_SESSION 37647617 0 par défaut : SESSION SUPPRIMÉE 2001:DB8 : 3:4 IP du client : Port:TD 192.0.2. 51:2552:0, Natip:NATPort 203.0.113. 61:3002, IP de destination : Port TD 198.51.100. 250:80:0, Protocole : TG CP
Création d'un mappage LSN DS-Lite	Local4. Informational 10.102.37.115 14/08/2015:13:35:39 GMT 0-PPE-1 : LSN LSN_EIM_MAPPING 37647610 0 par défaut : EIM CREATED 2001:DB8 : 3:4 IP du client : Port:TD 192.0.2. 51:2552:0, Natip:NATPort 198.51.100. 250:80, Protocole : TCP
Suppression du mappage DSLite LSN	Local 4. Informational 10.102.37.115 14/08/2015:13:38:25 GMT 0-PPE-1 : LSN LSN_EIM_MAPPING 37647618 0 par défaut : EIM DELETED 2001:DB8 : 3:4 IP du client : Port:TD 192.0.2. 51:2552:0, Natip:NATPort 198.51.100. 250:80, Protocole : TCP

Affichage des sessions DS-Lite en cours

Vous pouvez afficher les sessions DS-Lite en cours pour détecter toute session indésirable ou inefficace sur l'appliance NetScaler. Vous pouvez afficher toutes les sessions DS-Lite ou certaines d'entre elles en fonction des paramètres de sélection.

Pour afficher toutes les sessions DS-Lite à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show lsn session  -nattype DS-Lite
<!--NeedCopy-->
```

Pour afficher les sessions DS-Lite sélectionnées à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show lsn session  -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

L'exemple de sortie suivant affiche toutes les sessions DS-Lite existantes sur une appliance NetScaler :

> afficher la session lsn —nattype DS-Lite

```
  B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
     NatPort Proto Dir

1. 2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
    3002 TCP OUT

2. 2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
    52862 TCP OUT

3. 2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
    48116 ICMP OUT

4. 2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
    48305 TCP OUT
Done
<!--NeedCopy-->
```

Configuration à l'aide de l'utilitaire de configuration

Pour afficher toutes les sessions DS-Lite ou certaines d'entre elles à l'aide de l'utilitaire de configuration

1. **Accédez à Système** > **NAT à grande échelle** > **Sessions**, puis cliquez sur l'onglet **DS-Lite** .
2. **Pour afficher les sessions DS-Lite en fonction des paramètres de sélection, cliquez sur Rechercher.**

Effacer des sessions DS-Lite

Vous pouvez supprimer toutes les sessions DS-Lite indésirables ou inefficaces de l'appliance NetScaler. L'appliance libère immédiatement les ressources (telles que l'adresse IP NAT, le port et la mémoire) allouées à ces sessions, les rendant ainsi disponibles pour de nouvelles sessions. L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions DS-Lite ou certaines d'entre elles de l'appliance NetScaler.

Pour effacer toutes les sessions DS-Lite à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
flush lsn session -nattype DS-Lite

show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

Pour effacer les sessions DS-Lite sélectionnées à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
flush lsn session -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]

show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

Pour effacer toutes les sessions DS-Lite ou certaines d'entre elles à l'aide de l'utilitaire de configuration

1. Accédez à **Système** > **NAT à grande échelle** > **Sessions**, puis cliquez sur l'onglet **DS-Lite** .
2. Cliquez sur **Vider les sessions**.

Enregistrement des informations d'en-tête HTTP

L'appliance NetScaler peut enregistrer les informations d'en-tête de demande d'une connexion HTTP utilisant la fonctionnalité DS-Lite. Les informations d'en-tête suivantes d'un paquet de requête HTTP peuvent être enregistrées :

- URL à laquelle la requête HTTP est destinée
- Méthode HTTP spécifiée dans la requête HTTP

- Version HTTP utilisée dans la requête HTTP
- Adresse IPv4 de l'abonné qui a envoyé la requête HTTP

Les journaux d'en-tête HTTP peuvent être utilisés par les FAI pour voir les tendances liées au protocole HTTP parmi un ensemble d'abonnés. Par exemple, un fournisseur de services Internet peut utiliser cette fonctionnalité pour trouver le site Web le plus populaire parmi un ensemble d'abonnés.

Étapes de configuration

Effectuez les tâches suivantes pour configurer l'appliance NetScaler afin qu'elle enregistre les informations d'en-tête HTTP :

- **Créez un profil de journal d'en-tête HTTP**. Un profil de journal d'en-tête HTTP est un ensemble d'attributs d'en-tête HTTP (par exemple, URL et méthode HTTP) qui peuvent être activés ou désactivés pour la journalisation.
- **Liez l'en-tête HTTP à un groupe LSN d'une configuration LSN DS-Lite**. Liez le profil de journal d'en-tête HTTP à un groupe LSN d'une configuration LSN en définissant le paramètre de nom du profil de journal d'en-tête HTTP sur le nom du profil de journal d'en-tête HTTP créé. L'appliance NetScaler enregistre ensuite les informations d'en-tête HTTP de toutes les requêtes HTTP liées au groupe LSN. Un profil de journal d'en-tête HTTP peut être lié à plusieurs groupes LSN, mais un groupe LSN ne peut avoir qu'un seul profil de journal d'en-tête HTTP.

Pour créer un profil de journal d'en-tête HTTP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

Pour lier un profil de journal d'en-tête HTTP à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```


Exemple de configuration

Dans la configuration LSN DS-Lite suivante, le profil de journal d'en-tête HTTP HTTP-Header-Log-1 est lié au groupe LSN LSN-DSLITE-GROUP-1. Le profil de journal contient tous les attributs HTTP (URL, méthode HTTP, version HTTP et adresse IP HOST) activés pour la journalisation, de sorte que tous ces attributs sont enregistrés pour toutes les requêtes HTTP provenant de périphériques B4 (sur le réseau 2001:DB 8:5001 : :/96).

Exemple de configuration :

```
1  add lsn httphdrlogprofile HTTP-HEADER-LOG-1
2
3  Done
4
5  add lsn client LSN-DSLITE-CLIENT-1
6
7  Done
8
9  bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
10
11 Done
12
13 add lsn pool LSN-DSLITE-POOL-1
14
15 Done
16
17 bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
18
19 Done
20
21 add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
      DB8::5:6
22
23 Done
24
25 add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
      portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1
26
27 Done
28
29 bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
30
31 Done
32
33 bind lsn group LSN-DSLITE-GROUP-1 -httphdrlogprofilename HTTP-HEADER-
```



```
        LOG-1
34
35  Done
36  <!--NeedCopy-->
```

Journalisation IPFIX

L'appliance NetScaler prend en charge l'envoi d'informations sur les événements LSN au format IPFIX (Internet Protocol Flow Information Export) vers l'ensemble configuré de collecteurs IPFIX. L'appliance utilise la fonctionnalité AppFlow existante pour envoyer des événements LSN au format IPFIX aux collecteurs IPFIX.

La journalisation basée sur IPFIX est disponible pour les événements suivants liés à DS_Lite :

- Création ou suppression d'une session LSN.
- Création ou suppression d'une entrée de mappage LSN.
- Allocation ou désallocation de blocs de ports dans le contexte d'un NAT déterministe.
- Allocation ou désallocation de blocs de ports dans le contexte d'un NAT dynamique.
- Chaque fois que le quota de sessions d'abonnés est dépassé.

Points à prendre en compte avant de configurer la journalisation IPFIX

Avant de commencer à configurer IPsec ALG, tenez compte des points suivants :

- Vous devez configurer la fonctionnalité AppFlow et le ou les collecteurs IPFIX sur l'appliance NetScaler. Pour obtenir des instructions, reportez-vous à la section Configuration de la fonctionnalité AppFlow.

Étapes de configuration

Effectuez les tâches suivantes pour enregistrer les informations LSN au format IPFIX :

- **Activez la journalisation LSN dans la configuration AppFlow**. Activez le paramètre de journalisation LSN dans le cadre de la configuration d'AppFlow.
- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre IPFIX qui active ou désactive les informations du journal au format IPFIX.
- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN**. Liez le profil du journal LSN à un ou plusieurs groupes LSN. Les événements liés au groupe LSN lié seront enregistrés au format IPFIX.

Pour activer la journalisation LSN dans la configuration AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set appflow param -lsnLogging (ENABLED |DISABLED )

show appflow param
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide de la CLI à l'invite de commande, tapez

À l'invite de commande, tapez :

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide de l'interface graphique

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur l'onglet **Journal**, puis ajoutez un profil de journal.

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface graphique

1. Accédez à **Système** > **NAT à grande échelle** > Groupe **LSN, puis ouvrez le groupeLSN.**
2. Dans **Paramètres avancés,** cliquez sur **+ Profil de journal** pour lier le profil de journal créé au groupe LSN.

Protocole de contrôle des ports pour DS-Lite

May 5, 2023

Les appliances NetScaler prennent désormais en charge le protocole PCP (Port Control Protocol) pour le NAT à grande échelle (LSN). De nombreuses applications réservées aux abonnés d'un fournisseur de services Internet doivent être accessibles depuis Internet (par exemple, les appareils Internet des objets (IoT), tels qu'une caméra IP qui assure la surveillance sur Internet). L'un des moyens de répondre à cette exigence consiste à créer des cartes NAT (LSN) statiques à grande échelle. Mais pour un très grand nombre d'abonnés, la création de cartes NAT LSN statiques n'est pas une solution réalisable.

Le protocole PCP (Port Control Protocol) permet à un abonné de demander des mappages NAT LSN spécifiques pour lui-même et/ou pour d'autres appareils tiers. Le périphérique NAT à grande échelle crée une carte LSN et l'envoie à l'abonné. L'abonné envoie aux appareils distants sur Internet l'adresse IP NAT:port NAT sur lequel ils peuvent se connecter à l'abonné.

Les applications envoient généralement des messages de maintien en activité fréquents au périphérique NAT à grande échelle afin que leurs mappages LSN n'arrivent pas à expiration. Le PCP permet de réduire la fréquence de tels messages de maintien en activité en permettant aux applications de connaître les paramètres de délai d'expiration des mappages LSN. Cela permet de réduire la consommation de bande passante sur le réseau d'accès du FAI et la consommation de batterie sur les appareils mobiles.

Le PCP est un modèle client-serveur qui s'exécute via le protocole de transport UDP. Une appliance NetScaler implémente le composant serveur PCP et est conforme à la RFC 6887.

Étapes de configuration

Effectuez les tâches suivantes pour configurer le PCP :

- (Facultatif) Créez un profil PCP. Un profil PCP inclut des réglages pour les paramètres liés au PCP (par exemple, pour écouter le mappage et les requêtes PCP homologues). Un profil PCP peut être lié à un serveur PCP. Un profil PCP lié à un serveur PCP applique tous ses paramètres au serveur PCP. Un profil PCP peut être lié à plusieurs serveurs PCP. Par défaut, un profil PCP avec des paramètres par défaut est lié à tous les serveurs PCP. Un profil PCP que vous liez à un serveur PCP remplace les paramètres de profil PCP par défaut de ce serveur. Un profil PCP par défaut possède les paramètres suivants :
  - Mappage : activé
  - Homologue : activé
  - Durée de vie minimale de la carte : 120 secondes
  - Durée de vie maximale maximale : 86400 secondes
  - Nombre d'annonces : 10
  - Tierce partie : désactivée
- Créez un serveur PCP et liez-y un profil PCP. Créez un serveur PCP sur l'appliance NetScaler pour écouter les demandes et les messages liés au PCP provenant des abonnés. Une adresse IP de sous-réseau (SNIP) doit être attribuée à un serveur PCP pour y accéder. Par défaut, un serveur

PCP écoute sur le port 5351.

- Liez le serveur PCP à un groupe LSN d'une configuration LSN. Liez le serveur PCP créé à un groupe LSN d'une configuration LSN en définissant le paramètre PCP Server pour spécifier le serveur PCP créé. Le serveur PCP créé n'est accessible qu'aux abonnés de ce groupe LSN. Remarque : Un serveur PCP destiné à une configuration NAT à grande échelle ne traite pas les demandes des abonnés identifiés à partir des règles ACL.

Pour créer un profil PCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

Pour créer un serveur PCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Exemple de configuration pour DS-LITE

Dans l'exemple de configuration suivant, le serveur PCP PCP-SERVER-1, dont les paramètres PCP proviennent de PCP-DSLITE-PROFILE-1, est lié au groupe LSN LSN-DSLITE-GROUP-1. Le PCP-SERVER-9 traite les requêtes PCP des abonnés IPv4 derrière les appareils B4 du réseau 2001:DB8 : : 3:0 /100.

Exemple de configuration :

```
add pcp profile PCP-DSLITE-PROFILE-1 -minMapLife 300
Done
add pcp server PCP-DSLITE-SERVER-1 192.0.3.10  -pcpProfile PCP-DSLITE-
    PROFILE-1
```



```
Done
add lsn client LSN-DSLITE-CLIENT-1
Done
bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
Done
add lsn pool LSN-DSLITE-POOL-1
Done
bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6
Done
add lsn group LSN-DSLITE-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -poolname  PCP-NAT64-SERVER-1
Done
<!--NeedCopy-->
```

NAT64 à grande échelle

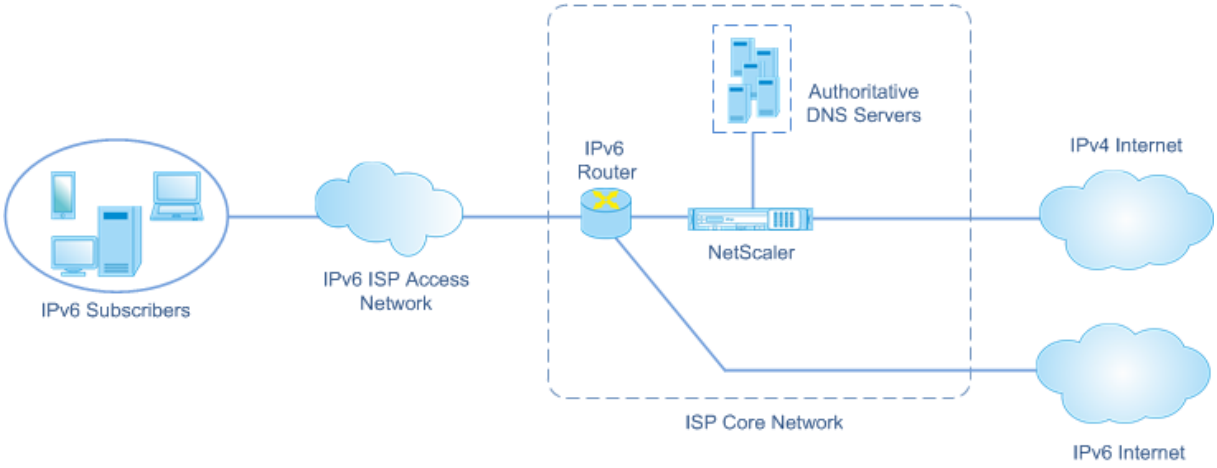
May 5, 2023

En raison de l'épuisement imminent des adresses IPv4, les FAI ont commencé à passer à l'infrastructure IPv6. Mais pendant la transition, les fournisseurs d'accès Internet doivent continuer à prendre en charge le protocole IPv4 en même temps que le protocole IPv6, car la majeure partie de l'Internet public utilise toujours le protocole IPv4. NAT64 à grande échelle est une solution de transition IPv6 destinée aux fournisseurs d'accès Internet dotés d'une infrastructure IPv6 afin de connecter leurs abonnés IPv6 uniquement à Internet IPv4. DNS64 est une solution permettant la découverte de domaines uniquement IPv6 par des clients utilisant uniquement IPv6. Le DNS64 est utilisé avec le protocole NAT64 à grande échelle pour permettre une communication fluide entre les clients uniquement IPv6 et les serveurs uniquement IPv6.

Une appliance NetScaler implémente des protocoles NAT64 et DNS64 à grande échelle et est conforme aux RFC 6145, 6146, 6147, 6052, 3022, 2373, 2765 et 2464.

Architecture

L'architecture NAT64 d'un fournisseur de services Internet utilisant une appliance NetScaler consiste en des abonnés IPv6 accédant à Internet IPv4 via une appliance NetScaler déployée sur le réseau central du fournisseur de services Internet. Les abonnés IPv6 sont connectés au réseau central du FAI via le réseau d'accès IPv6 uniquement du FAI.



La fonctionnalité NAT64 à grande échelle d'une appliance NetScaler permet la communication entre les clients IPv6 et les serveurs IPv4 via la traduction de paquets IPv6 vers IPv4, et vice versa, tout en conservant les informations de session sur l'appliance NetScaler. La fonctionnalité NetScaler DNS64 représente les domaines uniquement IPv4 aux abonnés IPv6 en synthétisant les enregistrements DNS AAAA pour les domaines uniquement IPv4 et en les envoyant aux abonnés.

Le NAT64 à grande échelle comporte deux composants principaux : le préfixe NAT64 et le pool NAT IPv4. DNS64 possède un composant principal, le préfixe DNS64, qui a la même valeur que le préfixe NAT64.

Lors de la réception d'une demande AAAA d'un abonné IPv6 uniquement pour un nom de domaine hébergé sur un serveur Web uniquement IPv4 sur Internet, la fonctionnalité NetScaler DNS64 synthétise un enregistrement AAAA pour le nom de domaine et l'envoie à l'abonné. L'enregistrement AAAA est synthétisé en concaténant le préfixe DNS64 (qui est défini sur le préfixe NAT64) et l'adresse IPv4 réelle du nom de domaine.

L'abonné dispose désormais d'une adresse de destination IPv6 qui correspond au nom de domaine souhaité. L'abonné envoie la demande à l'adresse IPv6 synthétisée. À la réception de la requête IPv6, la fonctionnalité NetScaler NAT64 à grande échelle traduit le paquet de requête IPv6 en un paquet de requête IPv4. Le protocole NAT64 à grande échelle définit l'adresse de destination de la demande IPv4 comme adresse IPv4, qui est extraite de l'adresse de destination de la demande IPv6 en supprimant le préfixe NAT64 de l'adresse IPv6. Le port de destination est conservé à partir de la requête IPv6. Large Scale NAT64 définit également l'adresse IP source:port source du paquet IPv4 sur l'adresse IP NAT:port NAT sélectionné dans le pool NAT configuré.

L'appliance conserve un enregistrement de toutes les sessions actives qui utilisent la fonctionnalité NAT64 à grande échelle. Ces sessions sont appelées sessions NAT64 à grande échelle. L'appliance gère également les mappages entre l'adresse et le port IPv6 de l'abonné, et l'adresse et le port NAT IPv4, pour chaque session NAT64 à grande échelle. Ces mappages sont appelés mappages NAT64 à grande échelle. À partir d'entrées de session NAT64 à grande échelle et d'entrées de mappage NAT64 à grande échelle, l'appliance NetScaler reconnaît qu'un paquet de réponse (reçu depuis Internet) appartient à une session NAT64 particulière.

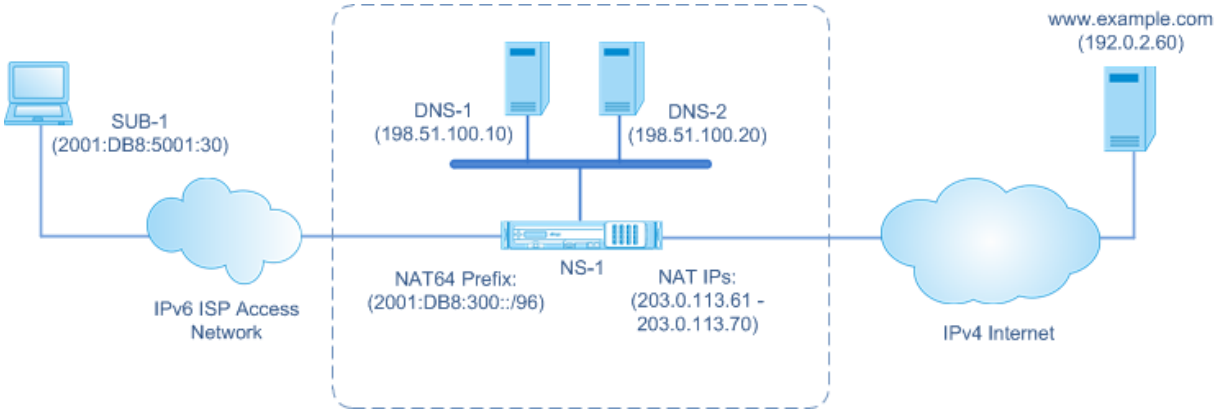
Lorsque l'appliance reçoit un paquet de réponse IPv4 appartenant à une session NAT64 particulière, elle utilise les informations stockées dans la session NAT64 pour traduire le paquet IPv4 en paquet IPv6, puis envoie le paquet de réponse IPv6 à l'abonné.

Exemple : Flux de trafic du déploiement de NAT64 et DNS64

Prenons l'exemple d'un déploiement à grande échelle de NAT64 et DNS64 comprenant l'appliance NetScaler NS-1 et deux serveurs DNS locaux, DNS-1 et DNS-2, dans le réseau central d'un fournisseur de services Internet, et un abonné IPv6 SUB-1. Le SUB-1 est connecté au NS-1 via le réseau d'accès IPv6 du fournisseur de services Internet. Le NS-1 inclut des configurations NAT64 et DNS64 à grande échelle pour permettre la communication entre les abonnés IPv6 SUB-1 et les hôtes IPv4 (internes et externes).

La configuration NAT64 à grande échelle inclut un préfixe NAT64 (2001:DB 8:300 : :/96) et un pool NAT IPv4 pour la traduction des requêtes IPv6 en requêtes IPv4 et des réponses IPv4 en réponses IPv6.

La configuration DNS64 inclut un serveur virtuel d'équilibrage de charge DNS LBVS-DNS64-1 (2001:DB 8:9999 : :99) et un préfixe DNS64 (2001:DB 8:300 : :/96). LBVS-DNS64-1 représente les serveurs DNS locaux DNS-1 et DNS-2 pour les abonnés du fournisseur de services Internet. Le préfixe DNS64, qui a la même valeur que le préfixe NAT64, est utilisé pour synthétiser les enregistrements DNS AAAA à partir des enregistrements DNS A reçus des serveurs DNS DNS-1 et DNS-2. Le NS-1 répond par un enregistrement AAAA synthétisé à SUB-1 pour une requête DNS visant à résoudre un hôte IPv4.



Flux de trafic DNS64

Le trafic circule entre l'abonné IPv6 SUB-1 et le site `www.example.com`, qui réside sur un serveur Web uniquement IPv4 sur Internet, comme suit :

1. L'abonné IPv6 SUB-1 envoie une requête DNS AAAA `www.example.com` à son serveur DNS désigné (2001:DB 8:9999 : :99).
2. Le serveur virtuel d'équilibrage de charge DNS LBVS-DNS64-1 (2001:DB 8:9999 : :99) sur l'appliance NetScaler NS1 reçoit la demande AAAA. L'algorithme d'équilibrage de charge de LBVS-DNS64-1 sélectionne le serveur DNS DNS-1 et lui transmet la requête AAAA.
3. Le DNS-1 renvoie un enregistrement vide ou un message d'erreur, car aucun enregistrement AAAA n'est disponible pour. `www.example.com`
4. Étant donné que l'option DNS64 est activée sur LBVS-DNS64-1 et que la requête AAAA du CL1 correspond à la condition spécifiée dans DNS64-Policy-1, NS1 envoie une demande DNS A à DNS-1 pour l'adresse IPv4 de. `www.example.com`
5. Le DNS-1 répond avec l'enregistrement A de 192.0.2.60 pour. `www.example.com`
6. Le module DNS64 sur NS1 synthétise un enregistrement AAAA pour `www.example.com` en concaténant le préfixe DNS64 (2001:DB 8:300 : :/96) associé à LBVS-DNS64-1, et l'adresse IPv4 (192.0.2.60) pour = 2001:DB 8:300 : :192.0.2.60 `www.example.com`
7. NS1 envoie l'enregistrement AAAA synthétisé au client IPv6 CL1. NS1 met également en cache l'enregistrement A dans sa mémoire. NS1 utilise l'enregistrement A mis en cache pour synthétiser les enregistrements AAAA pour les demandes AAAA suivantes.

Flux de trafic NAT64

1. L'abonné IPv6 SUB-1 envoie une demande à 2001:DB 8:5001:30. `www.example.com` Le paquet IPv6 contient :
   - Adresse IP source = 2001:DB 8:5001:30
   - Port source = 2552
   - Adresse IP de destination = 2001:DB 8:300 : :192.0.2.60
   - Port de destination = 80
2. L'abonné IPv6 SUB-1 envoie une demande à 2001:DB 8:5001:30. `www.example.com` Le paquet IPv6 contient :
   - Adresse IP source = 2001:DB 8:5001:30
   - Port source = 2552
   - Adresse IP de destination = 2001:DB 8:300 : :192.0.2.60
   - Port de destination = 80
3. Lorsque NS-1 reçoit le paquet IPv6, le module NAT64 à grande échelle crée un paquet de requête IPv4 traduit avec :

- Adresse IP source = L'une des adresses IPv4 disponibles dans le pool NAT configuré (203.0.113.61)
- Port source = L'un des ports disponibles avec l'adresse IPv4 NAT allouée (3002)
- Adresse IP de destination = adresse IPv4 extraite de l'adresse de destination de la requête IPv6 en supprimant le préfixe NAT64 (2001:DB 8:300 : :/96) de l'adresse IPv6 (192.0.2.60)
- Port de destination = port de destination de la requête IPv6 (80)

4. Le module NAT64 à grande échelle crée également des entrées de mappage et de session pour ce flux NAT64 à grande échelle. Les entrées de session et de mappage incluent les informations suivantes :

   - Adresse IP source du paquet IPv6 = 2001:DB 8:5001:30
   - Port source du paquet IPv6 = 2552
   - Adresse IP NAT = 203.0.113.61
   - Port NAT = 3002
   - Le NS-1 envoie le paquet IPv4 résultant vers sa destination sur Internet.

5. À la réception du paquet de demande, le serveur `www.example.com` traite le paquet et envoie un paquet de réponse à NS-1. Le paquet de réponse IPv4 contient :

   - Adresse IP source = 192.0.2.60
   - Port source = 80
   - Adresse IP de destination = 203.0.113.61
   - Port de destination = 3002

6. À la réception du paquet de réponse IPv4, le NS-1 examine le mappage NAT64 à grande échelle et les entrées de session et constate que le paquet de réponse IPv4 appartient à une session NAT64 à grande échelle. Le module NAT64 à grande échelle crée un paquet de réponse IPv6 traduit :

   - Adresse IP source = 2001:DB 8:300 : :192.0.2.60
   - Port source = 80
   - Adresse IP de destination = 2001:DB 8:5001:30
   - Port de destination = 2552

7. NS-1 envoie la réponse IPv6 traduite au client SUB-1.

Fonctionnalités NAT64 à grande échelle prises en charge sur les appliances NetScaler

Le protocole NAT64 à grande échelle sur une appliance NetScaler prend en charge l'ensemble de fonctionnalités LSN standard. Pour plus d'informations sur ces fonctionnalités LSN, voir Architecture LSN.

Voici quelques-unes des fonctionnalités NAT64 à grande échelle prises en charge par les appliances NetScaler :

- ALG. Support de la passerelle ALG (Application Layer Gateway) pour les protocoles SIP, RTSP, FTP, ICMP et TFTP.
- NAT déterministique/fixe. Prise en charge de la pré-allocation de blocs de ports aux abonnés afin de minimiser la journalisation.
- Cartographie. Prise en charge du mappage indépendant du point de terminaison (EIM), du mappage dépendant de l'adresse (ADM) et du mappage dépendant du port d'adresse (APDM).
- Filtrage. Prise en charge du filtrage indépendant du point de terminaison (EIF), du filtrage dépendant de l'adresse (ADF) et du filtrage dépendant du port d'adresse (APDF).
- Quotas. Limites configurables du nombre de ports, de sessions par abonné et de sessions par groupe LSN.
- Cartographie statique. Prise en charge de la définition manuelle d'un mappage NAT64 à grande échelle.
- Hairpin Flow. Prise en charge de la communication entre les abonnés ou les hôtes internes à l'aide d'adresses IP NAT.
- Connexions 464XLAT. Prise en charge de la communication entre les applications IPv4 uniquement sur les hôtes abonnés IPv6 et les hôtes IPv4 sur Internet via le réseau IPv6.
- Préfixes NAT64 et DNS64 de longueur variable. L'appliance NetScaler prend en charge la définition de préfixes NAT64 et DNS64 de longueurs de 32, 40, 48, 56, 64 et 96.
- Préfixes NAT64 et DNS64 multiples. L'appliance NetScaler prend en charge plusieurs préfixes NAT64 et DNS64.
- Clients LSN. Prise en charge de la spécification ou de l'identification des abonnés pour un système NAT64 à grande échelle à l'aide de préfixes IPv6 et de règles ACL6 étendues.
- Journalisation. Support pour la journalisation des sessions NAT64 pour les forces de l'ordre. En outre, les éléments suivants sont également pris en charge pour la journalisation.
  - **SYSLOG fiable**. Prise en charge de l'envoi de messages SYSLOG via TCP à des serveurs de journalisation externes pour un mécanisme de transport plus fiable.
  - **Équilibrage de charge des serveurs de journaux**. Prise en charge de l'équilibrage de charge des serveurs de journaux externes afin d'empêcher le stockage de messages de journal redondants.
  - **Journalisation minimale**. Les configurations LSN déterministes ou les configurations LSN dynamiques avec bloc de ports réduisent considérablement le volume de journaux NAT64 à grande échelle.
  - **Enregistrement des informations MSISDN.** Prise en charge de l'inclusion des informations MSISDN des abonnés dans des journaux NAT64 à grande échelle afin d'identifier et de suivre l'activité des abonnés sur Internet.

Points à prendre en compte lors de la configuration du NAT64 à grande échelle

May 5, 2023

Avant de commencer à configurer NAT64 et DNS64 à grande échelle, tenez compte des points suivants :

1. Assurez-vous de bien comprendre les différents composants du NAT64 à grande échelle, décrits dans les RFC.
2. L'appliance NetScaler prend uniquement en charge les ALG suivants pour le NAT64 à grande échelle :
   - FTP
   - TFTP
   - ICMP
   - SIP
   - RTSP
3. Dans une configuration à haute disponibilité composée de deux appliances NetScaler, la synchronisation de sessions NAT64 de grande envergure (mise en miroir des connexions) n'est pas prise en charge.

Configuration de DNS64

May 5, 2023

La création des entités requises pour une configuration NAT64 dynamique sur l'appliance NetScaler implique les procédures suivantes :

- Ajoutez des services DNS. Les services DNS sont des représentations logiques des serveurs DNS pour lesquels l'appliance NetScaler fait office de serveur proxy DNS. Pour plus d'informations sur la définition des paramètres facultatifs d'un service, voir Équilibrage de charge.
- Ajouter une action DNS64 et une stratégie DNS64, puis liez l'action DNS64 à la stratégie DNS64. Une politique DNS64 spécifie les conditions à mettre en correspondance avec le trafic pour le traitement DNS64 conformément aux paramètres de l'action DNS64 associée. L'action DNS64 spécifie le préfixe DNS64 obligatoire et les paramètres facultatifs de règle d'exclusion et de règle mappée.
- Créez un serveur virtuel d'équilibrage de charge DNS et liez-y les services DNS et la politique DNS64. Le serveur virtuel d'équilibrage de charge DNS agit comme un serveur proxy DNS pour les serveurs DNS représentés par les services DNS liés. Le trafic arrivant sur le serveur virtuel est mis en correspondance avec la stratégie DNS64 liée pour le traitement DNS64. Pour plus

d'informations sur la définition des paramètres facultatifs d'un serveur virtuel d'équilibrage de charge, voir Équilibrage de charge.

> **Remarque**
>
> L'interface de ligne de commande comporte des commandes distinctes pour ces deux tâches, mais l'interface graphique les combine dans une seule boîte de dialogue.

- Activez la mise en cache des enregistrements DNS. Activez le paramètre global pour que l'appliance NetScaler mette en cache les enregistrements DNS, qui sont obtenus via des opérations de proxy DNS. Pour plus d'informations sur l'activation de la mise en cache des enregistrements DNS, consultez Activation de la mise en cache des enregistrements DNS.

Pour créer un service de type DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <name> <IP> <serviceType> <port> …
<!--NeedCopy-->
```

Pour créer une action DNS64 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add dns action64 <actionName> -Prefix <ipv6_addr|*> [-mappedRule <
   expression>] [-excludeRule <expression>]
<!--NeedCopy-->
```

Pour créer une politique DNS64 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add dns policy64 <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Pour créer un serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> DNS <IPAddress> <port> -dns64 (ENABLED | DISABLED
   ) [-bypassAAAA ( YES | NO)] …
<!--NeedCopy-->
```


Pour lier les services DNS et la politique DNS64 au serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb vserver <name> <serviceName> ...

bind lb vserver <name> -policyName <string> -priority <positive_integer> ...
<!--NeedCopy-->
```

Exemple de configuration :

```
add service SVC-DNS-1 203.0.113.50 DNS 53
Done
add service SVC-DNS-2 203.0.113.60 DNS 53
Done
add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
Done
add dns Policy64 DNS64-Policy-1 -rule "CLIENT.IPv6.SRC.IN_SUBNET(2001:DB8:5001::/64)" -action DNS64-Action-1
Done
add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
Done
bind lb vserver LBVS-DNS64-1 SVC-DNS-1
Done
bind lb vserver LBVS-DNS64-1 SVC-DNS-2
Done
bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
Done
<!--NeedCopy-->
```

Configuration de Large Scaler NAT64

May 5, 2023

Une configuration NAT64 à grande échelle sur une appliance NetScaler utilise les jeux de commandes LSN. Dans une configuration NAT64 à grande échelle, l'entité cliente LSN spécifie l'adresse IPv6 ou l'adresse réseau IPv6, ou les règles ACL6, pour identifier les abonnés IPv6. Une configuration NAT64 inclut également un profil IPv6, qui spécifie un préfixe NAT64.

La configuration de NAT64 sur une appliance NetScaler comprend les tâches suivantes :

- Définissez les paramètres LSN globaux. Les paramètres globaux incluent la quantité de mémoire NetScaler réservée à la fonctionnalité LSN et la synchronisation des sessions LSN dans une configuration haute disponibilité.
- Créez une entité cliente LSN pour identifier le trafic provenant des abonnés IPv6. L'entité cliente LSN fait référence à un ensemble d'abonnés IPv6. L'entité cliente inclut des adresses IPv6 ou des préfixes réseau IPv6, ou des règles ACL6, pour identifier le trafic provenant de ces abonnés. Un client LSN ne peut être lié qu'à un seul groupe LSN. L'interface de ligne de commande comporte deux commandes permettant de créer une entité cliente LSN et de lier un abonné à l'entité cliente LSN. L'interface graphique combine ces deux opérations sur un seul écran.
- Créez un pool LSN et liez des adresses IP NAT à celui-ci. Un pool LSN définit un pool d'adresses IP NAT à utiliser par l'appliance NetScaler pour exécuter des opérations NAT64 à grande échelle. L'interface de ligne de commande comporte deux commandes permettant de créer un pool LSN et de lier des adresses IP NAT au pool LSN. L'interface graphique combine ces deux opérations sur un seul écran.
- Créez un profil IP6 LSN. Un profil IP6 LSN définit le préfixe NAT64 pour une configuration NAT64 à grande échelle.
- (Facultatif) Créez un profil de transport LSN pour un protocole spécifié. Un profil de transport LSN définit différents délais et limites, tels que le nombre maximal de sessions NAT64 à grande échelle et l'utilisation maximale des ports qu'un abonné peut avoir pour un protocole donné. Vous liez un profil de transport LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil de transport LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP est lié à un groupe LSN lors de sa création. Ce profil est appelé profil de transport par défaut. Un profil de transport LSN que vous liez à un groupe LSN remplace le profil de transport LSN par défaut pour ce protocole.
- (Facultatif) Créez un profil d'application LSN pour un protocole spécifié et liez un ensemble de ports de destination à celui-ci. Un profil d'application LSN définit les contrôles de mappage LSN et de filtrage LSN d'un groupe pour un protocole donné et pour un ensemble de ports de destination. Pour un ensemble de ports de destination, vous liez un profil LSN pour chaque protocole (TCP, UDP et ICMP) à un groupe LSN. Un profil peut être lié à plusieurs groupes LSN. Un profil d'application LSN lié à un groupe LSN s'applique à tous les abonnés d'un client LSN lié au même groupe. Par défaut, un profil d'application LSN avec des paramètres par défaut pour les protocoles TCP, UDP et ICMP pour tous les ports de destination est lié à un groupe LSN lors de sa création. Ce profil est appelé profil d'application par défaut. Lorsque vous liez un profil d'application LSN, avec un ensemble spécifié de ports de destination, à un groupe LSN, le profil lié remplace le profil d'application LSN par défaut pour ce protocole sur cet ensemble de ports de destination. L'interface de ligne de commande comporte deux commandes permettant de créer un profil d'application LSN et de lier un ensemble de ports de destination au profil d'application LSN. L'interface graphique combine ces deux opérations sur un seul écran.

- Créez un groupe LSN et liez des pools LSN, un profil IPv6 LSN, des profils de transport LSN (facultatifs) et des profils d'application LSN (facultatifs) au groupe LSN. Un groupe LSN est une entité composée d'un client LSN, d'un profil IPv6 LSN, d'un ou de plusieurs pools LSN, d'un ou de plusieurs profils de transport LSN et de profils d'application LSN. Des paramètres sont affectés à un groupe, tels que la taille du bloc de ports et la journalisation des sessions LSN. Les paramètres s'appliquent à tous les abonnés d'un client LSN lié au groupe LSN. Un seul profil IPv6 LSN peut être lié à un groupe LSN, et un profil LSN IPv6 lié à un groupe LSN ne peut pas être lié à d'autres groupes LSN. Seuls les pools LSN et les groupes LSN avec les mêmes paramètres de type NAT peuvent être liés entre eux. Plusieurs pools LSN peuvent être liés à un groupe LSN. Une seule entité cliente LSN peut être liée à un groupe LSN, et une entité cliente LSN liée à un groupe LSN ne peut pas être liée à d'autres groupes LSN. L'interface de ligne de commande comporte deux commandes permettant de créer un groupe LSN et de lier des pools LSN, des profils de transport LSN et des profils d'application LSN au groupe LSN. L'interface graphique combine ces deux opérations sur un seul écran.

Configuration à l'aide de la ligne de commande

Vous pouvez créer différentes configurations à l'aide de l'interface de ligne de commande. Suivez les étapes ci-dessous.

Pour créer un client LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn client <clientname

show lsn client
<!--NeedCopy-->
```

Pour lier un réseau IPv6 ou une règle ACL6 à un client LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
   string>)

show lsn client
<!--NeedCopy-->
```


Pour créer un pool de réseaux locaux à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn pool <poolname>

show lsn pool <poolname>
<!--NeedCopy-->
```

Pour lier des adresses IP NAT à un pool LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

> **Remarque**
>
> Pour supprimer les adresses IP NAT (adresses IP LSN) d'un pool LSN, utilisez la commande unbind lsn pool.

Pour configurer un profil LSN IPv6 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn ip6profile <name>  -type NAT64 -natprefix <ipv6_addr|*>

show lsn ip6profile
<!--NeedCopy-->
```

Pour créer un profil de transport LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```


Pour créer un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )]

show lsn appsprofile
<!--NeedCopy-->
```

Pour lier une plage de ports de protocole d'application à un profil d'application LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

Pour créer un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
    DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging(
    ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
    sessionSync ( ENABLED | DISABLED )] [-snmptraplimit<positive_integer
    >] [-ftp ( ENABLED | DISABLED )] [-sipalg ( ENABLED | DISABLED )] [-
    rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]

show lsn group
<!--NeedCopy-->
```

Pour lier des profils de protocole LSN et des pools LSN à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -httphdrlogprofilename <string> | -appsprofilename <
    string> | -sipalgprofilename <string> | rtspalgprofilename <string>)
```



```
2
3 show lsn group
4 <!--NeedCopy-->
```

Exemples de configurations NAT64 à grande échelle

Voici quelques exemples de configurations de NAT64 à grande échelle :

Configuration NAT64 simple à grande échelle avec paramètres par défaut :

```
1 add lsn client LSN-NAT64-CLIENT-1
2
3 bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
4
5 add lsn pool LSN-NAT64-POOL-1
6
7 bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
8
9 add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96
10
11 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1
12
13 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
14
15 <!--NeedCopy-->
```

Configuration NAT64 simple à grande échelle avec une règle ACL6 étendue pour identifier les abonnés :

```
1 add ns acl6 LSN-NAT64-ACL-2 ALLOW  -srcIPv6 = 2001:DB8:5002::20 - 2001:
    DB8:5002::200
2
3 apply acl6s
4
5 add lsn client LSN-NAT64-CLIENT-2
6
7 bind lsn client LSN-NAT64-CLIENT-2  -acl6name LSN-NAT64-ACL-2
8
9 add lsn pool LSN-NAT64-POOL-2
10
11 bind lsn pool LSN-NAT64-POOL-2 203.0.113.5-203.0.113.10
12
```



```
13 add lsn ip6profile LSN-NAT64-PROFILE-2 -type NAT64 -natprefix 2001:DB8
      :302::/96
14
15 add lsn group LSN-NAT64-GROUP-2 -clientname LSN-NAT64-CLIENT-2 -
      ip6profile LSN-NAT64-PROFILE-2
16
17 bind lsn group LSN-NAT64-GROUP-2 -poolname LSN-NAT64-POOL-2
18
19 <!--NeedCopy-->
```

Configuration NAT64 à grande échelle avec allocation déterministe des ressources NAT :

```
1  add lsn client LSN-NAT64-CLIENT-7
2
3  bind lsn client LSN-NAT64-CLIENT-7 -network6 2001:DB8:1002::7/128
4
5  add lsn pool LSN-NAT64-POOL-7 -nattype DETERMINISTIC
6
7  bind lsn pool LSN-NAT64-POOL-7 203.0.113.24-203.0.113.27
8
9  add lsn ip6profile LSN-NAT64-PROFILE-7 -type NAT64 -natprefix 2001:DB8
      :307::/96
10
11 add lsn group LSN-NAT64-GROUP-7 -clientname LSN-NAT64-CLIENT-7 -
      ip6profile LSN-NAT64-PROFILE-7 -nattype DETERMINISTIC -portblocksize
       256
12
13 bind lsn group LSN-NAT64-GROUP-7 -poolname LSN-POOL-7
14
15 <!--NeedCopy-->
```

Configuration des passerelles de la couche application pour NAT64 à grande échelle

May 5, 2023

Pour certains protocoles de couche application, les adresses IP et les numéros de port du protocole sont également communiqués dans la charge utile du paquet. La passerelle de couche application d'un protocole analyse la charge utile du paquet et apporte les modifications nécessaires pour garantir que le protocole continue de fonctionner sur un protocole NAT64 à grande échelle.

L'appliance NetScaler prend en charge le protocole ALG pour les protocoles NAT64 à grande échelle

suivants :

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Passerelle de couche d'application pour les protocoles FTP, ICMP et TFTP

January 21, 2021

Vous pouvez activer ou désactiver ALG pour le protocole FTP pour une configuration NAT64 à grande échelle en activant ou en désactivant l'option ALG FTP du groupe LSN de la configuration.

ALG pour le protocole ICMP est activé par défaut et aucune disposition ne permet de le désactiver.

ALG pour le protocole TFTP est désactivé par défaut. TFTP ALG est activé automatiquement pour une configuration NAT64 à grande échelle lorsque vous liez un profil d'application UDP LSN, avec mappage indépendant du point de terminaison, filtrage indépendant du point de terminaison et port de destination 69 (port bien connu pour TFTP), au groupe LSN.

Passerelle de couche d'application pour le protocole SIP

May 5, 2023

L'utilisation du protocole NAT64 à grande échelle avec le protocole SIP (Session Initiation Protocol) est complexe, car les messages SIP contiennent des adresses IP dans les en-têtes SIP ainsi que dans le corps du SIP. Lorsque le LSN est utilisé avec SIP, les en-têtes SIP contiennent des informations sur l'appelant et le récepteur, et l'appareil traduit ces informations pour les masquer au réseau extérieur. Le corps du SIP contient les informations du protocole SDP (Session Description Protocol), qui incluent les adresses IP et les numéros de port pour la transmission du média. Le SIP ALG pour NAT64 à grande échelle est conforme aux normes RFC 3261, RFC 3581, RFC 4566 et RFC 4475.

> **Remarque**
>
> Le SIP ALG est pris en charge dans une appliance autonome NetScaler, dans une configuration haute disponibilité NetScaler, ainsi que dans une configuration de cluster NetScaler.

Limites du SIP ALG

SIP ALG pour NAT64 à grande échelle présente les limites suivantes :

- Seule la charge utile SDP est prise en charge.
- Les éléments suivants ne sont pas pris en charge :
  - Adresses IP de multidiffusion
  - SDP crypté
  - EXPÉDITION TLS
  - Traduction du FQDN
  - Authentification de couche SIP
  - Domaines de trafic
  - Partitions d'administration
  - Carrosserie en plusieurs parties
  - Pliage en ligne

Configuration de SIP ALG

Vous devez configurer le SIP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration du LSN, voir Configuration NAT64 à grande échelle. Lors de la configuration de LSN, assurez-vous que vous :

- Définissez les paramètres suivants lors de l'ajout d'un profil d'application LSN :
  - Regroupement d'adresses IP = APPARIÉ
  - Mappage des adresses et des ports = INDÉPENDANT DU POINT DE TERMINAISON
  - Filtrage = INDÉPENDANT DU POINT DE TERMINAISON
- Créez un profil SIP ALG et assurez-vous de définir la plage de ports source ou la plage de ports de destination. Liez le profil SIP ALG au groupe LSN.
- Activez SIP ALG dans le groupe LSN.

Pour activer SIP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn group <groupname> -clientname <string> [-sipalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```


Pour activer SIP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn sipalgprofile <sipalgprofilename>[-dataSessionIdleTimeout <
    positive_integer>][-sipSessionTimeout <positive_integer>] [-
    registrationTimeout <positive_integer>] [-sipsrcportrange <port[-
    port]>] [-sipdstportrange <port[-port]>] [-openRegisterPinhole (
    ENABLED | DISABLED )] [-openContactPinhole ( ENABLED | DISABLED )]
    [-openViaPinhole ( ENABLED | DISABLED )] [-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP ) [-
    openRoutePinhole ( ENABLED | DISABLED )] [-rport ( ENABLED |
    DISABLED )]

show lsn sipalgprofile <sipalgprofilename
<!--NeedCopy-->
```

Exemple de configuration

Dans l'exemple de configuration NAT64 à grande échelle suivant, SIP ALG est activé pour le trafic TCP provenant des appareils abonnés du réseau 2001:DB 8:1003 : :/96.

```
add lsn client LSN-NAT64-CLIENT-9

Done
bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96

Done
add lsn pool LSN-NAT64-POOL-9

Done
bind lsn pool LSN-NAT64-POOL-9 203.0.113.90

Done
add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
    :309::/96

Done
add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
    mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done
add lsn sipalgprofile SIPALGPROFILE-9  -sipdstportrange 5060  -
    sipTransportProtocol TCP

```



```
Done
add lsn group LSN-NAT64-GROUP-9 -clientnameLSN-NAT64-CLIENT-9 -
    ip6profile LSN-NAT64-PROFILE-7 -sipalg ENABLED

Done
bind lsn group LSN-NAT64-GROUP-9 -poolnameLSN-NAT64-POOL-9
Done
bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
    PROFILE-9
Done
bind lsn group LSN-NAT64-GROUP-9 -sipalgprofilename SIPALGPROFILE-9
Done
<!--NeedCopy-->
```

Passerelle de couche application pour le protocole RTSP

May 5, 2023

Le protocole RTSP (Real Time Streaming Protocol) est un protocole au niveau de l'application pour le transfert de données multimédia en temps réel. Utilisé pour établir et contrôler des sessions multimédia entre les points de terminaison, le RTSP est un protocole de canal de contrôle entre le client multimédia et le serveur multimédia. La communication classique se fait entre un client et un serveur de streaming multimédia.

La diffusion de contenu multimédia d'un réseau privé vers un réseau public nécessite la traduction des adresses IP et des numéros de port sur le réseau. Les fonctionnalités de NetScaler incluent une passerelle de couche d'application (ALG) pour RTSP, qui peut être utilisée avec un NAT à grande échelle (LSN) pour analyser le flux multimédia et apporter les modifications nécessaires pour garantir que le protocole continue de fonctionner sur le réseau.

La manière dont la traduction des adresses IP est effectuée dépend du type et de la direction du message, ainsi que du type de média pris en charge par le déploiement client-serveur. Les messages sont traduits comme suit :

- Requête sortante : adresse IP privée vers une adresse IP publique appartenant à NetScaler appelée adresse IP LSN.
- Réponse entrante : adresse IP LSN vers adresse IP privée.
- Demande entrante : aucune traduction.
- Réponse sortante : adresse IP privée vers l'adresse IP du pool LSN.

> **Remarque**
>
> L'ALG RTSP est pris en charge dans une appliance autonome NetScaler, dans une configuration haute disponibilité NetScaler, ainsi que dans une configuration de cluster NetScaler.

Limites de RTSP ALG

Le RTSP ALG ne prend pas en charge les éléments suivants :

- Sessions RTSP multidiffusion
- Session RTSP via UDP
- Partitions d'administration
- Authentification RTSP
- Tunneling HTTP

Configuration de RTSP ALG

Configurez RTSP ALG dans le cadre de la configuration LSN. Pour obtenir des instructions sur la configuration du LSN, consultez la section Configuration de NAT64 à grande échelle. Lors de la configuration, assurez-vous de :

- Définissez les paramètres suivants lors de l'ajout d'un profil d'application LSN :
  - Regroupement d'adresses IP = APPARIÉ
  - Mappage des adresses et des ports = INDÉPENDANT DU POINT DE TERMINAISON
  - Filtrage = INDÉPENDANT DU POINT DE TERMINAISON
- Activer RTSP ALG dans le groupe LSN
- Créez un profil RTSP ALG et liez le profil RTSP ALG au groupe LSN

Pour activer RTSP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

Pour activer RTSP ALG pour une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
    positive_integer>] -rtspportrange <port[-port]> [-
    rtspTransportProtocol (TCP|UDP)]

show lsn rtspalgprofile <rtspalgprofilename>
<!--NeedCopy-->
```

Exemple de configuration RTSP ALG

L'exemple de configuration NAT64 à grande échelle suivant, RTSP ALG, est activé pour le trafic TCP provenant des appareils abonnés du réseau 2001:DB 8:1002 : :/96.

```
add lsn client LSN-NAT64-CLIENT-9
Done
bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96
Done
add lsn pool LSN-NAT64-POOL-9
Done
bind lsn pool LSN-NAT64-POOL-9 203.0.113.90
Done
add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
    :309::/96
Done
add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
    mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn rtspalgprofile RTSPALGPROFILE-9 -rtspIdleTimeout 1000 -
    rtspportrange 554
Done
add lsn group LSN-NAT64-GROUP-9 -clientname LSN-NAT64-CLIENT-9 -
    ip6profile LSN-NAT64-PROFILE-7 -rtspalg ENABLED
Done
bind lsn group LSN-NAT64-GROUP-9 -poolname LSN-NAT64-POOL-9
Done
bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
    PROFILE-9
Done
bind lsn group LSN-NAT64-GROUP-9  -rtspalgprofilename RTSPALGPROFILE-9
Done
<!--NeedCopy-->
```


Configuration des cartes NAT64 statiques à grande échelle

May 5, 2023

L'appliance NetScaler prend en charge la création manuelle de mappages NAT64, qui contiennent le mappage entre les informations suivantes :

- Adresse IP et port de l'abonné
- Adresse IP et port NAT

Les mappages NAT64 statiques à grande échelle sont utiles lorsque vous souhaitez vous assurer que les connexions IPv4 initiées vers une adresse IP NAT : port sont traduites en IPv6 et mappées vers l'adresse IP:port de l'abonné (par exemple, les serveurs Web situés sur le réseau interne).

Pour créer un mappage NAT64 à grande échelle à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort>  [<
    natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Cartes NAT64 statiques à grande échelle avec ports Wildcard

Une entrée de mappage NAT64 statique à grande échelle est généralement un mappage biunivoque entre une adresse IPv6 d'abonné : port et une adresse IPv4 NAT : port. Une entrée de mappage NAT64 statique biunivoque à grande échelle n'expose qu'un seul port de l'adresse IP de l'abonné à Internet.

Dans certaines situations, il peut être nécessaire d'exposer tous les ports (64 000, dans la limite du nombre maximum de ports d'une adresse IPv4 NAT) d'une adresse IP d'abonné à Internet (par exemple, un serveur hébergé sur un réseau interne et exécutant un service différent sur chaque port). Pour rendre ces services internes accessibles via Internet, vous devez exposer tous les ports du serveur à Internet.

L'un des moyens de répondre à cette exigence consiste à ajouter 64 000 entrées de mappage statiques individuelles, une entrée de mappage pour chaque port. La création de ces entrées est très fastidieuse et représente une tâche ardue. Ce grand nombre d'entrées de configuration peut également entraîner des problèmes de performances dans l'appliance NetScaler.

Une méthode plus simple consiste à utiliser des ports génériques dans une entrée de mappage statique. Il vous suffit de créer une entrée de mappage statique avec les paramètres du port NAT et du

port abonné définis sur le caractère générique (*), et le paramètre de protocole défini sur ALL, pour exposer tous les ports d'une adresse IP d'abonné pour tous les protocoles vers Internet.

Pour les connexions entrantes ou sortantes d'un abonné correspondant à une entrée de mappage statique générique, le port de l'abonné ne change pas après l'opération NAT. Lorsqu'une connexion à Internet initiée par un abonné correspond à une entrée de mappage statique générique, l'appliance NetScaler attribue un port NAT portant le même numéro que le port d'abonné à partir duquel la connexion est initiée. De même, un hôte Internet se connecte au port d'un abonné en se connectant au port NAT qui porte le même numéro que le port de l'abonné.

Pour configurer l'appliance NetScaler afin de fournir un accès à tous les ports d'une adresse IPv6 d'abonné, créez une carte statique générique avec les paramètres obligatoires suivants :

- Protocol=Tout
- Port d'abonné = *
- Port NAT = *

Dans une carte statique générique, contrairement à une carte statique un à un, la définition du paramètre IP NAT est obligatoire. De plus, l'adresse IP NAT attribuée à une carte statique générique ne peut être utilisée pour aucun autre abonné.

Pour créer une carte statique avec caractères génériques à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
     positive_integer>] [-destIP <ip_addr>
2
3 show lsn static
4 <!--NeedCopy-->
```

Dans l'exemple de configuration suivant d'une carte statique générique, tous les ports d'un abonné dont l'adresse IP est 2001:DB 8:5001 : :3 sont rendus accessibles via l'adresse IP NAT 203.0.11.33.

```
1 add lsn static NAT64-WILDCARD-STATIC-1 ALL 2001:DB8:5001::3 *
     203.0.113.33 *
2 Done
3 <!--NeedCopy-->
```

Enregistrement et surveillance NAT64 à grande échelle

May 5, 2023

Vous pouvez enregistrer des informations NAT64 à grande échelle pour diagnostiquer et résoudre les problèmes, et pour respecter les exigences légales. Vous pouvez surveiller les performances du déploiement NAT64 à grande échelle en utilisant des compteurs statistiques et en affichant les sessions en cours associées.

Enregistrement de données NAT64 à grande échelle

L'enregistrement d'informations NAT64 à grande échelle est nécessaire pour que les FAI respectent les exigences légales et identifient la source du trafic à tout moment.

Un message de journal pour une entrée de mappage NAT64 à grande échelle contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal.
- Horodatage.
- Type d'entrée (MAPPING).
- Si l'entrée de mappage a été créée ou supprimée.
- Adresse IP, port et ID de domaine de trafic de l'abonné.
- Adresse IP et port NAT.
- Nom du protocole.
- L'adresse IP de destination, le port et l'ID du domaine de trafic peuvent être présents, selon les conditions suivantes :
  - L'adresse IP et le port de destination ne sont pas enregistrés pour le mappage indépendant du point de terminaison.
  - Seule l'adresse IP de destination est enregistrée pour le mappage dépendant de l'adresse. Le port n'est pas enregistré.
  - L'adresse IP et le port de destination sont enregistrés pour un mappage dépendant du port d'adresse.

Un message de journal pour une session NAT64 à grande échelle contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage
- Type d'entrée (SESSION)
- Si la session est créée ou supprimée
- Adresse IP, port et ID de domaine de trafic de l'abonné
- Adresse IP et port NAT
- Nom du protocole
- Adresse IP de destination, port et ID de domaine de trafic

Le tableau suivant présente des exemples d'entrées de journal NAT64 à grande échelle de chaque

type stockées sur les serveurs de journaux configurés. Les entrées du journal indiquent qu'un abonné dont l'adresse IPv6 est 2001:db 8:5001 : :9 a été connecté à l'adresse IP de destination 23.0.0. 1:80 via l'adresse NAT IP:port 203.0.113. 63:45195 le 7 avril 2016, de 14:07:57 GMT à 14:010:59 GMT.

Type d'entrée de journal	Exemple d'entrée dans le journal
Création d'une session	**04/07/2016 : 14:07:57 GMT Informatif 0-PPE-10 : LSN LSN_SESSION 5532 0 par défaut : SESSION CRÉÉE Port IP du client : TD 2001:db 8:5001 : : 9-34937:0, Natip:NATPort 203.0.113. 63:45195, IP de destination : Port:TD 23.0.0. 1:0:80, Protocole : TCP**
Création d'un mappage	**04/07/2016 : 14:07:57 GMT Informatif 0-PPE-10 : LSN LSN_ADDR_MAPPING 5533 0 par défaut : ADM CREATED Client IP-Port : TD 2001:db 8:5001 : : 9-34937:0, Natip:NATPort 203.0.113. 63:45195, IP de destination : TD 23.0.0. 1:80, Protocole : TCP**
Suppression de session	**04/07/2016 : 14:10:59 GMT 0-PPE-10 : LSN LSN_SESSION 25012 0 par défaut : SESSION SUPPRIMÉE Port IP du client : TD 2001:db 8:5001 : : 9-34937:0, Natip:NATPort 203.0.113. 63:45195, IP de destination : Port:TD 23.0.0. 1:0:80, Protocole : TCP**
Suppression du mappage	**04/07/2016 : 14:10:59 GMT 0-PPE-10 : LSN LSN_ADDR_MAPPING 25013 0 par défaut : ADM DELETED Port IP du client : TD 2001:db 8:5001 : : 9-34937:0, IP natif : NATPort 203.0.113. 63:45195, IP de destination : Port:TD 23.0.0. 1:0:80, Protocole : TCP**

Étapes de configuration

Vous pouvez configurer la journalisation des informations NAT64 à grande échelle pour une configuration NAT64 à grande échelle en définissant les paramètres de journalisation et de journalisation de session des groupes LSN. Il s'agit de paramètres au niveau du groupe qui sont désactivés par défaut. L'appliance NetScaler enregistre les sessions NAT64 à grande échelle pour un groupe LSN uniquement

lorsque les paramètres de journalisation et de journalisation de session sont activés.

Le tableau suivant présente le comportement de journalisation d'un groupe LSN pour différents paramètres de journalisation et de journalisation de session.

Journalisation	Journalisation des sessions	Comportement d'enregistrement
Activé	Activé	Enregistre les entrées de mappage LSN ainsi que les sessions LSN
Activé	Désactivé	Enregistre les entrées de mappage LSN mais pas les sessions LSN
Désactivé	Activé	N'enregistre ni les entrées de mappage ni les sessions LSN

Pour enregistrer des informations NAT64 à grande échelle à l'aide de l'interface de ligne de commande

Pour définir les paramètres de journalisation et de journalisation de session lors de l'ajout d'un groupe LSN, à l'invite de commandes, tapez :

```
add lsn group <groupname> -clientname <string> [-logging (ENABLED|
    DISABLED)] [-sessionLogging (ENABLED|DISABLED)]

show lsn group
<!--NeedCopy-->
```

Pour définir les paramètres de journalisation et de journalisation de session pour un groupe LSN existant, à l'invite de commandes, tapez :

```
set lsn group <groupname> [-logging (ENABLED|DISABLED)] [-
    sessionLogging (ENABLED|DISABLED)]

show lsn group
<!--NeedCopy-->
```

Exemple de configuration

Dans cet exemple de configuration NAT64 à grande échelle, les paramètres de journalisation et de journalisation de session sont activés pour le groupe LSN LSN-NAT64-GROUP-1.

L'appliance NetScaler enregistre les informations de session NAT64 et de mappage à grande échelle pour les connexions des abonnés (sur le réseau 2001:DB 8:5001 : :/96).

Exemple de configuration :

```
add lsn client LSN-NAT64-CLIENT-1 Done
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96
Done
add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1  -logging ENABLED -sessionLogging
    ENABLED
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
<!--NeedCopy-->
```

Enregistrement des informations MSISDN pour un système NAT64 à grande échelle

Un numéro de répertoire d'abonnés intégré à une station mobile (MSISDN) est un numéro de téléphone identifiant de manière unique un abonné sur plusieurs réseaux mobiles. Le MSISDN est associé à un code de pays et à un code de destination national identifiant l'opérateur de l'abonné.

Vous pouvez configurer une appliance NetScaler pour inclure MsisDNS dans les entrées de journal LSN NAT64 à grande échelle pour les abonnés des réseaux mobiles. La présence de MSISDNS dans les journaux du LSN permet de retrouver plus rapidement et avec précision un abonné mobile qui a enfreint une politique ou une loi, ou dont les informations sont requises par des agences d'interception légales.

Les exemples d'entrées de journal LSN suivants incluent des informations MSISDN pour une connexion depuis un abonné mobile dans une configuration LSN. Les entrées du journal indiquent qu'un abonné mobile dont le MSISDN est E 164:5556543210 et l'adresse IPv6 est 2001:db 8:5001 : :9 a été connecté à l'adresse IP de destination 23.0.0. 1:80 via le port NAT 203.0.113. 63:45195 le 7 avril 2016, de 14:07:57 GMT à 14:010:59 GMT.

Type d'entrée de journal	Exemple d'entrée dans le journal
Création d'une session	**04/07/2016 : 14:07:57 GMT Informatif 0-PPE-10 : LSN LSN_SESSION 5532 0 par défaut : SESSION CRÉÉE**E 164:5556543210 Port IP du client : TD 2001:db 8:5001 : : 9-34937:0, Natip:NATPort 203.0.113. 63:45195**, IP de destination : Port:TD 23.0.0. 1:0:80, Protocole : TCP**
Création d'un mappage	**04/07/2016 : 14:07:57 GMT Informatif 0-PPE-10 : LSN LSN_ADDR_MAPPING 5533 0 par défaut : ADM CREATED**E 164:5556543210**Port IP du client : TD 2001:db 8:5001 : : 9-34937:0, Natip:NATPort 203.0.113. 63:45195, IP de destination : TD 23.0.0. 1:80, Protocole : TCP**
Suppression de session	**04/07/2016 : 14:10:59 GMT 0-PPE-10 : LSN LSN_SESSION 25012 0 par défaut : SESSION SUPPRIMÉE**E 164:5556543210 Port IP du client : TD 2001:db 8:5001 : : 9-34937:0, IP natif : NATPort 203.0.113. 63:45195**, IP de destination : Port:TD 23.0.0. 1:0:80, Protocole : TCP**
Suppression du mappage	**04/07/2016 : 14:10:59 GMT 0-PPE-10 : LSN LSN_ADDR_MAPPING 25013 0 par défaut : ADM DELETED**E 164:5556543210**Port IP du client : TD 2001:db 8:5001 : : 9-34937:0, Natip:NATPort 203.0.113. 63:45195, IP de destination : Port:TD 23.0.0. 1:0:80, Protocole : TCP**

Étapes de configuration

Effectuez les tâches suivantes pour inclure les informations MSISDN dans les journaux LSN :

- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre ID d'abonné au journal, qui indique s'il faut ou non inclure les informations MSISDN dans les journaux LSN d'une configuration LSN.
- Liez le profil de journal LSN à un groupe LSN d'une configuration LSN. Liez le profil de journal

LSN créé à un groupe LSN d'une configuration LSN en définissant le paramètre de nom du profil de journal sur le nom du profil de journal LSN créé. Les informations MSISDN sont incluses dans tous les journaux LSN relatifs aux abonnés mobiles de ce groupe LSN.

Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn logprofile <logprofilename> -logSubscriberID ( ENABLED |
   DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Pour lier un profil de journal LSN à un groupe LSN d'une configuration LSN NAT64 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Exemple de configuration

Dans cet exemple de configuration LSN NAT64, le paramètre ID d'abonné au journal est activé pour le profil de journal LSN LOG-PROFILE-MSISDN-1. LOG-PROFILE-MSISDN-1 est lié au groupe LSN LSN-NAT64-GROUP-1. Les informations MSISDN sont incluses dans les journaux de session LSN et de mappage LSN pour les connexions des abonnés mobiles (dans le réseau 2001:DB 8:5001 : :/96).

```
add lsn logprofile  LOG-PROFILE-MSISDN-1  -logSubscriberID ENABLED
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
   :300::/96
```



```
Done
add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1 -logprofilename  LOG-PROFILE-MSISDN-1
Done
<!--NeedCopy-->
```

Journalisation compacte pour un NAT à grande échelle

L'enregistrement des informations LSN est l'une des fonctions importantes dont les FAI ont besoin pour répondre aux exigences légales et être en mesure d'identifier la source du trafic à tout moment. Cela se traduit finalement par un énorme volume de données de journalisation, obligeant les FAI à réaliser d'importants investissements pour maintenir l'infrastructure de journalisation.

La journalisation compacte est une technique qui permet de réduire la taille du journal en utilisant un changement de notation impliquant des codes courts pour les noms d'événements et de protocoles. Par exemple, C pour le client, SC pour la session créée et T pour TCP. La journalisation compacte entraîne une réduction moyenne de 40 % de la taille des journaux.

Étapes de configuration

Effectuez les tâches suivantes pour enregistrer les informations LSN au format compact :

1. Créez un profil de journal LSN. Un profil de journal LSN inclut le paramètre Log Compact, qui indique si les informations doivent être enregistrées au format compact pour une configuration LSN.
2. Liez le profil de journal LSN à un groupe LSN d'une configuration LSN. Liez le profil de journal LSN créé à un groupe LSN d'une configuration LSN en définissant le paramètre Nom du profil de journal sur le nom du profil de journal LSN créé. Toutes les sessions et tous les mappages de ce groupe LSN sont enregistrés au format compact.

Pour créer un profil de journal LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```


Pour lier un profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Exemple de configuration pour NAT64 :

```
add lsn logprofile  LOG-PROFILE-COMPACT-1 -logCompact ENABLED
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
   :300::/96
Done
add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1  - logProfileName LOG-PROFILE-COMPACT-1
Done
<!--NeedCopy-->
```

Enregistrement des informations d'en-tête HTTP

L'appliance NetScaler peut enregistrer les informations d'en-tête de demande d'une connexion HTTP qui utilise la fonctionnalité NAT64 à grande échelle de NetScaler. Les informations d'en-tête suivantes d'un paquet de requête HTTP peuvent être enregistrées :

- URL à laquelle la requête HTTP est destinée
- Méthode HTTP spécifiée dans la requête HTTP
- Version HTTP utilisée dans la requête HTTP
- Adresse IPv6 de l'abonné qui a envoyé la requête HTTP

Les journaux d'en-tête HTTP peuvent être utilisés par les FAI pour voir les tendances liées au protocole HTTP parmi un ensemble d'abonnés. Par exemple, un fournisseur de services Internet peut utiliser cette fonctionnalité pour trouver le site Web le plus populaire parmi un ensemble d'abonnés.

Étapes de configuration

Effectuez les tâches suivantes pour configurer l'appliance NetScaler afin qu'elle enregistre les informations d'en-tête HTTP :

- Créez un profil de journal d'en-tête HTTP. Un profil de journal d'en-tête HTTP est un ensemble d'attributs d'en-tête HTTP (par exemple, URL et méthode HTTP) qui peuvent être activés ou désactivés pour la journalisation.
- Liez l'en-tête HTTP à un groupe LSN d'une configuration NAT64 à grande échelle. Liez le profil de journal d'en-tête HTTP à un groupe LSN d'une configuration LSN en définissant le paramètre de nom du profil de journal d'en-tête HTTP sur le nom du profil de journal d'en-tête HTTP créé. L'appliance NetScaler enregistre ensuite les informations d'en-tête HTTP de toutes les requêtes HTTP liées au groupe LSN. Un profil de journal d'en-tête HTTP peut être lié à plusieurs groupes LSN, mais un groupe LSN ne peut avoir qu'un seul profil de journal d'en-tête HTTP.

Pour créer un profil de journal d'en-tête HTTP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

Pour lier un profil de journal d'en-tête HTTP à un groupe LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```


Exemple de configuration

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done
add lsn client LSN-NAT64-CLIENT-1 Done
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
   :300::/96
Done
add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1 -httphdrlogprofilename HTTP-HEADER-LOG
   -1
Done
<!--NeedCopy-->
```

Affichage des sessions NAT64 à grande échelle en cours

Vous pouvez afficher les sessions NAT64 à grande échelle actuelles afin de détecter toute session indésirable ou inefficace sur l'appliance NetScaler. Vous pouvez afficher toutes les sessions NAT64 à grande échelle ou certaines d'entre elles en fonction des paramètres de sélection.

> **Remarque**
>
> Lorsque plus d'un million de sessions NAT64 à grande échelle existent sur l'appliance NetScaler, Citrix recommande d'utiliser les paramètres de sélection pour afficher les sessions NAT64 à grande échelle sélectionnées au lieu de les afficher toutes.

Pour afficher toutes les sessions NAT64 à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show lsn session  - nattype NAT64
<!--NeedCopy-->
```


Pour afficher des sessions NAT64 sélectives à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show lsn session  -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
    <string>] [-natIP <ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Affichage de statistiques NAT64 à grande échelle

Vous pouvez afficher des statistiques relatives au module NAT64 à grande échelle et évaluer ses performances ou résoudre des problèmes. Vous pouvez afficher un résumé des statistiques de toutes les configurations NAT64 à grande échelle ou d'une configuration NAT64 à grande échelle particulière. Les compteurs statistiques reflètent les événements survenus depuis le dernier redémarrage de l'appliance NetScaler. Tous ces compteurs sont remis à 0 lorsque l'appliance NetScaler est redémarrée.

Pour afficher les statistiques totales de NAT64 à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat lsn nat64
<!--NeedCopy-->
```

Pour afficher les statistiques d'une configuration NAT64 à grande échelle spécifiée à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat lsn group <groupname>
<!--NeedCopy-->
```

Effacement de sessions NAT64 à grande échelle

Vous pouvez supprimer toutes les sessions NAT64 à grande échelle indésirables ou inefficaces de l'appliance NetScaler. L'appliance libère immédiatement les ressources (telles que l'adresse IP NAT, le port et la mémoire) allouées à ces sessions, les rendant ainsi disponibles pour de nouvelles sessions.

L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions NAT64 à grande échelle ou certaines d'entre elles de l'appliance NetScaler.

Pour effacer toutes les sessions NAT64 à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
flush lsn session  -nattype NAT64

show lsn session  -nattype NAT64
<!--NeedCopy-->
```

Pour effacer des sessions NAT64 sélectives à grande échelle à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
flush lsn session  -nattype NAT64 [-network6 <ipv6_addr|*>] [-
   clientname <string>] [-natIP <ip_addr> [-natPort <port>]]

show lsn session  -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
    <string>] [-natIP <ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Exemple de configuration :

Effacez toutes les sessions NAT64 à grande échelle existantes sur une appliance NetScaler

```
flush lsn session   -nattype NAT64
Done
<!--NeedCopy-->
```

Efface toutes les sessions NAT64 à grande échelle liées à l'entité cliente LSN-NAT64-CLIENT-1

```
flush lsn session  -nattype NAT64 -clientname LSN-NAT64-CLIENT-1
Done
<!--NeedCopy-->
```

Efface toutes les sessions NAT64 à grande échelle liées à un réseau d'abonnés (2001:DB 8:5001 : :/96) de l'entité cliente LSN LSN-NAT64-CLIENT-2


```
flush lsn session -nattype NAT64 -network6 2001:DB8:5001::/96 -
   clientname LSN-NAT64-CLIENT-2
Done
<!--NeedCopy-->
```

Journalisation IPFIX

L'appliance NetScaler prend en charge l'envoi d'informations sur les événements LSN au format IPFIX (Internet Protocol Flow Information Export) vers l'ensemble configuré de collecteurs IPFIX. L'appliance utilise la fonctionnalité AppFlow existante pour envoyer des événements LSN au format IPFIX aux collecteurs IPFIX.

La journalisation basée sur IPFIX est disponible pour les événements suivants liés à NAT64 :

- Création ou suppression d'une session LSN.
- Création ou suppression d'une entrée de mappage LSN.
- Allocation ou désallocation de blocs de ports dans le contexte d'un NAT déterministe.
- Allocation ou désallocation de blocs de ports dans le contexte d'un NAT dynamique.
- Chaque fois que le quota de sessions d'abonnés est dépassé.

Points à prendre en compte avant de configurer la journalisation IPFIX

Avant de commencer à configurer IPsec ALG, tenez compte des points suivants :

- Vous devez configurer la fonctionnalité AppFlow et le ou les collecteurs IPFIX sur l'appliance NetScaler. Pour obtenir des instructions, reportez-vous à la section Configuration de la fonctionnalité AppFlow.

Étapes de configuration

Effectuez les tâches suivantes pour enregistrer les informations LSN au format IPFIX :

- **Activez la journalisation LSN dans la configuration AppFlow**. Activez le paramètre de journalisation LSN dans le cadre de la configuration d'AppFlow.
- **Créez un profil de journal LSN**. Un profil de journal LSN inclut le paramètre IPFIX qui active ou désactive les informations du journal au format IPFIX.
- **Liez le profil de journal LSN à un groupe LSN d'une configuration LSN**. Liez le profil du journal LSN à un ou plusieurs groupes LSN. Les événements liés au groupe LSN lié seront enregistrés au format IPFIX.

Pour activer la journalisation LSN dans la configuration AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set appflow param -lsnLogging ( ENABLED | DISABLED )

show appflow param
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide de la CLI à l'invite de commande, tapez

À l'invite de commande, tapez :

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Pour créer un profil de journal LSN à l'aide de l'interface graphique

Accédez à **Système** > **NAT à grande échelle** > **Profils**, cliquez sur l'onglet **Journal**, puis ajoutez un profil de journal.

Pour lier le profil de journal LSN à un groupe LSN d'une configuration LSN à l'aide de l'interface graphique

1. Accédez à **Système** > **NAT à grande échelle** > Groupe **LSN, puis ouvrez le groupeLSN.**
2. Dans **Paramètres avancés,** cliquez sur **+ Profil de journal** pour lier le profil de journal créé au groupe LSN.

Protocole de contrôle des ports pour NAT64 à grande échelle

May 5, 2023

Les appliances NetScaler prennent désormais en charge le protocole PCP (Port Control Protocol) pour le NAT à grande échelle (LSN). De nombreuses applications réservées aux abonnés d'un fournisseur de services Internet doivent être accessibles depuis Internet (par exemple, les appareils Internet des objets (IoT), tels qu'une caméra IP qui assure la surveillance sur Internet). L'un des moyens de répondre à cette exigence consiste à créer des cartes NAT (LSN) statiques à grande échelle. Mais pour un très grand nombre d'abonnés, la création de cartes NAT LSN statiques n'est pas une solution réalisable.

Le protocole PCP (Port Control Protocol) permet à un abonné de demander des mappages NAT LSN spécifiques pour lui-même et/ou pour d'autres appareils tiers. Le périphérique NAT à grande échelle crée une carte LSN et l'envoie à l'abonné. L'abonné envoie aux appareils distants sur Internet l'adresse IP NAT:port NAT sur lequel ils peuvent se connecter à l'abonné.

Les applications envoient généralement des messages de maintien en activité fréquents au périphérique NAT à grande échelle afin que leurs mappages LSN n'arrivent pas à expiration. Le PCP permet de réduire la fréquence de tels messages de maintien en activité en permettant aux applications de connaître les paramètres de délai d'expiration des mappages LSN. Cela permet de réduire la consommation de bande passante sur le réseau d'accès du FAI et la consommation de batterie sur les appareils mobiles.

Le PCP est un modèle client-serveur qui s'exécute via le protocole de transport UDP. Une appliance NetScaler implémente le composant serveur PCP et est conforme à la RFC 6887.

Étapes de configuration

Effectuez les tâches suivantes pour configurer le PCP :

- **(Facultatif) Créez un profil PCP**. Un profil PCP inclut des réglages pour les paramètres liés au PCP (par exemple, pour écouter le mappage et les requêtes PCP homologues). Un profil PCP peut être lié à un serveur PCP. Un profil PCP lié à un serveur PCP applique tous ses paramètres au serveur PCP. Un profil PCP peut être lié à plusieurs serveurs PCP. Par défaut, un profil PCP avec des paramètres par défaut est lié à tous les serveurs PCP. Un profil PCP que vous liez à un serveur PCP remplace les paramètres de profil PCP par défaut de ce serveur. Un profil PCP par défaut possède les paramètres suivants :
  - Mappage : activé
  - Homologue : activé
  - Durée de vie minimale de la carte : 120 secondes
  - Durée de vie maximale maximale : 86400 secondes
  - Nombre d'annonces : 10

  - Tierce partie : désactivée
- **Créez un serveur PCP et liez-y un profil PCP**. Créez un serveur PCP sur l'appliance NetScaler pour écouter les demandes et les messages liés au PCP provenant des abonnés. Une adresse IP de sous-réseau (SNIP) ou (SNIP6) doit être attribuée à un serveur PCP pour y accéder. Par défaut, un serveur PCP écoute sur le port 5351.
- **Liez le serveur PCP à un groupe LSN d'une configuration LSN**. Liez le serveur PCP créé à un groupe LSN d'une configuration LSN en définissant le paramètre PCP Server pour spécifier le serveur PCP créé. Le serveur PCP créé n'est accessible qu'aux abonnés de ce groupe LSN.

> **Remarque**
>
> Un serveur PCP destiné à une configuration NAT à grande échelle ne répond pas aux demandes des abonnés identifiés à partir des règles ACL.

Pour créer un profil PCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

Pour créer un serveur PCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Exemple de configuration pour NAT64

Dans l'exemple de configuration suivant, le serveur PCP PCP-SERVER-1, dont les paramètres PCP proviennent de PCP-PROFILE-1, est lié au groupe LSN LSN-NAT64-GROUP-1. PCP-SERVER-1 traite les requêtes PCP des abonnés IPv6 du réseau 2001:DB 8:5001 : :/96.

Exemple de configuration :


```
add pcp profile PCP-PROFILE-1 -minMapLife 400
Done
add pcp server PCP-SERVER-1 2001:DB8:6001::90  -pcpProfile PCP-PROFILE
   -1
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
   :300::/96
Done
add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1  - pcpServer PCP-NAT64-SERVER-1
Done
<!--NeedCopy-->
```

LSN64 dans une configuration de cluster

May 5, 2023

Les configurations NAT64 à grande échelle sont prises en charge sur une configuration de cluster NetScaler.

Un cluster NetScaler est un groupe d'appliances NetScaler configurées et gérées comme un seul système. Un cluster NetScaler garantit évolutivité et disponibilité. Chaque appliance NetScaler d'une configuration de cluster agit comme une entité LSN indépendante et est gérée comme un système unique.

La configuration LSN dans une configuration en cluster est identique à celle d'une appliance autonome, sauf qu'un pool spécifique d'adresses IP LSN appartient à un seul nœud à la fois. En d'autres termes, une entité de pool d'adresses IP LSN est configurée en tant qu'entité repérée dans un nœud particulier. Tous les nœuds d'une configuration de cluster peuvent avoir une entité de pool IP LSN

spécifique. Pour s'assurer que les paquets liés à une session LSN sont reçus sur le même nœud de cluster qui a effectué l'opération NAT, le pilotage du backplane basé sur des politiques (PBS) est configuré. PBS dirige les paquets associés reçus d'une session LSN vers le même nœud de cluster.

Exemple de configuration :

```
add lsn client LSN-NAT64-CLIENT-1

Done

bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96

Done

add lsn pool LSN-NAT64-POOL-1

Done

bind lsn pool LSN-NAT64-POOL-1 -ownerNode 1  203.0.113.61 -
    203.0.113.70

Done

bind lsn pool LSN-NAT64-POOL-1 -ownerNode 2  203.0.113.101 -
    203.0.113.110

Done

add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96

Done

add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1

Done

bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1

Done

add ns acl6 NAT64-DFD ALLOW -srcIPv6 = 2001:DB8:5001:: -type DFD -
    dfdhash SIP -dfdprefix 64

```



```
Done

apply ns acls6 -type DFD

Done
<!--NeedCopy-->
```

Mappage d'adresse et de port à l'aide

May 5, 2023

Mapping Address and Port using Translation (MAP-T) est une solution de transition IPv6 destinée aux fournisseurs d'accès Internet dotés d'une infrastructure IPv6 pour connecter leurs abonnés IPv4 à l'Internet IPv4. Elle_.MAP-T repose sur des technologies de traduction d'adresses IPv4 et IPv6 apatrides. Le MAP-T est un mécanisme qui effectue une double traduction (IPv4 vers IPv6 et vice versa) sur les appareils clients (CE) et les routeurs périphériques (dans le réseau central du FAI).

Dans un déploiement MAP-T, le dispositif CE met en œuvre une combinaison de traduction NAPT44 dynamique et de traduction NAT46 apatride. Le dispositif CE obtient le protocole NAT-IP et le bloc de port à utiliser pour la traduction via DHCPv6 ou toute autre méthode.

Lorsqu'un paquet IPv4 provenant d'un dispositif abonné arrive sur le dispositif CE, celui-ci exécute le protocole NAPT44 et stocke les informations de liaison NAPT44. Après la traduction NAT44, le paquet est soumis à une traduction NAT46 puis transmis au périphérique routeur (BR) situé dans le réseau central du fournisseur de services Internet. Le dispositif BR reçoit les paquets IPv6 du dispositif CE, extrait et valide l'IP NAT-IP et le bloc de port intégrés dans l'en-tête IPv6, puis transmet le paquet IPv4 vers Internet IPv4. Lorsque le BR reçoit le paquet IPv4 d'Internet, il traduit le paquet IPv4 en paquet IPv6 et envoie le paquet IPv6 au dispositif CE.

MAP-T est apatride sur un périphérique BR, il n'est donc pas nécessaire que le périphérique BR exécute une NAT sur le trafic. Au lieu de cela, la fonctionnalité NAT est déléguée aux appareils CE. Cette fonctionnalité de délégation et d'apatride des appareils BR permet au déploiement de BR d'évoluer proportionnellement au volume de trafic.

L'appliance NetScaler implémente la fonctionnalité BR d'une solution MAP-T telle que décrite par la RFC 7599.

Configuration de MAP-T

La configuration de MAP-T sur une appliance NetScaler comprend les tâches suivantes :

- Ajouter une règle de mappage par défaut

- Ajouter une règle de mappage de base
- Liez une plage d'adresses NAT IPv4 de périphériques CE à une règle de mappage de base
- Ajouter un domaine cartographique et lier une règle de mappage de base et une règle de mappage par défaut au domaine

Pour ajouter une règle de mappage par défaut à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add MapDmr <name> -BRIpv6Prefix ( <ipv6_addr> | <*> )

show MapDmr <name>
<!--NeedCopy-->
```

Pour ajouter une règle de mappage de base à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add MapBmr <name> -RuleIpv6Prefix <ipv6_addr> | <*>  [-psidoffset <
    positive_integer>] [-EAbitLength <positive_integer>]  [-psidlength <
    positive_integer>]

show MapBmr <name>
<!--NeedCopy-->
```

Pour lier la plage d'adresses NAT IPv4 des périphériques CE à une règle de mappage de base à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind MapBmr <name> (-network <ip_addr>  [-netmask <netmask>])

show MapBmr <name>
<!--NeedCopy-->
```

Pour ajouter un domaine cartographique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add MapDomain <name> -MapDmrName <string>

show MapDomain <name>
```



```
<!--NeedCopy-->
```

Pour lier une règle de mappage de base à un domaine cartographique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind MapDomain <name> -MapBmrName <string>

show MapDomain <name>
<!--NeedCopy-->
```

Exemple de configuration

```
add mapdmr DMR-1 -BRIpv6Prefix 2002:db8::/64

Done

add mapbmr BMR-1 -ruleIpv6Prefix 2002:db8:89ab::/48 -eAbitLength 16 -
    psidlength 8 -psidoffset 6

Done

bind mapbmr BMR-1 -network 192.0.1.0 -netmask 255.255.255.0

Done

add MapDomain MAP-DOMAIN-1 -mapdmrname DMR-1

Done

bind MapDomain MAP-DOMAIN-1 -mapbmrname BMR-1
Done
<!--NeedCopy-->
```

Gestion des abonnés Telco

May 5, 2023

Le nombre d'abonnés d'un réseau de télécommunications augmente à un rythme sans précédent, et leur gestion devient un défi pour les fournisseurs de services. Les appareils plus récents, plus rapides

et plus intelligents sollicitent fortement le réseau et les systèmes de gestion des abonnés. Il n'est plus possible de fournir à chaque abonné le même niveau de service, et il est impératif de traiter le trafic par abonné.

L'appliance NetScaler fournit les informations nécessaires pour profiler les abonnés en fonction de leurs informations stockées dans la fonction PCRF (Policy and Charging Rules Function). Lorsqu'un abonné mobile se connecte à Internet, la passerelle de paquets associe une adresse IP à l'abonné et transmet le paquet de données à l'appliance. L'appliance reçoit les informations sur les abonnés de manière dynamique, ou vous pouvez configurer des abonnés statiques. Ces informations permettent à l'appliance d'appliquer ses riches fonctionnalités de gestion du trafic, telles que la commutation de contenu, la mise en cache intégrée, la réécriture et le répondeur, pour chaque abonné afin de gérer le trafic.

Avant de configurer l'appliance NetScaler pour gérer les abonnés, vous devez allouer de la mémoire au module qui stocke les sessions des abonnés. Pour les abonnés dynamiques, vous devez configurer une interface via laquelle l'appliance reçoit les informations de session. Les abonnés statiques doivent se voir attribuer des identifiants et vous pouvez les associer à des politiques.

Vous pouvez également effectuer les opérations suivantes :

- Application et gestion des politiques relatives aux abonnés.
- Configurez l'appliance pour identifier de manière unique un abonné en utilisant uniquement le préfixe IPv6 au lieu de l'adresse IPv6 complète.
- Utilisez des politiques pour optimiser le trafic TCP pour les abonnés dynamiques et statiques. Ces politiques associent différents profils TCP à différents types d'utilisateurs.
- Gérez les sessions inactives sur une appliance NetScaler.
- Activez la journalisation sur un serveur de journaux.
- Supprimez les sessions LSN pour les sessions d'abonnés supprimées.

Allocation de mémoire pour le module de stockage des sessions d'abonné

Chaque entrée de session d'abonné consomme 1 Ko de mémoire. Le stockage de 500 000 sessions d'abonnés à tout moment nécessite 500 Mo de mémoire. Cette valeur doit être ajoutée à la mémoire minimale requise, qui est affichée dans le résultat de la commande « show extendedmemoryparam ». Dans l'exemple suivant, la sortie concerne une instance NetScaler VPX avec 3 moteurs de paquets et 8 Go de mémoire.

Pour stocker 500 000 sessions d'abonnés sur cette appliance, la mémoire configurée doit être de 2058+500 Mo (500 000 x 1 Ko = 500 Mo).

> **Remarque**
>
> La mémoire configurée doit être exprimée en multiples de 2 Mo et ne doit pas dépasser la limite d'utilisation maximale de la mémoire. L'appliance doit être redémarrée pour que les modifica-

> tions prennent effet.

Exemple

```
show extendedmemoryparam
       Extended Memory Global Configuration. This memory is utilized by
           LSN and Subscriber Session Store Modules:
        Active Memory Usage: 0 MBytes
        Configured Memory Limit: 0 MBytes
        Minimum Memory Required: 2058 MBytes
        Maximum Memory Usage Limit: 2606 MBytes
    Done
    set extendedmemoryparam -memLimit 2558
    Done
    show extendedmemoryparam
            Extended Memory Global Configuration. This memory is
               utilized by LSN and Subscriber Session Store Modules:

            Active Memory Usage: 2558 MBytes
            Configured Memory Limit: 2558 MBytes
            Minimum Memory Required: 2058 MBytes
            Maximum Memory Usage Limit: 2606 MBytes
    Done
<!--NeedCopy-->
```

Configuration d'une interface pour les abonnés dynamiques

L'appliance NetScaler reçoit dynamiquement les informations sur les abonnés via l'un des types d'interface suivants :

- Interface Gx
- Interface RADIUS
- Interface RADIUS et Gx

> **Remarque**
>
> - À partir de NetScaler version 12.0 build 57.19, l'interface Gx est prise en charge pour un déploiement de cluster. Pour plus d'informations, voir Interface Gx dans une topologie de cluster.
> - Dans une configuration HA, les sessions d'abonné sont continuellement synchronisées sur le nœud secondaire. En cas de basculement, les informations relatives à l'abonné restent disponibles sur le nœud secondaire.

Interface Gx

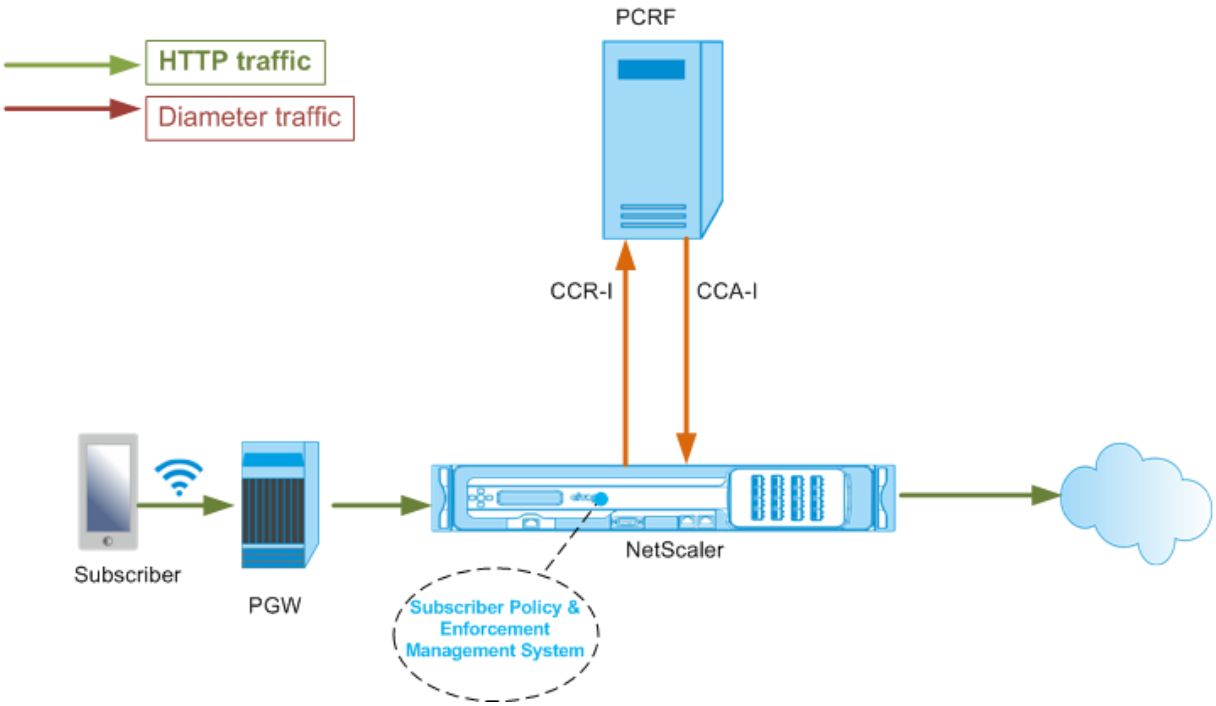
Une interface Gx (telle que spécifiée dans la norme 3GPP 29.212) est une interface standard basée sur le protocole Diameter qui permet l'échange de règles de contrôle et de facturation entre une PCRF et une entité PCEF (Policy and Charging Enforcement Function) au sein d'un réseau de télécommunications.

Lorsqu'une session IP-CAN est établie, la passerelle de paquets transmet l'identifiant de l'abonné, tel que le MSISDN, et les informations d'adresse IP encadrée concernant l'abonné au PCRF sous forme de message Diameter. Lorsque le paquet de données arrive à l'appliance depuis la passerelle de paquets (PGW), l'appliance utilise l'adresse IP de l'abonné pour interroger le PCRF afin d'obtenir les informations sur l'abonné. Cette fonctionnalité est également connue sous le nom de fonctionnalité PCEF secondaire.

Les règles PCC (Policy and Charging Control) reçues par l'appliance via l'interface Gx sont stockées sur l'appliance pendant la session de l'abonné, c'est-à-dire jusqu'à ce que le PCRF envoie un message de demande de réauthentification (RAR) avec une AVP Session-Release-Cause ou jusqu'à ce que la session de l'abonné soit terminée depuis la CLI ou l'utilitaire de configuration. Si des mises à jour sont apportées à un abonné existant, le PCRF envoie les mises à jour dans un message RAR. Une session d'abonné est initiée lorsqu'un abonné ouvre une session sur le réseau et se termine lorsqu'il ferme sa session.

> **Remarque** : Si le serveur PCRF est en panne, l'appliance NetScaler crée des sessions négatives pour les demandes d'abonnés Gx en attente ou entrantes. Lorsque le serveur PCRF est à nouveau opérationnel, l'appliance NetScaler évite une tempête de demandes en attendant l'expiration des sessions négatives avant d'exécuter les demandes spécifiques des abonnés.

L'illustration suivante montre le flux de trafic élevé. Il suppose que le trafic du plan de données est HTTP. L'appliance envoie une demande de contrôle de crédit (CCR) via une interface Gx au serveur PCRF et, dans la réponse de contrôle de crédit (CCA), reçoit les règles PCC et, facultativement, d'autres informations, telles que le type de technologie d'accès radio (RAT), qui s'appliquent à l'abonné en question. Les règles PCC incluent un ou plusieurs noms de politique (règle) et d'autres paramètres. L'appliance utilise ces informations pour récupérer les règles prédéfinies stockées sur l'appliance et pour diriger le flux de trafic. Il stocke également ces informations dans le système de gestion de la politique d'abonnement et de son application pendant la session de l'abonné. Une fois la session d'un abonné terminée, l'appliance supprime toutes les informations concernant l'abonné.



L'exemple suivant montre les commandes permettant de configurer une interface Gx. Les commandes sont en gras.

Pour configurer une interface Gx, effectuez les tâches suivantes

Ajoutez un service DIAMETER pour chaque interface Gx. Par exemple :

```
1 add service pcrf-svc1 203.0.113.1 DIAMETER 3868
2
3 add service pcrf-svc2 203.0.113.2 DIAMETER 3868
4 <!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge DIAMETER non adressable et liez les services créés à l'étape 1 à ce serveur virtuel. Pour plusieurs services, spécifiez un PersistenceType et le PersistaVPN afin que des sessions spécifiques soient gérées par le même serveur PCRF. Par exemple :

```
1 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
2
3 bind lb vserver vdiam pcrf-svc1
4
5 bind lb vserver vdiam pcrf-svc2
6 <!--NeedCopy-->
```

Configurez l'identité et le domaine du diamètre de NetScaler. L'identité et le domaine sont utilisés

comme AVP Origin-Host et Origin-Realm dans les messages Diameter envoyés par le client Gx. Par exemple :

```
set ns diameter  -identity netscaler.com  -realm com
<!--NeedCopy-->
```

Configurez l'interface Gx pour utiliser le serveur virtuel créé à l'étape 2 en tant que serveur virtuel PCRF. Spécifiez le domaine PCRF à utiliser comme domaine de destination AVP dans les messages Diameters envoyés par le client Gx. Par exemple :

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com
<!--NeedCopy-->
```

Définissez le type d'interface d'abonné sur GXOnly. Par exemple :

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Pour voir la configuration et l'état de l'interface Gx, tapez :

```
show subscriber gxinterface
<!--NeedCopy-->
```

Exemple

```
show subscriber gxinterface
    Gx Interface parameters:
        PCRF Vserver: vdiam (DOWN)
        Gx Client Identity...:  netscaler1.com
        Gx Client Realm ..........:  com
        PCRF Realm: epc.mnc030.mcc234.3gppnetwork.org
        Hold Packets On Subscriber Absence: YES
        CCR Request Timeout: 4 Seconds
        CCR Request Retry Attempts: 1
        Gx HealthCheck enabled: NO
        Gx HealthCheck TTL : 30 Seconds
        CER Request Timeout: 10 Seconds
        RevalidationTimeout: 30 Seconds
        NegativeTTL: 60 Seconds
        NegativeTTL Limited Success: NO
        Purge SDB on Gx Failure: YES
        ServicePath AVP code: 262099    ServicePath AVP VendorID: 3845
        PCRF Connection State: PCRF is not ready
    Done
```



```
20
21 <!--NeedCopy-->
```

ARGUMENTS

Serveur virtuel

Nom du serveur virtuel d'équilibrage de charge ou de commutation de contenu auquel les connexions Gx sont établies. Le type de service du serveur virtuel doit être DIAMETER ou SSL_DIAMETER. Ce paramètre s'exclut mutuellement du paramètre de service. Par conséquent, vous ne pouvez pas définir à la fois le service et le serveur virtuel dans l'interface Gx.

Service

Nom du service DIAMETER ou SSL_DIAMETER correspondant au PCRF auquel la connexion Gx est établie. Ce paramètre s'exclut mutuellement du paramètre vserver. Par conséquent, vous ne pouvez pas définir à la fois le service et le serveur virtuel dans l'interface Gx.

PCR Realm

Domaine du PCRF vers lequel le message doit être acheminé. Il s'agit du domaine utilisé dans Destination-Realm AVP par le client NetScaler Gx (en tant que nœud Diameter).

Suspend l'absence de l'abonné

Définissez la valeur Oui pour conserver les paquets jusqu'à ce que les informations de session de l'abonné soient extraites du serveur PCRF. S'il est défini sur Non, le profil d'abonné par défaut est appliqué jusqu'à ce que les informations de session de l'abonné soient extraites du serveur PCRF. Si aucun profil d'abonné par défaut n'est configuré, une valeur UNDEF est générée pour les expressions qui utilisent des attributs d'abonné.

Délai d'expiration de la demande

Durée, en secondes, pendant laquelle la demande Gx CCR doit être terminée. Si la demande n'est pas terminée dans ce délai, elle est retransmise le nombre de fois spécifié dans le paramètre RequestRetryAttempts. Si la demande n'est pas complète même après la retransmission, le profil d'abonné par défaut est appliqué à cet abonné. Si aucun profil d'abonné par défaut n'est configuré, une valeur UNDEF est générée pour les expressions qui utilisent des attributs d'abonné. La valeur zéro désactive le délai d'expiration. Valeur par défaut : 10

Tentatives de demande de nouvelle tentative

Spécifiez le nombre de fois qu'une demande doit être retransmise si la demande ne se termine pas dans les limites de la valeur spécifiée dans le paramètre RequestTimeout. Valeur par défaut : 3.

Bilet de santé

Réglez sur Oui pour activer la vérification de l'état de santé en ligne de l'homologue Gx. Lorsque cette option est activée, NetScaler envoie des paquets DWR au serveur PCRF. Lorsque la session Gx est inactive, le temporisateur HealthCheck expire et des paquets DWR sont lancés pour vérifier si le serveur PCRF est actif. Valeur par défaut : Non.
Remarque : Ce paramètre est pris en charge dans NetScaler 12.1 build 51.xx et versions ultérieures.

Contrôle de santé TTL

Durée en secondes définie pour la supervision du chien de garde. Une fois le délai TTL de vérification de l'état expiré, un DWR est envoyé pour vérifier l'état du serveur PCRF. Tout message CCR, CCA, RAR ou RAA réinitialise le chronomètre.
Valeur minimale : 6 secondes. Valeur par défaut : 30 secondes.
Remarque : Ce paramètre est pris en charge dans NetScaler 12.1 build 51.xx et versions ultérieures.

Délai d'expiration de la demande CER

Durée en secondes définie pour la retransmission de la demande d'échange de capacités. NetScaler lance un nouveau message CER s'il ne reçoit pas de CEA de la part du PCRF dans ce délai configuré. Si aucune réponse n'est reçue du serveur PCRF, l'appliance essaie d'envoyer le message CER 5 fois. S'il n'y a pas de réponse même après 5 messages CER, l'appliance ferme la connexion TCP et signale un échec. Si la valeur du délai d'expiration est définie sur 0, la fonction de vérification de l'état de l'application est désactivée.
Valeur minimale : 0 seconde. Valeur par défaut : 0 secondes.
Remarque : Ce paramètre est pris en charge dans NetScaler 12.1 build 51.xx et versions ultérieures.

Délai de revalidation

Durée, en secondes, après laquelle la demande Gx CCR-U est envoyée après toute activité PCRF sur une session. Tout message RAR ou CCA réinitialise le chronomètre. La valeur zéro désactive le délai d'inactivité.

TTL négatif

Durée, en secondes, après laquelle la demande Gx CCR-I est renvoyée pour les sessions qui n'ont pas été résolues par PCRF parce que le serveur est en panne, qu'il n'y a pas de réponse ou qu'une réponse a

échoué est reçue. Au lieu d'interroger constamment le serveur PCRF, un TTL négatif oblige l'appliance à conserver une session non résolue. Pour les sessions négatives, l'appliance hérite des attributs du profil d'abonné par défaut, s'il est configuré, et du message de gestion RADIUS, s'il en reçoit un. La valeur zéro désactive les sessions négatives. L'appliance n'installe pas de sessions négatives même si la session d'un abonné n'a pas pu être récupérée. Valeur par défaut : 600

Succès limité du TTL négatif

Définissez la valeur Oui pour créer une session négative en cas de code de réponse de réussite partiel (2002). Si ce paramètre est défini sur Non, une session normale est créée. Valeur par défaut : Non.

Ce paramètre est pris en charge dans NetScaler 12.1 build 49.xx et versions ultérieures.

Purge en cas de défaillance de GX

Définissez la valeur sur Oui pour vider la base de données des abonnés en cas de défaillance de l'interface Gx. La défaillance de l'interface Gx inclut à la fois la surveillance DWR (si activée) et la vérification de l'état du réseau (si activée). Lorsque ce paramètre est défini sur Oui, toutes les sessions des abonnés sont effacées.
Valeur par défaut : Non.
Remarque : Ce paramètre est pris en charge dans NetScaler 12.1 build 51.xx et versions ultérieures.

Chemin de service AVP

Code AVP dans lequel PCRF envoie le chemin de service applicable à un abonné.

ID du fournisseur ServicePath

L'identifiant du fournisseur de l'AVP dans lequel PCRF envoie le chemin de service applicable à un abonné.

Pour configurer l'interface Gx à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Cliquez sur **Configurer les paramètres de l'abonné**.
3. Dans Type d'interface, sélectionnez **GXOnly**.
4. Spécifiez les valeurs de tous les paramètres requis.
5. Cliquez sur **OK**.

Détectez les défaillances de transport sur les connexions Gx établies

Remarque : Cette fonctionnalité est prise en charge dans NetScaler 12.1 build 51.xx et versions ultérieures.

Une appliance NetScaler peut être configurée pour détecter les défaillances de transport sur les connexions Gx établies à l'aide de messages DWR (Device Watchdog request) et DWA (Device Watchdog Answer).

Une fois qu'une session Gx est établie, un temporisateur prédéfini est déclenché pour détecter si une session est inactive. Un message DWR est envoyé à l'expiration du délai d'inactivité. Le temporisateur d'inactivité est réinitialisé chaque fois que l'appliance NetScaler reçoit un message via une session Gx établie. La disponibilité du pair est confirmée sur la base du message DWA après l'envoi d'un message DWR.

- Si le DWA est reçu, la disponibilité d'un homologue est confirmée et le chronomètre de surveillance est réinitialisé.
- Si le DWA n'est pas reçu et que le chronomètre de surveillance expire deux fois de suite, la session est considérée comme étant interrompue et l'homologue non disponible. L'appliance ferme la session et essaie d'établir une nouvelle session avec l'homologue Gx.

Lorsque le temporisateur de surveillance expire deux fois sans réponse, l'appliance NetScaler considère que la connexion Gx est défectueuse et lance une fermeture de connexion. Une fois la connexion fermée, aucune autre requête de surveillance n'est envoyée à l'homologue Gx. L'appliance NetScaler utilise la prochaine session Gx disponible pour toutes les demandes PCRF.

Pour détecter les défaillances de transport sur des connexions Gx établies à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set subscriber gxInterface [-vServer <string>] [-service <string>] [-
    healthCheck ( YES | NO )] [-healthCheckTTL<positive_integer>][-
    cerRequestTimeout <positive_integer>] [-purgeSDBonGxFailure ( YES |
    NO )]
<!--NeedCopy-->
```

Exemple :

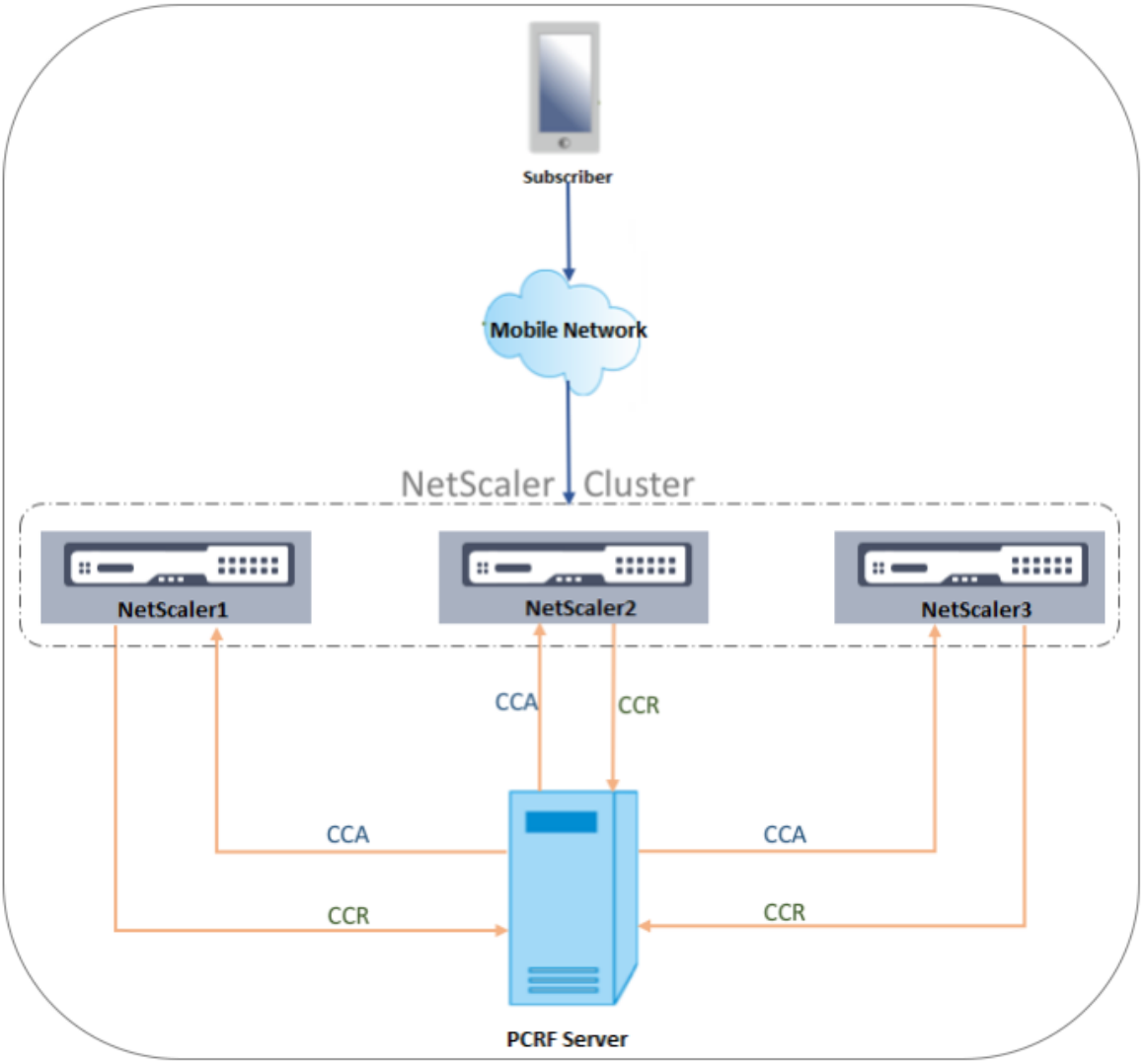
```
set subscriber gxInterface set subscriber gxInterface -vServer vdiam -
    healthCheck YES -healthCheckTTL 31 -cerRequestTimeout 15
    purgeSDBonGxFailure  YES
<!--NeedCopy-->
```


Pour détecter les défaillances de transport sur des connexions Gx établies à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Cliquez sur **Configurer les paramètres de l'abonné**.
3. Dans **Type d'interface**, sélectionnez **GXOnly**.
4. Spécifiez les valeurs de tous les paramètres requis.
5. Sélectionnez **Health Check** et spécifiez des valeurs pour **Health Check TTL** et **CER Request Timeout**.
6. Cliquez sur **OK**.

Interface Gx dans une topologie de cluster

L'appliance NetScaler prend en charge l'interface Gx dans une topologie de cluster.



Les nœuds NetScaler du cluster communiquent avec un serveur PCRF externe via l'interface Gx. Lorsqu'un nœud reçoit du trafic client, l'appliance effectue les opérations suivantes :

- Envoie une requête CCR-I au serveur PCRF pour récupérer les informations sur les abonnés.
- Le serveur PCRF répond par un CCR-A.
- Le nœud NetScaler stocke ensuite les informations d'abonné reçues dans son magasin d'abonnés et applique les règles au trafic client.

Chaque nœud gère un magasin d'abonnés indépendant et les sessions des abonnés ne sont pas synchronisées avec les autres nœuds.

Conformément au protocole de base Diameter RFC 6733, chaque homologue doit être configuré avec une identité diameter unique pour communiquer avec d'autres homologues via le protocole Diameter. Ainsi, lors d'un déploiement en cluster, la configuration de l'identité du diamètre est détectée. Les paramètres de diamètre (identité, domaine, propagation à proximité du serveur) pour chaque nœud peuvent être configurés individuellement à l'aide de l'interface graphique ou de l'interface de ligne de commande.

Lorsqu'un nœud est ajouté à un cluster, il utilise les paramètres de diamètre par défaut (identity=netscaler.com, realm=com, serverClosePropogation=no). Une fois les nœuds ajoutés, les paramètres de diamètre de chaque nœud doivent être configurés.

Pour configurer les paramètres de diamètre à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet de détails, cliquez sur **Modifier les paramètres de Diameter**.
3. **Sur la page Paramètres de Diameter, sélectionnez le nœud NetScaler pour lequel vous souhaitez configurer les paramètres de diamètre, puis cliquez sur Configurer.**
4. Sur la page Configurer les paramètres de Diameter, configurez l'identité du diamètre, le domaine du diamètre et la propagation de proximité du serveur pour le nœud sélectionné.
5. Cliquez sur **OK**.

Pour configurer les paramètres de diamètre à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ns diameter [-identity <string>] [-ownerNode <positive_integer>]
<!--NeedCopy-->
```

ARGUMENTS

Identité

L'identité Diameter est utilisée pour identifier un nœud Diameter de manière unique. Avant de configurer la configuration du diamètre, l'appliance NetScaler (en tant que nœud Diameter) doit se voir attribuer une identité de diamètre unique.

Par exemple, définissez ns diameter -identity netscaler.com -OwnerNode 1. Ainsi, chaque fois que le système NetScaler doit utiliser l'identité dans les messages Diameter, il utilise « netscaler.com » comme AVP Origin-Host, comme défini dans la RFC3588.

Longueur maximale : 255

Nœud propriétaire

OwnerNode représente l'ID du nœud du cluster pour lequel l'ID de diamètre est défini. OwnerNode ne peut être configuré que via CLIP.

Valeur minimale : 0

Valeur maximale : 31

Exemple :

définir le diamètre ns -identity netscaler1.com -OwnerNode 1

Remarque :

L'option OwnerNode est également ajoutée à la commande show ns diameter.

Exemple :

```
show diameter -ownerNode <0-31>
<!--NeedCopy-->
```

Lorsque la commande show ns diameter est exécutée, elle affiche les paramètres de diamètre pour un nœud donné.

Pour configurer une interface Gx pour le déploiement de clusters

Pour configurer une interface Gx, effectuez les tâches suivantes :

Ajoutez un service DIAMETER pour chaque interface Gx.

Exemple :

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868
add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```


Ajoutez un serveur virtuel d'équilibrage de charge DIAMETER et liez les services créés à l'étape 1 à ce serveur virtuel.

Exemple :

```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam pcrf-svc1

bind lb vserver vdiam pcrf-svc2
<!--NeedCopy-->
```

Configurez le diamètre, l'identité et le domaine de NetScaler sur tous les nœuds du cluster. L'identité et le domaine sont utilisés comme AVP Origin-Host et Origin-Realm dans les messages Diameter envoyés par le client Gx.

Exemple :

```
set ns diameter -identity node0.netscaler.com -realm netscaler.com -
    ownerNode 0

set ns diameter -identity node1.netscaler.com -realm netscaler.com -
    ownerNode 1
<!--NeedCopy-->
```

Configurez l'interface Gx pour utiliser le serveur virtuel créé à l'étape 2 en tant que serveur virtuel PCRF et définissez également le domaine PCRF.

Exemple :

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com

Set the subscriber interface type to GxOnly.
<!--NeedCopy-->
```

Exemple :

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Pour voir la configuration et l'état de l'interface Gx, tapez :

```
show subscriber gxinterface
<!--NeedCopy-->
```


Interface RADIUS

Avec une interface RADIUS, la passerelle de paquets transmet les informations sur les abonnés contenues dans un message RADIUS Accounting Start à l'appliance via l'interface RADIUS lorsqu'une session IP-CAN est établie. Un service de type RADIUSListener traite les messages RADIUS Accounting. Ajoutez un secret partagé pour le client RADIUS. Si aucun secret partagé n'est configuré, le message RADIUS est supprimé silencieusement. L'exemple suivant montre les commandes permettant de configurer une interface RADIUS. Les commandes sont en gras.

Pour configurer une interface RADIUS, effectuez les tâches suivantes :

Créez un service d'écoute RADIUS à l'adresse SNIP où les messages RADIUS sont reçus. Par exemple :

```
add service srad1 192.0.0.206 RADIUSLISTENER 1813
<!--NeedCopy-->
```

Configurez l'interface RADIUS de l'abonné pour utiliser ce service. Par exemple :

```
set subscriber radiusInterface -listeningService srad1
<!--NeedCopy-->
```

Définissez le type d'interface d'abonné sur RADIUSOnly. Par exemple :

```
set subscriber param -interfaceType RadiusOnly
<!--NeedCopy-->
```

Ajoutez un client RADIUS en spécifiant un sous-réseau et un secret partagé. Par exemple :

```
add radius client 192.0.2.0/24 -radkey client123
<!--NeedCopy-->
```

Un sous-réseau de 0.0.0.0/0 implique qu'il s'agit du secret partagé par défaut pour tous les clients. Pour voir la configuration et l'état de l'interface RADIUS, tapez :

```
show subscriber radiusInterface
<!--NeedCopy-->
```

Paramètres de l'interface RADIUS :

Service d'écoute Radius : srad1 (UP)

Terminé

Exemple :

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868

```



```
add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

ARGUMENTS

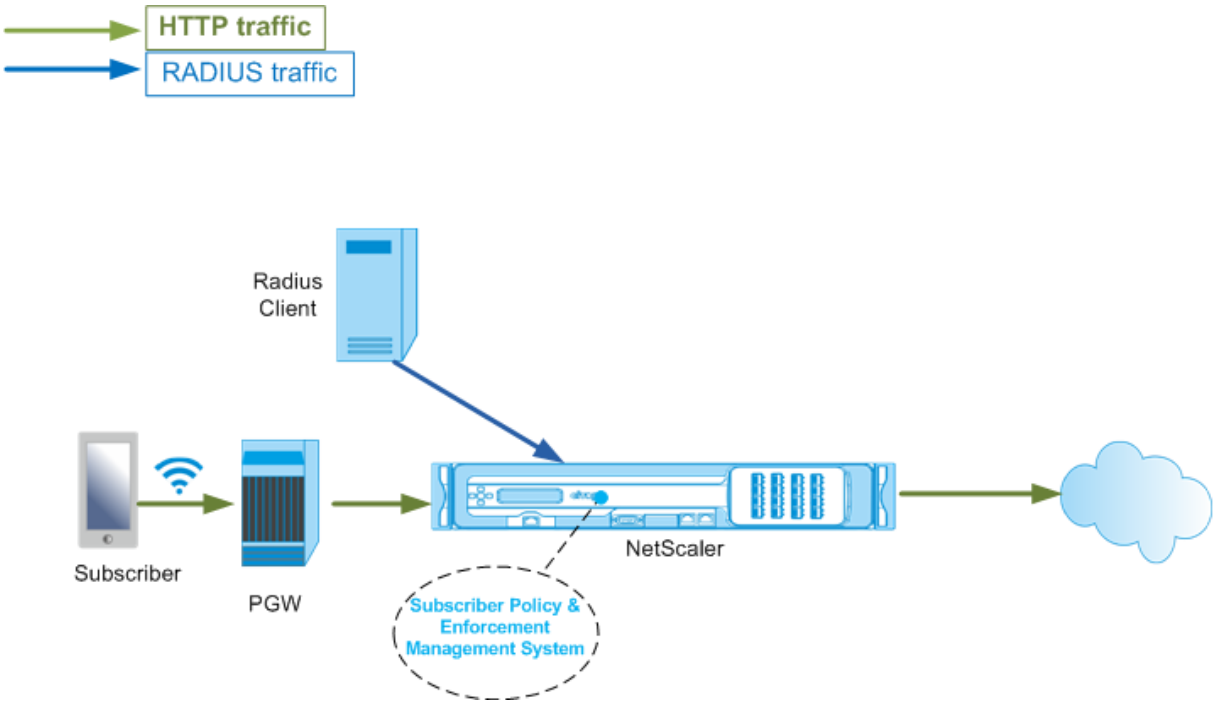
Service d'écoute

Nom du service d'écoute RADIUS qui traite les demandes de comptabilité RADIUS.

État SVR

État du service d'écoute RADIUS.

L'illustration suivante montre le flux de trafic élevé.



Pour configurer l'interface RADIUSOnly à l'aide de l'interface graphique

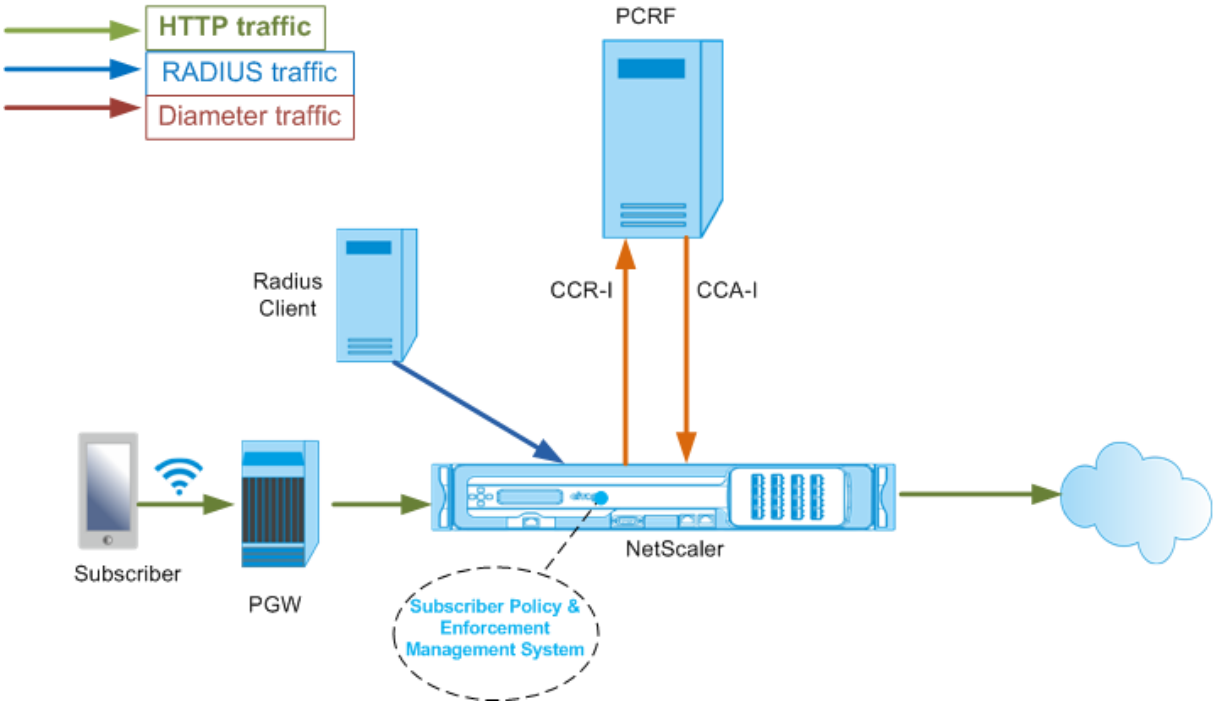
1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Cliquez sur **Configurer les paramètres de l'abonné**.
3. Dans Type d'interface, sélectionnez **RADIUSOnly**.
4. Spécifiez les valeurs de tous les paramètres requis.
5. Cliquez sur **OK**.

Interface RADIUS et Gx

Avec une interface RADIUS et Gx, lorsqu'une session IP-CAN est établie, la passerelle de paquets transmet l'ID de l'abonné, tel que le MSISDN, et les informations d'adresse IP encadrée concernant l'abonné à l'appliance via l'interface RADIUS. L'appliance utilise cet ID d'abonné pour interroger le PCRF sur l'interface Gx afin d'obtenir les informations sur l'abonné. C'est ce que l'on appelle la fonctionnalité PCEF principale. L'exemple suivant montre les commandes permettant de configurer une interface RADIUS et Gx.

```
set subscriber param -interfaceType RadiusandGx
add service pcrf-svc 203.0.113.1 DIAMETER 3868
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263
bind lb vserver vdiam pcrf-svc
set subscriber gxInterface -vServer vdiam -pcrfRealm testrealm1.net -
    holdOnSubscriberAbsence YES -revalidationTimeout 60 -negativeTTL 120
add service srad1 192.0.0.206 RADIUSLISTENER 1813    set subscriber
    radiusInterface -listeningService srad1
<!--NeedCopy-->
```

L'illustration suivante montre le flux de trafic élevé.



Pour configurer l'interface RadiusandGX à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.

2. Cliquez sur **Configurer les paramètres de l'abonné**.
3. Dans Type d'interface, sélectionnez **RadiusandGX**.
4. Spécifiez les valeurs de tous les paramètres requis.
5. Cliquez sur **OK**.

Configuration des abonnés statiques

Vous pouvez configurer les abonnés manuellement sur l'appliance NetScaler à l'aide de la ligne de commande ou de l'utilitaire de configuration. Vous créez des abonnés statiques en attribuant un identifiant d'abonné unique et en associant éventuellement une politique à chaque abonné. Les exemples suivants présentent les commandes permettant de configurer un abonné statique.

Dans les exemples suivants, **SubscriptionIDValue** indique le numéro de téléphone international et **SubscriptionIdType** (E164 dans cet exemple) indique le format général des numéros de téléphone internationaux.

```
1     add subscriber profile 203.0.113.6 -subscriberRules policy1 policy2
          -subscriptionIdType E164 -subscriptionIdvalue 98767543211
2     add subscriber profile 2002::a66:e8d3/64 -subscriberRules policy1
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543212
3     add subscriber profile 203.0.24.2 10 -subscriberRules policy2
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543213
4 <!--NeedCopy-->
```

Pour afficher les profils d'abonnés configurés, tapez :

> afficher le profil de l'abonné

```
1     > show subscriber profile
2
3     1)  Subscriber IP: 203.0.24.2 VLAN:10
4         Profile Attributes:
5                 Active Rules: policy2, policy3
6                 Subscriber Id Type: E164
7                 Subscriber Id Value: 98767543213
8     2)  Subscriber IP: 2002::/64
9         Profile Attributes:
10                Active Rules: policy1, policy3
11                Subscriber Id Type: E164
12                Subscriber Id Value: 98767543212
13    3)  Subscriber IP: 203.0.113.6
14        Profile Attributes:
```



```
                Active Rules: policy1, policy2
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543211

     Done
<!--NeedCopy-->
```

Profil d'abonné par défaut

Un profil d'abonné par défaut est utilisé si l'adresse IP de l'abonné n'est pas trouvée dans le magasin de sessions d'abonné de l'appliance. Dans l'exemple suivant, un profil d'abonné par défaut est ajouté avec la règle d'abonnement policy1.

```
    > add subscriber profile * -subscriberRules policy1
<!--NeedCopy-->
```

Afficher et effacer les sessions des abonnés

Utilisez la commande suivante pour afficher toutes les sessions d'abonnés statiques et dynamiques.

> afficher les sessions des abonnés

```
    > show subscriber sessions
    1)  Subscriber IP: 2002::/64
        Session Attributes:
                Active Rules: policy1, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543212
    2)  Subscriber IP: *
        Session Attributes:
                Active Rules: policy1
    3)  Subscriber IP: 203.0.24.2 VLAN:10
        Session Attributes:
                Active Rules: policy2, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543213
    4)  Subscriber IP: 203.0.113.6
        Session Attributes:
                Active Rules: policy1, policy2
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543211
    5)  Subscriber IP: 192.168.0.11
        Session Attributes:
```



```
22                  Idle TTL remaining: 361 Seconds
23                  Active Rules: policy1
24                  Subscriber Id Type: E164
25                  Subscriber Id Value: 1234567811
26                  Service Path: policy1
27                  AVP(44): 34 44 32 42 42 38 41 43  2D 30 30 30 30 30 30
                        31 31
28                  AVP(257): 00 01 C0 A8 0A 02
29                  PCRF-Host: host.pcrf.com
30                  AVP(280): 74 65 73 74 2E 63 6F 6D
31
32      Done
33  <!--NeedCopy-->
```

Utilisez la commande suivante pour effacer une session ou la totalité du magasin de sessions. Si vous ne spécifiez pas d'adresse IP, l'ensemble du magasin de sessions des abonnés est effacé.

```
1  clear subscriber sessions <ip>
2  <!--NeedCopy-->
```

Système d'application et de gestion des politiques d'abonnement

L'appliance NetScaler utilise l'adresse IP de l'abonné comme clé du système d'application et de gestion des politiques d'abonnement.

Vous pouvez ajouter des expressions d'abonné pour lire les informations sur les abonnés disponibles dans le système d'application et de gestion des politiques d'abonnement. Ces expressions peuvent être utilisées avec des règles de politique et des actions configurées pour les fonctionnalités de NetScaler, telles que la mise en cache intégrée, la réécriture, le répondeur et la commutation de contenu.

Les commandes suivantes constituent un exemple d'ajout d'une action et d'une politique de réponse basées sur les abonnés. La politique est évaluée comme vraie si la valeur de la règle d'abonné est « pol1 ».

```
1      add responder action error_msg respondwith '"HTTP/1.1 403 OKrnrn" +
           " You are  not authorized to access Internet"'
2      add responder policy no_internet_access "SUBSCRIBER.RULE_ACTIVE("
          pol1")" error_msg
3  <!--NeedCopy-->
```

L'exemple suivant montre les commandes permettant d'ajouter une action et une politique de réécriture basées sur les abonnés. L'action insère un en-tête HTTP « X-Nokia-MSISDN » en utilisant la valeur AVP (45) dans la session de l'abonné.


```
1      > add rewrite action AddHDR-act insert_http_header X-Nokia-MSISDN "
          SUBSCRIBER.AVP(45).VALUE"
2      > add rewrite policy AddHDR-pol "HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.
          URL).EQUALS_ANY("patset-test")" AddHDR-act
3  <!--NeedCopy-->
```

Dans l'exemple suivant, deux politiques sont configurées sur l'appliance. Lorsque l'appliance vérifie les informations de l'abonné et que la règle d'abonné est cache_enable, elle effectue la mise en cache. Si la règle d'abonné est cache_disable, l'appliance n'effectue pas de mise en cache.

```
1      > add cache policy nocachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_disable")" - action NOCACHE
2      > add cache policy cachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_enable")" - action CACHE -storeInGroup cg1
3  <!--NeedCopy-->
```

Pour obtenir la liste complète des expressions commençant par « ABONNER », consultez le Guide de configuration des politiques.

> **Important**
>
> : la version 12.1 du logiciel NetScaler prend en charge la méthode de recherche de clés IPAND-VLAN lorsque l'interface d'abonné est définie sur GXOnly. Pour plus de détails, reportez-vous à la section Méthode de recherche de clé d'adresse IP et d'ID VLAN

Sessions d'abonné basées sur le préfixe IPv6

Un utilisateur de télécommunications est identifié par le préfixe IPv6 plutôt que par l'adresse IPv6 complète. L'appliance NetScaler utilise désormais le préfixe au lieu de l'adresse IPv6 complète (/128) pour identifier un abonné dans la base de données (magasin d'abonnés). Pour communiquer avec le serveur PCRF (par exemple, dans un message CCR-I), l'appliance utilise désormais le préfixe IPv6 encadré AVP au lieu de l'adresse IPv6 complète. La longueur du préfixe par défaut est /64, mais vous pouvez configurer l'appliance pour qu'elle utilise une valeur différente.

Pour configurer le préfixe IPv6 à l'aide de la ligne de commande

```
set subscriber param [-ipv6PrefixLookupList <positive_integer> ...]
```

Le premier exemple de commande ci-dessous définit un seul préfixe et le second exemple de commande définit plusieurs préfixes.

```
1      set subscriber param -ipv6PrefixLookupList 64
2      set subscriber param -ipv6PrefixLookupList 64 72 96
```



```
<!--NeedCopy-->
```

Pour configurer le préfixe IPv6 à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Configurer les paramètres de l'abonné** et dans **Liste de recherche de préfixes IPv6**, spécifiez un ou plusieurs préfixes.

Méthode de recherche d'adresse IP et de clé d'ID VLAN

L'appliance NetScaler utilise l'adresse IP de l'abonné comme méthode de recherche clé pour accéder au système d'application et de gestion des politiques d'abonnement. Cette méthode n'est pas efficace si les adresses IP se chevauchent. Dans ce cas, vous pouvez utiliser l'ID du VLAN comme type de recherche d'abonné supplémentaire. La méthode de recherche de clés IPANDVLAN n'est prise en charge que lorsque l'interface d'abonné est définie sur GxOnly. Lorsque IPANDVLAN est configuré comme méthode de recherche, l'appliance NetScaler effectue les opérations suivantes :

- Inclut l'ID du VLAN d'origine dans la requête Gx pour les abonnés IPv4.
- Inclut le VLAN Gx AVP dans toutes les réponses Gx. Toutefois, en cas de non-concordance d'ID de VLAN, l'appliance ignore les réponses.

Par exemple, si l'appliance envoie un CCR-I avec GxSessionID-A:IPv4-B:VLAN-C et que la réponse contient GXSessionId-A:IPv4-B:VLAN-D, la réponse est supprimée et une entrée d'abonné par défaut est créée.

> **Remarque**
>
> - Les types d'interface RadiusAndGX et RadiusOnly ne peuvent pas être configurés avec le type de clé IPANDVLAN.
> - Si le trafic provient d'une adresse IPv6, l'appliance NetScaler utilise la méthode de recherche IP.

Pour configurer IP ou IPANDVLAN comme méthode de recherche de clés à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set subscriber param [-keytype ( IP | IPANDVLAN )] [-interfaceType <
    interfaceType>]
<!--NeedCopy-->
```

Exemple :


```
set subscriber param -keytype IPANDVLAN -interfaceType GxOnly

set subscriber param -keytype IP -interfaceType GxOnly
<!--NeedCopy-->
```

> **Remarque**
>
> La modification du paramètre keytype de IP en IPANDVLAN et inversement efface toutes les données des abonnés.

Paramètre VLAN

Le paramètre VLAN est également ajouté pour les commandes suivantes.

```
add subscriber profile <ip>@ [-vlan]

set subscriber profile <ip>@ [-vlan] [-subscriptionIdType  <
    subscriptionIdType>]

show subscriber profile [<ip>@] [-vlan]

rm subscriber profile <ip>@ [-vlan <positive_integer>]
<!--NeedCopy-->
```

Arguments

IP

Représente l'adresse IP de l'abonné. Il s'agit d'un argument obligatoire qui ne peut pas être modifié après l'ajout du profil d'abonné.

vlan

Représente le numéro de VLAN sur lequel se trouve l'abonné. Le numéro de VLAN ne peut pas être modifié après l'ajout du profil d'abonné.

Valeur minimale : 1

Valeur maximale : 4096

```
add subscriber profile 192.0.2.23 10

set subscriber profile 192.0.2.23 10 -subscriptionIdtype E164
```



```
4
5 show subscriber profile 192.0.2.23 10
6
7 rm subscriber profile 192.0.2.23 10
8
9 <!--NeedCopy-->
```

Pour configurer IP ou IPANDVLAN comme méthode de recherche de clés à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres.**
2. Cliquez sur **Configurer les paramètres de l'abonné.**
3. Dans **Type de clé**, sélectionnez **IP** ou **IPANDVLAN selon vos** besoins.
4. Terminez la configuration et cliquez sur **OK**.

Gestion des sessions inactives des sessions d'abonnés dans un réseau de télécommunications

Le nettoyage de la session des abonnés sur une appliance NetScaler est basé sur les événements du plan de contrôle, tels qu'un message RADIUS Accounting Stop, un message Diameter RAR (libération de session) ou une commande « effacer la session de l'abonné ». Dans certains déploiements, les messages provenant d'un client RADIUS ou d'un serveur PCRF peuvent ne pas atteindre l'appliance. De plus, en cas de trafic intense, les messages peuvent être perdus. Une session d'abonné qui est inactive pendant une longue période continue de consommer de la mémoire et des ressources IP sur l'appliance NetScaler. La fonction de gestion des sessions inactives fournit des minuteries configurables pour identifier les sessions inactives et nettoie ces sessions en fonction de l'action spécifiée.

Une session est considérée comme inactive si aucun trafic en provenance de cet abonné n'est reçu sur le plan de données ou le plan de contrôle. Vous pouvez spécifier une action de mise à jour, d'arrêt (informer la PCRF puis supprimer la session) ou de supprimer (sans en informer la PCRF). L'action est exécutée uniquement lorsque la session est inactive pendant la durée spécifiée dans le paramètre de délai d'inactivité.

Pour configurer le délai d'inactivité de la session et l'action associée à l'aide de la ligne de commande

```
1 set subscriber param [-idleTTL <positive_integer>] [-idleAction <
     idleAction>]
2 <!--NeedCopy-->
```

Exemples :


```
set subscriber param -idleTTL 3600 -idleAction ccrTerminate

set subscriber param -idleTTL 3600 -idleAction ccrUpdate

set subscriber param -idleTTL 3600 -idleAction delete
<!--NeedCopy-->
```

Pour désactiver le délai d'inactivité de la session, définissez le délai d'inactivité sur zéro.

définir le paramètre d'abonné —IdLettl 0

Pour configurer le délai d'inactivité de la session et l'action associée à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Configurer les paramètres de l'abonné** et spécifiez une **durée d'inactivité** et une **action d'inactivité**.

Enregistrement des événements de session d'abonné

Si vous activez la journalisation des abonnés, vous pouvez suivre les messages du plan de contrôle RADIUS et Gx spécifiques à un abonné et utiliser les données historiques pour analyser les activités des abonnés. Certains des attributs clés sont le MSISDN et l'horodatage. Les attributs suivants sont également enregistrés :

- Événement de session (installation, mise à jour, suppression, erreur)
- Type de message Gx (CCR-I, CCR-U, CCR-T, RAR)
- Type de message Radius (début, arrêt)
- IP de l'abonné
- Type d'identifiant d'abonné (MSISDN (E164), IMSI)
- Valeur de l'ID d'abonné

À l'aide de ces journaux, vous pouvez suivre les utilisateurs par adresse IP et, le cas échéant, par MSISDN.

Vous pouvez activer la journalisation des sessions des abonnés sur un serveur syslog ou nslog local ou distant. L'exemple suivant montre comment activer la journalisation des abonnés sur un serveur Syslog distant.

```
    > add syslogAction sysact1 192.0.2.0 -loglevel EMERGENCY ALERT
       CRITICAL ERROR WARNING NOTICE INFORMATIONAL -subscriberlog
       enabled
<!--NeedCopy-->
```


À partir de ces journaux, vous pouvez en savoir plus sur toute activité liée à un utilisateur, telle que l'heure à laquelle une session a été mise à jour, supprimée ou créée (installée). En outre, les messages d'erreur sont également enregistrés.

Exemples :

1. Les entrées de journal suivantes sont des exemples de création, de mise à jour et de suppression de sessions RadiusandGX.

   > 30/09/2015 : 16:29:18 GMT Informatif 0-PPE-0 : SUBSCRIBER SESSION_EVENT 147 0 par défaut : Installation de la session, type de message GX : CCR-I, type de message RADIUS : Démarrer, IP : 100.10.1.1, ID : E164 - 30000000001
   >
   > 30/09/2015 : 16:30:18 GMT Informatif 0-PPE-0 : SUBSCRIBER SESSION_EVENT 148 0 par défaut : mise à jour de session, type de message GX : CCR-U, IP : 100.10.1.1, ID : E164 - 30000000001
   >
   > 30/09/2015 : 17:27:56 GMT Informatif 0-PPE-0 : SUBSCRIBER SESSION_EVENT 185 0 par défaut : Suppression de session, type de message GX : CCR-T, type de message RADIUS : Stop, IP : 100.10.1.1, ID : E164 - 30000000001

2. Les entrées de journal suivantes sont des exemples de messages d'échec, par exemple lorsqu'un abonné est introuvable sur le serveur PCRF et lorsque l'appliance ne parvient pas à se connecter au serveur PCRF.

   > 30/09/2015 : 16:44:15 GMT Erreur 0-PPE-0 : SUBSCRIBER SESSION_FAILURE par défaut 169 0 : Raison de l'échec : réponse à un échec PCRF, type de message GX : CCR-I, IP : 100.10.1.1
   >
   > 30 septembre 13:03:01 30/09/2015:16:49:08 GMT 0-PPE-0 : SESSION D'ABONNÉ PAR DÉFAUT _FAILURE 176 0 : Raison de l'échec : Impossible de se connecter à PCRF, GX Type de message : CCR-I, RADIUS Type de message : Démarrer, IP : 100.10.1.1, ID : E164 - 30000000001 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000

Fin de session LSN consciente de l'abonné

Dans les versions précédentes, si une session d'abonné était supprimée lors de la réception d'un message RADIUS Accounting STOP ou PCRF-RAR, ou à la suite de tout autre événement, tel que l'expiration ou le vidage du TTL, les sessions LSN correspondantes de l'abonné étaient supprimées uniquement après le délai d'expiration du délai LSN configuré. Les sessions LSN qui restent ouvertes jusqu'à l'expiration de ce délai continuent de consommer des ressources sur l'appliance.

À partir de la version 11.1, un nouveau paramètre (SubscrSessionRemoval) est ajouté. Si ce paramètre est activé et que les informations de l'abonné sont supprimées de la base de données des abonnés, les sessions LSN correspondant à cet abonné sont également supprimées. Si ce paramètre est désactivé, les sessions des abonnés expirent conformément aux paramètres de délai d'expiration du LSN.

Pour configurer la fermeture de session LSN consciente des abonnés à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

définir le paramètre lsn -SubscrSessionRemoval (ACTIVÉ)	DÉSACTIVÉ)

```
1      > set lsn parameter -subscrSessionRemoval ENABLED
2      Done
3      > sh lsn parameter
4                  LSN Global Configuration:
5
6                  Active Memory Usage: 0 MBytes
7                  Configured Memory Limit: 0 MBytes
8                  Maximum Memory Usage Limit: 912 MBytes
9                  Session synchronization: ENABLED
10                 Subscriber aware session removal: ENABLED
11 <!--NeedCopy-->
```

Pour configurer la fermeture de session LSN consciente des abonnés à l'aide de l'interface graphique

1. Accédez à **Système** > **NAT à grande échelle**.
2. Dans **Mise en route**, cliquez sur **Définir le paramètre LSN.**
3. Définissez le **paramètre Subscriber Aware Session Suppression**.

Dépannage

Si votre déploiement ne fonctionne pas comme prévu, utilisez les commandes suivantes pour résoudre les problèmes :

- show subscriber gxinterface La sortie de
  cette commande peut inclure les messages d'erreur suivants (affichés ici avec des suggestions de réponses) :
  - Interface Gx non configurée - Utilisez la commande set subscriber param pour configurer le type d'interface correct.
  - PCRF non configuré : configurez un vServer ou un service Diameter sur GXinterface-Utilisez la commande set subscriber gx interface pour attribuer un serveur ou un service virtuel Diameter à cette interface.

  - Le PCRF n'est pas prêt. Vérifiez le serveur v/le service correspondant pour plus de détails. Utilisez la commande show LB vserver ou show service pour vérifier l'état du service.
  - NetScaler attend le CEA de la part du PCRF. La négociation entre le PCRF et NetScaler risque d'échouer. Il peut s'agir d'un état intermittent. Si cela persiste, vérifiez les paramètres DIAMETER sur votre serveur PCRF.
  - La mémoire n'est pas configurée pour stocker les sessions des abonnés. Veuillez utiliser 'set extendedmemoryparam -memlimit <>' - Utilisez la commande set extendedmemoryparam pour configurer la mémoire étendue.
- show subscriber radiusinterface
  Si « Non configuré » est le résultat de cette commande, utilisez la commande set subscriber radiusinterface pour spécifier un service RadiusListener.

Si la journalisation des abonnés est activée, vous pouvez obtenir des informations plus détaillées à partir des fichiers journaux.

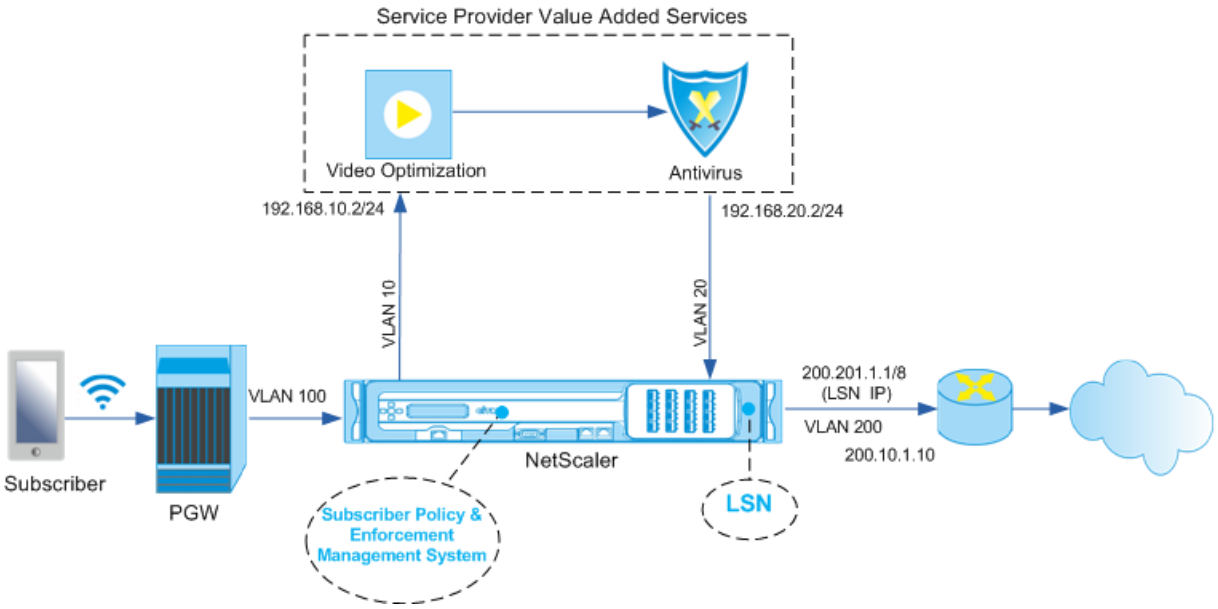
Direction de la circulation consciente des abonnés

May 5, 2023

La gestion du trafic dirige le trafic des abonnés d'un point à un autre. Lorsqu'un abonné se connecte au réseau, la passerelle de paquets associe une adresse IP à l'abonné et transmet le paquet de données à l'appliance NetScaler. L'appliance communique avec le serveur PCRF via l'interface Gx pour obtenir les informations de politique. En fonction des informations de politique, l'appliance exécute l'une des actions suivantes :

- Transférez le paquet de données vers un autre ensemble de services (comme indiqué dans l'illustration suivante).
- Déposez le paquet.
- Effectuez uniquement un NAT à grande échelle (LSN), si le LSN est configuré sur l'appliance.

Les valeurs affichées dans la figure suivante sont configurées dans la procédure CLI qui suit la figure. Un serveur virtuel de commutation de contenu sur l'appliance NetScaler dirige les demandes vers les services à valeur ajoutée ou les ignore, selon la règle définie, puis envoie le paquet vers Internet après avoir effectué le LSN.



Pour configurer le pilotage du trafic pour le déploiement ci-dessus à l'aide de l'interface de ligne de commande

Ajoutez les adresses IP de sous-réseau (SNIP) de l'appliance.

Exemple :

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 100.100.100.1 255.0.0.0 -type snip

add ns ip 200.200.200.1 255.0.0.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip

add ns ip 200.201.1.1 255.0.0.0 -type snip
<!--NeedCopy-->
```

Ajoutez les VLAN. Les VLAN aident l'appliance à identifier la source du trafic. Liez les VLAN aux interfaces et aux adresses IP des sous-réseaux.

Exemple :

```
add vlan 10

add vlan 20
```



```
4
5 add vlan 100
6
7 add vlan 200
8
9 bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0
10
11 bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0
12
13 bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0
14
15 bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.1.1.1 255.0.0.0
16 <!--NeedCopy-->
```

Spécifiez le VLAN sur lequel le trafic des abonnés arrive sur l'appliance. Spécifiez le chemin de service AVP qui indique à l'appliance où rechercher le nom du chemin de service dans la session de l'abonné. Pour les fonctionnalités PCEF principales, spécifiez le type d'interface sous la forme RadiusAndGX.

Exemple :

```
1 set ns param -servicePathIngressVLAN 100
2
3 set subscriber gxinterface -servicepathAVP 1001 1005 -
     servicepathVendorid 10415
4
5 set subscriber param -interfaceType RadiusAndGx
6 <!--NeedCopy-->
```

Configurez un service et un serveur virtuel de type Diameter, puis liez le service au serveur virtuel. Spécifiez ensuite le domaine PCRF et les paramètres de l'interface Gx de l'abonné. Pour les fonctionnalités PCEF principales, configurez un service d'écoute RADIUS et une interface RADIUS.

Exemple :

```
1 add service sd1 10.102.232.200 DIAMETER 3868
2
3 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
4
5 bind lb vserver vdiam sd1
6
7 set ns diameter -identity netscaler.sc1.net -realm pcrf1.net
8
9 set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
     holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120
```



```
10
11 add service srad1 10.102.232.236 RADIUSListener 1813
12
13 set subscriber radiusInterface -listeningService srad1
14 <!--NeedCopy-->
```

Ajoutez des fonctions de service pour associer un VAS à un VLAN d'entrée. Ajoutez un chemin de service pour définir la chaîne, c'est-à-dire spécifier le VAS auquel le paquet doit être envoyé et l'ordre dans lequel il doit être envoyé à ce VAS. Le nom du chemin du service est généralement envoyé par le PCRF. Toutefois, le chemin de service du profil d'abonné par défaut (*) s'applique si l'une des conditions suivantes est vraie :

- PCRF ne dispose pas des informations sur les abonnés.
- Les informations sur les abonnés n'incluent pas cet AVP.
- L'appliance ne parvient pas à interroger le PCRF. Par exemple, le service représentant le PCRF est DOWN.

Le chemin de service AVP qui contient ce nom doit déjà être configuré dans le cadre de la configuration globale. Liez la fonction de service au chemin de service. L'indice de service spécifie l'ordre dans lequel le VAS est ajouté à la chaîne. Le chiffre le plus élevé (255) indique le début de la chaîne.

Exemple :

```
1 add ns servicefunction SF1 -ingressVLAN 20
2
3 add ns servicepath pol1
4
5 bind ns servicepath pol1 -servicefunction SF1 -index 255
6
7 add subscriber profile * -subscriberrules default_path
8 <!--NeedCopy-->
```

Ajoutez la configuration LSN. En d'autres termes, définissez le pool NAT et identifiez les clients pour lesquels l'appliance doit exécuter le LSN.

```
1 add lsn pool pool1
2
3 bind lsn pool pool1 200.201.1.1
4
5 add lsn client client1
6
7 bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0
8
9 add lsn group group1 -clientname client1
10
```



```
bind lsn group group1 -poolname pool1
<!--NeedCopy-->
```

L'appliance exécute le LSN par défaut. Pour remplacer le LSN, vous devez créer un profil réseau avec le paramètre OverrideLSN activé et lier ce profil à tous les serveurs virtuels d'équilibrage de charge configurés pour les services à valeur ajoutée (VAS).

Exemple :

```
add netprofile np1

set netprofile np1 -overrideLsn ENABLED

set lb vserver vs1 -netprofile np1
<!--NeedCopy-->
```

Configurez le VAS sur l'appliance. Cela inclut la création des services et des serveurs virtuels, puis la liaison des services aux serveurs virtuels.

```
add service vas1 192.168.10.2 ANY 80 -usip YES

add service sint 200.10.1.10 ANY 80 -usip YES

add lb vserver vs1 ANY -m MAC -l2Conn ON

add lb vserver vint ANY -m MAC -l2Conn ON

bind lb vserver vs1 vas1

bind lb vserver vint sint
<!--NeedCopy-->
```

Ajoutez la configuration de commutation de contenu (CS). Cela inclut les serveurs virtuels, les politiques et leurs actions associées. Le trafic arrive sur le serveur virtuel CS et est ensuite redirigé vers le serveur virtuel d'équilibrage de charge approprié. Définissez des expressions qui associent un serveur virtuel à une fonction de service.

Exemple :

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csactint -targetLBVserver vint

```



```
add cs policy cspol1 -rule  SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
   SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```

Pour configurer le pilotage du trafic sur l'appliance à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **IP** et ajoutez les adresses IP du sous-réseau.
2. Accédez à Système > Réseau > **VLAN** et ajoutez des VLAN, liez les VLAN aux interfaces et aux adresses IP des sous-réseaux.
3. Accédez à **Gestion du trafic** > Chaîne de **services > Configurer leVLAN d'entrée du chemin de service et spécifiez un VLAN** d'entrée.
4. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres > Configurer les paramètresde l'abonné** et spécifiez les informations suivantes :
   - Type d'interface : Spécifiez **RadiusandGX**.
   - Configurez un serveur virtuel Diameter, un domaine PCRF et les paramètres de l'interface GX de l'abonné.
   - Spécifiez les paramètres de l'interface RADIUS.
5. Accédez à **Gestion du trafic** > Chaîne de **services >**Fonction de service**et ajoutez des fonctions de service pour associer un service à valeur ajoutée à un VLAN** d'entrée.
6. Accédez à **Système** > **Réseau** > **NAT à grande échelle**. Cliquez sur **Pools** et ajoutez un pool. Cliquez sur **Clients** et ajoutez un client. Cliquez sur **Groupes**, ajoutez un groupe et spécifiez le client. Modifiez le groupe et liez le pool à ce groupe.
7. Accédez à **Système** > **Réseau** > **Profils réseau** et ajoutez un profil réseau. Sélectionnez **Remplacer le LSN**. Accédez éventuellement à **Système** > **Réseau** > **Paramètres > Configurer les paramètresde la couche 3**et vérifiez que l'option**Remplacer le LSN n'est pas sélectionnée.**
8. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et configurez les serveurs virtuels et les services à valeur ajoutée sur l'appliance. Liez les services et le profil réseau au serveur virtuel.
9. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels** et configurez un serveur virtuel, une politique et une action. Spécifiez le serveur virtuel d'équilibrage de charge cible.

Pour configurer le chaînage de services sur l'appliance à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **IP** et ajoutez les adresses IP du sous-réseau.

2. Accédez à Système > Réseau > **VLAN** et ajoutez des VLAN, liez les VLAN aux interfaces et aux adresses IP des sous-réseaux.
3. Accédez à **Gestion du trafic** > Chaîne de **services > Configurer leVLAN d'entrée du chemin de service et spécifiez un VLAN** d'entrée.
4. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres > Configurer les paramètresde l'abonné** et spécifiez les informations suivantes :
   - Type d'interface : Spécifiez **RadiusandGX**.
   - Configurez un serveur virtuel Diameter, un domaine PCRF et les paramètres de l'interface GX de l'abonné.
   - Spécifiez les paramètres de l'interface RADIUS.
5. Accédez à **Gestion du trafic** > Chaîne de **services >**Fonction de service**et ajoutez des fonctions de service pour associer un service à valeur ajoutée à un VLAN** d'entrée.
6. Accédez à **Système** > **Réseau** > **NAT à grande échelle**. Cliquez sur **Pools** et ajoutez un pool. Cliquez sur **Clients** et ajoutez un client. Cliquez sur **Groupes**, ajoutez un groupe et spécifiez le client. Modifiez le groupe et liez le pool à ce groupe.
7. Accédez à **Système** > **Réseau** > **Profils réseau** et ajoutez un profil réseau. Sélectionnez **Remplacer le LSN**. Accédez éventuellement à **Système** > **Réseau** > **Paramètres > Configurer les paramètresde la couche 3**et vérifiez que l'option**Remplacer le LSN n'est pas sélectionnée.**
8. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et configurez les serveurs virtuels et les services à valeur ajoutée sur l'appliance. Liez les services et le profil réseau au serveur virtuel.
9. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels** et configurez un serveur virtuel, une politique et une action. Spécifiez le serveur virtuel d'équilibrage de charge cible.

Chaînage de service à compatibilité d'abonnés

May 5, 2023

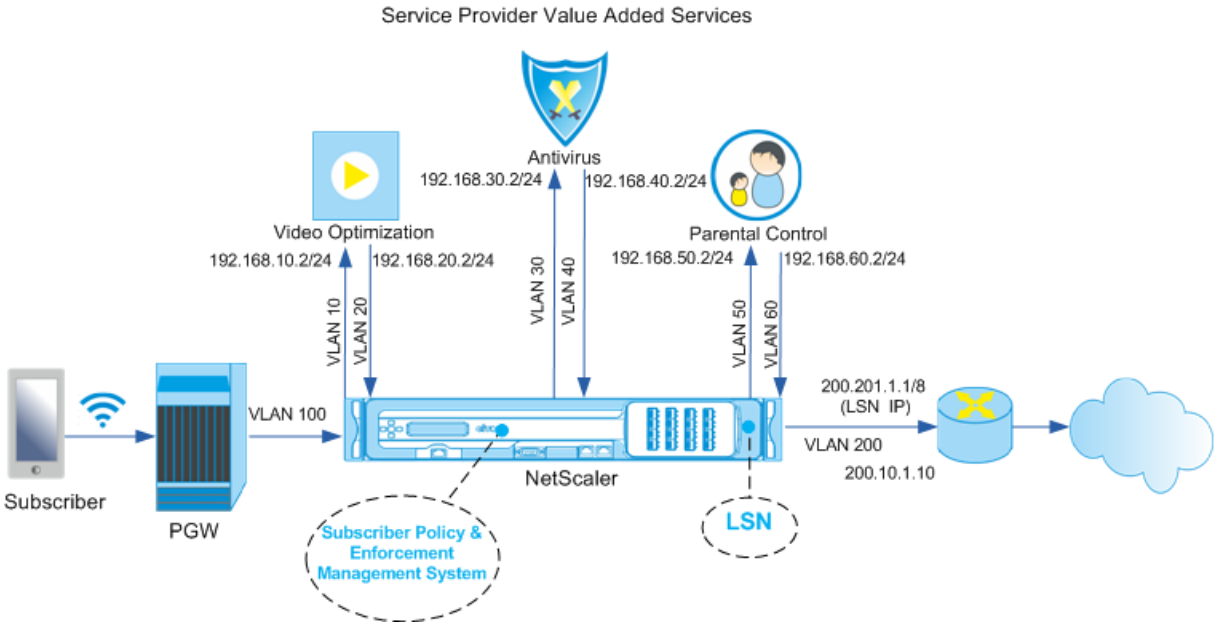
En raison de l'augmentation considérable du trafic de données transitant par les réseaux de télécommunications, il n'est plus possible pour les fournisseurs de services de diriger tout le trafic via tous les services à valeur ajoutée (VAS). Un fournisseur de services doit être en mesure d'optimiser l'utilisation du VAS et de diriger intelligemment le trafic afin d'améliorer l'expérience utilisateur. Par exemple, l'optimisation vidéo n'est pas requise pour le trafic qui n'inclut pas de vidéo. De plus, si un abonné est connecté à un réseau 4G, le contenu peut être diffusé en haute définition (HD) et l'optimisation vidéo n'est peut-être pas nécessaire. Toutefois, l'optimisation vidéo améliore l'expérience de l'utilisateur sur un réseau 3G. De même, la mise en cache offre une expérience utilisateur plus rapide et meilleure et peut être activée en fonction du plan d'abonnement. Un autre exemple de SAV est le contrôle parental. Si les parents fournissent un téléphone portable à un enfant mineur, ils souhaiteraient avoir

un certain contrôle sur les sites Web que leur enfant consulte.

Pour faire tout ce qui précède et bien plus encore, les fournisseurs de services doivent être en mesure de fournir des services à valeur ajoutée par abonné. En d'autres termes, les entités du réseau du fournisseur de services doivent être capables d'extraire les informations sur les abonnés et de diriger intelligemment le paquet sur la base de ces informations.

Le chaînage des services détermine l'ensemble des services par lesquels le trafic d'un abonné doit transiter avant d'accéder à Internet. Au lieu d'envoyer tout le trafic vers tous les services, NetScaler achemine intelligemment toutes les demandes d'un abonné vers un ensemble spécifique de services sur la base de la politique définie pour cet abonné.

La figure suivante montre les entités impliquées dans le chaînage des services. Les valeurs affichées sont configurées selon la procédure qui suit la figure. Un serveur virtuel de commutation de contenu sur l'appliance NetScaler dirige les demandes vers les services à valeur ajoutée ou les ignore, selon la règle définie, puis envoie le paquet vers Internet après avoir effectué le LSN.



Pour configurer le chaînage de services pour le déploiement ci-dessus à l'aide de l'interface de ligne de commande

Ajoutez les adresses IP de sous-réseau (SNIP) de l'appliance.

Exemple :

```
1 add ns ip 192.168.10.1 255.255.255.0 -type snip
2
3 add ns ip 192.168.20.1 255.255.255.0 -type snip
4
```



```
add ns ip 192.168.30.1 255.255.255.0 -type snip

add ns ip 192.168.40.1 255.255.255.0 -type snip

add ns ip 192.168.50.1 255.255.255.0 -type snip

add ns ip 192.168.60.1 255.255.255.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip

add ns ip 200.201.1.1 255.0.0.0 -type snip
<!--NeedCopy-->
```

Ajoutez les VLAN. Les VLAN aident l'appliance à identifier la source du trafic. Liez les VLAN aux interfaces et aux adresses IP des sous-réseaux. Ajoutez un VLAN d'entrée et un VLAN de sortie pour chaque VAS.

Exemple :

```
add vlan 10

add vlan 20

add vlan 30

add vlan 40

add vlan 50

add vlan 60

add vlan 100

add vlan 200

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.30.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.40.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.50.1 255.255.255.0

```



```
bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.60.1 255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0

bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.201.1.1 255.0.0.0
<!--NeedCopy-->
```

Spécifiez le VLAN sur lequel le trafic des abonnés arrive sur l'appliance. Spécifiez le chemin de service AVP qui indique à l'appliance où rechercher le nom du chemin de service dans la session de l'abonné. Pour les fonctionnalités PCEF principales, spécifiez le type d'interface sous la forme RadiusAndGX.

Exemple :

```
set ns param -servicePathIngressVLAN 100

set subscriber gxinterface -servicepathAVP 1001 1005 -
   servicepathVendorid 10415

set subscriber param -interfaceType RadiusAndGx
<!--NeedCopy-->
```

Configurez un service et un serveur virtuel de type Diameter, puis liez le service au serveur virtuel. Spécifiez ensuite le domaine PCRF et les paramètres de l'interface Gx de l'abonné. Pour les fonctionnalités PCEF principales, configurez un service d'écoute RADIUS et une interface RADIUS.

Exemple :

```
add service sd1 10.102.232.200 DIAMETER 3868

add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
   persistAVPno 263

bind lb vserver vdiam sd1

set ns diameter -identity netscaler.sc1.net -realm pcrf1.net

set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
   holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120

add service srad1 10.102.232.236 RADIUSListener 1813

set subscriber radiusInterface -listeningService srad1
<!--NeedCopy-->
```

Ajoutez des fonctions de service pour associer un VAS à un VLAN d'entrée. Ajoutez un chemin de ser-

vice pour définir la chaîne, c'est-à-dire spécifier le VAS auquel le paquet doit être envoyé et l'ordre dans lequel il doit être envoyé à ce VAS. Le nom du chemin du service est généralement envoyé par le PCRF. Toutefois, le chemin de service du profil d'abonné par défaut (*) s'applique si l'une des conditions suivantes est vraie :

- PCRF ne dispose pas des informations sur les abonnés.
- Les informations sur les abonnés n'incluent pas cet AVP.
- L'appliance ne parvient pas à interroger le PCRF. Par exemple, le service représentant le PCRF est DOWN.

Le chemin de service AVP qui contient ce nom doit être configuré au préalable dans le cadre de la configuration globale. Liez la fonction de service au chemin de service. L'indice de service spécifie l'ordre dans lequel le VAS est ajouté à la chaîne. Le chiffre le plus élevé (255) indique le début de la chaîne.

Exemple :

```
add ns servicefunction SF1 -ingressVLAN 20

add ns servicefunction SF2 -ingressVLAN 40

add ns servicefunction SF3 -ingressVLAN 60

add ns servicepath pol1

bind ns servicepath pol1 -servicefunction SF1 -index 255

bind ns servicepath pol1 -servicefunction SF2 -index 254

bind ns servicepath pol1 -servicefunction SF3 -index 253

add ns servicepath pol2

bind ns servicepath pol2 -servicefunction SF2 -index 255

add ns servicepath pol3

bind ns servicepath pol3 -servicefunction SF1 -index 255

add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

Ajoutez la configuration LSN. En d'autres termes, définissez le pool NAT et identifiez les clients pour lesquels l'appliance doit exécuter le LSN.

Exemple :


```
add lsn pool pool1

bind lsn pool pool1 200.201.1.1

add lsn client client1

bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0

add lsn group group1 -clientname client1

bind lsn group group1 -poolname pool1
<!--NeedCopy-->
```

L'appliance exécute le LSN par défaut. Pour remplacer le LSN, vous devez créer un profil réseau avec le paramètre OverrideLSN activé et lier ce profil à tous les serveurs virtuels d'équilibrage de charge configurés pour les services à valeur ajoutée (VAS).

Exemple :

```
add netprofile np1

set netprofile np1 -overrideLsn ENABLED

set lb vserver vs1 -netprofile np1
<!--NeedCopy-->
```

Configurez le VAS sur l'appliance. Cela inclut la création des services et des serveurs virtuels, puis la liaison des services aux serveurs virtuels.

Exemple :

```
add service vas1 192.168.10.2 ANY 80 -usip YES

add service vas2 192.168.30.2 ANY 80 -usip YES

add service vas3 192.168.50.2 ANY 80 -usip YES

add service sint 200.10.1.10 ANY 80 -usip YES

add lb vserver vs1 ANY -m MAC -l2Conn ON

add lb vserver vs2 ANY -m MAC -l2Conn ON

add lb vserver vs3 ANY -m MAC -l2Conn ON

```



```
add lb vserver vint ANY -m MAC -l2Conn ON

bind lb vserver vs1 vas1

bind lb vserver vs2 vas2

bind lb vserver vs3 vas3

bind lb vserver vint sint
<!--NeedCopy-->
```

Ajoutez la configuration de commutation de contenu (CS). Cela inclut les serveurs virtuels, les politiques et leurs actions associées. Le trafic arrive sur le serveur virtuel CS et est ensuite redirigé vers le serveur virtuel d'équilibrage de charge approprié. Définissez des expressions qui associent un serveur virtuel à une fonction de service.

Exemple :

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csact2 -targetLBVserver vs2

add cs action csact3 -targetLBVserver vs3

add cs action csactint -targetLBVserver vint

add cs policy cspol1 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
   SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

add cs policy cspol2 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF2") &&
   SYS.VSERVER("vs2").STATE.EQ(UP)" -action csact2

add cs policy cspol3 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF3") &&
   SYS.VSERVER("vs3").STATE.EQ(UP)" -action csact3

bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -policyName cspol2 -priority 120

bind cs vserver cs1 -policyName cspol3 -priority 130

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```


Pour configurer le chaînage de services sur l'appliance à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **IP** et ajoutez les adresses IP du sous-réseau.
2. Accédez à **Système** > **Réseau** > **VLAN** et ajoutez des VLAN, liez les VLAN aux interfaces et aux adresses IP des sous-réseaux.
3. Accédez à **Gestion du trafic** > Chaîne de **services > Configurer leVLAN d'entrée du chemin de service et spécifiez un VLAN** d'entrée.
4. Accédez à **Gestion du trafic** > **Abonné** > **Paramètres > Configurer les paramètresde l'abonné** et spécifiez les informations suivantes :
   - Type d'interface : Spécifiez **RadiusandGX**.
   - Configurez un serveur virtuel Diameter, un domaine PCRF et les paramètres de l'interface GX de l'abonné.
   - Spécifiez les paramètres de l'interface RADIUS.
5. Accédez à **Gestion du trafic** > Chaîne de **services >**Fonction de service**et ajoutez des fonctions de service pour associer un service à valeur ajoutée à un VLAN** d'entrée.
6. Accédez à **Système** > **Réseau** > **NAT à grande échelle**. Cliquez sur **Pools** et ajoutez un pool. Cliquez sur **Clients** et ajoutez un client. Cliquez sur **Groupes**, ajoutez un groupe et spécifiez le client. Modifiez le groupe et liez le pool à ce groupe.
7. Accédez à **Système** > **Réseau** > **Profils réseau** et ajoutez un profil réseau. Sélectionnez **Remplacer le LSN**. Accédez éventuellement à **Système** > **Réseau** > **Paramètres > Configurer les paramètresde la couche 3**et vérifiez que l'option**Remplacer le LSN n'est pas sélectionnée.**
8. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et configurez les serveurs virtuels et les services à valeur ajoutée sur l'appliance. Liez les services et le profil réseau au serveur virtuel.
9. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels** et configurez un serveur virtuel, une politique et une action. Spécifiez le serveur virtuel d'équilibrage de charge cible.

Direction du trafic sensible aux abonnés avec optimisation TCP

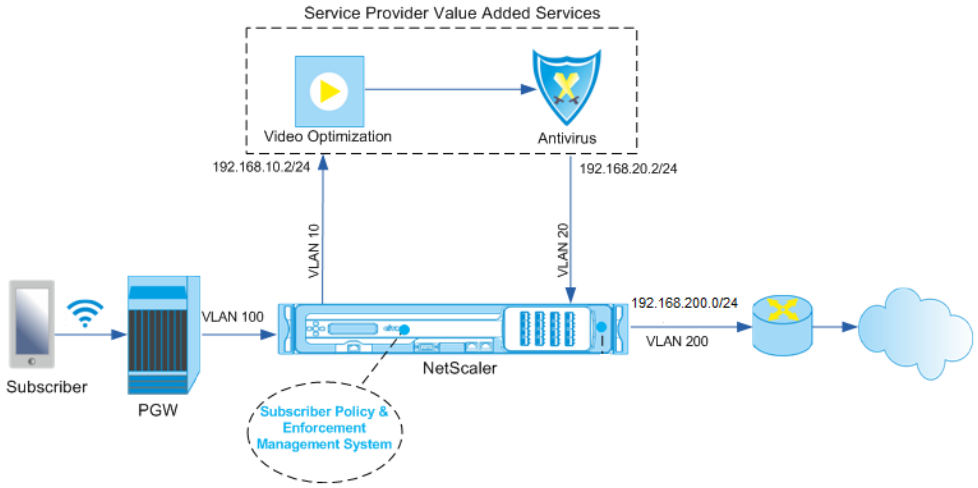
May 5, 2023

La gestion du trafic dirige le trafic des abonnés d'un point à un autre. Lorsqu'un abonné se connecte au réseau, la passerelle de paquets associe une adresse IP à l'abonné et transmet le paquet de données à l'appliance NetScaler. L'appliance communique avec le serveur PCRF via l'interface Gx pour obtenir les informations de politique d'abonnement. En fonction des informations de politique, l'appliance exécute l'une des actions suivantes :

- Transférez le paquet de données vers un autre ensemble de services (comme indiqué dans l'illustration suivante).

- Effectuez uniquement une optimisation TCP.

Les valeurs affichées dans la figure suivante sont configurées dans la procédure CLI qui suit la figure. Un serveur virtuel de commutation de contenu sur l'appliance NetScaler dirige les demandes vers les services à valeur ajoutée ou les ignore et effectue une optimisation TCP, en fonction de la règle définie, puis envoie le paquet vers Internet.



> **Remarque**
>
> La prise en charge de la configuration présentée ci-dessous a été introduite dans la version 11.1 build 50.10.

Pour configurer le pilotage du trafic pour le déploiement ci-dessus à l'aide de l'interface de ligne de commande :

1. Ajoutez les adresses IP de sous-réseau (SNIP) de l'appliance.

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 192.168.100.1 255.255.255.0 -type snip

add ns ip 192.168.200.1 255.255.255.0 -type snip

add ns ip 10.102.232.236 255.255.255.0  - type snip
<!--NeedCopy-->
```

2. Ajoutez les VLAN. Les VLAN aident l'appliance à identifier la source du trafic. Liez les VLAN aux interfaces et aux adresses IP des sous-réseaux.


```
add vlan 10

add vlan 20

add vlan 100

add vlan 200

add vlan 102

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1
   255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1
   255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 192.168.100.1
   255.255.255.0

bind vlan 200 -ifnum 1/2 -tagged -IPAddress 192.168.200.1
   255.255.255.0

bind vlan 102  - ifnum 1/1  - tagged  - IPAddress 10.102.232.236
   255.255.255.0
<!--NeedCopy-->
```

3. Configurez un service et un serveur virtuel de type Diameter, puis liez le service au serveur virtuel. Spécifiez le domaine PCRF et les valeurs des paramètres de l'interface Gx de l'abonné. Spécifiez également le chemin de service AVP qui indique où l'appliance peut trouver le nom du chemin de service dans la session de l'abonné. Pour les fonctionnalités PCEF principales, configurez un service d'écoute RADIUS et une interface RADIUS, puis spécifiez le type d'interface comme « RadiusAndGX ».

```
add service sd1 10.102.232.200 DIAMETER 3868

add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER
   -persistAVPno 263

bind lb vserver vdiam sd1

set ns diameter -identity netscaler.sc1.net -realm pcrf1.net

set extendedmemoryparam -memLimit 2558

```



```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net

set subscriber gxinterface -servicepathAVP 1001 1005 -
    servicepathVendorid 10415

add service srad1 10.102.232.236 RADIUSListener 1813

set subscriber radiusInterface -listeningService srad1

set subscriber param -interfaceType RadiusAndGx
<!--NeedCopy-->
```

4. Spécifiez un profil d'abonné par défaut (*) à appliquer si l'une des conditions suivantes est vraie :

   - PCRF ne dispose pas des informations sur les abonnés.
   - Les informations relatives à l'abonné n'incluent pas le chemin de service AVP.
   - L'appliance ne parvient pas à interroger le PCRF. Par exemple, le service représentant le PCRF est DOWN.

```
add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

5. Créez des profils TCP pour le VAS et le chemin d'optimisation TCP, respectivement. Le trafic dirigé vers le VAS ne fera l'objet d'aucune optimisation TCP avant ou après avoir quitté le VAS. Par conséquent, le mode TCP du profil VAS doit être défini sur TRANSPARENT tandis que le mode TCP du profil TCPpt doit être défini sur ENDPOINT.

   ajouter ns TCPProfile VAS —TCPMode TRANSPARENT

   add ns TCPProfile TCPpt -WS ACTIVÉ -SACK ACTIVÉ -WSVal 8 -mss 1460 -MaxBurst 30 -InitialCwnd 16 -OooqSize 15000 -Minto 800 -Taille du tampon 4000000 -flavor BIC -DynamicReceiveBuffering ACTIVÉ -KA ACTIVÉ -KA ACTIVÉ -SendBuffSize 4000000 -Atténuate RSTWindow ACTIVÉ -SpoofSyndrop ACTIVÉ -ecn ACTIVÉ -ecn ACTIVÉ -frto ACTIVÉ -maxc wnd 1000000 -fack ACTIVÉ -RSTMaxack activé -tcpmode ENDPOINT

6. Configurez l'équilibrage de charge pour les serveurs VAS. Créez un serveur virtuel non adressable de type TCP. Créez des services TCP avec les adresses IP des serveurs VAS et liez les services au serveur virtuel. Le serveur virtuel et les services utiliseront le profil TCP transparent créé pour le chemin VAS :

```
add service vas1 192.168.10.2 TCP * -usip YES -useproxyport NO -
    TCPB NO -tcpProfileName VAS

add service vas2 192.168.10.3 TCP * -usip YES -useproxyport NO -
    TCPB NO -tcpProfileName VAS
```



```
4
5 add lb vserver vs1 TCP -m MAC -l2Conn ON  - tcpProfileName VAS
6
7 bind lb vserver vs1 vas1
8
9 bind lb vserver vs1 vas2
10 <!--NeedCopy-->
```

7. Ajoutez un serveur virtuel d'équilibrage de charge pour capturer le trafic sortant du VAS. Ce serveur virtuel surveillera le VLAN de sortie du VAS et utilisera le profil TCP transparent :

```
1 add lb vserver vsint TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ(20)"
      - Listenpriority 30  - l2Conn ON  - tcpProfileName VAS
2 <!--NeedCopy-->
```

8. Ajoutez un serveur virtuel d'optimisation TCP qui écoute tout trafic sur le VLAN côté sans fil et utilise le profil TCP du point de terminaison créé pour le chemin d'optimisation TCP :

```
1 add lb vserver vs-TcpOpt TCP * * -Listenpolicy "client.vlan.id.eq
     (100)"  - Listenpriority 20 -l2Conn ON -tcpProfileName TCPOpt
2 <!--NeedCopy-->
```

9. Ajoutez la configuration de commutation de contenu (CS). Cela inclut les serveurs virtuels, les politiques et leurs actions associées. Le serveur virtuel CS reçoit le trafic et le redirige vers le serveur virtuel d'équilibrage de charge approprié conformément aux politiques CS définies. Créez un serveur virtuel CS TCP qui écoute tout trafic sur le VLAN côté sans fil avec la priorité la plus élevée et utilise le profil TCP du point de terminaison. Créez une politique CS qui donne la valeur TRUE lorsque « vas » est la règle d'abonné, et spécifiez une action CS qui oriente le trafic vers le VAS. Faites du serveur virtuel d'optimisation TCP le serveur virtuel LB par défaut. Tout trafic d'abonnés avec une règle autre que « vas » passera par le vserver LB par défaut.

```
1 add cs vserver cs1 TCP * * -Listenpolicy "client.vlan.id.eq(100)"
      - Listenpriority 10 -l2Conn ON  - tcpProfileName TCPOpt
2
3 add cs action csact1 -targetLBVserver vs1
4
5 add cs policy cspol1 -rule  SUBSCRIBER.RULE_ACTIVE("vas") && SYS.
     VSERVER("vs1").STATE.EQ(UP)" -action csact1
6
7 bind cs vserver cs1 -policyName cspol1
8
9 bind cs vserver cs1 -lbvserver vs-TcpOpt
10 <!--NeedCopy-->
```


10. Ajoutez des itinéraires statiques ou basés sur des règles vers Internet. Le routage dynamique est également pris en charge dans cette configuration. L'exemple suivant utilise des itinéraires basés sur des politiques :

```
add ns pbr pbr-vlan100-to-vlan200 ALLOW -nextHop 192.168.200.10 -
    vlan 100 -priority 10

add ns pbr pbr-vlan20-to-vlan200 ALLOW -nextHop 192.168.200.10 -
    vlan 20 -priority 11

apply ns pbrs
<!--NeedCopy-->
```

Remarque

- Les politiques CS peuvent contenir des adresses IP et des numéros de port en plus des expressions des abonnés. Par exemple, SUBSCRIBER.RULE_ACTIVE (« vas ») && && (CLIENT.TCP.DSTPORT.EQ (80) || CLIENT.TCP.DSTPORT.EQ (443). Ils peuvent également contenir des expressions basées sur HTTP, par exemple, HTTP.REQ.HOSTNAME.DOMAIN.EQ (« somedomain.com »). Dans ce cas, remplacez les entités TCP (vserver, service, etc.) par HTTP. La configuration du profil TCP reste la même.
- Ajoutez une configuration IPv6 (adresses, itinéraires, PBR) pour prendre en charge les abonnés IPv6. Les applications clientes Happy Eyeballs fonctionneront sans problème pour les chemins d'optimisation VAS et TCP.
- Ajoutez des VLAN, des adresses IP, des PBR et des serveurs virtuels LB devant le VAS (vs1, vs2, etc.) pour prendre en charge plusieurs flux d'abonnés. Modifiez les politiques d'écoute de CS vserver « cs1 » et de LB vserver « vsint » pour inclure les VLAN supplémentaires.

Sélection de profil TCP basée sur une stratégie

May 5, 2023

Vous pouvez configurer l'appliance NetScaler pour effectuer une optimisation TCP en fonction des attributs des abonnés. Par exemple, l'appliance peut sélectionner différents profils TCP au moment de l'exécution, en fonction du réseau auquel l'équipement utilisateur (UE) est connecté. Par conséquent, vous pouvez améliorer l'expérience d'un utilisateur mobile en définissant certains paramètres dans les profils TCP, puis en utilisant une politique pour sélectionner le profil approprié.

Créez des profils TCP distincts pour les abonnés se connectant via un réseau 4G et pour les utilisateurs se connectant via n'importe quel autre réseau. Définissez une règle de politique sélectionnée en fonction d'un paramètre d'abonné, tel que le type de technologie d'accès radio (type RAT). Dans

les exemples suivants, si le type RAT est EUTRAN, un profil TCP prenant en charge une connexion plus rapide est sélectionné (Exemple 1). Pour toutes les autres valeurs de type RAT, un profil TCP différent est sélectionné (Exemple 2).

Pour plus d'informations sur la technologie d'accès radio et sa configuration de politique, consultez la RFC 29.212.

> **Remarque**
>
> L'AVP de type RAT (code AVP 1032) est de type « Enumerated » et est utilisé pour identifier la technologie d'accès radio desservant l'UE.
>
> La valeur « 1004 » indique que le RAT est EUTRAN.

Exemple 1 :

```
add ns tcpProfile tcp2 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
    16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 1000000 -flavor BIC
     - dynamicReceiveBuffering DISABLED -sendBuffsize 1000000 -dsack
    DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 500 -maxburst 15

add appqoe action appact2 -priority HIGH -tcpprofile tcp2

add appqoe policy apppol2 -rule "SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).EQ(1004)" -action appact2

bind cs vserver <name>  -policyname apppol2 -priority 20 -type request
<!--NeedCopy-->
```

Exemple 2 :

```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
    16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 150000 -flavor BIC
    - dynamicReceiveBuffering DISABLED -sendBuffsize 150000 -dsack
    DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 200 -maxburst 15

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule "SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).NE(1004)" -action appact1

bind cs vserver <name>  -policyname apppol1 -priority 10 -type request
<!--NeedCopy-->
```


Trafic du plan de contrôle de l'équilibrage de charge basé sur les protocoles Diameter, SIP et SMPP

May 5, 2023

Avec l'augmentation du trafic au niveau du plan de contrôle, les serveurs peuvent devenir un goulot d'étranglement car le trafic n'est pas réparti de manière optimale entre les serveurs. Par conséquent, la charge des messages doit être équilibrée. L'appliance NetScaler prend en charge l'équilibrage de charge Diameter, SIP et SMPP.

SIP

NetScaler vous permet d'équilibrer la charge des messages SIP via UDP ou TCP (y compris TLS) vers un groupe de serveurs proxy. NetScaler fournit également une méthode de persistance basée sur l'ID d'appel et d'équilibrage de la charge par hachage de l'identifiant d'appel à l'aide de laquelle vous dirigez les paquets d'une session SIP particulière vers le même serveur SIP à équilibrage de charge.
Le langage d'expressions par défaut de NetScaler contient un certain nombre d'expressions qui fonctionnent sur les connexions SIP (Session Initiation Protocol). Ces expressions sont destinées à être utilisées dans les politiques du protocole SIP qui fonctionne sur la base d'une demande/réponse. Ces expressions peuvent être utilisées dans les stratégies de commutation de contenu, de limitation de débit, de répondeur et de réécriture.

Pour plus d'informations, consultez la section Équilibrage de charge d'un groupe de serveurs SIP.

SMPP

Des millions de messages courts sont échangés quotidiennement entre des particuliers et des fournisseurs de services à valeur ajoutée, tels que des banques, des annonceurs et des services d'annuaire, à l'aide du protocole de message court pair à pair (SMPP). La livraison des messages est souvent retardée car les serveurs sont surchargés et le trafic n'est pas réparti de manière optimale entre les serveurs.
L'appliance NetScaler assure une distribution optimale des messages sur vos serveurs, évitant ainsi les mauvaises performances et les pannes. L'appliance NetScaler :

- Équilibre la charge des messages provenant du serveur et du client
- Surveille l'état des centres de messagerie
- Fournit un support de commutation de contenu pour les centres de messagerie
- Gère les messages concaténés

Limitation : les ID de message provenant du centre de messagerie d'une longueur supérieure à 59 octets ne sont pas pris en charge. Si la longueur de l'ID de message renvoyé par le centre de mes-

sagerie est supérieure à 59 octets, les opérations auxiliaires échouent et l'appliance NetScaler répond par un message d'erreur.

Pour plus d'informations, voir Équilibrage de charge SMPP

Diameter

Diameter est un protocole de base qui repose sur plus de 50 protocoles (également appelés applications). Par conséquent, le diamètre du trafic généré dans un réseau de télécommunications est élevé. Pour maintenir de manière optimale ce diamètre de trafic, l'appliance NetScaler effectue un équilibrage de charge, une commutation de contenu et agit en tant qu'agent relais. En outre, l'appliance offre des fonctionnalités de réécriture et de répondeur. L'appliance prend en charge la limitation de débit des messages de Diameter.

Pour plus d'informations, voir Configuration de l'équilibrage de charge de diamètre.

Fournir des services d'infrastructure DNS et de trafic, tels que l'équilibrage de charge, la mise en cache et la journalisation pour les fournisseurs de services de télécommunications

May 5, 2023

Les fournisseurs de services de télécommunications peuvent configurer l'appliance NetScaler pour qu'elle fonctionne comme un proxy DNS. La mise en cache des enregistrements DNS, qui constitue une fonction importante d'un proxy DNS, est activée par défaut sur l'appliance NetScaler. Cela permet à l'appliance NetScaler de fournir des réponses rapides pour les traductions répétées, améliorant ainsi l'expérience client tout en économisant de la bande passante. Les réponses des serveurs de noms DNS sont mises en cache. Lorsque l'appliance reçoit une requête DNS, elle vérifie la présence du domaine interrogé dans son cache. Si l'adresse du domaine interrogé est présente dans son cache, l'appliance NetScaler renvoie l'adresse correspondante au client. Sinon, il transmet la requête à un serveur de noms DNS qui vérifie la disponibilité de l'adresse et la renvoie à l'appliance NetScaler. L'appliance NetScaler renvoie ensuite l'adresse au client.

Pour les demandes concernant un domaine qui a déjà été mis en cache, l'appliance NetScaler fournit l'enregistrement d'adresse du domaine à partir du cache sans interroger le serveur DNS configuré, ce qui permet d'économiser de la bande passante.

À partir de la version 11.0, NetScaler enregistre également les requêtes DNS qu'il reçoit ainsi que les réponses qu'il envoie au client. Les fournisseurs de services de télécommunications peuvent utiliser ce journal pour :

- Audit des réponses DNS au client
- Audit des clients DNS
- Détecter et prévenir les attaques DNS
- Dépannage

Pour plus d'informations, voir Système de noms de domaine.

Distribution de la charge des abonnés à l'aide de la GSLB sur les réseaux principaux d'un fournisseur de services de télécommunications

May 5, 2023

L'évolutivité, la haute disponibilité et les performances sont essentielles aux déploiements des fournisseurs de services. Bien que de nombreux fournisseurs de services déploient leur infrastructure sur un ou plusieurs sites, ces déploiements sont soumis à un certain nombre de limitations inhérentes, telles que :

- Si le site perd la connectivité à tout ou partie de l'Internet public, il sera inaccessible aux utilisateurs et aux clients, ce qui peut avoir un impact significatif sur l'activité.
- Les utilisateurs accédant au site depuis des sites géographiquement éloignés peuvent subir des retards importants et très variables, qui sont exacerbés par le grand nombre d'allers-retours nécessaires au protocole HTTP pour transférer du contenu.

L'équilibrage global de la charge des serveurs (GSLB) de l'appliance NetScaler permet de surmonter ces problèmes en répartissant le trafic entre les sites déployés dans plusieurs zones géographiques. En diffusant du contenu à partir de différents points d'Internet, le GSLB atténue l'impact des goulots d'étranglement de la bande passante du réseau et assure la robustesse en cas de défaillance du réseau sur un site donné. Les utilisateurs peuvent être automatiquement dirigés vers le site le plus proche ou le moins chargé au moment de la demande, minimisant ainsi la probabilité de longs délais de téléchargement et/ou d'interruptions de service.

Vous pouvez utiliser l'équilibrage de charge de serveur global de l'appliance NetScaler pour :

- Reprise après sinistre ou haute disponibilité en configurant une configuration de centre de données actif en veille composée d'un centre de données actif et d'un centre de données de secours. Lorsqu'un basculement survient à la suite d'un sinistre, le centre de données de secours devient opérationnel.
- Disponibilité et rapidité élevées grâce à la configuration d'un centre de données actif-actif composé de plusieurs centres de données actifs. Les demandes des clients sont équilibrées de charge entre les datacenters actifs.
- Diriger les demandes des clients vers le centre de données le plus proche en termes de distance géographique ou de distance réseau en configurant une configuration de proximité.

- Résolutions DNS complètes, le GSLB traite les requêtes DNS des types A, AAAA et CNAME, et l'option de fonction DNS peut traiter les requêtes DNS de tous les autres types, tels que MX et PTR. De plus, si la résolution récursive est activée, l'appliance transmettra les requêtes DNS pour les noms de domaine qui ne sont pas configurés sur l'appliance NetScaler.

Pour plus d'informations, voir Global Server Load Balancing.

Utilisation de la bande passante avec la fonctionnalité de redirection du cache

May 5, 2023

Le volume du trafic Web sur Internet est énorme et une grande partie de ce trafic est redondant. Plusieurs clients demandent à plusieurs reprises aux serveurs Web le même contenu, ce qui entraîne une utilisation inefficace de la bande passante. Pour soulager le serveur Web d'origine du traitement de chaque demande, les fournisseurs de services Internet (ISP) peuvent utiliser la fonctionnalité de redirection du cache de l'appliance NetScaler et diffuser le contenu à partir d'un serveur de cache plutôt que depuis le serveur d'origine. L'appliance NetScaler analyse les demandes entrantes, envoie des demandes de données pouvant être mises en cache aux serveurs de cache et envoie des demandes non mises en cache et des requêtes HTTP dynamiques aux serveurs d'origine. La fonctionnalité de redirection du cache de NetScaler est basée sur des règles et, par défaut, les demandes qui correspondent à une politique sont envoyées au serveur d'origine et toutes les autres demandes sont envoyées à un serveur de cache. Vous pouvez combiner la commutation de contenu avec la redirection de cache pour mettre en cache du contenu sélectif et diffuser du contenu à partir de serveurs de cache spécifiques pour des types spécifiques de contenu demandé.

Pour plus d'informations, voir Redirection du cache.

Optimisation du protocole TCP avec NetScaler

May 5, 2023

L'appliance NetScaler fournit des techniques et des fonctionnalités avancées de réglage et d'optimisation du TCP parfaitement adaptées aux réseaux 3,5 et 4G modernes, améliorant ainsi de manière significative l'expérience utilisateur et les vitesses de téléchargement perçues.

Cette section se concentre sur des instructions détaillées concernant :

- Choix et insertion d'un modèle NetScaler série T1000 approprié dans un réseau mobile pour l'optimisation du protocole TCP

- Instructions de configuration complètes relatives non seulement à l'optimisation TCP, mais également à la configuration appropriée des couches 2 et 3 du périphérique T1

La section inclut les rubriques suivantes :

Mise en route

May 5, 2023

Matériel

NetScaler propose un large éventail de modèles NetScaler qui peuvent être librement basés sur deux facteurs :

- Capacité, comprise actuellement entre des centaines de Mbit/s pour l'appliance VPX bas de gamme et 160 Gbit/s pour l'appliance haut de gamme de la série 25000 MPX
- Niveau Telco, avec la disponibilité de la série T1000 pour les centres de données Telco.

Votre représentant commercial ou de support NetScaler peut vous aider à sélectionner le matériel approprié pour vos besoins de démonstration, d'essai ou de production.

Le reste de cette section utilise un NetScaler T1200 comme matériel de référence. Notez que si l'on met de côté les différences superficielles liées au nombre et à la notation des interfaces disponibles (voir * note) ou les limitations bien documentées de NetScaler VPX (voir * note), les instructions doivent s'appliquer pour la plupart mot pour mot quel que soit le modèle NetScaler sélectionné.

> **Remarque**
>
> * Par exemple, le modèle T1010 ne possède que du 12x1GbE, généralement marqué 1/1-1/12 au lieu de la notation 10/x utilisée dans ce document.
>
> ** Une instance NetScaler VPX ne prend généralement pas en charge l'agrégation LACP ; elle peut également ne pas prendre en charge le balisage VLAN.

Configuration initiale

Par le biais de la console série

Une fois qu'un câble série est connecté, vous pouvez vous connecter à l'appliance NetScaler à l'aide des informations d'identification suivantes :

- Nom d'utilisateur : nsroot
- Mot de passe : nsroot

Une fois connecté, configurez les détails de base de l'appliance NetScaler comme indiqué dans la capture d'écran ci-dessous.

Exemple :

```
set ns config  - IPAddress <ip_addr> -netmask <netmask>

saveconfig

reboot -warm
<!--NeedCopy-->
```

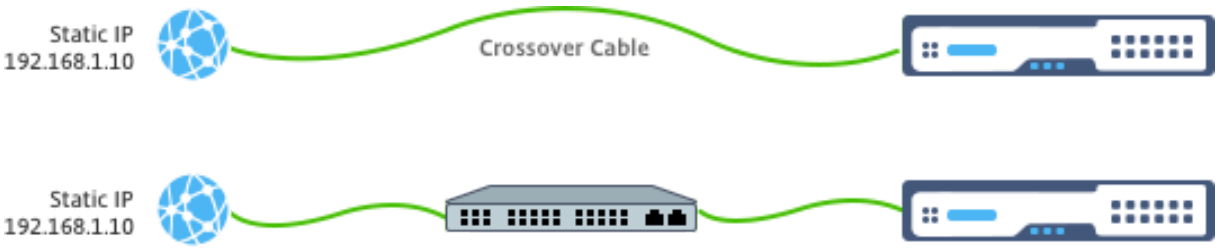
Après avoir redémarré l'appliance, vous pouvez utiliser SSH pour poursuivre la configuration des nœuds T1100.

Grâce à LOM

Le port Lights Out Management (LOM) situé sur le panneau avant de l'appliance NetScaler permet à l'opérateur de surveiller et de gérer à distance l'appliance indépendamment du système d'exploitation. L'opérateur peut modifier l'adresse IP, le cycle d'alimentation et effectuer un vidage de code en se connectant à l'appliance NetScaler via le port LOM.

L'adresse IP par défaut du port LOM est 192.168.1.3

Chiffre. Configuration initiale du module LOM



Définissez une adresse IP statique sur votre ordinateur portable et branchez-la directement à l'interface LOM à l'aide d'un câble croisé ou à un commutateur situé dans le même domaine de diffusion que l'interface LOM.

Pour la configuration initiale, saisissez l'adresse par défaut du port : http://192.168.1.3 dans un navigateur Web et modifiez l'adresse IP par défaut du port LOM.

Reportez-vous aux guides de configuration pour plus de détails.

Logiciel

L'optimisation TCP de NetScaler pour les réseaux mobiles est en constante évolution. Les fonctionnalités et les réglages décrits dans ce document nécessitent une version NetScaler Telco. Voici un exemple illustrant la version NetScaler Telco.

Exemple :

```
1 show ver
2
3 NetScaler NS11.0: Build 64.957.nc, Date: Aug 26 2016, 02:00:23
4 <!--NeedCopy-->
```

Si le T1000 n'a pas été livré avec la révision de build appropriée, contactez le support client de NetScaler.

> **Important**
>
> Les deux appliances doivent avoir la même image logicielle.

Client SSH

Une appliance NetScaler peut être configurée à l'aide de la CLI ou de l'interface graphique HTML5. Toutefois, cette section fournit uniquement des instructions basées sur l'interface de ligne de commande.

Bien que la CLI soit accessible via la console série NetScaler, un client SSH est normalement recommandé pour permettre la configuration NetScaler à distance.

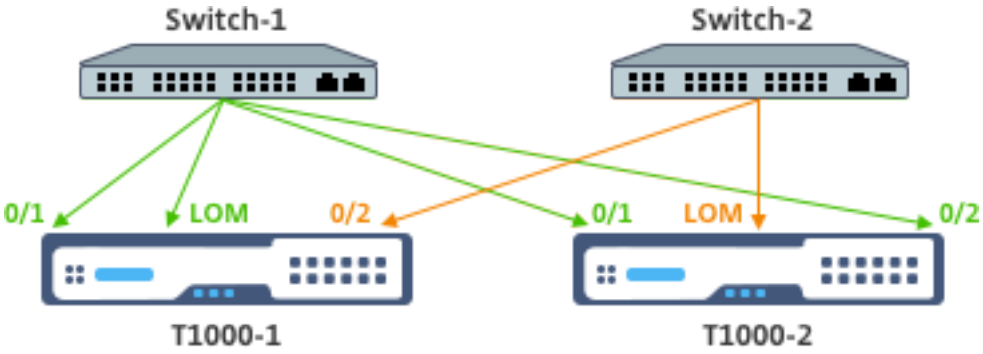
Réseau de gestion

May 5, 2023

Connectivité

La plupart des appareils NetScaler proposent des ports OAM 1 GbE redondants, notés 0/1 et 0/2. Pour assurer la redondance en cas de panne d'un commutateur, vous devez connecter les ports concernés aux différents commutateurs en amont.

Un aperçu général de la connectivité recommandée est présenté dans le schéma suivant :



Une fois que l'appliance NetScaler est connectée au réseau de gestion, les étapes de configuration suivantes peuvent être effectuées à distance à l'aide de SSH ou d'une connectivité Web à l'interface de ligne de commande et à l'interface graphique respectivement.

Routage

La commande add route peut être utilisée pour configurer tous les itinéraires appropriés au réseau de gestion. La passerelle appropriée doit être accessible sur le sous-réseau NSIP, comme indiqué ci-dessous.

Exemple :

```
add route <network>  <netmask>  <gateway>
<!--NeedCopy-->
```

Gestion des licences

May 5, 2023

Un fichier de licence valide doit être installé sur l'appliance NetScaler. La licence doit prendre en charge au moins autant de Gbit/s que le débit Gi-LAN maximal attendu.

Les fichiers de licence doivent être copiés via un client SCP vers le fichier /nsconfig/license de l'appliance, comme indiqué dans la capture d'écran ci-dessous.

Exemple :

```
shell ls /nsconfig/license/

CNS_V3000_SERVER_PLT_Retail.lic ssl
<!--NeedCopy-->
```

Redémarrez à chaud pour appliquer la nouvelle licence, comme indiqué dans la capture d'écran ci-dessous.

Exemple :

```
reboot -warm

Are you sure you want to restart NetScaler (Y/N)? [N]:y

Done
<!--NeedCopy-->
```

Une fois le redémarrage terminé, vérifiez que la licence a été correctement appliquée, à l'aide de l'interface de ligne de commande show license.

Dans l'exemple ci-dessous, une licence Premium 3 Gbit/s a été installée avec succès.

Exemple :

```
> show license

            License status:

                                    Web Logging: YES

                                            ...

                                Model Number ID: 3000

                                   License Type: Premium License

Done

<!--NeedCopy-->
```

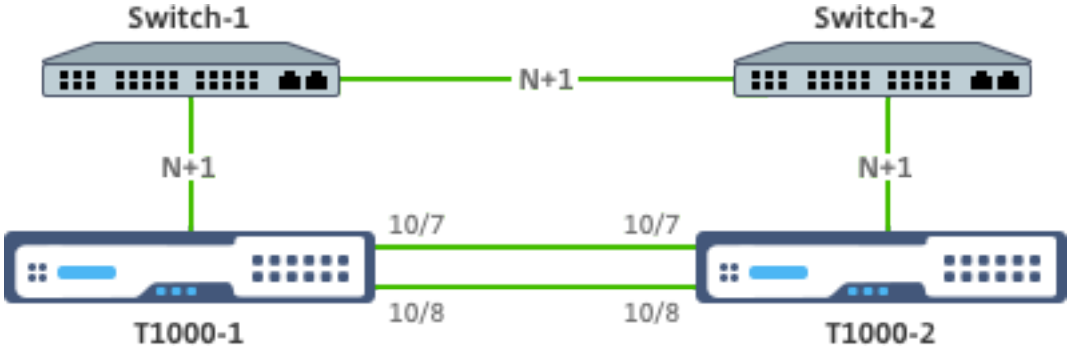

Haute disponibilité

May 5, 2023

La haute disponibilité (HA) fait référence au mode de fonctionnement actif-veille d'une paire d'appareils NetScaler. Chaque appareil possède sa propre adresse IP de gestion dédiée. Toutes les autres adresses IP appartiennent à l'appareil actif de la paire.

Connectivité

Bien qu'il existe plusieurs options de connectivité pour une paire NetScaler HA, la plus recommandée est illustrée dans le schéma suivant :



Dans le diagramme ci-dessus, les liaisons rouges N+1 entre chaque T1000 et le commutateur respectif impliquent une redondance N+1, comme expliqué dans Connectivité. Par exemple, considérer un Gi-LAN 45 Gbit/s N=5 est une valeur appropriée, avec des canaux LACP 6x10GbE entre chaque commutateur et le T1000 respectif ainsi qu'entre les deux commutateurs.

Une paire de liens supplémentaire est recommandée entre la paire NetScaler, afin d'isoler les communications HA du réseau OAM.

Intégration Gi-LAN

May 5, 2023

Généralement, une appliance NetScaler est insérée en tant que nœud L3 en ligne distinct dans le Gi-LAN, de la même manière qu'un routeur L3.

Figure : Une représentation simple d'un Gi-LAN

Connectivité

Une connectivité NetScaler physique aux commutateurs en amont est recommandée pour garantir une redondance suffisante. Par exemple, en supposant qu'une appliance NetScaler soit insérée dans un Gi-LAN qui gère un total (liaison montante et liaison descendante) de 24 Gbit/s, une connectivité avec 4 interfaces 10 GbE ou plus est recommandée. Cela permet une redondance N+1 en cas de défaillance de la liaison.

Les ports concernés du commutateur en amont doivent être configurés pour l'agrégation de ports LACP. La configuration appropriée sur NetScaler est décrite ci-dessous :

Configuration de la connectivité :

```
set interface 10/1 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/2 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/3 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/4 -tagall ON -lacpMode ACTIVE -lacpKey 1
<!--NeedCopy-->
```

Vous pouvez vérifier la fonctionnalité appropriée de LACP à l'aide de la commande « show interface » :

Afficher l'interface :

```
sh interface LA/1

    1)      Interface LA/1 (802.3ad Link Aggregate) #39

             flags=0x4100c020 <ENABLED, UP, AGGREGATE, UP, HAMON, 802.1
                q>

             MTU=1500, native vlan=1, MAC=02:e0:ed:33:88:b0, uptime 340
                h11m56s

             Requested: media NONE, speed AUTO, duplex NONE, fctl NONE,

```



```
11              throughput 0
12
13              Actual: throughput 4000
14
15              LLDP Mode: NONE,
16
17              RX: Pkts(918446) Bytes(110087414) Errs(0) Drops(795989)
                    Stalls(0)
18
19              TX: Pkts(124113) Bytes(15255532) Errs(0) Drops(0) Stalls
                    (0)
20
21              NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
                    Muted(0)
22
23              Bandwidth thresholds are not set.
24
25  Disable the remaining unused interfaces and turn off the monitor.
26
27  set interface 10/5  -haMonitor OFF
28  <!--NeedCopy-->
```

Commande :

```
1  set interface 10/24  -haMonitor OFF
2
3  disable interface 10/5
4
5  disable interface 10/24
6  <!--NeedCopy-->
```

La configuration des interfaces physiques n'est pas partagée entre les deux unités NetScaler. Par conséquent, les commandes ci-dessus doivent être exécutées sur les deux nœuds NetScaler en cas de déploiement d'une paire HA.

Configuration HA

Tous les autres paramètres de configuration sont partagés entre les nœuds NetScaler d'une paire HA. Par conséquent, la synchronisation HA doit être activée avant l'exécution de toute autre commande de configuration. La configuration HA de base implique les étapes suivantes :

1. Utilisation du même matériel, du même logiciel et de la même licence NetScaler : les paires HA ne sont pas prises en charge entre différents modèles (par exemple, un T1100 et un MPX21550) ou entre des modèles identiques avec des niveaux de microprogramme différents. Reportez-vous aux

instructions appropriées sur la mise à niveau d'une paire HA existante - Mise à niveau vers la version 11.1.

2. Mise en place de la paire HA.

Exemple :

```
netscaler-1> add HA node 1 <netscaler-2-NSIP>

netscaler-2> add HA node 1 <netscaler-1-NSIP>
<!--NeedCopy-->
```

3. Vérifiez l'établissement de la paire HA exécutant la commande suivante dans l'un ou l'autre des nœuds ; les deux nœuds doivent être visibles, l'un d'eux en tant que principal (actif), l'autre en tant que secondaire (en veille).

Exemple :

```
show HA node
<!--NeedCopy-->
```

4. Activez le mode Failsafe et MaxFlips. Cela garantit qu'en cas de défaillance du moniteur de route sur les deux nœuds, au moins un nœud reste actif sans changement constant d'état actif/de veille.

Exemple :

```
set HA node  - failsafe ON

set HA node -maxFlips 3 -maxFlipTime 1200
<!--NeedCopy-->
```

5. Enfin, autorisez la synchronisation HA sur les ports intra-NetScaler dédiés plutôt que sur le réseau OAM.

Exemple :

```
add vlan 4080 -aliasName syncVlan

set HA node -syncvlan 4080
<!--NeedCopy-->
```

> **Remarque**
>
> Le VLAN 4080 dans les commandes de l'exemple ci-dessus ne doit pas être pris à la lettre. Tout ID de VLAN inutilisé peut être réservé.

Configuration du VLAN

Une fois que les interfaces physiques ont été correctement configurées, vous pouvez configurer les VLAN Gi-LAN appropriés. Par exemple, considérez un environnement Gi-LAN plutôt simple avec une paire de VLAN d'entrée et de sortie avec un identificateur VLAN 100/101 respectivement.

Les commandes suivantes configurent les VLAN appropriés au-dessus du canal LACP créé à l'étape précédente.

```
add vlan 100
add vlan 101
bind vlan 100 -ifnum LA/1 -tagged
bind vlan 101 -ifnum LA/1 -tagged
<!--NeedCopy-->
```

Configuration IPv4

Généralement, une appliance NetScaler nécessite un SNIP par VLAN. L'exemple ci-dessous suppose que les réseaux décrits dans le diagramme d'intégration Gi-LAN, indiqué au début de cette page, ont un masque de sous-réseau /24 :

```
add ns ip 192.168.1.254 255.255.255.0 -vserver DISABLED -mgmtAccess
    DISABLED
add ns ip 192.168.2.254 255.255.255.0 -vserver DISABLED -mgmtAccess
    DISABLED
<!--NeedCopy-->
```

Une fois les SNIP configurés, ils doivent être associés au VLAN approprié :

```
bind vlan 100 -IPAddress 192.168.1.254 255.255.255.0
bind vlan 101 -IPAddress 192.168.2.254 255.255.255.0
<!--NeedCopy-->
```

Routage statique IPv4

L'exemple décrit dans la section Réseau de gestion n'appelle que quelques règles de routage statiques :

- Une route statique 10.0.0.0/8 vers les clients via le routeur d'entrée
- Un itinéraire par défaut vers Internet via le routeur de sortie

Exemple :

```
add route 0.0.0.0 0.0.0.0 192.168.2.1
```



```
add route 10.0.0.0 255.0.0.0 192.168.1.1
<!--NeedCopy-->
```

Routage basé sur des stratégies IPv4 (VLAN - VLAN)

Une appliance NetScaler permet un routage basé sur des politiques plutôt que sur un routage statique, les décisions de routage étant généralement prises en fonction de l'interface entrante et/ou du VLAN plutôt que de l'adresse IP de destination. Le routage basé sur des règles est soit une alternative pratique, dans le cas où la plage d'adresses IP source du client est sujette à des modifications périodiques, soit une considération obligatoire, dans le cas où l'adresse IP de destination d'un paquet ne suffit pas à elle seule pour prendre une décision de routage (c'est-à-dire en cas de chevauchement des adresses IP du client sur plusieurs VLAN).

Exemple :

```
add ns pbr fromWirelessToInternet ALLOW -nextHop 192.168.2.1 -vlan
    100 -priority 10

Done

 add ns pbr fromInternetToWireless ALLOW -nextHop 192.168.1.1 -vlan
     200 -priority 20

Done

apply ns pbrs
<!--NeedCopy-->
```

Configuration IPv6

Les commandes suivantes attribuent un SNIP IPv6 par VLAN. L'exemple ci-dessous suppose que les réseaux décrits dans la Figure : Une représentation simple d'un Gi-LAN dans cette page ont un masque de sous-réseau /64 :

Commande :

```
add ns ip6 fd00:192:168:1::254/64 -vServer DISABLED -mgmtAccess
    DISABLED
add ns ip6 fd00:192:168:2::254/64 -vServer DISABLED -mgmtAccess
    DISABLED
bind vlan 100 -IPAddress fd00:192:168:1::254/64
bind vlan 200 -IPAddress fd00:192:168:2::254/64
<!--NeedCopy-->
```


Routage IPv6

Une fois l'adressage IPv6 terminé, le routage statique IPv6 peut être configuré :

- Une route statique fd 00:10 : :/64 vers les clients via le routeur d'entrée
- Un itinéraire par défaut vers Internet via le routeur de sortie

Exemple :

```
add route6 fd00:10::/64 fd00:192:168:1::1
add route6 ::/0 fd00:192:168:2::1
<!--NeedCopy-->
```

Ou en utilisant un routage basé sur des règles :

Exemple :

```
add ns pbr6 fromWirelessToInternetv6 ALLOW -vlan 100 -priority 10 -
    nextHop fd00:192:168:2::1

add ns pbr6 fromInternetToWirelessv6 ALLOW -vlan 200 -priority 20 -
    nextHop fd00:192:168:1::1

apply ns pbr6
<!--NeedCopy-->
```

Redondance et basculement LACP

Dans le cas d'une configuration HA, il est recommandé de tirer parti de l'option de débit pour configurer un seuil bas pour le canal LACP. Par exemple, considérez un Gi-LAN 25 Gbit/s et un canal 4 x 10 GbE entre chaque appliance NetScaler de la paire HA et le commutateur en amont pour fournir une redondance des liens N+1 :

Exemple :

```
set interface LA/1 -haMonitor ON -throughput 29000
<!--NeedCopy-->
```

En cas de défaillance de double liaison entre l'appliance principale et le commutateur en amont, le débit Gi-LAN maximal pouvant être pris en charge tombera à 20 Gbps. Un seuil bas de 29 Gbit/s selon l'exemple ci-dessus entraînerait un événement de basculement de redondance vers l'appliance secondaire (qui n'a pas subi de défaillances de liaison similaires), de sorte que le trafic Gi-LAN n'est pas affecté.

Moniteurs d'itinéraire

Outre la redondance LACP, les vérifications du moniteur d'itinéraire peuvent être configurées et associées à la configuration de la paire HA. Les contrôles de routage peuvent être utiles pour détecter les défaillances entre l'appliance NetScaler et les routeurs du prochain saut, en particulier si ces routeurs ne sont pas directement connectés mais via un commutateur en amont.

Une configuration typique du moniteur de routage HA selon l'exemple de GI-LAN dans la section 2.5.1 est décrite ci-dessous :

```
add route 192.168.1.0 255.255.255.0 192.168.1.1 -msr ENABLED -monitor
    arp
add route 192.168.2.0 255.255.255.0 192.168.2.1 -msr ENABLED -monitor
    arp
bind HA node -routeMonitor 192.168.1.0 255.255.255.0
bind HA node -routeMonitor 192.168.2.0 255.255.255.0
<!--NeedCopy-->
```

Configuration d'optimisation TCP

May 5, 2023

Avant de configurer l'optimisation TCP, appliquez les paramètres de configuration de base suivants sur l'appliance NetScaler :

Configuration initiale :

```
enable ns feature LB IPv6PT
enable ns mode FR L3 USIP MBF Edge USNIP PMTUD
disable ns feature SP
disable ns mode TCPB
set lb parameter -preferDirectRoute NO
set lb parameter -vServerSpecificMac ENABLED
set l4param -l2ConnMethod Vlan
set rsskeytype -rsstype SYMMETRIC
set ns param -useproxyport DISABLED
<!--NeedCopy-->
```

> **Remarque**
>
> Redémarrez l'appliance NetScaler si vous modifiez le paramètre système rsskeytype.

Terminaison TCP

Pour que NetScaler T1 applique l'optimisation TCP, il doit d'abord mettre fin au trafic TCP entrant. À cette fin, un vserver TCP générique doit être créé et configuré pour intercepter le trafic entrant, puis le transmettre au routeur Internet.

Environnement de routage statique ou dynamique

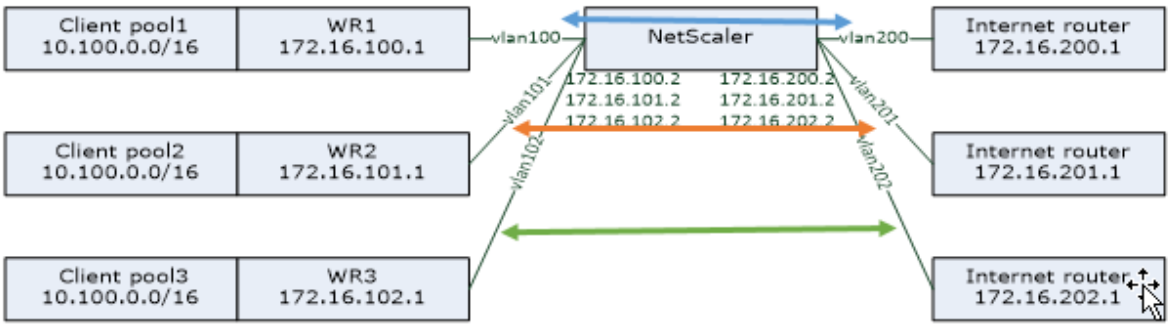
Pour les environnements dans lesquels un routage statique ou dynamique est en place, vserver peut s'appuyer sur les informations de la table de routage pour transférer les paquets vers un routeur Internet. La route par défaut doit pointer vers le routeur Internet et les entrées de routage des sous-réseaux clients vers le routeur sans fil doivent également être en place :

Exemple :

```
1 add lb vserver vsrv-wireless TCP * * -persistenceType NONE -
     Listenpolicy "CLIENT.VLAN.ID.EQ(100) && SYS.VSERVER("vsrv-wireless")
     .STATE.EQ(UP)" -m IP -cltTimeout 9000
2 add route 0.0.0.0 0.0.0.0 192.168.2.1
3 add route 10.0.0.0 255.0.0.0 192.168.1.1
4 <!--NeedCopy-->
```

Environnement VLAN-to-VLAN (PBR)

Dans certains environnements clients, le trafic des abonnés est segmenté en plusieurs flux et doit être transféré vers différents routeurs en fonction des paramètres du trafic entrant. Le routage basé sur des politiques (PBR) peut être utilisé pour acheminer des paquets en fonction des paramètres des paquets entrants, tels que le VLAN, l'adresse MAC, l'interface, l'adresse IP source, le port source, l'adresse IP de destination et le port de destination.



Exemple :


```
add lb vserver vsrv-wireless TCP * * -m IP -l2Conn ON -listenpolicy "
    CLIENT.VLAN.ID.EQ(100) || CLIENT.VLAN.ID.EQ(101) || CLIENT.VLAN.ID.
    EQ(102)"

add ns pbr pbr-vlan100-to-vlan200 ALLOW -vlan 100 -nexthop 172.16.200.1

add ns pbr pbr-vlan101-to-vlan201 ALLOW -vlan 101 -nexthop 172.16.201.1

add ns pbr pbr-vlan102-to-vlan202 ALLOW -vlan 102 -nexthop 172.16.202.1
<!--NeedCopy-->
```

L'utilisation du routage basé sur des politiques pour acheminer le trafic optimisé TCP est une nouvelle fonctionnalité ajoutée dans la version 11.1 50.10. Dans les versions précédentes, le fait d'avoir plusieurs entités vserver « en mode MAC » par VLAN était une solution alternative pour les environnements multi-VLAN. Chaque serveur virtuel possède un service lié représentant le routeur Internet pour le flux en question.

Exemple :

```
add server internet_router_1 172.16.200.1

add server internet_router_2 172.16.201.1

add server internet_router_3 172.16.202.1

add service svc-internet-1 internet_router_1 TCP * -usip YES -
    useproxyport NO

add service svc-internet-2 internet_router_2 TCP * -usip YES -
    useproxyport NO

add service svc-internet-3 internet_router_3 TCP * -usip YES -
    useproxyport NO

bind service svc-internet-1 -monitorName arp

bind service svc-internet-2 -monitorName arp

bind service svc-internet-3 -monitorName arp

add lb vserver vsrv-wireless-1 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
    (100) && SYS.VSERVER("vsrv-wireless-1").STATE.EQ(UP)" -m MAC -l2Conn
     ON

add lb vserver vsrv-wireless-2 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
```



```
    (101) && SYS.VSERVER("vsrv-wireless-2").STATE.EQ(UP)" -m MAC -l2Conn
     ON

add lb vserver vsrv-wireless-3 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
    (102) && SYS.VSERVER("vsrv-wireless-3").STATE.EQ(UP)" -m MAC -l2Conn
     ON

bind lb vserver vsrv-wireless-1 svc-internet-1

bind lb vserver vsrv-wireless-2 svc-internet-2

bind lb vserver vsrv-wireless-3 svc-internet-3
<!--NeedCopy-->
```

> **Remarque :**
>
> Le mode vserver est MAC contrairement aux exemples précédents où il s'agit du mode IP. Cela est nécessaire pour conserver les informations IP de destination lorsque des services sont liés à vserver. De plus, la configuration PBR supplémentaire doit acheminer le trafic non optimisé.

Optimisation TCP

La terminaison TCP NetScaler prête à l'emploi est configurée pour la fonctionnalité de transmission TCP. Le transfert TCP signifie essentiellement que NetScaler T1 peut intercepter de manière transparente un flux TCP client-serveur mais ne conserve pas de tampons client-serveur séparés et n'applique aucune technique d'optimisation.

Pour activer l'optimisation TCP, un profil TCP, nommé nstcpprofile, est utilisé pour spécifier les configurations TCP qui sont utilisées si aucune configuration TCP n'est fournie au niveau du service ou du serveur virtuel et il doit être modifié comme suit :

Commande :

```
add ns tcpProfile nstcpprofile -WS ENABLED -SACK ENABLED -WSVal 8 -mss
    1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
    ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
    spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
    fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT
<!--NeedCopy-->
```

> **Remarque :**
>
> Si aucun profil n'est explicitement créé et lié à vserver et à service, le profil nstcp_default_profile

> est lié par défaut.
>
> En cas de besoin de plusieurs profils TCP, des profils TCP supplémentaires peuvent être créés et associés au serveur virtuel approprié

Commande :

```
add ns tcpProfile custom_profile -WS ENABLED -SACK ENABLED -WSVal 8 -
    mss 1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
    ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
    spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
    fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT

set lb vserver vsrv-wireless -tcpProfileName custom_profile
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour les déploiements avec vserver -m MAC et service, le même profil doit être associé au service.

```
set service svc-internet -tcpProfileName custom_profile
<!--NeedCopy-->
```

Capacités d'optimisation TCP

La plupart des fonctionnalités d'optimisation TCP pertinentes d'une appliance NetScaler sont exposées via un profil TCP correspondant. Les paramètres CLI typiques à prendre en compte lors de la création d'un profil TCP sont les suivants :

1. **Dimensionnement des fenêtres (WS)** : le dimensionnement des fenêtres TCP permet d'augmenter la taille de la fenêtre de réception TCP au-delà de 65 535 octets. Il contribue à améliorer les performances TCP en général et en particulier dans les réseaux à bande passante élevée et à long retard. Il permet de réduire la latence et d'améliorer le temps de réponse via TCP.
2. **Accusé de réception sélectif (SACK)** : le protocole TCP SACK résout le problème de la perte de plusieurs paquets, ce qui réduit la capacité de débit globale. Grâce à un accusé de réception sélectif, le destinataire peut informer l'expéditeur de tous les segments reçus avec succès, ce qui permet à l'expéditeur de ne retransmettre que les segments perdus. Cette technique permet à T1 d'améliorer le débit global et de réduire la latence de connexion.
3. **Facteur de mise à l'échelle de la fenêtre (WSVal)** : facteur utilisé pour calculer la nouvelle taille de fenêtre. Il doit être configuré avec une valeur élevée afin de permettre à la fenêtre annoncée par NS d'être au moins égale à la taille de la mémoire tampon.

4. **Taille maximale de segment (MSS)** : MSS d'un seul segment TCP. Cette valeur dépend du paramètre MTU sur les routeurs intermédiaires et les clients finaux. Une valeur de 1460 correspond à un MTU de 1500.
5. **MaxBurst** : nombre maximum de segments TCP autorisés dans une rafale.
6. **Taille de la fenêtre de congestion initiale (InitialCWND)** : La taille initiale de la fenêtre de congestion TCP détermine le nombre d'octets qui peuvent être en attente au début de la transaction. Cela permet à T1 d'envoyer ces nombreux octets sans se soucier de la congestion du fil.
7. **Taille maximale de la file d'attente de paquets OOO (oooQSize)** : TCP gère la file d'attente hors ordre afin de conserver les paquets OOO dans la communication TCP. Ce paramètre a un impact sur la mémoire système si la taille de la file d'attente est longue car les paquets doivent être conservés dans la mémoire d'exécution. Cela doit donc être maintenu à un niveau optimisé en fonction du type de réseau et des caractéristiques de l'application.
8. **RTO minimum (minRTO)** : le délai de retransmission TCP est calculé sur chaque ACK reçu en fonction de la logique d'implémentation interne. Le délai de retransmission par défaut est d'une seconde au départ et peut être modifié avec ce paramètre. Pour la seconde retransmission de ces paquets, RTO sera calculé par N*2, puis N*4… N*8… se poursuit jusqu'à la dernière tentative de retransmission.
9. **BufferSize/SendBuffSize** : il s'agit de la quantité maximale de données que le T1 peut recevoir du serveur et de la mettre en mémoire tampon en interne sans les envoyer au client. Ils doivent être définis sur une valeur supérieure (au moins le double) au produit de retard de bande passante du canal de transmission sous-jacent.
10. **flavor** : il s'agit de l'algorithme de contrôle de congestion TCP. Les valeurs valides sont Default, BIC, CUBIC, Westwood et Nile.
11. Mise**en mémoire tampon dynamique** : permet d'ajuster dynamiquement la mémoire tampon de réception en fonction des conditions de la mémoire et du réseau. Il remplira la mémoire tampon autant que nécessaire pour maintenir le canal de téléchargement du client plein au lieu de remplir, en lisant à l'avance depuis le serveur, une mémoire tampon de taille fixe, car cette dernière est spécifiée dans le profil TCP et généralement basée sur des critères tels que 2*BDP, pour une connexion. NetScaler T1 surveille l'état du réseau pour le client et estime la quantité de données qu'il doit lire à l'avance sur le serveur.
12. **Keep-Alive (KA)** : envoyez des sondes TCP Keep-Alive (KA) périodiques pour vérifier si le pair est toujours actif.
13. RSTWindowAtténuate : défense du protocole TCP contre les attaques par usurpation d'identité. Il répondra avec un ACK correctif lorsqu'un numéro de séquence n'est pas valide.
14. **RSTMaxack** : active ou désactive l'acceptation d'un RST qui est hors fenêtre mais qui fait écho au numéro de séquence ACK le plus élevé.
15. **SpoofSyndrop** : suppression des paquets SYN non valides pour se protéger contre l'usurpation d'identité.

16. **Notification d'encombrement explicite (ecn)** : elle envoie une notification de l'état de congestion du réseau à l'expéditeur des données et prend des mesures correctives en cas de congestion ou de corruption des données.
17. **Restauration RTO directe** : en cas de retransmissions intempestives, les configurations de contrôle de congestion sont rétablies à leur état d'origine.
18. **Fenêtre de congestion maximale TCP (maxcwnd)** : taille de fenêtre d'encombrement maximale TCP configurable par l'utilisateur.
19. **Accusé de réception (FACK)** : pour éviter l'encombrement du protocole TCP en mesurant explicitement le nombre total d'octets de données restant sur le réseau et en aidant l'expéditeur (T1 ou client) à contrôler la quantité de données injectées dans le réseau pendant les délais de retransmission.
20. **tcpmode** : modes d'optimisation TCP pour un profil spécifique. Il existe deux modes d'optimisation TCP : Transparent et Endpoint.

    - Point final. Dans ce mode, l'appliance gère les connexions client et serveur séparément.
    - Transparent. En mode transparent, les clients doivent accéder directement aux serveurs, sans aucun serveur virtuel intermédiaire. Les adresses IP du serveur doivent être publiques car les clients doivent pouvoir y accéder.

Suppression silencieuse des connexions inactives

Dans un réseau de télécommunications, près de 50 % des connexions TCP d'une appliance NetScaler deviennent inactives et l'appliance envoie des paquets RST pour les fermer. Les paquets envoyés via des canaux radio activent ces canaux inutilement, provoquant un flot de messages qui, à leur tour, amènent l'appliance à générer un flot de messages de rejet de service. Le profil TCP par défaut inclut désormais les paramètres DropHalfClosedConnOnTimeout et DropEstConnOnTimeout, qui sont désactivés par défaut. Si vous activez les deux, ni une connexion à moitié fermée ni une connexion établie n'entraînent l'envoi d'un paquet RST au client lorsque la connexion expire. L'appliance interrompt simplement la connexion.

```
set ns tcpProfile nstcpprofile  -DropHalfClosedConnOnTimeout ENABLED
set ns tcpProfile nstcpprofile  -DropEstConnOnTimeout ENABLED
<!--NeedCopy-->
```

Analyses et rapports

May 5, 2023

Le rapport de vitesse TCP est une fonctionnalité de NetScaler qui extrait les statistiques de connexion TCP, afin de mesurer les performances de téléchargement et de chargement TCP, et est

utilisée dans les rapports TCP Insight de NetScaler Application Delivery Management (ADM). Pour ce faire, NetScaler surveille chaque connexion TCP, localise les rafales de paquets en fonction du délai d'inactivité et rapporte des mesures clés (telles que le nombre d'octets, le nombre d'octets retransmis et la durée) pour la rafale maximale identifiée. La fonctionnalité de rapport de vitesse TCP est activée par défaut, prend en charge les vServers TCP et HTTP et dépend de l'infrastructure de reporting AppFlow/ULFD.

Statistiques en temps réel

August 20, 2021

La commande stat peut être utilisée pour vérifier que l'optimisation TCP est correctement appliquée :

Commande :

```
> stat lb vserver vsrv-wireless
Virtual Server Summary
                      vsrvIP  port     Protocol        State   Health
                         actSvcs
vsrv...eless               *     0          TCP           UP      100
           1

            inactSvcs
vsrv...eless       0
Virtual Server Statistics
                                          Rate (/s)
                                             Total
Vserver hits                                      0
    10
Requests                                          0
                      0
Responses                                         0
                      0
Request bytes                                     0
    1580
Response bytes                                    0
    532594360
Total Packets rcvd                                0
    216463
Total Packets sent                                0
    369898
Current client connections                       --
                      0
```



```
18 Current Client Est connections                    --
                         0
19 Current server connections                        --
                         0
20 Requests in surge queue                           --
                         0
21 Requests in vserver's surgeQ                      --
                         0
22 Requests in service's surgeQs                     --
                         0
23 Spill Over Threshold                              --
                         0
24 Spill Over Hits                                   --
                         0
25 Labeled Connection                                --
                         0
26 Push Labeled Connection                           --
                         0
27 Deferred Request                                   0
                         0
28 Invalid Request/Response                          --
                         0
29 Invalid Request/Response Dropped                  --
                         0
30 Bound Service(s) Summary
31                          IP  port         Type        State     Hits
                                  Hits/s
32 svc-internet     192.168.2.2     0          TCP           UP       10
         0/s
33
34                 Req    Req/s      Rsp    Rsp/s Throughp ClntConn
                      SurgeQ
35 svc-internet      0      0/s        0      0/s        0        0
           0
36                  SvrConn   ReuseP  MaxConn ActvTran  SvrTTFB     Load
37 svc-internet        0        0        0        0        0        0
```

Les compteurs Total devraient constamment augmenter pour un système opérationnel. En outre, les compteurs de taux doivent être non nuls.

> **Remarque**
>
> La sortie précédente provient d'un système de laboratoire opérationnel mais inactif, expliquant le taux zéro.

SNMP

May 5, 2023

L'agent SNMP peut être interrogé pour obtenir des informations spécifiques au système à partir d'un périphérique distant (SNMP Manager). Sur la base de la requête, l'agent recherche l'identifiant d'objet égal (OID) dans la base d'informations de gestion (MIB) pour les données demandées et envoie les informations au gestionnaire SNMP. Les OID SNMP les plus utiles pour les déploiements de télécommunications sont les suivants :

Mémoire

- **Utilisation de ResMem (1.3.6.1.4.1.5951.4.1.1.41.2)**

Pourcentage d'utilisation de la mémoire sur NetScaler.

Processeur du moteur de paquets

- **Utilisation du reCPU (1.3.6.1.4.1.5951.4.1.1.41.1)**

Pourcentage d'utilisation du processeur.

- **NSCPUtable (1.3.6.1.4.1.5951.4.1.1.41.6)**

Ce tableau contient des informations sur chaque processeur de NetScaler.

Indexé sur : NSCPUname

- **Nom du NSCP (1.3.6.1.4.1.5951.4.1.1.41.6.1.1)**

Le nom du processeur.

- **Utilisation du NSCPU (1.3.6.1.4.1.5951.4.1.1.41.6.1.2)**

Pourcentage d'utilisation du processeur.

Débit

- **Tous les bits NIC vers TRXM (1.3.6.1.4.1.5951.4.1.1.71.1)**

Nombre de mégabits reçus par l'appliance NetScaler.

- **Tous les bits NIC en TTX (1.3.6.1.4.1.595 1.4.1.1.71.2)**

Nombre de mégabits transmis par l'appliance NetScaler.

- **IP vers TRXPKTS (1.3.6.1.4.1.5951.4.1.1.43.25)**

Paquets IP reçus.

- **IP vers TRXMbits (1.3.6.1.4.1.5951.4.1.1.43.27)**

Mégabits de données IP reçus.

- **IP en TXPKTS (1.3.6.1.4.1.5951.4.1.1.43.28)**

Paquets IP transmis.

- **IP en bits TXMbits (1.3.6.1.4.1.5951.4.1.1.43.30)**

Mégabits de données IP transmis.

Connexions

Connexions actives :

- **TCP ActiveServerConn (1.3.6.1.4.1.5951.4.1.1.46.8)**

Connexions à un serveur qui répond actuellement à des demandes.

Nombre total de connexions :

- **TCPCURServerConn (1.3.6.1.4.1.5951.4.1.1.46.1)**

Connexions au serveur, y compris les connexions à l'état Ouvrir, Établi et Fermer.

- **TCPCurClientConn (1.3.6.1.4.1.5951.4.1.1.46.2)**

Connexions client, y compris les connexions à l'état Ouvrir, Établi et Fermer.

Remarque : En raison du cookie de synchronisation, cela n'inclut pas le client en état d'ouverture

- **TCP vers Zombie CLTConnFlushed (1.3.6.1.4.1.5951.4.1.1.46.26)**

Connexions client qui sont vidées parce que le client est resté inactif pendant un certain temps.

- **TCP vers Zombies VRConnFlushed (1.3.6.1.4.1.5951.4.1.1.46.27)**

Connexions au serveur qui sont vidées car aucune demande client n'a été enregistrée dans la file d'attente depuis un certain temps.

Erreurs

- **TCP pour RSyngiveUp (1.3.6.1.4.1.5951.4.1.1.46.37)**

Tente d'établir une connexion sur NetScaler après expiration du délai imparti.

- **TC par transmission RF (1.3.6.1.4.1.595 1.4.1.1.46.60)**

Nombre de fois que NetScaler met fin à une connexion après avoir retransmis le paquet sept fois sur cette connexion. La retransmission se produit lorsque l'extrémité réceptrice n'accuse pas réception du paquet.

- **Si je trouve des cartes IS (1.3.6.1.2.1.2.2.1.13)**

Le nombre de paquets entrants qui ont été choisis pour être supprimés alors qu'aucune erreur n'avait été détectée pour empêcher leur distribution vers un protocole de couche supérieure. L'une des raisons possibles de la suppression d'un tel paquet pourrait être de libérer de l'espace tampon.

- **En cas de rejet (1.3.6.1.2.1.2.2.1.19)**

Le nombre de paquets sortants qui ont été choisis pour être supprimés alors qu'aucune erreur n'avait été détectée pour empêcher leur transmission. L'une des raisons possibles de la suppression d'un tel paquet pourrait être de libérer de l'espace tampon.

- **Dépassement d'IFERRTX (1.3.6.1.4.1.5951.4.1.1.54.1.36)**

Nombre de paquets qui sont passés par les files d'attente de débordement, lors de la transmission sur l'interface spécifiée, depuis le démarrage de l'appliance NetScaler ou depuis l'effacement des statistiques de l'interface. Cela n'est incrémenté que sur les ports encombrés.

Connexions optimisées/contournées

- **Optimisation TCP activée (1.3.6.1.4.1.5951.4.1.1.46.131)**

Nombre total de connexions activées avec l'optimisation TCP.

- **Optimisation TCP contournée (1.3.6.1.4.1.5951.4.1.1.46.132)**

Nombre total de connexions ayant contourné l'optimisation TCP.

Recettes techniques

May 5, 2023

Les modèles NetScaler T1 fournissent des fonctionnalités avancées et un puissant langage de configuration des politiques qui permettent d'évaluer des décisions complexes en cours d'exécution.

Bien qu'il ne soit pas possible d'évaluer toutes les fonctionnalités potentiellement débloquées par le guide de configuration des fonctionnalités et des politiques du T1000, les recettes techniques tiennent compte de la mise en œuvre de diverses exigences formulées par les opérateurs de télécommunications. N'hésitez pas à réutiliser les « recettes » telles qu'elles sont ou à les adapter à votre environnement.

Limite de connexion par utilisateur

Le modèle NetScaler T1 peut être configuré pour limiter le nombre de connexions par adresse IP d'abonné unique. Avec la configuration ci-dessous, N connexions TCP simultanées par IP

(CLIENT.IP.SRC) sont autorisées. Pour chaque tentative de connexion au-delà du seuil configuré, T1 envoie un RST. Pour un maximum de 2 connexions simultanées par utilisateur :

Commande :

```
add stream selector streamSel_usrlimit CLIENT.IP.SRC
add ns limitIdentifier limitId_usrlimit -threshold 2 -mode CONNECTION -
    selectorName streamSel_usrlimit
add responder policy respPol_usrlimit "SYS.CHECK_LIMIT("
    limitId_usrlimit")" RESET
bind lb vserver vsrv-wireless -policyName respPol_usrlimit -priority 1
    -gotoPriorityExpression END
<!--NeedCopy-->
```

Insertion et suppression fluides de Vserver

De nombreux opérateurs s'inquiètent de l'interruption des connexions TCP lorsque le modèle NetScaler T1 est activé en ligne pour l'optimisation du protocole TCP ou lorsqu'il est désactivé à des fins de maintenance. Pour éviter d'interrompre les connexions existantes lors de l'introduction de vserver, la configuration suivante doit être appliquée avant de configurer ou d'activer vserver pour l'optimisation TCP :

Commande :

```
add ns acl acl-ingress ALLOW  - vlan 100
add forwardingSession fwd-ingress  - aclname acl-ingress
apply ns acls
<!--NeedCopy-->
```

Les sessions de transfert s'ajoutent au routage (statique, dynamique ou PBR) et créent des entrées de session pour le trafic routé (mode L3). Toute connexion existante est gérée par le transfert de session en raison des sessions correspondantes, et lors de l'introduction de vserver, il commence à capturer uniquement les nouvelles connexions TCP.

Les ACL peuvent être configurées pour capturer uniquement des ports spécifiques tels que vserver, afin d'éviter de créer des sessions pour du trafic inutile, qui consomme de la mémoire. Une autre option consiste à supprimer une configuration spécifique après l'activation du vserver.

Pour des raisons de maintenance, vserver doit être désactivé et son état doit apparaître comme HORS SERVICE. Dans ce cas, le serveur virtuel met immédiatement fin à toutes les connexions par défaut. Pour que vserver continue à servir les connexions existantes et n'en accepte pas de nouvelles, la configuration suivante doit être appliquée :

Commande :


```
set lb vserver vsrv-wireless  -downStateFlush DISABLED
<!--NeedCopy-->
```

Les nouvelles connexions passent par la table de routage et les entrées de session correspondantes sont créées en raison des sessions de transfert.

Profilage TCP basé sur des règles

La sélection du profil TCP basée sur des règles permet aux opérateurs de configurer le profil TCP de manière dynamique pour les clients provenant de différents domaines de trafic (3G ou 4G, par exemple). Certaines mesures de QoS sont différentes pour ces domaines de trafic et, afin d'obtenir de meilleures performances, vous devez modifier certains paramètres TCP de manière dynamique. Prenons le cas où des clients provenant de la 3G et de la 4G accèdent au même serveur virtuel et utilisent le même profil TCP, ce qui a un impact négatif sur les performances de certains clients. La fonctionnalité AppQoE permet de classer ces clients et de modifier dynamiquement le profil TCP sur vserver.

Exemple :

```
enable feature AppQoE

add ns tcpProfile nstcpprofile1 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    slowStartIncr 1 -bufferSize 4000000 -flavor BIC -KA ENABLED -
    sendBuffsize 4000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 1000000 -fack ENABLED -tcpmode
    ENDPOINT

add ns tcpProfile nstcpprofile2 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 15 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    slowStartIncr 1 -bufferSize 128000 -flavor BIC -KA ENABLED -
    sendBuffsize 6000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 64000 -fack ENABLED -tcpmode ENDPOINT

add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1

add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2

add appqoe policy appqoe_4G -rule "CLIENT.VLAN.ID.EQ(100)" -action
    action_1

add appqoe policy appqoe_3G -rule "CLIENT.VLAN.ID.EQ(200)" -action
    action_2
```



```
14
15 bind lb vserver vsrv-wireless -policyName appqoe_4G -priority 100
16
17 bind lb vserver vsrv-wireless -policyName appqoe_3G -priority 110
18 <!--NeedCopy-->
```

Le modèle NetScaler T1 est capable de recevoir les informations sur les abonnés de manière dynamique via l'interface Gx ou Radius ou Radius et Gx et d'appliquer un profil TCP différent pour chaque abonné.

Commande :

```
1 add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1
2
3 add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2
4
5 add appqoe policy appqoe_4G -rule "SUBSCRIBER.RULE_ACTIVE("3G")" -
     action action_1
6
7 add appqoe policy appqoe_3G -rule "SUBSCRIBER.RULE_ACTIVE("4G")" -
     action action_2
8 <!--NeedCopy-->
```

Pour l'intégration du modèle NetScaler T1 au réseau du plan de contrôle de l'opérateur, voir Gestion des abonnés des opérateurs de télécommunications.

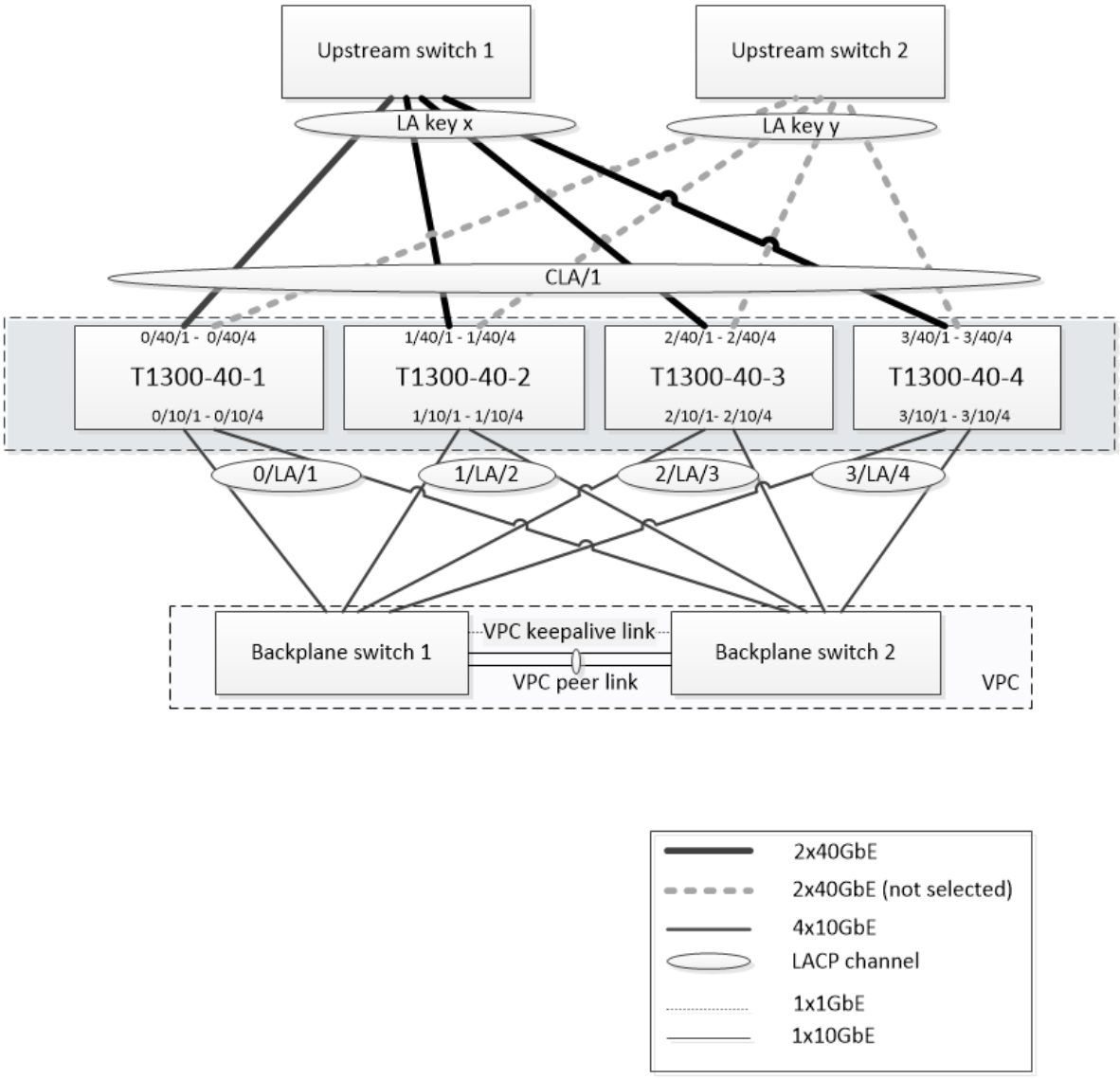
Scalabilité

May 5, 2023

L'optimisation TCP étant gourmande en ressources, une seule appliance NetScaler, même haut de gamme, peut ne pas être en mesure de supporter des débits Gi-LAN élevés. Pour étendre la capacité de votre réseau, vous pouvez déployer des appliances NetScaler dans une formation de clusters N+1. Dans un déploiement en cluster, les appliances NetScaler fonctionnent ensemble comme une seule image système. Le trafic client est réparti entre les nœuds du cluster à l'aide d'un commutateur externe.

Topologie

La figure 1 est un exemple de cluster composé de quatre nœuds T1300-40G.



La configuration illustrée à la Figure 1 possède les propriétés suivantes :

1. Tous les nœuds du cluster appartiennent au même réseau (également appelé cluster L2).
2. Le trafic du plan de données et du fond de panier est géré par différents commutateurs.
3. En supposant que le débit Gi-LAN est de 200 Gbit/s et qu'une appliance T1300-40G peut supporter un débit de 80 Gbit/s, nous avons besoin de trois appliances T1300-40G. Pour assurer la redondance en cas de défaillance d'un seul nœud de cluster, nous déployons quatre appliances au total.
4. Chaque nœud recevra jusqu'à 67 Gbit/s de trafic (50 Gbit/s dans des conditions de fonctionnement normales et 67 Gbit/s en cas de défaillance d'un nœud de cluster). Il a donc besoin de connexions de 2 x 40 Gbit/s au commutateur en amont. Pour assurer la redondance en cas de panne d'un commutateur, nous déployons deux commutateurs en amont et doublons le nombre de connexions.

5. L'agrégation de liens de cluster (CLAG) est utilisée pour répartir le trafic entre les nœuds du cluster. Un seul CLAG gère à la fois le trafic client et serveur. La redondance des liens est activée sur le CLAG, de sorte qu'un seul « sous-canal » est sélectionné à la fois et gère le trafic. Si une liaison échoue ou si le débit tombe en dessous du seuil spécifié, l'autre sous-canal est sélectionné.
6. Le commutateur en amont effectue un équilibrage de charge symétrique des canaux de port (par exemple, l'algorithme source-dest-ip uniquement de Cisco IOS 7.0 (8) N1 (1)) afin que les flux de trafic aller et retour soient gérés par le même nœud de cluster. Cette propriété est souhaitable car elle élimine la réorganisation des paquets, qui dégraderait les performances du protocole TCP.
7. 50 % du trafic de données devrait être dirigé vers le backplane, ce qui signifie que chaque nœud dirigera jusqu'à 34 Gbit/s vers d'autres nœuds du cluster (25 Gbit/s dans des conditions de fonctionnement normales et 34 Gbit/s en cas de défaillance d'un nœud de cluster). Ainsi, chaque nœud a besoin d'au moins 4 connexions 10G au commutateur de fond de panier. Pour assurer la redondance en cas de panne du commutateur, nous déployons deux commutateurs de fond de panier et doublons le nombre de connexions. La redondance des liens n'est actuellement pas prise en charge pour le backplane. C'est pourquoi il est préférable de disposer d'un VPC Cisco ou d'une technologie équivalente pour obtenir une redondance au niveau du commutateur.
8. La taille MTU des paquets dirigés est de 1 578 octets. Les commutateurs du backplane doivent donc prendre en charge un MTU supérieur à 1 500 octets.

Remarque : La conception illustrée à la figure 1 s'applique également aux appareils T1120 et T1310. Pour le T1310, nous utiliserions des interfaces 40 GbE pour les connexions du fond de panier, car il ne dispose pas de ports 10 GbE.

Remarque : Bien que ce document utilise Cisco VPC comme exemple, si vous travaillez avec des commutateurs autres que Cisco, d'autres solutions équivalentes peuvent être utilisées, telles que le MLAG de Juniper.

Remarque : Bien que d'autres topologies telles que ECMP au lieu de CLAG soient possibles, elles ne sont actuellement pas prises en charge pour ce cas d'utilisation particulier.

Configuration de l'optimisation TCP dans un cluster NetScaler T1000

Une fois l'installation physique, la connectivité physique, l'installation du logiciel et la gestion des licences terminées, vous pouvez procéder à la configuration réelle du cluster. Les configurations décrites ci-dessous s'appliquent au cluster représenté à la figure 1.

Remarque : Pour plus d'informations sur la configuration du cluster, consultez la section Configuration d'un cluster NetScaler.

Supposons que les quatre nœuds T1300 de la figure 1 ont les adresses NSIP suivantes :

Quatre nœuds T1300 avec adresse NSIP :


```
T1300-40-1: 10.102.29.60
T1300-40-2: 10.102.29.70
T1300-40-3: 10.102.29.80
T1300-40-4: 10.102.29.90
```

Le cluster sera géré via l'adresse IP du cluster (CLIP), qui est supposée être 10.78.16.61.

Configuration du cluster

Pour commencer à configurer le cluster illustré à la Figure 1, ouvrez une session sur le premier dispositif que vous souhaitez ajouter au cluster (par exemple, T1300-40-1) et procédez comme suit.

1. À l'invite de commandes, saisissez les commandes suivantes :

   Commande :

   ```
   > add cluster instance 1
   > add cluster node 0 10.102.29.60 -state ACTIVE
   > add ns ip 10.102.29.61 255.255.255.255 -type clip
   > enable cluster instance 1
   > save ns config
   > reboot  - warm
   ```

2. Après le redémarrage de l'appliance, connectez-vous à l'adresse IP du cluster (CLIP) et ajoutez le reste des nœuds au cluster :

   Commande :

   ```
   > add cluster node 1 10.102.29.70 -state ACTIVE
   > add cluster node 2 10.102.29.80 -state ACTIVE
   > add cluster node 3 10.102.29.90  - state ACTIVE
   > save ns config
   ```

3. Connectez-vous à l'adresse NSIP de chacun des nœuds nouvellement ajoutés et rejoignez le cluster :

   Commande :

   ```
   > join cluster -clip 10.102.29.61 -password nsroot
   > save ns config
   > reboot  - warm
   ```

4. Après le redémarrage des nœuds, procédez à la configuration du fond de panier. Sur l'adresse IP du cluster, entrez les commandes suivantes pour créer un canal LACP pour le lien du backplane de chaque nœud du cluster :

Commande :

```
> set interface 0/10/[1-8] -lacpkey 1 -lacpmode ACTIVE
> set interface 1/10/[1-8] -lacpkey 2 -lacpmode ACTIVE
> set interface 2/10/[1-8] -lacpkey 3 -lacpmode ACTIVE
> set interface 3/10/[1-8] -lacpkey 4 -lacpmode ACTIVE
```

5. De même, configurez LA et VPC dynamiques sur les commutateurs de fond de panier. Assurez-vous que la MTU des interfaces du commutateur de fond de panier est d'au moins 1 578 octets.
6. Vérifiez que les canaux sont opérationnels :

   Commande :

```
> show channel 0/LA/1
> show channel 1/LA/2
> show channel 2/LA/3
> show channel 3/LA/4
```

7. Configurez les interfaces de fond de panier du nœud de cluster.

   Commande :

```
> set cluster node 0 -backplane 0/LA/1
> set cluster node 1 -backplane 1/LA/2
> set cluster node 2 -backplane 2/LA/3
> set cluster node 3 -backplane 3/LA/4
```

8. Vérifiez l'état du cluster et vérifiez que le cluster est opérationnel :

```
> show cluster instance
> show cluster node
```

Pour plus d'informations sur la configuration du cluster, voir Configuration d'un cluster NetScaler

Répartition du trafic entre les nœuds de cluster

Après avoir créé le cluster NetScaler, déployez Cluster Link Aggrégation (CLAG) pour répartir le trafic entre les nœuds du cluster. Un seul lien CLAG gérera à la fois le trafic client et serveur.

Sur l'adresse IP du cluster, exécutez les commandes suivantes pour créer le groupe CLAG (Cluster Link Aggrégation) illustré à la Figure 1 :

Commande :

```
> set interface 0/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
```



```
3 > set interface 2/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
4 > set interface 3/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
```

Configurez l'agrégation de liens dynamiques sur les commutateurs externes.

Activez ensuite la redondance des liens comme suit :

Code :

```
1 > set channel CLA/1 -linkRedundancy ON -lrMinThroughput 240000
```

Enfin, vérifiez l'état de la chaîne en entrant :

Commande :

```
1 > show channel CLA/1
```

Le canal doit être UP et le débit réel devrait être 320000.

Pour plus d'informations sur l'agrégation de liens de clusters, consultez les rubriques suivantes :

- Agrégation de liens de cluster dynamique
- Lier la redondance dans un cluster avec LACP.

Parce que nous allons utiliser le transfert basé sur Mac (MBF), configurez un jeu de liens et le lier au groupe CLAG comme suit :

Commande :

```
1 > add linkset LS/1
2 > bind linkset LS/1 -ifnum CLA/1
```

Pour plus d'informations sur les jeux de liens, consultez les rubriques suivantes :

- Configuration des ensembles de liens
- Utilisation du canal Cluster LA avec des ensembles de liens

Configuration du VLAN et des adresses IP

Nous utiliserons la configuration IP par bandes, ce qui signifie que les adresses IP sont actives sur tous les nœuds (paramètre par défaut). Voir Configurations rayées, partiellement rayées et tachetées pour plus d'informations sur cette rubrique.

1. Ajouter les SNIP d'entrée et de sortie :

   Commande :


```
> add ns ip 172.16.30.254 255.255.255.0 -type SNIP
> add ns ip 172.16.31.254 255.255.255.0 -type SNIP
> add ns ip6 fd00:172:16:30::254/112 -type SNIP
> add ns ip6 fd00:172:16:31::254/112 -type SNIP
```

2. Ajoutez les VLAN d'entrée et de sortie correspondants :

   Commande :

```
> add vlan 30 -aliasName wireless
> add vlan 31 -aliasName internet
```

3. Liez des VLAN avec des adresses IP et un jeu de liens :

   Commande :

```
> bind vlan 31 -ifnum LS/1 -tagged
> bind vlan 30 -ifnum LS/1 -tagged
> bind vlan 30 -IPAddress 172.16.30.254 255.255.255.0
> bind vlan 31 -IPAddress 172.16.31.254 255.255.255.0
> bind vlan 30 -IPAddress fd00:172:16:30::254/112
> bind vlan 31 -IPAddress fd00:172:16:31::254/112
```

Plus de VLAN d'entrée et de sortie peuvent être ajoutés si nécessaire.

Configuration de l'optimisation TCP

À ce stade, nous avons appliqué toutes les commandes spécifiques au cluster. Pour terminer la configuration, suivez les étapes décrites dans Configuration de l'optimisation TCP.

Configuration du routage dynamique

Un cluster NetScaler peut être intégré à l'environnement de routage dynamique du réseau du client. Vous trouverez ci-dessous un exemple de configuration de routage dynamique utilisant le protocole de routage BGP (l'OSPF est également pris en charge).

1. À partir de l'adresse CLIP, activez le BGP et le routage dynamique sur les adresses IP d'entrée et de sortie :

   Commande :

```
> enable ns feature bgp
> set ns ip 172.16.30.254 -dynamicRouting ENABLED
> set ns ip 172.16.31.254 -dynamicRouting ENABLED
```


2. Ouvrez vtysh et configurez BGP pour le côté sortie :

   Code :

```
> shell
root@ns# vtysh
ns# configure terminal
ns(config)# router bgp 65531
ns(config-router)# network 10.0.0.0/24
ns(config-router)# neighbor 172.16.31.100 remote-as 65530
ns(config-router)# neighbor 172.16.31.100 update-source
    172.16.31.254
ns(config-router)# exit
ns(config)# ns route-install propagate
ns(config)# ns route-install default
ns(config)# ns route-install bgp
ns(config)# exit
```

3. Configurez l'homologue BGP côté sortie pour annoncer la route par défaut vers le cluster NetScaler. Par exemple :

   Commande :

```
router bgp 65530
 bgp router-id 172.16.31.100
 network 0.0.0.0/0
 neighbor 172.16.31.254 remote-as 65531
```

4. Suivez les étapes similaires pour configurer le côté entrée.

5. À partir de vtysh, vérifiez que la configuration est propagée à tous les nœuds du cluster en saisissant :

   Commande :

```
ns# show running-config
```

6. Enfin, connectez-vous à l'adresse NSIP de chaque nœud de cluster et vérifiez les routes annoncées par le pair BGP :

   Commande :

```
> show route | grep BGP
```


Optimisation des performances TCP à l'aide de TCP Nile

May 5, 2023

Le protocole TCP utilise les techniques d'optimisation et les stratégies (ou algorithmes) de contrôle de la congestion suivantes pour éviter la congestion du réseau lors de la transmission de données.

Stratégies de contrôle de la congestion

Le protocole TCP (Transmission Control Protocol) est utilisé depuis longtemps pour établir et gérer les connexions Internet, gérer les erreurs de transmission et connecter facilement les applications Web aux appareils clients. Mais le trafic réseau est devenu plus difficile à contrôler, car la perte de paquets ne dépend pas uniquement de la congestion du réseau, et la congestion n'entraîne pas nécessairement la perte de paquets. Par conséquent, pour mesurer la congestion, un algorithme TCP doit se concentrer à la fois sur la perte de paquets et sur la bande passante.

Algorithme NILE

Citrix Systems a développé un nouvel algorithme de contrôle de la congestion, NILE, un algorithme d'optimisation TCP conçu pour les réseaux haut débit tels que LTE, LTE advanced et 3G. Nile répond aux défis uniques liés à la décoloration, aux pertes aléatoires ou congestives, aux retransmissions par couche de liaison et à l'agrégation de supports.

L'algorithme NILE :

- Base les estimations de la latence des files d'attente sur des mesures du temps aller-retour.
- Utilise une fonction d'augmentation de la fenêtre de congestion qui est inversement proportionnelle à la latence de file d'attente mesurée. Cette méthode permet d'approcher le point de congestion du réseau plus lentement que ne le fait la méthode TCP standard et de réduire les pertes de paquets pendant la congestion.
- Peut faire la distinction entre les pertes aléatoires et les pertes liées à la congestion sur le réseau en utilisant la latence estimée de la file d'attente.

Les fournisseurs de services de télécommunications peuvent utiliser l'algorithme NILE dans leur infrastructure TCP pour :

- Optimisez les réseaux mobiles et longue distance : l'algorithme NILE permet d'obtenir un débit supérieur à celui du protocole TCP standard. Cette fonctionnalité est particulièrement importante pour les réseaux mobiles et longue distance.
- Réduisez la latence perçue par les applications et améliorez l'expérience des abonnés : l'algorithme Nile utilise les informations relatives aux pertes de paquets pour déterminer si la taille de la fenêtre de transmission doit être augmentée ou diminuée, et utilise les informations

relatives au délai de mise en file d'attente pour déterminer la taille de l'incrément ou de la décrémentation. Ce paramètre dynamique de la taille de la fenêtre de transmission réduit la latence des applications sur le réseau.

Pour configurer le support NILE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
set ns tcpProfile <name> [-flavor NILE]
<!--NeedCopy-->
```

Configuration du support NILE à l'aide de l'utilitaire de configuration

1. Accédez à **Système** > **Profils > ProfilsTCP et cliquez sur ProfilsTCP**.
2. Dans la liste déroulante **TCP Flavor**, sélectionnez **NILE**.

Exemple :

```
set ns tcpProfile tcpprofile1 -flavor NILE
<!--NeedCopy-->
```

Algorithme de récupération du débit proportionnel (PRR)

Les mécanismes de restauration rapide TCP réduisent la latence Web causée par les pertes de paquets. Le nouvel algorithme PRR (Proportional Rate Recovery) est un algorithme de restauration rapide qui évalue les données TCP lors d'une restauration après perte. Il est calqué sur la réduction de moitié du débit, en utilisant la fraction appropriée pour la fenêtre cible choisie par l'algorithme de contrôle de congestion. Cela minimise l'ajustement de la fenêtre et la taille réelle de la fenêtre à la fin de la restauration est proche du seuil de démarrage lent (ssthresh).

Ouverture rapide TCP (TFO)

Le protocole TCP Fast Open (TFO) est un mécanisme TCP qui permet un échange de données rapide et sécurisé entre un client et un serveur lors de l'établissement de connexion initial du protocole TCP. Cette fonctionnalité est disponible en tant qu'option TCP dans le profil TCP lié à un serveur virtuel d'une appliance NetScaler. TFO utilise un cookie TCP Fast Open (un cookie de sécurité) généré par l'appliance NetScaler pour valider et authentifier le client initiant une connexion TFO au serveur virtuel. En utilisant le mécanisme TFO, vous pouvez réduire la latence réseau d'une application du temps nécessaire pour un aller-retour complet, ce qui réduit considérablement le retard subi lors de courts transferts TCP.

Comment fonctionne TFO

Lorsqu'un client essaie d'établir une connexion TFO, il inclut un cookie TCP Fast Open avec le segment SYN initial pour s'authentifier. Si l'authentification est réussie, le serveur virtuel de l'appliance NetScaler peut inclure des données dans le segment SYN-ACK même s'il n'a pas reçu le dernier segment ACK de l'établissement de liaison tripartite. Cela permet d'économiser jusqu'à un aller-retour complet par rapport à une connexion TCP normale, qui nécessite une liaison à trois voies avant de pouvoir échanger des données.

Un client et un serveur principal effectuent les étapes suivantes pour établir une connexion TFO et échanger des données en toute sécurité lors de l'établissement de connexion TCP initial.

1. Si le client ne dispose pas d'un cookie d'ouverture rapide TCP pour s'authentifier, il envoie une demande de cookie d'ouverture rapide dans le paquet SYN au serveur virtuel de l'appliance NetScaler.
2. Si l'option TFO est activée dans le profil TCP lié au serveur virtuel, l'appliance génère un cookie (en chiffrant l'adresse IP du client sous une clé secrète) et répond au client par un SYN-ACK qui inclut le cookie d'ouverture rapide généré dans un champ d'option TCP.
3. Le client met en cache le cookie pour les futures connexions TFO au même serveur virtuel sur l'appliance.
4. Lorsque le client essaie d'établir une connexion TFO avec le même serveur virtuel, il envoie un SYN qui inclut le cookie Fast Open mis en cache (en tant qu'option TCP) ainsi que des données HTTP.
5. L'appliance NetScaler valide le cookie et, si l'authentification est réussie, le serveur accepte les données du paquet SYN et accuse réception de l'événement à l'aide d'un SYN-ACK, d'un cookie TFO et d'une réponse HTTP.

Remarque : Si l'authentification du client échoue, le serveur supprime les données et accuse réception de l'événement uniquement avec un SYN indiquant un délai d'expiration de session.

1. Côté serveur, si l'option TFO est activée dans un profil TCP lié à un service, l'appliance NetScaler détermine si le cookie d'ouverture rapide TCP est présent dans le service auquel elle tente de se connecter.
2. Si le cookie TCP Fast Open n'est pas présent, l'appliance envoie une demande de cookie dans le paquet SYN.
3. Lorsque le serveur principal envoie le cookie, l'appliance stocke le cookie dans le cache d'informations du serveur.
4. Si l'appliance possède déjà un cookie pour la paire d'adresses IP de destination donnée, elle remplace l'ancien cookie par le nouveau.
5. Si le cookie est disponible dans le cache d'informations du serveur lorsque le serveur virtuel tente de se reconnecter au même serveur principal en utilisant la même adresse SNIP, l'appliance combine les données du paquet SYN avec le cookie et les envoie au serveur principal.

6. Le serveur principal accuse réception de l'événement à l'aide de données et d'un SYN.

Remarque : Si le serveur accuse réception de l'événement avec uniquement un segment SYN, l'appliance NetScaler renvoie immédiatement le paquet de données après avoir supprimé le segment SYN et les options TCP du paquet d'origine.

Configuration de TCP Fast Open

Pour utiliser la fonctionnalité TCP Fast Open (TFO), activez l'option TCP Fast Open dans le profil TCP concerné et définissez le paramètre TFO Cookie Timeout sur une valeur qui répond aux exigences de sécurité de ce profil.

Pour activer ou désactiver TFO à l'aide de la ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver TFO dans un profil nouveau ou existant.

Remarque : La valeur par défaut est DISABLED.

```
add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
unset tcpprofile <TCP Profile Name> - tcpFastOpen
<!--NeedCopy-->
```

Exemples :

ajouter le profil TCP1 — TCPFastOpen
Définir le profil TCP1 — TCPFastOpen activé Désactiver le profil TCP1 — TCPFastOpen

Pour définir la valeur du délai d'expiration du cookie TCP Fast Open à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set tcpparam - tcpfastOpenCookieTimeout <Timeout Value>
<!--NeedCopy-->
```

Exemple :

```
set tcpprofile - tcpfastOpenCookieTimeout 30secs
<!--NeedCopy-->
```


Pour configurer le TCP Fast Open à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils** > puis cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, cochez la case **TCP Fast Open** .
3. Cliquez sur **OK**, puis sur **Terminé**.

Pour configurer la valeur du délai d'expiration du cookie rapide TCP à l'aide de l'interface graphique

Accédez à **Configuration** > **Système** > **Paramètres > Modifier les paramètresTCP, puis à la page Configurer les paramètresTCP** pour définir la valeur du délai d'expiration du cookie d'ouverture rapide TCP.

Hystart TCP

Un nouveau paramètre de profil TCP, hystart, active l'algorithme Hystart, qui est un algorithme de démarrage lent qui détermine dynamiquement un point sûr auquel se terminer (ssthresh). Il permet une transition vers la prévention de la congestion sans pertes importantes de paquets. Ce nouveau paramètre est désactivé par défaut.

Si une congestion est détectée, Hystart entre dans une phase d'évitement de la congestion. Son activation vous permet d'obtenir un meilleur débit sur les réseaux à haut débit présentant de fortes pertes de paquets. Cet algorithme permet de maintenir une bande passante proche de la limite maximale lors du traitement des transactions. Il peut donc améliorer le débit.

Configuration de TCP Hystart

Pour utiliser la fonctionnalité Hystart, activez l'option Cubic Hystart dans le profil TCP approprié.

Pour configurer Hystart à l'aide de l'interface de ligne de commande (CLI)

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver Hystart dans un profil TCP nouveau ou existant.

```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
unset tcprofile <profileName> -hystart
<!--NeedCopy-->
```

Exemples :


```
add tcpprofile Profile1 - tcpFastOpen
Set tcpprofile Profile1 - tcpFastOpen Enabled
unset tcpprofile Profile1 - tcpFastOpen
<!--NeedCopy-->
```

Pour configurer le support Hystart à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils** > et cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, cochez la case **Cubic Hystart** .
3. Cliquez sur **OK**, puis sur **Terminé**.

Techniques d'optimisation

TCP utilise les techniques et méthodes d'optimisation suivantes pour optimiser les contrôles de flux.

Sélection du profil TCP basée sur des politiques

Le trafic réseau d'aujourd'hui est plus diversifié et plus gourmand en bande passante que jamais. Avec l'augmentation du trafic, l'effet de la qualité de service (QoS) sur les performances du protocole TCP est significatif. Pour améliorer la QoS, vous pouvez désormais configurer des politiques AppQoE avec différents profils TCP pour différentes classes de trafic réseau. La politique AppQoE classe le trafic d'un serveur virtuel afin d'associer un profil TCP optimisé pour un type de trafic particulier, tel que la 3G, la 4G, le LAN ou le WAN.

Pour utiliser cette fonctionnalité, créez une action de stratégie pour chaque profil TCP, associez une action aux stratégies AppQoE et associez les stratégies aux serveurs virtuels d'équilibrage de charge.

Configuration de la sélection du profil TCP basée sur des politiques

La configuration de la sélection du profil TCP basée sur des politiques comprend les tâches suivantes :

- Activation d'AppQoE. Avant de configurer la fonctionnalité de profil TCP, vous devez activer la fonctionnalité AppQoE.
- Ajout d'une action AppQoE. Après avoir activé la fonctionnalité AppQoE, configurez une action AppQoE avec un profil TCP.
- Configuration de la sélection du profil TCP basée sur AppQoE. Pour implémenter la sélection du profil TCP pour différentes classes de trafic, vous devez configurer des politiques AppQoE grâce auxquelles votre appliance NetScaler peut distinguer les connexions et lier l'action AppQoE correcte à chaque politique.

- Liaison de la politique AppQoE au serveur virtuel. Une fois que vous avez configuré les politiques AppQoE, vous devez les lier à un ou plusieurs serveurs virtuels d'équilibrage de charge, de commutation de contenu ou de redirection de cache.

Configuration à l'aide de l'interface de ligne de commande

Pour activer AppQoE à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour activer la fonctionnalité et vérifier qu'elle est activée :

```
enable ns feature appqoe

show ns feature
<!--NeedCopy-->
```

Pour lier un profil TCP lors de la création d'une action AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande d'action AppQoE suivante avec l'option tcpprofiletobind.

Lier un profil TCP :

```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS |
    NS ) [<CustomFile>] [-altContentSvcName <string>] [-altContentPath <
    string>] [-maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth
     <positive_integer>] [-priqDepth <positive_integer>] [-
    dosTrigExpression <expression>] [-dosAction ( SimpleResponse |
    HICResponse )] [-tcpprofiletobind <string>]

show appqoe action
<!--NeedCopy-->
```

Pour configurer une politique AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add appqoe policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```


Pour lier une politique AppQoE à des serveurs virtuels d'équilibrage de charge, de redirection de cache ou de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <
    priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <
    priority>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <
    priority>
<!--NeedCopy-->
```

Exemple :

```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
    ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500 -
    slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
    sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack ENABLED
    -tcpmode ENDPOINT

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
    action appact1

bind lb vserver lb2 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST

bind cs vserver cs1 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Configuration du profilage TCP basé sur des règles à l'aide de l'interface graphique

Pour activer AppQoE à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet de détails, cliquez sur **Configurer les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, cochez la case **AppQoE** .
4. Cliquez sur **OK**.

Pour configurer la politique AppQoE à l'aide de l'interface graphique

1. **Accédez à**App-Expert**>**AppQoE > Actions**.**
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
3. Pour créer une nouvelle action, cliquez sur **Ajouter**.
4. Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Modifier**.
5. Dans l'écran **Créer une action AppQoE** ou **Configurer une action AppQoE**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres de configuration de l'action AppQoE » comme suit (un astérisque indique un paramètre obligatoire) :
    a) Nom—nom
    b) Type d'action : répondre par
    c) Priorité : priorité
    d) Profondeur de la file d'attente des politiques : PolqDepth
    e) Profondeur de la file d'attente : PriqDepth
    f) Action DOS : action DOS
6. Cliquez sur **Create**.

Pour lier la politique AppQoE à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez un serveur, puis cliquez sur **Modifier**.
2. Dans la section **Politiques**, cliquez sur (+) pour lier une politique AppQoE.
3. Dans le curseur **Politiques**, procédez comme suit :
    a) Sélectionnez un type de politique comme AppQoE dans la liste déroulante.
    b) Sélectionnez un type de trafic dans la liste déroulante.
4. Dans la section **Politiques contraignantes**, procédez comme suit :
    a) Cliquez sur **Nouveau** pour créer une nouvelle politique AppQoE.
    b) Cliquez sur **Stratégie existante pour sélectionner une politique** AppQoE dans la liste déroulante.
5. Définissez la priorité de liaison et cliquez sur **Lier** la politique au serveur virtuel.
6. Cliquez sur **Terminé**.

Génération de blocs SACK

Les performances du protocole TCP ralentissent lorsque plusieurs paquets sont perdus dans une fenêtre de données. Dans un tel scénario, un mécanisme d'accusé de réception sélectif (SACK)

combiné à une politique de retransmission sélective permet de surmonter cette limitation. Pour chaque paquet entrant hors service, vous devez générer un bloc SACK.

Si le paquet hors ordre entre dans le bloc de la file d'attente de réassemblage, insérez les informations du paquet dans le bloc et définissez les informations du bloc complètes sur SACK-0. Si un paquet en panne ne rentre pas dans le bloc de réassemblage, envoyez le paquet au format SACK-0 et répétez les blocs SACK précédents. Si un paquet hors ordre est un doublon et que les informations du paquet sont définies comme SACK-0, alors D-SACK le bloc.

Remarque : Un paquet est considéré comme D-SACK s'il s'agit d'un paquet accusé de réception ou d'un paquet hors service déjà reçu.

Le client renie

Une appliance NetScaler peut gérer les renégats du client lors d'une restauration basée sur SACK.

Les vérifications de la mémoire pour le marquage du point de terminaison sur un circuit imprimé ne tiennent pas compte de la quantité totale de mémoire disponible

Dans une appliance NetScaler, si le seuil d'utilisation de la mémoire est défini sur 75 % au lieu d'utiliser la mémoire totale disponible, les nouvelles connexions TCP contournent l'optimisation TCP.

Retransmissions inutiles en raison de l'absence de blocs SACK

En mode hors point de terminaison, lorsque vous envoyez des DUPACKS, si des blocs SACK sont absents pour quelques paquets hors service, cela déclenche des retransmissions supplémentaires depuis le serveur.

Le protocole SNMP pour le nombre de connexions a contourné l'optimisation en raison d'une surcharge

Les identifiants SNMP suivants ont été ajoutés à une appliance NetScaler pour suivre le nombre de connexions contournées par l'optimisation TCP en raison d'une surcharge.

1. 1.3.6.1.4.1.5951.4.1.1.46.13 (optimisation TCP activée). Pour suivre le nombre total de connexions activées grâce à l'optimisation TCP.
2. 1.3.6.1.4.1.5951.4.1.1.46.132 (optimisation TCP contournée). Pour suivre le nombre total de connexions contournées, optimisez TCP.

Buffer de réception dynamique

Pour optimiser les performances TCP, une appliance NetScaler peut désormais ajuster dynamiquement la taille de la mémoire tampon de réception TCP.

Directives de dépannage

May 5, 2023

Support technique

Toutes les requêtes de dépannage et d'escalade nécessitent un bundle de support technique NetScaler récent, qui capture la configuration actuelle, la version du microprogramme installée, les fichiers journaux, les cœurs exceptionnels, etc.

Exemple :

```
show techsupport

showtechsupport data collector tool - $Revision: #5 $!
...
<!--NeedCopy-->
```

Toutes les données seront collectées sous

```
...
Archiving all the data into "/var/tmp/support/collector_P_192
   .168.121.117_18Jun2015_09_53.tar.gz" ....
Created a symbolic link for the archive with /var/tmp/support/support.
   tgz
/var/tmp/support/support.tgz  ---- points to ---> /var/tmp/support/
   collector_P_192.168.121.117_18Jun2015_09_53.tar.gz
<!--NeedCopy-->
```

Une fois qu'un bundle de support technique a été généré, il peut être copié à l'aide de SCP.

Traces

Les problèmes d'optimisation TCP de NetScaler nécessitent normalement des traces NetScaler pour être résolus correctement. Notez qu'il faut essayer de capturer des traces dans des conditions similaires, c'est-à-dire sur la même cellule, au même moment de la journée, en utilisant le même équipement utilisateur et la même application, entre autres.

Les commandes start nstrace et stop nstrace peuvent être utilisées pour capturer des traces :

- Il est fortement recommandé d'utiliser le filtre approprié pour éviter de capturer des paquets superflus et inutiles sur la trace. Par exemple, utilisez start nstrace -filter 'IP == 10.20.30.40' pour capturer uniquement les paquets envoyés ou reçus depuis l'adresse IP 10.20.30.40, qui est l'adresse IP de l'équipement utilisateur.
- N'utilisez pas l'option -tcpdump, car elle supprime les en-têtes nstrace nécessaires au débogage.

Analyse des traces

Une fois qu'une trace NetScaler a été capturée, elle peut être visualisée avec Wireshark 1.12 ou version ultérieure. Vérifiez que les traces capturées incluent les en-têtes NetScaler Packet Trace appropriés, comme indiqué dans la capture d'écran ci-dessous :

Les en-têtes de débogage supplémentaires sont également visibles selon l'illustration ci-dessous :

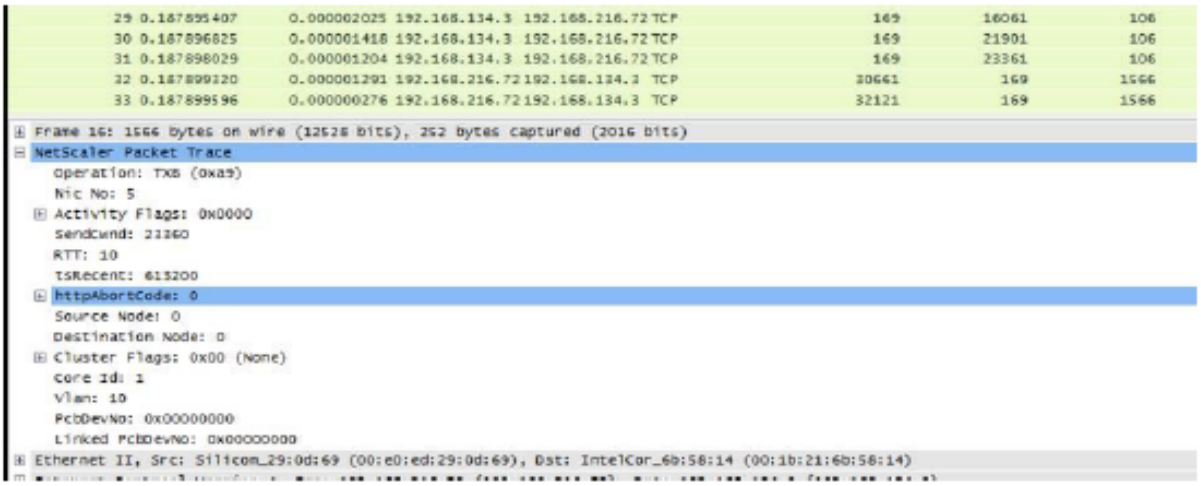


Tableau de connexion

Lorsque le problème est lié à l'optimisation TCP et qu'il peut être reproduit ou qu'il est en cours, il est préférable d'obtenir également la table de connexion lorsque le problème survient à partir du nœud T1 principal.

Pour obtenir le tableau, vous devez passer au shell BSD et exécuter la commande suivante :

```
shell
...

nscli -U 127.0.0.1:nsroot:nsroot show connectiontable -detail full link
    > /var/tmp/contable.log
<!--NeedCopy-->
```

> **Remarque**
>
> La commande peut être exécutée plus longtemps et l'UC de gestion peut être stressée à ce moment-là (dépend du nombre d'entrées de table de connexion), mais elle n'affecte pas le service.

Questions fréquemment posées

May 5, 2023

Délais d' expiration

> **Important**
>
> Avant *d'utiliser un bouton nsapimgr*, consultez le support client Citrix.

Vous trouverez ci-dessous une liste des différents délais d'inactivité de connexion qui peuvent être définis sur les serveurs et services virtuels NetScaler T1. Les délais d'inactivité définis pour les connexions client ou serveur au niveau du serveur virtuel ou du service ne s'appliquent qu'aux connexions dans l'état TCP ESTABLISHED et qui sont inactives.

- Le paramètre CLTTimeout du serveur virtuel d'équilibrage de charge spécifie la durée en secondes pendant laquelle une connexion entre un client et un serveur virtuel d'équilibrage de charge doit être inactive avant que l'appliance ne ferme la connexion.
- Le paramètre Service SvrTimeout spécifie la durée en secondes pendant laquelle une connexion entre l'appliance et un service ou un serveur doit être inactive avant que l'appliance ne ferme la connexion.
- Le paramètre Service CLTTimeout spécifie la durée en secondes pendant laquelle une connexion entre un client et un service doit être inactive avant que l'appliance ne ferme la connexion.

Lorsqu'un service est lié à un serveur virtuel d'équilibrage de charge, le CLTTimeout du serveur virtuel d'équilibrage de charge est prioritaire et le service CLTTimeout pour le service est ignoré.

Dans le cas où aucun service n'est lié au serveur virtuel d'équilibrage de charge, le délai d'inactivité

global, à savoir TCPServer, est utilisé pour les connexions côté serveur. Il peut être configuré comme suit :

Commande :

```
set ns timeout -tcpServer 9000
<!--NeedCopy-->
```

Les connexions dans un autre état ont des valeurs de délai d'expiration différentes :

- Délai d'inactivité des connexions semi-ouvertes : 120 secondes (valeur codée en dur)
- Délai d'inactivité des connexions TIME_WAIT : 40 secondes (valeur codée en dur)
- Délai d'inactivité des connexions à moitié fermées. Par défaut, il est de 10 s et peut être configuré entre 1 s et 600 à l'aide de l'extrait de code

Commande :

```
 set ns timeout -halfclose 10
<!--NeedCopy-->
```

Lorsque le délai de demi-fermeture est déclenché, la connexion passe à l'état zombie. Lorsque le délai d'expiration pour les zombies expire, le nettoyage des zombies démarre et T1 envoie par défaut du RST côté client et côté serveur pour une connexion donnée.

- Délai d'expiration pour les zombies : intervalle pendant lequel le processus de nettoyage des zombies doit s'exécuter pour nettoyer les connexions TCP inactives. La valeur du délai d'expiration par défaut est de 120 s et peut être configurée entre 1 s et 600 s.

Commande :

```
set ns timeout -zombie 120
<!--NeedCopy-->
```

Tableau des tailles de segment maximales

Une appliance NetScaler T1 se défend contre les attaques SYN flood en utilisant des cookies SYN au lieu de maintenir des connexions semi-ouvertes sur la pile de mémoire système. L'appliance envoie un cookie à chaque client qui demande une connexion TCP, mais elle ne conserve pas l'état des connexions semi-ouvertes. Au lieu de cela, l'appliance alloue de la mémoire système à une connexion uniquement lors de la réception du dernier paquet ACK ou, pour le trafic HTTP, lors de la réception d'une demande HTTP. Cela empêche les attaques SYN et permet aux communications TCP normales avec des clients légitimes de se poursuivre sans interruption. Une fonction spécifique est activée par défaut sans option de désactivation.

Toutefois, il existe une mise en garde car les cookies SYN standard limitent les connexions à l'utilisation de huit valeurs de taille maximale de segment (MSS) uniquement. Si le MMS de connexion ne correspond à aucune valeur prédéfinie, il récupérera la prochaine valeur inférieure disponible à la fois côté client et côté serveur.

Les valeurs de taille maximale de segment (MSS) TCP prédéfinies sont les suivantes et peuvent être configurées via un nouveau bouton nsapimgr.

1460	1440	1330	1220	956	536	384	128

Le nouveau tableau MSS :

- Il n'est pas nécessaire de contenir le support Jumbo-Frame. Même si, par défaut, 8 valeurs sont réservées dans le tableau MSS pour les trames Jumbo, les paramètres du tableau peuvent être modifiés pour inclure uniquement les trames de taille Ethernet standard.
- Doit avoir 16 valeurs
- Les valeurs doivent être classées par ordre décroissant
- Devrait inclure 128 comme dernière valeur

Si la nouvelle table MSS est valide, elle est stockée et les anciennes valeurs sont supprimées au moment de la rotation du cookie SYN-cookie. Dans le cas contraire, la nouvelle table renvoie une erreur. Les modifications sont appliquées aux nouvelles connexions tandis que les connexions existantes conservent l'ancienne table MSS jusqu'à ce qu'elles expirent ou soient interrompues.

Pour afficher la table MSS actuelle dans une appliance NetScaler, tapez la commande suivante.

Commande :

```
>shell

#nsapimgr -d mss_table
```

Exemple :

```
#nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1440,1330,1212,956,536,384,128
      }


```



```
Done.
```

Pour modifier la table mss, tapez la commande suivante :

Commande :

```
>shell

#nsapimgr -s mss_table=<16 comma seperated values>
```

Exemple :

```
#nsapimgr -ys mss_table
   =9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128


# nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128
     }


Done.
```

Un exemple d'utilisation de valeurs standard Ethernet est illustré ci-dessous :

Exemple :

```
#nsapimgr -ys mss_table
   =1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128


# nsapimgr -d mss_table

MSS table

{
 1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128
     }


Done.
```


Pour que cette modification soit permanente même après le redémarrage de l'appliance NetScaler, incluez la commande `##nsapimgr -ys mss_table=<16 comma seperated values>` dans le fichier « /nsconfig/rc.netscaler ». Si le fichier « rc.netscaler » n'existe pas, créez-le dans le dossier « /nsconfig », puis ajoutez la commande.

Protection contre les surcharges de mémoire

Un moteur de traitement des paquets (PPE) NetScaler commence à contourner les connexions issues de l'optimisation TCP si la mémoire utilisée par ce PPE est supérieure à une valeur de filigrane élevée spécifiée. Si l'utilisation de la mémoire d'un PPE dépasse environ 2,6 Go, il commence à contourner *toute nouvelle* connexion due à l'optimisation. Les connexions existantes (celles précédemment admises pour l'optimisation) continuent d'être optimisées. Cette valeur de filigrane a été sélectionnée à dessein et son réglage n'est pas recommandé.

> **Remarque**
>
> Si vous pensez qu'il existe une bonne raison de modifier la valeur de ce filigrane, contactez le support client.

Assistance pour les clients de Happy Eyeballs

Si l'appliance NetScaler reçoit un SYN pour une destination dont l'état est inconnu, elle vérifie d'abord l'accessibilité du serveur, puis accuse réception du client. Ce mécanisme de sondage permet aux clients disposant de deux piles IP de découvrir l'accessibilité des serveurs Internet à double pile. Si le client découvre que les accès IPv6 et IPv4 sont disponibles, il établit une connexion avec le serveur qui répond plus rapidement et réinitialise l'autre. Lorsque la connexion à l'appliance NetScaler est réinitialisée, elle réinitialisera la connexion côté serveur correspondante.

Remarque : Cette fonctionnalité ne comporte aucun paramètre TCP configurable par l'utilisateur pouvant être désactivé/activé sur l'appliance NetScaler.

Pour plus d'informations sur le support de Happy Eyeballs, consultez la RFC 6555.

Optimisation vidéo NetScaler

June 20, 2023

> **Avertissement :**
>
> L'optimisation vidéo n'est prise en charge que pour une solution de télécommunication par proxy direct. N'activez l'optimisation vidéo pour aucun autre type d'utilisation. L'optimisation vidéo

> n'est pas prise en charge sur les topologies de partition d'administration et de cluster.

L'appliance NetScaler fournit des techniques et des fonctionnalités d'optimisation pour optimiser le trafic vidéo ABR pour le trafic vidéo sur les réseaux mobiles. Cela améliore l'expérience utilisateur et réduit la consommation globale de bande passante du réseau.

La section inclut les rubriques suivantes :

- Mise en route
- Gestion des licences
- Configuration de l'optimisation vidéo sur TCP
- Configuration de l'optimisation vidéo via UDP

Mise en route

May 5, 2023

Les fichiers multimédia génèrent un trafic croissant sur les réseaux mobiles, et la migration vers des technologies réseau plus rapides a considérablement augmenté le volume du trafic vidéo crypté. La technologie de diffusion multimédia traditionnelle (téléchargement progressif) ne parvient pas à fournir une qualité d'expérience (QoE) acceptable à un débit de transmission élevé. Cela a conduit à l'introduction du protocole ABR (Adaptive Bit Rate). Il peut adapter le débit de diffusion à la bande passante réseau disponible et restreindre la qualité du streaming en fonction de la capacité du téléphone recevant la vidéo. Cependant, le protocole ABR ne fonctionne pas aussi bien sur les réseaux mobiles que sur Internet. Les opérateurs mobiles doivent donc optimiser le trafic ABR.

Une appliance NetScaler possède des fonctionnalités uniques pour détecter le trafic vidéo entrant et optimiser de manière sélective les vidéos ABR.

Comment fonctionne l'optimisation vidéo de NetScaler

Une appliance NetScaler peut identifier et optimiser le trafic ABR crypté (y compris le trafic vidéo Facebook) via TCP, et le trafic ABR YouTube via QUIC. L'appliance possède les fonctionnalités suivantes :

1. Détectez les vidéos à téléchargement progressif (PDF) via HTTP.
2. Détectez et optimisez les vidéos ABR via HTTP.
3. Détectez et optimisez les vidéos ABR via HTTPS.
4. Détectez et optimisez les vidéos YouTube ABR via QUIC.

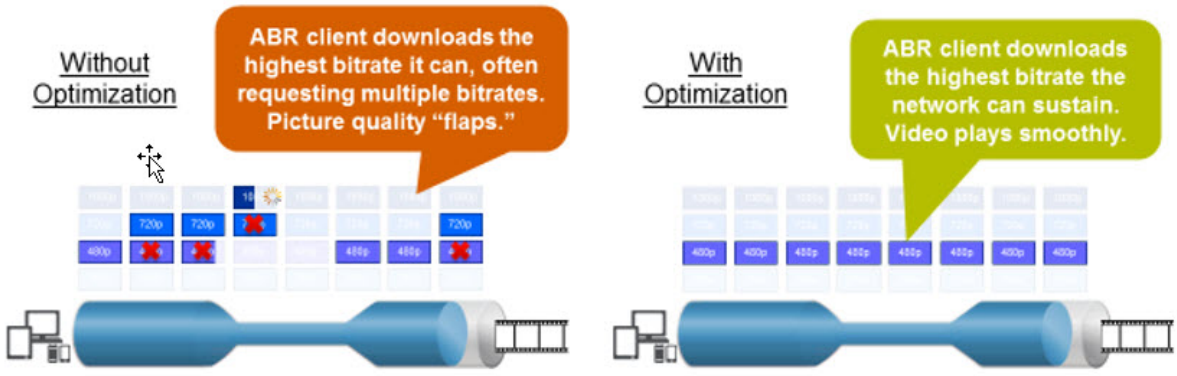
L'appliance utilise également les domaines de support suivants pour détecter le trafic vidéo via les protocoles TCP et QUIC.

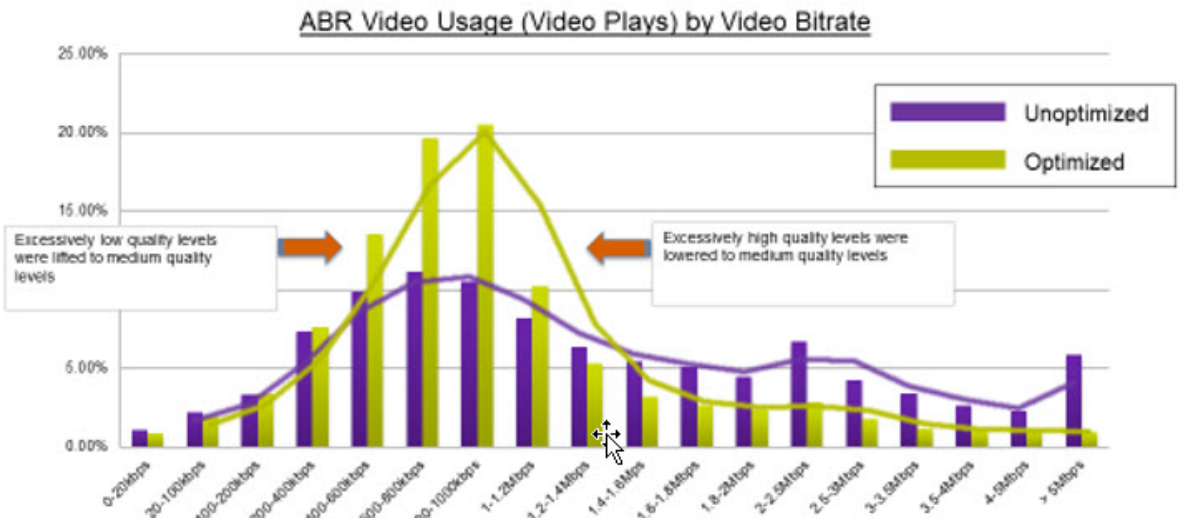
- Vidéos ABR non cryptées via TCP. L'appliance détecte tous les sites Web de streaming vidéo conformes aux normes. L'appliance détecte les sessions ABR en inspectant l'en-tête de la charge utile de la vidéo de réponse, l'URL et les en-têtes HTTP.
- Vidéo ABR cryptée via TCP. L'appliance détecte les sessions ABR à l'aide d'un algorithme générique et heuristique basé sur le domaine, l'en-tête SSL et les modèles de trafic. Grâce à cela, l'appliance dispose d'un support intégré lui permettant de détecter les principaux sites Web de vidéos, avec une précision de 95 %, et nous continuons à ajouter la prise en charge de nouveaux types de vidéos. NetScaler dispose également d'un programme qui fournit une vérification supplémentaire pour les principaux sites ABR chiffrés d'une région ou d'un pays afin de garantir la couverture réseau.
- Vidéos ABR cryptées via QUIC. L'appliance détecte les sessions ABR pour un fournisseur de vidéos basé sur QUIC, tel que YouTube. L'algorithme de détection repose sur une heuristique exploitant les en-têtes et le domaine QUIC. NetScaler continuera de prendre en charge les nouveaux sites vidéo utilisant QUIC.

Avantages

L'optimisation du trafic vidéo ABR peut apporter les avantages suivants :

- Gérez le réseau en cas de congestion aux heures de pointe.
- Améliorez la cohérence de la lecture vidéo et réduisez le blocage vidéo.
- Activez de nouvelles offres de services vidéo (par exemple, des services vidéo en rafale).
- Permettez aux clients de sélectionner la meilleure qualité vidéo durable.
- Offrez une expérience utilisateur cohérente à l'abonné.





Optimisation vidéo via TCP

L'optimisation du trafic ABR via TCP par NetScaler fonctionne comme suit :

1. Le trafic HTTP ou HTTPS que l'appliance reçoit via TCP est envoyé au serveur virtuel d'équilibrage de charge correspondant.
2. Les politiques de détection intégrées liées au serveur virtuel associées à d'autres algorithmes de détection propriétaires évaluent le trafic.
3. Les politiques utilisent un ensemble de signatures de détection vidéo intégrées pour détecter le type de vidéo. La politique qui correspond au trafic applique une action qui classe le type de vidéo dans l'une des catégories suivantes :
   a) PDF en texte clair
   b) ABR en texte clair
   c) ABR crypté
   d) Autre
4. Les politiques d'optimisation liées au même serveur virtuel évaluent le trafic et déterminent le débit d'optimisation à appliquer au trafic.
5. Le débit d'optimisation est appliqué si le trafic est soit un ABR en texte clair, soit un ABR crypté.

Un fournisseur de services mobiles peut améliorer la qualité de l'expérience (QoE) en définissant la vitesse de téléchargement pour le trafic mobile 2G, 3G et 4G. Cela réduit les heures de démarrage des vidéos ou la mise en mémoire tampon des événements. L'optimisation peut également réduire la quantité de bande passante réseau consommée par les sessions vidéo.

Les techniques d'optimisation incluent le contrôle dynamique des rafales et l'échantillonnage aléatoire.

Contrôle dynamique des rafales

L'optimisation ABR de NetScaler s'adapte de manière dynamique à l'évolution des conditions du réseau. Il permet une fréquence de rafale initiale de 1,3 fois la fréquence de stimulation configurée pendant 15 secondes. Le débit de rafale initial s'applique au début de chaque session vidéo ABR optimisée, même lorsque plusieurs sessions utilisent la même connexion TCP ou le même groupe de connexions TCP.

L'appliance prend également en charge les rafales de restauration au cas où le débit binaire pris en charge par le réseau tombe en dessous du débit configuré. Par exemple, si le débit effectif chute à la 7e seconde et se rétablit à la 15e seconde après la rafale initiale, l'appliance récupère la perte lors du cycle de rafale suivant. Ce faisant, l'appliance optimise dynamiquement la bande passante réseau pour tous les abonnés afin que la qualité de la vidéo reste constante par pixel.

Remarque : Lorsqu'une rafale de restauration se produit pendant une rafale initiale, le débit de stimulation ne doit pas dépasser les débits maximaux de rafale de restauration et de rafale initiale (vous ne devez pas ajouter le facteur de rafale de restauration en plus du facteur de rafale initiale). Sinon, cela risque d'être si rapide que le lecteur multimédia passe à un mode de qualité supérieure. Toutefois, si nécessaire, vous pouvez prolonger la durée de la rafale initiale pour compenser la bande passante inutilisée.

Échantillonnage aléatoire

Pour estimer les économies résultant de l'optimisation vidéo, l'appliance NetScaler met en œuvre un échantillonnage aléatoire. Avec cette technique, l'appliance sélectionne de manière aléatoire un pourcentage configurable du trafic vidéo détecté (le paramètre d'échantillonnage aléatoire est un nombre entier compris entre 0 et 100, donc moins de 1 % n'est pas possible). Ces transactions (et sessions) sélectionnées aléatoirement et non optimisées deviennent un groupe de référence et sont identifiées dans les journaux de transactions (avec d'autres caractéristiques, telles que la taille des octets et les champs de temporisation). Les caractéristiques des sessions optimisées sont également enregistrées, et le moteur de génération de rapports compare les statistiques des groupes optimisés et de référence afin d'estimer les économies résultant de l'optimisation (y compris les économies résultant de l'optimisation ABR).

Optimisation vidéo sur UDP

Google a introduit un nouveau protocole de transport appelé QUIC. Le protocole QUIC de Google est très similaire à TCP+TLS+HTTP/2 et est implémenté au-dessus du protocole UDP. NetScaler peut détecter les vidéos YouTube ABR diffusées via le protocole QUIC et appliquer l'optimisation vidéo ABR de la même manière que l'ABR via TCP.

Gestion des licences

May 5, 2023

La fonctionnalité d'optimisation vidéo fonctionne sur les plateformes de télécommunications avec l'achat d'une licence CBM de base et d'une licence CBM Premium et pour les autres plateformes NetScaler, la fonctionnalité fonctionne avec l'achat d'une licence CNS Premium. Avant de configurer la fonctionnalité d'optimisation vidéo, votre appliance doit disposer d'une licence appropriée.

Support en matière de licences pour les plateformes de télécommunications :

- **CBM_TXXX_Server_Retail.lic**
- **CBM_TPRE_Server_Retail.lic**
- **CNS_WEBF_SSERVER_Retail.lic**

Où XXX est le débit, par exemple NetScaler T1000.

Support de licence pour d'autres plateformes NetScaler :

- **CNS_XXX_Server_PLT_Retail.lic**

Où XXX est le débit.

Pour télécharger un fichier de licence Premium, procédez comme suit :

1. Un fichier de licence valide doit être installé sur l'appliance NetScaler. La licence doit prendre en charge au moins autant de Gbit/s que le débit Gi-LAN maximal attendu.

   Les fichiers de licence doivent être copiés via un client SCP vers le fichier /nsconfig/license de l'appliance, comme indiqué dans la capture d'écran ci-dessous.

   ```
   > shell ls /nsconfig/license/
   CNS_V3000_SERVER_PLT_Retail.lic ssl
   <!--NeedCopy-->
   ```

2. Redémarrez à chaud pour demander la nouvelle licence, comme indiqué dans la capture d'écran ci-dessous.

   ```
   > reboot -warm
   Are you sure you want to restart NetScaler (Y/N)? [N]:y
    Done
   <!--NeedCopy-->
   ```

3. Une fois le redémarrage terminé, vérifiez que la licence a été correctement appliquée, à l'aide de l'interface de ligne de commande show license.

Dans l'exemple ci-dessous, une licence Premium avec édition Premium a été installée avec succès.


```
    > show license

                License status:

                                        Video Optimization: YES

                                                  ...

                                     Model Number ID: 110050

                                        License Type: Premium License
<!--NeedCopy-->
```

Configuration de l'optimisation vidéo sur TCP

May 5, 2023

> **Avertissement :**
>
> Dans le cadre de l'optimisation vidéo, la fonctionnalité de stimulation vidéo est obsolète et sera supprimée de l'appliance NetScaler dans les prochaines versions.

Pour optimiser le trafic vidéo sur TCP, commencez par activer la fonctionnalité d'optimisation vidéo. L'appliance active ensuite les stratégies de détection intégrées pour détecter le trafic vidéo entrant et identifier le type de vidéo. Les stratégies d'optimisation configurables par l'utilisateur pour chaque type de vidéo spécifient le débit binaire d'optimisation nécessaire à l'optimisation du trafic.

Configuration de l'optimisation vidéo sur TCP à l'aide de l'interface de ligne de commande

Pour configurer l'optimisation vidéo sur une appliance NetScaler, vous devez effectuer les tâches suivantes :

1. Activez la fonction d'optimisation vidéo.
2. Ajoutez des serveurs virtuels pour le trafic HTTP et HTTPS.
3. Liez toutes les stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge pour le trafic HTTP.
4. Liez toutes les stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge SSL Bridge pour le trafic HTTPS.
5. Ajoutez les stratégies d'optimisation souhaitées pour le trafic HTTP et HTTPS.
6. Liez les stratégies d'optimisation à un serveur virtuel d'équilibrage de charge pour le trafic HTTP.

7. Liez les stratégies d'optimisation à un serveur virtuel d'équilibrage de charge SSL Bridge pour le trafic HTTPS.

Activation de l'optimisation vidéo

Si vous souhaitez que l'appliance NetScaler détecte, optimise et signale le trafic vidéo, vous devez activer la fonctionnalité d'optimisation vidéo et définir l'optimisation sur ON. Après avoir activé la fonctionnalité, vous pouvez utiliser des stratégies de détection intégrées pour identifier le trafic vidéo entrant, et vous pouvez configurer des stratégies d'optimisation pour optimiser le trafic ABR chiffré. Pour optimiser le trafic vidéo ABR, vous devez configurer le débit binaire de téléchargement (également appelé *débit de rythme*).

Vous devez également activer la fonctionnalité d'équilibrage de charge, et si vous souhaitez utiliser l'optimisation vidéo pour le trafic HTTPS, vous devez activer la fonctionnalité SSL.

Pour activer la fonctionnalité d'optimisation vidéo

À l'invite de commandes, tapez la commande suivante :

```
enable ns feature VideoOptimization
<!--NeedCopy-->
```

> **Remarque**
>
> Si vous souhaitez surveiller les performances d'optimisation vidéo et les rapports d'analyse vidéo, vous devez activer la fonctionnalité AppFlow, puis accéder à la fonctionnalité d'analyse vidéo sur NetScaler Application Delivery Management (ADM). Pour plus d'informations, consultez la documentation Video Insight .

Création de serveurs virtuels pour le trafic vidéo HTTP et HTTPS

Une appliance NetScaler utilise différents serveurs virtuels pour détecter et optimiser les différents types de trafic vidéo entrant. La solution matérielle-logicielle prend en charge les types de serveurs virtuels suivants pour le trafic TCP.

- **Serveur virtuel d'équilibrage de charge HTTP**. Pour détecter le trafic vidéo HTTP, la solution matérielle-logicielle utilise un serveur virtuel d'équilibrage de charge HTTP. Il gère les demandes vidéo HTTP que la solution matérielle-logicielle reçoit des clients.
- **Serveur virtuel d'équilibrage de charge SSL-Bridge**. Pour détecter le trafic vidéo chiffré, vous devez configurer un serveur virtuel de pont SSL sur l'appliance.

Pour ajouter un serveur virtuel d'équilibrage de charge HTTP pour détecter le trafic vidéo HTTP

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name> HTTP * 80 -persistenceType NONE
<!--NeedCopy-->
```

Exemple :

```
add lb vserver ProxyVserver-HTTP HTTP * 80 -persistenceType NONE -
   cltTimeout 120
<!--NeedCopy-->
```

Pour ajouter un serveur virtuel SSL Bridge pour détecter le trafic vidéo HTTPS

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name> SSL_BRIDGE * 443 -persistenceType NONE
<!--NeedCopy-->
```

Exemple :

```
add lb vserver ProxyVserver-SSL SSL_BRIDGE * 443 -persistenceType NONE
   -cltTimeout 180
<!--NeedCopy-->
```

Liaison des stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge HTTP

Pour détecter le trafic vidéo via une connexion HTTP, vous devez lier toutes les stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge. Vous devez lier les stratégies au traitement en temps de demande ou au traitement en temps de réponse, selon le type de stratégie.

> **Remarque :**
>
> La stratégie d'optimisation `ns_videoopt_http_body_detection` vidéo ne prend pas en charge la méthode de requête `CONNECT` HTTP.

Pour lier des stratégies de détection pour différents types de vidéo à un serveur virtuel d'équilibrage de charge HTTP

À l'invite de commandes, tapez la commande appropriée pour chaque type. Les commandes disponibles sont les suivantes :


```
bind lb vserver <name> -policyName ns_videoopt_http_abr_netflix -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_netflix2 -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube2  -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>   -policyName ns_videoopt_http_pd_youtube3 -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>  -policyName ns_videoopt_http_abr_generic -
    priority <integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix -priority 400  type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix2 -priority 500 -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_youtube -priority 600  -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_pd_youtube -priority 800  -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_pd_youtube2 -priority 900 -type RESPONSE

bind lb vserver  ProxyVserver-HTTP   -policyName
    ns_videoopt_http_pd_youtube3 -priority 1000 -type REQUEST

bind lb vserver  ProxyVserver-HTTP   -policyName
    ns_videoopt_http_abr_generic -priority 1100 -type RESPONSE
```



```
<!--NeedCopy-->
```

Liaison de la stratégie de détection du contenu du corps HTTP au serveur virtuel d'équilibrage de charge

Pour détecter le trafic vidéo via HTTP, vous devez lier la stratégie de détection du contenu du corps au serveur virtuel d'équilibrage de charge. Vous pouvez utiliser la commande suivante :

```
bind lb vserver <name> -policyName ns_videoopt_http_body_detection -
    priority <integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver ProxyVserver-HTTP -policyName
    ns_videoopt_http_body_detection -priority 1500 -type REQUEST
<!--NeedCopy-->
```

Liaison de stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge SSL

Pour détecter le trafic vidéo via une connexion HTTPS, vous devez lier des stratégies de détection intégrées à un serveur virtuel d'équilibrage de charge du pont SSL.

Pour lier une stratégie de détection à un serveur virtuel d'équilibrage de charge de pont SSL

À l'invite de commandes, tapez la commande appropriée pour chaque type. Les commandes disponibles sont les suivantes :

```
bind lb vserver <name> -policyName ns_videoopt_https_abr_netflix -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_youtube -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_generic -
    priority <positive_integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Exemple :


```
bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_netflix -priority 120 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_youtube -priority 140 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_generic -priority 150 -type REQUEST
<!--NeedCopy-->
```

Ajout de stratégies d'optimisation pour le rythme du trafic ABR

Pour optimiser le trafic ABR, vous devez configurer des stratégies d'optimisation et les actions associées. Vous liez ensuite les stratégies aux mêmes serveurs virtuels d'équilibrage de charge auxquels vous avez lié les stratégies de détection. Pour chaque stratégie, créez d'abord l'action, afin de pouvoir l'inclure lors de la création de la stratégie.

Pour ajouter une action d'optimisation

À l'invite de commande, tapez :

```
add videooptimization pacingaction <action Name> -rate <integer> [-
    comment <string>]
<!--NeedCopy-->
```

Où le paramètre **rate** spécifie le débit en Kbps auquel envoyer le trafic (la fréquence de rythme).

Exemple :

```
add videooptimization pacingaction MyOptAct2000 -rate 2000
<!--NeedCopy-->
```

Pour ajouter une stratégie d'optimisation

À l'invite de commande, tapez :

```
add videooptimization pacingpolicy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

Exemple :


```
add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
   MyOptAct2000
<!--NeedCopy-->
```

Liaison des stratégies d'optimisation à un serveur virtuel d'équilibrage de charge HTTP

Pour optimiser le trafic vidéo ABR via une connexion HTTP, vous devez lier les stratégies d'optimisation à un serveur virtuel d'équilibrage de charge auquel les stratégies de détection sont liées.

Pour lier une stratégie d'optimisation à un serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez la commande suivante :

```
bind lb vserver <name> -policyName <policy_name> -priority <
   positive_integer> -type  (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver ProxyVserver-HTTP -policyName myOptPolicy2000 -priority
    3400 -type  REQUEST
<!--NeedCopy-->
```

Liaison des stratégies d'optimisation aux serveurs virtuels SSL-Bridge

Pour optimiser le trafic vidéo ABR via une connexion HTTPS, vous devez lier les stratégies d'optimisation au serveur virtuel SSL Bridge auquel les stratégies de détection intégrées sont liées.

Pour lier une stratégie d'optimisation au serveur virtuel SSL Bridge afin de rythmer le trafic chiffré

À l'invite de commandes, tapez la commande suivante :

```
bind lb vserver <name> -policyName <policy_name> -priority <
   positive_integer> -type  (REQUEST |RESPONSE)
<!--NeedCopy-->
```

Exemple :


```
bind lb vserver ProxyVserver-SSL -policyName myOptPolicy2000 -priority
    3400 -type  REQUEST
<!--NeedCopy-->
```

Définition des paramètres de stimulation de l'optimisation vidéo

L'interface de ligne de commande vous permet de définir les paramètres de rythme d'optimisation vidéo, tels que le pourcentage d'échantillonnage aléatoire.

Pour définir le pourcentage d'échantillonnage aléatoire

À l'invite de commandes, tapez la commande suivante :

```
set videooptimization parameter  - RandomSamplingPercentage <realNumber>
<!--NeedCopy-->
```

Où, un RealNumber est une valeur comprise entre 0,0 et 100,0.

Exemple :

```
set videooptimization parameter -RandomSamplingPercentage 50
<!--NeedCopy-->
```

Configuration de l'optimisation vidéo sur TCP à l'aide de l'interface graphique

L'interface graphique vous permet de :

- Activez la fonction d'optimisation vidéo.
- Créez un serveur virtuel d'équilibrage de charge HTTP.
- Créez un serveur virtuel d'équilibrage de charge SSL Bridge.
- Liez les stratégies de détection intégrées au serveur virtuel d'équilibrage de charge HTTP.
- Liez les stratégies de détection intégrées au serveur virtuel d'équilibrage de charge SSL Bridge.
- Créez une stratégie d'optimisation.
- Créez une action d'optimisation.
- Configuration du paramètre de rythme d'optimisation.
- Liez la stratégie d'optimisation au serveur virtuel d'équilibrage de charge pour le trafic HTTP.
- Liez la stratégie d'optimisation au serveur virtuel d'équilibrage de charge SSL-Bridge pour le trafic HTTPS.

Pour activer la fonctionnalité d'optimisation vidéo

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Sur la page **Paramètres**, cliquez sur le lien **Configurer les fonctionnalités avancées** .
3. Sur la page **Configurer les fonctionnalités avancées**, cochez la case **Optimisation vidéo** .
4. Cliquez sur **OK**, puis sur **Fermer**.

Pour créer un serveur virtuel d'équilibrage de charge pour le trafic HTTP

1. Connectez-vous à l'appliance NetScaler et accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur l'écran Serveur virtuel d'équilibrage de charge, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Sélectionnez le type de protocole HTTP
   c) **Type d'adresse IP**. Type d'adresse IP : IPv4 ou IPv6.
   d) **Adresse IP**. Adresse IPv4 ou IPv6 attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur **OK** pour poursuivre la configuration d'autres paramètres facultatifs. Pour plus d'informations, voir Création d'un serveur virtuel.
5. Cliquez sur **Créer** et **Fermer**.

Pour créer un serveur virtuel d'équilibrage de charge pour le trafic HTTPS

1. Connectez-vous à l'appliance NetScaler et accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur l'écran **Serveur virtuel d'équilibrage de charge**, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Sélectionnez le type de protocole en tant que pont SSL.
   c) **Type d'adresse IP**. Type d'adresse IP : IPv4 ou IPv6.
   d) **Adresse IP**. Adresse IPv4 ou IPv6 attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur **OK** pour poursuivre la configuration d'autres paramètres facultatifs. Pour plus d'informations, voir Création d'un serveur virtuel.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour lier une stratégie de détection intégrée à un serveur virtuel d'équilibrage de charge

1. Connectez-vous à l'appliance NetScaler et accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .

2. Dans le volet d'informations, sélectionnez le serveur virtuel d'équilibrage de charge et cliquez sur **Modifier**.
    a) Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
    b) Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies** .
    c) Dans la section **Stratégies**, définissez les paramètres suivants.
    d) Choisissez Policy. Sélectionnez une stratégie de détection d'optimisation vidéo dans la liste déroulante.
    e) Sélectionnez Type. Sélectionnez le type de stratégie en tant que demande.
    f) Cliquez sur **Continuer**.
3. Sélectionnez la stratégie de détection vidéo dans la liste, puis cliquez sur **Fermer**.

Pour lier une stratégie de détection intégrée à un serveur virtuel d'équilibrage de charge SSL Bridge

1. Connectez-vous à l'appliance NetScaler et accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, sélectionnez le serveur virtuel d'équilibrage de charge SSL-Bridge, puis cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies** .
5. Dans la section **Stratégies**, définissez les paramètres suivants.
    a) Choisissez Policy. Sélectionnez la stratégie de détection de l'optimisation vidéo dans la liste déroulante.
    b) Sélectionnez Type. Sélectionnez le type de stratégie en tant que demande.
6. Cliquez sur **Continuer**.
7. Sélectionnez la stratégie de détection vidéo dans la liste, puis cliquez sur **Fermer**.

Pour créer une action d'optimisation vidéo

1. ****Connectez-vous à l'appliance NetScaler et accédez à **Configuration** > **Optimisation > Optimisationvidéo** > **Pacing > Actions.****
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer une action de rythme d'optimisation vidéo**, définissez les paramètres suivants.
    a) **Nom**. Nom de l'action d'optimisation.
    b) **Taux d'optimisation ABR (Kbps).** Taux de rythme auquel envoyer le trafic vidéo ABR. Le débit par défaut pour l'optimisation ABR est de 1000 Kbps. La valeur minimale est 1 et la valeur maximale est 2147483647.
    c) **Commentaire**. Une brève description de l'action.
4. Cliquez sur **Créer** et **Fermer**.

Pour créer une stratégie d'optimisation vidéo

1. ****Connectez-vous à l'appliance NetScaler et accédez à **Configuration** > **Optimisation > Optimisationvidéo** > **Pacing > Politiques.****
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer une stratégie de rythme d'optimisation vidéo**, définissez les paramètres suivants.
   a) **Nom**. Nom de la stratégie d'optimisation
   b) **Expression** : Expressions régex personnalisées qui implémentent la stratégie.
   c) **Action**. Action d'optimisation associée à la stratégie pour gérer le trafic vidéo entrant.
   d) **Action du FNUD.** Événement non défini si la demande entrante ne correspond pas à la stratégie d'optimisation.
   e) **Commentaire**. Une brève description de la politique.
   f) **Action de journalisation.** Sélectionnez l'action du journal d'audit qui crée les messages de journal souhaités.
4. Cliquez sur **Créer**, puis sur **Fermer.**

Pour définir les paramètres de rythme d'optimisation vidéo

1. Connectez-vous à l'appliance NetScaler et accédez à **Configuration** > **Optimisation > Optimisationvidéo**.
2. Dans la page **Optimisation vidéo**, cliquez sur **le lien Modifier les paramètres d'optimisation vidéo** .
3. Dans la page **Paramètres d'optimisation vidéo**, définissez le paramètre suivant.
   a) **Pourcentage d'échantillonnage aléatoire (%)**. Pourcentage de paquets sélectionnés pour un échantillonnage aléatoire.
4. Cliquez sur **OK** et sur **Fermer**.

Pour lier une stratégie d'optimisation vidéo à un serveur virtuel d'équilibrage de charge HTTP

1. Connectez-vous à l'appliance NetScaler et accédez à **Configuration** > **Optimisation > Optimisationvidéo**.
2. Sur la page **Optimisation vidéo**, cliquez sur le lien **Video Optimization Pacing Policy Manager** .
3. Définissez les paramètres suivants.
   a) **Point de liaison**. Point auquel appliquer la stratégie d'optimisation pendant le traitement de la demande ou de la réponse.
   b) **Type de connexion**. Type de connexion Request ou Response.
   c) **Serveur virtuel**. Serveur virtuel d'équilibrage de charge auquel lier la stratégie.
   d) Cliquez sur **Continuer**.

4. Dans la section **Point de liaison**, effectuez l'une des opérations suivantes :
   a) Sélectionnez une stratégie dans la liste.
   b) Cliquez sur **Ajouter une liaison** pour accéder au curseur **Liaison des stratégies** .
      i. Sélectionnez une stratégie existante ou ajoutez-en une nouvelle.
      ii. Saisissez les détails de la liaison et cliquez sur **Liaison**.
5. Cliquez sur **Fermer**.

Pour lier une stratégie d'optimisation vidéo à un serveur virtuel d'équilibrage de charge SSL Bridge

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configuration**>**Optimisation > Optimisation****vidéo**.**
2. Sur la page **Optimisation vidéo**, cliquez sur le lien **Video Optimization Pacing Policy Manager** .
3. Sur la page **Video Optimization Policy Manager**, définissez les paramètres suivants.
   a) Point de liaison. Point auquel appliquer la stratégie d'optimisation pendant le traitement de la demande/réponse.
   b) Type de connexion. Type de connexion Request ou Response.
   c) Serveur virtuel. Serveur virtuel d'équilibrage de charge SSL Bridge auquel lier la stratégie.
4. Cliquez sur **Continuer**.
5. Dans la section **Point de liaison**, effectuez l'une des opérations suivantes :
   a) Sélectionnez une liaison de stratégie dans la liste.
   b) Cliquez sur **Ajouter une liaison** pour accéder au curseur **Liaison des stratégies** .
      i. Sélectionnez une stratégie existante ou ajoutez-en une nouvelle.
      ii. Saisissez les détails de la liaison et cliquez sur **Liaison**.
6. Cliquez sur **Fermer**.

Configuration de l'optimisation vidéo via UDP

May 5, 2023

Pour optimiser le trafic vidéo QUIC ABR via UDP, commencez par activer la fonctionnalité d'optimisation vidéo. Une fois la configuration terminée, l'appliance détecte le trafic vidéo ABR basé sur QUIC et applique le débit d'optimisation configuré sur l'appliance.

Configuration de l'optimisation vidéo pour QUIC à l'aide de l'interface de ligne de commande

Pour configurer l'optimisation vidéo pour le trafic vidéo QUIC via UDP, vous devez effectuer les tâches suivantes :

1. Activez l'optimisation vidéo.
2. Créez un service QUIC.
3. Créez un serveur virtuel d'équilibrage de charge QUIC.
4. Liez le service Web QUIC au serveur virtuel d'équilibrage de charge.
5. Créez une politique d'optimisation vidéo pour rythmer le trafic UDP basé sur QUIC.
6. Liez la politique d'optimisation à un serveur virtuel d'équilibrage de charge basé sur QUIC.

Activer l'optimisation vidéo pour le trafic QUIC

Si vous souhaitez que l'appliance NetScaler détecte, optimise et signale le trafic vidéo, vous devez activer la fonctionnalité d'optimisation vidéo et activer l'optimisation.

> **Remarque**
>
> Si vous souhaitez utiliser l'optimisation vidéo pour le trafic QUIC, vous devez activer les fonctionnalités d'équilibrage de charge et d'AppFlow.

Pour activer l'optimisation vidéo

À l'invite de commandes, tapez la commande suivante :

```
enable ns feature VideoOptimization
<!--NeedCopy-->
```

Création d'un service pour le trafic QUIC

Une appliance NetScaler utilise un service QUIC pour que le serveur virtuel d'équilibrage de charge se connecte au routeur de sortie en mode de routage statique.

> **Remarque**
>
> Actuellement, le routage dynamique n'est pas pris en charge.

Pour créer un service Web d'équilibrage de charge pour le trafic vidéo QUIC

À l'invite de commande, tapez :


```
add service <name> <router-IP> <serviceType> <port> -usip yes -
   useproxyport  [yes | no]
<!--NeedCopy-->
```

Exemple :

```
add service svc-quic 10.102.29.200 QUIC 443  -usip yes  -useproxyport
   no

where IP address is the internet router address.
<!--NeedCopy-->
```

Création d'un serveur virtuel d'équilibrage de charge pour le trafic QUIC

Une appliance NetScaler utilise un serveur virtuel d'équilibrage de charge pour détecter et optimiser le trafic vidéo QUIC via UDP.

Pour créer un serveur virtuel d'équilibrage de charge pour le trafic vidéo QUIC

À l'invite de commande, tapez :

```
add lb vserver <name> <serviceType> <ip> <port> -m MAC
<!--NeedCopy-->
```

Exemple :

```
add lb vserver vs-quic QUIC * 443 -persistenceType NONE -m MAC -
   cltTimeout 120
<!--NeedCopy-->
```

Liaison d'un service Web QUIC au serveur virtuel d'équilibrage de charge

Après avoir créé les services Web et le serveur virtuel d'équilibrage de charge pour le trafic QUIC, vous devez lier les services au serveur virtuel.

Pour lier un service Web à un serveur virtuel d'équilibrage de charge pour le trafic vidéo QUIC

À l'invite de commande, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```


Exemple :

```
bind lb vserver vs-quic svc-quic
<!--NeedCopy-->
```

Création d'une politique d'optimisation vidéo pour le trafic UDP basé sur QUIC

Pour optimiser le trafic UDP basé sur QUIC, vous devez configurer les politiques d'optimisation et leurs actions. Vous devez ensuite lier les politiques aux serveurs virtuels d'équilibrage de charge basés sur QUIC. Pour chaque stratégie, créez d'abord une action afin de pouvoir l'associer à la stratégie.

Pour ajouter une action d'optimisation

À l'invite de commande, tapez :

```
add videooptimization pacingaction <action Name> -rate <integer> [-
    comment <string>]
<!--NeedCopy-->
```

Où, le paramètre **rate** spécifie le débit en Kbits/s auquel envoyer le trafic (le rythme cardiaque).

Exemple :

```
set videooptimization parameter -QUICPacingRate 1000
<!--NeedCopy-->
```

où 1000 représente le rythme souhaité en Kbits/sec.

Pour ajouter une stratégie d'optimisation

À l'invite de commande, tapez :

```
add videooptimization pacingpolicy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

Exemple :

```
add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
    MyOptAct2000
<!--NeedCopy-->
```


Liaison de politiques d'optimisation à un serveur virtuel d'équilibrage de charge QUIC

Pour optimiser le trafic vidéo QUIC via une connexion UDP, vous devez lier les politiques d'optimisation à un serveur virtuel d'équilibrage de charge QUIC.

Pour lier une politique d'optimisation à un serveur virtuel QUIC Load Balancing

À l'invite de commandes, tapez la commande suivante :

```
bind lb vserver <name> -policyName <policy_name> -priority <
    positive_integer> -type (REQUEST)
<!--NeedCopy-->
```

> **Remarque**
>
> Les politiques de rythme doivent être liées à un serveur virtuel d'équilibrage de charge QUIC uniquement au moment de la demande.

Exemple :

```
bind lb vserver vs-quic -policyName myOptPolicy2000 -priority 3400 -
    type  REQUEST
<!--NeedCopy-->
```

Configuration de l'optimisation vidéo pour QUIC à l'aide de l'interface graphique

Pour configurer la fonctionnalité sur l'appliance via l'interface graphique, vous devez effectuer les tâches suivantes :

1. Activer l'optimisation vidéo
2. Configurer un serveur QUIC
3. Configurer le service QUIC
4. Configurer un serveur virtuel d'équilibrage de charge QUIC
5. Liez le service Web QUIC au serveur virtuel d'équilibrage de charge
6. Créez une politique d'optimisation.
7. Créez une action d'optimisation.
8. Configuration du paramètre de rythme d'optimisation.
9. Liez la politique d'optimisation au serveur virtuel d'équilibrage de charge pour le trafic QUIC.

Pour activer l'optimisation vidéo

1. **Connectez-vous à l'appliance NetScaler et accédez à**Système > Paramètres**.**
2. Sur la page de détails, sélectionnez le lien **Configurer les fonctionnalités avancées** .
3. Sur la page **Configurer les fonctionnalités avancées**, cochez la case **Optimisation vidéo** .

Pour créer un serveur QUIC

1. Connectez-vous à l'appliance NetScaler et accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs** .
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer un serveur**, définissez les paramètres suivants :
   a) Nom. Nom du serveur QUIC.
   b) Adresse IP Adresse IP du serveur QUIC
   c) Domaine de trafic. Nom de domaine du serveur.
   d) Activation après la création. État initial du serveur.
   e) Commentaires. Brèves informations sur le serveur.
4. Cliquez sur **Create**.

Pour créer un service QUIC

1. Connectez-vous à l'appliance NetScaler et accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Service d'équilibrage** de charge, définissez les paramètres suivants :
   a) **Nom du service**. Nom du service QUIC.
   b) **Adresse IP** Adresse IP attribuée au service QUIC.
   c) **Protocole**. Sélectionnez le protocole QUIC.
   d) **Port**. Numéro de port du service Web.
4. Cliquez sur **OK** pour continuer. Vous pouvez ensuite configurer d'autres paramètres facultatifs. Pour plus d'informations, voir Configuration des services.
5. Une fois que vous avez configuré les paramètres facultatifs, cliquez sur **OK** et **Fermer** .

Pour créer un serveur virtuel d'équilibrage de charge

1. Connectez-vous à l'appliance NetScaler et accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Serveur virtuel d'équilibrage** de charge, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Protocole utilisé par le service pour envoyer des requêtes QUIC.
   c) Type d'adresse IP. Type d'adresse IP : IPv4 ou IPv6.
   d) **Adresse IP**. Adresse IP 4 ou IP6 attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur OK pour poursuivre la configuration d'autres paramètres facultatifs. Pour plus d'informations, voir Création d'un serveur virtuel.

Pour lier un serveur virtuel d'équilibrage de charge à un service QUIC

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis sélectionnez un serveur virtuel.
2. Cliquez sur **Services et groupes de services** pour accéder à l'écran de **liaison des services du serveur virtuel d'équilibrage de charge** .
3. Sélectionnez un service Web basé sur QUIC et cliquez sur **Bind**.
4. Cliquez sur **Terminé**.

Pour lier un serveur virtuel d'équilibrage de charge à un service QUIC

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis sélectionnez un serveur virtuel.
2. Cliquez sur **Services et groupes de services** pour accéder à l'écran de **liaison des services du serveur virtuel d'équilibrage de charge** .
3. Sélectionnez un service Web basé sur QUIC et cliquez sur **Bind**.
4. Cliquez sur **Terminé**.

Pour créer une action d'optimisation vidéo pour le trafic QUIC

1. ****Connectez-vous à l'appliance NetScaler et accédez à **Configuration** > **Optimisation > Optimisationvidéo** > **Pacing > Actions.****
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer une action de rythme d'optimisation vidéo**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action d'optimisation.
   b) **Taux d'optimisation ABR (Kbps).** Taux de rythme auquel envoyer le trafic vidéo ABR. Le débit par défaut pour l'optimisation ABR est de 1000 Kbps. La valeur minimale est 1 et la valeur maximale est 2147483647.
   c) **Commentaire**. Une brève description de l'action.
4. Cliquez sur **Créer** et **Fermer**.

Pour créer une politique d'optimisation vidéo pour le trafic QUIC

1. ****Connectez-vous à l'appliance NetScaler et accédez à **Configuration** > **Optimisation > Optimisationvidéo** > **Pacing > Politiques.****
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer une stratégie de rythme d'optimisation vidéo**, définissez les paramètres suivants.
   a) Nom. Nom de la stratégie d'optimisation
   b) Expression : Expressions regrex personnalisées qui implémentent la politique.

c) Action. Action d'optimisation associée à la stratégie pour gérer le trafic vidéo entrant.
d) Action du FNUD. Événement non défini si la demande entrante ne correspond pas à la stratégie d'optimisation.
e) Commentaire. Une brève description de la politique.
f) Action de journalisation. Sélectionnez l'action du journal d'audit qui crée les messages de journal souhaités.

4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour lier une politique d'optimisation vidéo à un serveur virtuel d'équilibrage de charge QUIC

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configuration**>**Optimisation > Optimisation****vidéo**.**
2. Sur la page **Optimisation vidéo**, cliquez sur le lien **Video Optimization Pacing Policy Manager** .
3. Sur la page **Video Optimization Policy Manager**, définissez les paramètres suivants.
   a) Point de liaison. Point auquel appliquer la politique d'optimisation pendant le traitement de la demande. **Remarque** : Les politiques de rythme doivent être liées à un serveur virtuel d'équilibrage de charge QUIC uniquement au moment de la demande.
   b) Type de connexion. Type de connexion Request ou Response.
   c) Serveur virtuel. Serveur virtuel d'équilibrage de charge auquel lier la stratégie.
4. Cliquez sur **Continuer**.
5. Dans la section **Point de liaison**, effectuez l'une des opérations suivantes :
   a) Sélectionnez une stratégie dans la liste.
   b) Cliquez sur **Ajouter une liaison** pour accéder au curseur **Liaison des stratégies** .
      i. Sélectionnez une stratégie existante ou ajoutez-en une nouvelle.
      ii. Saisissez les détails de la liaison et cliquez sur **Liaison**.
6. Cliquez sur **Fermer**.

Filtrage d'URL NetScaler

May 5, 2023

Le filtrage des URL permet de contrôler les sites Web selon des règles en utilisant les informations contenues dans les URL. Cette fonctionnalité permet aux administrateurs réseau de surveiller et de contrôler l'accès des utilisateurs aux sites Web malveillants sur les réseaux mobiles.

En tant qu'administrateur, vous pouvez configurer une stratégie de filtrage d'URL à l'aide de la fonction de catégorisation d'URL ou de la fonction de liste d'URL.

Liste d'URL. Contrôle l'accès aux sites Web et aux pages Web figurant sur la liste noire en bloquant l'accès aux URL figurant dans un ensemble d'URL importé dans l'appliance.

Catégorisation des URL. Contrôle l'accès aux sites Web et aux pages Web en filtrant le trafic sur la base d'une liste prédéfinie de catégories.

Liste des URL

May 5, 2023

La fonctionnalité Liste d'URL vous permet de contrôler l'accès à des listes d'URL personnalisées (jusqu'à un million d'entrées). La fonctionnalité filtre les sites Web en appliquant une politique de filtrage des URL liée à un serveur virtuel.

En tant qu'administrateur, vous devez importer la liste d'URL dans l'appliance NetScaler. Cette liste importée est stockée en interne sous la forme d'un ensemble de données de politique appelé *ensemble d'URL*. L'appliance applique ensuite un algorithme unique de correspondance rapide d'URL aux demandes d'URL entrantes. Si la demande d'URL entrante correspond à une entrée de l'ensemble, l'appliance applique l'action de politique associée pour contrôler l'accès.

Types de listes d'URL

Chaque entrée d'un ensemble d'URL peut inclure une URL et, éventuellement, ses métadonnées (catégorie d'URL, groupes de catégories ou toute autre donnée associée). Pour les URL avec une métadonnées, l'appliance utilise une expression de stratégie qui évalue les métadonnées. Pour plus d'informations, voir Jeux d'URL.

Liste d'URL personnalisée. Vous pouvez créer un ensemble d'URL personnalisé contenant jusqu'à 1 000 000 d'entrées d'URL et l'importer sous forme de fichier texte dans votre appliance. La liste peut contenir des URL avec ou sans métadonnées (qui peuvent ressembler à une catégorie d'URL). La plateforme NetScaler détecte automatiquement la présence de métadonnées. Il prend également en charge le stockage sécurisé des listes importées. Pour plus d'informations, voir Jeu d'URL.

Vous pouvez héberger la liste d'URL et configurer l'appliance NetScaler pour qu'elle mette régulièrement à jour la liste sans intervention manuelle. Une fois la liste d'URL mise à jour, l'appliance peut détecter automatiquement les métadonnées et les catégories en utilisant des expressions de politique pour évaluer chaque URL entrante, puis appliquer des actions telles que autoriser, bloquer, rediriger ou informer l'utilisateur.

Expressions de politique relatives aux listes d'URL

Le tableau suivant décrit les expressions de base que vous pouvez utiliser pour évaluer le trafic entrant. Une fois que vous avez importé une liste d'URL dans l'appliance, elle est appelée *ensemble d'URL*.

Expression	Operation
<URL expression>.URLSET_MATCHES_ANY (<URLSET>)	Évalue la valeur TRUE si l'URL correspond exactement à n'importe quelle entrée de l'ensemble d'URL.
<URL expression>. GET_URLSET_METADATA(<URLSET>)	L'expression GET_URLSET_METADATA () renvoie les métadonnées associées si l'URL correspond exactement à un modèle de l'ensemble d'URL. Une chaîne vide est renvoyée s'il n'y a pas de correspondance.
<URL expression>.GET_ URLSET_METADATA(<URLSET>).EQ(< METADATA>)	Évalue la valeur TRUE si les métadonnées correspondantes sont égales à <METADATA>.
<URLexpression>.GET_URLSET_METADATA (<URLSET>).TYPECAST_LIST_T(',').GET (0).EQ(<CATEGORY>)	Renvoie la valeur TRUE si les métadonnées correspondantes se trouvent au début de la catégorie. Ce modèle peut être utilisé pour coder des champs distincts au sein des métadonnées, mais uniquement pour faire correspondre le 1st champ.
HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL)	Joint les paramètres de l'hôte et de l'URL, qui peuvent ensuite être utilisés <URL expression> pour la mise en correspondance.

Actions de politique relatives aux listes d'URL

La mesure d'application la plus courante pour les URL qui correspondent à une liste d'URL consiste à restreindre l'accès. Créez une politique de liste d'URL avec l'expression de liste d'URL souhaitée et une action d'application. L'utilisation du groupe de règles dépend du type de trafic entrant (HTTP ou HTTPS) et du serveur virtuel configuré sur l'appliance. Vous pouvez utiliser une politique de répondeur pour le trafic HTTP ou une politique d'optimisation vidéo pour le trafic HTTPS. Spécifiez les actions à appliquer aux URL qui correspondent aux expressions des politiques. Le tableau suivant répertorie les actions disponibles.

Action Type	Stratégie	Description
ALLOW	Répondeur	Autorisez la demande à accéder à l'URL cible.
REDIRIGER	Répondeur	Redirigez la demande vers l'URL spécifiée comme cible.
DENY	Répondeur	Refusez la demande.
RÉINITIALISER	Répondeur, optimisation vidéo	Réinitialisez la connexion.
ABANDONNER	Répondeur, optimisation vidéo	Oubliez la connexion.

Composants requis

Pour configurer la fonctionnalité de liste d'URL, assurez-vous d'avoir configuré le serveur suivant.

Serveur DNS pour les demandes DNS

Vous devez configurer un serveur DNS si vous importez un ensemble d'URL à partir de l'URL d'un nom d'hôte.

À l'invite de commande, tapez :

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>) [-state (
    ENABLED | DISABLED )] [-type <type>] [-dnsProfileName <string>]
<!--NeedCopy-->
```

Exemple :

```
add dns nameServer 10.140.50.5
<!--NeedCopy-->
```

Importation d'une liste d'URL personnalisée

Pour importer un ensemble d'URL, reportez-vous à la rubrique Jeu d'URL .

Configuration d'une liste d'URL pour le trafic HTTP

L'appliance NetScaler prend en charge le trafic HTTP et HTTPS. Pour configurer un serveur virtuel d'équilibrage de charge pour le trafic HTTP et lier les politiques de liste d'URL au serveur, procédez

comme suit :

- Ajoutez des actions de liste d'URL.
- Ajoutez des politiques de liste d'URL.
- Ajouter un serveur virtuel d'équilibrage de charge HTTP pour le trafic HTTP
- Liez les politiques de liste d'URL au serveur virtuel d'équilibrage de charge HTTP pour le trafic HTTP

Pour ajouter une action de liste d'URL

À l'invite de commandes, tapez ce qui suit :

```
1 add responder action <name> <type> (<target> | <htmlpage>) [-comment <
     string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
     string>]
2 <!--NeedCopy-->
```

Pour ajouter un serveur virtuel d'équilibrage de charge HTTP pour le trafic HTTP

À l'invite de commandes, tapez ce qui suit :

```
1 add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
     imeout <secs>]
2 <!--NeedCopy-->
```

Exemple :

```
1 add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout
     120
2 <!--NeedCopy-->
```

Pour lier la politique de liste d'URL au serveur virtuel d'équilibrage de charge HTTP

À l'invite de commandes, tapez ce qui suit :

```
1 bind lb vserver <vServerName> -policyName <string> [-priority <
     positive_integer>]
2 <!--NeedCopy-->
```

Configuration de la liste d'URL pour le trafic HTTPS

L'appliance NetScaler prend en charge le trafic HTTP et HTTPS. Pour configurer un serveur virtuel d'équilibrage de charge SSL Bridge pour le trafic HTTPS et lier les politiques de liste d'URL au serveur,

procédez comme suit :

- Ajoutez des actions de liste d'URL.
- Ajoutez des politiques de liste d'URL.
- Ajouter un serveur virtuel d'équilibrage de charge SSL Bridge pour le trafic HTTP
- Liez les politiques de liste d'URL au serveur virtuel d'équilibrage de charge SSL-Bridge pour le trafic HTTP

Pour ajouter une politique de liste d'URL pour le trafic HTTPS

À l'invite de commande, tapez :

```
add videooptimization detectionpolicy <name> -rule <expression> -action
     <string> [-undefAction <string>] [-comment <string>] [-logAction <
    string>]
<!--NeedCopy-->
```

Pour ajouter un serveur virtuel d'équilibrage de charge SSL Bridge

À l'invite de commandes, tapez :

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
    imeout <secs>]
<!--NeedCopy-->
```

Exemple :

```
add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -
    cltTimeout 180
<!--NeedCopy-->
```

Pour lier la politique de liste d'URL à l'équilibrage de charge du pont SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```


Configuration d'une liste d'URL à l'aide de l'interface graphique

L'interface graphique vous permet de :

- Importez une liste d'URL.
- Ajoutez une liste d'URL.
- Configurez les actions de la liste d'URL.
- Configurez les politiques de liste d'URL pour le trafic HTTP.
- Ajoutez un serveur virtuel d'équilibrage de charge HTTP pour le trafic HTTP.
- Ajoutez un serveur virtuel d'équilibrage de charge SSL Bridge pour le trafic HTTPS.
- Liez les politiques de liste d'URL au serveur virtuel d'équilibrage de charge HTTP.
- Liez les politiques d'une liste d'URL au serveur virtuel d'équilibrage de charge SSL-Bridge.

Pour importer une liste d'URL

1. Dans le volet de navigation, ouvrez **AppExpert** > **Ensembles d'URL**.
2. Dans le volet de détails, cliquez sur **Importer**.
3. Sur la page **Configurer l'ensemble d'URL**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'ensemble d'URL.
   b) **URL**. Adresse Web de l'emplacement à partir duquel accéder à l'ensemble d'URL.
   c) **Ecraser.** Remplacez un ensemble d'URL précédemment importé.
   d) **Délimiteur**. Séquence de caractères qui délimite un enregistrement de fichier CSV.
   e) **Séparateur de lignes**. Séparateur de lignes utilisé dans le fichier CSV. Une valeur d'un seul caractère est autorisée, par exemple « /n ».
   f) **Intervalle**. Intervalle en secondes, arrondi aux 15 minutes les plus proches, auquel l'ensemble d'URL est mis à jour.
   g) **Coffret privé.** Option permettant d'empêcher l'exportation de l'ensemble d'URL
   h) **URL du Canary**. URL interne permettant de vérifier si le contenu de l'ensemble d'URL doit rester confidentiel. La longueur maximale de l'URL est de 2 047 caractères
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour ajouter une liste d'URL

1. Dans le volet de navigation, ouvrez **AppExpert** > **Ensembles d'URL**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer un ensemble d'URL**, définissez les paramètres suivants.
   a) **Nom**. Le nom de l'ensemble d'URL qui a été donné lors de son importation.
   b) **Commentaires**. Brève description de l'ensemble d'URL.
4. Cliquez sur **Create**.

Pour configurer une action de liste d'URL

1. Connectez-vous à l'appliance NetScaler et accédez à l'onglet **Configuration** .
2. **Dans le volet de menu, accédez à**AppExpert**>**Responder**> Actions.**
3. Dans le volet de détails, cliquez sur **Ajouter**.
4. Sur la page **Créer une action de répondeur**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action de politique de liste d'URL.
   b) **Tapez**. Sélectionnez un type d'action.
   c) **Expression** : Utilisez l'éditeur d'expressions pour créer l'expression de politique.
   d) **Commentaires**. Brève description de l'action politique.
5. Cliquez sur **Créer** et **Fermer**.

Pour configurer une politique de liste d'URL

1. **Dans le volet de navigation, ouvrez**AppExpert**>**Responder > Policies**.**
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer une politique de répondeur**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action de politique de liste d'URL.
   b) **Action**. Sélectionnez l'action Liste d'URL que vous préférez associer à la politique.
   c) **Action de journalisation**. Sélectionnez l'action de journalisation.
   d) **AppFlow**. Sélectionnez une action AppFlow.
   e) **Expression** : Utilisez l'éditeur d'expressions pour créer l'expression de politique.
   f) **Commentaires**. Brève description de la politique.
4. Cliquez sur **Créer** et **Fermer**.

Pour ajouter un serveur virtuel d'équilibrage de charge HTTP

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur l'écran **Serveur virtuel d'équilibrage de charge**, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Choisissez le type de protocole HTTP.
   c) **Type d'adresse IP**. Type adressable par IP.
   d) **Adresse IP**. Adresse IP 4 ou IP6 attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur **OK** pour poursuivre la configuration d'autres paramètres facultatifs. Pour plus d'informations, voir Création d'un serveur virtuel.

Pour lier une politique de liste d'URL au serveur virtuel d'équilibrage de charge HTTP

1. Accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .

2. Dans le volet d'informations, sélectionnez le serveur virtuel d'équilibrage de charge et cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies** .
5. Dans la section **Stratégies**, définissez les paramètres suivants.
   a) Choisissez Policy. Sélectionnez une politique de catégorisation d'URL dans la liste déroulante.
   b) Sélectionnez Type. Sélectionnez le type de stratégie en tant que demande.
6. Cliquez sur **Continuer**.
7. Sur la page Politiques, sélectionnez la politique de liste d'URL dans la liste et cliquez sur **Sélectionner**.
8. Dans le curseur **Politiques**, cliquez sur **Lier** et **fermer**.

Pour ajouter une politique de liste d'URL pour le trafic HTTPS

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configuration**>**Optimisation > Optimisation****vidéo** > **Détection**.**
2. Sur la page **Détection**, cliquez sur le lien **Politiques de détection pour l'optimisation vidéo** .
3. Sur la page **Stratégies de détection d'optimisation vidéo**, cliquez sur **Ajouter**.
4. Sur la page **Créer une politique de détection pour l'optimisation vidéo**, définissez les paramètres suivants.
   a) **Nom**. Nom de la stratégie d'optimisation
   b) **Expression** : Configurez la politique à l'aide d'expressions personnalisées.
   c) **Action**. Action d'optimisation associée à la stratégie pour gérer le trafic vidéo entrant.
   d) **Action du UNDEF.** Événement non défini si la demande entrante ne correspond pas à la stratégie d'optimisation.
   e) **Commentaire**. Une brève description de la politique.
   f) **Action de journalisation**. Sélectionnez une action du journal d'audit qui spécifie l'action à effectuer pour les messages du journal.
5. Cliquez sur **Créer** et **Fermer**.

Pour ajouter un serveur virtuel d'équilibrage de charge SSL Bridge pour le trafic HTTPS

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur l'écran **Serveur virtuel d'équilibrage de charge**, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Sélectionnez le type de protocole en tant que pont SSL.
   c) **Type d'adresse IP**. Type d'adresse IP : IPv4 ou IPv6.
   d) **Adresse IP**. Adresse IPv4 ou IP6VIP attribuée au serveur virtuel.

e) **Port**. Numéro de port du serveur virtuel.

4. Cliquez sur **OK** pour poursuivre la configuration d'autres paramètres facultatifs. Pour plus d'informations, consultez la rubrique « Création d'un serveur virtuel ».

Pour lier une politique de liste d'URL au serveur virtuel d'équilibrage de charge SSL-Bridge

1. Accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, sélectionnez le serveur virtuel d'équilibrage de charge SSL-Bridge, puis cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies** .
5. Définissez les paramètres suivants.
   a) **Choisissez Policy.** Sélectionnez la politique de détection vidéo dans la liste déroulante.
   b) **Choisissez le type**. Sélectionnez le type de stratégie en tant que demande.
6. Cliquez sur **Continuer**.
7. Sélectionnez la stratégie de détection vidéo dans la liste, puis cliquez sur **Fermer**.

Configuration de la messagerie du journal d'audit

La journalisation des audits vous permet de passer en revue une condition ou une situation à n'importe quelle phase du processus de création d'une liste d'URL. Lorsqu'une appliance NetScaler reçoit une URL entrante, si la politique du répondeur comporte une expression de politique avancée URL Set, la fonction de journal d'audit collecte les informations relatives à l'ensemble d'URL dans l'URL et stocke les détails sous forme de message de journal pour toute cible autorisée par la journalisation des audits.

Le message du journal contient les informations suivantes :

1. Horodatage.
2. Type de message de journal.
3. Les niveaux de journalisation prédéfinis (Critique, Erreur, Notification, Avertissement, Informatif, Débogage, Alerte et Urgence).
4. Informations sur les messages du journal, telles que le nom de l'ensemble d'URL, l'action de politique, l'URL.

Pour configurer la journalisation des audits pour la fonctionnalité de liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message de journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, voir Journalisation des audits.

Sémantique de la liste d'URL

Le tableau suivant répertorie les modèles de correspondance d'URL et décrit comment les URL d'une liste d'URL sont mises en correspondance avec les URL des demandes entrantes. Par exemple, le modèle www.example.com/bar ne correspond qu'à une seule page sur www.example.com/bar. Pour faire correspondre toutes les pages dont l'URL commence par « www.example.com/bar », vous devez ajouter un astérisque (*) à la fin de l'URL.

Sémantique	Modèle d'URL	Correspondant	Incomparable
Correspondance de sous-domaines	domaine.com	domaine .com www.domain.com ; sub.one.domain.com	votredomaine.com ; wwwdomain.com
Correspondance d'URL, chemin exact	domain.com/exemple/bar/index.html	domain.com/exemple/bar/index.html ; www.domain.com/exemple/bar/index.html ; s.domain.com/exemple/bar/index.html	wwwdomaincom/example/bar/index domain.com/example/bar/index.html/
Correspondance d'URL, chemin exact	domain.com/exemple/l	domain.com/example/l html?key=valeur ; www.domain.com/exar s.domain.com/exemple	wwwdomaincom/example/bar/index do- main.com/example/bar/index.html/
Correspondance d'URL, correspondance de sous-chemins	domain.com/exemple/bar/	domain.com/exemple/bar/ ; do- main.com/exemple/bar/index.html www.domain.com/ example/bar/ index.html ; do- main.com/exemple/bar/index.html/one.jpg	wwwdomaincom/example/bar/index

Catégorisation des URL

May 5, 2023

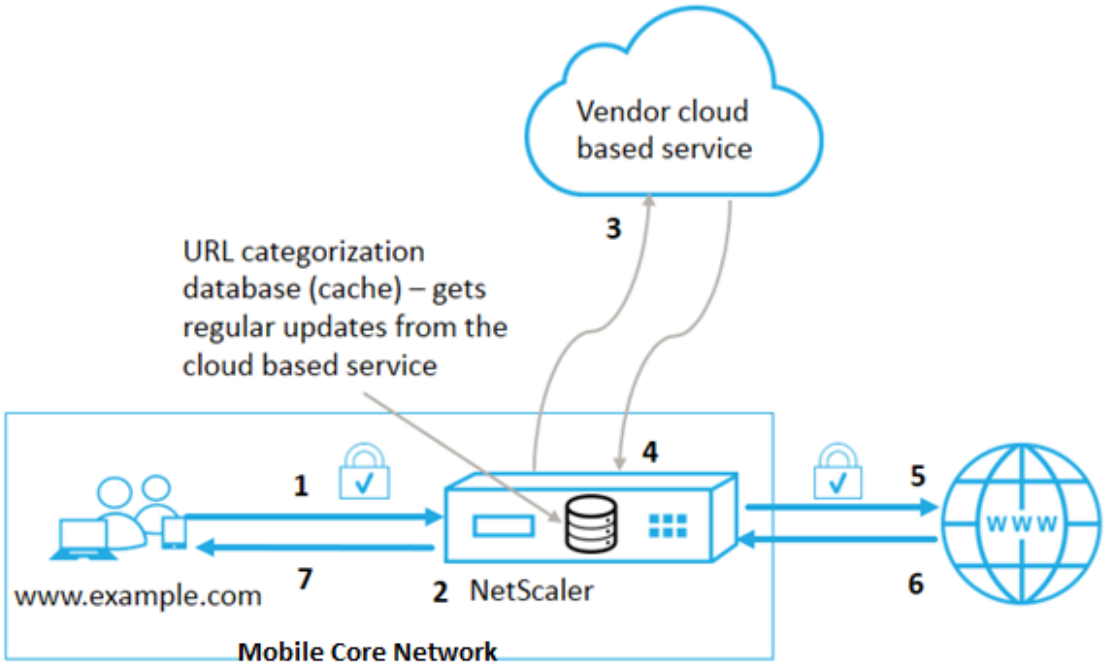
La catégorisation des URL limite l'accès des utilisateurs à des sites Web et à des catégories de sites Web spécifiques. En tant que service abonné en collaboration avec NetSTAR, la fonctionnalité permet aux entreprises clientes de filtrer le trafic Web à l'aide d'une base de données de catégorisation commerciale. La NetSTAR base de données contient un grand nombre (milliards) d'URL classées en différentes catégories, telles que les réseaux sociaux, les jeux de hasard, le contenu pour adultes, les

nouveaux médias et les achats. En plus de la catégorisation, chaque URL possède un score de réputation mis à jour en fonction du profil de risque historique du site. Nous pouvons utiliser NetSTAR les données pour filtrer le trafic en configurant des politiques avancées basées sur des catégories, des groupes de catégories (tels que le terrorisme, les drogues illégales) ou des scores de réputation du site.

Par exemple, vous pouvez bloquer l'accès à des sites dangereux, tels que des sites infectés par des logiciels malveillants, ou restreindre de manière sélective l'accès à du contenu réservé aux adultes ou à des contenus de divertissement en streaming.

Comment fonctionne la catégorisation des URL

La figure suivante montre comment le service de filtrage d'URL NetScaler est intégré à une base de données commerciale de catégorisation d'URL et à des services cloud pour des mises à jour fréquentes.



Les composants interagissent comme suit :

1. Le client envoie une demande d'URL liée à Internet.
2. Une politique NetScaler tente d'évaluer la demande en termes de détails de catégorisation (tels que la catégorie, le groupe de catégories et le score de réputation du site) extraits de la base de données de catégorisation des URL. Si la base de données renvoie les détails de la catégorie, le processus passe à l'étape 5.
3. Si la base de données ne renvoie pas de détails de catégorisation, la demande est envoyée à un

service de recherche basé sur le cloud géré par un fournisseur de catégorisation d'URL. Toutefois, l'appliance n'attend pas de réponse. Au lieu de cela, il marque l'URL comme Non classé et passe à l'étape 5. Cependant, il continue de surveiller les commentaires des requêtes dans le cloud et les utilise pour mettre à jour le cache afin que les requêtes futures puissent bénéficier de la recherche dans le cloud.

4. L'appliance NetScaler reçoit les détails de la catégorie d'URL (catégorie, groupe de catégories et score de réputation) du service basé sur le cloud et les stocke dans le cache cloud.
5. Si la politique autorise l'URL, la demande est envoyée au serveur d'origine. Dans le cas contraire, l'appliance supprime ou redirige la demande, ou répond par une page HTML personnalisée.
6. Le serveur d'origine répond avec les données demandées à l'appliance NetScaler.
7. L'appliance envoie la réponse au client.

Vous pouvez utiliser la fonction de filtrage des URL pour détecter les sites qui enfreignent les mandats d'utilisation sécurisée d'Internet émis par le gouvernement et mettre en œuvre des politiques pour bloquer ces sites. Sites hébergeant du contenu pour adultes, des médias en streaming ou des réseaux sociaux identifiés comme dangereux pour les enfants ou interdits comme illégaux.

Composants requis

La fonctionnalité fonctionne sur les plateformes de télécommunications avec l'achat d'une licence CBM de base et d'une licence CBM Premium et pour les autres plateformes NetScaler, la fonctionnalité fonctionne avec l'achat d'une licence CNS Premium.

Remarque : Outre une licence CBM Basic et une licence CBM Premium, l'appliance doit disposer d'une licence URL Threat Intelligence assortie d'un service d'abonnement d'une durée d'un an ou de trois ans. Avant d'activer et de configurer la fonctionnalité, vous devez installer les licences suivantes :

Support en matière de licences pour les plateformes de télécommunications :

- **CBM_TXXX_Server_Retail.lic**
- **CBM_TPRE_Server_Retail.lic**
- **CNS_WEBF_SSERVER_Retail.lic**

Où XXX est le débit, par exemple NetScaler T1000.

Support de licence pour d'autres plateformes NetScaler :

- **CNS_XXX_Server_PLT_Retail.lic**

Où XXX est le débit.

Expressions de politique de catégorisation d'URL

Le tableau suivant répertorie les différentes expressions de politique de catégorisation d'URL permettant d'identifier les URL entrantes et applique une action configurée.

Expression	Operation
<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)	Renvoie un objet URL_CATEGORY. Le score de réputation est un nombre de 1 à 4. Pour obtenir des objets, tous les scores de réputation utilisent 0,0 comme <min reputation> et . En cas est supérieur à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est inférieure à . En cas est supérieur à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est supérieure à . Si la catégorie ne parvient pas à résoudre en temps opportun, la valeur undef est renvoyée.
<url_category>. CATÉGORIE	Renvoie la chaîne de catégorie pour cet objet. Si l'URL ne comporte pas de catégorie ou si elle est mal formée, la valeur renvoyée est « Uncategorized ».
<url_category>. GROUPE	Renvoie une chaîne identifiant le groupe de catégories de l'objet. Il s'agit d'un regroupement de catégories de niveau supérieur, ce qui est utile dans les opérations qui nécessitent des informations moins détaillées sur la catégorie d'URL. Si l'URL ne comporte pas de catégorie ou si elle est mal formée, la valeur renvoyée est « Uncategorized ».
<url_category>. RÉPUTATION	Renvoie le score de réputation sous la forme d'un nombre compris entre 1 et 4, où 4 indique la réputation la plus risquée. Si la catégorie est « Non classé », la valeur de réputation est 2.

Exemples d'expressions de politique

Stratégie	Expressions de politique
Politique de sélection des demandes d'URL appartenant à la catégorie des moteurs de recherche	ajoute la politique de répondeur p1 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (0,0). CATEGORY.EQ (« Moteur de recherche »)
Politique de sélection des demandes d'URL appartenant au groupe de catégories Adultes	ajoute la politique de répondeur p1 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (0,0). GROUP.EQ (« Adulte ») '
Politique permettant de sélectionner les requêtes pour les URL des moteurs de recherche ayant un score de réputation égal à 4.	ajouter la politique de répondeur p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (4,0). CATEGORY.EQ (« Moteur de recherche ») '
Politique de sélection des requêtes pour les moteurs de recherche et les URL d'achats	ajouter une politique patset good_categories ; une politique de liaison good_categories « Moteur de recherche » ; une politique de liaison good_categories « Shopping » ; ajouter une politique de réponse p3 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (0,0). CATÉGORIE .EGALS_ANY (« good_categories »)
Politique permettant de sélectionner les requêtes pour les URL des moteurs de recherche ayant un score de réputation égal à 4.	ajouter la politique de répondeur p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE (4,0). CATEGORY.EQ (« Moteur de recherche »)

Actions relatives à la politique de catégorisation des URL

Une politique de filtrage des URL évalue le trafic afin d'identifier les demandes appartenant à une catégorie particulière. Le tableau suivant répertorie les actions que vous pouvez attribuer à une politique de filtrage d'URL.

Action politique	Groupe de politiques	Description
ALLOW	Répondeur	Autoriser la demande entrante à accéder à l'URL cible

Action politique	Groupe de politiques	Description
REDIRIGER	Répondeur	Redirigez la demande entrante vers l'URL spécifiée comme cible.
DENY	Répondeur	Refuser la demande entrante.
RÉINITIALISER	Répondeur, optimisation vidéo	Réinitialisez la connexion.
ABANDONNER	Répondeur, optimisation vidéo	Supprimer la connexion.

> **Remarque**
>
> Pour le trafic crypté, la politique d'optimisation vidéo inclut des actions qui implémentent les actions de filtrage des URL.

Configuration de la catégorisation des URL

Pour configurer la catégorisation des URL, commencez par activer la fonctionnalité de filtrage des URL. Vous devez ensuite configurer les limites de mémoire cache, la politique de catégorisation et les serveurs virtuels pour le trafic HTTP et HTTPS. Configuration de la catégorisation des URL à l'aide de l'interface de ligne de commande.

Pour utiliser la CLI et configurer la catégorisation des URL sur une appliance NetScaler, procédez comme suit :

- Configurez la catégorisation des URL.
  - Activez la fonctionnalité de filtrage des URL.
  - Configurez la mémoire partagée pour limiter la mémoire cache.
  - Configurez les paramètres de catégorisation d'URL.
- Configurez la catégorisation des URL pour le trafic HTTP.
  - Ajoutez des actions de catégorisation d'URL.
  - Ajoutez des politiques de catégorisation des URL.
  - Ajoutez un serveur virtuel d'équilibrage de charge pour le trafic HTTP.
  - Liez les politiques de catégorisation d'URL au serveur virtuel d'équilibrage de charge.
- Configurez la catégorisation des URL pour le trafic HTTPS.
  - Ajoutez des politiques de catégorisation des URL.
  - Ajoutez un serveur virtuel d'équilibrage de charge SSL Bridge.
  - Liez les politiques de catégorisation d'URL au serveur virtuel d'équilibrage de charge.

Configuration de la catégorisation des URL

Pour configurer la fonctionnalité, vous devez activer la fonctionnalité de catégorisation des URL, configurer les paramètres de filtrage et définir la limite de mémoire partagée.

Pour activer la fonctionnalité de filtrage des URL

À l'invite de commande, tapez :

```
enable ns feature URLFiltering VideoOptimization Responder IC SSL AppFlow
```

Pour configurer la limite de mémoire partagée

À l'invite de commande, tapez :

```
set cache parameter [-memLimit <megaBytes>]
<!--NeedCopy-->
```

Où MemLimit est la limite de mémoire pour la mise en cache.

Exemple :

```
set cache parameter -memLimit 10
```

Pour configurer les paramètres de catégorisation des URL

À l'invite de commande, tapez :

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>]
   [-TimeOfDayToUpdateDB <HH:MM>]
<!--NeedCopy-->
```

***Exemple :**

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00
```

Configuration de la catégorisation des URL pour le trafic HTTP

Pour configurer la fonctionnalité de catégorisation des URL pour le trafic HTTP, vous devez configurer un serveur virtuel d'équilibrage de charge, ajouter des politiques de catégorisation des URL et lier les politiques au serveur virtuel. Ce faisant, le serveur virtuel reçoit le trafic HTTP et, en fonction de l'évaluation des politiques, le système attribue une action de filtrage.

Pour ajouter une action de catégorisation d'URL pour le trafic HTTP

À l'invite de commande, tapez :

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string
>] [-responseStatusCode <positive_integer>] [-reasonPhrase <string>]
```

Exemple :

```
add responder action act_url_categorize respondwith "\"HTTP/1.1 200 OK\r\n\
r\n\" + HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY
 + \"\n\""
```

Pour ajouter une politique de catégorisation d'URL pour le trafic HTTP

À l'invite de commande, tapez :

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
string>] [-logAction <string>] [-appflowAction <string>]
```

Exemple :

```
add responder policy pol_url_categorize_http "HTTP.REQ.HOSTNAME.APPEND(
HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Adult\")|| HTTP.REQ.HOSTNAME.
APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Gambling\")"RESET
```

Pour ajouter un serveur virtuel d'équilibrage de charge HTTP

Si aucun serveur virtuel pour le trafic HTTP n'est déjà configuré, à l'invite de commande, tapez :

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-clt Timeout
<secs>]
```

Exemple :

```
add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout 120
```

Pour lier la politique de catégorisation des URL au serveur virtuel d'équilibrage de charge

À l'invite de commande, tapez :

```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```

Exemple :

```
bind lb vserver vsrv-HTTP -policyName pol_url_categorize_http -priority 10
-gotoPriorityExpression END -type REQUEST
```


Configuration de la catégorisation des URL pour le trafic HTTPS

Pour configurer la fonctionnalité de catégorisation d'URL pour le trafic HTTPS, vous devez configurer un serveur virtuel d'équilibrage de charge SSL Bridge, ajouter des politiques de catégorisation d'URL et lier les politiques au serveur virtuel SSL-Bridge. Ce faisant, le serveur reçoit le trafic HTTPS et, en fonction de l'évaluation des politiques, le système attribue une action de filtrage.

Pour ajouter une politique de catégorisation d'URL pour le trafic HTTPS

À l'invite de commande, tapez :

```
add videooptimization detectionpolicy <name> -rule <expression> -action <
string> [-undefAction <string>] [-comment <string>] [-logAction <string>]
```

Exemple :

```
add videooptimization detectionpolicy pol_url_categorize_https_block_adult -
rule "CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(0,0).CATEGORY.EQ("Adult")' -
action RESET
```

Pour ajouter un serveur virtuel d'équilibrage de charge SSL-Bridge

À l'invite de commande, tapez :

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT imeout
<secs>]
```

Exemple :

```
add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -cltTimeout
 180
```

Pour lier la politique de catégorisation au serveur virtuel SSL-Bridge

À l'invite de commande, tapez :

```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```

Exemple :

```
bind lb vserver vsrv-HTTPS -policyName pol_url_categorize_https_block_adult
 -priority 20 -type REQUEST
```

Configuration de la catégorisation des URL à l'aide de l'interface graphique

L'interface graphique vous permet de :

- Activez la fonctionnalité de catégorisation des URL.
- Ajoutez des actions de catégorisation d'URL pour le trafic HTTP.
- Ajoutez des politiques de catégorisation d'URL pour le trafic HTTP.
- Ajoutez des politiques de catégorisation d'URL pour le trafic HTTPS.
- Ajoutez un serveur virtuel d'équilibrage de charge pour le trafic HTTP.
- Ajoutez un serveur virtuel d'équilibrage de charge via un pont SSL pour le trafic HTTPS.
- Liez les politiques de catégorisation d'URL au serveur virtuel d'équilibrage de charge.
- Liez les politiques de catégorisation d'URL au serveur virtuel d'équilibrage de charge SSL-Bridge.
- Configurez la limite de mémoire partagée.
- Configurez les paramètres de catégorisation d'URL.

Pour activer la catégorisation des URL

1. Dans le volet de navigation, ouvrez **Système**, puis cliquez sur **Paramètres**.
2. Sur la page **Paramètres**, cliquez sur le lien **Configurer les fonctionnalités avancées** .
3. Sur la page **Configurer les fonctionnalités avancées**, cochez la case **Filtrage des URL** .
4. Cliquez sur **OK** et sur **Fermer**.

Pour ajouter une action de catégorisation d'URL

1. **Dans le volet de navigation, ouvrez**AppExpert**>**Responder > Action**.**
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer une action de répondeur**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action de politique de catégorisation des URL.
   b) **Tapez**. Sélectionnez un type d'action.
   c) **Expression** : Utilisez l'éditeur d'expressions pour créer l'expression de politique.
   d) **Commentaires**. Brève description de l'action politique.
4. Cliquez sur **Créer** et **Fermer**.

Pour ajouter une politique de catégorisation d'URL pour le trafic HTTP

1. **Dans le volet de navigation, ouvrez**AppExpert**>**Responder > Policies**.**
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Sur la page **Créer une politique de répondeur**, définissez les paramètres suivants.
   a) **Nom**. Nom de l'action de politique de catégorisation des URL.
   b) **Action**. Sélectionnez l'action de catégorisation d'URL que vous préférez associer à la politique.
   c) **Action de journalisation**. Sélectionnez l'action de journalisation.
   d) **AppFlow**. Sélectionnez une action AppFlow.

e) **Expression** : Utilisez l'éditeur d'expressions pour créer l'expression de politique.
f) **Commentaires**. Brève description de l'action politique.

4. Cliquez sur **Créer** et **Fermer**.

Pour ajouter une politique de catégorisation pour le trafic HTTPS

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configuration**>**Optimisation > Optimisation****vidéo** > **Détection**.**
2. Sur la page **Détection**, cliquez sur le lien **Politiques de détection pour l'optimisation vidéo** .
3. Sur la page Politiques de détection pour l'optimisation vidéo, cliquez sur **Ajouter**.
4. Sur la page **Créer une politique de détection pour l'optimisation vidéo**, définissez les paramètres suivants.
   a) **Nom**. Nom de la stratégie d'optimisation
   b) **Expression** : Configurez la politique à l'aide d'expressions personnalisées.
   c) **Action**. Action d'optimisation associée à la stratégie pour gérer le trafic vidéo entrant.
   d) **Action du UNDEF.** Événement non défini si la demande entrante ne correspond pas à la stratégie d'optimisation.
   e) **Commentaire**. Brève description de la politique.
   f) **Action de journalisation.** Sélectionnez une action du journal d'audit qui spécifie l'action à effectuer pour les messages du journal.
5. Cliquez sur **Créer** et **Fermer**.

Pour ajouter un serveur virtuel d'équilibrage de charge pour le trafic HTTP

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Serveur virtuel d'équilibrage** de charge, définissez les paramètres suivants :
   a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
   b) **Protocole**. Choisissez le type de protocole HTTP.
   c) **Type d'adresse IP.** IPv4 ou IPv6.
   d) **Adresse IP.** IPv4 ou IPv6, adresse VIP attribuée au serveur virtuel.
   e) **Port**. Numéro de port du serveur virtuel.
4. Cliquez sur **OK** pour poursuivre la configuration d'autres paramètres facultatifs.
5. Cliquez sur **Créer** et **Fermer**.

Pour ajouter un serveur virtuel d'équilibrage de charge SSL Bridge

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Sur la page **Serveur virtuel d'équilibrage** de charge, définissez les paramètres suivants :

a) **Nom**. Nom du serveur virtuel d'équilibrage de charge.
b) **Protocole**. Sélectionnez le type de protocole en tant que pont SSL.
c) **Type d'adresse IP**. Type adressable par IP.
d) **Adresse IP**. Adresse IP 4 ou IP6 attribuée au serveur virtuel.
e) **Port**. Numéro de port du serveur virtuel.

4. Cliquez **sur OK** pour poursuivre la configuration des autres paramètres facultatifs.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour lier une politique de catégorisation d'URL au serveur virtuel d'équilibrage de charge HTTP

1. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, sélectionnez le serveur virtuel d'équilibrage de charge et cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Stratégies**, cliquez sur l'icône **+** pour accéder au curseur **Stratégies** .
5. Définissez les paramètres suivants.
   a) **Choisissez Policy**. Sélectionnez la politique de catégorisation des URL dans la liste déroulante.
   b) **Choisissez le type**. Sélectionnez le type de stratégie en tant que demande.
6. Cliquez sur **Continuer**.
7. Sélectionnez la politique de catégorisation des URL dans la liste et cliquez sur **Fermer**.

Pour lier une politique de catégorisation au serveur virtuel d'équilibrage de charge SSL-Bridge

1. Accédez à l'écran **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** .
2. Dans le volet de détails, sélectionnez le serveur virtuel d'équilibrage de charge SSL-Bridge, puis cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
4. Dans la section **Politiques**, cliquez sur l'icône **+** pour accéder au curseur **Politiques** .
5. Dans la section **Stratégies**, définissez les paramètres suivants.
   a) **Choisissez Policy**. Sélectionnez la politique de détection vidéo dans la liste déroulante.
   b) **Choisissez le type**. Sélectionnez le type de stratégie en tant que demande.
6. Cliquez sur **Continuer**.
7. Sélectionnez la stratégie de détection vidéo dans la liste, puis cliquez sur **Fermer**.

Pour configurer la limite de mémoire partagée

1. Connectez-vous à l'appliance et accédez à **Optimisation** > Mise en **cache intégrée**.
2. Dans le volet de détails, cliquez sur **le lien Modifier les paramètres du cache** .

3. Sur la page **Paramètres généraux du cache**, définissez les paramètres suivants.
   a) **Limite d'utilisation de la mémoire (Mo).**
   b) **Limite d'utilisation de la mémoire active**.
   c) **Via l'en-tête**.
   d) **Longueur maximale du corps du message à mettre en cache**
   e) **Action globale à résultat non défini**
   f) **Activer la persistance des objets HA**
   g) **Vérifier la persistance de l'objet mis en cache**
   h) **Préfetches**
4. Cliquez sur **OK** et sur **Fermer**.

Pour configurer les paramètres de catégorisation des URL

1. Connectez-vous à l'appliance et accédez à **Sécurité**.
2. Dans le volet de détails, cliquez sur le lien **Modifier les paramètres de filtrage des URL** .
3. Sur la page **Configuration des paramètres de filtrage d'URL**, définissez les paramètres suivants.
   a) Heures entre les mises à jour des bases Heures de filtrage d'URL entre les mises à jour de Valeur minimale : 0 et valeur maximale : 720.
   b) Heure de mise à jour de la base de données. Heure du jour du filtrage des URL pour mettre à jour la base de données.
4. Cliquez sur **OK** et sur **Fermer.**

Configuration de la messagerie du journal d'audit

Lorsqu'une appliance NetScaler reçoit une URL entrante, si la politique du répondeur comporte une expression de filtrage des URL, la fonctionnalité du journal d'audit collecte des informations de catégorisation et les affiche sous forme de messages de journal sur n'importe quel serveur de journal d'audit cible configuré. Les informations sont enregistrées.

- Adresse IP source (adresse IP du client qui a fait la demande).
- Adresse IP de destination (adresse IP du serveur demandé).
- URL demandée contenant le schéma, l'hôte et le nom de domaine (`http://www.example.com`).
- Catégorie d'URL renvoyée par le cadre de filtrage d'URL.
- Groupe de catégories d'URL renvoyé par le cadre de filtrage d'URL.
- Numéro de réputation d'URL renvoyé par le cadre de filtrage d'URL.
- Action du journal d'audit prise conformément à la politique de catégorisation des URL.

Pour configurer la journalisation d'audit pour la fonctionnalité Liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message de journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, consultez la rubrique Audit Logging .

Stockage des erreurs d'échec à l'aide de la messagerie SYSLOG

À n'importe quel stade du processus de filtrage des URL, en cas de défaillance au niveau du système, l'appliance NetScaler utilise le mécanisme des journaux d'audit pour stocker les journaux dans le fichier ns.log. Les erreurs sont stockées sous forme de messages texte au format SYSLOG afin qu'un administrateur puisse les consulter ultérieurement dans un ordre chronologique d'occurrence des événements. Ces journaux sont également envoyés à un serveur SYSLOG externe pour archivage. Pour plus d'informations, consultez l'article CTX229399.

Par exemple, si un échec se produit lorsque vous initialisez le SDK de filtrage d'URL, le message d'erreur est stocké dans le format de messagerie suivant.

3 octobre 15:43:40 <local0.err> ns URLFiltrage [1349] : Erreur lors de l'initialisation du SDK NetStar (erreur SDK =-1). (statut = 1).

L'appliance NetScaler stocke les messages d'erreur dans quatre catégories d'échec différentes :

- Échec du téléchargement. Si une erreur se produit lorsque vous tentez de télécharger la base de données de catégorisation.
- échec de l'intégration. Si une erreur se produit lors de l'intégration d'une mise à jour dans la base de données de catégorisation existante.
- Échec d'initialisation. Si une erreur se produit lorsque vous initialisez la fonctionnalité de catégorisation d'URL, définissez des paramètres de catégorisation ou mettez fin à un service de catégorisation.
- Échec de récupération. Si une erreur se produit lorsque l'appliance récupère les détails de catégorisation de la demande.

Score de réputation d'URL

La fonction de catégorisation d'URL fournit un contrôle basé sur des stratégies pour restreindre les URL sur la liste rouge. Vous pouvez contrôler l'accès aux sites Web en fonction de la catégorie d'URL, du score de réputation ou de la catégorie d'URL et du score de réputation. Si un administrateur réseau surveille un utilisateur accédant à des sites Web à haut risque, il peut utiliser une politique de réponse liée au score de réputation des URL pour bloquer ces sites Web à risque.

À la réception d'une demande d'URL entrante, la solution matérielle-logicielle récupère la catégorie et le score de réputation dans la base de données de catégorisation des URL. En fonction du score de réputation renvoyé par la base de données, la solution matérielle-logicielle attribue une note de

réputation aux sites Web. La valeur peut aller de 1 à 4, 4 étant le type de site Web le plus risqué, comme indiqué dans le tableau suivant.

Évaluation de la réputation des URL	Commentaire de réputation
1	Site propre.
2	Site inconnu.
3	Potentiellement dangereux ou affilié à un site dangereux.
4	Site malveillant.

FAQ

May 5, 2023

Cette section fournit la FAQ sur les fonctionnalités suivantes de NetScaler

- Partition d'administration
- AppFlow
- Call Home
- Mise en cluster
- Gestion des connexions
- Commutation de contenu
- Débogage
- Matériel
- Haute disponibilité
- Mise en cache intégrée
- Installation, mise à niveau et rétrogradation
- Équilibrage de charge
- Interface graphique NetScaler
- SSL

Partition d'administration

May 5, 2023

Où puis-je obtenir le fichier de configuration NetScaler pour une partition ?

Le fichier de configuration (*ns.conf*) de la partition par défaut est disponible dans le répertoire */nsconfig.* <partitionName>Pour les partitions d'administration, le fichier est disponible dans le répertoire */nsconfig/partitions/* .

Comment configurer la mise en cache intégrée dans une appliance NetScaler partitionnée ?

> **Remarque**
>
> La mise en cache intégrée dans les partitions d'administration est prise en charge à partir de NetScaler 11.0.

Pour configurer la mise en cache intégrée sur un NetScaler partitionné, après avoir défini la mémoire IC sur la partition par défaut, le superutilisateur peut configurer la mémoire IC sur chaque partition d'administration de telle sorte que la mémoire IC totale allouée à toutes les partitions d'administration ne dépasse pas la mémoire IC définie sur la partition par défaut. La mémoire qui n'est pas configurée pour les partitions d'administration reste disponible pour la partition par défaut.

Par exemple, si une appliance NetScaler dotée de deux partitions d'administration dispose de 10 Go de mémoire IC alloués à la partition par défaut et que l'allocation de mémoire IC pour les deux partitions d'administration est la suivante :

- Partition 1 : 4 Go
- Partition 2 : 3 Go

Ensuite, la partition par défaut dispose de 10 - (4 + 3) = 3 Go de mémoire IC disponible pour l'utilisation.

> **Remarque**
>
> Si toute la mémoire IC est utilisée par les partitions d'administration, aucune mémoire IC n'est disponible pour la partition par défaut.

Quelle est la portée des paramètres L2 et L3 dans les partitions d'administration ?

> **Remarque**
>
> - Applicable à partir de NetScaler 11.0.
> - Pour que l'ARP fonctionne dans une partition autre que celle par défaut, vous devez activer le paramètre « ProxyARP » dans la commande « set l2param ».

Sur une appliance NetScaler partitionnée, l'étendue de la mise à jour des paramètres L2 et L3 est la suivante :

- Pour les paramètres L2 définis à l'aide de la commande « set L2Param », les paramètres suivants ne peuvent être mis à jour qu'à partir de la partition par défaut, et leurs valeurs sont applicables

à toutes les partitions d'administration :

MaxBridge Collision, BDGSetting, GarponVRIDintF, GarpReply, ProxyARP, Reset Interface On-Hafailover et skip_proxying_bsd_traffic.

Les autres paramètres L2 peuvent être mis à jour dans des partitions d'administration spécifiques, et leurs valeurs sont locales à ces partitions.

- Pour les paramètres L3 définis à l'aide de la commande « set L3Param », tous les paramètres peuvent être mis à jour dans des partitions d'administration spécifiques, et leurs valeurs sont locales à ces partitions. De même, les valeurs mises à jour dans la partition par défaut s'appliquent uniquement à la partition par défaut.

Comment activer le routage dynamique dans une partition d'administration ?

> **Remarque**
>
> Le routage dynamique dans les partitions d'administration est pris en charge à partir de NetScaler 11.0.

Alors que le routage dynamique (OSPF, RIP, BGP, ISIS, BGP+) est activé par défaut sur la partition par défaut, dans une partition d'administration, il doit être activé à l'aide de la commande suivante :

```
> set L3Param -dynamicRouting ENABLED
```

> **Remarque**
>
> Un maximum de 63 partitions peuvent exécuter le routage dynamique (62 partitions d'administration et 1 partition par défaut).

Lors de l'activation du routage dynamique sur une partition d'administration, un routeur virtuel (VR) est créé.

- <partition-name>Chaque VR gère son propre vlan0 qui sera affiché sous la forme vlan0_.
- Toutes les adresses IP indépendantes qui sont exposées à ZEBOS sont liées à vlan0.
- La VR par défaut (de la partition par défaut) affiche toutes les VR configurées.
- La VR par défaut affiche les VLAN qui sont liés à ces VR (à l'exception des VLAN par défaut).

Où puis-je trouver les journaux d'une partition ?

Les journaux NetScaler ne sont pas spécifiques à une partition. Les entrées du journal pour toutes les partitions doivent être stockées dans le répertoire */var/log/.*

Comment puis-je obtenir les journaux d'audit d'une partition d'administration ?

Dans un NetScaler partitionné, vous ne pouvez pas disposer de serveurs de journaux spécifiques pour une partition spécifique. Les serveurs définis à la partition par défaut sont applicables à toutes les par-

titions d'administration. Par conséquent, pour afficher les journaux d'audit d'une partition spécifique, vous devez utiliser la commande « afficher les messages d'audit ».

> **Remarque**
>
> Les utilisateurs d'une partition d'administration n'ont pas accès au shell et ne peuvent donc pas accéder aux fichiers journaux.

Comment puis-je obtenir les journaux Web d'une partition d'administration ?

Vous pouvez obtenir les journaux Web d'une partition d'administration comme suit :

- **Pour NetScaler 11.0 et versions ultérieures**

  La fonctionnalité de journalisation Web doit être activée sur chacune des partitions nécessitant une journalisation Web. À l'aide du client NetScaler Web Logging (NSWL), NetScaler extrait les journaux Web de toutes les partitions auxquelles l'utilisateur est associé.

- **Pour les versions antérieures à NetScaler 11.0**

  Les journaux Web ne peuvent être obtenus que par `nsroot` d'autres superutilisateurs. De plus, même si la journalisation Web est activée sur la partition par défaut, le client NetScaler Web Logging (NSWL) extrait les journaux Web pour toutes les partitions.

Pour afficher la partition de chaque entrée de journal, personnalisez le format du journal pour inclure l'option %P. Vous pouvez ensuite filtrer les journaux pour afficher les journaux d'une partition spécifique.

Comment puis-je obtenir la trace d'une partition d'administration ?

Vous pouvez obtenir la trace d'une partition d'administration comme suit :

- **Pour NetScaler 11.0 et versions ultérieures**

  Dans une appliance NetScaler partitionnée, l' `nstrace` opération peut être effectuée sur des partitions d'administration individuelles. <partitionName>Les fichiers de trace sont stockés dans le répertoire*/var/partitions/ /nstrace/*.

  Remarque : Vous ne pouvez pas obtenir la trace d'une partition d'administration à l'aide de l'interface graphique. Vous devez utiliser l'interface de ligne de commande.

- **Pour les versions antérieures à NetScaler 11.0**

  L' `nstrace` opération ne peut être effectuée que sur la partition par défaut. Par conséquent, les captures de paquets sont disponibles pour l'ensemble du système NetScaler. Pour obtenir des captures de paquets spécifiques à une partition, utilisez des filtres basés sur VLAN-ID.

Comment puis-je obtenir le pack de support technique spécifique à une partition d'administration ?

Pour obtenir le bundle de support technique pour une partition spécifique, exécutez la commande suivante depuis la partition par défaut :

```
> show techsupport -scope partition <partitionName>
```

Remarque : Cette commande fournit également des informations spécifiques au système.

AppFlow

May 5, 2023

- **Quelle version de NetScaler prend en charge AppFlow ?**

  AppFlow est pris en charge sur les appliances NetScaler exécutant la version 9.3 et les versions ultérieures avec nCore build.

- **Quel est le format utilisé par AppFlow pour transmettre les données ?**

  AppFlow transmet les informations au format IPFIX (Internet Protocol Flow Information Export), qui est une norme ouverte de l'Internet Engineering Task Force (IETF) définie dans la RFC 5101. IPFIX (la version normalisée de NetFlow de Cisco) est largement utilisé pour surveiller les informations de flux réseau.

- **Que contiennent les enregistrements AppFlow ?**

  Les enregistrements AppFlow contiennent des informations NetFlow ou IPFIX standard, telles que les horodatages pour le début et la fin d'un flux, le nombre de paquets et le nombre d'octets. Les enregistrements AppFlow contiennent également des informations au niveau de l'application (telles que les URL HTTP, les méthodes de requête HTTP et les codes d'état de réponse, le temps de réponse du serveur et la latence). Les enregistrements de flux IPFIX sont basés sur des modèles qui doivent être envoyés avant d'envoyer des enregistrements de flux.

- **Après une mise à niveau vers NetScaler Version 9.3 Build 48.6 Cl, pourquoi une tentative d'ouverture d'un serveur virtuel à partir de l'interface graphique entraîne-t-elle le message d'erreur « La fonctionnalité AppFlow n'est disponible que sur NetScaler Ncore » ?**

  AppFlow est pris en charge uniquement sur les appliances nCore. Lorsque vous ouvrez l'onglet Configuration du serveur virtuel, désactivez la case à cocher **AppFlow** .

- **Que contient l'ID de transaction dans un enregistrement AppFlow ?**

  Un ID de transaction est un numéro 32 bits non signé identifiant une transaction au niveau de l'application. Pour HTTP, une transaction correspond à une paire demande/réponse. Tous les

enregistrements de flux qui correspondent à cette paire demande et réponse ont le même ID de transaction. Une transaction type comporte quatre enregistrements de flux. Si NetScaler génère lui-même la réponse (fournie à partir du cache intégré ou par une politique de sécurité), il se peut qu'il n'y ait que deux enregistrements de flux pour la transaction.

- **Qu' est-ce qu'une action AppFlow ?**

  Une action AppFlow est un ensemble de collecteurs auxquels les enregistrements de flux sont envoyés si la stratégie AppFlow associée correspond.

- **Quelles commandes puis-je exécuter sur l'appliance NetScaler pour vérifier que l'action AppFlow est un succès ?**

  L'action Afficher AppFlow. Par exemple :

```
> show appflow action
1) Name: aFL-act-collector-1
  Collectors: collector-1
  Hits: 0
  Action Reference Count: 2
 2) Name: apfl-act-collector-2-and-3
  Collectors: collector-2, collecter-3
  Hits: 0
  Action Reference Count: 1
 3) Name: apfl-act-collector-1-and-3
  Collectors: collector-1, collecter-3
  Hits: 0
  Action Reference Count: 1
<!--NeedCopy-->
```

- **Qu'est-ce qu'un collecteur AppFlow ?**

Un collecteur reçoit les enregistrements de flux générés par l'appliance NetScaler. Pour pouvoir envoyer des enregistrements de flux, vous devez spécifier au moins un collecteur. Vous pouvez en spécifier jusqu'à quatre. Vous pouvez supprimer les collecteurs non utilisés.

- **Quelle version de NetScaler est requise pour utiliser AppFlow ?**

  Utilisez NetScaler version 9.3.49.5 ou supérieure et n'oubliez pas qu'AppFlow n'est disponible que dans les versions nCore.

- **Quel est le protocole de transport utilisé par AppFlow ?**

  AppFlow utilise le protocole UDP comme protocole de transport.

- **Quels ports doivent être ouverts si mon réseau est équipé d'un pare-feu ?**

  Port 4739. Il s'agit du port UDP par défaut utilisé par le collecteur AppFlow pour écouter des

messages IPFIX. Si l'utilisateur modifie le port par défaut, ce port doit être ouvert sur le pare-feu.

- **Comment puis-je modifier le port par défaut utilisé par AppFlow ?**

  Lorsque vous ajoutez un collecteur AppFlow à l'aide de la commande add AppFlowCollector, vous pouvez spécifier le port à utiliser.

```
1  > add appflowCollector coll1 -IPAddress 10.102.29.251 -port 8000
2   Done
3  <!--NeedCopy-->
```

- **À quoi sert le paramètre ClientTrafficOnly ?**

  NetScaler génère des enregistrements AppFlow uniquement pour le trafic côté client.

- **Combien de collecteurs peuvent être configurés à la fois ?**

  Vous pouvez configurer jusqu'à quatre collecteurs AppFlow à la fois sur l'appliance NetScaler. Notez que le nombre maximum de collecteurs pouvant être configurés sur une appliance NetScaler est de quatre.

Call Home

June 2, 2023

- **Qu'est-ce que Call Home sur une appliance NetScaler ?**

  Call Home surveille et signale les événements critiques sur une appliance NetScaler. En activant Call Home, vous pouvez automatiser le processus de notification d'erreur. Vous évitez non seulement d'appeler le support NetScaler, de faire une demande de service et de télécharger des données système avant que le support NetScaler ne puisse résoudre le problème, mais vous pouvez également identifier et résoudre les problèmes avant qu'ils ne surviennent.

- **Call Home est-il activé par défaut sur une appliance NetScaler ?**

  Oui, Call Home est activé par défaut sur l'appliance. Si vous effectuez une mise à niveau vers la dernière version du logiciel à partir d'une version antérieure dans laquelle Call Home était désactivé par défaut, le processus de mise à niveau active automatiquement cette fonctionnalité. Si vous décidez ultérieurement de le désactiver, le paramètre mis à jour est mémorisé pour toutes les mises à niveau ultérieures. Pour plus d'informations, voir Call Home.

- **Quelles sont les conditions préalables pour que Call Home fonctionne ?**

  Accès à une connexion Internet.

Remarque : Si votre appliance NetScaler ne dispose pas d'une connexion Internet, vous pouvez configurer un serveur proxy via lequel NetScaler peut générer des journaux système et les télécharger sur le serveur de support technique Citrix (CIS).

- **Quels sont les avantages de l'utilisation de Call Home ?**
  - Surveillez les conditions d'erreur matérielles et logicielles.
  - Avertissez l'apparition d'événements critiques qui ont un impact sur votre réseau.
  - Envoyez des données de performances et des journaux système à Citrix à l'adresse suivante :
    * Analysez et améliorez la qualité des produits.
    * Fournir des informations de dépannage en temps réel pour une identification proactive des problèmes et une résolution plus rapide des problèmes.
- **Quelle version du logiciel NetScaler prend en charge Call Home ?**

  NetScaler versions 10.0 et ultérieures.
- **Quels modèles de plateforme NetScaler prennent en charge Call Home ?**

  La fonction Call Home est activée par défaut sur toutes les plateformes NetScaler et tous les modèles d'appliances (MPX, VPX et SDX).
  - NetScaler MPX : Tous les modèles MPX.
  - NetScaler VPX : Tous les modèles VPX. En outre, il est pris en charge sur les appliances VPX qui obtiennent leurs licences à partir de pools de licences externes ou centraux. Toutefois, la fonctionnalité reste la même que pour une appliance VPX standard.
  - NetScaler SDX : surveille le lecteur de disque et les puces SSL attribuées pour détecter toute erreur ou défaillance. Toutefois, les instances VPX n'ont pas accès au bloc d'alimentation (PSU) et leur état n'est donc pas surveillé. Sur une plateforme SDX, vous pouvez configurer Call Home soit directement sur une instance individuelle, soit par l'intermédiaire de la SVM.
- **Dois-je configurer l'alarme SNMP pour Call Home afin de signaler les conditions d'erreur ?**

  Non, il n'est pas nécessaire de configurer le protocole SNMP pour Call Home pour surveiller les conditions d'erreur, car les téléchargements SNMP et Call Home sont indépendants l'un de l'autre. Si vous souhaitez être averti chaque fois qu'une condition d'erreur survient, vous pouvez configurer l'alarme SNMP CALLHOME-UPLOAD-EVENT pour générer une alerte SNMP chaque fois qu'un téléchargement de Call Home a lieu. L'alerte SNMP informe l'administrateur local de la survenue d'événements critiques.
- **Comment contacter un support technique ?**

  Pour tous les événements critiques liés au matériel, Call Home crée automatiquement une demande de service à NetScaler. Pour les autres erreurs, après avoir consulté les journaux système, vous pouvez contacter l'équipe de support technique de NetScaler pour ouvrir une de-

mande de service en vue d'une enquête plus approfondie. Pour contacter le support, rendez-vous sur https://www.netscaler.com/resources/support.

- **Quelles sont les conditions d'erreur surveillées par Call Home dans une appliance NetScaler ?**

  Call Home prend en charge la surveillance des événements suivants dans une appliance NetScaler :

  - Erreurs de lecteur flash compact
  - Erreurs de disque dur
  - Panne du bloc d'alimentation
  - Panne de carte SSL
  - Redémarrage à chaud
  - Anomalies de mémoire
  - Baisse de la limite de taux

- **Avez-vous besoin d'une licence distincte pour Call Home ?**

  Non, Call Home ne nécessite pas de licence distincte. Vous pouvez l'activer dans toutes les licences de la plateforme NetScaler.

- **Quelles sont les données que Call Home envoie au serveur de support NetScaler et à quelle fréquence sont-elles envoyées ?**

  Call Home collecte et envoie deux types de données au CIS. Ils sont :

  - Informations système de base (version NetScaler en cours d'exécution, mode de déploiement (autonome, HA, cluster), détails matériels, etc.). Il est envoyé au moment de l'enregistrement de Call Home et dans le cadre des pulsations cardiaques périodiques. Le rythme cardiaque est envoyé tous les 30 jours, mais vous pouvez configurer cet intervalle entre 1 et 30 jours. Cependant, une valeur inférieure à 5 jours n'est pas recommandée, car les chargements fréquents ne sont généralement pas très utiles.
  - Une version abrégée de la condition `show tech support bundle` lorsqu'il y a une erreur. Il est envoyé lors de la première apparition d'une condition d'erreur particulière depuis le dernier démarrage de l'appliance. Autrement dit, une réoccurrence de la même condition d'erreur ne déclenche pas un autre chargement à moins que l'appliance ait été redémarrée après l'occurrence précédente.

- **Call Home peut-il générer et télécharger des journaux système via un serveur proxy ?**

  Oui. Si votre appliance NetScaler ne dispose pas d'une connexion Internet directe, vous pouvez configurer un serveur proxy et télécharger les journaux système sur le serveur de support technique Citrix (CIS).

- **Puis-je consulter les données de Call Home avant qu'elles ne soient envoyées à SIC ?**

Malheureusement, vous ne pouvez pas consulter les Call Home avant d'être envoyées à SIC. Call Home ne collecte aucune autre donnée en plus de celles que vous fournirez lorsque vous contacterez l'équipe d'assistance de NetScaler.

- **Dans quelle mesure les téléchargements Call Home sont-ils sécurisés et privés ?**

  Call Home assure la sécurité et la confidentialité des données de la manière suivante :

  - Utilise un canal SSL/TLS sécurisé pour transférer des données vers des serveurs Citrix.
  - Les données téléchargées sont examinées uniquement par le personnel autorisé et ne sont partagées avec aucun tiers.

Mise en cluster

August 20, 2021

Cliquez ici pour consulter les questions fréquentes sur le clustering.

Gestion des connexions

May 5, 2023

- **Qu'est-ce qu'une connexion administrateur ?**

  Une connexion administrateur établit une connexion à l'adresse NSIP et permet aux administrateurs de configurer et de surveiller l'appliance NetScaler.

- **Quels sont les types de connexions d'administration ?**

  Il existe deux types de connexions d'administration :

  - Connexion SSH : les utilisateurs administrateurs utilisent un client SSH pour se connecter via l'adresse NSIP.
  - Connexion à l'API NITRO : les utilisateurs administrateurs utilisent les API NITRO pour automatiser le processus de connexion à l'appliance NetScaler.

> **Remarque**
>
> Les utilisateurs administrateurs peuvent également ouvrir une session via l'interface graphique pour se connecter, à l'aide d'un navigateur pour se connecter à l'adresse NSIP. L'interface graphique ouvre en interne une connexion d'API NITRO. Par conséquent, une session GUI équivaut à une connexion API NITRO, et les FAQ relatives à l'API NITRO s'appliquent à l'interface graphique.

- **Combien de connexions d'administration simultanées sont autorisées sur une appliance NetScaler ?**

  L'appliance autorise jusqu'à 20 connexions d'administration simultanées.

- **Quels sont les identifiants de connexion requis pour une connexion administrateur ?**

  La connexion administrateur nécessite un nom d'utilisateur et un mot de passe.

  Remarque : Il est possible d'utiliser une clé d'authentification à la place d'un mot de passe.

- **Quelles sont les méthodes d'authentification externes prises en charge par une appliance NetScaler ?**

  L'appliance prend en charge les méthodes d'authentification externe suivantes :

  - RADIUS
  - LDAP
  - TACACS

- **Qu' est-ce qu'un client ?**

  Un client est un appareil (ordinateur portable ou ordinateur de bureau) utilisé par l'utilisateur administrateur pour ouvrir une connexion administrateur.

- **Qu' est-ce qu'un jeton de session ?**

  Un jeton de session est un identifiant unique que l'appliance NetScaler émet à un client qui envoie une demande de connexion à l'API NITRO.

  - Les clients API peuvent réutiliser le jeton de session, s'il n'a pas expiré, pour les requêtes API ultérieures sur les nouvelles connexions TCP
  - Les clients de l'interface graphique ouvrent en interne des connexions à l'API NITRO et gardent le jeton de session actif pendant la session de l'interface graphique.

- **Qu'est-ce qu'une session active sur une appliance NetScaler ?**

  Une session CLI est considérée comme active si elle n'a pas expiré et si une connexion SSH est ouverte avec un dispositif NetScaler.

  Une session d'API NITRO est considérée comme active si le délai d'expiration du jeton de session n'a pas expiré sur l'appliance NetScaler.

- **Comment NetScaler applique-t-il la limite de connexions simultanées ?**

  Chaque fois que l'appliance NetScaler reçoit une demande de connexion administrateur (SSH ou API NITRO), elle vérifie le nombre de connexions d'administration ouvertes. Si le nombre est inférieur à 20, une nouvelle connexion est ouverte.

- **Quel compteur reflète le nombre de connexions d'administration sur une appliance NetScaler ?**

Le compteur de connexions (nsconfigd_cur_clients) reflète le nombre de connexions actives. Ce compteur est incrémenté lorsqu'un client ouvre une nouvelle connexion à l'appliance et est décrémenté lorsqu'une connexion est fermée.

- **Quel compteur reflète le nombre de jetons actifs sur l'appliance NetScaler ?**

  Le compteur *configd_cur_tokens reflète le nombre de jetons* actifs sur l'appliance NetScaler.

- **Comment l'appliance NetScaler gère-t-elle les erreurs de connexion ?**

  L'appliance NetScaler ferme immédiatement la connexion client (CLI, API et GUI) si elle rencontre des erreurs lors d'une connexion.

- **Une session CLI ou GUI sur une connexion à l'adresse de gestion est-elle prise en compte dans la limite de connexion de l'administrateur ?**

  Oui, toutes les connexions CLI et GUI sont des connexions TCP, et chaque connexion TCP à l'adresse de gestion est prise en compte dans la limite de connexion de l'administrateur.

- **Une session NITRO est-elle prise en compte dans la limite de connexion de l'administrateur ?**

  Une session NITRO est prise en compte dans la limite de connexion administrateur s'il existe une connexion TCP ouverte utilisant le jeton de session émis par l'appliance NetScaler.

- **Quel est le délai d'expiration par défaut pour les sessions d'API, d'interface graphique et de CLI sur l'appliance NetScaler ?**

  Le tableau suivant répertorie le délai d'expiration par défaut pour les sessions d'API, d'interface graphique et de CLI sur l'appliance NetScaler :

Versions de NetScaler	Délai d'expiration par défaut de la CLI (min)	Délai d'expiration par défaut de l'API (min)	Délai d'expiration par défaut de l'interface graphique (min)
NetScaler 9.3	Aucun	30 minutes	30 minutes
NetScaler 10.1	Aucun	30 minutes	30 minutes
NetScaler 10.5 et versions ultérieures	15 minutes	30 minutes	15 minutes

- **Comment définir le délai d'expiration des sessions CLI sur une appliance NetScaler ?**

  Le délai d'expiration de la session CLI peut être configuré en exécutant la commande suivante à l'invite de l'interface de ligne de commande :

  ```
  set cli mode -timeout \<xx seconds>
  ```

- **Comment remplacer le délai d'expiration par défaut lors de l'utilisation de l'API NITRO ?**

Vous pouvez remplacer le délai d'expiration par défaut d'une API NITRO en définissant la durée du délai d'expiration dans le champ « timeout » de l'objet de connexion. Si le délai d'expiration de session est défini sur zéro, le jeton de session a un délai d'expiration infini.

Remarque : Un délai d'expiration infini n'est pas recommandé, car les sessions qui n'expirent pas continuent d'être prises en compte dans le nombre de connexions de l'administrateur.

- **Que se passe-t-il si un compte utilisateur est supprimé de l'appliance NetScaler après la création d'une session d'administration ?**

  Pour les utilisateurs internes du système, l'appliance NetScaler ferme la session CLI ou API NITRO existante.

  Pour les utilisateurs du système externes, la session reste active jusqu'à son expiration.

- **Les clients de l'API NITRO peuvent-ils utiliser un jeton de session unique pour ouvrir plusieurs connexions d'administration sur l'appliance NetScaler ?**

  Oui. Chacune de ces connexions est prise en compte dans la limite de connexion de l'administrateur.

- **Si l'accès à la gestion est activé pour une adresse SNIP, les connexions administrateur à cette adresse compte-t-elle dans la limite du nombre de connexions administrateur ?**

  Oui, les connexions d'administrateur à l'adresse de gestion (SNIP) sont prises en compte dans la limite de connexions d'administrateur sur NetScaler.

- **Un administrateur NetScaler peut-il se connecter à l'appliance NetScaler une fois que la limite maximale de connexions est atteinte ?**

  Oui. Une autre connexion administrateur est autorisée une fois la limite maximale de connexion atteinte.

- **Les points de terminaison de l'API NITRO peuvent-ils ouvrir plusieurs connexions d'administration sur l'appliance NetScaler ?**

  Oui, les points de terminaison de l'API NITRO peuvent ouvrir plusieurs connexions d'administration et dépasser la limite de connexions d'administration simultanées sur une appliance NetScaler. Dans de telles situations, une connexion SSH/CLI supplémentaire est autorisée et l'administrateur peut forcer la fermeture des anciennes sessions API ou réduire la durée du délai d'expiration de la session pour les sessions API existantes.

- **Le même client peut-il ouvrir plusieurs sessions d'API sur une appliance NetScaler ?**

  Oui, un client peut ouvrir plusieurs sessions API en se connectant à plusieurs reprises. Par exemple, le client peut se reconnecter après un redémarrage.
  Remarque : Les connexions client répétées sont prises en compte dans la limite de connexions administrateur sur l'appliance NetScaler.

- **Les clients d'API peuvent-ils utiliser la totalité de la limite de jetons de session d'API ?**

  Oui, les clients d'API peuvent utiliser la totalité de la limite de jetons de session d'API, fournie en se connectant à plusieurs reprises sans utiliser de jeton précédemment émis.

  Remarque : Si le délai d'expiration de la session d'un client est égal à zéro, le jeton est valide pour toujours. Les connexions répétées à l'aide de nouveaux jetons de session peuvent être prises en compte dans la limite des jetons de session d'API.

- **Les sessions CLI sont-elles prises en compte dans la limite des jetons de session API ?**

  Non, les sessions CLI ne sont pas prises en compte dans la limite des jetons de session API.

- **Les utilisateurs administrateurs peuvent-ils utiliser Telnet pour ouvrir une session CLI ?**

  Non. Seul un client SSH peut ouvrir une session CLI.

- **Quelles sont les limites de connexion et de session d'API applicables aux différentes versions de NetScaler ?**

  Le tableau suivant répertorie les limites maximales de connexions d'administrateur simultanées et de sessions d'API actives applicables aux différentes versions de NetScaler :

Versions de NetScaler	9.3	10.1 (Avant 130.x)	10.1 (Avant 130.10)	10,1 (à partir de 130,10)
Nombre maximum de connexions d'administration simultanées	20	20	20	20
Nombre maximum de sessions API actives*	1000	20	1000	1000

Remarque :

- Les sessions d'API sont considérées comme actives si elles n'ont pas expiré. Par exemple, si 500 sessions d'API ont été créées mais que 100 ont expiré, 400 sessions d'API sont actives.
- Il n'est pas nécessaire qu'une session d'API ouvre une connexion TCP à l'appliance NetScaler.

Commutation de contenu

May 5, 2023

- **J'ai installé une appliance d'équilibrage de charge autre que NetScaler sur le réseau. Cependant, je souhaite utiliser la fonctionnalité de commutation de contenu de l'appliance NetScaler pour diriger les demandes des clients vers l'appliance d'équilibrage de charge. Est-il possible d'utiliser la fonctionnalité de commutation de contenu de l'appliance NetScaler avec une appliance d'équilibrage de charge autre que NetScaler ?**

  Oui. Vous pouvez utiliser la fonctionnalité de commutation de contenu de l'appliance NetScaler avec la fonction d'équilibrage de charge de l'appliance NetScaler ou une appliance d'équilibrage de charge non NetScaler. Toutefois, lorsque vous utilisez l'appliance d'équilibrage de charge autre que NetScaler, assurez-vous de créer un serveur virtuel d'équilibrage de charge sur l'appliance NetScaler et de le lier à l'appliance d'équilibrage de charge non NetScaler en tant que service.

- **En quoi un serveur virtuel de commutation de contenu diffère-t-il d'un serveur virtuel d'équilibrage de charge ?**

  Un serveur virtuel de commutation de contenu est uniquement capable d'envoyer les demandes des clients à d'autres serveurs virtuels. Il ne communique pas avec les serveurs.

  Un serveur virtuel d'équilibrage de charge équilibre la charge du client entre les serveurs et communique avec les serveurs. Il surveille la disponibilité du serveur et peut être utilisé pour appliquer différents algorithmes d'équilibrage de charge afin de répartir la charge du trafic.

  La commutation de contenu est une méthode utilisée pour diriger les demandes des clients pour des types spécifiques de contenu vers des serveurs ciblés au moyen de serveurs virtuels d'équilibrage de charge. Vous pouvez diriger les demandes des clients vers les serveurs les mieux adaptés pour les traiter. Il en résulte une réduction des frais généraux de traitement des demandes des clients sur les serveurs.

- **Je souhaite implémenter la fonctionnalité de commutation de contenu de l'appliance NetScaler pour diriger les demandes des clients. Quels types de demandes client puis-je adresser à l'aide de la fonction de changement de contenu ?**

  Vous pouvez diriger uniquement des demandes de clients HTTP, HTTPS, FTP, TCP, TCP sécurisé et RTSP à l'aide de la fonction de commutation de contenu. Pour diriger les demandes des clients HTTPS, vous devez configurer la fonctionnalité de déchargement SSL sur l'appliance.

- **Je souhaite créer des règles de commutation de contenu sur l'appliance NetScaler. Quels sont les différents éléments de la demande du client sur lesquels je peux créer une règle de changement de contenu ?**

Vous pouvez créer les règles de changement de contenu en fonction des éléments suivants et de leurs valeurs dans la demande du client :

- URL
- jetons URL
- version HTTP
- En-têtes HTTP
- Adresse IP source du client
- Version client
- Port TCP de destination

- **Je suis conscient que la fonctionnalité de commutation de contenu de l'appliance NetScaler contribue à améliorer les performances du réseau. Est-ce que c'est exact ?**

  Oui. Vous pouvez diriger les demandes des clients vers les serveurs les mieux adaptés pour les traiter. Il en résulte une réduction de la surcharge de traitement des demandes des clients sur les serveurs.

- **Quelle fonctionnalité de l'appliance NetScaler dois-je configurer sur l'appliance NetScaler pour améliorer la gestion du site et le temps de réponse aux demandes des clients ?**

  Vous pouvez configurer la fonctionnalité de commutation de contenu de l'appliance NetScaler pour améliorer la gestion du site et le temps de réponse à la demande du client. Cette fonctionnalité vous permet de créer des groupes de contenu au sein du même nom de domaine et de la même adresse IP. Cette approche est flexible, contrairement à l'approche commune consistant à partitionner explicitement le contenu en différents noms de domaine et adresses IP, qui sont visibles par l'utilisateur.

  Plusieurs partitions divisant un site Web en différents noms de domaine et adresses IP forcent le navigateur à créer une connexion distincte pour chaque domaine qu'il trouve lors du rendu et de la récupération du contenu d'une page Web. Ces connexions WAN supplémentaires dégradent le temps de réponse de la page Web.

- **J'ai hébergé un site Web sur une batterie de serveurs Web. Quels sont les avantages de la fonctionnalité de commutation de contenu de NetScaler pour ce type de configuration ?**

  La fonctionnalité de commutation de contenu offre les avantages suivants sur une appliance NetScaler installée sur un site basé sur une batterie de serveurs Web :

  - Gérez le contenu du site en créant un groupe de contenus au sein du même domaine et de la même adresse IP.
  - Améliorez le temps de réponse aux demandes des clients en utilisant le groupe de contenus au sein du même domaine et de la même adresse IP.
  - Évitez de recourir à la réplication complète du contenu entre les domaines.

- Activez le partitionnement de contenu spécifique à l'application. Par exemple, vous pouvez diriger les demandes des clients vers un serveur qui gère uniquement le contenu dynamique ou uniquement le contenu statique, selon le cas.
- Prend en charge le multi-hébergement de plusieurs domaines sur le même serveur et utilise la même adresse IP.
- Réutilisez les connexions aux serveurs.

- **Je souhaite implémenter la fonctionnalité de commutation de contenu sur l'appliance NetScaler. Je souhaite diriger les demandes des clients vers les différents serveurs après avoir évalué les différents paramètres de chaque demande. Quelle approche dois-je suivre pour implémenter cette configuration lors de la configuration de la fonctionnalité de changement de contenu ?**

  Vous pouvez utiliser des expressions de stratégie pour créer des stratégies pour la fonctionnalité de changement de contenu. Une expression est une condition évaluée en comparant les qualificatifs de la demande du client à un opérande à l'aide d'un opérateur. Vous pouvez utiliser les paramètres suivants de la demande du client pour créer une expression :

  - **Method** : méthode de requête HTTP.
  - **URL** : URL dans l'en-tête HTTP.
  - **JETONS D'URL**- Jetons spéciaux dans l'URL.
  - **VERSION : version**de la requête HTTP.
  - **URL QUERY**- Contient le LEN de requête d'URL, le LEN d'URL et l'en-tête HTTP.
  - **SOURCEIP** : adresse IP du client.

  Voici la liste complète des opérateurs que vous pouvez utiliser pour créer une expression :

  - == (égal à)
  - ! = (pas égal à)
  - EXISTE
  - N'EXISTE PAS
  - CONTIENT
  - NE CONTIENT PAS
  - GT (supérieur à)
  - LT (inférieur à)

Vous pouvez également créer diverses règles, qui sont des agrégations logiques d'un ensemble d'expressions. Vous pouvez combiner plusieurs expressions pour créer des règles. Pour combiner des expressions, vous pouvez utiliser && (AND) et	opérateurs (OR). Vous pouvez également utiliser des parenthèses pour créer des règles imbriquées et complexes.

- **Je souhaite configurer une stratégie basée sur des règles ainsi qu'une stratégie basée sur une URL pour le même serveur virtuel de commutation de contenu. Est-il possible de créer les deux types de stratégies pour le même serveur virtuel de commutation de contenu ?**

  Oui. Vous pouvez créer les deux types de stratégies pour le même serveur virtuel de commutation de contenu. Toutefois, veillez à attribuer des priorités afin de définir une priorité appropriée pour les stratégies.

- **Je souhaite créer des stratégies de changement de contenu qui évaluent le nom de domaine, ainsi qu'un préfixe et un suffixe d'une URL, et dirigent les demandes des clients en conséquence. Quel type de stratégie de changement de contenu dois-je créer ?**

  Vous pouvez créer une stratégie de domaine et d'URL exacte. Lorsque ce type de politique est évalué, l'appliance NetScaler sélectionne un groupe de contenus si le nom de domaine complet et l'URL figurant dans la demande du client correspondent à ceux configurés. La demande du client doit correspondre au nom de domaine configuré et correspondre exactement au préfixe et au suffixe de l'URL s'ils sont configurés.

- **Je souhaite créer des stratégies de changement de contenu qui évaluent le nom de domaine, ainsi qu'un préfixe et un suffixe partiels d'URL, et dirigent les demandes des clients en conséquence. Quel type de stratégie de changement de contenu dois-je créer ?**

  Vous pouvez créer une stratégie de domaine et d'URL générique pour le serveur virtuel de commutation de contenu. Lorsque ce type de politique est évalué, l'appliance NetScaler sélectionne un groupe de contenus si la demande correspond au nom de domaine complet et partiellement au préfixe d'URL.

- **Qu'est-ce qu'une stratégie d'URL générique ?**

  Vous pouvez utiliser des caractères génériques pour évaluer des URL partielles dans les demandes des clients vers l'URL que vous avez configurée sur l'appliance NetScaler. Vous pouvez utiliser des caractères génériques dans les types de stratégies basées sur les URL suivants :

- Préfixe uniquement. Par exemple, l'expression /sports/* correspond à toutes les URL disponibles sous l'URL /sports. De même, l'expression /sports* correspond à toutes les URL dont le préfixe est /sports.
- Suffixe seulement. Par exemple, l'expression /*.jsp correspond à toutes les URL dont l'extension de nom de fichier est jsp.
- Préfixe et suffixe. Par exemple, l'expression /sports/ *.jsp correspond à toutes les URL de l'URL /sports/ qui possèdent également l'extension de nom de fichier jsp. De même, l'expression /sports *.jsp correspond à toutes les URL avec un préfixe /sports * et une extension de nom de fichier de jsp.

- **Qu' est-ce qu'une politique de domaine et de règle ?**

  Lorsque vous créez une politique de domaine et de règle, la demande du client doit correspondre au domaine complet et à la règle configurée sur l'appliance NetScaler.

- **Quelle est la priorité par défaut définie pour l'évaluation des stratégies ?**

  Par défaut, les stratégies basées sur des règles sont évaluées en premier.

- **Si une partie du contenu est identique pour toutes les demandes du client, quel type de priorité dois-je utiliser pour évaluer les stratégies ?**

  Si une partie du contenu est identique pour tous les utilisateurs et qu'un contenu différent doit être diffusé sur la base d'attributs client, vous pouvez utiliser la priorité basée sur l'URL pour l'évaluation des stratégies.

- **Quelles syntaxes d'expression de stratégie sont prises en charge dans le changement de contenu ?**

  La commutation de contenu prend en charge deux types d'expressions de stratégie :

  - **Syntaxe classique :** la syntaxe classique de la commutation de contenu commence par le mot-clé REQ et est plus avancée que la stratégie Avancé. Les stratégies classiques ne peuvent pas être liées à une action. Par conséquent, le serveur virtuel d'équilibrage de charge cible peut être ajouté uniquement après avoir lié le serveur virtuel de commutation de contenu.
  - **Stratégie avancée :** la stratégie avancée commence généralement par le mot clé HTTP et est plus facile à configurer. Une action de serveur virtuel d'équilibrage de charge cible peut être liée à une stratégie avancée, et la stratégie peut être utilisée sur plusieurs serveurs virtuels de commutation de contenu.

- **Puis-je lier une stratégie de commutation de contenu unique à plusieurs serveurs virtuels ?**

  Oui. Vous pouvez lier une stratégie de commutation de contenu unique à plusieurs serveurs virtuels en utilisant des stratégies avec des actions définies. Les stratégies de commutation

de contenu qui utilisent une action peuvent être liées à plusieurs serveurs virtuels de commutation de contenu, car le serveur virtuel d'équilibrage de charge cible n'est plus spécifié dans la stratégie de commutation de contenu. La possibilité de lier une seule stratégie à plusieurs serveurs virtuels de commutation de contenu permet de réduire davantage la taille de la configuration de commutation de contenu.

Pour plus d'informations, consultez les articles suivants du centre de connaissances et les rubriques de documentation de NetScaler :

- Voir CTX122918 - Comment lier la même politique de commutation de contenu à deux serveurs virtuels de commutation de contenu sur une applianceNetScaler.
- Voir CTX122736 - Comment lier la même stratégie avancée à plusieurs serveurs virtuels de commutation de contenu à l'aide d'étiquettes de stratégie.
- Configuration de la commutation de contenu de base.

- **Puis-je créer une stratégie basée sur l'action en utilisant des expressions classiques ?**

  Non. À l'heure actuelle, NetScaler ne prend pas en charge les politiques utilisant des expressions syntaxiques classiques associées à des actions. Le serveur virtuel d'équilibrage de charge cible doit être ajouté lors de la liaison de la stratégie au lieu de la définir dans une action.

Débogage

May 5, 2023

- **Comment puis-je déterminer l'interface (CLI, GUI ou API) via laquelle une opération a été effectuée ?**

  NetScaler assure le suivi des interfaces via lesquelles les opérations sont effectuées. Vous pouvez consulter ces informations dans syslogs (dans l'interface graphique, accédez à Configuration > Système > Audit > Messages d'audit > Messages Syslog) ou dans le fichier ns.log (situé dans le répertoire /var/log/).

  Par exemple, les opérations effectuées via l'API sont signalées comme « API CMD_EXECUTED ». «

Matériel

April 11, 2023

Cliquez ici pour consulter la FAQ sur le matériel MPX.

Haute disponibilité

August 20, 2021

- **Quels sont les différents ports utilisés pour échanger les informations relatives à la HA entre les nœuds d'une configuration HA ?**

  Dans une configuration HA, les deux nœuds utilisent les ports suivants pour échanger des informations relatives à HA :

  - UDP Port 3003, pour échanger des paquets de pulsations
  - Port 3010, pour la synchronisation et la propagation des commandes

- **Quelles configurations ne sont pas synchronisées ou propagées dans une configuration HA en mode INC ou non-INC ?**

  Les configurations implémentées avec les commandes suivantes ne sont ni propagées ni synchronisées avec le nœud secondaire :

  - Toutes les commandes de configuration HA spécifiques au nœud. Par exemple `add ha node`, `set ha node`, et `bind ha node`.
  - Toutes les commandes de configuration liées à l'interface. Par exemple, set interface et unset interface.
  - Toutes les commandes de configuration associées au canal. Par exemple, add channel, set channel et bind channel.

  Pour plus d'informations sur la configuration HA en mode INC, consultez Configuration des nœuds haute disponibilité dans différents sous-réseaux.

- **Quelles configurations ne sont pas synchronisées ou propagées dans une configuration HA en mode INC ?**

  Les configurations suivantes ne sont ni synchronisées ni propagées. Chaque nœud a son propre.

  - MIP
  - SNIP
  - VLAN
  - Itinéraires (sauf les routes LLB)
  - Moniteurs de routage
  - Règles RNAT (sauf toute règle RNAT avec VIP comme IP NAT)
  - Configurations de routage dynamique.

- **Quelles sont les conditions qui déclenchent la synchronisation ?**

  La synchronisation est déclenchée par l'une des conditions suivantes :

  - Le numéro d'incarnation du nœud principal, reçu par le nœud secondaire, ne correspond pas à celui du nœud secondaire.

Remarque : Les deux nœuds d'une configuration HA conservent un compteur appelé *numéro d'incarnation*, qui compte le nombre de configurations dans le fichier de configuration du nœud. Chaque nœud envoie son numéro d'incarnation à l'autre nœud dans les messages de pulsation. Le numéro d'incarnation n'est pas incrémenté pour les commandes suivantes :

  * Toutes les commandes associées à la configuration HA. Par exemple `add ha node`, `set ha node`, et `bind ha node`.
  * Toutes les commandes liées à l'interface. Par exemple, set interface et unset interface.
  * Toutes les commandes liées au canal. Par exemple, add channel, set channel et bind channel.

- Le nœud secondaire apparaît après un redémarrage.
- Le nœud principal devient secondaire après un basculement.

- **Une configuration ajoutée au nœud secondaire est-elle synchronisée sur le principal ?**

  Non, une configuration ajoutée au nœud secondaire n'est pas synchronisée avec le nœud principal.

- **Quelle pourrait être la raison pour laquelle les deux nœuds prétendent être les principaux dans une configuration HA ?**

  La raison la plus probable est que les nœuds primaire et secondaire sont tous les deux sains, mais que le secondaire ne reçoit pas les paquets de pulsations du primaire. Le problème peut être lié au réseau entre les nœuds.

- **Une configuration HA se heurte-t-elle à des problèmes si vous déployez les deux nœuds avec des paramètres d'horloge système différents ?**

  Différents paramètres d'horloge système sur les deux nœuds peuvent causer les problèmes suivants :

  - Les horodatages dans les entrées du fichier journal ne correspondent pas. Cette situation rend difficile l'analyse des entrées de journal pour tout problème.
  - Après un basculement, vous pouvez rencontrer des problèmes avec tout type de persistance basée sur les cookies pour l'équilibrage de charge. Une différence significative entre les temps peut faire expirer un cookie plus tôt que prévu, entraînant la fin de la session de persistance.
  - Des considérations similaires s'appliquent à toutes les décisions liées au temps sur les nœuds.

- **Quelles sont les conditions d'échec de la commande *force HA sync* ?**

  La synchronisation forcée échoue dans l'une des circonstances suivantes :

  - Vous forcez la synchronisation lorsque la synchronisation est déjà en cours.
  - Le nœud secondaire est désactivé.

- La synchronisation HA est désactivée sur le nœud secondaire actuel.
- La propagation HA est désactivée sur le nœud principal actuel et vous forcez la synchronisation à partir du nœud principal.

- **Quelles sont les conditions d'échec de la commande *synchroniser les fichiers HA* ?**

  La synchronisation des fichiers de configuration échoue si le nœud secondaire est désactivé.

- **Dans une configuration HA, si le nœud secondaire prend le relais en tant que principal, revient-il à l'état secondaire si le principal d'origine revient en ligne ?**

  Non. Une fois que le nœud secondaire prend le relais comme principal, il reste comme principal même si le nœud principal d'origine revient en ligne. Pour échanger le statut principal et secondaire des nœuds, exécutez la commande *force failover*.

- **Quelles sont les conditions d'échec de la commande *force basculement* ?**

  Un basculement forcé échoue dans l'une des circonstances suivantes :

  - Le nœud secondaire est désactivé.
  - Le nœud secondaire est configuré pour rester secondaire.
  - Le nœud principal est configuré pour rester principal.
  - L'état du nœud homologue est inconnu.

Mise en cache intégrée

May 5, 2023

Groupes de contenus

- **En quoi un groupe de contenus DEFAULT diffère-t-il des autres groupes de contenus ?**

  Le comportement du groupe de contenus DEFAULT est le même que celui de n'importe quel autre groupe. Le seul attribut qui rend le groupe de contenus DEFAULT spécial est qu'un objet est mis en cache et qu'aucun groupe de contenus n'a été créé. L'objet est mis en cache dans le groupe DEFAULT.

- **Qu'est-ce que l'option « Contrôle du cache » au niveau du groupe de contenus ?**

  Vous pouvez envoyer n'importe quel en-tête de contrôle du cache au navigateur. Il existe une option au niveau du groupe de contenus, -CacheControl, qui vous permet de spécifier l'en-tête de contrôle du cache que vous souhaitez insérer dans la réponse au navigateur.

- **Qu' est-ce que l'option « Minhit » au niveau du groupe de contenu ?**

`Minhit` est une valeur entière spécifiant le nombre minimum de sélection dans une stratégie de cache avant la mise en cache de l'objet. Cette valeur est configurable au niveau du groupe de contenus. Voici la syntaxe pour configurer cette valeur à partir de l'interface de ligne de commande.

```
add/set cache contentGroup \<Content_Group_Name> [-minHits \<Integer>]
```

- **À quoi sert l'option ExpireAtLastByte ?**

  L'option ExpireAtLastByte permet au cache intégré de faire expirer l'objet lors de son téléchargement. Seules les demandes en suspens sont alors traitées à partir du cache. Toute nouvelle demande est envoyée au serveur. Ce paramètre est utile lorsque l'objet est fréquemment modifié, comme dans le cas des cotations boursières. Ce mécanisme d'expiration fonctionne conjointement avec la fonctionnalité Flash Cache. Pour configurer une option ExpireAtLastByte, exécutez la commande suivante depuis l'interface de ligne de commande :

  ```
  add cache contentGroup \<Group_Name> -expireAtLastByte YES
  ```

Politique de cache

- **Qu'est-ce qu'une politique de mise en cache ?**

  Les politiques déterminent quelles transactions peuvent être mises en cache et lesquelles ne le sont pas. De plus, les politiques ajoutent ou remplacent le comportement de mise en cache HTTP standard. Les politiques déterminent une action, telle que CACHE ou NOCACHE, en fonction des caractéristiques spécifiques de la demande ou de la réponse. Si une réponse correspond aux règles de la politique, l'objet de la réponse est ajouté au groupe de contenus configuré dans la politique. Si vous n'avez pas configuré de groupe de contenus, l'objet est ajouté au groupe de contenus DEFAULT.

- **Qu'est-ce qu'un échec politique ?**

  Une sélection se produit lorsqu'une demande ou une réponse correspond à une politique de cache.

- **Qu'est-ce qu'un échec ?**

  Un échec se produit lorsqu'une demande ou une réponse ne correspond à aucune politique de cache. Un échec peut également se produire si la demande ou la réponse correspond à une politique de cache mais qu'une certaine dérogation au comportement RFC empêche le stockage de l'objet dans le cache.

- **J'ai configuré la fonctionnalité de mise en cache intégrée de l'appliance NetScaler. Lors de l'ajout de la politique suivante, un message d'erreur s'affiche. Y a-t-il une erreur dans la commande ?**


```
add cache policy image_caching -rule exp1 | ns_ext_not_jpeg -action
cache

\> ERROR: No such command
```

Dans la commande précédente, l'expression doit se trouver entre guillemets. Sans guillemets, l'opérateur est considéré comme l'opérateur du tube.

Exigences en matière de mémoire

- **Quelles sont les commandes que je peux exécuter sur l'appliance NetScaler pour vérifier la mémoire allouée au cache ?**

  Pour afficher la mémoire allouée au cache dans l'appliance NetScaler, exécutez l'une des commandes suivantes à partir de l'interface de ligne de commande :

  - `show cache parameter`

    Dans la sortie, vérifiez la valeur du paramètre Limite d'utilisation de la mémoire. Il s'agit de la mémoire maximale allouée au cache.

  - `show cache \<Content_Group_Name>`

    Dans la sortie, vérifiez les valeurs des paramètres Utilisation de la mémoire et Limite d'utilisation de la mémoire indiquant la mémoire utilisée et allouée pour chaque groupe de contenus.

- **Mon appliance NetScaler dispose de 2 Go de mémoire. Existe-t-il une limite de mémoire recommandée pour le cache ?**

  Quel que soit le modèle d'appliance NetScaler, vous pouvez allouer la moitié de la mémoire au cache. Citrix recommande toutefois d'allouer un peu moins de la moitié de la mémoire, en raison de la dépendance à la mémoire interne. Vous pouvez exécuter la commande suivante pour allouer 1 Go de mémoire au cache :

  ```
  set cache parameter -memLimit 1024
  ```

- **Est-il possible d'allouer de la mémoire à des groupes de contenus individuels ?**

  Oui. <Integer>Même si vous allouez de la mémoire au cache intégré de manière globale en exécutant le paramètre set cache —memlimit<Integer>, vous pouvez allouer de la mémoire à des groupes de contenus individuels en exécutant la commande set cache <Content_Group_Name>—memLimit. La mémoire maximale que vous pouvez allouer aux groupes de contenus (combinés) ne peut pas dépasser la mémoire que vous avez allouée au cache intégré.

- **Quelle est la dépendance de la mémoire entre le cache intégré et la mémoire tampon TCP ?**

Si l'appliance NetScaler dispose de 2 Go de mémoire, elle réserve environ 800 Mo à 900 Mo de mémoire et le reste est alloué au système d'exploitation FreeBSD. Par conséquent, vous pouvez allouer jusqu'à 512 Mo de mémoire au cache intégré et le reste est alloué à la mémoire tampon TCP.

- **Cela affecte-t-il le processus de mise en cache si je n'alloue pas de mémoire globale au cache intégré ?**

  Si vous n'allouez pas de mémoire au cache intégré, toutes les demandes sont envoyées au serveur. Pour vous assurer que vous avez alloué de la mémoire au cache intégré, exécutez la commande show cache parameter. En fait, aucun objet n'est mis en cache si la mémoire globale est égale à 0, elle doit donc être définie en premier.

Commandes de vérification

- **Quelles sont les options pour afficher les statistiques du cache ?**

  Vous pouvez utiliser l'une des options suivantes pour afficher les statistiques relatives au cache :

  - `stat cache`

    Pour afficher le résumé des statistiques du cache.

  - `stat cache -detail`

    Pour afficher les détails complets des statistiques du cache.

- **Quelles sont les options pour afficher le contenu mis en cache ?**

  Pour afficher le contenu mis en cache, vous pouvez exécuter la `show cache object` commande.

- **Quelle est la commande que je peux exécuter pour afficher les caractéristiques d'un objet stocké en cache ?**

  Si l'objet stocké dans le cache est, par exemple, GET //10.102.12.16:80/index.html, vous pouvez afficher les détails de l'objet en exécutant la commande suivante depuis l'interface de ligne de commande de l'appliance :

  ```
  show cache object -url '/index.html'-host 10.102.3.96 -port 80
  ```

- **Est-il obligatoire de spécifier le nom du groupe en tant que paramètre pour afficher les objets paramétrés dans le cache ?**

  Oui. Il est obligatoire de spécifier le nom du groupe en tant que paramètre pour afficher les objets paramétrés dans le cache. Par exemple, considérez que vous avez ajouté les politiques suivantes avec la même règle :


```
add cache policy p2 -rule ns_url_path_cgibin -action CACHE -
    storeInGroup g1
add cache policy p1 -rule ns_url_path_cgibin -action CACHE -
    storeInGroup g2
<!--NeedCopy-->
```

Dans ce cas, pour les multiples demandes, si la politique p1 est évaluée, son compteur de sélection est incrémenté et la politique stocke l'objet dans le groupe g1, qui possède des paramètres de sélection. Vous devez donc exécuter la commande suivante pour afficher les objets du cache :

```
show cache object -url "/cgi-bin/setCookie.pl"-host 10.102.18.152
groupName g1
```

De même, pour un autre ensemble de requêtes multiples, si la politique p2 est évaluée, son compteur de sélection est incrémenté et la politique stocke l'objet dans le groupe g2, qui ne possède pas de paramètres de sélection. Vous devez donc exécuter la commande suivante pour afficher les objets du cache :

```
show cache object -url "/cgi-bin/setCookie2.pl"-host 10.102.18.152
```

- **Je remarque qu'il y a des entrées vides dans la sortie de la commande nscachemgr. Quelles sont ces entrées ?**

  Tenez compte de l'exemple de sortie suivant de la `nscachemgr` commande. Les entrées vides de cette sortie sont surlignées en gras pour votre référence :

```
root@ns# /netscaler/nscachemgr -a
//10.102.3.89:80/image8.png
//10.102.3.97:80/staticdynamic.html
//10.102.3.97:80/
//10.102.3.89:80/image1.png
//10.102.3.89:80/file5.html
//10.102.3.96:80/
//10.102.3.97:80/bg_logo_segue.png
//10.102.3.89:80/file500.html
//10.102.3.92:80/
//10.102.3.96:80/cgi-bin/rfc/ccProxyReval.pl
Total URLs in IC = 10
<!--NeedCopy-->
```

  Les entrées vides dans la sortie sont dues aux propriétés de mise en cache par défaut de GET/HTTP/1.1.

Rincer des objets

- **Comment puis-je vider un objet sélectif du cache ?**

  Vous pouvez identifier un objet de manière unique grâce à son URL complète. Pour vider un tel objet, vous pouvez effectuer l'une des tâches suivantes :

  - Vider le cache
  - Groupe de contenus Flush
  - Rincer l'objet spécifique

  Pour vider l'objet spécifique, vous devez spécifier les paramètres de la requête. Vous spécifiez le paramètre InvalParam pour vider l'objet. Ce paramètre s'applique uniquement à une requête.

- **Toute modification de la configuration du cache provoque-t-elle le vidage du cache ?**

  Oui. Lorsque vous modifiez la configuration du cache, toutes les commandes de cache SET vident intrinsèquement les groupes de contenus appropriés.

- **J'ai mis à jour les objets sur le serveur. Dois-je vider les objets mis en cache ?**

  Oui. Lorsque vous mettez à jour des objets sur le serveur, vous devez vider les objets mis en cache, ou au moins les objets et groupes de contenus concernés. Le cache intégré n'est pas affecté par une mise à jour du serveur. Il continue à servir les objets mis en cache jusqu'à leur expiration.

Cache Flash

- **Qu'est-ce que la fonctionnalité Flash Cache de l'appliance NetScaler ?**

  Le phénomène des foules Flash se produit lorsque de nombreux clients accèdent au même contenu. Il en résulte une augmentation soudaine du trafic vers le serveur. La fonctionnalité Flash Cache permet à l'appliance NetScaler d'améliorer les performances dans une telle situation en n'envoyant qu'une seule demande au serveur. Toutes les autres demandes sont mises en file d'attente sur l'appliance et la réponse unique est fournie aux demandes. Vous pouvez utiliser l'une des commandes suivantes pour activer la fonctionnalité Fast Cache :

  - `add cache contentGroup \<Group_Name> -flashCache YES`
  - `set cache contentGroup \<Group_Name> -flashCache YES`

- **Quelle est la limite pour les clients Flash Cache ?**

  Le nombre de clients Flash Cache dépend de la disponibilité des ressources sur l'appliance NetScaler.

Comportement par défaut

- **L'appliance NetScaler reçoit-elle des objets de manière proactive à leur expiration ?**

L'appliance NetScaler ne reçoit jamais d'objets de manière proactive à l'expiration. Cela est vrai même pour les objets négatifs. Le premier accès après expiration déclenche une demande auprès du serveur.

- **Le cache intégré ajoute-t-il des clients à la file d'attente avant même qu'il ne commence à recevoir la réponse ?**

  Oui. Le cache intégré ajoute des clients à la file d'attente avant même qu'il ne commence à recevoir la réponse.

- **Quelle est la valeur par défaut du paramètre Verify cached object using de la configuration du cache ?**

  HOSTNAME_AND_IP est la valeur par défaut.

- **L'appliance NetScaler crée-t-elle des entrées de journal dans les fichiers journaux ?**

  Oui. L'appliance NetScaler crée des entrées de journal dans les fichiers journaux.

- **Les objets compressés sont-ils stockés dans le cache ?**

  Oui. Les objets compressés sont stockés dans le cache.

Interopérabilité avec d'autres fonctionnalités

- **Qu'advient-il des objets actuellement stockés dans le cache et auxquels on accède via le VPN SSL ?**

  Les objets stockés dans le cache et accessibles régulièrement sont servis en cache, sélectionnés lorsqu'ils sont accessibles via le VPN SSL.

- **Qu' advient-il des objets stockés dans le cache lorsqu'ils sont accessibles via SSL VPN et plus tard accessibles via une connexion régulière ?**

  Les objets stockés via l'accès VPN SSL sont servis de sélection lorsqu'ils sont accessibles via la connexion normale.

- **Lors de l'utilisation de la journalisation Web, comment différencier les entrées qui indiquent la réponse servie du cache de celles desservies par le serveur ?**

  Pour les réponses envoyées à partir du cache intégré, le champ du journal du serveur contient la valeur IC. Pour les réponses envoyées depuis un serveur, le champ du journal du serveur contient la valeur envoyée par le serveur. Voici un exemple d'entrée de journal pour une transaction de mise en cache intégrée :

  ```
  "10.102.1.52 - "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 4.0; .NET
   CLR 1.0.3705)""GET /"200 0 "IC"10.102.1.45"
  ```

  En plus d'une demande du client, la réponse enregistrée est celle envoyée au client et pas nécessairement celle envoyée par le serveur.

> **Remarque**
>
> Lorsque vous utilisez la journalisation Web, les réponses du cache intégré contiennent la valeur IC dans le champ du journal du serveur. Le champ journal du serveur est présent dans le client NSWL avec le spécificateur de format « %o1 ».

Divers

- **Que voulez-vous dire par la configuration de relexpiry et absexpiry ?**

  En configurant `relexpiry` et `absexpiry`, cela signifie que vous remplacez l'en-tête indépendamment de ce qui apparaît dans l'en-tête. Vous pouvez configurer un paramètre d'expiration différent et le niveau du groupe de contenu. Avec `relexpiry`, l'expiration de l'en-tête est basée sur l'heure à laquelle l'objet est reçu par NetScaler. Avec `absexpiry`, l'expiration est basée sur l'heure configurée sur NetScaler. `Relexpiry` est configuré en termes de secondes. `Absexpiry` est un moment de la journée.

- **Que voulez-vous dire par la configuration de weakpos et heuristic ?**

  Les `weakpos` et heuristiques sont comme des valeurs de secours. S'il y a un en-tête d'expiration, il n'est considéré que si le dernier en-tête modifié est présent. L'appliance NetScaler définit l'expiration en fonction de la dernière modification de l'en-tête et du paramètre heuristique. Le calcul heuristique de l'expiration détermine le délai d'expiration en vérifiant le dernier en-tête modifié. Un certain pourcentage de la durée écoulée depuis la dernière modification de l'objet est utilisé comme délai d'expiration. L'heuristique d'un objet qui reste inchangé pendant de longues périodes et qui est susceptible d'avoir des délais d'expiration plus longs. –heurExpiryParam spécifie la valeur de pourcentage à utiliser dans ce calcul. Sinon, l'appliance utilise la valeur `weakpos`.

- **Que dois-je considérer avant de configurer la mise en cache dynamique ?**

  Si certains paramètres se présentent sous forme de nom-valeur et ne contiennent pas la requête URL complète, ou si l'appliance reçoit le paramètre dans un en-tête de cookie ou un corps POST, envisagez de configurer la mise en cache dynamique. Pour configurer la mise en cache dynamique, vous devez configurer le paramètre HitParams.

- **Comment le codage hexadécimal est-il pris en charge dans les noms de paramètres ?**

  Sur l'appliance NetScaler, le codage %HEXHEX est pris en charge dans les noms des paramètres. Dans les noms que vous spécifiez pour HitParams ou InvalParams, vous pouvez spécifier un nom contenant le codage %HEXHEX dans les noms. Par exemple, name, name%65 et n %61m%65 sont équivalents.

- **Quel est le processus de sélection d'un paramètre HitParam ?**

  Examinez l'extrait suivant d'un en-tête HTTP pour une requête POST :


```
POST /data2html.asp?param1=value1&param2=&param3&param4=value4
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash, \*/\*
Referer: http://10.102.3.97/forms.html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 10.102.3.97
Content-Length: 153
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQGQGGRNY=NNLLKDADEENOAFLCCDGFGDMO
S1=This+text+is+only+text%2C+not+more+and+not+less%2C+%0D%0Ajust+
   text+to+be+itself%2C+namely+%22Text%22+to+be+posted+as+text
   +%28what+else...%29&B1=Submit
<!--NeedCopy-->
```

Dans la demande précédente, vous pouvez utiliser S1 et B1, surlignés en gras à titre de référence, comme hitParams en fonction de vos besoins. De même, si vous utilisez -MatchCookies YES dans le groupe de contenus ASPSESSIONIDQGQGGRNY, vous pouvez également utiliser ces paramètres en tant que hitParams.

- **Qu'arrive-t-il aux clients en file d'attente si la réponse ne peut pas être mise en cache ?**

  Si la réponse ne peut pas être mise en cache, tous les clients de la file d'attente reçoivent la même réponse que le premier client.

- **Puis-je activer les fonctionnalités Poll every time (PET) et Flash Cache sur le même groupe de contenus ?**

  Non. Vous ne pouvez pas activer PET et Flash Cache sur le même groupe de contenus. Le cache intégré n'exécute pas la fonction AutoPet sur les groupes de contenus Flash Cache. La fonction PET garantit que le cache intégré ne dessert pas un objet stocké sans consulter le serveur. Vous pouvez configurer le PET de manière explicite pour un groupe de contenus.

- **Quand les entrées de journal sont-elles créées pour les clients en file d'attente ?**

  Les entrées du journal sont créées pour les clients en file d'attente peu après que l'appliance a reçu l'en-tête de réponse. Les entrées du journal sont créées uniquement si l'en-tête de réponse ne rend pas l'objet impossible à mettre en cache.

- **Que signifient les valeurs DNS, HOSTNAME et HOSTNAME_AND_IP du paramètre Verify cached object using de la configuration du cache ?**

Les significations sont les suivantes :

- `set cache parameter -verifyUsing HOSTNAME`

  La commande ignore l'adresse IP de destination.

- `set cache parameter -verifyUsing HOSTNAME_AND_IP`

  La commande correspond à l'adresse IP de destination.

- `set cache parameter -verifyUsing DNS`

  La commande utilise le serveur DNS.

- **J'ai réglé WeakneGrelExpiry sur 600, soit 10 minutes. J'ai remarqué que les réponses 404 ne sont pas mises en cache. Quelle en est la raison ?**

  Cela dépend entièrement de votre configuration. Par défaut, les réponses 404 sont mises en cache pendant 10 minutes. Si vous souhaitez que toutes les réponses 404 soient récupérées depuis le serveur, spécifiez—WeakneGrelExpiry 0. Vous pouvez ajuster la valeur —WeakneGrelExpiration à la valeur souhaitée, par exemple supérieure ou inférieure pour que les 404 réponses soient mises en cache de manière appropriée. Si vous avez configuré —AbsExpiry pour les réponses positives, il se peut que cela ne donne pas les résultats souhaités.

- **Lorsque l'utilisateur accède au site à l'aide du navigateur Mozilla Firefox, le contenu mis à jour est diffusé. Toutefois, lorsque l'utilisateur accède au site à l'aide du navigateur Microsoft Internet Explorer, du contenu obsolète est diffusé. Quelle pourrait en être la raison ?**

  Le navigateur Microsoft Internet Explorer extrait peut-être le contenu de son cache local au lieu du cache intégré de NetScaler. Cela peut être dû au fait que le navigateur Microsoft Internet Explorer ne respecte pas l'en-tête relatif à l'expiration dans la réponse.

  Pour résoudre ce problème, vous pouvez désactiver le cache local d'Internet Explorer et effacer le contenu hors connexion. Après avoir effacé le contenu hors connexion, le navigateur doit afficher le contenu mis à jour.

- **Et si les Hits sont nuls ?**

  Vérifiez si l'heure du serveur et l'heure NS sont synchronisées. Et la limite WeakPosRelExpiry définie doit correspondre à la différence de temps entre NS et le serveur comme suit :

```
root@ns180# date
Tue May 15 18:53:52 IST 2012
<!--NeedCopy-->
```

- **Pourquoi les politiques sont-elles touchées alors que rien n'est mis en cache ?**

  Vérifiez que la mémoire est allouée au cache intégré et que l'allocation est supérieure à zéro.

- **Est-il possible de remettre à zéro les compteurs de cache ?**

  Il n'existe pas de ligne de commande ni d'option d'interface graphique permettant de mettre les compteurs de cache à zéro, et le fait de vider le cache ne permet pas non plus de le vider. Le redémarrage de la boîte définit automatiquement ces compteurs à zéro.

Installation, mise à niveau et rétrogradation

May 5, 2023

Installation et mise à niveau

Comment télécharger le package de compilation d'une version spécifique de NetScaler ?

Pour plus d'informations sur le téléchargement d'un package de version NetScaler spécifique, voir Télécharger un package de version NetScaler.

Comment mettre à niveau le logiciel système d'une appliance NetScaler ?

Pour plus d'informations sur la mise à niveau du logiciel système d'une appliance NetScaler, voir Mettre à niveau une appliance autonome NetScaler.

Où puis-je trouver les notes de mise à jour d'une version de NetScaler ?

Le document des notes de mise à jour d'une version de NetScaler répertorie les informations suivantes pour cette version :

- Améliorations
- Problèmes résolus
- Problèmes connus

Le document relatif aux notes de mise à jour d'une version de NetScaler se trouve aux emplacements suivants :

- Page de téléchargement du microprogramme ou de l'appliance virtuelle NetScaler d'une version spécifique.
- Page desnotes de mise à jour d'ADC sur le site de documentation NetScaler

Où puis-je trouver les mises à jour de sécurité pour les appliances NetScaler ?

L'équipe de sécurité de Citrix publie régulièrement des bulletins de sécurité sur les vulnérabilités et les expositions courantes (CVE) pour tous les produits NetScaler associés. Ces informations peuvent être consultées dans le bulletin de sécurité. Vous pouvez également rechercher un CVE spécifique sur le site de support de NetScaler.

À quoi sert le fichier zebos.conf disponible dans une version de NetScaler ?

Une appliance NetScaler utilise ZebOS comme suite de routage. Le fichier zebos.conf disponible dans une version de NetScaler est le fichier de configuration de ZebOS.

Je souhaite remplacer le port SSH (22) de l'appliance NetScaler par un autre port. Est-il possible de modifier le port SSH de l'appliance ?

Oui. Vous pouvez modifier le port SSH sur l'appliance NetScaler en modifiant le fichier sshd_config dans le répertoire /nsconfig. Si le fichier n'existe pas dans le répertoire /nsconfig, copiez-le depuis le répertoire /etc.

Dans le fichier sshd_config, modifiez l'entrée du port 22 en Port<Number>, où se <Number>trouve le numéro du port cible. Si vous ne souhaitez pas redémarrer l'appliance et appliquer les modifications, mettez fin au `sshd` processus à l'aide de la commande kill, puis redémarrez-le.

Le répertoire flash est absent de l'appliance NetScaler. Quelle procédure dois-je suivre pour monter le répertoire Flash ?

Pour monter le répertoire flash, procédez comme suit :

1. Démarrez l'appliance NetScaler en mode mono-utilisateur.

   Au démarrage de l'appliance, le message suivant s'affiche :

   Sélectionnez [Enter] pour démarrer immédiatement, ou n'importe quelle autre touche de l'invite de commande. Démarrage du [noyau] en 10 secondes… » Sélectionnez un espace et l'invite suivante doit s'afficher :

   Tapez '?' pour une liste de commandes, 'help' pour une aide plus détaillée.

2. Entrez la commande suivante pour démarrer FreeBSD en mode mono-utilisateur :

   bottes —s

   Après le démarrage de l'appliance, le message suivant s'affiche :

   Entrez le chemin complet du shell ou entrez la valeur RETURN pour /bin/sh :

3. Appuyez sur Entrée pour afficher le message #.

4. Exécutez la commande suivante pour monter le répertoire flash :

```
mount /dev/ad0s1a /flash

Note: If the preceding command displays an error message about
   permissions, run the following command to check the disk for
   consistency:

fsck /dev/ad0s1a

Run the mount command again to mount the flash directory.
```

5. Redémarrez l'appliance.
6. À partir de l'invite de shell, exécutez la commande suivante pour vérifier que le répertoire flash est monté :

```
df -kh
```

Je souhaite me connecter à l'appliance NetScaler sans saisir le mot de passe. Est-il possible de configurer SSH sur l'appliance pour l'autoriser ?

Oui. Vous pouvez configurer SSH sur l'appliance NetScaler pour vous connecter sans mot de passe. Toutefois, vous devez fournir votre nom d'utilisateur. Pour configurer SSH afin de vous connecter sans mot de passe, procédez comme suit :

1. Exécutez la commande suivante pour générer les clés publiques et privées :

```
\# ssh-keygen -t rsa
```

2. Exécutez la commande suivante pour copier le fichier id_rsa.pub dans le répertoire .ssh de l'hôte distant sur lequel vous souhaitez vous connecter :

```
\# scp id_dsa.pub \<user>@\<remote_host>/.ssh/id_dsa.pub
```

3. Ouvrez une session sur l'hôte distant.
4. Accédez au répertoire .ssh.
5. Exécutez les commandes suivantes pour ajouter la clé publique du client aux clés publiques connues :

```
\# cat id_dsa.pub >> authorized_keys2

\# chmod 640 authorized_keys2

```



```
\# rm id_dsa.pub
```

Quelle est la procédure pour réinitialiser le BIOS de l'appliance NetScaler ? Dans quelles circonstances dois-je réinitialiser le BIOS ?

Pour réinitialiser le BIOS de l'appliance NetScaler, procédez comme suit :

1. Connectez-vous à l'appliance via le port série.
2. Démarrez l'appliance et appuyez sur Supprimer lorsque le processus de démarrage commence.

   Appuyez sur Supprimer pendant le processus POST pour afficher les paramètres du BIOS de l'appliance.
3. Activez la page de sortie des paramètres du BIOS.
4. Sélectionnez l'option Charger les valeurs par défaut optimales. La boîte de message Charger les paramètres optimaux s'affiche.
5. Sélectionnez OK.
6. Apportez les modifications suivantes aux paramètres du BIOS dans les différents onglets :

   Tab
7. Activez la page de sortie des paramètres du BIOS.
8. Sélectionnez Enregistrer les modifications et Quitter.
9. Sélectionnez OK pour confirmer.
10. Vérifiez que l'appliance démarre correctement et que la console série affiche la sortie après le démarrage de l'appliance.

    Vous devez réinitialiser le BIOS lorsque la console série ne répond pas. Cela se produit généralement après la mise à niveau de l'appliance et la désactivation de la console série. Toutefois, vous pouvez toujours accéder à l'appliance à l'aide de l'utilitaire telnet ou SSH.

Je dois rétablir les paramètres d'usine de l'appliance NetScaler. Quelle procédure dois-je suivre ?

Pour rétablir les paramètres d'usine de l'appliance NetScaler, vous devez réinitialiser deux environnements : l'environnement d'application NetScaler et l'environnement de base FreeBSD.
Pour rétablir les paramètres d'usine de l'environnement d'application NetScaler de l'appliance, procédez comme suit :

1. Effectuez une sauvegarde du fichier /nsconfig/ns.conf.
2. Supprimez le fichier /nsconfig/ns.conf.

3. Redémarrez l'appliance. Pour rétablir les paramètres d'usine par défaut de l'environnement FreeBSD de l'appliance, procédez comme suit :
   a) Installez une nouvelle image de code NetScaler sur l'appliance. Cela remplace plusieurs fichiers de configuration au niveau de FreeBSD par des valeurs par défaut.
   b) Supprimez tous les utilisateurs et groupes ajoutés à l'appliance, c'est-à-dire tous sauf les utilisateurs par défaut.
   c) Supprimez le fichier /etc/resolv.conf.
   d) Supprimez les entrées que vous avez ajoutées au fichier /etc/hosts.
   e) Si le fichier /etc/rc.netscaler existe, supprimez-le.
   f) Ouvrez le fichier /etc/nsperm_group_suser et assurez-vous que toutes les entrées IOCTL sont des entrées de commentaires.
   g) Ouvrez le fichier /etc/rc.conf et assurez-vous que l'entrée Syslogd_enable=no n'est pas remplacée par Syslogd_enable=yes.
   h) Ouvrez le fichier /etc/syslog.conf et assurez-vous qu'il ne contient aucune entrée supplémentaire.
   i) Supprimez le contenu des fichiers /var/nslog, /var/nstrace et /var/crash.
   j) Si le processus syslog est activé sur l'appliance et que celle-ci crée des fichiers journaux localement, supprimez le contenu des fichiers journaux répertoriés dans le fichier /etc/syslog.conf. Les fichiers sont créés dans le répertoire /var/log. Par exemple, si le processus syslog écrit des événements système dans le fichier /var/log/events et `sslvpn` accède aux événements dans le fichier /var/log/sslvpnevents, supprimez ces fichiers.

L'appliance affiche un message similaire au message « 21 juin 12:20:18 ns /flash/ns-10.0-47.15 : [1/2] dc0 : NIC hangs condition #663 : TX 10000/10000, RX 0, HF 0 » sur la console. Quelle est la signification de ce message ?

Le message comprend les éléments suivants (présentés ici à titre d'exemples) :

- #663 : Nombre de fois que cette condition s'est produite sur l'appliance.
- TX 10000/10000 : nombre de paquets que l'appliance a tenté de transmettre et nombre de paquets transmis. Si les deux numéros sont identiques, comme dans cet exemple, la carte réseau a transmis tous les paquets que l'appliance a tenté de transmettre.
- RX 0 : Nombre de paquets reçus. Dans cet exemple, aucun paquet n'a été reçu.
- HF0 : nombre de problèmes matériels signalés par la carte réseau. Dans cet exemple, la carte réseau n'a signalé aucun problème matériel.

Si l'appliance ne reçoit aucun paquet, elle signale une condition de blocage, car sur un réseau, il est peu probable qu'elle ne reçoive aucun paquet. Toutefois, si l'appliance est branchée sur l'interface, vous pouvez ignorer ce message d'erreur.

Après la mise à niveau de la version de NetScaler sur l'appliance, celle-ci affiche toujours la version ou la version précédente. Quelle peut être la raison ?

L'appliance affiche le numéro de version logicielle figurant dans le fichier /flash/boot/loader.conf. Si l'entrée du noyau pour la version actuelle de NetScaler est absente de ce fichier, l'appliance affiche la dernière version de NetScaler pour laquelle l'entrée était disponible.
Pour résoudre ce problème, procédez comme suit :

1. Vérifiez que le fichier du noyau existe dans le répertoire /nsconfig.
2. Vérifiez si le fichier /flash/boot/loader.conf contient une entrée pour le noyau.

   (Vous pouvez vous attendre à ce que l'entrée correspondant au noyau de la version ou de la version que vous avez installée ne figure pas dans le fichier.)
3. Ouvrez le fichier loader.conf dans un éditeur de texte, tel que l'éditeur vi, et mettez à jour l'entrée du noyau pour la nouvelle version/build.
4. Enregistrez, puis fermez le fichier.
5. Répétez les étapes 2 à 4 pour le fichier /flash/boot/loader.conf.local.
6. Mettez à jour l'entrée release/build dans le fichier ns.conf.
7. Redémarrez l'appliance.

Depuis la mise à niveau de la version NetScaler de l'appliance, l'écran LCD situé sur le panneau avant de l'appliance affiche le message de mise hors service ou n'affiche rien. Comment puis-je résoudre ce problème ?

Exécutez la commande suivante à partir de l'invite de shell de l'appliance :

```
1 /netscaler/nslcd -k
```

J'ai mis à jour la version/build de NetScaler. Toutefois, après le processus de mise à niveau, l'appliance ne démarre pas. Puis-je rétrograder le logiciel de l'appliance vers la version ou la version précédente ?

Oui. Vous pouvez démarrer l'appliance à l'aide du fichier de noyau kernel.old. Lorsque vous redémarrez l'appliance, appuyez sur la touche F1 lorsque la console appliance affiche le message Appuyez sur F1. **Tapez kernel.old et appuyez sur Entrée.**

Après la mise à niveau de la version NetScaler sur l'appliance, j'ai accidentellement supprimé le fichier du noyau du répertoire /flash. Par conséquent, je ne suis pas en mesure de démarrer l'appareil. Existe-t-il une méthode pour démarrer l'appareil dans ce cas ?

Oui. Vous pouvez démarrer l'appliance à l'aide du fichier `kernel.GENERIC` noyau, comme suit :

1. Lorsque vous redémarrez l'appliance, appuyez sur la touche F1 lorsque la console appliance affiche le message Appuyez sur F1.
2. Tapez le noyau. GENERIC et appuyez sur Entrée.
3. Connectez-vous en tant qu'utilisateur racine.
4. Réinstallez la version de NetScaler.
5. Redémarrez l'appliance.

Après la mise à niveau du logiciel de l'appliance, je ne parviens pas à me connecter à l'appliance et le message suivant s'affiche. J'ai essayé de résoudre ce problème en utilisant la procédure de récupération du mot de passe, mais sans succès. Qu'ai-je fait de mal ?

```
1 ```
2 login: nsroot
3 Password:
4 connect: No such file or directory
5 nsnet_connect: No such file or directory
6 Login incorrect
7 <!--NeedCopy--> ```
```

Vous ne pouvez pas résoudre ce problème en utilisant la procédure de récupération de mot de passe. NetScaler version 12.1 ou ultérieure utilise le nouveau système de licences, basé sur le `Imgrd` démon, qui s'exécute pendant la procédure de démarrage. Pour que ce démon fonctionne correctement, le nom d'hôte de l'appliance NetScaler, qui est défini dans le fichier /nsconfig/rc.conf, doit être résolu par un serveur de noms à l'adresse NSIP. <Host_Name>Vous pouvez également créer un fichier hosts dans le répertoire /nsconfig et y ajouter l'entrée 127.0.0.1.

Assurez-vous également d'avoir copié les fichiers de licence dans le répertoire /nsconfig/license/.

Lors de la mise à niveau d'une paire de haute disponibilité, le message suivant s'affiche à plusieurs reprises. Quelle peut être la raison ?

ns sshd [5035] : erreur : nom d'utilisateur ou mot de passe non valide
Ce message d'erreur s'affiche lorsque les appliances impliquées dans le couplage haute disponibilité disposent d'une version différente de NetScaler ou d'une version différente de la même version installée. Une version différente des appliances peut être installée si vous avez mis à niveau ou rétrogradé une appliance mais pas l'autre.

Je souhaite modifier le masque réseau de l'adresse NSIP sur une appliance NetScaler. Puis-je le faire sans provoquer de panne ?

La modification du masque réseau de l'adresse IP NetScaler peut entraîner une interruption de courte durée. Assurez-vous de modifier le masque de réseau sur l'appliance secondaire, puis de rompre le couplage haute disponibilité. Vérifiez le bon fonctionnement de l'appareil. Si tout fonctionne comme prévu, reconstruisez le couplage haute disponibilité.

Pour modifier le masque de réseau sur l'appliance, exécutez la 'config ns' commande à partir de l'invite CLI, puis choisissez la deuxième option dans le menu.

J'ai configuré une paire d'appliances NetScaler à haute disponibilité. Après la mise à niveau de la version logicielle d'une version préliminaire vers une version finale, j'ai remarqué que certaines configurations de l'appliance étaient manquantes. Puis-je récupérer les configurations perdues ?

Vous pouvez utiliser la procédure suivante pour restaurer la configuration :

1. Ouvrez une session sur la ligne de commande NetScaler de l'appliance principale.
2. Exécutez les commandes suivantes :

save config
shell
\#cp /nsconfig/ns.conf /nsconfig/ns.conf.bkup
The ns.conf.bkup file is a backup for the running configuration.

3. Mettez à niveau le logiciel des deux appliances vers la version finale.
4. Ouvrez une session sur la ligne de commande NetScaler de l'appliance principale.

L'appliance principale et l'appliance secondaire peuvent-elles avoir des versions distinctes ?

La pratique recommandée consiste à utiliser la même version et le même numéro de build sur l'appliance principale et secondaire.

Les deux appliances d'une paire High Availability (HA) peuvent-elles être mises à niveau en même temps ?

Non. Dans une paire HA, mettez d'abord à niveau le nœud secondaire, puis mettez à niveau le nœud principal.

Pour plus de détails, reportez-vous [à la section Mise à niveau d'une paire haute disponibilité](/fr-fr/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-HA-pair.html).

NetScaler prend-il en charge les mises à niveau du microprogramme dans le cloud Amazon Web Services ?

Oui.

Puis-je mettre à niveau l'instance NetScaler indépendamment de la version SDX ?

Il n'est pas nécessaire de mettre à niveau la version SDX lors de la mise à niveau de l'appliance NetScaler. Toutefois, certaines fonctionnalités peuvent ne pas fonctionner.

Puis-je utiliser le serveur FTP pour mettre à niveau l'appliance NetScaler ?

Non. Vous devez d'abord télécharger le microprogramme depuis le site NetScaler, l'enregistrer sur votre ordinateur local, puis mettre à niveau l'appliance.

La procédure de mise à niveau de l'appliance NetScaler avec des configurations GSLB est-elle différente de la mise à niveau d'une appliance qui n'est pas impliquée dans GSLB ?
Non. La procédure de mise à niveau est similaire à la procédure de mise à niveau de base. La seule différence est que vous pouvez mettre à niveau les appliances autonomes ou HA sur différents sites de manière progressive.
Mettre à niveau vers une version antérieure
J'ai reçu une appliance NetScaler sur laquelle la dernière version de NetScaler est installée. Cependant, je souhaite rétrograder la version du logiciel. Est-ce que je peux le faire ?
Non. Si vous tentez de rétrograder la version logicielle, l'appliance risque de ne pas fonctionner comme prévu, car le fichier ns.conf de la version ultérieure n'est peut-être pas compatible avec la version précédente et l'appliance risque de rétablir les paramètres d'usine.
Lors de la rétrogradation de la version NetScaler, j'ai suivi les instructions. Toutefois, l'appliance affiche le message suivant. Comment s'effectue la procédure de restauration sur une appliance NetScaler ?
root@LBCOL03B# ./installns
installns version (10.0-47.7) kernel (ns-10.0-47.7.gz)
Note:
Installation may pause for up to 3 minutes while data is written to the flash.
Caution:
Do not interrupt the installation process.
Doing so may cause the system to become unusable.
Installation will proceed in 5 seconds, CTRL-C to abort
No Valid NetScaler Version Detected
root@LBCOL03B#
La procédure d'annulation est similaire à la procédure de mise à niveau de base. Sélectionnez la version cible vers laquelle vous souhaitez revenir et effectuez la rétrogradation. Avant de revenir à une autre version, Citrix recommande de créer une copie de vos fichiers de configuration actuels. Pour passer à une version antérieure à une version, consultez la section [Rétrogradation d'une appliance autonome NetScaler](/fr-fr/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/downgrade-standalone-appliance.html).

Équilibrage de charge

May 5, 2023

- **Quelles sont les différentes politiques d'équilibrage de charge que je peux créer sur l'appliance NetScaler ?**

  Vous pouvez créer les types de politiques d'équilibrage de charge suivants sur l'appliance

NetScaler :

- Connexions moindres
- Round Robin
- Temps de réponse le plus court
- Bande passante minimale
- Moins de paquets
- Hachage d'URL
- Hachage du nom de domaine
- Hachage de l'adresse IP source
- Hachage de l'adresse IP de destination
- IP source - Hachage IP de destination
- Jeton
- LRTM

- **Puis-je garantir la sécurité de la batterie de serveurs Web en mettant en œuvre un équilibrage de charge à l'aide de l'appliance NetScaler ?**

  Oui. Vous pouvez garantir la sécurité d'une ferme de serveurs Web en mettant en œuvre un équilibrage de charge à l'aide de l'appliance NetScaler. L'appliance NetScaler vous permet d'implémenter les options suivantes de la fonctionnalité d'équilibrage de charge :

  - Masquage des adresses IP : vous permet d'installer les serveurs réels sur un espace d'adresses IP privé pour des raisons de sécurité et de conservation des adresses IP. Ce processus est transparent pour l'utilisateur final car l'appliance NetScaler accepte les demandes au nom du serveur. En mode masquage d'adresses, l'appliance isole complètement les deux réseaux. Par conséquent, un client peut accéder à un service s'exécutant sur le sous-réseau privé, tel qu'un serveur FTP ou Telnet, via un autre VIP sur l'appliance pour ce service.
  - Mappage des ports : permet d'héberger les services TCP réels sur des ports non standard pour des raisons de sécurité. Ce processus est transparent pour l'utilisateur final car l'appliance NetScaler accepte les demandes au nom du serveur sur l'adresse IP et le numéro de port standard annoncés.

- **Quels sont les différents appareils que je peux utiliser pour équilibrer la charge avec une appliance NetScaler ?**

  Vous pouvez équilibrer la charge des appareils suivants à l'aide d'une appliance NetScaler :

  - Batteries de serveurs
  - Caches ou proxies inverses
  - Dispositifs de pare-feu
  - Systèmes de détection d'intrusion
  - Appareils de déchargement SSL

  - Appareils de compression
  - Serveurs d'inspection de contenu

- **Pourquoi devrais-je implémenter la fonctionnalité d'équilibrage de charge pour le site Web ?**

  Vous pouvez implémenter la fonctionnalité d'équilibrage de charge pour le site Web afin de tirer les avantages suivants :

  - Réduisez le temps de réponse : lorsque vous implémentez la fonctionnalité d'équilibrage de charge pour le site Web, l'un des principaux avantages est l'augmentation du temps de chargement auquel vous pouvez vous attendre. Comme deux serveurs ou plus se partagent la charge du trafic Web, chacun des serveurs gère moins de trafic qu'un seul serveur. Cela signifie que davantage de ressources sont disponibles pour répondre aux demandes des clients. Cela se traduit par un site Web plus rapide.
  - Redondance : La mise en œuvre de la fonctionnalité d'équilibrage de charge introduit un peu de redondance. Par exemple, si le site est équilibré sur trois serveurs et que l'un d'eux ne répond pas du tout, les deux autres peuvent continuer à fonctionner et les visiteurs du site ne remarquent même pas de temps d'arrêt. Toute solution d'équilibrage de charge cesse immédiatement d'envoyer du trafic vers le serveur principal qui n'est pas disponible.

- **Pourquoi dois-je désactiver l'option MBF (Mac Based Forwarding) pour Link Load Balancing (LLB) ?**

  - Si vous activez l'option MBF, l'appliance NetScaler considère que le trafic entrant en provenance du client et le trafic sortant vers le même client transitent par le même routeur en amont. Toutefois, la fonctionnalité LLB nécessite que le meilleur chemin soit choisi pour le trafic de retour.
  - L'activation de l'option MBF rompt cette conception de topologie en envoyant le trafic sortant via le routeur qui a transféré le trafic client entrant.

- **Quels sont les différents types de persistance disponibles sur l'appliance NetScaler ?**

  L'appliance NetScaler prend en charge les types de persistance suivants :

  - IP source
  - Insert à biscuits
  - ID de session SSL
  - URL passive
  - ID de serveur personnalisé
  - Rule
  - DESTIP

GUI

May 5, 2023

- **Lorsque j'utilise Firefox pour comparer deux configurations NetScaler, le navigateur semble se figer ?**

  Firefox affiche finalement la différence entre les configurations, mais le processus prend beaucoup de temps s'il y a plus de 1000 différences. Utilisez Chrome pour une réponse plus rapide.

- **J'utilise un navigateur Mac Safari pour mettre à jour un NetScaler. Dans l'assistant de mise à niveau, lorsque je clique sur le bouton Parcourir pour sélectionner le fichier de génération dans l'appliance, la boîte de dialogue n'affiche aucun fichier ou dossier. De plus, lorsque je reviens au dossier racine, la boîte de dialogue affiche le dossier de niveau supérieur, mais je ne peux pas le parcourir. Que dois-je faire ?**

  Dans le navigateur Safari, cliquez sur l'icône Paramètres et accédez à **Préférences > Sécurité > Gérer les paramètres du site Web > Java**. Modifiez la valeur du paramètre **Lorsque vous visitez d'autres sites Web** sur Exécuter en mode non sécurisé.

- **Que dois-je faire avant d'accéder à l'interface graphique ?**

  Avant d'accéder à une nouvelle version du logiciel NetScaler :

  - Videz le cache du navigateur, y compris les cookies.
  - Accédez à l'interface graphique en mode navigation privée du navigateur.
  - Accéder à l'interface graphique dans un autre navigateur.
  - Désactivez l'option **Utiliser l'accélération logicielle** dans les paramètres et redémarrez le navigateur.
  - Accédez à **Chrome : extensions**, décochez la case **Activer** et redémarrez le navigateur Chrome.

- **Quel port dois-je ouvrir pour accéder à l'interface graphique en utilisant HTTP ou HTTPS ?**

  La liste suivante répertorie les numéros de port par défaut pour les services de gestion (GUI) HTTP et HTTPS dans les appliances NetScaler MPX, VPX et CPX :

  - Appliances NetScaler MPX et VPX : 80 (HTTP) et 443 (HTTPS)
  - Appliances NetScaler CPX : 9080 (HTTP) et 9443 (HTTPS)

  En outre, vous pouvez configurer des ports pour les services de gestion HTTP et HTTPS autres que les ports 80 et 443. Pour plus d'informations, voir Configurer les ports de gestion HTTP et HTTPS.

- **Avec quels navigateurs l'interface graphique est-elle compatible avec différents systèmes d'exploitation ?**

Le tableau suivant répertorie les navigateurs compatibles avec les versions 12.1, 13.0 et 13.1 de NetScaler GUI :

Système d'exploitation	Navigateur	Versions
Windows 10 et versions ultérieures	Bord	110.1587.63 et versions ultérieures
Windows 10 et versions ultérieures	Mozilla Firefox	102 et versions ultérieures
Windows 10 et versions ultérieures	Chrome	108 et versions ultérieures
MAC	Mozilla Firefox	10.0.1 et versions ultérieures
MAC	Safari	15.5 et versions ultérieures

SSL

August 20, 2021

Cliquez ici pour consulter les questions fréquentes sur SSL.

Authentification, autorisation et audit du trafic des applications

May 5, 2023

De nombreuses entreprises limitent l'accès au site Web aux seuls utilisateurs valides et contrôlent le niveau d'accès autorisé à chaque utilisateur. La fonctionnalité d'authentification, d'autorisation et d'audit permet à un administrateur de site de gérer les contrôles d'accès avec l'appliance NetScaler au lieu de gérer ces contrôles séparément pour chaque application. L'authentification sur la solution matérielle-logicielle permet également de partager ces informations sur tous les sites Web du même domaine qui sont protégés par la solution matérielle-logicielle.

Pour utiliser l'authentification, l'autorisation et l'audit, vous devez configurer des serveurs virtuels d'authentification pour gérer le processus d'authentification et des serveurs virtuels de gestion du trafic pour gérer le trafic vers les applications Web nécessitant une authentification. Vous configurez également votre DNS pour attribuer des noms de noms de noms de niveau de qualité à chaque serveur virtuel. Après avoir configuré les serveurs virtuels, vous configurez un compte utilisateur pour chaque utilisateur qui s'authentifiera via l'appliance NetScaler. Vous pouvez également créer des groupes et

attribuer des comptes utilisateurs à des groupes. Après avoir créé des comptes d'utilisateurs et des groupes, vous configurez des stratégies qui indiquent à la solution matérielle-logicielle comment authentifier les utilisateurs, quelles ressources autoriser les utilisateurs à accéder et comment consigner les sessions utilisateur. Pour mettre en œuvre les stratégies, vous liez chaque stratégie globalement, à un serveur virtuel spécifique ou aux comptes ou groupes d'utilisateurs appropriés. Après avoir configuré vos stratégies, vous personnalisez les sessions utilisateur en configurant les paramètres de session et en liant vos stratégies de session au serveur virtuel de gestion du trafic. Enfin, si votre intranet utilise des certificats clients, vous configurez la configuration du certificat client.

Pour comprendre le fonctionnement de l'authentification, de l'autorisation et de l'audit dans un environnement distribué, envisagez une organisation dotée d'un intranet auquel ses employés accèdent au bureau, à domicile et en déplacement. Le contenu de l'intranet est confidentiel et nécessite un accès sécurisé. Tout utilisateur souhaitant accéder à l'intranet doit disposer d'un nom d'utilisateur et d'un mot de passe valides. Pour répondre à ces exigences, l'ADC effectue les opérations suivantes :

- Redirige l'utilisateur vers la page de connexion s'il accède à l'intranet sans s'être connecté.
- Collecte les informations d'identification de l'utilisateur, les remet au serveur d'authentification et les met en cache dans un répertoire accessible via le protocole LDAP (Lightweight Directory Access Protocol). Pour plus d'informations, voir Déterminer les attributs dans votre annuaire LDAP.
- Vérifie que l'utilisateur est autorisé à accéder au contenu intranet spécifique avant de remettre la demande de l'utilisateur au serveur d'applications.
- Conserve un délai d'expiration de session après lequel les utilisateurs doivent s'authentifier à nouveau pour pouvoir accéder à nouveau à l'intranet. (Vous pouvez configurer le délai d'expiration.)
- Consigne l'accès de l'utilisateur, y compris les tentatives de connexion non valides, dans un journal d'audit.

types d'authentification pris en charge

- Local
- LDAP
- RADIUS
- SAML
- TACACS+
- Authentification du certificat client (incluant l'authentification par carte à puce)
- Web
- Une authentification avancée
- Authentification par formulaire
- Authentification basée sur 401

- OTP natif
- Notification Push
- Envoyer un e-mail à OTP
- reCAPTCHA

NetScaler Gateway prend également en charge RSA SecurID, Gemalto Protiva et SafeWord. Vous utilisez un serveur RADIUS pour configurer ces types d'authentification.

Avant de configurer l'authentification, l'autorisation et l'audit, vous devez connaître et comprendre comment configurer l'équilibrage de charge, la commutation de contenu et le protocole SSL sur l'appliance NetScaler.

Authentification sans autorisation

L'autorisation spécifie les ressources réseau auxquelles les utilisateurs ont accès lorsqu'ils ouvrent une session sur la solution matérielle-logicielle. Le paramètre par défaut de l'autorisation consiste à refuser l'accès à toutes les ressources réseau. Citrix recommande d'utiliser le paramètre global par défaut, puis de créer des stratégies d'autorisation pour définir les ressources réseau auxquelles les utilisateurs peuvent accéder.

Vous configurez l'autorisation sur la solution matérielle-logicielle à l'aide d'une stratégie d'autorisation et d'expressions. Après avoir créé une stratégie d'autorisation, vous pouvez la lier aux utilisateurs ou aux groupes que vous avez configurés sur l'appliance.

Vous pouvez configurer la solution matérielle-logicielle pour qu'elle utilise uniquement l'authentification, sans autorisation. Lorsque vous configurez l'authentification sans autorisation, la solution matérielle-logicielle n'effectue pas de vérification d'autorisation de groupe. Les stratégies que vous configurez pour l'utilisateur ou le groupe sont attribuées à l'utilisateur.

Activation de l'authentification, de l'autorisation et de l'audit

Pour utiliser la fonctionnalité d'authentification, d'autorisation et d'audit, vous devez l'activer. Vous pouvez configurer les entités d'authentification, d'autorisation et d'audit, telles que les serveurs virtuels d'authentification et de gestion du trafic, avant d'activer la fonctionnalité d'authentification, d'autorisation et d'audit, mais les entités ne fonctionnent pas tant que la fonctionnalité n'est pas activée.

Pour activer l'authentification, l'autorisation et l'audit à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer l'authentification, l'autorisation et l'audit et vérifier la configuration :


```
enable ns feature AAA
<!--NeedCopy-->
```

Pour activer l'authentification, l'autorisation et l'audit à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**.
2. Dans le volet d'informations, sous **Modes et fonctionnalités**, cliquez sur **Modifier les fonctionnalités de base**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités de base**, activez la case à cocher **Authentification, autorisation et audit** .
4. Cliquez sur **OK**.

Désactivation de l'authentification

Si votre déploiement ne nécessite pas d'authentification, vous pouvez le désactiver. Vous pouvez désactiver l'authentification pour chaque serveur virtuel qui ne nécessite pas d'authentification.

> **Important :**
>
> **Important :** Citrix recommande de désactiver l'authentification avec prudence. Si vous n'utilisez pas de serveur d'authentification externe, créez des utilisateurs et des groupes locaux pour permettre à la solution matérielle-logicielle d'authentifier les utilisateurs. La désactivation de l'authentification arrête l'utilisation des fonctionnalités d'authentification, d'autorisation et de comptabilité qui contrôlent et surveillent les connexions à l'appliance. Lorsque les utilisateurs saisissent une adresse Web pour se connecter à la solution matérielle-logicielle, la page d'ouverture de session n'apparaît pas.

Pour désactiver l'authentification

1. Accédez à **Configuration > NetScaler Gateway > Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans la page **Paramètres de base**, **désactivez la case à cocher Activer l'authentification** .

Fonctionnement de l'authentification, de l'autorisation et de l'audit

May 5, 2023

L'authentification, l'autorisation et l'audit assurent la sécurité d'un environnement Internet distribué en permettant à tout client disposant des informations d'identification appropriées de se connecter

en toute sécurité à des serveurs d'applications protégés depuis n'importe où sur Internet. Cette fonctionnalité intègre les trois fonctions de sécurité que sont l'authentification, l'autorisation et l'audit. L'authentification permet à NetScaler de vérifier les informations d'identification du client, localement ou auprès d'un serveur d'authentification tiers, et d'autoriser uniquement les utilisateurs approuvés à accéder aux serveurs protégés. L'autorisation permet à l'ADC de vérifier le contenu d'un serveur protégé auquel il autorise chaque utilisateur à accéder. L'audit permet à l'ADC de conserver un enregistrement de l'activité de chaque utilisateur sur un serveur protégé.

Pour comprendre le fonctionnement de l'authentification, de l'autorisation et de l'audit dans un environnement distribué, envisagez une organisation dotée d'un intranet auquel ses employés accèdent au bureau, à domicile et en déplacement. Le contenu de l'intranet est confidentiel et nécessite un accès sécurisé. Tout utilisateur souhaitant accéder à l'intranet doit disposer d'un nom d'utilisateur et d'un mot de passe valides. Pour répondre à ces exigences, l'ADC effectue les opérations suivantes :

- Redirige l'utilisateur vers la page de connexion s'il accède à l'intranet sans s'être connecté.
- Collecte les informations d'identification de l'utilisateur, les transmet au serveur d'authentification et les met en cache dans un répertoire accessible via LDAP. Pour plus d'informations, voir Déterminer les attributs dans votre annuaire LDAP.
- Vérifie que l'utilisateur est autorisé à accéder au contenu intranet spécifique avant de remettre la demande de l'utilisateur au serveur d'applications.
- Conserve un délai d'expiration de session après lequel les utilisateurs doivent s'authentifier à nouveau pour pouvoir accéder à nouveau à l'intranet. (Vous pouvez configurer le délai d'expiration.)
- Consigne l'accès de l'utilisateur, y compris les tentatives de connexion non valides, dans un journal d'audit.

Configuration des stratégies d'authentification, d'autorisation et d'audit

Après avoir configuré vos utilisateurs et groupes, vous configurez ensuite les stratégies d'authentification, les stratégies d'autorisation et les stratégies d'audit pour définir les utilisateurs autorisés à accéder à votre intranet, les ressources auxquelles chaque utilisateur ou groupe est autorisé à accéder, et le niveau d'authentification, d'autorisation et d'audit détaillé. sera conservé dans les journaux d'audit. Une stratégie d'authentification définit le type d'authentification à appliquer lorsqu'un utilisateur tente d'ouvrir une session. Si l'authentification externe est utilisée, la stratégie spécifie également le serveur d'authentification externe. Les stratégies d'autorisation spécifient les ressources réseau auxquelles les utilisateurs et les groupes peuvent accéder après leur ouverture de session. Les stratégies d'audit définissent le type et l'emplacement du journal d'audit.

Vous devez lier chaque stratégie pour la mettre en œuvre. Vous liez les stratégies d'authentification aux serveurs virtuels d'authentification, les stratégies d'autorisation à un ou plusieurs comptes ou

groupes d'utilisateurs et les stratégies d'audit globalement et à un ou plusieurs comptes ou groupes d'utilisateurs.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel nombre entier positif. Dans le système d'exploitation NetScaler, les priorités des politiques fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible. Par exemple, si vous avez trois stratégies avec des priorités de 10, 100 et 1000, la stratégie affectée d'une priorité de 10 est exécutée en premier, puis la stratégie attribuée une priorité de 100 et enfin la stratégie affectée d'un ordre de 1000. La fonctionnalité d'authentification, d'autorisation et d'audit implémente uniquement la première de chaque type de stratégie correspondant à une demande, et non les stratégies supplémentaires de ce type qu'une demande peut également correspondre. La priorité de stratégie est donc importante pour obtenir les résultats souhaités.

Vous pouvez vous laisser suffisamment d'espace pour ajouter d'autres stratégies dans n'importe quel ordre, tout en les définissant pour qu'elles soient évaluées dans l'ordre souhaité, en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous liez les stratégies. Vous pouvez ensuite ajouter des stratégies supplémentaires à tout moment sans avoir à réaffecter la priorité d'une stratégie existante.

Pour plus d'informations sur les politiques de liaison sur l'appliance NetScaler, consultez la documentation du produit NetScaler.

Configurer la stratégie No_Auth pour contourner certains trafic

Vous pouvez désormais configurer la stratégie No_Auth pour contourner certains trafics de l'authentification lorsque l'authentification basée sur 401 est activée sur le serveur virtuel de gestion du trafic. Pour ce type de trafic, vous devez lier une stratégie « No_Auth ».

Pour configurer la stratégie No_Auth afin de contourner certains trafics à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add authentication policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Exemple :

```
add authentication policy ldap -rule ldapAct1 -action No_Auth
<!--NeedCopy-->
```


Composants de base de la configuration de l'authentification, de l'autorisation et de l'audit

May 5, 2023

Les composants de base de la configuration d'authentification, d'autorisation et d'audit sont les suivants :

- **Serveur virtuel d'authentification** : toutes les demandes d'authentification sont redirigées par le serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu) vers le serveur virtuel d'authentification. Ce serveur virtuel traite les stratégies d'authentification associées et donne donc accès à l'application. Pour plus de détails, voir Serveur virtuel d'authentification.
- **Profils d'** authentification - Un profil d'authentification spécifie le serveur virtuel d'authentification, l'hôte d'authentification, le domaine d'authentification et un niveau d'authentification.

Vous pouvez créer un ou plusieurs profils d'authentification pour spécifier différents paramètres d'authentification et lier ces profils d'authentification aux serveurs de gestion du trafic pertinents en fonction de vos besoins. Pour plus de détails, voir Profils d'authentification.

- **Politiques d'authentification** : lorsque les utilisateurs se connectent à l'appliance NetScaler ou NetScaler Gateway, ils sont authentifiés conformément à une politique que vous créez. Une politique d'authentification comprend une expression et une action. Les politiques d'authentification utilisent des expressions NetScaler. Pour plus de détails, voir Stratégies d'authentification.
- **Stratégies d'autorisation** - Lorsque vous configurez une stratégie d'autorisation, vous pouvez la définir pour autoriser ou refuser l'accès aux ressources réseau du réseau interne. Pour plus de détails, voir Stratégies d'autorisation.
- **Utilisateurs et groupes :** - Après avoir configuré la configuration de base de l'authentification, de l'autorisation et de l'audit, vous créez des utilisateurs et des groupes. Vous créez d'abord un compte utilisateur pour chaque personne qui s'authentifiera via l'appliance NetScaler. Si vous utilisez l'authentification locale contrôlée par l'appliance NetScaler elle-même, vous créez des comptes d'utilisateurs locaux et attribuez des mots de passe à chacun de ces comptes. Pour plus de détails, voir Utilisateurs et groupes.

Authentification serveur virtuel

May 5, 2023

Le serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu) redirige toutes les demandes d'authentification vers le serveur virtuel d'authentification. Ce serveur virtuel traite les stratégies d'authentification associées et donne donc accès à l'application.

Remarque : Vous ne pouvez pas lier les stratégies de gestion du trafic aux serveurs virtuels d'authentification, d'autorisation et d'audit.

Configurer le serveur virtuel d'authentification

Les étapes de configuration d'un serveur virtuel d'authentification sont les suivantes :

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit.

```
enable ns feature AAA
<!--NeedCopy-->
```

2. Configurez un serveur virtuel d'authentification. Il doit être de type SSL et assurez-vous de lier la paire de clés de certificat SSL au serveur virtuel.

```
add authentication vserver <name> SSL <ipaddress> <port>

bind ssl certkey <auth-vserver-name> <certkey>
<!--NeedCopy-->
```

3. Spécifiez le nom de domaine complet du domaine pour le serveur virtuel d'authentification.

```
set authentication vserver <name> -authenticationDomain <FQDN>
<!--NeedCopy-->
```

4. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic concerné.

   Points à noter :

   - Le nom de domaine complet du serveur virtuel de gestion du trafic doit se trouver dans le même domaine que le nom de domaine complet du serveur virtuel d'authentification pour que le cookie de session de domaine fonctionne correctement. Sur le serveur virtuel de gestion du trafic :
     - Activez l'authentification.
     - Spécifiez le nom de domaine complet du serveur virtuel d'authentification en tant qu'hôte d'authentification du serveur virtuel de gestion du trafic.
     - [Facultatif] Spécifiez le domaine d'authentification sur le serveur virtuel de gestion du trafic.
     - Si vous ne configurez pas le domaine d'authentification, l'appliance affecte un nom de domaine complet constitué du nom de domaine complet du serveur

virtuel d'authentification sans la partie nom d'hôte. Par exemple, si le nom de domaine du serveur virtuel d'authentification est **tm.xyz.bar.com**, l'appliance affecte **xyz.bar.com** comme domaine d'authentification.

* Pour l'équilibrage de charge :

```
set lb vserver <name> -authentication ON -
   authenticationhost <FQDN> [-authenticationdomain <
   authdomain>]
<!--NeedCopy-->
```

* Pour le changement de contenu :

```
set cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

- Si vous devez définir un cookie à l'échelle du domaine pour un domaine d'authentification, vous devez activer le profil d'authentification sur un serveur virtuel d'équilibrage de charge.

5. Vérifiez que les deux serveurs virtuels sont actifs et configurés correctement.

```
show authentication vserver <name>
<!--NeedCopy-->
```

Pour configurer un serveur virtuel d'authentification à l'aide de l'interface graphique

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit.

   Accédez à **Système > Paramètres**, cliquez sur **Configurer les fonctionnalités de base**et activez **l'authentification, l'autorisation et l'audit**.

2. Configurez le serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**, puis configurez le cas échéant.

3. Configurez le serveur virtuel de gestion du trafic pour l'authentification.

   - **Pour l'équilibrage de charge :**

     Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis configurez le serveur virtuel selon vos besoins.

   - **Pour le changement de contenu :**

     Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis configurez le serveur virtuel selon vos besoins.

4. • Vérifiez la configuration de l'authentification.

   Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**, puis vérifiez les détails du serveur virtuel d'authentification correspondant.

Configurez le serveur virtuel d'authentification

Pour configurer l'authentification, l'autorisation et l'audit, configurez d'abord un serveur virtuel d'authentification pour gérer le trafic d'authentification. Ensuite, liez une paire de clés de certificat SSL au serveur virtuel pour lui permettre de gérer les connexions SSL.
Pour plus d'informations sur la configuration de SSL et la création d'une paire de clés de certificat, voir Certificats SSL.

Configurer un serveur virtuel d'authentification à l'aide de l'interface de ligne de commande

Pour configurer un serveur virtuel d'authentification et vérifier la configuration, à l'invite de commandes, tapez les commandes suivantes dans le même ordre :

```
add authentication vserver <name> ssl <ipaddress>

show authentication vserver <name>

bind ssl certkey <certkeyName>

show authentication vserver <name>

set authentication vserver <name>

show authentication vserver <name>
<!--NeedCopy-->
```

Exemple :

```
add authentication vserver Auth-Vserver-2 SSL 10.102.29.77 443 Done

show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
    ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
    Primary Vserver On Down : DISABLED Authentication : ON Current AAA
    Users: 0 Done

bind ssl certkey Auth-Vserver-2 Auth-Cert-1 Done

```



```
show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: UP Client Idle Timeout
    : 180 sec Down state flush: DISABLED Disable Primary Vserver On Down
     : DISABLED Authentication : ON Current AAA Users: 0 Done

set authentication vserver Auth-Vserver-2

show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
    ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
    Primary Vserver On Down : DISABLED Authentication : ON Current AAA
    Users: 0 Done
<!--NeedCopy-->
```

> **Remarque**
>
> Le paramètre Authentication Domain est obsolète. Utilisez le profil d'authentification pour définir des cookies à l'échelle du domaine.

Configuration d'un serveur virtuel d'authentification à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau serveur virtuel d'authentification, cliquez sur **Ajouter**.
   - Pour modifier un serveur virtuel d'authentification existant, sélectionnez le serveur virtuel, puis cliquez sur **Modifier**. La boîte de dialogue Configuration s'ouvre avec la zone Paramètres de base développée.
3. Spécifiez les valeurs des paramètres comme suit (un astérisque indique un paramètre obligatoire) :
   - Nom* : nom (ne peut pas être modifié pour un serveur virtuel créé précédemment)
   - Type d'adresse IP* : type d'adresse IP du serveur virtuel d'authentification
   - Adresse IP* : adresse IP du serveur virtuel d'authentification
   - PORT* : port TCP sur lequel le serveur virtuel accepte les connexions.
   - Failed login timeout : failedLoginTimeout (secondes autorisées avant l'échec de la connexion, et l'utilisateur doit recommencer le processus de connexion.)
   - Tentatives de connexion maximales : maxLoginAttempts (nombre de tentatives de connexion autorisées avant que l'utilisateur ne soit verrouillé)

   > **Remarque :**
   >
   > Le serveur virtuel d'authentification utilise uniquement le protocole SSL et le port 443. Ces

> options sont donc grisées. Toutes les options qui ne sont pas mentionnées peuvent être ignorées.

4. Cliquez sur **Continuer** pour afficher la zone Certificats.
5. Dans la zone **Certificats**, configurez tous les certificats SSL que vous souhaitez utiliser avec ce serveur virtuel.
    - Pour configurer un certificat d'autorité de certification, cliquez sur la flèche à droite de Certificat d'autorité de certification pour afficher la boîte de dialogue Clé de certificat d'autorité de certification, sélectionnez le certificat que vous souhaitez lier à ce serveur virtuel, puis cliquez sur **Enregistrer**.
    - Pour configurer un certificat de serveur, cliquez sur la flèche à droite de Certificat de serveur et suivez le même processus que pour le certificat d'autorité de certification.
6. Cliquez sur **Continuer** pour afficher la zone **Stratégies d'authentification avancées** .
7. Si vous souhaitez lier une stratégie d'authentification avancée au serveur virtuel, cliquez sur la flèche située à droite de la ligne pour afficher la boîte de dialogue **Stratégie d'authentification**, choisissez la stratégie à lier au serveur, définissez la priorité, puis cliquez sur **OK**.
8. Cliquez sur **Continuer** pour afficher la zone **Stratégies d'authentification de base** .
9. Si vous souhaitez créer une stratégie d'authentification de base et la lier au serveur virtuel, cliquez sur le signe plus pour afficher la boîte de dialogue **Stratégies**, puis suivez les invites pour configurer la stratégie et la lier à ce serveur virtuel.
10. Cliquez sur **Continuer** pour afficher la zone Serveurs virtuels 401.
11. Dans la zone Serveurs virtuels 401, configurez tous les serveurs virtuels d'équilibrage de charge ou de commutation de contenu que vous souhaitez lier à ce serveur virtuel.
    - Pour lier un serveur virtuel d'équilibrage de charge, cliquez sur la flèche située à droite du serveur virtuel d'équilibrage de charge pour afficher la boîte de dialogue Serveurs virtuels d'équilibrage de charge, puis suivez les instructions.
    - Pour lier un serveur virtuel de commutation de contenu, cliquez sur la flèche située à droite du serveur virtuel de commutation de contenu pour afficher la boîte de dialogue Serveurs virtuels de commutation de contenu et suivez le même processus que pour lier un serveur virtuel de base de données.
12. Si vous souhaitez créer ou configurer un groupe, dans la zone Groupes, cliquez sur la flèche pour afficher la boîte de dialogue Groupes, puis suivez les instructions.
13. Vérifiez vos paramètres et, lorsque vous avez terminé, cliquez sur **Terminé**. La boîte de dialogue se ferme. Si vous avez créé un nouveau serveur virtuel d'authentification, il apparaît désormais dans la liste de la fenêtre **Configuration** .

Serveur virtuel de gestion du trafic

Après avoir créé et configuré votre serveur virtuel d'authentification, vous devez ensuite créer ou configurer un serveur virtuel de gestion du trafic et y associer votre serveur virtuel d'authentification. Vous pouvez utiliser un serveur virtuel d'équilibrage de charge ou de commutation de contenu pour un serveur virtuel de gestion du trafic.
Pour plus d'informations sur la création et la configuration de l'un ou l'autre type de serveur virtuel, reportez-vous au *Guide Citrix Traffic Management* dans Traffic Management.

> **Remarque :**
>
> le nom de domaine complet du serveur virtuel de gestion du trafic doit se trouver dans le même domaine que le nom de domaine complet du serveur virtuel d'authentification pour que le cookie de session de domaine fonctionne correctement.

Vous configurez un serveur virtuel de gestion du trafic pour l'authentification, l'autorisation et l'audit en activant l'authentification, puis en attribuant le nom de domaine complet du serveur d'authentification au serveur virtuel de gestion du trafic. Vous pouvez également configurer le domaine d'authentification sur le serveur virtuel de gestion du trafic actuellement. Si vous ne configurez pas cette option, l'appliance NetScaler attribue au serveur virtuel de gestion du trafic un nom de domaine complet composé du nom de domaine complet du serveur virtuel d'authentification sans la partie nom d'hôte. Par exemple, si le nom de domaine du serveur virtuel d'authentification est tm.xyz.bar.com, l'appliance affecte xyz.bar.com. comme domaine d'authentification.

Pour configurer un serveur virtuel de gestion du trafic à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'un des jeux de commandes suivants :

```
set lb vserver <name>  - authentication ON -authenticationhost <FQDN> [-
    authenticationdomain <authdomain>]
show lb vserver <name>
set cs vserver <name>  - authentication ON -authenticationhost <FQDN> [-
    authenticationdomain <authdomain>]
show cs vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vs-cont-sw -Authentication ON -AuthenticationHost mywiki
    .index.com Done

show lb vserver vs-cont-sw vs-cont-sw (0.0.0.0:0) - TCP Type: ADDRESS
    State: DOWN Last state change was at Wed Aug 19 10:03:15 2009 (+410
```



```
    ms) Time since last state change: 5 days, 20:00:40.290 Effective
    State: DOWN Client Idle Timeout: 9000 sec Down state flush: ENABLED
    Disable Primary Vserver On Down : DISABLED No. of Bound Services : 0
     (Total) 0 (Active) Configured Method: LEASTCONNECTION Mode: IP
    Persistence: NONE Connection Failover: DISABLED Authentication: ON
    Host: mywiki.index.com
4 Done
5 <!--NeedCopy-->
```

Pour configurer un serveur virtuel de gestion du trafic à l'aide de l'interface graphique

1. Dans le volet de navigation, effectuez l'une des opérations suivantes.
   - Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
   - Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**
   - Dans le volet d'informations, sélectionnez le serveur virtuel sur lequel vous souhaitez activer l'authentification, puis cliquez sur **Modifier**.
   - Dans la zone de texte Domaine, tapez le domaine d'authentification.
   - Dans le menu **Avancé** de droite, sélectionnez **Authentification**.
   - Sélectionnez **Authentification basée sur un formulaire ou Authentificationbasée sur 401**, puis renseignez les informations d'authentification.
     - Pour Authentification basée sur un formulaire, entrez le nom de domaine complet de l'authentification (nom de domaine complet du serveur d'authentification), le serveur virtuel d'authentification (l'adresse IP du serveur virtuel d'authentification) et le profil d'authentification (le profil à utiliser pour l'authentification).
     - Pour l'authentification basée sur 401, entrez le serveur virtuel d'authentification et le profil d'authentification uniquement.
   - Cliquez sur **OK**. Un message apparaît dans la barre d'état, indiquant que le serveur virtuel a été correctement configuré.

Prise en charge simplifiée du protocole de connexion pour l'authentification, l'autorisation et l'audit

Le protocole de connexion entre les serveurs virtuels d'authentification, d'autorisation et d'audit de gestion du trafic et les serveurs virtuels d'authentification, d'autorisation et d'audit est simplifié pour utiliser des mécanismes internes plutôt que d'envoyer les données chiffrées via des paramètres de requête. Cette fonctionnalité empêche la relecture des demandes.

Configurer le DNS

Pour que le cookie de session de domaine utilisé dans le processus d'authentification fonctionne correctement, vous devez configurer DNS pour affecter à la fois l'authentification et les serveurs virtuels de gestion du trafic aux FQDN dans le même domaine. Pour plus d'informations sur la configuration des enregistrements d'adresses DNS, voir Système de noms de domaine.

Vérifier l'authentification serveur virtuel

Après avoir configuré les serveurs virtuels d'authentification et de gestion du trafic et avant de créer des comptes d'utilisateurs, vous devez vérifier que les deux serveurs virtuels sont correctement configurés et qu'ils sont à l'état UP.

Configurer une authentification NoAuth à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
show authentication vserver <name>
<!--NeedCopy-->
```

Exemple :

```
show authentication vserver Auth-Vserver-2
Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
State: UP
Client Idle Timeout: 180 sec
Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Authentication : ON
Current AAA Users: 0
Authentication Domain: myCompany.employee.com
Done
<!--NeedCopy-->
```

Configurer une authentification NoAuth à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler AAA - Trafic d'applications > Serveurs virtuels**.
   Remarque : Dans NetScaler Gateway, accédez à **NetScaler Gateway**> Serveurs virtuels.
2. Consultez les informations du volet **Serveurs virtuels AAA** pour vérifier que votre configuration est correcte et que votre serveur virtuel d'authentification accepte le trafic. Vous pouvez sélectionner un serveur virtuel spécifique pour afficher des informations détaillées dans le volet de détails.

Stratégies d'autorisation

May 5, 2023

Lorsque vous configurez une stratégie d'autorisation, vous pouvez la définir pour autoriser ou refuser l'accès aux ressources réseau du réseau interne. Par exemple, pour autoriser les utilisateurs à accéder au réseau 10.3.3.0, utilisez l'expression suivante :

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

Les stratégies d'autorisation sont appliquées aux utilisateurs et aux groupes. Une fois qu'un utilisateur est authentifié, NetScaler Gateway effectue une vérification d'autorisation de groupe en obtenant les informations de groupe de l'utilisateur auprès d'un serveur RADIUS, LDAP ou TACACS+. Si les informations de groupe sont disponibles pour l'utilisateur, NetScaler Gateway vérifie les ressources réseau autorisées pour le groupe.

Pour contrôler les ressources auxquelles les utilisateurs peuvent accéder, vous devez créer des stratégies d'autorisation. Si vous n'avez pas besoin de créer des stratégies d'autorisation, vous pouvez configurer l'autorisation globale par défaut.

Si vous créez une expression dans la stratégie d'autorisation qui refuse l'accès à un chemin d'accès au fichier, vous ne pouvez utiliser que le chemin d'accès au sous-répertoire et non le répertoire racine. Par exemple, utilisez fs.path contient « \ \ dir1 \ \ dir2" au lieu de fs.path contient « \ \ rootdir \ \ dir1 \ \ dir2". Si vous utilisez la deuxième version de cet exemple, la stratégie échoue.

Après avoir configuré la politique d'autorisation, vous la liez à un utilisateur ou à un groupe.

Par défaut, les stratégies d'autorisation sont d'abord validées par rapport aux stratégies que vous liez au serveur virtuel, puis par rapport aux stratégies liées globalement. Si vous liez une stratégie globalement et que vous souhaitez qu'elle soit prioritaire sur une stratégie que vous liez à un utilisateur, un groupe ou un serveur virtuel, vous pouvez modifier le numéro de priorité de la stratégie. Les numéros de priorité commencent à zéro. Un numéro de priorité inférieur donne à la stratégie une priorité plus élevée.

Par exemple, si la stratégie globale a un numéro de priorité et que l'utilisateur a une priorité de deux, la stratégie d'authentification globale est appliquée en premier.

> **Important :**
>
> - Les stratégies d'autorisation classiques sont appliquées uniquement au trafic TCP.
> - La stratégie d'autorisation avancée peut être appliquée à tous les types de trafic (TCP/UDP/ICMP/DNS).
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.

> - While binding, if “type” is not explicitly mentioned or “type” is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
> - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

Pour plus d’informations sur les stratégies d’autorisation avancées, consultez l’article https://support.citrix.com/article/CTX232237.

Configurer et lier une politique d’autorisation

Configuration d’une politique d’autorisation à l’aide de l’interface graphique

1. Accédez à **NetScaler Gateway > Politiques > Autorisation**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la stratégie.
4. Dans **Action**, sélectionnez **Autoriser** ou **Refuser**.
5. Dans **Expression**, cliquez sur **Expression Editor**.
6. Pour commencer à configurer l’expression, cliquez sur **Sélectionner** et choisissez les éléments nécessaires.
7. Cliquez sur **Terminé** lorsque votre expression est terminée.
8. Cliquez sur **Create**.

Lier une politique d’autorisation à un utilisateur à l’aide de l’interface graphique

1. Accédez à **NetScaler Gateway > Administration des utilisateurs**.
2. Cliquez sur **Utilisateurs AAA**.
3. Dans le volet d’informations, sélectionnez un utilisateur, puis cliquez sur **Modifier**.
4. Dans les **paramètres avancés**, cliquez sur **Stratégies d’autorisation**.
5. Dans **la page Liaison** de stratégie, sélectionnez une stratégie ou créez une stratégie.
6. Dans **Priorité**, définissez le numéro de priorité.
7. Dans **Type**, sélectionnez le type de demande, puis cliquez sur **OK**.

Lier une politique d’autorisation à un groupe à l’aide de l’interface graphique

1. Accédez à **NetScaler Gateway > Administration des utilisateurs**.
2. Cliquez sur **AAA Groups**.
3. Dans le volet d’informations, sélectionnez un groupe, puis cliquez sur **Modifier**.
4. Dans les **paramètres avancés**, cliquez sur **Stratégies d’autorisation**.
5. Dans **la page Liaison** de stratégie, sélectionnez une stratégie ou créez une stratégie.
6. Dans **Priorité**, définissez le numéro de priorité.

7. Dans **Type**, sélectionnez le type de demande, puis cliquez sur **OK**.

L'autorisation spécifie les ressources réseau auxquelles les utilisateurs ont accès lorsqu'ils se connectent à NetScaler Gateway. Le paramètre par défaut de l'autorisation consiste à refuser l'accès à toutes les ressources réseau. Citrix recommande d'utiliser le paramètre global par défaut, puis de créer des stratégies d'autorisation pour définir les ressources réseau auxquelles les utilisateurs peuvent accéder.

Vous configurez l'autorisation sur NetScaler Gateway à l'aide d'une stratégie et d'expressions d'autorisation. Après avoir créé une stratégie d'autorisation, vous pouvez la lier aux utilisateurs ou aux groupes que vous avez configurés sur l'appliance.

Autorisation globale par défaut

Pour définir les ressources auxquelles les utilisateurs ont accès sur le réseau interne, vous pouvez configurer l'autorisation globale par défaut. Vous configurez l'autorisation globale en autorisant ou en refusant l'accès aux ressources réseau globalement sur le réseau interne.

Toute action d'autorisation globale que vous créez est appliquée à tous les utilisateurs auxquels aucune stratégie d'autorisation n'est déjà associée, soit directement, soit par l'intermédiaire d'un groupe. Une stratégie d'autorisation d'utilisateur ou de groupe remplace toujours l'action d'autorisation globale. Si l'action d'autorisation par défaut est définie sur Refuser, vous devez appliquer des politiques d'autorisation à tous les utilisateurs ou groupes afin de rendre les ressources réseau accessibles à ces utilisateurs ou groupes. Cette exigence contribue à améliorer la sécurité.

Pour définir l'autorisation globale par défaut :

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres généraux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet Sécurité, en regard de Action d'autorisation par défaut, sélectionnez Autoriser ou Refuser, puis cliquez sur OK.

Profils d'authentification

May 5, 2023

Lorsque vous souhaitez que les mêmes paramètres d'authentification soient utilisés par plusieurs serveurs virtuels de gestion du trafic, vous pouvez créer un profil d'authentification qui spécifie le serveur virtuel d'authentification, l'hôte d'authentification, le domaine d'authentification et le niveau d'authentification.

Ce profil d'authentification peut être associé aux serveurs virtuels de gestion du trafic concernés.

Configuration d'un profil d'authentification

Configurer un profil d'authentification à l'aide de l'interface de ligne de commande

- Créez le profil d'authentification et définissez les paramètres requis.

  Par exemple, pour créer un profil avec un serveur virtuel d'authentification nommé « AuthVS ».

```
add authentication authnProfile authProfile1 -authnVsName authVS
   -authenticationHost authnVS.example.com -authenticationDomain
   example.com -authenticationLevel
<!--NeedCopy-->
```

> **Remarque :**
>
> Le poids ou le niveau d'authentification dépend du serveur virtuel auquel le trafic est lié. Une session créée en s'authentifiant auprès du serveur virtuel de gestion du trafic à un niveau donné ne peut pas être utilisée pour accéder au serveur virtuel de gestion du trafic à un niveau supérieur.

- Liez le profil d'authentification aux serveurs virtuels de gestion du trafic concernés.

  Par exemple, pour lier AuthProfile1 à un serveur virtuel d'équilibrage de charge nommé « vserver1 ».

```
set lb vserver vserver1 -authnProfile authProfile1
<!--NeedCopy-->
```

Configuration d'un profil d'authentification à l'aide de l'interface graphique

Dans l'onglet **Configuration**, accédez à **Security > AAA - Application Traffic > Profil d'authentification**, puis configurez le profil d'authentification selon vos besoins.

> **Remarque :**
>
> - Vous pouvez également créer un profil d'authentification à l'aide de l'assistant NetScaler Gateway. Le profil contient tous les paramètres de la politique d'authentification. Vous configurez le profil lorsque vous créez la stratégie d'authentification.
> - Avec l'assistant NetScaler Gateway, vous pouvez utiliser le type d'authentification choisi pour configurer l'authentification. Si vous souhaitez configurer d'autres stratégies d'authentification après l'exécution de l'Assistant, vous pouvez utiliser l'utilitaire de configuration. Pour plus d'informations sur l'assistant NetScaler Gateway, voir Configuration des paramètres à l'aide de l'assistant NetScalerGateway].

Stratégies d'authentification

May 5, 2023

Lorsque les utilisateurs se connectent à l'appliance NetScaler ou NetScaler Gateway, ils sont authentifiés conformément à une politique que vous créez. Une politique d'authentification comprend une expression et une action. Les politiques d'authentification utilisent des expressions NetScaler.

Après avoir créé une action d'authentification et une stratégie d'authentification, liez-la à un serveur virtuel d'authentification et attribuez-lui une priorité. Lors de la liaison, désignez-la également en tant que stratégie principale ou secondaire. Les politiques primaires sont évaluées avant les politiques secondaires. Dans les configurations qui utilisent les deux types de stratégie, les stratégies principales sont normalement des stratégies plus spécifiques tandis que les stratégies secondaires sont normalement des stratégies plus générales. Il est destiné à gérer l'authentification de tous les comptes d'utilisateurs qui ne répondent pas aux critères plus spécifiques. La stratégie définit le type d'authentification. Une stratégie d'authentification unique peut être utilisée pour des besoins d'authentification simples et est généralement liée au niveau global. Vous pouvez également utiliser le type d'authentification par défaut, qui est local. Si vous configurez l'authentification locale, vous devez également configurer les utilisateurs et les groupes sur l'appliance.

Vous pouvez configurer plusieurs stratégies d'authentification et les lier pour créer une procédure d'authentification détaillée et des serveurs virtuels. Par exemple, vous pouvez configurer l'authentification en cascade et à deux facteurs en configurant plusieurs stratégies. Vous pouvez également définir la priorité des stratégies d'authentification afin de déterminer quels serveurs et l'ordre dans lequel l'appliance vérifie les informations d'identification des utilisateurs. Une stratégie d'authentification inclut une expression et une action. Par exemple, si vous définissez l'expression sur la valeur True, lorsque les utilisateurs ouvrent une session, l'action évalue l'ouverture de session utilisateur sur True, puis les utilisateurs ont accès aux ressources réseau.

Après avoir créé une stratégie d'authentification, vous liez la stratégie au niveau global ou aux serveurs virtuels. Lorsque vous liez au moins une stratégie d'authentification à un serveur virtuel, les stratégies d'authentification que vous avez liées au niveau global ne sont pas utilisées lorsque les utilisateurs ouvrent une session sur le serveur virtuel, sauf si le type d'authentification globale a une priorité supérieure à la stratégie liée au serveur virtuel.

Lorsqu'un utilisateur ouvre une session sur l'appliance, l'authentification est évaluée dans l'ordre suivant :

- Le serveur virtuel est vérifié pour détecter toute stratégie d'authentification liée.
- Si les stratégies d'authentification ne sont pas liées au serveur virtuel, l'appliance vérifie les stratégies d'authentification globales.
- Si une stratégie d'authentification n'est pas liée à un serveur virtuel ou globalement, l'utilisateur est authentifié via le type d'authentification par défaut.

Si vous configurez des stratégies d'authentification LDAP et RADIUS et que vous souhaitez lier les stratégies globalement pour l'authentification à deux facteurs, vous pouvez sélectionner la stratégie dans l'utilitaire de configuration, puis choisir si la stratégie est le type d'authentification principal ou secondaire. Vous pouvez également configurer une stratégie d'extraction de groupe.

> **Remarque :**
>
> L'appliance NetScaler ou NetScaler Gateway code uniquement des caractères UTF-8 à des fins d'authentification et n'est pas compatible avec les serveurs utilisant les caractères ISO-8859-1.

Création d'une stratégie d'authentification

Créer une stratégie d'authentification à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**, puis sélectionnez le type de stratégie que vous souhaitez créer.
   Pour NetScaler Gateway, accédez à **NetScaler Gateway > Politiques**Authentification.
2. Dans le volet d'informations, sous **l'onglet Stratégies**, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle stratégie, cliquez sur **Ajouter**.
   - Pour modifier une stratégie existante, sélectionnez l'action, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue Créer une stratégie d'authentification ou Configurer une stratégie d'authentification, tapez ou sélectionnez les valeurs des paramètres.
   - **Nom** : nom de la stratégie (ne peut pas être modifié pour une action précédemment configurée)
   - **Type d'authentification** : `authtype`
   - **Serveur** — `authVsName`
   - **Expression** : règle (Vous entrez des expressions en choisissant d'abord le type d'expression dans la liste déroulante la plus à gauche sous la fenêtre Expression, puis en saisissant votre expression directement dans la zone de texte de l'expression, ou en cliquant sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant la liste déroulante pour construire votre expression.)
4. Cliquez sur **Créer** ou **sur OK**. La stratégie que vous avez créée s'affiche sur la page Stratégies.
5. Cliquez sur l'onglet **Serveurs** et, dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour utiliser un serveur existant, sélectionnez-le, puis cliquez sur.
   - Pour créer un serveur, cliquez sur Ajouter et suivez les instructions.

6. Si vous souhaitez désigner cette stratégie en tant que stratégie d'authentification secondaire, sous l'onglet Authentification, cliquez sur Secondaire. Si vous souhaitez désigner cette stratégie en tant que stratégie d'authentification principale, ignorez cette étape.
7. Cliquez sur **Insérer une stratégie**.
8. Choisissez la stratégie que vous souhaitez lier au serveur virtuel d'authentification dans la liste déroulante.
9. Dans la colonne **Priorité** de gauche, modifiez la priorité par défaut pour vous assurer que la stratégie est évaluée dans le bon ordre.
10. Cliquez sur **OK**. Un message apparaît dans la barre d'état, indiquant que la stratégie a été correctement configurée.

Modifier une stratégie d'authentification à l'aide de l'interface graphique

Vous pouvez modifier les stratégies et profils d'authentification configurés, tels que l'adresse IP du serveur d'authentification ou l'expression.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **NetScaler Gateway > Politiques > Authentification**.
   Remarque : Vous pouvez également configurer la stratégie dans **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**, puis sélectionner le type de stratégie que vous souhaitez modifier.
2. Dans le volet de navigation, sous Authentification, sélectionnez un type d'authentification.
3. Dans le volet d'informations, sous l'onglet Serveurs, sélectionnez un serveur, puis cliquez sur Ouvrir.

Supprimer une stratégie d'authentification à l'aide de l'interface graphique

Si vous avez modifié ou supprimé un serveur d'authentification de votre réseau, supprimez la politique d'authentification correspondante de NetScaler Gateway.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **NetScaler Gateway > Politiques > Authentification**.
   Remarque : Pour configurer à partir d'ADC, accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**, puis sélectionnez le type de stratégie que vous souhaitez supprimer.
2. Dans le volet de navigation, sous Authentification, sélectionnez un type d'authentification.
3. Dans le volet d'informations, sous l'onglet Stratégies, sélectionnez une stratégie, puis cliquez sur Supprimer.

Créer une stratégie d'authentification à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes :

```
add authentication negotiatePolicy <name> <rule> <reqAction>

show authentication localPolicy <name>

bind authentication vserver <name> -policy <policyname> [-priority <
   priority>][-secondary]]

show authentication vserver <name>
<!--NeedCopy-->
```

Exemple :

```
add authentication localPolicy Authn-Pol-1 ns_true
Done

show authentication localPolicy
1)      Name: Authn-Pol-1       Rule: ns_true          Request action:
   LOCAL   Done

bind authentication vserver Auth-Vserver-2 -policy Authn-Pol-1
Done

show authentication vserver Auth-Vserver-2
Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT State: UP Client
   Idle
Timeout: 180 sec Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Authentication : ON
Current AAA Users: 0
Authentication Domain: myCompany.employee.com
1)  Primary authentication policy name:  Authn-Pol-1 Priority: 0
Done
<!--NeedCopy-->
```

Modifier une stratégie d'authentification à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour modifier une stratégie d'authentification existante :

```
set authentication localPolicy <name> <rule> [-reqaction <action>]
<!--NeedCopy-->
```


Exemple

```
set authentication localPolicy Authn-Pol-1 'ns_true'
<!--NeedCopy-->
```

Supprimer une stratégie d'authentification à l'aide de la CLI

À l'invite de commandes, tapez la commande suivante pour supprimer une stratégie d'authentification :

```
rm authentication localPolicy <name>
<!--NeedCopy-->
```

Exemple

```
rm authentication localPolicy Authn-Pol-1
<!--NeedCopy-->
```

Lier une stratégie d'authentification

Après avoir configuré les stratégies d'authentification, vous les liez globalement ou à un serveur virtuel. Vous pouvez utiliser l'utilitaire de configuration pour lier une stratégie d'authentification.

Pour lier une stratégie d'authentification globalement à l'aide de l'utilitaire de configuration :

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **NetScaler Gateway > Politiques > Authentification**.
   Remarque : Pour configurer à partir d'ADC, accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**
2. Cliquez sur un type d'authentification.
3. Dans le volet d'informations, sous l'onglet Stratégies, cliquez sur un serveur, puis dans Action, cliquez sur **Liaisons globales**.
4. Dans l'onglet Principal ou Secondaire, sous Détails, cliquez sur **Insérer une stratégie**.
5. Sous Nom de la stratégie, sélectionnez la stratégie, puis cliquez sur **OK**.

   Remarque : Lorsque vous sélectionnez la politique, NetScaler Gateway attribue automatiquement à l'expression la valeur True.

Pour dissocier une stratégie d'authentification globale à l'aide de l'utilitaire de configuration :

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **NetScaler Gateway > Politiques > Authentification**.
   Remarque : Pour configurer à partir d'ADC, accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification**
2. Dans l'onglet Stratégies, dans Action, cliquez sur **Liaisons globales**.
3. Dans la boîte de dialogue Lier/délier les stratégies d'authentification à Global, sous l'onglet Principal ou Secondaire, dans Nom de la stratégie, sélectionnez la stratégie, cliquez sur **Dissocier la stratégie**, puis cliquez sur **OK**.

Ajouter une action d'authentification

Ajouter une action d'authentification à l'aide de la CLI

Si vous n'utilisez pas l'authentification LOCALE, vous devez ajouter une action d'authentification explicite. À l'invite de commandes, tapez la commande suivante :

```
add authentication tacacsAction <name> -serverip <IP> [-serverPort <
    port>][-authTimeout <positive_integer>][ ... ]
<!--NeedCopy-->
```

Exemple

```
add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812 -authtimeout 15 -tacacsSecret "minotaur" -
    authorization OFF -accounting ON -auditFailedCmds OFF -
    defaultAuthenticationGroup "users"
<!--NeedCopy-->
```

Configurer une action d'authentification à l'aide de la CLI

Pour configurer une action d'authentification existante, tapez la commande suivante à l'invite de commandes :

```
set authentication tacacsAction <name> -serverip <IP> [-serverPort <
    port>][-authTimeout <positive_integer>][ ... ]
<!--NeedCopy-->
```

Exemple

```
set authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812 -authtimeout 15 -tacacsSecret "minotaur" -
    authorization OFF -accounting ON -auditFailedCmds OFF -
    defaultAuthenticationGroup "users"
```



```
<!--NeedCopy-->
```

Supprimer une action d'authentification à l'aide de l'interface de ligne de commande

Pour supprimer une action RADIUS existante, tapez la commande suivante à l'invite de commandes :

```
rm authentication radiusAction <name>
<!--NeedCopy-->
```

Exemple

```
rm authentication tacacsaction Authn-Act-1
<!--NeedCopy-->
```

L'authentification NoAuth

L'appliance NetScaler prend en charge la fonctionnalité d'authentification NoAuth qui permet au client de configurer un paramètre DefaultAuthenticationGroup dans la commande, lorsqu'un utilisateur applique cette politique. `noAuthAction` L'administrateur peut vérifier la présence de ce groupe dans le groupe de l'utilisateur afin de déterminer la navigation de l'utilisateur dans la stratégie NoAuth.

Pour configurer une authentification NoAuth à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
add authentication noAuthAction <name> [-defaultAuthenticationGroup <
    string>]
<!--NeedCopy-->
```

Exemple

```
add authentication noAuthAction noauthact  -defaultAuthenticationGroup
    mynoauthgroup
<!--NeedCopy-->
```

Types d'authentification globale par défaut

Lorsque vous avez installé NetScaler Gateway et exécuté l'assistant NetScaler Gateway, vous avez configuré l'authentification dans l'assistant. Cette politique d'authentification est liée automatiquement au niveau global de NetScaler Gateway. Le type d'authentification que vous configurez dans

l'assistant NetScaler Gateway est le type d'authentification par défaut. Vous pouvez modifier le type d'autorisation par défaut en exécutant à nouveau l'assistant NetScaler Gateway ou vous pouvez modifier les paramètres d'authentification globaux dans l'utilitaire de configuration.

Si vous devez ajouter d'autres types d'authentification, vous pouvez configurer des politiques d'authentification sur NetScaler Gateway et lier les politiques à NetScaler Gateway à l'aide de l'utilitaire de configuration. Lorsque vous configurez l'authentification globalement, vous définissez le type d'authentification, configurez les paramètres et définissez le nombre maximal d'utilisateurs pouvant être authentifiés.

Après avoir configuré et lié la stratégie, vous pouvez définir la priorité pour définir le type d'authentification prioritaire. Par exemple, vous configurez les stratégies d'authentification LDAP et RADIUS. Si la stratégie LDAP a un numéro de priorité de 10 et que la stratégie RADIUS a un numéro de priorité de 15, la stratégie LDAP est prioritaire, quel que soit l'endroit où vous liez chaque stratégie. C'est ce qu'on appelle l'authentification en cascade.

Vous pouvez choisir de fournir des pages de connexion à partir du cache en mémoire de NetScaler Gateway ou à partir du serveur HTTP exécuté sur NetScaler Gateway. Si vous choisissez de diffuser la page de connexion depuis le cache en mémoire, la diffusion de la page de connexion depuis NetScaler Gateway est plus rapide que depuis le serveur HTTP. Le fait de choisir de diffuser la page d'ouverture de session à partir du cache en mémoire réduit le temps d'attente lorsque de nombreux utilisateurs ouvrent une session en même temps. Vous pouvez uniquement configurer la remise des pages d'ouverture de session à partir du cache dans le cadre d'une stratégie d'authentification globale.

Vous pouvez également configurer l'adresse IP NAT (Network Address Translation) qui est une adresse IP spécifique pour l'authentification. Cette adresse IP est unique pour l'authentification et ne correspond pas au sous-réseau NetScaler Gateway, aux adresses IP mappées ou virtuelles. Ce paramètre est facultatif.

> **Remarque :**
>
> - Vous ne pouvez pas utiliser l'assistant NetScaler Gateway pour configurer l'authentification SAML.
> - Vous pouvez utiliser l'assistant de configuration rapide pour configurer l'authentification par certificat LDAP, RADIUS et client. Lorsque vous exécutez l'assistant, vous pouvez sélectionner un serveur LDAP ou RADIUS existant configuré sur NetScaler Gateway. Vous pouvez également configurer les paramètres de LDAP ou de RADIUS. Si vous utilisez l'authentification à deux facteurs, Citrix recommande d'utiliser LDAP comme type d'authentification principal.

Configurer les types d'authentification globale par défaut

1. Dans l'interface graphique, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway,** puis cliquez sur Paramètres **généraux**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur **Modifier les paramètres d'authentification**.
3. Dans **Nombre maximum d'utilisateurs**, tapez le nombre d'utilisateurs qui peuvent être authentifiés à l'aide de ce type d'authentification.
4. Dans **Adresse IP NAT**, saisissez l'adresse IP unique pour l'authentification.
5. Sélectionnez Activer la mise**en cache statique pour diffuser les pages d'ouverture de session plus rapidement**.
6. Sélectionnez **Activer les commentaires sur l'authentification améliorée pour envoyer un message aux utilisateurs en cas d'échec de l'authentification**. Les messages que les utilisateurs reçoivent incluent les erreurs de mot de passe, le compte désactivé ou verrouillé, ou l'utilisateur est introuvable, pour n'en nommer que quelques-uns.
7. Dans **Type d'authentification par défaut**, sélectionnez le type d'authentification.
8. Configurez les paramètres de votre type d'authentification, puis cliquez sur **OK**.

Prise en charge de la récupération des tentatives de connexion actuelles d'un utilisateur

L'appliance NetScaler fournit une option permettant de récupérer la valeur des tentatives de connexion en cours pour un utilisateur à l'aide d'une nouvelle expression. `aaa.user.login_attempts` L'expression prend soit un argument (nom d'utilisateur), soit aucun argument. S'il n'y a aucun argument, l'expression récupère le nom d'utilisateur à partir de `aaa_session` ou `aaa_info`.

Vous pouvez utiliser l'expression `aaa.user.login_attempts` avec des stratégies d'authentification pour un traitement ultérieur.

Pour configurer le nombre de tentatives de connexion par utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add expression er aaa.user.login_attempts
```

Utilisateurs et groupes

May 5, 2023

Après avoir configuré la configuration de base de l'authentification, de l'autorisation et de l'audit, vous créez des utilisateurs et des groupes. Vous créez d'abord un compte utilisateur pour chaque personne qui s'authentifie via l'appliance NetScaler. Si vous utilisez l'authentification locale contrôlée par l'appliance NetScaler elle-même, vous créez des comptes d'utilisateurs locaux et attribuez des mots de passe à chacun de ces comptes.

Vous créez également des comptes utilisateur sur l'appliance NetScaler si vous utilisez un serveur d'authentification externe. Dans ce cas, toutefois, chaque compte utilisateur doit correspondre exactement au compte de cet utilisateur sur le serveur d'authentification externe, et vous n'attribuez pas de mot de passe aux comptes utilisateur que vous créez sur NetScaler. Le serveur d'authentification externe gère les mots de passe des utilisateurs qui s'authentifient auprès du serveur d'authentification externe.

Si vous utilisez un serveur d'authentification externe, vous pouvez toujours créer des comptes utilisateurs locaux sur l'appliance NetScaler si, par exemple, vous souhaitez autoriser des utilisateurs temporaires (tels que des visiteurs) à se connecter sans créer d'entrées pour ces utilisateurs sur le serveur d'authentification. Vous attribuez un mot de passe à chaque compte utilisateur local, comme vous le feriez si vous utilisiez l'authentification locale pour tous les comptes utilisateur.

Chaque compte utilisateur doit être lié à des politiques d'authentification et d'autorisation. Pour simplifier cette tâche, vous pouvez créer un ou plusieurs groupes et leur attribuer des comptes utilisateurs. Vous pouvez ensuite lier les politiques à des groupes plutôt qu'à des comptes d'utilisateurs individuels.

Configurer des politiques avec des groupes

Après avoir configuré les groupes, vous pouvez utiliser la boîte de dialogue **Groupe** pour appliquer des politiques et des paramètres qui spécifient l'accès des utilisateurs. Si vous utilisez l'authentification locale, vous créez des utilisateurs et vous les ajoutez à des groupes configurés sur NetScaler Gateway. Les utilisateurs héritent ensuite des paramètres de ce groupe.

Vous pouvez configurer les politiques ou paramètres suivants pour un groupe d'utilisateurs dans la boîte de dialogue **Groupe** :

- Utilisateurs
- Stratégies d'autorisation
- Stratégies d'audit
- Stratégies de session
- Politiques de trafic
- Signets
- Applications Intranet
- Adresses IP Intranet

Dans votre configuration, certains utilisateurs peuvent appartenir à plusieurs groupes. En outre, chaque groupe peut avoir une ou plusieurs stratégies de session liées, avec différents paramètres configurés. Les utilisateurs appartenant à plusieurs groupes héritent des stratégies de session attribuées à tous les groupes auxquels ils appartiennent. Pour vous assurer que l'évaluation de la stratégie de session est prioritaire sur l'autre, vous devez définir la priorité de la stratégie de session.

Par exemple, le groupe1 est lié à une stratégie de session configurée avec la page d'accueil www.homepage1.com. Group2 est lié à une stratégie de session configurée avec la page d'accueil www.homepage2.com. Lorsque ces stratégies sont liées à des groupes respectifs sans numéro de priorité ou avec le même numéro de priorité, la page d'accueil qui apparaît aux utilisateurs appartenant aux deux groupes dépend de la stratégie traitée en premier. En définissant un numéro de priorité inférieur, qui donne une priorité plus élevée, pour la stratégie de session avec la page d'accueil www.homepage1.com, vous pouvez vous assurer que les utilisateurs appartenant aux deux groupes reçoivent la page d'accueil www.homepage1.com.

Si aucun numéro de priorité n'est attribué aux stratégies de session ou n'ont pas le même numéro de priorité, la priorité est évaluée dans l'ordre suivant :

- Utilisateur
- Groupe
- Serveur virtuel
- Global

Si les stratégies sont liées au même niveau, sans numéro de priorité ou si les stratégies ont le même numéro de priorité, l'ordre d'évaluation est celui de l'ordre de liaison des stratégies. Les stratégies qui sont liées en premier à un niveau sont prioritaires par rapport aux stratégies liées ultérieurement.

Si nous avons un utilisateur lié à plusieurs groupes avec chaque groupe lié à l'IIP, l'utilisateur peut obtenir une adresse IP gratuite de n'importe quel groupe lié.

Création d'utilisateurs et de groupes

Configuration de l'authentification, de l'autorisation et de l'audit des utilisateurs locaux à l'aide de l'interface graphique

1. **Accédez à**Sécurité > AAA - Trafic applicatif > Utilisateurs**
   depuis NetScaler Gateway, développez**NetScaler Gateway > Administration des utilisateurs**, puis cliquez sur Utilisateurs AAA.**
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau compte utilisateur, cliquez sur **Ajouter**.
   - Pour modifier un compte utilisateur existant, sélectionnez le compte utilisateur, puis cliquez sur **Ouvrir**.

3. Dans la boîte de dialogue **Créer un utilisateur AAA**, dans la zone de texte **Nom d'utilisateur**, tapez le nom de l'utilisateur.
4. Si vous créez un compte utilisateur authentifié localement, désactivez la case **Authentification externe** et fournissez un mot de passe local que l'utilisateur utilise pour se connecter.
5. Cliquez sur **Créer** ou **sur OK**, puis sur **Fermer**. Un message s'affiche dans la barre d'état, indiquant que l'utilisateur a été correctement configuré.

Configurez l'authentification, l'autorisation et l'audit des groupes locaux et ajoutez-y des utilisateurs à l'aide de l'utilitaire de configuration

1. **Accédez à**Sécurité > AAA - Trafic d'applications > Groupes**
   depuis NetScaler Gateway, développez**NetScaler Gateway > Administration des utilisateurs**, puis cliquez sur Groupes AAA.**
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau groupe, cliquez sur **Ajouter**.
   - Pour modifier un groupe existant, sélectionnez le groupe, puis cliquez sur **Modifier**.
3. Si vous créez un nouveau groupe, dans la boîte de dialogue **Créer un groupe AAA**, dans la zone de texte **Nom du groupe**, tapez le nom du groupe.
4. Dans la zone **avancée** à droite, cliquez sur **Utilisateurs AAA**.
   - Pour ajouter un utilisateur au groupe, sélectionnez-le, puis cliquez sur **Ajouter**.
   - Pour supprimer un utilisateur du groupe, sélectionnez-le, puis cliquez sur **Supprimer**.
   - Pour créer un nouveau compte utilisateur et l'ajouter au groupe, cliquez sur l'icône **Plus**, puis suivez les instructions de la section « Pour configurer l'authentification, l'autorisation et l'audit des utilisateurs locaux à l'aide de l'utilitaire de configuration ». «
5. Cliquez sur **Créer** ou **sur OK**. Le groupe que vous avez créé apparaît sur la page **AAA Groups** .

Supprimer un groupe à l'aide de l'interface graphique

Vous pouvez également supprimer des groupes d'utilisateurs de NetScaler Gateway.

1. **Accédez à**Sécurité > AAA - Trafic d'applications > Groupes**
   depuis NetScaler Gateway, ExpandCitrix**Gateway > Administration des utilisateurs,**puis cliquez sur Groupes AAA.**
   Dans le volet d'informations, sélectionnez le groupe, puis cliquez sur Supprimer.

Configurer l'authentification, l'autorisation et l'audit des utilisateurs locaux à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
add aaa group <groupname>

bind aaa group <groupname> -username <username>
<!--NeedCopy-->
```

Exemple :

```
add aaa group group-2

bind aaa group group-2 -username user-2
<!--NeedCopy-->
```

Supprimer des utilisateurs d'un groupe d'authentification, d'autorisation et d'audit à l'aide de l'interface de ligne de commande

À l'invite de commandes, dissociez les utilisateurs du groupe en saisissant la commande suivante une fois pour chaque compte utilisateur lié au groupe :

```
unbind aaa group <groupname> -username <username><!--NeedCopy-->
```

```
**Exemple :**

<!--NeedCopy-->
```

unbind aaa group group-hr -username user-hr-1

```
### Supprimer un groupe d'authentification, d'autorisation et d'audit à
    l'aide de l'interface de ligne de commande

Supprimez d'abord tous les utilisateurs du groupe. Ensuite, à l'invite
   de commandes, tapez la commande suivante pour supprimer un groupe
   NetScaler AAA et vérifier la configuration :

<!--NeedCopy-->
```

rm aaa group

```
**Exemple :**

```



```
<!--NeedCopy-->
```

rm aaa group group-hr

```
> **Remarque**
>
>Vous ne pouvez pas ajouter de nom d'utilisateur avec un domaine si le nom d'utilisateur est déjà ajouté sans domaine. Si le nom d'utilisateur avec domaine est ajouté en premier, suivi du même nom d'utilisateur sans domaine, l'appliance NetScaler ajoute le nom d'utilisateur à la liste des utilisateurs.

L'exemple suivant montre comment ajouter un nom d'utilisateur avec un domaine n'est pas autorisé si le même nom d'utilisateur est ajouté sans domaine.

<!--NeedCopy-->
```

```
add aaa user u47985
Done
show aaa users
1) UserName: u47985
Done
add aaa user u47985@domain.com
ERROR: User already exists
‘‘‘
```

L’exemple suivant montre si le nom d’utilisateur avec domaine est ajouté en premier, suivi du même nom d’utilisateur sans domaine, l’appliance NetScaler ajoute le nom d’utilisateur à la liste des utilisateurs.

```
> add aaa user u47985@domain.com
Done
> add aaa user u47985
Done
> sh aaa user
1)    UserName: u47985@domain.com
2)    UserName: u47985
```

‘‘‘

Méthodes d'authentification

May 5, 2023

L'appliance NetScaler peut authentifier les utilisateurs à l'aide de comptes d'utilisateurs locaux ou à l'aide d'un serveur d'authentification externe. L'appliance prend en charge les types d'authentification suivants :

- **LOCAL :** s'authentifie auprès de l'appliance NetScaler à l'aide d'un mot de passe, sans référence à un serveur d'authentification externe. Les données utilisateur sont stockées localement sur l'appliance NetScaler.
- **RADIUS :** authentifiez-vous auprès d'un serveur RADIUS externe.
- **LDAP :** authentifie auprès d'un serveur d'authentification LDAP externe.
- **TACACS :** S'authentifie auprès d'un serveur d'authentification TACACS (Terminal Access Controller Access-Control System) externe.
- **CERT :** authentifie auprès de l'appliance NetScaler à l'aide d'un certificat client, sans référence à un serveur d'authentification externe.
- **NÉGOCIER :** S'authentifie auprès d'un serveur d'authentification Kerberos. En cas d'erreur lors de l'authentification Kerberos, NetScaler utilise l'authentification NTLM.
- **SAML :** authentifie auprès d'un serveur qui prend en charge le langage SAML (Security Assertion Markup Language).
- **IDP SAML :** configure NetScaler pour qu'il serve de fournisseur d'identité (IDP) en langage SAML (Security Assertion Markup Language).
- **WEB :** s'authentifie auprès d'un serveur Web en fournissant les informations d'identification requises par le serveur Web dans une requête HTTP et en analysant la réponse du serveur Web pour déterminer si l'authentification de l'utilisateur a été réussie.
- **OTP natif :** l'appliance NetScaler prend en charge les mots de passe à usage unique (OTP) sans avoir à utiliser un serveur tiers.
- **Notification push :** NetScaler Gateway prend en charge les notifications push pour OTP. Les utilisateurs n'ont pas à saisir manuellement l'OTP reçu sur leurs appareils enregistrés pour se connecter à NetScaler Gateway. Les administrateurs peuvent configurer NetScaler Gateway de telle sorte que les notifications de connexion soient envoyées aux appareils enregistrés des utilisateurs à l'aide de services de notification push.
- **E-mail OTP :** La méthode Email OTP vous permet de vous authentifier à l'aide du mot de passe à usage unique (OTP) envoyé à l'adresse e-mail enregistrée. Lorsque vous essayez de vous authentifier sur n'importe quel service, le serveur envoie un OTP à l'adresse e-mail enregistrée de l'utilisateur.

- **Authentification reCAPTCHA** : NetScaler Gateway prend en charge une nouvelle action de première classe, CaptchaAction, qui simplifie la configuration du reCAPTCHA. Le reCAPTCHA étant un recours collectif de premier ordre, il peut constituer un facteur à part entière. Vous pouvez injecter reCAPTCHA n'importe où dans le flux nFactor.
- **Authentification nFactor :** L'authentification multifactorielle renforce la sécurité d'une application en obligeant les utilisateurs à fournir plusieurs preuves d'identité pour y accéder. L'appliance NetScaler offre une approche extensible et flexible de la configuration de l'authentification multifactorielle. Cette approche est appelée authentification nFactor.
- Authentification**OAuth : l'** authentification OAuth autorise et authentifie les utilisateurs auprès de services hébergés sur des applications telles que Google, Facebook et Twitter.

Authentification nFactor

May 5, 2023

> **Important**
>
> - L'authentification nFactor est prise en charge à partir de NetScaler 11.0 Build 62.x.
> - Pour que l'authentification nFactor fonctionne avec NetScaler, une licence Advanced ou Premium est requise.
> - À partir de la version 13.0 build 67.x, l'authentification NFactor est prise en charge avec la licence Standard uniquement pour le serveur virtuel Gateway/VPN. Pour plus d'informations sur l'authentification nFactor avec NetScaler Gateway, consultez nFactorpour l'authentification par passerelle.
> - L'authentification nFactor n'est pas prise en charge pour le client Linux.

L'authentification multifacteur améliore la sécurité d'une application en obligeant les utilisateurs à fournir plusieurs preuves d'identité pour y accéder. L'appliance NetScaler offre une approche extensible et flexible de la configuration de l'authentification multifactorielle. Cette approche est appelée *authentification nFactor*.

Comment fonctionne l'authentification nFactor

Chaque facteur d'authentification effectue les tâches suivantes :

- Collecte les informations d'identification auprès de l'utilisateur. Les mécanismes d'authentification pris en charge par NetScaler incluent LDAP, RADIUS, l'assertion SAML, le certificat client, OAuth OpenID Connect, Kerberos, etc.

- Évalue les informations d'identification fournies pour décider si l'authentification a réussi, échoué ou si des actions telles que l'extraction de groupe ou l'extraction d'attributs doivent être effectuées.
- Sur la base des résultats de l'évaluation, l'accès est soit accordé, soit refusé, soit un facteur suivant est sélectionné.
- Répétez ces étapes jusqu'à ce qu'il n'y ait plus aucun autre facteur à évaluer.

Avec l'authentification nFactor, vous pouvez :

- Configurez un nombre illimité de facteurs d'authentification.
- Baser la sélection du facteur suivant sur le résultat de l'exécution du facteur précédent.
- Personnalisez l'interface de connexion. Par exemple, vous pouvez personnaliser les noms des étiquettes, les messages d'erreur et le texte d'aide.
- Extrayez les informations du groupe d'utilisateurs sans authentification.
- Configurez le relais pour un facteur d'authentification. Cela signifie qu'aucune interaction de connexion explicite n'est requise pour ce facteur.
- Configurez l'ordre dans lequel les différents types d'authentification sont appliqués. Tous les mécanismes d'authentification pris en charge sur l'appliance NetScaler peuvent être configurés comme n'importe quel facteur de la configuration de l'authentification nFactor. Ces facteurs sont exécutés dans l'ordre dans lequel ils sont configurés.
- Configurez l'appliance NetScaler pour passer à un facteur d'authentification qui doit être exécuté en cas d'échec de l'authentification. Pour ce faire, vous configurez une autre politique d'authentification avec la même condition, mais avec la priorité la plus élevée et avec l'action définie sur « NO_AUTH ». Vous devez configurer le facteur suivant, qui doit spécifier l'autre mécanisme d'authentification à appliquer.

Chiffrement des informations de connexion à NetScaler Gateway pour l'authentification nFactor

NetScaler Gateway avec authentification nFactor peut crypter les champs de demande de connexion soumis par un client (navigateur ou applications SSO) pendant le processus d'authentification. Les champs de demande de connexion cryptés fournissent une couche de sécurité supplémentaire pour protéger les données sensibles de l'utilisateur contre la divulgation.

Navigateurs compatibles

Le tableau suivant répertorie les navigateurs ainsi que les détails de version qui prennent en charge le cryptage de connexion.

Navigateurs	Version
Chrome	78 et plus
Firefox	69 ans et plus
Bord	42 et plus
Safari	11,0 et plus
Opéra	66

Clients compatibles

La section suivante répertorie les clients ainsi que les détails des versions qui prennent en charge le chiffrement des informations de connexion à NetScaler Gateway.

- L'application Citrix Workspace sur Mac prend en charge le chiffrement uniquement lorsque la version du système d'exploitation est 10.14.x et supérieure.
- L'application Citrix SSO sur Mac prend en charge le cryptage uniquement lorsque la version du système d'exploitation est 10.14.x et supérieure.
- L'application Windows SSO n'est soumise à aucune restriction quant à la compatibilité.

Pour activer le chiffrement de connexion à l'aide de la CLI

À l'invite de commande, tapez :

```
set aaa parameter [-loginEncryption (ENABLED | DISABLED)]
```

> **Remarque**
>
> Le paramètre LoginEncryption est DÉSACTIVÉ par défaut. Vous devez l'ACTIVER.

Pour activer le cryptage de connexion à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic des applications**, cliquez sur **Modifier les paramètres AAA d'authentification** dans la section **Paramètres d'authentification** .
2. Sur la page **Configurer le paramètre AAA**, faites défiler vers le bas jusqu'à l'option **Chiffrement de connexion** et activez-la.

Concepts, entités et terminologie nFactor

May 5, 2023

Cette rubrique présente certaines des principales entités impliquées dans l'authentification nFactor et leur importance.

Schéma de connexion

nFactor découple la « vue », l'interface utilisateur, avec le « modèle » qui gère l'exécution. La vue de nFactor est définie par le schéma de connexion. Le schéma de connexion est une entité qui définit ce que voit l'utilisateur et spécifie comment extraire les données de l'utilisateur.

Pour définir une vue, le schéma de connexion pointe vers un fichier sur le disque qui définit le formulaire d'ouverture de session. Ce fichier doit être conforme à la spécification du « Citrix Common Forms Protocol. » Ce fichier est essentiellement une définition XML du formulaire d'ouverture de session.

Outre le fichier XML, le schéma de connexion contient des expressions de stratégie avancées pour glaner le nom d'utilisateur et le mot de passe à partir de la demande de connexion de l'utilisateur. Ces expressions sont facultatives et peuvent être omises si le nom d'utilisateur et le mot de passe de l'utilisateur arrivent avec des noms de variables de formulaire attendus.

Le schéma de connexion définit également si l'ensemble actuel d'informations d'identification doit être utilisé comme informations d'identification SingleSignon par défaut.

Le schéma de connexion peut être créé en exécutant la commande CLI suivante :

```
1    add authentication loginSchema <name> -authenticationSchema <string>
         [-userExpression <string>] [-passwdExpression <string>] [-
        userCredentialIndex <positive_integer>] [-passwordCredentialIndex
         <positive_integer>] [-authenticationStrength <positive_integer>]
         [-SSOCredentials ( YES | NO )]
2 <!--NeedCopy-->
```

> **Remarque :**
>
> Les**informations d'identification SSO** indiquent si les informations d'identification du facteur en cours sont les informations d'identification SSO par défaut. La valeur par défaut est NON.
>
> Dans la configuration de l'authentification nFactor, les informations d'identification du dernier facteur sont utilisées par défaut pour l'authentification unique. En utilisant la configuration **SSO-Credentials**, les informations d'identification du facteur actuel peuvent être utilisées. Dans le cas où cette configuration est définie selon différents facteurs, le facteur final qui a cet ensemble de configuration prend la priorité.

Pour plus d'informations sur chaque paramètre, reportez-vous à la section https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-loginSchema/#add-authentication-loginschema.

Libellé politique

Une étiquette de stratégie est un ensemble de stratégies. Il s'agit d'une construction qui n'est pas étrangère à l'infrastructure de politique de NetScaler. L'étiquette de stratégie définit un facteur d'authentification. En d'autres termes, il contient toutes les stratégies nécessaires pour déterminer si les informations d'identification de l'utilisateur sont satisfaites. Toutes les politiques d'un label peuvent être considérées comme homogènes. L'étiquette de stratégie pour l'authentification ne peut pas prendre de stratégies de type différent, par exemple la réécriture. En d'autres termes, toutes les stratégies d'une étiquette de stratégie valident le même mot de passe/informations d'identification de l'utilisateur, pour la plupart. Le résultat des stratégies dans un PolicyLabel suit la condition logique OR. Par conséquent, si l'authentification spécifiée par la première stratégie réussit, les autres stratégies qui la suivent sont ignorées.

L'étiquette de stratégie peut être créée en exécutant la commande CLI suivante :

```
1 add authentication policy label mylabel  - loginSchema <>
2 <!--NeedCopy-->
```

Une étiquette de stratégie prend le schéma de connexion comme propriété. Le schéma de connexion définit la vue de cette étiquette de stratégie. Si le schéma de connexion n'est pas spécifié, un schéma de connexion implicite, LSCHEMA_INT, est associé à cette étiquette de stratégie. Le schéma de connexion détermine si une étiquette de stratégie devient un relais ou non.

Étiquette du serveur virtuel

Dans l'infrastructure de politique avancée de NetScaler, un serveur virtuel est également une étiquette de politique implicite. Cela est dû au fait que le serveur virtuel peut également être lié à plusieurs stratégies. Cependant, un serveur virtuel est spécial car il constitue le point d'entrée du trafic client et peut prendre des stratégies d'un type différent. Chacune des stratégies qu'il a placées sous sa propre étiquette au sein du serveur virtuel. Le serveur virtuel est donc un conglomérat d'étiquettes.

Facteur suivant

Chaque fois qu'une stratégie est liée à un serveur virtuel ou à une étiquette de stratégie, elle peut être spécifiée avec le facteur suivant. Le facteur suivant détermine ce qui doit être fait si une authentification donnée réussit. S'il n'y a pas de facteur suivant, le processus d'authentification pour cet utilisateur est terminé.

Chaque stratégie liée à un serveur virtuel ou à une étiquette de stratégie peut avoir un facteur suivant différent. Cela permet une flexibilité ultime dans laquelle le succès de chaque stratégie peut définir un nouveau chemin pour l'authentification de l'utilisateur. L'administrateur peut tirer parti de ce fait et créer des facteurs de secours intelligents pour les utilisateurs qui ne respectent pas certaines règles.

Politique de non-autorisation

nFactor introduit une stratégie intégrée spéciale appelée NO_AUTHN. La stratégie NO_AUTHN renvoie toujours le succès en tant que résultat de l'authentification. La stratégie `No-auth` peut être créée en exécutant la commande CLI suivante :

```
1 add authentication policy noauthpolicy -rule <> -action NO_AUTHN
2 <!--NeedCopy-->
```

Conformément à la commande, la stratégie `no-authentication` prend une règle qui peut être n'importe quelle expression de stratégie avancée. Le résultat de l'authentification est toujours un succès de NO_AUTHN.

Une `no-auth` politique en soi ne semble pas apporter de valeur ajoutée. Cependant, lorsqu'il est utilisé avec des étiquettes de stratégie de relais, il offre une grande flexibilité pour prendre des décisions logiques afin de stimuler le flux d'authentification des utilisateurs. La stratégie NO_AUTHN et les facteurs de passthrough offrent une nouvelle dimension à la flexibilité de nFactor.

Remarque : Consultez les exemples illustrant l'utilisation de `no-auth` et du passthrough dans les sections suivantes.

Facteur/étiquette de passage

Une fois que l'utilisateur a réussi l'authentification sur le serveur virtuel (pour le premier facteur), les authentifications suivantes ont lieu au niveau des étiquettes de stratégie ou des facteurs définis par l'utilisateur (secondaires).
Chaque étiquette/facteur de stratégie est associé à une entité de schéma de connexion pour afficher la vue de ce facteur. Cela permet de personnaliser les vues en fonction du chemin que l'utilisateur aurait emprunté pour arriver à un facteur donné.

Il existe des types spécialisés d'étiquettes de stratégie qui ne pointent pas explicitement vers un schéma de connexion. Les étiquettes de stratégie spécialisées pointent vers un schéma de connexion qui ne pointe pas réellement vers le fichier XML de la vue. Ces étiquettes/facteurs politiques sont appelés facteurs de « transmission ».

Les facteurs de relais peuvent être créés en exécutant les commandes CLI suivantes :

Exemple 1 :

```
1 add authentication policylabel example1
2 <!--NeedCopy-->
```

Exemple 2 :

```
1 add loginschema passthrough_schema -authenticationSchema noschema
```



```
2
3 add authentication policylabel example2 -loginschema
     passthrough_schema
4 <!--NeedCopy-->
```

Le facteur de transmission implique que le sous-système d'authentification, d'autorisation et d'audit ne doit pas revenir vers l'utilisateur pour obtenir les informations d'identification définies pour ce facteur. Il s'agit plutôt d'un conseil pour que l'authentification, l'autorisation et l'audit continuent avec les informations d'identification déjà obtenues. Cela est utile dans les cas où l'intervention de l'utilisateur n'est pas souhaitée. Par exemple,

- Lorsque deux champs de mot de passe sont présentés à l'utilisateur, après le premier facteur, le second facteur n'a pas besoin d'intervention de l'utilisateur.
- Lorsque l'authentification d'un type (par exemple un certificat) est effectuée et que l'administrateur doit extraire des groupes pour cet utilisateur.

Le facteur de transmission peut être utilisé avec une stratégie `NO_AUTH` pour effectuer des sauts conditionnels.

Flux d'authentification nFactor

L'authentification commence toujours au niveau du serveur virtuel dans nFactor. Le serveur virtuel définit le premier facteur pour l'utilisateur. Le premier formulaire que l'utilisateur voit est servi par le serveur virtuel. Le formulaire d'ouverture de session que l'utilisateur voit peut être personnalisé sur le serveur virtuel à l'aide de stratégies de schéma de connexion. S'il n'existe aucune stratégie de schéma de connexion, un seul champ de nom d'utilisateur et de mot de passe s'affiche pour l'utilisateur.

Si plusieurs champs de mot de passe doivent être affichés à l'utilisateur sur un formulaire personnalisé, des stratégies de schéma de connexion doivent être utilisées. Ils permettent d'afficher différents formulaires en fonction des règles configurées (tels que l'utilisateur intranet par rapport à l'utilisateur externe, le fournisseur de services A par rapport au fournisseur de services B).

Une fois les informations d'identification de l'utilisateur publiées, l'authentification commence au niveau du serveur virtuel d'authentification, le premier facteur. Étant donné que le serveur virtuel d'authentification peut être configuré avec plusieurs stratégies, chacune d'elles est évaluée dans un ordre. À tout moment, si une stratégie d'authentification aboutit, le facteur suivant spécifié par rapport à elle est pris en compte. S'il n'y a pas de facteur suivant, le processus d'authentification prend fin. Si le facteur suivant existe, il est vérifié s'il s'agit d'un facteur de transmission ou d'un facteur régulier. S'il s'agit d'un relais, les stratégies d'authentification relatives à ce facteur sont évaluées sans intervention de l'utilisateur. Sinon, le schéma de connexion associé à ce facteur est affiché pour l'utilisateur.

Exemple d'utilisation du facteur de transmission et des politiques de non-authentification pour prendre des décisions logiques

L'administrateur souhaite décider de NextFactor en fonction des groupes.

```
add authentication policylabel group check

add authentication policy admin group -rule http.req.user.is_member_of ("Administrators") -action NO_AUTHN

add authentication policy nonadmins -rule true -action NO_AUTHN

bind authentication policy label group check -policy admingroup -pri 1 -nextFactor factor-for-admin

bind authentication policy label groupcheck -policy nonadmins -pri 10 -nextfactor factor-for-others

add authentication policy first_factor_policy -rule <> -action <>

bind authentication vserver <> -policy first_factor_policy -priority 10 -nextFactor groupcheck
<!--NeedCopy-->
```

Configuration de l'authentification NFactor

June 20, 2023

Vous pouvez configurer plusieurs facteurs d'authentification à l'aide de la configuration nFactor. La configuration nFactor est prise en charge uniquement dans les éditions NetScaler Advanced et Premium.

Méthodes de configuration de NFactor

Vous pouvez configurer l'authentification NFactor en utilisant l'une des méthodes suivantes :

- **nFactor Visualizer :** nFactor Visualizer vous permet de lier facilement des facteurs ou des étiquettes de stratégie dans un seul volet et de modifier la liaison des facteurs dans le même volet. Vous pouvez créer un flux nFactor à l'aide du visualiseur et lier ce flux à un serveur virtuel d'authentification, d'autorisation et d'audit. Pour plus de détails sur le visualiseur nFactor et un exemple de configuration nFactor utilisant le visualiseur, voir Visualiseur nFactor pour une configuration simplifiée.

- **Interface graphique NetScaler :** pour plus de détails, consultez la section **Éléments de configuration impliqués dans la configuration de nFactor**.
- **NetScaler CLI :** pour un exemple d'extrait de code sur la configuration de nFactor à l'aide de la CLI NetScaler, voir Exemple d'extrait de code sur la configuration de nFactor à l'aide de l'interface de ligne de commande NetScaler.

> **Important :** Cette rubrique contient des détails sur la configuration de nFactor à l'aide de l'interface graphique NetScaler.

Éléments de configuration impliqués dans la configuration NFactor

Les éléments suivants sont impliqués dans la configuration de NFactor. Pour connaître les étapes détaillées, reportez-vous aux sections appropriées de cette rubrique.

Élément de configuration	Tâches à effectuer
Serveur virtuel AAA	Créer un serveur virtuel AAA
	Liez le thème du portail au serveur virtuel AAA
	Activer l'authentification par certificat client
Schéma de connexion	Configuration d'un profil de schéma de connexion
	Créer et lier une stratégie de schéma de connexion
Stratégies d'authentification avancées	Créer des stratégies d'authentification avancées
	Liez la stratégie d'authentification avancée à premier facteur au serveur virtuel NetScaler AAA
	Utiliser les groupes LDAP extraits pour sélectionner le facteur d'authentification suivant
Étiquette de stratégie d'authentification	Créer une étiquette de stratégie d'authentification
	Libellé de stratégie d'authentification de liaison
nFactor pour NetScaler Gateway	Créez un profil d'authentification pour lier un serveur virtuel NetScaler AAA au serveur virtuel NetScaler Gateway

Élément de configuration	Tâches à effectuer
	Configurer les paramètres SSL et le certificat CA pour NetScaler Gateway
	Configurer la stratégie de trafic de NetScaler Gateway pour l'authentification unique de nFactor à StoreFront

Comment fonctionne NFactor

Lorsqu'un utilisateur se connecte au serveur virtuel d'authentification, d'autorisation et d'audit ou à NetScaler Gateway, la séquence des événements est la suivante :

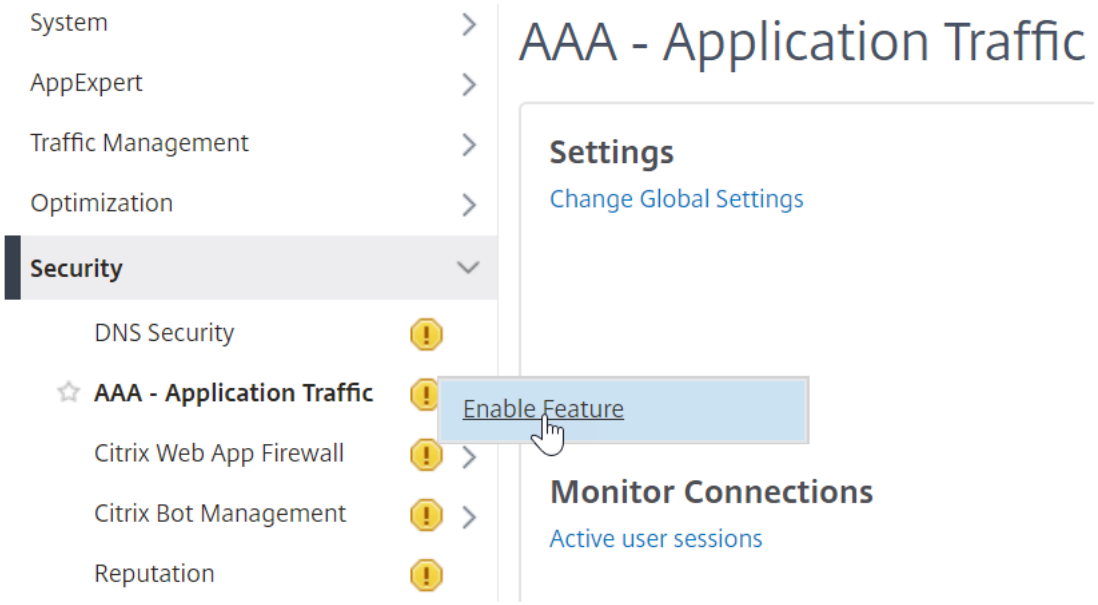
1. Si l'authentification basée sur des formulaires est utilisée, le schéma de connexion lié au serveur virtuel d'authentification, d'autorisation et d'audit s'affiche.
2. Les stratégies d'authentification avancées liées au serveur virtuel d'authentification, d'autorisation et d'audit sont évaluées.
    - Si la stratégie d'authentification avancée aboutit et si le facteur suivant (étiquette de stratégie d'authentification) est configuré, le facteur suivant est évalué. Si Next Factor n'est pas configuré, l'authentification est terminée et réussie.
    - Si la stratégie d'authentification avancée échoue et si l'expression Goto est définie sur Suivant, la stratégie d'authentification avancée liée suivante est évaluée. Si aucune des stratégies d'authentification avancée ne réussit, l'authentification échoue.
3. Si l'étiquette de stratégie d'authentification des facteurs suivante est liée à un schéma de connexion, il est affiché pour l'utilisateur.
4. Les stratégies d'authentification avancées liées à l'étiquette de stratégie d'authentification du facteur suivant sont évaluées.
    - Si la stratégie d'authentification avancée aboutit et si le facteur suivant (étiquette de stratégie d'authentification) est configuré, le facteur suivant est évalué.
    - Si Next Factor n'est pas configuré, l'authentification est terminée et réussie.
5. Si la stratégie d'authentification avancée échoue et si Goto Expression est Next (Suivant), la stratégie d'authentification avancée liée suivante est évaluée.
6. Si les stratégies aboutissent, l'authentification échoue.

Serveur virtuel d'authentification, d'autorisation et d'audit

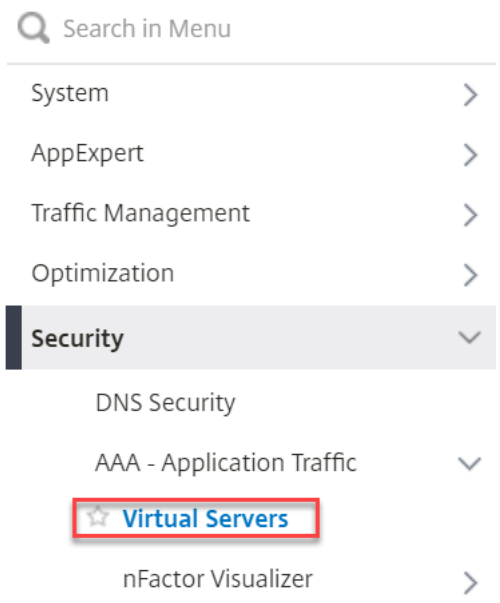
Pour utiliser nFactor avec NetScaler Gateway, vous devez d'abord le configurer sur un serveur virtuel d'authentification, d'autorisation et d'audit. Ensuite, vous lierez le serveur virtuel d'authentification, d'autorisation et d'audit au serveur virtuel NetScaler Gateway.

Créer un serveur virtuel d'authentification, d'autorisation et d'audit

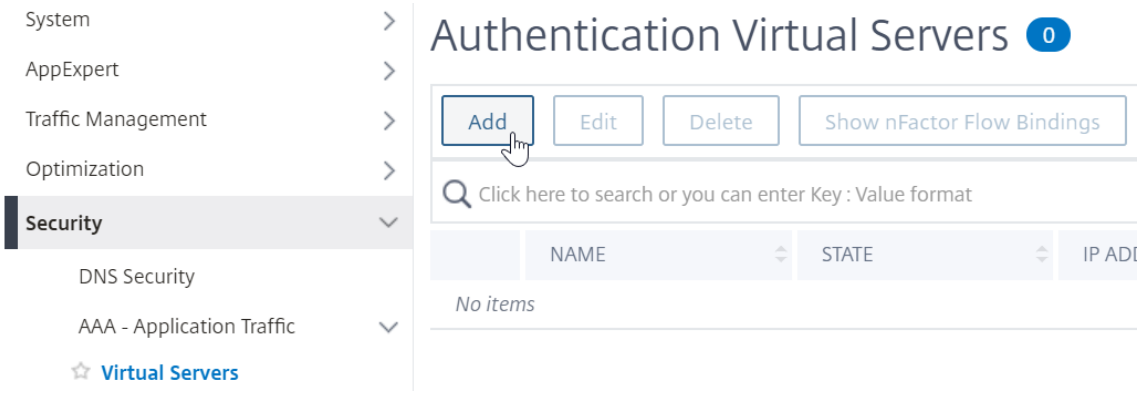
1. Si la fonctionnalité Authentification, autorisation et audit n'est pas déjà activée, accédez à **Sécurité > AAA — Trafic des applications**, puis cliquez avec le bouton droit pour activer la fonctionnalité.



2. Accédez à **Configuration > Sécurité > AAA - Trafic des applications > Serveurs virtuels**.

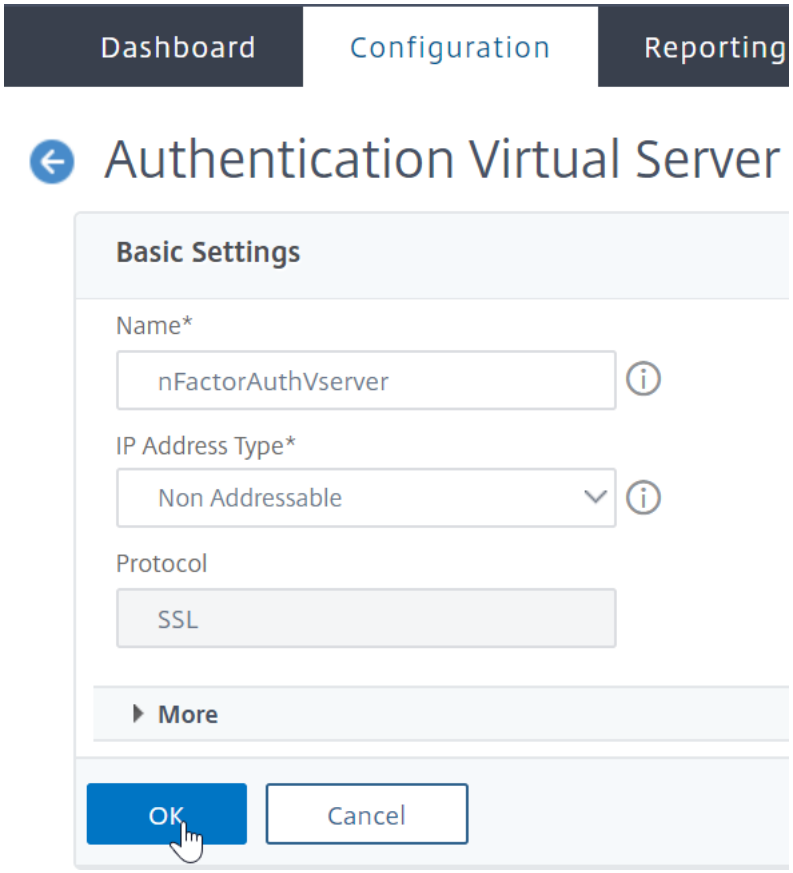


3. Cliquez sur **Ajouter** pour créer un serveur virtuel d'authentification.

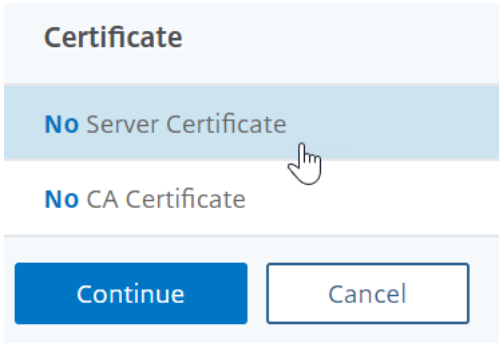


4. Entrez les informations suivantes et cliquez sur **OK**.

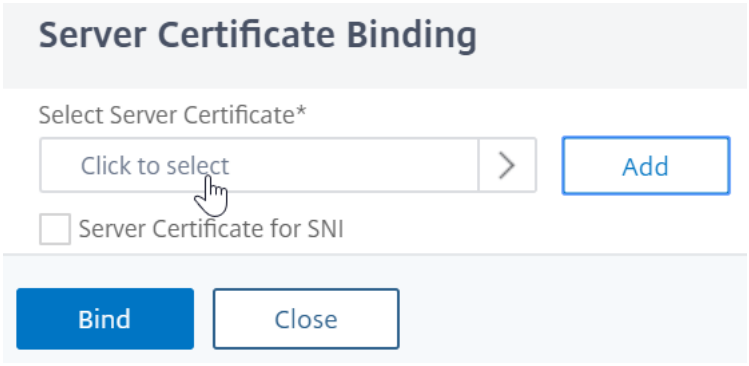
Nom du paramètre	Description des paramètres
Nom	Nom du serveur virtuel d'authentification, d'autorisation et d'audit.
Type d'adresse IP	Modifiez le type d'adresse IP sur **Non adressable** si ce serveur virtuel est utilisé uniquement pour NetScaler Gateway.



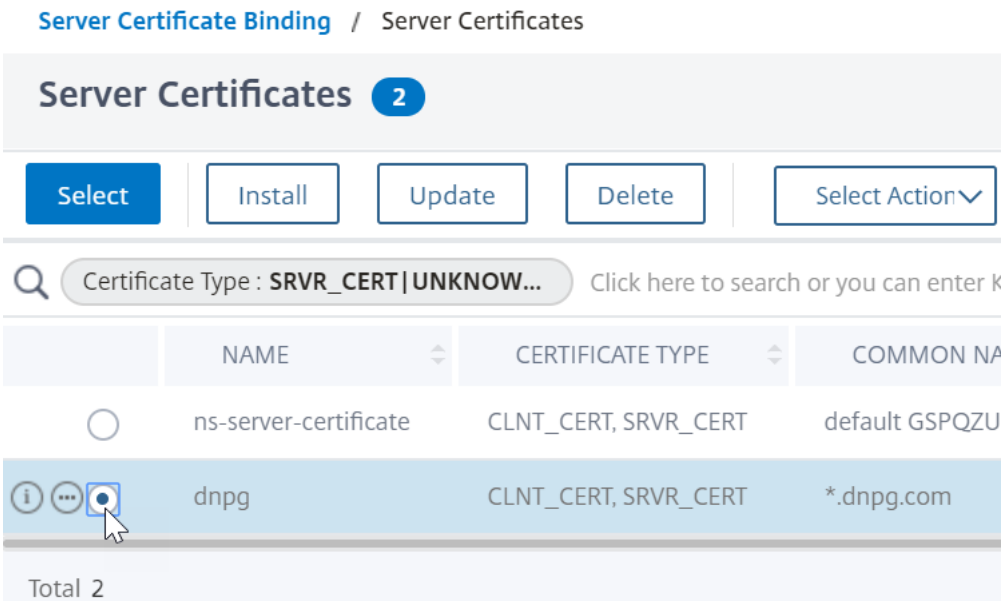
5. Sous Certificat, sélectionnez **Aucun certificat de serveur**.



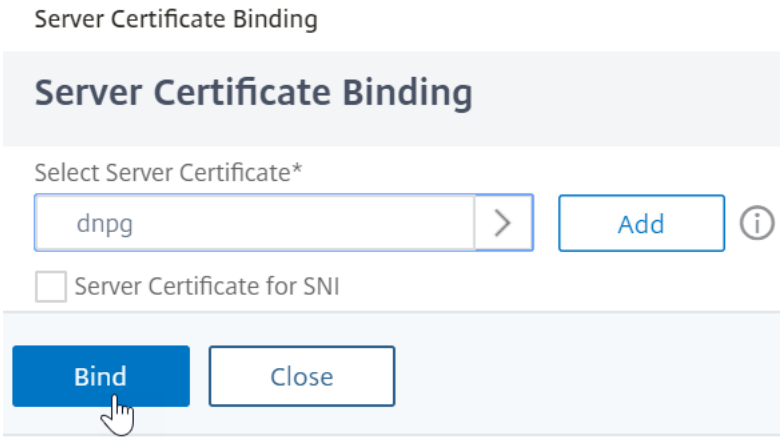
6. Cliquez sur le texte, **cliquez sur pour sélectionner** le certificat de serveur.



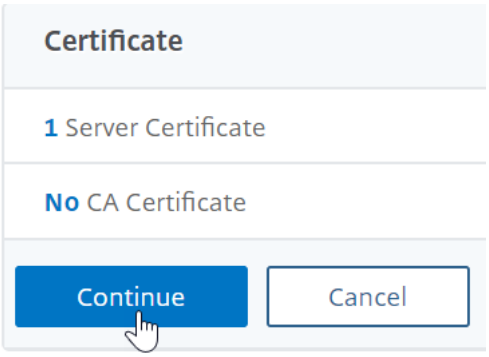
7. Cliquez sur la case d'option en regard d'un certificat pour le serveur virtuel d'authentification, d'autorisation et d'audit, puis cliquez sur **Sélectionner**. Le certificat choisi n'a pas d'importance car ce serveur n'est pas directement accessible.



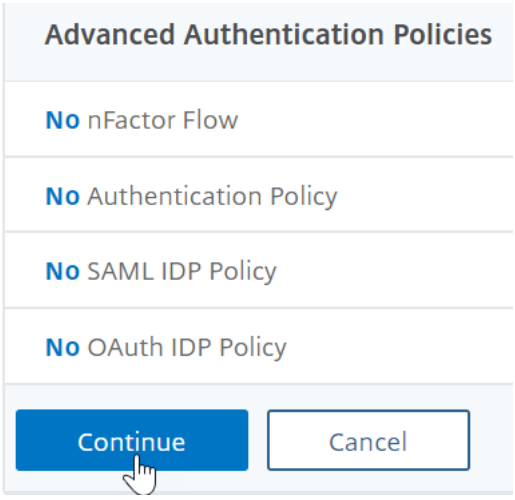
8. Cliquez sur **Bind**.



9. Cliquez sur **Continuer** pour fermer la section **Certificat** .

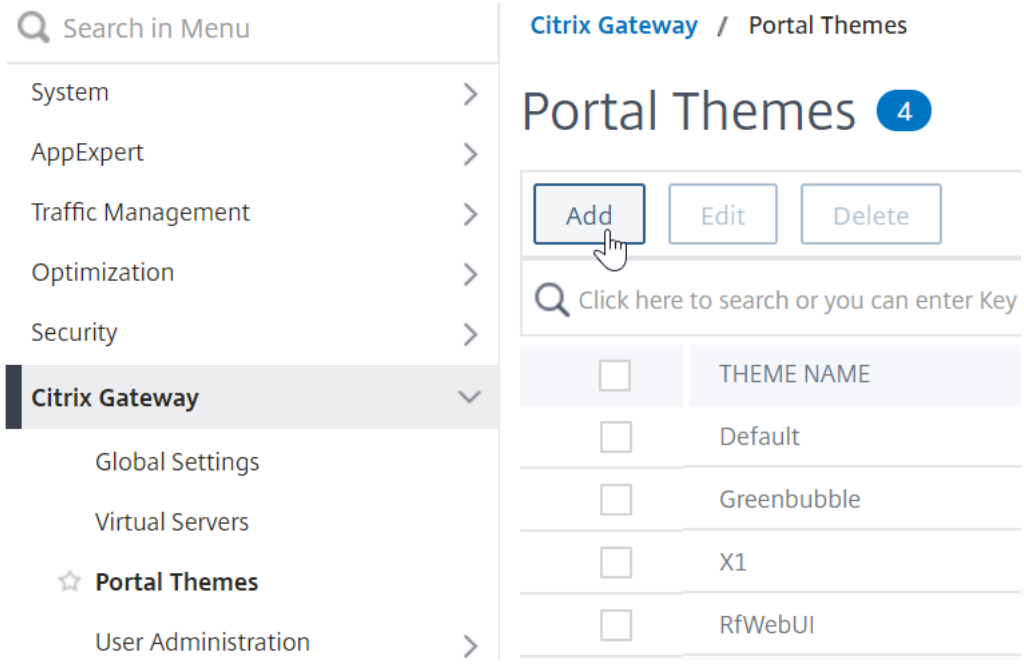


10. Cliquez sur **Continuer**.

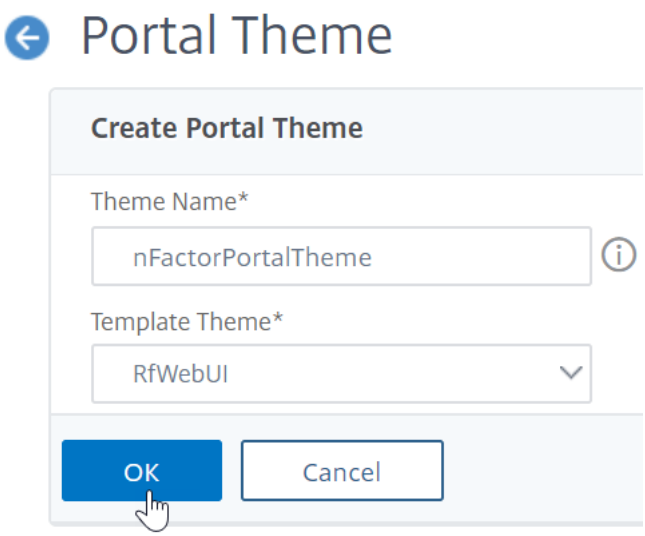


Liez le thème du portail au serveur virtuel d'authentification, d'autorisation et d'audit

1. Accédez à **NetScaler Gateway > Thèmes du portail**, puis ajoutez un thème. Vous créez le thème sous NetScaler Gateway, puis vous le liez ultérieurement au serveur virtuel d'authentification, d'autorisation et d'audit.

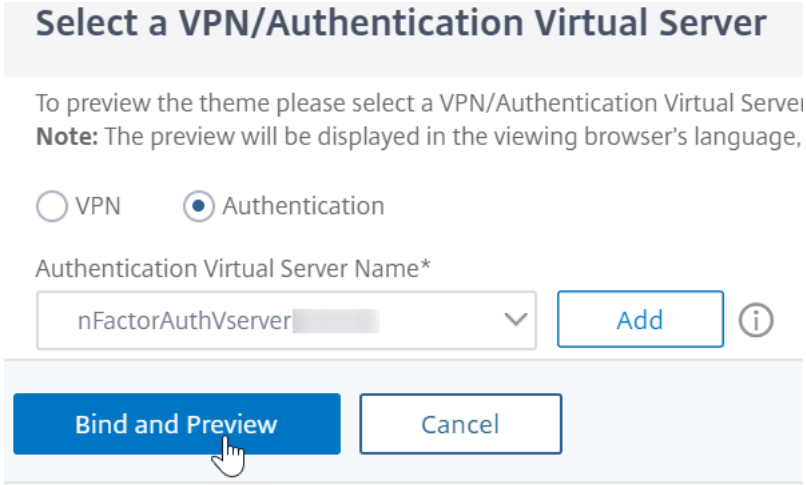


2. Créez un thème basé sur le thème du modèle RFWebUI.



3. Après avoir ajusté le thème comme vous le souhaitez, en haut de la page d'édition du thème du portail, **cliquez sur Cliquez pour lier et afficher le thème configuré**.

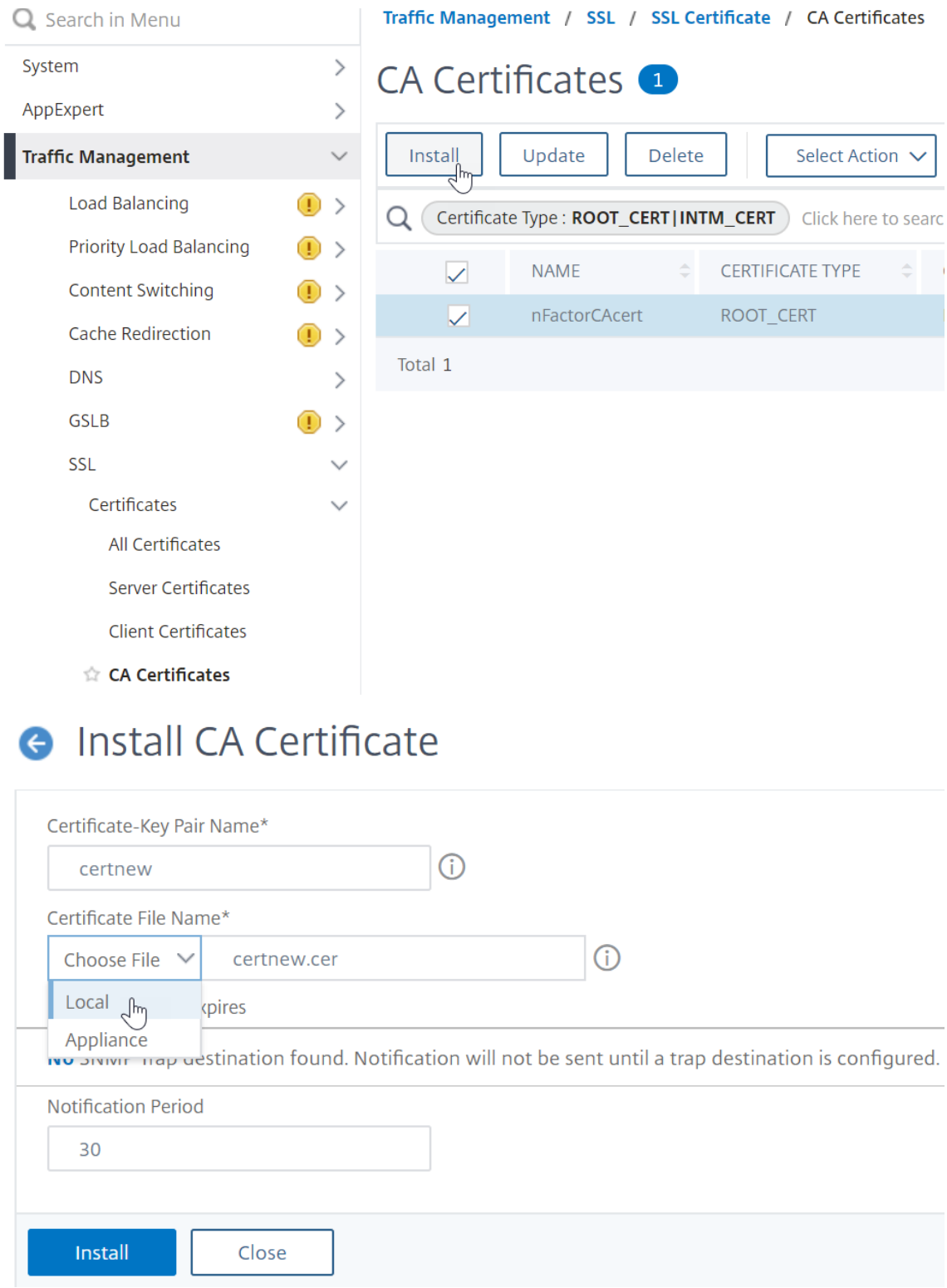
4. Changez la sélection sur Authentification. Dans le menu déroulant **Nom du serveur virtuel d'authentification**, sélectionnez le serveur virtuel d'authentification, d'autorisation et d'audit, puis cliquez sur **Lier et prévisualiser** et fermez la fenêtre d'aperçu.



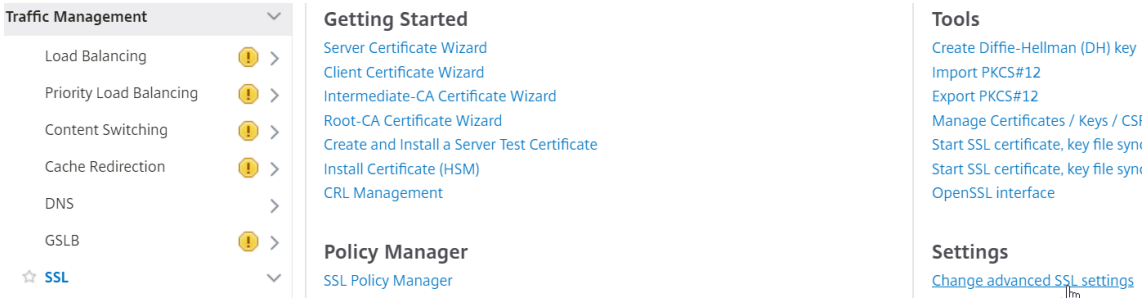
Activer l'authentification par certificat client

Si l'un de vos facteurs d'authentification est le certificat client, vous devez effectuer une certaine configuration SSL sur le serveur virtuel d'authentification, d'autorisation et d'audit :

1. Accédez à **Gestion du trafic > SSL > Certificats > Certificats d'autorité**de certification, puis installez le certificat racine de l'émetteur des certificats clients. Les certificats racine n'ont pas de fichier clé.



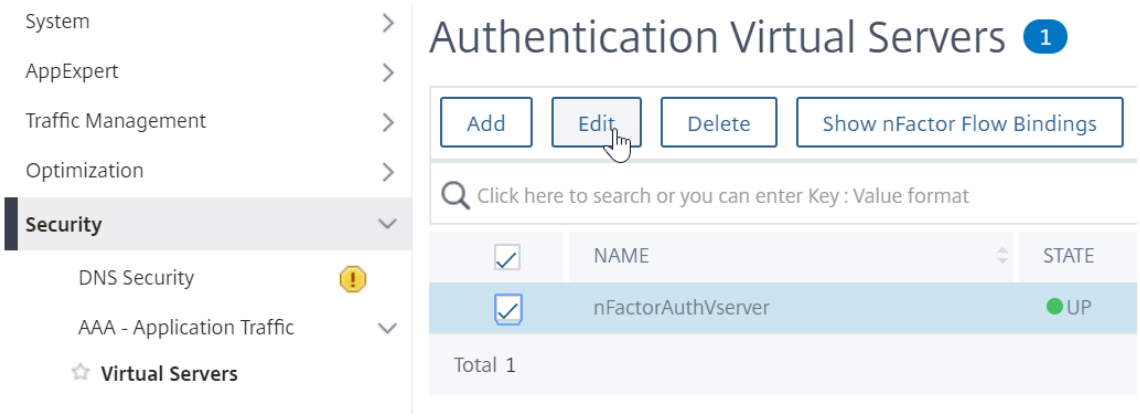
2. Accédez à **Gestion du trafic > SSL > Modifier les paramètres SSL avancés**.



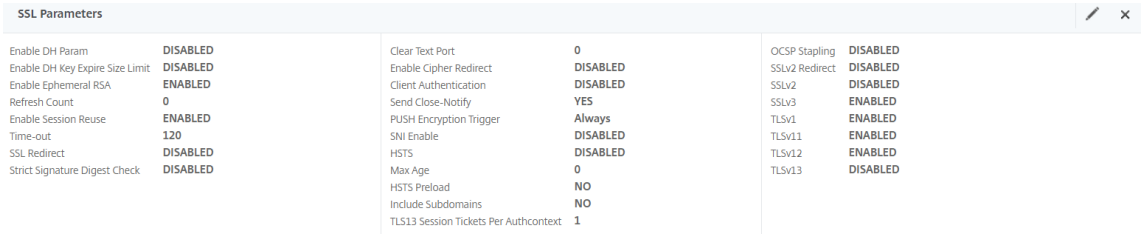
a) Faites défiler vers le bas pour vérifier si le **profil par défaut** est **ACTIVÉ**. Si oui, vous devez utiliser un profil SSL pour activer l'authentification par certificat client. Sinon, vous pouvez activer l'authentification par certificat client directement sur le serveur virtuel d'authentification, d'autorisation et d'audit dans la section Paramètres SSL.

3. Si les profils SSL par défaut ne sont pas activés :

a) Accédez à **Sécurité > AAA - Application > Serveurs virtuels**, puis modifiez un serveur virtuel d'authentification, d'autorisation et d'audit existant.

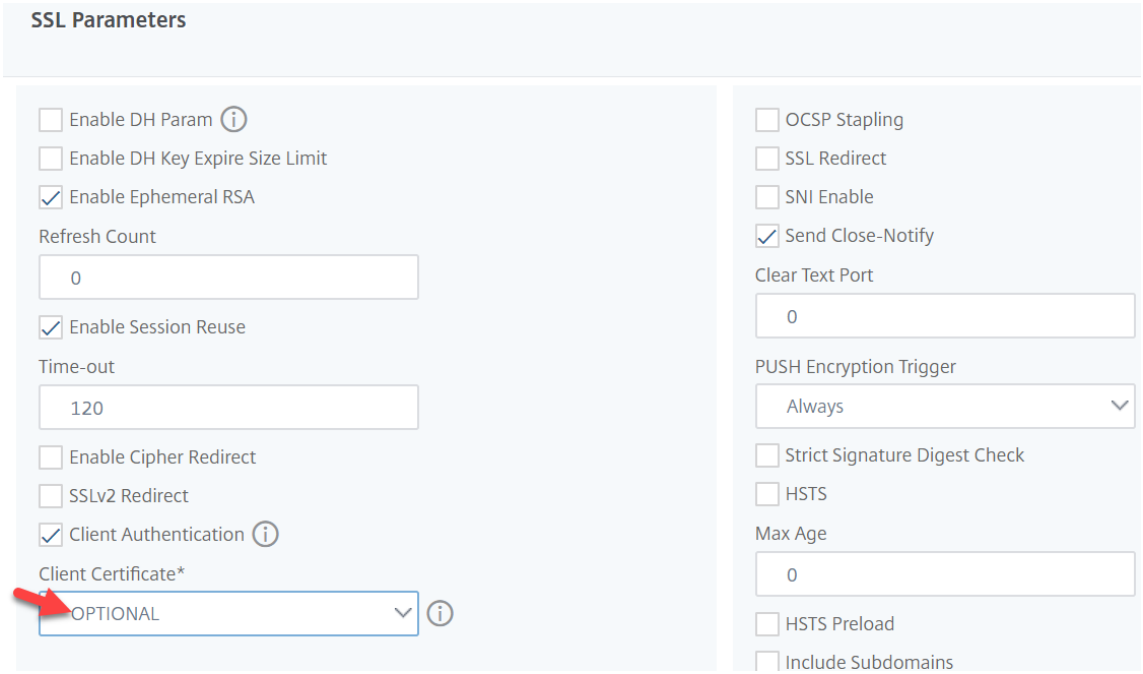


a) Sur la gauche, dans la section **Paramètres SSL**, cliquez sur l'icône en forme de crayon.



a) Cochez la case en regard de **Authentification du client**.

b) Assurez-vous que l' **option Facultatif** est sélectionnée dans le menu déroulant **Certificat client**, puis cliquez sur **OK**.



4. Si les profils SSL par défaut sont activés, créez un profil SSL avec l'authentification client activée :

   a) Dans le menu de gauche, développez Système, puis cliquez sur Profils.

   b) Dans l'angle supérieur droit, accédez à l'onglet Profil SSL.

   c) Cliquez avec le bouton droit de la souris sur le profil ns_default_ssl_profile_frontend, puis cliquez sur Ajouter. Cette option permet de copier les paramètres du profil par défaut.

   d) Donnez un nom au profil. Le but de ce profil est d'activer les certificats clients.

   e) Faites défiler vers le bas et recherchez la case à cocher Authentification client. Cochez la case.

   f) Changez le menu déroulant Certificat client sur FACULTATIF.

   g) La copie du profil SSL par défaut ne copie pas les chiffrements SSL. Vous devez les refaire.

   h) Cliquez sur Terminé lorsque vous avez terminé de créer le profil SSL.

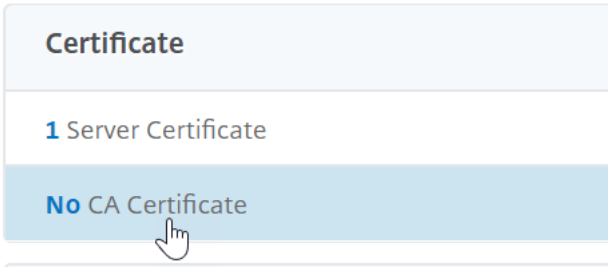
   i) Accédez à **Sécurité > AAA — Trafic des applications > Serveurs virtuels**, puis modifiez un serveur virtuel d'authentification, d'autorisation et d'audit.

   j) Faites défiler l'écran jusqu'à la section Profil SSL et cliquez sur le crayon.

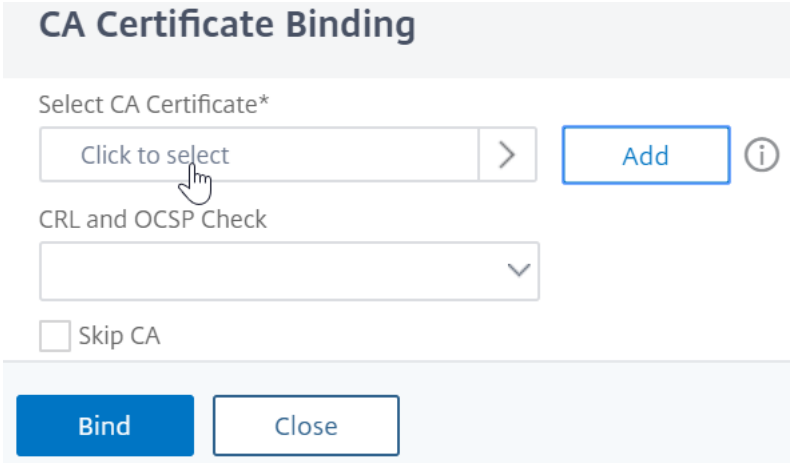
   k) Dans le menu déroulant Profil SSL, choisissez le profil pour lequel les certificats clients sont activés. Cliquez sur OK.

   l) Faites défiler cet article jusqu'à ce que vous obteniez les instructions pour lier le certificat d'autorité de certification.

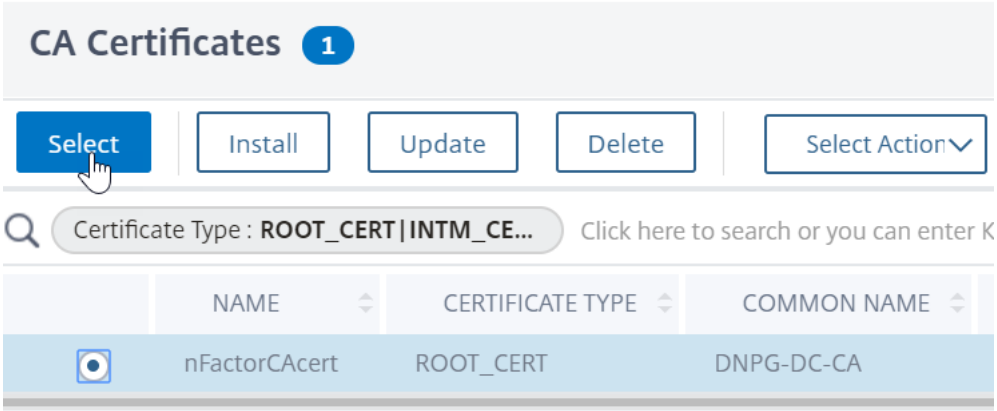
5. Sur la gauche, dans la section **Certificats**, cliquez à l'endroit où il est indiqué **Aucun certificat d'autorité de certification**.



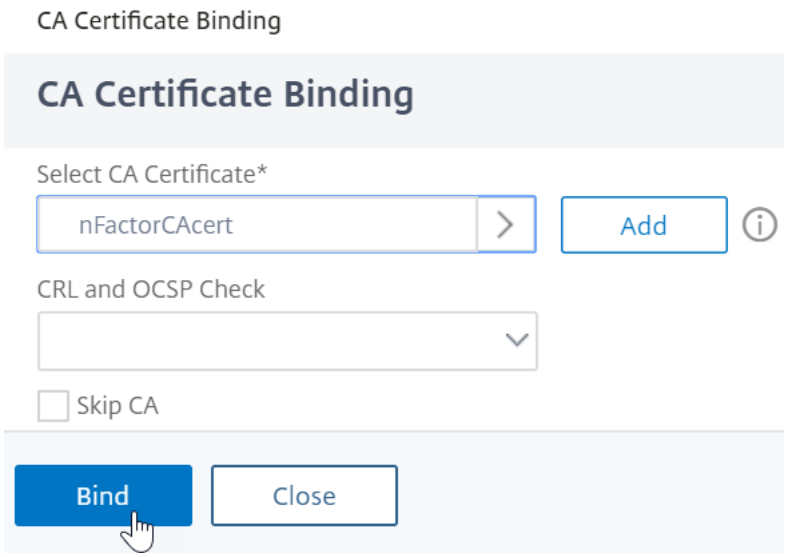
6. Cliquez sur le texte, **cliquez sur pour le sélectionner**.



7. Cliquez sur le bouton radio en regard du certificat racine de l'émetteur des certificats clients, puis cliquez sur **Sélectionner**.



8. Cliquez sur **Bind**.



Fichier XML du schéma de connexion

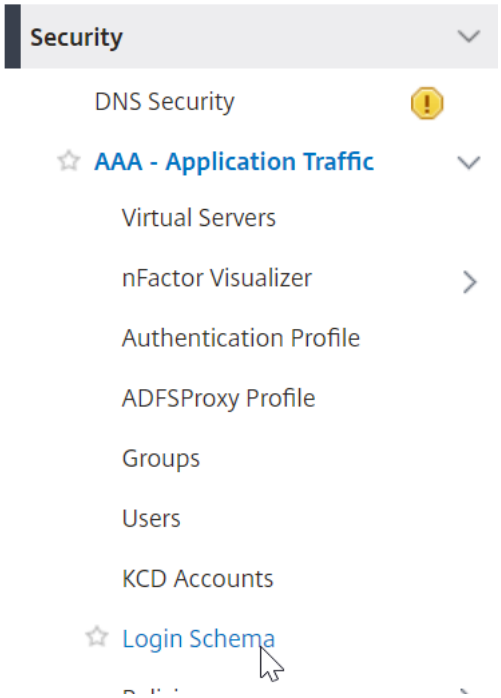
Le schéma de connexion est un fichier XML fournissant la structure des pages d'ouverture de session d'authentification basées sur des formulaires.

nFactor implique plusieurs facteurs d'authentification qui sont enchaînés ensemble. Chaque facteur peut avoir des pages/fichiers de schéma de connexion différents. Dans certains scénarios d'authentification, plusieurs écrans d'ouverture de session peuvent être présentés aux utilisateurs.

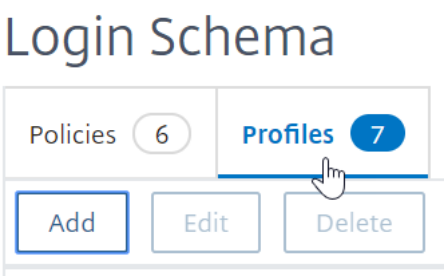
Configuration d'un profil de schéma de connexion

Pour configurer un profil de schéma de connexion, procédez comme suit :

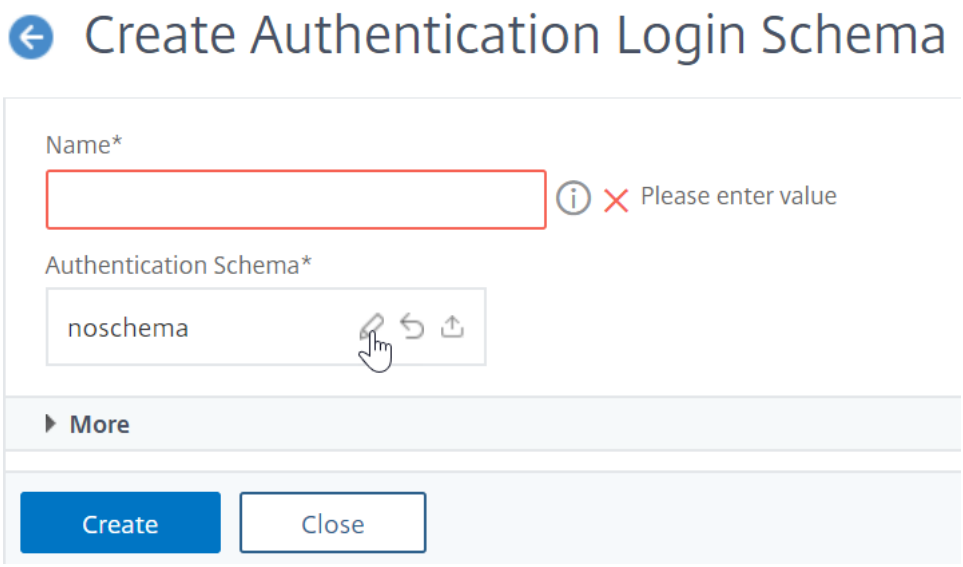
1. Créez ou modifiez un fichier .XML de schéma de connexion basé sur votre conception nFactor.
2. Accédez à **Sécurité > AAA - Trafic des applications > Schéma de connexion**.



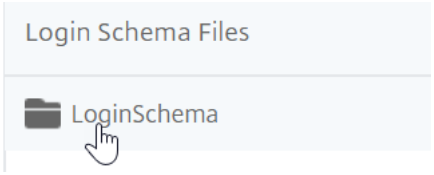
3. Sur la droite, accédez à l'onglet **Profils**, puis cliquez sur **Ajouter**.



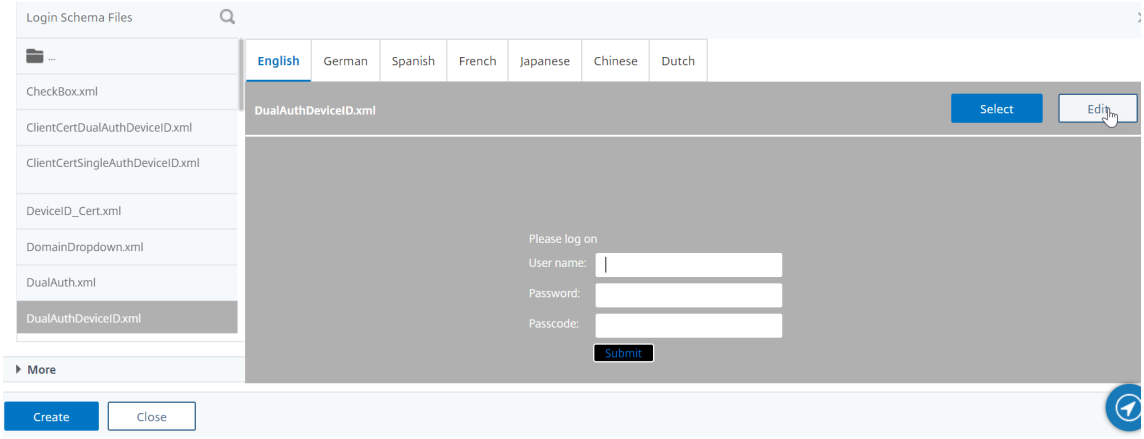
4. Dans le champ **Schéma d'authentification**, cliquez sur l'icône en forme de crayon.



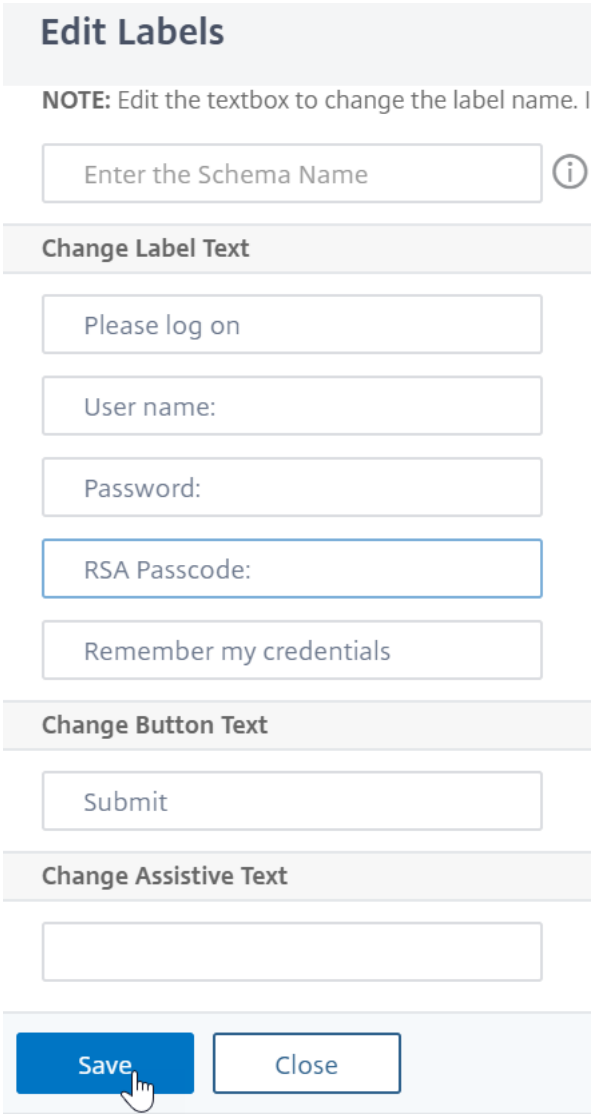
5. Cliquez sur le dossier LoginSchema pour afficher les fichiers qu'il contient.



6. Sélectionnez l'un des fichiers. Vous pouvez voir un aperçu sur la droite. Les étiquettes peuvent être modifiées en cliquant sur le bouton **Modifier** en haut à droite.

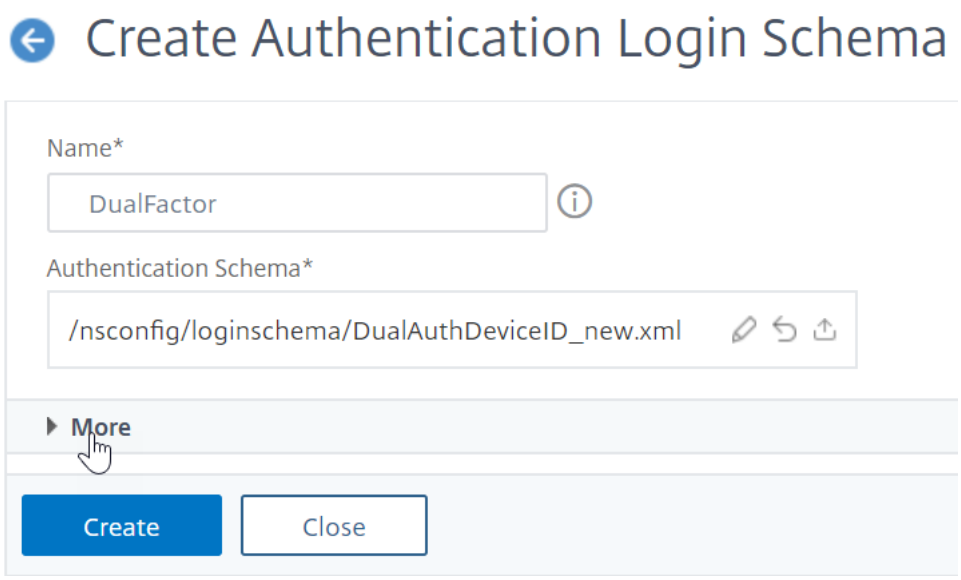


7. Lorsque vous enregistrez les modifications, un nouveau fichier est créé sous /NSconfig/loginSchema.



8. En haut à droite, cliquez sur **Sélectionner**.

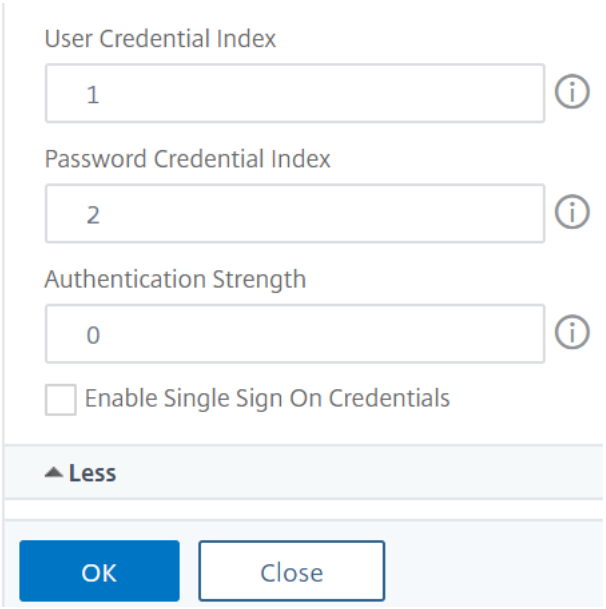
9. Donnez un nom au schéma de connexion, puis cliquez sur **Plus**.



10. Utilisez le nom d'utilisateur et le mot de passe saisis dans le schéma de connexion pour l'authentification unique (SSO) à un service principal, par exemple StoreFront.

    Vous pouvez utiliser les informations d'identification saisies dans le schéma de connexion comme informations d'identification Single Sign-On en utilisant l'une des méthodes suivantes.

    - Cliquez sur **Plus** en bas de la page **Créer un schéma de connexion d'authentification** et sélectionnez **Activer les informations d'identification de connexion unique**.
    - Cliquez sur **Plus** en bas de la page **Créer un schéma de connexion d'authentification** et entrez des valeurs uniques pour l'index des informations d'identification de l'utilisateur et l'index des informations d'identification de mot de passe. Ces valeurs peuvent être comprises entre 1 et 16. Plus tard, vous référencerez ces valeurs d'index dans une stratégie/un profil de trafic en utilisant l'expression AAA.USER.ATTRIBUTE (#).



11. Cliquez sur **OK** pour créer le profil de schéma de connexion.

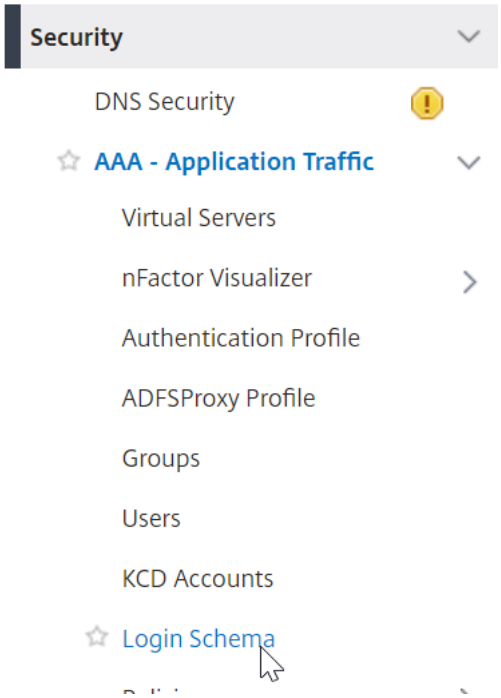
> **Remarque :** Si vous modifiez le fichier de schéma de connexion (.xml) ultérieurement, pour que les modifications soient prises en compte, vous devez modifier le profil de schéma de connexion et sélectionner à nouveau le fichier de schéma de connexion (.xml).

Créer et lier une stratégie de schéma de connexion

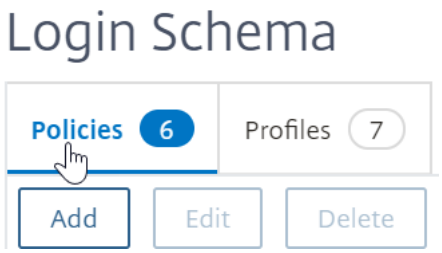
Pour lier un profil de schéma de connexion à un serveur virtuel d'authentification, d'autorisation et d'audit, vous devez d'abord créer une stratégie de schéma de connexion. Les stratégies de schéma de connexion ne sont pas obligatoires lorsque vous liez le profil de schéma de connexion à une étiquette de stratégie d'authentification, comme indiqué plus loin.

Pour créer et lier une stratégie de schéma de connexion, procédez comme suit :

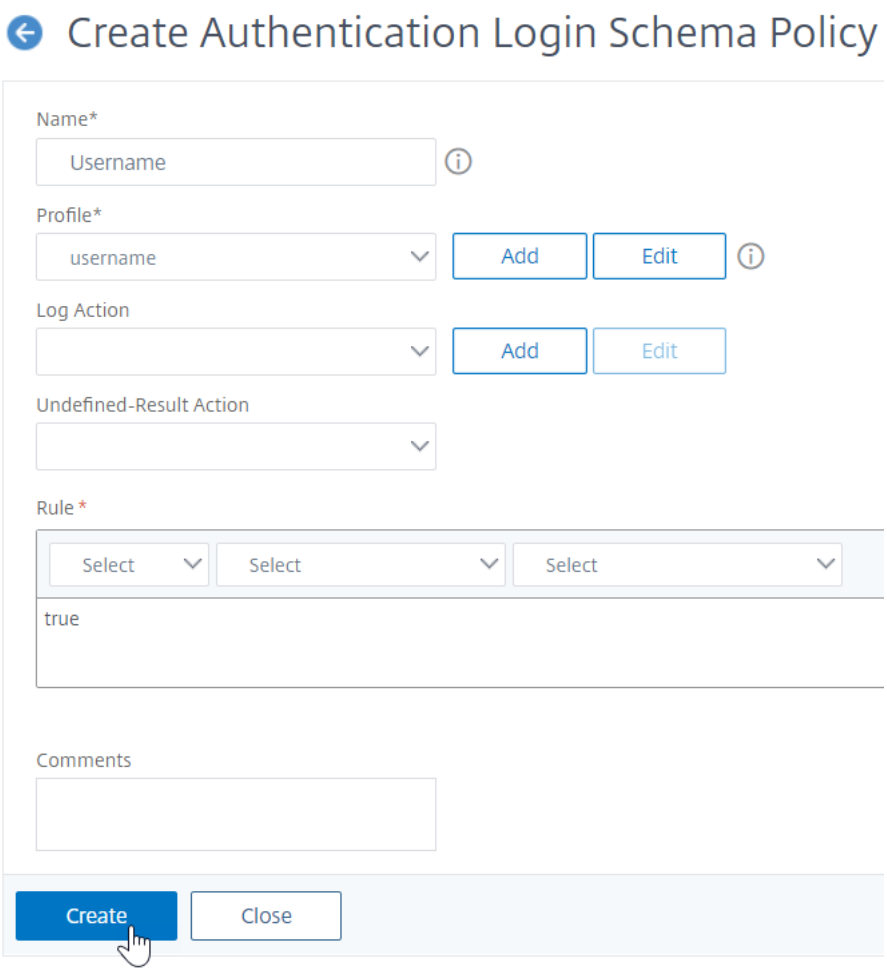
1. Accédez à **Sécurité > AAA - Trafic des applications > Schéma de connexion**.



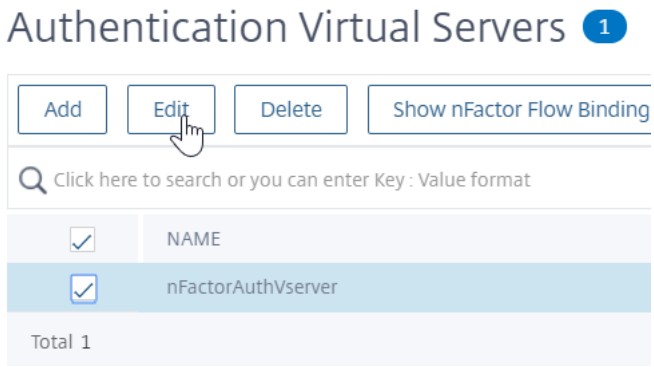
2. Dans l'onglet **Policies**, cliquez sur **Add**.



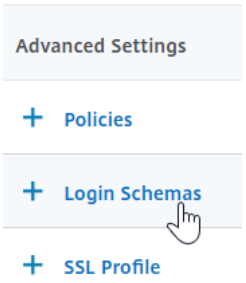
3. Utilisez le menu déroulant **Profil** pour sélectionner le profil de schéma de connexion que vous avez déjà créé.
4. Entrez une expression de stratégie avancée dans la zone **Règle**, puis cliquez sur **Créer**.



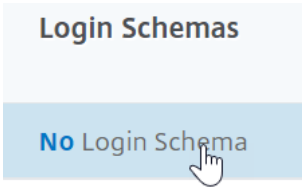
5. Sur la gauche, accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**, puis modifiez un serveur virtuel d'authentification, d'autorisation et d'audit existant.



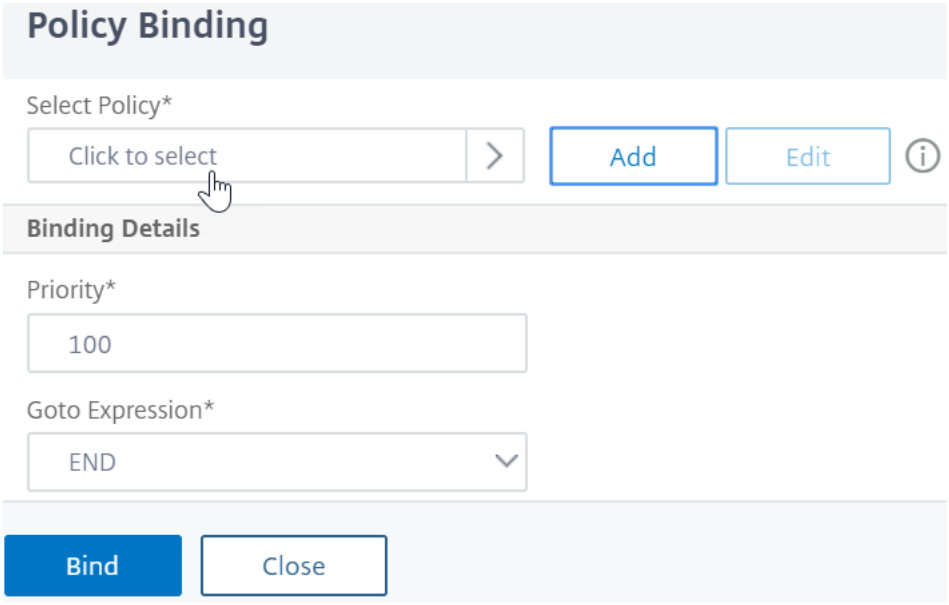
6. Dans la colonne Paramètres avancés, cliquez sur **Schémas de connexion**.



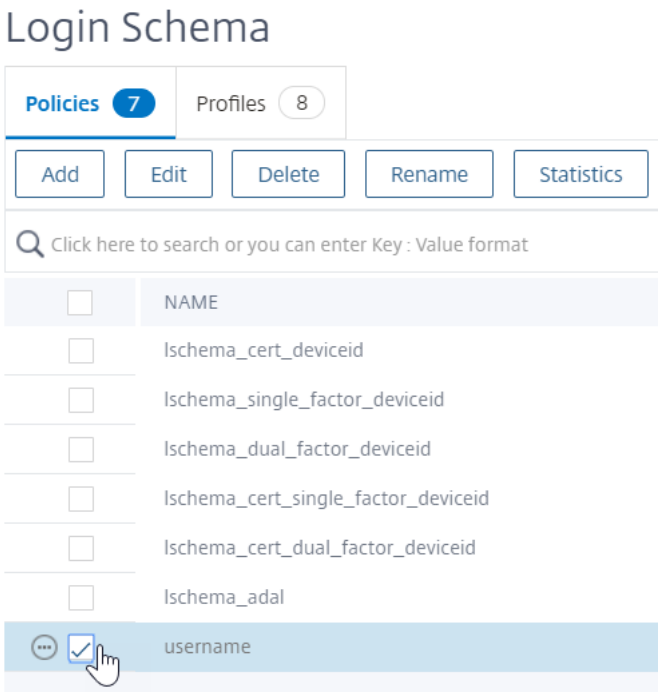
7. Dans la section Schémas de connexion, cliquez sur le texte **Aucun schéma de connexion**.



8. Cliquez sur le texte, **cliquez sur pour le sélectionner**.



9. Cliquez sur le bouton radio en regard de la stratégie de schéma de connexion, puis cliquez sur **Sélectionner**. Seules les stratégies de schéma de connexion apparaissent dans cette liste. Les profils de schéma de connexion (sans stratégie) n'apparaissent pas.



10. Cliquez sur **Bind**.

Stratégies d'authentification avancées

Les stratégies d'authentification sont une combinaison d'expression de stratégie et d'action de stratégie. Si l'expression est vraie, évaluez l'action d'authentification.

Créer des stratégies d'authentification avancées

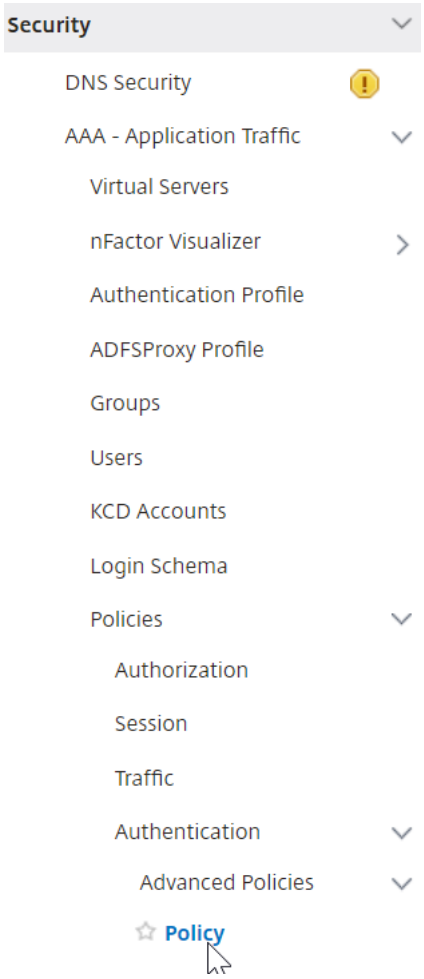
Les stratégies d'authentification sont une combinaison d'expression de stratégie et d'action de stratégie. Si l'expression est vraie, évaluez l'action d'authentification.

Vous avez besoin d'actions/serveurs d'authentification (par exemple LDAP, RADIUS, CERT, SAML, etc.) Lors de la création d'une stratégie d'authentification avancée, une icône plus (Ajouter) vous permet de créer des actions/serveurs d'authentification.

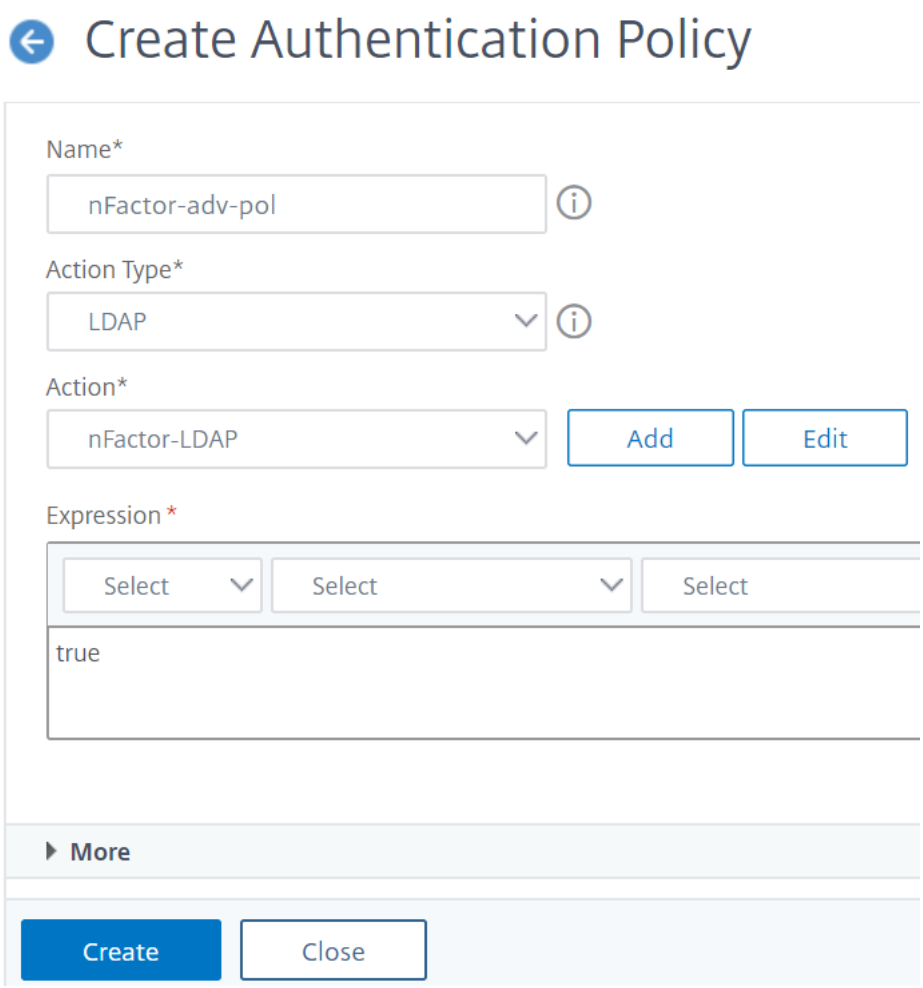
Vous pouvez également créer des actions d'authentification (serveurs) avant de créer la stratégie d'authentification avancée. Les serveurs d'authentification se trouvent sous **Authentification > Tableau de bord**. Sur la droite, cliquez sur Ajouter et sélectionnez un type de serveur. Les instructions relatives à la création de ces serveurs d'authentification ne sont pas détaillées ici. Consultez les procédures Authentification — NetScaler 12/NetScaler 12.1.

Pour créer une stratégie d'authentification avancée, procédez comme suit :

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégie**



2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une stratégie, cliquez sur **Ajouter**.
   - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Créer une stratégied'authentification ou Configurer la stratégie** d'authentification, tapez ou sélectionnez des valeurs pour les paramètres.



- **Nom** : nom de la stratégie. Impossible de modifier une stratégie précédemment configurée.
- **Type d'action** : type de stratégie : Cert, Negotiate, LDAP, RADIUS, SAML, SAMLIDP, TACACS ou WEBAUTH.
- **Action : action** d'authentification (profil) à associer à la stratégie. Vous pouvez choisir une action d'authentification existante ou cliquer sur le signe plus et créer une action du type approprié.
- **Action de journalisation** : action d'audit à associer à la stratégie. Vous pouvez choisir une action d'audit existante ou cliquer sur le signe plus et créer une action.
  Aucune action n'est configurée, ou pour créer une action, cliquez sur **Ajouter** et terminez les étapes.
- **Expression** : règle qui sélectionne les connexions auxquelles vous souhaitez appliquer l'action que vous avez spécifiée. La règle peut être simple (« true » sélectionne tout le trafic) ou complexe. Pour entrer des expressions, commencez par choisir le type d'expression dans la liste déroulante située le plus à gauche sous la fenêtre Expression, puis en tapant votre expression directement dans la zone de texte de l'expression, ou en

cliquant sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant les listes déroulantes qu'elle contient pour créer votre expression.)

- **Commentaire** : vous pouvez saisir un commentaire décrivant le type de trafic auquel cette stratégie d'authentification s'applique. Facultatif.

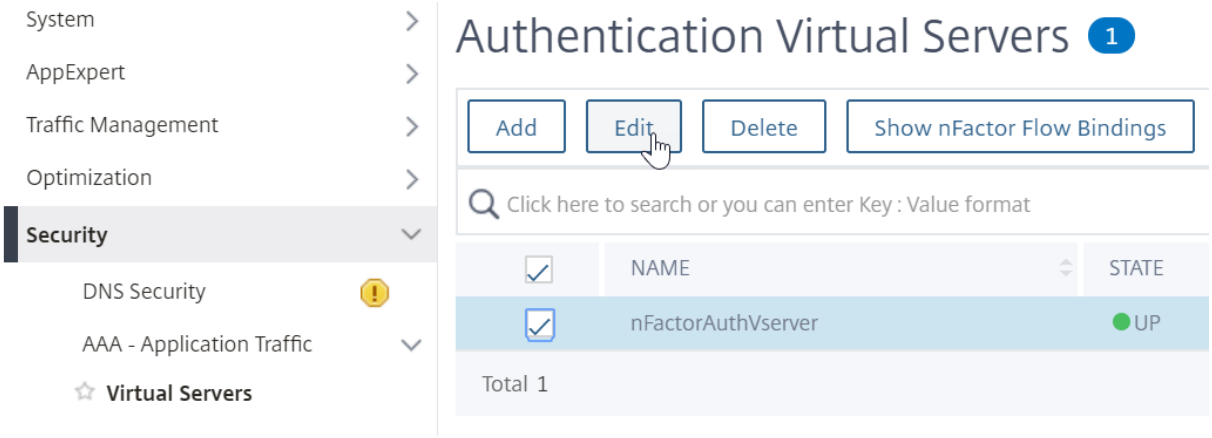
4. Cliquez sur **Create**, puis cliquez sur **Close**. Si vous avez créé une stratégie, cette stratégie apparaît dans la page Stratégies et serveurs d'authentification.

Créez des stratégies d'authentification avancées supplémentaires selon vos besoins en fonction de votre conception nFactor.

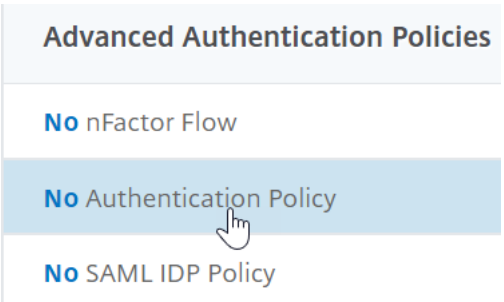
Lier la stratégie d'authentification avancée premier facteur à l'authentification, à l'autorisation et à l'audit

Vous pouvez lier directement des stratégies d'authentification avancées pour le premier Factor le serveur virtuel d'authentification, d'autorisation et d'audit. Pour les facteurs suivants, vous devez lier les stratégies d'authentification avancées aux étiquettes de stratégie d'authentification.

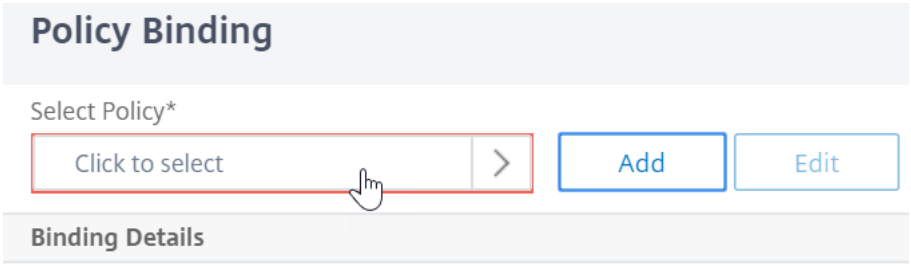
1. Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**. Modifiez un serveur virtuel existant.



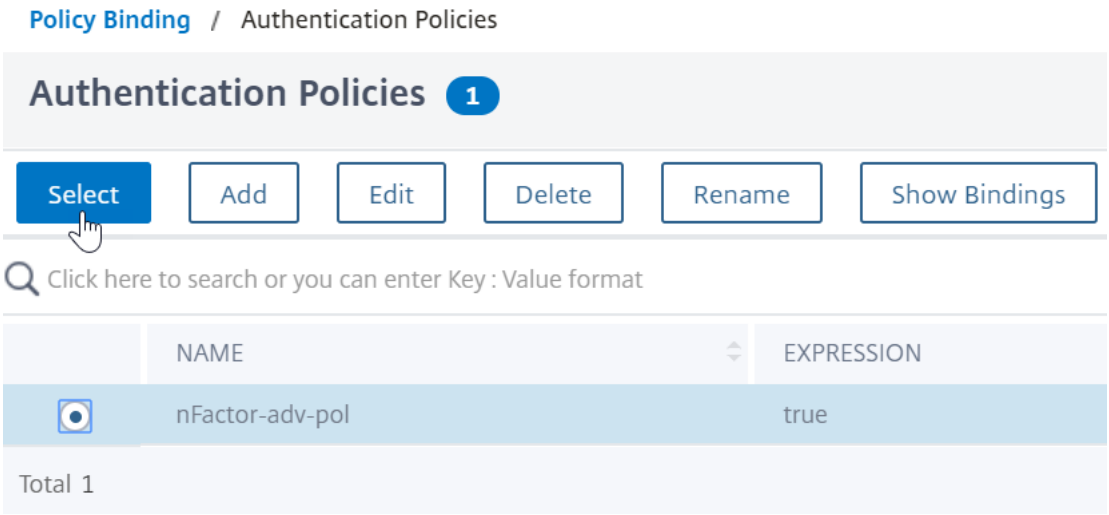
1. Sur la gauche, dans la section Stratégies d'authentification avancées, cliquez sur **Aucune stratégie d'authentification**.



2. Dans **Sélectionner une stratégie**, cliquez sur le texte, **cliquez sur pour sélectionner**.

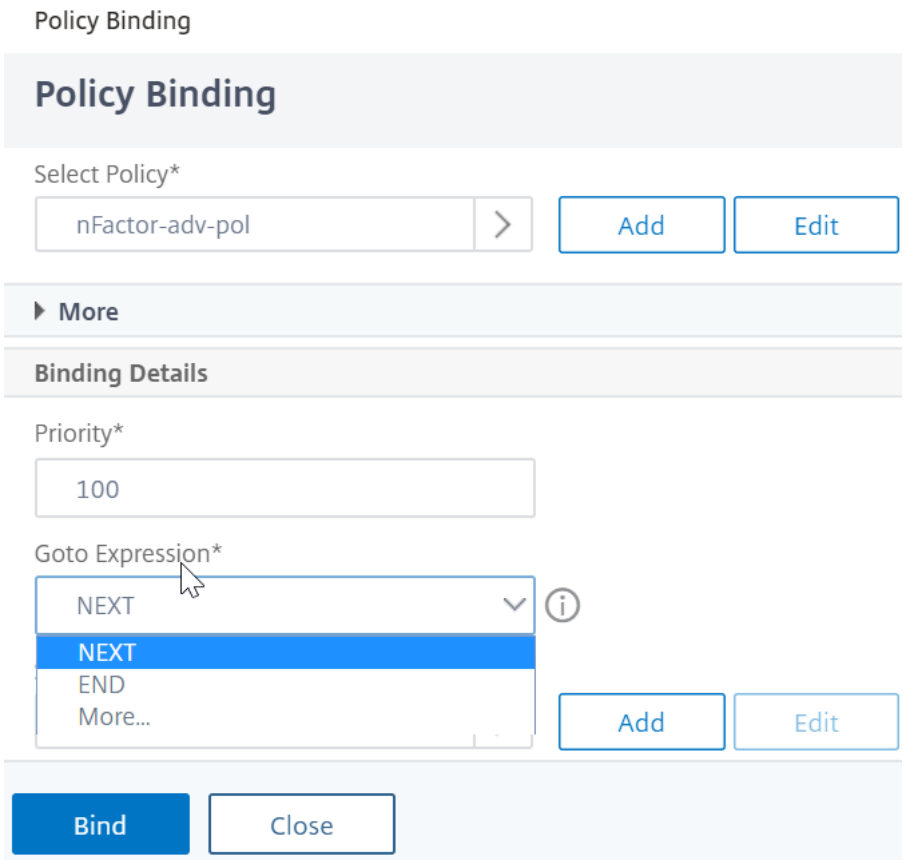


3. Cliquez sur le bouton radio en regard de la **stratégie d'authentification avancée**, puis cliquez sur **Sélectionner**.

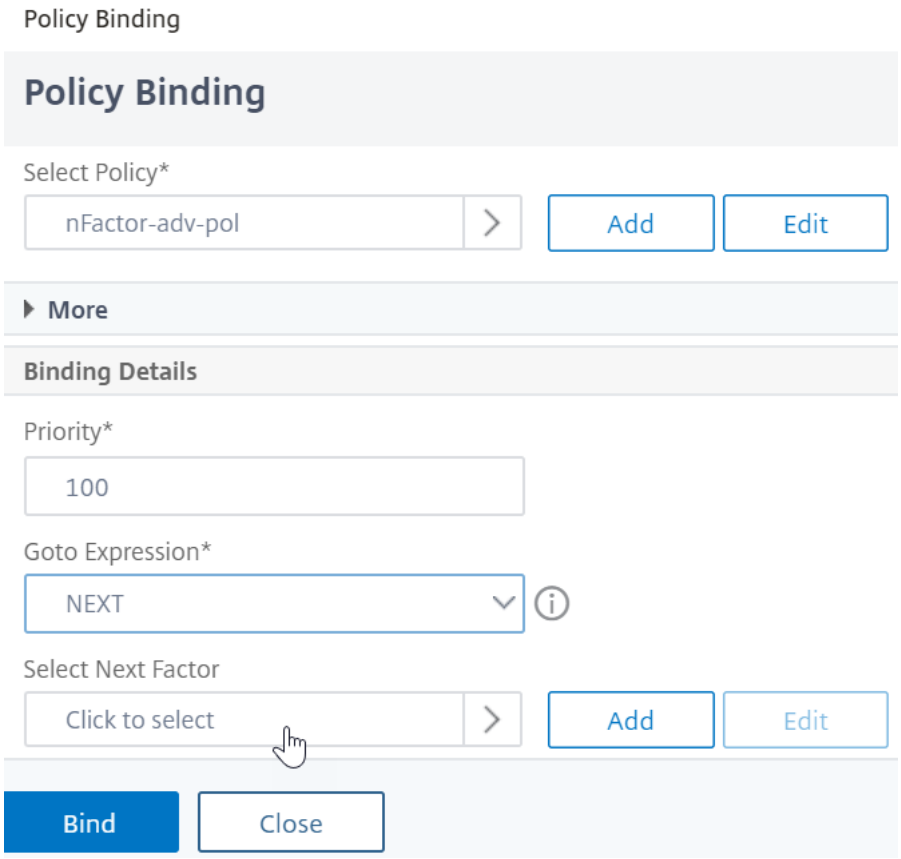


4. Dans la section Détails de la liaison, l' **expression Goto** détermine ce qui se passe ensuite si cette stratégie d'authentification avancée échoue.

   - Si **l'expression Goto** est définie sur **NEXT**, la stratégie d'authentification avancée suivante liée à ce serveur virtuel d'authentification, d'autorisation et d'audit est évaluée.
   - Si **l'expression Goto** est définie sur **END**ou s'il n'existe plus de stratégie d'authentification avancée liée à ce serveur virtuel d'authentification, d'autorisation et d'audit, l'authentification est terminée et marquée comme ayant échoué.



5. Dans **Sélectionner le facteur suivant**, vous pouvez sélectionner peut pointer vers une étiquette de stratégie d'authentification. Le facteur suivant est évalué uniquement si la stratégie d'authentification avancée réussit. Enfin, cliquez sur **Bind**.



Utiliser les groupes LDAP extraits pour sélectionner le facteur d'authentification suivant

Vous pouvez utiliser les groupes LDAP extraits pour sélectionner le prochain facteur d'authentification sans authentifier réellement avec LDAP.

1. Lorsque vous créez ou modifiez un serveur LDAP ou une action LDAP, désactivez la case à cocher **Authentification** .
2. Dans **Autres paramètres**, sélectionnez les valeurs appropriées dans **Attribut de groupe** et **Nom de sous-attribut**.

Authentification de l'étiquette de stratégie

Lorsque vous liez une stratégie d'authentification avancée au serveur virtuel d'authentification, d'autorisation et d'audit et que vous avez sélectionné un facteur suivant, le facteur suivant est évalué uniquement si la stratégie d'authentification avancée aboutit. Le prochain facteur qui est évalué est une étiquette de stratégie d'authentification.

L'étiquette de stratégie d'authentification spécifie un ensemble de stratégies d'authentification pour un facteur particulier. Chaque étiquette de stratégie correspond à un seul facteur. Il spécifie également le formulaire de connexion qui doit être présenté à l'utilisateur. L'étiquette de stratégie

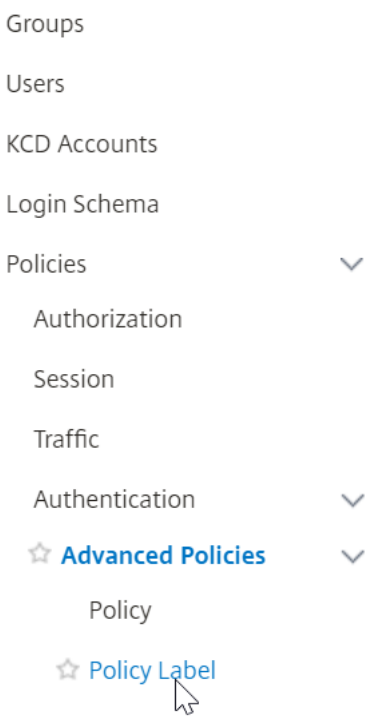
d'authentification doit être liée en tant que facteur suivant d'une stratégie d'authentification ou d'une autre étiquette de stratégie d'authentification.

Remarque : Chaque facteur n'a pas besoin d'un schéma de connexion. Le profil de schéma de connexion n'est requis que si vous liez un schéma de connexion à une étiquette de stratégie d'authentification.

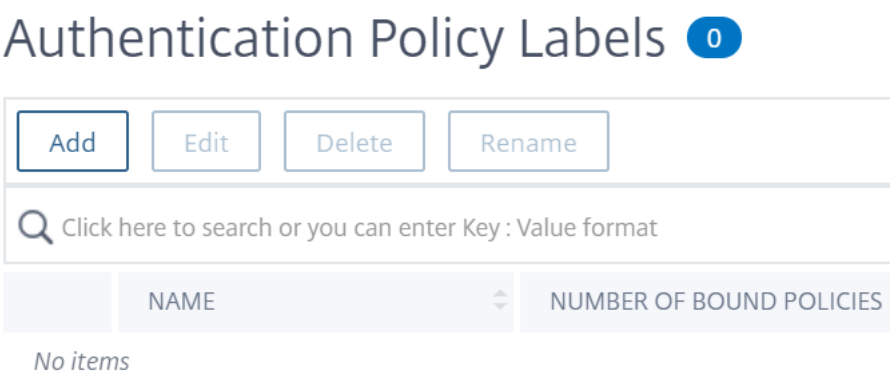
Création d'une étiquette de stratégie d'authentification

Une étiquette de stratégie spécifie les stratégies d'authentification pour un facteur particulier. Chaque étiquette de stratégie correspond à un seul facteur. L'étiquette de stratégie spécifie le formulaire de connexion qui doit être présenté à l'utilisateur. L'étiquette de stratégie doit être liée en tant que facteur suivant d'une stratégie d'authentification ou d'une autre étiquette de stratégie d'authentification. En règle générale, une étiquette de stratégie inclut des stratégies d'authentification pour un mécanisme d'authentification spécifique. Toutefois, vous pouvez également avoir une étiquette de stratégie qui comporte des stratégies d'authentification pour différents mécanismes d'authentification.

1. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Authentification > Stratégies avancées > Libellé de stratégie**.



2. Cliquez sur le bouton **Add**.

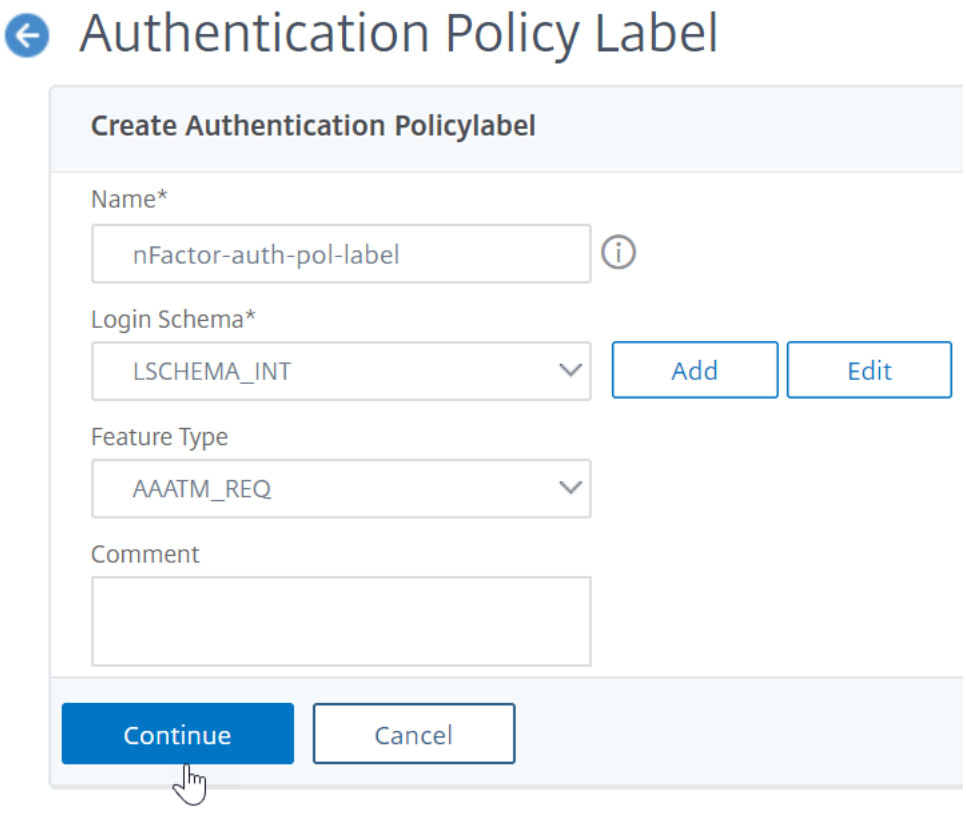


3. Remplissez les champs suivants pour créer une étiquette de stratégie d'authentification :

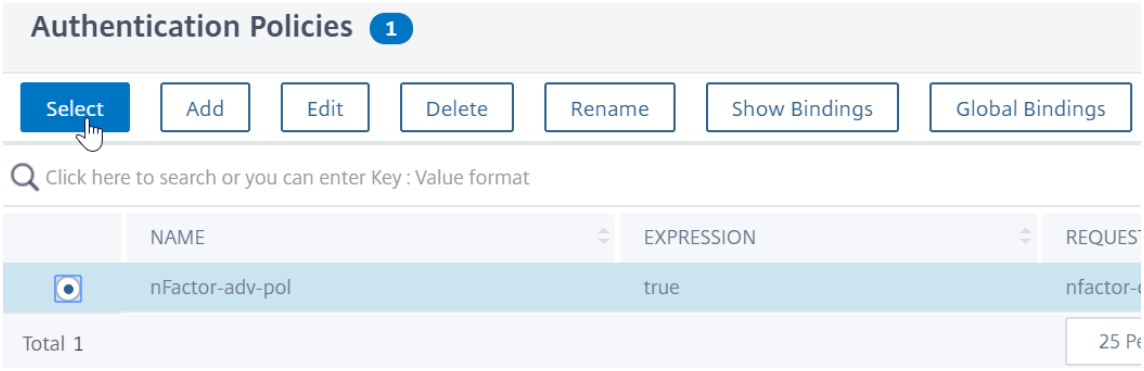
   a) Entrez le **nom de** la nouvelle étiquette de stratégie d'authentification.

   b) Sélectionnez le **schéma de connexion** associé à l'étiquette de stratégie d'authentification. SI vous ne souhaitez rien afficher pour l'utilisateur, vous pouvez sélectionner un profil de schéma de connexion défini sur aucun schéma (LSCHEMA_INT).

   c) Cliquez sur **Continuer**.



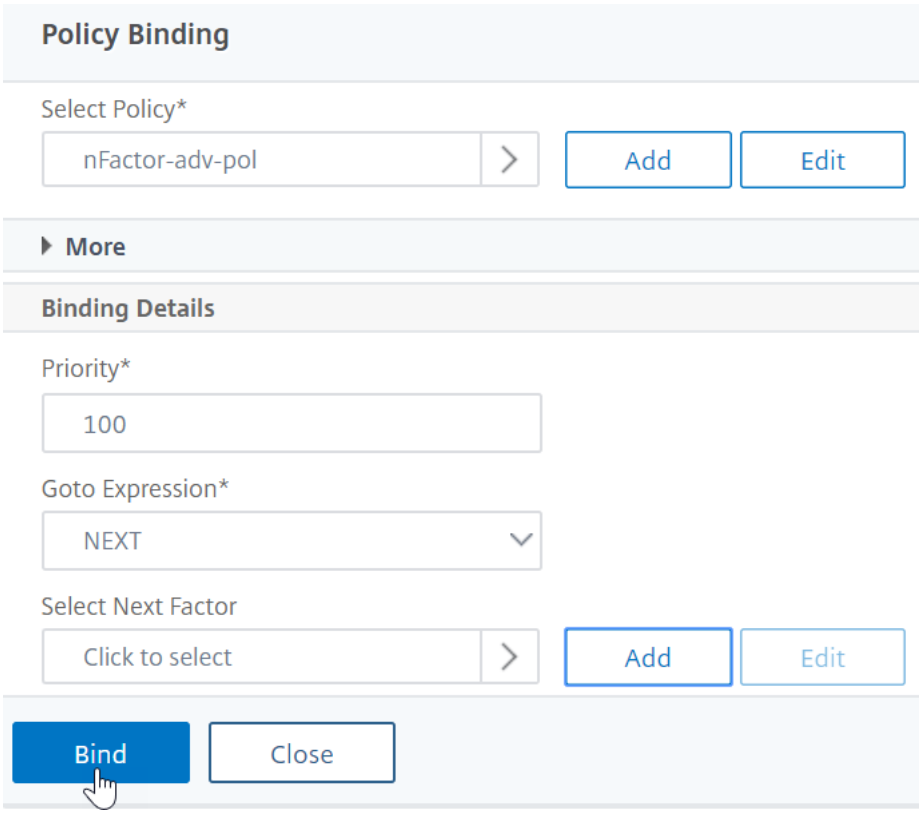
4. Dans la section **Liaison de stratégie**, cliquez à l'endroit où il est indiqué **Cliquez pour sélectionner**.
5. Sélectionnez la stratégie d'authentification qui évalue ce facteur.



6. Renseignez les champs suivants :

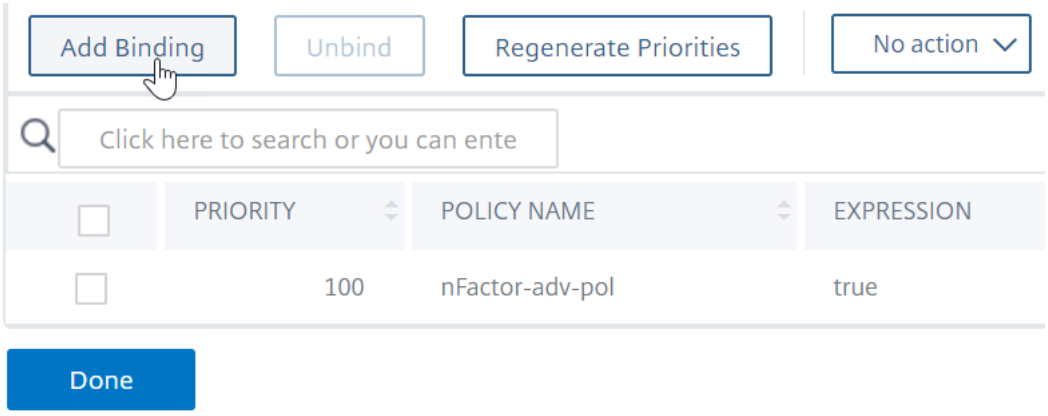
   a) Entrez la **priorité** de la liaison de stratégie.

   b) Dans **Goto Expression**, sélectionnez **SUIVANT** si vous souhaitez lier des stratégies d'authentification plus avancées à ce facteur ou sélectionnez **FIN**.



7. Dans **Sélectionner le facteur suivant**, si vous souhaitez ajouter un autre facteur, cliquez sur pour sélectionner et lier l'étiquette de stratégie d'authentification suivante (facteur suivant). Si vous ne sélectionnez pas le facteur suivant, et si cette stratégie d'authentification avancée réussit, l'authentification est réussie et terminée.
8. Cliquez sur **Bind**.
9. Vous pouvez cliquer sur **Ajouter une liaison** pour ajouter des stratégies d'authentification plus

avancées à cette étiquette de stratégie (facteur). Cliquez sur **Terminé lorsque vous avez** terminé.



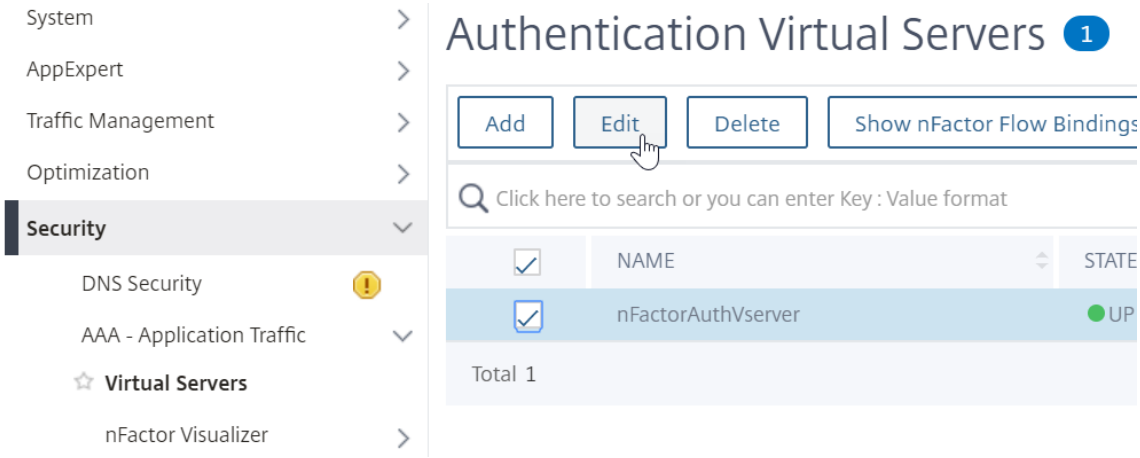
Libellé de stratégie d'authentification de liaison

Après avoir créé l'étiquette de stratégie, vous la liez à une stratégie d'authentification avancée existante pour enchaîner les facteurs ensemble.

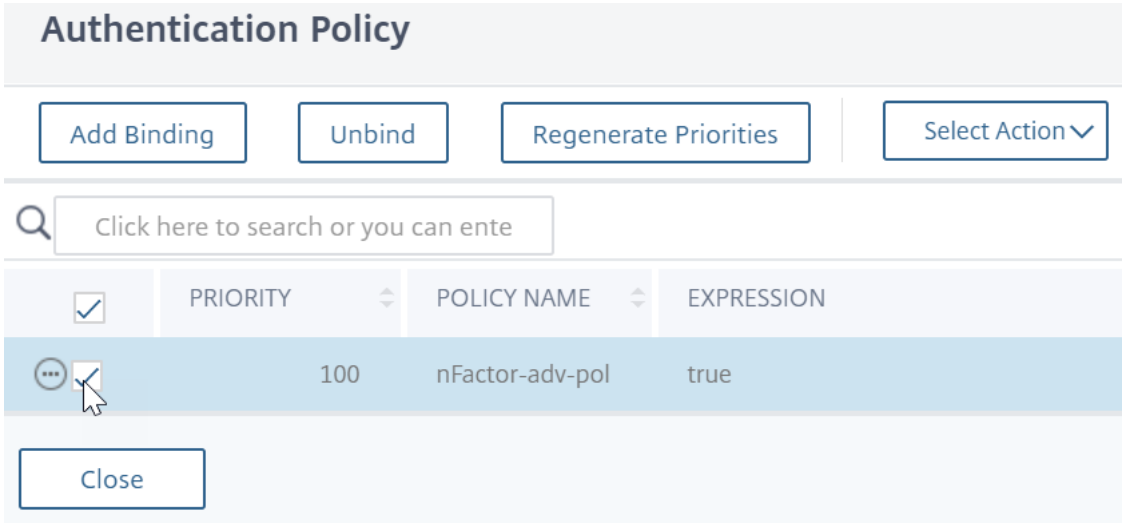
Vous pouvez sélectionner le facteur suivant lorsque vous modifiez un serveur virtuel d'authentification, d'autorisation et d'audit existant qui possède une stratégie d'authentification avancée liée ou lorsque vous modifiez une étiquette de stratégie différente pour inclure le facteur suivant.

Pour modifier un serveur virtuel d'authentification, d'autorisation et d'audit existant auquel est déjà liée une stratégie d'authentification avancée

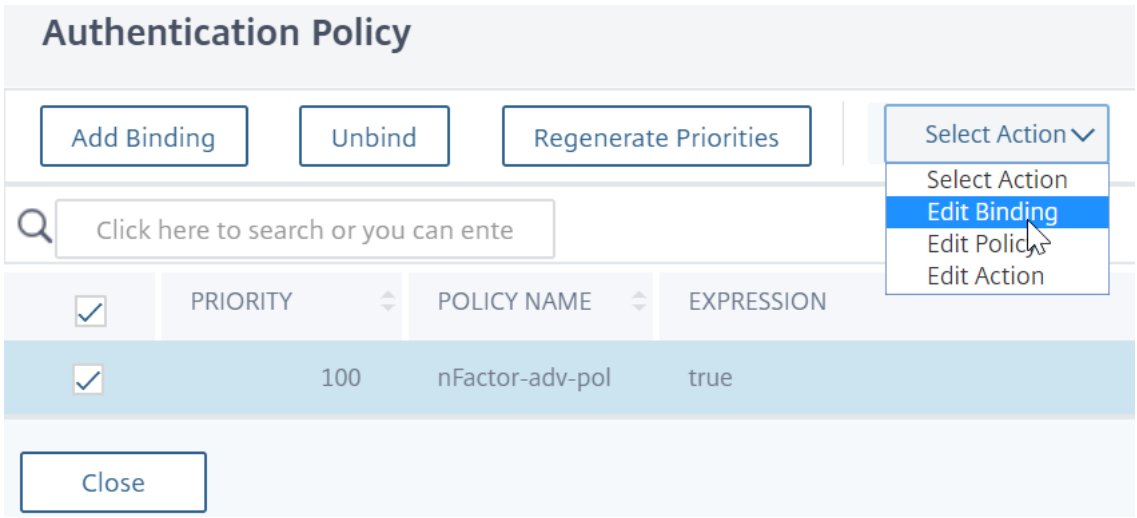
1. Accédez à **Sécurité > AAA — Trafic d'applications > Serveurs virtuels.** Sélectionnez le serveur virtuel et cliquez sur **Modifier**.



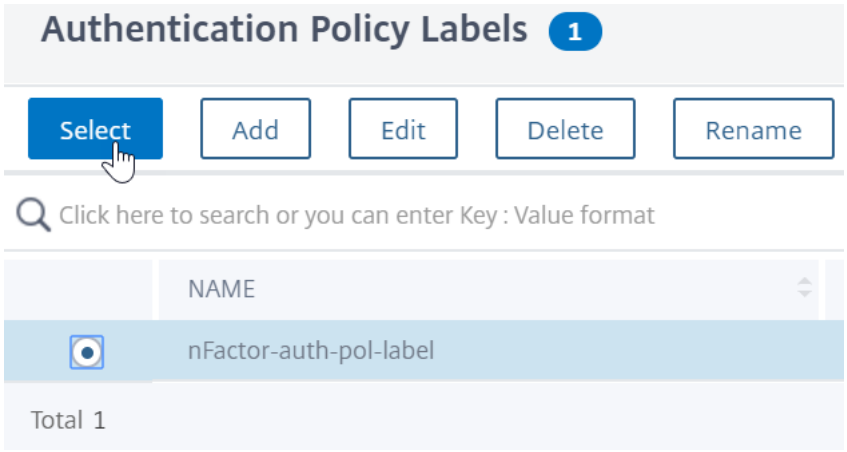
2. Sur la gauche, dans la section **Stratégies d'authentification avancées**, cliquez sur une liaison de stratégie d'authentification existante.



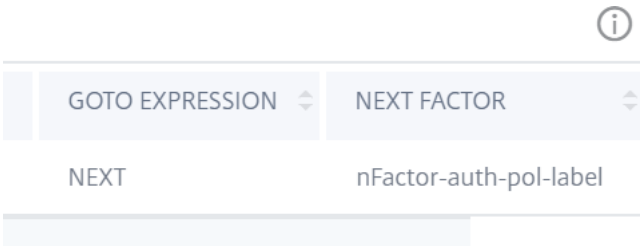
3. Dans **Sélectionner une action**, cliquez sur **Modifier la liaison**.



4. Dans **Sélectionner le facteur suivant**, cliquez sur, puis sélectionnez une étiquette de stratégie d'authentification existante (facteur suivant).

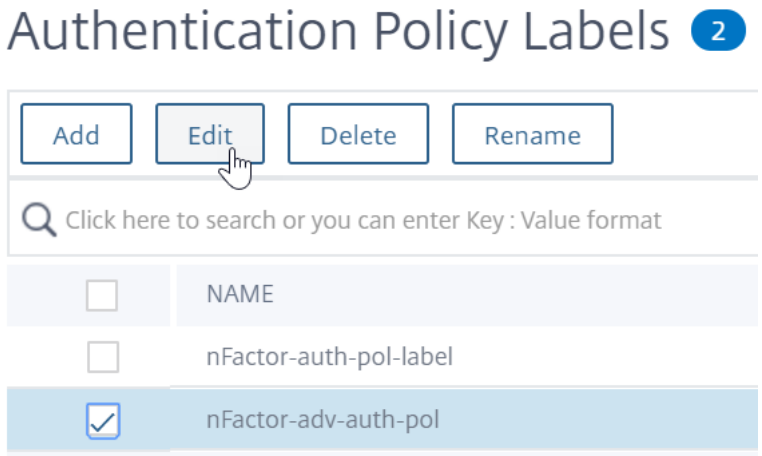


5. Cliquez sur **Bind**. Vous pouvez voir le facteur suivant à l'extrême droite.

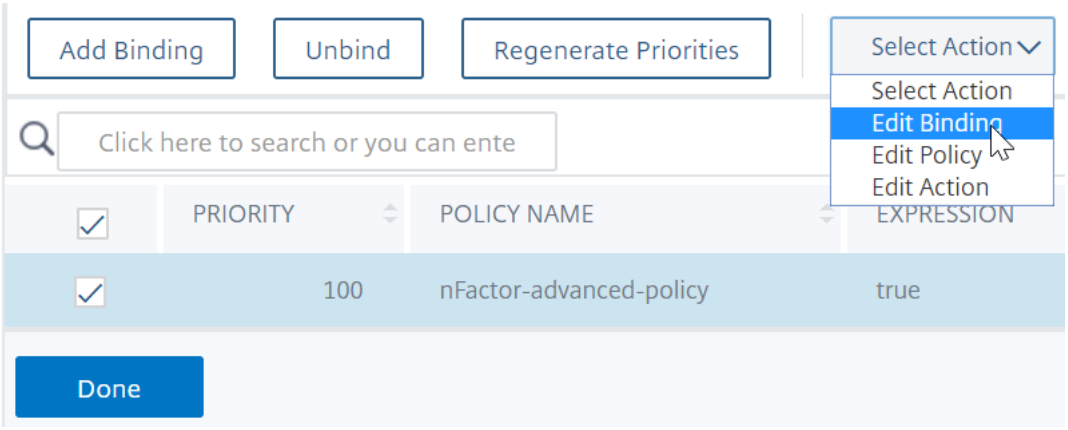


Pour ajouter un facteur suivant d'étiquette de stratégie à un autre libellé de stratégie

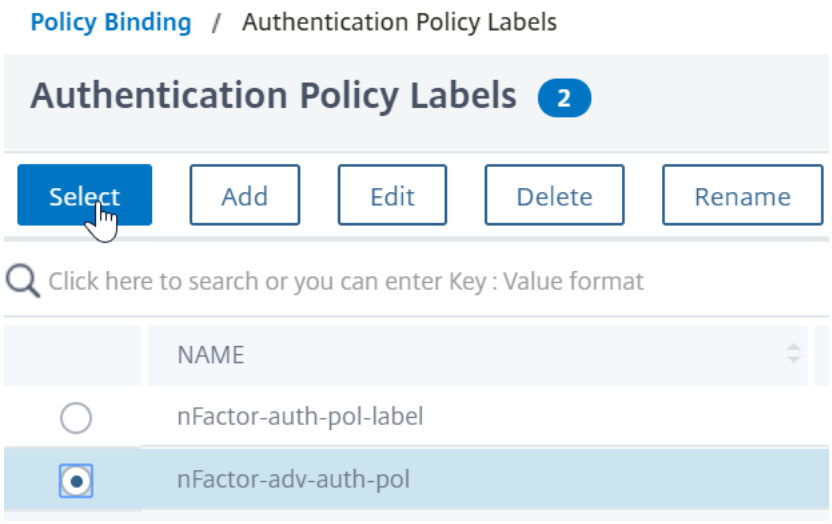
1. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Authentification > Stratégies avancées > Libellé de stratégie**. Sélectionnez un autre libellé de stratégie, puis cliquez sur **Modifier.**



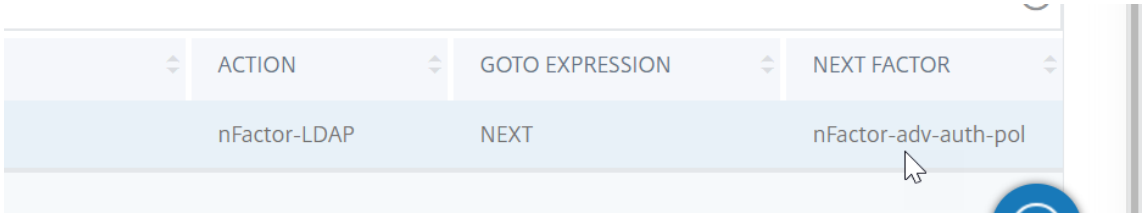
2. Dans **Sélectionner une action**, cliquez sur **Modifier la liaison**.



3. Dans **Détails de la liaison > Sélectionner le facteur suivant**, cliquez sur pour sélectionner le facteur suivant.
4. Choisissez le libellé de stratégie pour le facteur suivant, puis cliquez sur le bouton **Sélectionner** .



5. Cliquez sur **Bind.** Vous pouvez voir le facteur suivant sur la droite.

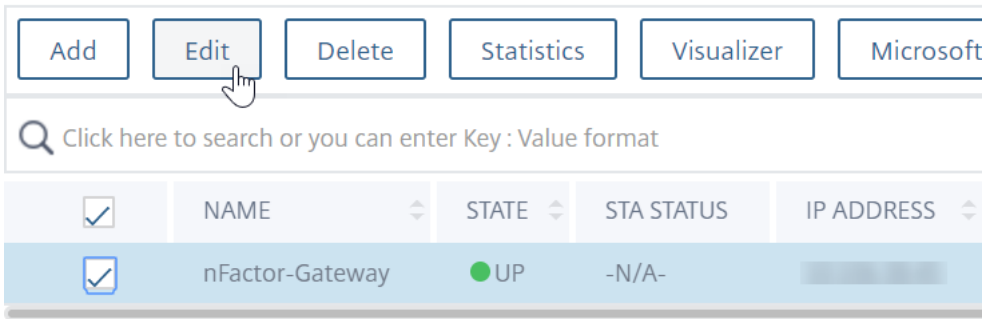


nFactor pour NetScaler Gateway

Pour activer nFactor sur NetScaler Gateway, un profil d'authentification doit être lié à un serveur virtuel d'authentification, d'autorisation et d'audit.

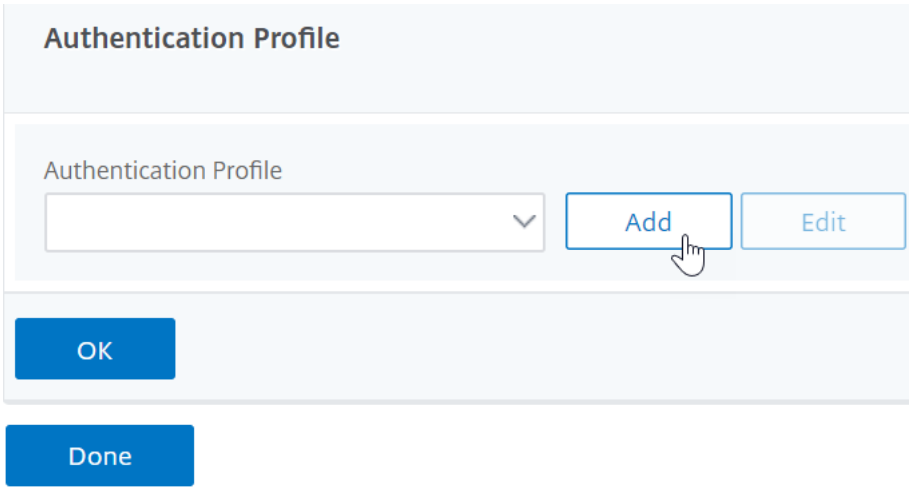
Créez un profil d'authentification pour lier un serveur virtuel d'authentification, d'autorisation et d'audit au serveur virtuel NetScaler Gateway

1. Accédez à **NetScaler Gateway > Serveurs virtuels** et sélectionnez un serveur virtuel de passerelle existant à modifier.

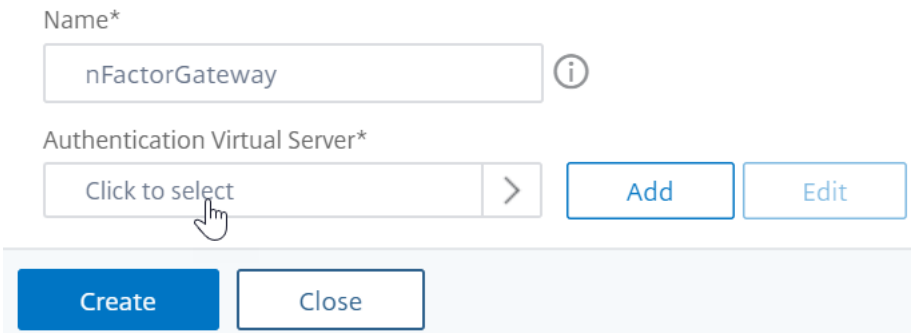


2. Dans **les paramètres avancés**, cliquez sur **Profil d'authentification**.

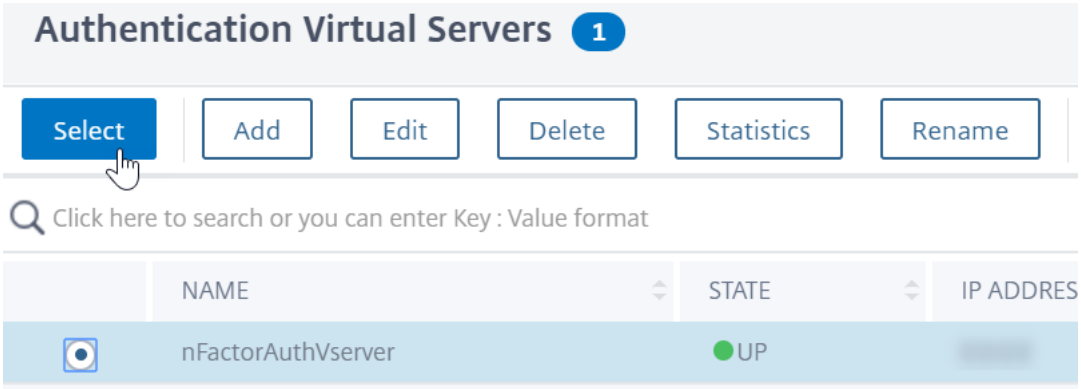
3. Cliquez sur **Ajouter** sous **Profil d'authentification**



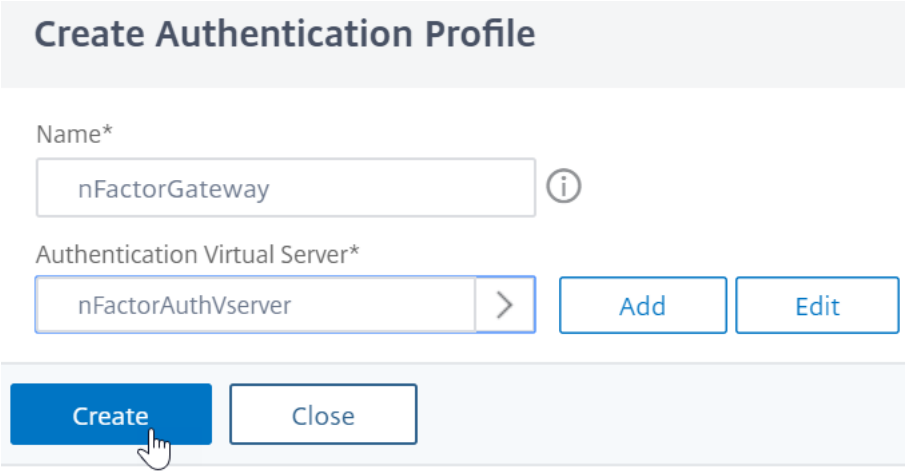
4. Entrez le nom du profil d'authentification et cliquez à l'endroit où il est indiqué **Cliquez pour sélectionner**.



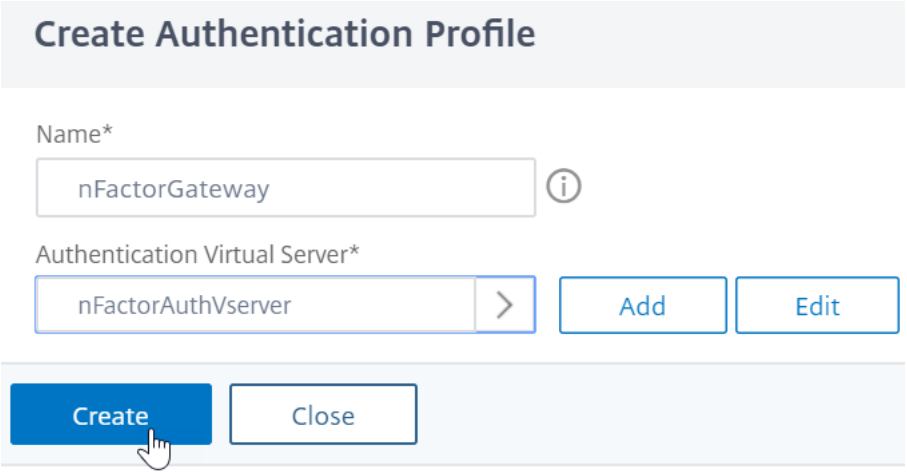
5. Dans **Authentication Virtual Server**, sélectionnez un serveur existant dont le schéma de connexion, la stratégie d'authentification avancée et les étiquettes de stratégie d'authentification sont configurés. Vous pouvez également créer un serveur virtuel d'authentification. Le serveur virtuel d'authentification, d'autorisation et d'audit n'a pas besoin d'adresse IP. Cliquez sur **Sélectionner**.



6. Cliquez sur **Create**.



7. Cliquez sur **OK** pour fermer la section Profil d'authentification.



Remarque : Si vous avez configuré l'un des facteurs en tant que certificats clients, vous devez configurer les paramètres SSL et le certificat CA.

Une fois que vous avez lié le profil d'authentification à un serveur virtuel d'authentification, d'autorisation et d'audit, et lorsque vous accédez à votre NetScaler Gateway, vous pouvez afficher les écrans d'authentification nFactor.

Configuration des paramètres SSL et du certificat d'autorité de certification

Si l'un des facteurs d'authentification est un certificat, vous devez effectuer une configuration SSL sur le serveur virtuel NetScaler Gateway.

1. Accédez à **Gestion du trafic > SSL > Certificats > Certificats d'autorité**de certification, puis installez le certificat racine de l'émetteur des certificats clients. Les certificats d'autorité de certification n'ont pas besoin de fichiers clés.

   Si les profils SSL par défaut sont activés, cela signifie que vous avez déjà créé un profil SSL pour

lequel l'authentification client est activée.

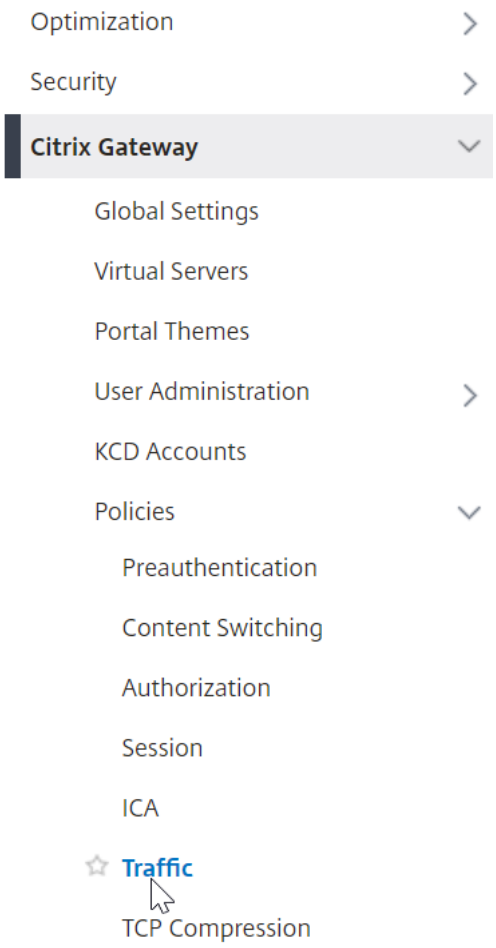
2. Accédez à **NetScaler Gateway > Serveurs virtuels**et modifiez un serveur virtuel NetScaler Gateway existant qui est activé pour nFactor.
    - Si les profils SSL par défaut sont activés, cliquez sur l'icône de modification.
    - Dans la liste Profil SSL, sélectionnez le profil SSL pour lequel l'authentification du client est activée et définie sur FACULTATIF.
    - Si les profils SSL par défaut ne sont pas activés, cliquez sur l'icône de modification.
    - Cochez la case Authentification du client.
    - Assurez-vous que le certificat client est défini sur Facultatif
3. Cliquez sur OK.
4. Dans la section Certificats, cliquez sur **Aucun certificat d'autorité de certification.**
5. Dans Sélectionner un certificat d'autorité de certification, cliquez sur pour sélectionner et sélectionner le certificat racine de l'émetteur des certificats clients.
6. Cliquez sur Bind.

Remarque : Il se peut que vous deviez également lier tous les certificats d'autorité de certification intermédiaires qui ont émis les certificats clients.

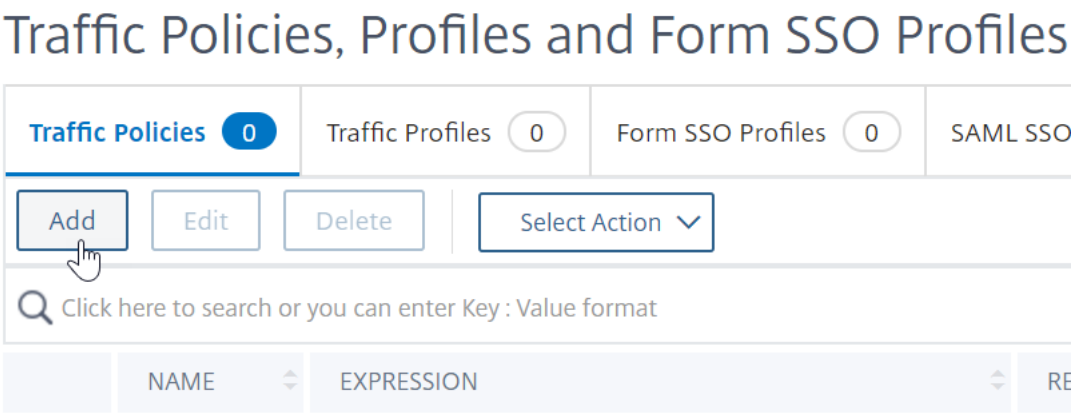
Configurer la stratégie de trafic de NetScaler Gateway pour l'authentification unique de nFactor à StoreFront

Pour l'authentification unique à StoreFront, nFactor utilise par défaut le dernier mot de passe saisi. Si LDAP n'est pas le dernier mot de passe saisi, vous devez créer une stratégie/un profil de trafic pour remplacer le comportement par défaut de NFactor.

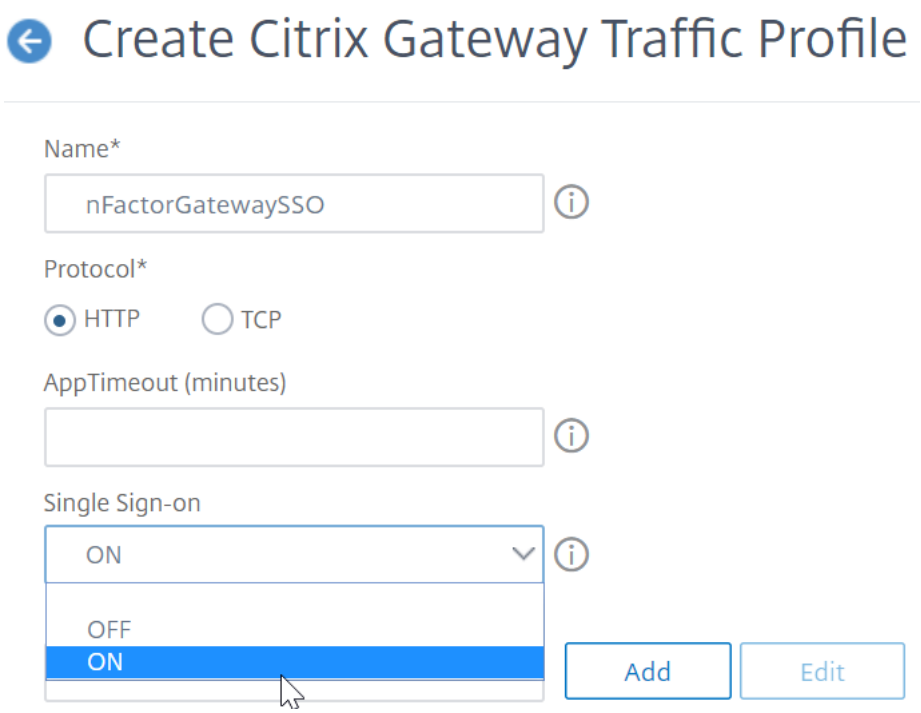
1. Accédez à **NetScaler Gateway > Stratégies > Trafic**.



2. Dans l'onglet **Profils de trafic**, cliquez sur **Ajouter**.

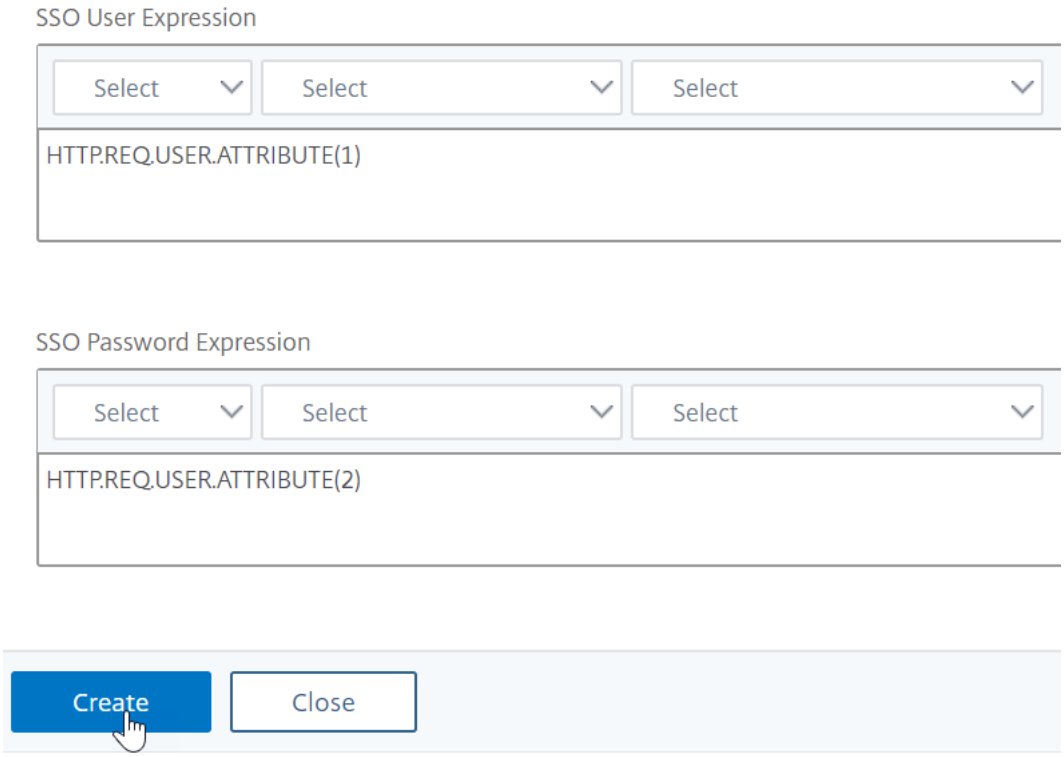


3. Entrez le nom du profil de trafic. Sélectionnez le protocole **HTTP** .
   Dans **Single Sign-on**, sélectionnez **ON**.

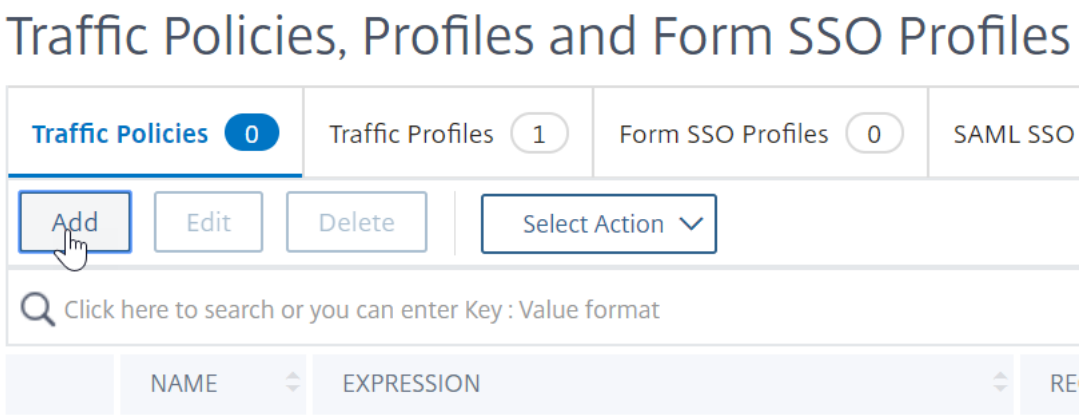


4. Dans l' **expression SSO**, entrez une expression AAA.USER.ATTRIBUTE (#) qui correspond aux index spécifiés dans le schéma de connexion, puis cliquez sur **Créer**.

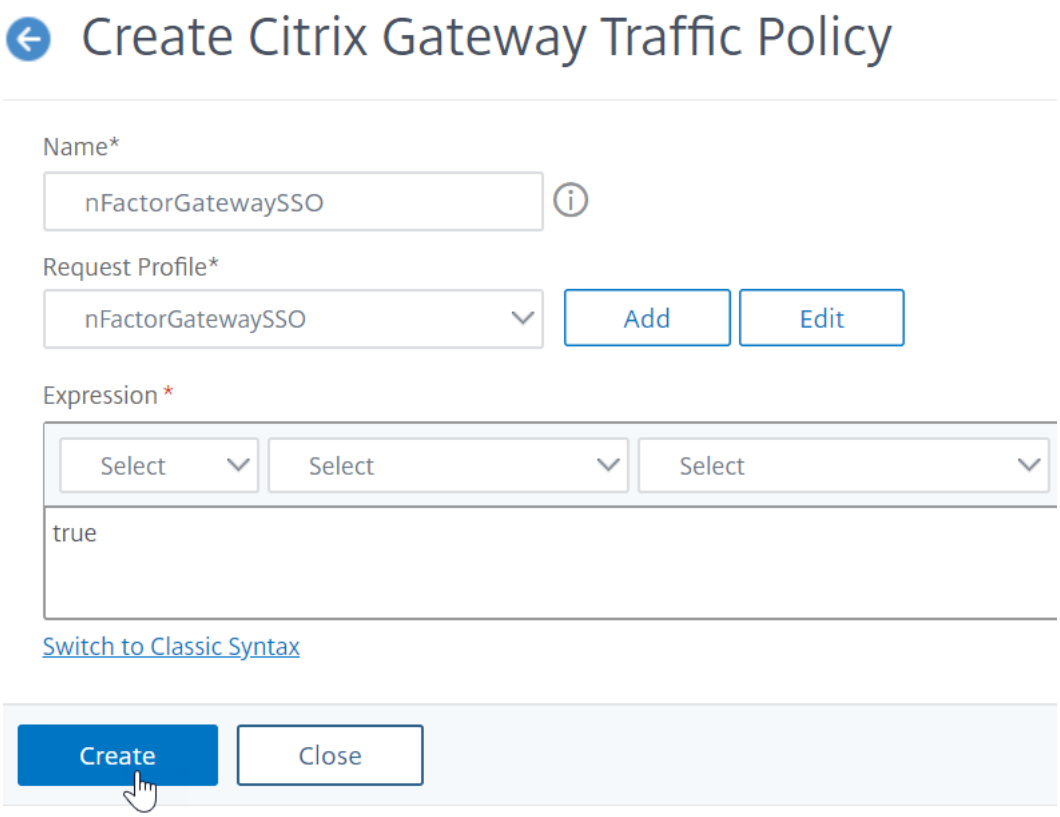
> **Remarque :**
> L'expression AAA.USER est maintenant implémentée pour remplacer les expressions HTTP.REQ.USER obsolètes.



5. Cliquez sur **l'onglet Stratégies de trafic**, puis sur **Ajouter**.



6. Entrez un nom pour la stratégie. Sélectionnez le profil de trafic créé à l'étape précédente. Dans **Expression**, entrez une expression avancée, puis cliquez sur **Créer**.



7. Accédez à **NetScaler Gateway > Serveur virtuel NetScaler**Gateway.
   - Sélectionnez un serveur virtuel existant et cliquez sur **Modifier**.
   - Dans la section **Stratégies**, cliquez sur le signe **+** .
   - Dans **Choisir une stratégie**, sélectionnez **Trafic**.
   - Dans **Choisir le type**, sélectionnez **Demande**.
   - Sélectionnez la stratégie de trafic que vous avez créée, puis cliquez sur **Liaison**.

Exemple d'extrait de code sur la configuration de nFactor à l'aide de l'interface de ligne de commande

Pour comprendre les configurations pas à pas de l'authentification nFactor, considérons un déploiement d'authentification à deux facteurs dans lequel le premier facteur est l'authentification LDAP et le second est l'authentification RADIUS.

Cet exemple de déploiement nécessite que l'utilisateur se connecte aux deux facteurs à l'aide d'un seul formulaire de connexion. Par conséquent, nous définissons un formulaire de connexion unique qui accepte deux mots de passe. Le premier mot de passe est utilisé pour l'authentification LDAP et l'autre pour l'authentification RADIUS.
Voici les configurations qui sont effectuées :

1. Configurer le serveur virtuel d'équilibrage de charge pour l'authentification

ajouter lb vserver lbvs89 HTTP 1.136.19.55 80 -AuthenticationHost auth56.aaatm.com -Authentication ON

2. Configurez le serveur virtuel d'authentification.

   ajouter authentification vserver auth56 SSL 10.106.30.223 443 - AuthenticationDomain aaatm.com

3. Configurez le schéma de connexion pour le formulaire de connexion et liez-le à une stratégie de schéma de connexion.

   add authentication loginSchema login1 -authenticationSchema login-2passwd.xml -userCredentialIndex 1 -passwordCredentialIndex 2

   Remarque :

   Utilisez le nom d'utilisateur et l'un des mots de passe saisis dans le schéma de connexion pour l'authentification unique (SSO) à un service principal, par exemple StoreFront. Vous pouvez référencer ces valeurs d'index dans l'action de trafic en utilisant l'expression AAA.USER.ATTRIBUTE (#). Les valeurs peuvent être comprises entre 1 et 16.

   Vous pouvez également utiliser les informations d'identification saisies dans le schéma de connexion comme informations d'identification Single Sign-On à l'aide de la commande suivante.

```
1 add authentication loginSchema login1 -authenticationSchema login
     -2passwd.xml -SSOCredentials YES
2
3  add authentication loginSchemaPolicy login1 -rule true -action
      login1
4 <!--NeedCopy-->
```

4. Configurez un schéma de connexion pour le relais et liez-le à une étiquette de stratégie

```
1 add authentication loginSchema login2 -authenticationSchema
     noschema
2
3 add authentication policylabel label1 -loginSchema login2
4 <!--NeedCopy-->
```

5. Configurez les stratégies LDAP et RADIUS.

```
1 add authentication ldapAction ldapAct1 -serverIP 10.17.103.28 -
     ldapBase "dc=aaatm, dc=com" -ldapBindDn administrator@aaatm.com
      -ldapBindDnPassword 81
     qw1b99ui971mn1289op1abc12542389b1f6c111n0d98e1d78ae90c8545901 -
     encrypted -encryptmethod ENCMTHD_3 -ldapLoginName
     samAccountName -groupAttrName memberOf -subAttributeName CN
2
```



```
add authentication Policy ldap -rule true -action ldapAct1

add authentication radiusAction radius -serverIP 10.101.14.3 -
    radKey
    n231d9a8cao8671or4a9ace940d8623babca0f092gfv4n5598ngc40b18876hj32
     -encrypted -encryptmethod ENCMTHD_3 -radNASip ENABLED -
    radNASid NS28.50 -radAttributeType 11 -ipAttributeType 8

add authentication Policy radius -rule true -action radius
<!--NeedCopy-->
```

6. Liez la stratégie de schéma de connexion au serveur virtuel d'authentification

```
bind authentication vserver auth56 -policy login1 -priority 1 -
    gotoPriorityExpression END
<!--NeedCopy-->
```

7. Liez la stratégie LDAP (premier facteur) au serveur virtuel d'authentification.

```
bind authentication vserver auth56 -policy ldap -priority 1 -
    nextFactor label1 -gotoPriorityExpression next
<!--NeedCopy-->
```

8. Liez la stratégie RADIUS (deuxième facteur) à l'étiquette de stratégie d'authentification.

```
bind authentication policylabel label1 -policyName radius -
    priority 2 -gotoPriorityExpression end
<!--NeedCopy-->
```

Visualizer nFactor pour une configuration simplifiée

May 5, 2023

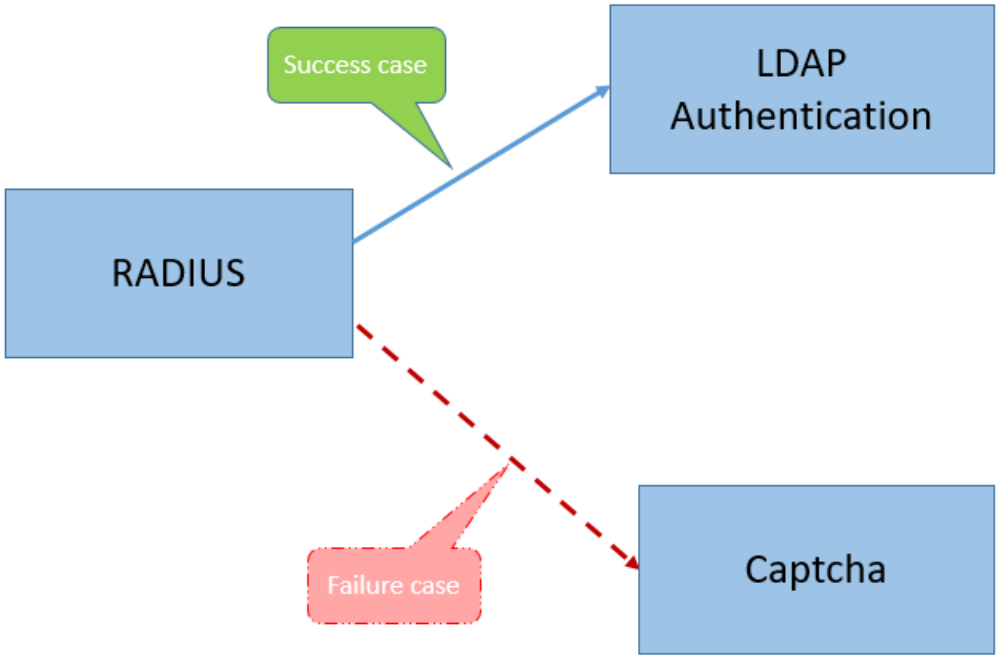
À partir de la version 13.0 de NetScaler build 36.27, la configuration de nFactor via l'interface graphique est simplifiée à l'aide du visualiseur nFactor. Le visualiseur nFactor aide les administrateurs à ajouter plusieurs facteurs sans perdre de vue chaque facteur. Le groupe de facteurs intégrés au flux est affiché au même endroit. Les administrateurs peuvent ajouter séparément les chemins de réussite et d'échec de l'authentification. Après avoir créé le flux, les administrateurs doivent lier le flux nFactor à un serveur virtuel d'authentification.

> **Remarque**
>
> - Tous les facteurs créés par un administrateur dans le flux nFactor sont conservés pour toute utilisation future.
> - À partir de la version 13.0 build 64.35 et ultérieure de la fonctionnalité NetScaler, vous pouvez démarrer le flux nFactor avec un bloc de décision à l'aide du visualiseur nFactor.

Auparavant, la configuration de nFactor était fastidieuse et les administrateurs devaient visiter de nombreuses pages pour la configurer. Si une modification était requise, les administrateurs devaient à chaque fois revoir les sections configurées. De plus, il n'était pas possible d'afficher la configuration complète en un seul endroit.

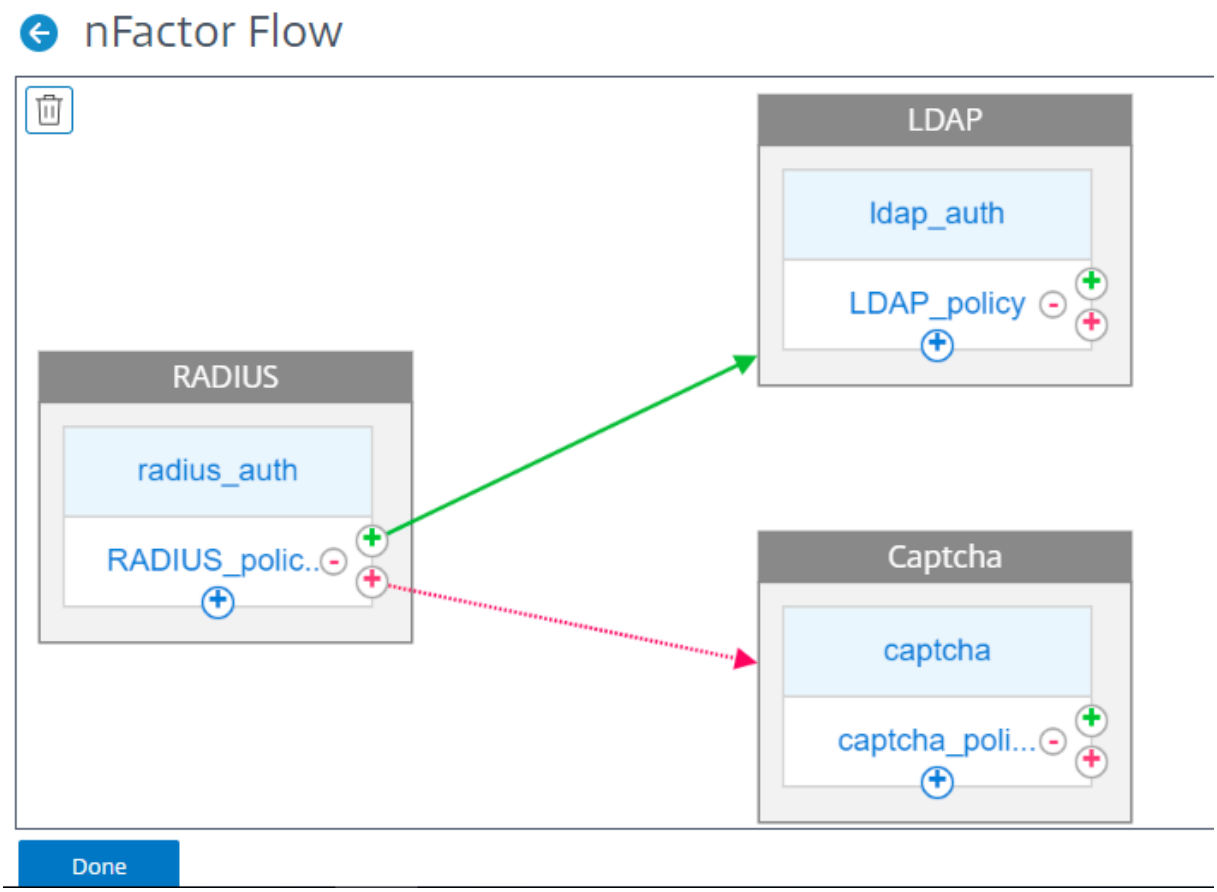
Cas d'utilisation 1 : RADIUS suivi d'une authentification LDAP, sinon retour au Captcha via nFactor Visualizer

Réalisez l'authentification RADIUS en tant qu'authentification de premier niveau, suivie de l'authentification LDAP. En cas d'échec de RADIUS, l'authentification doit revenir au Captcha.



Pour réaliser ce cas d'utilisation, vous pouvez utiliser le visualiseur nFactor. Le visualiseur fournit diverses commandes qui peuvent être utilisées pour ajouter ce flux et les éléments associés.

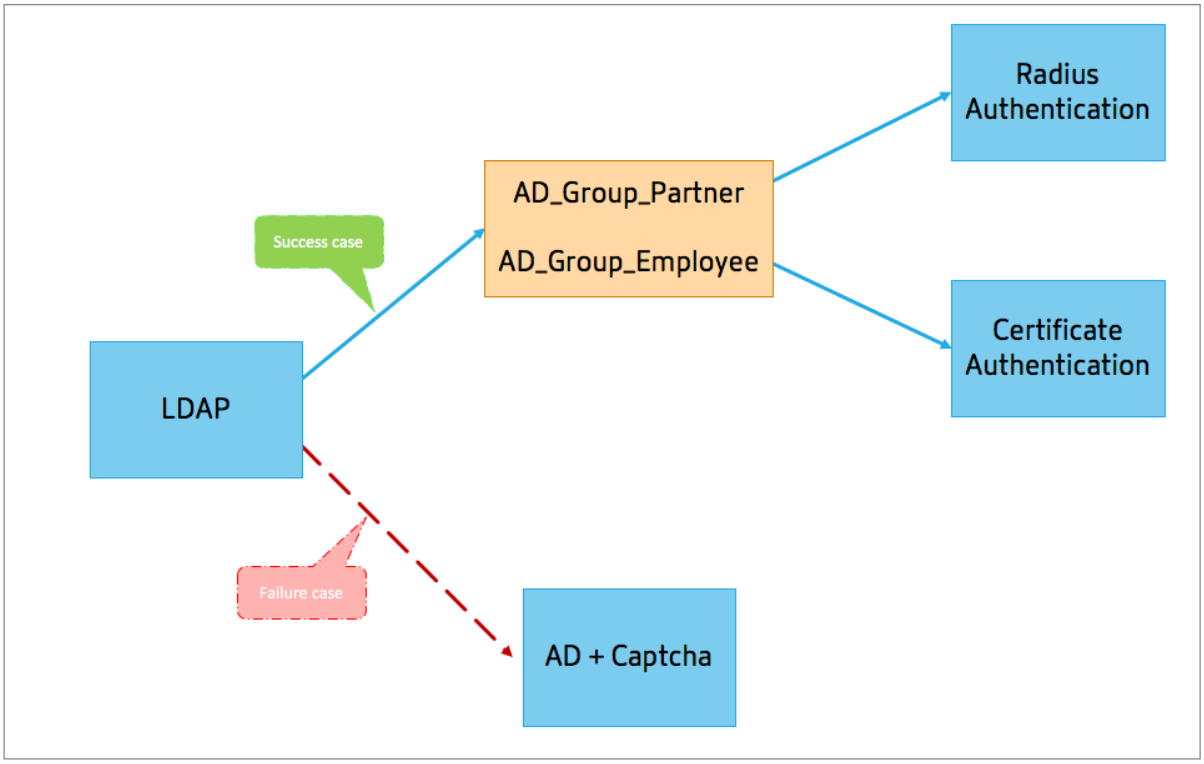
La figure suivante montre le flux nFactor créé pour le cas d'utilisation mentionné précédemment à l'aide du visualiseur.



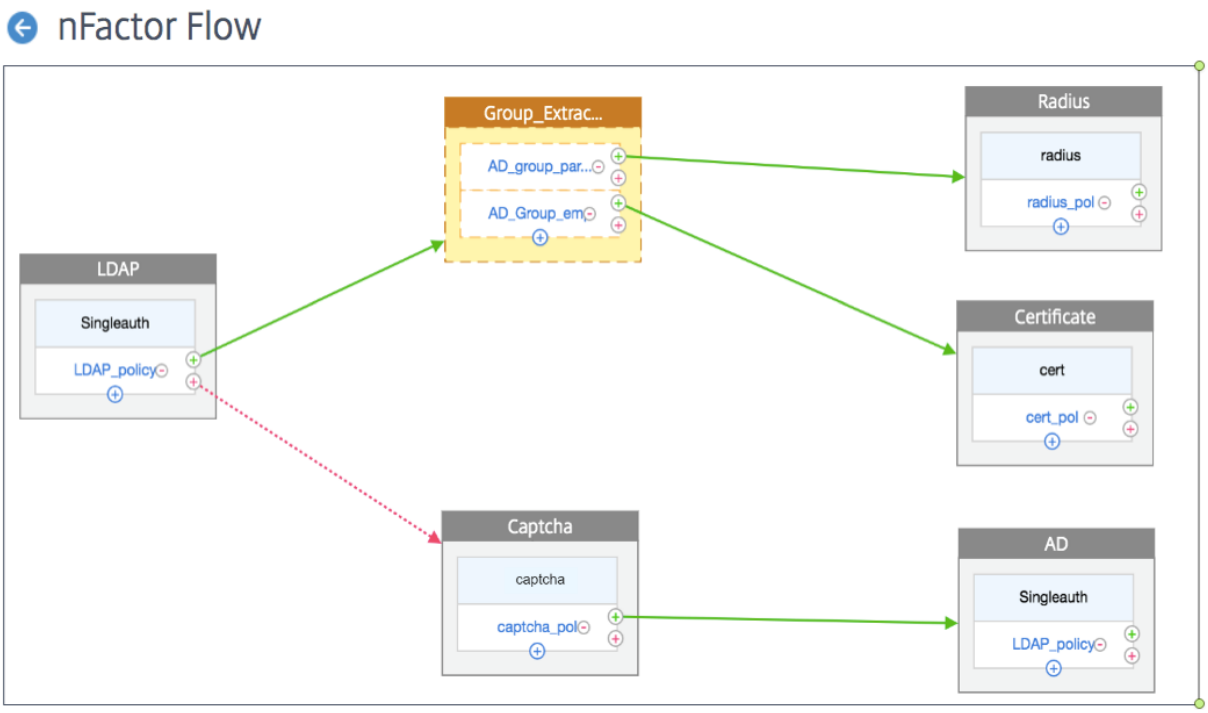
- **RAYON.** Vous configurez RADIUS comme premier facteur. Vous ajoutez un schéma de connexion et une politique. Dans cet exemple, radius_auth et RADIUS_policy sont le schéma de connexion et la politique ajoutés. Pour le RADIUS_Policy, vous pouvez ajouter un autre facteur de réussite. Dans cet exemple, un bloc de facteurs LDAP est ajouté en cas de réussite. Pour le cas d'échec, vous pouvez ajouter un facteur Captcha.
- **LDAP.** Vous configurez l'authentification LDAP comme deuxième facteur. Vous ajoutez un schéma de connexion et une politique. Dans cet exemple, ldap_auth et LDAP_Policy sont le schéma de connexion et la politique ajoutés.
- **Captcha.** Pour le cas d'échec de la politique RADIUS, vous créez un facteur Captcha. Dans cet exemple, captcha et captcha_policy sont le schéma de connexion et la politique ajoutés.

Cas d'utilisation 2 : LDAP suivi d'une authentification RADIUS/certificat avec Captcha basée sur l'appartenance à un groupe LDAP via nFactor Visualizer

Réalisez l'authentification RADIUS en tant qu'authentification de premier niveau, suivie de l'authentification LDAP. En cas d'échec de RADIUS, l'authentification doit revenir au Captcha.



La figure suivante montre le flux nFactor créé pour le cas d'utilisation mentionné précédemment à l'aide du visualiseur.



- **LDAP.** Vous configurez LDAP comme premier facteur. Vous ajoutez un schéma de connexion et une politique. Dans cet exemple, SingleAuth et LDAP_Policy sont le schéma de connexion et la

politique ajoutés. Pour le LDAP_Policy, vous pouvez ajouter un autre facteur de réussite. Dans cet exemple, un bloc de décision est ajouté pour le cas de réussite. En cas d'échec, vous pouvez ajouter un Captcha suivi du facteur AD.

- **Extraction de groupes LDAP.** Le bloc de décision est-il ajouté pour le cas de réussite du protocole LDAP ? Le bloc de décision est utilisé comme facteur de dérivation pour diversifier les utilisateurs en fonction des règles de politique. Le visualiseur permet de configurer uniquement une politique NO_AUTHN pour le bloc de décision.

  Dans cet exemple, Group_Extraction_LDAP est le bloc de décision. Vous ajoutez deux politiques (`AD_Group_Partner and AD_Group_Employee`) à ce bloc de décision. Comme expliqué dans les cas d'utilisation, toutes les demandes acheminées via la politique AD_Group_Partner utilisent l'authentification RADIUS. Par conséquent, vous associez le cas de réussite de cette politique au facteur suivant, à savoir le facteur RADIUS. De même, toutes les demandes acheminées via la politique AD_Group_Employee utilisent l'authentification par certification. Par conséquent, vous associez le cas de réussite de cette politique au facteur suivant, à savoir le facteur d'authentification de la certification.

  - **RAYON.** Pour garantir la réussite de la politique AD_Group_Partner, vous devez créer le facteur d'authentification RADIUS.
  - **Certificat.** Pour le cas de réussite de la politique AD_Group_Employee, vous créez le facteur d'authentification du certificat.

- **Captcha.** Pour le cas d'échec de la politique LDAP, vous devez créer deux facteurs suivants, Captcha et AD factor.

> **Remarque**
>
> - Si vous avez un cas d'utilisation dans lequel vous souhaitez commencer par vous diversifier, vous pouvez soit créer deux flux et les lier séparément, soit créer un flux avec le premier en tant que branche, et le lier au serveur virtuel.
> - Si vous avez plusieurs blocs, et pour afficher l'intégralité du flux sur l'écran nFactor Flow, cliquez sur le visualiseur et faites glisser le flux vers l'extrême gauche.
> - Citrix recommande de modifier les flux nFactor à l'aide de la page nFactor Flows uniquement.

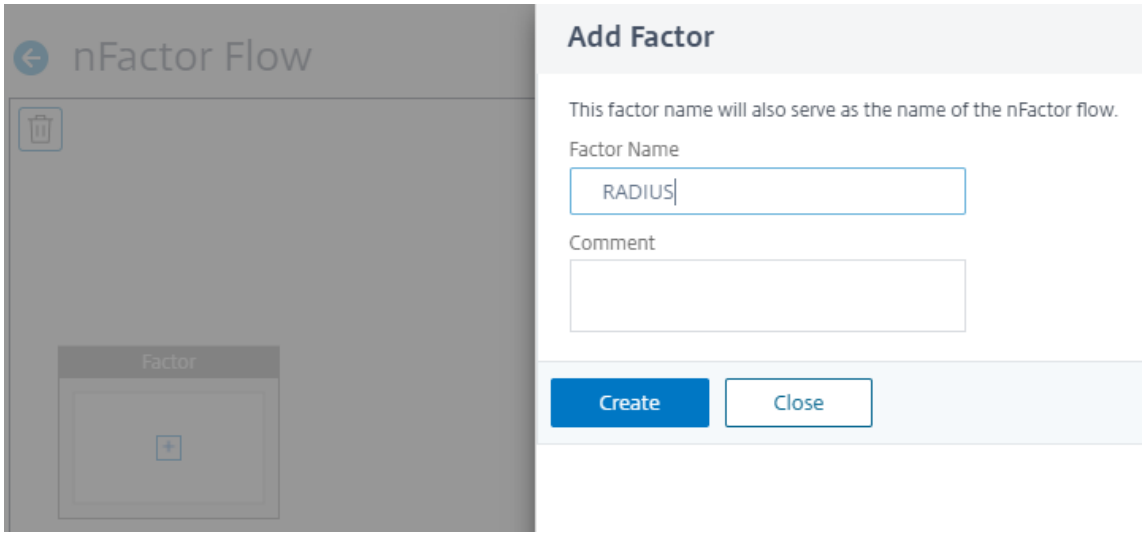
Pour configurer nFactor à l'aide du visualiseur nFactor

> **Remarque**
>
> La configuration nFactor suivante est un exemple simple qui vous aide à réaliser les configurations du scénario d'utilisation 1.

1. Accédez à **Sécurité > AAA — Trafic d'applications > Visualiseur nFactor > NFactor Flows**.
2. Cliquez sur **Ajouter**.

3. Sur la page **nFactor Flows**, cliquez sur **+** pour ajouter un premier facteur au flux. Le premier facteur sert également d'identifiant pour ce flux nFactor.

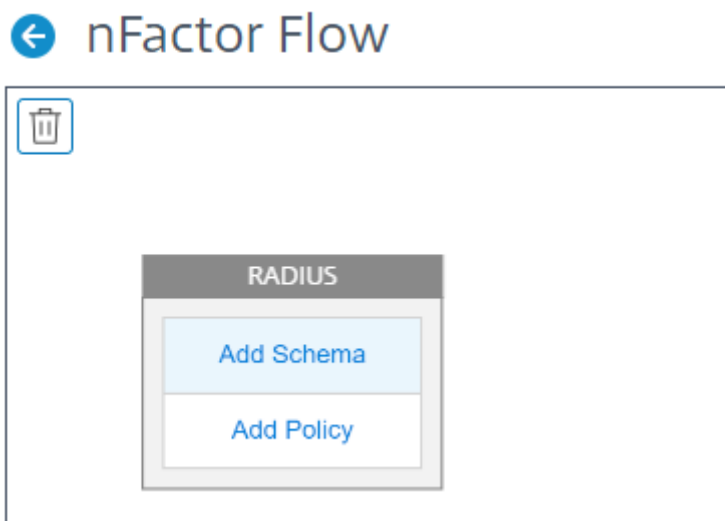
4. Entrez le nom du facteur et cliquez sur **Créer**.



Le nom du facteur apparaît sur le bloc de facteurs de la page nFactor Flow.

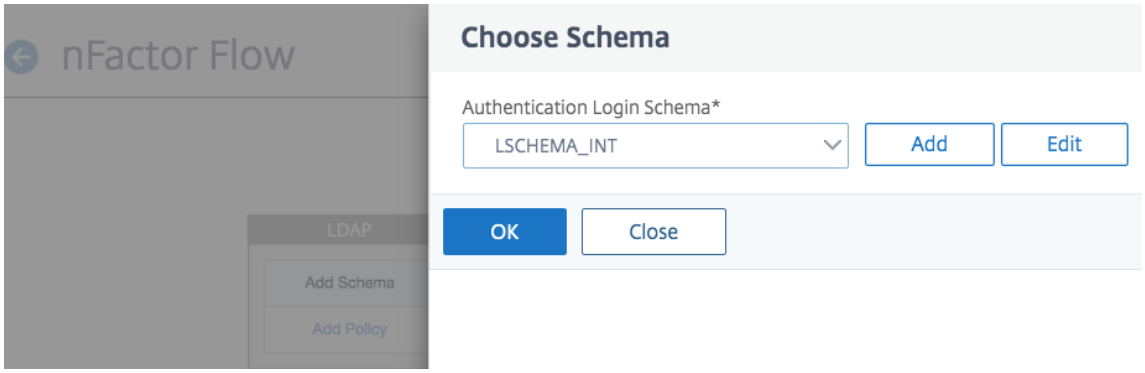
> **Remarque**
>
> Citrix recommande de ne pas utiliser de noms d'étiquettes de politique tels que, `__root` et `__<flow_name>` comme suffixe et `_db_` comme préfixe. Il est utilisé comme nom de facteur créé dans le flux nFactor.

5. Une fois le facteur RADIUS créé, les options Ajouter un schéma et Ajouter une politique doivent être créées.

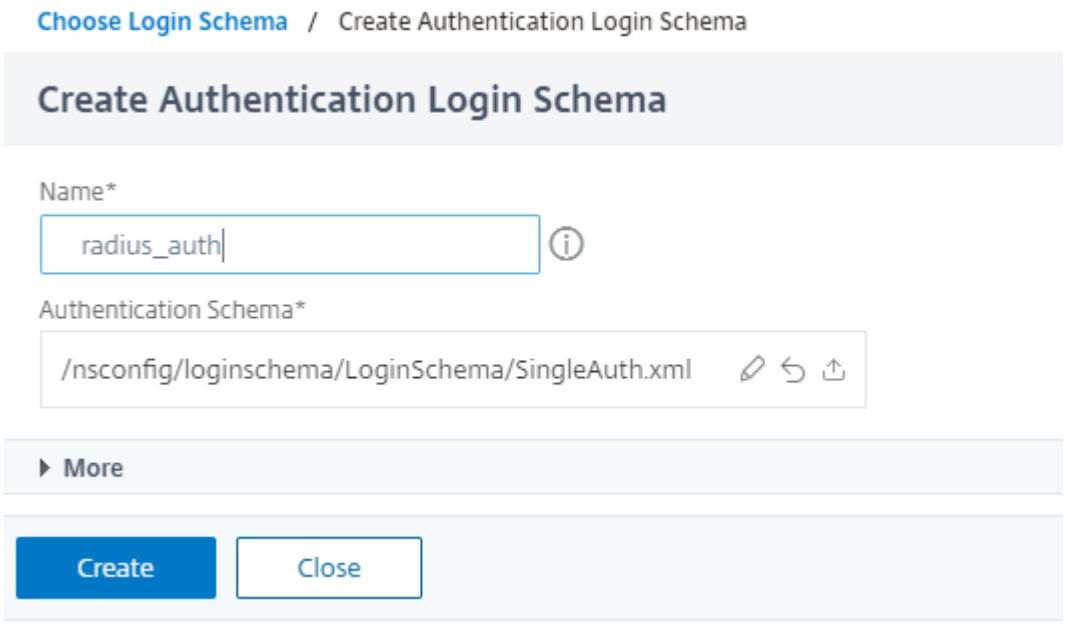


> **Remarque**
>
> Pour plus d'informations, consultez la section Concepts, entités et terminologie nFactor.

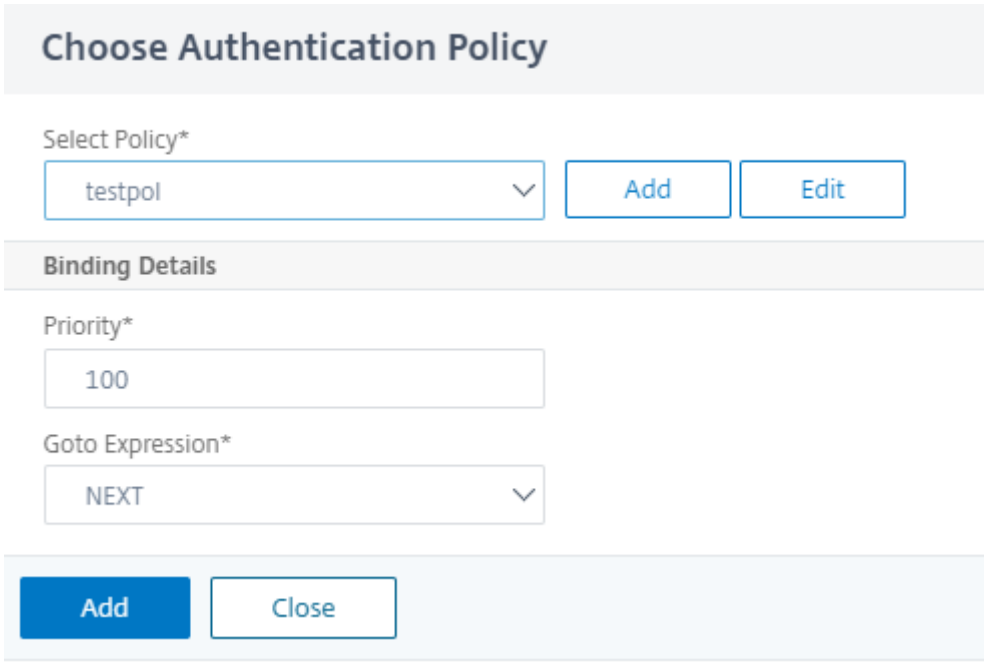
6. Cliquez sur **Ajouter un schéma**. Vous pouvez soit ajouter un nouveau schéma de connexion, soit sélectionner un schéma de connexion existant dans la liste **Schéma de connexion d'authentification** .



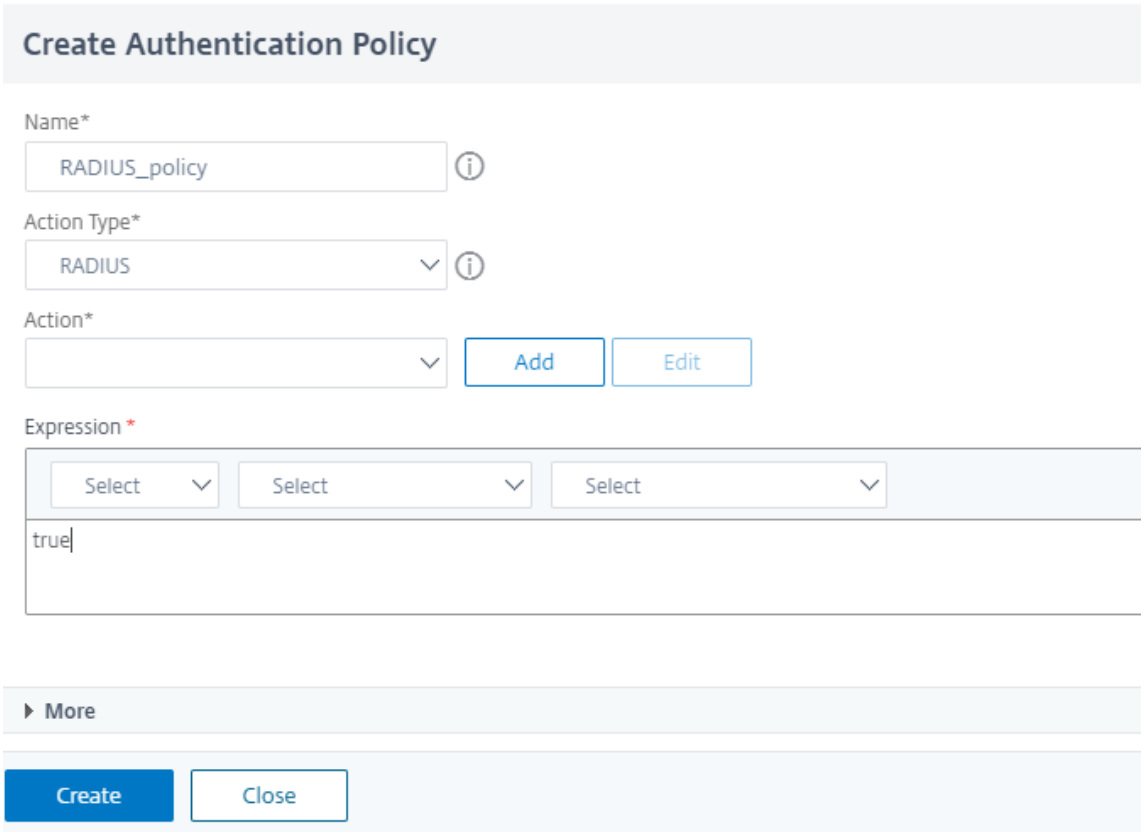
7. Pour créer un schéma de connexion, cliquez sur **Ajouter** et sur la page **Créer un schéma de connexion d'authentification**, entrez le nom du schéma. Cliquez sur **Modifier** (icône en forme de crayon) pour sélectionner les **fichiers du schéma de connexion** dans la liste.



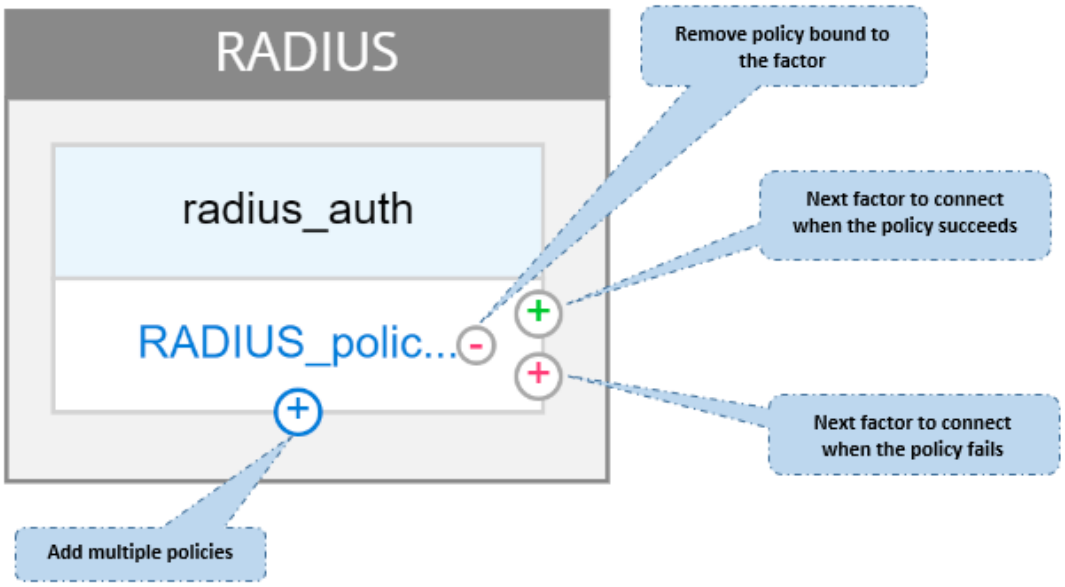
8. Cliquez sur **Ajouter une politique**. Vous pouvez créer une politique d'authentification ou sélectionner une politique d'authentification existante.



9. Pour créer une nouvelle politique, cliquez sur **Ajouter** et sur la page **Créer une politique d'authentification**, entrez le nom de la politique et cliquez sur **Créer**.



10. Une fois que vous avez ajouté un schéma et une politique de connexion au facteur, le schéma et la politique de connexion apparaissent sur le facteur dans le visualiseur, comme illustré dans la figure suivante. Pour un facteur donné, vous pouvez ajouter plusieurs stratégies et définir le facteur suivant pour le succès et l'échec de chaque stratégie. Vous pouvez également supprimer les politiques qui font partie du facteur.



11. Après avoir créé le flux, vous pouvez lier le flux nFactor à un serveur virtuel d'authentification.

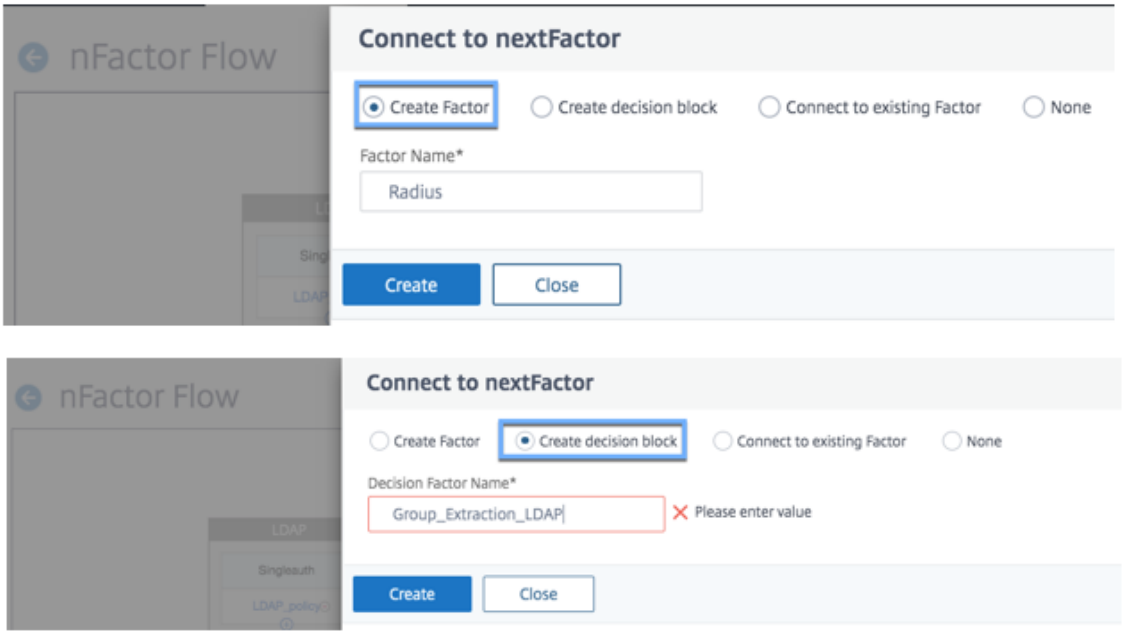
Ajouter le facteur suivant

Pour ajouter le facteur suivant, vous pouvez sélectionner l'une des options suivantes selon vos besoins :

- **Créez un facteur**. Créez un facteur. Chaque facteur créé dans un flux est exclusif à ce flux.
- **Créez un bloc de décision.** Créez un bloc de décision qui servira de facteur de diversification. Vous ne pouvez pas ajouter de schéma de connexion au bloc de décision. Le visualiseur permet de configurer uniquement une politique NO_AUTHN pour le bloc de décision.

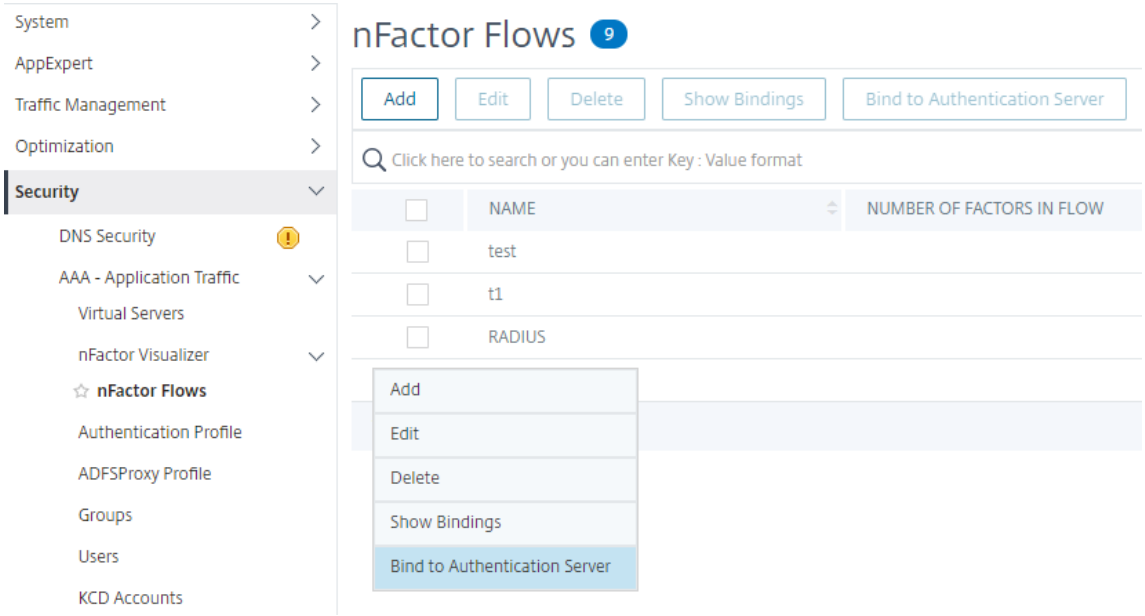
  > **Remarque**
  >
  > Vous pouvez uniquement ajouter ou modifier le bloc de décision via l'interface graphique de NetScaler. Il n'existe aucune option permettant de configurer le bloc de décision à partir de la commande CLI.

- **Connectez-vous à un Factor existant**. Sélectionnez un facteur existant comme facteur suivant. Tous les facteurs qui apparaissent dans la liste existante sont créés exclusivement pour ce flux.
- **None.** Supprimez une connexion existante.



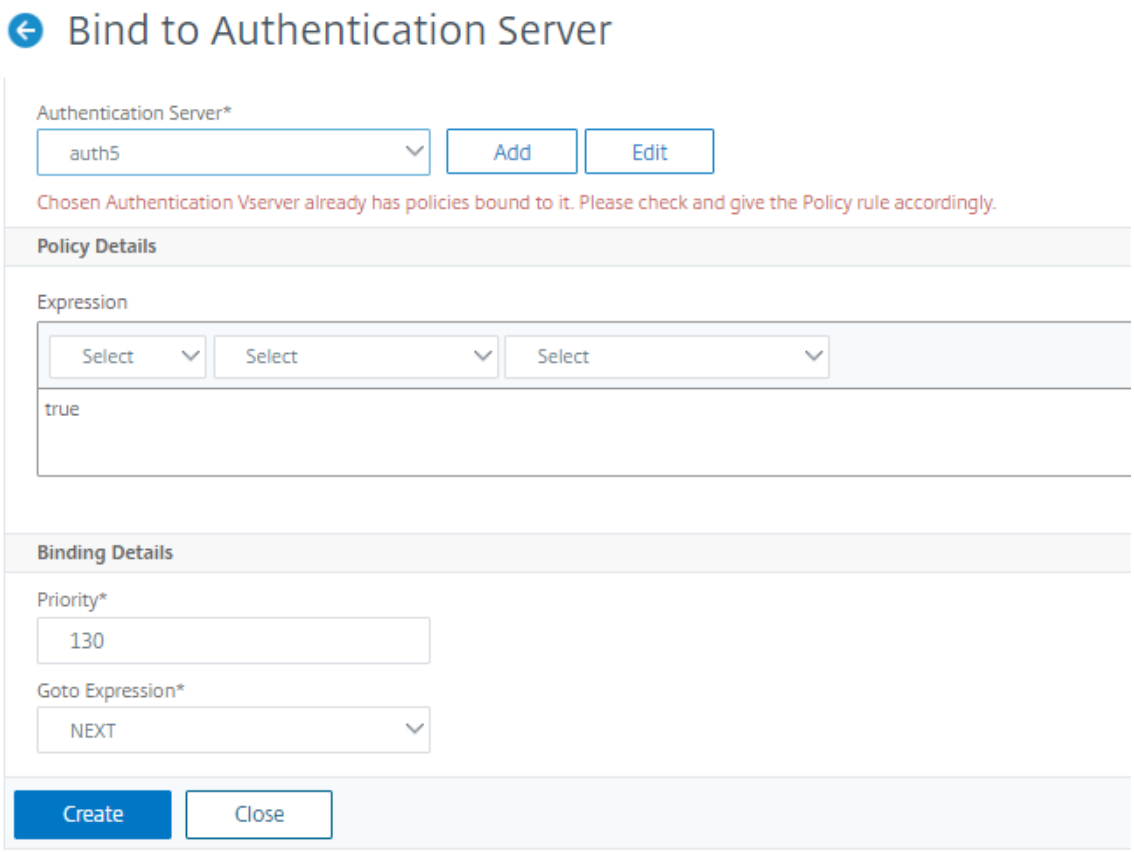
Pour lier le flux nFactor au serveur d'authentification

1. Sur la page **nFactor Flows**, sélectionnez un flux nFactor que vous préférez lier à un serveur virtuel d'authentification.
2. Cliquez sur l'icône en forme de hamburger pour sélectionner l'option **Lier au serveur d'authentification** ou, dans le volet de détails, cliquez sur **Lier au serveur d'authentification**.

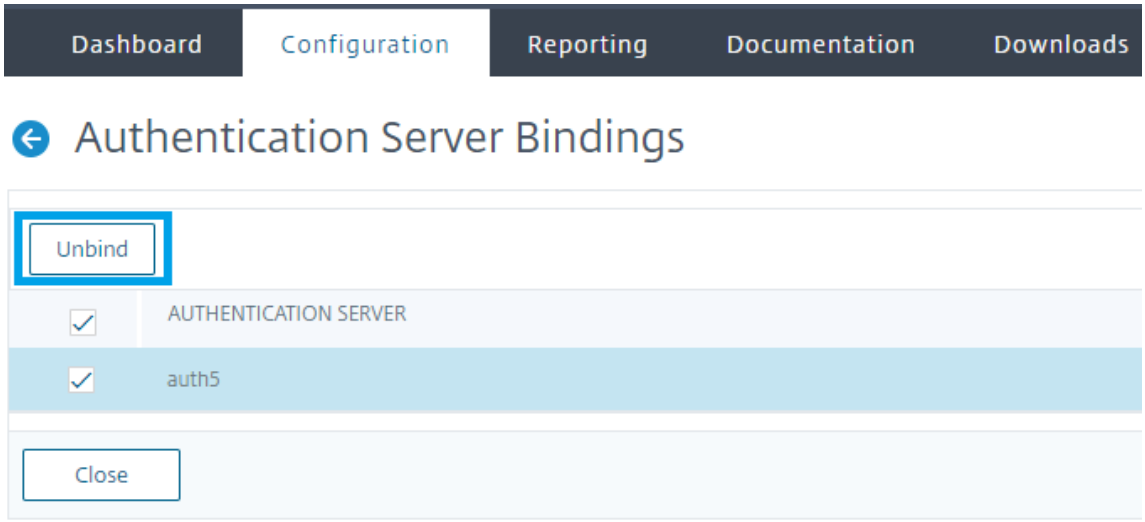


3. Sur la **page Lier au serveur d'authentification**, vous pouvez effectuer les actions suivantes :
   - Pour ajouter un **serveur virtuel d'authentification**, cliquez sur **Ajouter**.

- Pour sélectionner un serveur d'authentification existant dans la liste, cliquez sur le champ **Serveur d'authentification** .



4. Cliquez sur **Afficher les liaisons** à partir de l'icône du hamburger pour afficher les liaisons.
5. Pour dissocier le serveur d'authentification du flux nFactor spécifique, effectuez les opérations suivantes :
   - Sur la page **NFactor Flows**, cliquez sur **Afficher les liaisons** à partir de l'icône Hamburger.
   - **Sur la page**Liaisons du serveur d'authentification**, sélectionnez le serveur d'authentification à dissocier et cliquez sur Dissocier.** Cliquez sur **Fermer**.



Pour plus d'informations sur l'authentification nFactor, consultez les rubriques suivantes :

- Concept : Authentification multi-facteurs (nFactor).
- Workflow : Fonctionnement de l'authentification NFactor.
- Configuration : configuration de l'authentification NFactor.

Améliorations apportées au visualiseur nFactor

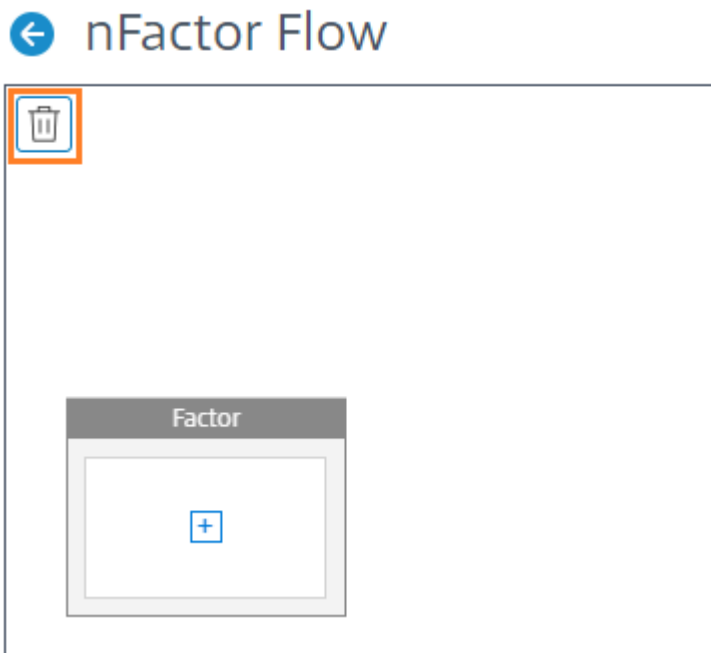
À partir de la version 13.0 de NetScaler build 41.20, les améliorations suivantes sont apportées au visualiseur nFactor.

- Les administrateurs peuvent déplacer les facteurs créés vers l'icône de la corbeille.
- Affichez les flux nFactor sur la page du serveur virtuel d'authentification.

Icône de la corbeille Les administrateurs peuvent uniquement supprimer les nœuds qui n'ont aucune connexion. Toutefois, les politiques sous-jacentes ou les schémas créés pour le facteur ne sont pas supprimés si le facteur est placé dans la corbeille.

Pour afficher l'icône de la corbeille,

1. Accédez à **Sécurité > AAA — Trafic d'applications > Visualiseur nFactor > NFactor Flows**.

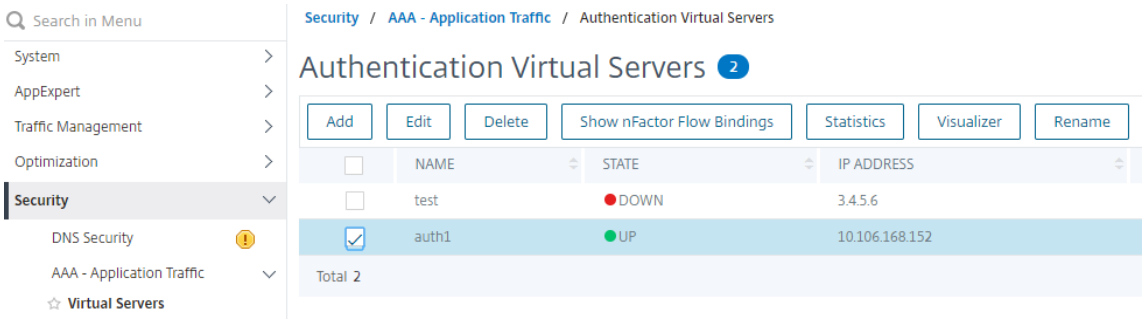


2. Pour supprimer le facteur, cliquez sur le bloc de facteurs et faites-le glisser vers la corbeille.

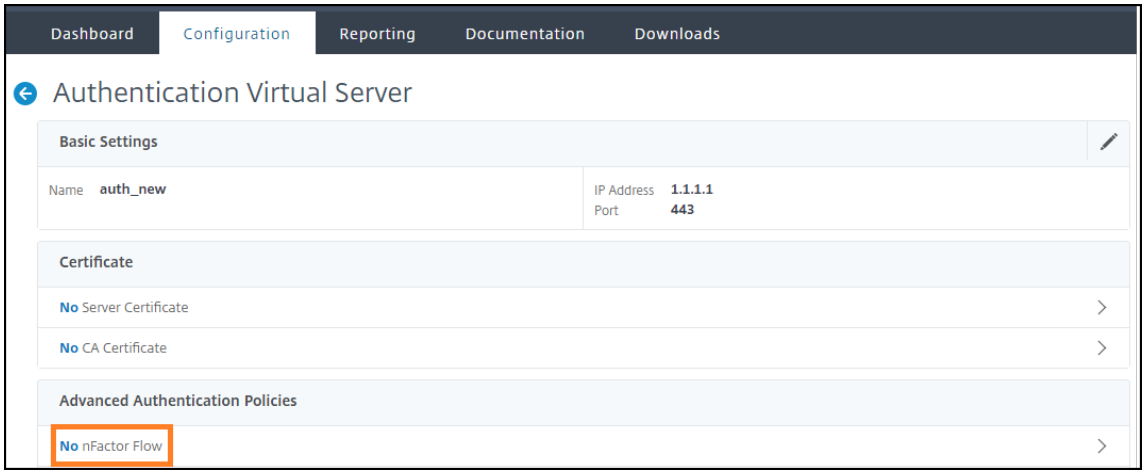
Affichez le flux nFactor depuis le serveur virtuel d'authentification. Les administrateurs peuvent également consulter les flux nFactor créés à partir de la page Serveur virtuel d'authentification.

Pour afficher le flux nFactor depuis la page Authentication Virtual Server,

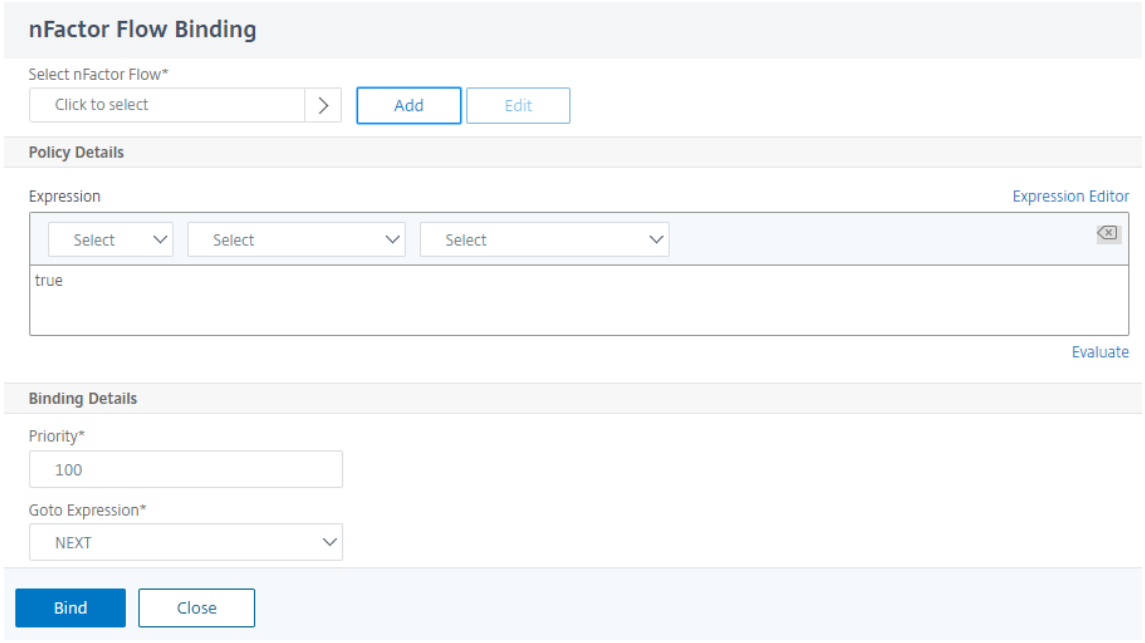
1. Accédez à **Sécurité > AAA — Trafic d'applications > Serveurs virtuels**. Sur la page **Serveurs virtuels d'authentification**, vous pouvez effectuer les étapes suivantes :
   - Pour ajouter un serveur virtuel d'authentification, cliquez sur **Ajouter**.
   - Pour modifier un serveur virtuel d'authentification existant, cliquez sur l'option **Modifier** dans le volet de détails.



2. Sur la page **Serveur virtuel d'authentification**, vous pouvez afficher l'option **nFactor Flow** sous **Politiques d'authentification avancées**.



3. Si aucun flux nFactor n'est lié au serveur virtuel, vous pouvez cliquer sur l'option **Aucun flux nFactor** dans la section **Politiques d'authentification avancées** pour ajouter un nouveau flux nFactor ou sélectionner le flux nFactor existant dans la liste.



Extensibilité nFactor

May 5, 2023

Le cadre d'authentification nFactor offre la flexibilité d'ajouter des personnalisations pour rendre l'interface d'ouverture de session plus intuitive pour une expérience utilisateur enrichie. Vous pouvez ajouter des étiquettes de connexion personnalisées, des informations d'identification de connexion personnalisées, la personnalisation de l'affichage de l'interface utilisateur, etc.

Avec nFactor, chaque facteur peut avoir son propre écran d'ouverture de session. Dans chaque écran d'ouverture de session, vous pouvez présenter toutes les informations provenant de l'un des facteurs précédents ou d'autres informations invisibles dans d'autres facteurs. Par exemple, votre dernier facteur peut être une page informative où l'utilisateur lit les instructions et clique sur Continuer.

Avant nFactor, les pages de connexion personnalisées étaient limitées et les personnalisations et nécessitaient une assistance. Il était possible de remplacer le fichier tmindex.html ou d'appliquer des règles de réécriture pour modifier certains de ses comportements. Cependant, il n'a pas été possible d'obtenir la fonctionnalité sous-jacente.

Les personnalisations liées à nFactor suivantes sont capturées en détail dans cette rubrique.

- Personnaliser les étiquettes de connexion
- Personnaliser l'interface utilisateur pour afficher les images
- Personnaliser le formulaire de connexion à NetScaler nFactor

Les hypothèses

Vous connaissez bien nFactor, les commandes Shell, XML et les éditeurs de texte.

Composants requis

- La personnalisation décrite dans cette rubrique n'est possible que lorsque le thème de l'interface utilisateur RFWeb (ou basé sur un thème) est configuré sur NetScaler.
- La stratégie d'authentification doit être liée au serveur virtuel d'authentification, d'autorisation et d'audit, sinon le flux ne fonctionne pas comme prévu.
- Vous avez les éléments suivants liés à nFactor
  - Schéma XML
  - JavaScript
  - Actions d'authentification
  - Authentification serveur virtuel
  - NetScaler version 11.1 et versions ultérieures

Personnaliser les étiquettes d'ouverture de session

Pour personnaliser les étiquettes d'ouverture de session, vous avez besoin des éléments suivants :

- Schéma XML qui décrit l'apparence de la page d'ouverture de session.
- Le fichier script.js qui contient le code JavaScript utilisé pour modifier le processus de rendu.

> **Remarque :**
>
> Le fichier script.js se trouve dans le répertoire `/var/netscaler/logon/themes/<`

> custom_theme>/.

Fonctionnement

Le JavaScript analyse le fichier XML et affiche chaque élément à l'intérieur de la balise <Requirements>. Chaque élément correspond à une ligne du formulaire HTML. Par exemple, un champ de connexion est une ligne, le champ de mot de passe est une autre ligne, tout comme le bouton d'ouverture de session. Pour introduire de nouvelles lignes, vous devez les spécifier dans le fichier de schéma XML à l'aide du SDK StoreFront. Le SDK StoreFront permet à la page d'ouverture de session avec un schéma XML d'utiliser la <Requirement> balise et de définir des éléments dessus. Ces éléments permettent d'utiliser JavaScript pour introduire dans cet espace tous les éléments HTML nécessaires. Dans ce cas, une ligne est créée avec du texte sous forme de HTML.

Le code XML qui peut être utilisé est le suivant :

```
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<!--NeedCopy-->
```

<Requirement>: espace disponible sur la page d'ouverture de session. Les informations d'identification remplissent l'espace et les autres pièces acheminent le moteur vers les informations correctes. Dans ce cas, tapez nsg-custom-cred. Il s'agit d'un texte brut et l'étiquette est définie pour son corps.
Le code XML requis est associé au code JavaScript pour obtenir les résultats requis.

```
// Custom Label Handler for Self Service Links
CTXS.ExtensionAPI.addCustomAuthLabelHandler({

getLabelTypeName: function () {
  return "nsg-custom-label";  }
 ,
getLabelTypeMarkup: function (requirements) {

return $("< Enter your HTML codes here>");
 }
 ,
// Instruction to parse the label as if it was a standard type
```



```
parseAsType: function () {

return "plain";
 }

 }
 );
//Custom Credential Handler for Self Service Links
CTXS.ExtensionAPI.addCustomCredentialHandler({

getCredentialTypeName: function () {
  return "nsg-custom-cred";  }
 ,
getCredentialTypeMarkup: function (requirements) {

return $("<div/>");
 }
 ,
 }
 );
<!--NeedCopy-->
```

> **Important :**
>
> Lorsque vous ajoutez le code HTML, assurez-vous que la valeur renvoyée commence par une balise HTML.

La partie XML indique à la page d'ouverture de session ce qu'il faut afficher et le code JavaScript fournit le texte réel. Le gestionnaire d'informations d'identification ouvre l'espace et l'étiquette remplit l'espace. Étant donné que tout le trafic d'authentification est désormais invisible pour la réécriture et le répondeur, vous pouvez modifier l'aspect et la convivialité de la page.
Configuration pour personnaliser les étiquettes de connexion

1. Créez et liez un thème basé sur RFWeb.

   ```
   add vpn portaltheme RfWebUI_MOD -basetheme RfWebUI

   bind vpn vserver TESTAAA  - portaltheme RfWebUI_MOD
   <!--NeedCopy-->
   ```

   Le chemin des fichiers basés sur le thème est disponible dans le répertoire ; /var/netscaler/logon/themes/RFWEBUI_MOD

2. Ajoutez l'extrait suivant à la fin du fichier script.js :

> **Remarque :**
>
> Le fait de ne pas inclure les lignes précédentes dans le bon fichier ou de ne pas inclure de fonctions JavaScript empêche le chargement du code XML. L'erreur ne peut être vue que dans la Developer Console du navigateur avec le texte suivant : « Type non défini `nsg-custom-cred`. »

```
// Custom Label Handler for Self Service Links
CTXS.ExtensionAPI.addCustomAuthLabelHandler({

getLabelTypeName: function () {
  return "nsg-custom-label";  }
 ,
getLabelTypeMarkup: function (requirements) {

return $("<a href="https://identity.test.com/identity/faces/
   register" style="font-size: 16px;" style="text-align: center;">
   Self Registration</a><br><a href="https://identity.test.com/
   identity/faces/forgotpassword" style="font-size: 16px;" style="
   text-align: center;">Forgot Password</a><br><a href="https://
   identity.test.com/identity/faces/forgotuserlogin" style="font-
   size: 16px;" style="text-align: center;">Forgot User Login</a
   >");
 }
 ,
// Instruction to parse the label as if it was a standard type
parseAsType: function () {

return "plain";
 }

 }
 );
//Custom Credential Handler for Self Service Links
CTXS.ExtensionAPI.addCustomCredentialHandler({

getCredentialTypeName: function () {
  return "nsg-custom-cred";  }
 ,
getCredentialTypeMarkup: function (requirements) {

return $("<div/>");
 }
 ,
 }
```



```
32   );
33  <!--NeedCopy-->
```

> **Important :**
>
> Lorsque vous ajoutez le code HTML, assurez-vous que la valeur renvoyée commence par une balise HTML.

Schéma de connexion utilisé dans cet exemple

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <AuthenticateResponse xmlns="http://citrix.com/authentication/response
      /1">
3  <Status>success</Status>
4  <Result>more-info</Result>
5  <StateContext/>
6  <AuthenticationRequirements>
7  <PostBack>/nf/auth/doAuthentication.do</PostBack>
8  <CancelPostBack>/Citrix/Authentication/ExplicitForms/CancelAuthenticate
      </CancelPostBack>
9  <CancelButtonText>Cancel</CancelButtonText>
10 <Requirements>
11 <Requirement>
12 <Credential>
13 <ID>login</ID>
14 <SaveID>Username</SaveID>
15 <Type>username</Type>
16 </Credential>
17 <Label>
18 <Text>User name</Text>
19 <Type>plain</Type>
20 </Label>
21 <Input>
22 <AssistiveText>Please supply either domain\username or user@fully.
      qualified.domain</AssistiveText>
23 <Text>
24 <Secret>false</Secret>
25 <ReadOnly>false</ReadOnly>
26 <InitialValue></InitialValue>
27 <Constraint>.+</Constraint>
28 </Text>
29 </Input>
30 </Requirement>
31 <Requirement>
```



```
<Credential>
<ID>passwd</ID>
<SaveID>Password</SaveID>
<Type>password</Type>
</Credential>
<Label>
<Text>Password:</Text>
<Type>plain</Type>
</Label>
<Input>
<Text>
<Secret>true</Secret>
<ReadOnly>false</ReadOnly>
<InitialValue/>
<Constraint>.+</Constraint>
</Text>
</Input>
</Requirement>
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<Requirement>
<Credential>
<ID>loginBtn</ID>
<Type>none</Type>
</Credential>
<Label>
<Type>none</Type>
</Label>
<Input>
<Button>Please Log On</Button>
</Input>
</Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

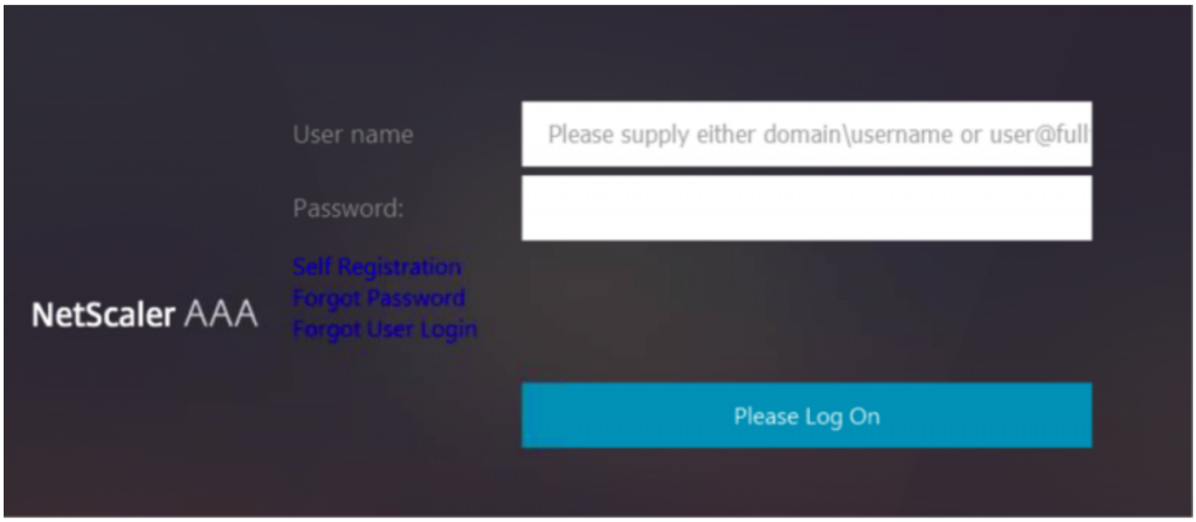
Exécutez les commandes suivantes pour charger le schéma personnalisé à configurer.


```
add authentication loginSchema custom -authenticationSchema custom.xml

add authentication loginSchemaPolicy custom -rule true -action custom

bind authentication vserver AAATEST -policy custom -priority 100 -
    gotoPriorityExpression END
<!--NeedCopy-->
```

La figure suivante affiche la page de connexion affichée avec cette configuration.



Personnaliser l'interface utilisateur pour afficher les images

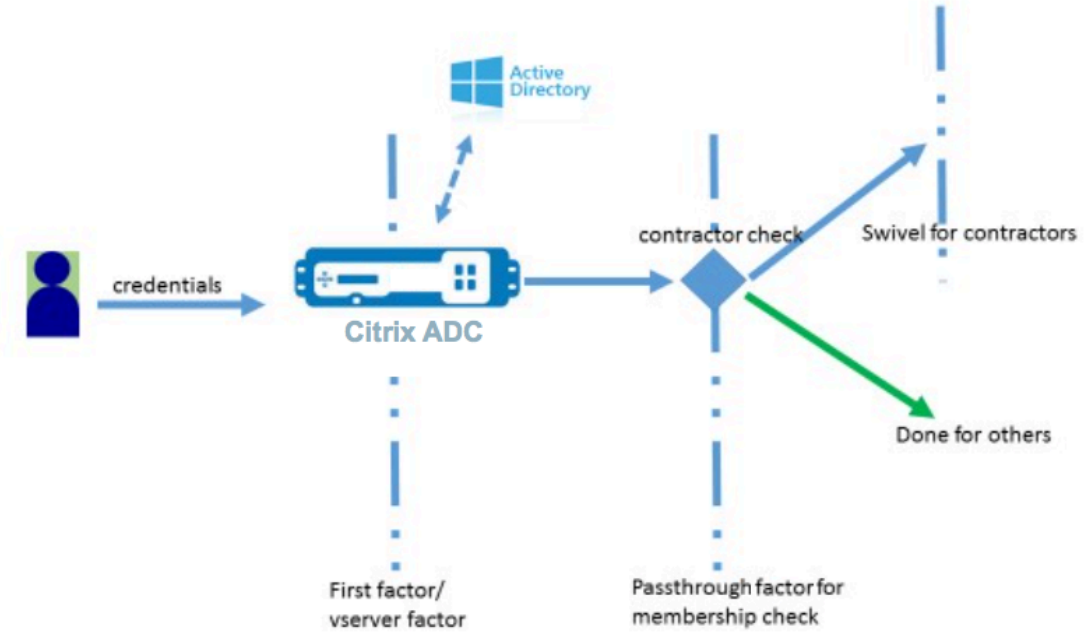
nFactor permet un affichage personnalisé à l'aide de fichiers de schéma de connexion. Des personnalisations supplémentaires autres que celles proposées par les fichiers de schéma de connexion intégrés peuvent être nécessaires. Par exemple, afficher un lien hypertexte ou écrire une logique personnalisée dans l'interface utilisateur. Cela peut être réalisé en utilisant des « informations d'identification personnalisées » qui comprennent l'extension du schéma de connexion et le fichier javascript correspondant.

Les fichiers de schéma de connexion se trouvent dans le répertoire `/nsconfig/loginschema/LoginSchema`.

Pour la personnalisation de l'interface utilisateur afin d'afficher des images, un flux de déploiement dans l'intégration « NetScaler-Swivel » est utilisé à titre d'exemple.

Ce flux tient compte de deux facteurs.

- Premier facteur : vérifie les informations d'identification AD de l'utilisateur.
- Deuxième facteur : invite l'utilisateur à ouvrir une session en fonction de l'appartenance au groupe.



Dans ce flux, tous les utilisateurs passent par le premier facteur. Avant le deuxième facteur, il existe un pseudo facteur pour vérifier si certains utilisateurs peuvent être omis du facteur « pivot ». Si l'utilisateur a besoin du facteur « pivot », une image et une zone de texte s'affichent pour saisir le code.

Solution

La solution de personnalisation de l'interface utilisateur pour afficher des images contient deux parties :

- Extension du schéma de connexion.
- Script personnalisé pour traiter l'extension du schéma de connexion.

Extension de schéma de connexion

Pour contrôler le rendu du formulaire, un 'id'/'credential' personnalisé est injecté dans le schéma de connexion. Cela peut être fait en réutilisant le schéma existant et en le modifiant selon les besoins.

Dans cet exemple, un schéma de connexion qui ne comporte qu'un seul champ de texte (tel que /nsconfig/loginschema/LoginSchema/OnlyPassword.xml) est pris en compte.
L'extrait suivant est ajouté au schéma de connexion.

```
<Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><
   Input><Text><Hidden>true</Hidden><InitialValue>${
 http.req.user.name }
 </InitialValue></Text></Input></Credential></Requirement>
<!--NeedCopy-->
```


Dans l'extrait, « swivel_cred » est spécifié comme « Type » des informations d'identification. Étant donné que ce n'est pas reconnu comme une « information d'identification » intégrée, l'interface utilisateur recherche un gestionnaire pour ce type et l'appelle s'il existe.
Une valeur initiale est envoyée pour ces informations d'identification. Il s'agit d'une expression que NetScaler remplit dynamiquement. Dans l'exemple, il s'agit du nom de l'utilisateur utilisé pour notifier le nom d'utilisateur au serveur pivotant. Elle n'est peut-être pas nécessaire à tout moment ou elle peut être complétée par d'autres données. Ces informations doivent être ajoutées au besoin.

Javascript pour gérer les informations d'identification personnalisées

Lorsque l'interface utilisateur trouve des informations d'identification personnalisées, elle recherche un gestionnaire. Tous les gestionnaires personnalisés sont écrits dans /var/netscaler/logon/LogonPoint/custom/script.js pour le thème de portail par défaut.

Pour les thèmes de portail personnalisés, script.js se trouve dans le répertoire `/var/netscaler/logon/themes/<custom_theme>/`.

Le script suivant est ajouté pour afficher le balisage des informations d'identification personnalisées.

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the
       server
    getCredentialTypeName: function () {
  return "swivel_cred";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        var image = $("<img/>");
        var username = requirements.input.text.initialValue; //Get the
           secret from the response
        image.attr({

            "style" : "width:200px;height:200px;",
            "id" : "qrcodeimg",
            "<Enter your server URL here>"
         }
 );
        div.append(image);
        return div;
     }

 }
```



```
25  );
26 <!--NeedCopy-->
```

Cet extrait sert à gérer le balisage pour « swivel_cred ». Le nom des informations d'identification mis en surbrillance doit correspondre au « type » spécifié précédemment dans l'extension du schéma de connexion.
Pour générer un balisage, une image dont la source pointe vers le serveur pivotant doit être ajoutée. Une fois cela fait, l'interface utilisateur charge l'image à partir de l'emplacement spécifié. Étant donné que ce schéma de connexion possède également une zone de texte, l'interface utilisateur affiche cette zone de texte.

> **Remarque :**
>
> L'administrateur peut modifier le « style » de l'élément d'image pour redimensionner l'image. Actuellement, il est configuré pour 200x200 pixels.

Configuration pour personnaliser l'interface utilisateur pour afficher les images

La configuration nFactor est mieux construite de bas en haut, c'est-à-dire le dernier facteur en premier car lorsque vous essayez de spécifier « NextFactor » pour les facteurs précédents, vous avez besoin du nom du facteur suivant.

Configuration du facteur de pivotement :

```
1 add loginschema swivel_image -authenticationSchema /nsconfig/
     loginschema/SwivelImage.xml
2
3 add authentication policylabel SwivelFactor -loginSchema swivel_image
4
5 bind authentication policylabel SwivelFactor -policy <policy-to-check-
     swivel-image> -priority 10
6 <!--NeedCopy-->
```

> **Remarque :**
>
> Téléchargez SwivelImage.xml à partir du schéma de connexion utilisé dans l'exemple.

Pseudo facteur pour la configuration des vérifications de groupe:

```
1 add authentication policylabel GroupCheckFactor
2
3 add authentication policy contractors_auth_policy -rule 'http.req.
     user.is_member_of( "contractors" )' -action NO_AUTHN
4
5 add authentication policy not_contractors _auth_policy -rule true -
     action NO_AUTHN
```



```
6
7 bind authentication policylabel GroupCheckFactor -policy
     contractors_auth_policy -pri 10 -nextFactor SwivelFactor
8
9 bind authentication policylabel GroupCheckFactor -policy
     not_contractors_auth_policy -pri 20
10 <!--NeedCopy-->
```

Premier facteur pour la connexion à Active Directory :

```
1 add ldapAction <>
2
3 add authentication policy user_login_auth_policy -rule true -action
     <>
4
5 bind authentication vserver <> -policy user_login_auth_policy -pri 10
     -nextFactor GroupCheckFactor
6 <!--NeedCopy-->
```

Dans la configuration, trois facteurs sont spécifiés dont un est implicite/pseudo.

Schéma de connexion utilisé dans cet exemple

Voici un exemple de schéma avec des informations d'identification pivotantes et une zone de texte.

> **Remarque :**
>
> Lors de la copie de données pour un navigateur Web, les guillemets peuvent s'afficher différemment. Copiez les données dans des éditeurs comme le bloc-notes avant de les enregistrer dans des fichiers.

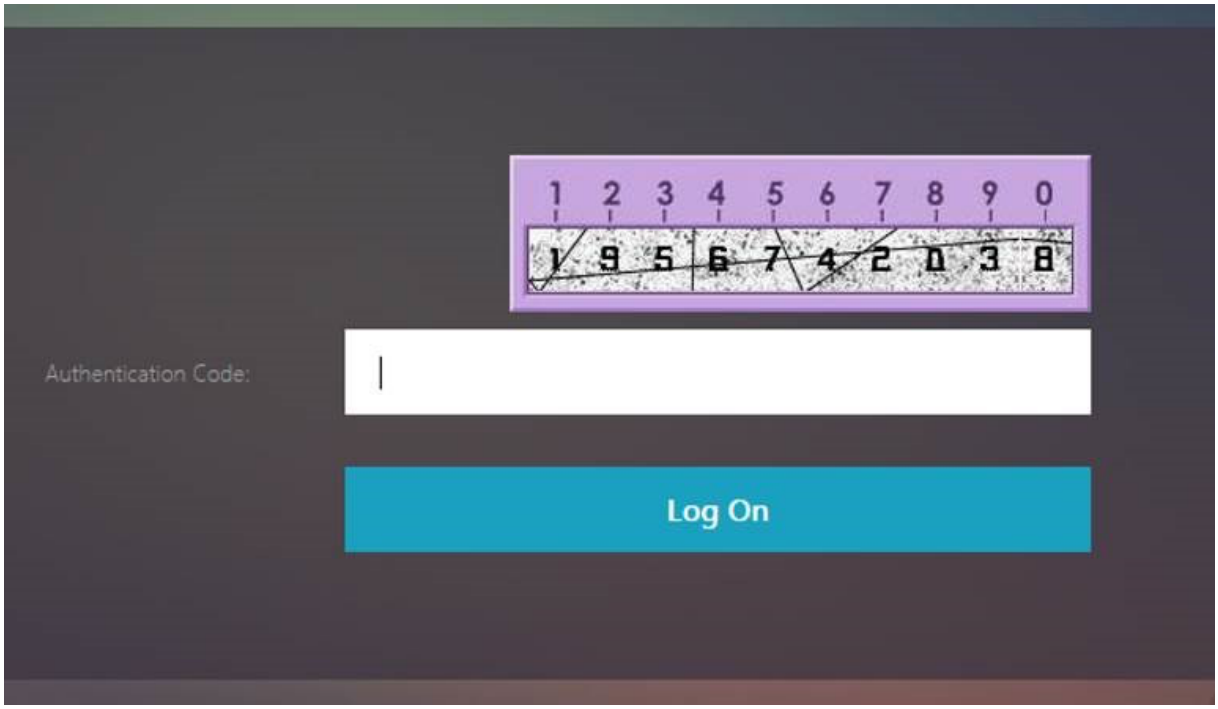
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <AuthenticateResponse xmlns="http://citrix.com/authentication/response
     /1">
3 <Status>success</Status>
4 <Result>more-info</Result>
5 <StateContext></StateContext>
6 <AuthenticationRequirements>
7 <PostBack>/nf/auth/doAuthentication.do</PostBack>
8 <CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
9 <CancelButtonText>Cancel</CancelButtonText>
10 <Requirements>
11 <Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><
     Input><Text><Hidden>true</Hidden><InitialValue>${
12  http.req.user.name }
```



```
 </InitialValue></Text></Input></Credential></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password
   </SaveID><Type>password</Type></Credential><Label><Text>Password:</
   Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><
   ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint
   >.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>
   Hello ${
 http.req.user.name }
 , Please enter passcode from above image.</Text><Type>confirmation</
    Type></Label><Input /></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials
   </Type></Credential><Label><Text>Remember my password</Text><Type>
   plain</Type></Label><Input><CheckBox><InitialValue>false</
   InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential
   ><Label><Type>none</Type></Label><Input><Button>Log On</Button></
   Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

Résultat

Une fois la configuration effectuée, l'image suivante s'affiche.



> **Remarque :**
>
> La hauteur et le placement de l'image peuvent être modifiés dans le JavaScript.

Personnalisez le formulaire de connexion NetScaler nFactor pour afficher ou masquer des champs

L'interface utilisateur RFWeb de NetScaler Gateway permet de nombreuses personnalisations. Cette fonctionnalité, associée au cadre d'authentification nFactor, permet aux clients de configurer des flux complexes sans compromettre les flux de travail existants.

Dans cet exemple, deux options d'authentification, OAuth et LDAP, sont disponibles dans la liste Type d'ouverture de session. Lors du premier chargement du formulaire, les champs du nom d'utilisateur et du mot de passe (LDAP est affiché en premier) s'affichent. Si OAuth est sélectionné, tous les champs sont masqués car OAuth implique un déchargement de l'authentification vers un serveur tiers. De cette façon, un administrateur peut configurer des flux de travail intuitifs selon la commodité de l'utilisateur.

> **Remarque :**
>
> - Les valeurs de la liste Type d'ouverture de session peuvent être modifiées par de simples modifications apportées au fichier de script.
> - Cette section décrit uniquement la partie UI du flux. La gestion de l'exécution de l'authentification sort du cadre de cet article. Les utilisateurs sont invités à consulter la documentation nFactor pour la configuration de l'authentification.

Comment personnaliser le formulaire d'ouverture de session nFactor

La personnalisation du formulaire d'ouverture de session nFactor peut être classée en deux parties

- Envoi du bon schéma de connexion à l'interface utilisateur
- Écriture d'un gestionnaire pour interpréter le schéma de connexion et les sélections des utilisateurs

Envoyer le bon schéma de connexion à l'interface utilisateur

Dans cet exemple, une simple réclamation/exigence est envoyée dans le schéma de connexion.

Pour cela, le fichier SingleAuth.xml est modifié. Le fichier SingleAuth.xml est livré avec le microprogramme NetScaler et se trouve dans le `/nsconfig/loginschema/LoginSchema` répertoire.

Étapes pour envoyer le schéma de connexion :

1. Connectez-vous via SSH et déposez-les sur le shell (tapez 'shell').
2. Copiez SingleAuth.xml dans un autre fichier pour modification.

   > **Remarque :**
   >
   > Le dossier de destination est différent du dossier des schémas de connexion NetScaler par défaut.
   >
   > cp /nsconfig/loginschema/LoginSchema/SingleAuth.xml /nsconfig/loginschema/SingleAuthDynamic.xml

3. Ajoutez la revendication suivante à SingleAuthDynamic.xml.

```
<Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</Type></Credential><Label><Text>Logon Type:</Text><Type>plain</Type></Label></Requirement>
<!--NeedCopy-->
```

4. Configurez NetScaler pour envoyer ce schéma de connexion afin de charger le premier formulaire.

```
add loginschema single_auth_dynamic -authenticationSchema SingleAuthDynamic.xml

add loginschemaPolicy single_auth_dynamic -rule true -action single_auth_dynamic

bind authentication vserver aaa_nfactor -policy single_auth_dynamic -pri 10
<!--NeedCopy-->
```


Modifications du script pour charger le formulaire et gérer les événements utilisateur

Vous pouvez modifier le code JavaScript qui permet à un administrateur de personnaliser l'affichage du formulaire d'ouverture de session. Dans cet exemple, le champ du nom d'utilisateur et du mot de passe s'affichent si LDAP est choisi et sont masqués si OAuth est choisi. L'administrateur peut également masquer uniquement le mot de passe.

Les administrateurs doivent ajouter l'extrait suivant dans "script.js" qui se trouve dans le répertoire « /var/netscaler/logon/LogonPoint/Custom ».

> **Remarque :**
>
> étant donné que ce répertoire est un répertoire global, créez un thème de portail et modifiez le fichier "script.js" dans ce dossier, à l'adresse `"/var/netscaler/logon/themes/<THEME_NAME>"`.

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the
       server
    getCredentialTypeName: function () {
  return "nsg_dropdown";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        var select = $("<select name='nsg_dropdown'></select>").attr("
           id", "nsg_dropdown");

        var rsa = $("<option></option>").attr("selected", "selected").
           text("LDAP").val("LDAP");
        var OAuthID = $("<option></option>").text("OAuth").val("OAuth")
           ;
        select.append(rsa, OAuthID);

        select.change(function(e) {

            var value = $(this).val();
            var ldapPwd = $($(".credentialform").find(".
               CredentialTypepassword")[0]);
            var ldapUname = $($(".credentialform").find(".
               CredentialTypeusername"));
            if(value == "OAuth") {

                if (ldapPwd.length)
```



```
                        ldapPwd.hide();
                if (ldapUname.length)
                        ldapUname.hide();
            }
   else if(value == "LDAP") {

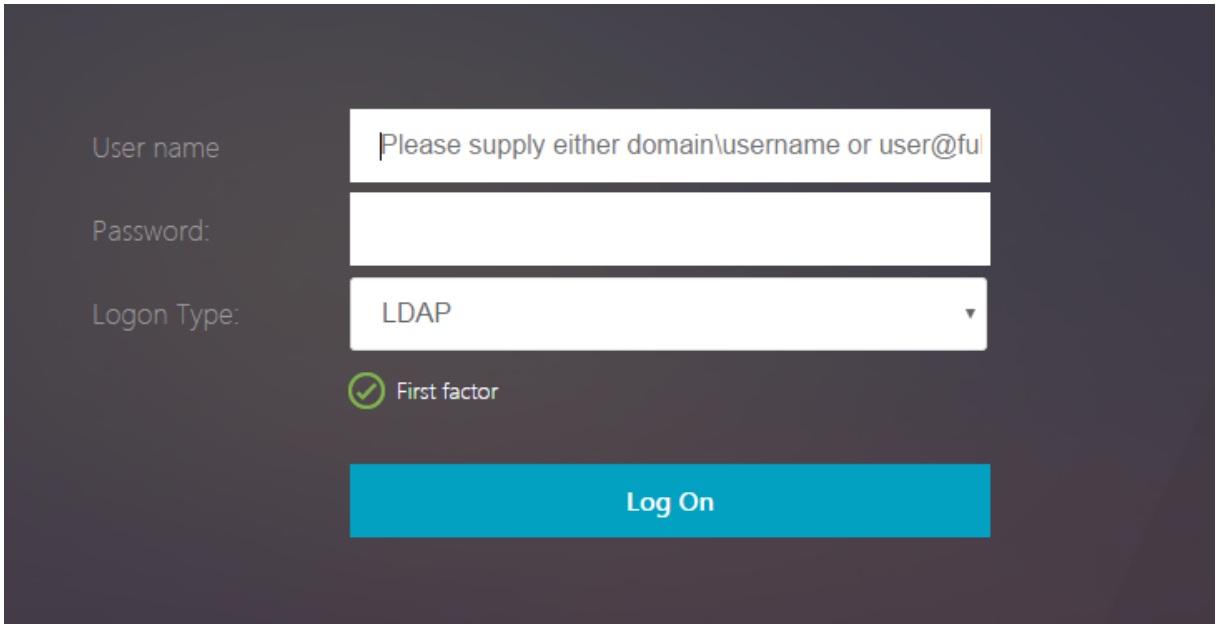
                if (ldapPwd.length)
                        ldapPwd.show();
                if (ldapUname.length)
                        ldapUname.show();
            }

          }
 );
       div.append(select);
        return div;
     }

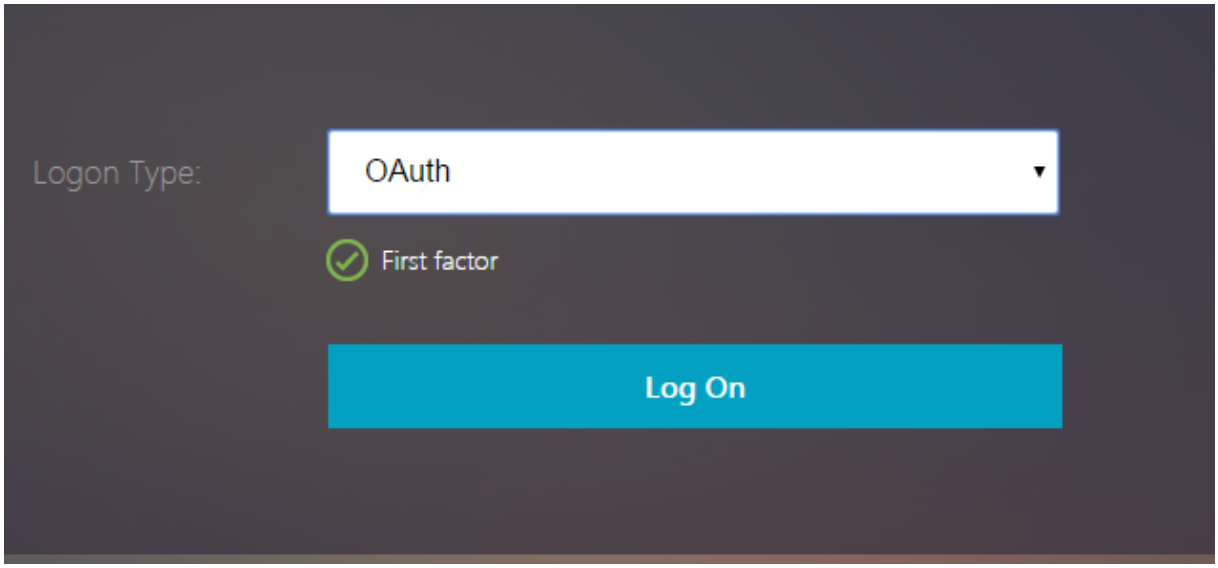
 }
 );
<!--NeedCopy-->
```

Expérience pour l'utilisateur final

Lorsqu'un utilisateur final charge la page d'ouverture de session pour la première fois, l'écran suivant s'affiche.



Si **OAuth** est sélectionné dans **Type d'ouverture de session, les**champs du nom d'utilisateur et du mot de passe sont masqués.



Si **LDAP** est sélectionné, le nom d'utilisateur et le mot de passe s'affichent. De cette façon, la page d'ouverture de session peut être chargée dynamiquement en fonction de la sélection de l'utilisateur.

Schéma de connexion utilisé dans cet exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</SaveID><Type>username</Type></Credential><Label><Text>User name</Text><Type>plain</Type></Label><Input><AssistiveText>Please supply either domain\username or user@fully.qualified.domain</AssistiveText><Text><Secret>false</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>Password:</Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><
```



```
      ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint
      >.+</Constraint></Text></Input></Requirement>
13 <Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</Type
      ></Credential><Label><Text>Logon Type:</Text><Type>plain</Type></
      Label></Requirement>
14 <Requirement><Credential><Type>none</Type></Credential><Label><Text>
      First factor</Text><Type>confirmation</Type></Label><Input /></
      Requirement>
15 <Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials
      </Type></Credential><Label><Text>Remember my password</Text><Type>
      plain</Type></Label><Input><CheckBox><InitialValue>false</
      InitialValue></CheckBox></Input></Requirement>
16 <Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential
      ><Label><Type>none</Type></Label><Input><Button>Log On</Button></
      Input></Requirement>
17 </Requirements>
18 </AuthenticationRequirements>
19 </AuthenticateResponse>
20 <!--NeedCopy-->
```

> **Remarque :**
>
> Pour plus de détails sur les différentes rubriques liées à nFactor, consultez Authentification nFactor.

Définir un cookie à l'aide de NFactor

May 5, 2023

Vous pouvez appliquer les étiquettes personnalisées nFactor et définir un cookie en tant que facteur du flux d'authentification. Grâce aux étiquettes personnalisées, vous pouvez utiliser JavaScript pour manipuler le schéma de connexion.

Pour définir un cookie en tant que facteur, vous n'avez pas besoin d'afficher d'informations à l'utilisateur, ce qui est effectué sans connexion de schéma. Au lieu de cela, vous devez interagir avec le navigateur de l'utilisateur pour demander au schéma de connexion de stocker les données souhaitées. Un schéma de connexion est nécessaire pour définir le cookie lorsque la page est chargée. Le cookie est défini avec une étiquette personnalisée et un code JavaScript.

Pour implémenter un facteur qui définit un cookie, créez un fichier XML appelé cookie.xml pour stocker le schéma dans le répertoire /nsconfig/loginschema/ avec le contenu suivant :

```
1 <?xml version="1.0" encoding="UTF-8"?>
```



```
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
   /1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>

<Requirement>
<Credential><ID>nsg_cookie</ID><Type>nsg_cookie</Type></Credential>
<Label><Text>Logon Type:</Text><Type>Plain</Type></Label>
</Requirement>

<Requirement>
<Credential><ID>loginBtn</ID><Type>none</Type></Credential>
<Label><Type>none</Type></Label><Input><Button>Log On</Button></Input>
</Requirement>

</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

Dans ce code XML ;

- L'étiquette personnalisée nsg_cookie est utilisée pour créer le cookie et envoyer le formulaire, ainsi que le bouton du formulaire.
- Le RFWebUI_Custom est le nouveau thème du portail basé sur le thème RFWebUI.

Étapes pour définir un cookie à l'aide de nFactor

1. Créez un thème de portail basé sur le thème RFWebUI.

   ```
   add vpn portaltheme RfWebUI_custom -basetheme RfWebUI
   <!--NeedCopy-->
   ```

   Cette commande crée un dossier pour ce thème dans /var/netscaler/logon/themes/RFWEBUI_CUSTOM

2. Modifiez le fichier /var/netscaler/logon/themes/RfWebUI_custom/script.js et ajoutez le script suivant :


```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by
        the server
    getCredentialTypeName: function () {
  return "nsg_cookie";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        $(document).ready(function() {

        //Set cookie valid for 1000 days
        var exdays = 1000;
        var d = new Date();
        d.setTime(d.getTime() + (exdays\*24\*60\*60\*1000));
        var expires = "expires="+ d.toUTCString();
        document.cookie = "NSC_COOKIE_NAME=CookieValue;" + expires
            + ";path=/";

        //Submit form
        document.getElementById('loginBtn').click();
         }
 );
        return div;
     }

 }
 );
<!--NeedCopy-->
```

Ce code effectue les opérations suivantes :

- Attend que le navigateur ait fini de charger la page
- Définit un cookie appelé NSC_COOKIE_NAME avec la valeur CookieValue, valide pendant 1000 jours
- Soumet automatiquement le formulaire.

Le cookie est créé et l'utilisateur n'a pas besoin d'interagir avec la page.

3. Créez un schéma de connexion à lier à l'étiquette de stratégie qui représente le facteur de cookie défini.


```
add authentication loginSchema Cookie_LS -authenticationSchema "/
    nsconfig/loginschema/cookie.xml"
<!--NeedCopy-->
```

4. Créez une stratégie d'authentification NO_AUTHN à lier à l'étiquette de stratégie qui représente le facteur de cookie défini.

```
add authentication Policy NO_AUTHN_POL -rule TRUE -action NO_AUTHN
<!--NeedCopy-->
```

   Cette stratégie est toujours évaluée comme vraie, en déplaçant l'utilisateur vers le facteur suivant ou en complétant le flux d'authentification.

5. Liez le thème du portail RFWebUI_Custom au serveur virtuel NetScaler Gateway ou au serveur virtuel NetScaler AAA.

Exemples de déploiements utilisant l'authentification NFactor

June 2, 2023

Voici des exemples de déploiements utilisant l'authentification nFactor :

- Obtenir deux mots de passe à l'avance, le pass-through dans le prochain facteur. Read
- Extraction de groupe suivie d'une authentification par certificat ou LDAP, basée sur l'appartenance au groupe. Read
- SAML suivi d'une authentification LDAP ou par certificat, basée sur les attributs extraits pendant SAML. Read
- SAML en premier facteur, suivi de l'extraction de groupe, puis de l'authentification LDAP ou de certificat, en fonction des groupes extraits. Read
- Préremplissage du nom d'utilisateur à partir du certificat. Read
- Authentification du certificat suivie d'une extraction de groupe pour les serveurs virtuels de gestion du trafic compatibles 401. Read
- Nom d'utilisateur et deux mots de passe avec extraction de groupe en troisième facteur. Read
- Remplacement du certificat vers LDAP dans la même cascade ; un seul serveur virtuel pour l'authentification par certificat et LDAP. Read
- LDAP dans le premier facteur et WebAuth dans le second facteur. Read
- Liste déroulante des domaines dans le premier facteur, puis différentes évaluations de stratégies basées sur le groupe. Read
- Configurez l'extraction de groupe basée sur la saisie de l'identifiant e-mail (ou du nom d'utilisateur) au premier facteur pour décider du flux d'authentification suivant. Read

Liste des articles pratiques

May 5, 2023

Les articles « Comment faire » sur l'authentification, l'autorisation et l'audit sont simples, pertinents et faciles à mettre en œuvre. Ces articles contiennent des informations sur certaines des fonctionnalités populaires d'authentification, d'autorisation et d'audit telles que l'authentification LDAP et l'authentification multifacteur. Pour consulter certains des articles les plus populaires sur la configuration et la résolution des problèmes d'authentification via NetScaler, voir [NetScaler Authentication :]How do I ?(https://support.citrix.com/pages/citrix-adc-authentication-how#nfactor)

Analyse des points de terminaison

Configurer l'analyse Endpoint Analysis de pré-authentification en tant que facteur d'authentification nFactor

Configurer le scan d'Endpoint Analysis après authentification comme facteur d'authentification NetScaler nFactor

Configurer l'analyse EPA de pré-authentification et de post-authentification en tant que facteur d'authentification nFactor

Configurer l'analyse périodique d'Endpoint Analysis en tant que facteur d'authentification nFactor

Configurer le scan EPA de pré-authentification de NetScaler Gateway pour la vérification du domaine

Combinaisons de configuration du premier facteur et du deuxième facteur

Configurer nFactor pour NetScaler Gateway avec WebAuth comme premier facteur et LDAP avec changement de mot de passe comme deuxième facteur

Configurez SAML suivi de l'authentification LDAP ou de certificat basée sur l'extraction d'attributs SAML dans l'authentification nFactor

Configurer l'authentification par certificat comme premier facteur et LDAP comme second facteur dans l'authentification NetScaler nFactor

Configurer l'authentification à deux facteurs avec un schéma de connexion et un schéma de transmission dans l'authentification NetScaler nFactor

Configurer le nom d'utilisateur et deux mots de passe avec extraction de groupe en troisième facteur par authentification nFactor

Configurer la liste déroulante du domaine, le nom d'utilisateur et le champ mot de passe dans le premier facteur et l'évaluation de stratégie en fonction des groupes du facteur suivant

Configurer l'extraction de groupe basée sur l'ID de messagerie (ou nom d'utilisateur) au premier facteur pour décider du flux d'authentification du facteur suivant

Configurer une liste déroulante de domaine pour la saisie de l'utilisateur dans le premier facteur afin de décider du prochain flux d'authentification du facteur

CLUF en tant que facteur d'authentification

Configurer le CLUF en tant que facteur d'authentification dans le système NetScaler nFactor

Préremplissage du nom d'utilisateur à partir du certificat

Configurer le nom d'utilisateur prérempli à partir du certificat dans l'authentification NetScaler nFactor

Authentification par étapes

Configurer nFactor pour les applications ayant des exigences de site de connexion différentes, y compris l'authentification renforcée

Authentification SAML

May 5, 2023

Le langage SAML (Security Assertion Markup Language) est un mécanisme d'authentification basé sur XML qui fournit une fonctionnalité d'authentification unique et est défini par le comité technique des services de sécurité d'OASIS.

> Remarque
>
> À partir de NetScaler 12.0 Build 51.x, l'appliance NetScaler utilisée en tant que fournisseur de services SAML (SP) avec authentification multifactorielle (nFactor) préremplit désormais le champ du nom d'utilisateur sur la page de connexion. L'appliance envoie un attribut NameID dans le cadre d'une demande d'autorisation SAML, extrait la valeur de l'attribut NameID auprès du fournisseur d'identité SAML NetScaler (IdP) et préremplit le champ du nom d'utilisateur.

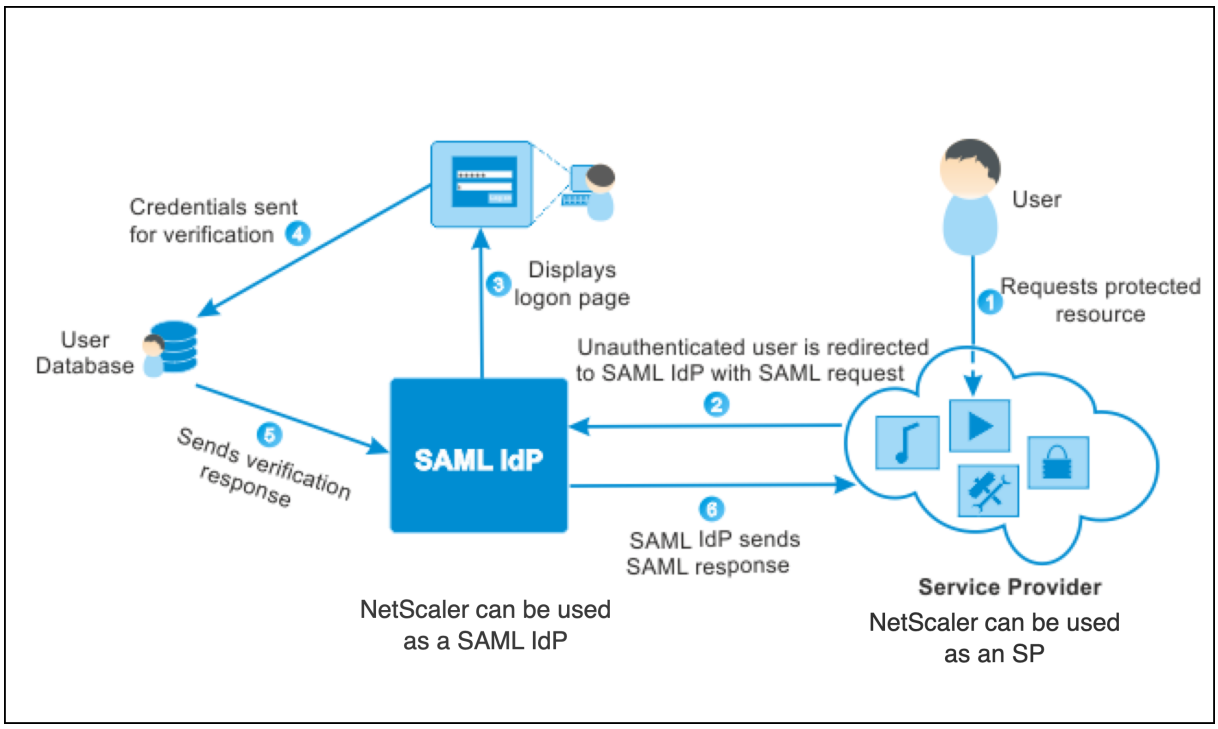
Pourquoi utiliser l'authentification SAML

Imaginons un scénario dans lequel un fournisseur de services (LargeProvider) héberge un certain nombre d'applications pour un client (BigCompany). BigCompany a des utilisateurs qui doivent accéder facilement à ces applications. Dans une configuration traditionnelle, LargeProvider devrait gérer une

base de données des utilisateurs de BigCompany. Cela soulève certaines préoccupations pour chacune des parties prenantes suivantes :

- LargeProvider doit garantir la sécurité des données des utilisateurs.
- BigCompany doit valider les utilisateurs et maintenir les données utilisateur à jour, non seulement dans sa propre base de données, mais également dans la base de données utilisateur gérée par LargeProvider. Par exemple, un utilisateur supprimé de la base de données BigCompany doit également être supprimé de la base de données LargeProvider.
- Un utilisateur doit se connecter individuellement à chacune des applications hébergées.

Le mécanisme d'authentification SAML fournit une approche alternative. Le schéma de déploiement suivant montre le fonctionnement du SAML (flux initié par le SP).



Les problèmes soulevés par les mécanismes d'authentification traditionnels sont résolus comme suit :

- LargeProvider n'a pas à gérer de base de données pour les utilisateurs de BigCompany. Libéré de la gestion des identités, LargeProvider peut se concentrer sur la fourniture de meilleurs services.
- BigCompany n'a pas la charge de s'assurer que la base de données utilisateur LargeProvider est synchronisée avec sa propre base de données utilisateur.
- Un utilisateur peut se connecter une seule fois à une application hébergée sur LargeProvider et être automatiquement connecté aux autres applications qui y sont hébergées.

L'appliance NetScaler peut être déployée en tant que fournisseur de services SAML (SP) et fournisseur d'identité SAML (IdP). Lisez les rubriques pertinentes pour comprendre les configurations qui doivent être effectuées sur l'appliance NetScaler.

Une appliance NetScaler configurée en tant que fournisseur de services SAML peut désormais appliquer un contrôle des restrictions d'audience. La condition de restriction d'audience est évaluée comme « Valide » uniquement si le répondant SAML est membre d'au moins une des audiences spécifiées.

Vous pouvez configurer une appliance NetScaler pour analyser les attributs des assertions SAML en tant qu'attributs de groupe. Leur analyse en tant qu'attributs de groupe permet à l'appliance de lier des stratégies aux groupes.

NetScaler en tant que SP SAML

May 5, 2023

Le fournisseur de services SAML (SP) est une entité SAML déployée par le fournisseur de services. Lorsqu'un utilisateur tente d'accéder à une application protégée, le SP évalue la demande du client. Si le client n'est pas authentifié (ne possède pas de cookie NSC_TMAA ou NSC_TMAS valide), le SP redirige la demande vers le fournisseur d'identité SAML (IdP).

Le SP valide également les assertions SAML reçues de l'IdP.

Lorsque l'appliance NetScaler est configurée en tant que SP, un serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu) reçoit toutes les demandes des utilisateurs associées à l'action SAML correspondante.

L'appliance NetScaler prend également en charge les liaisons POST et Redirect lors de la déconnexion.

> **Remarque**
>
> Une appliance NetScaler peut être utilisée comme SP SAML dans un déploiement où l'IdP SAML est configuré soit sur l'appliance, soit sur n'importe quel IdP SAML externe.

Lorsqu'elle est utilisée comme SP SAML, une appliance NetScaler :

- Peut extraire les informations utilisateur (attributs) du jeton SAML. Ces informations peuvent ensuite être utilisées dans les politiques configurées sur l'appliance NetScaler. ****Par exemple, si vous souhaitez extraire les attributs GroupMember et **emailaddress**, dans SAMLAction, spécifiez le paramètre **Attribute2 comme GroupMember et le paramètre Attribute3** comme adresse e-mail.**

  > **Remarque**
  >
  > Les attributs par défaut tels que le nom d'utilisateur, le mot de passe et l'URL de déconnexion ne doivent pas être extraits dans les attributs 1 à 16, car ils sont implicitement analysés et stockés dans la session.

- Peut extraire des noms d'attributs d'une taille maximale de 127 octets à partir d'une assertion SAML entrante. La limite précédente était de 63 octets.
- Supporte les liaisons de publication, de redirection et d'artefacts.

  > **Remarque**
  >
  > N'utilisez pas la liaison de redirection pour de grandes quantités de données lorsque l'assertion après le gonflage ou le décodage est supérieure à 10 Ko.

- Peut déchiffrer des assertions.
- Peut extraire des attributs à valeurs multiples d'une assertion SAML. Ces attributs sont envoyés sous forme de balises XML imbriquées telles que :

  <AttributeValue> <AttributeValue>Value1</AttributeValue>
  <AttributeValue>Value2</AttributeValue>
  \</AttributeValue\>

  > **Remarque**
  >
  > À partir de NetScaler 13.0 Build 63.x et versions ultérieures, la longueur maximale individuelle des attributs SAML a été augmentée pour permettre un maximum de 40 000 octets. La taille de tous les attributs ne doit pas dépasser 40 000 octets.

  Lorsqu'on lui présente la version précédente du code XML, l'appliance NetScaler peut extraire à la fois Value1 et Value2 en tant que valeurs d'un attribut donné, contrairement à l'ancien microprogramme qui extrayait uniquement la Value1.
- Peut spécifier la validité d'une assertion SAML.

  Si l'heure système sur NetScaler SAML IdP et sur le SP SAML homologue n'est pas synchronisée, les messages peuvent être invalidés par l'une ou l'autre des parties. Pour éviter de tels cas, vous pouvez désormais configurer la durée pendant laquelle les assertions sont valides.

  Cette durée, appelée « temps d'inclinaison », indique le nombre de minutes pendant lesquelles le message peut être accepté. Le temps d'inclinaison peut être configuré sur le SP SAML et le fournisseur d'identité SAML.
- Peut envoyer un attribut supplémentaire appelé « ForceAuth » dans la demande d'authentification à un IdP externe (fournisseur d'identité). Par défaut, le ForceAuthn est défini sur « False ». Il peut être défini sur « True » pour suggérer à IdP de forcer l'authentification malgré le contexte d'authentification existant. NetScaler SP effectue également une demande d'authentification dans le paramètre de requête lorsqu'il est configuré avec une liaison aux artefacts.

Configurer l'appliance NetScaler en tant que SP SAML à l'aide de l'interface de ligne de commande

1. Configurez une action de SP SAML.

   Exemple

   La commande suivante ajoute une action SAML qui redirige les demandes utilisateur non authentifiées.

   ```
   add authentication samlAction SamlSPAct1 -samlIdPCertName nssp -samlSigningCertNa
    nssp -samlRedirectUrl https://auth1.example.com -relaystateRule "AAA.
   LOGIN.RELAYSTATE.EQ(\"https://lb.example1.com/\")"
   ```

   Points à noter

   - Le certificat prévu `-samlIdPCertName` dans la commande SamlAction doit correspondre au certificat correspondant de l'IdP pour que la vérification de la signature réussisse.
   - SAML ne prend en charge que le certificat RSA. Les autres certificats tels que HSM et FIPS ne sont pas pris en charge.
   - Il est recommandé d'avoir un nom de domaine complet avec un «/» à la fin de l'expression.
   - Les administrateurs doivent configurer une expression pour **RelaysStateRule** dans la commande SamlAction. L'expression doit contenir la liste des domaines publiés auxquels l'utilisateur se connecte avant d'être redirigé vers le serveur virtuel d'authentification. Par exemple, l'expression doit contenir les domaines du serveur virtuel frontal (VPN, LB ou CS) qui utilise cette action SAML pour l'authentification.

   > **Remarque**
   >
   > S'il existe plusieurs stratégies SAML dans le cadre d'une chaîne IdP, il suffit de configurer une règle d'état de relais uniquement sur la première stratégie SAML.

   Pour plus de détails sur la commande, reportez-vous https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction aux sections et https://support.citrix.com/article/CTX316577.

2. Configurez la stratégie SAML.

   Exemple

   La commande suivante définit une stratégie SAML qui applique l'action SAML précédemment définie à l'ensemble du trafic.

   ```
   add authentication policy SamlSPPol1 -rule true -action SamlSPAct1
   ```

3. Liez la stratégie SAML au serveur virtuel d'authentification.

   Exemple

La commande suivante lie la stratégie SAML à un serveur virtuel d'authentification nommé « av_saml ».

```
bind authentication vserver av_saml -policy SamlSPPol1
```

4. Liez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic approprié.

   Exemple

   La commande suivante ajoute un serveur virtuel d'équilibrage de charge nommé « lb1_ssl » et associe le serveur virtuel d'authentification nommé « av_saml » au serveur virtuel d'équilibrage de charge.

   ```
   add lb vserver lb1_ssl SSL 10.217.28.224 443 -persistenceType NONE -
   cltTimeout 180 -AuthenticationHost auth1.example.com -Authentication ON
    -authnVsName av_saml
   ```

   Pour plus de détails sur la commande, voir https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction

Configurer une appliance NetScaler en tant que SP SAML à l'aide de l'interface graphique

1. Accédez à **Sécurité>Stratégies AAA->Authentification>Stratégies de base>SAML**.
2. Sélectionnez l'onglet **Serveurs**, cliquez sur **Ajouter**, entrez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   Descriptions des paramètres :

   - Nom : nom du serveur.
   - URL de redirection : URL à partir de laquelle les utilisateurs s'authentifient. Certains IdP ont des URL spéciales qui ne sont pas accessibles à moins qu'ils ne soient configurés sur une configuration SAML.
   - URL de déconnexion unique : URL spécifiée pour que NetScaler puisse reconnaître quand renvoyer le client à l'IdP pour terminer le processus de déconnexion. Nous ne l'utiliserons pas dans ce simple déploiement.
   - Liaison SAML : mécanisme utilisé pour transporter les messages du demandeur et du répondeur SAML entre le SP et l'IdP. Lorsque NetScaler agit en tant que SP, il prend en charge les liaisons Post, Redirect et Artifact. La méthode de liaison par défaut est POST.

     > **Remarque :**
     >
     > pour la liaison d'artefacts, le mécanisme de transport sur le SP et l'IdP doit être le même.

- Liaison de déconnexion : spécifie le mécanisme de transport des messages de déconnexion SAML. Le mécanisme de liaison par défaut est Post.
- Nom du certificat IdP : certificat IDPCert (Base64) présent sous le certificat de signature SAML.
- Champ utilisateur : section du formulaire d'authentification SAML de l'IdP qui contient le nom d'utilisateur que SP doit extraire si nécessaire.
- Nom du certificat de signature : sélectionnez le certificat SP SAML (avec clé privée) que NetScaler utilise pour signer les demandes d'authentification auprès de l'IdP. Le même certificat (sans clé privée) doit être importé sur l'IdP, de sorte que l'IdP puisse vérifier la signature de la demande d'authentification. La plupart des IDP n'ont pas besoin du nom du certificat de signature.
- IssuerName - Identifiant. ID unique spécifié à la fois sur le SP et sur l'IdP pour aider à identifier le fournisseur de services l'un par rapport à l'autre.
- Rejeter l'assertion non signée : option que vous pouvez spécifier si vous souhaitez que les assertions de l'IdP soient signées. L'option par défaut est Activé.
  - ACTIVÉ : Rejette les assertions sans signature
  - STRICT : garantit que la réponse et l'assertion sont signées
  - OFF : autorise les assertions non signées
- Audience - Audience pour laquelle une assertion envoyée par IdP est applicable. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente le fournisseur de services.
- Algorithme de signature : algorithme à utiliser pour signer/vérifier les transactions SAML. La valeur par défaut est RSA-SHA256.
- Méthode de synthèse : algorithme à utiliser pour calculer/vérifier le condensé des transactions SAML. La valeur par défaut est SHA256.
- Groupe d'authentification par défaut : groupe par défaut choisi lorsque l'authentification réussit, en plus des groupes extraits.
- Champ de nom de groupe : nom de la balise dans une assertion qui contient des groupes d'utilisateurs.
- Temps d'inclinaison (minutes) : cette option spécifie le décalage d'horloge en minutes autorisé par le fournisseur de services NetScaler sur une assertion entrante. Par exemple, si vous définissez le temps d'inclinaison sur 10 minutes à 16 h, l'assertion SAML est valide de 15 h 50 à 16 h 10, soit 20 minutes au total. La durée d'inclinaison par défaut est de 5 minutes.

3. Créez une politique SAML correspondante.

Accédez à **Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Stratégie**, puis cliquez sur **Ajouter**.

Sur la page **Créer une stratégie SAML d'authentification**, fournissez les informations suivantes :

- Nom : spécifiez le nom de la stratégie SAML.
- Type d'action : sélectionnez **SAML** comme type d'action d'authentification.
- Action : sélectionnez le profil de serveur SAML auquel lier la stratégie SAML.
- Expression : affiche le nom de la règle ou de l'expression utilisée par la stratégie SAML pour déterminer si l'utilisateur doit s'authentifier auprès du serveur SAML. Dans la zone de texte, définissez la valeur « rule = true » pour que la politique SAML prenne effet et que l'action SAML correspondante soit exécutée.

4. Liez la stratégie SAML au serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**et associez la stratégie SAML au serveur virtuel d'authentification.

5. Associez le serveur d'authentification au serveur virtuel de gestion du trafic approprié.

   Accédez à **Gestion du trafic > Équilibrage de charge** (ou **Commutation de contenu**) > **Serveurs virtuels**, sélectionnez le serveur virtuel et associez le serveur virtuel d'authentification à celui-ci.

NetScaler en tant qu'IdP SAML

June 20, 2023

L'IdP SAML (Identity Provider) est une entité SAML déployée sur le réseau client. L'IdP reçoit les demandes du SP SAML et redirige les utilisateurs vers une page d'ouverture de session, où ils doivent entrer leurs informations d'identification. L'IdP authentifie ces informations d'identification auprès d'Active Directory (serveur d'authentification externe, tel que LDAP), puis génère une assertion SAML qui est envoyée au SP.

Le SP valide le jeton, et l'utilisateur est ensuite autorisé à accéder à l'application protégée demandée.

Lorsque l'appliance NetScaler est configurée en tant qu'IdP, toutes les demandes sont reçues par un serveur virtuel d'authentification associé au profil IdP SAML pertinent.

> **Remarque**
>
> Une appliance NetScaler peut être utilisée comme IdP dans un déploiement où le SP SAML est configuré soit sur l'appliance, soit sur n'importe quel SP SAML externe.

Lorsqu'elle est utilisée en tant qu'IdP SAML, une appliance NetScaler :

- Prend en charge toutes les méthodes d'authentification prises en charge pour les ouvertures de session traditionnelles.
- Signe numériquement les assertions.
- Prend en charge l'authentification à un ou deux facteurs. SAML ne doit pas être configuré en tant que mécanisme d'authentification secondaire.
- Peut chiffrer les assertions à l'aide de la clé publique du SP SAML. Cela est recommandé lorsque l'assertion inclut des informations sensibles.
- Peut être configuré pour accepter uniquement les demandes signées numériquement provenant du SP SAML.
- Peut se connecter à l'IdP SAML à l'aide des mécanismes d'authentification basés sur 401 suivants : Negotiate, NTLM et Certificate.
- Peut être configuré pour envoyer 16 attributs en plus de l'attribut NameID. Les attributs doivent être extraits du serveur d'authentification approprié. Pour chacun d'eux, vous pouvez spécifier le nom, l'expression, le format et un nom convivial dans le profil IdP SAML.
- Si l'appliance NetScaler est configurée en tant qu'IdP SAML pour plusieurs SP SAML, un utilisateur peut accéder aux applications des différents SP sans s'authentifier explicitement à chaque fois. L'appliance NetScaler crée un cookie de session pour la première authentification, et chaque demande suivante utilise ce cookie pour l'authentification.
- Peut envoyer des attributs à plusieurs valeurs dans une assertion SAML.
- Prend en charge les liaisons de publication et de redirection. La prise en charge de la liaison aux artefacts est introduite dans la version 13.0 Build 36.27 de NetScaler.
- Peut spécifier la validité d'une assertion SAML.

  Si l'heure système sur NetScaler SAML IdP et sur le SP SAML homologue n'est pas synchronisée, les messages peuvent être invalidés par l'une ou l'autre des parties. Pour éviter de tels cas, vous pouvez désormais configurer la durée pendant laquelle les assertions sont valides.

  Cette durée, appelée « temps d'inclinaison », indique le nombre de minutes pendant lesquelles le message doit être accepté. Le temps d'inclinaison peut être configuré sur le SP SAML et le fournisseur d'identité SAML.
- Peut être configuré pour diffuser des assertions uniquement aux SP SAML préconfigurés sur l'IdP ou approuvés par celui-ci. Pour cette configuration, l'IdP SAML doit avoir l'ID de fournisseur de services (ou le nom de l'émetteur) des SP SAML concernés.

  > **Remarque**
  >
  > – Avant de poursuivre, assurez-vous que vous disposez d'une stratégie d'authentification liée à un serveur virtuel d'authentification LDAP.

> – Pour plus d'informations sur la façon de configurer une action LDAP pour récupérer les attributs requis, consultez la section Prise en charge des attributs nom-valeur pour l'authentification LDAP.

Configurer une appliance NetScaler en tant qu'IdP SAML à l'aide de l'interface de ligne de commande

1. Créez un profil IDP SAML.

   Exemple

   Ajout de l'appliance NetScaler en tant qu'IdP avec SiteMinder en tant que SP.

   ```
   add authentication samlIdPProfile samlIDPProf1 -samlSPCertName siteminder
   -cert -encryptAssertion ON -metadataUrl https://samlidp.example.com/
   metadata -samlIdPCertName ns-cert -assertionConsumerServiceURL https
   ://example.com/cgi/samlauth -rejectUnsignedRequests ON -signatureAlg
   RSA-SHA256 -digestMethod SHA256 -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.
   REGEX_MATCH(re##^https://example\.com/cgi/samlauth$##)
   ```

2. Configurez le profil IDP SAML. Dans l'exemple suivant, la session IdP contient l'attribut « User-PrincipalName ».

   ```
   set samlidPProfile SAML-IDP-Profile -Attribute1 "userPrincipalName"-
   Attribute1Expr "AAA.USER.ATTRIBUTE(\"userPrincipalName\")"
   ```

   Points à noter

   - Dans le profil IdP SAML, configurez **AcSurlRule** qui prend une expression de la liste des URL de fournisseurs de services applicables à cet IdP. Cette expression dépend du SP utilisé. Si NetScaler est configuré en tant que SP, l'URL ACS est. `https://<SP-domain_name>/cgi/samlauth` Il est recommandé d'inclure une URL complète dans l'expression à des fins de correspondance.
   - Si vous souhaitez que l'IdP SAML n'autorise qu'une seule URL ACS, utilisez la commande suivante :

     L'exemple de CLI suivant utilise `https://testlb.aaa.local` l'URL ACS :

     ```
     set samlidpprofile SAML_IDP_profile -acsurlrule  "AAA.LOGIN.
        SAML_REQ_ACS_URL.eq("https://testlb.aaa.local")"
     <!--NeedCopy-->
     ```

   - Si vous souhaitez que l'IdP SAML corresponde à l'URL ACS avec une expression régulière, utilisez l'expression suivante :


```
-acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.REGEX_MATCH(re##^https://
example.com/cgi/samlauth$##)
```

L'expression ci-dessus garantit que l'URL ACS correspond à `https://example.com/cgi/samlauth`. Le signe « ^ » au début de l'expression régulière garantit que NetScaler n'autorise rien avant « https ». Le signe « $ » à la fin de l'expression régulière garantit que NetScaler n'autorise rien après « samlauth ».

Si l'expression est `-acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.REGEX_MATCH(re##https://example.com/cgi/##)`, l'IdP SAML autorise n'importe quelle URL ACS, comme indiqué dans les exemples ci-dessous :

- `https://example.com/cgi/samlauth`
- `abcdhttps://example.com/cgi/xyz`
- `https://example.com/cgi/abcde`

- SAML prend uniquement en charge le certificat RSA. Les autres certificats tels que HSM et FIPS ne sont pas pris en charge.

Pour plus de détails sur la commande, reportez-vous https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction aux sections et https://support.citrix.com/article/CTX316577.

- Si l'URL de déconnexion de l'IdP est différente de l'URL de redirection et que l'utilisateur reste sur la page de connexion NetScaler pendant plus de 2 minutes, une erreur du serveur`HTTP/1.1 Internal Server Error 43549` apparaît lorsque l'utilisateur tente de s'authentifier. Les journaux NetScaler affichent un message indiquant que l'URL de redirection après déconnexion entrante ne figure pas dans les URL de redirection de déconnexion autorisées pour l'utilisateur.

  Pour résoudre ce problème, liez le jeu de modèles comme indiqué dans l'exemple ci-dessous :

  ```
  bind patset ns_aaa_oauthidp_logout_redirect_uris "https://FQDN and
  path to the logout url"
  ```

3. Configurez la stratégie d'authentification SAML et associez le profil IdP SAML comme action de la stratégie.

   ```
   add authentication samlIdPPolicy samlIDPPol1 -rule true -action samlIDPProf1
   ```

> **Remarque :**
>
> Si le nom de la stratégie comporte un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « ma stratégie » ou « ma stratégie »).

4. Liez la stratégie au serveur virtuel d'authentification.

   ```
   bind authentication vserver saml-auth-vserver -policy samlIDPPol1 -
   priority 100
   ```

   Pour plus de détails sur la commande, reportez-vous à la section https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlIdPProfile.

Configurer une appliance NetScaler en tant qu'IdP SAML à l'aide de l'interface graphique

1. Configurez un profil IdP SAML. Ce profil est utilisé pour vérifier les demandes d'authentification entrantes provenant du SP, et pour créer et signer l'assertion avant de l'envoyer au SP.

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Stratégies avancées d'authentification > Stratégies IDP SAML**.

   Sélectionnez **Serveurs**, cliquez sur **Ajouter**, entrez les valeurs des paramètres suivants, puis cliquez sur **Créer**.

   Descriptions des paramètres :

   - Nom : nom du nouveau profil d'authentification unique SAML.
   - Exporter les métadonnées IDP SAML : cliquez sur ce lien si vous souhaitez exporter les métadonnées du profil IDP SAML vers un serveur virtuel VPN NetScaler Gateway.
   - Importer des métadonnées : cette option importe les métadonnées IDP SAML. Cette option est activée par défaut.
   - URL du service client de l'assertion : URL à laquelle l'assertion doit être envoyée.
   - URL de déconnexion du fournisseur de services : point de terminaison du SP auquel les messages de déconnexion doivent être envoyés.
   - Liaison de déconnexion : spécifie le mécanisme de transport des messages de déconnexion SAML. Les options disponibles sont POST et REDIRECT.
   - URL des métadonnées SAML SP : URL utilisée pour obtenir les métadonnées IDP SAML.

     > **Remarque :**
     >
     > Lorsque l'URL des métadonnées du SP SAML est configurée, les paramètres suivants proviennent du profil IDP SAML et sont remplis automatiquement dans la configuration du SP SAML :
     >
     > - URL du service client Assertion
     > - URL de déconnexion du fournisseur de services

  - Nom du certificat SP
  - Liaison de déconnexion
  - Liaison SAML
  - Signer une assertion

- Intervalle d'actualisation des métadonnées (minutes) : intervalle de temps (en minutes) pour récupérer les métadonnées à partir de l'URL de métadonnées spécifiée. L'intervalle de temps par défaut est de 3 600 minutes.
- Règle d'URL Assertion Consumer Service : expression qui définit les URL ACS autorisées provenant d'un SP SAML. En d'autres termes, il permet de répertorier les URL ACS pour empêcher les attaques qui insèrent des URL ACS non autorisées dans les requêtes SAML.
- URL du service client Assertion : URL vers laquelle l'utilisateur authentifié est redirigé.
- Nom du certificat IdP : paire de clés de certificat utilisée pour la page d'authentification.
- Nom du certificat SP - Certificat du fournisseur de services dans ce scénario, la clé n'est pas requise pour cela.
- Signer l'assertion : option permettant de signer l'assertion et la réponse lors de la redirection du client vers le fournisseur de services.
- Nom de l'émetteur : valeur de chaîne incluse dans l'assertion SAML émise par l'IdP.
- ID du fournisseur de services : identifiant unique spécifié sur le SP pour aider à identifier le fournisseur de services. L'identifiant peut être n'importe quoi et n'est pas nécessairement une URL. Mais l'identifiant doit être le même sur les profils SP et IdP.
- Groupe d'authentification par défaut : groupe par défaut choisi lorsqu'une authentification réussit, en plus des groupes extraits. Ce groupe est utile pour les administrateurs qui utilisent le flux nFactor pour décider des configurations appropriées pour le relais. Par exemple, lorsque vous configurez une stratégie d'authentification, vous pouvez spécifier le nom de groupe par défaut dans le cadre de l'expression suivante :

  ```
  AAA.USER.IS_MEMBER_OF("Default Authentication Group name").
  ```

- Refuser les demandes non signées : option que vous pouvez spécifier pour garantir que seules les assertions signées avec le certificat SP sont acceptées.
- Public : public auquel l'assertion est envoyée par l'IdP. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente le SP.
- Temps d'inclinaison (minutes) - Durée d'inclinaison (minutes) : cette option spécifie le décalage d'horloge en minutes autorisé par le fournisseur de services NetScaler sur une assertion entrante. Par exemple, si vous définissez le temps d'inclinaison sur 10 minutes à 16 h, l'assertion SAML est valide de 15 h 50 à 16 h 10, soit 20 minutes au total. La durée d'inclinaison par défaut est de 5 minutes.

- Format NAME ID : format de l'identifiant de nom envoyé dans l'assertion.
- Expression d'identifiant de nom : expression évaluée pour obtenir l'identifiant de nom à envoyer dans l'assertion.
- Signer une assertion : option permettant de signer des parties de l'assertion envoyée par l'IdP. Les options disponibles sont Aucune, Assertion, Réponse ou les deux.
- Algorithme de signature - Algorithme utilisé pour signer et vérifier les assertions entre l'IdP et le SP. Il doit être identique sur le profil IdP et le profil SP.
- Méthode Digest - Algorithme utilisé pour vérifier l'intégrité des assertions entre l'IdP et le SP, il doit être identique sur le profil IdP et le profil SP.
- Liaison SAML : mécanisme utilisé pour transporter les messages du demandeur et du répondeur SAML entre le SP et l'IdP. Lorsque NetScaler agit en tant que SP, il prend en charge les liaisons Post, Redirect et Artifact. La méthode de liaison par défaut est POST. Associez la stratégie IdP SAML à un serveur virtuel d'authentification. Pour la liaison aux artefacts, le mécanisme de transport sur le SP et l'IdP doit être le même.
- Attribut 1 : nom de l'attribut dans l'assertion SAML dont la valeur doit être extraite et stockée en tant qu'attribut1. Un schéma similaire s'applique également aux autres attributs.
- Attribute1Expr : expression évaluée pour obtenir la valeur de l'attribut 1.
- Attribute1FriendlyName : nom de l'attribut 1 qui doit être envoyé dans l'assertion SAML.
- Attribute1Format : format de l'attribut 1 à envoyer dans l'assertion SAML.

2. Configurez la stratégie d'authentification SAML et associez le profil IdP SAML comme action de la stratégie.

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Stratégies avancées d'authentification > Stratégies IDP SAML**.

   Sélectionnez **Stratégies**, cliquez sur **Ajouter**, entrez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   Descriptions des paramètres :

   - Nom : nom de la stratégie d'authentification SAML IdP.
   - Action : nom du profil IDP SAML à appliquer aux demandes ou aux connexions qui correspondent à cette stratégie.
   - Action de consignation : nom de l'action du journal des messages à utiliser lorsqu'une demande correspond à cette stratégie. Sélectionnez une action de journal dans la liste déroulante ou créez une action de journal en cliquant sur Ajouter.

- Action à résultat non défini : action à exécuter si le résultat de l'évaluation de la stratégie n'est pas défini. Un événement non défini indique une condition d'erreur interne. Seules les actions intégrées peuvent être utilisées.
- Commentaires - Tout commentaire visant à préserver les informations relatives à cette stratégie.

3. Associez la stratégie IdP SAML à un serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**et liez la stratégie IDP SAML au serveur virtuel d'authentification.

Configuration de l'authentification unique SAML

May 5, 2023

Pour fournir des fonctionnalités d'authentification unique aux applications hébergées sur le fournisseur de services, vous pouvez configurer l'authentification unique SAML sur le SP SAML.

Configuration de l'authentification unique SAML à l'aide de l'interface de ligne de commande

1. Configurez le profil SSO SAML.

   Exemple

   Dans la commande suivante, Exemple est le serveur virtuel d'équilibrage de charge doté d'un lien Web depuis le portail SharePoint. NSSP.Example.com est le serveur virtuel de gestion du trafic qui équilibrent la charge du serveur SharePoint.

```
1  add tm samlSSOProfile tm-saml-sso -samlSigningCertName nssp -
      assertionConsumerServiceURL "https://nssp2.example.com/cgi/
      samlauth" -relaystateRule "\\"https://nssp2.example.com/
      samlsso.html\\"" -sendPassword ON -samlIssuerName nssp.example
      .com
2  <!--NeedCopy-->
```

2. Associez le profil SSO SAML à l'action de trafic.

   Exemple

   La commande suivante active l'accès SSO et lie le profil SSO SAML créé ci-dessus à une action de trafic.


```
add tm trafficAction html_act -SSO ON -samlSSOProfile tm-saml-sso
<!--NeedCopy-->
```

3. Configurez la stratégie de trafic qui spécifie quand l'action doit être exécutée.

   Exemple

   La commande suivante associe l'action de trafic à une stratégie de trafic.

```
add tm trafficPolicy html_pol "HTTP.REQ.URL.CONTAINS(\\"abc.html\\
    ")" html_act
<!--NeedCopy-->
```

4. Liez la stratégie de trafic créée précédemment à un serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu). Alternativement, la stratégie de trafic peut être associée globalement.

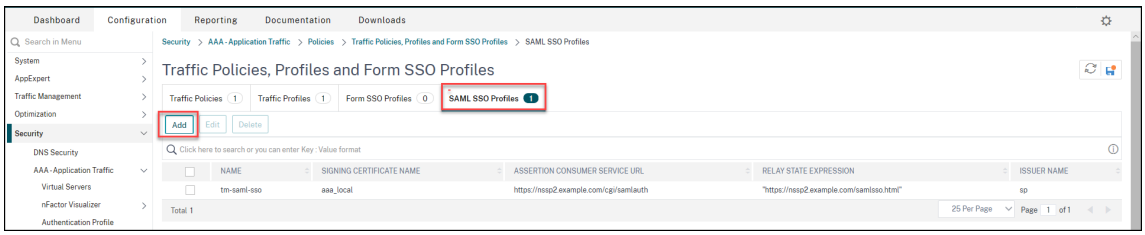
   > **Remarque**
   >
   > Ce serveur virtuel de gestion du trafic doit être associé au serveur virtuel d'authentification approprié associé à l'action SAML.

```
bind lb vserver lb1_ssl -policyName html_pol -priority 100 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Configuration de l'authentification unique SAML à l'aide de l'interface graphique

Pour configurer l'authentification unique SAML, vous devez définir le profil SSO SAML, le profil de trafic et la politique de trafic, puis lier la politique de trafic à un serveur virtuel de gestion du trafic ou globalement à l'appliance NetScaler.

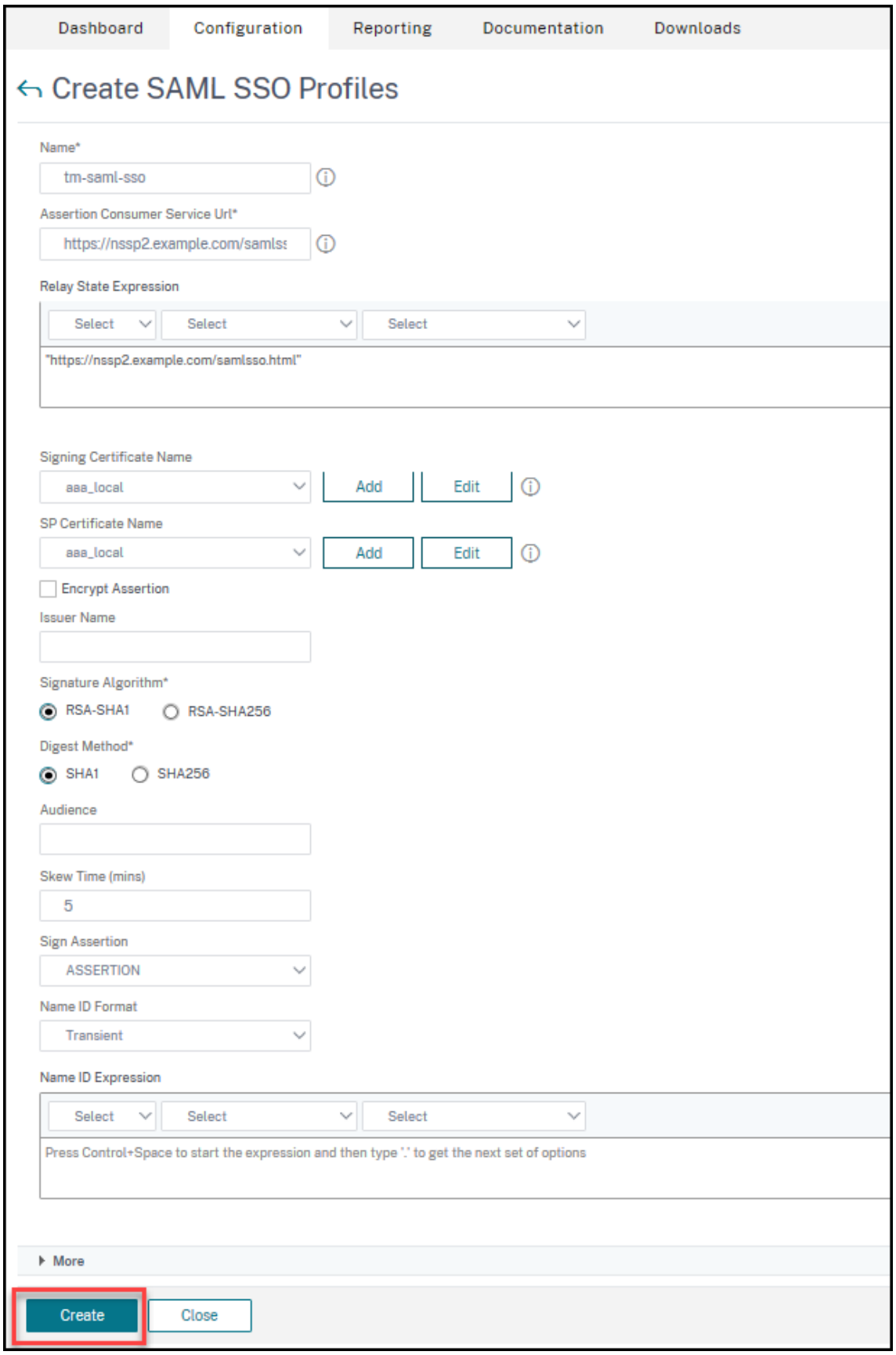
1. Accédez à **Sécurité > Trafic des applications AAA > Stratégies > Trafic > Profils SSO SAML**, puis cliquez sur **Ajouter**.



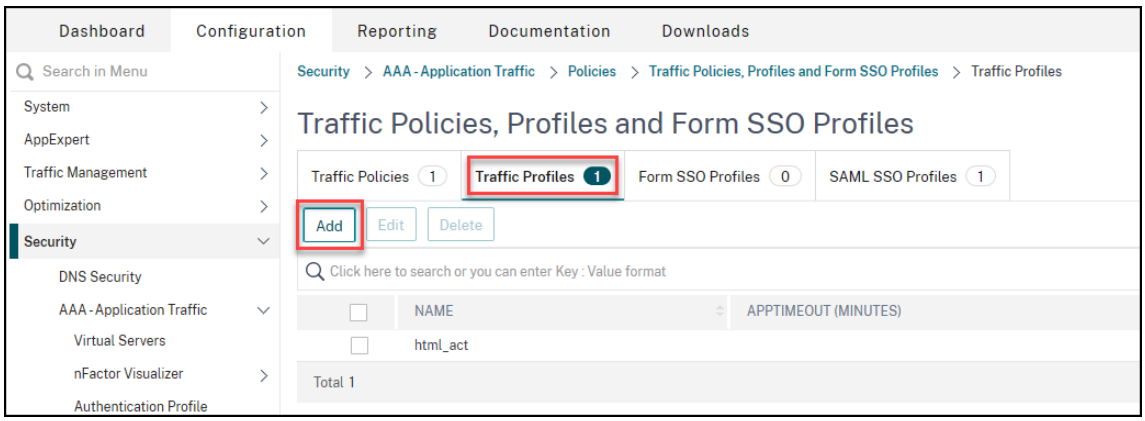
2. Sur la page **Créer des profils SSO SAML**, entrez les valeurs des champs suivants, puis cliquez sur **Créer**.

   - Nom : nom du profil SSO SAML

- Assertion Consumer Service Url - URL à laquelle l'assertion doit être envoyée
- Nom du certificat de signature : nom du certificat SSL utilisé pour signer une assertion
- Nom du certificat SP : nom du certificat SSL d'un homologue/destinataire utilisant lequel l'assertion est chiffrée
- Nom de l'émetteur : nom à utiliser dans les demandes envoyées par NetScaler à l'IdP pour identifier NetScaler de manière unique
- Algorithme de signature - Algorithme à utiliser pour signe/vérifier les transactions SAML
- Digest Method - Algorithme à utiliser pour calculer/vérifier le résumé pour les transactions SAML
- Audience - Audience pour laquelle une assertion envoyée par IdP est applicable. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente un fournisseur de services.
- Audience - Audience pour laquelle une assertion envoyée par IdP est applicable. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente un fournisseur de services.
- Temps d'inclinaison (minutes) : nombre de minutes de chaque côté de l'heure actuelle pendant lesquelles l'assertion serait valide
- Signer l'assertion : option permettant de signer des parties d'une assertion lorsque NetScaler IdP en envoie une. En fonction de la sélection de l'utilisateur, l'assertion ou la réponse ou les deux ou aucun ne peut être signé.
- Format d'ID de nom : format de l'identificateur de nom envoyé dans l'assertion
- Name ID Expression : expression évaluée pour obtenir NameIdentifier à envoyer dans l'assertion

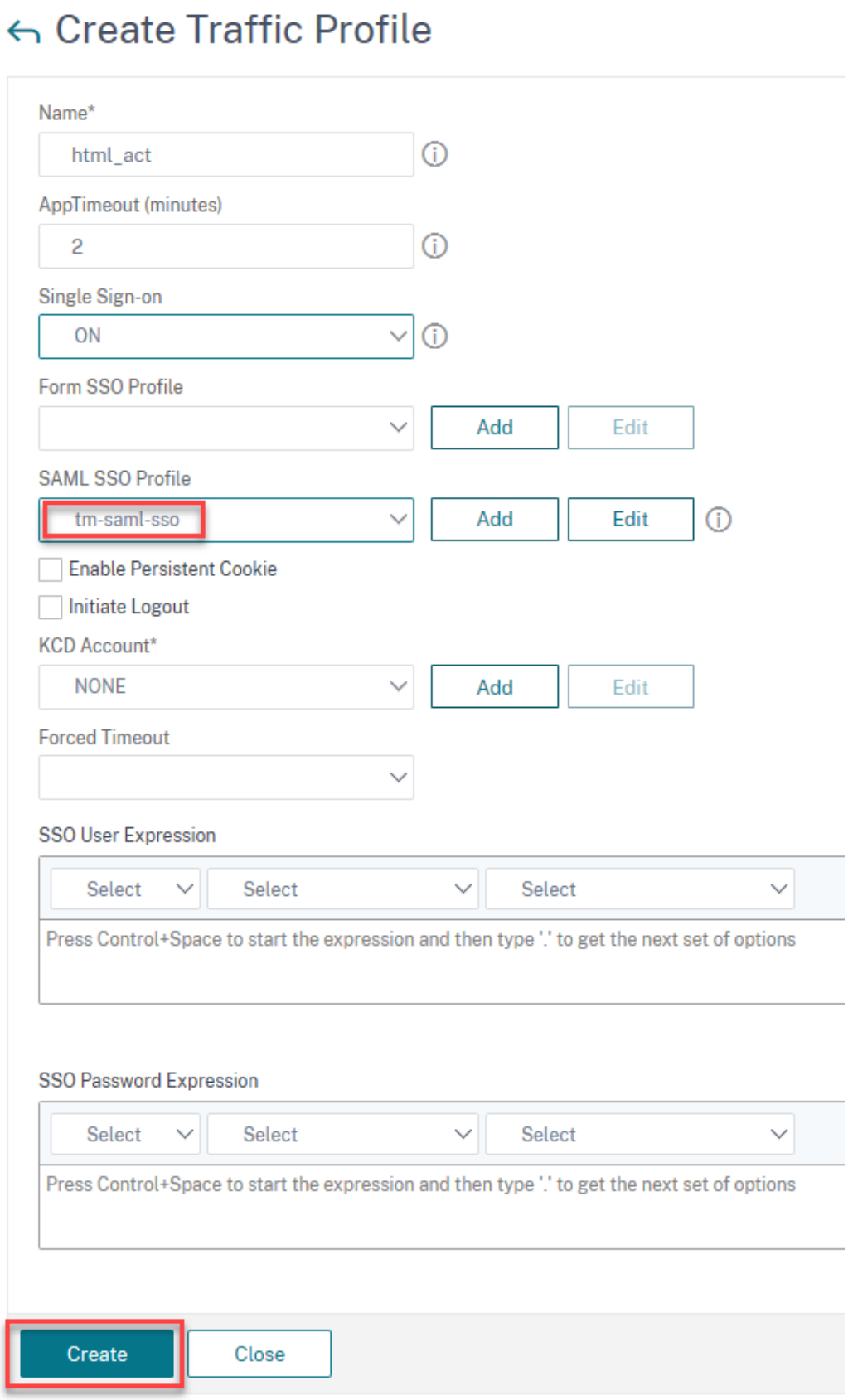


3. Accédez à **Sécurité > Trafic des applications AAA > Stratégies> Trafic > Profils de trafic**, puis cliquez sur **Ajouter**.

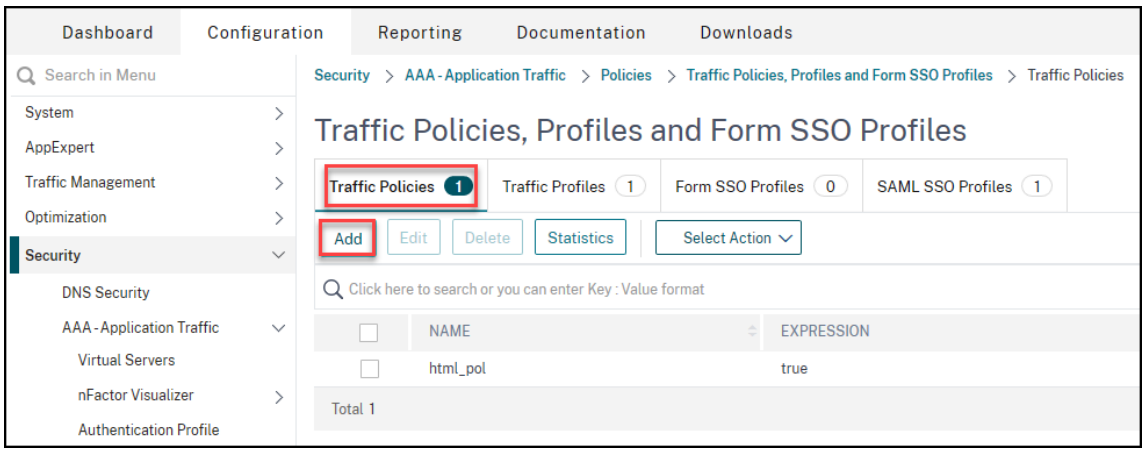


4. Sur la page **Créer un profil de trafic**, entrez des valeurs pour les champs suivants, puis cliquez sur **Créer**.

   - Nom : nom de l'action de trafic.
   - AppTimeout (minutes) - Intervalle de temps, en minutes, d'inactivité de l'utilisateur après lequel la connexion est fermée.
   - Single Sign-On - Sélectionnez ON
   - Profil SSO SAML - Sélectionnez le profil SSSO SAML créé
   - Compte KCD - Nom de compte de délégation contrainte Kerberos
   - SSO User Expression : expression évaluée pour obtenir le nom d'utilisateur pour Single-Signon
   - Expression de mot de passe SSO : expression évaluée pour obtenir le mot de passe pour SingleSignon

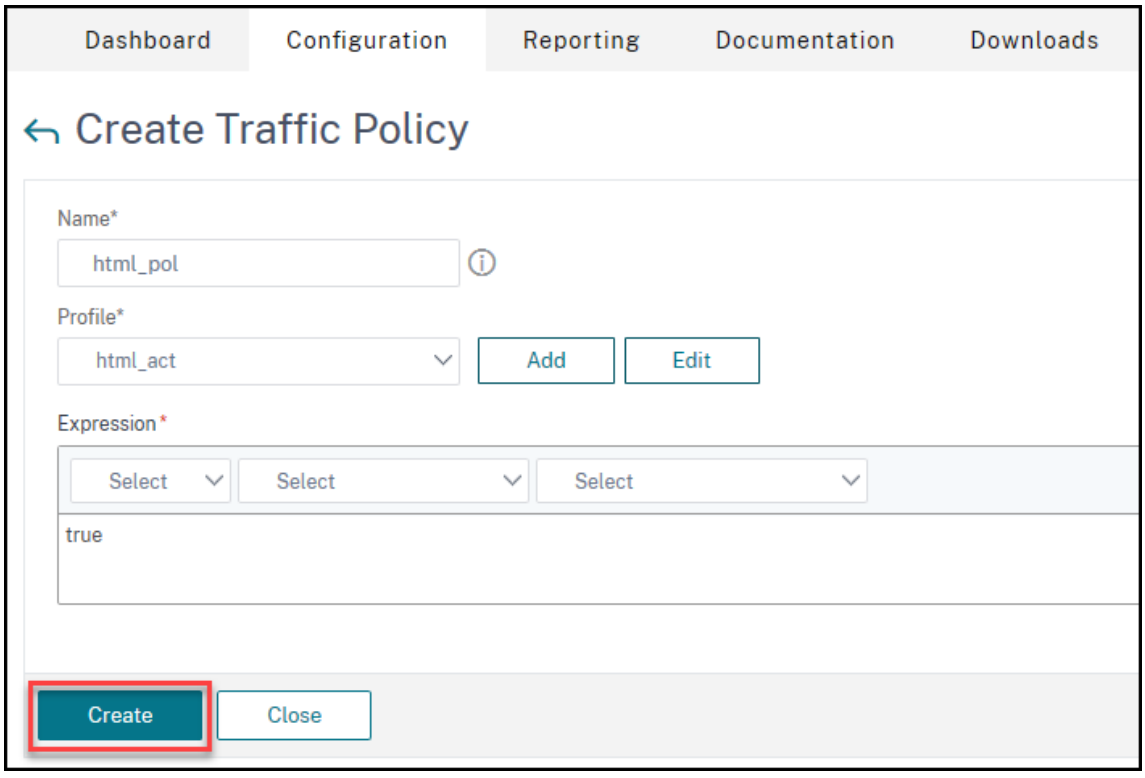


5. Accédez à **Sécurité > Trafic des applications AAA > Stratégies > Trafic > Stratégies de trafic**, puis cliquez sur **Ajouter**.

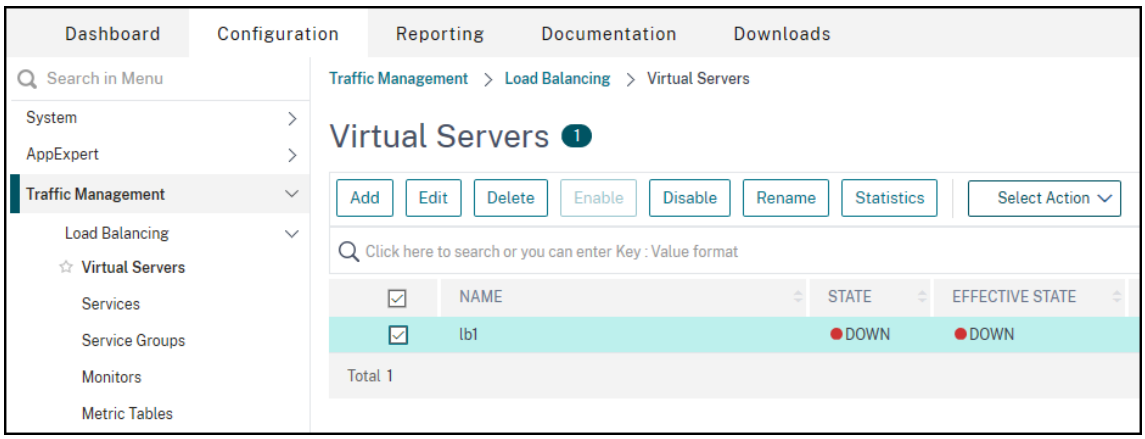


6. Sur la page **Créer une stratégie de trafic**, entrez les valeurs suivantes, puis cliquez sur **Créer**.

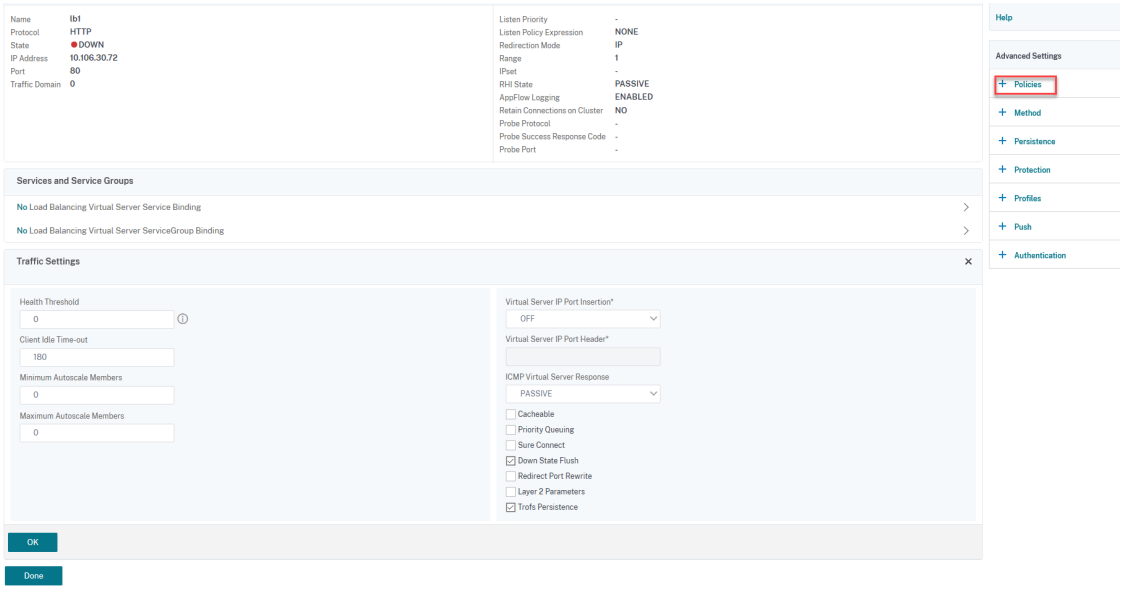
   - Nom : nom de la stratégie de trafic à créer.
   - Profil : sélectionnez le profil de trafic créé
   - Expression — Expression de stratégie avancée utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, true.



7. Pour lier la stratégie de trafic à un serveur virtuel de gestion du trafic, sélectionnez un serveur virtuel.



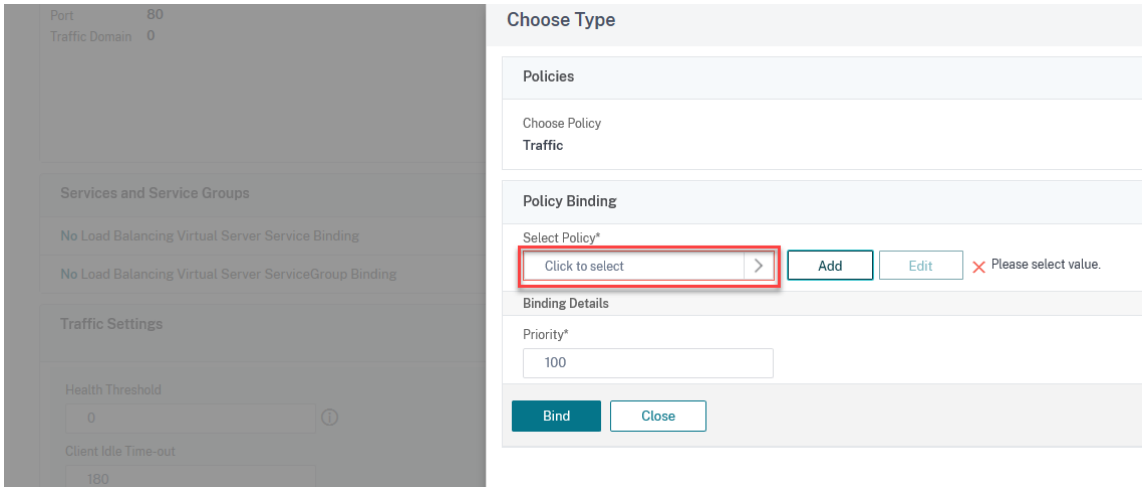
8. Cliquez sur **Stratégies**.



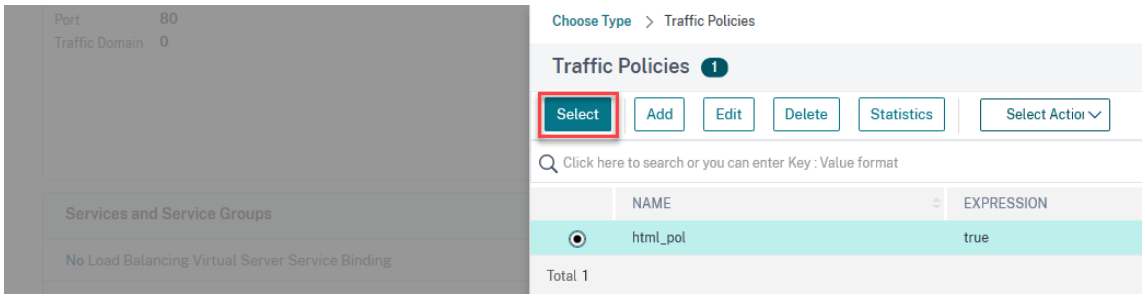
9. Sélectionnez **Trafic** dans le champ **Choisir une stratégie** et sélectionnez **Demander** dans le champ **Choisir un type**, puis cliquez sur **Continuer**.

   ![Cliquez ici pour ajouter une stratégie(/en-us/citrix-adc/media/saml-9.png)

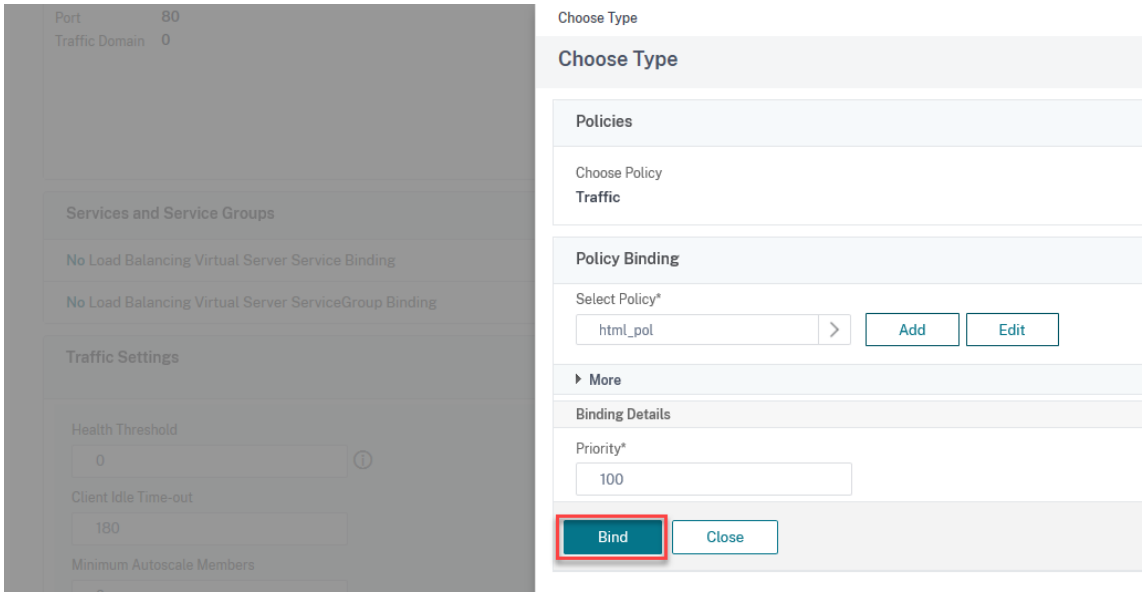
10. Sous **le champ Sélectionner une stratégie**, cliquez pour sélectionner le trafic créé.



11. Cliquez sur **Sélectionner**.



12. Cliquez sur **Lier pour lier** la stratégie de trafic au serveur virtuel.



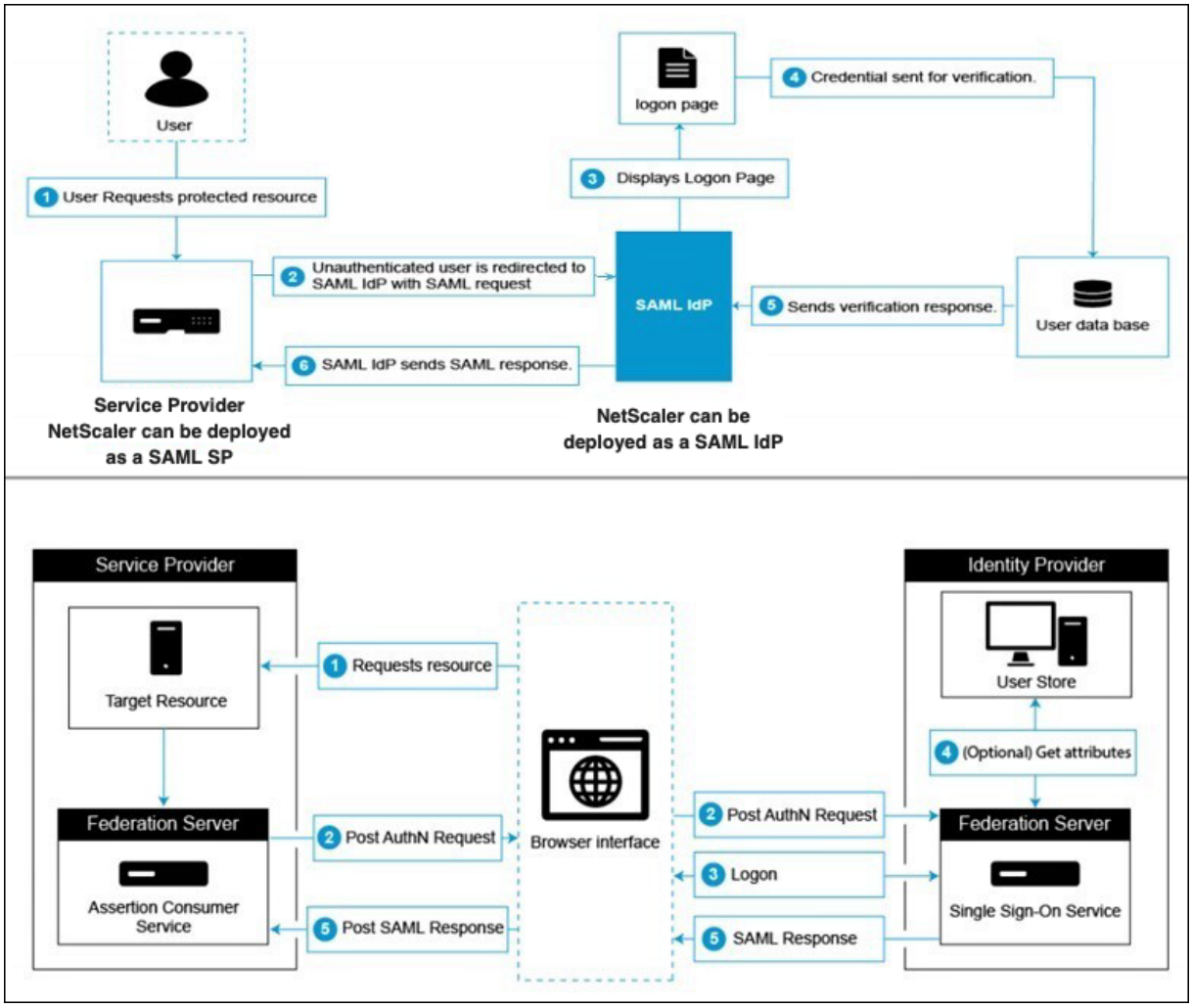
Configurer Azure AD en tant qu'IdP SAML et NetScaler en tant que SP SAML

May 5, 2023

Le fournisseur de services SAML (SAML SP) est une entité SAML déployée par le fournisseur de services. Lorsqu'un utilisateur tente d'accéder à une application protégée, le SP évalue la demande du client. Si le client n'est pas authentifié (ne possède pas de cookie NSC_TMAA ou NSC_TMAS valide), le SP redirige la demande vers le fournisseur d'identité SAML (IdP). Le SP valide également les assertions SAML reçues de l'IdP.

Le fournisseur d'identité SAML (IDP SAML) est une entité SAML déployée sur le réseau du client. L'IdP reçoit les demandes du SP SAML et redirige les utilisateurs vers une page d'ouverture de session, où ils doivent entrer leurs informations d'identification. L'IdP authentifie ces informations d'identification auprès de l'annuaire des utilisateurs (serveur d'authentification externe, tel que LDAP), puis génère une assertion SAML qui est envoyée au SP. Le SP valide le jeton, et l'utilisateur est ensuite autorisé à accéder à l'application protégée demandée.

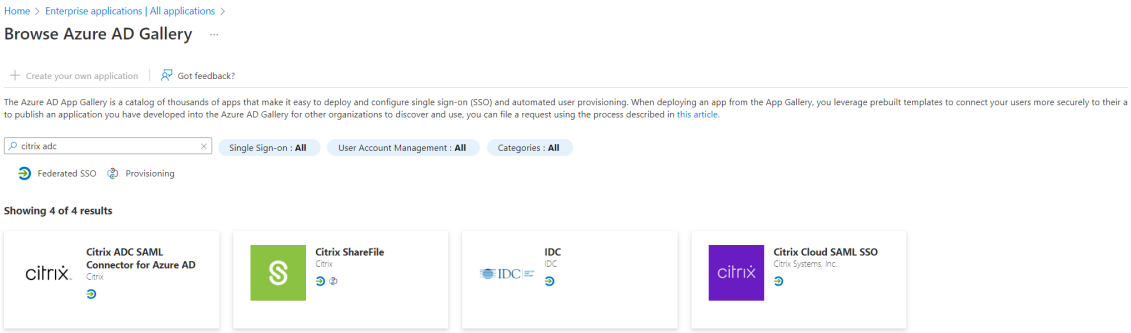
Le diagramme suivant illustre le mécanisme d'authentification SAML.



Configurations côté Azure AD

Configurez les paramètres d'authentification unique :

1. Sur le portail Azure, cliquez sur **Azure Active Directory**.
2. Dans la section **Gérer** du volet de navigation, cliquez sur **Applications d'entreprise**. Un échantillon aléatoire des applications de votre locataire Azure AD apparaît.
3. Dans la barre de recherche, saisissez **NetScaler SAML Connector pour Azure AD**.



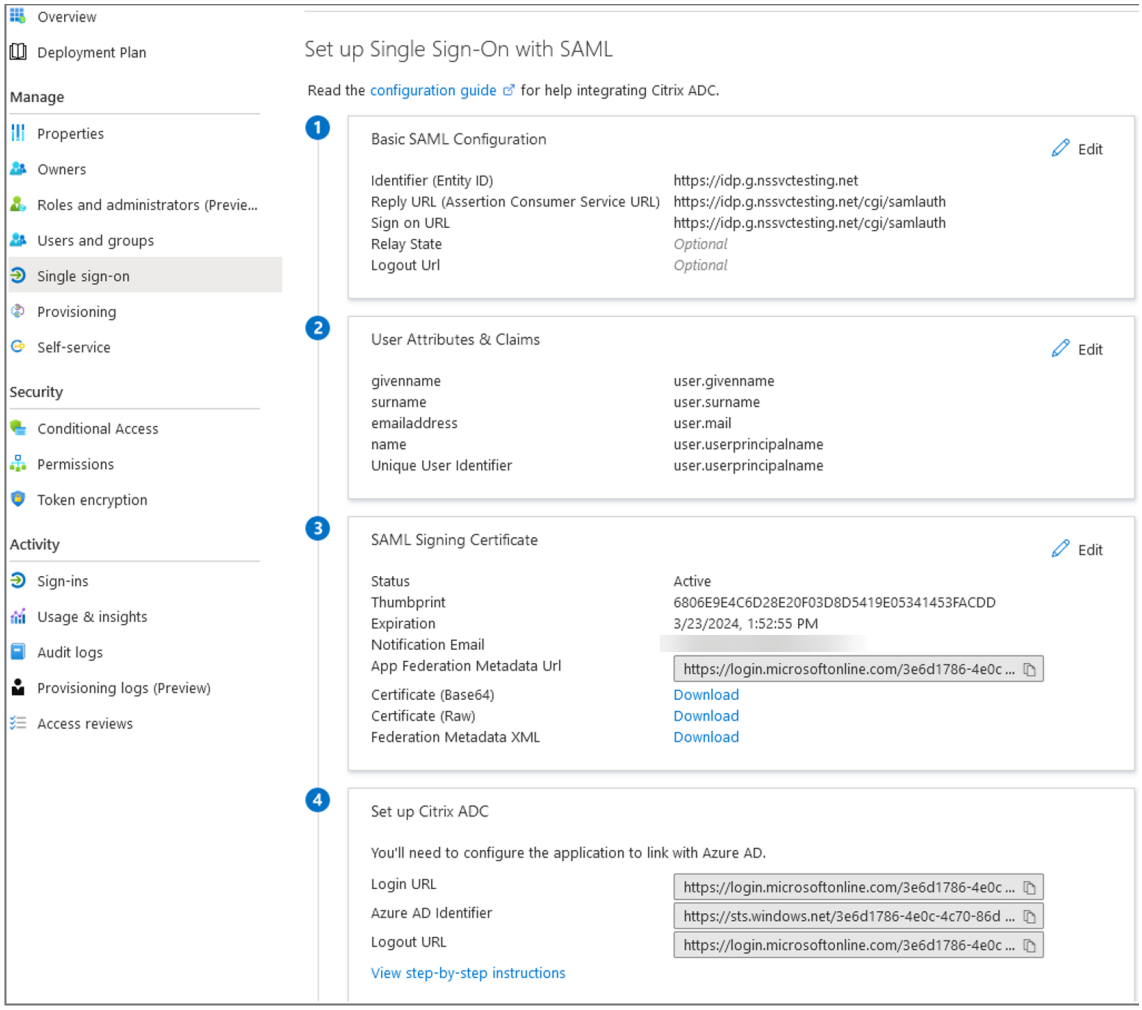
4. Dans la section **Gérer**, sélectionnez **Single Sign-On**.
5. Sélectionnez **SAML** pour configurer l'authentification unique. La page **Configurer l'authentification unique avec SAML - Aperçu** apparaît. Ici, Azure agit en tant qu'IdP SAML.
6. **Configurez les options SAML de base :**

   Identifiant (ID d'entité) : requis pour certaines applications. Identifie de manière unique l'application pour laquelle l'authentification unique est en cours de configuration. Azure AD envoie l'identificateur à l'application en tant que paramètre d'audience du jeton SAML. L'application est censée le valider. Cette valeur apparaît également sous la forme d'ID d'entité dans toutes les métadonnées SAML fournies par l'application.

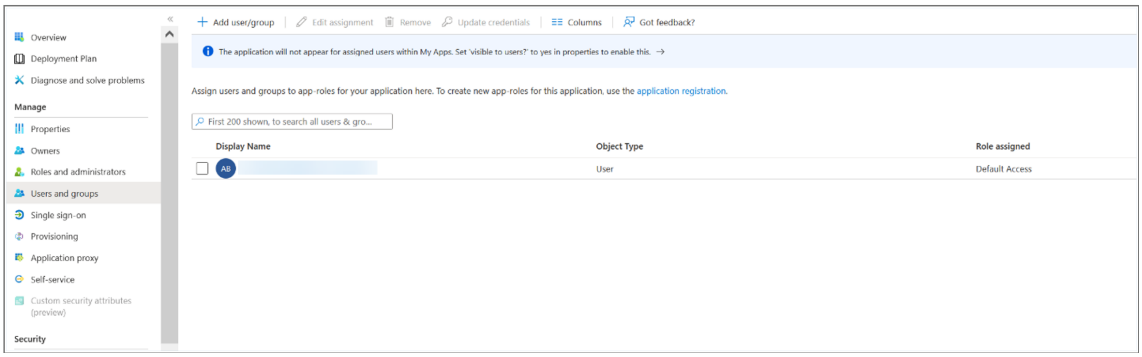
   URL de réponse - Obligatoire. Spécifie l'endroit où l'application s'attend à recevoir le jeton SAML. L'URL de réponse est également appelée URL ASSERTION Consumer Service (ACS). Spécifiez l'URL de réponse au format `http(s)://<SP_URL>/cgi/samlauth`.

   URL de connexion - Lorsqu'un utilisateur ouvre cette URL, le fournisseur de services redirige vers Azure AD pour s'authentifier et se connecter à l'utilisateur.

   État du relais : indique à l'application où rediriger l'utilisateur une fois l'authentification terminée.
7. Téléchargez le certificat (Base64) depuis la section **Certificat de signature SAML** . Le certificat est utilisé en tant que SAMLidpCertName lors de la configuration de NetScaler en tant que SAML SP.



8. Une fois la configuration côté Azure AD terminée, ajoutez les utilisateurs et les groupes d'utilisateurs autorisés à accéder à l'application. Accédez à l'onglet **Utilisateurs et groupes** et cliquez sur **+Ajouter un utilisateur/un groupe**.



Configurations côté NetScaler

1. Créez une action SAML.

- Accédez à **Sécurité > Stratégies de trafic des applications AAA > Authentification > Stratégies avancées > Actions > SAML**.
- Sélectionnez l'onglet **Serveurs**, cliquez sur **Ajouter**, entrez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

  Description du paramètre :

  La valeur des paramètres en gras doit provenir des configurations côté Azure.

  - Nom : nom du serveur
  - **URL de redirection** : entrez l'URL de connexion utilisée précédemment dans la section « Configuration de NetScaler » d'Azure AD. `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`
  - URL de déconnexion unique - `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`
  - Liaison SAML : mécanisme utilisé pour transporter les messages du demandeur et du répondeur SAML entre le SP et l'IdP. Lorsque NetScaler agit en tant que SP, il prend en charge les liaisons Post, Redirect et Artifact. La méthode de liaison par défaut est Post.
  - Liaison de déconnexion : spécifie le mécanisme de transport des messages de déconnexion SAML. Le mécanisme de liaison par défaut est Post.
  - **Nom du certificat IDP** : certificat IDPCert (Base64) présent dans la section **Certificat de signature SAML** .

```
1  add ssl certkey <IDP-CERT-NAME> -cert <Name of the IdP
      certificate downloaded above>
2  <!--NeedCopy-->
```

  - **Champ utilisateur** - UserPrincipalName. Pris de la section « Attributs et revendications de l'utilisateur » d'Azure IdP.
  - **Nom du certificat de signature** - Non nécessaire pour Azure AD. Sélectionnez le certificat SP SAML (avec clé privée) que NetScaler utilise pour signer les demandes d'authentification à l'IdP. Le même certificat (sans clé privée) doit être importé sur l'IdP, de sorte que l'IdP puisse vérifier la signature de la demande d'authentification. Ce champ n'est pas nécessaire à la plupart des déplacés internes.
  - **IssuerName** - ID de l'entité ou identifiant. `https://idp.g.nssvctesting.net` dans ce cas.
  - Rejeter l'assertion non signée : option que vous pouvez spécifier si vous souhaitez que les assertions de l'IdP soient signées. L'option par défaut est Activé.

- Audience : audience pour laquelle l'assertion envoyée par l'IdP est applicable. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente le fournisseur de services.
- Algorithme de signature : algorithme à utiliser pour signer/vérifier les transactions SAML. La valeur par défaut est RSA-SHA256.
- Méthode de synthèse : algorithme à utiliser pour calculer/vérifier le condensé des transactions SAML. La valeur par défaut est SHA256.
- Groupe d'authentification par défaut : groupe par défaut choisi lorsque l'authentification réussit, en plus des groupes extraits.
- Champ de nom de groupe : nom de la balise dans une assertion qui contient des groupes d'utilisateurs.
- Temps d'inclinaison (minutes) : cette option spécifie le décalage d'horloge en minutes autorisé par le fournisseur de services NetScaler sur une assertion entrante. Par exemple, si vous définissez le temps d'inclinaison sur 10 minutes à 16 h, l'assertion SAML est valide de 15 h 50 à 16 h 10, soit 20 minutes au total. La durée d'inclinaison par défaut est de 5 minutes.
- Deux facteurs - OFF
- Contexte d'authentification demandé - exact
- Type de classe d'authentification - Aucune
- Envoyer une empreinte de pouce - OFF
- Appliquer le nom d'utilisateur - ON
- Forcer l'authentification - OFF
- Réponse SAML de stockage - OFF

2. Créez une stratégie SAML correspondante pour l'action SAML et liez la stratégie au serveur virtuel d'authentification.
   - Accédez à **Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Stratégie**, puis cliquez sur **Ajouter**.
   - Sur la page **Créer une stratégie SAML d'authentification**, fournissez les informations suivantes :
     - Nom : spécifiez le nom de la stratégie SAML.
     - Type d'action : sélectionnez SAML comme type d'action d'authentification.
     - Action : sélectionnez le profil de serveur SAML auquel lier la stratégie SAML.
     - Expression : affiche le nom de la règle ou de l'expression utilisée par la stratégie SAML pour déterminer si l'utilisateur doit s'authentifier auprès du serveur SAML. Dans la

zone de texte, définissez la valeur « rule = true » pour que la stratégie SAML prenne effet et que l'action SAML correspondante soit exécutée.

3. Liez la stratégie SAML au serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**et associez la stratégie SAML au serveur virtuel d'authentification.

Remarque :

- Azure AD ne s'attend pas à ce que le champ Subject ID figure dans la demande SAML.
- Pour que NetScaler n'envoie pas le champ Subject ID, tapez la commande suivante sur l'interface de ligne de commande NetScaler.
  ```
  nsapimgr_wr.sh -ys call="ns_saml_dont_send_subject"
  ```
  Cette commande s'applique uniquement aux flux de travail d'authentification nFactor.

Plus de fonctionnalités prises en charge pour SAML

May 5, 2023

Les fonctionnalités suivantes sont prises en charge pour SAML.

Prise en charge de la lecture et de la génération des métadonnées pour la configuration du SP et de l'IdP SAML

L'appliance NetScaler prend désormais en charge les fichiers de métadonnées en tant qu'entités de configuration pour le fournisseur de services SAML (SP) et le fournisseur d'identité (IdP). Le fichier de métadonnées est un fichier XML structuré qui décrit la configuration d'une entité. Les fichiers de métadonnées pour le SP et l'IdP sont distincts. Selon le déploiement, et parfois, une entité SP ou IdP peut avoir plusieurs fichiers de métadonnées.
En tant qu'administrateur, vous pouvez exporter et importer des fichiers de métadonnées (SAML SP et IdP) sur NetScaler.
Les fonctionnalités d'exportation et d'importation de métadonnées pour le SP et l'IdP SAML sont expliquées dans les sections suivantes.

Export des métadonnées pour le SP SAML

Prenons l'exemple d'un NetScaler configuré en tant que SP SAML et où un IdP SAML souhaiterait importer des métadonnées contenant la configuration du SP NetScaler. Supposons que l'appliance NetScaler soit déjà configurée avec un attribut « SAMLAction » qui spécifie la configuration SAML SP.

Pour exporter les métadonnées des utilisateurs ou de l'administrateur, interrogez NetScaler Gateway ou le serveur virtuel d'authentification comme indiqué ci-dessous :

```
https://vserver.company.com/metadata/samlsp/<action-name>
```

Importation de métadonnées pour SAML SP

Actuellement, la configuration de l'action SAML sur l'appliance NetScaler prend différents paramètres. L'administrateur spécifie ces paramètres manuellement. Cependant, les administrateurs ignorent souvent la nomenclature lorsqu'il s'agit d'interagir avec différents systèmes SAML. Si des métadonnées de l'IdP sont disponibles, une grande partie de la configuration dans l'entité « SAMLaction » peut être évitée. En fait, l'intégralité de la configuration spécifique à l'IdP peut être omise si le fichier de métadonnées IdP est fourni. L'entité 'SamlAction' prend désormais un paramètre supplémentaire pour lire la configuration à partir du fichier de métadonnées.

Lorsque vous importez des métadonnées dans une appliance NetScaler, les métadonnées ne contiennent aucun algorithme de signature à utiliser, elles contiennent les détails du point de terminaison. Les métadonnées peuvent être signées à l'aide de certains algorithmes qui peuvent être utilisés pour vérifier les métadonnées elles-mêmes. Les algorithmes ne sont pas stockés dans l'entité « SAMLaction ».

Par conséquent, ce que vous spécifiez dans l'entité « SamlAction » sont ceux utilisés lors de l'envoi des données. Les données entrantes peuvent contenir un algorithme différent à traiter par une appliance NetScaler.

Vous pouvez importer une taille maximale de 64 Ko de métadonnées.

Pour récupérer les fichiers de métadonnées à l'aide de l'interface de ligne de commande.

```
set samlAction <name> [-metadataUrl <url> [-metadataRefreshInterval <
    int>] https://idp.citrix.com/samlidp/metadata.xml
```

> **Remarque**
>
> Le paramètre MetadataRefreshInterval est l'intervalle en minutes d'extraction des informations de métadonnées à partir de l'URL de métadonnées spécifiée. Valeur par défaut 36000.

Importation de métadonnées pour IdP SAML

Le paramètre « SamlIDPProfile » prend un nouvel argument pour lire l'ensemble de la configuration spécifique au SP. La configuration du fournisseur d'identité SAML peut être simplifiée en remplaçant les propriétés spécifiques au SP par un fichier de métadonnées SP. Ce fichier est interrogé via HTTP.

Pour lire à partir du fichier de métadonnées à l'aide de l'interface de ligne de commande :


```
set samlIdPProfile <name> [-metadataUrl <url>] [-
    metadataRefreshInterval <int>]
```

Prise en charge des attributs nom-valeur pour l'authentification SAML

Vous pouvez désormais configurer les attributs d'authentification SAML avec un nom unique ainsi que des valeurs. Les noms sont configurés dans le paramètre d'action SAML et les valeurs sont obtenues en interrogeant les noms. En spécifiant la valeur d'attribut name, les administrateurs peuvent facilement rechercher la valeur d'attribut associée au nom d'attribut. De plus, les administrateurs n'ont plus besoin de se souvenir de l'attribut uniquement par sa valeur.

> **Important**
>
> - Dans la commande SAMLaction, vous pouvez configurer un maximum de 64 attributs séparés par des virgules avec une taille totale inférieure à 2048 octets.
> - Citrix vous recommande d'utiliser la liste des attributs. L'utilisation de « l'attribut 1 à l'attribut 16 » provoquera l'échec de la session si la taille de l'attribut extrait est importante.

Pour configurer les attributs nom-valeur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add authentication samlAction <name> [-Attributes <string>]
```

Exemple :

```
add authentication samlAction samlAct1 -attributes  "mail,sn,
    userprincipalName"
```

Prise en charge de l'URL du service de consommation d'assertion pour IdP SAML

Une appliance NetScaler configurée en tant que fournisseur d'identité SAML (IdP) prend désormais en charge l'indexation Assertion Consumer Service (ACS) pour traiter les demandes du fournisseur de services SAML (SP). L'IdP SAML importe la configuration d'indexation ACS à partir des métadonnées du fournisseur de services ou permet la saisie manuelle des informations d'index ACS.
Le tableau suivant répertorie certains articles spécifiques aux déploiements dans lesquels l'appliance NetScaler est utilisée en tant que SP SAML ou IdP SAML.

Quelques informations sur d'autres déploiements spécifiques :

- NetScaler en tant que SP SAML sur un périphérique FIPS

- Configuration d'Office365 pour l'authentification unique avec NetScaler en tant que fournisseur d'identité SAML

Prise en charge du type d'identification WebView pour les mécanismes d'authentification

L'authentification d'une appliance NetScaler peut désormais prendre en charge le protocole AuthV3. Le type d'informations d'identification WebView dans le protocole Authv3 prend en charge tous les types de mécanismes d'authentification (y compris SAML et OAuth). Le type d'informations d'identification WebView fait partie d'Authv3, qui est implémenté par Citrix Receiver et le navigateur dans les applications Web.

L'exemple suivant explique le flux des événements WebView via NetScaler Gateway et Citrix Receiver :

1. Citrix Receiver négocie avec NetScaler Gateway pour la prise en charge du protocole AuthV3.
2. L'appliance NetScaler répond positivement et suggère une URL de démarrage spécifique.
3. Citrix Receiver se connecte ensuite au point de terminaison spécifique (URL).
4. NetScaler Gateway envoie une réponse au client pour démarrer le WebView.
5. Citrix Receiver démarre WebView et envoie la demande initiale à l'appliance NetScaler.
6. L'appliance NetScaler redirige l'URI vers le point de connexion du navigateur.
7. Une fois l'authentification terminée, l'appliance NetScaler envoie une réponse d'achèvement à WebView.
8. Le WebView se ferme maintenant et redonne le contrôle à Citrix Receiver pour continuer le protocole AuthV3 pour l'établissement de session.

Augmentation de la taille de SessionIndex dans le SP SAML

La taille SessionIndex du fournisseur de services (SP) SAML est augmentée à 96 octets. Auparavant, la taille maximale par défaut de SessionIndex était de 63 octets.

> **Remarque**
>
> Prise en charge introduite dans NetScaler 13.0 Build 36.x

Prise en charge de référence de classe d'authentification personnalisée pour SP SAML

Vous pouvez configurer un attribut de référence de classe d'authentification personnalisé dans la commande **d'action SAML** . À l'aide de l'attribut de référence de classe d'authentification personnalisé, vous pouvez personnaliser les noms de classe dans les balises SAML appropriées. L'attribut de référence de la classe d'authentification personnalisée ainsi que l'espace de noms sont envoyés à l'IdP SAML dans le cadre de la demande d'authentification SP SAML.

Auparavant, à l'aide de la commande d'action SAML, vous pouviez configurer uniquement un ensemble de classes prédéfinies définies dans l'attribut AuthnCTXClassRef.

> **Important**
>
> Lors de la configuration de l'attribut CustomAuthnctxClassRef, vérifiez les points suivants :

- Les noms des classes doivent inclure des caractères alphanumériques ou une URL valide avec des balises XML appropriées.
- Si vous devez configurer plusieurs classes personnalisées, chaque classe doit être séparée par des virgules

Pour configurer les attributs CustomAuthnCTXClassRef à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

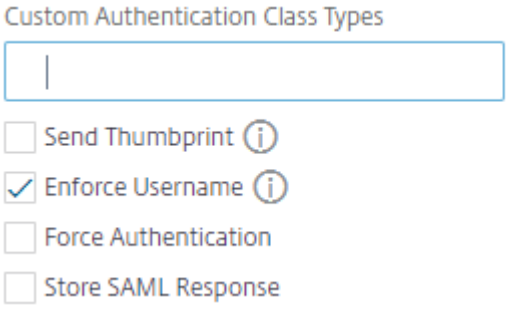
- add authentication samlAction <name> [-customAuthnCtxClassRef <string>]
- set authentication samlAction <name> [-customAuthnCtxClassRef <string>]

Exemple :

- `add authentication samlAction samlact1 -customAuthnCtxClassRef http://www.class1.com/LoA1,http://www.class2.com/LoA2`
- `set authentication samlAction samlact2 -customAuthnCtxClassRef http://www.class3.com/LoA1,http://www.class4.com/LoA2`

Pour configurer les attributs CustomAuthnctxClassRef à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Actions > SAML**.
2. Sur la page SAML, sélectionnez l'onglet **Serveurs** et cliquez sur **Ajouter**.
3. Sur la page **Créer un serveur SAML d'authentification**, entrez le nom de l'action SAML.
4. Faites défiler vers le bas pour configurer les types de classe dans la section **Types de classe d'authentification personnalisés** .



Prise en charge de la liaison d'artefacts dans l'IdP SAML

L'appliance NetScaler configurée en tant que fournisseur d'identité SAML (IdP) prend en charge la liaison aux artefacts. La liaison d'artefact améliore la sécurité de l'IdP SAML et empêche les utilisateurs malveillants d'inspecter l'assertion.

Prise en charge de l'URL du service de consommation d'assertion pour IdP SAML

Une appliance NetScaler configurée en tant que fournisseur d'identité SAML (IdP) prend désormais en charge l'indexation Assertion Consumer Service (ACS) pour traiter les demandes du fournisseur de services SAML (SP). L'IdP SAML importe la configuration d'indexation ACS à partir des métadonnées du fournisseur de services ou permet la saisie manuelle des informations d'index ACS.

Prise en charge du déchargement FIPS

Une appliance NetScaler MPX FIPS utilisée comme fournisseur de services SAML prend désormais en charge les assertions cryptées. En outre, une appliance NetScaler MPX FIPS fonctionnant en tant que fournisseur de services SAML ou fournisseur d'identité SAML peut désormais être configurée pour utiliser les algorithmes SHA2 sur du matériel FIPS.

> **Remarque**
>
> En mode FIPS, seul l'algorithme RSA-V1_5 est pris en charge en tant qu'algorithme de transport de clés.

Configuration de la prise en charge du déchargement FIPS via l'interface de ligne de commande :

1. Ajouter SSL FIPS

   add ssl fipsKey fips-key

2. Créez un CSR et utilisez-le sur le serveur de l'autorité de certification pour générer un certificat. Vous pouvez ensuite copier le certificat dans **/nsconfig/ssl**. Supposons que le fichier soit *fips3cert.cer*.

   ```
   add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key<!--
   NeedCopy-->
   ```

3. Spécifiez ce certificat dans l'action SAML pour le module SP SAML

   ```
   set samlAction <name> -samlSigningCertName fips-cert<!--NeedCopy-->
   ```

4. Utiliser le certificat dans le module SamlIDPProfile pour fournisseur d'identité SAML

   ```
   set samlidpprofile fipstest -samlIdpCertName fips-cert<!--NeedCopy-->
   ```


Terminologies SAML courantes

Voici quelques terminologies SAML courantes :

- **Assertion :** Une assertion SAML est un document XML renvoyé par le fournisseur d'identité au fournisseur de services après l'authentification de l'utilisateur. L'assertion possède une structure spécifique, telle que définie par la norme SAML.
- **Types d'assertions :** Voici les types d'assertion.
  - Authentification : l'utilisateur est authentifié par un moyen particulier à un moment donné
  - Autorisation : l'utilisateur s'est vu accorder ou refuser l'accès à une ressource spécifiée
  - Attributs : l'utilisateur est associé aux attributs fournis
- **Service consommateur d'assertion (ACS) :** point de terminaison (URL) du fournisseur de services chargé de recevoir et d'analyser une assertion SAML
- **Restriction d'audience :** valeur de l'assertion SAML qui spécifie à qui (et uniquement à qui) l'assertion est destinée. Le « public » sera le fournisseur de services et est généralement une URL mais peut techniquement être formaté comme n'importe quelle chaîne de données.
- **Fournisseur d'identité (IdP) :** En termes de SAML, le fournisseur d'identité est l'entité qui vérifie l'identité de l'utilisateur, en réponse à une demande du fournisseur de services.

  Le fournisseur d'identité est responsable du maintien et de l'authentification de l'identité de l'utilisateur.
- **Fournisseur de services (SP) :** En termes de SAML, le fournisseur de services (SP) offre un service à l'utilisateur et permet à l'utilisateur de se connecter en utilisant SAML. Lorsque l'utilisateur tente de se connecter, le SP envoie une demande d'authentification SAML au fournisseur d'identité (IdP)
- **Liaison SAML :** les demandeurs et les répondeurs SAML communiquent en échangeant des messages. Le mécanisme de transport de ces messages s'appelle une liaison SAML.
- **Artefact HTTP :** l'une des options de liaison prises en charge par le protocole SAML. L'artefact HTTP est utile dans les scénarios où le demandeur et le répondeur SAML utilisent un User-Agent HTTP et ne souhaitent pas transmettre l'intégralité du message, que ce soit pour des raisons techniques ou de sécurité. Au lieu de cela, un artefact SAML est envoyé, qui est un identifiant unique pour les informations complètes. L'IdP peut ensuite utiliser l'artefact pour récupérer les informations complètes. L'émetteur de l'artefact doit conserver son état tant que l'artefact est en attente. Un service de résolution d'artefacts (ARS) doit être configuré.

  L'artefact HTTP envoie l'artefact en tant que paramètre de requête.
- **HTTP POST :** L'une des options de liaison prises en charge par le protocole SAML.

  HTTP POST envoie le contenu du message en tant que paramètre POST, dans la charge utile.

- **Redirection HTTP :** l'une des options de liaison prises en charge par le protocole SAML.

  Lorsque la redirection HTTP est utilisée, le fournisseur de services redirige l'utilisateur vers le fournisseur d'identité où la connexion a lieu, et le fournisseur d'identité redirige l'utilisateur vers le fournisseur de services. La redirection HTTP nécessite l'intervention de l'agent utilisateur (le navigateur).

  La redirection HTTP envoie le contenu du message dans l'URL. Pour cette raison, elle ne peut pas être utilisée pour la réponse SAML, car la taille de la réponse dépasse généralement la longueur d'URL autorisée par la plupart des navigateurs.

  Remarque : L'appliance NetScaler prend en charge les liaisons POST et Redirect lors de la déconnexion.

- Métadonnées : Les métadonnées sont les données de configuration dans SP et IdP pour savoir comment communiquer entre eux, ce qui sera dans les normes XML

Autres articles Citrix utiles relatifs à l'authentification SAML

Les articles suivants relatifs à l'authentification SAML peuvent être utiles.

- https://support.citrix.com/article/CTX277558
- https://support.citrix.com/article/CTX259127
- https://support.citrix.com/article/CTX228135
- https://support.citrix.com/article/CTX221631
- https://support.citrix.com/article/CTX138988

Authentification OAuth

May 5, 2023

La fonctionnalité de gestion du trafic d'authentification, d'autorisation et d'audit prend en charge l'authentification OAuth et OpenID Connect (OIDC). Il autorise et authentifie les utilisateurs sur des services hébergés sur des applications telles que Google, Facebook et Twitter.

Points à noter

- NetScaler Advanced Edition ou version ultérieure est requis pour que la solution fonctionne.
- Une appliance NetScaler doit disposer de la version 12.1 ou ultérieure pour qu'elle fonctionne en tant qu'IdP OAuth à l'aide d'OIDC.
- OAuth sur une appliance NetScaler est qualifié pour tous les IDP SAML conformes à « OpenID connect 2.0 ».

Une appliance NetScaler peut être configurée pour se comporter comme un fournisseur de services (SP) ou un fournisseur d'identité (IdP), à l'aide de SAML et OIDC. Auparavant, une appliance NetScaler configurée en tant qu'IdP ne prenait en charge que le protocole SAML. À partir de la version 12.1 de NetScaler, NetScaler prend également en charge l'OIDC.

OIDC est une extension de l'autorisation/délégation OAuth. Une appliance NetScaler prend en charge les protocoles OAuth et OIDC dans la même classe que les autres mécanismes d'authentification. OIDC est un module complémentaire à OAuth car il fournit un moyen d'obtenir des informations utilisateur à partir du serveur d'autorisation, contrairement à OAuth qui n'obtient qu'un jeton qui ne peut pas être glané pour les informations utilisateur.

Le mécanisme d'authentification facilite la vérification en ligne des jetons OpenID. Une appliance NetScaler peut être configurée pour obtenir des certificats et vérifier les signatures sur le jeton.

L'un des principaux avantages de l'utilisation des mécanismes OAuth et OIDC est que les informations utilisateur ne sont pas envoyées aux applications hébergées. Par conséquent, le risque de vol d'identité est considérablement réduit.

L'appliance NetScaler configurée pour l'authentification, l'autorisation et l'audit accepte désormais les jetons entrants signés à l'aide de l'algorithme HMAC HS256. En outre, les clés publiques du fournisseur d'identité SAML (IdP) sont lues à partir d'un fichier, au lieu d'apprendre à partir d'un point de terminaison d'URL.

Dans l'implémentation de NetScaler, l'application est accessible par le serveur virtuel de gestion du trafic d'authentification, d'autorisation et d'audit. Par conséquent, pour configurer OAuth, vous devez configurer une stratégie OAuth qui doit ensuite être associée à un serveur virtuel de gestion du trafic d'authentification, d'autorisation et d'audit.

Configurer le protocole OpenID Connect

Une appliance NetScaler peut désormais être configurée en tant que fournisseur d'identité à l'aide du protocole OIDC. Le protocole OIDC renforce les fonctionnalités de fourniture d'identité de l'appliance NetScaler. Vous pouvez désormais accéder à l'application hébergée à l'échelle de l'entreprise avec une authentification unique. L'OIDC offre plus de sécurité en ne transférant pas le mot de passe utilisateur, mais fonctionne avec des jetons ayant une durée de vie spécifique. OIDC est également conçu pour s'intégrer à des clients autres que des navigateurs, tels que des applications et des services. Par conséquent, de nombreuses implémentations adoptent largement l'OIDC.

Avantages de la prise en charge d'OpenID Connect

- OIDC élimine les frais généraux liés à la gestion de plusieurs mots de passe d'authentification, car l'utilisateur possède une identité unique au sein de l'organisation.

- OIDC fournit une sécurité solide pour votre mot de passe, car le mot de passe est partagé uniquement avec votre fournisseur d'identité et non avec aucune application à laquelle vous accédez.
- L'OIDC dispose d'une grande interopérabilité avec divers systèmes, ce qui facilite l'acceptation d'OpenID par les applications hébergées.
- OIDC est un protocole simple qui permet aux clients natifs de s'intégrer facilement aux serveurs.

Pour configurer une appliance NetScaler en tant qu'IdP à l'aide du protocole OpenID Connect à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > IdP OAuth**.
2. Cliquez sur **Profil**, puis sur **Ajouter.**

   Dans l'écran **Créer un profil de fournisseur d'identité OAuth d'authentification**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   - **Nom** : nom du profil d'authentification.
   - **Client ID** : chaîne unique qui identifie le fournisseur de services.
   - **Client Secret** : secret unique qui identifie le SP.
   - **URL de redirection** : point de terminaison sur le SP auquel le code/jeton doit être publié.
   - **Nom de l'émetteur** : chaîne qui identifie le fournisseur d'identité.
   - **Audience** : destinataire cible du jeton envoyé par l'IdP. Cela peut être vérifié par le destinataire.
   - **Skew Time (Temps** d'inclinaison) : durée pendant laquelle le jeton reste valide.
   - **Groupe d'authentification par défaut** : groupe ajouté à la session pour ce profil afin de simplifier l'évaluation des stratégies et d'aider à personnaliser les stratégies.
3. Cliquez sur **Stratégies** et cliquez sur **Ajouter.**
4. Dans l'écran **Créer une stratégie de fournisseur d'identité OAuth d'authentification**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   - **Nom :** nom de la politique d'authentification.
   - **Action** : nom du profil créé précédemment.
   - **Action de consignation : nom de l'action du journal** des messages à utiliser lorsqu'une demande correspond à cette stratégie. Ce n'est pas un dépôt obligatoire.
   - **Action à résultat non défini** — Action à exécuter si le résultat de l'évaluation de la stratégie n'est pas défini (UNDEF). Ce champ n'est pas obligatoire.
   - **Expression** — Expression de stratégie avancée utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, true.
   - **Comments** : tout commentaire concernant la stratégie.

Liaison de la stratégie OAuthIDP et de la stratégie LDAP au serveur virtuel d'authentification

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Actions > LDAP**.
2. Dans l'écran **Actions LDAP**, cliquez sur **Ajouter**.
3. Dans l'écran **Créer un serveur LDAP d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer**.
    - **Nom :** nom de l'action LDAP
    - **ServerName/ServerIP :** fournit le nom de domaine complet ou l'adresse IP du serveur LDAP
    - Choisissez les valeurs appropriées **pour le type de sécurité, le port, le type de serveur et le délai d'expiration**
    - Assurez-vous que **l'authentification** est cochée
    - **DN de base :** base à partir de laquelle lancer la recherche LDAP. Par exemple, dc=aaa, dc=local.
    - **Administrator Bind DN :** nom d'utilisateur de la liaison au serveur LDAP. Par exemple, admin@aaa.local.
    - **Mot de passe administrateur/Confirmer le mot de passe : mot de passe pour lier LDAP**
    - Cliquez sur **Tester la connexion** pour tester vos paramètres.
    - **Attribut de nom d'ouverture de session du serveur :** choisissez **« SAMAccountName »**
    - Les autres champs ne sont pas obligatoires et peuvent donc être configurés comme requis.
4. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Stratégie.**
5. Dans **l'écran Stratégies d'authentification**, cliquez sur **Ajouter**.
6. Sur la page **Créer une stratégie d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer.**
    - **Nom :** nom de la stratégie d'authentification LDAP.
    - **Type d'action :** choisissez **LDAP.**
    - **Action :** choisissez l'action LDAP.
    - **Expression :** expression de politique avancée que la politique utilise pour répondre à une demande spécifique. Par exemple, true**.

Pour configurer l'appliance NetScaler en tant qu'IdP à l'aide du protocole OpenID Connect à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- add authentication OAuthIDPProfile <name> [-clientID <string>][-clientSecret][-redirectURL <URL>][-issuer <string>][-audience <string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]<!--NeedCopy-->
- add authentication OAuthIdPPolicy <name> -rule <expression> [-action <string> [-undefAction <string>] [-comment <string>][-logAction <string >]<!--NeedCopy-->
- add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -ldapBase "dc=aaa,dc=local"<!--NeedCopy-->
- ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -ldapLoginName sAMAccountName<!--NeedCopy-->
- add authentication policy aaa-ldap-adv-pol -rule **true** -action aaa-ldap-act<!--NeedCopy-->
- bind authentication vserver auth_vs -policy <ldap_policy_name> -priority 100 -gotoPriorityExpression NEXT<!--NeedCopy-->
- bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -priority 5 -gotoPriorityExpression END<!--NeedCopy-->
- bind vpn global -certkey <><!--NeedCopy-->

> **Remarque**
>
> Vous pouvez lier plusieurs clés. Les parties publiques des certificats liés sont envoyées en réponse à jwks_uri query (https://gw/oauth/idp/certs).

NetScaler en tant que SP OAuth

May 5, 2023

La fonctionnalité de gestion du trafic d'authentification, d'autorisation et d'audit prend en charge l'authentification OAuth pour authentifier les utilisateurs auprès d'applications hébergées sur des applications telles que Google, Facebook et Twitter.

Points à noter

- NetScaler Advanced Edition ou version ultérieure est requis pour que la solution fonctionne.
- L'appliance OAuth sur NetScaler est qualifiée pour tous les IDP SAML conformes à « OpenID connect 2.0 ».

> **Important :**
>
> L'appliance NetScaler peut répondre par une erreur CSRF lorsqu'un site Web riche en contenu envoie plusieurs demandes d'authentification à l'expiration de la session. Pour contourner le problème, il est recommandé, lorsque vous configurez la stratégie OAuth, de vous assurer que la stratégie est configurée à la fois pour le nom d'hôte et le chemin d'accès qui sont les principaux points d'entrée.

Configurer OAuth à l'aide de l'interface graphique

1. Configurez l'action et la stratégie OAuth.

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégie**, puis créez une stratégie avec OAuth comme type d'action, puis associez l'action OAuth requise à la stratégie.

2. Associez la stratégie OAuth à un serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**, puis associez la stratégie OAuth au serveur virtuel d'authentification.

> **Remarque :**
>
> Les attributs (1 à 16) peuvent être extraits dans la réponse OAuth. Ces attributs ne sont actuellement pas évalués. Ils sont ajoutés pour référence future.

Configurer OAuth à l'aide de la CLI

1. Définissez une action OAuth.

```
add authentication OAuthAction <name> -authorizationEndpoint <URL>
     -tokenEndpoint <URL> [-idtokenDecryptEndpoint <URL>] -clientID
     <string> -clientSecret <string> [-defaultAuthenticationGroup <
    string>][-tenantID <string>][-GraphEndpoint <string>][-
    refreshInterval <positive_integer>] [-CertEndpoint <string>][-
    audience <string>][-userNameField <string>][-skewTime <mins>][-
    issuer <string>][-Attribute1 <string>][-Attribute2 <string>][-
    Attribute3 <string>]
<!--NeedCopy-->
```

2. Associez l'action à une stratégie d'authentification avancée.

```
add authentication Policy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```


Exemple :

```
add authentication oauthAction a -authorizationEndpoint https://
    example.com/ -tokenEndpoint https://example.com/ -clientiD sadf
     -clientsecret df
<!--NeedCopy-->
```

Pour plus d'informations sur les paramètres OAuthAction d' authentification, voir AuthAction AuthAction d'authentification.

> **Remarque :**
>
> Lorsqu'un CertEndpoint est spécifié, l'appliance NetScaler interroge ce point de terminaison à la fréquence configurée pour connaître les clés.

Pour configurer un NetScaler afin qu'il lise le fichier local et analyse les clés de ce fichier, une nouvelle option de configuration est introduite comme suit :

```
set authentication OAuthAction <> -CertFilePath <path to local file
    with jwks>
<!--NeedCopy-->
```

La fonctionnalité OAuth prend désormais en charge les fonctionnalités suivantes dans l'API des jetons du côté de la partie dépendante (RP) et du côté IdP de NetScaler Gateway et NetScaler.

- Prise en charge de PKCE (Proof Key for Code Exchange)
- Prise en charge de client_assertion

Prise en charge des attributs nom-valeur pour l'authentification OAuth

Vous pouvez désormais configurer les attributs d'authentification OAuth avec un nom unique ainsi que les valeurs. Les noms sont configurés dans le paramètre d'action OAuth en tant que « Attributs » et les valeurs sont obtenues en interrogeant les noms. Les attributs extraits sont stockés dans la session d'authentification, d'autorisation et d'audit. Les administrateurs peuvent interroger ces attributs à l'aide de `http.req.user.attribute("attribute name")` ou `http.req.user.attribute(1)`, selon la méthode choisie pour spécifier les noms d'attributs.

En spécifiant le nom de l'attribut, les administrateurs peuvent facilement rechercher la valeur d'attribut associée à ce nom d'attribut. De plus, les administrateurs n'ont plus à se souvenir de « l'attribut1 à l'attribut16 » uniquement par son numéro.

> **Important**
>
> Dans une commande OAuth, vous pouvez configurer un maximum de 64 attributs séparés par des virgules avec une taille totale inférieure à 1 024 octets.

> **Remarque**
>
> L'échec de session peut être évité si la taille totale de la valeur de « l'attribut 1 à l'attribut 16 » et les valeurs des attributs spécifiés dans « Attributs » ne dépassent pas 10 Ko.

Pour configurer les attributs nom-valeur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add authentication OAuthAction <name> [-Attributes <string>]

set authentication OAuthAction <name> [-Attributes <string>]
<!--NeedCopy-->
```

Exemples :

```
add authentication OAuthAction a1  -attributes "email,company"  -
   attribute1 email

set authentication OAuthAction oAuthAct1 -attributes "mail,sn,
   userprincipalName"
<!--NeedCopy-->
```

NetScaler en tant qu'IdP OAuth

May 5, 2023

Une appliance NetScaler peut désormais être configurée en tant que fournisseur d'identité à l'aide du protocole OpenID-Connect (OIDC). Le protocole OIDC renforce les fonctionnalités de fourniture d'identité de l'appliance NetScaler. Vous pouvez désormais accéder à l'application hébergée à l'échelle de l'entreprise avec une authentification unique, car OIDC offre plus de sécurité en ne transférant pas le mot de passe de l'utilisateur mais en utilisant des jetons avec une durée de vie spécifique. OpenID est également conçu pour s'intégrer à des clients autres que des navigateurs, tels que des applications et des services. Par conséquent, le protocole OIDC est largement adopté par de nombreuses implémentations.

> **Remarque**
>
> NetScaler doit disposer de la version 12.1 ou ultérieure pour que l'appliance fonctionne en tant qu'IdP OAuth à l'aide du protocole OIDC.

Avantages de l'utilisation de NetScaler en tant qu'IdP OAuth

- Élimine les frais liés à la gestion de plusieurs mots de passe d'authentification, car l'utilisateur possède une identité unique au sein de l'organisation.
- Fournit une sécurité solide pour votre mot de passe, car le mot de passe est partagé uniquement avec votre fournisseur d'identité et non avec les applications auxquelles vous accédez.
- Fournit une interopérabilité étendue avec divers systèmes, ce qui facilite l'acceptation d'OpenID par les applications hébergées.

> **Remarque**
>
> NetScaler Advanced Edition ou version ultérieure est requis pour que la solution fonctionne.

Pour configurer l'appliance NetScaler en tant qu'IdP OAuth à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > IdP OAuth**.
2. Cliquez sur **Profil**, puis sur **Ajouter.**

   Dans l'écran **Créer un profil de fournisseur d'identité OAuth d'authentification**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   - **Nom** : nom du profil d'authentification. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Impossible de modifier une fois le profil créé.
   - **Client ID** : chaîne unique qui identifie le fournisseur de services. Le serveur d'autorisation déduit la configuration du client en utilisant cet ID. Longueur maximale : 127.
   - **Client Secret** : chaîne secrète établie par l'utilisateur et le serveur d'autorisation. Longueur maximale : 239.
   - **URL de redirection** : point de terminaison sur le SP auquel le code/jeton doit être publié.
   - **Nom de l'émetteur** : identité du serveur dont les jetons doivent être acceptés. Longueur maximale : 127.
   - **Audience** : destinataire cible du jeton envoyé par l'IdP. Cela peut être vérifié par le destinataire.
   - **Temps d'inclinaison** : cette option spécifie le décalage d'horloge autorisé en minutes par NetScaler sur un jeton entrant. Par exemple, si SkewTime est 10, le jeton sera valide de (heure actuelle - 10) min à (heure actuelle + 10) min, soit 20 min en tout. Valeur par défaut : 5.

- **Groupe d'authentification par défaut** : groupe ajouté à la liste des groupes internes de la session lorsque ce profil est choisi par l'IdP qui peut être utilisé dans le flux nFactor. Il peut être utilisé dans l'expression (AAA.USER.IS_MEMBER_OF (« xxx »)) pour les stratégies d'authentification destinées à
  identifier le flux nFactor lié à la partie de confiance. Longueur maximale : 63

A group added to the session for this profile to simplify policy evaluation and help in customizing policies. This is the default group that is chosen when the authentication succeeds in addition to the extracted groups. Maximum Length: 63.

3. Cliquez sur **Stratégies** et cliquez sur **Ajouter.**
4. Dans l'écran **Créer une stratégie de fournisseur d'identité OAuth d'authentification**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   - **Nom** : nom de la stratégie d'authentification.
   - **Action** : nom du profil créé précédemment.
   - **Action du journal** : nom de l'action du journal des messages à utiliser lorsqu'une demande correspond à cette stratégie. Ce n'est pas un dépôt obligatoire.
   - **Action à résultat non défini** — Action à exécuter si le résultat de l'évaluation de la stratégie n'est pas défini (UNDEF). Ce champ n'est pas obligatoire.
   - **Expression** — Expression de stratégie avancée utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, true.
   - **Comments** : tout commentaire concernant la stratégie.

Liaison de la stratégie OAuthIDP et de la stratégie LDAP au serveur virtuel d'authentification

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Actions > LDAP**.
2. Dans l'écran **Actions LDAP**, cliquez sur **Ajouter**.
3. Dans l'écran **Créer un serveur LDAP d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer**.

   - **Nom :** nom de l'action LDAP
   - **ServerName/ServerIP :** fournit le nom de domaine complet ou l'adresse IP du serveur LDAP
   - Choisissez les valeurs appropriées **pour le type de sécurité, le port, le type de serveur et le délai d'expiration**
   - Assurez-vous que **l'option Authentification** est cochée
   - **DN de base :** base à partir de laquelle lancer la recherche LDAP. Par exemple, dc=aaa, dc=local.

- **Administrator Bind DN :** nom d'utilisateur de la liaison au serveur LDAP. Par exemple, admin@aaa.local.
- **Mot de passe administrateur/Confirmer le mot de passe : mot de passe pour lier LDAP**
- Cliquez sur **Tester la connexion** pour tester vos paramètres.
- **Attribut de nom d'ouverture de session du serveur :** choisissez « **SAMAccountName** »
- Les autres champs ne sont pas obligatoires et peuvent donc être configurés comme requis.

4. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Stratégie.**
5. Dans l'écran **Stratégies d'authentification**, cliquez sur **Ajouter**.
6. Sur la page **Créer une stratégie d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer.**

   - **Nom :** nom de la stratégie d'authentification LDAP.
   - **Type d'action :** choisissez **LDAP.**
   - **Action :** choisissez l'action LDAP.
   - **Expression :** expression de politique avancée que la politique utilise pour répondre à une demande spécifique. Par exemple, true**.

La fonctionnalité OAuth prend désormais en charge les fonctionnalités suivantes dans l'API des jetons du côté de la partie dépendante (RP) et du côté IdP de NetScaler Gateway et NetScaler.

- Prise en charge de PKCE (Proof Key for Code Exchange)
- Prise en charge de client_assertion

Pour configurer l'appliance NetScaler en tant qu'IdP à l'aide du protocole OIDC à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes :

```
add authentication OAuthIDPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <
    string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-action <
    string> [-undefAction <string>] [-comment <string>][-logAction <
    string>]

add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -
    ldapBase "dc=aaa,dc=local"

ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -
    ldapLoginName sAMAccountName

```



```
add authentication policy aaa-ldap-adv-pol -rule true -action aaa-ldap-act

bind authentication vserver auth_vs -policy <ldap_policy_name> -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -priority 5 -gotoPriorityExpression END

bind vpn global  - certkey <>
<!--NeedCopy-->
```

Remarque :

- Vous pouvez lier plusieurs clés. Les parties publiques des certificats liés sont envoyées en réponse à `jwks\\_uri query (https://gw/oauth/idp/certs)`.
- Le point de terminaison introspectif OAuth IdP prend en charge la propriété `active: true`.

Prise en charge des jetons cryptés sur le protocole OIDC

L'appliance NetScaler dotée du mécanisme OIDC prend désormais en charge l'envoi de jetons chiffrés ainsi que de jetons signés. L'appliance NetScaler utilise les spécifications de chiffrement Web JSON pour calculer les jetons chiffrés et prend uniquement en charge la sérialisation compacte des jetons cryptés. Pour crypter un jeton OpenID, une appliance NetScaler a besoin de la clé publique de la partie dépendante (RP). La clé publique est obtenue dynamiquement en interrogeant le point de terminaison de configuration bien connu de la partie de confiance.

Une nouvelle option « relyingPartyMetadataUrl » est introduite dans le profil « authentification OAuthIDPProfile. »

Pour configurer le point final de la partie de confiance à l'aide de l'interface

À l'invite de commande, tapez :

"'set authentication OAuthIDPProfile [-relyingPartyMetadataURL] [-refreshInterval] [-status < >]

```
-  **RelyingPartyMetadataURL**  : point de terminaison auquel NetScaler IdP peut obtenir des informations sur la partie de confiance en cours de configuration. La réponse aux métadonnées doit inclure des points de terminaison pour jwks_uri pour les clés publiques RP.

```



```
3  -  **RefreshInterval**  : définit la fréquence à laquelle ce point de
       terminaison doit être interrogé pour mettre à jour les certificats
       en quelques minutes.
4
5  -  **status** - Indique le statut de l'opération d'interrogation. L'é
       tat est terminé une fois que l'appliance NetScaler a réussi à
       obtenir les clés publiques.
6
7      **Exemple**
8
9      ```
10     set authentication OAuthIDPProfile sample_profile -
          relyingPartyMetadataURL https://rp.customer.com/metadata -
          refreshInterval 50 -status < >
11     <!--NeedCopy-->
```

Une fois le point de terminaison configuré, une appliance NetScaler interroge d'abord le point de terminaison connu de la partie dépendante pour lire la configuration. Actuellement, l'appliance NetScaler traite uniquement le point de terminaison « jwks_uri ».

- Si le « jwks_uri » est absent de la réponse, l'état du profil n'est pas complet.
- Si le « jwks_uri » est présent dans la réponse, NetScaler interroge également ce point de terminaison pour lire les clés publiques de l'utilisateur.

> **Remarque :**
>
> Seuls les algorithmes de type de cryptage RSAES-OAEP et AES256 GCM sont pris en charge pour le cryptage des jetons.

Prise en charge des attributs personnalisés sur OpenID Connect

Les parties utilisatrices OpenID peuvent avoir besoin de plus qu'un nom d'utilisateur ou un nom d'utilisateur principal (UPN) dans le jeton pour créer le profil utilisateur ou prendre des décisions d'autorisation. Le plus souvent, les groupes d'utilisateurs sont tenus d'appliquer des stratégies d'autorisation pour l'utilisateur. Parfois, des détails supplémentaires, tels que le prénom ou le nom de famille, sont nécessaires pour provisionner un compte d'utilisateur.

L'appliance NetScaler configurée en tant qu'IdP peut être utilisée pour envoyer des attributs supplémentaires dans le jeton OIDCID_Token à l'aide d'expressions. Les expressions de stratégie avancées sont utilisées pour envoyer les attributs personnalisés conformément aux exigences. L'IdP Citrix évalue les expressions correspondant aux attributs, puis calcule le jeton final.

L'appliance NetScaler enregistre automatiquement JSONify les données de sortie. Par exemple, les nombres (tels que SSN) ou les valeurs booléennes (true ou false) ne sont pas entourés de guillemets.

Les attributs à valeurs multiples, tels que les groupes, sont placés dans un marqueur de tableau (« [» et «] »). Les attributs de type complexe ne sont pas calculés automatiquement et vous pouvez configurer l'expression PI de ces valeurs complexes selon votre besoin.

Pour configurer le point final de la partie de confiance à l'aide de l'interface

À l'invite de commande, tapez :

```
set oauthidpprofile <name> -attributes <AAA-custom-attribute-pattern>
<!--NeedCopy-->
```

Le <AAA-custom-attribute-pattern> peut être décrit comme :

Attribute1=PI-Expression@@@attribute2=PI-Expression@@@

« attribute1 », « attribute2 » sont des chaînes littérales qui représentent le nom de l'attribut à insérer dans le id_token.

> **Remarque :** Vous pouvez configurer jusqu'à 2 000 octets d'attributs.

Exemple : `set oauthidpprofile sample_1 -attributes q{ myname=http.req.user.name@@@ssn="123456789"@@@jit="false"@@@groups=http.req.user.groups }`

- L'expression PI précédente est une expression de stratégie avancée qui représente la valeur à utiliser pour l'attribut. L'expression PI peut être utilisée pour envoyer un littéral de chaîne, tel que "'chaîne codée en dur"'. Le littéral de chaîne est entouré de guillemets doubles autour de guillemets simples ou de guillemets doubles autour d'un début et d'un motif (comme indiqué précédemment, le modèle de début est "q{"). Si la valeur de l'attribut n'est pas un littéral de chaîne, l'expression est évaluée au moment de l'exécution et sa valeur est envoyée en jeton. Si la valeur au moment de l'exécution est vide, l'attribut correspondant n'est pas ajouté au jeton d'identification.
- Comme défini dans l'exemple, « false » est une chaîne littérale pour l'attribut « jit ». En outre, "ssn" a une valeur codée en dur pour référence. Les groupes et « myname » sont des expressions PI qui génèrent des chaînes de caractères.

Support pour les déploiements GSLB actifs-actifs sur NetScaler Gateway

NetScaler Gateway configuré en tant que fournisseur d'identité (IdP) à l'aide du protocole OIDC peut prendre en charge les déploiements GSLB actifs et actifs. Le déploiement GSLB actif-actif sur NetScaler Gateway IdP permet d'équilibrer la charge d'une demande de connexion utilisateur entrante sur plusieurs sites géographiques.

> **Important**
>
> Citrix vous recommande de lier des certificats d'autorité de certification au service SSL et d'activer la validation des certificats sur le service SSL pour une sécurité accrue.

Pour plus d'informations sur la configuration de la configuration de GSLB, voir Exemple de configuration et de configuration GSLB.

Authentification par API avec l'appliance NetScaler

May 5, 2023

Il y a un changement de paradigme dans la façon dont les applications modernes interagissent avec leurs clients. Traditionnellement, les clients du navigateur étaient utilisés pour accéder aux services. Les applications configurent généralement des cookies de session pour suivre le contexte de l'utilisateur. Les applications modernes et distribuées compliquent la gestion des sessions utilisateur entre les microservices. De ce fait, la plupart des accès aux applications sont désormais basés sur des API.

Les clients qui communiquent avec ces services distribués ont également évolué. La plupart des clients obtiennent des jetons auprès d'une entité de confiance appelée Serveur d'autorisation pour prouver l'identité et l'accès des utilisateurs. Ces clients présentent ensuite le jeton à l'application à chaque demande d'accès. Par conséquent, les appareils proxy traditionnels tels que NetScaler doivent évoluer pour prendre en charge ces clients. Une appliance NetScaler permet aux administrateurs de gérer ce trafic. NetScaler peut être déployé en tant que passerelle d'API pour gérer tout le trafic destiné aux services publiés. Une passerelle d'API peut être déployée pour des environnements traditionnels (multicloud hybride ou HMC) ou natifs du cloud. La passerelle API met fin à tout le trafic entrant pour proposer plusieurs services tels que l'authentification, l'autorisation, la limitation du débit, le routage, la mise en cache, le déchargement SSL, le pare-feu des applications, etc. Il devient donc un élément essentiel de l'infrastructure.

Types de jetons

Les jetons échangés lors de l'accès à l'API sont généralement conformes au protocole OAuth/OpenID Connect (OIDC). Les jetons d'accès utilisés uniquement pour un « accès délégué » sont conformes au protocole OAuth, tandis que les jetons d'identification conformes à l'OIDC contiennent également des informations sur les utilisateurs.

Les jetons d'accès sont généralement des blobs de données opaques ou aléatoires. Cependant, il peut parfois s'agir de jetons signés conformes aux normes JWT (Json Web Token). Les jetons d'identification sont toujours des JWT signés.

Accès à l'API avec OAuth

Le type d'authentification OAuth sur une appliance NetScaler peut être utilisé pour gérer à la fois les protocoles OAuth et OIDC. OIDC est une extension du protocole OAuth.

OAuthAction sur une appliance NetScaler peut être utilisé pour gérer des clients interactifs tels que des navigateurs et des clients natifs tels que des applications clientes. Les clients interactifs sont redirigés vers Identity Provider pour se connecter à l'aide du protocole OIDC. Les clients natifs peuvent obtenir des jetons hors bande et les présenter à une appliance NetScaler pour y accéder.

> **Remarque :**
>
> Le jeton d'accès obtenu à partir des points de terminaison peut être mis en cache pour les demandes suivantes, améliorant ainsi les performances de l'API.

Pour configurer la prise en charge de la mise en cache des jetons à l'aide de l'interface de ligne de commande, tapez la commande suivante à l'invite de commandes :

```
set aaaparameter  - apITokenCache <ENABLED>
<!--NeedCopy-->
```

Les sections suivantes décrivent la méthode d'accès à l'API exécutée par les clients natifs.

Serveur virtuel pour l'accès aux API

Pour déployer une appliance NetScaler pour un accès à une API, un serveur virtuel de gestion du trafic (TM) est déployé avec l'authentification 401. Il est associé à un serveur virtuel d'authentification (authentification, autorisation et audit) pour héberger les politiques d'authentification et de session. L'extrait de configuration suivant crée l'un de ces serveurs virtuels.

```
Add lb vserver lb-api-access SSL <IP> 443 -authn401 On -AuthnVsName
   auth-api-access

Bind ssl vserver lb-api-access -certkeyName <ssl-cert-entity>

Add authentication vserver auth-api-access SSL
<!--NeedCopy-->
```

> **Remarque :**
>
> Vous devez lier un service au serveur virtuel de gestion du trafic et une politique d'authentification (avec OAuthAction décrite comme suit) au serveur virtuel d'authentification pour terminer la configuration.

Après avoir créé le serveur virtuel, il faut ajouter une OAuthAction ainsi que la politique correspondante. Il existe plusieurs autres options au sein d'une action OAuth en fonction du type de jeton et

d'autres mécanismes de sécurité.

Configuration OAuth pour les jetons d'identification

Les jetons d'identification sont toujours des JWT signés. C'est-à-dire qu'ils portent un en-tête, une charge utile et une signature. Comme il s'agit de jetons autonomes, une appliance NetScaler peut valider ces jetons localement. Pour valider ces jetons, l'appliance doit connaître la clé publique de la clé privée correspondante utilisée pour signer ces jetons.

Voici un exemple d'OAuthAction avec certains arguments obligatoires ainsi que « CertEndpoint ».

```
1   Add authentication OAuthAction oauth-api-access -clientid <your-
       client-id> -clientsecret <your-client-secret> -
       authorizationEndpoint <URL to which users would be redirected for
       login> -tokenEndpoint <endpoint at which tokens could be obtained>
        -certEndpoint <URL at which public keys of IdP are published>
2   <!--NeedCopy-->
```

Où,

- **Client ID** : chaîne unique qui identifie le fournisseur de services. Le serveur d'autorisation déduit la configuration du client en utilisant cet ID. Longueur maximale : 127.
- **Client Secret** : chaîne secrète établie par l'utilisateur et le serveur d'autorisation. Longueur maximale : 239.
- **AuthorizationEndpoint** : URL à laquelle les utilisateurs se connectent normalement (lorsqu'ils utilisent des clients interactifs).
- **TokenEndpoint** : URL sur le serveur d'autorisation sur laquelle les jetons/le code sont obtenus/échangés
- **CertEndpoint** : URL à laquelle le serveur d'autorisation publie les clés publiques utilisées pour signer les jetons. Le serveur d'autorisation peut publier plusieurs clés et choisir l'une d'entre elles pour signer les jetons.

> **Remarque :**
>
> Client ID/Client Secret/AuthorizationEndpoint/TokenEndpoint sont des paramètres facultatifs pour l'accès à l'API. Toutefois, il est recommandé de fournir des valeurs pour ces paramètres, car l'entité d'action peut être réutilisée à différentes fins.

Dans la configuration précédente, « CertEndpointPoint » est essentiel pour la validation du jeton d'identification. Ce point de terminaison contient les clés publiques du certificat utilisé pour signer les jetons. Ces clés publiques doivent correspondre à la spécification JWK (Json Web Keys).

Une fois que le CertEndpoint est configuré sur l'appliance NetScaler, il interroge régulièrement le point de terminaison (avec un intervalle par défaut d'un jour qui peut être personnalisé dans la configuration) pour maintenir les clés publiques à jour. Une fois les clés publiques disponibles, ADC peut effectuer une validation locale des jetons d'identification entrants.

Configuration OAuth pour les jetons d'accès opaques

Les jetons opaques ne peuvent pas être vérifiés localement sur l'appliance NetScaler. Ils doivent être validés sur le serveur d'autorisation. Une appliance NetScaler utilise le « protocole d'introspection » mentionné dans les spécifications OAuth afin de vérifier ces jetons. Une nouvelle option, IntroSpectURL, est fournie dans la configuration OAuth pour vérifier les jetons opaques.

```
1   set oauthAction oauth-api-acccess -introspectURL <URL of the
       Authorization Server for introspection>
2   <!--NeedCopy-->
```

Le format de l'API d'introspection est conforme à la spécification https://tools.ietf.org/html/rfc7662##section-2.1 suivante :

```
1   POST /introspect HTTP/1.1
2   Host: server.example.com
3   Accept: application/json
4   Content-Type: application/x-www-form-urlencoded
5   Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
6   token=mF_9.B5f-4.1JqM&token_type_hint=access_token
7   <!--NeedCopy-->
```

Politique de liaison au serveur virtuel d'authentification

Une fois OAuthAction créé, la politique correspondante doit être créée pour l'invoquer.

```
1   add authentication policy oauth-api-access -rule <> -action <oauth-
       api-access>
2
3   bind authentication vserver auth-api-access -policy oauth-api-access
       -pri 100
4   <!--NeedCopy-->
```

Paramètres de sécurité supplémentaires sur une appliance NetScaler

La validation des jetons inclut la vérification de la durée de vie des jetons. Les jetons en dehors du délai acceptable sont rejetés. Vous trouverez ci-dessous les paramètres supplémentaires pour une

sécurité accrue. Il est recommandé de toujours configurer certains d'entre eux.

Public : l'action OAuth peut être configurée avec le destinataire prévu du jeton. Tous les jetons sont comparés à cette URL configurée. Une appliance NetScaler possède une fonctionnalité supplémentaire selon laquelle le champ d'audience pointe réellement vers un modèle défini sur l'appliance. À l'aide de cet ensemble de modèles, un administrateur peut configurer plusieurs URL pour l'audience.

```
add policy patset oauth_audiences

bind patset oauth_audiences https://app1.company.com

bind patset oauth_audiences https://app2.company.com

bind patset oauth_audiences httpsL//app1.company.com/path1

set oAuthAccess oauth-api-access -audience oauth_audiences
<!--NeedCopy-->
```

Dans l'exemple précédent, plusieurs audiences sont spécifiées dans un ensemble de modèles. Par conséquent, un jeton entrant n'est autorisé que s'il contient l'une des URL configurées dans le jeu de modèles.

Émetteur : identité du serveur dont les jetons doivent être acceptés. Longueur maximale : 127. Il est recommandé de configurer l'émetteur des jetons dans l'action OAuth. Cela garantit que les jetons émis par un mauvais serveur d'autorisation ne sont pas autorisés.

SkewTime : Spécifie le décalage d'horloge autorisé en nombre de minutes qu'une appliance NetScaler autorise sur un jeton entrant. Par exemple, si SkewTime est 10, le jeton sera valide de (heure actuelle - 10) min à (heure actuelle + 10) min, soit 20 min en tout. Valeur par défaut : 5

AllowedAlgorithms : cette option permet à l'administrateur de restreindre certains algorithmes dans les jetons entrants. Par défaut, toutes les méthodes prises en charge sont autorisées. Cependant, vous pouvez les contrôler à l'aide de cette option.

La configuration suivante garantit que seuls les jetons utilisant RS256 et RS512 sont autorisés :

```
set oAuthAction oauth-api-access -allowedAlgorithms RS256 RS512
<!--NeedCopy-->
```

Une fois la configuration ci-dessus effectuée, seuls les jetons utilisant RS256 et RS512 sont autorisés.

Contourner l'authentification à certains trafics

Dans de nombreux cas, certaines API de découverte sont accessibles publiquement aux clients. Ces API révèlent généralement la configuration et les fonctionnalités du service lui-même. Un administra-

teur peut configurer l'appliance NetScaler pour contourner l'authentification à partir de ces URL de métadonnées en utilisant la politique « Aucune authentification » décrite comme suit :

```
add authentication policy auth-bypass-policy -rule <> -action
   NO_AUTHN

bind authentication vserver auth-api-access -policy auth-bypass-
   policy -pri 110
<!--NeedCopy-->
```

NO_AUTHN est une action implicite qui entraîne la fin de l'authentification lorsque la règle correspond. Il existe d'autres utilisations de l'action NO_AUTHN qui dépassent le cadre de l'accès à l'API.

Authentification LDAP

June 20, 2023

Comme pour les autres types de stratégies d'authentification, une stratégie d'authentification LDAP (Lightweight Directory Access Protocol) comprend une expression et une action. Après avoir créé une stratégie d'authentification, vous la liez à un serveur virtuel d'authentification et vous lui attribuez une priorité. Lorsque vous la liez, vous la désignez également en tant que stratégie principale ou secondaire. Outre les fonctions d'authentification standard, LDAP peut rechercher sur d'autres serveurs Active Directory (AD) des comptes d'utilisateurs qui n'existent pas localement. Cette fonction s'appelle support d'informations d'identification ou recherche d'informations d'identification.

Normalement, vous configurez NetScaler pour qu'il utilise l'adresse IP du serveur d'authentification lors de l'authentification. Avec les serveurs d'authentification LDAP, vous pouvez également configurer l'ADC pour utiliser le nom de domaine complet du serveur LDAP au lieu de son adresse IP pour authentifier les utilisateurs. L'utilisation d'un nom de domaine complet peut simplifier une configuration d'authentification, d'autorisation et d'audit autrement beaucoup plus complexe dans des environnements où le serveur d'authentification peut se trouver sur plusieurs adresses IP, mais utilise toujours un seul nom de domaine complet. Pour configurer l'authentification à l'aide du nom de domaine complet d'un serveur au lieu de son adresse IP, vous suivez le processus de configuration normal sauf lors de la création de l'action d'authentification. Lors de la création de l'action, vous utilisez le paramètre **ServerName** au lieu du paramètre **ServerIP** et vous remplacez son adresse IP par le nom de domaine complet du serveur.

Avant de décider de configurer l'ADC pour utiliser l'adresse IP ou le nom de domaine complet de votre serveur LDAP pour authentifier les utilisateurs, considérez que la configuration de l'authentification, de l'autorisation et de l'audit pour s'authentifier auprès d'un nom de domaine complet au lieu d'une adresse IP ajoute une étape supplémentaire au processus d'authentification. Chaque fois que

l'ADC authentifie un utilisateur, il doit résoudre le nom de domaine complet. Si un grand nombre d'utilisateurs tentent de s'authentifier simultanément, les recherches DNS qui en résultent peuvent ralentir le processus d'authentification.

La prise en charge des références LDAP est désactivée par défaut et ne peut pas être activée globalement. Elle doit être explicitement activée pour chaque action LDAP. Assurez-vous que le serveur AD accepte les mêmes `binddn credentials` que celles utilisées avec le serveur de référence (GC). Pour activer la prise en charge des références, vous configurez une action LDAP pour suivre les références et spécifiez le nombre maximum de références à suivre.

Si la prise en charge des références est activée et que NetScaler reçoit une réponse LDAP_REFERRAL à une demande, l'authentification, l'autorisation et l'audit suivent la référence au serveur Active Directory (AD) contenue dans la référence et effectuent la mise à jour sur ce serveur. Tout d'abord, l'authentification, l'autorisation et l'audit recherchent le serveur de référence dans le DNS et se connectent à ce serveur. Si la stratégie de référence nécessite SSL/TLS, elle se connecte via SSL/TLS. Elle se lie ensuite au nouveau serveur avec le `binddn credentials` qu'elle a utilisé avec le serveur précédent, et effectue l'opération qui a généré la référence. Cette fonctionnalité est transparente pour l'utilisateur.

Les numéros de port des connexions LDAP sont les suivants :

- 389 pour les connexions LDAP non sécurisées (pour le LDAP en texte brut)
- 636 pour les connexions LDAP sécurisées (pour SSL LDAP)
- 3268 pour les connexions LDAP non sécurisées Microsoft (pour le serveur de catalogue global en texte brut)
- 3269 pour les connexions LDAP sécurisées Microsoft (pour le serveur de catalogue global SSL)

Le tableau suivant contient des exemples de champs d'attribut utilisateur pour les serveurs LDAP :

serveur LDAP	Attribut utilisateur	Sensibles à
Serveur Microsoft Active Directory	sAMAccountName	Non
Novell eDirectory	ou	Oui
IBM Directory Server	uid	Oui
Lotus Domino	CN	Oui
Sun ONE directory (anciennement iPlanet)	uid ou cn	Oui

Ce tableau contient des exemples de nom unique de base :

serveur LDAP	DN de base
Serveur Microsoft Active Directory	DC =citrix, DC = local
Novell eDirectory	ou=users, ou=dev
IBM Directory Server	cn=utilisateurs
Lotus Domino	OU=ville, O=Citrix, C = États-Unis
Sun ONE directory (anciennement iPlanet)	OU=personnes, dc =citrix, dc = com

Le tableau suivant contient des exemples de nom unique de liaison :

serveur LDAP	DN de liaison
Serveur Microsoft Active Directory	CN = administrateur, CN = utilisateurs, DC =citrix, DC = local
Novell eDirectory	cn=admin, o=citrix
IBM Directory Server	LDAP_DN
Lotus Domino	CN=Notes Administrateur, O=Citrix, C=US
Sun ONE directory (anciennement iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

Pour plus d'informations sur la configuration des stratégies d'authentification en général, voir Stratégies d'authentification. Pour plus d'informations sur les expressions NetScaler utilisées dans la règle de stratégie, consultez la section Stratégies etexpressions.

Pour créer un serveur d'authentification LDAP à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes :

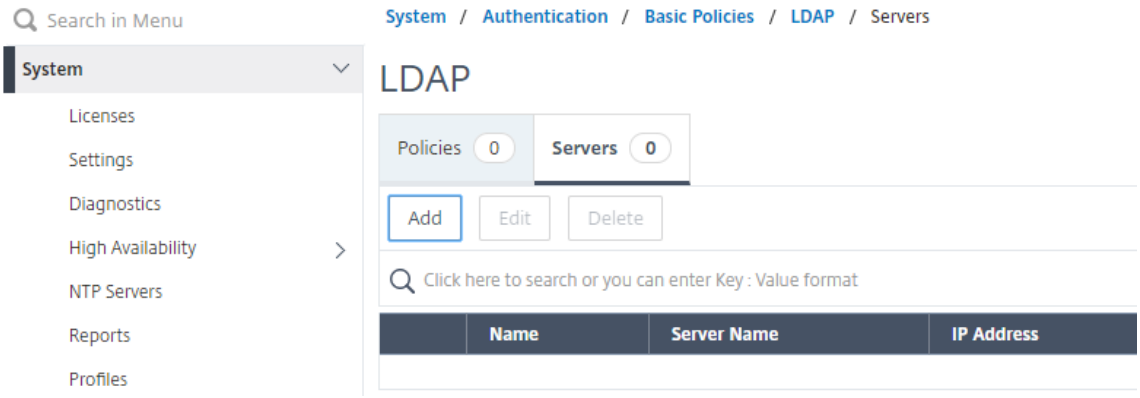
```
add authentication ldapAction <name> {
 -serverIP }
  <ip_addr|ipv6_addr|> | {
 -serverName <string> }
  }
```

Exemple

```
add authentication ldapAction ldap_server -serverip 1.1.1.1 -serverName
    ldap_test
```


Pour créer un serveur d'authentification LDAP à l'aide de l'interface graphique

1. Accédez à **Système > Authentification > Stratégies de base > LDAP > Serveurs > Ajouter**.



2. Sur la page **Créer un serveur LDAP d'authentification**, configurez les paramètres du serveur LDAP.
3. Cliquez sur **Create**.

Pour activer une stratégie d'authentification à l'aide de la CLI

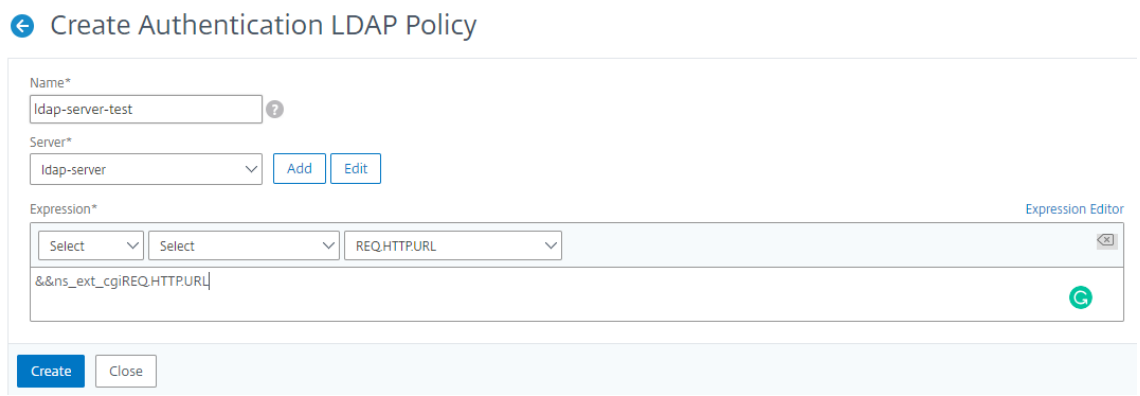
```
add authentication ldappolicy <name> <rule> [<reqAction>]
```

Exemple :

```
add authentication ldappolicy ldap-service-policy ns_true ldap_Server
```

Pour créer une stratégie d'authentification LDAP à l'aide de l'interface graphique

1. Accédez à **Système > Authentification > Stratégies de base > LDAP > Stratégies > Ajouter**
2. Sur la page **Créer une stratégie LDAP d'authentification**, configurez les paramètres de la stratégie LDAP.



3. Cliquez sur **Create**.

> **Remarque**
>
> Vous pouvez configurer des serveurs/stratégies LDAP via l'onglet **Sécurité** . Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies de base > LDAP > Serveurs/Stratégies**.

Pour activer la prise en charge des références LDAP à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
set authentication ldapAction <name> -followReferrals ON
set authentication ldapAction <name> -maxLDAPReferrals <integer>
<!--NeedCopy-->
```

Exemple

```
set authentication ldapAction ldapAction-1 -followReferrals ON
set authentication ldapAction ldapAction-1 -maxLDAPReferrals 2
<!--NeedCopy-->
```

Prise en charge de l'authentification basée sur les clés pour les utilisateurs LDAP

Avec l'authentification par clé, vous pouvez désormais extraire la liste des clés publiques stockées sur l'objet utilisateur dans le serveur LDAP via SSH. Au cours du processus d'authentification basée sur les rôles (RBA), l'appliance NetScaler doit extraire les clés SSH publiques du serveur LDAP. La clé publique récupérée, compatible avec SSH, doit vous permettre de vous connecter via la méthode RBA.

Un nouvel attribut « sshPublicKey » est introduit dans les commandes « add authentication ldapAction » et « set authentication ldapAction ». En utilisant cet attribut, vous pouvez obtenir les avantages suivants :

- Peut stocker la clé publique récupérée, et l'action LDAP utilise cet attribut pour récupérer les informations de clé SSH à partir du serveur LDAP.
- Peut extraire des noms d'attributs d'une taille maximale de 24 Ko.

> Remarque
>
> Le serveur d'authentification externe, tel que LDAP, est utilisé uniquement pour récupérer les informations de clé SSH. Il n'est pas utilisé à des fins d'authentification.

Voici un exemple de flux d'événements via SSH :

- Le démon SSH envoie une demande AAA_AUTHENTICATE avec le champ de mot de passe vide au port du démon d'authentification, d'autorisation et d'audit.

- Si LDAP est configuré pour stocker la clé publique SSH, l'authentification, l'autorisation et l'audit répondent avec l'attribut « SSHPublicKey » ainsi que d'autres attributs.
- Le démon SSH vérifie ces clés avec les clés client.
- Le démon SSH transmet le nom d'utilisateur dans la charge utile de la demande, et l'authentification, l'autorisation et l'audit renvoient les clés spécifiques à cet utilisateur ainsi que les clés génériques.

Pour configurer l'attribut SSHPublicKey, tapez les commandes suivantes à l'invite de commandes :

- Avec l'opération d'ajout, vous pouvez ajouter l'attribut « SSHPublicKey » lors de la configuration de la commande `ldapAction`.

```
add authentication ldapAction <name> {
-serverIP <ip_addr|ipv6_addr|*> | {
-serverName <string> }
 }
 [-serverPort <port>] … [-Attribute1 <string>] … [-Attribute16
    <string>][-sshPublicKey <string>][-authentication off]
<!--NeedCopy-->
```

- Avec l'opération set, vous pouvez configurer l'attribut « SSHPublicKey » sur une commande LDAPAction déjà ajoutée.

```
set authentication ldapAction <name> [-sshPublicKey <string>][-
   authentication off]
<!--NeedCopy-->
```

Prise en charge des attributs nom-valeur pour l'authentification LDAP

Vous pouvez désormais configurer les attributs de l'authentification LDAP avec un nom unique et des valeurs. Les noms sont configurés dans le paramètre d'action LDAP et les valeurs sont obtenues en interrogeant le nom. En utilisant cette fonctionnalité, un administrateur de l'appliance NetScaler peut désormais bénéficier des avantages suivants :

- Réduit les efforts des administrateurs en mémorisant l'attribut par son nom (et pas seulement par sa valeur)
- Améliore la recherche pour interroger la valeur d'attribut associée à un nom
- Fournit une option pour extraire plusieurs attributs

Pour configurer cette fonctionnalité à l'invite de commande de l'appliance NetScaler, tapez :

```
add authentication ldapAction <name> [-Attributes <string>]
<!--NeedCopy-->
```


Exemple

```
add authentication ldapAction ldapAct1 -attributes "company, mail"
<!--NeedCopy-->
```

Prise en charge de la validation de l'authentification LDAP de bout en bout

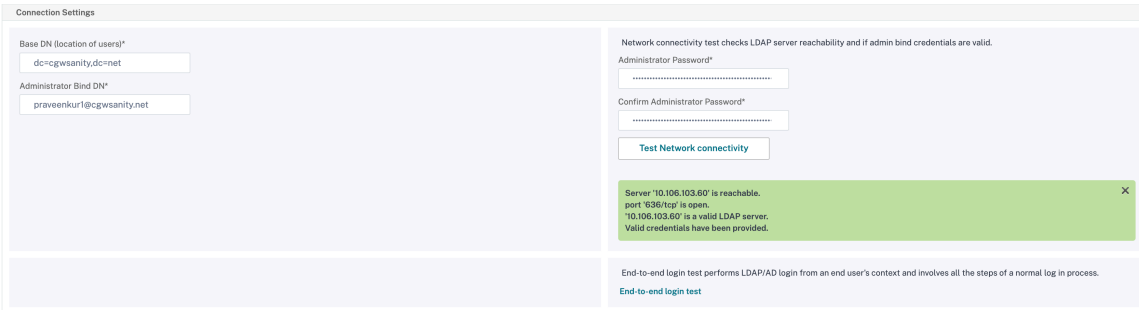
L'appliance NetScaler peut désormais valider l'authentification LDAP de bout en bout via l'interface graphique. Pour valider cette fonctionnalité, un nouveau bouton « test » est introduit dans l'interface graphique. Un administrateur d'appliance NetScaler peut utiliser cette fonctionnalité pour bénéficier des avantages suivants :

- Consolide le flux complet (moteur de paquets, démon NetScaler AAA, serveur externe) pour fournir une meilleure analyse
- Réduction du temps de validation et de dépannage des problèmes liés à des scénarios individuels

Vous disposez de deux options pour configurer et afficher les résultats des tests de l'authentification de bout en bout LDAP à l'aide de l'interface graphique.

Depuis l'option système

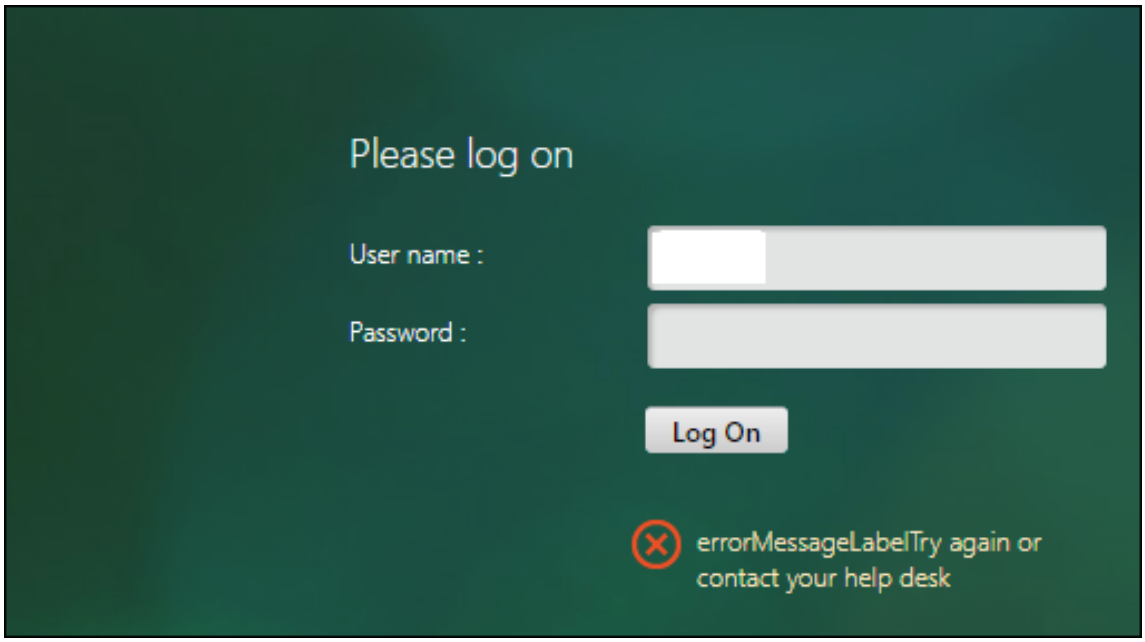
1. Accédez à **Système > Authentification > Stratégies de base > LDAP,** cliquez sur l'onglet **Serveurs** .
2. Sélectionnez l'**action LDAP** disponible dans la liste.
3. Sur la page **Configurer le serveur LDAP d'authentification**, faites défiler vers le bas jusqu'à la section **Paramètres de connexion** .
4. Cliquez sur **Tester la connectivité réseau** pour vérifier la connexion au serveur LDAP. Vous pouvez afficher un message contextuel de connexion réussie au serveur LDAP avec les détails du port TCP et l'authenticité des informations d'identification valides.



5. Pour afficher l'authentification LDAP de bout en bout, cliquez sur le lien de **test de connexion de bout en bout** .

6. Sur la page **Test de connexion de bout en bout**, cliquez sur **Test**.
   - Sur la page d'authentification, saisissez les informations d'identification valides pour vous connecter. L'écran de réussite s'affiche.

   - Si l'authentification échoue, l'écran d'erreur s'affiche.

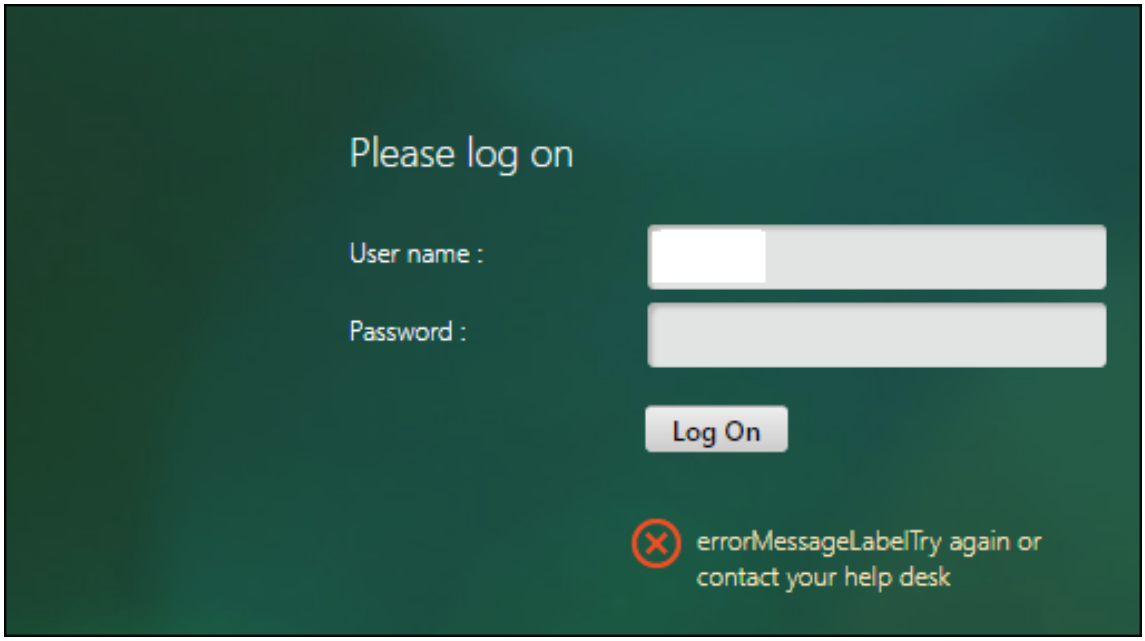


Depuis l'option Authentification

1. Accédez à **Authentification > Tableau de bord**, sélectionnez l'action LDAP disponible dans la liste.
2. Sur la page **Configurer le serveur LDAP d'authentification**, vous avez deux options dans la section **Paramètres de connexion** .
3. Pour vérifier la connexion au serveur LDAP, cliquez sur l'onglet **Tester l'accessibilité LDAP** . Vous pouvez afficher un message contextuel de connexion réussie au serveur LDAP avec les détails du port TCP et l'authenticité des informations d'identification valides.

4. Pour afficher l'état de l'authentification LDAP de bout en bout, cliquez sur le lien **Tester la connexion de l'utilisateur final** .
5. Sur la page **Tester la connexion de l'utilisateur final**, cliquez sur **Tester**.
   - Sur la page d'authentification, saisissez les informations d'identification valides pour vous connecter. L'écran de réussite s'affiche.

   - Si l'authentification échoue, l'écran d'erreur s'affiche.



Notification d'expiration de 14 jours pour l'authentification LDAP

L'appliance NetScaler prend désormais en charge la notification d'expiration des mots de passe de 14 jours pour l'authentification basée sur LDAP. En utilisant cette fonctionnalité, les administrateurs peuvent informer les utilisateurs finaux du délai d'expiration du mot de passe en jours. La notification d'expiration du mot de passe de 14 jours est un précurseur de la réinitialisation en libre-service du mot de passe (SSPR).

> **Remarque**
>
> La valeur maximale ou le délai seuil en jours pour la notification d'expiration du mot de passe est de 255 jours.

Avantages de la notification d'expiration du mot

- Permettez aux utilisateurs de réinitialiser eux-mêmes leurs mots de passe et offrez aux administrateurs un moyen flexible d'informer l'utilisateur final de l'expiration de leur mot de passe en quelques jours.
- Élimine la dépendance des utilisateurs finaux pour suivre les jours d'expiration de leurs mots
- Envoie des notifications à la page du portail VPN aux utilisateurs (en fonction du nombre de jours) pour modifier leur mot de passe avant l'expiration.

> **Remarque**
>
> Cette fonctionnalité n'est applicable que pour les schémas d'authentification basés sur LDAP, et non pour RADIUS ou TACACS.

Comprendre la notification de mot de passe de 14 jours

L'appliance NetScaler récupère deux attributs (`Max-Pwd-Age and Pwd-Last-Set`) depuis le serveur d'authentification LDAP.

- **Max-Pwd-Age.** Cet attribut indique la durée maximale, par intervalles de 100 nanosecondes, jusqu'à ce que le mot de passe soit valide. La valeur est stockée sous la forme d'un grand nombre entier qui représente le nombre d'intervalles de 100 nanosecondes à partir du moment où le mot de passe a été défini avant son expiration.
- **Pwd-Last-Set.** Cet attribut détermine la date et l'heure auxquelles le mot de passe d'un compte a été modifié pour la dernière fois.

En récupérant les deux attributs depuis le serveur d'authentification LDAP, l'appliance NetScaler détermine le temps restant avant l'expiration du mot de passe pour un utilisateur particulier. Ces informations sont collectées lorsque les informations d'identification de l'utilisateur sont validées sur le serveur d'authentification et qu'une notification est renvoyée à l'utilisateur.

Un nouveau paramètre « PwdExpiryNotification » est introduit dans la commande `set aaa parameter`. En utilisant ce paramètre, un administrateur peut suivre le nombre de jours restants pour l'expiration du mot de passe. L'appliance NetScaler peut désormais commencer à informer l'utilisateur final de l'expiration de son mot de passe.

> **Remarque**
>
> Actuellement, cette fonctionnalité ne fonctionne que pour les serveurs d'authentification dotés

> de serveurs Microsoft AD avec implémentation LDAP. La prise en charge des serveurs basés sur OpenLDAP sera ciblée ultérieurement.

Voici un exemple de flux d'événements pour définir une notification d'expiration de mot de passe de 14 jours :

1. À l'aide de l'appliance NetScaler, un administrateur définit un délai (14 jours) pour l'expiration du mot de passe.
2. L'utilisateur envoie une demande HTTP ou HTTPS pour accéder à une ressource sur le serveur principal.
3. Avant de fournir l'accès, l'appliance NetScaler valide les informations d'identification de l'utilisateur à l'aide de ce qui est configuré sur le serveur d'authentification LDAP.
4. Parallèlement à cette requête adressée au serveur d'authentification, l'appliance NetScaler transmet la demande visant à récupérer les détails des deux attributs ().`Max-Pwd-Age and Pwd-Last-Set`
5. En fonction du temps restant pour que le mot de passe expire, une notification d'expiration s'affiche.
6. L'utilisateur prend ensuite les mesures appropriées pour mettre à jour le mot de passe.

Pour configurer la notification d'expiration de 14 jours à l'aide de l'interface de ligne de commande

> **Remarque**
>
> La notification d'expiration de 14 jours peut être configurée pour les cas d'utilisation d'un VPN sans client et d'un VPN complet, et non pour le proxy ICA.

À l'invite de commandes, tapez les commandes suivantes :

```
set aaa parameter  - pwdExpiryNotificationDays <positive_integer>

show aaa parameter
<!--NeedCopy-->
```

Exemple

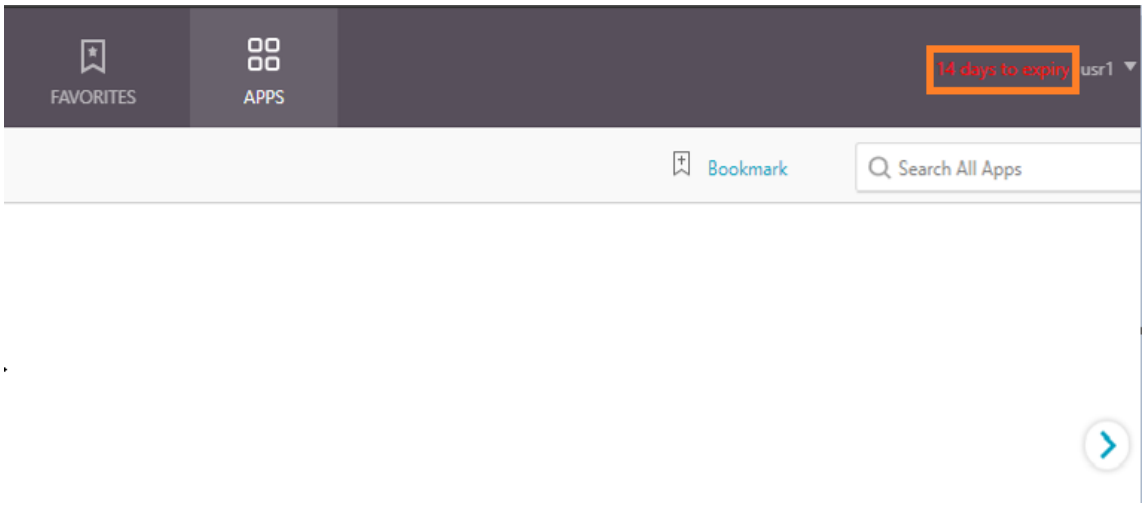
```
    > set aaa parameter -pwdExpiryNotificationDays 14
    Done
    > show aaa parameter                          Configured AAA
       parameters  EnableStaticPageCaching: YES
       EnableEnhancedAuthFeedback: NO  DefaultAuthType: LOCAL
       MaxAAAUsers:           Unlimited
                                          AAAD nat ip: None
                  EnableSessionStickiness : NO  aaaSessionLoglevel :
```



```
          INFORMATIONAL                AAAD Log Level : INFORMATIONAL
                              Dynamic address: OFF
4         GUI mode: ON
5         Max Saml Deflate Size: 1024              Password Expiry
             Notification Days: 14
6 <!--NeedCopy-->
```

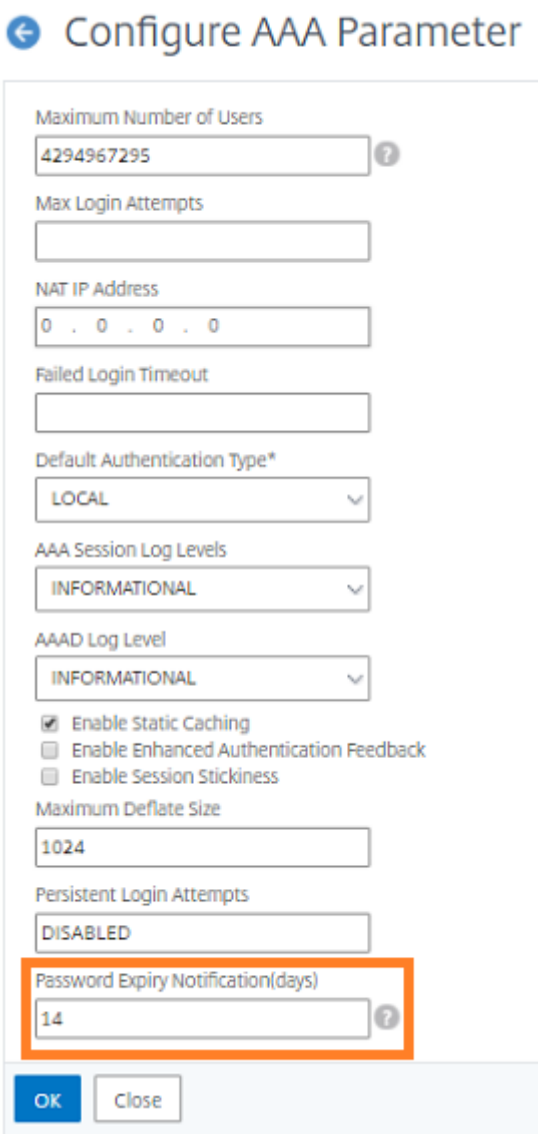
Pour configurer une notification d'expiration de 14 jours à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Paramètres d'authentification**.
2. Cliquez sur **Modifier les paramètres AAA d'authentification**.
3. Sur la page **Configurer le paramètre AAA**, spécifiez les jours dans le champ **Notification d'expiration du mot de passe (jours)** .



4. Cliquez sur **OK.**

   La notification s'affiche dans le coin supérieur droit de la page du portail VPN.



Configurer l'authentification LDAP sur l'appliance NetScaler à des fins de gestion

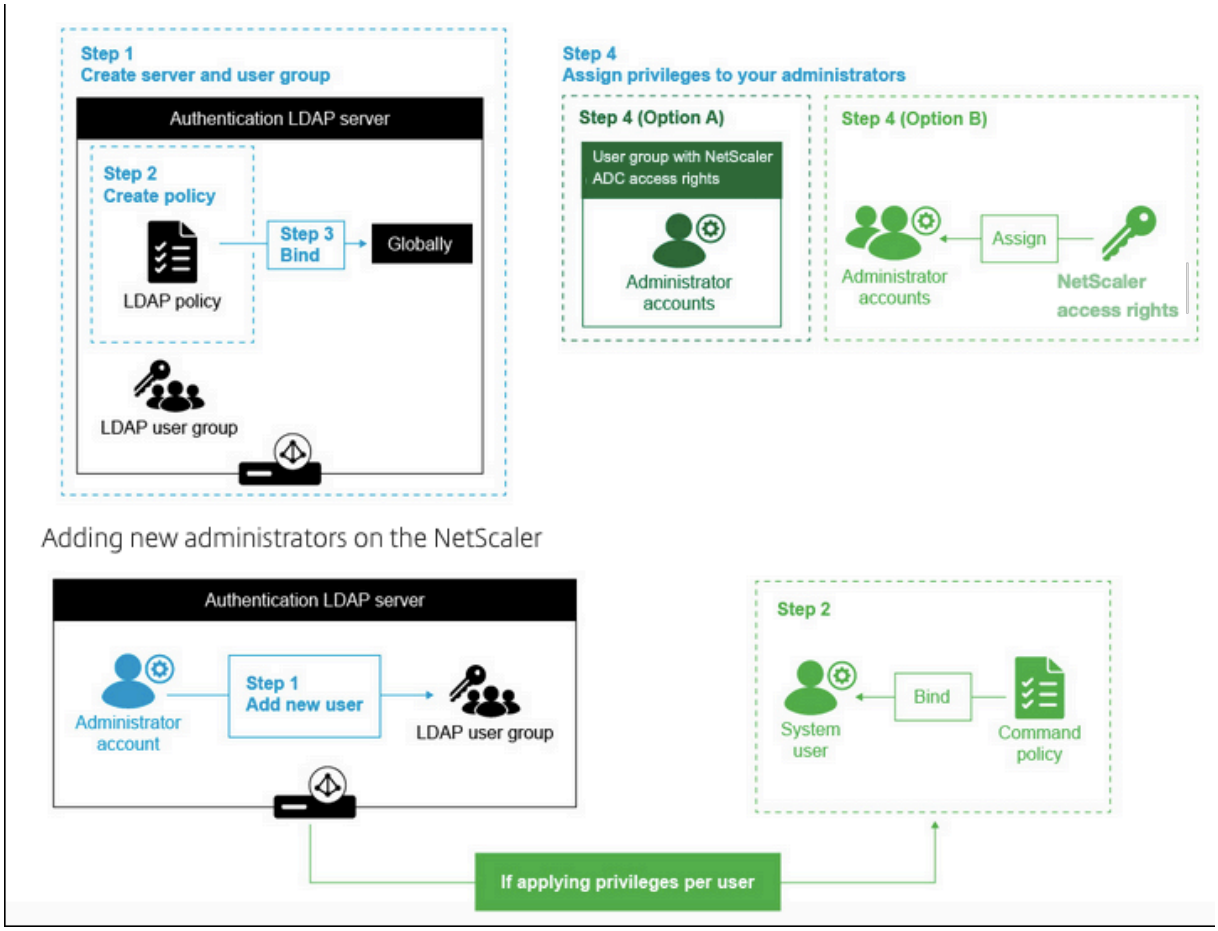
May 5, 2023

Vous pouvez configurer la connexion utilisateur à l'appliance NetScaler à l'aide des informations d'identification Active Directory (nom d'utilisateur et mot de passe) à des fins de gestion (superutilisateur, lecture seule, privilèges réseau, etc.).

Composants requis

- Serveurs de contrôleurs de domaine Windows Active Directory
- Un groupe de domaines dédié pour les administrateurs NetScaler
- NetScaler Gateway 10.1 et versions ultérieures

Les figures suivantes illustrent l'authentification LDAP sur l'appliance NetScaler.

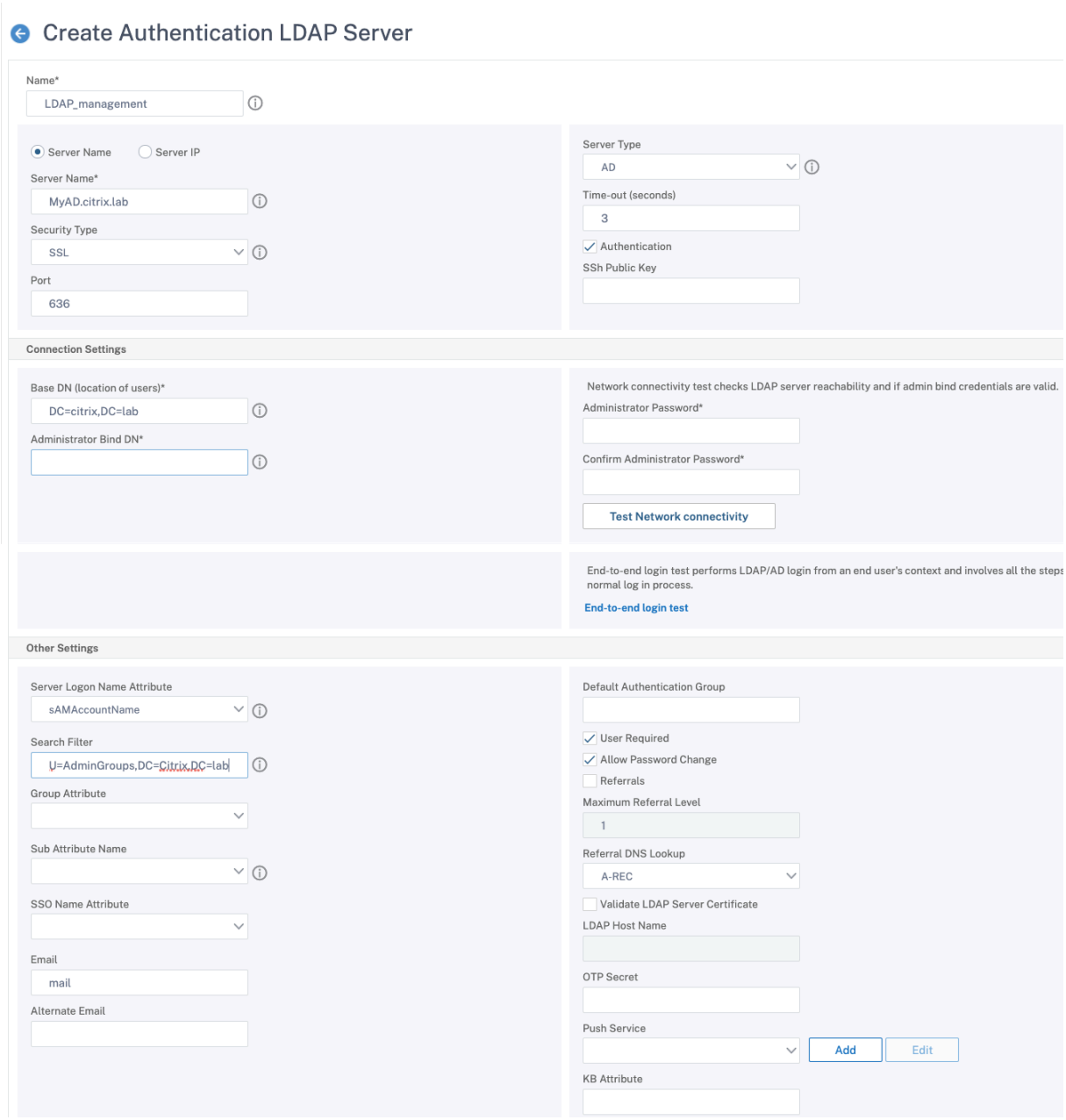


Étapes de configuration de haut niveau

1. Création d'un serveur LDAP
2. Création d'une stratégie LDAP
3. Lier la stratégie LDAP
4. Attribuez des privilèges à vos administrateurs de l'une des manières suivantes :
    - Appliquer les privilèges sur le groupe
    - Appliquer des privilèges individuellement pour chaque utilisateur

Création d'un serveur LDAP d'authentification

1. Accédez à **Système > Authentification > LDAP**.
2. Cliquez sur l'onglet **Serveur**, puis sur **Ajouter**.
3. Terminez la configuration, puis cliquez sur **Créer**.



Remarque :

Dans cet exemple, l'accès est limité à l'appliance NetScaler en filtrant l'authentification en fonction de l'appartenance au groupe d'utilisateurs en définissant le filtre de recherche. La valeur utilisée pour cet exemple est - & (memberof=CN=NSG_Admin, OU=AdminGroups, DC=Citrix,

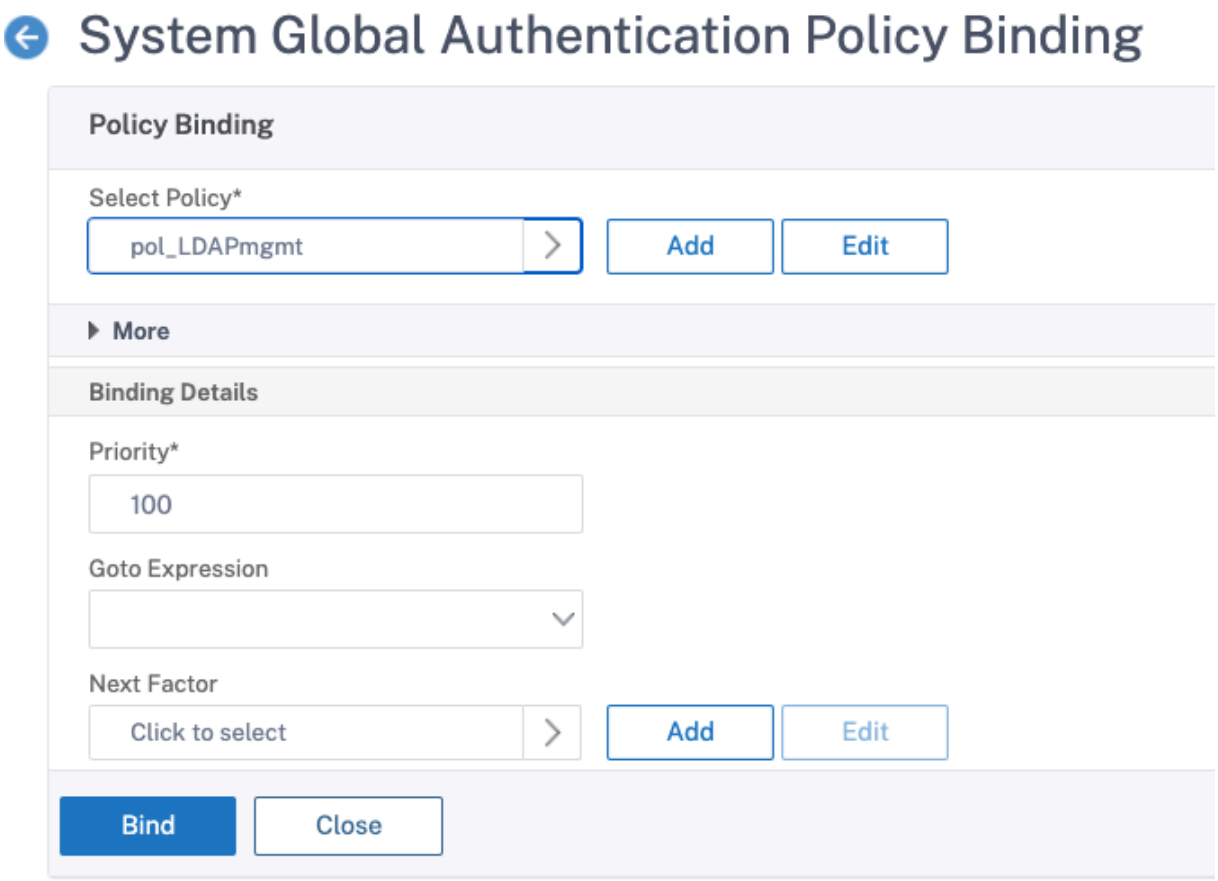
> DC=Lab)

Création d'une stratégie LDAP

1. Accédez à **Système > Authentification > Politiques avancées > Stratégie**.
2. Cliquez sur **Ajouter**.
3. Entrez un nom pour la stratégie, sélectionnez le serveur que vous avez créé au cours des étapes précédentes.
4. Dans le champ de texte Expression, saisissez l'expression appropriée, puis cliquez sur **Créer**.

Liez la stratégie LDAP globalement

1. Accédez à **Système > Authentification > Politiques avancées > Stratégie**.
2. Dans la page Stratégies d'authentification, cliquez sur **Liaisons globales**.
3. Sélectionnez la stratégie que vous avez créée (dans cet exemple, POL_LDAPMgmt).
4. Choisissez une priorité en conséquence (plus le nombre est bas, plus la priorité est élevée)
5. Cliquez sur **Lier,** puis sur **Terminé**. Une coche verte apparaît dans la colonne **Globally Bound** .



Attribuez des privilèges à vos administrateurs

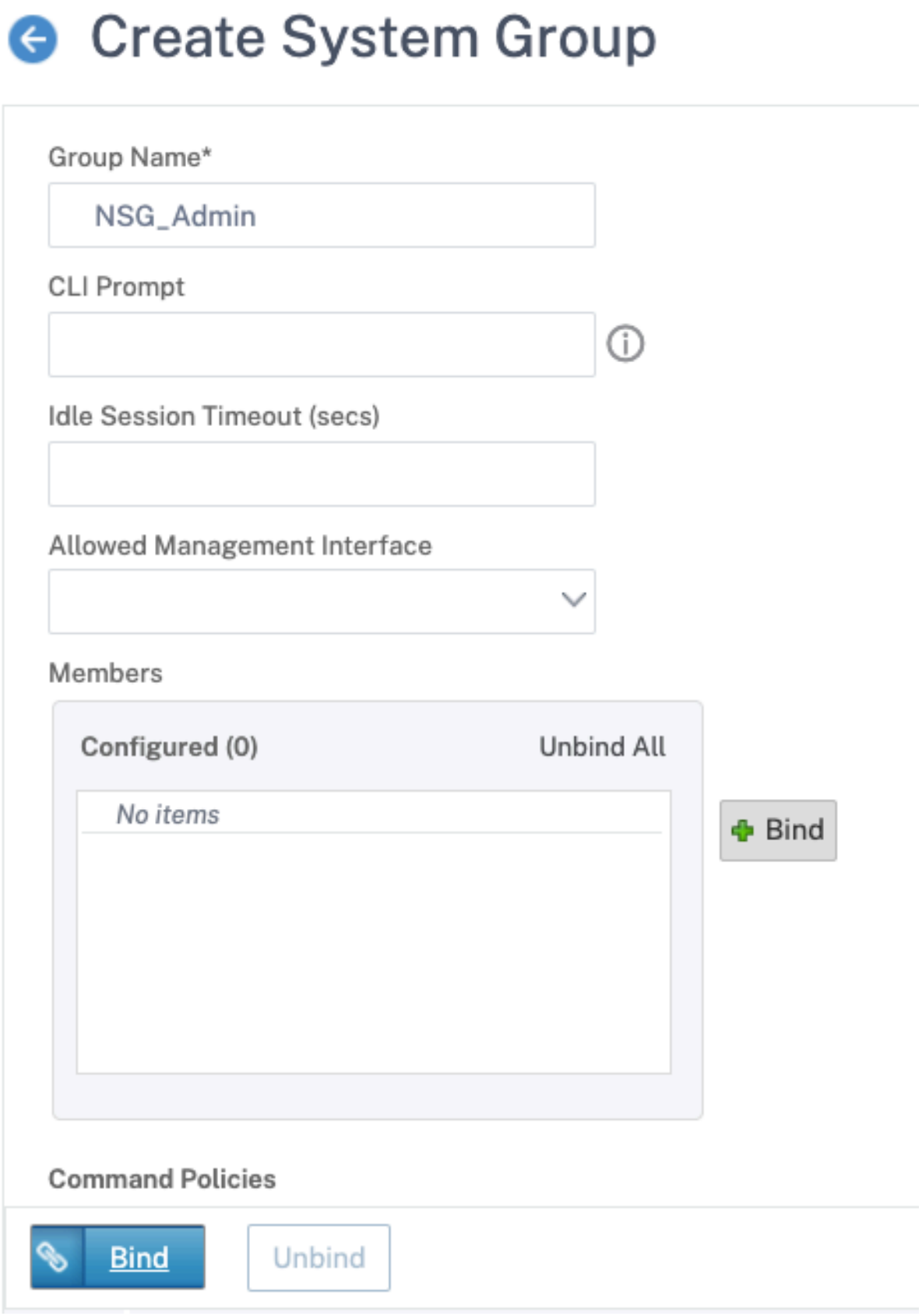
Vous pouvez choisir l'une des deux options suivantes.

- **Appliquer des privilèges à un groupe :** ajoutez un groupe dans l'appliance NetScaler et attribuez les mêmes droits d'accès à chaque utilisateur membre de ce groupe.
- **Appliquez des privilèges individuellement pour chaque utilisateur :** créez chaque compte administrateur utilisateur et attribuez des droits à chacun d'eux.

Appliquer des privilèges sur un groupe

Lorsque vous appliquez des privilèges à un groupe, les utilisateurs membres du groupe Active Directory configuré dans le filtre de recherche (dans cet exemple, NSG_Admin) peuvent se connecter à l'interface de gestion NetScaler et disposer d'une politique de commande pour les superutilisateurs.

1. Accédez à **Système > Administration des utilisateurs > Groupes**.
2. Entrez les détails conformément à la condition requise, puis cliquez sur **Créer**.



Vous avez défini le groupe Active Directory auquel appartiennent les utilisateurs ainsi que le niveau de stratégie de commande qui doit être associé au compte lors de la connexion. Vous pouvez ajouter de nouveaux utilisateurs administrateurs au groupe LDAP que vous avez configuré dans le filtre de recherche.

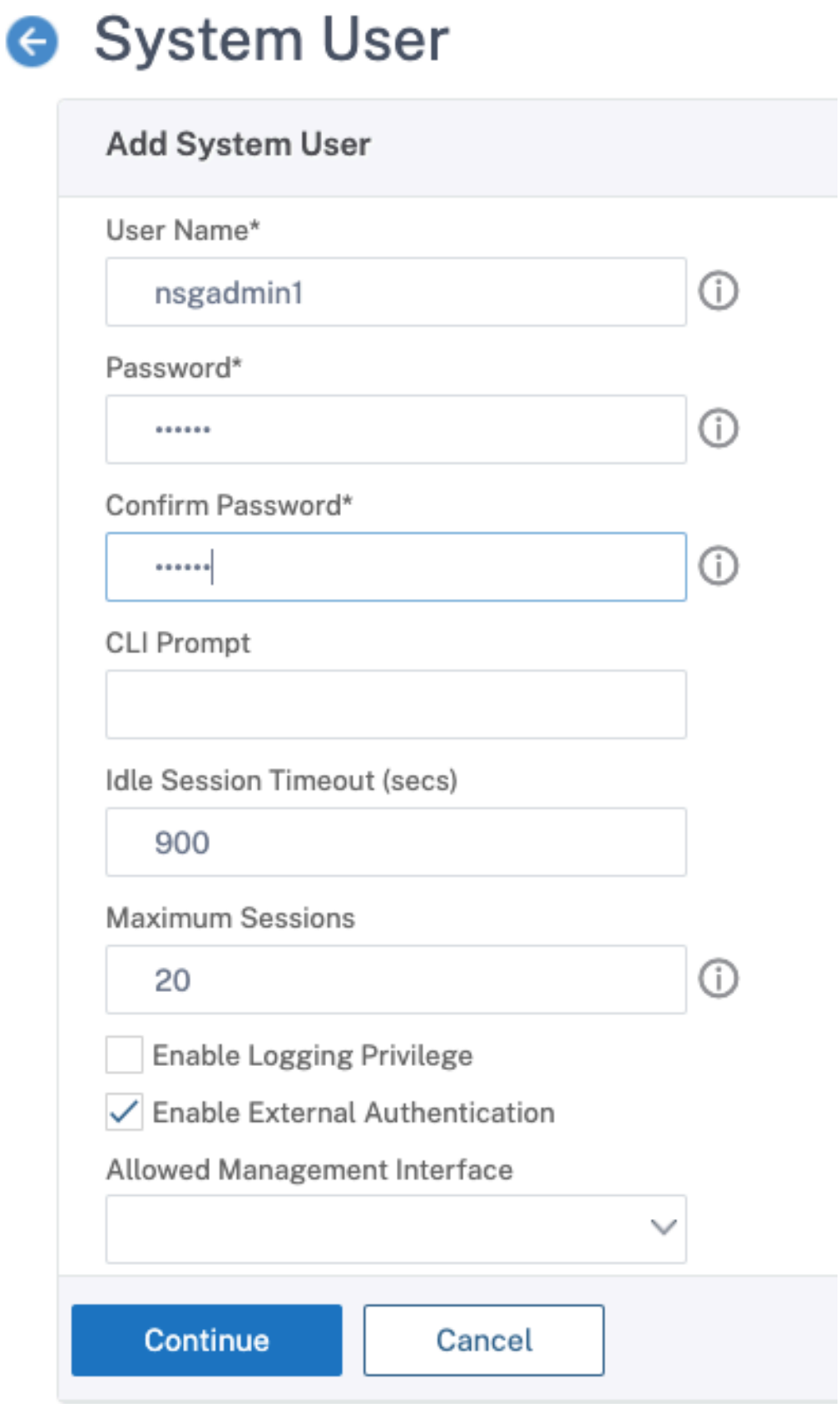
> **Remarque :**
>
> Le nom du groupe doit correspondre à l'enregistrement Active Directory.

Appliquer des privilèges individuellement pour chaque utilisateur

Dans ce scénario, les utilisateurs membres de votre groupe Active Directory configuré dans le filtre de recherche (dans cet exemple, NSG_Admin) peuvent se connecter à l'interface de gestion NetScaler mais ne disposent d'aucun privilège tant que vous n'avez pas créé l'utilisateur spécifique sur l'appliance NetScaler et que vous y liez la politique de commande.

1. Accédez à **Système > Administration des utilisateurs > Utilisateurs**.
2. Cliquez sur **Ajouter**.
3. Entrez les détails conformément au besoin.

   Remarque : Assurez-vous de sélectionner **Activer l'authentification externe**.



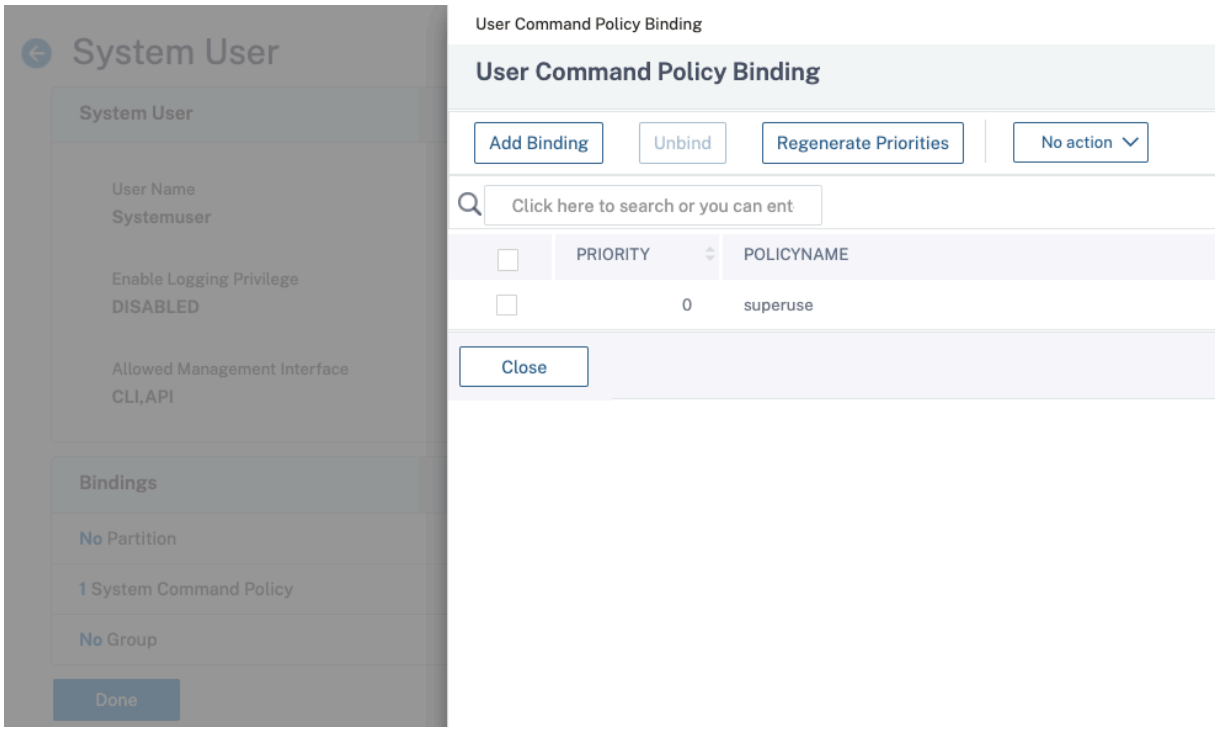
1. Cliquez sur **Continuer**.

Vous avez défini l'utilisateur Active Directory et le niveau de stratégie de commande qui doit être associé au compte lors de la connexion.

> **Remarque :**
>
> - Le nom d'utilisateur doit correspondre à l'enregistrement Active Directory de l'utilisateur existant.
> - Lorsque vous ajoutez un utilisateur à NetScaler pour une authentification externe, vous devez fournir un mot de passe si l'authentification externe n'est pas disponible. Pour que l'authentification externe fonctionne correctement, le mot de passe interne ne doit pas être identique au mot de passe LDAP du compte d'utilisateur.

Ajouter une stratégie de commande à l'utilisateur

1. Accédez à **Système > Administration des utilisateurs > Utilisateurs**.
2. Sélectionnez l'utilisateur que vous avez créé, puis cliquez sur **Modifier.**
3. Dans Liaisons, cliquez sur **Stratégie de commande système**.
4. Sélectionnez la stratégie de commande appropriée à appliquer à votre utilisateur.
5. Cliquez sur **Lier,** puis sur **Fermer**.



Pour ajouter d'autres administrateurs ;

- Ajoutez les utilisateurs administrateurs au groupe LDAP que vous avez configuré sur le filtre de recherche.

- Créez l'utilisateur du système dans NetScaler et attribuez la politique de commande appropriée.

Pour configurer l'authentification LDAP sur l'appliance NetScaler à des fins de gestion à l'aide de l'interface de ligne de commande

Utilisez les commandes suivantes comme référence pour configurer l'ouverture de session pour un groupe disposant de privilèges de superutilisateur sur l'interface de ligne de commande de l'appliance NetScaler.

1. Création d'un serveur LDAP

```
add authentication ldapAction LDAP_mgmt -serverIP myAD.citrix.lab
    -serverPort 636 -ldapBase "DC=citrix,DC=lab" -ldapBindDn
    readonly@citrix.lab -ldapBindDnPassword -ldapLoginName
    sAMAccountName -searchFilter "&(memberof=CN=NSG_Admin,OU=
    AdminGroups,DC=citrix,DC=lab)" -groupAttrName memberOf
<!--NeedCopy-->
```

2. Création et stratégie LDAP

```
add authentication ldapPolicy pol_LDAPmgmt ns_true LDAP_mgmt
<!--NeedCopy-->
```

3. Liaison de la stratégie LDAP

```
bind system global pol_LDAPmgmt -priority 110
<!--NeedCopy-->
```

4. Attribuez des privilèges à vos administrateurs

   - Pour appliquer des privilèges au groupe

```
add system group NSG_Admin
bind system group NSG_Admin -policyName superuser 100
<!--NeedCopy-->
```

   - Pour appliquer des privilèges individuellement à chaque utilisateur

```
add system user admyoa
bind system user admyoa superuser 100
<!--NeedCopy-->
```


Configurer le protocole LDAP après avoir déchargé le protocole SSL vers un serveur virtuel d'équilibrage de charge

June 2, 2023

Dans une appliance NetScaler, le processus AAAD est utilisé pour effectuer une authentification de base telle que LDAP, RADIUS, TACACS pour l'accès à la gestion ou pour l'autorisation d'authentification et l'accès à la passerelle. Comme AAAD s'exécute sur le processeur de gestion, il peut y avoir des problèmes liés à des échecs d'authentification intermittents. Pour éviter ces défaillances, le serveur virtuel d'équilibrage de charge peut être utilisé pour décharger la fonctionnalité SSL d'AAAD.

Avantages du transfert du protocole SSL vers un serveur virtuel d'équilibrage de charge

- Performances AAAD améliorées. Dans AAAD, pour chaque demande d'authentification pour le serveur LDAP de type SSL, une nouvelle session SSL est établie. Comme le processus AAAD s'exécute sur le processeur de gestion, l'établissement de la session SSL a un impact sur les performances lors de requêtes élevées adressées à l'AAAD. Le transfert de la fonctionnalité SSL vers un serveur virtuel d'équilibrage de charge améliore les performances du processus AAAD.
- Rendez le certificat client au serveur. La bibliothèque LDAP cliente d'AAAD effectue uniquement la validation du certificat du serveur, il n'est pas possible de rendre le certificat client au serveur. Comme l'authentification mutuelle SSL nécessite le rendu du certificat client pour établir la connexion SSL, le transfert de la fonctionnalité SSL au serveur virtuel d'équilibrage de charge permet de restituer le certificat client au serveur.

Configurer le protocole LDAP après avoir déchargé le protocole SSL vers le serveur virtuel d'équilibrage de charge

Remarque : Une fois que vous avez créé une adresse IP de serveur virtuel d'équilibrage de charge pour LDAP et que vous avez pointé le serveur de requêtes LDAP vers l'adresse IP du serveur virtuel, le trafic provient du SNIP.

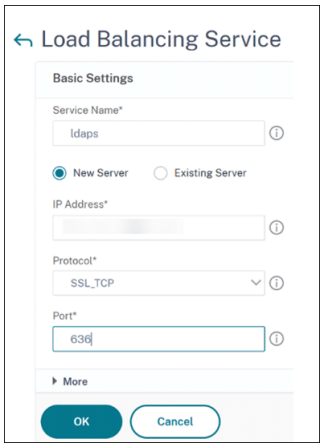
Composants requis

- Assurez-vous que le protocole LDAP sécurisé est activé sur les contrôleurs de domaine que l'appliance NetScaler utilise pour l'authentification. Par défaut, avec une autorité de certification d'entreprise, tous les contrôleurs de domaine s'inscrivent pour obtenir un certificat à l'aide du modèle de certificat de contrôleur de domaine.

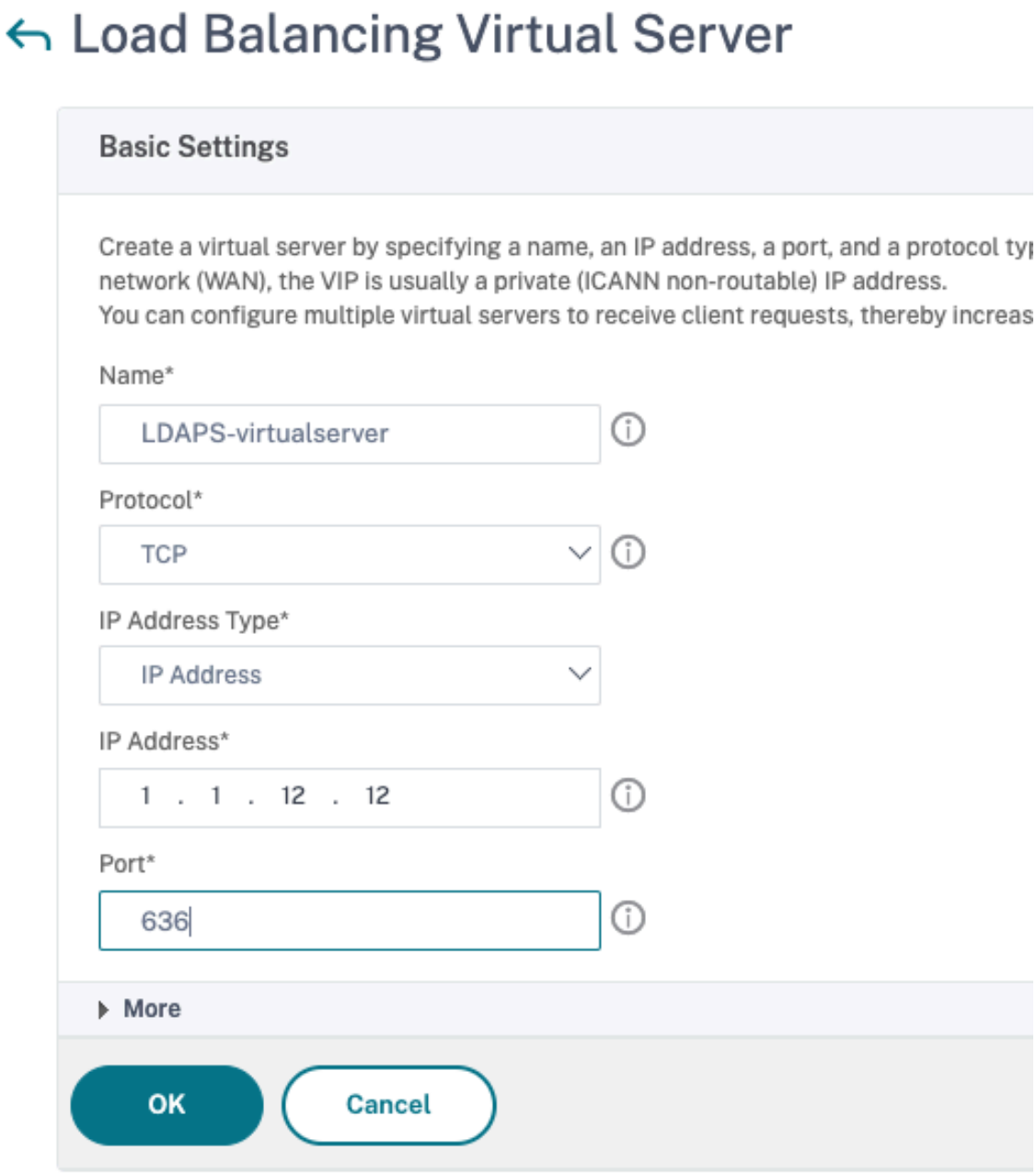
- Assurez-vous que le protocole LDAP sécurisé fonctionne en utilisant le fichier ldp.exe et en vous connectant au contrôleur de domaine via le port 636 et le protocole SSL.

Configurer LDAP après avoir déchargé le protocole SSL vers le serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Créez un service d'équilibrage de charge avec le protocole défini sur SSL_TCP.
   - Accédez à **Gestion du trafic > Équilibrage de charge > Services** et cliquez sur **Ajouter**.
   - Spécifiez l'adresse IP du contrôleur de domaine et définissez le numéro de port sur 636.
   - Cliquez sur **OK**.

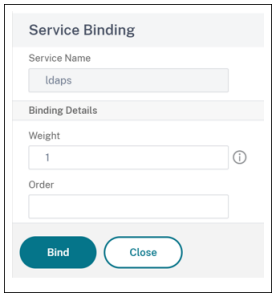


2. Créez un serveur virtuel d'équilibrage de charge pour le service d'équilibrage de charge LDAPS.
   a) Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
   b) Définissez le protocole sur TCP, entrez l'adresse IP, définissez le port sur 636, puis cliquez sur **OK**.



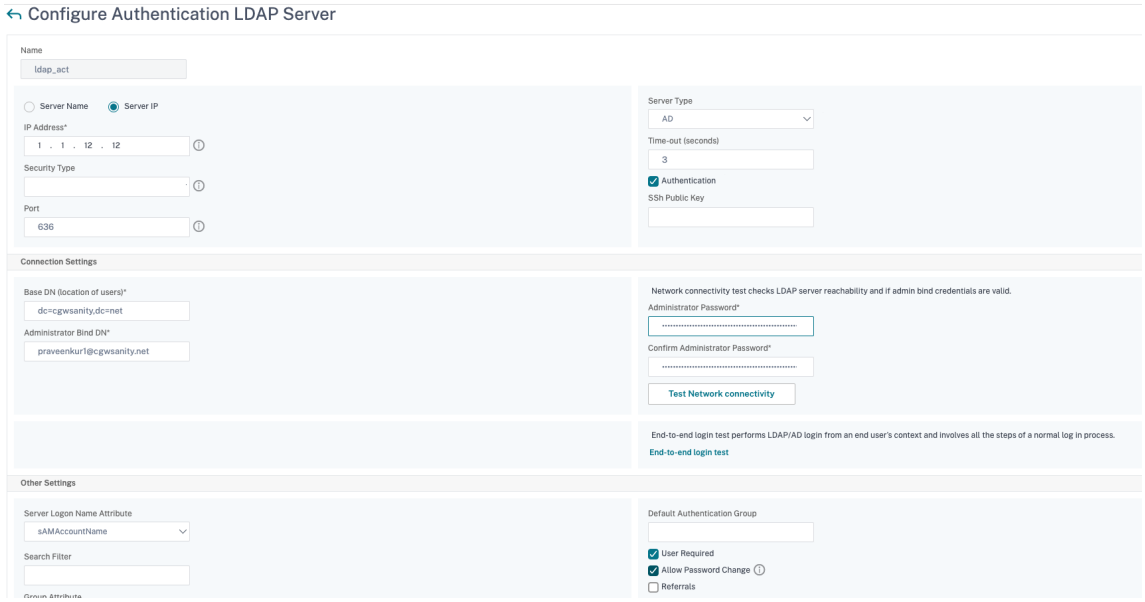
3. Liez le service LDAPS au serveur virtuel d'équilibrage de charge.
   - Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
   - Sélectionnez le serveur virtuel LDAP. La page **Serveur virtuel d'équilibrage** de charge s'affiche.
   - Dans la section **Services et groupes de services**, cliquez sur **Aucune liaison de service de serveur virtuel d'équilibrage de charge**. La page **Service Binding** s'affiche.
   - Sélectionnez le service d'équilibrage de charge. Mettez à jour les autres champs obligatoires et cliquez sur **Lier**.

- Cliquez sur **Terminé**.



4. Modifiez maintenant le serveur de stratégies d'authentification LDAP pour qu'il pointe vers le serveur virtuel d'équilibrage de charge pour un LDAP sécurisé. Le type de sécurité doit être PLAINTEXT.

   a) Accédez à **NetScaler Gateway > Stratégies > Authentification > LDAP**.
   b) Sélectionnez le serveur LDAP et cliquez sur **Modifier**.
   c) Remplacez l'adresse IP par l'adresse VIP LDAPS hébergée sur l'appliance NetScaler créée précédemment.
   d) Changez le type de sécurité en **PLAINTEXT**, changez le port en 636, cochez la case **Autoriser la modification du mot de passe**, si nécessaire (SLDAP autorise les modifications de mot de passe).
   e) Cliquez sur **Tester la connectivité réseau** pour vérifier la connectivité.
   f) Cliquez sur **OK**.



Vous pouvez consulter le tableau de bord d'authentification pour vérifier que l'état du serveur LDAP est activé. Consultez également les journaux d'authentification pour vérifier que l'authentification fonctionne comme prévu.

Configurer LDAP après avoir déchargé le protocole SSL vers le serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

1. Configurez un serveur LDAP pour le processus AAAD. L'exemple de configuration suivant établit la connexion SSL avec un serveur virtuel d'équilibrage de charge sans authentification mutuelle SSL.

```
add authentication ldapAction ldap_act -serverIP 1.1.12.12 -
    serverPort 636 -secTYPE PLAINTEXT -ldapBase "dc=aaatm-test,dc=
    com" -ldapBindDn administrator@aaatm-test.com -
    ldapBindDnPassword <password> -ldapLoginName samAccountName
<!--NeedCopy-->
```

2. Configurez un serveur virtuel d'équilibrage de charge pour le serveur virtuel LDAP. Le serveur virtuel d'équilibrage de charge est de type TCP.

```
add lb vserver ldaps TCP 1.1.1.12 636 -persistenceType NONE -
    cltTimeout 9000
<!--NeedCopy-->
```

3. Configurez un service pour le serveur virtuel d'équilibrage de charge. Le type de service est SSL-TCP.

```
add service ldaps 1.1.10.1 SSL_TCP 636
<!--NeedCopy-->
```

4. Configurez un certificat CA pour le service et définissez le paramètre « ServerAuth » pour la validation du certificat du serveur.

```
bind ssl service ldaps -certkeyName ca-cert -CA
set ssl service ldaps -serverAuth enabled
<!--NeedCopy-->
```

5. Joignez le certificat au service rendu au serveur LDAP.

```
bind ssl service ldaps -certkeyName usr_cert [client-certificate
    for client-authentication]
<!--NeedCopy-->
```

6. Liez le service au serveur virtuel d'équilibrage de charge.

```
bind lb vserver ldaps ldaps
<!--NeedCopy-->
```


Authentification RADIUS

May 8, 2023

Comme pour les autres types de politiques d'authentification, une politique d'authentification RADIUS (Remote Authentication Dial In User Service) comprend une expression et une action. Après avoir créé une stratégie d'authentification, vous la liez à un serveur virtuel d'authentification et vous lui attribuez une priorité. Lorsque vous la liez, vous la désignez également en tant que stratégie principale ou secondaire. Toutefois, la mise en place d'une politique d'authentification RADIUS comporte certaines exigences particulières qui sont décrites ci-dessous.

Normalement, vous configurez NetScaler pour qu'il utilise l'adresse IP du serveur d'authentification lors de l'authentification. Avec les serveurs d'authentification RADIUS, vous pouvez désormais configurer l'ADC pour qu'il utilise le nom de domaine complet du serveur RADIUS au lieu de son adresse IP pour authentifier les utilisateurs. L'utilisation d'un nom de domaine complet peut simplifier une configuration d'authentification, d'autorisation et d'audit autrement beaucoup plus complexe dans des environnements où le serveur d'authentification peut se trouver sur plusieurs adresses IP, mais utilise toujours un seul nom de domaine complet. Pour configurer l'authentification à l'aide du nom de domaine complet d'un serveur au lieu de son adresse IP, vous suivez le processus de configuration normal sauf lors de la création de l'action d'authentification. Lors de la création de l'action, vous remplacez le paramètre **ServerName** par le paramètre **ServerIP** .

Avant de décider de configurer NetScaler pour qu'il utilise l'adresse IP ou le nom de domaine complet de votre serveur RADIUS pour authentifier les utilisateurs, considérez que la configuration de l'authentification, de l'autorisation et de l'audit pour s'authentifier auprès d'un FQDN plutôt que d'une adresse IP ajoute une étape supplémentaire au processus d'authentification. Chaque fois que l'ADC authentifie un utilisateur, il doit résoudre le nom de domaine complet. Si un grand nombre d'utilisateurs tentent de s'authentifier simultanément, les recherches DNS qui en résultent peuvent ralentir le processus d'authentification.

> **Remarque**
>
> Ces instructions supposent que vous connaissez déjà le protocole RADIUS et que vous avez déjà configuré le serveur d'authentification RADIUS que vous avez choisi.

Pour ajouter une action d'authentification pour un serveur RADIUS à l'aide de l'interface de ligne de commande

Si vous vous authentifiez auprès d'un serveur RADIUS, vous devez ajouter une action d'authentification explicite. Pour ce faire, à l'invite de commandes, tapez la commande suivante :

```
1 add authentication radiusAction <name> [-serverip <IP> | -serverName] <
      FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
```



```
 -radKey  }
  [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
     <positive_integer>][-radAttributeType <positive_integer>][-
     radGroupsPrefix <string>] [-radGroupSeparator <string>][-
     passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
     ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
     pwdVendorID <positive_integer> [-pwdAttributeType <
     positive_integer>]] [-defaultAuthenticationGroup <string>] [-
     callingstationid ( ENABLED | DISABLED )]

<!--NeedCopy-->
```

L'exemple suivant ajoute une action d'authentification RADIUS nommée Authn-Act-1**, avec l'adresse IP du serveur**10.218.24.65**, le port du serveur**1812**, le délai d'authentification de**15**minutes, la clé Radius**WareTheLorax, l'adresse IP du NAS désactivée et l'ID NAS NAS1**.**

```
add authentication radiusaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
    DISABLED -radNASid NAS1
Done

<!--NeedCopy-->
```

L'exemple suivant ajoute la même action d'authentification RADIUS, mais en utilisant le nom de domaine complet du serveur **rad01.example.com** au lieu de l'adresse IP.

```
add authentication radiusaction Authn-Act-1 -serverName rad01.example.
    com -serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
    DISABLED -radNASid NAS1
Done

<!--NeedCopy-->
```

Pour configurer une action d'authentification pour un serveur RADIUS externe à l'aide de la ligne de commande

Pour configurer une action RADIUS existante, à l'invite de commandes, tapez la commande suivante :

```
set authentication radiusAction <name> [-serverip <IP> | -serverName] <
    FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -radKey  }
  [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
     <positive_integer>][-radAttributeType <positive_integer>][-
     radGroupsPrefix <string>] [-radGroupSeparator <string>][-
```



```
        passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
        ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
        pwdVendorID <positive_integer> [-pwdAttributeType <
        positive_integer>]] [-defaultAuthenticationGroup <string>] [-
        callingstationid ( ENABLED | DISABLED )]

<!--NeedCopy-->
```

Pour supprimer une action d'authentification pour un serveur RADIUS externe à l'aide de l'interface de ligne de commande

Pour supprimer une action RADIUS existante, tapez la commande suivante à l'invite de commandes :

```
rm authentication radiusAction <name>

<!--NeedCopy-->
```

Exemple

```
rm authentication radiusaction Authn-Act-1
Done

<!--NeedCopy-->
```

Pour configurer un serveur RADIUS à l'aide de l'utilitaire de configuration

> **Remarque**
>
> Dans l'utilitaire de configuration, le terme serveur est utilisé au lieu d'action, mais fait référence à la même tâche.

1. Accédez à **Sécurité > AAA - Trafic applicatif > Politiques > Authentification > Radius**
2. Dans le volet d'informations, sous l'onglet **Serveurs**, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau serveur RADIUS, cliquez sur **Ajouter**.
   - Pour modifier un serveur RADIUS existant, sélectionnez le serveur, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Créer un serveur RADIUSd'authentification ou Configurer un serveur RADIUS d'authentification**, tapez ou sélectionnez des valeurs pour les paramètres. Pour remplir les paramètres qui apparaissent sous**Send Calling Station ID**, développez**Détails**.
   - Name* : RadiusActionName (ne peut pas être modifié pour une action précédemment configurée)

- Type d'authentification* : AuthType (défini sur RADIUS, ne peut pas être modifié)
- Nom du serveur/Adresse IP* : choisissez le nom du serveur ou l'adresse IP du serveur
  - Nom du serveur*—serverName <FQDN>
  - Adresse IP*—serverIp <IP> Si une adresse IP IPv6 est attribuée au serveur, cochez la case IPv6.
- Port* : port du serveur
- Délai d'expiration (secondes) *—AuthTimeout
- Clé secrète* : RADKey (secret partagé RADIUS.)
- Confirmer la clé secrète* : saisissez le secret partagé RADIUS une seconde fois. (Aucun équivalent en ligne de commande.)
- Envoyer l'identifiant du poste d'appel — ID du poste d'appel
- Identifiant du fournisseur du groupe : RADvendorID
- Type d'attribut de groupe : RADAttributeType
- Identifiant du fournisseur d'adresses IP : IPVendorID
- ID du fournisseur PWD — ID du fournisseur PWD
- Codage du mot de passe — PassEncoding
- Groupe d'authentification par défaut : groupe d'authentification par défaut
- Identifiant NAS : identifiant NAS
- Activer l'extraction des adresses IP du NAS — RadNasip
- Préfixe de groupe—RadGroupPrefix
- Séparateur de groupes : séparateur de groupe RAD
- Type d'attribut d'adresse IP : IPAttributeType
- Type d'attribut de mot de passe : PWDAttributeType
- Comptabilité — Comptabilité

4. Cliquez sur **Créer** ou **sur OK**. La politique que vous avez créée apparaît sur la page Serveurs.

Support pour passer par l'attribut RADIUS 66 (Tunnel-Client-Endpoint)

L'appliance NetScaler autorise désormais le transfert de l'attribut RADIUS 66 (Tunnel-Client-Endpoint) lors de l'authentification RADIUS. En appliquant cette fonctionnalité, l'adresse IP du client est reçue par authentification à second facteur, en confiant la prise de décisions d'authentification basées sur les risques.

Un nouvel attribut « TunnelEndpointClientIP » est introduit à la fois dans les commandes « add authentication RadiusAction » et « set RadiusParams ».

Pour utiliser cette fonctionnalité, à l'invite de commande de l'appliance NetScaler, tapez :

```
add authentication radiusAction <name> {
 -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> }
  }
  [-serverPort <port>] … [-tunnelEndpointClientIP (ENABLED|DISABLED)]

set radiusParams {
 -serverIP <ip_addr|ipv6_addr|*> |{
 -serverName <string> }
  }
  [-serverPort<port>] … [-tunnelEndpointClientIP(ENABLED|DISABLED)]

<!--NeedCopy-->
```

Exemple

```
add authentication radiusAction radius -severIP 1.217.22.20 -serverName
     FQDN -serverPort 1812 -tunnelEndpointClientIp ENABLED

set radiusParams -serverIp 1.217.22.20 -serverName FQDN1 -serverPort
    1812 -tunnelEndpointClientIP ENABLED

<!--NeedCopy-->
```

Prise en charge de la validation de l'authentification RADIUS de bout en bout

L'appliance NetScaler peut désormais valider l'authentification RADIUS de bout en bout via une interface graphique. Pour valider cette fonctionnalité, un nouveau bouton « test » est introduit dans l'interface graphique. Un administrateur d'appliance NetScaler peut tirer parti de cette fonctionnalité pour bénéficier des avantages suivants :

- Consolide le flux complet (moteur de paquets — démon aaa — serveur externe) pour fournir une meilleure analyse
- Réduction du temps de validation et de dépannage des problèmes liés à des scénarios individuels

Vous disposez de deux options pour configurer et afficher les résultats des tests de l'authentification de bout en bout RADIUS à l'aide de l'interface graphique.

Depuis l'option système

1. Accédez à **Système > Authentification > Politiques de base > RADIUS,** puis cliquez sur l'onglet **Serveurs** .
2. Sélectionnez l' **action RADIUS** disponible dans la liste.
3. Sur la page **Configurer le serveur RADIUS d'authentification**, vous disposez de deux options dans la section **Paramètres de connexion** .
4. Pour vérifier la connexion au serveur RADIUS, cliquez sur l'onglet **Tester l'accessibilité de RADIUS** .
5. Pour consulter l'authentification RADIUS de bout en bout, cliquez sur le lien **Tester la connexion de l'utilisateur final** .

À partir de l'option d'authentification

1. Accédez à **Authentification > Tableau de bord**, sélectionnez l'action RADIUS disponible dans la liste.
2. Sur la page **Configurer le serveur RADIUS d'authentification**, vous disposez de deux options dans la section **Paramètres de connexion** .
3. Pour vérifier la connexion au serveur RADIUS, cliquez sur l'onglet **Tester l'accessibilité de RADIUS** .
4. Pour afficher l'état de l'authentification RADIUS de bout en bout, cliquez sur le lien **Tester la connexion de l'utilisateur final** .

Authentification RADIUS via TCP ou TLS

November 29, 2022

À partir des versions 13.1-27.59, l'authentification RADIUS est également prise en charge sur les protocoles TCP et TLS.

> **Remarque :**
>
> - L'option **Test RADIUS Reachability** n'est pas prise en charge pour les types de transport RADIUS sur TCP et TLS.
> - L'authentification RADIUS utilisant UDP n'est pas prise en charge sur les appliances FIPS.

Configurer RADIUS sur TCP à l'aide de la CLI

À l'invite de commandes, tapez :


```
add authentication radiusAction <name> [-serverIP] [-serverPort ] [-
    transport <transport>]
<!--NeedCopy-->
```

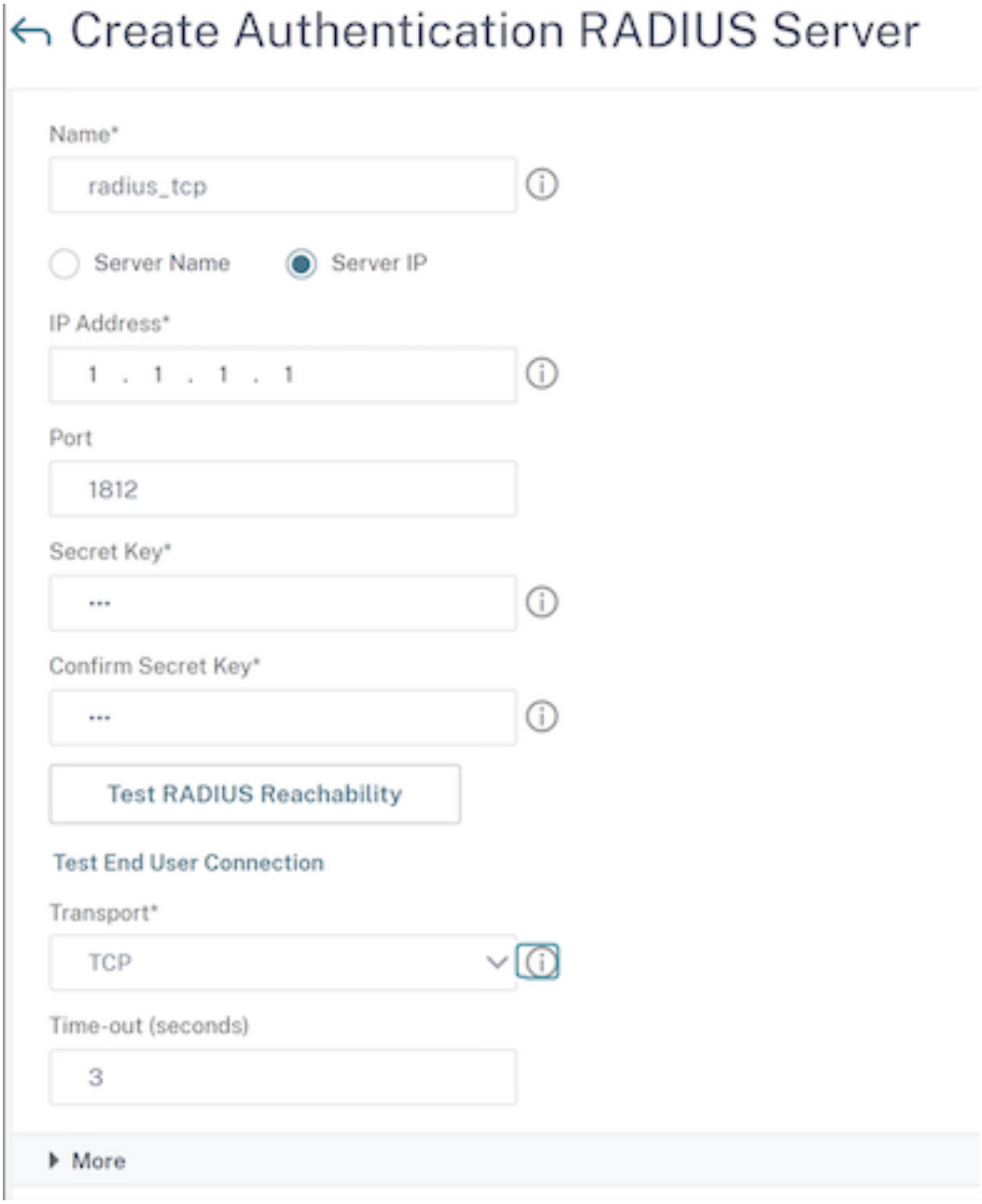
Exemple :

```
add authentication radiusAction RadAction -serverIP 1.1.1.1 -radkey 123
     -transport TCP
<!--NeedCopy-->
```

Configurer RADIUS sur TCP à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Actions > RADIUS**.
2. Sélectionnez un serveur existant ou créez-en un.

   Pour plus de détails sur la création d'un serveur, consultez Pour configurer un serveur RADIUS à l'aide de l'interface graphique.



3. Dans **Transport**, sélectionnez **TCP**.
4. Cliquez sur **Create**.

Configurer RADIUS sur TLS à l'aide de la CLI

À l'invite de commandes, tapez :

```
1 add authentication radiusAction <name> [-serverIP] [-serverPort ] [-
     transport <transport>] [-targetLBVserver <string>]
2 <!--NeedCopy-->
```


Exemple

```
1 add authentication radiusAction RadAction -serverIP 1.1.1.1 -radkey 123
      -transport TLS -targetLBVserver rad-lb
2 <!--NeedCopy-->
```

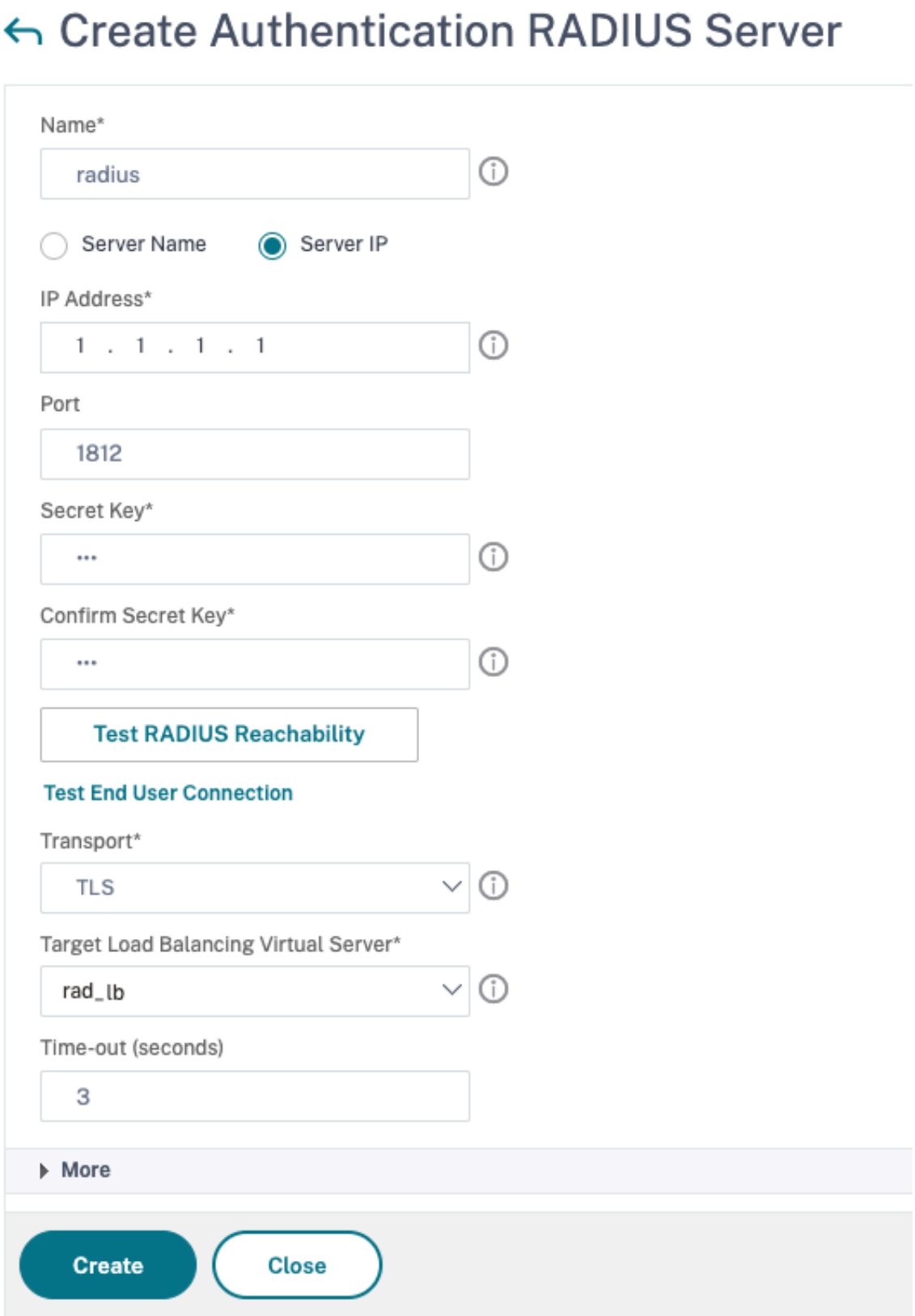
Remarque :

- Le nom du serveur n'est pas pris en charge pour le type de transport TLS
- Pour le type de transport TLS, configurez un serveur virtuel d'équilibrage de charge cible de type TCP et liez un service de type SSL_TCP à ce serveur virtuel.
- L'adresse IP et le numéro de port configurés pour l'action RADIUS doivent correspondre à l'adresse IP et au numéro de port du serveur virtuel d'équilibrage de charge cible configuré.

Configurer RADIUS sur TLS à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Actions > Serveurs**.
2. Sélectionnez un serveur existant ou créez-en un.

   Pour plus d'informations sur la création d'un serveur, consultez Pour configurer un serveur RADIUS à l'aide de l'interface graphique.



3. Dans **Transport**, sélectionnez **TLS**.
4. Dans **Target Load Balancing Virtual Server**, sélectionnez le serveur virtuel. Pour plus d'informations sur la création d'un serveur virtuel d'équilibrage de charge, consultez Création d'un serveur virtuel.

   > **Remarque :**
   >
   > - Le nom du serveur n'est pas pris en charge pour le type de transport TLS
   > - Pour le type de transport TLS, configurez un serveur virtuel d'équilibrage de charge cible de type TCP et liez un service de type SSL_TCP à ce serveur virtuel.
   > - L'adresse IP et le numéro de port configurés pour l'action RADIUS doivent correspondre à l'adresse IP et au numéro de port du serveur virtuel d'équilibrage de charge cible configuré.

5. Cliquez sur **Créer.**

authentification TACACS

May 5, 2023

La politique d'authentification TACACS permet de s'authentifier auprès d'un serveur d'authentification TACACS (Terminal Access Controller Access-Control System) externe.
Une fois qu'un utilisateur s'est authentifié auprès d'un serveur TACACS, NetScaler se connecte au même serveur TACACS pour toutes les autorisations suivantes. Lorsqu'un serveur TACACS principal n'est pas disponible, cette fonctionnalité évite tout retard pendant que l'ADC attend l'expiration du premier serveur TACACS. Cela se produit avant de renvoyer la demande d'autorisation au second serveur TACACS.

> **Remarque :**
>
> Le serveur d'autorisation TACACS ne prend pas en charge les commandes dont la longueur de chaîne dépasse 255 caractères.
>
> **Solution :** utilisez l'autorisation locale au lieu d'un serveur d'autorisation TACACS.

Lors de l'authentification via un serveur TACACS, les journaux de gestion du trafic d'authentification, d'autorisation et d'audit exécutent uniquement correctement les commandes TACACS. Cela empêche les journaux d'afficher les commandes TACACS saisies par les utilisateurs qui n'étaient pas autorisés à les exécuter.

À partir de NetScaler 12.0 Build 57.x, le système de contrôle d'accès du Terminal Access Controller (TACACS) ne bloque pas le démon d'authentification, d'autorisation et d'audit lors de l'envoi de la demande TACACS. Autorisez les authentifications LDAP et RADIUS à poursuivre la demande. La de-

mande d'authentification TACACS reprend une fois que le serveur TACACS accuse réception de la demande TACACS.

> **Important :**
>
> - Citrix vous recommande de ne pas modifier les configurations associées TACACS lorsque vous exécutez une commande « clear ns config ».
> - La configuration liée à TACACS liée aux politiques avancées est effacée et réappliquée lorsque le paramètre « RBAconfig » est défini sur NON dans la commande « clear ns config » pour la politique avancée.

Prise en charge des attributs nom-valeur pour l'authentification TACACS

Vous pouvez désormais configurer les attributs d'authentification TACACS avec un nom unique ainsi que des valeurs. Les noms sont configurés dans le paramètre d'action TACACS et les valeurs sont obtenues en interrogeant les noms. En spécifiant la valeur d'attribut name, les administrateurs peuvent facilement rechercher la valeur d'attribut associée au nom d'attribut. De plus, les administrateurs n'ont plus besoin de se souvenir de l'attribut uniquement par sa valeur.

> **Important**
>
> - Dans la commande TacAcsAction, vous pouvez configurer un maximum de 64 attributs séparés par des virgules avec une taille totale inférieure à 2 048 octets.

Pour configurer les attributs nom-valeur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add authentication tacacsAction <name> [-Attributes <string>]
<!--NeedCopy-->
```

Exemple :

```
add authentication tacacsAction tacacsAct1 -attributes  "mail,sn,
   userprincipalName"
<!--NeedCopy-->
```

Pour ajouter une action d'authentification à l'aide de l'interface de ligne de commande

Si vous n'utilisez pas l'authentification LOCALE, vous devez ajouter une action d'authentification explicite. À l'invite de commandes, tapez la commande suivante :

```
add authentication tacacsAction <name> -serverip <IP> [-serverPort <
   port>][-authTimeout <positive_integer>][ ... ]
```



```
<!--NeedCopy-->
```

Exemple

```
add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812                    -authtimeout 15 -tacacsSecret "
    minotaur" -authorization OFF -accounting ON -auditFailedCmds OFF -
    defaultAuthenticationGroup "users"
<!--NeedCopy-->
```

Pour configurer une action d'authentification à l'aide de l'interface de ligne de commande

Pour configurer une action d'authentification existante, tapez la commande suivante à l'invite de commandes :

```
set authentication tacacsAction <name> -serverip <IP> [-serverPort <
    port>][-authTimeout <positive_integer>][ ... ]
<!--NeedCopy-->
```

Exemple

```
     > set authentication tacacsaction Authn-Act-1 -serverip
        10.218.24.65 -serverport 1812                    -authtimeout 15
        -tacacsSecret "minotaur" -authorization OFF -accounting ON -
        auditFailedCmds OFF -defaultAuthenticationGroup "users"    Done
<!--NeedCopy-->
```

Pour supprimer une action d'authentification à l'aide de l'interface de ligne de commande

Pour supprimer une action RADIUS existante, tapez la commande suivante à l'invite de commandes :

```
rm authentication radiusAction <name>
<!--NeedCopy-->
```

Exemple

```
rm authentication tacacsaction Authn-Act-1
<!--NeedCopy-->
```


Authentification du certificat client

June 20, 2023

Les sites Web contenant du contenu sensible, tels que les sites Web de banque en ligne ou les sites Web contenant des informations personnelles sur les employés, nécessitent parfois des certificats clients pour l'authentification. Pour configurer l'authentification, l'autorisation et l'audit afin d'authentifier les utilisateurs en fonction des attributs de certificat côté client, vous devez d'abord activer l'authentification du client sur le serveur virtuel de gestion du trafic et lier le certificat racine au serveur virtuel d'authentification. Ensuite, vous implémentez l'une des deux options suivantes. Vous pouvez configurer le type d'authentification par défaut sur le serveur virtuel d'authentification en tant que CERT, ou vous pouvez créer une action de certificat qui définit ce que NetScaler doit faire pour authentifier les utilisateurs sur la base d'un certificat client. Dans les deux cas, votre serveur d'authentification doit prendre en charge les CRL. Vous configurez l'ADC pour extraire le nom d'utilisateur du champ **SubjectCN** ou d'un autre champ spécifié dans le certificat client.

Lorsque l'utilisateur essaie de se connecter à un serveur virtuel d'authentification pour lequel aucune stratégie d'authentification n'est configurée et qu'aucune cascade globale n'est configurée, les informations de nom d'utilisateur sont extraites du champ spécifié du certificat. Si le champ requis est extrait, l'authentification aboutit. Si l'utilisateur ne fournit pas de certificat valide pendant la négociation SSL, ou si l'extraction du nom d'utilisateur échoue, l'authentification échoue. Après avoir validé le certificat client, l'ADC présente une page de connexion à l'utilisateur.

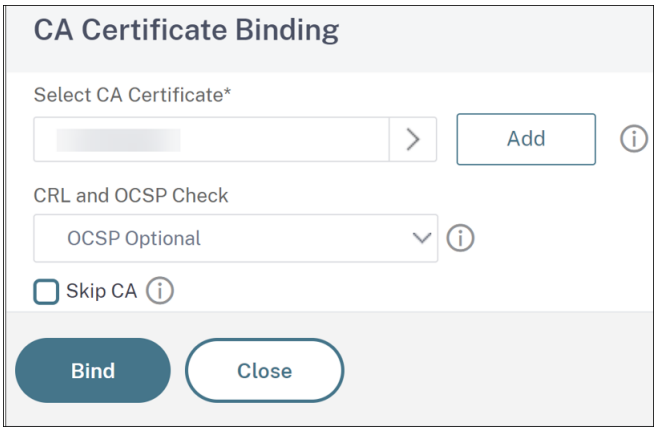
Les procédures suivantes supposent que vous avez déjà créé une configuration d'authentification, d'autorisation et d'audit fonctionnelle. Elles expliquent donc uniquement comment activer l'authentification à l'aide de certificats clients. Ces procédures supposent également que vous avez obtenu votre certificat racine et vos certificats clients et que vous les avez placés sur l'ADC dans le répertoire /nsconfig/ssl.

Configurer l'authentification du certificat client

Configurer les paramètres du certificat client à l'aide de l'interface graphique

1. Installez un certificat CA et liez-le à un serveur virtuel d'authentification.
    a) Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**.
    b) Sur la page **Serveurs virtuels d'authentification** qui s'affiche, sélectionnez le serveur virtuel que vous souhaitez configurer pour gérer l'authentification par certificat client, puis cliquez sur **Modifier.**
    c) Sur la page **Serveur virtuel d'authentification**, accédez à la section **Certificat** et cliquez sur la flèche droite « > ».

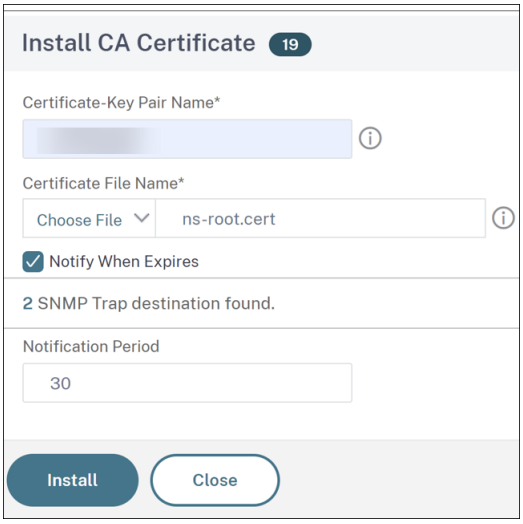
d) Sur la page de **liaison des certificats CA**, sélectionnez un certificat CA, mettez à jour les autres champs obligatoires, puis cliquez sur **Lier**.



e) Si aucun certificat CA n'est disponible, sélectionnez **Ajouter**.

f) Sur la page **Installer le certificat**, mettez à jour les champs suivants et cliquez sur **Installer**, puis sur **Fermer**.

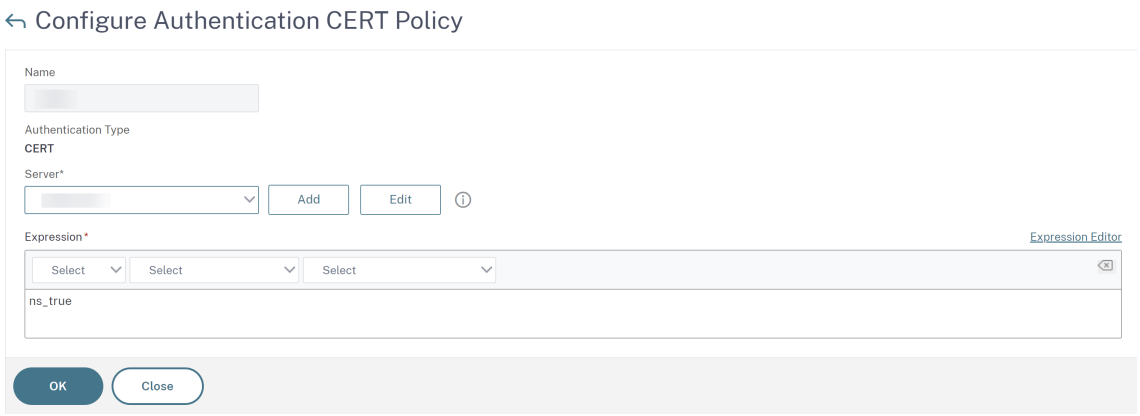
- Nom de la paire de clés de certificat : nom du certificat et de la paire de clés privées
- Nom du fichier de certificat : nom du fichier de certificat utilisé pour former la paire de clés de certificat. Le fichier de certificat doit être présent sur le disque dur ou le disque SSD de NetScaler. Le stockage d'un certificat dans un emplacement autre que celui par défaut peut entraîner des incohérences dans une configuration de haute disponibilité. Le chemin par défaut est /nsconfig/ssl/.
- Période de notification : nombre de jours avant l'expiration du certificat pendant lesquels NetScaler informe l'administrateur que le certificat est sur le point d'expirer.
- Notifier en cas d'expiration : activez cette option pour recevoir une alerte lorsque le certificat est sur le point d'expirer.



g) Une fois le certificat CA installé, accédez à la page **CA Certificate Binding**, liez-le à un

serveur virtuel d'authentification.

2. Retournez à la page **Sécurité > AAA - Trafic applicatif > Serveurs virtuels** .
3. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies de base > CERT.**
4. Sélectionnez la stratégie que vous souhaitez configurer pour gérer l'authentification par certificat client, puis cliquez sur **Modifier**.
5. Sur la page **Configurer la stratégie CERT d'authentification**, accédez à la liste déroulante **Serveur** et sélectionnez le serveur virtuel configuré pour gérer l'authentification par certificat client.
6. Cliquez sur **OK**.



Configurer les paramètres du certificat client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué, pour configurer le certificat et vérifier la configuration :

```
add ssl certKey <certkeyName> -cert <certFile> -key <keyFile> -password
    -inform <inform> -expiryMonitor <expiryMonitor> -notificationPeriod
    <notificationPeriod>

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
   positive_integer>]

show ssl certKey [<certkeyName>]

set aaa parameter -defaultAuthType CERT

show aaa parameter

set aaa certParams -userNameField "Subject:CN"
```



```
12
13 show aaa certParams
14 <!--NeedCopy-->
```

Configurer les stratégies d'authentification avancées des certificats clients à l'aide de l'interface graphique

1. Installez le certificat CA et liez-le à une paire de clés de certificat.
    a) Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**.
    b) Sur la page **Serveurs virtuels d'authentification** qui s'affiche, sélectionnez le serveur virtuel que vous souhaitez configurer pour gérer l'authentification par certificat client, puis cliquez sur **Modifier.**
    c) Sur la page **Serveur virtuel d'authentification**, accédez à la section **Certificat** et cliquez sur la flèche droite « > ».
    d) Sur la page de **liaison des certificats CA**, sélectionnez un certificat CA, mettez à jour les autres champs obligatoires, puis cliquez sur **Lier**.
    e) Si aucun certificat CA n'est disponible, sélectionnez **Ajouter**.
    f) Sur la page **Installer le certificat**, mettez à jour les champs suivants et cliquez sur **Installer**, puis sur **Fermer**.
        - Nom de la paire de clés de certificat : nom du certificat et de la paire de clés privées
        - Nom du fichier de certificat : nom du fichier de certificat utilisé pour former la paire de clés de certificat. Le fichier de certificat doit être présent sur le disque dur ou le disque SSD de NetScaler. Le stockage d'un certificat dans un emplacement autre que celui par défaut peut entraîner des incohérences dans une configuration de haute disponibilité. Le chemin par défaut est /nsconfig/ssl/.
        - Période de notification : nombre de jours avant l'expiration du certificat pendant lesquels NetScaler informe l'administrateur que le certificat est sur le point d'expirer.
        - Notifier en cas d'expiration : activez cette option pour recevoir une alerte lorsque le certificat est sur le point d'expirer.
    g) Une fois le certificat CA installé, accédez à la page **CA Certificate Binding** et répétez l'étape 4.
2. Retournez à la page **Sécurité > AAA - Trafic applicatif > Serveurs virtuels** .

    > **Remarque :**
    >
    > Si vous avez importé un certificat CA et un certificat de serveur valides pour le serveur virtuel, vous pouvez ignorer **les étapes 1 et 2**.

3. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées**, puis sélectionnez **Stratégie**.

4. Sur la page **Stratégies d'authentification**, effectuez l'une des opérations suivantes :
    - Pour créer une stratégie, cliquez sur **Ajouter**.
    - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Modifier**.
5. Sur la page **Créer une stratégie d'authentification** ou **Configurer une stratégie d'authentification**, tapez ou sélectionnez des valeurs pour les paramètres.
    - Nom : nom de la stratégie. Vous ne pouvez pas modifier le nom d'une stratégie précédemment configurée.
    - Type d'action : type de l'action d'authentification.
    - Action : nom de l'action d'authentification à effectuer si la stratégie correspond. Vous pouvez choisir une action d'authentification existante ou cliquer sur **Ajouter** pour créer une action.
    - Expression : règle qui sélectionne les connexions auxquelles vous souhaitez appliquer l'action que vous avez spécifiée. La règle peut être simple (« true » sélectionne tout le trafic) ou complexe. Pour saisir des expressions, choisissez d'abord le type d'expression dans la liste déroulante la plus à gauche sous la fenêtre Expression, puis en saisissant votre expression directement dans la zone de texte de l'expression, ou en cliquant sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant les listes déroulantes qu'elle contient pour définir votre expression.
    - Action de journalisation : nom de l'action d'audit à utiliser lorsqu'une demande d'authentification correspond à cette stratégie. Vous pouvez choisir une action d'audit existante ou cliquer sur **Ajouter** pour créer une action.
    - Commentaire : Vous pouvez saisir un commentaire qui décrit le type de trafic auquel s'applique cette stratégie d'authentification. Ce champ est facultatif.
6. Cliquez sur **Créer** ou sur **OK**, puis sur **Fermer**.

Transfert de certificat client

NetScaler peut désormais être configuré pour transmettre les certificats clients aux applications protégées qui nécessitent des certificats clients pour l'authentification des utilisateurs. L'ADC authentifie d'abord l'utilisateur, puis insère le certificat client dans la demande et l'envoie à l'application. Cette fonctionnalité est configurée en ajoutant des stratégies SSL appropriées.

Le comportement exact de cette fonctionnalité lorsqu'un utilisateur présente un certificat client dépend de la configuration du serveur virtuel VPN.

- Si le serveur virtuel VPN est configuré pour accepter les certificats clients mais ne les exige pas, l'ADC insère le certificat dans la demande, puis la transmet à l'application protégée.
- Si l'authentification du certificat client est désactivée sur le serveur virtuel VPN, l'ADC renégocie le protocole d'authentification et authentifie à nouveau l'utilisateur avant d'insérer le certificat client dans l'en-tête et de transmettre la demande à l'application protégée.

- Si le serveur virtuel VPN est configuré pour exiger l'authentification par certificat client, l'ADC utilise le certificat client pour authentifier l'utilisateur, puis insère le certificat dans l'en-tête et transmet la demande à l'application protégée.

Dans tous ces cas, vous configurez le pass-through du certificat client comme suit.

Création et configuration du transfert de certificats clients à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
add vpn vserver <name> SSL <IP> 443
<!--NeedCopy-->
```

Pour **name**, remplacez le nom du serveur virtuel par un nom. Le nom doit contenir entre un et 127 caractères ASCII, commençant par une lettre ou un trait de soulignement (_), et ne contenant que des lettres, des chiffres et le trait de soulignement, hachage (#), point (.), espace, deux-points (:), à (@), égal à (=) et tiret (-). Pour <IP>, remplacez l'adresse IP attribuée au serveur virtuel.

```
set ssl vserver <name> -clientAuth ENABLED -clientCert <clientcert>
<!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel que vous avez créé. Pour <clientCert>, remplacez l'une des valeurs suivantes :

- disabled—désactive l'authentification du certificat client sur le serveur virtuel VPN.
- obligatoire : configure le serveur virtuel VPN pour qu'il exige des certificats clients pour s'authentifier.
- facultatif : configure le serveur virtuel VPN pour autoriser l'authentification par certificat client, mais pas pour l'exiger.

```
bind vpn vserver <name> -policy local
<!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel VPN que vous avez créé.

```
bind vpn vserver <name> -policy cert
<!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel VPN que vous avez créé.

```
bind ssl vserver <name> -certkeyName <certkeyname>
<!--NeedCopy-->
```


Pour <name>, remplacez le nom du serveur virtuel que vous avez créé. Pour <certkeyName>, remplacez la clé de certificat client.

```
bind ssl vserver <name> -certkeyName <cacertkeyname> -CA -ocspCheck
   Optional
<!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel que vous avez créé. Pour <cacertkeyName>, remplacez la clé de certificat CA.

```
add ssl action <actname> -clientCert ENABLED -certHeader CLIENT-CERT
<!--NeedCopy-->
```

Pour <actname>, remplacez le nom de l'action SSL.

```
add ssl policy <polname> -rule true -action <actname>
<!--NeedCopy-->
```

Pour <polname>, remplacez le nom de votre nouvelle stratégie SSL. Pour <actname>, remplacez le nom de l'action SSL que vous avez créée.

```
bind ssl vserver <name> -policyName <polname> -priority 10
<!--NeedCopy-->
```

Pour <name>, remplacez le nom du serveur virtuel VPN.

Exemple

```
add vpn vserver vs-certpassthru SSL 10.121.250.75 443
set ssl vserver vs-certpassthru -clientAuth ENABLED -clientCert
   optional
bind vpn vserver vs-certpassthru -policy local
bind vpn vserver vs-certpassthru -policy cert
bind ssl vserver vs-certpassthru -certkeyName mycertKey
bind ssl vserver vs-certpassthru -certkeyName mycertKey -CA -ocspCheck
   Optional
add ssl action act-certpassthru -clientCert ENABLED -certHeader CLIENT-
   CERT
add ssl policy pol-certpassthru -rule true -action act-certpassthru
bind ssl vserver vs-certpassthru -policyName pol-certpassthru -priority
    10
<!--NeedCopy-->
```


Négocier l'authentification

May 5, 2023

Comme pour les autres types de politiques d'authentification, une politique d'authentification Negotiate comprend une expression et une action. Après avoir créé une stratégie d'authentification, vous la liez à un serveur virtuel d'authentification et vous lui attribuez une priorité. Lorsque vous la liez, vous la désignez également en tant que stratégie principale ou secondaire.

Outre les fonctions d'authentification standard, la commande Negotiate Action permet désormais d'extraire les informations utilisateur d'un fichier keytab au lieu de vous demander de les saisir manuellement. Si un keytab possède plusieurs SPN, l'authentification, l'autorisation et l'audit sélectionnent le SPN approprié. Vous pouvez configurer cette fonctionnalité via la ligne de commande ou à l'aide de l'utilitaire de configuration.

> **Remarque**
>
> Ces instructions supposent que vous connaissez déjà le protocole LDAP et que vous avez déjà configuré le serveur d'authentification LDAP de votre choix.

Pour configurer l'authentification, l'autorisation et l'audit afin d'extraire les informations utilisateur d'un fichier keytab à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande appropriée :

```
add authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd  }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]

set authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]
<!--NeedCopy-->
```


Parameter description

- **name** : nom de l'action de négociation à utiliser.
- **domain :** nom de domaine du principal de service qui représente NetScaler.
- **DomainUser** : nom d'utilisateur du compte mappé avec NetScaler principal. Cela peut être fourni avec le domaine et le mot de passe lorsque le fichier keytab n'est pas disponible. Si le nom d'utilisateur est fourni avec le fichier keytab, ce fichier keytab sera recherché pour les informations d'identification de cet utilisateur. Longueur maximale : 127
- **DomainUserPassWD** : mot de passe du compte mappé au principal NetScaler.
- **DefaultAuthenticationGroup** : il s'agit du groupe par défaut qui est choisi lorsque l'authentification réussit en plus des groupes extraits. Longueur maximale : 63
- **keytab** : chemin d'accès au fichier keytab utilisé pour déchiffrer les tickets Kerberos présentés à NetScaler. Si keytab n'est pas disponible, le domaine/le nom d'utilisateur/le mot de passe peuvent être spécifiés dans la configuration de l'action de négociation. Longueur maximale : 127
- **NTLMPath** : chemin d'accès au site activé pour l'authentification NTLM, y compris le nom de domaine complet du serveur. Ceci est utilisé lorsque les clients se rabattent sur NTLM. Longueur maximale : 127

Pour configurer l'authentification, l'autorisation et l'audit afin d'extraire les informations utilisateur d'un fichier keytab à l'aide de l'utilitaire de configuration

> Remarque
>
> Dans l'utilitaire de configuration, le terme serveur est utilisé au lieu d'action, mais fait référence à la même tâche.

1. Accédez à **Sécurité > AAA - Trafic applicatif > Authentification > Politiques avancées > Actions > Actions NEGOTIATE**.
2. Dans le volet d'informations, sous l'onglet **Serveurs**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez créer une nouvelle action de **négociation**, cliquez sur **Ajouter**.
   - Si vous souhaitez modifier une action de **négociation** existante, sélectionnez l'action dans le volet de données, puis cliquez sur **Modifier**.
3. Si vous créez une nouvelle action de **négociation**, dans la zone de texte **Nom**, tapez le nom de votre nouvelle action. Le nom peut comporter de 1 à 127 caractères et peut être composé de lettres majuscules et minuscules, de chiffres, de traits d'union (-) et de traits de soulignement (_). Si vous modifiez une action de négociation existante, ignorez cette étape. Le nom est en lecture seule ; vous ne pouvez pas le modifier.
4. Sous **Négocier**, si la case Utiliser le fichier Keytab n'est pas déjà cochée, cochez-la.

5. Dans la zone de texte du chemin du fichier Keytab, tapez le chemin complet et le nom du fichier Keytab que vous souhaitez utiliser.
6. Dans la zone de texte Groupe d'authentification par défaut, tapez le groupe d'authentification que vous souhaitez définir par défaut pour cet utilisateur.
7. Cliquez sur **Créer** ou **sur OK** pour enregistrer vos modifications.

Points à noter lorsque des cryptages avancés sont utilisés pour l'authentification Kerberos

- **Exemple de configuration lorsque keytab est utilisé :** ajouter une authentification NegotiateAction neg_act_aes256 -keytab « /nsconfig/krb/lbvs_aes256.keytab »
- **Utilisez la commande suivante lorsque keytab possède plusieurs types de cryptage.** La commande capture également les paramètres utilisateur du domaine : add authentication NegotiateAction neg_act_keytab_all -keytab « /nsconfig/krb/lbvs_all.keytab » -DomainUser « http://lbvs.aaa.local »
- **Utilisez les commandes suivantes lorsque les informations d'identification utilisateur sont utilisées : add authentication NegotiateAction neg_act_user -domain AAA.LOCAL** -DomainUser « http://lbvs.AAA.local » -DomainUserPasswd <password>
- Assurez-vous que les informations **DomainUser** correctes sont fournies. Vous pouvez rechercher le nom d'ouverture de session de l'utilisateur dans AD.

authentification Web

May 5, 2023

L'authentification, l'autorisation et l'audit permettent désormais d'authentifier un utilisateur auprès d'un serveur Web, en fournissant les informations d'identification requises par le serveur Web dans une requête HTTP et en analysant la réponse du serveur Web pour déterminer si l'authentification de l'utilisateur a réussi. Comme pour les autres types de stratégies d'authentification, une stratégie d'authentification Web est composée d'une expression et d'une action. Après avoir créé une stratégie d'authentification, vous la liez à un serveur virtuel d'authentification et vous lui attribuez une priorité. Lorsque vous la liez, vous la désignez également en tant que stratégie principale ou secondaire.

Pour configurer l'authentification Web avec un serveur Web spécifique, vous devez d'abord créer une action d'authentification Web. Étant donné que l'authentification sur les serveurs Web n'utilise pas de format rigide, vous devez spécifier exactement quelles informations le serveur Web a besoin et dans quel format lors de la création de l'action. Pour ce faire, vous créez une expression dans la politique avancée de l'appliance NetScaler qui contient les éléments suivants :

- **IP du serveur** : adresse IP du serveur Web d'authentification.

- **Port du serveur** : port du serveur Web d'authentification.
- **Règle d'authentification** : expression de la politique avancée de l'appliance NetScaler qui contient les informations d'identification de l'utilisateur dans le format attendu par le serveur Web.
- **Scheme**—HTTP (pour l'authentification Web non chiffrée) ou HTTPS (pour l'authentification Web cryptée).
- **Règle de réussite** : expression de la politique avancée de l'appliance NetScaler qui correspond à la chaîne de réponse du serveur Web indiquant que l'utilisateur s'est authentifié avec succès.

Pour tous les autres paramètres, suivez les règles normales de la commande d'ajout d'une action d'authentification.

Vous créez ensuite une stratégie associée à cette action. La politique est similaire à une politique LDAP et, comme les politiques LDAP, elle utilise la syntaxe de l'appliance NetScaler.

> **Remarque**
>
> Ces instructions supposent que vous connaissez déjà les exigences d'authentification du ou des serveurs Web sur lesquels vous souhaitez vous authentifier et que vous avez déjà configuré le serveur d'authentification Web.

Pour configurer une action d'authentification Web à l'aide de l'interface de ligne de commande

Pour créer une action d'authentification Web sur la ligne de commande, tapez la commande suivante sur la ligne de commande :

```
1 add authentication webAuthAction <name> -serverIP <ip_addr|ipv6_addr
      |\*> -serverPort <port|\*> [-fullReqExpr <string>] -scheme ( http |
      https ) -successRule <expression> [-defaultAuthenticationGroup <
      string>][-Attribute1 <string>][-Attribute2 <string>] [-Attribute3 <
      string>][-Attribute4 <string>] [-Attribute5 <string>][-Attribute6 <
      string>] [-Attribute7 <string>][-Attribute8 <string>] [-Attribute9 <
      string>][-Attribute10 <string>] [-Attribute11 <string>][-Attribute12
       <string>] [-Attribute13 <string>][-Attribute14 <string>] [-
      Attribute15 <string>][-Attribute16 <string>]
2 <!--NeedCopy-->
```

Exemple

```
1 add policy expression post_data ""username=" + http.REQ.BODY(1000).
      SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&") + "&
      passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR
      ("passwd=")"
2
```



```
add policy expression length_post_data "("username= " + http.REQ.BODY
    (1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&")
     + "passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).
    AFTER_STR("passwd=")).length"

add authentication webAuthAction webAuth_POST -serverIP 10.106.187.54 -
    serverPort 80 -fullReqExpr q{
 "POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." + http.req
     .version.major + "\r\nAccept:\*/\*\r\nHost: 10.106.187.54\r\
     nReferer: http://10.106.187.54/MyPHP/auth.php\r\nAccept-Language:
     en-US\r\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT
     6.1; Trident/5.0)\r\nContent-Type: application/x-www-form-
     urlencoded\r\n" + "Content-Length: " + length_post_data + "\r\
     nConnection: Keep-Alive\r\n\r\n" + post_data }
  -scheme http -successRule "http.res.status.eq(200)"
<!--NeedCopy-->
```

Pour configurer une action d'authentification Web à l'aide de l'utilitaire de configuration

> **Remarque**
>
> Dans l'utilitaire de configuration, le terme serveur est utilisé au lieu d'action, mais fait référence à la même tâche.

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > LDAP**.
2. Dans le volet d'informations, sous l'onglet **Serveurs**, effectuez l'une des opérations suivantes :
   - Si vous souhaitez créer une nouvelle action d'authentification Web, cliquez sur **Ajouter**.
   - Si vous souhaitez modifier une action d'authentification Web existante, sélectionnez l'action dans le volet de données, puis cliquez sur **Modifier**.
3. Si vous créez une nouvelle action d'authentification Web, dans la boîte de dialogue **Créer un serveur Web d'authentification**, zone de texte **Nom**, tapez un nom pour la nouvelle action d'authentification Web. Le nom peut comporter de un à 127 caractères et peut être composé de lettres majuscules et minuscules, de chiffres et de traits d'union (-) et de traits de soulignement (_). Si vous modifiez une action d'authentification Web existante, ignorez cette étape. Le nom est en lecture seule ; vous ne pouvez pas le modifier.
4. Dans la zone de texte **Adresse IP du serveur Web**, tapez l'adresse IP IPv4 ou IPv6 du serveur Web d'authentification. Si l'adresse est une adresse IP IPv6, cochez d'abord la case IPv6.
5. Dans la zone de texte Port, tapez le numéro de port sur lequel le serveur Web accepte les connexions.

6. Sélectionnez **HTTP** ou **HTTPS** dans la liste déroulante **Protocole** .
7. Dans la zone de texte Expression de demande HTTP, tapez une expression régulière au format PCRE qui crée la demande de serveur Web qui contient les informations d'identification de l'utilisateur dans le format exact attendu par le serveur Web d'authentification.
8. Dans la zone de texte Expression pour valider l'authentification, tapez une expression de politique avancée de l'appliance NetScaler qui décrit les informations contenues dans la réponse du serveur Web indiquant que l'authentification de l'utilisateur a été réussie.
9. Remplissez les champs restants comme décrit dans la documentation générale des actions d'authentification.
10. Cliquez sur **OK**.

Configurer SMS OTP pour l'authentification Web

June 20, 2023

NetScaler peut désormais être intégré à un fournisseur de SMS tiers pour fournir un niveau d'authentification supplémentaire.

L'appliance NetScaler peut être configurée pour envoyer un OTP sur le mobile de l'utilisateur en tant que deuxième facteur d'authentification. L'appliance présente à l'utilisateur un formulaire d'ouverture de session pour entrer dans l'OTP après une connexion AD réussie. Ce n'est qu'après la validation réussie de l'authentification OTP par SMS que l'utilisateur reçoit la ressource demandée.

Pour réaliser l'authentification OTP par SMS, l'appliance NetScaler s'appuie sur les facteurs suivants dans le back-end.

1. Authentifiez l'utilisateur à l'aide de l'authentification LDAP et extrayez le numéro de téléphone portable de l'utilisateur.
2. Créez OTP et stockez-le dans la variable NS. Configuration et utilisation de variables.
3. Envoyez l'OTP via la méthode d'authentification WebAuth au numéro de téléphone portable extrait de LDAP.
4. Validez l'OTP.

Composants requis

Configurer le magasin OTP

Les administrateurs configurent une base de données/un magasin pour enregistrer les OTP utilisés pour l'authentification par SMS à l'aide de la commande CLI suivante.


```
add ns variable otp_store -type "map(text(65),text(6),100000)" -
    ifValueTooBig undef -ifNoValue undef -expires 5
<!--NeedCopy-->
```

Générer un OTP aléatoire par session utilisateur

Utilisez la commande suivante pour générer un OTP aléatoire à 6 chiffres par session utilisateur et enregistrez-le dans le magasin OTP.

```
add ns assignment generate_otp -variable "$otp_store[AAA.USER.SESSIONID
    ]" -set ("000000" + SYS.RANDOM.MUL(1000000).
    TYPECAST_UNSIGNED_LONG_AT.TYPECAST_TEXT_T).SUFFIX(6)
<!--NeedCopy-->
```

Configurer l'authentification OTP par SMS avec NetScaler

- Avant de configurer la fonctionnalité d'authentification à deux facteurs par SMS, vous devez configurer une authentification LDAP sur une appliance NetScaler comme premier facteur avec l'authentification activée. Pour obtenir des instructions sur la configuration de l'authentification LDAP, reportez-vous à la section Pour configurer l'authentification LDAP à l'aide de l'utilitaire de configuration.
- Configurez LDAP et extrayez le numéro de téléphone portable à utiliser pour l'authentification OTP par SMS.

Exemple de configuration du premier facteur

```
add authentication ldapAction ldap_action -serverIP 1.1.1.1 -serverPort
     3268 -authTimeout 30 -ldapBase "dc=nsi-test,dc=com" -ldapBindDn
    Administrator@nsi-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samaccountname -groupAttrName memberOf -
    ssoNameAttribute samaccountname  -Attribute1 mobile -email mail

add authentication Policy ldap_policy -rule true -action ldap_action
<!--NeedCopy-->
```

> **Remarque**
>
> Le numéro de téléphone portable peut être extrait à l'aide de AAA.USER.ATTRIBUTE (1) et peut être inclus lors de son envoi au serveur principal.

Exemple de configuration du deuxième facteur

À l'aide de l'exemple de configuration suivant, un OTP qui doit être envoyé à l'utilisateur final est généré.

```
add authentication policylabel set_otp -loginSchema LSCHEMA_INT

add authentication Policy set_otp -rule true -action test

add authentication policy cascade_noauth -rule true -action NO_AUTHN

add authentication Policy check_otp -rule "$test.valueExists(AAA.USER.
    SESSIONID)" -action NO_AUTHN

add authentication policylabel check_otp -loginSchema LSCHEMA_INTbind
    authentication policylabel set_otp -policyName set_otp -priority 1 -
    gotoPriorityExpression NEXT

bind authentication policylabel set_otp -policyName cascade_noauth -
    priority 2 -gotoPriorityExpression NEXT -nextFactor check_otpbind
    authentication policylabel check_otp -policyName wpp -priority 1 -
    gotoPriorityExpression NEXT

bind authentication policylabel check_otp -policyName
    wpp_cascade_noauth -priority 2 -gotoPriorityExpression NEXT -
    nextFactor otp_verifyadd authentication Policy wpp -rule true -
    action webAuth_POST

add authentication Policy wpp_cascade_noauth -rule true -action
    NO_AUTHNadd authentication Policy otp_verify -rule "AAA.LOGIN.
    PASSWORD.EQ($test[AAA.USER.SESSIONID])" -action NO_AUTHN

add authentication policylabel otp_verify -loginSchema onlyPassword

bind authentication policylabel otp_verify -policyName otp_verify -
    priority 1 -gotoPriorityExpression NEXTadd authentication vserver
    avs SSL 10.106.40.121 443

bind authentication vserver avs -policy ldap_policy  -priority 1 -
    nextFactor set_otp -gotoPriorityExpression NEXT
<!--NeedCopy-->
```


Exemple de configuration du troisième facteur

À l'aide de l'exemple de configuration suivant, l'OTP généré dans la configuration du second facteur est envoyé à l'utilisateur final à l'aide de la méthode d'authentification Web. Pour plus de détails sur l'authentification Web, voir Authentification Web.

- Exemple de configuration d'authentification Web lorsque le serveur SMS expose l'API via la méthode GET.

```
add policy expression otp_exp_get ""method=sendMessage&send_to="
    + AAA.USER.ATTRIBUTE(1) + "&msg=OTP is " + $otp_store[AAA.USER
    .SESSIONID] + "for login into secure access  gateway. Valid
    till EXPIRE_TIME. Do not share the OTP with anyone for
    security reasons.&userid=######&password=###=1.0""

add authentication webAuthAction webAuth_Get -serverIP
    10.106.168.210 -serverPort 8080 -fullReqExpr q{
"GET /GatewayAPI/rest?" + otp_exp_get + "HTTP/" + http.req.
    version.major + "." + http.req.version.minor.sub(1) + "\r\
    nAccept:\*/\*\r\nHost: <FQDN>\r\n" }
 -successRule "http.res.status.eq(200)" -scheme http
<!--NeedCopy-->
```

- Exemple de configuration d'authentification Web lorsque le serveur SMS expose l'API via la méthode POST.

```
add policy expression otp_exp_post ""Message: OTP is " +
    $otp_store[AAA.USER.SESSIONID] + "for login into secure access
      gateway. Valid till EXPIRE_TIME. Do not share the OTP with
    anyone for security reasons&Mobile:" + AAA.USER.ATTRIBUTE(1)"

add authentication webAuthAction webAuth_POST -serverIP
    10.106.168.210 -serverPort 8080 -fullReqExpr q{
"POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." +
    http.req.version.major + "\r\nAccept:\*/\*\r\nHost:
    10.106.168.210 \r\nContent-Length: 10\r\n\r\n" + otp_exp_post
    }
 -scheme http -successRule true
<!--NeedCopy-->
```

```
add authentication webAuthAction webAuth_Get -serverIP
    10.106.168.210 -serverPort 8080 -fullReqExpr q{
"GET /GatewayAPI/rest?" + otp_exp_get + "HTTP/" + http.req.
    version.major + "." + http.req.version.minor.sub(1) + "\r\
    nAccept:/\r\nHost: <FQDN>\r\n" }
```



```
3    -successRule "http.res.status.eq(200)" -scheme http
4
5    add policy expression otp_exp_post "$otp_store[AAA.USER.SESSIONID
        ]"
6    <!--NeedCopy-->
```

- Enfin, envoyez l'OTP.

```
1    add authentication Policy wpp -rule true -action webAuth_POST
2
3    add authentication policylabel send_otp -loginSchema LSCHEMA_INT
4    bind authentication policylabel send_otp -policyName wpp -
        priority 1 -gotoPriorityExpression NEXT
5    <!--NeedCopy-->
```

Exemple de configuration du quatrième facteur

À l'aide de l'exemple de configuration suivant, validez l'OTP envoyé à l'utilisateur final.

Dans cette configuration, une règle de stratégie est utilisée pour valider l'OTP par rapport à celui qui est envoyé à l'utilisateur final.

```
1  add authentication Policy otp_verify -rule "AAA.LOGIN.PASSWORD.EQ(
       $otp_store[AAA.USER.SESSIONID])" -action NO_AUTHN
2
3  add authentication policylabel otp_verify -loginSchema onlyPassword
4
5  bind authentication policylabel otp_verify -policyName otp_verify -
       priority 1 -gotoPriorityExpression NEXT
6
7  <!--NeedCopy-->
```

Utilisez la commande suivante pour ajouter le schéma de connexion OnlyPassword :

```
1  add authentication loginSchema onlypassword -authenticationschema /
       nsconfig/loginschema/LoginSchema/OnlyPassword.xml"
2  <!--NeedCopy-->
```

Liez tous les facteurs d'une authentification OTP par SMS réussie

Utilisez les commandes CLI suivantes pour relier tous les facteurs entre eux.

```
1  bind authentication policylabel send_otp -policyName wpp -priority 1 -
       gotoPriorityExpression NEXT -nextFactor otp_verify
```



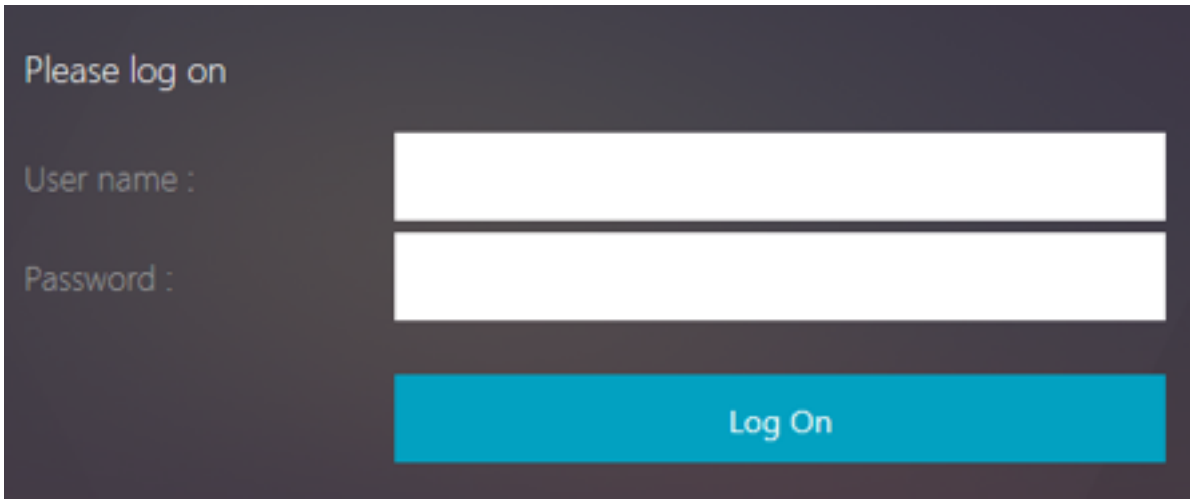
```
<!--NeedCopy-->
```

> **Remarque :**
>
> La stratégie d'authentification en cascade a été ajoutée pour permettre une authentification fiable et continue pour les utilisateurs finaux. Si le facteur actuel échoue, le facteur suivant est évalué de telle sorte qu'il n'y ait aucun impact sur l'expérience utilisateur.

Authentification par formulaire

January 21, 2021

Avec l'authentification basée sur les formulaires, un formulaire d'ouverture de session est présenté à l'utilisateur final. Ce type de formulaire d'authentification prend en charge à la fois l'authentification multifacteur (nFactor) et l'authentification classique.



Assurez-vous de ce qui suit pour que l'authentification basée sur les formulaires fonctionne :

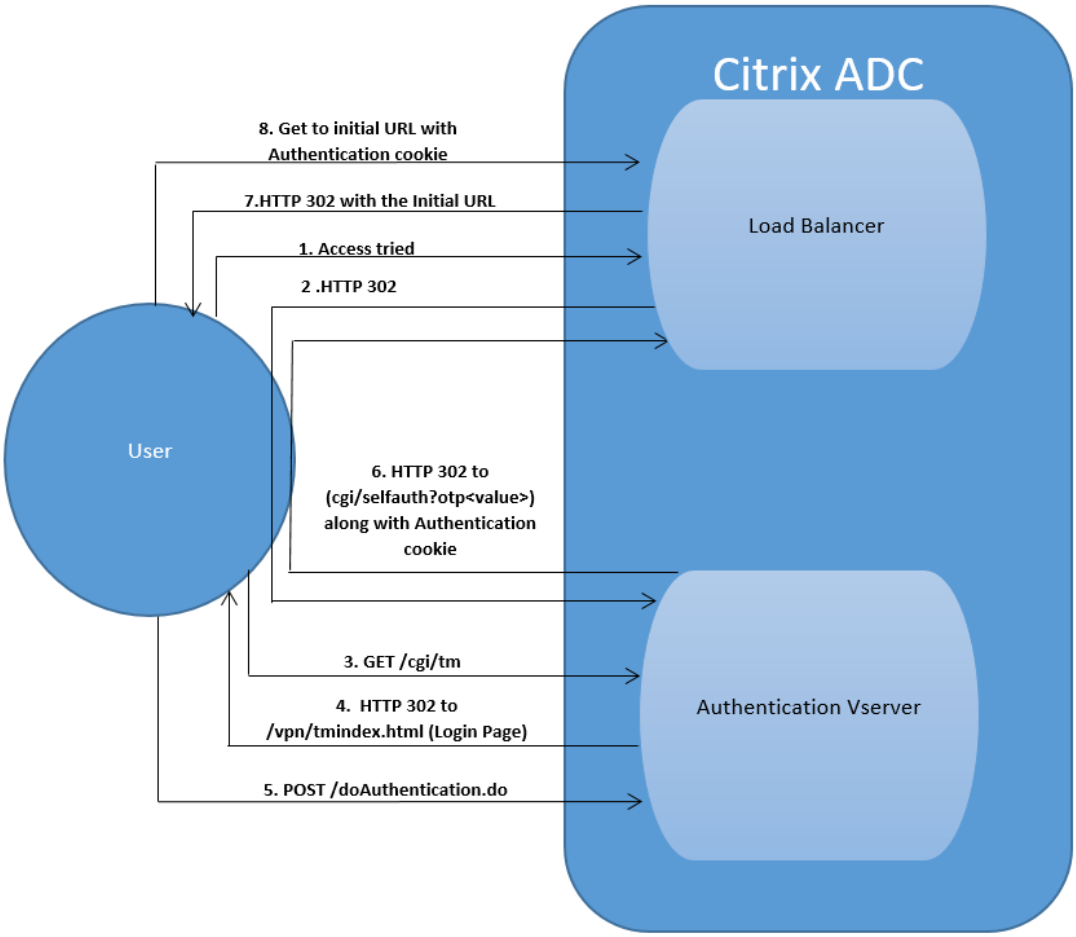
- L'authentification du serveur virtuel d'équilibrage de charge doit être **activée**.
- Le paramètre 'AuthenticationHost' doit être spécifié vers lequel l'utilisateur doit être redirigé pour l'authentification. La commande pour configurer la même chose est la suivante :

```
set lb vs lb1 -authentication on  - authenticationhost aaavs-ip/
   fqdn
```

- L'authentification basée sur les formulaires est compatible avec le navigateur qui prend en charge HTML

Les étapes suivantes expliquant le fonctionnement de l'authentification basée sur les formulaires :

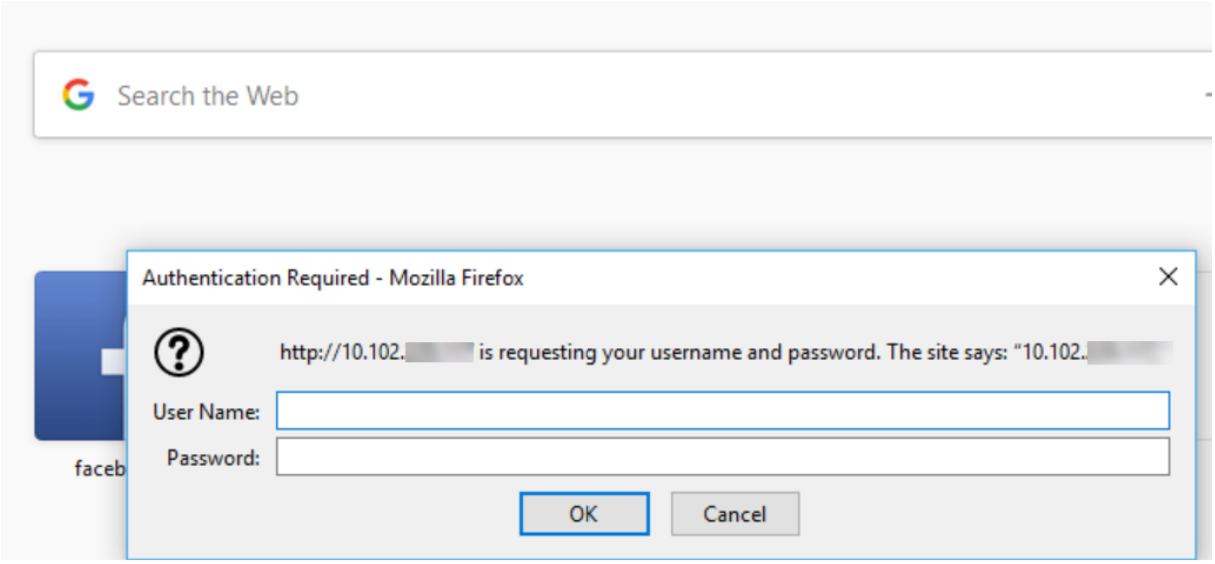
1. Le client (navigateur) envoie une requête GET pour une URL sur le serveur virtuel TM (équilibrage de charge/CS).
2. Le serveur virtuel TM détermine que le client n'a pas été authentifié et envoie une réponse HTTP 302 au client. La réponse contient un script masqué qui provoque le client à émettre une requête GET pour /cgi/tm au serveur virtuel d'authentification.
3. Le client envoie GET /cgi/tm contenant l'URL cible au serveur virtuel d'authentification.
4. Le serveur virtuel d'authentification envoie une redirection vers la page de connexion.
5. L'utilisateur envoie ses informations d'identification au serveur virtuel d'authentification avec un POST /doAuthentication.do. L'authentification est effectuée par le serveur virtuel d'authentification.
6. Si les informations d'identification sont correctes, le serveur virtuel d'authentification envoie une réponse HTTP 302 à l'URL cgi/selfauth sur le serveur d'équilibrage de charge avec un jeton unique (OTP).
7. Le serveur d'équilibrage de charge envoie HTTP 302 au client.
8. Le client envoie une requête GET pour son URL cible initiale avec un cookie de 32 octets.



Authentification basée sur 401

May 5, 2023

Avec l'authentification basée sur 401, l'appliance NetScaler présente une boîte de dialogue contextuelle à l'utilisateur final.



AAA-TM basé sur un formulaire fonctionne sur les messages de redirection. Certaines applications ne prennent pas en charge les redirections. Dans ce cas, l'authentification 401 AAA-TM activée est utilisée.

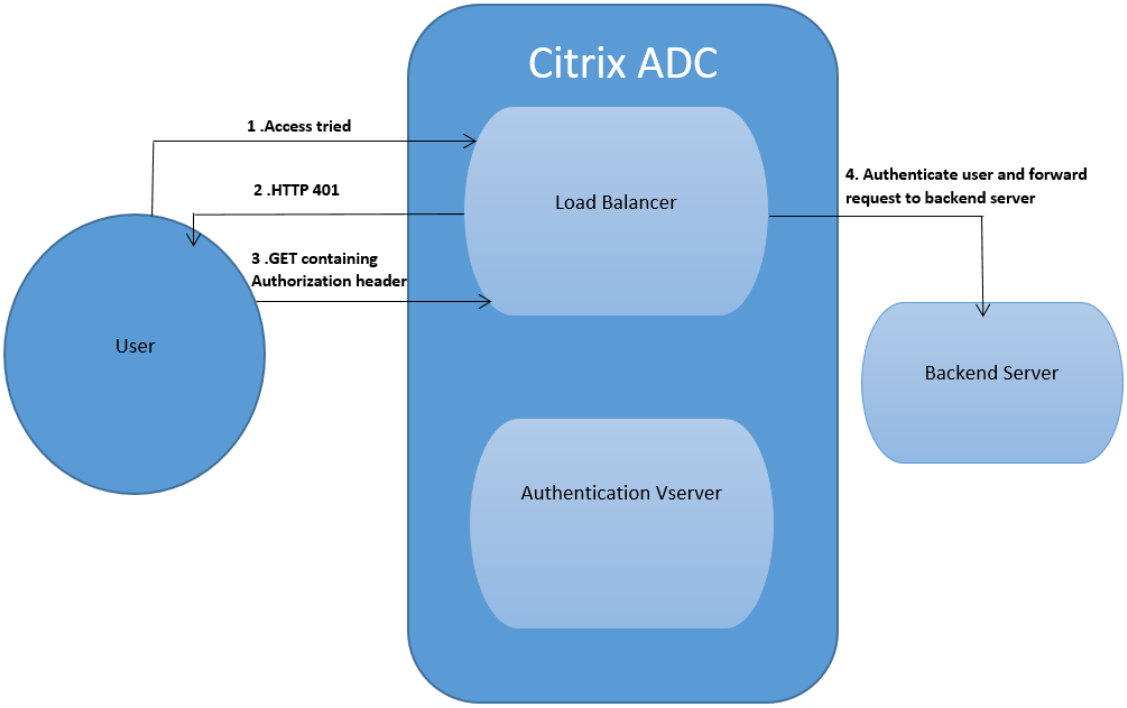
Activez les paramètres suivants pour que 401 Authentication AAA-TM fonctionne.

- La valeur du paramètre « AuthNvsName » du serveur virtuel d'équilibrage de charge doit être le nom du serveur virtuel d'authentification à utiliser pour authentifier les utilisateurs.
- Le paramètre « authn401 » doit être activé. La commande pour configurer la même chose est la suivante :

```
1  set lb vs lb1 -authn401 on -authnvsName <aaavs-name>
```

Les étapes suivantes expliquant le fonctionnement de l'authentification 401 :

1. L'utilisateur essaie d'accéder à une URL particulière à l'aide du serveur virtuel d'équilibrage de charge.
2. Le serveur virtuel d'équilibrage de charge renvoie une réponse HTTP 401 à l'utilisateur indiquant que l'authentification est requise pour l'accès.
3. L'utilisateur envoie ses informations d'identification au serveur virtuel d'équilibrage de charge dans l'en-tête d'autorisation.
4. Le serveur virtuel d'équilibrage de charge authentifie l'utilisateur, puis connecte l'utilisateur aux serveurs principaux.



> **Important :**
>
> Pour un serveur virtuel d'équilibrage de charge avec l'authentification 401 activée, plusieurs sessions d'authentification et d'autorisation peuvent être créées pour le même utilisateur en peu de temps. Cette configuration peut entraîner un pic de mémoire. Vous pouvez appliquer la configuration suivante sur l'appliance NetScaler pour déboguer et identifier l'application cliente finale.

```
1 set syslogparams -userDefinedAuditlog yes
2
3 add audit messageaction 401_log_act InFORMATIONAL '"LB-401 accessed:
     User: <" + AAA.USER.NAME + "> SessionID <"+ AAA.USER.SESSIONID + ">
     Client :<" + CLIENT.IP.SRC + "> accessed URL: <" + HTTP.REQ.URL +
     ">"'
4
5 add rewritepolicy rewrite_401_log true NOREWRITE -logAction 401_log_act
6
7 bind lb vserver <lb_name> -policyName rewrite_401_log -priority 100 -
     type reqUEST
8 <!--NeedCopy-->
```


Configuration Re-captcha pour l'authentification NFactor

May 5, 2023

NetScaler Gateway prend en charge une nouvelle action de premier ordre `captchaAction` qui simplifie la configuration du re-CAPTCHA. Le re-captcha étant une action de première classe, il peut être un facteur à part entière. Vous pouvez injecter Re-captcha n'importe où dans le flux nFactor.

Auparavant, vous deviez également écrire des stratégies WebAuth personnalisées avec des modifications apportées à l'interface RFWebUI. Avec l'introduction de `captchaAction`, vous n'avez pas à modifier le code JavaScript.

> **Important :**
>
> Si Re-captcha est utilisé avec les champs de nom d'utilisateur ou de mot de passe dans le schéma, le bouton **Soumettre** est désactivé jusqu'à ce que le re-captcha soit atteint.

Configuration du re-captcha

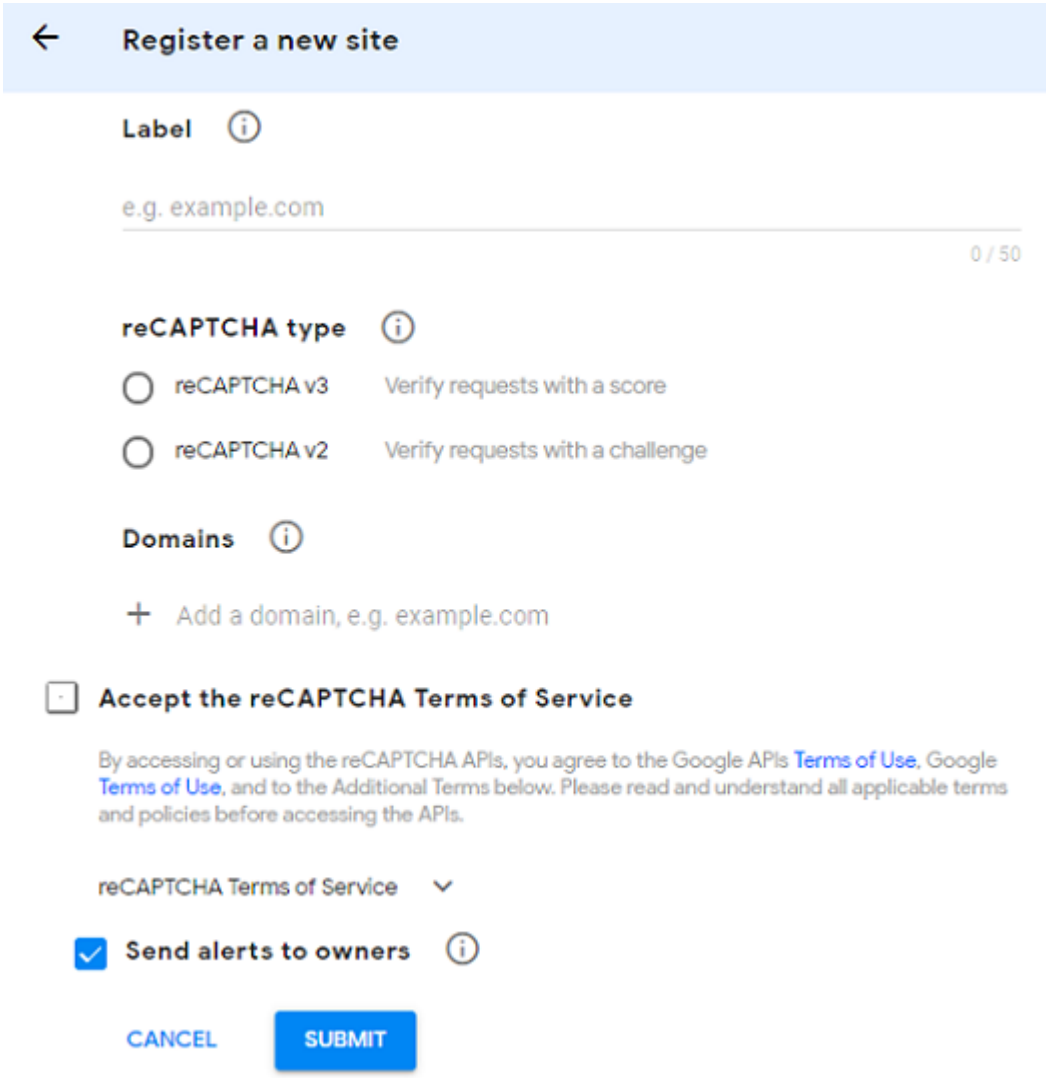
La configuration du re-captcha comporte deux parties.

1. Configuration sur Google pour l'enregistrement de re-CAPTCHA.
2. Configuration sur l'appliance NetScaler pour utiliser re-Captcha dans le cadre du flux de connexion.

Configuration du re-captcha sur Google

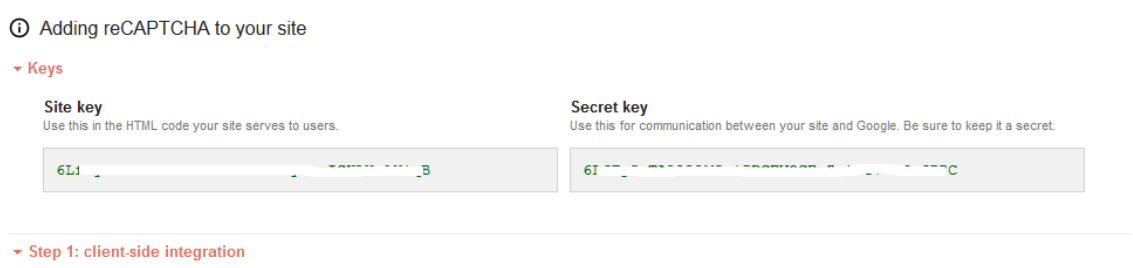
Enregistrez un domaine pour re-CAPTCHA sur https://www.google.com/recaptcha/admin#llist.

1. Lorsque vous accédez à cette page, l'écran suivant apparaît.



> **Remarque**
>
> Utilisez uniquement reCAPTCHA v2. Le re-captcha invisible est toujours en prévisualisation.

2. Une fois qu'un domaine est enregistré, la « SiteKey » et la « SecretKey » sont affichées.



> **Remarque**
>
> La « SiteKey » et la « SecretKey » sont grisées pour des raisons de sécurité. « SecretKey » doit être conservé en lieu sûr.

Configuration Re-Captcha sur une appliance NetScaler

La configuration Re-Captcha sur l'appliance NetScaler peut être divisée en trois parties :

- Afficher l'écran de re-captcha
- Publier la réponse Re-CAPTCHA sur le serveur Google
- La configuration LDAP est le deuxième facteur d'ouverture de session utilisateur (facultatif)

Afficher l'écran de re-captcha

La personnalisation du formulaire de connexion s'effectue via le schéma de connexion SingleAuthCaptcha.xml. Cette personnalisation est spécifiée au niveau du serveur virtuel d'authentification et est envoyée à l'interface utilisateur pour afficher le formulaire de connexion. Le schéma de connexion intégré, SingleAuthCaptcha.xml, se trouve dans le `/nsconfig/loginSchema/LoginSchema` répertoire de l'appliance NetScaler.

> **Important**
>
> - Le schéma de connexion SingleAuthCaptcha.xml peut être utilisé lorsque LDAP est configuré comme premier facteur.
> - En fonction de votre cas d'utilisation et de différents schémas, vous pouvez modifier le schéma existant. Par exemple, si vous n'avez besoin que du facteur Re-captcha (sans nom d'utilisateur ni mot de passe) ou d'une double authentification avec Re-Captcha.
> - Si des modifications personnalisées sont effectuées ou si le fichier est renommé, Citrix recommande de copier tous les loginSchemas du répertoire `/nsconfig/loginschema/LoginSchema` vers le répertoire parent `/nsconfig/loginschema`.

Pour configurer l'affichage de re-captcha à l'aide de la CLI

```
1 add authentication loginSchema singleauthcaptcha -authenticationSchema
    /nsconfig/loginschema/SingleAuthCaptcha.xml
2
3 add authentication loginSchemaPolicy singleauthcaptcha -rule true -
    action singleauthcaptcha
4
5 add authentication vserver auth SSL <IP> <Port>
6
```



```
add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-file>

bind ssl vserver auth -certkey vserver-cert

bind authentication vserver auth -policy singleauthcaptcha -priority 5 -gotoPriorityExpression END
<!--NeedCopy-->
```

Publier la réponse Re-CAPTCHA sur le serveur Google

Après avoir configuré le re-captcha qui doit être affiché aux utilisateurs, les administrateurs ajoutent la configuration au serveur Google pour vérifier la réponse de re-captcha du navigateur.

Pour vérifier la réponse de re-captcha depuis le navigateur

```
add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-from-google> -secretkey <secretkey-from-google>

add authentication policy myrecaptcha -rule true -action myrecaptcha

bind authentication vserver auth -policy myrecaptcha -priority 1
<!--NeedCopy-->
```

Les commandes suivantes sont nécessaires pour configurer si l'authentification AD est souhaitée. Sinon, vous pouvez ignorer cette étape.

```
add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort 636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup

add authenticationpolicy ldap-new -rule true -action ldap-new
<!--NeedCopy-->
```

La configuration LDAP est le deuxième facteur d'ouverture de session utilisateur (facultatif)

L'authentification LDAP se produit après re-captcha, vous l'ajoutez au second facteur.

```
add authentication policylabel second-factor

```



```
bind authentication policylabel second-factor -policy ldap-new -
    priority 10

bind authentication vserver auth -policy myrecaptcha -priority 1 -
    nextFactor second-factor
<!--NeedCopy-->
```

L'administrateur doit ajouter des serveurs virtuels appropriés selon que le serveur virtuel d'équilibrage de charge ou l'appliance NetScaler Gateway est utilisé pour l'accès. L'administrateur doit configurer la commande suivante si un serveur virtuel d'équilibrage de charge est requis :

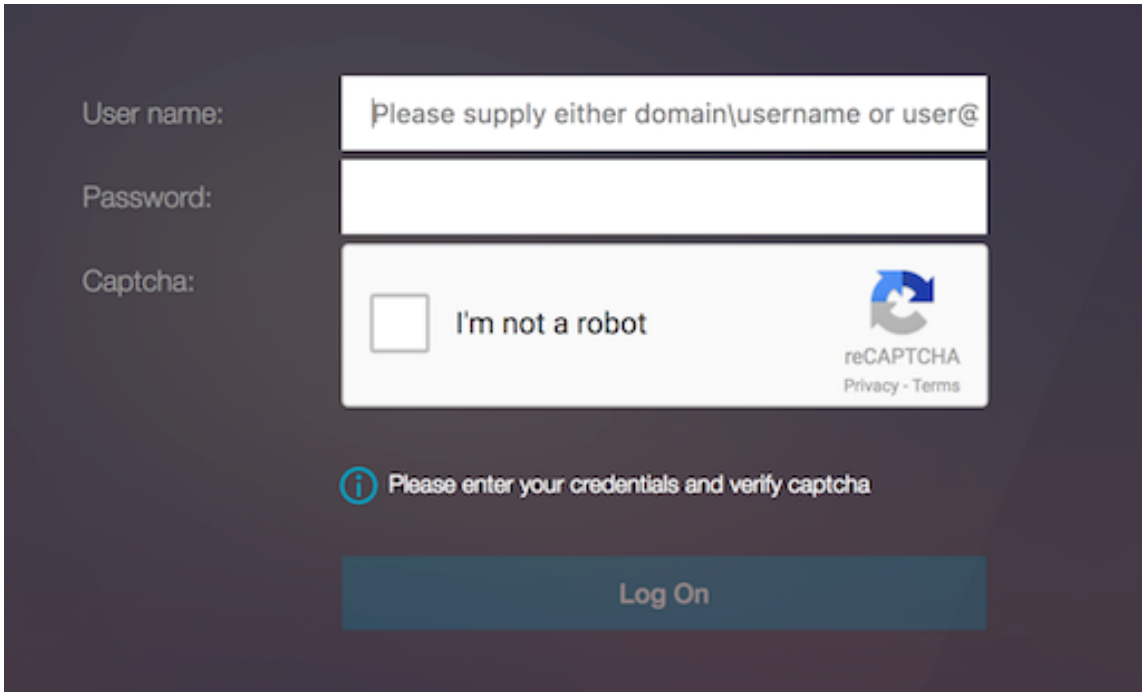
```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
    authenticationHost nssp.aaatm.com
<!--NeedCopy-->
```

nssp.aaatm.com — Résolution en serveur virtuel d'authentification.

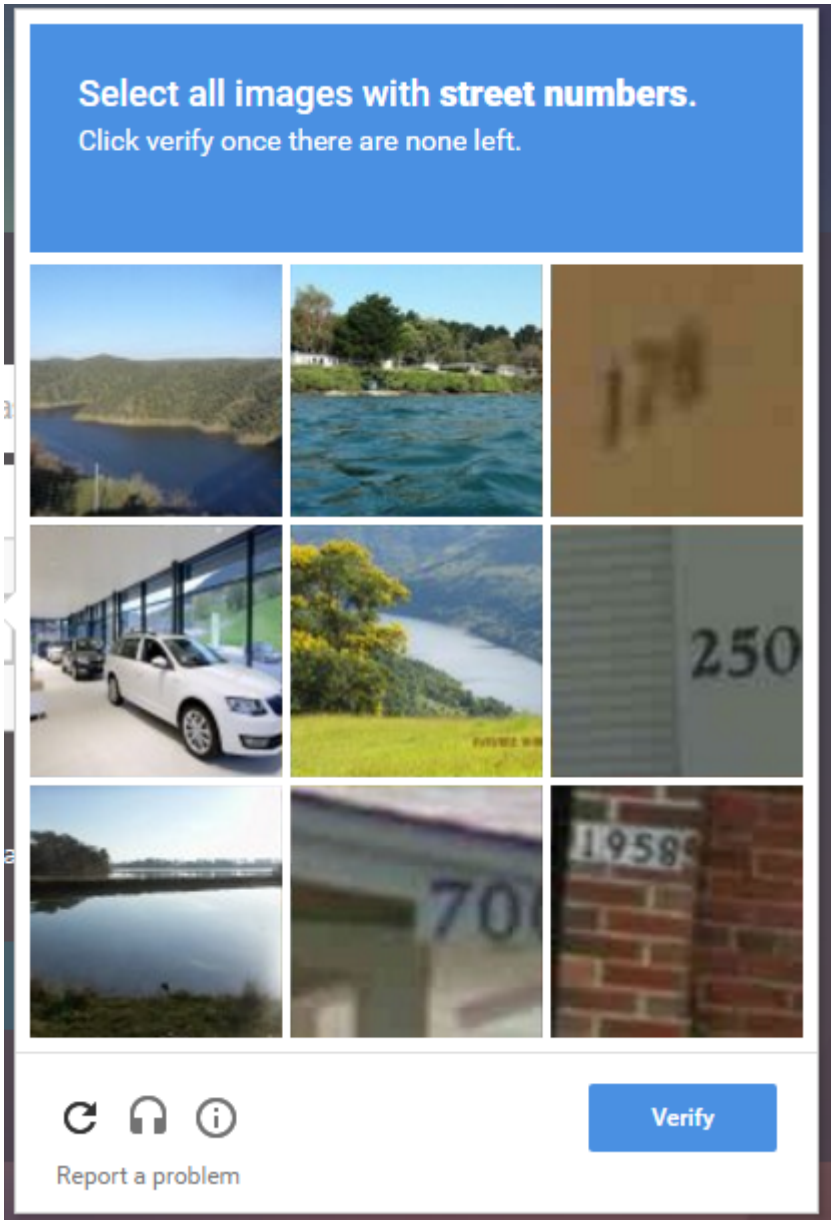
Validation utilisateur de re-CAPTCHA

Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir l'interface utilisateur suivante.

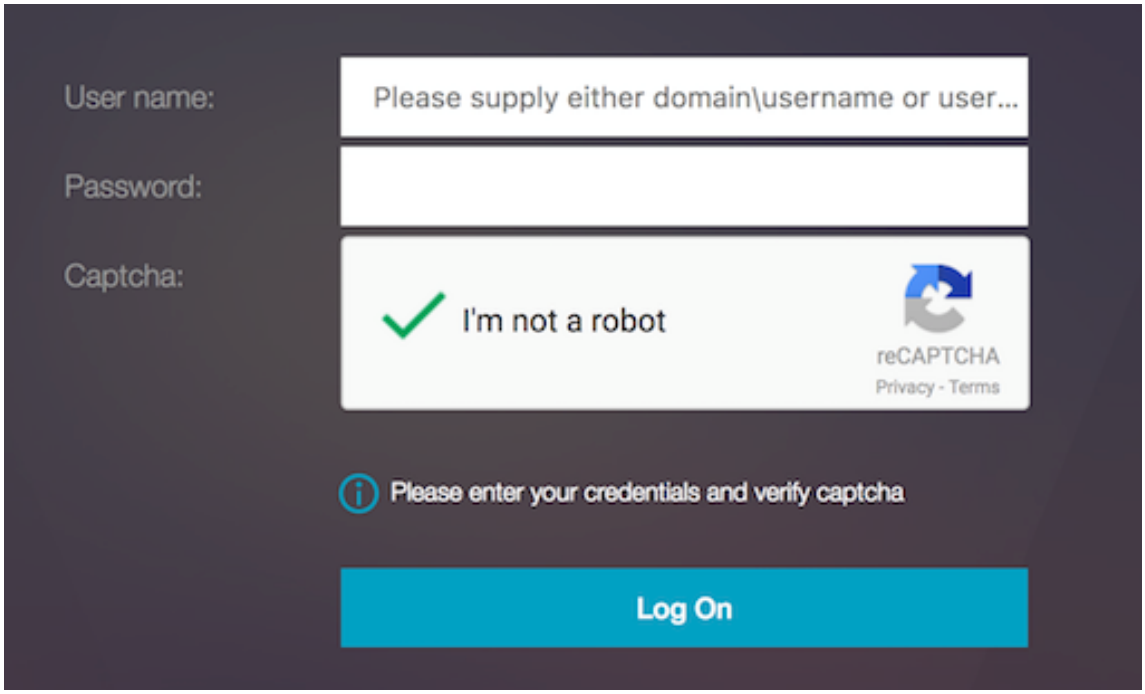
1. Une fois que le serveur virtuel d'authentification charge la page de connexion, l'écran de connexion s'affiche. La **connexion** est désactivée tant que le re-captcha n'est pas terminé.



2. Sélectionnez l'option Je ne suis pas un robot. Le widget Re-captcha s'affiche.



3. Vous parcourez une série d'images re-captcha, avant que la page de fin ne s'affiche.
4. Entrez les informations d'identification AD, activez la case à cocher **Je ne suis pas un robot** et cliquez **sur Ouvrir une session**. Si l'authentification réussit, vous êtes redirigé vers la ressource souhaitée.



Remarques :

- Si Re-captcha est utilisé avec l'authentification AD, le bouton **Envoyer** pour les informations d'identification est désactivé jusqu'à ce que le re-captcha soit terminé.
- Le re-captcha se produit dans un facteur qui lui est propre. Par conséquent, toutes les validations ultérieures telles que AD doivent avoir lieu dans le `nextfactor` du Re-CAPTCHA.

Prise en charge OTP native pour l'authentification

May 5, 2023

NetScaler prend en charge les mots de passe à usage unique (OTP) sans avoir à utiliser un serveur tiers. Le mot de passe à usage unique est une option hautement sécurisée pour l'authentification auprès de serveurs sécurisés, car le numéro ou le code d'accès généré est aléatoire. Auparavant, des entreprises spécialisées, telles que RSA avec des appareils spécifiques générant des nombres aléatoires, proposaient les OTP.

Outre la réduction des dépenses d'investissement et d'exploitation, cette fonctionnalité renforce le contrôle de l'administrateur en conservant l'intégralité de la configuration sur l'appliance NetScaler.

Remarque :

Étant donné que les serveurs tiers ne sont plus nécessaires, l'administrateur NetScaler doit con-

> figurer une interface pour gérer et valider les machines utilisateur.

L'utilisateur doit être enregistré auprès d'un serveur virtuel NetScaler pour utiliser la solution OTP. L'enregistrement n'est requis qu'une seule fois par appareil unique et peut être limité à certains environnements. La configuration et la validation d'un utilisateur enregistré sont similaires à la configuration d'une stratégie d'authentification supplémentaire.

Avantages de la prise en charge native d'OTP

- Réduit les coûts d'exploitation en éliminant la nécessité de disposer d'une infrastructure supplémentaire sur un serveur d'authentification en plus d'Active Directory.
- Consolide la configuration uniquement sur l'appliance NetScaler, offrant ainsi un contrôle optimal aux administrateurs.
- Élimine la dépendance du client à l'égard d'un serveur d'authentification supplémentaire pour générer un nombre attendu par les clients.

Workflow OTP natif

La solution OTP native est un processus à deux volets et le flux de travail est classé comme suit :

- Enregistrement de l'appareil
- Connexion de l'utilisateur final

Important :

> Vous pouvez ignorer le processus d'enregistrement si vous utilisez des solutions tierces ou si vous gérez d'autres appareils en dehors de l'appliance NetScaler. La dernière chaîne que vous ajoutez doit être au format spécifié par NetScaler.

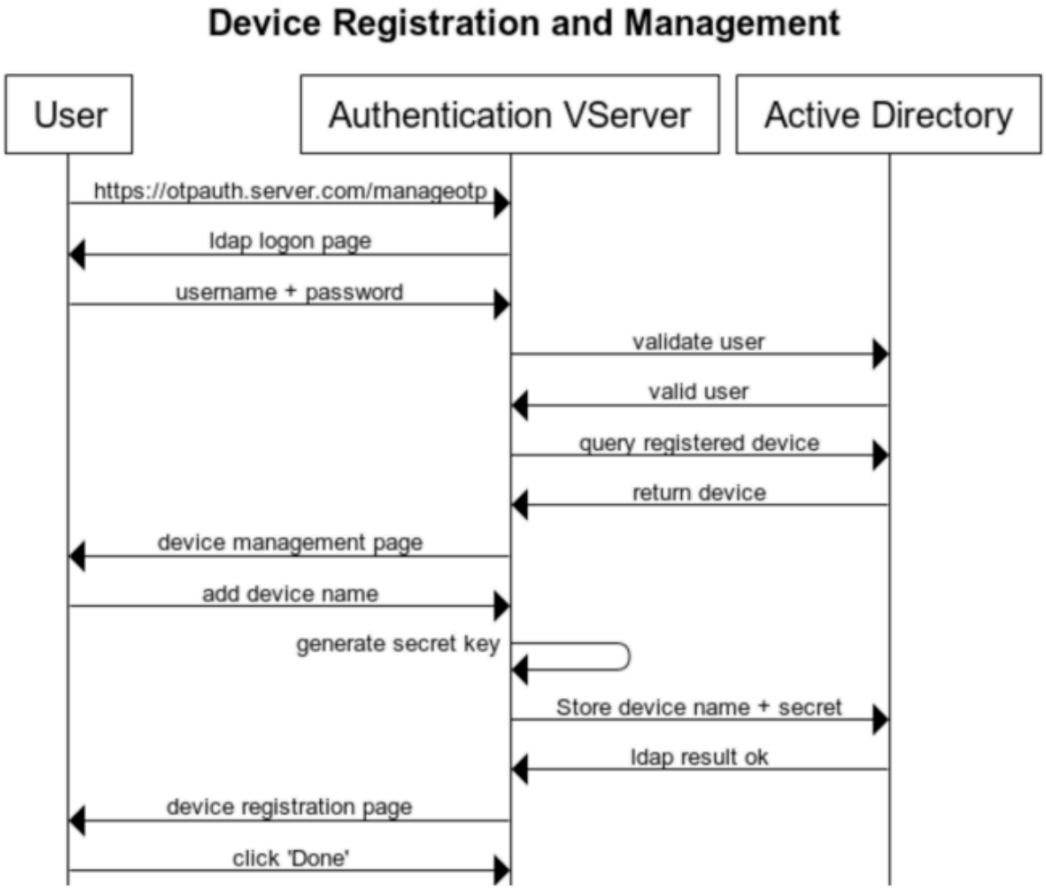
La figure suivante illustre le flux d'enregistrement des appareils pour enregistrer un nouveau périphérique à recevoir OTP.

Remarque :

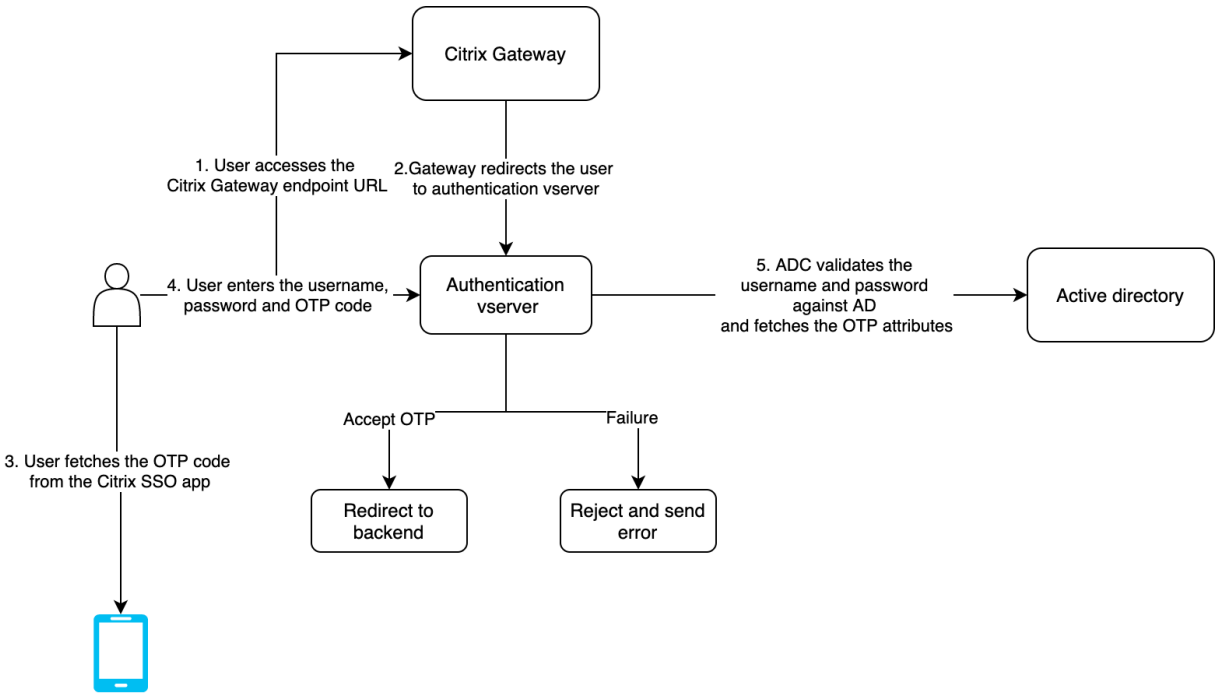
> L'enregistrement de l'appareil peut être effectué en utilisant un certain nombre de facteurs. Le facteur unique (tel que spécifié dans la figure précédente) est utilisé à titre d'exemple pour expliquer le processus d'enregistrement des appareils.

La figure suivante illustre la vérification de l'OTP via l'appareil enregistré.

La figure suivante illustre le flux d'enregistrement et de gestion des appareils.



La figure suivante illustre le flux de l'utilisateur final pour la fonctionnalité OTP native.



Composants requis

Pour utiliser la fonctionnalité OTP native, assurez-vous que les conditions préalables suivantes sont remplies.

- La version finale des fonctionnalités de NetScaler est la version 12.0 build 51.24 et les versions ultérieures.
- La licence d'édition avancée ou Premium est installée sur NetScaler Gateway.
- NetScaler est configuré avec une adresse IP de gestion et la console de gestion est accessible à la fois à l'aide d'un navigateur et d'une ligne de commande.
- NetScaler est configuré avec un serveur virtuel d'authentification, d'autorisation et d'audit pour authentifier les utilisateurs. Pour plus d'informations, voir Serveur virtuel d'authentification
- L'appliance NetScaler est configurée avec Unified Gateway et le profil d'authentification, d'autorisation et d'audit est attribué au serveur virtuel Gateway.
- La solution OTP native est limitée au flux d'authentification nFactor. Des stratégies avancées sont nécessaires pour configurer la solution. Pour plus de détails, voir OTP natif

Vérifiez également ce qui suit pour Active Directory :

- La longueur minimale des attributs est de 256 caractères.
- Le type d'attribut doit être « DirectoryString » tel que UserParameters. Ces attributs peuvent contenir des valeurs de chaîne.
- Le type de chaîne d'attribut doit être Unicode, si le nom de l'appareil est en caractères non anglais.

- L'administrateur LDAP de NetScaler doit disposer d'un accès en écriture à l'attribut AD sélectionné.
- L'appliance NetScaler et la machine cliente doivent être synchronisées avec un serveur Network Time commun.

Configuration du protocole OTP natif à l'aide de l'interface graphique

L'enregistrement OTP natif n'est pas seulement une authentification à facteur unique. Les sections suivantes vous aident à configurer l'authentification à un facteur et à un deuxième facteur.

Créer un schéma de connexion pour le premier facteur

1. Accédez à **Sécurité AAA > Trafic des applications > Schéma de connexion**.
2. Accédez à **Profils** et cliquez sur **Ajouter**.
3. Sur la page **Créer un schéma de connexion d'authentification**, saisissez *lschema_single_auth_manage_otp* dans le champ **Nom** et cliquez sur **Modifier** en regard de **noschema**.
4. Cliquez sur le dossier **LoginSchema** .
5. Faites défiler l'écran vers le bas pour sélectionner **SingleAuthManageOTP.xml** et cliquez sur **Sélectionner**.
6. Cliquez sur **Create**.
7. Cliquez sur **Stratégies**, puis sur **Ajouter**.
8. Dans l'écran **Créer une stratégie de schéma de connexion d'authentification**, entrez les valeurs suivantes.

   Nom : lpol_single_auth_manage_otp_by_url

   Profil : Sélectionnez lschema_single_auth_manage_otp dans la liste.

   Règle : HTTP.REQ.COOKIE.VALUE (« NSC_TASS ») .EQ (»`manageotp`«)

Configuration du serveur virtuel d'authentification, d'autorisation et d'audit

1. Accédez à **Sécurité > AAA — Trafic des applications > Serveurs virtuels d'authentification**. Cliquez pour modifier le serveur virtuel existant. Pour plus d'informations, voir Serveur virtuel d'authentification
2. Cliquez sur l'icône **+** en regard de **Schemas de connexion** sous **Paramètres avancés** dans le volet droit.
3. Sélectionnez **Aucun schéma de connexion**.

4. Cliquez sur la flèche et sélectionnez la stratégie **lpol_single_auth_manage_otp_by_url**, cliquez sur **Sélectionner**, puis sur **Lier**.
5. Faites défiler la page vers le haut et sélectionnez **1 Stratégie d'authentification** sous **Stratégie d'authentification avancée** .
6. Cliquez avec le bouton droit sur la **stratégie nFactor** et sélectionnez **Modifier la liaison** . Cliquez avec le bouton droit sur la stratégie nFactor déjà configurée ou reportez-vous à NFactor pour en créer une et sélectionner Modifier la liaison.
7. Cliquez sur la flèche située sous **Sélectionner le facteur suivant** pour sélectionner une configuration existante ou cliquez sur **Ajouter** pour créer un facteur.
8. Dans l'écran **Créer une stratégie d'authentification**, entrez ce qui suit et cliquez sur **Continuer** :

   Nom : manage_otp_flow_label

   Schéma de connexion : Lschema_Int
9. Sur l'écran **Étiquette de stratégie d'authentification**, cliquez sur **Ajouter** pour créer une stratégie.

   ```
   Create a policy for a normal LDAP server.
   ```
10. Dans l'écran **Créer une stratégie d'authentification**, entrez les éléments suivants :

    Nom : auth_pol_ldap_native_otp
11. Sélectionnez le type d'action comme **LDAP** à l'aide de la liste **Type d'action** .
12. Dans le champ **Action**, cliquez sur **Ajouter** pour créer une action.

    ```
    Create the first LDAP action with authentication enabled to be used for
     single factor.
    ```
13. Dans la page **Créer un serveur LDAP d'authentification**, sélectionnez le bouton radio **IP du serveur**, désélectionnez la case à cocher en regard de **Authentification**, entrez les valeurs suivantes, puis sélectionnez **Tester la connexion**. Voici un exemple de configuration.

    Nom : ldap_native_otp

    Adresse IP : 192.8.xx.xx

    DN de base : DC=Formation, DC=Lab

    Administrateur : Administrator@training.lab

    Mot de passe : `xxxxx`

    ```
    Create a policy for OTP .
    ```


14. Dans l'écran **Créer une stratégie d'authentification**, entrez les éléments suivants :

    Nom : auth_pol_ldap_otp_action

15. Sélectionnez le type d'action comme **LDAP** à l'aide de la liste **Type d'action** .

16. Dans le champ **Action**, cliquez sur **Ajouter** pour créer une action.

    ```
    Create the second LDAP action to set OTP authenticator with OTP secret
    configuration and authentication unchecked.
    ```

17. Dans la page **Créer un serveur LDAP d'authentification**, sélectionnez le bouton radio **IP du serveur**, désélectionnez la case à cocher en regard de **Authentification**, entrez les valeurs suivantes, puis sélectionnez **Tester la connexion**. Voici un exemple de configuration.

    Nom : ldap_otp_action

    Adresse IP : 192.8.xx.xx

    DN de base : DC=Formation, DC=Lab

    Administrateur : Administrator@training.lab

    Mot de passe : `xxxxx`

18. Faites défiler l'écran jusqu'à la section **Autres paramètres** . Utilisez le menu déroulant pour sélectionner les options suivantes.
    Attribut de nom d'ouverture de session du serveur comme **nouveau** et saisissez **userprincipalname**.

19. Utilisez le menu déroulant pour sélectionner **Attribut de nom SSO** comme **Nouveau** et saisissez **userprincipalname**.

20. Saisissez « UserParameters » dans le champ **secret OTP** et cliquez sur **Plus**.

21. Saisissez les attributs suivants.

    Attribut 1 = mail
    Attribut 2 = ObjectGuid
    Attribut 3 = ImmutableID

22. Cliquez sur **OK**.

23. Sur la page **Créer une stratégie d'authentification**, définissez l'expression sur **true** et cliquez sur **Créer**.

24. Sur la page **Créer une étiquette de stratégie d'authentification**, cliquez sur **Liaison**, puis sur **Terminé.**

25. Sur la page **Liaison de stratégie**, cliquez sur **Liaison**.

26. Dans la page **Stratégie d'authentification**, cliquez sur **Fermer** et cliquez sur **Terminé** .

    ```
    Create OTP for OTP verification.
    ```


27. Dans l'écran **Créer une stratégie d'authentification**, entrez les éléments suivants :

    Nom : auth_pol_ldap_otp_verify

28. Sélectionnez le type d'action comme **LDAP** à l'aide de la liste **Type d'action** .

29. Dans le champ **Action**, cliquez sur **Ajouter** pour créer une action.

    `Create the third LDAP action to verify OTP.`

30. Dans la page **Créer un serveur LDAP d'authentification**, sélectionnez le bouton radio **IP du serveur**, désélectionnez la case à cocher en regard de **Authentification**, entrez les valeurs suivantes, puis sélectionnez **Tester la connexion**. Voici un exemple de configuration.

    Nom : ldap_verify_otp

    Adresse IP : 192.168.xx.xx

    DN de base : DC=Formation, DC=Lab

    Administrateur : Administrator@training.lab

    Mot de passe : `xxxxx`

31. Faites défiler l'écran jusqu'à la section **Autres paramètres** . Utilisez le menu déroulant pour sélectionner les options suivantes.
    Attribut de nom d'ouverture de session du serveur comme **nouveau** et saisissez **userprincipalname**.

32. Utilisez le menu déroulant pour sélectionner **Attribut de nom SSO** comme **Nouveau** et saisissez **userprincipalname**.

33. Saisissez « UserParameters » dans le champ **secret OTP** et cliquez sur **Plus**.

34. Saisissez les attributs suivants.

    Attribut 1 = mail
    Attribut 2 = ObjectGuid
    Attribut 3 = ImmutableID

35. Cliquez sur **OK**.

36. Sur la page **Créer une stratégie d'authentification**, définissez l'expression sur **true** et cliquez sur **Créer**.

37. Sur la page **Créer une étiquette de stratégie d'authentification**, cliquez sur **Liaison**, puis sur **Terminé.**

38. Sur la page **Liaison de stratégie**, cliquez sur **Liaison**.

39. Dans la page **Stratégie d'authentification**, cliquez sur **Fermer** et cliquez sur **Terminé** .

Vous n'avez probablement pas encore de stratégie d'authentification avancée pour votre serveur LDAP normal.
Changez le type d'action sur LDAP.
Sélectionnez votre serveur LDAP normal, qui est celui sur lequel l'authentification est activée.
Saisissez true comme expression. Cette option utilise la stratégie avancée au lieu de la syntaxe classique.
Cliquez sur **Créer**.

> **Remarque :**
>
> Le serveur virtuel d'authentification doit être lié au thème du portail RFWebUI. Liez un certificat de serveur au serveur. L'adresse IP du serveur '1.2.3.5' doit avoir un nom de domaine complet correspondant, otpauth.server.com, pour une utilisation ultérieure.

Créer un schéma de connexion pour le deuxième facteur OTP

1. Accédez à **Sécurité > Trafic des applications AAA > Serveurs virtuels**. Sélectionnez le serveur virtuel à modifier.
2. Faites défiler l'écran vers le bas et sélectionnez **1 schéma de connexion**.
3. Cliquez sur **Ajouter une liaison**.
4. Dans la section **Liaison de stratégie**, cliquez sur **Ajouter** pour ajouter une stratégie.
5. Sur la page **Créer une stratégie de schéma de connexion d'authentification**, entrez Nom comme OTP, puis cliquez sur **Ajouter** pour créer un profil.
6. Sur la page **Créer un schéma de connexion d'authentification**, entrez Nom en tant qu'OTP, puis cliquez sur l'icône en forme de crayon en regard de **noschema**.
7. Cliquez sur le dossier **Loginschema**, sélectionnez **DualAuthManageOTP.xml**, puis cliquez sur **Sélectionner**.
8. Cliquez sur **Plus** et faites défiler vers le bas.
9. Dans le champ **Index des informations d'identification du mot** de passe, entrez 1. Cela amène nFactor à enregistrer le mot de passe de l'utilisateur dans l'attribut d'authentification, d'autorisation et d'audit #1, qui peut être utilisé ultérieurement dans une stratégie de trafic pour l'authentification unique à StoreFront. Si vous ne le faites pas, NetScaler Gateway essaie d'utiliser le code d'accès pour s'authentifier auprès de StoreFront, ce qui ne fonctionne pas.
10. Cliquez sur **Create**.
11. Dans la section **Règle**, saisissez **Vrai**. Cliquez sur **Create**.
12. Cliquez sur **Bind**.
13. Notez les deux facteurs d'authentification. Cliquez sur **Fermer**, puis sur **Terminé** .

Stratégie de trafic pour l'authentification unique

1. Accédez à **NetScaler Gateway > Politiques > Trafic**

2. Dans l'onglet **Profils de trafic**, cliquez sur **Ajouter**.
3. Entrez un nom pour le profil de trafic pour OTP.
4. Faites défiler vers le bas, dans la zone Expression de mot de passe SSO, entrez ce qui suit, puis cliquez sur **Créer**. C'est ici que nous utilisons l'attribut mot de passe du schéma de connexion spécifié pour le deuxième facteur OTP.

   ```
   http.REQ.USER.ATTRIBUTE(1)
   ```

5. Dans l'onglet **Stratégies de trafic**, cliquez sur **Ajouter**.
6. Dans le champ **Nom**, entrez un nom pour la stratégie de trafic.
7. Dans le champ **Demander un profil**, sélectionnez le profil de trafic que vous avez créé.
8. Dans la zone Expression, saisissez **True**. Si votre serveur virtuel NetScaler Gateway autorise un VPN complet, modifiez l'expression comme suit.

   ```
   http.req.method.eq(post)||http.req.method.eq(get)&& false
   ```

9. Cliquez sur **Create**.

Configurer la stratégie de commutation de contenu pour gérer OTP

Les configurations suivantes sont requises si vous utilisez Unified Gateway.

1. Accédez à **Gestion du trafic > Changement de contenu > Stratégies**. Sélectionnez la stratégie de changement de contenu, cliquez avec le bouton droit de la souris et sélectionnez **Modifier**.
2. Modifiez l'expression pour évaluer l'instruction OR suivante, puis cliquez sur **OK** :

   ```
   is_vpn_url\|\|HTTP.REQ.URL.CONTAINS("manageotp")
   ```

Configuration du protocole OTP natif à l'aide de la CLI

Vous devez disposer des informations suivantes pour configurer la page de gestion des appareils OTP :

- IP attribuée au serveur virtuel d'authentification
- FQDN correspondant à l'adresse IP attribuée
- Certificat de serveur pour serveur virtuel d'authentification

> **Remarque :**
>
> Native OTP est une solution Web uniquement.

Pour configurer la page d'enregistrement et de gestion des appareils OTP

Créer un serveur virtuel d'authentification


```
1 ```
2 add authentication vserver authvs SSL 1.2.3.5 443
3 bind authentication vserver authvs -portaltheme RFWebUI
4 bind ssl vserver authvs -certkeyname otpauthcert
5 <!--NeedCopy--> ```
```

> **Remarque :**
>
> Le serveur virtuel d'authentification doit être lié au thème du portail RFWebUI. Liez un certificat de serveur au serveur. L'adresse IP du serveur '1.2.3.5' doit avoir un nom de domaine complet correspondant, otpauth.server.com, pour une utilisation ultérieure.

Pour créer une action d'ouverture de session LDAP

```
1 add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
      -  serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
      ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

Exemple :

```
1 add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -
      serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
      administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
      ldapLoginName userprincipalname
```

Pour ajouter une stratégie d'authentification pour l'ouverture de session LDAP

```
1 add authentication Policy auth_pol_ldap_logon -rule true -action
      ldap_logon_action
```

Pour présenter l'interface utilisateur via LoginsChema

Afficher le champ nom d'utilisateur et le champ de mot de passe aux utilisateurs lors de l'ouverture de session

```
1 add authentication loginSchema lschema_single_auth_manage_otp -
      authenticationSchema "/nsconfig/loginschema/LoginSchema/
      SingleAuthManageOTP.xml"
```


Afficher la page d'enregistrement et de gestion des périphériques

Citrix recommande deux façons d'afficher l'écran d'enregistrement et de gestion des appareils : URL ou nom d'hôte.

> **Remarque :**
>
> Actuellement, l'enregistrement et la gestion des appareils ne peuvent être effectués qu'à l'aide d'un navigateur.

- **Utilisation de l'URL**

  Lorsque l'URL contient « /manageotp »

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule "http.req.cookie.value("NSC_TASS").contains("manageotp")"-action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END`

- **Utiliser le nom d'hôte**

  Lorsque le nom d'hôte est « alt.server.com »

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule "http.req.header("host").eq("alt.server.com")"-action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_host -priority 20 -gotoPriorityExpression END`

Pour configurer la page de connexion utilisateur à l'aide de l'interface de ligne de commande

Vous devez disposer des informations suivantes pour configurer la page Ouverture de session utilisateur :

- IP pour un serveur virtuel d'équilibrage de charge
- Nom de domaine complet correspondant pour le serveur virtuel d'équilibrage de charge
- Certificat de serveur pour le serveur virtuel d'équilibrage de charge

```
1  bind ssl virtual server lbvs_https -certkeyname lbvs_server_cert
2  <!--NeedCopy-->
```

Le service back-end dans l'équilibrage de charge est représenté comme suit :

```
1  ```
2  add service iis_backendsso_server_com 1.2.3.210 HTTP 80
3  bind lb vserver lbvs_https iis_backendsso_server_com
```



```
<!--NeedCopy--> ```
```

Pour créer une action de validation du code secret OTP

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
    -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
    ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
    authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>`
```

Exemple :

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname -authentication DISABLED -OTPSecret
    userParameters
```

> **Important :**
>
> La différence entre l'ouverture de session LDAP et l'action OTP réside dans la nécessité de désactiver l'authentification et d'introduire un nouveau paramètre `OTPSecret`. N'utilisez pas la valeur de l'attribut AD.

Pour ajouter une stratégie d'authentification pour la validation du code d'accès OTP

```
add authentication Policy auth_pol_otp_validation -rule true -action
    ldap_otp_action
```

Pour présenter l'authentification à deux facteurs via LoginSchema

Ajoutez l'interface utilisateur pour l'authentification à deux facteurs.

```
add authentication loginSchema lscheme_dual_factor -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/DualAuth.xml
    "
add authentication loginSchemaPolicy lpol_dual_factor -rule true -
    action lscheme_dual_factor
```

Pour créer un facteur de validation de code secret via l'étiquette de stratégie

Créer une étiquette de stratégie de flux OTP de gestion pour le facteur suivant (le premier facteur est l'ouverture de session LDAP)


```
add authentication loginSchema lschema_noschema -authenticationSchema
    noschema
add authentication policylabel manage_otp_flow_label -loginSchema
    lschema_noschema
```

Pour lier la stratégie OTP à l'étiquette de stratégie

```
bind authentication policylabel manage_otp_flow_label -policyName
    auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

Pour lier le flux de l'interface utilisateur

Liez l'ouverture de session LDAP suivie de la validation OTP avec le serveur virtuel d'authentification.

```
bind authentication vserver authvs -policy auth_pol_ldap_logon -
    priority 10 -nextFactor  manage_otp_flow_label -
    gotoPriorityExpression NEXT
bind authentication vserver authvs -policy lpol_dual_factor -priority
    30 -gotoPriorityExpression END
```

Enregistrez votre appareil auprès de NetScaler

1. Sur votre navigateur, accédez à votre nom de domaine complet NetScaler (première adresse IP publique), avec le suffixe /manageotp. Par exemple, https://otpauth.server.com/manageotp connectez-vous avec les informations d'identification de l'utilisateur.
2. Cliquez sur l'icône **+** pour ajouter un appareil.
3. Entrez le nom d'un appareil et appuyez sur **Go**. Un code-barres apparaît à l'écran.
4. Cliquez sur **Commencer la configuration**, puis sur **Scanner le code-barres**.
5. Survolez le code QR avec la caméra de l'appareil. Vous pouvez éventuellement saisir le code.

   > **Remarque** :
   >
   > Le code QR affiché est valide pendant 3 minutes.

6. Une fois la numérisation réussie, un code temporel à 6 chiffres vous est présenté, qui peut être utilisé pour vous connecter.
7. Pour tester, cliquez sur **Terminé** sur l'écran QR, puis cliquez sur la coche verte à droite.
8. Sélectionnez votre appareil dans le menu déroulant et saisissez le code de Google Authenticator (il doit être bleu et non rouge), puis cliquez sur **OK**.

9. Assurez-vous de vous déconnecter à l'aide du menu déroulant situé dans le coin supérieur droit de la page.

Connectez-vous à NetScaler à l'aide de l'OTP

1. Accédez à votre première URL publique et saisissez votre OTP à partir de Google Authenticator pour ouvrir une session.
2. Authentifiez-vous sur la page d'accueil de NetScaler.

Stocker les données secrètes OTP dans un format crypté

May 5, 2023

À partir de la version 13.0 de NetScaler build 41.20, les données secrètes OTP peuvent être stockées dans un format crypté plutôt qu'en texte brut.

Auparavant, l'appliance NetScaler stockait le secret OTP sous forme de texte brut dans AD. Le stockage du secret OTP en texte brut constitue une menace pour la sécurité, car un attaquant malveillant ou un administrateur peut exploiter les données en consultant le secret partagé par d'autres utilisateurs.

Le paramètre de chiffrement active le chiffrement du secret OTP dans AD. Lorsque vous enregistrez un nouvel appareil auprès de NetScaler version 13.0 build 41.20 et que vous activez le paramètre de cryptage, le secret OTP est stocké dans un format crypté, par défaut. Toutefois, si le paramètre de chiffrement est désactivé, le secret OTP est stocké au format texte brut.

Pour les appareils enregistrés avant la version 13.0 41.20, vous devez effectuer les opérations suivantes en tant que bonne pratique :

1. Mettez à niveau l'appliance NetScaler 13.0 vers la version 13.0 41.20.
2. Activez le paramètre de chiffrement sur l'appliance.
3. Utilisez l'outil de migration secrète OTP pour migrer les données secrètes OTP du format texte brut au format crypté.

Pour plus de détails sur l'outil de migration secret OTP, consultez la section Outil de chiffrement OTP.

> **Important**
>
> : Citrix vous recommande, en tant qu'administrateur, de vous assurer que les critères suivants sont remplis :
>
> - Un nouveau certificat doit être configuré pour chiffrer les secrets OTP si vous n'utilisez pas KBA dans le cadre de la fonctionnalité de réinitialisation de mot de passe en libre-service.
>   - To bind the certificate to VPN global, you can use the following command:


```
bind vpn global -userDataEncryptionKey <certificate name>
```

- Si vous utilisez déjà un certificat pour chiffrer KBA, vous pouvez utiliser le même certificat pour chiffrer les secrets OTP.
- Les nouveaux enregistrements OTP se font toujours avec le dernier certificat relié, car celui-ci a la plus haute priorité. Dans l'exemple ci-dessous, si vous liez un certificat (cert1) puis un autre certificat (cert2), cert2 est pris en compte pour l'enregistrement de l'appareil. Si le certificat requis pour l'enregistrement de l'appareil est manquant, la connexion de l'utilisateur final échoue.

```
1    bind vpn global -userDataEncryptionKey otp-cert1
2    bind vpn global -userDataEncryptionKey otp-cert2
3    <!--NeedCopy-->
```

Dans l'exemple suivant, le certificat `cert2` est affiché en tant que première entrée sur la sortie de la commande `show vpn global` :

‘‘‘

show vpn global

Portal Theme: RfWebUI
Userdata Encryption Certificate: cert2
Userdata Encryption Certificate: cert1
1) VPN Clientless Access Policy Name: ns_cvpn_owa_policy Priority: 95000
Bindpoint: REQ_DEFAULT
2) VPN Clientless Access Policy Name: ns_cvpn_sp_policy Priority: 96000
Bindpoint: REQ_DEFAULT
3) VPN Clientless Access Policy Name: ns_cvpn_sp2013_policy Priority: 97000
Bindpoint: REQ_DEFAULT
4) VPN Clientless Access Policy Name: ns_cvpn_default_policy Priority: 100000
Bindpoint: REQ_DEFAULT
‘‘‘

Pour activer le cryptage des données OTP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Exemple

```
set aaa otpparameter -encryption ON
```


Pour configurer le cryptage OTP à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic de l'application** et cliquez sur **Modifier le paramètre OTP AAAd'authentification sous la section Paramètres d'authentification** .
2. Sur la page **Configurer le paramètre OTP AAA**, sélectionnez **Chiffrement secret OTP**.
3. Cliquez sur OK.

Configuration du nombre d'appareils des utilisateurs finaux pour recevoir des notifications OTP

Les administrateurs peuvent désormais configurer le nombre d'appareils qu'un utilisateur final peut enregistrer pour recevoir une notification OTP ou une authentification.

Pour configurer le nombre d'appareils dans OTP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

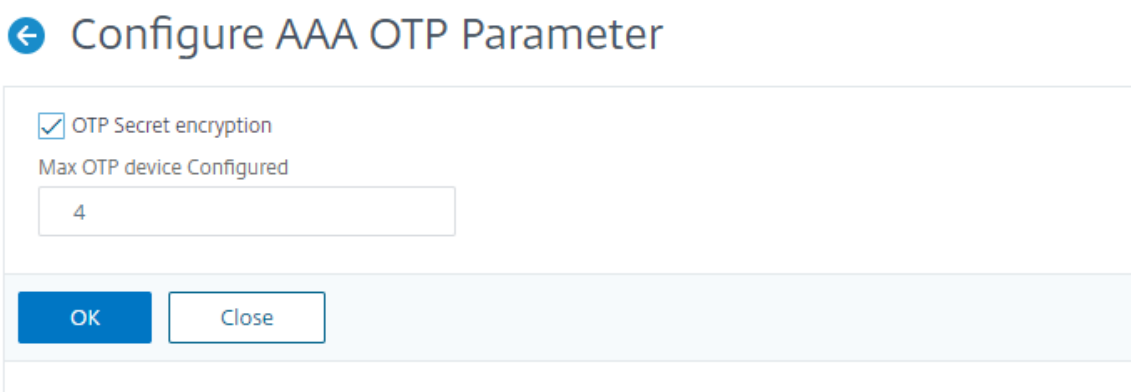
```
set aaa otpparameter [-maxOTPDevices <positive_integer>]
```

Exemple

```
set aaa otpparameter -maxOTPDevices 4
```

Pour configurer le nombre d'appareils à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic d'applications**, cliquez sur **Modifier le paramètre AAA OTPd'authentification dans la section Paramètres d'authentification** .
2. Sur la page **Configurer le paramètre OTP AAA**, entrez la valeur du nombre **maximal de périphériques OTP configurés**.
3. Cliquez sur **OK**.



Outil de cryptage OTP

May 5, 2023

À partir de la version 13.0 de NetScaler build 41.20, les données secrètes OTP sont stockées dans un format crypté plutôt qu'en texte brut pour une sécurité renforcée. Le stockage d'un secret OTP au format crypté est automatique et ne nécessite aucune intervention manuelle.

Auparavant, l'appliance NetScaler stockait un secret OTP sous forme de texte brut dans Active Directory. Le stockage d'un secret OTP au format texte brut représentait une menace pour la sécurité, car un attaquant malveillant ou un administrateur peut exploiter les données en consultant le secret partagé d'autres utilisateurs.

L'outil de chiffrement OTP offre les avantages suivants :

- N'entraîne aucune perte de données, même si vous possédez d'anciens appareils utilisant un ancien format (texte brut).
- La prise en charge de la rétrocompatibilité avec une ancienne version de NetScaler Gateway permet d'intégrer et de prendre en charge les appareils existants, ainsi que le nouvel appareil.
- L'outil de chiffrement OTP aide les administrateurs à migrer toutes les données secrètes OTP de tous les utilisateurs à la fois.

> **Remarque**
>
> L'outil de chiffrement OTP ne chiffre ni ne déchiffre les données d'enregistrement KBA ou d'enregistrement des e-mails.

Utilisation de l'outil de chiffrement OTP

L'outil de chiffrement OTP peut être utilisé pour les opérations suivantes :

- **Chiffrement**. Stockez le secret OTP dans un format crypté. L'outil extrait les données OTP des appareils enregistrés auprès de NetScaler, puis convertit les données OTP au format texte brut en format crypté.
- **Décryptage**. Rétablissez le code secret OTP au format texte brut.
- **Mettre à jour les certificats**. Les administrateurs peuvent mettre à jour le certificat vers un nouveau certificat à tout moment. Les administrateurs peuvent utiliser l'outil pour entrer le nouveau certificat et mettre à jour toutes les entrées avec les nouvelles données de certificat. Le chemin d'accès au certificat doit être soit un chemin absolu, soit un chemin relatif.

> **Important**
>
> - Vous devez activer le paramètre de chiffrement dans l'appliance NetScaler pour utiliser l'outil de chiffrement OTP.

- Pour les appareils enregistrés auprès de NetScaler avant la version 41.20, vous devez effectuer les opérations suivantes :
  - Upgrade the 13.0 NetScaler appliance to 13.0 build 41.20.
  - Enable the encryption parameter on the appliance.
  - Use the OTP Secret migration tool to migrate OTP secret data from plain text format to encrypted format.
- L'outil de chiffrement OTP ne prend en charge que les attributs utilisateur à valeur unique. Il ne prend pas en charge les attributs utilisateur à valeurs multiples.

Données secrètes OTP au format texte brut

Exemple :

```
##@devicename=<16 or more bytes>&tag=<64bytes>&,
```

Comme vous pouvez le constater, le motif de départ d'un ancien format est toujours « #@ » et le motif de fin est toujours « & ». Toutes les données entre « devicename= » et end pattern constituent les données OTP de l'utilisateur.

Données secrètes OTP au format crypté

Le nouveau format crypté des données OTP est au format suivant :

Exemple :

```
1     {
2
3          "otpdata" : {
4
5           "devices" : {
6
7                              "device1" :  "value1" ,
8                              "device2" :  "value2" , ···
9                         }
10
11                }
12
13       }
14
15 <!--NeedCopy-->
```

Où, value1 est une valeur codée en base64 des données de chiffrement KID + IV +

Les données chiffrées sont structurées comme suit :


```
    {

      secret:<16-byte secret>,
      tag : <64-byte tag value>
      alg: <algorithm used> (not mandatory, default is sha1, specify
          the algorithm only if it is not default)
     }

<!--NeedCopy-->
```

- Dans « appareils », vous avez une valeur associée à chaque nom. La valeur est base64encode (KID) .base64encode (IV) .base64encode (cipherdata).
- KID est la valeur d'identification de la clé utilisée pour identifier le certificat utilisé pour le chiffrement des données secrètes OTP. L'ID de clé est particulièrement utile lorsque plusieurs certificats sont utilisés pour le chiffrement des données secrètes OTP.
- Dans les algorithmes AES standard, IV est toujours envoyé sous forme de 16 ou 32 premiers octets de données chiffrées. Vous pouvez suivre le même modèle.
- IV diffère pour chaque appareil, bien que la clé reste la même.

> **Remarque :**
>
> Le format crypté des données OTP est stocké dans un attribut utilisateur AD.

Configuration de l'outil de chiffrement OTP

> **Remarque**
>
> Pour exécuter l'outil de chiffrement OTP, Citrix vous recommande d'utiliser une autre plateforme avec un environnement Python au lieu de l'appliance NetScaler.

L'outil de chiffrement OTP se trouve dans le répertoire `\var\netscaler\otptool`. Vous devez télécharger le code depuis la source NetScaler et exécuter l'outil avec les informations d'identification AD requises.

- Conditions préalables à l'utilisation de l'outil de chiffrement OTP :
  - Installez la version Python 3.5 ou supérieure dans l'environnement dans lequel cet outil est exécuté.
  - Installez pip3 ou une version ultérieure.
- Exécutez les commandes suivantes :
  - **pip install requirements.txt**. Installe automatiquement les exigences
  - **fichier main.py de python**. Appelle l'outil de chiffrement OTP. Vous devez fournir les arguments requis en fonction de votre besoin de migration des données secrètes OTP.
- L'outil peut être situé à `\var\netscaler\otptool` partir d'une invite de shell.

- Exécutez l'outil avec les informations d'identification AD requises.

Interface de l'outil de chiffrement OTP

La figure suivante présente un exemple d'interface d'outil de chiffrement OTP. L'interface contient tous les arguments qui doivent être définis pour le chiffrement/le déchiffrement/la mise à niveau du certificat. En outre, une brève description de chaque argument est capturée.

Argument OPÉRATION

Vous devez définir l'argument OPERATION pour utiliser l'outil de chiffrement OTP pour le chiffrement, le déchiffrement ou la mise à niveau du certificat.

Le tableau suivant récapitule certains des scénarios dans lesquels vous pouvez utiliser l'outil de chiffrement OTP et les valeurs d'argument OPERATION correspondantes.

Scénario	Valeur de l'argument d'opération et autres arguments
Convertir le code secret OTP en texte brut au format crypté dans le même attribut	Entrez la valeur de l'argument OPERATION sur 0 et fournissez la même valeur pour l'attribut source et cible. **Exemple :** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute unixhomedirectory -operation 0 -cert_path aaatm_wild_all.cert`
Convertir le code secret OTP en texte brut au format crypté dans un attribut différent	Entrez la valeur de l'argument OPERATION sous la forme 0 et indiquez les valeurs correspondantes pour les attributs source et cible. **Exemple :** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 0 -cert_path aaatm_wild_all.cert`

Scénario	Valeur de l'argument d'opération et autres arguments
Convertissez les entrées cryptées en texte brut	Entrez la valeur de l'argument OPERATION sur 1 et indiquez les valeurs correspondantes pour les attributs source et cible. **Exemple :** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 1 -cert_path aaatm_wild_all.cert`
Mettre à jour le certificat vers un nouveau certificat	Entrez la valeur de l'argument OPERATION sur 2 et fournissez tous les détails du certificat précédent et du nouveau certificat dans les arguments correspondants. **Exemple :** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -operation 2 -cert_path aaatm_wild_all.cert -new_cert_path aaatm_wild_all_new.cert`

Argument CERT_PATH

L'argument CERT_PATH est un fichier contenant le certificat utilisé dans NetScaler pour crypter les données. L'utilisateur doit fournir cet argument pour les trois opérations, à savoir les **certificats de **chiffrement**, de **déchiffrement**et de mise à jour**.

Le fichier d'arguments CERT_PATH doit contenir à la fois le certificat et la clé privée associée au format PEM ou CERT (pfx n'est pas pris en charge).

Par exemple, si les fichiers certificate.cert et certificate.key correspondent au fichier de certificat et à sa clé privée, dans un système similaire à Unix, la commande suivante crée le fichier `certkey.merged` qui peut être utilisé comme valeur pour l'indicateur cert_path.


```
$ cat certificate.cert certificate.key > certkey.merged
$
<!--NeedCopy-->
```

> **Points à noter sur le certificat**
>
> - L'utilisateur doit fournir le même certificat qui est lié globalement à l'appliance NetScaler pour le chiffrement des données utilisateur.
> - Le certificat doit contenir le certificat public codé Base64 et sa clé privée RSA correspondante dans le même fichier.
> - Le format du certificat doit être PEM ou CERT. Le certificat doit respecter le format X509.
> - Le format de certificat protégé par mot de passe et le fichier *.pfx* ne sont pas acceptés par cet outil. L'utilisateur doit convertir les certificats PFX en *.cert* avant de fournir les certificats à l'outil.

Argument SEARCH_FILTER

L'argument SEARCH_FILTER est utilisé pour filtrer les domaines ou les utilisateurs d'Active Directory.

Exemples :

- `-search_filter "(sAMAccountName=OTP*)"`: filtre les utilisateurs dont les SAMAccountNames (noms de connexion utilisateur) commencent par « OTP ».
- `-search_filter "(objectCategory=person)"`: filtre la catégorie d'objet de type personne.
- `-search_file "(objectclass=*)"`: filtre tous les objets.

Activation de l'option de chiffrement dans l'appliance NetScaler

Pour crypter le format de texte brut, vous devez activer l'option de cryptage dans l'appliance NetScaler.

Pour activer les données de chiffrement OTP à l'aide de l'interface de ligne de commande, à l'invite de commandes, tapez :

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Exemple :

```
set aaa otpparameter -encryption ON
```

Cas d'utilisation de l'outil de chiffrement OTP

L'outil de chiffrement OTP peut être utilisé pour les cas d'utilisation suivants.

Enregistrez de nouveaux appareils avec l'appliance NetScaler version 13.0 build 41.20

Lorsque vous enregistrez votre nouvel appareil auprès de l'appliance NetScaler version 13.0 build 41.x, et si l'option de cryptage est activée, les données OTP sont enregistrées dans un format crypté. Vous pouvez éviter toute intervention manuelle.

Si l'option de cryptage n'est pas activée, les données OTP sont stockées au format texte brut.

Migrer les données OTP pour les appareils enregistrés avant la version 13.0 build 41.20

Vous devez effectuer les opérations suivantes pour chiffrer les données secrètes OTP des appareils enregistrés auprès de l'appliance NetScaler avant la version 13.0 41.20.

- Utilisez l'outil de conversion pour migrer les données OTP du format texte brut au format crypté.
- Activez le paramètre « Chiffrement » sur l'appliance NetScaler.
  - Pour activer l'option de cryptage à l'aide de la CLI :
    - `set aaa otpparameter -encryption ON`
  - Pour activer les options de chiffrement à l'aide de l'interface graphique :
    - Accédez à **Sécurité > AAA — Trafic de l'application** et cliquez sur **Modifier le paramètre OTP AAAd'authentification sous la section Paramètres d'authentification** .
    - Sur la page **Configurer le paramètre OTP AAA**, sélectionnez **Chiffrement secret OTP**, puis cliquez sur **OK**.
  - Connectez-vous avec les informations d'identification AD valides.
  - Si nécessaire, enregistrez d'autres appareils (facultatif).

Migrer les données cryptées d'un ancien certificat vers un nouveau certificat

Si les administrateurs souhaitent mettre à jour le certificat vers un nouveau certificat, l'outil fournit une option pour mettre à jour les nouvelles entrées de données de certificat.

Pour mettre à jour le certificat en un nouveau à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

Exemple :

```
python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local
-search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -
target_attribute userparameters -operation 2 -cert_path aaatm_wild_all.cert
 -new_cert_path aaatm_wild_all_new.cert
```

> **Remarque**
>
> - Les certificats doivent comporter des clés privées et publiques.

> • Actuellement, la fonctionnalité n'est fournie que pour OTP.

Rechiffrer ou migrer vers un nouveau certificat pour les appareils enregistrés après la mise à niveau de l'appliance vers la version 13.0 build 41.20 avec chiffrement

L'administrateur peut utiliser l'outil sur les appareils déjà chiffrés avec un certificat et peut mettre à jour ce certificat avec un nouveau certificat.

Reconvertir les données cryptées au format texte brut

L'administrateur peut déchiffrer le secret OTP et le rétablir au format texte brut d'origine. L'outil de cryptage OTP analyse tous les utilisateurs à la recherche d'un secret OTP au format crypté et les convertit au format déchiffré.

Pour mettre à jour le certificat en un nouveau à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

Exemple :

```
python3 main.py -Host 192.0.2.1 - Port 636 -username ldapbind_user@aaa
    .local -search_base cn=users,dc=aaa,dc=local -source_attribute
    unixhomedirectory -target_attribute userparameters -operation 1
<!--NeedCopy-->
```

Dépannage

L'outil génère les fichiers journaux suivants.

- **Fichier app.log**. Consigne toutes les principales étapes d'exécution et les informations sur les erreurs, les avertissements et les échecs.
- **Fichier unmodified_users.txt**. Contient une liste de noms distinctifs utilisateur qui n'ont pas été mis à niveau du texte brut au format crypté. Ces journaux sont générés à une erreur de format ou peuvent être dus à une autre raison.

Notification Push pour OTP

May 5, 2023

NetScaler Gateway prend en charge les notifications push pour OTP. Les utilisateurs n'ont pas à saisir manuellement l'OTP reçu sur leurs appareils enregistrés pour se connecter à NetScaler Gateway. Les

administrateurs peuvent configurer NetScaler Gateway de telle sorte que les notifications de connexion soient envoyées aux appareils enregistrés des utilisateurs à l'aide de services de notification push. Lorsque les utilisateurs reçoivent la notification, ils doivent simplement appuyer sur Autoriser sur la notification pour se connecter à NetScaler Gateway. Lorsque la passerelle reçoit un accusé de réception de la part de l'utilisateur, elle identifie la source de la demande et envoie une réponse à cette connexion de navigateur.

Si la réponse à la notification n'est pas reçue dans le délai imparti (30 secondes), les utilisateurs sont redirigés vers la page de connexion de NetScaler Gateway. Les utilisateurs peuvent ensuite entrer l'OTP manuellement ou cliquer sur **Renvoyer la notification** pour recevoir à nouveau la notification sur l'appareil enregistré.

Les administrateurs peuvent faire de l'authentification par notification push l'authentification par défaut en utilisant les schémas de connexion créés pour les notifications push.

> **Important :**
>
> la fonctionnalité de notification push est disponible avec une licence NetScaler Premium Edition.

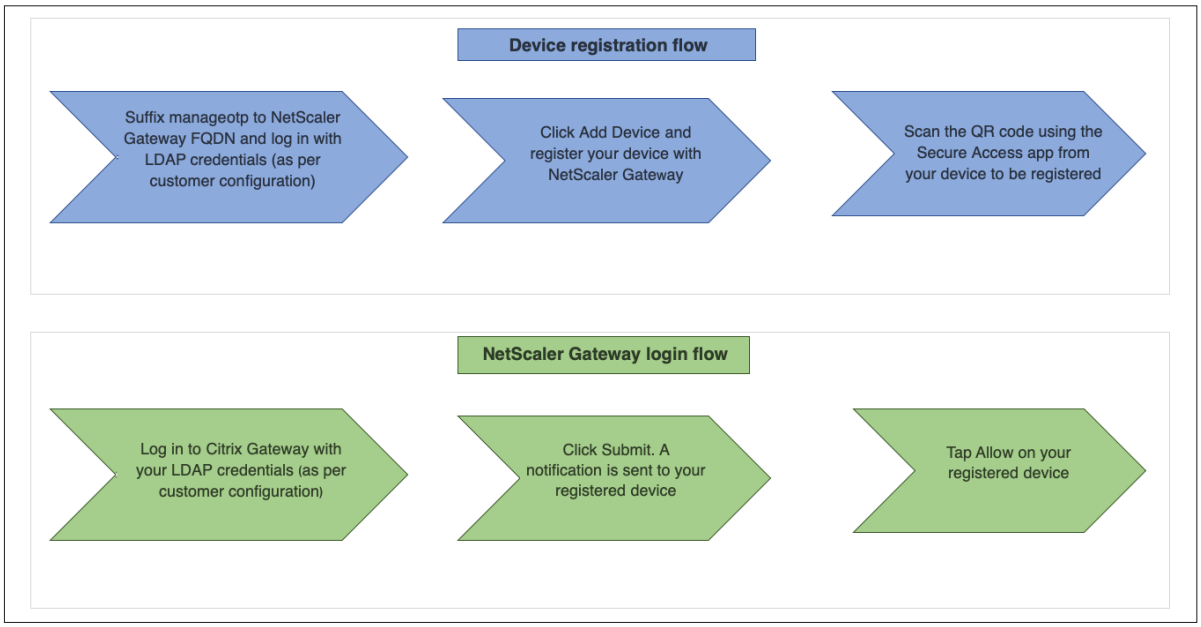
Avantages des notifications push

- Les notifications push fournissent un mécanisme d'authentification multifacteur plus sécurisé. L'authentification auprès de NetScaler Gateway échoue tant que l'utilisateur n'a pas approuvé la tentative de connexion.
- La notification Push est facile à administrer et à utiliser. Les utilisateurs doivent télécharger et installer l'application mobile Citrix SSO qui ne nécessite aucune assistance d'administrateur.
- Les utilisateurs n'ont pas besoin de copier ou de mémoriser le code. Ils doivent simplement appuyer sur l'appareil pour s'authentifier.
- Les utilisateurs peuvent enregistrer plusieurs appareils.

Fonctionnement des notifications push

Le flux de travail de notification push peut être classé en deux catégories :

- Enregistrement de l'appareil
- Connexion de l'utilisateur final



Conditions préalables à l'utilisation de la notification push

- Terminez le processus d'intégration de Citrix Cloud.
  1. Créez un compte d'entreprise Citrix Cloud ou rejoignez un compte existant. Pour des procédures détaillées et des instructions sur la marche à suivre, consultez la section Inscription à Citrix Cloud.
  2. Connectez-vous https://citrix.cloud.comà et sélectionnez le client.
  3. Dans Menu, sélectionnez **Identity and Access Management**, puis accédez à l'onglet **API Access** pour créer un client pour le compte.
  4. Copiez l'ID, le secret et l'ID client. L'ID et le secret sont nécessaires pour configurer le service push dans NetScaler en tant que « ClientID » et « ClientSecret » respectivement.

> **Important :**
>
> - Les mêmes informations d'identification d'API peuvent être utilisées sur plusieurs centres de données.
> - Les appliances NetScaler locales doivent être capables de résoudre les adresses de serveur mfa.cloud.com et trust.citrixworkspacesapi.net et être accessibles depuis l'appliance. Cela permet de s'assurer qu'il n'y a pas de pare-feu ou de blocage d'adresse IP pour ces serveurs sur le port 443.

- Téléchargez l'application mobile Citrix SSO sur l'App Store et le Play Store pour les appareils iOS et Android respectivement. La notification push est prise en charge sur iOS à partir de la version 1.1.13 sur Android à partir de la version 2.3.5.

- Vérifiez les points suivants pour Active Directory.
  - La longueur minimale des attributs doit être d'au moins 256 caractères.
  - Le type d'attribut doit être « DirectoryString », par exemple UserParameters. Ces attributs peuvent contenir des valeurs de chaîne.
  - Le type de chaîne d'attribut doit être Unicode, si le nom de l'appareil est en caractères non anglais.
  - L'administrateur LDAP de NetScaler doit disposer d'un accès en écriture à l'attribut AD sélectionné.
  - NetScaler et la machine cliente doivent être synchronisés avec un serveur Network Time commun.

Configuration des notifications Push

Voici les étapes de haut niveau qui doivent être effectuées pour utiliser la fonctionnalité de notification push.

- L'administrateur de NetScaler Gateway doit configurer l'interface pour gérer et valider les utilisateurs.
  1. Configurez un service Push.
  2. Configurez NetScaler Gateway pour la gestion des OTP et la connexion des utilisateurs finaux.

     Les utilisateurs doivent enregistrer leurs appareils auprès de la passerelle pour se connecter à NetScaler Gateway.
  3. Enregistrez votre appareil auprès de NetScaler Gateway.
  4. Connectez-vous à NetScaler Gateway.

Créer un service Push

1. Accédez à **Sécurité** > **Trafic des applications AAA** > **Stratégies** > **Authentification** > **Stratégies avancées** > **Actions** > **Service push**, puis cliquez sur **Ajouter**.
2. Dans la zone **Nom**, saisissez le nom du service Push.
3. Dans **Client ID**, entrez l'identité unique de la partie de confiance pour communiquer avec le serveur NetScaler Push dans le cloud.
4. Dans **Client Secret**, entrez le secret unique de la partie qui se fie pour communiquer avec le serveur NetScaler Push dans le cloud.
5. Dans **ID client**, entrez l'ID client ou le nom du compte dans le cloud qui est utilisé pour créer la paire ID client et secret client.

> **Important**
>
> La version TLS 1.2 est requise pour le service push. Pour plus d'informations, reportez-vous à la section Détails de configuration TLS 1.2.

Configurer NetScaler Gateway pour la gestion des OTP et la connexion des utilisateurs finaux

Suivez les étapes suivantes pour la gestion OTP et la connexion de l'utilisateur final.

- Créer un schéma de connexion pour la gestion OTP
- Configuration du serveur virtuel d'authentification, d'autorisation et d'audit
- Configuration de serveurs virtuels VPN ou d'équilibrage de charge
- Configuration de l'étiquette de stratégie
- Créer un schéma de connexion pour la connexion de l'utilisateur final

Pour plus de détails sur la configuration, voir Prise en charge OTP native.

Important : Pour les notifications push, les administrateurs doivent configurer explicitement les éléments suivants :

- Créez un service Push.
- Lors de la création d'un schéma de connexion pour la gestion OTP, sélectionnez le schéma de connexion SingleAuthManageOTP.xml ou équivalent selon vos besoins.
- Lors de la création d'un schéma de connexion pour la connexion de l'utilisateur final, sélectionnez le schéma de connexion DualAuthOrPush.xml ou équivalent selon les besoins.

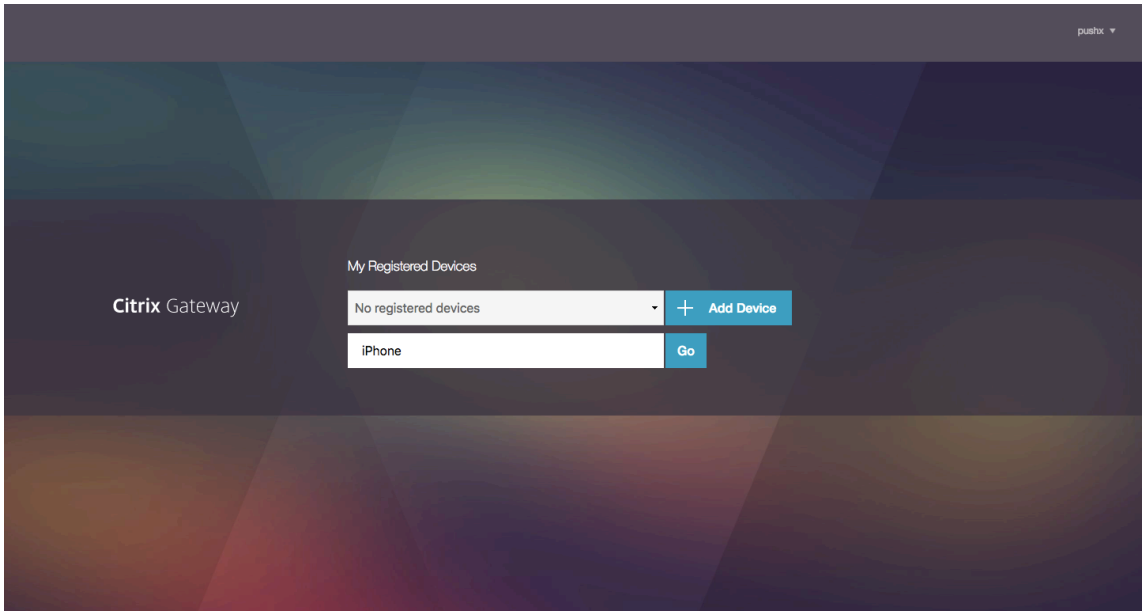
Enregistrez votre appareil auprès de NetScaler Gateway

Les utilisateurs doivent enregistrer leurs appareils auprès de NetScaler Gateway pour utiliser la fonctionnalité de notification push.

1. Dans votre navigateur Web, accédez à votre nom de domaine complet NetScaler Gateway et ajoutez-y le suffixe **/manageotp** .

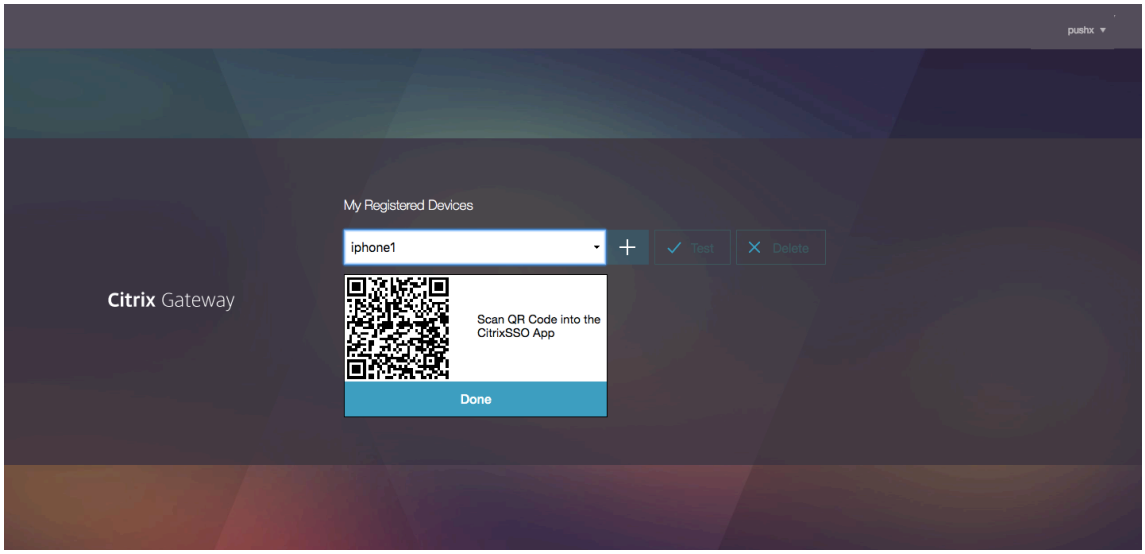
   La page d'authentification est chargée.
   Exemple : https://gateway.company.com/manageotp

2. Connectez-vous à l'aide de vos informations d'identification LDAP ou des mécanismes d'authentification à deux facteurs appropriés, le cas échéant.



3. Cliquez sur **Ajouter appareil**.
4. Entrez un nom pour votre appareil, puis cliquez sur **OK**.

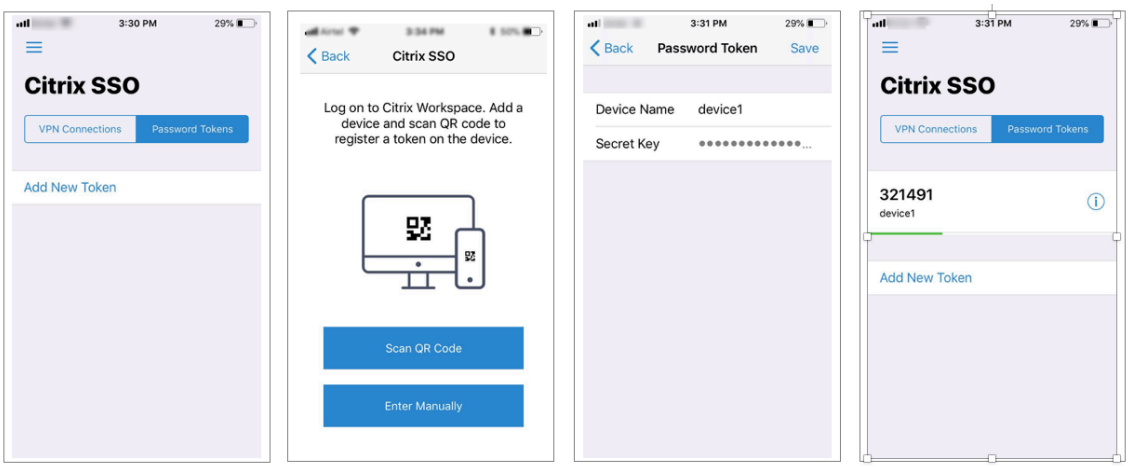
   Un code QR s'affiche sur la page du navigateur NetScaler Gateway.



5. Scannez ce code QR à l'aide de l'application Citrix SSO depuis l'appareil à enregistrer.

   Citrix SSO valide le code QR, puis s'enregistre auprès de la passerelle pour recevoir des notifications push. S'il n'y a pas d'erreur dans le processus d'inscription, le jeton est correctement ajouté à la page des jetons de mot de passe.

   > **Important :**
   >
   > La connexion échoue si vous entrez manuellement la clé secrète fournie dans le code QR.



6. S'il n'y a pas d'autres appareils à ajouter/gérer, déconnectez-vous à l'aide de la liste située dans le coin supérieur droit de la page.

Test de l'authentification par mot de passe unique

1. Pour tester l'OTP, cliquez sur votre appareil dans la liste, puis cliquez sur **Test**.
2. Saisissez le code OTP que vous avez reçu sur votre appareil, puis cliquez sur **OK**.

   Le message de vérification OTP réussi s'affiche.
3. Déconnectez-vous en utilisant la liste en haut à droite de la page.

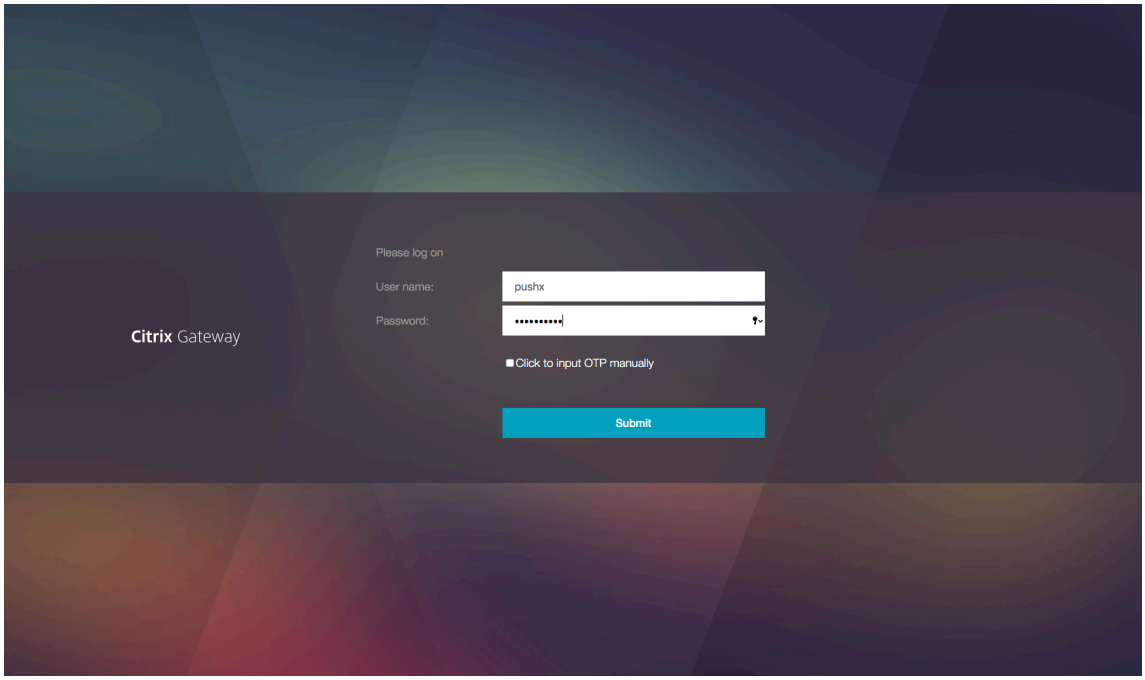
Remarque : Vous pouvez utiliser le portail de gestion OTP à tout moment pour tester l'authentification, supprimer des appareils enregistrés ou enregistrer d'autres appareils.

Connectez-vous à NetScaler Gateway

Après avoir enregistré leurs appareils auprès de NetScaler Gateway, les utilisateurs peuvent utiliser la fonctionnalité de notification push pour s'authentifier.

1. Accédez à votre page d'authentification NetScaler Gateway (par exemple :) https://gateway.company.com

   Vous êtes invité à entrer uniquement vos informations d'identification LDAP en fonction de la configuration du schéma de connexion.

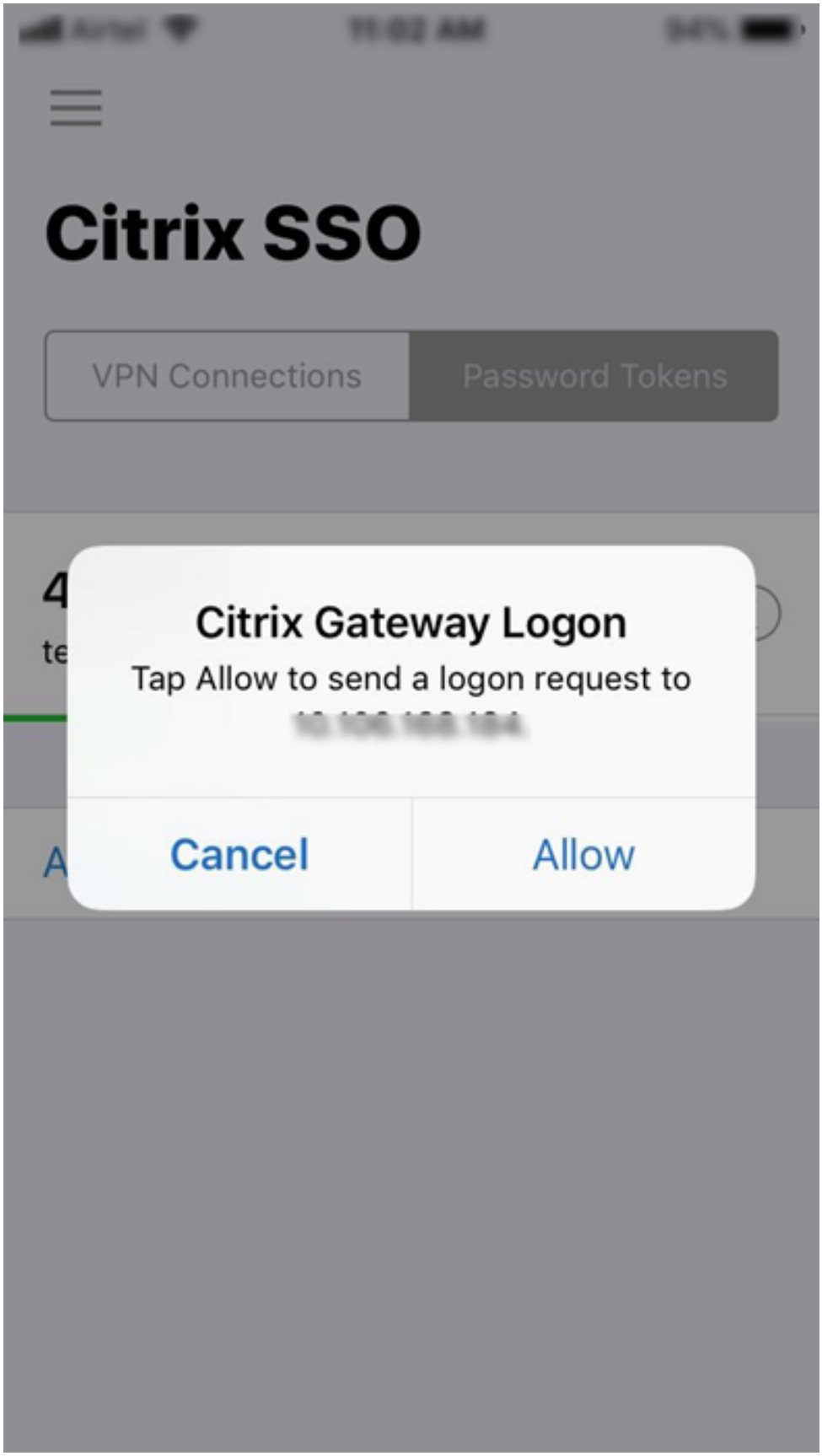


2. Saisissez votre nom d'utilisateur et votre mot de passe LDAP, puis sélectionnez **Soumettre**.

   Une notification est envoyée sur votre appareil enregistré.

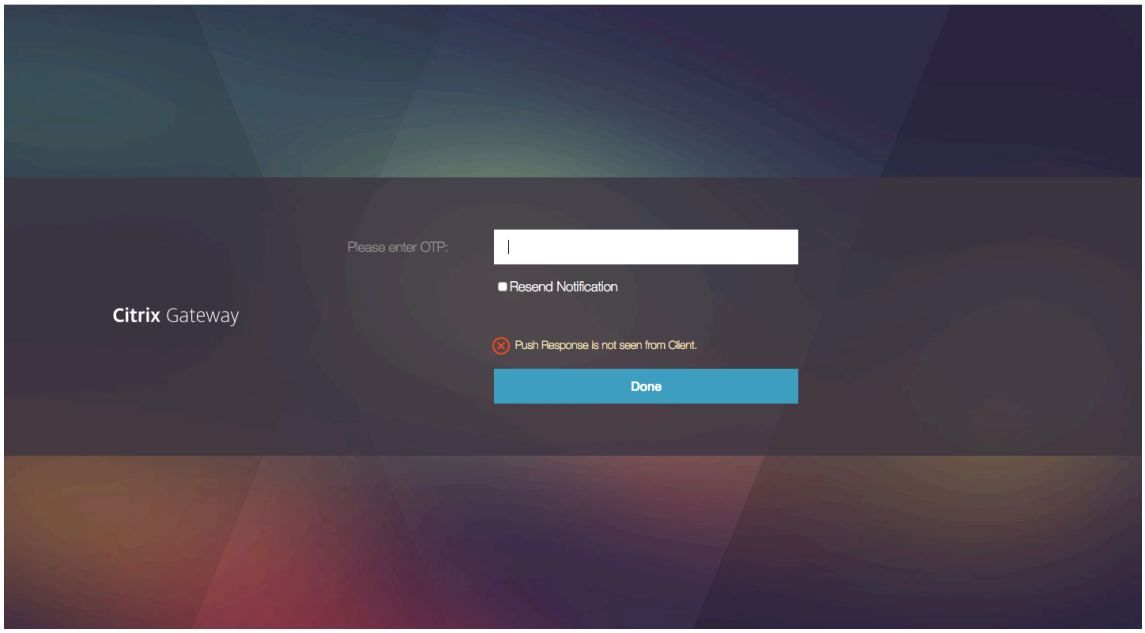
   Remarque : Si vous souhaitez entrer manuellement l'OTP, vous devez sélectionner **Cliquer** pour saisir manuellement le code OTP et entrer l'OTP dans le champ **TOTP** .

3. Ouvrez l'application Citrix SSO sur votre appareil enregistré et appuyez sur **Autoriser**.



Remarque :

- Sur un appareil iOS, vous êtes invité à saisir Touch-ID/Face-ID/Passcode comme facteur supplémentaire d'authentification.
- Le serveur d'authentification attend la réponse de notification du serveur push jusqu'à ce que le délai d'expiration configuré expire. Une fois le délai écoulé, NetScaler Gateway affiche la page de connexion. Les utilisateurs peuvent ensuite entrer l'OTP manuellement ou cliquer sur **Renvoyer la notification** pour recevoir à nouveau la notification sur l'appareil enregistré. En fonction de l'option que vous avez sélectionnée, la passerelle valide l'OTP que vous avez saisi ou renvoie la notification sur votre appareil enregistré.



- Aucune notification n'est envoyée à votre appareil enregistré concernant un échec de connexion.

Conditions de panne

- L'enregistrement de l'appareil peut échouer dans les cas suivants.
  - Le certificat de serveur n'est peut-être pas approuvé par la machine de l'utilisateur final.
  - NetScaler Gateway utilisé pour s'inscrire à OTP n'est pas accessible par le client.
- Les notifications peuvent échouer dans les cas suivants.
  - La machine utilisateur n'est pas connectée à Internet
  - Les notifications sur la machine utilisateur sont bloquées
  - L'utilisateur n'approuve pas la notification sur l'appareil

Dans ces cas, le serveur d'authentification attend l'expiration du délai d'expiration configuré. Une fois le délai écoulé, NetScaler Gateway affiche une page de connexion avec les options permettant de

saisir manuellement l'OTP ou de renvoyer la notification sur votre appareil enregistré. En fonction de l'option sélectionnée, une validation supplémentaire se produit.

Journaux d'échec

Les journaux suivants sont attendus lorsque le service Push OTP n'est pas accessible.

- Échec de la notification Push lorsque la machine utilisateur n'est pas connectée à Internet - Push : échec de la préparation de la demande Push à "`client name`" pour le service Push.
- Journal d'échec de l'enregistrement des appareils - Push : Aucun appareil n'est enregistré pour envoyer une demande Push au cloud pour "`client name`".
- Dans le cas où l'utilisateur n'accepte pas le push - Push : La réponse n'est pas vue du client, pour "`user name`", vérifier les options de nouvelles tentatives.

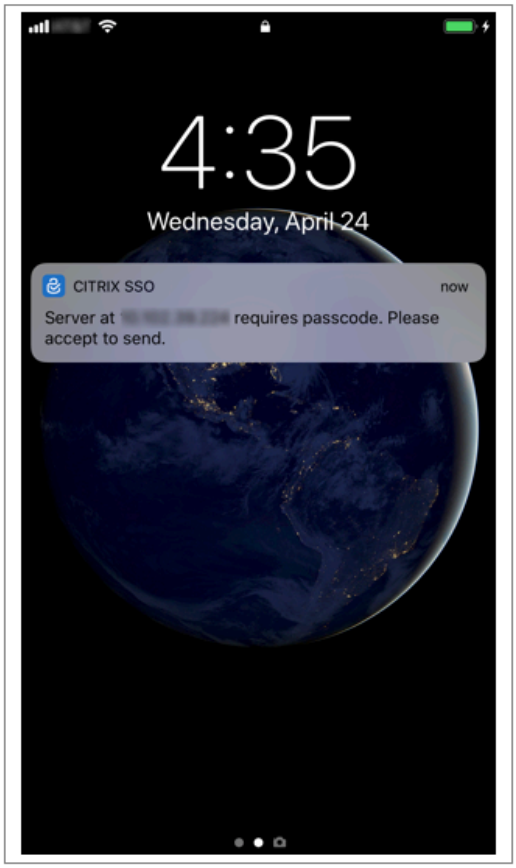
Comportement de l'application Citrix SSO sur iOS — points à noter

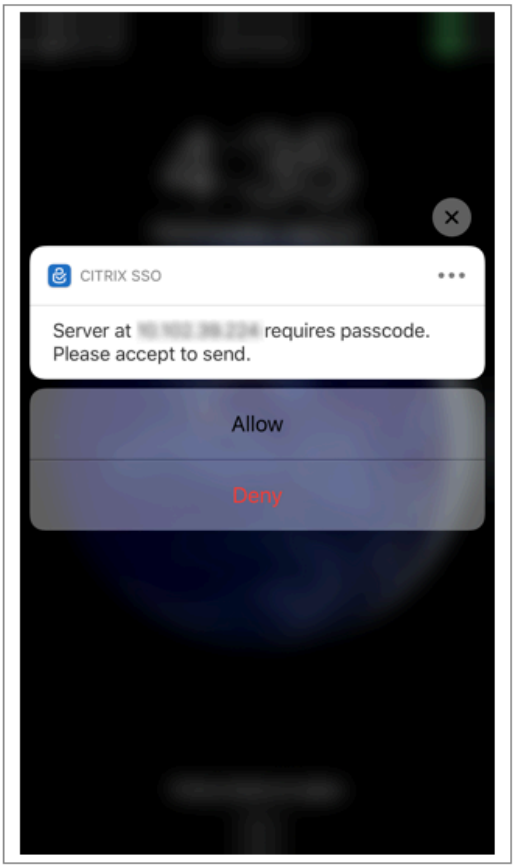
Raccourcis de notification

L'application Citrix SSO iOS inclut la prise en charge des notifications exploitables afin d'améliorer l'expérience utilisateur. Une fois qu'une notification est reçue sur un appareil iOS, et si l'appareil est verrouillé ou si l'application Citrix SSO n'est pas au premier plan, les utilisateurs peuvent utiliser les raccourcis intégrés à la notification pour approuver ou refuser la demande de connexion.

Pour accéder aux raccourcis de notification, les utilisateurs doivent soit forcer le toucher (3D touch), soit appuyer longuement sur la notification en fonction du matériel de l'appareil. La sélection de l'action de raccourci Autoriser envoie une demande de connexion à NetScaler. Selon la façon dont la stratégie d'authentification est configurée sur le serveur virtuel d'authentification, d'autorisation et d'audit ;

- La demande de connexion peut être envoyée en arrière-plan sans qu'il soit nécessaire de lancer l'application au premier plan ou de déverrouiller l'appareil.
- L'application peut demander un code Touch-ID/Face-ID/Passcode comme facteur supplémentaire, auquel cas l'application est lancée au premier plan.



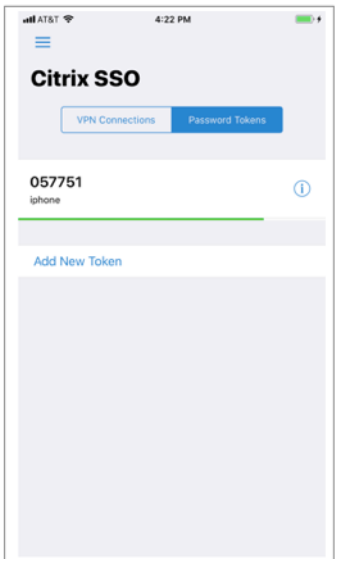


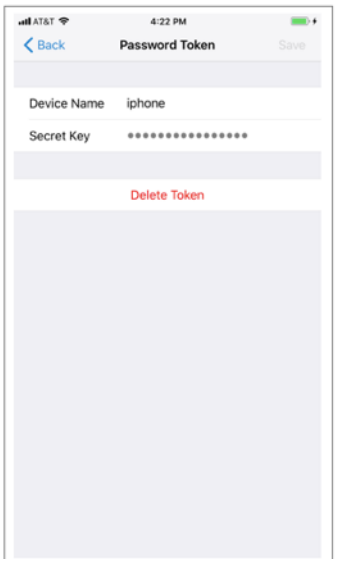
Suppression des jetons de mot de passe de Citrix SSO

1. Pour supprimer un jeton de mot de passe enregistré pour le push dans l'application Citrix SSO, les utilisateurs doivent effectuer les opérations suivantes :
2. Désenregistrez (supprimez) l'appareil iOS/Android sur la passerelle. Le code QR permettant de supprimer l'enregistrement de l'appareil apparaît.
3. Ouvrez l'application Citrix SSO et appuyez sur le bouton d'informations du jeton de mot de passe à supprimer.
4. Appuyez sur **Supprimer le jeton** et scannez le code QR.

Remarque :

- Si le code QR est valide, le jeton est correctement supprimé de l'application Citrix SSO.
- Les utilisateurs peuvent appuyer sur Forcer la suppression pour supprimer un jeton de mot de passe sans avoir à scanner le code QR si l'appareil est déjà supprimé de la passerelle. La suppression forcée peut faire en sorte que l'appareil continue de recevoir des notifications s'il n'a pas été supprimé de NetScaler Gateway.





Authentification OTP par e-mail

May 5, 2023

L'OTP de messagerie est introduit avec NetScaler 12.1 build 51.x. La méthode OTP par e-mail vous permet de vous authentifier à l'aide du mot de passe à usage unique (OTP) envoyé à l'adresse e-mail enregistrée. Lorsque vous essayez de vous authentifier sur n'importe quel service, le serveur envoie un OTP à l'adresse e-mail enregistrée de l'utilisateur.

Pour utiliser la fonctionnalité E-mail OTP, vous devez d'abord enregistrer votre autre adresse e-mail. Un autre enregistrement d'identifiant de messagerie est nécessaire pour que l'OTP puisse être envoyé à cet identifiant de messagerie, car vous ne pourrez pas accéder à l'adresse e-mail principale en cas de verrouillage du compte ou en cas d'oubli du mot de passe AD.

Vous pouvez utiliser la validation OTP d'e-mail sans enregistrement d'identifiant d'e-mail si vous avez déjà fourni l'autre ID d'e-mail dans le cadre d'un attribut AD. Vous pouvez faire référence au même attribut dans l'action e-mail au lieu de spécifier l'autre ID e-mail dans la section Adresse e-mail.

Composants requis

Avant de configurer la fonctionnalité OTP par e-mail, passez en revue les conditions préalables suivantes :

- Fonctionnalité NetScaler version 12.1 build 51.28 et versions ultérieures
- La fonctionnalité OTP des e-mails est disponible uniquement dans le flux d'authentification nFactor

- Pour plus de détails, reportez-vous à https://support.citrix.com/pages/citrix-adc-authentication-how#nfactor
- Compatible avec AAA-TM, NetScaler Gateway (navigateur, plug-in natif et récepteur).

Paramètre Active Directory

- La version prise en charge est le niveau de fonction du domaine Active Directory 2016/2012 et 2008
- Le nom d'utilisateur NetScaler LDAPbind doit disposer d'un accès en écriture au chemin AD de l'utilisateur

Serveur de messagerie

- Pour que la solution Email OTP fonctionne, assurez-vous que l'authentification basée sur la connexion est activée sur le serveur SMTP. NetScaler prend uniquement en charge l'authentification basée sur AUTH LOGIN pour que Email OTP fonctionne.
- Pour vous assurer que l'authentification basée sur AUTH LOGIN est activée, tapez la commande suivante sur le serveur SMTP. Si l'authentification basée sur la connexion est activée, vous remarquerez que le texte AUTH LOGIN apparaît en **gras** dans la sortie.

```
root@ns# telnet <IP address of the SMTP server><Port number of the server>
ehlo
root@ns# telnet 10.106.3.
Trying 10.106.
Connected to 10.106.
Escape character is '^]'.
220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22 Nov
2019 16:24:17 +0530
ehlo
250-E2K13.NSGSanity.com Hello [10.221.
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
For information on how to enable login based authentication, see
https://support.microfocus.com/kb/doc.php?id=7020367
```

Limitations

- Cette fonctionnalité n'est prise en charge que si le back-end d'authentification est LDAP.
- L'autre adresse e-mail déjà enregistrée est introuvable.

- Seul l'autre adresse e-mail de la page d'inscription KBA ne peut pas être mise à jour.
- L'authentification OTP par e-mail ne peut pas être le premier facteur du flux d'authentification. Ceci est conçu pour obtenir une authentification robuste.
- Si l'ID de messagerie alternatif et le KBA sont configurés à l'aide de la même action d'authentification, l'attribut doit être le même pour les deux.
- Pour le module externe natif et Receiver, l'enregistrement est pris en charge uniquement via un navigateur.

Configuration d'Active Directory

- L'OTP de messagerie utilise l'attribut Active Directory comme stockage des données utilisateur.
- Une fois que vous avez enregistré l'identifiant de messagerie secondaire, celui-ci est envoyé à l'appliance NetScaler et l'appliance le stocke dans l'attribut KB configuré de l'objet utilisateur AD.
- L'autre ID d'e-mail est crypté et stocké dans l'attribut AD configuré.

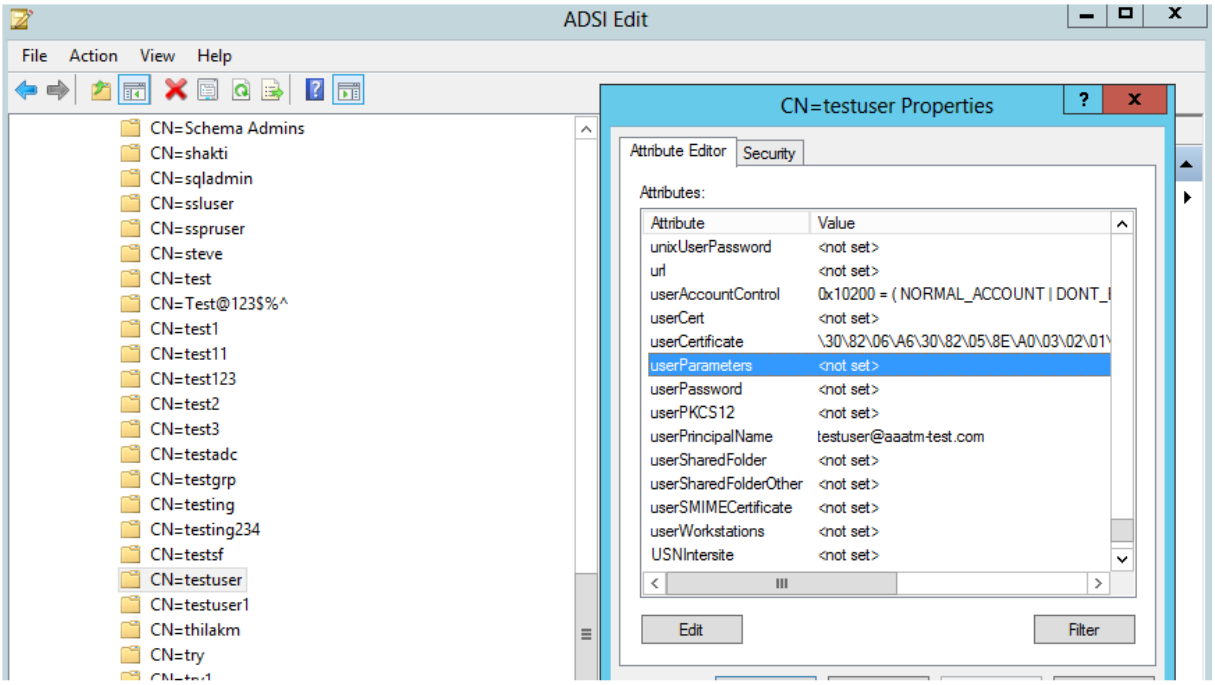
Lors de la configuration d'un attribut AD, prenez en compte les points suivants :

- La longueur du nom d'attribut prise en charge doit comporter au moins 128 caractères.
- Le type d'attribut doit être « DirectoryString ».
- Le même attribut AD peut être utilisé pour les données d'enregistrement OTP natives et OTP par e-mail.
- L'administrateur LDAP doit disposer d'un accès en écriture à l'attribut AD sélectionné.

Utilisation d'attributs existants

L'attribut utilisé dans cet exemple est `Userparameters`. Comme il s'agit d'un attribut existant au sein de l'utilisateur AD, vous n'avez pas besoin d'apporter de modifications à l'AD lui-même. Cependant, vous devez vous assurer que l'attribut n'est pas utilisé.

Pour vous assurer que l'attribut n'est pas utilisé, accédez à **ADSI** et sélectionnez l'utilisateur, cliquez avec le bouton droit de la souris sur l'utilisateur et faites défiler jusqu'à la liste des attributs. Vous devez voir la valeur d'attribut pour **UserParametersnon définie**. Cela indique que l'attribut n'est pas utilisé pour le moment.



Configurer l'OTP par e-mail

La solution OTP pour les e-mails comprend les deux parties suivantes :

- Inscription par e-mail
- Validation des e-mails

Enregistrement de l'adresse e-mail

Effectuez la configuration suivante à l'aide de l'interface de ligne de commande après la création réussie du schéma d'enregistrement KBA :

1. Liez le thème du portail et le certificat au VPN global.

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```

> **Remarque :**
>
> La liaison de certificat précédente est requise pour chiffrer les données utilisateur (Q&R de la base de connaissances et ID de messagerie secondaire enregistré) stockées dans l'attribut AD.

2. Créez une stratégie d'authentification LDAP.


```
add authentication ldapAction ldap -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL
add authentication Policy ldap -rule true -action ldap
<!--NeedCopy-->
```

3. Créez une stratégie d'authentification LDAP pour l'enregistrement des e-mails.

```
add authentication ldapAction ldap_email_registration -serverIP
    10.102.2.2 -serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -
    ldapBindDn administrator@aaatm-test.com -ldapBindDnPassword
    freebsd -ldapLoginName samAccountName -secType SSL -KBAttribute
     userParameters -alternateEmailAttr userParameters
add authentication Policy ldap_email_registration -rule true -
    action ldap_email_registration
<!--NeedCopy-->
```

4. Créez un schéma de connexion et une étiquette de stratégie pour l'enregistrement des e-mails.

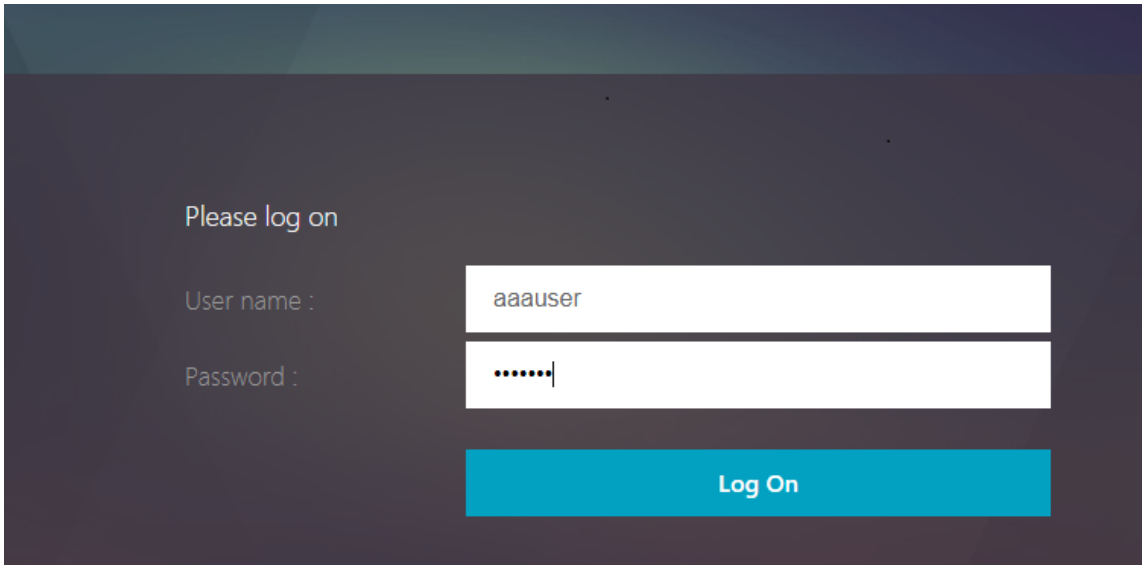
```
add authentication loginSchema onlyEmailRegistration -
    authenticationSchema /nsconfig/loginschema/LoginSchema/
    AltEmailRegister.xml
add authentication policylabel email_Registration_factor -
    loginSchema onlyEmailRegistration
bind authentication policylabel email_Registration_factor -
    policyName ldap_email_registration -priority 1 -
    gotoPriorityExpression NEXT
<!--NeedCopy-->
```

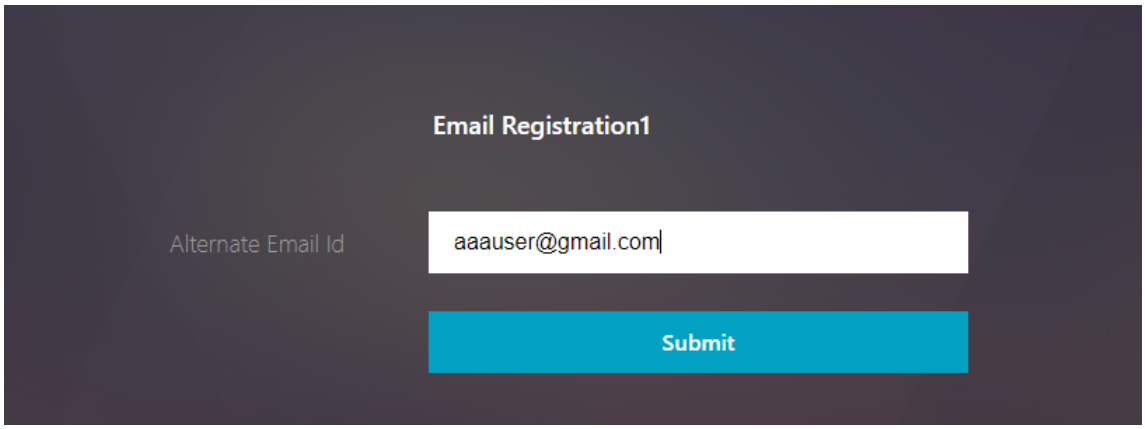
5. Liez la stratégie d'authentification au serveur virtuel d'authentification.

```
bind authentication vserver authvs  - policy ldap -priority 1 -
    nextFactor email_Registration_factor -gotoPriorityExpression
    NEXT
<!--NeedCopy-->
```

6. Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir l'écran graphique suivant. Lors de l'accès via l'URL, par exemple, https://lb1.server.com/ une page de connexion initiale qui nécessite uniquement les informations d'identification de connexion LDAP s'affiche, suivie d'une autre page d'inscription par e-mail.

   Remarque : Le domaine https://lb1.server.com/ peut appartenir à une passerelle ou à un serveur virtuel d'authentification.





> **Remarque :**
>
> - Vous pouvez utiliser le même schéma d'authentification pour l'enregistrement KBA et pour l'enregistrement de l'adresse e-mail.
> - Lors de la configuration de l'enregistrement KBA, vous pouvez sélectionner **Enregistrer une autre adresse e-mail** dans la section Enregistrement par e-mail pour enregistrer un autre identifiant d'e-mail.

Validation des e-mails

Procédez comme suit pour la validation des e-mails.

1. Liez le thème du portail et le certificat au VPN global

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```


> **Remarque :**
>
> La liaison de certificat précédente est requise pour déchiffrer les données utilisateur (Q&R de la base de connaissances et ID de messagerie secondaire enregistrés) stockées dans l'attribut AD.

2. Créez une stratégie d'authentification LDAP. LDAP doit être un facteur antérieur au facteur de validation de l'e-mail, car vous avez besoin de l'ID e-mail de l'utilisateur ou de l'autre ID e-mail pour la validation OTP de l'e-mail.

```
add authentication ldapAction ldap1 -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -   ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL -KBAttribute
    userParameters -alternateEmailAttr userParameters
add authentication Policy ldap1 -rule true -action ldap1
<!--NeedCopy-->
```

3. Créez une stratégie d'authentification des e-mails.

```
add authentication emailAction email -userName sqladmin@aaa.com -
    password freebsd-encrypted -encryptmethod ENCMTHD_3 -serverURL
    "smtps://10.2.3.3:25" -content "OTP is $code" -
    defaultAuthenticationGroup emailgrp -emailAddress "aaa.user.
    attribute("alternate_mail")"
add authentication Policy email -rule true  - action email
<!--NeedCopy-->
```

   Dans la commande mentionnée précédemment, l'**adresse e-mail** est l'autre ID e-mail fourni par l'utilisateur lors de l'enregistrement KBA.

4. Créez une étiquette de stratégie de validation OTP par e-mail.

```
add authentication policylabel email_Validation_factor
bind authentication policylabel email_Validation_factor -
    policyName email -priority 1 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

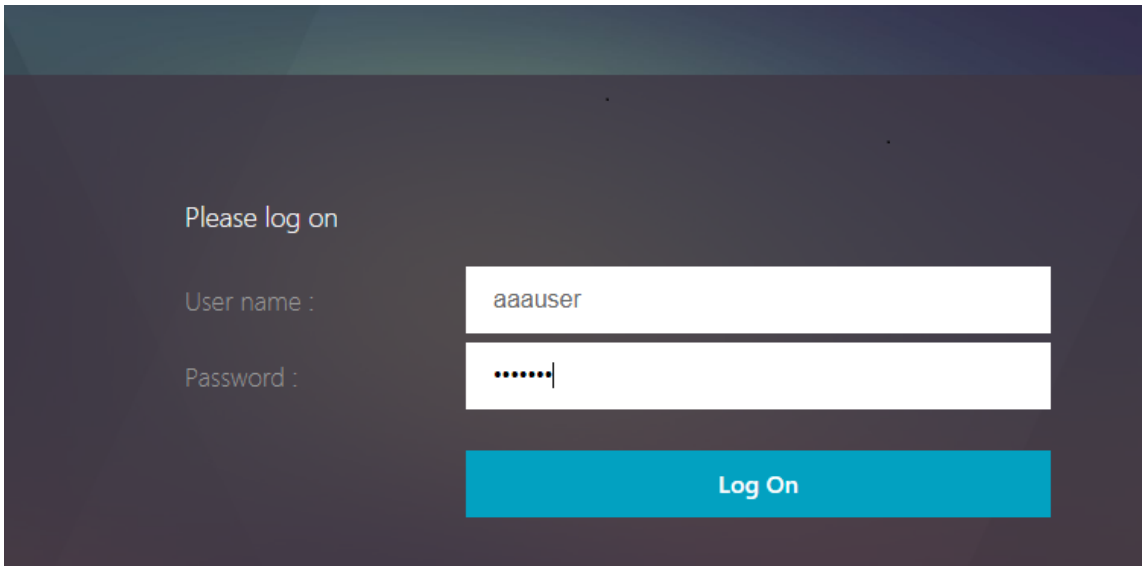
5. Liez la stratégie d'authentification au serveur virtuel d'authentification.

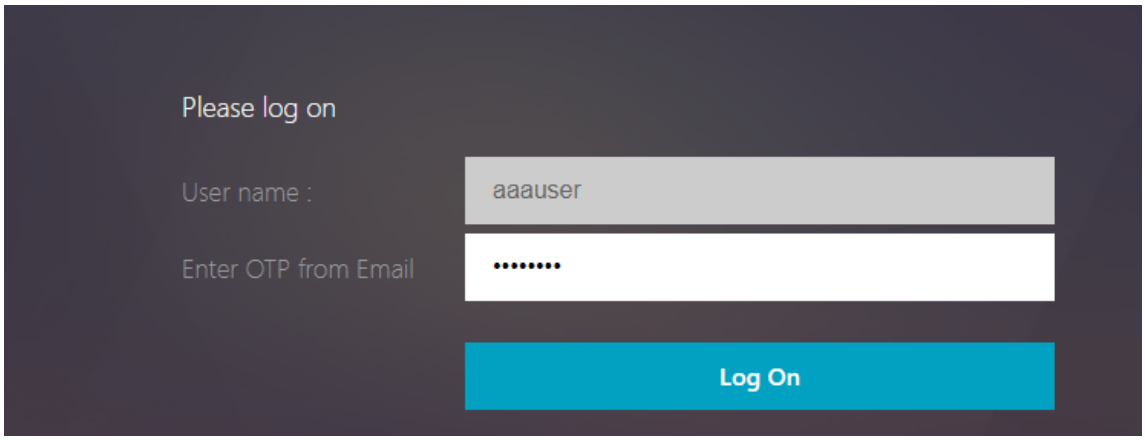
```
bind authentication vserver authvs  -  policy ldap1 -priority 1 -
    nextFactor email_Validation_factor -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

6. Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir l'écran graphique suivant pour la validation OTP par E-MAIL. Lors de l'accès via

l'URL, par exemple, https://lb1.server.com/ une page de connexion initiale qui nécessite uniquement les informations d'identification d'ouverture de session LDAP, suivie de la page de validation OTP d'EMAIL s'affiche.

> **Remarque :**
>
> Dans la stratégie LDAP, il est important de configurer `alternateEmailAttr` pour pouvoir interroger l'identifiant e-mail de l'utilisateur à partir de l'attribut AD.





Dépannage

Avant d'analyser le journal, il est préférable de définir le niveau de journalisation à déboguer comme suit.

```
set syslogparams -loglevel DEBUG
<!--NeedCopy-->
```


Inscription - Scénario réussi

Les entrées suivantes indiquent que l'enregistrement de l'utilisateur a réussi.

```
"ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1"
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  "
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw=="

<!--NeedCopy-->
```

Enregistrement - Scénario d'échec

Sur la page de connexion de l'utilisateur, le message d'erreur suivant s'affiche, « Impossible de terminer votre demande ». Cela indique que la clé de certification à lier au VPN global pour crypter les données utilisateur est manquante.

```
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:4 6 GMT
    0-PPE-1 : default SSLVPN Message 696 0 :  "Encrypt UserData: No
    Encryption cert is bound to vpn global"
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:46 GMT  0-
    PPE-1 : default SSLVPN Message 697 0 :  "KBA Register: Alternate
    email id Encrypted blob length is ZERO aaauser"
<!--NeedCopy-->
```

Validation des e-mails — Scénario réussi

Les entrées suivantes indiquent une validation OTP par e-mail réussie.

```
"NFactor: Successfully completed email auth, nextfactor is pwd_reset"
<!--NeedCopy-->
```

Validation des e-mails : scénario d'échec

Sur la page de connexion de l'utilisateur, le message d'erreur « Impossible de terminer votre demande » s'affiche. Cela indique que l'authentification basée sur la connexion n'est pas activée sur le serveur de messagerie et qu'elle doit être activée.

```
" /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp
    [100]: void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID:
    8]SMTP Configuration is Secure..
```



```
2 /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[108]:
    void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID: 8]
    First login succeeded
3 Wed Mar  4 17:16:28 2020
4 /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/naaad.c[697]: main
    0-0: timer 2 firing...
5 /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[127]:
    void ThreadWorker_SendMailJob(SMTPJob*) 0-0: [POCO-ERROR][JobID: 8]
    Poco SMTP Mail Dispatch  Failed. SMTP TYPE:1, SMTPException:
    Exception occurs. SMTP Exception: The mail service does not support
    LOGIN authentication: 250-smtprelay.citrix.com Hello [10.9.154.239]
6 250-SIZE 62914560
7 250-PIPELINING
8 250-DSN
9 250-ENHANCEDSTATUSCODES
10 250-8BITMIME
11 250-BINARYMIME
12 250 CHUNKING
13 <!--NeedCopy-->
```

Configuration Re-captcha pour l'authentification NFactor

May 5, 2023

NetScaler Gateway prend en charge une nouvelle action de premier ordre `captchaAction` qui simplifie la configuration du re-CAPTCHA. Le re-captcha étant une action de première classe, il peut être un facteur à part entière. Vous pouvez injecter Re-captcha n'importe où dans le flux nFactor.

Auparavant, vous deviez également écrire des stratégies WebAuth personnalisées avec des modifications apportées à l'interface RFWebUI. Avec l'introduction de `captchaAction`, vous n'avez pas à modifier le code JavaScript.

> **Important :**
>
> Si Re-captcha est utilisé avec les champs de nom d'utilisateur ou de mot de passe dans le schéma, le bouton **Soumettre** est désactivé jusqu'à ce que le re-captcha soit atteint.

Configuration du re-captcha

La configuration du re-captcha comporte deux parties.

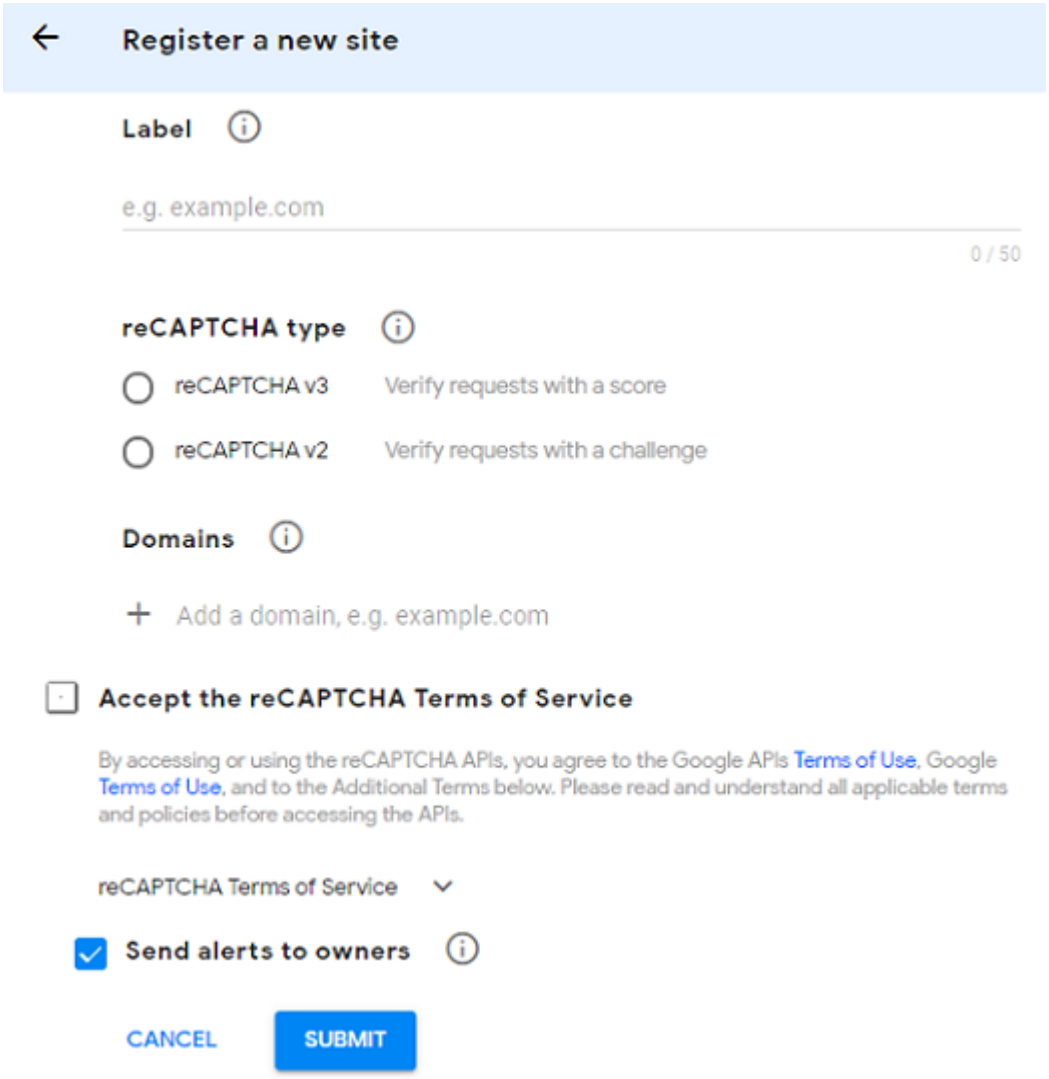
1. Configuration sur Google pour l'enregistrement de re-CAPTCHA.

2. Configuration sur l'appliance NetScaler pour utiliser re-Captcha dans le cadre du flux de connexion.

Configuration du re-captcha sur Google

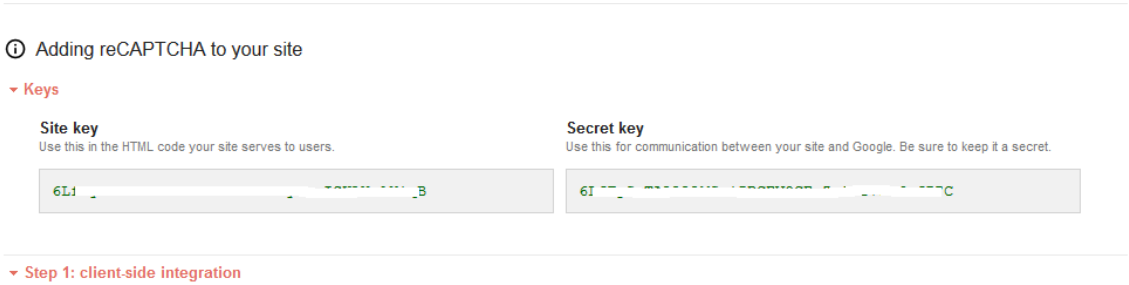
Enregistrez un domaine pour re-CAPTCHA sur https://www.google.com/recaptcha/admin#llist.

1. Lorsque vous accédez à cette page, l'écran suivant apparaît.



> **Remarque**
>
> Utilisez uniquement reCAPTCHA v2. Le re-captcha invisible est toujours en prévisualisation.

2. Une fois qu'un domaine est enregistré, la « SiteKey » et la « SecretKey » sont affichées.



> **Remarque**
>
> La « SiteKey » et la « SecretKey » sont grisées pour des raisons de sécurité. « SecretKey » doit être conservé en lieu sûr.

Configuration Re-Captcha sur une appliance NetScaler

La configuration Re-Captcha sur l'appliance NetScaler peut être divisée en trois parties :

- Afficher l'écran de re-captcha
- Publier la réponse Re-CAPTCHA sur le serveur Google
- La configuration LDAP est le deuxième facteur d'ouverture de session utilisateur (facultatif)

Afficher l'écran de re-captcha

La personnalisation du formulaire de connexion s'effectue via le schéma de connexion SingleAuthCaptcha.xml. Cette personnalisation est spécifiée au niveau du serveur virtuel d'authentification et est envoyée à l'interface utilisateur pour afficher le formulaire de connexion. Le schéma de connexion intégré, SingleAuthCaptcha.xml, se trouve dans le `/nsconfig/loginSchema/LoginSchema` répertoire de l'appliance NetScaler.

> **Important**
>
> - Le schéma de connexion SingleAuthCaptcha.xml peut être utilisé lorsque LDAP est configuré comme premier facteur.
> - En fonction de votre cas d'utilisation et de différents schémas, vous pouvez modifier le schéma existant. Par exemple, si vous n'avez besoin que du facteur Re-captcha (sans nom d'utilisateur ni mot de passe) ou d'une double authentification avec Re-Captcha.
> - Si des modifications personnalisées sont effectuées ou si le fichier est renommé, Citrix recommande de copier tous les loginSchemas du répertoire `/nsconfig/loginschema/LoginSchema` vers le répertoire parent `/nsconfig/loginschema`.

Pour configurer l'affichage de re-captcha à l'aide de la CLI

```
1 add authentication loginSchema singleauthcaptcha -authenticationSchema
    /nsconfig/loginschema/SingleAuthCaptcha.xml
```



```
2
3 add authentication loginSchemaPolicy singleauthcaptcha -rule true -
     action singleauthcaptcha
4
5 add authentication vserver auth SSL <IP> <Port>
6
7 add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-
     key-file>
8
9 bind ssl vserver auth -certkey vserver-cert
10
11 bind authentication vserver auth -policy singleauthcaptcha -priority 5
     -gotoPriorityExpression END
12 <!--NeedCopy-->
```

Publier la réponse Re-CAPTCHA sur le serveur Google

Après avoir configuré le re-captcha qui doit être affiché aux utilisateurs, les administrateurs ajoutent la configuration au serveur Google pour vérifier la réponse de re-captcha du navigateur.

Pour vérifier la réponse de re-captcha depuis le navigateur

```
1 add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-
     from-google> -secretkey <secretkey-from-google>
2
3 add authentication policy myrecaptcha -rule true -action myrecaptcha
4
5 bind authentication vserver auth -policy myrecaptcha -priority 1
6 <!--NeedCopy-->
```

Les commandes suivantes sont nécessaires pour configurer si l'authentification AD est souhaitée. Sinon, vous pouvez ignorer cette étape.

```
1 add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
     636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm
     .com -ldapBindDnPassword <password> -encrypted -encryptmethod
     ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -
     subAttributeName CN -secType SSL -passwdChange ENABLED -
     defaultAuthenticationGroup ldapGroup
2
3 add authenticationpolicy ldap-new -rule true -action ldap-new
4 <!--NeedCopy-->
```


La configuration LDAP est le deuxième facteur d'ouverture de session utilisateur (facultatif)

L'authentification LDAP se produit après re-captcha, vous l'ajoutez au second facteur.

```
add authentication policylabel second-factor

bind authentication policylabel second-factor -policy ldap-new -
    priority 10

bind authentication vserver auth -policy myrecaptcha -priority 1 -
    nextFactor second-factor
<!--NeedCopy-->
```

L'administrateur doit ajouter des serveurs virtuels appropriés selon que le serveur virtuel d'équilibrage de charge ou l'appliance NetScaler Gateway est utilisé pour l'accès. L'administrateur doit configurer la commande suivante si un serveur virtuel d'équilibrage de charge est requis :

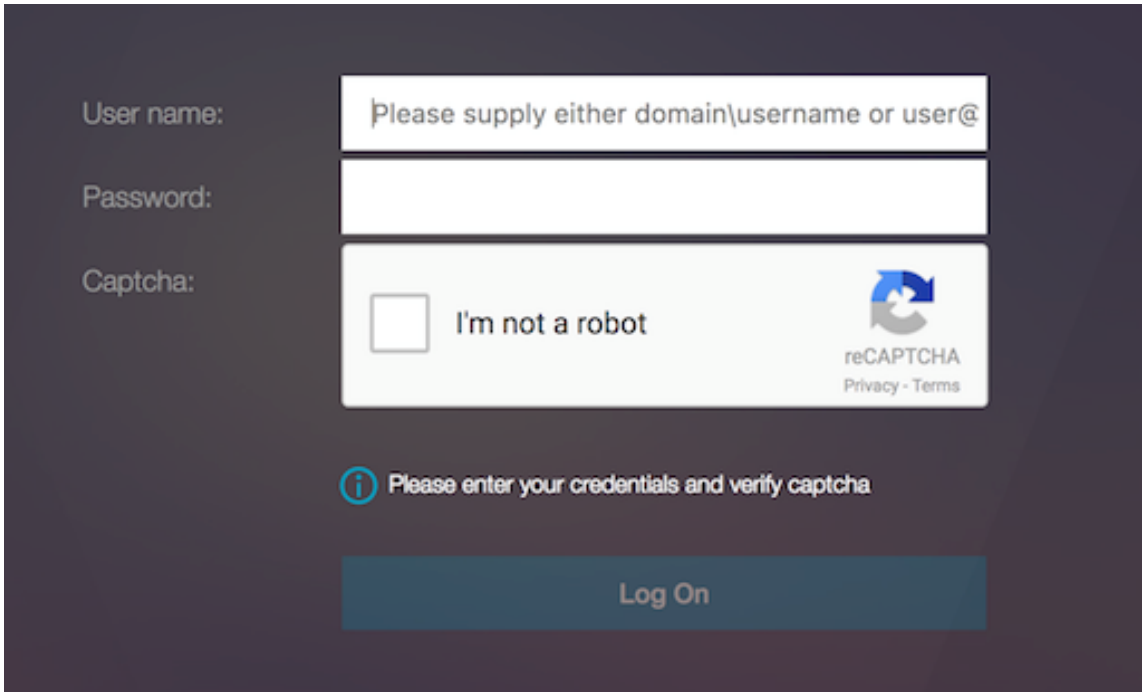
```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
    authenticationHost nssp.aaatm.com
<!--NeedCopy-->
```

nssp.aaatm.com — Résolution en serveur virtuel d'authentification.

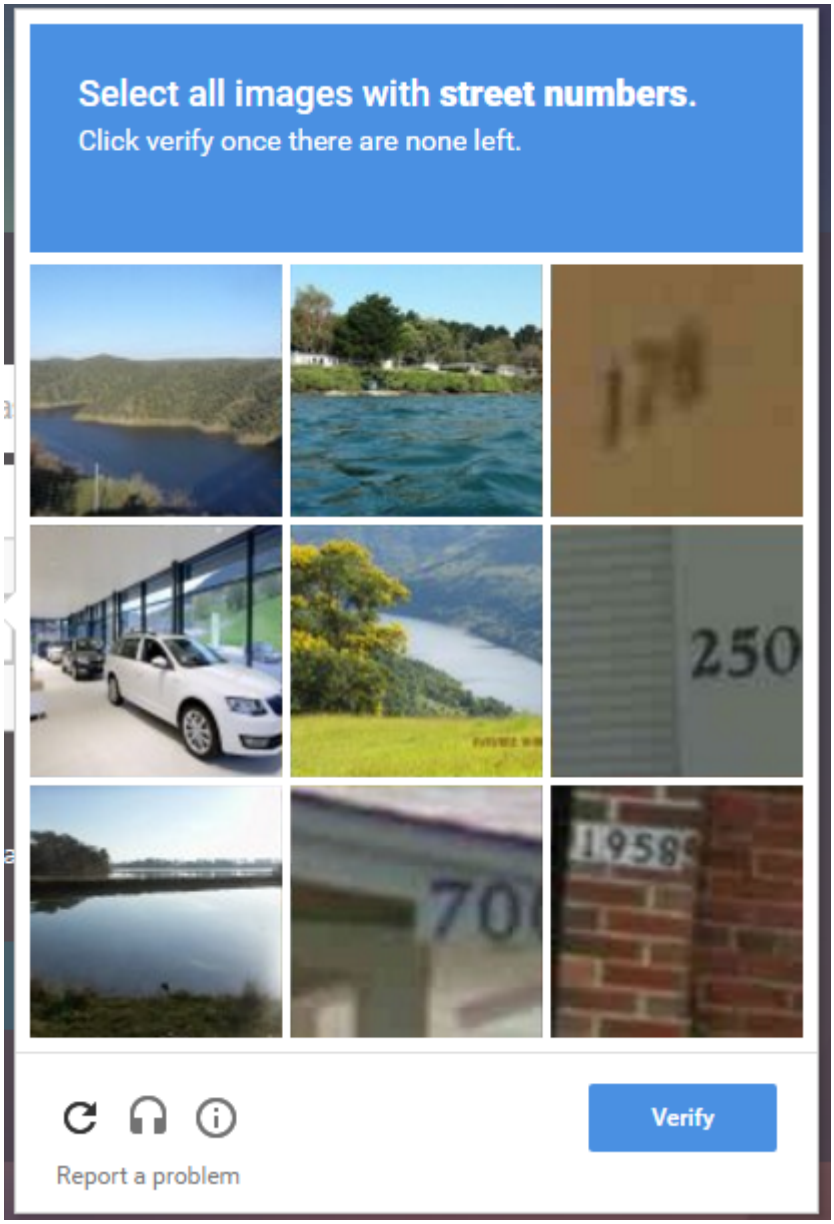
Validation utilisateur de re-CAPTCHA

Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir l'interface utilisateur suivante.

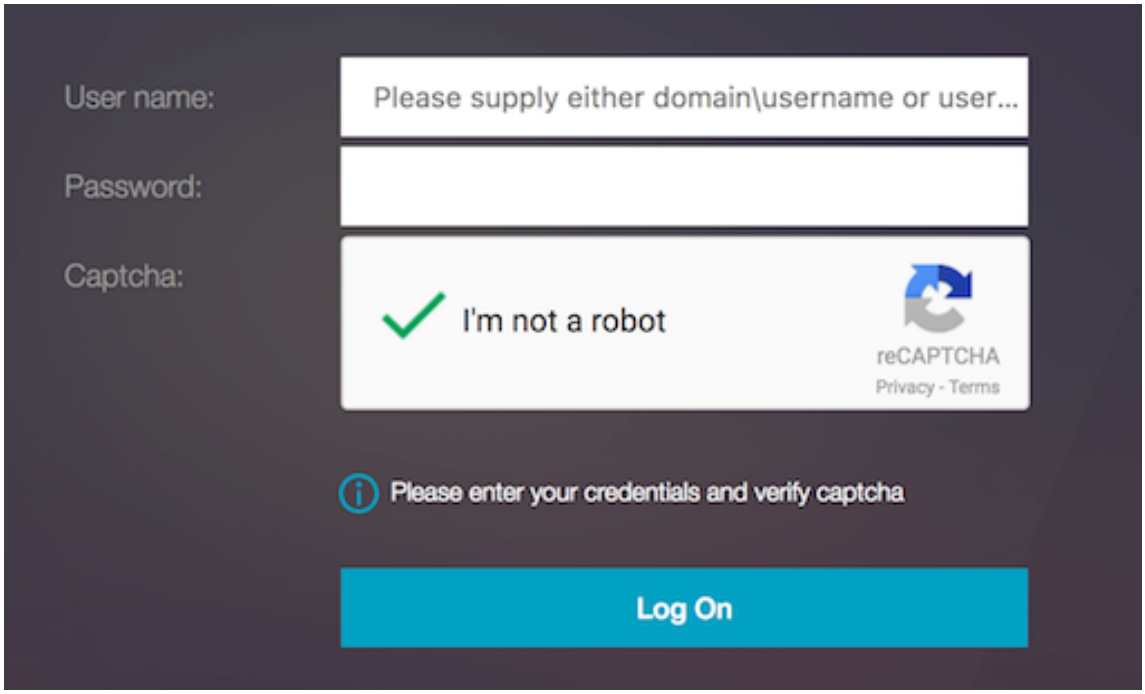
1. Une fois que le serveur virtuel d'authentification charge la page de connexion, l'écran de connexion s'affiche. La **connexion** est désactivée tant que le re-captcha n'est pas terminé.



2. Sélectionnez l'option Je ne suis pas un robot. Le widget Re-captcha s'affiche.



3. Vous parcourez une série d'images re-captcha, avant que la page de fin ne s'affiche.
4. Entrez les informations d'identification AD, activez la case à cocher **Je ne suis pas un robot** et cliquez **sur Ouvrir une session**. Si l'authentification réussit, vous êtes redirigé vers la ressource souhaitée.



Remarques :

- Si Re-captcha est utilisé avec l'authentification AD, le bouton **Envoyer** pour les informations d'identification est désactivé jusqu'à ce que le re-captcha soit terminé.
- Le re-captcha se produit dans un facteur qui lui est propre. Par conséquent, toutes les validations ultérieures telles que AD doivent avoir lieu dans le `nextfactor` du Re-CAPTCHA.

Configuration de l'authentification, de l'autorisation et de l'audit pour les protocoles couramment utilisés

May 5, 2023

La configuration de l'appliance NetScaler pour l'authentification, l'autorisation et l'audit nécessite une configuration spécifique sur l'appliance NetScaler et les navigateurs des clients. La configuration varie selon le protocole utilisé pour l'authentification, l'autorisation et l'audit.

Pour plus d'informations sur la configuration de l'appliance NetScaler pour l'authentification Kerberos, consultez la section Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM.

Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM

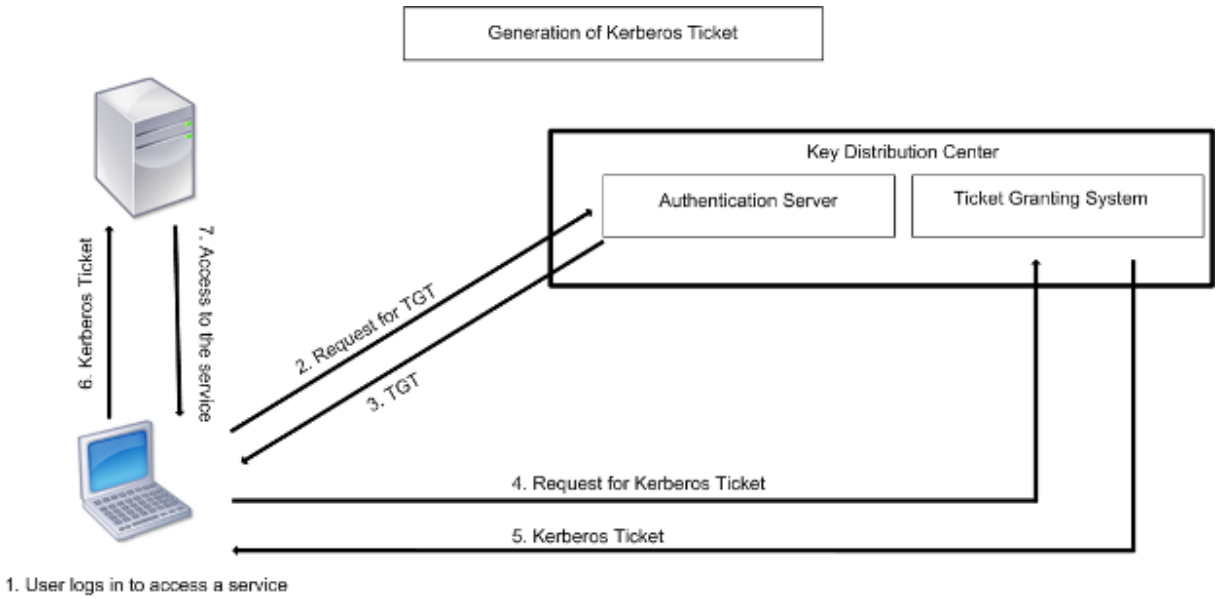
May 5, 2023

Kerberos, un protocole d'authentification de réseau informatique, fournit des communications sécurisées sur Internet. Conçu principalement pour les applications client-serveur, il fournit une authentification mutuelle grâce à laquelle le client et le serveur peuvent chacun garantir l'authenticité de l'autre. Kerberos fait appel à un tiers de confiance, appelé Key Distribution Center (KDC). Un KDC se compose d'un serveur d'authentification (AS), qui authentifie un utilisateur, et d'un serveur d'octroi de tickets (TGS).

Chaque entité du réseau (client ou serveur) possède une clé secrète qui n'est connue que d'elle-même et du KDC. La connaissance de cette clé implique l'authenticité de l'entité. Pour la communication entre deux entités du réseau, le KDC génère une clé de session, appelée ticket Kerberos ou ticket de service. Le client demande à l'AS des informations d'identification pour un serveur spécifique. Le client reçoit ensuite un ticket, appelé ticket d'octroi de tickets (TGT). Le client contacte ensuite le TGS, en utilisant le TGT qu'il a reçu de l'AS pour prouver son identité, et demande un service. Si le client est éligible au service, le TGS lui délivre un ticket Kerberos. Le client contacte ensuite le serveur hébergeant le service (appelé serveur de service) en utilisant le ticket Kerberos pour prouver qu'il est autorisé à recevoir le service. Le ticket Kerberos a une durée de vie configurable. Le client ne s'authentifie auprès de l'AS qu'une seule fois. S'il contacte le serveur physique à plusieurs reprises, il réutilise le ticket AS.

La figure suivante montre le fonctionnement de base du protocole Kerberos.

Figure 1. **Fonctionnement de Kerberos**



L'authentification Kerberos présente les avantages suivants :

- Authentification plus rapide. Lorsqu'un serveur physique reçoit un ticket Kerberos d'un client, le serveur dispose de suffisamment d'informations pour authentifier directement le client. Il n'est pas nécessaire de contacter un contrôleur de domaine pour l'authentification du client, ce qui accélère le processus d'authentification.
- Authentification mutuelle. Lorsque le KDC émet un ticket Kerberos à un client et que ce dernier utilise ce ticket pour accéder à un service, seuls les serveurs authentifiés peuvent déchiffrer le ticket Kerberos. Si le serveur virtuel de l'appliance NetScaler est capable de déchiffrer le ticket Kerberos, vous pouvez en conclure que le serveur virtuel et le client sont authentifiés. Ainsi, l'authentification du serveur se produit en même temps que l'authentification du client.
- Authentification unique entre Windows et les autres systèmes d'exploitation qui prennent en charge Kerberos.

L'authentification Kerberos peut présenter les inconvénients suivants :

- Kerberos impose des exigences temporelles strictes ; les horloges des hôtes concernés doivent être synchronisées avec l'horloge du serveur Kerberos pour garantir que l'authentification n'échoue pas. Vous pouvez atténuer cet inconvénient en utilisant les démons Network Time Protocol pour synchroniser les horloges des hôtes. Les tickets Kerberos ont une période de disponibilité que vous pouvez configurer.
- Kerberos a besoin que le serveur central soit disponible en permanence. Lorsque le serveur Kerberos est en panne, personne ne peut se connecter. Vous pouvez atténuer ce risque en utilisant plusieurs serveurs Kerberos et des mécanismes d'authentification de secours.
- Comme toutes les authentifications sont contrôlées par un KDC centralisé, toute compromission de cette infrastructure, telle que le vol du mot de passe d'un utilisateur pour un poste de travail local, peut permettre à un attaquant de se faire passer pour n'importe quel utilisateur. Vous pouvez atténuer ce risque dans une certaine mesure en utilisant uniquement un ordinateur de bureau ou un ordinateur portable auquel vous faites confiance, ou en appliquant la préauthentification au moyen d'un jeton matériel.

Pour utiliser l'authentification Kerberos, vous devez la configurer sur l'appliance NetScaler et sur chaque client.

Optimisation de l'authentification Kerberos en matière d'authentification, d'autorisation et d'audit

L'appliance NetScaler optimise et améliore désormais les performances du système lors de l'authentification Kerberos. Le démon d'authentification, d'autorisation et d'audit mémorise la requête Kerberos en attente pour le même utilisateur afin d'éviter de surcharger le Centre de distribution de clés (KDC), ce qui évitera les demandes dupliquées.

Comment NetScaler implémente Kerberos pour l'authentification des clients

May 5, 2023

> **Important**
>
> L'authentification Kerberos/NTLM n'est prise en charge que dans la version NetScaler 9.3 nCore ou ultérieure, et elle ne peut être utilisée que pour l'authentification, l'autorisation et l'audit des serveurs virtuels de gestion du trafic.

NetScaler gère les composants impliqués dans l'authentification Kerberos de la manière suivante :

Centre de distribution de clés (KDC)

Dans Windows 2000 Server ou versions ultérieures, le contrôleur de domaine et le KDC font partie de Windows Server. Si le Windows Server est opérationnel, cela indique que le contrôleur de domaine et le KDC sont configurés. Le KDC est également le serveur Active Directory.

> **Remarque**
>
> Toutes les interactions Kerberos sont validées avec le contrôleur de domaine Windows Kerberos.

Service d'authentification et négociation de protocoles

Une appliance NetScaler prend en charge l'authentification Kerberos sur les serveurs virtuels d'authentification, d'autorisation et d'audit de gestion du trafic. Si l'authentification Kerberos échoue, NetScaler utilise l'authentification NTLM.

Par défaut, Windows 2000 Server et les versions ultérieures de Windows Server utilisent Kerberos pour l'authentification, l'autorisation et l'audit. Si vous créez une politique d'authentification avec NEGOTIATE comme type d'authentification, NetScaler tente d'utiliser le protocole Kerberos pour l'authentification, l'autorisation et l'audit et si le navigateur du client ne reçoit pas de ticket Kerberos, NetScaler utilise l'authentification NTLM. Ce processus est appelé négociation.

Le client peut ne pas recevoir de ticket Kerberos dans les cas suivants :

- Kerberos n'est pas pris en charge sur le client.
- Kerberos n'est pas activé sur le client.
- Le client se trouve dans un domaine autre que celui du KDC.
- Le répertoire d'accès du KDC n'est pas accessible au client.

Pour l'authentification Kerberos/NTLM, NetScaler n'utilise pas les données présentes localement sur l'appliance NetScaler.

Authorization

Le serveur virtuel de gestion du trafic peut être un serveur virtuel d'équilibrage de charge ou un serveur virtuel de commutation de contenu.

Audit

L'appliance NetScaler prend en charge l'audit de l'authentification Kerberos grâce à la journalisation d'audit suivante :

- Piste d'audit complète de l'activité des utilisateurs finaux en matière de gestion du trafic
- SYSLOG et journalisation TCP à hautes performances
- Piste d'audit complète des administrateurs système
- Tous les événements du système
- Format de journal scriptable

Environnement pris en charge

L'authentification Kerberos ne nécessite aucun environnement spécifique sur NetScaler. Le client (navigateur) doit prendre en charge l'authentification Kerberos.

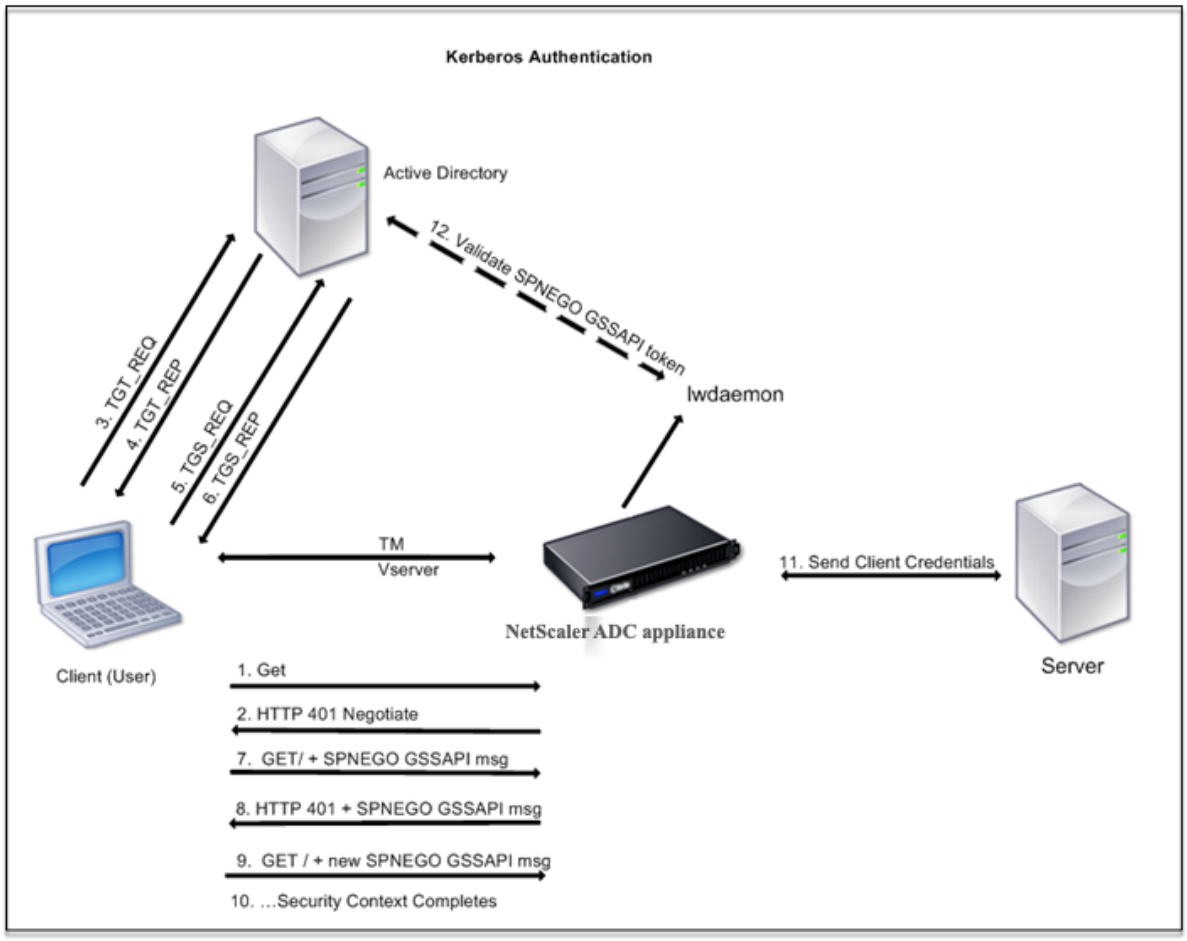
Haute disponibilité

Dans une configuration à haute disponibilité, seul le NetScaler actif rejoint le domaine. En cas de basculement, le démon NetScaler lwagent associe l'appliance NetScaler secondaire au domaine. Aucune configuration spécifique n'est requise pour cette fonctionnalité.

Processus d'authentification Kerberos

La figure suivante montre un processus typique d'authentification Kerberos dans l'environnement NetScaler.

Figure 1. Processus d'authentification Kerberos sur NetScaler



L'authentification Kerberos se déroule selon les étapes suivantes :

Le client s'authentifie auprès du KDC

1. L'appliance NetScaler reçoit une demande d'un client.
2. Le serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu) de l'appliance NetScaler envoie un défi au client.
3. Pour répondre à ce défi, le client reçoit un ticket Kerberos.
   - Le client envoie au serveur d'authentification du KDC une demande de ticket d'octroi de tickets (TGT) et reçoit le TGT. (Voir 3, 4 sur la figure, Processus d'authentification Kerberos.)
   - Le client envoie le TGT au serveur d'attribution de tickets du KDC et reçoit un ticket Kerberos. (Voir 5, 6 sur la figure, Processus d'authentification Kerberos.)

> **Remarque**
>
> Le processus d'authentification ci-dessus n'est pas nécessaire si le client possède déjà un ticket Kerberos dont la durée de vie n'a pas expiré. En outre, les clients tels que Web Services, .NET

> ou J2EE, qui prennent en charge SPNEGO, obtiennent un ticket Kerberos pour le serveur cible, créent un jeton SPNEGO et insèrent le jeton dans l'en-tête HTTP lorsqu'ils envoient une requête HTTP. Ils ne passent pas par le processus d'authentification du client.

Le client demande un service.

1. Le client envoie le ticket Kerberos contenant le jeton SPNEGO et la requête HTTP au serveur virtuel de gestion du trafic sur NetScaler. Le jeton SPNEGO contient les données GSSAPI nécessaires.
2. L'appliance NetScaler établit un contexte de sécurité entre le client et NetScaler. Si NetScaler ne peut pas accepter les données fournies dans le ticket Kerberos, le client est invité à obtenir un autre ticket. Ce cycle se répète jusqu'à ce que les données GSSAPI soient acceptables et que le contexte de sécurité soit établi. Le serveur virtuel de gestion du trafic sur NetScaler agit comme un proxy HTTP entre le client et le serveur physique.

L'appliance NetScaler termine l'authentification.

1. Une fois le contexte de sécurité terminé, le serveur virtuel de gestion du trafic valide le jeton SPNEGO.
2. À partir du jeton SPNEGO valide, le serveur virtuel extrait l'ID utilisateur et les informations d'identification GSS, puis les transmet au démon d'authentification.
3. Une authentification réussie termine l'authentification Kerberos.

Configuration de l'authentification Kerberos sur l'appliance NetScaler

May 9, 2023

Cette rubrique fournit les étapes détaillées pour configurer l'authentification Kerberos sur l'appliance NetScaler à l'aide de l'interface de ligne de commande et de l'interface graphique.

Configuration de l'authentification Kerberos sur la CLI

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit pour garantir l'authentification du trafic sur l'appliance.

   ns-cli-prompt> **enable ns feature** AAA

2. Ajoutez le fichier keytab à l'appliance NetScaler. Un fichier keytab est nécessaire pour déchiffrer le secret reçu du client lors de l'authentification Kerberos. Un seul fichier keytab contient les détails d'authentification de tous les services liés au serveur virtuel de gestion du trafic sur l'appliance NetScaler.

   Générez d'abord le fichier keytab sur le serveur Active Directory, puis transférez-le vers l'appliance NetScaler.

- Ouvrez une session sur le serveur Active Directory et ajoutez un utilisateur pour l'authentification Kerberos à l'aide de la commande suivante.

```
net user <username> <password> /add
```

> **Remarque**
>
> Dans la section **Propriétés de l'utilisateur**, assurez-vous que l'option « Modifier le mot de passe à la prochaine ouverture de session » n'est pas sélectionnée et que l'option « Le mot de passe n'expire pas » est sélectionnée.

- Mappez le service HTTP à l'utilisateur ci-dessus et exportez le fichier keytab. Par exemple, exécutez la commande suivante sur le serveur Active Directory :

```
ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM
   /pass <user password> /mapuser newacp\\dummy /ptype KRB5\
   _NT\_PRINCIPAL
```

> **Remarque**
>
> Vous pouvez mapper plusieurs services si l'authentification est requise pour plusieurs services. Si vous souhaitez mapper d'autres services, répétez la commande ci-dessus pour chaque service. Vous pouvez donner le même nom ou des noms différents au fichier de sortie.

- Transférez le fichier keytab vers l'appliance NetScaler à l'aide de la commande unix **ftp** ou de tout autre utilitaire de transfert de fichiers de votre choix. Téléchargez le fichier keytab dans le répertoire /nsconfig/krb/ de l'appliance NetScaler.

3. L'appliance NetScaler doit obtenir l'adresse IP du contrôleur de domaine à partir du nom de domaine complet (FQDN). Citrix recommande donc de configurer NetScaler avec un serveur DNS.

   ns-cli-prompt> **add dns nameserver** <ip-address>

   > **Remarque**
   >
   > Vous pouvez également ajouter des entrées d'hôte statiques ou utiliser tout autre moyen pour que l'appliance NetScaler puisse convertir le nom FQDN du contrôleur de domaine en adresse IP.

4. Configurez l'action d'authentification, puis associez-la à une stratégie d'authentification.

   - Configurez l'action de négociation.

     ns-cli-prompt> **add authentication negotiateAction** <name> -domain <domain name> -domainUser <domain user name> -domainUserPasswd <domain user password> -

defaultAuthenticationGroup <default authentication group> -keytab <string> -NTLMPath <string>

Remarque : Pour la configuration de l'utilisateur du domaine et du nom de domaine, accédez au client et utilisez la commande klist comme illustré dans l'exemple suivant :

Client: username @ AAA.LOCAL

Server: HTTP/onprem_idp.aaa.local @ AAA.LOCAL

add authentication negotiateAction <name> -domain -domainUser <HTTP/onprem_idp.aaa.local>

- Configurez la stratégie de négociation et associez l'action de négociation à cette stratégie.

  ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>

5. Créez un serveur virtuel d'authentification et associez-le à la stratégie de négociation.
   - Créez un serveur virtuel d'authentification.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>

   - Liez la stratégie de négociation au serveur virtuel d'authentification.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>

6. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu).

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

   > **Remarque**
   >
   > Des configurations similaires peuvent également être effectuées sur le serveur virtuel de commutation de contenu.

7. Vérifiez les configurations en procédant comme suit :
   - Accédez au serveur virtuel de gestion du trafic à l'aide du nom de domaine complet. Par exemple, Sample
   - Affichez les détails de la session sur l'interface de ligne de commande.

     ns-cli-prompt> **show aaa session**

Configuration de l'authentification Kerberos sur l'interface graphique

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit.

   Accédez à **Système** > **Paramètres**, cliquez sur **Configurer les fonctionnalités de base** et activez la fonctionnalité d'authentification, d'autorisation et d'audit.

2. Ajoutez le fichier keytab comme détaillé à l'étape 2 de la procédure CLI mentionnée ci-dessus.
3. Ajoutez un serveur DNS.

   Accédez à **Gestion du trafic > DNS > Serveurs de noms**et spécifiez l'adresse IP du serveur DNS.
4. Configurez l'action et la stratégie **Négocier** .

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégie**et créez une stratégie avec **Négocier** comme type d'action. Cliquez sur **AJOUTER** pour créer un nouveau serveur de négociation d'authentification ou sur **Modifier** pour configurer les détails existants.
5. Liez la stratégie de négociation au serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**et associez la stratégie de **négociation** au serveur virtuel d'authentification.
6. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu).

   Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et spécifiez les paramètres d'authentification appropriés.

   > **Remarque**
   >
   > Des configurations similaires peuvent également être effectuées sur le serveur virtuel de commutation de contenu.
7. Vérifiez les configurations décrites à l'étape 7 de la procédure CLI mentionnée ci-dessus.

Configuration de l'authentification Kerberos sur un client

May 5, 2023

La prise en charge de Kerberos doit être configurée sur le navigateur pour utiliser Kerberos pour l'authentification. Vous pouvez utiliser n'importe quel navigateur compatible Kerberos. Les instructions pour configurer la prise en charge de Kerberos sur Internet Explorer et Mozilla Firefox sont présentées ci-dessous. Pour les autres navigateurs, consultez la documentation du navigateur.

Pour configurer l'authentification Internet Explorer pour Kerberos

1. Dans le menu **Outils**, sélectionnez **Options Internet**.
2. Dans l'onglet **Sécurité**, cliquez sur **Intranet local**, puis sur **Sites**.
3. **Dans la boîte de dialogue**Intranet local**, assurez-vous que l'option Détecter automatiquement le réseau intranet est sélectionnée, puis cliquez sur Avancé.**

4. Dans la boîte de dialogue **Intranet local**, ajoutez les sites Web des domaines du serveur virtuel de gestion du trafic sur l'appliance NetScaler. Les sites spécifiés deviennent des sites intranet locaux.
5. Cliquez sur **Fermer** ou sur **OK** pour fermer les boîtes de dialogue.

Pour configurer l'authentification Mozilla Firefox pour Kerberos

1. Assurez-vous que Kerberos est correctement configuré sur votre ordinateur.
2. Tapez about:config dans la barre d'URL.
3. Dans la zone de texte du filtre, tapez network.negotiate.
4. Remplacez network.negotiate-auth.delegation-uris par le domaine que vous souhaitez ajouter.
5. Remplacez network.negotiate-auth.trusted-uris par le domaine que vous souhaitez ajouter.

> **Remarque :** Si vous exécutez Windows, vous devez également entrer sspi dans la zone de texte du filtre et changer l'option network.auth.use-sspi sur False.

Décharger l'authentification Kerberos des serveurs physiques

June 2, 2023

L'appliance NetScaler peut décharger les tâches d'authentification des serveurs. Au lieu que les serveurs physiques authentifient les demandes des clients, NetScaler authentifie toutes les demandes des clients avant de les transmettre à l'un des serveurs physiques qui lui sont liés. L'authentification de l'utilisateur est basée sur des jetons Active Directory.

Il n'existe aucune authentification entre NetScaler et le serveur physique, et le déchargement de l'authentification est transparent pour les utilisateurs finaux. Après l'ouverture de session initiale sur un ordinateur Windows, l'utilisateur final n'a pas besoin de saisir d'informations d'authentification supplémentaires dans une fenêtre contextuelle ou sur une page d'ouverture de session.

Dans la version actuelle de l'appliance NetScaler, l'authentification Kerberos n'est disponible que pour l'authentification, l'autorisation et l'audit des serveurs virtuels de gestion du trafic. L'authentification Kerberos n'est pas prise en charge pour le VPN SSL dans l'appliance NetScaler Gateway Advanced Edition ou pour la gestion de l'appliance NetScaler.

L'authentification Kerberos nécessite une configuration sur l'appliance NetScaler et sur les navigateurs clients.

Pour configurer l'authentification Kerberos sur l'appliance NetScaler

> **Remarque**
>
> Les mots de passe utilisés dans l'exemple de configuration suivant ne sont que des exemples et non les mots de passe de configuration réels.

1. Créez un compte utilisateur sur Active Directory. Lors de la création d'un compte utilisateur, vérifiez les options suivantes dans la section Propriétés de l'utilisateur :
   - Assurez-vous de ne pas sélectionner l'option Modifier le mot de passe lors de la prochaine connexion.
   - Assurez-vous de sélectionner l'option Le mot de passe n'expire pas.
2. Sur le serveur AD, à l'invite de commandes de l'interface de ligne de commande, tapez :
   - ktpass -princ HTTP/ kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass Citrix1 -out C:\kerbtabfile.txt

   > **Remarque**
   >
   > N'oubliez pas de taper la commande ci-dessus sur une seule ligne. La sortie de la commande ci-dessus est écrite dans le fichier C:\kerbtabfile.txt.
3. Téléchargez le fichier kerbtabfile.txt dans le répertoire /etc de l'appliance NetScaler à l'aide d'un client Secure Copy (SCP).
4. Exécutez la commande suivante pour ajouter un serveur DNS à l'appliance NetScaler.
   - add dns nameserver 1.2.3.4

   L'appliance NetScaler ne peut pas traiter les requêtes Kerberos sans le serveur DNS. Assurez-vous d'utiliser le même serveur DNS que celui utilisé dans le domaine Microsoft Windows.
5. Passez à l'interface de ligne de commande de NetScaler.
6. Exécutez la commande suivante pour créer un serveur d'authentification Kerberos :
   - add authentication negotiateAction KerberosServer -domain "crete.lab.net" -domainUser kerbuser -domainUserPasswd Citrix1 -keytab /var/mykcd.keytab

   > **Remarque**
   >
   > Si keytab n'est pas disponible, vous pouvez spécifier les paramètres suivants : domain, DomainUser et -DomainUserPasswd.
7. Exécutez la commande suivante pour créer une stratégie de négociation :
   - `add authentication negotiatePolicy Kerberos-Policy "REQ.IP.DESTIP == 192.168.17.200"KerberosServer<!--NeedCopy-->`
8. Exécutez la commande suivante pour créer un serveur virtuel d'authentification.
   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`

9. Exécutez la commande suivante pour lier la stratégie Kerberos au serveur virtuel d'authentification :

   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`

10. Exécutez la commande suivante pour lier un certificat SSL au serveur virtuel d'authentification. Vous pouvez utiliser l'un des certificats de test, que vous pouvez installer à partir de l'appliance GUI NetScaler. Exécutez la commande suivante pour utiliser l'exemple de certificat ServerTestCert.

    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`

11. Créez un serveur virtuel d'équilibrage de charge HTTP avec l'adresse IP 192.168.17.200.

    Assurez-vous de créer un serveur virtuel à partir de l'interface de ligne de commande pour les versions NetScaler 9.3 si elles sont antérieures à 9.3.47.8.

12. Exécutez la commande suivante pour configurer un serveur virtuel d'authentification :

    - `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy-->`

13. Entrez l' exemple de nom d'hôte dans la barre d'adresse du navigateur Web.

    Le navigateur Web affiche une boîte de dialogue d'authentification car l'authentification Kerberos n'est pas configurée dans le navigateur.

    > **Remarque**
    >
    > L'authentification Kerberos nécessite une configuration spécifique sur le client. Assurez-vous que le client peut résoudre le nom d'hôte, ce qui entraîne la connexion du navigateur Web à un serveur virtuel HTTP.

14. Configurez Kerberos sur le navigateur Web de l'ordinateur client.

    - Pour la configuration sur Internet Explorer, reportez-vous à la section Configuration de l'authentification Internet Explorer pour Kerberos.
    - Pour la configuration sur Mozilla Firefox, reportez-vous à la section Configuration de l'authentification Internet Explorer pour Kerberos.

15. Vérifiez si vous pouvez accéder au serveur physique principal sans authentification.

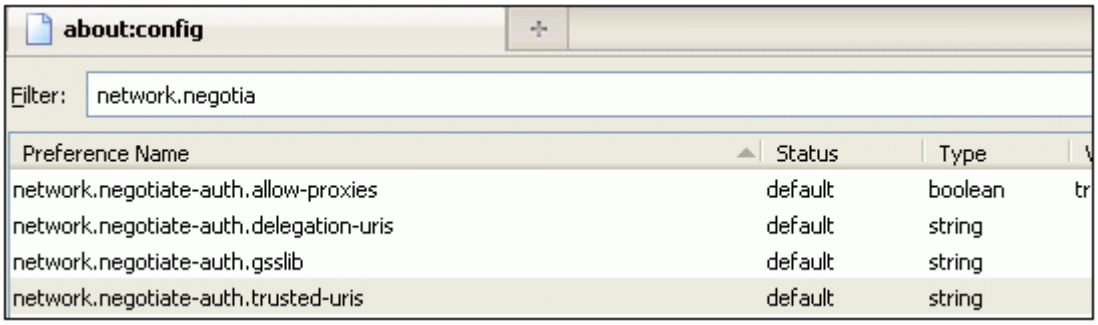
Pour configurer l'authentification Internet Explorer pour Kerberos

1. Sélectionnez **Options Internet** dans le menu **Outils** .
2. Activez l'onglet **Sécurité** .
3. Sélectionnez **Intranet local dans** la section Sélectionner une zone pour afficher les paramètres de sécurité des modifications.

4. Cliquez sur **Sites**.
5. Cliquez sur **Avancé**.
6. Spécifiez l'URL, Exemple, puis cliquez sur **Ajouter**.
7. Redémarrez **Internet Explorer**.

Pour configurer l'authentification Mozilla Firefox pour Kerberos

1. Entrez about:config dans la barre d'adresse du navigateur.
2. Cliquez sur l'avertissement de non-responsabilité.
3. Tapez **Network.Negotiate-Auth.Trusted-URIS** dans la zone **Filtre** .
4. Double-cliquez sur **Network.Negotiate-Auth.Trusted-URIS.** Un exemple d'écran est présenté ci-dessous.



5. Dans la boîte de dialogue Saisir une valeur de chaîne, spécifiez www.crete.lab.net.
6. Redémarrez Firefox.

Types d'authentification unique

May 5, 2023

Les fonctionnalités d'authentification, d'autorisation et d'audit de NetScaler prennent en charge les types d'authentification unique suivants.

- Authentification**unique NetScaler Kerberos : les appliances NetScaler prennent désormais en charge l'authentification** unique (SSO) à l'aide du protocole Kerberos 5. Les utilisateurs ouvrent une session sur un proxy, l'Application Delivery Controller (ADC), qui donne ensuite accès aux ressources protégées. Pour plus de détails, consultez NetScaler KerberosSingle Sign-On.
- **SSO pour les authentifications Basic, Digest et NTLM :** la configuration SSO (Single Sign-On) dans NetScaler et NetScaler Gateway peut être activée au niveau global et également par niveau

de trafic. Par défaut, la configuration SSO est désactivée et un administrateur peut activer le SSO par trafic ou globalement. Du point de vue de la sécurité, Citrix recommande aux administrateurs de désactiver globalement le SSO et de l'activer par trafic. Cette amélioration vise à rendre la configuration SSO plus sécurisée en désactivant certains types de méthodes SSO globalement. Pour plus de détails, voir SSO pour l'authentification Basic, Digest et NTLM.

Authentification unique NetScaler Kerberos

May 5, 2023

Les appliances NetScaler prennent désormais en charge l'authentification unique (SSO) à l'aide du protocole Kerberos 5. Les utilisateurs ouvrent une session sur un proxy, l'Application Delivery Controller (ADC), qui donne ensuite accès aux ressources protégées.

L'implémentation SSO de NetScaler Kerberos nécessite le mot de passe de l'utilisateur pour les méthodes SSO qui reposent sur une authentification de base, NTLM ou basée sur des formulaires. Le mot de passe de l'utilisateur n'est pas requis pour l'authentification unique Kerberos, mais si l'authentification unique Kerberos échoue et que l'appliance NetScaler possède le mot de passe de l'utilisateur, elle utilise le mot de passe pour tenter l'authentification SSO NTLM.

Si le mot de passe de l'utilisateur est disponible, si le compte KCD est configuré avec un domaine et qu'aucune information utilisateur déléguée n'est présente, le moteur SSO Kerberos de Citrix AD usurpe l'identité de l'utilisateur pour accéder aux ressources autorisées. L'usurpation d'identité est également appelée délégation sans contrainte.

Le moteur SSO NetScaler Kerberos peut également être configuré pour utiliser un compte délégué afin d'accéder aux ressources protégées au nom de l'utilisateur. Cette configuration nécessite des informations d'identification utilisateur déléguées, un keytab ou un certificat utilisateur délégué et un certificat CA correspondant. La configuration qui utilise un compte délégué est appelée délégation contrainte.

Présentation de NetScaler Kerberos SSO

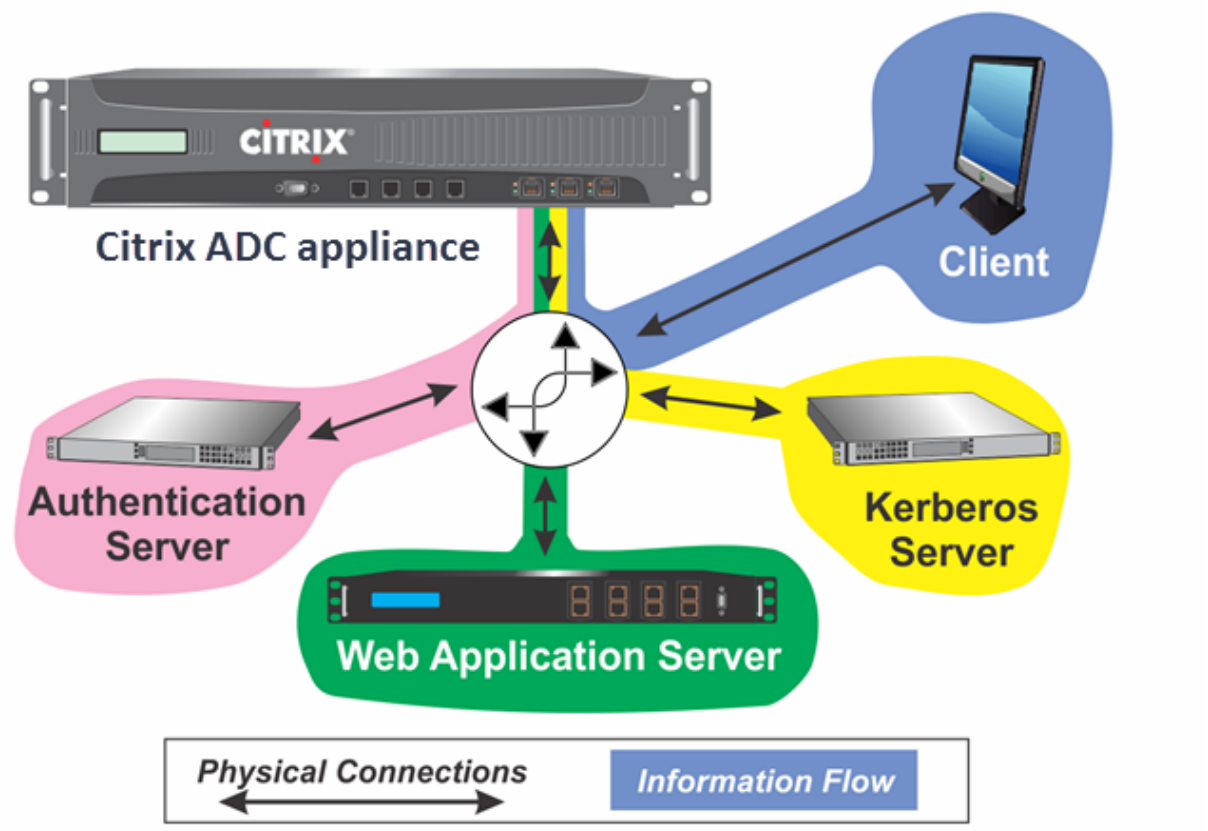
May 5, 2023

Pour utiliser la fonctionnalité SSO Kerberos de NetScaler, les utilisateurs doivent d'abord s'authentifier auprès de Kerberos ou d'un serveur d'authentification tiers compatible. Une fois authentifié, l'utilisateur demande l'accès à une application Web protégée. Le serveur Web répond en demandant la preuve que l'utilisateur est autorisé à accéder à cette application Web. Le navigateur de l'utilisateur contacte le serveur Kerberos, qui vérifie que l'utilisateur est autorisé à accéder à cette

ressource, puis fournit au navigateur de l'utilisateur un ticket de service qui en fournit la preuve. Le navigateur renvoie la demande de l'utilisateur au serveur d'applications Web avec le ticket de service joint. Le serveur d'applications Web vérifie le ticket de service, puis autorise l'utilisateur à accéder à l'application.

La gestion du trafic d'authentification, d'autorisation et d'audit met en œuvre ce processus comme indiqué dans le schéma suivant. Le diagramme illustre le flux d'informations via l'appliance NetScaler et la gestion du trafic d'authentification, d'autorisation et d'audit, sur un réseau sécurisé avec authentification LDAP et autorisation Kerberos. Les environnements de gestion du trafic d'authentification, d'autorisation et d'audit qui utilisent d'autres types d'authentification utilisent essentiellement le même flux d'informations, bien qu'ils puissent différer sur certains points.

Figure 1. Un réseau sécurisé avec LDAP et Kerberos



L'authentification, l'autorisation et l'audit de la gestion du trafic avec authentification et autorisation dans un environnement Kerberos nécessitent que les actions suivantes soient effectuées.

1. Le client envoie une demande de ressource au serveur virtuel de gestion du trafic sur l'appliance NetScaler.
2. Le serveur virtuel de gestion du trafic transmet la demande au serveur virtuel d'authentification, qui authentifie le client puis renvoie la demande au serveur virtuel de gestion du trafic.
3. Le serveur virtuel de gestion du trafic envoie la demande du client au serveur d'applications

Web.

4. Le serveur d'applications Web répond au serveur virtuel de gestion du trafic par un message 401 non autorisé demandant l'authentification Kerberos, avec recours à l'authentification NTLM si le client ne prend pas en charge Kerberos.
5. Le serveur virtuel de gestion du trafic contacte le démon SSO Kerberos.
6. Le démon SSO Kerberos contacte le serveur Kerberos et obtient un ticket d'octroi de tickets (TGT) lui permettant de demander des tickets de service autorisant l'accès à des applications protégées.
7. Le démon SSO Kerberos obtient un ticket de service pour l'utilisateur et envoie ce ticket au serveur virtuel de gestion du trafic.
8. Le serveur virtuel de gestion du trafic joint le ticket à la demande initiale de l'utilisateur et renvoie la demande modifiée au serveur d'applications Web.
9. Le serveur d'applications Web répond par un message 200 OK.

Ces étapes sont transparentes pour le client, qui envoie simplement une demande et reçoit la ressource demandée.

Intégration de NetScaler Kerberos SSO aux méthodes d'authentification

Tous les mécanismes d'authentification, d'autorisation et d'audit de la gestion du trafic prennent en charge le SSO NetScaler Kerberos. La gestion du trafic d'authentification, d'autorisation et d'audit prend en charge le mécanisme SSO Kerberos avec les mécanismes d'authentification Kerberos, CAC (carte à puce) et SAML avec toute forme d'authentification client auprès de l'appliance NetScaler. Il prend également en charge les mécanismes SSO HTTP-Basic, HTTP-Digest, basés sur Forms et NTLM (versions 1 et 2) si le client utilise l'authentification HTTP-Basic ou basée sur Forms pour se connecter à l'appliance NetScaler.

Le tableau suivant présente chaque méthode d'authentification côté client prise en charge, ainsi que la méthode d'authentification côté serveur prise en charge pour cette méthode côté client.

Tableau 1. Méthodes d'authentification prises en charge

	Basique/Digest/NTLM	Délégation Kerberos contrainte	Emprunt d'identité d'un utilisateur
CAC (carte à puce) : au niveau de la couche SSL/T LS		X	X
Basé sur des formulaires (LDAP/RADIUS/TACACS)	X	X	X

	Basique/Digest/NTLM	Délégation Kerberos contrainte	Emprunt d'identité d'un utilisateur
HTTP de base (LDAP/RADIUS/TA-CACS)	X	X	X
Kerberos		X	
NT LM v1/v2		X	X
SAML		X	
SAML à deux facteurs	X	X	X
Certificat à deux facteurs	X	X	X

Configurer NetScaler SSO

May 5, 2023

Vous pouvez configurer NetScaler SSO pour qu'il fonctionne de deux manières : par usurpation d'identité ou par délégation. Le SSO par usurpation d'identité est une configuration plus simple que le SSO par délégation, et est donc préférable lorsque votre configuration le permet. Pour configurer NetScaler SSO par usurpation d'identité, vous devez disposer du nom d'utilisateur et du mot de passe de l'utilisateur.

Pour configurer NetScaler SSO par délégation, vous devez disposer des informations d'identification de l'utilisateur délégué dans l'un des formats suivants : le nom d'utilisateur et le mot de passe de l'utilisateur, la configuration keytab qui inclut le nom d'utilisateur et un mot de passe crypté, ou le certificat utilisateur délégué et le certificat CA correspondant.

Conditions préalables à la configuration de NetScaler SSO

Avant de configurer un SSO NetScaler, votre appliance NetScaler doit être entièrement configurée pour gérer le trafic et l'authentification de vos serveurs d'applications Web. Par conséquent, vous devez configurer l'équilibrage de charge ou la commutation de contenu, puis l'authentification, l'autorisation et l'audit pour ces serveurs d'applications Web. Vous devez également vérifier le routage entre l'appliance, votre serveur LDAP et votre serveur Kerberos.

Si votre réseau n'est pas déjà configuré de cette manière, effectuez les tâches de configuration suivantes :

- Configurez un serveur et un service pour chaque serveur d'applications Web.
- Configurez un serveur virtuel de gestion du trafic pour gérer le trafic vers et depuis votre serveur d'applications Web.

Vous trouverez ci-dessous de brèves instructions et des exemples pour effectuer chacune de ces tâches à partir de la ligne de commande NetScaler. Pour obtenir de l'aide supplémentaire, voir Configuration d'un serveur virtuel d'authentification.

> **Remarque**
>
> À partir de la version 13.1 de NetScaler, la traversée entre le domaine racine et le domaine Tree est prise en charge lors de l'authentification SSO Kerberos pour le serveur principal à partir de l'appliance NetScaler.

Pour créer un serveur et un service à l'aide de l'interface de ligne de commande

Pour que NetScaler SSO obtienne un TGS (ticket de service) pour un service, soit le nom de domaine complet attribué à l'entité serveur sur l'appliance NetScaler doit correspondre au nom de domaine complet du serveur d'applications Web, soit le nom de l'entité serveur doit correspondre au nom NetBIOS du serveur d'applications Web. Vous pouvez adopter l'une des approches suivantes :

- Configurez l'entité du serveur NetScaler en spécifiant le nom de domaine complet du serveur d'applications Web.
- Configurez l'entité de serveur NetScaler en spécifiant l'adresse IP du serveur d'applications Web et attribuez à l'entité de serveur le même nom que le nom NetBIOS du serveur d'applications Web.

À l'invite de commandes, tapez les commandes suivantes :

```
1 -  add server name <serverFQDN>
2
3 -  add service name serverName serviceType port
4 <!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **ServerName**. Nom de l'appliance NetScaler à utiliser pour faire référence à ce serveur.
- Nom**de domaine complet du serveur**. Le nom de domaine complet du serveur. Si aucun domaine n'est attribué au serveur, utilisez l'adresse IP du serveur et assurez-vous que le nom de l'entité du serveur correspond au nom NetBIOS du serveur d'applications Web.
- **ServiceName**. Nom de l'appliance NetScaler à utiliser pour faire référence à ce service.
- **type**. Protocole utilisé par le service, HTTP ou MSSQLSVC.
- **port**. Port sur lequel le service écoute. Les services HTTP écoutent normalement sur le port 80. Les services HTTPS sécurisés écoutent normalement sur le port 443.

Exemple :

Les exemples suivants ajoutent des entrées de serveur et de service sur l'appliance NetScaler pour le serveur d'applications Web was1.example.com. Le premier exemple utilise le nom de domaine complet du serveur d'applications Web ; le second utilise l'adresse IP.

Pour ajouter le serveur et le service à l'aide du nom de domaine complet du serveur d'applications Web, was1.example.com, vous devez taper les commandes suivantes :

```
add server was1 was1.example.com
add service was1service was1 HTTP 80
<!--NeedCopy-->
```

Pour ajouter le serveur et le service à l'aide de l'adresse IP du serveur d'applications Web et du nom NetBIOS, où l'adresse IP du serveur d'applications Web est 10.237.64.87 et son nom NetBIOS est WAS1, vous devez taper les commandes suivantes :

```
add server WAS1 10.237.64.87
add service was1service WAS1 HTTP 80
<!--NeedCopy-->
```

Pour créer un serveur virtuel de gestion du trafic à l'aide de l'interface de ligne de commande

Le serveur virtuel de gestion du trafic gère le trafic entre le client et le serveur d'applications Web. Vous pouvez utiliser un serveur virtuel d'équilibrage de charge ou de commutation de contenu comme serveur de gestion du trafic. La configuration SSO est la même pour les deux types.

Pour créer un serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez la commande suivante :

```
add lb vserver <vserverName> <type> <IP> <port>
<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **vServerName** : nom de l'appliance NetScaler à utiliser pour faire référence à ce serveur virtuel.
- **type** : protocole utilisé par le service, HTTP ou MSSQLSVC.
- **IP** : adresse IP attribuée au serveur virtuel. Il s'agit normalement d'une adresse IP non publique réservée par l'IANA sur votre réseau local.
- **port**—Port sur lequel le service écoute. Les services HTTP écoutent normalement sur le port 80. Les services HTTPS sécurisés écoutent normalement sur le port 443.

Exemple :

Pour ajouter un serveur virtuel d'équilibrage de charge appelé tmvserver1 à une configuration qui gère le trafic HTTP sur le port 80, en lui attribuant une adresse IP LAN 10.217.28.20, puis en liant le serveur virtuel d'équilibrage de charge au service wasservice1, vous devez taper les commandes suivantes :

```
add lb vserver tmvserver1 HTTP 10.217.28.20 80
bind lb vserver tmvserv1 wasservice1
<!--NeedCopy-->
```

Pour créer un serveur virtuel d'authentification à l'aide de l'interface de ligne de commande

Le serveur virtuel d'authentification gère le trafic d'authentification entre le client et le serveur d'authentification (LDAP). Pour créer un serveur virtuel d'authentification, à l'invite de commandes, tapez les commandes suivantes :

```
add authentication vserver <authvserverName> SSL <IP> 443
<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **AuthvServerName** : nom que l'appliance NetScaler doit utiliser pour faire référence à ce serveur virtuel d'authentification. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Peut être modifié après l'ajout du serveur virtuel d'authentification à l'aide de la commande rename authentication vserver.
- **IP** : adresse IP attribuée au serveur virtuel d'authentification. Comme pour le serveur virtuel de gestion du trafic, cette adresse est normalement une adresse IP non publique réservée par l'IANA sur votre réseau local.
- **domain** : domaine attribué au serveur virtuel. Il s'agit généralement du domaine de votre réseau. Il est habituel, bien que non obligatoire, d'entrer le domaine dans toutes les capitales lors de la configuration du serveur virtuel d'authentification.

Exemple :

Pour ajouter un serveur virtuel d'authentification appelé authverver1 à votre configuration et lui attribuer l'adresse IP LAN 10.217.28.21 et le domaine EXAMPLE.COM, vous devez taper les commandes suivantes :

```
add authentication vserver authvserver1 SSL 10.217.28.21 443
<!--NeedCopy-->
```


Pour configurer un serveur virtuel de gestion du trafic afin qu'il utilise un profil d'authentification

Le serveur virtuel d'authentification peut être configuré pour gérer l'authentification pour un seul domaine ou pour plusieurs domaines. S'il est configuré pour prendre en charge l'authentification pour plusieurs domaines, vous devez également spécifier le domaine pour NetScaler SSO en créant un profil d'authentification, puis en configurant le serveur virtuel de gestion du trafic pour utiliser ce profil d'authentification.

> **Remarque**
>
> Le serveur virtuel de gestion du trafic peut être un serveur virtuel d'équilibrage de charge (lb) ou de commutation de contenu (cs). Les instructions suivantes supposent que vous utilisez un serveur virtuel d'équilibrage de charge. Pour configurer un serveur virtuel de commutation de contenu, il suffit de remplacer
> set cs vserver par set lb vserver. Sinon, la procédure est la même.

Pour créer le profil d'authentification, puis le configurer sur un serveur virtuel de gestion du trafic, tapez les commandes suivantes :

```
-  add authentication authnProfile <authnProfileName> {
 -authvserverName <string> }
  {
 -authenticationHost <string> }
  {
 -authenticationDomain <string> }

-  set lb vserver \<vserverName\> -authnProfile <authnprofileName>
<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **AuthnProfileName** : nom du profil d'authentification. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et doit comprendre de un à trente et un caractères alphanumériques ou un trait d'union (-), un point (.) livre (#), espace (), à (@), égal à (=), deux-points (:) et caractères de soulignement.
- **AuthvServerName** : nom du serveur virtuel d'authentification utilisé par ce profil pour l'authentification.
- **AuthenticationHost** : nom d'hôte du serveur virtuel d'authentification.
- **AuthenticationDomain : domaine**pour lequel NetScaler SSO gère l'authentification. Obligatoire si le serveur virtuel d'authentification effectue l'authentification pour plusieurs domaines, de sorte que le domaine approprié soit inclus lorsque l'appliance NetScaler définit le cookie du serveur virtuel de gestion du trafic.

Exemple :

Pour créer un profil d'authentification nommé AuthnProfile1 pour l'authentification du domaine example.com et pour configurer le serveur virtuel d'équilibrage de charge vserver1 pour utiliser le profil d'authentification AuthnProfile1, tapez les commandes suivantes :

```
1 add authentication authnProfile authnProfile1 -authnvsName
     authvsesrver1
2       -authenticationHost authvsesrver1 -authenticationDomain example.
           com
3 set lb vserver vserver1 -authnProfile authnProfile1
4 <!--NeedCopy-->
```

Configuration de l'authentification unique

May 5, 2023

La configuration de l'authentification unique (SSO) de NetScaler pour l'authentification par usurpation d'identité est plus simple que la configuration de l'authentification unique pour l'authentification par délégation, et est donc préférable lorsque votre configuration le permet. Vous créez un compte KCD. Vous pouvez utiliser le mot de passe de l'utilisateur.

Si vous ne disposez pas du mot de passe de l'utilisateur, vous pouvez configurer NetScaler SSO pour qu'il s'authentifie par délégation. Bien que plus complexe que la configuration du SSO pour s'authentifier par usurpation d'identité, la méthode de délégation offre une certaine flexibilité dans la mesure où les informations d'identification d'un utilisateur peuvent ne pas être disponibles pour l'appliance NetScaler en toutes circonstances.

Pour l'emprunt d'identité ou la délégation, vous devez également activer l'authentification intégrée sur le serveur d'applications Web.

Activer l'authentification intégrée sur le serveur d'applications Web

Pour configurer l'authentification unique NetScaler Kerberos sur chaque serveur d'applications Web géré par Kerberos SSO, utilisez l'interface de configuration de ce serveur pour configurer le serveur de manière à exiger une authentification. Sélectionnez l'authentification Kerberos (négocier) par préférence, avec recours à NTLM pour les clients qui ne prennent pas en charge Kerberos.

Les instructions suivantes permettent de configurer Microsoft Internet Information Server (IIS) pour exiger l'authentification. Si votre serveur d'applications Web utilise un logiciel autre que IIS, consultez la documentation de ce logiciel de serveur Web pour obtenir des instructions.

Pour configurer Microsoft IIS afin d'utiliser l'authentification intégrée

1. Ouvrez une session sur le serveur IIS et ouvrez le **Gestionnaire des services Internet.**
2. Sélectionnez le site Web pour lequel vous souhaitez activer l'authentification intégrée. Pour activer l'authentification intégrée pour tous les serveurs Web IIS gérés par IISM, configurez les paramètres d'authentification pour le site Web par défaut. Pour activer l'authentification intégrée pour des services individuels (tels que Exchange, Exadmin, ExchWeb et Public), configurez ces paramètres d'authentification pour chaque service individuellement.
3. Ouvrez la boîte de dialogue **Propriétés** du site Web par défaut ou du service individuel, puis cliquez sur l'onglet **Sécurité du répertoire** .
4. À côté de **Authentification** et **contrôle d'accès**, sélectionnez **Modifier.**
5. Désactivez l'accès anonyme.
6. Activez l'authentification Windows intégrée (uniquement). L'activation de l'authentification Windows intégrée doit automatiquement définir la négociation de protocole pour le serveur Web sur Négocier, NTLM, qui spécifie l'authentification Kerberos avec retour à NTLM pour les périphériques non compatibles Kerberos. Si cette option n'est pas sélectionnée automatiquement, définissez manuellement la négociation de protocole sur Négocier, NTLM.

Configurer l'authentification unique par emprunt d'identité

Vous pouvez configurer le compte KCD pour NetScaler SSO par usurpation d'identité. Dans cette configuration, l'appliance NetScaler obtient le nom d'utilisateur et le mot de passe de l'utilisateur lorsque celui-ci s'authentifie auprès du serveur d'authentification et utilise ces informations d'identification pour se faire passer pour l'utilisateur afin d'obtenir un ticket d'octroi de tickets (TGT). Si le nom de l'utilisateur est au format UPN, l'appliance obtient le domaine de l'utilisateur auprès de l'UPN. Sinon, il obtient le nom et le domaine de l'utilisateur en les extrayant du domaine SSO utilisé lors de l'authentification initiale ou du profil de session.

> **Remarque**
>
> Vous ne pouvez pas ajouter un nom d'utilisateur avec un domaine si le nom d'utilisateur est déjà ajouté sans domaine. Si le nom d'utilisateur avec domaine est ajouté en premier, suivi du même nom d'utilisateur sans domaine, l'appliance NetScaler ajoute le nom d'utilisateur à la liste des utilisateurs.

Lors de la configuration du compte KCD, vous devez définir le paramètre de domaine sur le domaine du service auquel l'utilisateur accède. Le même domaine est également utilisé comme domaine de l'utilisateur si le domaine de l'utilisateur ne peut pas être obtenu par authentification auprès de l'appliance NetScaler ou à partir du profil de session.

Pour créer le compte KCD pour l'authentification unique par emprunt d'identité à l'aide d'un mot de passe

À l'invite de commandes, tapez la commande suivante :

```
add aaa kcdaccount <accountname> -realmStr <realm>

<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **accountname**. Le nom du compte KCD.
- **realm**. Le domaine attribué au NetScaler SSO.

Exemple

Pour ajouter un compte KCD nommé kcdccount1 et utiliser le keytab nommé kcdvserver.keytab, tapez la commande suivante :

```
add aaa kcdAccount kcdaccount1 -keytab kcdvserver.keytab

<!--NeedCopy-->
```

Pour plus d'informations sur la configuration de l'usurpation d'identité Kerberos via l'interface graphique de NetScaler, consultez le support de NetScaler.

Configurer l'authentification SSO par délégation

Pour configurer l'authentification unique par délégation, vous devez effectuer les tâches suivantes :

- Si vous configurez la délégation par certificat utilisateur délégué, installez les certificats CA correspondants sur l'appliance NetScaler et ajoutez-les à la configuration NetScaler.
- Créez le compte KCD sur l'appliance. L'appliance utilise ce compte pour obtenir des tickets de service pour vos applications protégées.
- Configurez le serveur Active Directory.

> **Remarque**
>
> Pour plus d'informations sur la création d'un compte KCD et la configuration sur le boîtier NetScaler, reportez-vous aux rubriques suivantes :
>
> - Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM

- Comment NetScaler implémente Kerberos pour l'authentification des clients
- Configuration de l'authentification Kerberos sur l'appliance NetScaler

Installation du certificat CA client sur l'appliance NetScaler

Si vous configurez le NetScaler SSO avec un certificat client, vous devez copier le certificat CA correspondant pour le domaine du certificat client (le certificat CA client) sur l'appliance NetScaler, puis installer le certificat CA. Pour copier le certificat CA client, utilisez le programme de transfert de fichiers de votre choix pour transférer le certificat et le fichier de clé privée vers l'appliance NetScaler, puis stockez les fichiers dans /nsconfig/ssl.

Pour installer le certificat CA client sur l'appliance NetScaler

À l'invite de commandes, tapez la commande suivante :

```
add ssl certKey <certkeyName> -cert <cert> [(-key <key> [-password]) |
    -fipsKey <fipsKey>][-inform ( DER | PEM )][-expiryMonitor ( ENABLED
    | DISABLED | UNSET ) [-notificationPeriod <positive_integer>]] [-
    bundle ( YES | NO )]

<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **CertKeyName**. Nom du certificat d'autorité de certification client. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_) et doit comprendre de un à trente et un caractères. Les caractères autorisés sont les caractères alphanumériques ASCII, le trait de soulignement, le dièse (#), le point (.), l'espace, les deux points (:), l'arobase (@), le signe égal (=) et le trait d'union (-). Ne peut pas être modifié après la création de la paire de clés de certificat. Si le nom comprend un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « mon certificat » ou « mon certificat »).
- **cert**. Chemin d'accès complet et nom de fichier du fichier de certificat X509 utilisé pour former la paire de clés de certificat. Le fichier de certificat doit être stocké sur l'appliance NetScaler, dans le répertoire /nsconfig/ssl/.
- **key**. Chemin d'accès complet et nom de fichier du fichier contenant la clé privée du fichier de certificat X509. Le fichier clé doit être stocké sur l'appliance NetScaler dans le répertoire /nsconfig/ssl/.
- **password**. Si une clé privée est spécifiée, la phrase secrète utilisée pour chiffrer la clé privée. Utilisez cette option pour charger des clés privées chiffrées au format PEM.

- **fipsKey.** Nom de la clé FIPS créée dans le module de sécurité matérielle (HSM) d'un dispositif FIPS ou d'une clé importée dans le HSM.

  > **Remarque**
  >
  > Vous pouvez spécifier une clé ou une clé FipsKey, mais pas les deux.

- **inform**. Format du certificat et des fichiers de clé privée, PEM ou DER.
- **passplain**. Phrase secrète utilisée pour chiffrer la clé privée. Obligatoire lors de l'ajout d'une clé privée chiffrée au format PEM.
- **expiryMonitor**. Configurez l'appliance NetScaler pour émettre une alerte lorsque le certificat est sur le point d'expirer. Valeurs possibles : ENABLED, DISABLED, UNSET.
- **notificationPeriod**. Si cette option `expiryMonitor` est ACTIVÉE, le nombre de jours avant l'expiration du certificat pour émettre une alerte.
- **bundle**. Analysez la chaîne de certificats en tant que fichier unique après avoir lié le certificat du serveur au certificat de son émetteur dans le fichier. Valeurs possibles : OUI, NON.

Exemple

L'exemple suivant ajoute le certificat utilisateur délégué customer-cert.pem spécifié à la configuration NetScaler avec la clé customer-key.pem, et définit le mot de passe, le format du certificat, le moniteur d'expiration et la période de notification.

Pour ajouter le certificat d'utilisateur délégué, vous devez taper les commandes suivantes :

```
add ssl certKey customer -cert "/nsconfig/ssl/customer-cert.pem"
-key "/nsconfig/ssl/customer-key.pem" -password "dontUseDefaultPWs!"
-inform PEM -expiryMonitor ENABLED [-notificationPeriod 14]

<!--NeedCopy-->
```

Création du compte KCD

Si vous configurez NetScaler SSO par délégation, vous pouvez configurer le compte KCD pour utiliser le nom de connexion et le mot de passe de l'utilisateur, pour utiliser le nom de connexion et le keytab de l'utilisateur, ou pour utiliser le certificat client de l'utilisateur. Si vous configurez le SSO avec un nom d'utilisateur et un mot de passe, l'appliance NetScaler utilise le compte utilisateur délégué pour obtenir un ticket d'octroi de tickets (TGT), puis utilise le TGT pour obtenir des tickets de service pour les services spécifiques demandés par chaque utilisateur. Si vous configurez le SSO avec le fichier keytab, l'appliance NetScaler utilise le compte utilisateur délégué et les informations keytab. Si vous configurez le SSO avec un certificat utilisateur délégué, l'appliance NetScaler utilise le certificat utilisateur délégué.

> **Remarque :**
>
> Pour les domaines interdomaines, le ServicePrincipalName de l'utilisateur délégué doit être au format `host/<name>`. S'il n'est pas dans ce format, remplacez le ServicePrincipalName de l'utilisateur `<servicePrincipalName>` délégué par `host/<service-account-samaccountname>`. Vous pouvez vérifier l'attribut du compte d'utilisateur délégué dans le contrôleur de domaine. Une méthode de modification consiste à modifier l'attribut `logonName` de l'utilisateur délégué.

Pour créer le compte KCD pour l'authentification unique par délégation avec un mot de passe

À l'invite de commandes, tapez les commandes suivantes :

```
add aaa kcdAccount <kcdAccount> {
 -realmStr <string> }
  {
 -delegatedUser <string> }
  {
 -kcdPassword  }
  [-userRealm <string>]
[-enterpriseRealm <string>] [-serviceSPN <string>]
<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **kcdAccount** - Nom du compte KCD. Il s'agit d'un argument obligatoire. Longueur maximale : 31
- **realmStr** - Le royaume de Kerberos. Longueur maximale : 255
- **DelegatedUser** : nom d'utilisateur qui peut effectuer une délégation limitée Kerberos. Le nom d'utilisateur délégué est dérivé du ServicePrincipalName de votre contrôleur de domaine. Pour le cross-realm, le ServicePrincipalName de l'utilisateur délégué doit être au format `host/<name>`. Longueur maximale : 255.
- **kcdPassword** - Mot de passe pour l'utilisateur délégué. Longueur maximale : 31
- **userRealm** - Domaine de l'utilisateur. Longueur maximale : 255
- **enterpriseRealm** : domaine d'entreprise de l'utilisateur. Cela n'est donné que dans certains déploiements KDC où le KDC attend un nom d'utilisateur d'entreprise au lieu du nom principal. Longueur maximale : 255
- **serviceSPN** - Service SPN. Lorsqu'elle est spécifiée, elle est utilisée pour récupérer les tickets Kerberos. Si ce n'est pas spécifié, NetScaler construit le SPN à l'aide du FQDN du service. Longueur maximale : 255

Exemple (format UPN) :

Pour ajouter un compte KCD nommé kcdaccount1 à la configuration de l'appliance NetScaler avec le mot de passe password1 et le domaine EXAMPLE.COM, en spécifiant le compte utilisateur délégué au

format UPN (en tant que root), vous devez taper les commandes suivantes :

```
1 add aaa kcdaccount kcdaccount1 -delegatedUser root
2 -kcdPassword password1 -realmStr EXAMPLE.COM
3
4 <!--NeedCopy-->
```

Exemple (format SPN) :

Pour ajouter un compte KCD nommé kcdaccount1 à la configuration de l'appliance NetScaler avec le mot de passe password1 et le domaine EXAMPLE.COM, en spécifiant le compte utilisateur délégué au format SPN, vous devez taper les commandes suivantes :

```
1 add aaa kcdAccount kcdaccount1 -realmStr EXAMPLE.COM
2 -delegatedUser "host/kcdvserver.example.com" -kcdPassword password1
3
4 <!--NeedCopy-->
```

Création du compte KCD pour l'authentification unique par délégation avec un keytab

Si vous prévoyez d'utiliser un fichier keytab pour l'authentification, créez d'abord le keytab. Vous pouvez créer le fichier keytab manuellement en vous connectant au serveur AD et en utilisant l' `ktpass` utilitaire, ou vous pouvez utiliser l'utilitaire de configuration NetScaler pour créer un script batch, puis exécuter ce script sur le serveur AD pour générer le fichier keytab. Ensuite, utilisez FTP ou un autre programme de transfert de fichiers pour transférer le fichier keytab vers l'appliance NetScaler et le placer dans le répertoire /nsconfig/krb. Enfin, configurez le compte KCD pour NetScaler SSO par délégation et fournissez le chemin et le nom de fichier du fichier keytab à l'appliance NetScaler.

> **Remarque :**
>
> Pour les domaines interdomaines, si vous souhaitez obtenir le fichier Keytab dans le compte KCD, utilisez la commande suivante pour le nom d'utilisateur délégué mis à jour.
>
> Dans le contrôleur de domaine, créez un fichier Keytab mis à jour.
>
> `ktpass /princ <servicePrincipalName-with-prefix<host/>Of-delegateUser >@<DC REALM in uppercase> /ptype KRB5_NT_PRINCIPAL /mapuser <DC REALM in uppercase>\<sAMAccountName> /pass <delegatedUserPassword> -out filepathfor.keytab`
>
> Le `filepathfor.keytab` fichier peut être placé dans l'appliance NetScaler et peut être utilisé dans le cadre de la configuration Keytab du compte ADC KCD.

Pour créer le fichier keytab manuellement

Ouvrez une session sur la ligne de commande du serveur AD et, à l'invite de commandes, tapez la commande suivante :

```
ktpass princ <SPN> ptype KRB5_NT_PRINCIPAL mapuser <DOMAIN><username>
   pass <password> -out <File_Path>
<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **SPN**. Nom du principal de service pour le compte de service KCD.
- **DOMAIN**. Le domaine du serveur Active Directory.
- **username**. Le nom d'utilisateur du compte KSA.
- **password**. Le mot de passe du compte KSA.
- **path**. Le chemin d'accès complet du répertoire dans lequel stocker le fichier keytab après sa génération.

Pour utiliser l'utilitaire de configuration NetScaler pour créer un script afin de générer le fichier keytab

1. Accédez à **Sécurité > AAA - Trafic des applications.**
2. Dans le volet de données, sous **Délégation contrainte Kerberos**, cliquez sur Fichier **batch** pour générer Keytab.
3. Dans la boîte de dialogue **Générer un script Keytab KCD (délégation contrainte Kerberos)**, définissez les paramètres suivants :
   - **Nom d'utilisateur du domaine**. Le nom d'utilisateur du compte KSA.
   - **Mot de passe du domaine** Le mot de passe du compte KSA.
   - **Directeur de service**. Le nom principal de service pour le Royaume d'Arabie Saoudite.
   - **Nom du fichier de sortie**. Chemin d'accès complet et nom de fichier vers lesquels enregistrer le fichier keytab sur le serveur AD.
4. Désactivez la case à cocher **Créer un compte d'utilisateur de domaine** .
5. Cliquez sur **Générer un script**.
6. Ouvrez une session sur le serveur Active Directory et ouvrez une fenêtre de ligne de commande.
7. Copiez le script à partir de la fenêtre **Script généré** et collez-le directement dans la fenêtre de ligne de commande du serveur Active Directory. Le keytab est généré et stocké dans le répertoire sous le nom de fichier que vous avez spécifié comme **Nom du fichier de sortie**.
8. Utilisez l'utilitaire de transfert de fichiers de votre choix pour copier le fichier keytab du serveur Active Directory vers l'appliance NetScaler et le placer dans le répertoire /nsconfig/krb.

Pour créer le compte KCD

À l'invite de commandes, tapez la commande suivante :


```
add aaa kcdaccount <accountname>  - keytab <keytab>
<!--NeedCopy-->
```

Exemple

Pour ajouter un compte KCD nommé kcdccount1 et utiliser le keytab nommé kcdvserver.keytab, vous devez taper les commandes suivantes :

```
add aaa kcdaccount kcdaccount1  - keytab kcdvserver.keytab
<!--NeedCopy-->
```

Pour créer le compte KCD pour l'authentification unique par délégation avec un certificat utilisateur délégué

À l'invite de commandes, tapez la commande suivante :

```
add aaa kcdaccount <accountname> -realmStr <realm> -delegatedUser <
   user_nameSPN> -usercert <cert> -cacert <cacert>
<!--NeedCopy-->
```

Pour les variables, remplacez les valeurs suivantes :

- **accountname**. Nom du compte KCD.
- **realmStr**. Domaine du compte KCD, généralement le domaine pour lequel l'authentification unique est configurée.
- **delegatedUser**. Le nom d'utilisateur délégué, au format SPN.
- **usercert**. Le chemin complet et le nom du fichier de certificat utilisateur délégué sur l'appliance NetScaler. Le certificat utilisateur délégué doit contenir à la fois le certificat client et la clé privée, et doit être au format PEM. Si vous utilisez l'authentification par carte à puce, vous devez créer un modèle de certificat de carte à puce pour permettre l'importation de certificats avec la clé privée.
- **cacert**. Le chemin complet et le nom du fichier de certificat CA sur l'appliance NetScaler.

Exemple

Pour ajouter un compte KCD nommé kcdccount1 et utiliser le keytab nommé kcdvserver.keytab, tapez la commande suivante :

```
add aaa kcdaccount kcdaccount1 -realmStr EXAMPLE.COM
     -delegatedUser "host/kcdvserver.example.com" -usercert /certs/
        usercert
     -cacert /cacerts/cacert
<!--NeedCopy-->
```


Configuration d'Active Directory pour NetScaler SSO

Lorsque vous configurez le SSO par délégation, en plus de créer le compte KCDAccount sur l'appliance NetScaler, vous devez également créer un compte de service Kerberos (KSA) correspondant sur votre serveur LDAP Active Directory et configurer le serveur pour le SSO. Pour créer la KSA, utilisez le processus de création de compte sur le serveur Active Directory. Pour configurer l'authentification unique sur le serveur Active Directory, ouvrez la fenêtre des propriétés du KSA. Dans l'onglet **Délégation**, activez les options suivantes : Faire confiance à cet utilisateur pour la délégation à des services spécifiés uniquement et Utiliser un protocole d'authentification quelconque. (L'option Kerberos uniquement ne fonctionne pas car elle ne permet pas la transition de protocole ni la délégation sous contrainte.) Enfin, ajoutez les services gérés par NetScaler SSO.

> **Remarque :**
>
> Si l'onglet Délégation n'est pas visible dans la boîte de dialogue des propriétés du compte KSA, avant de pouvoir configurer le KSA comme décrit, vous devez utiliser l'outil de ligne de commande Microsoft
> setspn pour configurer le serveur Active Directory afin que l'onglet soit visible.

Pour configurer la délégation pour le compte de service Kerberos

1. Dans la boîte de dialogue de configuration du compte LDAP pour le compte de service Kerberos que vous avez créé, cliquez sur l'onglet **Délégation** .
2. Choisissez **Faire confiance à cet utilisateur pour la délégation aux services spécifiés uniquement**.
3. Sous Faire confiance à cet utilisateur pour la délégation aux services spécifiés uniquement, choisissez **Utiliser un protocole d'authentification quelconque**.
4. Sous Services auxquels ce compte peut présenter des informations d'identification déléguées, cliquez sur **Ajouter.**
5. Dans la boîte de dialogue **Ajouter des services**, cliquez sur **Utilisateurs** ou **Ordinateurs**, choisissez le serveur qui héberge les ressources à affecter au compte de service, puis cliquez sur **OK.**

   > **Remarque :**
   >
   > - La délégation contrainte ne prend pas en charge les services hébergés dans des domaines autres que le domaine attribué au compte, même si Kerberos peut avoir une relation d'approbation avec d'autres domaines.
   > - Utilisez la commande suivante pour créer `setspn` si un nouvel utilisateur est créé dans Active Directory : `setspn -A host/kcdvserver.example.com example\kcdtest`

6. De retour dans la boîte de dialogue **Ajouter des services**, dans la liste Services disponibles, choisit les services affectés au compte de service. NetScaler SSO prend en charge les services HTTP et MSSQLSVC.
7. Cliquez sur **OK.**

Changements de configuration pour permettre à KCD de prendre en charge les domaines enfants

Si le compte KCD est configuré avec `samAccountName` pour `-delegatedUser`, KCD ne fonctionne pas pour les utilisateurs qui accèdent aux services à partir de domaines enfants. Dans ce cas, vous pouvez modifier la configuration sur l'appliance NetScaler et sur Active Directory.

- Modifier le nom d'ouverture de session du compte de service `<service-account-samaccountname>` (qui est configuré en tant que DelegateUser sur le compte KCD) sur AD au format `host/<service-account-samaccountname>.<completeUSERDNSDOMAIN>` (par exemple, `host/svc_act.child.parent.com`).

  Vous pouvez modifier le compte de service manuellement ou à l'aide de la commande `ktpass`. `ktpass` met automatiquement à jour le compte de service.

  ```
  ktpass /princ host/svc_act.child.parent.com@CHILD.PARENT.COM /ptype KRB5_NT_PRINCIPAL /mapuser CHILD\sv_act /pass serviceaccountpassword -out filepathfor.keytab
  ```

- Modifiez l'utilisateur délégué dans le compte KCD sur l'appliance NetScaler.
- Modifiez le paramètre -delegatedUser dans le compte KCD en tant que `host/svc_act.child.parent.com`

Points à noter lorsque des cryptages avancés sont utilisés pour configurer le compte KCD

- **Exemple de configuration lorsque keytab est utilisé :** `add kcdaccount lbvs_keytab_aes256 -keytab "/nsconfig/krb/kcd2_aes256.keytab"`
- **Utilisez la commande suivante lorsque keytab possède plusieurs types de cryptage.** La commande capture également les paramètres utilisateur du domaine : `add kcdaccount lbvs_keytab_aes256 -keytab "/nsconfig/krb/kcd2_aes256.keytab"-domainUser "HTTP/lbvs.aaa.local"`
- **Utilisez les commandes suivantes lorsque les informations d'identification de l'utilisateur sont utilisées :** `add kcdaccount kslb2_user -realmStr AAA.LOCAL -delegatedUser lbvs -kcdPassword <password>`
- Assurez-vous que les informations **DomainUser** correctes sont fournies. Vous pouvez

> rechercher le nom d'ouverture de session de l'utilisateur dans AD.

Générer le script Keytab KCD

May 5, 2023

La boîte de dialogue KCD Keytab Script génère le script keytab, qui à son tour génère le fichier keytab nécessaire pour configurer KCD sur NetScaler.

Pour générer le script keytab KCD à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications.**
2. Dans le volet de détails, sous **Délégation contrainte Kerberos**, cliquez sur Fichier batch pour générer un keytab.
3. Dans la boîte de dialogue Generate KCD (Kerberos Constrained Delegation) **Keytab Script**, renseignez les champs comme décrit ci-dessous.
   - **Nom d'utilisateur du domaine :** nom de l'utilisateur du domaine.
   - **Mot de passe du domaine :** mot de passe de l'utilisateur du domaine.
   - **Principal de service :** Le principal de service.
   - **Nom du fichier de sortie : nom** de fichier pour le fichier de script KCD.
   - **Créer un compte utilisateur de domaine :** cochez cette case pour créer le compte utilisateur de domaine spécifié.
4. Cliquez sur **Générer un script** pour générer le script. Le script est généré et apparaît dans la zone de texte **Script généré** sous le bouton **Générer le script** .
5. Copiez le script et enregistrez-le sous forme de fichier sur votre contrôleur de domaine AD. Vous devez maintenant exécuter ce script sur le contrôleur de domaine pour générer le fichier keytab, puis copier le fichier keytab dans le répertoire /nsconfig/krb/ de l'appliance NetScaler.
6. Cliquez sur **OK.**

SSO pour les authentifications Basic, Digest et NTLM

May 5, 2023

La configuration de l'authentification unique (SSO) dans NetScaler et NetScaler Gateway peut être activée au niveau global et également par niveau de trafic. Par défaut, la configuration SSO est **désactivée** et un administrateur peut activer le SSO par trafic ou globalement. Du point de vue de la sécurité, Citrix recommande aux administrateurs de **désactiver** globalement le SSO et de l'activer par

trafic. Cette amélioration vise à rendre la configuration SSO plus sécurisée en déshonorant certains types de méthodes SSO à l'échelle mondiale.

> **Remarque :**
>
> à partir de la version 13.0 de la fonctionnalité NetScaler build 64.35 et versions ultérieures, les types de SSO suivants ne sont pas respectés à l'échelle mondiale.
>
> - Authentification basique
> - Authentification Digest Access
> - NTLM sans négociation, clé NTLM2 ou signe de négociation

Types de SSO non impactés

Les types de SSO suivants ne sont pas concernés par cette amélioration.

- Authentification Kerberos
- Authentification SAML
- Authentification par formulaire
- Authentification du porteur OAuth
- NTLM avec clé Negotiate NTLM2 ou signe de négociation

Configurations SSO affectées

Voici les configurations SSO impactées (non honorées).

Configurations globales

```
set tmsessionparam -SSO ON
set vpnparameter -SSO ON
add tmsessionaction tm_act -SSO ON
add vpn sessionaction tm_act -SSO ON
<!--NeedCopy-->
```

Configurations par trafic

```
add vpn trafficaction tf_act http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```


> Vous pouvez activer/désactiver l'option SSO dans son ensemble et ne pouvez pas modifier les types d'SSO individuels.

Mesures de sécurité à appliquer

Dans le cadre des mesures de sécurité, les types SSO sensibles à la sécurité ne sont pas respectés dans la configuration globale mais ne sont autorisés que par le biais d'une configuration Traffic Action. Ainsi, si un serveur principal attend Basic, Digest ou NTLM sans clé Negotiate NTLM2 ni Negotiate Sign, l'administrateur ne peut autoriser l'authentification unique que par le biais de la configuration suivante.

Action en matière de circulation

```
add vpn trafficaction tf_act  http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```

Stratégie de trafic

```
add tm trafficpolicy <name> <rule> tf_act
add vpn trafficpolicy <name> <rule> tf-act
<!--NeedCopy-->
```

> L'administrateur doit configurer une règle appropriée pour la politique de trafic afin de s'assurer que le SSO est activé uniquement pour le serveur principal de confiance.

AAA-TM

Scénarios basés sur la configuration globale :

```
set tmsessionparam -SSO ON
<!--NeedCopy-->
```

Solution :

```
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol true tf_act
<!--NeedCopy-->
```

Liez la politique de trafic suivante à tous les serveurs virtuels LB sur lesquels le SSO est attendu :


```
bind lb vserver <LB VS Name> -policy tf_pol -priority 65345
<!--NeedCopy-->
```

Scénarios basés sur la configuration de stratégie de session :

```
add tmsessionaction tm_act -SSO ON
add tmsession policy <name> <rule> tm_act
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol <same rule as session Policy> tf_act
<!--NeedCopy-->
```

Points à noter :

- L'utilisateur/le groupe NetScaler AAA pour la session précédente doit être remplacé par une politique de trafic.
- Liez la politique suivante aux serveurs virtuels d'équilibrage de charge pour la politique de session précédente,

```
bind lb vserver [LB VS Name] -policy tf_pol -priority 65345
<!--NeedCopy-->
```

- Si une politique de trafic avec une autre priorité est configurée, la commande précédente ne fonctionne pas correctement.

La section suivante traite des scénarios basés sur un conflit avec plusieurs politiques de trafic associées à un trafic :

Pour un trafic TM particulier, une seule politique de trafic TM est appliquée. En raison de la configuration globale des modifications des fonctionnalités SSO, l'application d'une politique de trafic TM supplémentaire de faible priorité peut ne pas être applicable dans le cas où une politique de trafic TM à priorité élevée (qui ne nécessite pas de configuration SSO) est déjà appliquée. La section suivante décrit la méthode permettant de s'assurer que de tels cas sont traités.

Sachez que les trois politiques de trafic suivantes avec une priorité plus élevée sont appliquées au serveur virtuel d'équilibrage de charge (LB) :

```
add tm trafficaction tf_act1 <Addition config>
add tm trafficaction tf_act2 <Addition config>
add tm trafficaction tf_act3 <Addition config>

add tm trafficpolicy tf_pol1 <rule1> tf_act1
add tm trafficpolicy tf_pol2 <rule2> tf_act2
add tm trafficpolicy tf_pol3 <rule3> tf_act3

bind lb vserver <LB VS Name> -policy tf_pol1 -priority 100
```



```
bind lb vserver <LB VS Name> -policy tf_pol2 -priority 200
bind lb vserver <LB VS Name> -policy tf_pol3 -priority 300
<!--NeedCopy-->
```

Méthode sujette aux erreurs - Pour résoudre la configuration SSO globale, vous ajoutez la configuration suivante :

```
add tm trafficaction tf_act_default -SSO ON
add tm trafficpolicy tf_pol_default true tf_act_default

bind lb vserver <LB VS Name> -policy tf_pol_default -priority 65345
<!--NeedCopy-->
```

Remarque : La modification précédente peut rompre l'authentification unique pour le trafic qui touche <tf_pol1/tf_pol2/tf_pol3> comme pour ce trafic, stratégie de trafic n'est pas appliqué.

Méthode correcte - Pour atténuer ce problème, la propriété SSO doit être appliquée individuellement pour chacune des actions de trafic correspondantes :

Par exemple, dans le scénario précédent, pour que l'authentification unique se produise pour le trafic touchant tf_pol1/tf_pol3, la configuration suivante doit être appliquée avec .

```
add tm trafficaction tf_act1 <Addition config> -SSO ON
add tm trafficaction tf_act3 <Addition config> -SSO ON
<!--NeedCopy-->
```

Boîtiers NetScaler Gateway

Scénarios basés sur la configuration globale :

```
set vpnparameter -SSO ON
<!--NeedCopy-->
```

Solution :

```
add vpn trafficaction vpn_tf_act http  -SSO ON
add vpn trafficpolicy vpn_tf_pol  true vpn_tf_act
bind the following traffic policy to all VPN virtual server where SSO
    is expected:
bind vpn vserver vpn_vs -policy vpn_tf_pol -priority 65345
<!--NeedCopy-->
```

Scénarios basés sur la configuration de stratégie de session :


```
add vpn sessionaction vpn_sess_act -SSO ON
add vpnsession policy <name> <rule> vpn_sess_act
<!--NeedCopy-->
```

Points à noter :

- L'utilisateur/le groupe NetScaler AAA pour la session précédente doit être remplacé par une politique de trafic.
- Liez la politique suivante aux serveurs virtuels LB pour la politique de session précédente, `bind lb virtual server [LB VS Name] -policy tf_pol -priority 65345`.
- Si une politique de trafic avec une autre priorité est configurée, la commande précédente ne fonctionne pas correctement. La section suivante traite des scénarios basés sur un conflit avec plusieurs politiques de trafic associées au trafic.

Scénarios fonctionnels basés sur un conflit avec plusieurs politiques de trafic associées à un trafic :

Pour un trafic NetScaler Gateway spécifique, une seule politique de trafic VPN est appliquée. En raison du paramétrage global des modifications des fonctionnalités SSO, l'application d'une politique de trafic VPN supplémentaire avec une faible priorité peut ne pas être applicable s'il existe d'autres politiques de trafic VPN avec une priorité élevée qui n'ont pas de configuration SSO requise.

La section suivante décrit la méthode permettant de s'assurer que de tels cas sont traités :

Supposons qu'il existe trois politiques de trafic avec une priorité plus élevée appliquées à un serveur virtuel VPN :

```
add vpn trafficaction tf_act1 <Addition config>
add vpn trafficaction tf_act2 <Addition config>
add vpn trafficaction tf_act3 <Addition config>

add vpn trafficpolicy tf_pol1 <rule1> tf_act1
add vpn trafficpolicy tf_pol2 <rule2> tf_act2
add vpn trafficpolicy tf_pol3 <rule3> tf_act3

bind vpn vserver <VPN VS Name> -policy tf_pol1 -priority 100
bind vpn vserver <VPN VS Name> -policy tf_pol2 -priority 200
bind vpn vserver <VPN VS Name> -policy tf_pol3 -priority 300
<!--NeedCopy-->
```

Méthode sujette aux erreurs : Pour résoudre la configuration SSO globale, vous ajoutez la configuration suivante :

```
add vpn trafficaction tf_act_default -SSO ON
```



```
add vpn trafficpolicy tf_pol_default true tf_act_default

bind vpn vserver <VPN VS Name> -policy tf_pol_default -priority 65345
<!--NeedCopy-->
```

Remarque : La modification précédente peut rompre l'authentification unique pour le trafic qui atteint, <tf_pol1/tf_pol2/tf_pol3> comme pour ce trafic, stratégie de trafic n'est pas appliqué.

Méthode correcte : pour atténuer ce problème, la propriété SSO doit être appliquée individuellement pour chacune des actions de trafic correspondantes.

Par exemple, dans le scénario précédent, pour que l'authentification unique se produise pour le trafic touchant tf_pol1/tf_pol3, la configuration suivante doit être appliquée avec .

```
add vpn trafficaction tf_act1 [Additional config] -SSO ON

add vpn trafficaction tf_act3 [Additional config] -SSO ON
<!--NeedCopy-->
```

Réécriture pour NetScaler Gateway et les réponses générées par le serveur d'authentification

July 12, 2023

La réécriture fait référence à la réécriture de certaines informations contenues dans les demandes ou les réponses gérées par l'appliance NetScaler. La réécriture peut aider à fournir un accès au contenu demandé sans exposer de détails inutiles sur la configuration réelle du site Web. Pour obtenir des informations détaillées sur le concept de réécriture, voir Réécriture.

À partir de la version 13.0-76.29 de NetScaler, la prise en charge des stratégies de réécriture a été étendue au serveur virtuel NetScaler Gateway et aux réponses générées par le serveur virtuel d'authentification.

> **Remarque**
>
> Un type de liaison **AAA_Response** est introduit pour prendre en charge les stratégies de réécriture pour le serveur virtuel NetScaler Gateway et les réponses générées par le serveur virtuel d'authentification.

Exemple d'utilisation de Rewrite

Vous pouvez utiliser Rewrite pour partager les ressources disponibles sur le déploiement local de NetScaler avec Citrix Cloud. Cela peut être atteint en toute sécurité en implémentant le partage des

ressources d'origine CORS. La réécriture peut être utilisée comme suit pour implémenter l'en-tête CORS.

Exemple de configuration

```
add rewrite action cors_header_action insert_http_header access-control-allow-credentials \"true\"

add rewrite policy cors_header_pol true cors_header_action

add rewrite action non_cors_header_action insert_http_header X-Frame-Options \'\"DENY\"\'

add rewrite policy non_cors_header_pol true non_cors_header_action

bind authentication vserver av_cors -policy cors_header_pol -priority 100 -type AAA_RESPONSE

bind vpn vserver av_cors -policy cors_header_pol -priority 100 -type AAA_RESPONSE
```

> **Remarque :**
>
> Pour obtenir des instructions sur la configuration d'une action et d'une stratégie de réécriture à l'aide de l'interface graphique, reportez-vous à la section Réécriture.

Prise en charge des en-têtes de réponse de la stratégie de sécurité du contenu pour NetScaler Gateway et authentification des réponses générées par le serveur virtuel

July 12, 2023

À partir des versions 13.0-76.29 de NetScaler, l'en-tête de réponse Content-Security-Policy (CSP) est pris en charge pour NetScaler Gateway et les réponses générées par le serveur virtuel d'authentification.

L'en-tête de réponse Content-Security-Policy (CSP) est une combinaison de stratégies que le navigateur utilise pour éviter les attaques par script intersite (CSS).
L'en-tête de réponse HTTP CSP permet aux administrateurs de sites Web de contrôler les ressources que l'agent utilisateur est autorisé à charger pour une page donnée. À quelques exceptions près, les

stratégies impliquent principalement la spécification des origines du serveur et des points de terminaison de script. Cela permet de se prémunir contre les attaques de scripts intersites.
L'en-tête CSP est conçu pour modifier la façon dont les navigateurs affichent les pages, et donc pour protéger contre diverses injections intersites, y compris le CSS. Il est important de définir correctement la valeur de l'en-tête, de manière à ne pas empêcher le bon fonctionnement du site Web. Par exemple, si l'en-tête est défini pour empêcher l'exécution de JavaScript en ligne, le site Web ne doit pas utiliser de JavaScript en ligne dans ses pages.

Voici les avantages de l'en-tête de réponse CSP.

- La fonction principale d'un en-tête de réponse CSP est de prévenir les attaques CSS.
- En plus de restreindre les domaines à partir desquels le contenu peut être chargé, le serveur peut spécifier quels protocoles peuvent être utilisés. Par exemple (et idéalement, du point de vue de la sécurité), un serveur peut spécifier que tous les contenus doivent être chargés à l'aide de HTTPS.
- CSP aide à protéger NetScaler contre les attaques par script intersites en sécurisant des fichiers tels que « tmindex.html » et « homepage.html ». Le fichier « tmindex.html » est lié à l'authentification et le fichier « homepage.html » est lié aux applications/liens publiés.

Configuration de l'en-tête Content-Security-Policy pour NetScaler Gateway et des réponses d'authentification générées par le serveur virtuel

Pour activer l'en-tête CSP, vous devez configurer votre serveur Web pour qu'il renvoie l'en-tête HTTP du CSP.

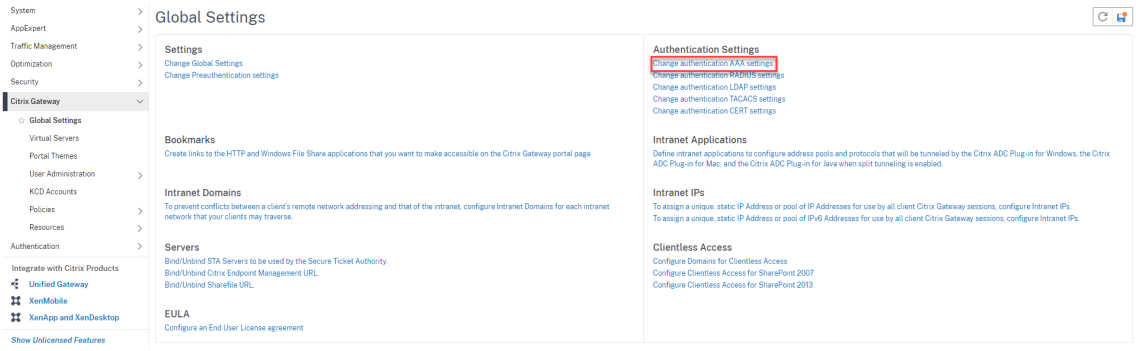
> **Points à noter**
>
> - Par défaut, l'en-tête CSP est désactivé.
> - Lors de l'activation ou de la désactivation de la stratégie CSP par défaut, il est recommandé d'exécuter la commande suivante. `Flush cache contentgroup loginstaticobjects`
> - Pour modifier le CSP pour /logon/LogonPoint/index.html, modifiez la valeur « Header set Content-Security-Policy » comme indiqué dans la section correspondant au répertoire de connexion qui se trouve sous le répertoire `/var/netscaler/logon`.
> - Pour obtenir des instructions sur la configuration d'une action et d'une stratégie de réécriture à l'aide de l'interface graphique, reportez-vous à la section Réécriture.

Pour configurer le CSP pour l'authentification du serveur virtuel et les réponses générées par NetScaler Gateway à l'aide de l'interface de ligne de commande, tapez la commande suivante à l'invite de commandes :

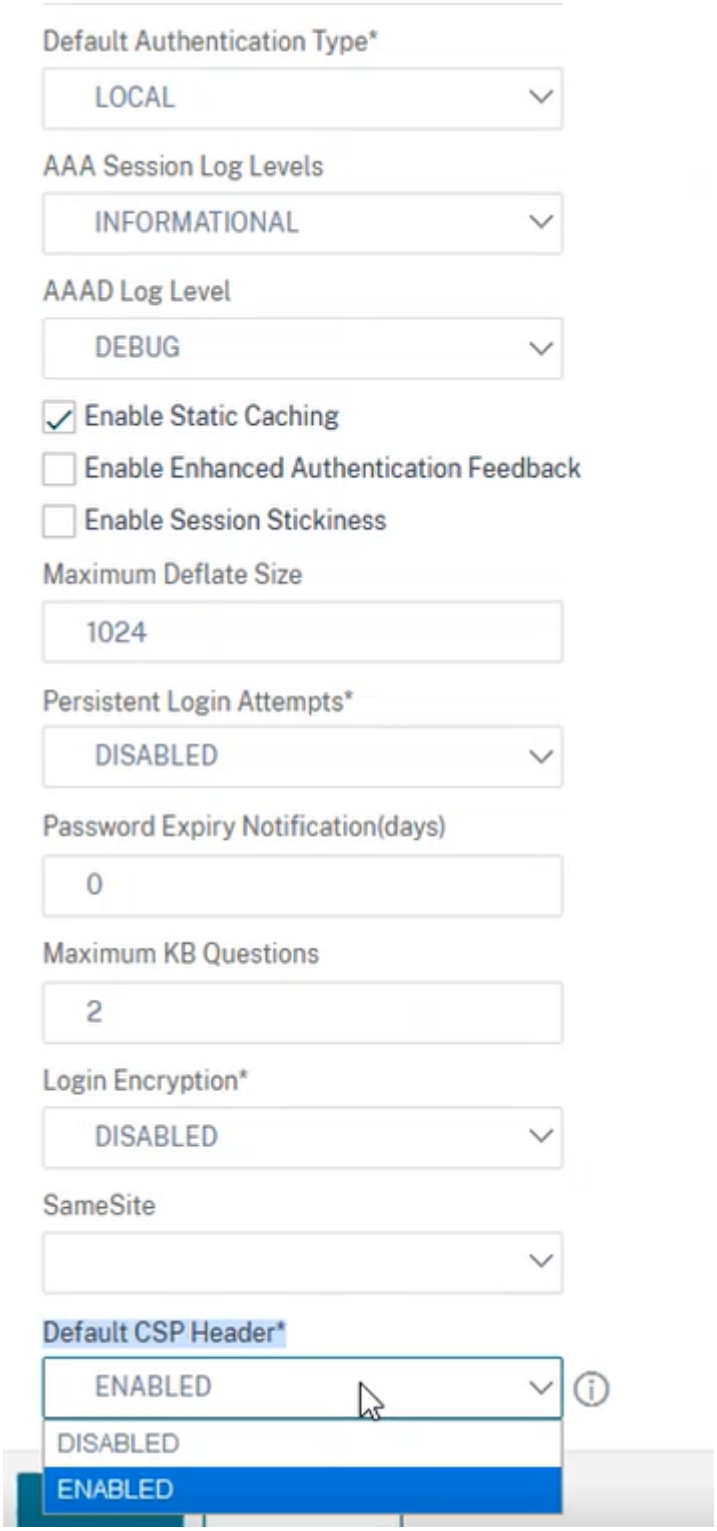
```
1 set aaa parameter -defaultCSPHeader <ENABLE/DISABLE>
```


Pour configurer le CSP pour NetScaler Gateway et authentifier les réponses générées par le serveur virtuel à l'aide de l'interface graphique.

1. Accédez à **NetScaler Gateway > Paramètres généraux**, puis cliquez sur **Modifier les paramètres d'authentification AAA sous Paramètres** d'authentification.



2. Sur la page **Configurer les paramètres AAA**, sélectionnez le **champ En-tête CSP par défaut** .



Exemple de personnalisation des en-têtes Content-Security-Policy

Voici un exemple de personnalisation des en-têtes CSP pour inclure des images et des scripts uniquement provenant des deux sources spécifiées suivantes, respectivement, `https://company.fqdn.com, https://example.com.`

Exemple de configuration

```
add rewrite action modify_csp insert_http_header Content-Security-Policy "\"default-src 'self'; script-src 'self' https://company.fqdn.com 'unsafe-inline' 'unsafe-eval'; connect-src 'self'; img-src http://localhost:* https://example.com 'self' data: http: https:; style-src 'self' 'unsafe-inline'; font-src 'self'; frame-src 'self'; child-src 'self' com.citrix.agmacepa://* citrixng://* com.citrix.nsgclient://*; form-action 'self'; object-src 'self'; report-uri /nscsp_violation/report_uri\""

add rewrite policy add_csp true modify_csp

bind authentication vserver auth1 -policy add_csp -priority 1 -gotoPriorityExpression NEXT -type AAA_RESPONSE
```

Réinitialisation du mot de passe

July 18, 2023

La réinitialisation en libre-service des mots de passe est une solution Web de gestion des mots de passe Il est disponible à la fois dans les fonctionnalités d'authentification, d'autorisation et d'audit de l'appliance NetScaler et de NetScaler Gateway. Il élimine la dépendance de l'utilisateur à l'égard de l'assistance de l'administrateur pour changer le mot de passe.

La réinitialisation en libre-service du mot de passe permet à l'utilisateur final de réinitialiser ou de créer un mot de passe en toute sécurité dans les scénarios suivants :

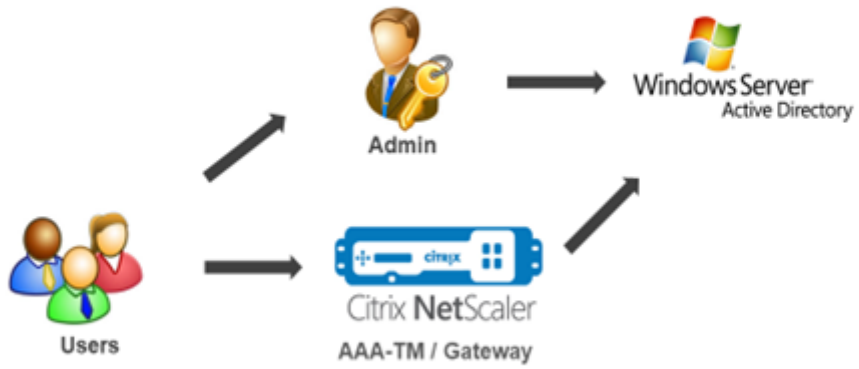
- L'utilisateur a oublié le mot de passe.
- L'utilisateur n'est pas en mesure de se connecter.

Jusqu'à présent, si un utilisateur final oublie un mot de passe AD, il devait contacter l'administrateur AD pour réinitialiser le mot de passe. Grâce à la fonctionnalité de réinitialisation du mot de passe en libre-service, un utilisateur final peut réinitialiser le mot de passe sans intervention de l'administrateur.

Voici certains des avantages de l'utilisation de la réinitialisation en libre-service des mots de passe :

- Productivité accrue grâce au mécanisme automatique de changement de mot de passe, qui élimine le délai d'attente des utilisateurs pour la réinitialisation du mot de passe.
- Grâce au mécanisme de modification automatique des mots de passe, les administrateurs peuvent se concentrer sur d'autres tâches critiques.

La figure suivante illustre le processus de réinitialisation du mot de passe en libre-service pour réinitialiser le mot de passe.



Pour utiliser la réinitialisation du mot de passe en libre-service, un utilisateur doit être enregistré auprès du service d'authentification, d'autorisation et d'audit NetScaler ou auprès du serveur virtuel NetScaler Gateway.

La réinitialisation en libre-service des mots de passe fournit les fonctionnalités suivantes :

- **Auto-enregistrement des nouveaux utilisateurs.** Vous pouvez vous inscrire vous-même en tant que nouvel utilisateur.
- **Configurez les questions basées sur les connaissances.** En tant qu'administrateur, vous pouvez configurer un ensemble de questions pour les utilisateurs.
- **Enregistrement d'un autre identifiant de messagerie.** Vous devez fournir un autre identifiant e-mail lors de l'inscription. L'OTP est envoyé à l'autre adresse e-mail car l'utilisateur a oublié le mot de passe de l'ID de messagerie principal.

  > **Remarque :**
  >
  > À partir de la version 12.1 build 51.xx, l'enregistrement d'un autre identifiant de messagerie peut être effectué de manière autonome. Un nouveau schéma de connexion, **AltEmailRegister.xml**, est introduit pour effectuer uniquement l'enregistrement d'un autre identifiant de messagerie. Auparavant, l'enregistrement d'un autre identifiant e-mail ne pouvait

> être effectué que lors de l'enregistrement KBA.

- **Réinitialisez le mot de passe oublié** L'utilisateur peut réinitialiser le mot de passe en répondant aux questions basées sur les connaissances. En tant qu'administrateur, vous pouvez configurer et stocker les questions.

La réinitialisation en libre-service du mot de passe fournit les deux nouveaux mécanismes d'authentification suivants :

- **Question et réponse basées sur les connaissances.** Vous devez vous inscrire à l'authentification, à l'autorisation et à l'audit NetScaler ou à NetScaler Gateway avant de sélectionner le schéma de questions-réponses basé sur les connaissances.
- **Authentification OTP par e-mail.** Un OTP est envoyé à l'autre adresse e-mail, que l'utilisateur a enregistrée lors de l'enregistrement de réinitialisation du mot de passe en libre-service.

> **Remarque**
>
> Ces mécanismes d'authentification peuvent être utilisés pour les cas d'utilisation de réinitialisation de mot de passe en libre-service, et à toutes fins d'authentification similaires à l'un des mécanismes d'authentification existants.

Pré-requis

Avant de configurer la réinitialisation en libre-service du mot de passe, vérifiez les conditions préalables suivantes :

- Fonctionnalité NetScaler version 12.1, build 50.28.
- La version prise en charge est le niveau de fonction du domaine AD 2016, 2012 et 2008.
- Le nom d'utilisateur LDAPbind lié à NetScaler doit disposer d'un accès en écriture au chemin AD de l'utilisateur.

  > **Remarque**
  > La réinitialisation du mot de passe en
  > libre-service est prise en charge dans le flux d'authentification nFactor uniquement. Pour plus d'informations, consultez la section Authentification nFactor via NetScaler.

Limitations

Voici certaines des limites de la réinitialisation en libre-service des mots de passe :

- La réinitialisation en libre-service des mots de passe est prise en charge sur LDAP La réinitialisation en libre-service des mots de passe n'est disponible que si le back-end d'authentification est LDAP (protocole LDAP).
- L'utilisateur ne peut pas voir l'autre adresse e-mail déjà enregistrée.

- Les questions et réponses basées sur les connaissances, ainsi que l'authentification et l'enregistrement OTP par e-mail ne peuvent pas être le premier facteur du flux d'authentification.
- Pour le plug-in natif et Receiver, l'enregistrement est pris en charge uniquement via le navigateur.
- La taille minimale du certificat utilisée pour la réinitialisation en libre-service des mots de passe est de 1 024 octets et doit respecter la norme x.509.
- Seul un certificat RSA est pris en charge pour la réinitialisation des mots de passe en libre-service.

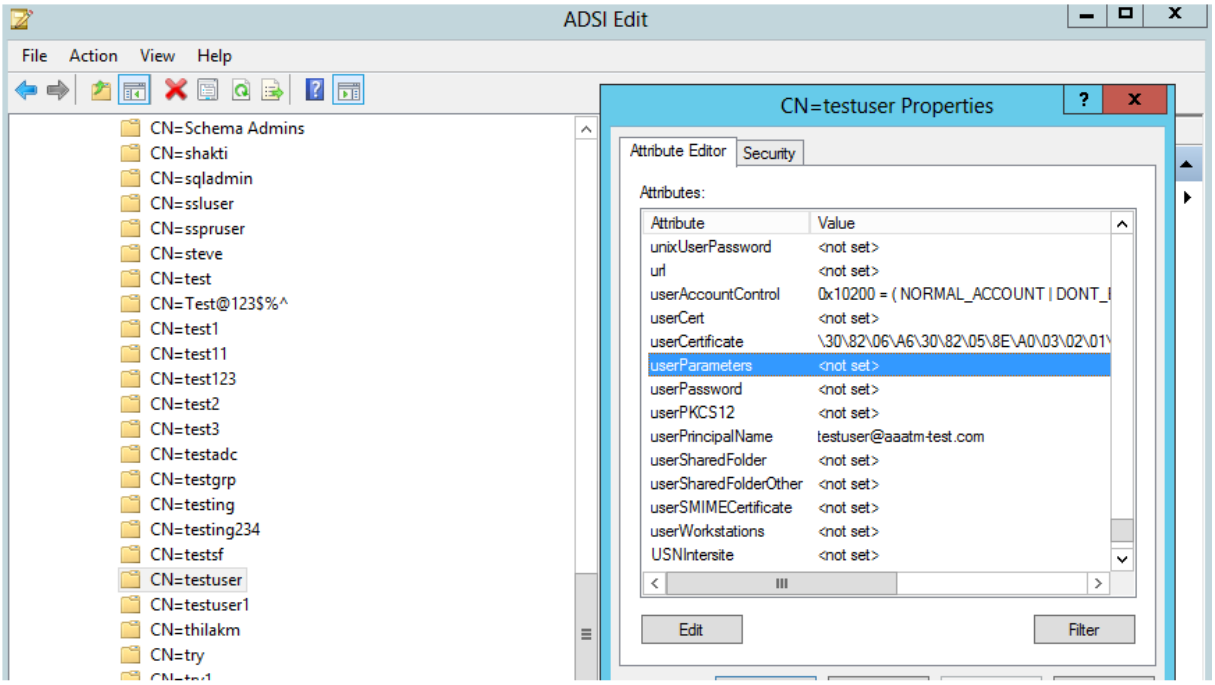
Paramètre Active Directory

L'OTP basé sur les connaissances et les e-mails de NetScaler utilise un attribut AD pour stocker les données des utilisateurs. Vous devez configurer un attribut AD pour stocker les questions et les réponses ainsi que l'autre ID d'e-mail. L'appliance NetScaler le stocke dans l'attribut KB configuré de l'objet utilisateur AD. Lors de la configuration d'un attribut AD, prenez en compte les points suivants :

- L'attribut AD doit prendre en charge une longueur maximale de 32 Ko.
- Le type d'attribut doit être un « DirectoryString ».
- Un seul attribut AD peut être utilisé pour les questions et réponses basées sur les connaissances et l'identifiant de messagerie secondaire.
- Un seul attribut AD ne peut pas être utilisé pour l'enregistrement d'un OTP natif et d'une question et réponse basées sur les connaissances ou d'un autre identifiant de messagerie.
- L'administrateur LDAP de NetScaler doit disposer d'un accès en écriture à l'attribut AD sélectionné.

Vous pouvez également utiliser un attribut AD existant. Cependant, assurez-vous que l'attribut que vous prévoyez d'utiliser n'est pas utilisé dans les autres cas. Par exemple, UserParameters est un attribut existant au sein de l'utilisateur AD que vous pouvez utiliser. Pour vérifier cet attribut, effectuez les opérations suivantes :

1. Accédez à **ADSI > sélectionnez un utilisateur**.
2. Cliquez avec le bouton droit de la souris et faites défiler l'écran
3. Dans le volet de fenêtre **CN=TestUser Properties**, vous pouvez voir que l'attribut **UserParameters** n'est pas défini.



Enregistrement en libre-service de réinitialisation du mot

Pour implémenter la solution de réinitialisation des mots de passe en libre-service sur une appliance NetScaler, vous devez effectuer les opérations suivantes :

- Enregistrement en libre-service pour la réinitialisation du mot de passe (question et réponse/identifiant e-mail basées sur les connaissances).
- Page d'ouverture de session de l'utilisateur (pour la réinitialisation du mot de passe, qui inclut la validation OTP par e-mail basée sur les connaissances et le facteur de réinitialisation du mot de passe final).

Un catalogue de questions prédéfinies est fourni sous forme de fichier JSON. En tant qu'administrateur, vous pouvez sélectionner les questions et créer le schéma de connexion en libre-service pour l'enregistrement de la réinitialisation du mot de passe via l'interface utilisateur graphique de NetScaler. Vous pouvez choisir l'une des options suivantes :

- Sélectionnez un maximum de quatre questions définies par le système.
- Offrez aux utilisateurs la possibilité de personnaliser deux questions et réponses.

Pour afficher le fichier JSON des questions basées sur les connaissances par défaut à partir de la CLI

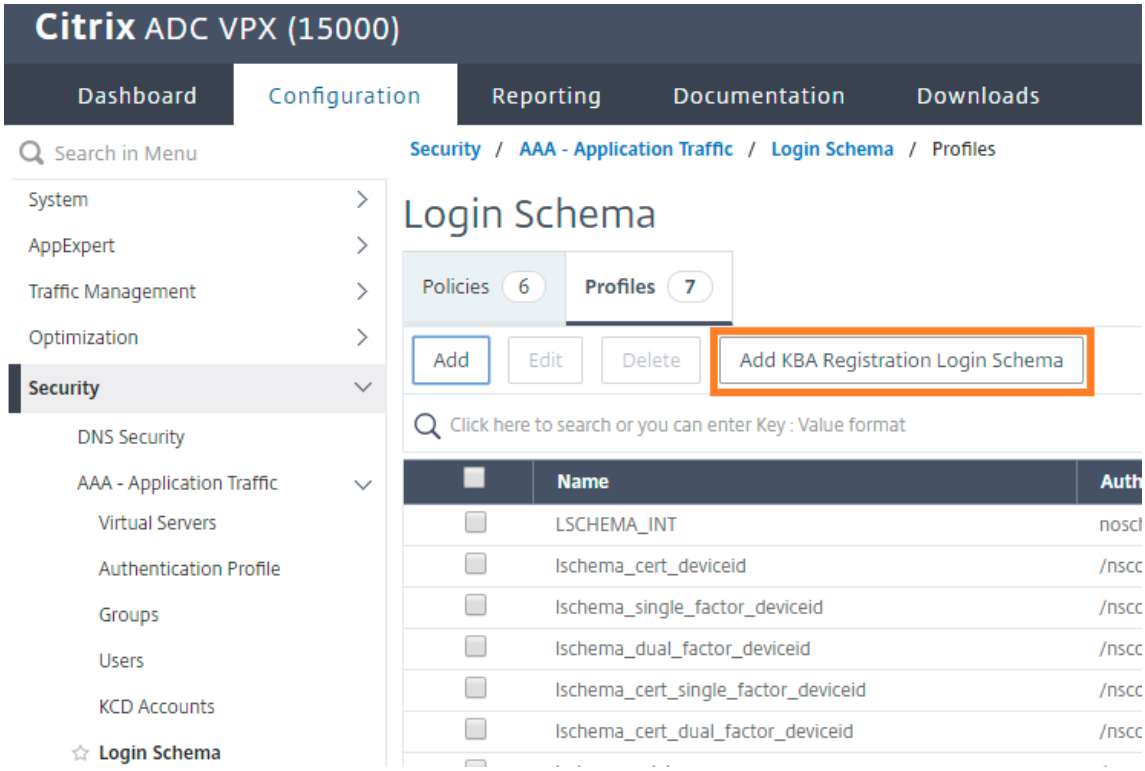
```
root@ns# cd /nsconfig/loginschema/LoginSchema/
root@ns# cat KBQuestions.json
[
    {"question":"What is the last name of the teacher who gave you your first failing
grade?"},
    {"question":"What is the name of your favourite childhood friend?"},
    {"question":"Where were you when you first heard about 9/11?"},
    {"question":"What is the name of a college you applied to but didn't attend?"},
    {"question":"What was the last name of your third grade teacher?"},
    {"question":"What was the name of your first stuffed animal?"},
    {"question":"What is the name of the teacher who gave you your first A?"},
    {"question":"What is the name of the city where you got lost?"},
    {"question":"In what city or town did your mother and father meet?"},
    {"question":"What was your most hated food as a child?"},
    {"question":"What was your most favourite food as a child?"},
    {"question":"What is your favourite website?"},
    {"question":"What is your most disliked website?"},
    {"question":"What is your dream job?"},
    {"question":"Why did the chicken cross the road?"},
    {"question":"Name your first boss."},
    {"question":"What is the name of your favorite school teacher?"},
    {"question":"What is the name of your favorite actor or actress?"},
    {"question":"What is the title of your favorite movie?"},
    {"question":"In what city or town did you spend most of your youth?"}
]
```

Remarque

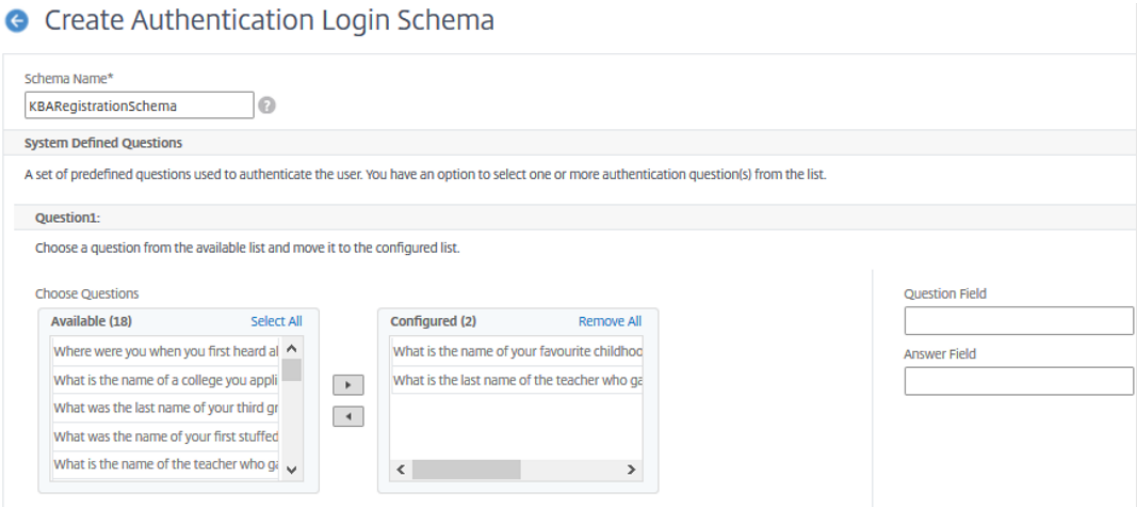
- NetScaler Gateway inclut l'ensemble de questions définies par le système par défaut. L'administrateur peut modifier le fichier « KBQuestions.json » pour y inclure les questions de son choix.
- Les questions définies par le système s'affichent uniquement en anglais et la prise en charge de la localisation linguistique n'est pas disponible pour ces questions.

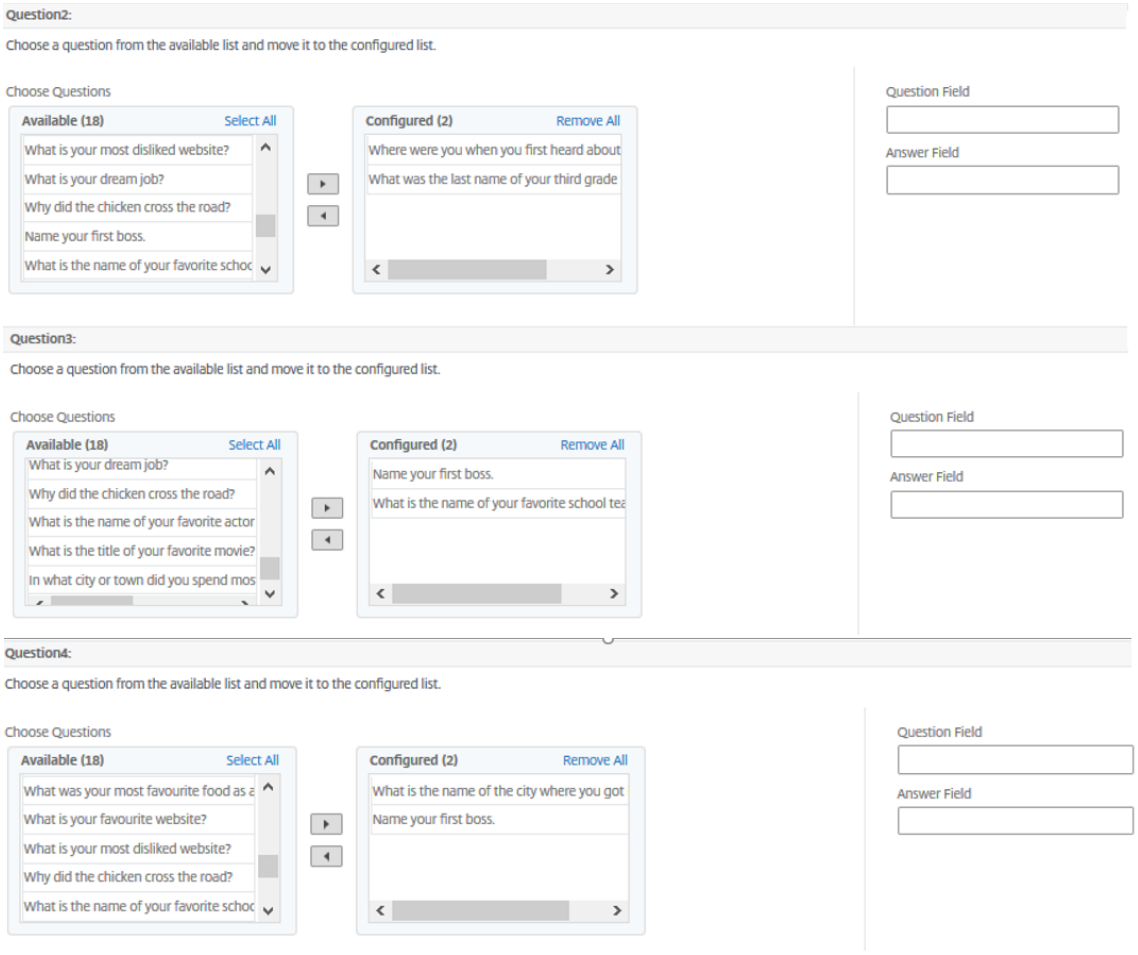
Pour terminer l'enregistrement des questions et réponses basées sur les connaissances Schéma de connexion à l'aide de

1. Accédez à **Sécurité > AAA — Trafic des applications > Schéma de connexion**.

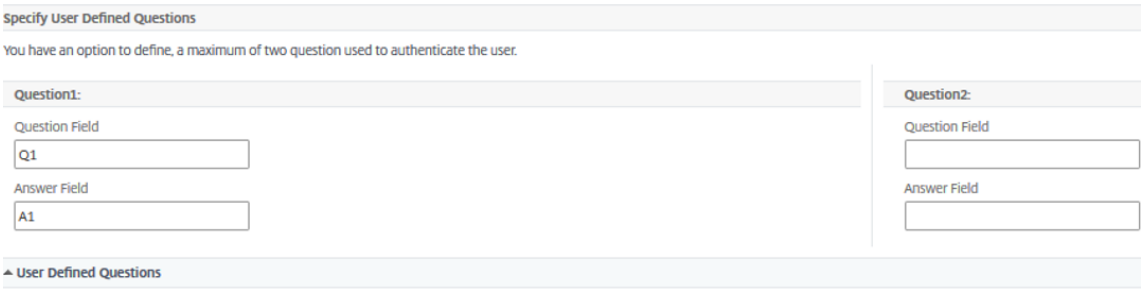


2. Sur la page **Schéma de connexion**, cliquez sur **Profils**.
3. Cliquez sur **Ajouter un schéma de connexion d'enregistrement KBA**.
4. Sur la page **Créer un schéma de connexion d'authentification**, spécifiez un nom dans le champ **Nom du schéma** .

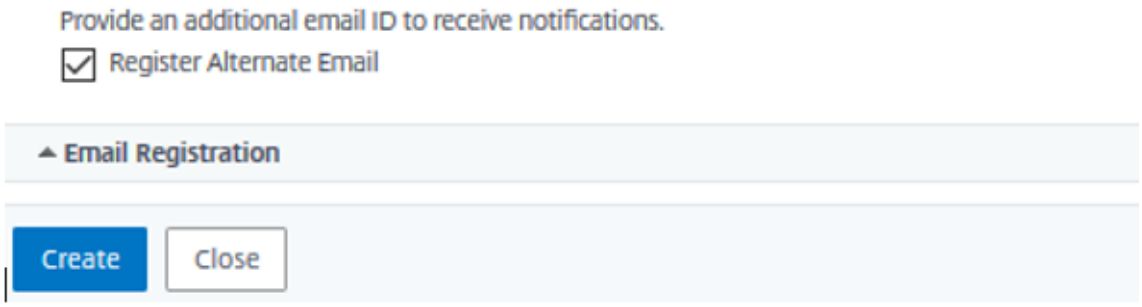




5. Sélectionnez les questions de votre choix et déplacez-les dans la liste **Configuré** .
6. Dans la section **Questions définies par l'utilisateur**, vous pouvez fournir des questions et des réponses dans les champs Q1 et A1.



7. Dans la section **Enregistrement par e-mail**, cochez l'option **Enregistrer un autre e-mail** . Vous pouvez enregistrer l' **ID e-mail alternatif** à partir de la page d'ouverture de session d'enregistrement de l'utilisateur pour recevoir l'OTP.



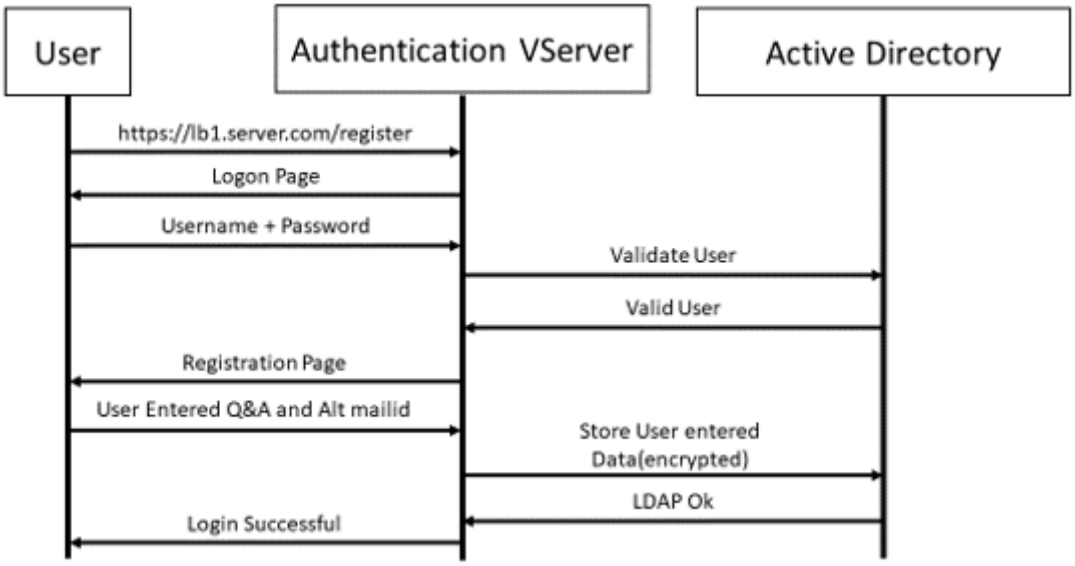
8. Cliquez sur **Create**. Le schéma de connexion une fois généré affiche toutes les questions configurées à l'utilisateur final pendant le processus d'inscription.

Création d'un flux de travail d'enregistrement et de gestion des utilisateurs

Les éléments suivants sont requis avant de commencer la configuration :

- Adresse IP attribuée au serveur virtuel d'authentification
- FQDN correspondant à l'adresse IP attribuée
- Certificat de serveur pour serveur virtuel d'authentification

Pour configurer la page d'enregistrement et de gestion des appareils, vous avez besoin d'un serveur virtuel d'authentification. La figure suivante illustre l'enregistrement de l'utilisateur.



Pour créer un serveur virtuel d'authentification

1. Configurez un serveur virtuel d'authentification. Il doit être de type SSL et assurez-vous de lier l'authentification serveur virtuel avec le thème du portail.


```
> add authentication vserver <vServerName> SSL <ipaddress> <port>
> bind authentication vserver <vServerName> [-portaltheme<string>]
```

2. Liez la paire de clés de certificat du serveur virtuel SSL.

```
> bind ssl vserver <vServerName> certkeyName <string>
```

Exemple :

```
> add authentication vserver authvs SSL 1.2.3.4 443
> bind authentication vserver authvs -portaltheme RFWebUI
> bind ssl vserver authvs -certkeyname c1
```

Pour créer une action d'ouverture de session LDAP

```
    > add authentication ldapAction <name> {
-serverIP <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE> ]
    [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
ldapLoginName <USER FORMAT>]
```

> **Remarque**
>
> Vous pouvez configurer n'importe quelle stratégie d'authentification en tant que premier facteur.

Exemple :

```
    > add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4
     -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
    ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
    PASSWORD -ldapLoginName samAccountName -serverport 636 -sectype
    SSL -KBAttribute userParameters
```

Pour créer une stratégie d'authentification pour l'ouverture de session LDAP

```
    > add authentication policy <name> <rule> [<reqAction]
```

Exemple :

```
    > add authentication policy ldap_logon -rule true -action
      ldap_logon_action
```


Pour créer une action d'enregistrement de questions et réponses basée sur les connaissances

Deux nouveaux paramètres sont introduits dans `ldapAction`. `KBAttribute` pour l'authentification KBA (enregistrement et validation) et `alternateEmailAttr` pour l'enregistrement de l'autre adresse e-mail de l'utilisateur.

```
1      > add authentication ldapAction <name> {
2   -serverIP  <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE>
       ] [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
       ldapLoginName <USER FORMAT>] [-KBAttribute <LDAP ATTRIBUTE>] [-
       alternateEmailAttr <LDAP ATTRIBUTE>]
```

Exemple :

```
1      > add authentication ldapAction ldap1 -serverIP 1.2.3.4 -sectype
          ssl -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
          ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
          PASSWORD -ldapLoginName samAccountName -KBAttribute
          userParameters -alternateEmailAttr userParameters
```

Afficher l'écran d'enregistrement et de gestion des utilisateurs

Le schéma de connexion "KBARegistrationSchema.xml" est utilisé pour afficher la page d'enregistrement de l'utilisateur à l'utilisateur final. Utilisez l'interface de ligne de commande suivante pour afficher le schéma de connexion.

```
1  > add authentication loginSchema <name> -authenticationSchema <string>
```

Exemple :

```
1  > add authentication loginSchema kba_register -authenticationSchema /
       nsconfig/loginschema/LoginSchema/KBARegistrationSchema.xml
```

Citrix recommande deux façons d'afficher l'écran d'enregistrement et de gestion des utilisateurs : URL ou attribut LDAP.

Utilisation de l'URL

Si le chemin d'accès de l'URL contient « /register » (par exemple, https://lb1.server.com/register), la page d'enregistrement de l'utilisateur s'affiche à l'aide de l'URL.

Pour créer et lier la stratégie d'enregistrement


```
> add authentication policylabel user_registration -loginSchema
   kba_register
> add authentication policy ldap1 -rule true -action ldap1
> bind authentication policylabel user_registration -policy ldap1 -
   priority 1
```

Pour lier la stratégie d'authentification à l'authentification, l'autorisation et l'audit du serveur virtuel lorsque l'URL contient '/register'

```
> add authentication policy ldap_logon -rule "http.req.cookie.value(\"
   NSC_TASS\").contains(\"register\")" -action ldap_logon
> bind authentication vserver authvs -policy ldap_logon -nextfactor
   user_registration -priority 1
```

Pour lier un certificat au VPN global

```
bind vpn global -userDataEncryptionKey c1
```

> **Remarque**
>
> - Vous devez lier le certificat pour chiffrer les données utilisateur (Q&R de la base de connaissances et autre ID e-mail enregistré) stockées dans l'attribut AD.
> - Si le certificat expire, vous devez lier un nouveau certificat et effectuer à nouveau l'enregistrement.

Utilisation de l'attribut

Vous pouvez lier une stratégie d'authentification au serveur virtuel d'authentification, d'autorisation et d'audit pour vérifier si l'utilisateur est déjà inscrit ou non. Dans ce flux, l'une des stratégies précédentes avant le facteur d'enregistrement des questions et réponses basé sur les connaissances doit être LDAP avec l'attribut KBA configuré. Ceci permet de vérifier si l'utilisateur AD est enregistré ou n'utilise pas un attribut AD.

> **Important**
>
> La règle "AAA.USER.ATTRIBUTE("kba_registered").EQ("0")" oblige les nouveaux utilisateurs à s'inscrire aux questions et réponses basées sur les connaissances et aux e-mails alternatifs.

Pour créer une stratégie d'authentification afin de vérifier si l'utilisateur n'est pas déjà inscrit


```
> add authentication policy switch_to_kba_register -rule "AAA.USER.
    ATTRIBUTE(\"kba_registered\").EQ(\"0\")" -action NO_AUTHN
> add authentication policy first_time_login_forced_kba_registration -
    rule true -action ldap1
```

Pour créer une étiquette de stratégie d'enregistrement et la lier à la stratégie d'enregistrement LDAP

```
> add authentication policylabel auth_or_switch_register -loginSchema
    LSCHEMA_INT
> add authentication policylabel kba_registration -loginSchema
    kba_register

> bind authentication policylabel auth_or_switch_register -policy
    switch_to_kba_register -priority 1 -nextFactor kba_registration
> bind authentication policylabel kba_registration -policy
    first_time_login_forced_kba_registration -priority 1
```

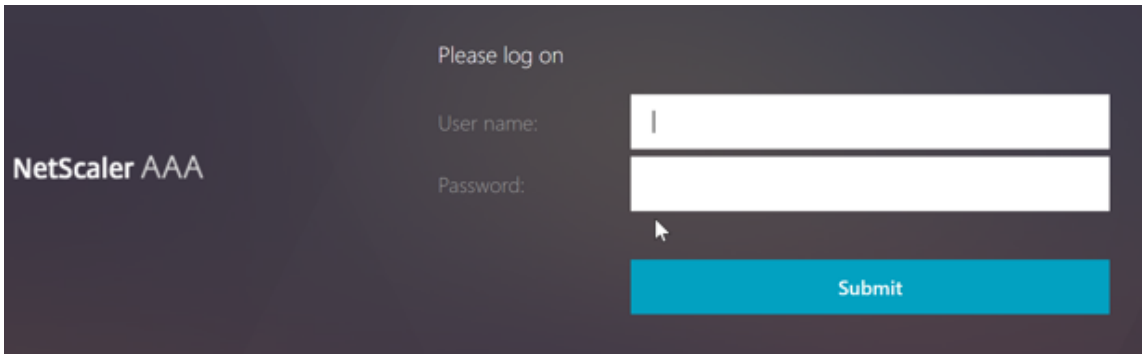
Pour lier la stratégie d'authentification à l'authentification, à l'autorisation et à l'audit du serveur virtuel

```
bind authentication vserver authvs -policy ldap_logon -nextfactor
    auth_or_switch_register -priority 2
```

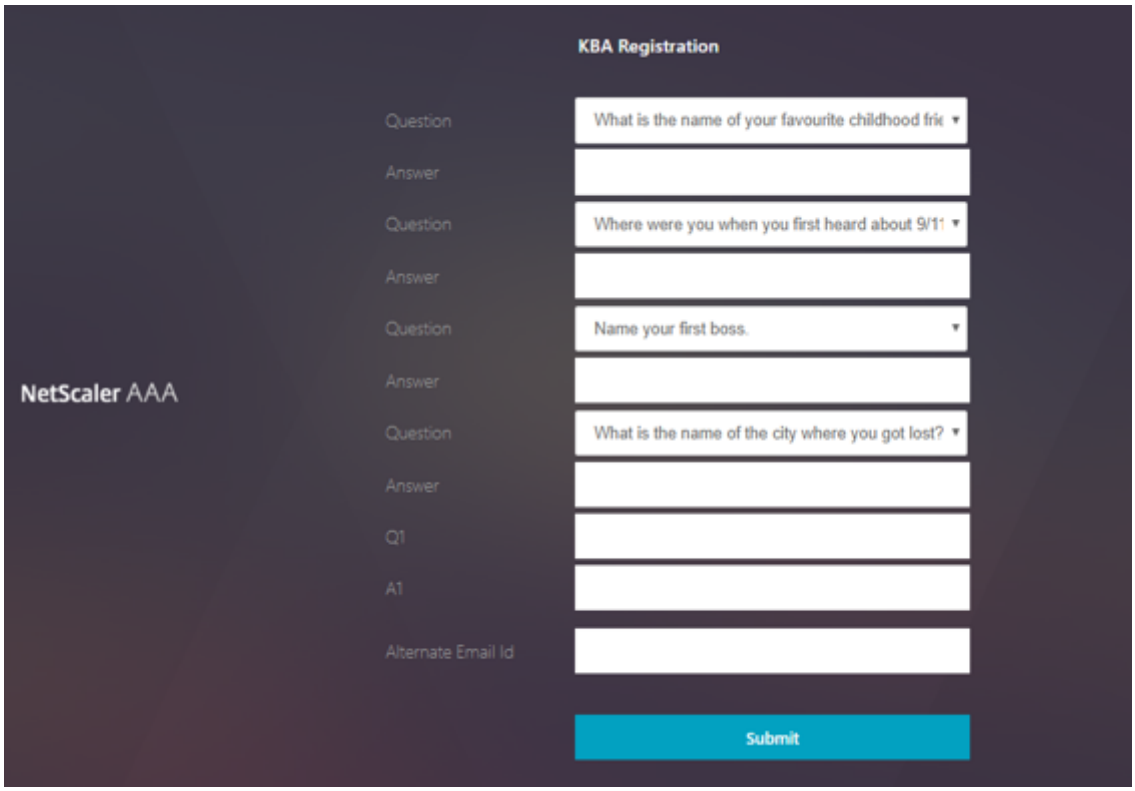
Enregistrement des utilisateurs et validation de la gestion

Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, vous devez voir l'écran d'interface utilisateur suivant.

1. Entrez l'URL du serveur virtuel lb ; par exemple, https://lb1.server.com. L'écran d'ouverture de session s'affiche.



2. Entrez le nom d'utilisateur et le mot de passe. Cliquez sur **Envoyer**. L'écran **Enregistrement de l'utilisateur** s'affiche.



3. Sélectionnez la question préférée dans la liste déroulante et saisissez la **réponse**.
4. Cliquez sur **Envoyer**. L'écran Enregistrement réussi de l'utilisateur s'affiche.

Page Configurer l'ouverture de session utilisateur

Dans cet exemple, l'administrateur suppose que le premier facteur est l'ouverture de session LDAP (pour laquelle l'utilisateur final a oublié le mot de passe). L'utilisateur suit ensuite l'enregistrement des questions et réponses basées sur les connaissances et la validation OTP de l'ID e-mail, puis réinitialise le mot de passe à l'aide de la réinitialisation en libre-service du mot de passe.

Vous pouvez utiliser n'importe quel mécanisme d'authentification pour la réinitialisation en libre-service du mot de passe. Citrix recommande d'avoir une question et une réponse basées sur les connaissances et un OTP par e-mail ou les deux pour garantir une confidentialité renforcée et éviter toute réinitialisation illégitime du mot de passe utilisateur.

Les éléments suivants sont requis avant de commencer à configurer la page d'ouverture de session utilisateur :

- Adresse IP pour le serveur virtuel d'équilibrage de charge
- Nom de domaine complet correspondant au serveur virtuel d'équilibrage de charge
- Certificat de serveur pour l'équilibreur de charge

Créer un serveur virtuel d'équilibrage de charge à l'aide de l'interface

Pour accéder au site Web interne, vous devez créer un serveur virtuel LB pour faire face au service principal et déléguer la logique d'authentification au serveur virtuel d'authentification.

```
> add lb vserver lb1 SSL 1.2.3.162 443 -persistenceType NONE -
   cltTimeout 180 -AuthenticationHost otpauth.server.com -
   Authentication ON -authnVsName authvs

> bind ssl vserver lb1 -certkeyname c1
```

Pour représenter le service principal dans l'équilibrage de charge :

```
> add service iis_backendsso_server_com 1.2.3.4 HTTP 80

> bind lb vserver lb1 iis_backendsso_server_com
```

Créer une action LDAP avec l'authentification désactivée en tant que première stratégie

```
> add authentication ldapAction ldap3 -serverIP 1.2.3.4 -serverPort 636
    -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
   administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
   ldapLoginName samAccountName -authentication disabled

> add authentication policy ldap3 -rule aaa.LOGIN.VALUE("passwdreset").
   EQ("1") -action ldap3
```

Créer une action de validation des questions et réponses basée sur les connaissances

Pour la validation des questions et réponses basée sur les connaissances dans le flux de réinitialisation en libre-service des mots de passe, vous devez configurer le serveur LDAP avec l'authentification désactivée.

```
> add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP
   > -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
   ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
   KBAttribute  <LDAP ATTRIBUTE> - alternateEmailAttr <LDAP ATTRIBUTE>
   -authentication DISABLED
```

Exemple :

```
> add authentication ldapAction ldap2 -serverIP 1.2.3.4 -serverPort 636
    -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
```



```
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName samAccountName -KBAttribute userParameters -
    alternateEmailAttr userParameters -authentication disabled
```

Pour créer une stratégie d'authentification pour la validation des questions et réponses basées sur les connaissances à l'aide de l'interface

```
1 add authentication policy kba_validation -rule true -action ldap2
```

Création d'une action de validation d'e-mail

LDAP doit être un facteur antérieur au facteur de validation de l'e-mail, car vous avez besoin de l'ID e-mail de l'utilisateur ou de l'autre adresse e-mail dans le cadre de l'enregistrement de réinitialisation en libre-service du mot de passe.

> **Remarque :**
>
> Pour que la solution OTP de messagerie fonctionne, assurez-vous que l'authentification basée sur la connexion est activée sur le serveur SMTP.

Pour vous assurer que l'authentification basée sur la connexion est activée, tapez la commande suivante sur le serveur SMTP. Si l'authentification basée sur la connexion est activée, vous remarquerez que le texte **AUTH LOGIN** apparaît en gras dans la sortie.

```
1 root@ns# telnet <IP address of the SMTP server><Port number of the
    server>
2 ehlo
```

Exemple :

```
1  root@ns# telnet 10.106.3.66 25
2  Trying 10.106.3.66...
3  Connected to 10.106.3.66.
4  Escape character is '^]'.
5  220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22
     Nov 2019 16:24:17 +0530
6  ehlo
7  250-E2K13.NSGSanity.com Hello [10.221.41.151]
8  250-SIZE 37748736
9  250-PIPELINING
10 250-DSN
11 250-ENHANCEDSTATUSCODES
12 250-STARTTLS
```



```
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
```

Pour plus d'informations sur l'activation de l'authentification basée sur la connexion, reportez-vous à la section https://support.microfocus.com/kb/doc.php?id=7020367.

Pour configurer une action de messagerie à l'aide de l'interface de ligne de commande

```
add authentication emailAction emailact -userName sender@example.com -
    password <Password> -serverURL "smtps://smtp.example.com:25" -
    content "OTP is $code"
```

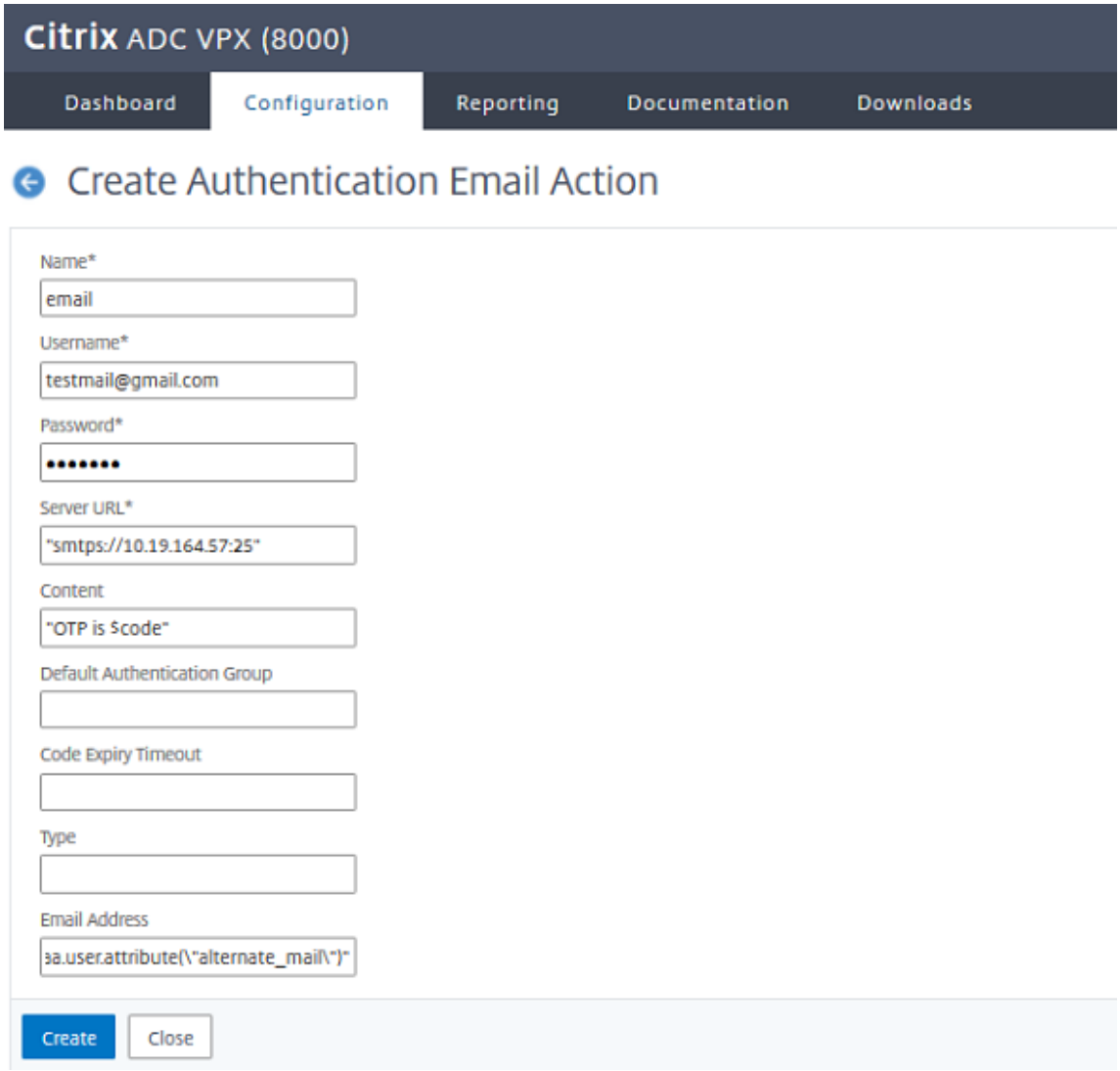
Exemple :

```
add authentication emailAction email -userName testmail@gmail.com -
    password 298
    a34b1a1b7626cd5902bbb416d04076e5ac4f357532e949db94c0534832670 -
    encrypted -encryptmethod ENCMTHD_3 -serverURL "smtps
    ://10.19.164.57:25" -content "OTP is $code" -emailAddress "aaa.user.
    attribute(\"alternate_mail\")"
```

> **Remarque**
>
> Le paramètre « EmailAddress » de la configuration est une expression PI. Par conséquent, il est configuré pour prendre soit l'ID e-mail de l'utilisateur par défaut de la session, soit l'autre ID e-mail déjà enregistré.

Pour configurer l'ID de messagerie à l'aide de

1. Accédez à **Sécurité > AAA — Trafic des applications > stratégies > Authentification > Stratégies avancées > Actions > Action d'authentification par e-mail**. Cliquez sur **Ajouter**.
2. Sur la page **Créer une action par e-mail d'authentification**, renseignez les détails, puis cliquez sur **Créer**.



Pour créer une stratégie d'authentification pour la validation des e-mails à l'aide de l'interface

```
add authentication policy email_validation -rule true -action email
```

Pour créer une stratégie d'authentification pour le facteur de réinitialisation du mot de

```
add authentication policy ldap_pwd -rule true -action ldap_logon_action
```

Présentation de l'interface utilisateur via le schéma de connexion

Il existe trois schémas de connexion pour la réinitialisation du mot de passe en libre-service afin de réinitialiser le mot de passe. Utilisez les commandes CLI suivantes pour afficher les trois schémas de

connexion :

```
root@ns# cd  /nsconfig/loginschema/LoginSchema/
root@ns# ls -ltr | grep -i password
-r--r--r--  1 nobody  wheel  2088 Nov 13 08:38
   SingleAuthPasswordResetRem.xml
-r--r--r--  1 nobody  wheel  1541 Nov 13 08:38
   OnlyUsernamePasswordReset.xml
-r--r--r--  1 nobody  wheel  1391 Nov 13 08:38 OnlyPassword.xml
```

Pour créer une réinitialisation de mot de passe d'authentification unique à l'aide de l'interface de ligne de commande

```
> add authentication loginSchema lschema_password_reset -
   authenticationSchema "/nsconfig/loginschema/LoginSchema/
   SingleAuthPasswordResetRem.xml"

> add authentication loginSchemaPolicy lpol_password_reset -rule true -
   action lschema_password_reset
```

Créer des questions et réponses basées sur les connaissances et envoyer un facteur de validation OTP par e-mail via une étiquette de stratégie

Si le premier facteur est l'ouverture de session LDAP, vous pouvez créer une question et une réponse basées sur les connaissances et envoyer des étiquettes de stratégie OTP pour le facteur suivant à l'aide des commandes suivantes.

```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

> add authentication policylabel kba_validation -loginSchema
   lschema_noschema

> add authentication policylabel email_validation -loginSchema
   lschema_noschema
```

Créer un facteur de réinitialisation du mot de passe via l'étiquette de stratégie

Vous pouvez créer le facteur de réinitialisation du mot de passe via l'étiquette de stratégie à l'aide des commandes suivantes.


```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

> add authentication policylabel password_reset -loginSchema
    lschema_noschema

> bind authentication policylabel password_reset -policyName ldap_pwd -
    priority 10 -gotoPriorityExpression NEXT
```

Liez la question et la réponse basées sur les connaissances et la stratégie d'e-mail aux stratégies créées précédemment à l'aide des commandes suivantes.

```
> bind authentication policylabel email_validation -policyName
    email_validation -nextfactor password_reset -priority 10 -
    gotoPriorityExpression NEXT

> bind authentication policylabel kba_validation -policyName
    kba_validation -nextfactor email_validation -priority 10 -
    gotoPriorityExpression NEXT
```

Lier le flux

Le flux d'ouverture de session LDAP doit être créé dans le cadre de la stratégie d'authentification pour l'ouverture de session LDAP. Dans ce flux, l'utilisateur clique sur le lien Mot de passe oublié présenté sur la première page de connexion LDAP, puis sur la validation KBA, puis sur la validation OTP et enfin sur la page de réinitialisation du mot de passe.

```
bind authentication vserver authvs -policy ldap3 -nextfactor
    kba_validation -priority 10 -gotoPriorityExpression NEXT
```

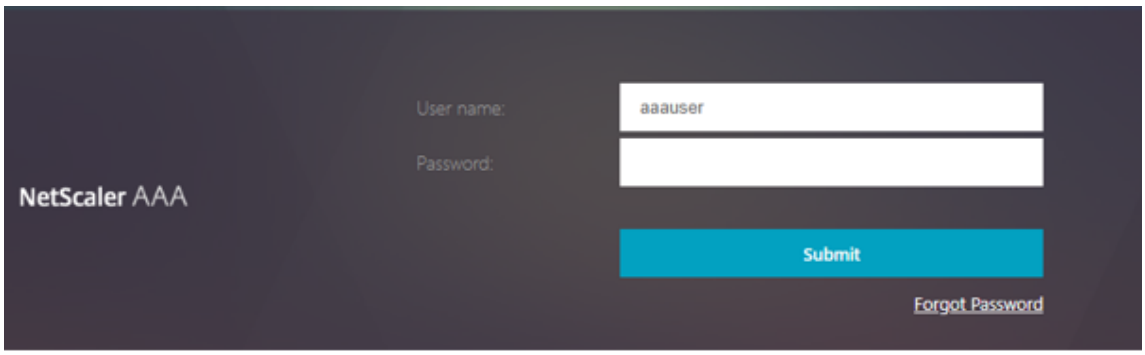
Pour lier tout le flux de l'interface utilisateur

```
bind authentication vserver authvs -policy lpol_password_reset -
    priority 20 -gotoPriorityExpression END
```

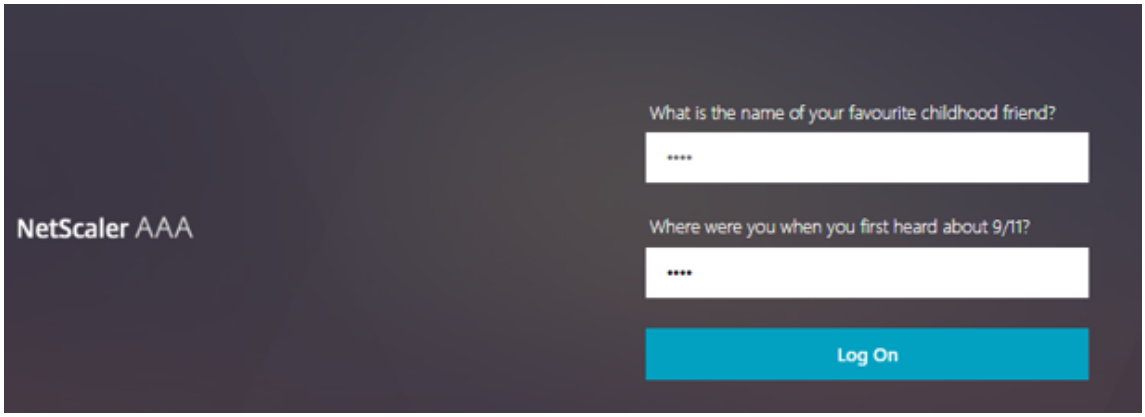
Workflow de connexion utilisateur pour réinitialiser le mot de passe

Voici un flux de travail d'ouverture de session utilisateur si l'utilisateur doit réinitialiser le mot de passe :

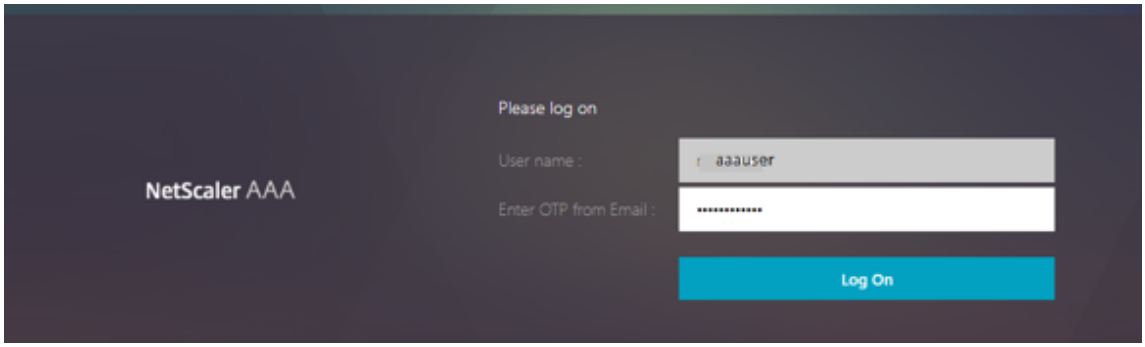
1. Entrez l'URL du serveur virtuel lb ; par exemple, https://lb1.server.com. L'écran d'ouverture de session s'affiche.



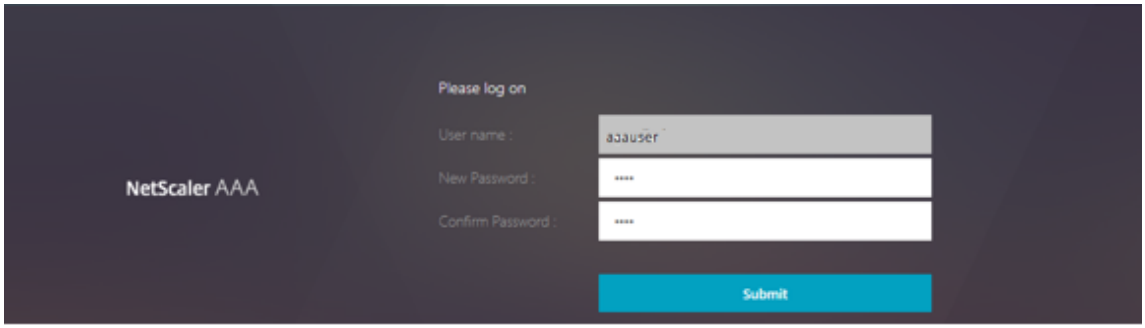
2. Cliquez sur **Mot de passe oublié**. Un écran de validation affiche deux questions sur un maximum de six questions et réponses enregistrées pour un utilisateur AD.



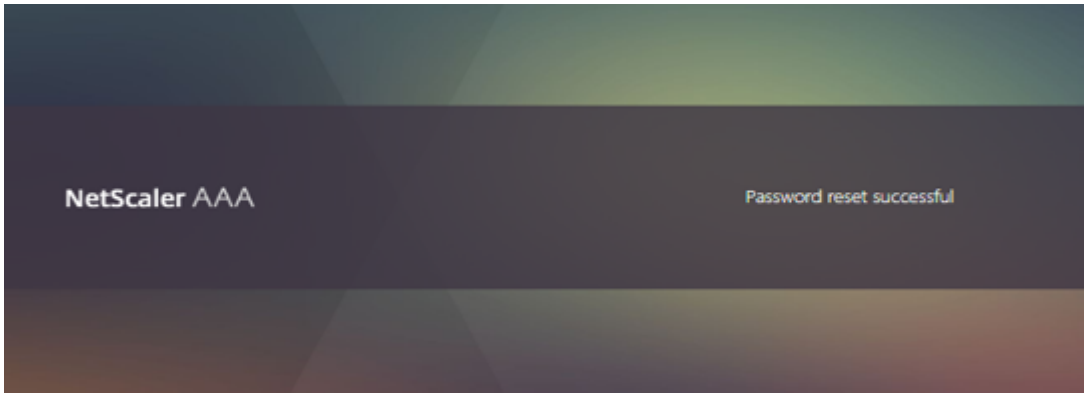
3. Répondez aux questions, puis cliquez **sur Connexion**. Un écran de validation OTP par e-mail dans lequel vous devez saisir l'OTP reçu sur l'autre adresse e-mail enregistrée s'affiche.



4. Entrez l'OTP de l'e-mail. Une fois la validation OTP de l'e-mail réussie, la page de réinitialisation du mot de passe s'affiche.



5. Entrez un nouveau mot de passe et confirmez le nouveau mot de passe. Cliquez sur **Envoyer**. Une fois la réinitialisation du mot de passe réussie, l'écran Réinitialisation du mot de passe réussie s'affiche.



Vous pouvez désormais vous connecter à l'aide du mot de passe de réinitialisation.

Dépannage

NetScaler propose une option permettant de résoudre certains des problèmes de base que vous pouvez rencontrer lors de l'utilisation de la réinitialisation des mots de passe en libre-service. La section suivante vous aide à résoudre certains des problèmes qui peuvent survenir dans des zones spécifiques.

Journal NS

Avant d'analyser le journal, il est recommandé de définir le niveau du journal pour le déboguer à l'aide de la commande suivante :

```
1 > set syslogparams -loglevel DEBUG
```

Enregistrement

Le message suivant indique que l'enregistrement de l'utilisateur a réussi.


```
"ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1"
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  "
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw=="
```

Validation des questions et réponses basée sur les connaissances

Le message suivant indique une validation réussie des questions et réponses basée sur les connaissances.

```
"NFactor: Successfully completed KBA Validation, nextfactor is email"
```

Validation de l'ID de courriel

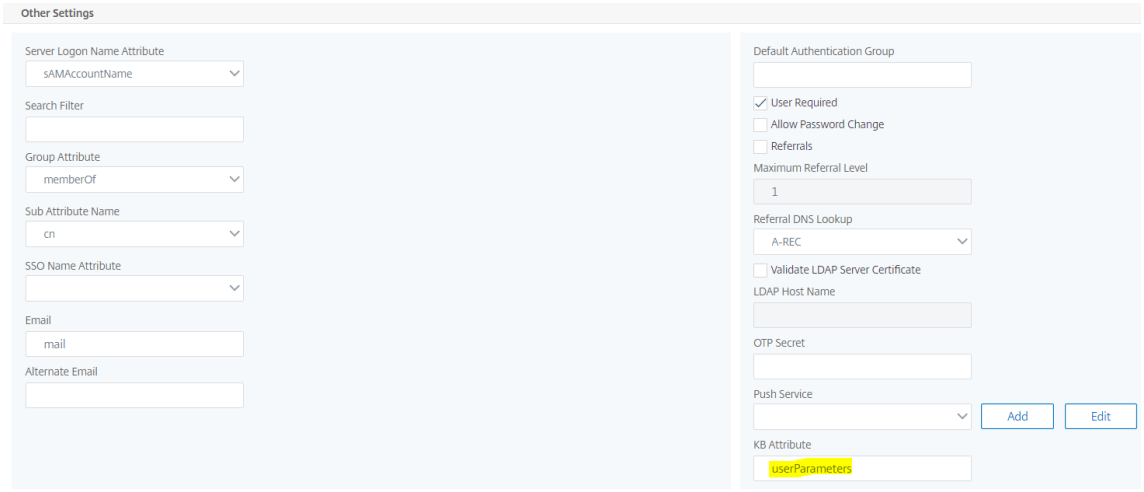
Le message suivant indique une réinitialisation réussie du mot de passe.

```
"NFactor: Successfully completed email auth, nextfactor is pwd_reset"
```

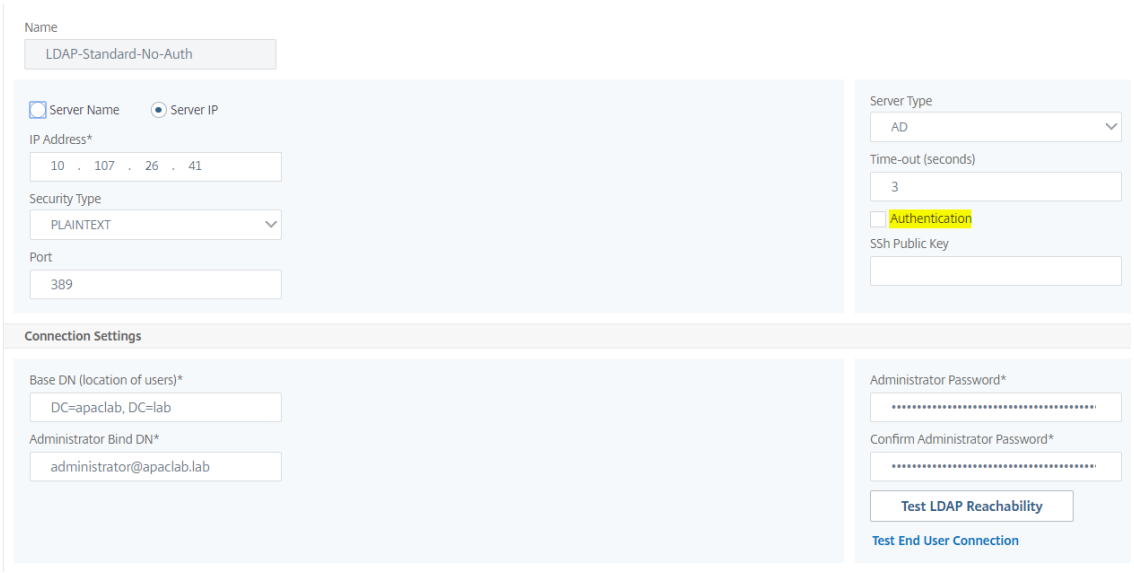
Configurer SSPR à l'aide du visualiseur NFactor

Avant de commencer la configuration SSPR, nous devons ajouter les serveurs LDAP suivants :

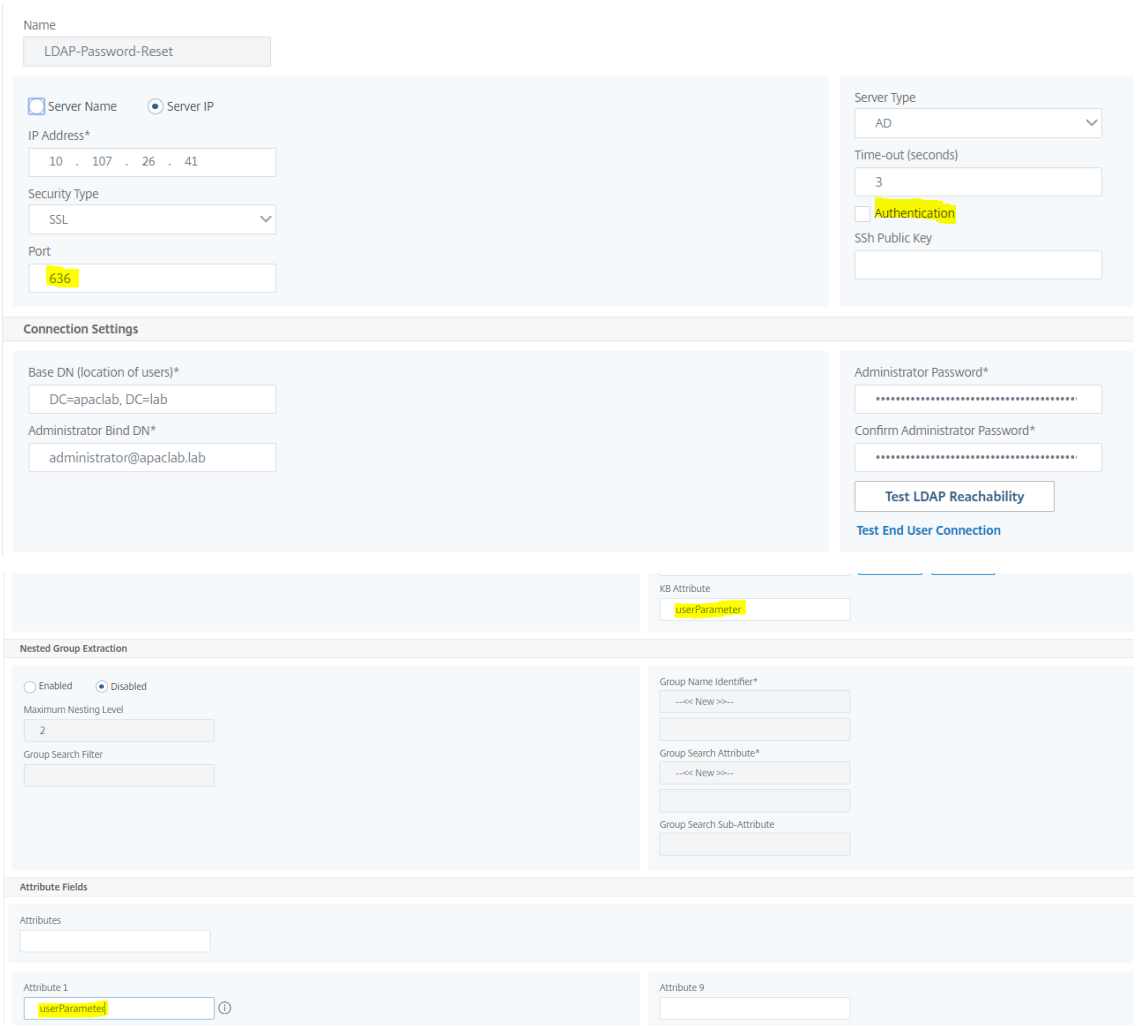
1. Serveur LDAP standard avec authentification activée pour l'authentification des utilisateurs et attribut AD spécifié.



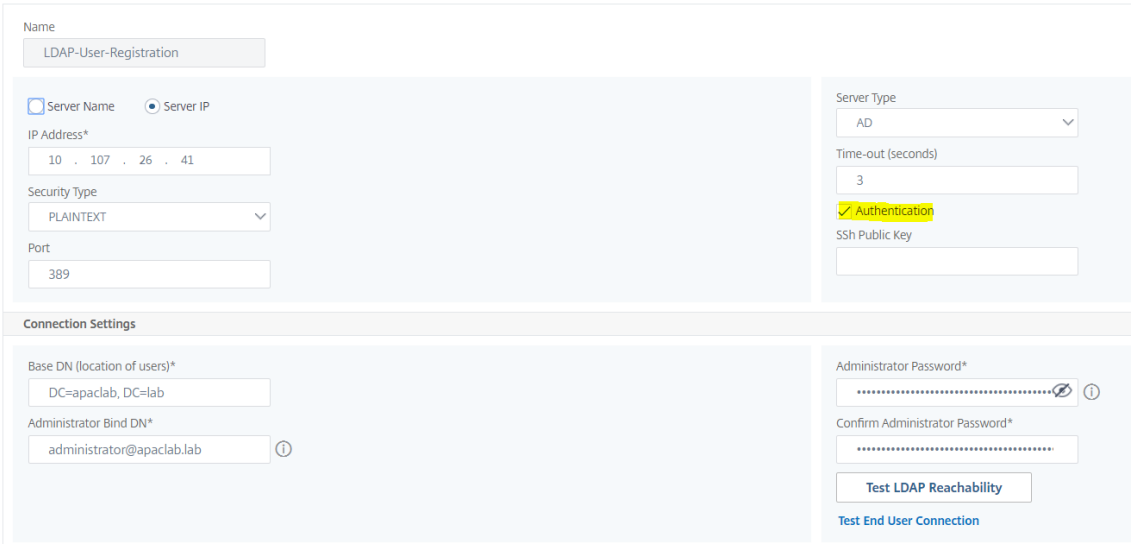
2. Serveur LDAP pour l'extraction des paramètres utilisateur sans authentification.



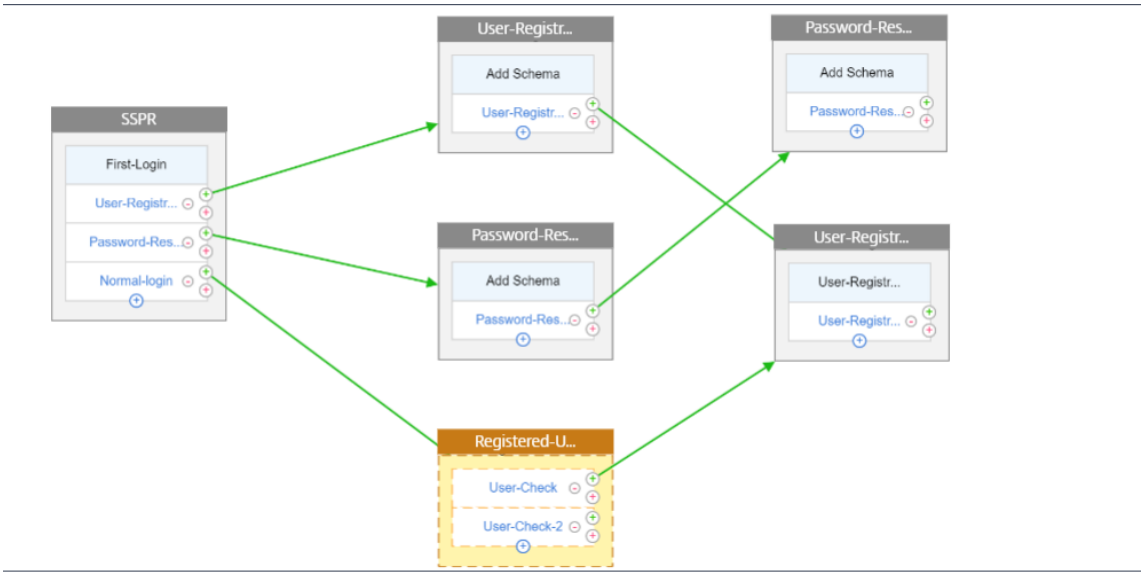
3. Serveur LDAP pour la réinitialisation du mot de passe sur SSL sans authentification. En outre, l'attribut AD à utiliser pour stocker les détails de l'utilisateur doit être défini sur ce serveur.



4. Serveur LDAP pour l'enregistrement des utilisateurs, avec authentification activée et attribut AD spécifié



5. La figure suivante montre le flux complet :



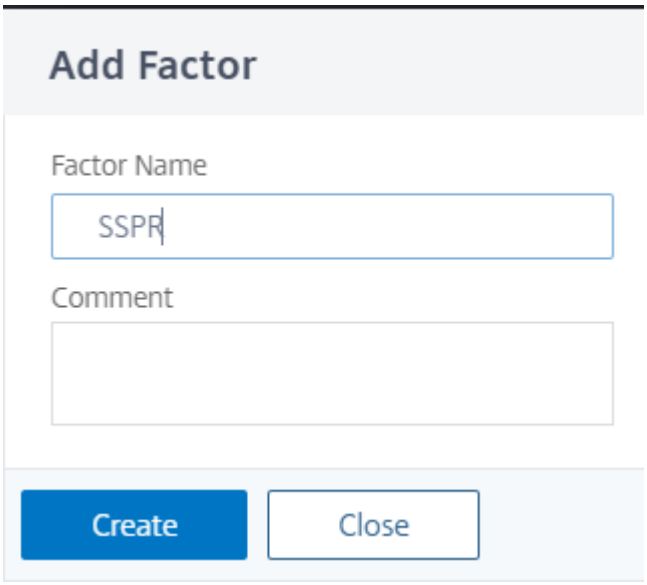
6. Liez le certificat globalement à l'aide de la commande CLI suivante :

```
1 bind vpn global -userDataEncryptionKey Wildcard
```

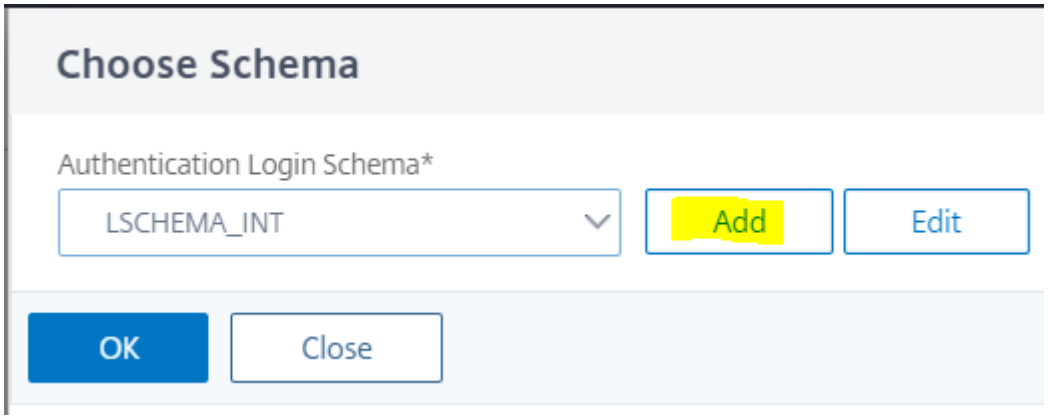
Maintenant que les serveurs LDAP sont ajoutés, procédez à la configuration de nFactor à l'aide du visualiseur

1. Accédez à **Sécurité > AAA > Trafic des applications > Visualiseur nFactor > Flux nFactor**, cliquez sur **Ajouter** et cliquez sur l'icône plus à l'intérieur de la zone.

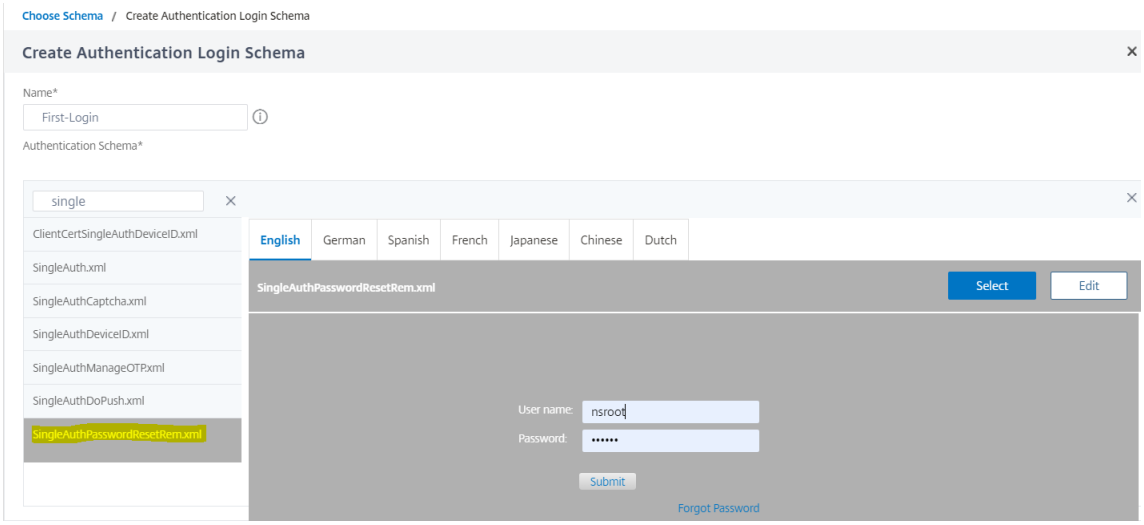
2. Donnez un nom au flux.



3. Cliquez sur **Ajouter un schéma** qui sert de schéma par défaut. Cliquez sur **Ajouter** sur la page du schéma de connexion.



4. Après avoir donné un nom au schéma, sélectionnez-le. Cliquez sur **Sélectionner** dans le coin supérieur droit du schéma à sélectionner.



5. Cliquez sur **Créer**, puis sur **OK**.

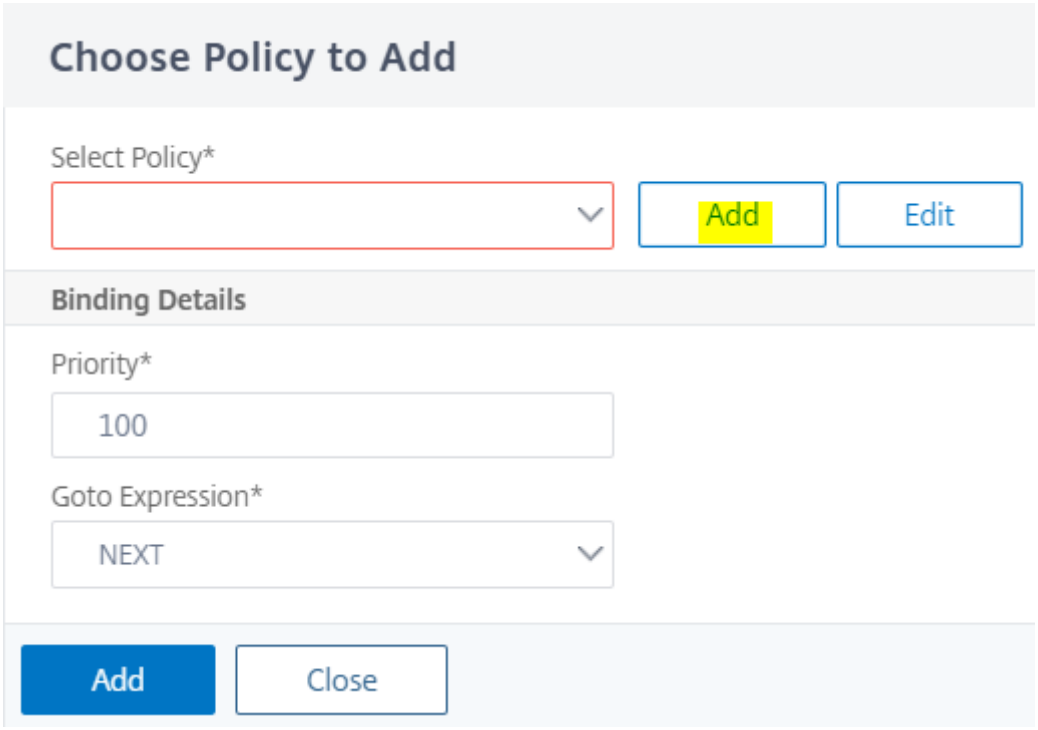
Une fois le schéma par défaut ajouté, nous devons configurer les trois flux suivants :

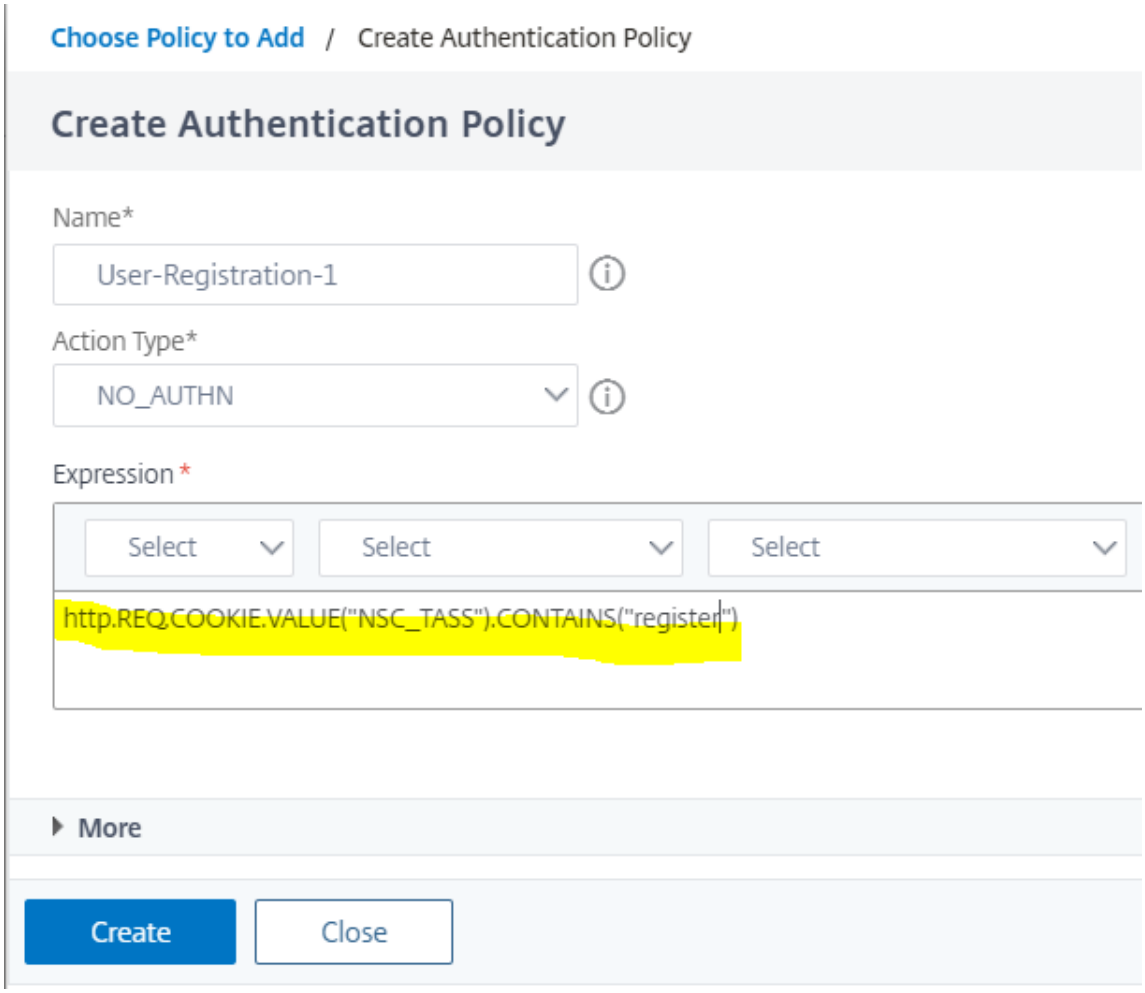
- **Enregistrement d'utilisateur** : pour l'enregistrement explicite des utilisateurs
- **Réinitialisation du mot**de passe : pour la réinitialisation
- **Connexion normale + Vérification de l'utilisateur enregistré** : Si l'utilisateur est enregistré et saisit le bon mot de passe, l'utilisateur est connecté. Dans le cas où l'utilisateur n'est pas enregistré, il est redirigé vers la page d'inscription.

Enregistrement des utilisateurs

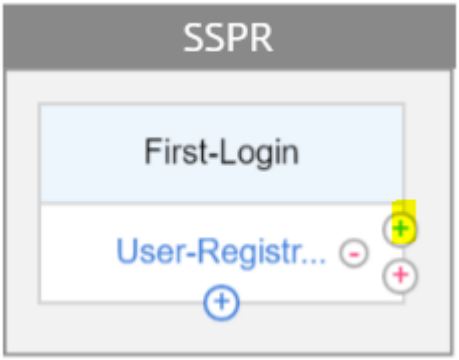
Reprenons là où nous sommes partis après avoir ajouté le schéma.

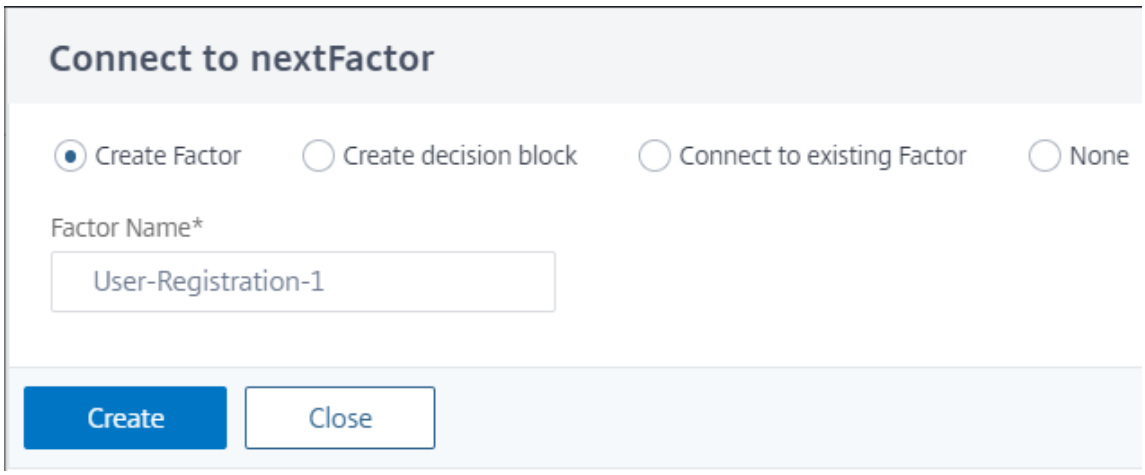
1. Cliquez sur **Add Policy**, cela vérifie si l'utilisateur essaie de s'inscrire explicitement.



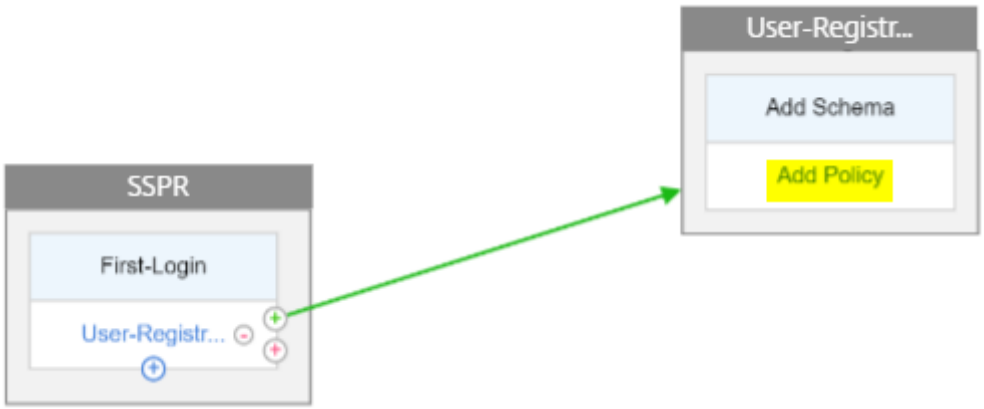


2. Cliquez sur **Créer**, puis sur **Ajouter**.
3. Cliquez sur l'icône verte « + » en surbrillance pour ajouter le facteur d'authentification suivant au flux d'enregistrement des utilisateurs.

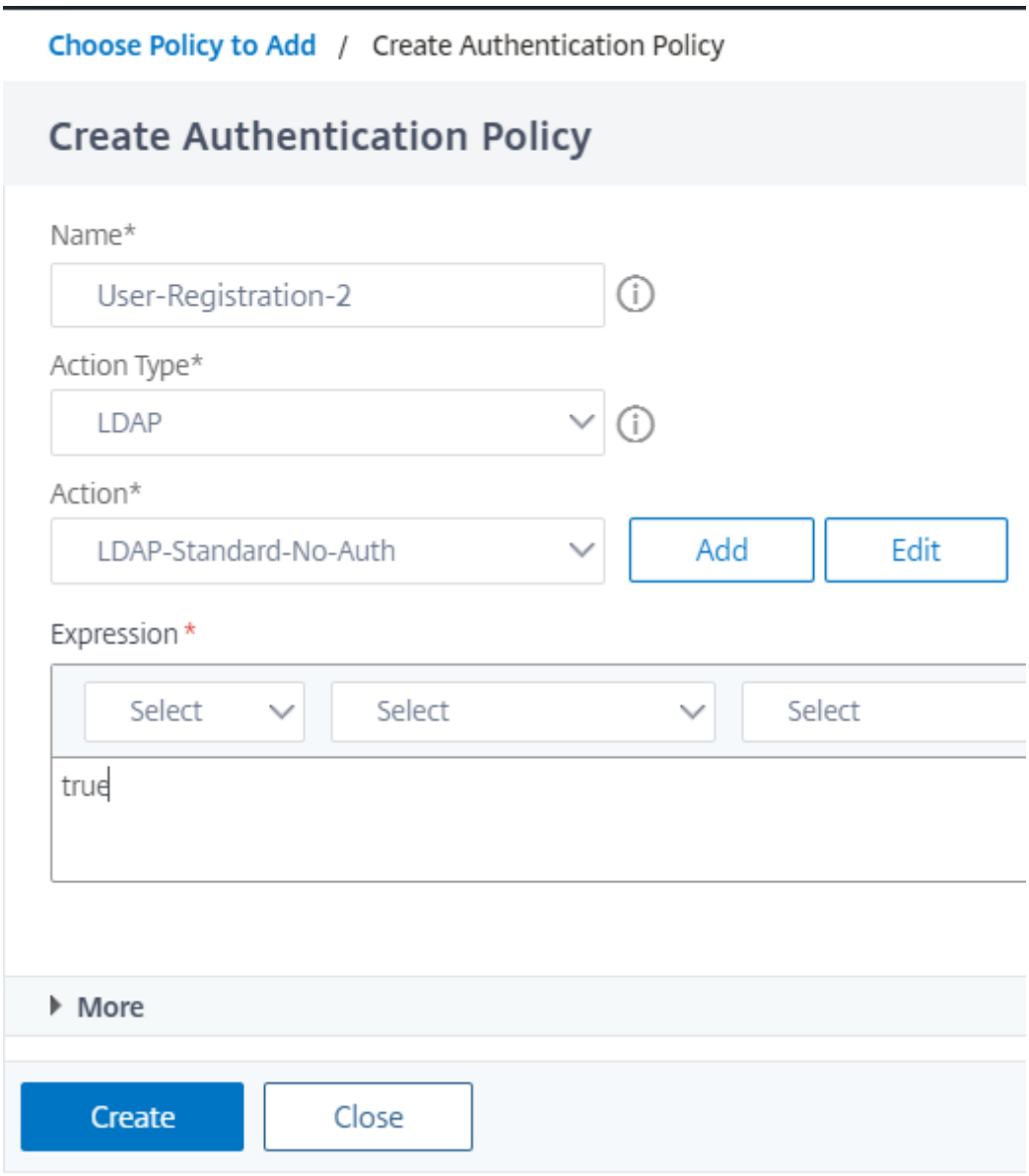




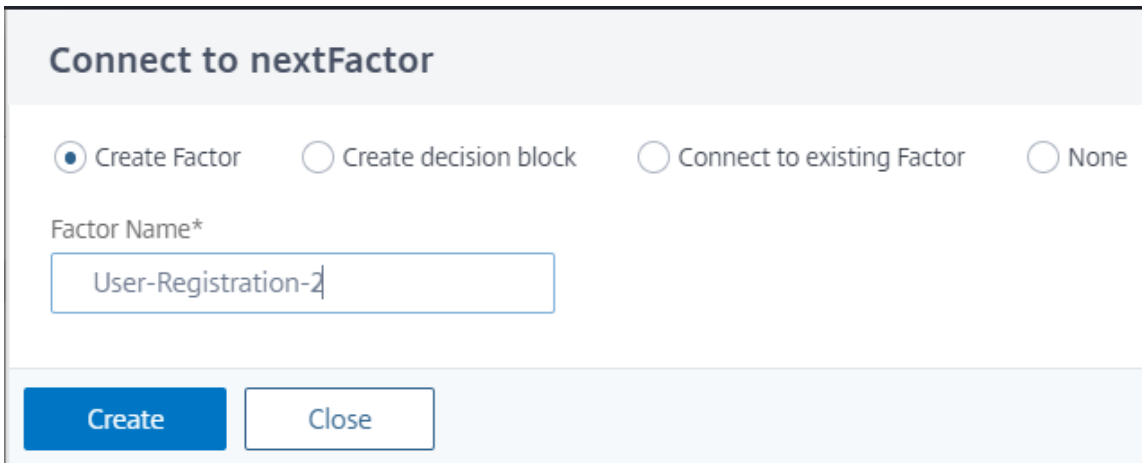
4. Cliquez sur **Create**.
5. Cliquez sur **Ajouter une stratégie** pour le facteur d'enregistrement des utilisateurs-1.



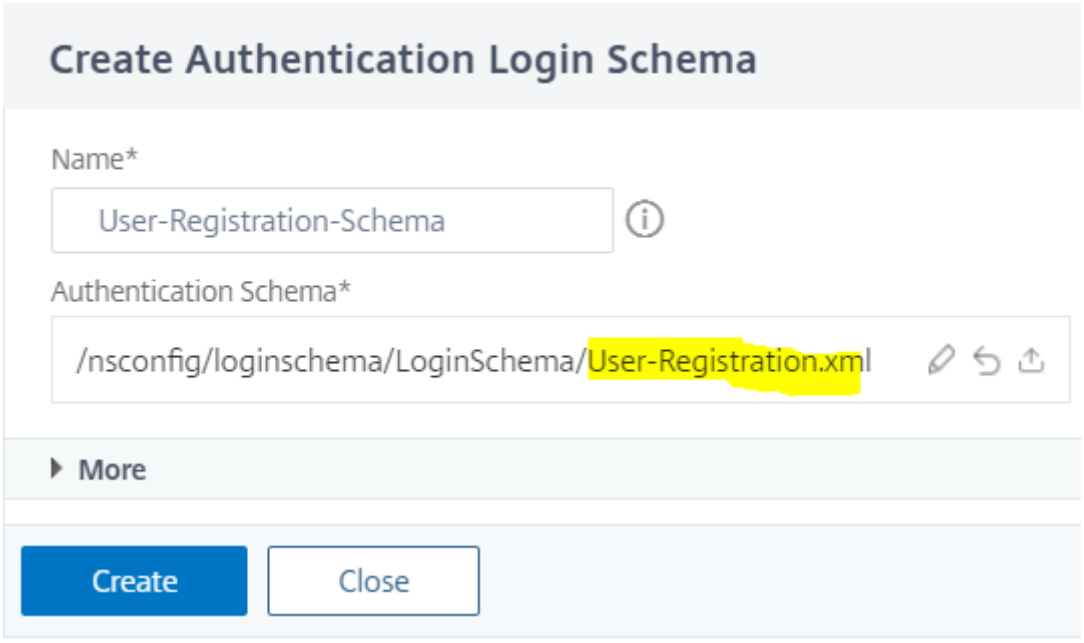
6. Créez la stratégie d'authentification. Cette stratégie extrait les informations utilisateur et les valide avant de les rediriger vers la page d'inscription.



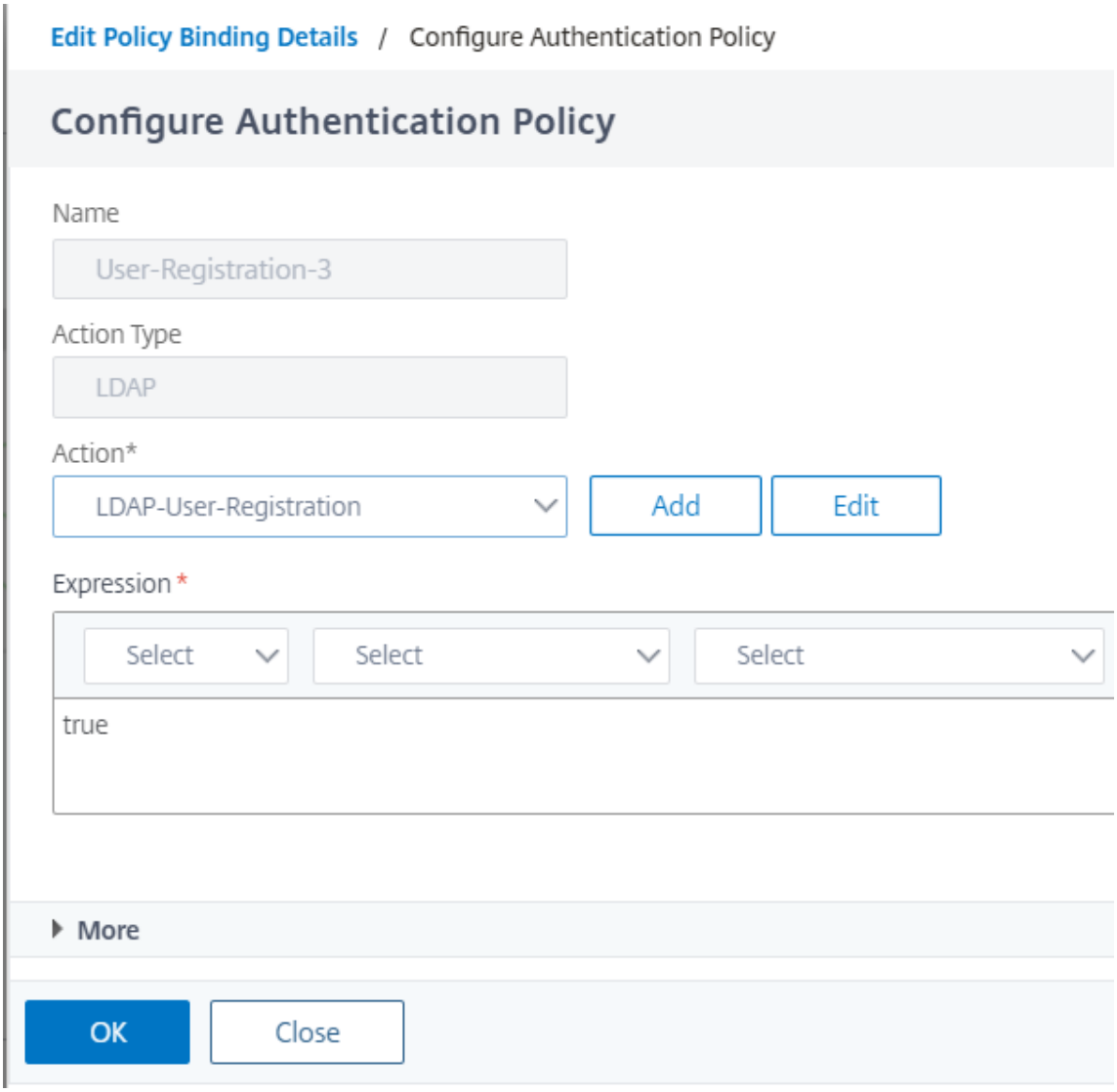
7. Cliquez sur **Créer**, puis sur **Ajouter**.
8. Cliquez maintenant sur l'icône verte « + » pour créer un autre facteur pour l'enregistrement de l'utilisateur, puis cliquez sur **Créer**. Cliquez sur **Ajouter un schéma**.



9. Créez le schéma suivant.



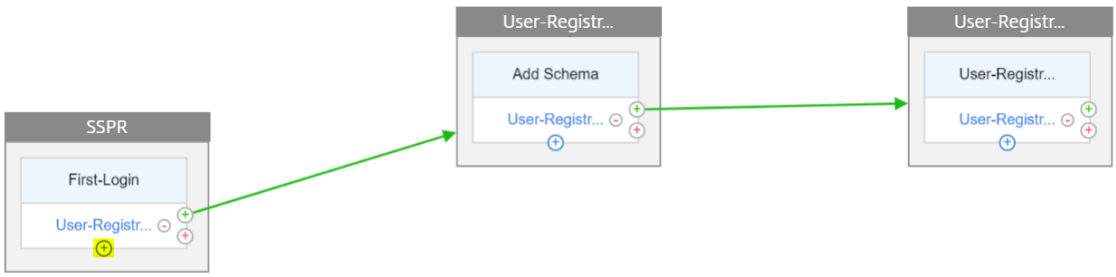
10. Cliquez sur **Ajouter une stratégie** et créez la stratégie d'authentification suivante.



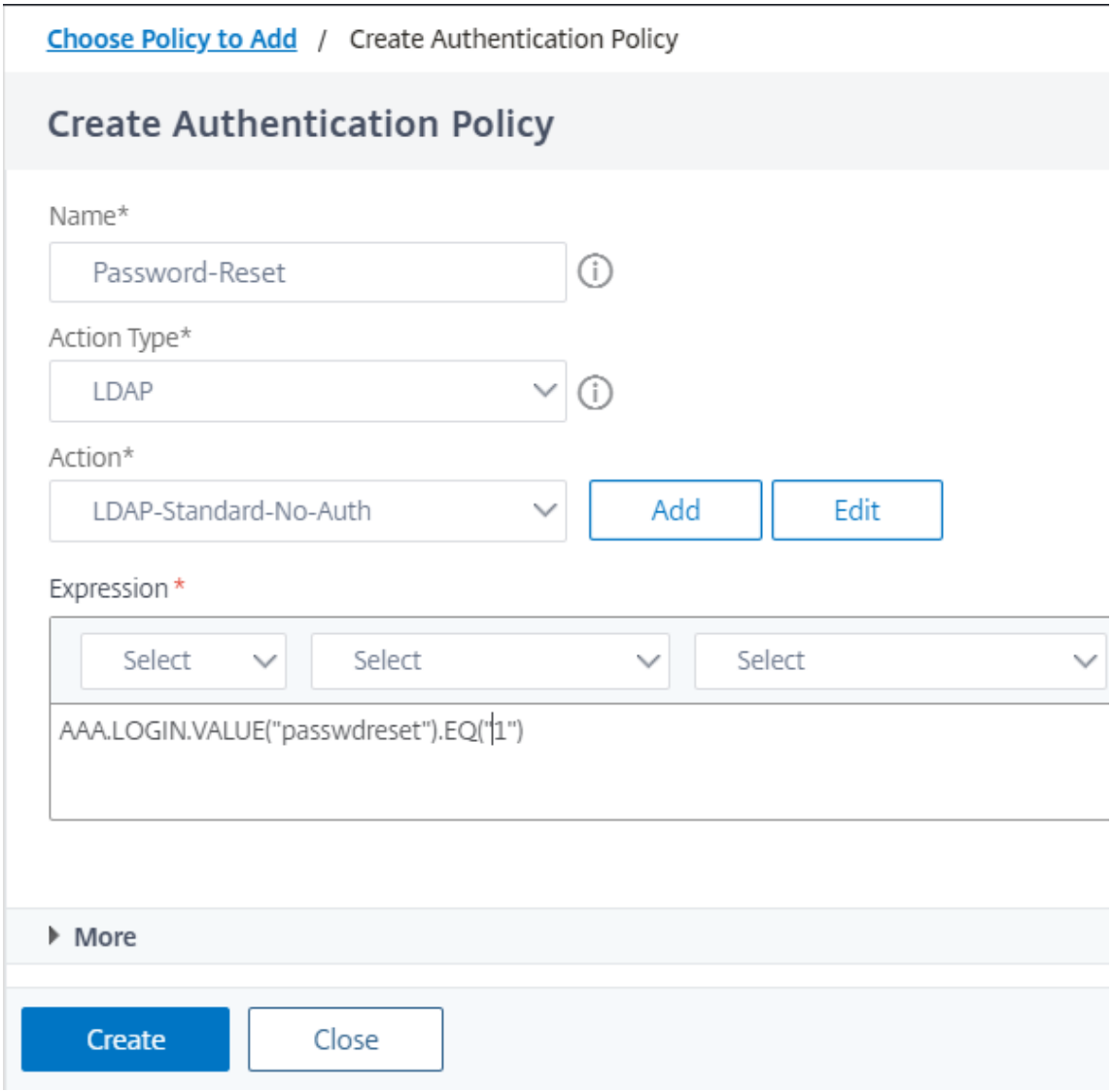
11. Cliquez sur **Créer**, puis sur **Ajouter**.

Réinitialisation du mot

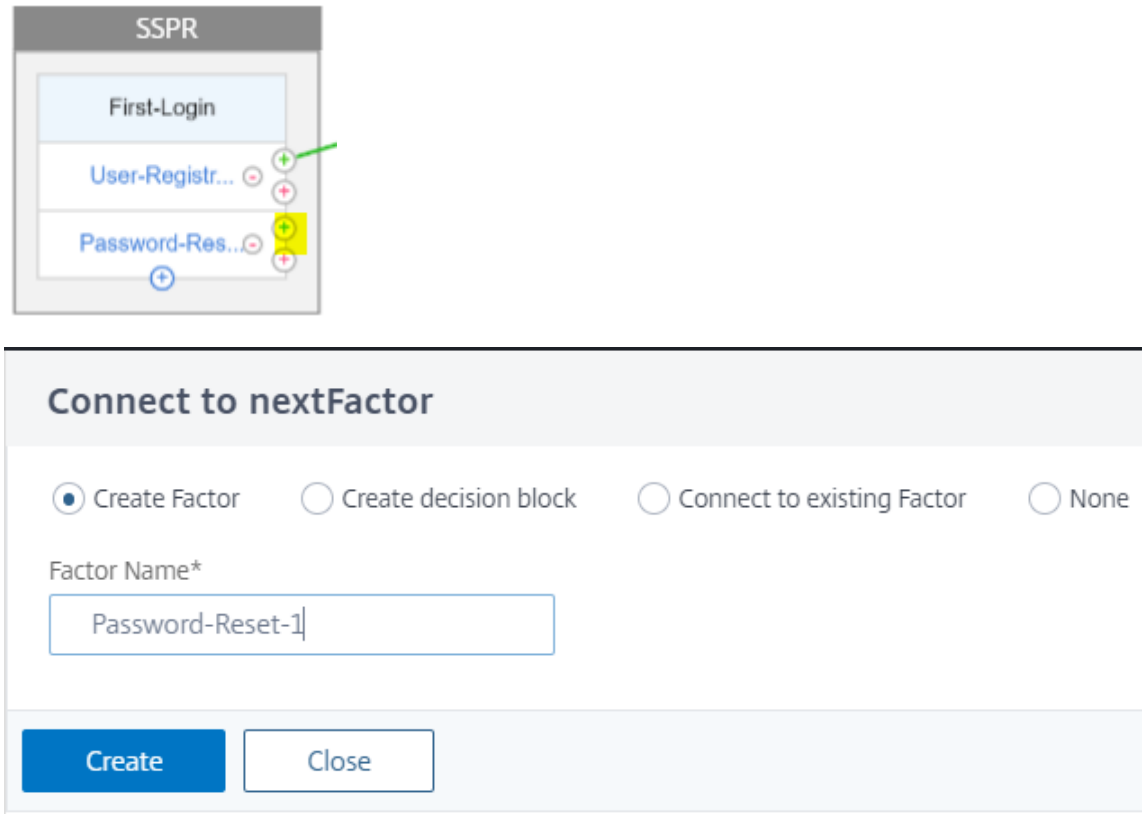
1. Cliquez sur l'icône bleue « + » pour ajouter une autre stratégie (flux de réinitialisation du mot de passe) pour le facteur SSPR parent.



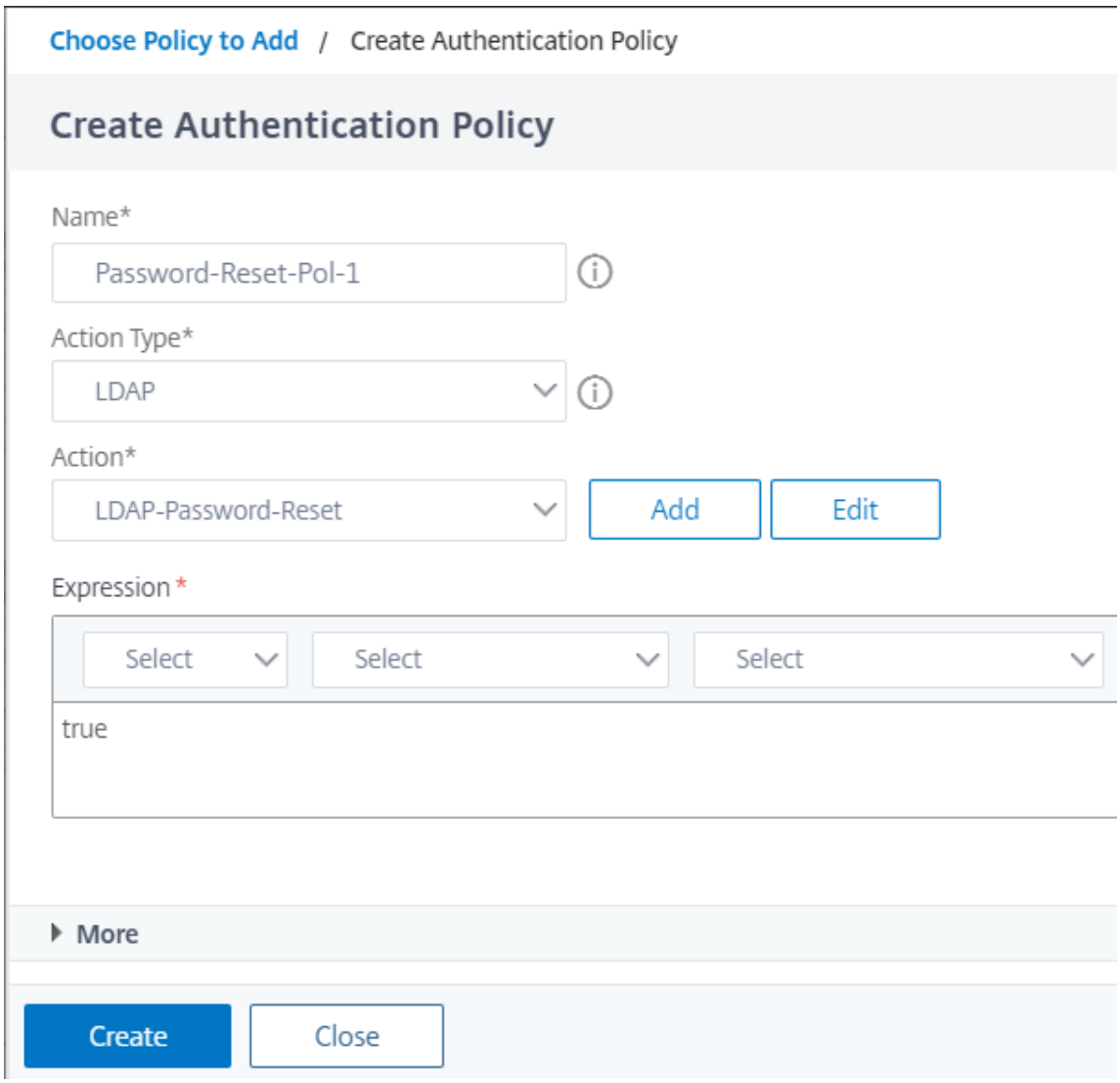
2. Cliquez sur **Ajouter** et créez une stratégie d'authentification. Cette stratégie est déclenchée si l'utilisateur clique sur « Mot de passe oublié » sur la page de connexion.



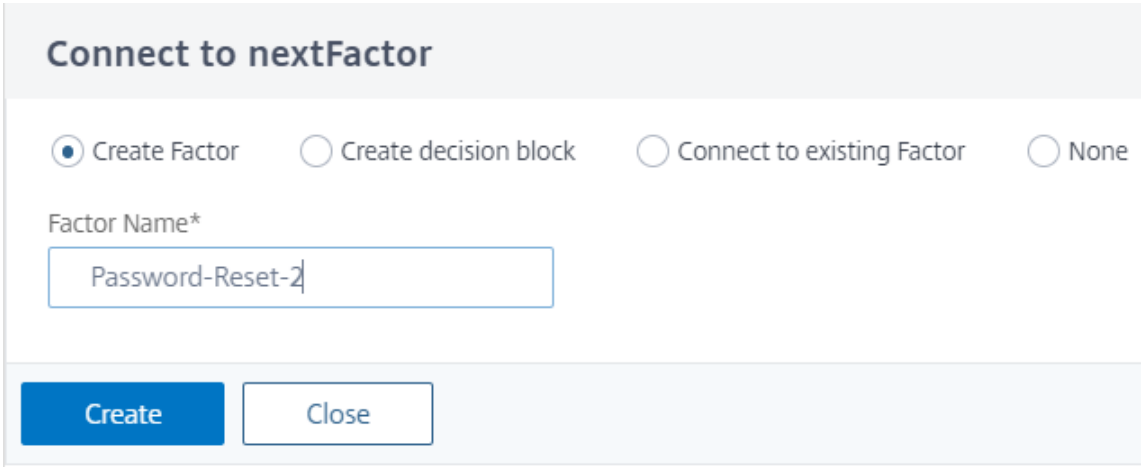
3. Cliquez sur **Créer**, puis sur **Ajouter**.
4. Cliquez sur l'icône verte « + » de la stratégie d'authentification de réinitialisation du mot de passe afin d'ajouter un autre facteur.



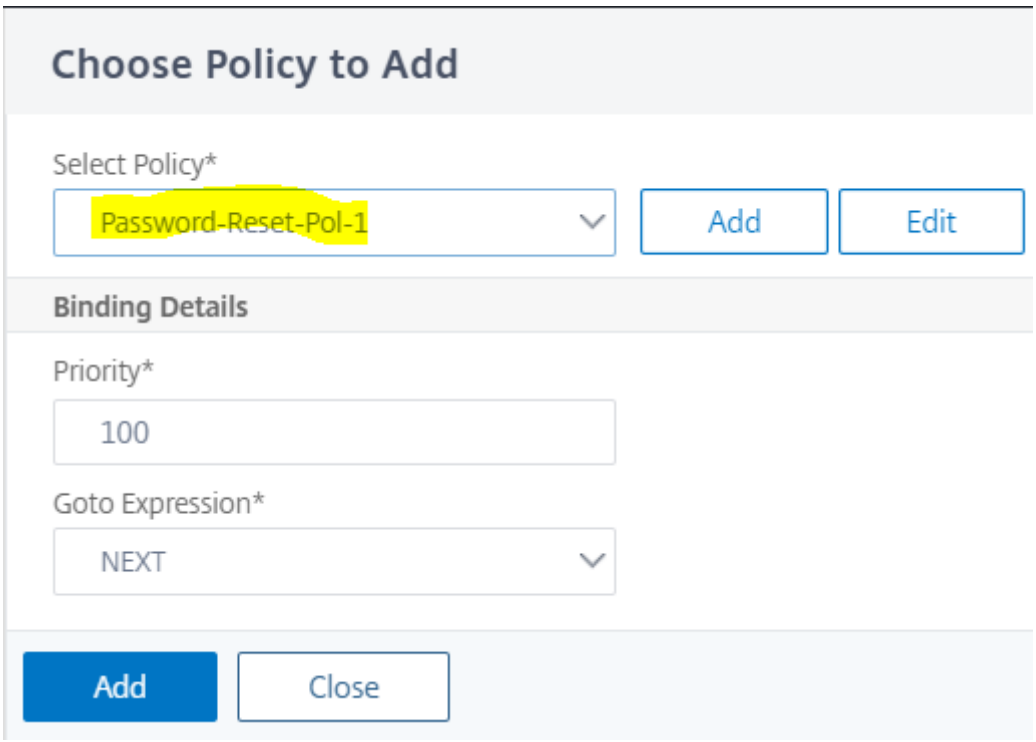
5. Cliquez sur **Create**.
6. Cliquez sur **Ajouter une stratégie** pour créer une stratégie d'authentification pour le facteur créé précédemment. Ce facteur sert à valider l'utilisateur.



7. Cliquez sur **Créer**, puis sur **Ajouter**.
8. Cliquez sur l'icône verte « + » pour ajouter un autre facteur pour le flux de facteurs de mot de passe, cela valide les réponses fournies pour réinitialiser le mot de passe. Cliquez sur **Create**.

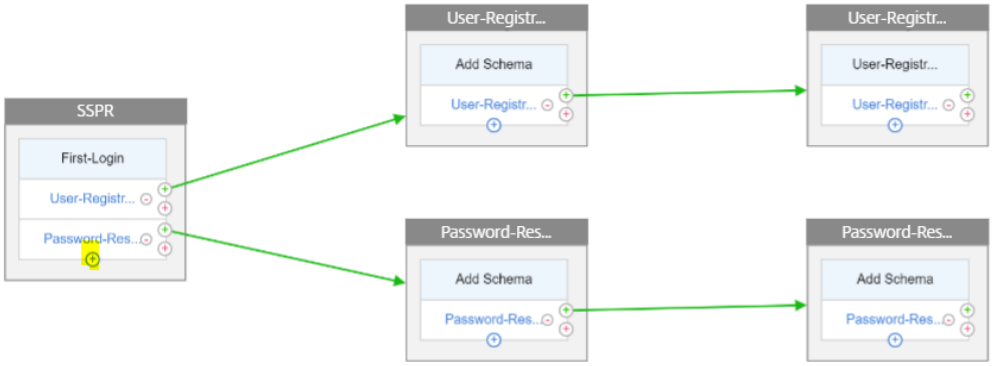


9. Cliquez sur **Add Policy** pour ajouter une stratégie d'authentification pour le facteur.
10. Sélectionnez la même stratégie d'authentification dans le menu déroulant que nous avons créé précédemment, puis cliquez sur **Ajouter**.

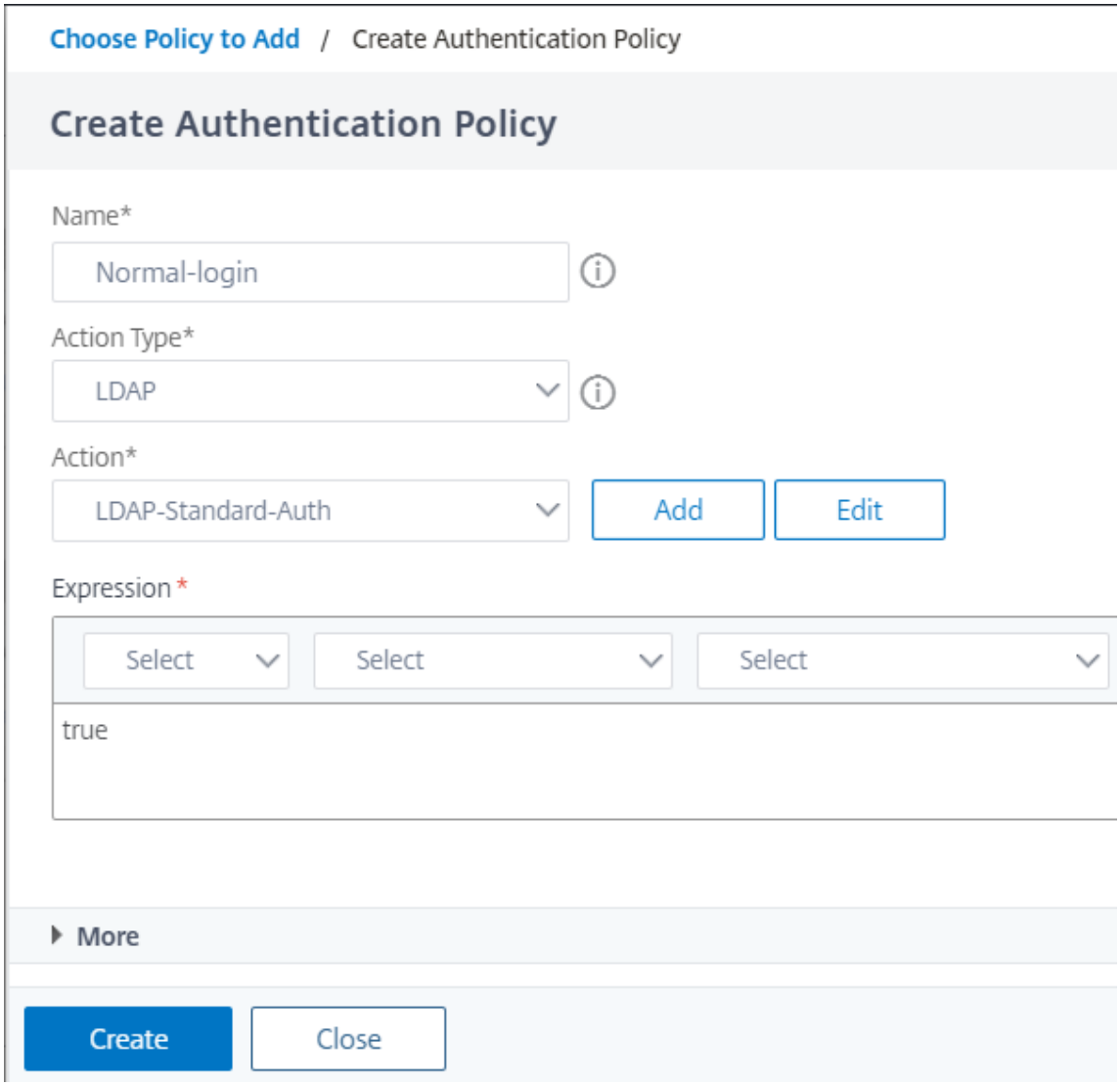


Connexion normale + Vérification de l'utilisateur enregistré

1. Cliquez sur l'icône bleue « + » pour ajouter une autre stratégie d'authentification (flux de connexion normal) au facteur SSPR parent.

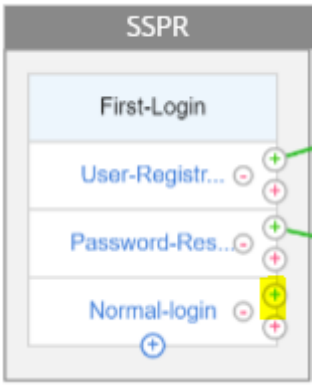


2. Cliquez sur **Ajouter**pour créer une stratégie d'authentification pour la connexion utilisateur normale.

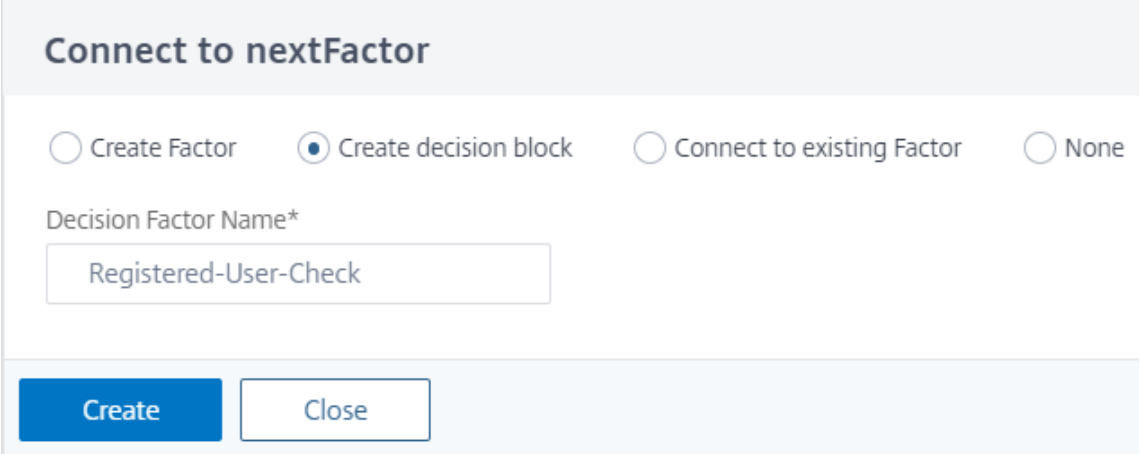


3. Cliquez sur **Créer**, puis sur **Ajouter**.

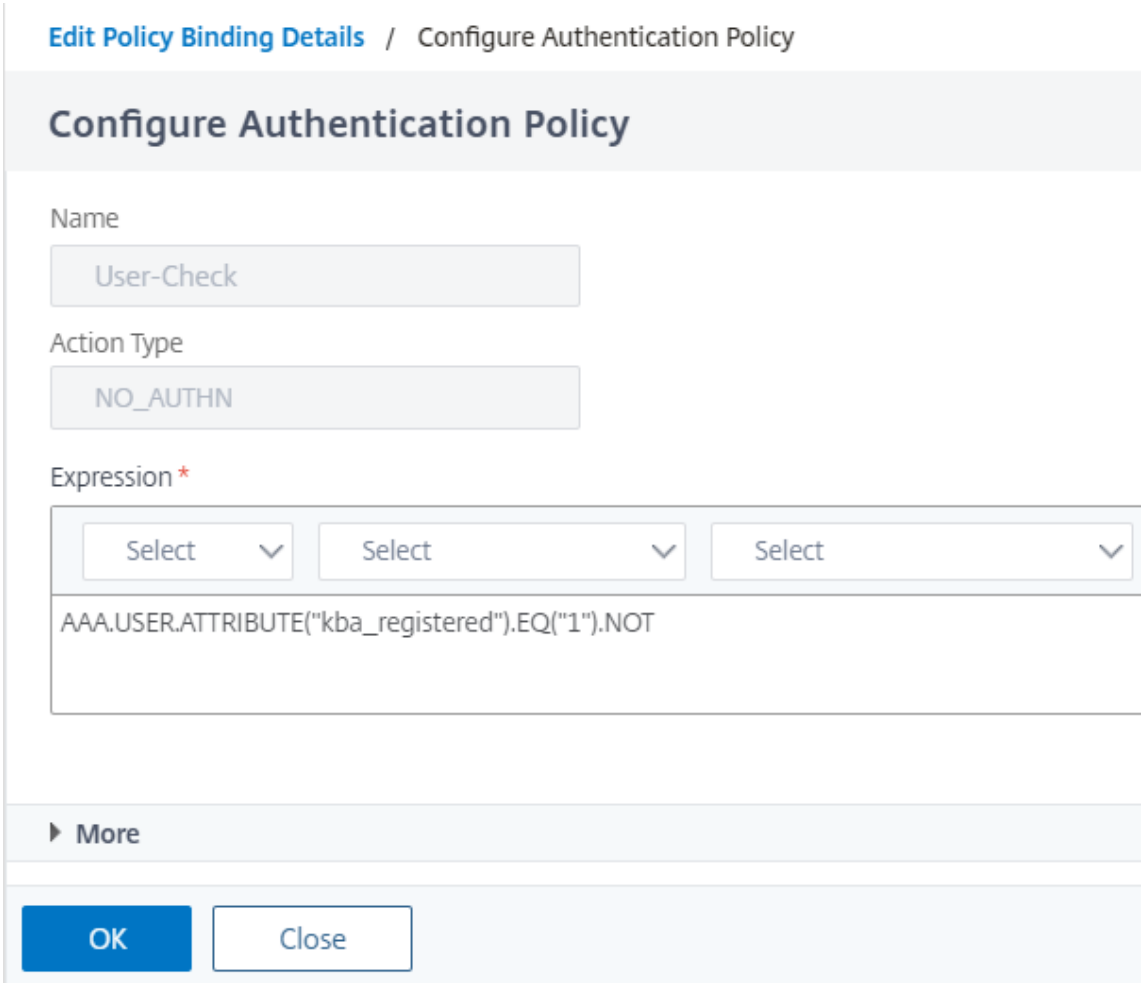
4. Cliquez sur l'icône verte « + » de la stratégie créée précédemment pour ajouter un autre facteur, à savoir le bloc de décision. Cliquez sur **Create**.



5. Cliquez sur **Create**.

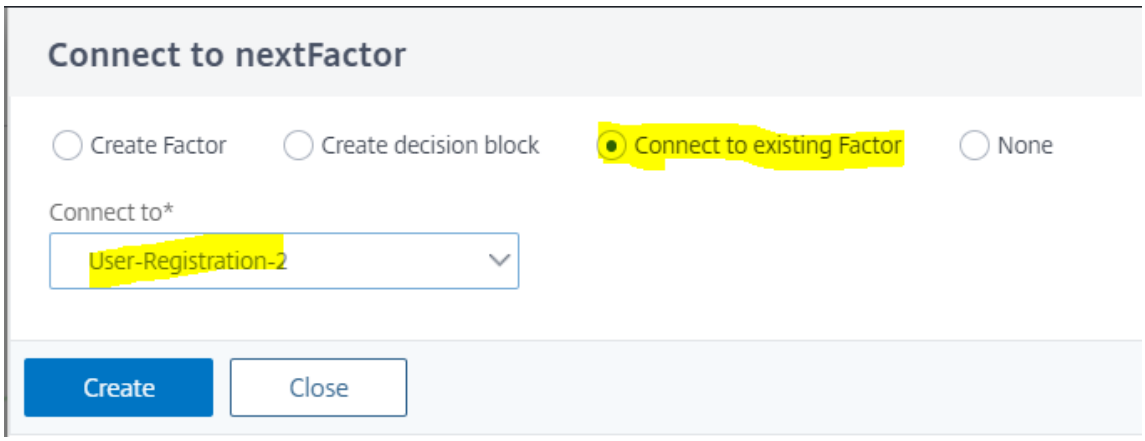


6. Cliquez sur **Ajouter une stratégie** pour créer une stratégie d'authentification pour ce facteur de décision.

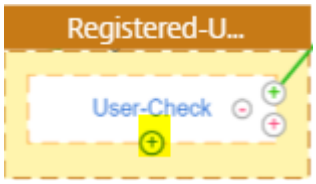


7. Cliquez sur **Créer**, puis sur **Ajouter**. Cela permet de vérifier si l'utilisateur est enregistré ou non.
8. Cliquez sur l'icône verte « + » pour diriger l'utilisateur vers la stratégie d'enregistrement.

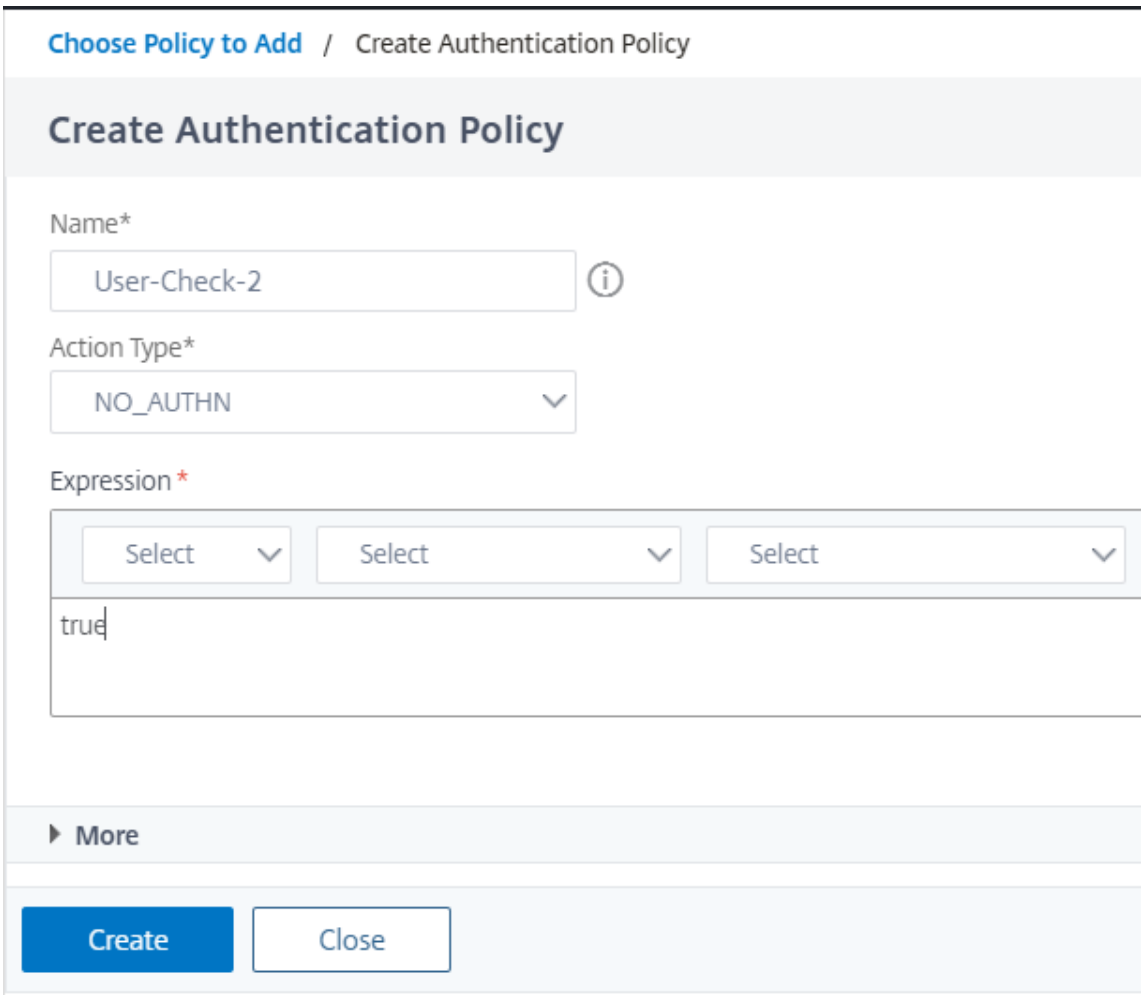
9. Sélectionnez le facteur d'enregistrement dans le menu déroulant et cliquez sur **Créer**.



10. Cliquez maintenant sur l'icône bleue « + » pour ajouter une autre stratégie au bloc de décision. Cette stratégie permet à l'utilisateur enregistré de mettre fin à l'authentification.



11. Cliquez sur **Add Policy** pour créer une stratégie d'authentification.



12. Cliquez sur **Créer**, puis sur **Ajouter**.

Interrogation pendant l'authentification

May 5, 2023

À partir de la version 13.0.79.64 de NetScaler, une appliance NetScaler peut être configurée pour le mécanisme de sondage lors de l'authentification multifactorielle.

Si le sondage est configuré sur une appliance NetScaler, les points de terminaison (tels qu'un navigateur Web ou une application) peuvent interroger (sonder) l'appliance pendant l'authentification aux intervalles configurés pour obtenir l'état de la demande d'authentification soumise.

Le sondage peut être configuré pour gérer les authentifications lorsqu'un point de terminaison abandonne une connexion TCP lors de l'authentification avec une appliance NetScaler.

Points à noter

- La configuration de sondage est prise en charge pour les méthodes d'authentification LDAP, RADIUS et TACACS.
- Le client peut sonner les demandes d'authentification à partir du second facteur.

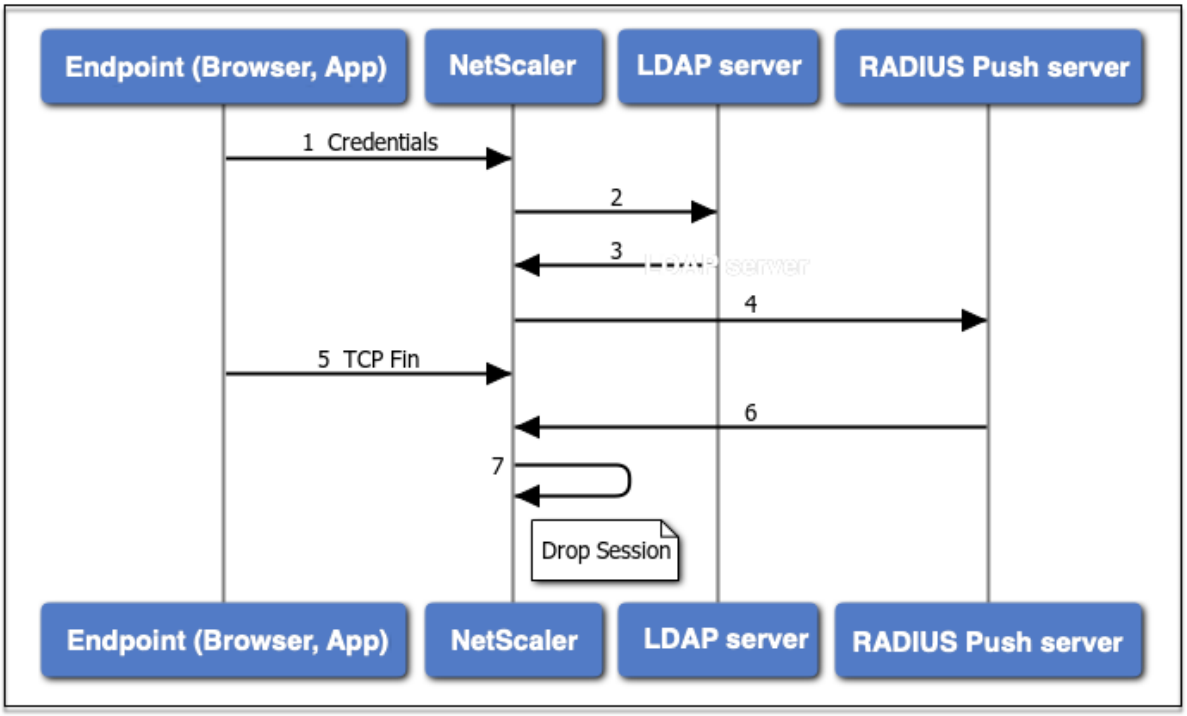
Pourquoi configurer l'interrogation ?

Parfois, lors de l'authentification, le passage d'une application à l'autre (par exemple, une application de connexion et une application d'authentification) entraîne la perte de connexion des terminaux avec l'appliance NetScaler, ce qui entraîne une interruption du flux d'authentification. Une fois l'interrogation configurée, cette interruption de l'authentification peut être évitée.

Comprendre le mécanisme de sondage

Voici un exemple de flux d'événements pendant l'authentification sans interrogation configurée.

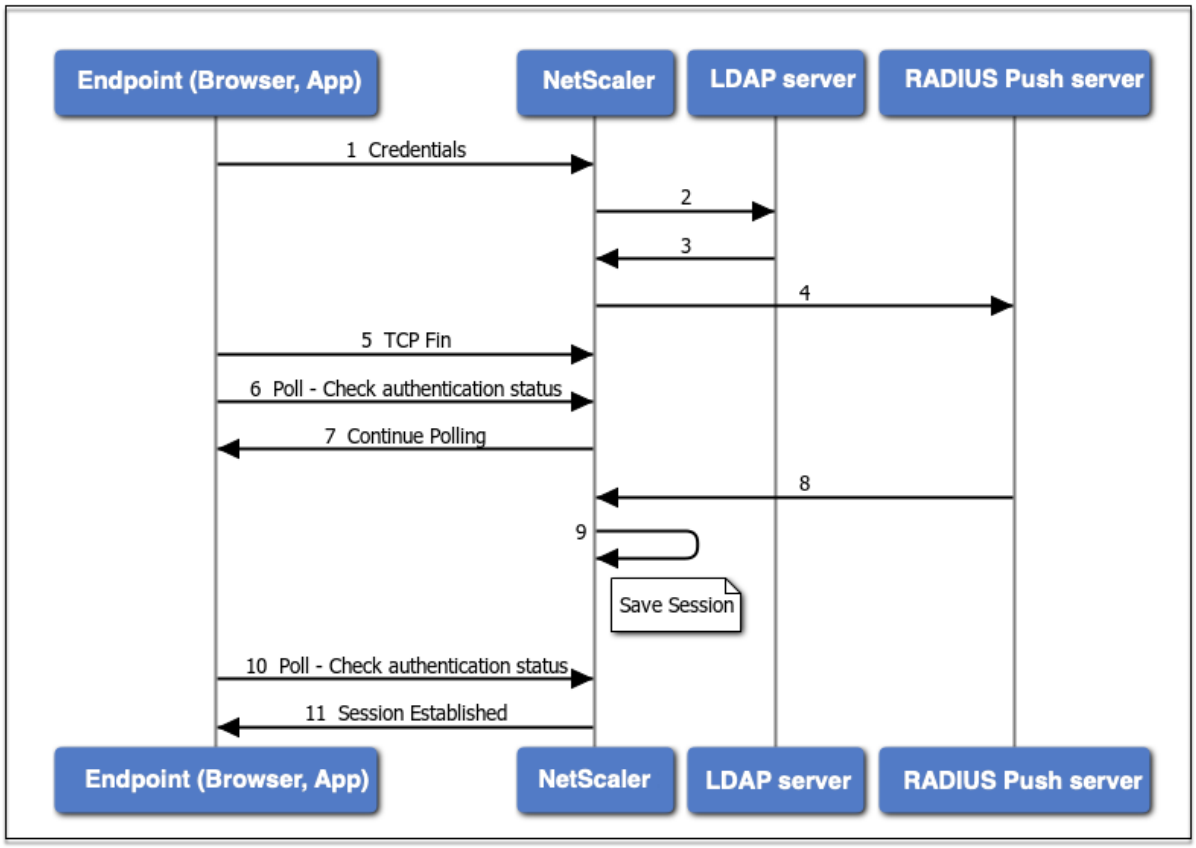
Le mécanisme de sondage permet à une appliance NetScaler de reprendre une authentification continue avec le point de terminaison sans avoir à redémarrer le processus d'authentification dans le cas rare d'une réinitialisation de la connexion TCP sur le point de terminaison.



1. Un point de terminaison (application ou navigateur Web) s'authentifie avec des informations d'identification.

2. Le nom d'utilisateur et le mot de passe sont vérifiés par rapport à un répertoire de premier facteur existant (LDAP/Active Directory).
3. Si les informations d'identification correctes sont fournies, l'authentification passe au facteur suivant.
4. À ce stade, l'appliance NetScaler envoie une demande au serveur RADIUS Push.
5. Pendant que l'appliance NetScaler attend une réponse du serveur RADIUS, le point de terminaison abandonne la connexion TCP.
6. NetScaler reçoit une réponse du serveur RADIUS Push.
7. Aucune connexion TCP client n'étant trouvée, l'appliance NetScaler abandonne la session et la connexion échoue.

L'exemple suivant illustre le flux d'événements pendant l'authentification avec Polling configuré.



1. Un point de terminaison (application ou navigateur Web) s'authentifie avec des informations d'identification.
2. Le nom d'utilisateur et le mot de passe sont vérifiés par rapport à un répertoire de premier facteur existant (LDAP/Active Directory).
3. Si les informations d'identification correctes sont fournies, l'authentification passe au facteur suivant.
4. À ce stade, l'appliance NetScaler envoie une demande au serveur RADIUS Push.
5. Pendant que l'appliance NetScaler attend une réponse du serveur RADIUS, le point de terminai-

son abandonne la connexion TCP.

6. Endpoint envoie un sondage (sonde) à l'appliance NetScaler pour vérifier l'état de l'authentification.
7. Comme l'appliance NetScaler ne reçoit pas de réponse du serveur RADIUS, elle demande au point de terminaison de poursuivre l'interrogation.
8. L'appliance NetScaler reçoit une réponse du serveur RADIUS Push.
9. Aucune connexion TCP client n'étant trouvée, ADC enregistre l'état de la session.
10. Endpoint interroge à nouveau pour vérifier l'état de l'authentification.
11. L'appliance NetScaler établit la session et la connexion réussit.

Configuration du sondage à l'aide de l'interface de ligne

Voici un exemple de configuration CLI.

Configurer le premier facteur

```
add authentication ldapAction ldap-new -serverIP 10.106.40.65 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword 2
    f63d3659103464a4fad0ade65e2ccfd4e8440e36ddff941d29796af03e01139 -
    encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -
    groupAttrName memberof -subAttributeName CN -secType SSL -
    alternateEmailAttr userParameters

add authentication Policy ldap-new -rule true -action ldap-new

bind authentication vserver avs -policy ldap-new -priority 1 -
    nextFactor rad_factor
<!--NeedCopy-->
```

Configurer le deuxième facteur

```
add authentication radiusAction rad1 -serverIP 10.102.229.120 -radKey 1
    b1613760143ce2371961e9a9eb5392c86a4954a62397f29a01b5d12b42ce232 -
    encrypted -encryptmethod ENCMTHD_3

add authentication Policy rad -rule true -action rad1
<!--NeedCopy-->
```

Configurer le schéma de connexion Poll.xml


```
add authentication loginSchema polling_schema -authenticationSchema
    LoginSchema/Poll.xml

add authentication policylabel rad_factor -loginSchema polling_schema

bind authentication policylabel rad_factor -policyName rad -priority 1
    -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Configuration du sondage à l'aide de l'interface

Pour obtenir des étapes détaillées sur la configuration de l'authentification multifacteur à l'aide de l'interface graphique, voir Configuration de l'authentification nFactor.

Vous trouverez ci-dessous des exemples d'étapes de haut niveau requises pour configurer NetScaler for Polling à partir du deuxième facteur.

1. Créez un premier facteur d'authentification, par exemple LDAP.
2. Créez un deuxième facteur d'authentification, par exemple RADIUS.
3. Ajoutez le **fichier Poll.xml** présent dans NetScaler (/NSConfig/LoginSchema/LoginSchema/) comme schéma de connexion pour le second facteur.

Gestion des sessions et du trafic

May 8, 2023

Paramètres de session

Après avoir configuré vos profils d'authentification, d'autorisation et d'audit, vous configurez les paramètres de session pour personnaliser vos sessions utilisateur. Les paramètres de session sont les suivants :

- **Le délai d'expiration de la session.**

  Contrôle la période après laquelle l'utilisateur est automatiquement déconnecté et doit s'authentifier à nouveau pour accéder à votre intranet.

- **Le paramètre d'autorisation par défaut.**

  Détermine si l'appliance NetScaler autorisera ou refusera par défaut l'accès au contenu pour lequel il n'existe aucune politique d'autorisation spécifique.

- **Le paramètre d'authentification unique.**

  Détermine si l'appliance NetScaler connectera automatiquement les utilisateurs à toutes les applications Web après leur authentification, ou s'il transférera les utilisateurs vers la page d'ouverture de session de l'application Web pour s'authentifier pour chaque application.

- **Le paramètre d'index des informations d'identification.**

  Détermine si l'appliance NetScaler utilise les informations d'authentification principales ou secondaires pour l'authentification unique.

Pour configurer les paramètres de session, vous pouvez adopter l'une des deux approches. Si vous souhaitez des paramètres différents pour différents comptes ou groupes d'utilisateurs, vous devez créer un profil pour chaque compte d'utilisateur ou groupe pour lequel vous souhaitez configurer des paramètres de session personnalisés. Vous créez également des stratégies pour sélectionner les connexions auxquelles appliquer des profils particuliers, et vous liez les stratégies aux utilisateurs ou aux groupes. Vous pouvez également lier une stratégie au serveur virtuel d'authentification qui gère le trafic auquel vous souhaitez appliquer le profil.

Si vous souhaitez obtenir les mêmes paramètres pour toutes les sessions, ou si vous souhaitez personnaliser les paramètres par défaut des sessions qui n'ont pas de profils et de stratégies spécifiques configurés, vous pouvez simplement configurer les paramètres de session globaux.

Profils de session

Pour personnaliser vos sessions utilisateur, vous devez d'abord créer un profil de session. Le profil de session vous permet de remplacer les paramètres globaux de tous les paramètres de session.

> **Remarque**
>
> Les termes « profil de session » et « action de session » signifient la même chose.

Pour créer un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un profil de session et vérifier la configuration :

```
1 add tm sessionAction <name> [-sessTimeout <mins>] [-
     defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
     ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
     httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
      )] [-persistentCookieValidity <minutes>]
2
3 show tm sessionAction <name>
4 <!--NeedCopy-->
```


Exemple

```
> add tm sessionAction session-profile -sessTimeout 30 -
   defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```

Pour modifier un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier un profil de session et vérifier la configuration :

```
set tm sessionAction <name> [-sessTimeout <mins>] [-
   defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
   ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
   httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
    )] [-persistentCookieValidity <minutes>]

show tm sessionAction
<!--NeedCopy-->
```

Exemple

```
> set tm sessionAction session-profile -sessTimeout 30 -
   defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```

Pour supprimer un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour supprimer un profil de session :

```
rm tm sessionAction <name>
<!--NeedCopy-->
```


Pour configurer les profils de session à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Session.**
2. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Session.**
3. Dans le volet de détails, cliquez sur l'onglet **Profils** .
4. Dans l'onglet **Profils**, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau profil de session, cliquez sur **Ajouter.**
   - Pour modifier un profil de session existant, sélectionnez-le, puis cliquez sur **Modifier.**
5. Dans la boîte de dialogue Créer un profil de session TM ou Configurer un profil de session TM, tapez ou sélectionnez des valeurs pour les paramètres.
   - Name* : actionName (ne peut pas être modifié pour une action de session précédemment configurée.)
   - Délai d'expiration de la session : SessTimeout
   - Connexion unique aux applications Web : authentification unique
   - Action d'autorisation par défaut : DefaultAuthorizationAction
   - Index des informations d'identification — SSOCredential
   - Domaine d'authentification unique : SSODomain
   - HTTPOnly Cookie—httpOnlyCookie
   - Enable Persistent Cookie—persistentCookie
   - Persistent Cookie Validity—persistentCookieValidity
6. Cliquez sur **Créer** ou **sur OK**. Le profil de session que vous avez créé apparaît dans le volet Stratégies et profils de session.

Stratégies de session

Après avoir créé un ou plusieurs profils de session, vous créez des stratégies de session, puis vous liez les stratégies globalement ou à un serveur virtuel d'authentification pour les mettre en œuvre.

Pour créer une stratégie de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une stratégie de session et vérifier la configuration :

```
1 -  add tm sessionPolicy <name> <rule> <action>
2 -  show tm sessionPolicy <name>
3 <!--NeedCopy-->
```

Exemple

```
1 > add tm sessionPolicy session-pol "URL == /\*.png" session-profile
2 Done
3 > show tm sessionPolicy session-pol
```



```
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```

Pour modifier une stratégie de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier une stratégie de session et vérifier la configuration :

```
-  set tm sessionPolicy <name> [-rule <expression>] [-action <action>]
-  show tm sessionPolicy <name>
<!--NeedCopy-->
```

Exemple

```
> set tm sessionPolicy session-pol "URL == /\*.png" session-profile
 Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```

Pour lier globalement une stratégie de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier globalement une stratégie de session et vérifier la configuration :

```
bind tm global -policyName <policyname> [-priority <priority>]
<!--NeedCopy-->
```

Exemple

```
> bind tm global -policyName session-pol
 Done

> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/*.png'
        Action: session-profile
        Policy is bound to following entities
        1) TM GLOBAL    PRIORITY : 0
 Done
```



```
10
11 <!--NeedCopy-->
```

Pour lier une stratégie de session à un serveur virtuel d'authentification à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour lier une stratégie de session à un virtuel d'authentification et vérifier la configuration :

```
1 bind authentication vserver <name> -policy <policyname> [-priority <
     priority>]
2 <!--NeedCopy-->
```

Exemple

```
1 bind authentication vserver auth-vserver-1 -policyName Session-Pol-1 -
     priority 1000
2 Done
3 <!--NeedCopy-->
```

Pour délier une stratégie de session d'un serveur virtuel d'authentification à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour délier une stratégie de session d'un serveur virtuel d'authentification et vérifier la configuration :

```
1 unbind authentication vserver <name> -policy <policyname>
2 <!--NeedCopy-->
```

Exemple

```
1 unbind authentication vserver auth-vserver-1 -policyName Session-Pol-1
2 Done
3 <!--NeedCopy-->
```

Pour annuler la liaison d'une stratégie de session globalement liée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier une stratégie de session liée globalement :


```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Exemple

```
unbind tm global -policyName Session-Pol-1
Done
<!--NeedCopy-->
```

Pour supprimer une stratégie de session à l'aide de l'interface de ligne de commande

Commencez par délier la stratégie de session de la stratégie globale, puis, à l'invite de commandes, tapez les commandes suivantes pour supprimer une stratégie de session et vérifier la configuration :

```
rm tm sessionPolicy <name>
<!--NeedCopy-->
```

Exemple

```
rm tm sessionPolicy Session-Pol-1
Done

<!--NeedCopy-->
```

Pour configurer et lier des stratégies de session à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic d'applications > Session**.
2. Accédez à **Sécurité > AAA - Trafic des applications > Politiques > Session**.
3. Dans le volet d'informations, sous **l'onglet Stratégies**, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle politique de session, cliquez sur **Ajouter**.
   - Pour modifier une politique de session existante, sélectionnez la politique, puis cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Créer une stratégie** de **session ou Configurer la stratégie** de session, tapez ou sélectionnez les valeurs des paramètres.
   - NAME* : PolicyName (ne peut pas être modifié pour une stratégie de session précédemment configurée.)
   - Profil de demande* — ActionName
   - Expression* : règle (Vous saisissez des expressions en choisissant d'abord le type d'expression dans la liste déroulante située à gauche sous la zone de texte Expression,

puis en tapant votre expression directement dans la zone de texte de l'expression, ou en cliquant sur **Ajouter** pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant la liste déroulante contient des listes pour construire votre expression.)

5. Cliquez sur **Créer** ou **sur OK**. La stratégie que vous avez créée apparaît dans le volet d'informations de la page **Stratégies** et **profils** de session.
6. Pour lier globalement une stratégie de session, dans le volet d'informations, sélectionnez **Liaisons globales** dans la liste déroulante **Action**, puis remplissez la boîte de dialogue.
   - Sélectionnez le nom de la stratégie de session que vous souhaitez lier globalement.
   - Cliquez sur **OK**.
7. Pour lier une stratégie de session à un serveur virtuel d'authentification, dans le volet de navigation, cliquez sur **Serveurs virtuels**, puis ajoutez cette stratégie à la liste des stratégies.
   - Dans le volet d'informations, sélectionnez le serveur virtuel, puis cliquez sur **Modifier**.
   - Dans les **sélections avancées** à droite de la zone de détails, cliquez sur **Stratégies**.
   - Sélectionnez une stratégie ou cliquez sur l'icône **Plus** pour ajouter une stratégie.
   - Dans la colonne **Priorité** de gauche, modifiez la priorité par défaut pour vous assurer que la stratégie est évaluée dans le bon ordre.
   - Cliquez sur **OK**.
     Un message apparaît dans la barre d'état, indiquant que la stratégie a été correctement configurée.

Paramètres de session globaux

En plus ou au lieu de créer des profils et des stratégies de session, vous pouvez configurer les paramètres de session globaux. Ces paramètres contrôlent la configuration de la session lorsqu'aucune stratégie explicite ne les remplace.

Pour configurer les paramètres de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer les paramètres de session globaux et vérifier la configuration :

```
set tm sessionParameter [-sessTimeout <mins>][-
    defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
    ssoCredential ( PRIMARY | SECONDARY )][-ssoDomain <string>][-
    httpOnlyCookie ( YES | NO )][-persistentCookie ( ENABLED | DISABLED
    )] [-persistentCookieValidity <minutes>]
<!--NeedCopy-->
```

Exemple

```
> set tm sessionParameter -sessTimeout 30
  Done
```



```
> set tm sessionParameter -defaultAuthorizationAction DENY
  Done
> set tm sessionParameter -SSO ON
  Done
> set tm sessionParameter -ssoCredential PRIMARY
  Done
<!--NeedCopy-->
```

Pour configurer les paramètres de session à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur Modifier les paramètres globaux.
3. Dans la boîte de dialogue **Paramètres globaux de la session**, saisissez ou sélectionnez des valeurs pour les paramètres.
   - Délai d'expiration de la session : SessTimeout
   - Action d'autorisation par défaut : DefaultAuthorizationAction
   - Connexion unique aux applications Web : authentification unique
   - Index des informations d'identification — SSOCredential
   - Domaine d'authentification unique : SSODomain
   - HTTPOnly Cookie—httpOnlyCookie
   - Enable Persistent Cookie—persistentCookie
   - Validité des cookies persistants (minutes) — PersistentCookieValidity
   - Page d'accueil : page d'accueil
4. Cliquez sur **OK**.

Paramètres de trafic

Si vous utilisez l'authentification unique (SSO) basée sur des formulaires ou SAML pour vos applications protégées, vous configurez cette fonctionnalité dans les paramètres de trafic. La connexion unique permet à vos utilisateurs de se connecter une seule fois pour accéder à toutes les applications protégées, plutôt que de leur demander de se connecter séparément pour accéder à chacune d'elles.

L'authentification unique basée sur les formulaires vous permet d'utiliser un formulaire Web de votre propre conception comme méthode de connexion au lieu d'une fenêtre contextuelle générique. Vous pouvez donc mettre le logo de votre entreprise et d'autres informations que vous souhaiteriez voir voir apparaître sur le formulaire d'ouverture de session. Le SSO SAML vous permet de configurer une appliance NetScaler ou une instance d'appliance virtuelle pour s'authentifier auprès d'une autre appliance NetScaler pour le compte des utilisateurs qui se sont authentifiés auprès de la première appliance.

Pour configurer l'un ou l'autre type d'authentification SSO, vous devez d'abord créer un formulaire ou un profil SSO SAML. Ensuite, vous créez un profil de trafic et vous le liez au profil SSO que vous avez

créé. Ensuite, vous créez une stratégie et vous la liez au profil de trafic. Enfin, vous liez la stratégie globalement ou à un serveur virtuel d'authentification pour mettre en œuvre votre configuration.

Profils de trafic

Après avoir créé au moins un formulaire ou un profil SSO SAML, vous devez ensuite créer un profil de trafic.

> **Remarque :**
>
> Dans cette fonctionnalité, les termes « profil » et « action » signifient la même chose.

Pour créer un profil de trafic à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add tm trafficAction <name> [-appTimeout <mins>][-SSO ( ON | OFF ) [-
    formSSOAction <string>]][-persistentCookie ( ENABLED | DISABLED )][-
    InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Exemple

```
add tm trafficAction Traffic-Prof-1  - appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```

Pour modifier un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set tm trafficAction <name> [-appTimeout <mins>] [-SSO ( ON | OFF ) [-
    formSSOAction <string>]] [-persistentCookie ( ENABLED | DISABLED )]
    [-InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Exemple

```
set tm trafficAction Traffic-Prof-1  - appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```


Pour supprimer un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm tm trafficAction <name>
<!--NeedCopy-->
```

Exemple

```
rm tm trafficAction Traffic-Prof-1
<!--NeedCopy-->
```

Pour configurer les profils de trafic à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Trafic.**
2. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Trafic.**
3. Dans le volet d'informations, cliquez sur l'onglet Profils.
4. Dans l'onglet Profils, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau profil de trafic, cliquez sur **Ajouter.**
   - Pour modifier un profil de trafic existant, sélectionnez-le, puis cliquez sur **Modifier.**
5. Dans la boîte de dialogue **Créer un profil de traficou Configurer le profil** de trafic, spécifiez les valeurs des paramètres.
   - NOM* : nom (ne peut pas être modifié pour une action de session précédemment configurée.)
   - AppTimeout — AppTimeout
   - Connexion unique : authentification unique
   - Action SSO de formulaire — FormssoAction
   - Action SSO SAML—SAMLSSOAction
   - Enable Persistent Cookie—persistentCookie
   - Initier la déconnexion : initiateLogout
6. Cliquez sur **Créer** ou **sur OK**. Le profil de trafic que vous avez créé apparaît dans les stratégies de trafic, les profils et le volet Form SSO Profiles ou SAML SSO Profiles, selon le cas.

Prise en charge des expressions AAA.USER et AAA.LOGIN

L'expression AAA.USER est maintenant implémentée pour remplacer les expressions HTTP.REQ.USER existantes. L'expression AAA.USER est applicable pour gérer le trafic non HTTP, tel que le mécanisme de Secure Web Gateway (SWG) et d'accès basé sur les rôles (RBA). Les expressions AAA.USER sont équivalentes aux expressions HTTP.REQ.USER.

Vous pouvez utiliser l'expression lors de différentes actions ou configurations de profils.

À l'invite de commande, tapez :


```
add tm trafficAction <name> [SSO (ON|OFF)] [-userExpression <string>]

add tm trafficAction <name> [SSO (ON|OFF)] [-passwdExpression <string>]

<!--NeedCopy-->
```

Exemple

```
add tm trafficAction tm_act -SSO ON -userExpression "AAA.USER.NAME"

add tm trafficAction tm_act -SSO ON -userExpression "AAA.USER.PASSWD"

add tm trafficPolicy tm_pol true tm_act

bind lb vserver lb1 -policyName tm_pol -priority 2
<!--NeedCopy-->
```

> **Remarque :**
>
> Si vous utilisez l'expression HTTP.REQ.USER, un message d'avertissement « HTTP.REQ.USER est obsolète. Utiliser AAA.USER à la place » apparaît à l'invite de commande.

- **Expression AAA.LOGIN.** L'expression LOGIN représente la pré-connexion, également appelée demande de connexion. La demande de connexion peut provenir de NetScaler Gateway, de SAML IdP ou d'une authentification OAuth. NetScaler va extraire les attributs requis de la configuration de la politique. L'expression AAA.LOGIN contient les attributs, qui peuvent être récupérés en fonction des éléments suivants :
  - **AAA.LOGIN.USERNAME.** Le nom d'utilisateur (s'il est trouvé) est extrait de la demande de connexion en cours. La même expression appliquée à une demande de non-connexion (déterminée par une authentification, une autorisation et un audit) génère une chaîne vide.
  - **AAA.LOGIN.PASSWORD.** Le mot de passe utilisateur (s'il est trouvé) est récupéré à partir de la demande de connexion en cours. L'expression génère une chaîne vide si le mot de passe n'est pas trouvé.
  - **AAA.LOGIN.PASSWORD2.** Le deuxième mot de passe (s'il est trouvé) est récupéré à partir de la demande de connexion.
  - **AAA.LOGIN.DOMAINE.** Les informations de domaine sont récupérées à partir de la demande de connexion.
- **AAA.USER.ATTRIBUTE (« # »).** L'expression est utilisée pour stocker l'attribut utilisateur. Ici, # peut être soit une valeur entière (entre 1 et 16), soit une valeur de chaîne. Vous pouvez utiliser ces valeurs d'index en utilisant l'expression AAA.USER.ATTRIBUTE (« # »). Le module d'authentification, d'autorisation et d'audit recherche l'attribut sessions utilisateur et

`AAA.USER.ATTRIBUTE("##")` interroge la table de hachage pour cet attribut particulier. Par exemple, s'il `Attributes("samaccountname")` est défini, `AAA.USER.ATTRIBUTE("samaccountname")` interroge la table de hachage et récupère la valeur correspondant à `samaccountname`.

Politiques de trafic

Après avoir créé un ou plusieurs profils d'identification unique et de trafic de formulaire, vous créez des stratégies de trafic, puis vous liez les stratégies, globalement ou à un serveur virtuel de gestion du trafic, pour les mettre en œuvre.

Pour créer une stratégie de trafic à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add tm trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Exemple

```
add tm trafficPolicy Traffic-Pol-1 "HTTP.REQ.HEADER("Cookie").CONTAINS(
    "login=true")" Traffic-Prof-1
<!--NeedCopy-->
```

Pour modifier une stratégie de trafic à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set tm trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Exemple

```
set tm trafficPolicy Traffic-Pol-1 "HTTP.REQ.HEADER("Cookie").CONTAINS(
    "login=true")" Traffic-Prof-1
<!--NeedCopy-->
```

Pour lier globalement une stratégie de trafic à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
bind tm global -policyName <string> [-priority <priority>]
<!--NeedCopy-->
```

Exemple

```
bind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

Pour lier une stratégie de trafic à un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
bind lb vserver <name> -policy <policyName> [-priority <priority>]

bind cs vserver <name> -policy <policyName> [-priority <priority>]
<!--NeedCopy-->
```

Exemple

```
bind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1 -
   priority 1000
<!--NeedCopy-->
```

Pour annuler la liaison d'une stratégie de trafic globalement liée à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Exemple

```
unbind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

Pour délier une stratégie de trafic d'un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :


```
unbind lb vserver <name> -policy <policyname>

unbind cs vserver <name> -policy <policyname>
<!--NeedCopy-->
```

Exemple

```
unbind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1
<!--NeedCopy-->
```

Pour supprimer une stratégie de trafic à l'aide de l'interface de ligne de commande

Commencez par délier la stratégie de session de global, puis, à l'invite de commandes, tapez :

```
rm tm trafficPolicy <name>
<!--NeedCopy-->
```

Exemple

```
rm tm trafficPolicy Traffic-Pol-1
<!--NeedCopy-->
```

Pour configurer et lier des stratégies de trafic à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Trafic.**
2. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Trafic.**
3. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle stratégie de session, cliquez sur **Ajouter.**
   - Pour modifier une stratégie de session existante, sélectionnez-la, puis cliquez sur **Modifier.**
4. Dans la boîte de dialogue **Créer une stratégie** de **trafic ou Configurer la stratégie** de trafic, spécifiez les valeurs des paramètres.
   - NAME* : PolicyName (ne peut pas être modifié pour une stratégie de session précédemment configurée.)
   - Profile* — ActionName
   - Expression : règle (Vous saisissez des expressions en choisissant d'abord le type d'expression dans la liste déroulante située à l'extrême gauche sous la zone de texte Expression, puis en tapant votre expression directement dans la zone de texte de l'expression, ou en cliquant sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et en utilisant les listes déroulantes qui s'y trouvent pour construisez votre expression.)

5. Cliquez sur **Créer** ou **sur OK**. La stratégie que vous avez créée apparaît dans le volet d'informations de la page **Stratégies** et **profils** de session.

Formulaire de profils SSO

Pour activer et configurer l'authentification SSO basée sur les formulaires, vous devez d'abord créer un profil SSO.

> **Remarque**
>
> - L'authentification unique basée sur les formulaires ne fonctionne pas si le formulaire est personnalisé pour inclure Javascript.
> - Dans cette fonctionnalité, les termes « profil » et « action » signifient la même chose.

Pour créer un profil SSO de formulaire à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]

show tm formSSOAction [<name>]
<!--NeedCopy-->
```

Exemple

```
add tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-nameValuePair "loginID passwd" -responsesize "9096"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nvtype STATIC -submitMethod GET
 - sessTimeout 10 -defaultAuthorizationAction ALLOW
<!--NeedCopy-->
```

Pour modifier une connexion unique de formulaire à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]
```



```
<!--NeedCopy-->
```

Exemple

```
set tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nameValuePair "loginID passwd" -responsesize "9096"
-nvtype STATIC -submitMethod GET
 - sessTimeout 10 -defaultAuthorizationAction ALLOW
<!--NeedCopy-->
```

Pour supprimer un profil SSO de formulaire à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm tm formSSOAction <name>
<!--NeedCopy-->
```

Exemple

```
rm tm sessionAction SSO-Prof-1
<!--NeedCopy-->
```

Pour configurer les profils SSO de formulaire à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic applicatif > Politiques > Trafic**.
2. Dans le volet d'informations, cliquez sur l'onglet **Form SSO Profiles** .
3. Dans l'onglet Form SSO Profiles, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau profil SSO de formulaire, cliquez sur **Ajouter**.
   - Pour modifier un profil SSO de formulaire existant, sélectionnez-le, puis cliquez sur Modifier.
4. Dans la boîte de dialogue **Créer un profil SSO deformulaire ou Configurer un profil SSO de** formulaire, spécifiez les valeurs des paramètres :
   - NOM* : nom (ne peut pas être modifié pour une action de session précédemment configurée.)
   - URL de l'action*—ActionUrl
   - Champ Nom d'utilisateur*—Champ utilisateur
   - Champ de mot de passe*—PassField
   - Expression* : règle de réussite SSO
   - Paire de valeurs de nom—NameValuePair

- Taille de la réponse : taille de la réponse
- Extraction : type NV
- Méthode d'envoi : méthode d'envoi

5. Cliquez sur **Créer** ou **sur OK**, puis sur **Fermer**. Le profil SSO de formulaire que vous avez créé apparaît dans le volet **Stratégies de trafic**, **Profils**et **Profils SSO de formulaire** .

Profils SSO SAML

Pour activer et configurer l'authentification SSO SAML, vous devez d'abord créer un profil SSO SAML.

Pour créer un profil SSO SAML à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
<!--NeedCopy-->
```

Exemple

```
add tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
<!--NeedCopy-->
```

Pour modifier un SSO SAML à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
<!--NeedCopy-->
```

Exemple

```
set tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
<!--NeedCopy-->
```


Pour supprimer un profil SSO SAML à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm tm samlSSOProfile <name>
<!--NeedCopy-->
```

Exemple

```
rm tm sessionAction saml-SSO-Prof-1
<!--NeedCopy-->
```

Pour configurer un profil SSO SAML à l'aide de l'utilitaire de configuration

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Trafic.**
2. Dans le volet d'informations, cliquez sur l'onglet **Profils SSO SAML** .
3. Dans l'onglet **Profils SSO SAML**, effectuez l'une des opérations suivantes :
   - Pour créer un nouveau profil SSO SAML, cliquez sur **Ajouter.**
   - Pour modifier un profil SSO SAML existant, sélectionnez-le, puis cliquez sur **OuvrirModifier**.
4. Dans la boîte de dialogue **Créer des profils SSOSAML ou Configurer les profils SSO** SAML, définissez les paramètres suivants :
   - Nom*
   - Nom du certificat de signation*
   - URL ACS *
   - Règle de l'état du relais *
   - Envoyer mot de passe
   - Nom de l'émetteur
5. Cliquez sur **Créer** ou sur **OK**, puis sur **Fermer.** Le profil SSO SAML que vous avez créé apparaît dans le volet Stratégies de trafic, profils et profils SSO SAML.

Délai d'expiration de session pour OWA 2010

Vous pouvez désormais forcer le délai d'expiration des connexions OWA 2010 après une période d'inactivité spécifiée. OWA envoie des requêtes Keepalive répétées au serveur pour éviter les délais d'expiration. Le fait de garder les connexions ouvertes peut interférer avec l'authentification unique.

Pour forcer l'expiration d'OWA 2010 après une période spécifiée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :


```
add tm trafficAction <actname> [-forcedTimeout <forcedTimeout> -
    forcedTimeoutVal <mins>]
<!--NeedCopy-->
```

Par <actname>, remplacez votre politique de trafic par un nom. <mins>Remplacez par le nombre de minutes après lequel vous souhaitez déclencher un délai d'attente forcé. <forcedTimeout>Remplacez par l'une des valeurs suivantes :

-**START** — Démarre le minuteur pour un délai d'expiration forcé si aucun minuteur n'a déjà été démarré. S'il existe un minuteur en cours d'exécution, n'a aucun effet.
-**STOP — Arrête** une minuterie en cours d'exécution. Si aucune minuterie n'est trouvée, n'a aucun effet.
-**RESET** — Redémarre une minuterie en cours d'exécution. Si aucune minuterie en cours d'exécution n'est trouvée, démarre une minuterie comme si l'option START avait été utilisée.

```
add tm trafficPolicy <polname> <rule> <actname>
<!--NeedCopy-->
```

Par <polname>, remplacez votre politique de trafic par un nom. Par <rule>, remplacez une règle dans la politique avancée de NetScaler.

```
bind lb vserver <vservername>  - policyName <name> -priority <number>
<!--NeedCopy-->
```

Par <vservername>, remplacez le nom du serveur virtuel de gestion du trafic d'authentification, d'autorisation et d'audit. <priority>Remplacez par un entier désignant la priorité de la politique.

Exemple

```
add tm trafficAction act-owa2010timeout -forcedTimeout RESET -
    forcedTimeoutVal 10
add tm trafficPolicy pol-owa2010timeout true act-owa2010timeout
bind lb vserver vs-owa2010 -policyName pol-owa2010timeout -priority 10
<!--NeedCopy-->
```

Limitation du débit pour NetScaler Gateway

May 5, 2023

La fonctionnalité de limitation de débit de NetScaler Gateway vous permet de définir la charge maximale pour une entité réseau ou une entité virtuelle donnée sur l'appliance NetScaler Gateway. Étant

donné que l'appliance NetScaler Gateway consomme tout le trafic non authentifié, elle est souvent exposée à des demandes de traitement à un rythme élevé. La fonctionnalité de limitation du débit vous permet de configurer l'appliance NetScaler Gateway pour surveiller le débit de trafic associé à une entité et prendre des mesures préventives, en temps réel, en fonction du trafic. Pour plus d'informations sur le fonctionnement de la limitation du débit dans une appliance NetScaler, consultez la section Limitation du débit.

NetScaler est doté d'une fonction de limitation du débit qui protège les serveurs principaux en cas de débit imprévu. Étant donné que la fonctionnalité de NetScaler ne permettait pas de traiter le trafic non authentifié géré par NetScaler Gateway, NetScaler Gateway avait besoin de sa propre fonctionnalité de limitation de débit. Cela est nécessaire pour vérifier un taux imprévu de demandes provenant de diverses sources auxquelles l'appliance NetScaler Gateway est exposée. Par exemple, les demandes de connexion/de contrôle non authentifiées et certaines API exposées pour les validations des utilisateurs finaux ou des appareils.

Cas d'utilisation courants pour la limitation de débit

- Limitez le nombre de demandes par seconde à partir d'une URL.
- Supprimer une connexion basée sur les cookies reçus à la demande d'un hôte particulier si la demande dépasse la limite de débit.
- Limitez le nombre de requêtes HTTP qui arrivent du même hôte (avec un masque de sous-réseau particulier) et qui ont la même adresse IP de destination.

Configurer la limitation de débit pour NetScaler Gateway

Composants requis

Un serveur virtuel d'authentification configuré.

Points à noter

- Au cours des étapes de configuration, un exemple d'identificateur de limite est configuré. La même chose peut être configurée avec tous les paramètres pris en charge comme le sélecteur de flux, mode. Pour obtenir une description exhaustive des capacités de limitation de débit, voir Limitation de débit.
- La stratégie peut également être liée à un serveur virtuel VPN comme suit. Vous avez besoin d'un serveur virtuel VPN configuré pour lier les stratégies à l'aide de la commande suivante.

```
bind vpn vserver  -policy denylogin  - pri 1  - type aaa_request
<!--NeedCopy-->
```


- AAA_REQUEST est un nouveau point de liaison introduit pour les stratégies de répondeur. Les stratégies configurées à ce point de liaison sont appliquées à toutes les demandes entrantes sur le serveur virtuel spécifié. Les stratégies sont traitées pour le trafic non authentifié/de contrôle avant tout autre traitement.
- La liaison de la politique au serveur virtuel NetScaler Gateway permet de limiter le débit au point de liaison AAA_REQUEST pour tout le trafic consommé par NetScaler Gateway, y compris les demandes non authentifiées.
- La liaison de la stratégie à un débit de serveur virtuel d'authentification limite les demandes non authentifiées/de contrôle qui touchent le serveur virtuel d'authentification.

Pour configurer la limitation de débit à l'aide de l'interface de ligne de commande, à l'invite de commandes, tapez les commandes suivantes :

```
add limitIdentifier <limitIdentifier name> -threshold <positive_integer
    > -timeslice <positive_integer> -mode <mode type>
<!--NeedCopy-->
```

Exemple :

```
add limitIdentifier limit_one_login -threshold 10 -timeslice 4294967290
    -mode REQUEST_RATE
<!--NeedCopy-->
```

```
add responderaction denylogin respondwith  ' "HTTP/1.1 200 OK\r\n\r\n"
    +  "Request is denied due to unusual rate" '
<!--NeedCopy-->
```

```
add responder policy denylogin 'sys.check_limit("limit_one_login")'
    denylogin
<!--NeedCopy-->
```

```
bind authentication vserver <vserver name> -policy denylogin -pri 1 -
    type aaa_request
<!--NeedCopy-->
```

Exemple :

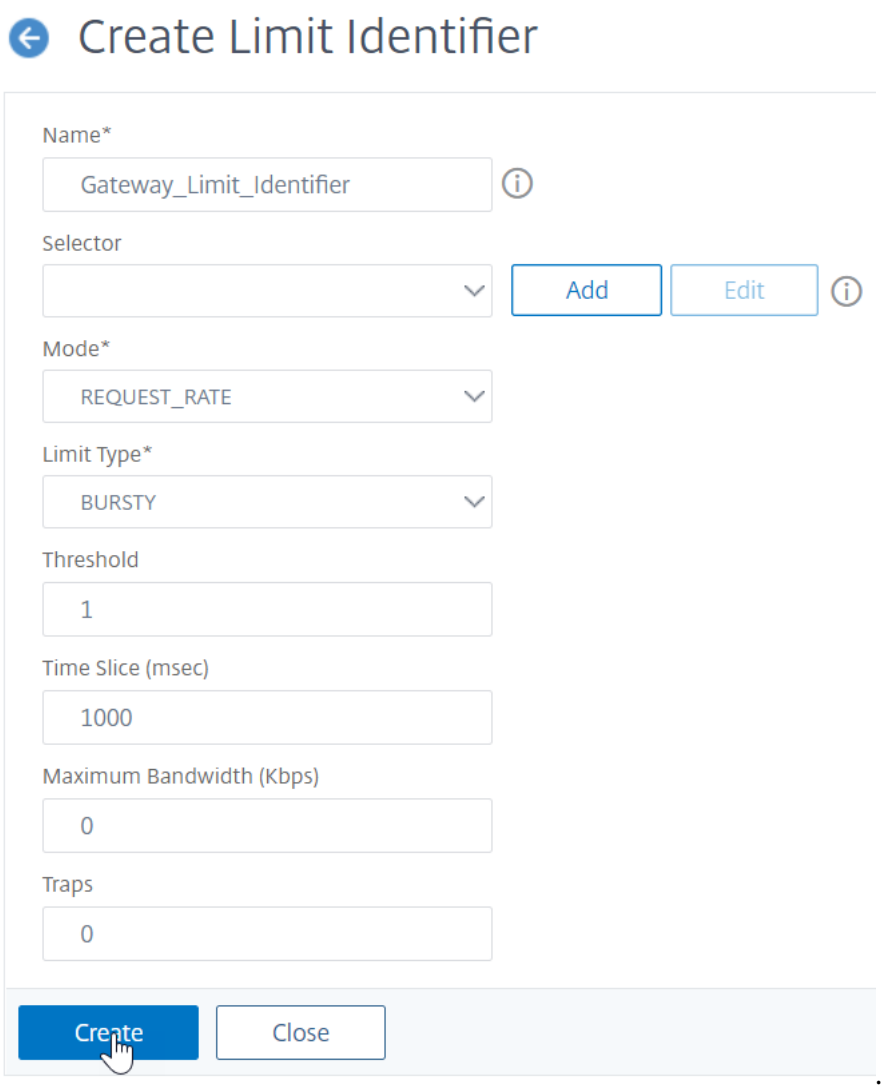
```
bind authentication vserver authvserver -policy denylogin -pri 1 -
    type aaa_request
<!--NeedCopy-->
```


Description des paramètres

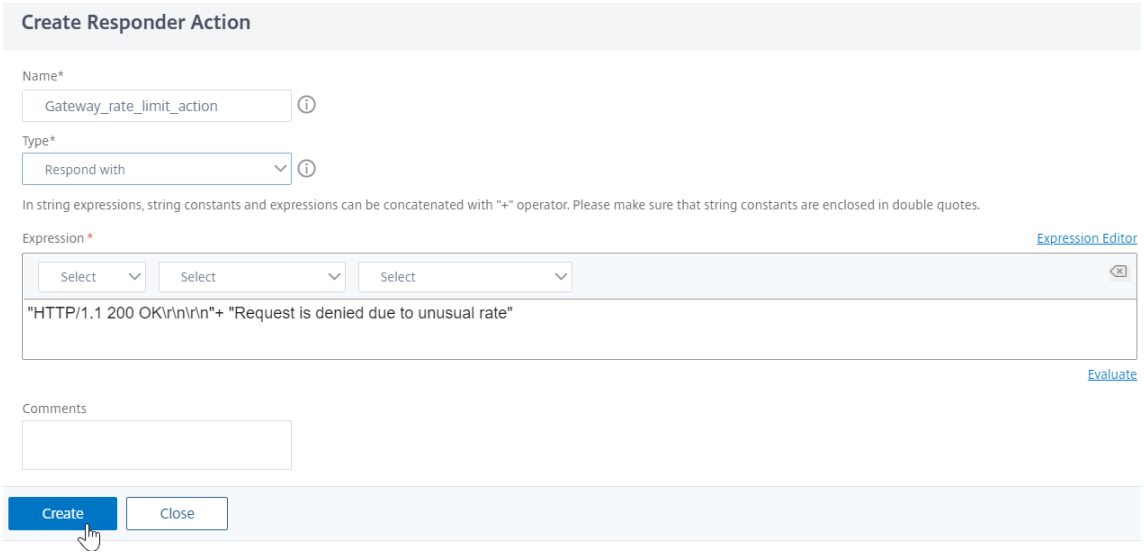
- **LimitIdentifier :** nom d'un identificateur de limite de taux. Doit commencer par une lettre ASCII ou un caractère de soulignement (_) et ne doit être composé que de caractères alphanumériques ou de soulignement ASCII. Les mots réservés ne doivent pas être utilisés. Il s'agit d'un argument obligatoire. Longueur maximale : 31
- **threshold :** nombre maximal de demandes autorisées dans la tranche de temps donnée lorsque les demandes (le mode est défini sur REQUEST_RATE) sont suivies par tranche de temps. Lorsque les connexions (le mode est défini sur CONNECTION) sont suivies, il s'agit du nombre total de connexions qui seraient laissées passer. Valeur par défaut : 1 Valeur minimale : 1 Valeur maximale : 4294967295
- **TimeSlice -** Intervalle de temps, en millisecondes, spécifié en multiples de 10, pendant lequel les demandes sont suivies pour vérifier si elles dépassent le seuil. L'argument n'est nécessaire que lorsque le mode est défini sur REQUEST_RATE. Valeur par défaut : 1000 Valeur minimale : 10 Valeur maximale : 4294967295
- **mode -** Définit le type de trafic à suivre.
  - REQUEST_RATE - Effectue le suivi des requêtes/tranche de temps.
  - CONNEXION - Effectue le suivi des transactions actives.

Pour configurer la limitation du débit à l'aide de l'interface graphique NetScaler :

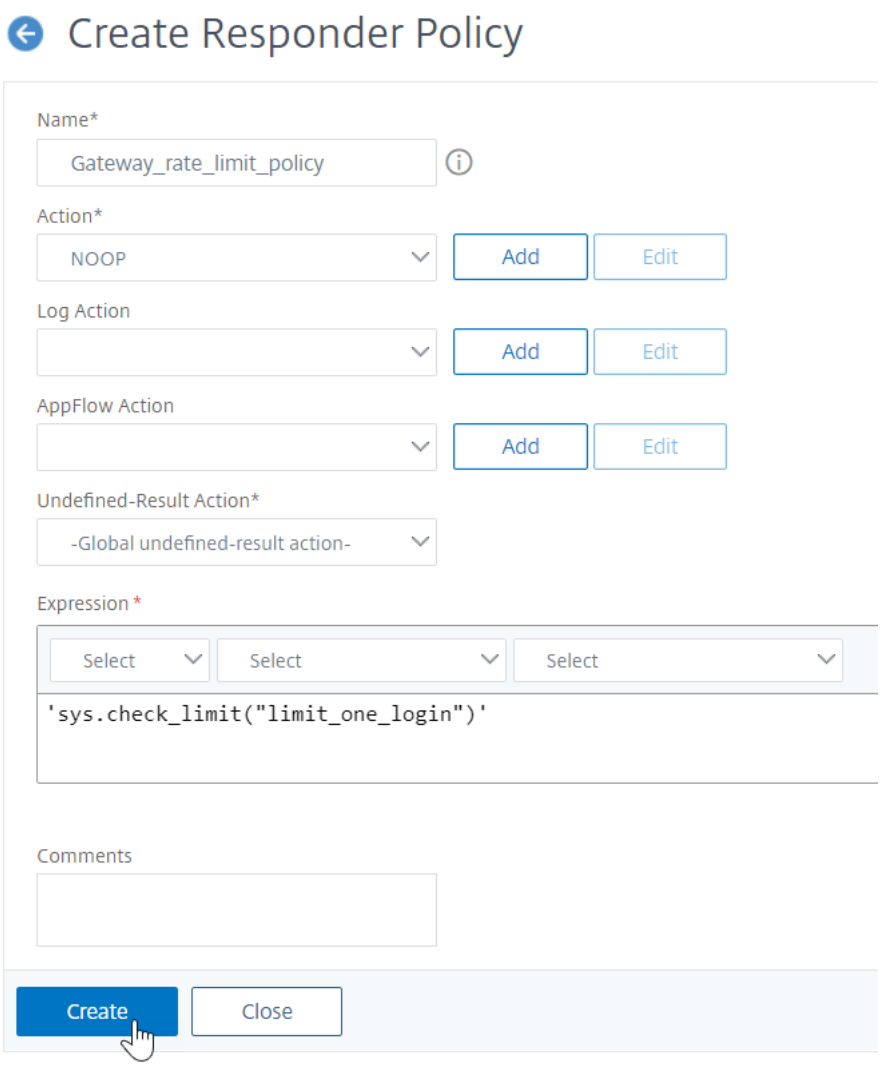
1. Accédez à **AppExpert > Limitation de débit > Identificateurs de limite**, cliquez sur **Ajouter** et spécifiez les détails pertinents comme indiqué dans la section CLI.



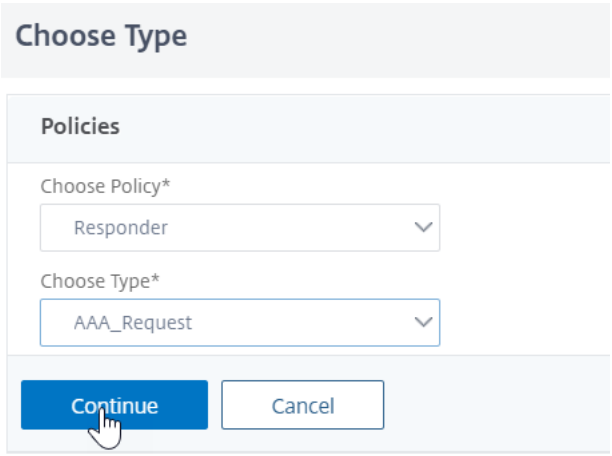
2. Accédez à **AppExpert>Responder>Stratégies**. Sur la page **Stratégies de répondeur**, cliquez sur **Ajouter**.
3. Sur la page **Créer une stratégie de répondeur**, créez une stratégie de répondeur avec une action de répondeur qui possède l'identificateur de limite.
4. Pour créer une action de répondeur, cliquez sur **Ajouter** en regard de **Action** et saisissez un nom pour l'action du répondeur.
5. Sélectionnez le type **Répondre avec** dans le menu déroulant, spécifiez l'expression suivante, « HTTP/1.1 200 OK\r\n\r\n » + « La demande est refusée en raison d'un taux inhabituel », puis cliquez sur **Créer**.



6. Pour créer une stratégie de répondeur, sur la page **Créer une stratégie de répondeur**, entrez un nom pour la stratégie de répondeur, spécifiez l'expression suivante, 'sys.check_limit (« limit_one_login ») ', puis cliquez sur **Créer**.



7. Liez la stratégie de répondeur au serveur virtuel d'authentification.
   - Accédez à **Security>AAA-Application Traffic>Virtual Server**.
   - Sélectionnez le serveur virtuel.
   - Ajoutez une stratégie.
   - Choisissez la stratégie de répondeur que vous souhaitez lier au serveur, définissez la priorité.
   - Choisissez le type **AAA-REQUEST** et cliquez sur **Continuer**.



> **Remarque :** Vous pouvez également activer la limitation de débit au point de liaison AAA_REQUEST pour le serveur virtuel VPN.

Configuration pour les cas d'utilisation courants d'application de la limitation de débit à NetScaler Gateway

Voici des exemples de commandes permettant de configurer des cas d'utilisation courants.

- Limitez le nombre de demandes par seconde à partir d'une URL.

```
add stream selector ipStreamSelector http.req.url “client.ip.src”

add ns limitIdentifier ipLimitIdentifier -threshold 4 -timeslice 1000 -mode request_rate -limitType smooth -selectorName ip StreamSelector

add responder policy ipLimitResponderPolicy “http.req.url.contains(\” myasp.asp\” ) && sys.check_limit(\” ipLimitIdentifier\” )” myWebSiteRedirectAction

bind authentication virtual server authvserver -policy denylogin -pri 1 -type aaa_request
<!--NeedCopy-->
```

- Supprimer une connexion basée sur les cookies reçus à la demande de www.yourcompany.com si la demande dépasse la limite de débit.

```
add stream selector cacheStreamSelector “http.req.cookie.value(\” mycookie\” )” “client.ip.src.subnet(24)”

```



```
add ns limitIdentifier myLimitIdentifier -Threshold 2 -
    timeSlice 3000 -selectorName reqCookieStreamSelector

add responder action sendRedirectURL redirect `"http://www.
    mycompany.com"` + http.req.url'

add responder policy rateLimitCookiePolicy

 “http.req.url.contains(\www.yourcompany.com) && sys.check_limit
    (\” myLimitIdentifier\” )”  sendRedirectUrl

<!--NeedCopy-->
```

- Limitez le nombre de requêtes HTTP qui arrivent du même hôte (avec un masque de sous-réseau de 32) et qui ont la même adresse IP de destination.

```
add stream selector ipv6_sel  “CLIENT.IPv6.src.subnet(32)” CLIENT
    .IPv6.dst

add ns limitIdentifier ipv6_id -imeSlice 20000 -selectorName
    ipv6_sel

add lb vserver ipv6_vip HTTP 3ffe:: 209 80 -persistenceType NONE
     -cltTime

add responder action redirect_page redirect  “\” `http://
    redirectpage.com/\” "`

add responder policy ipv6_resp_pol  “SYS.CHECK_LIMIT(\” ipv6_id\
    ” )”  redirect_page

bind responder global ipv6_resp_pol 5 END -type DEFAULT
<!--NeedCopy-->
```

Autorisation de l’accès des utilisateurs aux ressources de l’application

November 16, 2022

Vous pouvez contrôler les ressources auxquelles un utilisateur authentifié peut accéder au sein d’une application.

Pour ce faire, associez une politique d’autorisation à chacun des utilisateurs, soit individuellement, soit en associant la politique à un groupe d’utilisateurs. La politique d’autorisation doit spécifier les

éléments suivants :

- **Rule.** La ressource à laquelle l'accès doit être autorisé. Cela peut être spécifié à l'aide d'expressions de base ou avancées.
- **Action.** Si l'accès à la ressource doit être autorisé ou refusé.

Par défaut, l'accès à toutes les ressources d'une application est **REFUSÉ** à tous les utilisateurs. Toutefois, vous pouvez modifier cette action d'autorisation par défaut pour **AUTORISER** l'accès à tous les utilisateurs (en définissant les paramètres de session dans le profil de session ou en définissant les paramètres de session globaux).

> **Avertissement**
>
> Pour une sécurité optimale, Citrix vous recommande de ne pas modifier l'action d'autorisation par défaut de DENY en ALLOW. Il est plutôt conseillé de créer des politiques d'autorisation spécifiques pour les utilisateurs qui ont besoin d'accéder à des ressources spécifiques.

Pour configurer l'autorisation à l'aide de l'interface de ligne de commande

1. Configurez la politique d'autorisation.

   ns-cli-prompt> **add authorization policy <name> <rule> <action>**

2. Associez la politique à l'utilisateur ou au groupe approprié.

   - Liez la politique à un utilisateur spécifique.

     ns-cli-prompt> **bind aaa user <username> -policy** <policyname>

   - Liez la politique à un groupe spécifique.

     ns-cli-prompt> **bind aaa group <groupName> -policy** <policyname>

Pour configurer l'autorisation à l'aide de l'interface graphique (onglet Configuration)

1. Créez la politique d'autorisation.

   Accédez à **Sécurité > AAA - Trafic applicatif > Politiques > Autorisation**, cliquez sur **Ajouter**, puis définissez la politique selon vos besoins.

2. Associez la politique à l'utilisateur ou au groupe approprié.

   Accédez à **Sécurité > AAA - Trafic applicatif > Utilisateurs** ou **groupes**, puis modifiez l'utilisateur ou le groupe concerné pour l'associer à la politique d'autorisation.

Exemples de configurations d'autorisation

Voici quelques exemples de configurations pour autoriser l'accès des utilisateurs à certaines ressources de l'application. Notez qu'il s'agit de commandes CLI. Vous pouvez faire des configurations similaires à l'aide de l'interface graphique, bien que vous ne devez pas placer l'expression entre guillemets («).

- “‘
  ajouter la politique d'autorisation authzpol1 « HTTP.REQ.URL.SUFFIX.EQ (« gif ») » ALLOW
  “‘
  - ```
    bind aaa user user1 -policy authzpol1
    ```
- “‘
  ajouter une politique d'autorisation authzpol2 « HTTP.REQ.URL.SUFFIX.EQ (« png ») » DENY
  “‘
  - ```
    bind aaa group group1 -policy authzpol2
    <!--NeedCopy-->
    ```

Auditer les sessions authentifiées

May 9, 2023

Vous pouvez configurer l'appliance NetScaler pour conserver un journal de tous les événements déclenchés lors d'une session authentifiée. À l'aide de ces informations, vous pouvez vérifier l'état et les informations d'état, afin de consulter l'historique des utilisateurs par ordre chronologique.

Pour ce faire, définissez une politique d'audit qui précise les éléments suivants :

- **Type de journal.** Les journaux peuvent être stockés à distance (syslog) ou localement sur l'appliance NetScaler (nslog).
- **Rule.** Les conditions dans lesquelles les journaux sont stockés.
- **Action.** Détails du serveur de journaux et autres détails relatifs à la création des entrées de journal.

Cette politique d'audit peut être configurée à différents niveaux : au niveau de l'utilisateur, au niveau du groupe, de l'authentification, de l'autorisation et de l'audit du serveur virtuel, et au niveau du système global. Les politiques configurées au niveau de l'utilisateur ont la priorité la plus élevée.

> **Remarque**
>
> Cette rubrique détaille les étapes d'utilisation de syslog. Apportez les modifications nécessaires

> pour utiliser nslog.

Pour configurer l'audit Syslog à l'aide de l'interface de ligne de commande

1. Configurez le serveur d'audit avec les paramètres de journal appropriés.

   ns-cli-prompt<name> <serverIP> > **ajouter un syslogAction d'audit \ \...**

2. Configurez la politique d'audit en associant le serveur d'audit.

   ns-cli-prompt<name> <rule> > **ajouter une politique d'audit**SyslogPolicy \ \ \ <action>

3. Associez la politique d'audit à l'une des entités suivantes :

   - Liez la politique à un utilisateur spécifique.

     ns-cli-prompt<userName> <policyname> > **lier l'utilisateur aaa** \-policy \…

   - Liez la politique à un groupe spécifique.

     ns-cli-prompt<groupName> <policyname> > **lier le groupe aaa** \-policy \…

   - Liez la politique à un serveur virtuel d'authentification, d'autorisation et d'audit.

     ns-cli-prompt<name> <policyname> > **Authentification par liaison vserver** \ -policy \…

   - Liez la politique de manière globale à l'appliance NetScaler.

     ns-cli-prompt> bind tm global -PolicyName \... <policyname>

Pour configurer l'audit Syslog à l'aide de l'interface graphique (onglet Configuration)

1. Configurez le serveur d'audit et la politique.

   Accédez à **Sécurité > AAA - Trafic des applications > Politiques > Audit > Syslog**, puis configurez le serveur et la politique dans les onglets appropriés.

2. Associez la politique à l'une des options suivantes :

   - Liez la politique à un utilisateur spécifique.

     Accédez à **Sécurité > AAA - Trafic d'applications > Utilisateurs**, puis associez la politique d'autorisation à l'utilisateur concerné.

   - Liez la politique à un groupe spécifique.

     Accédez à **Sécurité > AAA - Trafic d'applications > Groupes**, puis associez la politique d'autorisation au groupe concerné.

   - Liez la politique à un serveur virtuel d'authentification, d'autorisation et d'audit.

     Accédez à **Sécurité > AAA - Trafic d'applications > Serveurs virtuels**, puis associez la politique d'autorisation au serveur virtuel concerné.

- Liez la politique de manière globale à l'appliance NetScaler.

  Accédez à **Sécurité > AAA - Trafic applicatif > Politiques > Audit > Syslog ou**Nslog****, sélectionnez la politique d'autorisation, puis cliquez sur **Action > Liaisons globales pour lier la politique de** manière globale.

NetScaler en tant que proxy Active Directory Federation Services

May 5, 2023

Active Directory Federation Services (ADFS) est un service Microsoft qui permet aux clients authentifiés par Active Directory d'accéder à des ressources extérieures au centre de données de l'entreprise. Une batterie de serveurs ADFS permet aux utilisateurs internes d'accéder à des services externes hébergés dans le cloud. Mais dès que les utilisateurs externes entrent dans le mix, ils doivent disposer d'un moyen de se connecter à distance et d'accéder aux services basés sur le cloud via une identité fédérée. La plupart des entreprises ne préfèrent pas que le serveur ADFS reste exposé dans la zone démilitarisée. Par conséquent, le proxy ADFS joue un rôle essentiel dans la connectivité des utilisateurs distants et l'accès aux applications.

Depuis plus de dix ans, l'appliance NetScaler joue des rôles similaires en matière de connectivité des utilisateurs distants et d'accès aux applications. L'appliance NetScaler devient la solution préférée à utiliser comme proxy ADFS pour prendre en charge une nouvelle implémentation ADFS afin d'activer les services suivants :

- Connectivité sécurisée.
- Authentification et gestion de l'identité fédérée.

Pour plus d'informations sur NetScaler en tant qu'IdP SAML, consultez NetScaleren tant qu'IdP SAML.

Avantages du proxy ADFS

- Réduit l'encombrement dans la zone démilitarisée pour répondre aux besoins de la plupart des entreprises.
- Fournit une expérience SSO aux utilisateurs finaux.
- Prend en charge de nombreuses méthodes de pré-authentification et permet une authentification multifactorielle.
- Prend en charge les clients actifs et passifs.

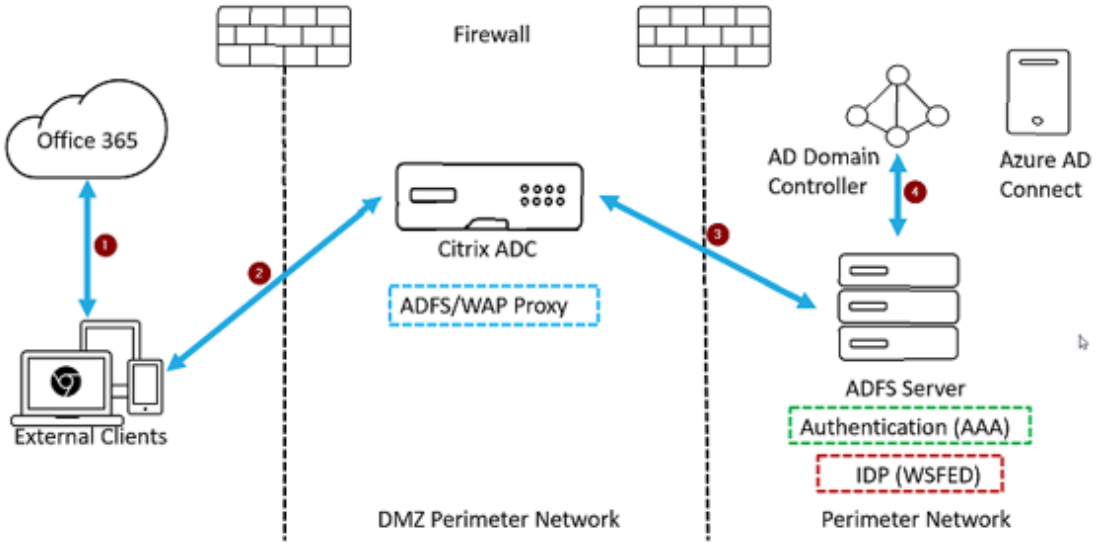
Conditions préalables à l'utilisation de NetScaler en tant que proxy ADFS

Avant de configurer l'appliance NetScaler en tant que proxy ADFS, assurez-vous que les conditions préalables suivantes sont remplies :

- Une appliance NetScaler dotée de la version 12.1 ou ultérieure.
- Serveur ADFS de domaine.
- Certificat SSL de domaine.
- Adresse IP virtuelle pour le serveur virtuel de commutation de contenu.
- Activez les fonctionnalités d'équilibrage de charge, de déchargement SSL, de commutation de contenu, de réécriture, d'authentification, d'autorisation et d'audit du trafic sur l'appliance NetScaler.

Configurer l'appliance NetScaler en tant que proxy ADFS

Pour réaliser ce cas d'utilisation, configurez NetScaler en tant que proxy ADFS dans une zone DMZ. Le serveur ADFS est configuré avec le contrôleur de domaine AD dans le back-end.



1. Une demande du client pour accéder à Microsoft Office365 est redirigée vers NetScaler déployé en tant que proxy ADFS.
2. Les informations d'identification de l'utilisateur sont transmises au serveur ADFS.
3. Le serveur ADFS authentifie les informations d'identification auprès de l'AD local du domaine.
4. Le serveur ADFS, une fois les informations d'identification validées avec AD, génère un jeton qui est transmis à Microsoft Office365 pour l'établissement de la session.

Voici les étapes de haut niveau nécessaires à la configuration de l'appliance NetScaler avant de la configurer en tant que proxy ADFS.

À l'invite de commandes NetScaler, tapez les commandes suivantes :

1. Créez un profil SSL pour le backend et activez le SNI dans le profil SSL. Désactivez SSLv3/TLS1.


```
add ssl profile <new SSL profile> -sslprofileType backEnd -sniEnable
ENABLED -ssl3 DISABLED -tls1 DISABLED -commonName <FQDN of ADFS>
```

2. Désactivez SSLv3/TLS1 pour le service.

```
set ssl service <adfs service name> -sslProfile <SSL profile created in
 the above step>
```

3. Activez l'extension SNI pour les poignées de contact du serveur principal.

   - `set vpn parameter -backendServerSni ENABLED`
   - `set ssl parameter -denySSLReneg NONSECURE`

Configurer l'appliance NetScaler en tant que proxy ADFS à l'aide de l'interface de ligne de commande

Les sections suivantes sont classées en fonction de la nécessité d'effectuer les étapes de configuration.

Pour configurer le service ADFS

1. Configurez le service ADFS sur le serveur NetScaler pour ADFS.

```
add service <Domain_ADFS_Service> <ADFS Server IP> SSL 443 -gslb NONE -
maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF
-cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
```

   Exemple

   add service CTXTEST_ADFS_Service 1.1.1.1 SSL 443 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

2. Configurez le FQDN pour le serveur virtuel de commutation de contenu et activez le SNI.

```
set ssl service <Domain_ADFS_Service> -SNIEnable ENABLED -commonName <
sts.domain.com>
```

   Exemple

   set ssl service CTXTEST_ADFS_Service -SNIEnable ENABLED -commonName sts.ctxtest.com

Pour configurer le serveur virtuel d'équilibrage de charge ADFS

> **Important**
>
> Un certificat SSL de domaine (SSL_CERT) est requis pour sécuriser le trafic.

1. Configurez le serveur virtuel d'équilibrage de charge ADFS.

   ```
   add lb vserver <Domain_ADFS_LBVS> SSL <IP_address> -persistenceType
   NONE -cltTimeout 180
   ```

   Exemple

   ```
   add lb vserver CTXTEST_ADFS_LBVS SSL 192.168.1.0 -persistenceType NONE
   -cltTimeout 180
   ```

2. Liez le serveur virtuel d'équilibrage de charge ADFS au service ADFS.

   ```
   bind lb vserver <Domain_ADFS_LBVS> <Domain_ADFS_Service>
   ```

   Exemple

   ```
   bind lb vserver CTXTEST_ADFS_LBVS CTXTEST_ADFS_Service
   ```

3. Liez une paire de clés de certificat de serveur virtuel SSL.

   ```
   bind ssl vserver <Domain_ADFS_LBVS> -certkeyName <SSL_CERT>
   ```

   Exemple

   ```
   bind ssl vserver CTXTEST_ADFS_LBVS -certkeyName ctxtest_newcert_2019
   ```

Pour configurer un serveur virtuel de commutation de contenu pour un domaine

> **Remarque**
>
> Une adresse IP virtuelle gratuite (par exemple, 2.2.2.2), associée à une adresse IP publique, est requise pour un serveur virtuel de commutation de contenu. Il doit être accessible à la fois pour le trafic externe et interne.

1. Créez un serveur virtuel de commutation de contenu avec un service VIP gratuit.

   ```
   add cs vserver <Domain_CSVS> SSL <FREE VIP> 443 -cltTimeout 180 -
   persistenceType NONE
   ```

   Exemple

   ```
   add cs vserver CTXTEST_CSVS SSL 2.2.2.2 443 -cltTimeout 180 -persistenceType
    NONE
   ```

2. Liez le serveur virtuel de commutation de contenu au serveur virtuel d'équilibrage de charge.

   ```
   bind cs vserver <Domain_CSVS> -lbvserver <Domain_ADFS_LBVS>
   ```

   Exemple

   - `bind cs vserver CTXTEST_CSVS -lbvserver CTXTEST_ADFS_LBVS`
   - `set ssl vserver CTXTEST_CSVS -sessReuse DISABLED`

3. Liez une paire de clés de certificat de serveur virtuel SSL.

   ```
   bind ssl vserver <Domain_CSVS> -certkeyName <SSL_CERT>
   ```

   Exemple

   ```
   bind ssl vserver CTXTEST_CSVS -certkeyName ctxtest_newcert_2019
   ```

Protocoles pris en charge

Les protocoles fournis par Microsoft jouent un rôle essentiel dans l'intégration à l'appliance NetScaler. NetScaler en tant que proxy ADFS prend en charge les protocoles suivants :

- **WS-Federation**. Pour plus de détails, voir Protocole Web Services Federation.
- **ADFSPIP**. Pour plus de détails, voir Conformité au protocole d'intégration du proxy Active Directory Federation Service

> **Remarque**
>
> L'appliance NetScaler ne prend pas en charge l'authentification par certificat de l'appareil lorsqu'elle est déployée en tant que proxy ADFS.

Protocole Web Services Federation

May 5, 2023

Web Services Federation (WS-Federation) est un protocole d'identité qui permet à un service de jeton de sécurité (STS) d'un domaine de confiance de fournir des informations d'authentification à un STS d'un autre domaine d'approbation lorsqu'il existe une relation d'approbation entre les deux domaines.

Avantages de WS-Federation

WS-Federation prend en charge les clients actifs et passifs tandis que le fournisseur d'identité SAML ne prend en charge que les clients passifs.

- Les clients actifs sont des clients natifs Microsoft tels que Outlook et des clients Office (Word, PowerPoint, Excel et OneNote).
- Les clients passifs sont des clients basés sur un navigateur tels que Google Chrome, Mozilla Firefox et Internet Explorer.

Conditions préalables à l'utilisation de NetScaler en tant que WS-Federation

Avant de configurer l'appliance NetScaler en tant que proxy ADFS, vérifiez les points suivants :

- Active Directory.
- Certificat SSL de domaine.
- Le certificat SSL NetScaler et le certificat de signature du jeton ADFS sur le serveur ADFS doivent être identiques.

> **Important**
>
> IDP SAML est désormais capable de gérer le protocole WS-Federation. Par conséquent, pour configurer l'IdP WS-Federation, vous devez configurer le fournisseur d'identité SAML. Aucune interface utilisateur ne mentionne explicitement WS-Federation.

Fonctionnalités prises en charge par NetScaler lorsqu'il est configuré en tant que proxy ADFS et WS-Federation IdP

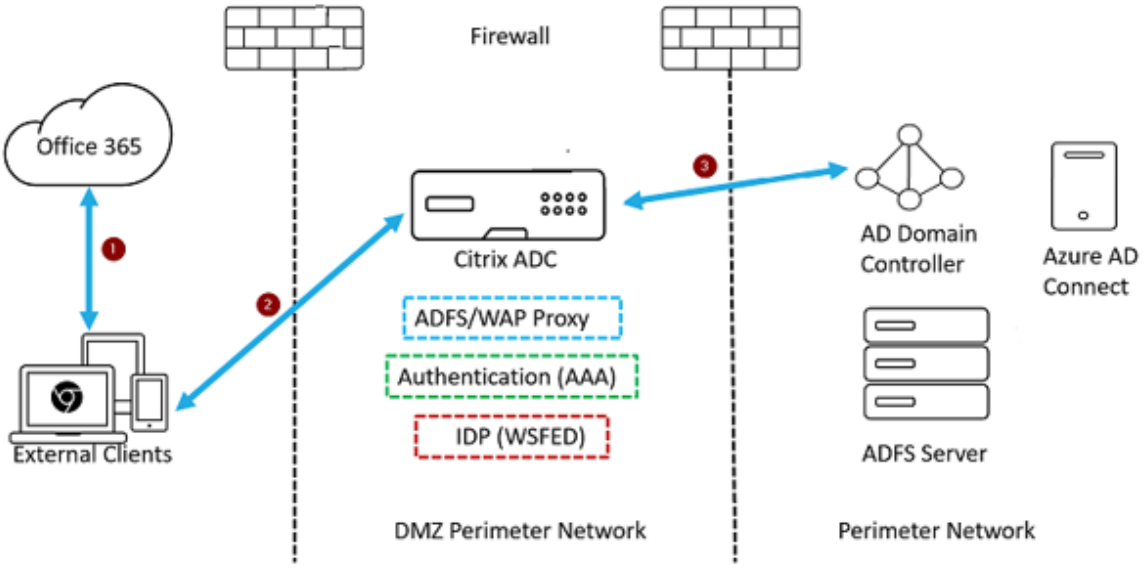
Le tableau suivant répertorie les fonctionnalités prises en charge par l'appliance NetScaler lorsqu'elle est configurée en tant que proxy ADFS et WS-Federation IdP.

Fonctionnalités	Configurer l'appliance NetScaler en tant que proxy ADFS	NetScaler en tant qu'IdP WS-Federation	NetScaler en tant qu'ADFSPIP
Équilibrage de charge	Oui	Oui	Oui
Résiliation SSL	Oui	Oui	Oui
Limitation de débit	Oui	Oui	Oui
Consolidation (réduit l'empreinte du serveur DMZ et sauvegarde l'adresse IP publique)	Oui	Oui	Oui
Pare-feu applicatif Web (WAF)	Oui	Oui	Oui
Déchargement de l'authentification vers l'appliance NetScaler	Oui	Oui (clients actifs et passifs)	Oui
Authentification unique (SSO)	Oui	Oui (clients actifs et passifs)	Oui

Fonctionnalités	Configurer l'appliance NetScaler en tant que proxy ADFS	NetScaler en tant qu'IdP WS-Federation	NetScaler en tant qu'ADFSPIP
Authentification multifacteur (nFactor)	Non	Oui (clients actifs et passifs)	Oui
Authentification multifacteur Azure	Non	Oui (clients actifs et passifs)	Oui
La batterie de serveurs ADFS peut être évitée	Non	Oui	Oui

Configurer l'appliance NetScaler en tant qu'IdP WS-Federation

Configurez NetScaler en tant qu'IdP WS-Federation (IDP SAML) dans une zone DMZ. Le serveur ADFS est configuré avec le contrôleur de domaine AD dans le back-end.



1. La demande du client à Microsoft Office365 est redirigée vers l'appliance NetScaler.
2. L'utilisateur saisit les informations d'identification pour l'authentification multifacteur.
3. NetScaler valide les informations d'identification avec AD et génère un jeton de manière native sur l'appliance NetScaler. Les informations d'identification sont transmises à Office365 pour y accéder.

> **Remarque**
>
> La prise en charge de l'IdP WS-Federation est assurée de manière native via l'appliance NetScaler

> par rapport à l'équilibreur de charge F5 Networks.

Configurer l'appliance NetScaler en tant qu'IdP WS-Federation (IDP SAML) à l'aide de l'interface de ligne de commande

Les sections suivantes sont classées en fonction de la nécessité d'effectuer les étapes de configuration.

Pour configurer l'authentification LDAP et ajouter une stratégie

> **Important**
>
> Pour que les utilisateurs du domaine puissent se connecter à l'appliance NetScaler à l'aide de leur adresse e-mail d'entreprise, vous devez configurer les éléments suivants :

- Configurez le serveur et la politique d'authentification LDAP sur l'appliance NetScaler.
- Liez-la à votre adresse IP virtuelle d'authentification, d'autorisation et d'audit (l'utilisation d'une configuration LDAP existante est également prise en charge).

```
1 add authentication ldapAction <Domain_LDAP_Action> -serverIP <Active
     Directory IP> -serverPort 636 -ldapBase "cn=Users,dc=domain,dc=com"
     -ldapBindDn "cn=administrator,cn=Users,dc=domain,dc=com" -
     ldapBindDnPassword <administrator password> -encrypted -
     encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
      memberOf -subAttributeName cn -secType SSL -ssoNameAttribute
     UserPrincipalName -followReferrals ON -Attribute1 mail -Attribute2
     objectGUID
2
3 add authentication Policy <Domain_LDAP_Policy> -rule true -action <
     Domain_LDAP_Action>
4 <!--NeedCopy-->
```

Exemple

```
1 add authentication ldapAction CTXTEST_LDAP_Action -serverIP 3.3.3.3 -
     serverPort 636 -ldapBase "cn=Users,dc=ctxtest,dc=com" -ldapBindDn "
     cn=administrator,cn=Users,dc=ctxtest,dc=com" -ldapBindDnPassword
     xxxxxxxxxx -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName
     sAMAccountName -groupAttrName memberOf -subAttributeName cn -secType
      SSL -ssoNameAttribute UserPrincipalName -followReferrals ON -
     Attribute1 mail -Attribute2 objectGUID
2
3 add authentication Policy CTXTEST_LDAP_Policy -rule true -action
     CTXTEST_LDAP_Action
4 <!--NeedCopy-->
```


Pour configurer NetScaler en tant qu'IdP WS-Federation ou IdP SAML

Créez une action et une stratégie WS-Federation IdP (SAML IdP) pour la génération de jetons. Liez-le au serveur virtuel d'authentification, d'autorisation et d'audit ultérieurement.

```
add authentication samlIdPProfile <Domain_SAMLIDP_Profile> -
    samlIdPCertName <SSL_CERT> -assertionConsumerServiceURL "https://
    login.microsoftonline.com/login.srf" -samlIssuerName <Issuer Name
    for Office 365 in ADFS Server> -rejectUnsignedRequests OFF -audience
     urn:federation:MicrosoftOnline -NameIDFormat persistent -NameIDExpr
     "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE" -Attribute1 IDPEmail -
    Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"

add authentication samlIdPPolicy <Domain_SAMLIDP_Policy> -rule "HTTP.
    REQ.HEADER("referer").CONTAINS("microsoft") || true" -action <
    Domain_SAMLIDP_Profile>
<!--NeedCopy-->
```

Exemple

```
add authentication samlIdPProfile CTXTEST_SAMLIDP_Profile -
    samlIdPCertName ctxtest_newcert_2019 -assertionConsumerServiceURL "
    https://login.microsoftonline.com/login.srf" -samlIssuerName "http
    ://ctxtest.com/adfs/services/trust/" -rejectUnsignedRequests OFF -
    audience urn:federation:MicrosoftOnline -NameIDFormat persistent -
    NameIDExpr "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE" -Attribute1
    IDPEmail -Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"

add authentication samlIdPPolicy CTXTEST_SAMLIDP_Policy -rule "HTTP.REQ
    .HEADER("referer").CONTAINS("microsoft") || true" -action
    CTXTEST_SAMLIDP_Profile
<!--NeedCopy-->
```

Pour configurer un serveur virtuel d'authentification, d'autorisation et d'audit afin d'authentifier les employés qui se connectent à Office365 à l'aide des informations d'identification de l'entreprise

```
add authentication vserver <Domain_AAA_VS> SSL <IP_address>`
<!--NeedCopy-->
```

Exemple

```
add authentication vserver CTXTEST_AAA_VS SSL 192.168.1.0

```



```
bind authentication vserver CTXTEST_AAA_VS -portaltheme RfWebUI
<!--NeedCopy-->
```

Pour lier le serveur virtuel d'authentification et la stratégie

```
bind authentication vserver <Domain_AAA_VS> -policy <
    Domain_SAMLIDP_Policy> -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver <Domain_AAA_VS> -policy <Domain_LDAP_Policy
    > -priority 100 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Exemple

```
bind authentication vserver CTXTEST_AAA_VS -policy
    CTXTEST_SAMLIDP_Policy -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver CTXTEST_AAA_VS -policy CTXTEST_LDAP_Policy
    -priority 100 -gotoPriorityExpression NEXT

bind ssl vserver CTXTEST_AAA_VS -certkeyName ctxtest_newcert_2019
<!--NeedCopy-->
```

Pour configurer le changement de contenu

```
add cs action <Domain_CS_Action> -targetVserver <Domain_AAA_VS>

add cs policy <Domain_CS_Policy> -rule "is_vpn_url || http.req.url.
    contains("/adfs/ls") || http.req.url.contains("/adfs/services/trust"
    ) || -action <Domain_CS_Action>
<!--NeedCopy-->
```

Exemple

```
add cs action CTXTEST_CS_Action -targetVserver CTXTEST_AAA_VS

add cs policy CTXTEST_CS_Policy -rule "is_vpn_url || http.req.url.
    contains("/adfs/ls") || http.req.url.contains("/adfs/services/trust"
    ) || -action CTXTEST_CS_Action
<!--NeedCopy-->
```

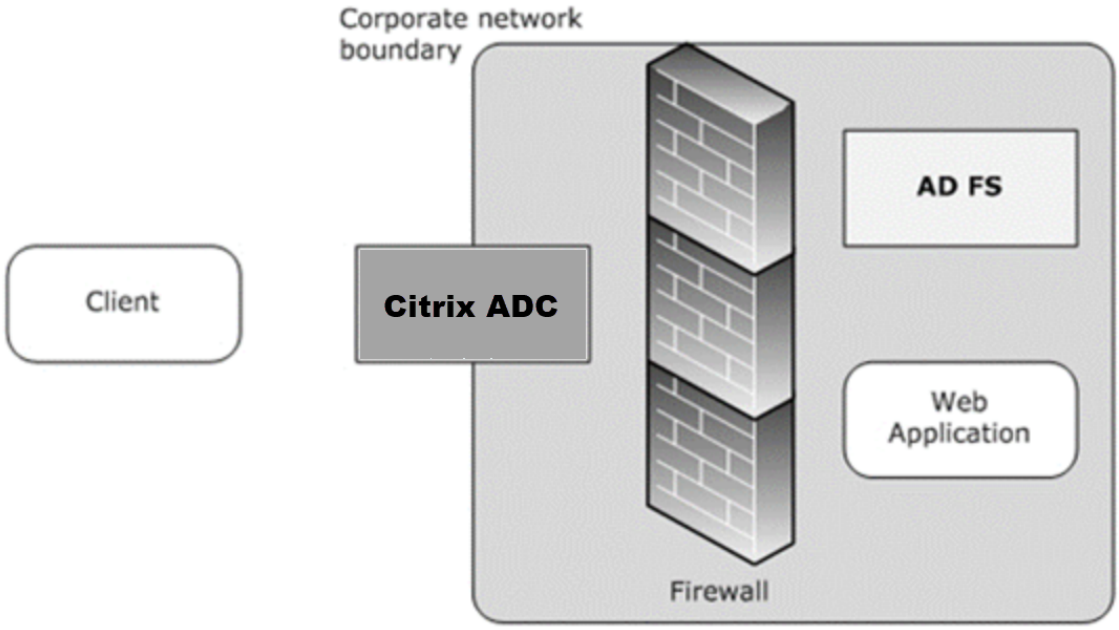

Pour lier le contenu commutant de serveur virtuel à une stratégie

```
bind cs vserver CTXTEST_CSVS -policyName CTXTEST_CS_Policy -priority
    100
<!--NeedCopy-->
```

Conformité au protocole d'intégration du proxy du service Active Directory

June 20, 2023

Si des proxys tiers doivent être utilisés à la place du proxy d'application Web, ils doivent prendre en charge le protocole MS-ADFSPIP qui spécifie les règles d'intégration ADFS et WAP. ADFSPIP intègre les services de fédération Active Directory à un proxy d'authentification et d'application pour permettre l'accès aux services situés à l'intérieur des limites du réseau d'entreprise pour les clients situés en dehors de cette limite.



Composants requis

Pour établir correctement la confiance entre le serveur proxy et la batterie de serveurs ADFS, passez en revue la configuration suivante dans l'appliance NetScaler :

- Créez un profil SSL pour le back-end et activez SNI dans le profil SSL. Désactivez SSLv3/TLS1. À l'invite de commandes, tapez la commande suivante :

```
add ssl profile <new SSL profile> -sniEnable ENABLED -ssl3
   DISABLED -tls1 DISABLED -commonName <FQDN of ADFS>
<!--NeedCopy-->
```

- Désactivez SSLv3/TLS1 pour le service. À l'invite de commandes, tapez la commande suivante :

```
set ssl service <adfs service name> -sslProfile
   ns_default_ssl_profile_backend
<!--NeedCopy-->
```

- Activez l'extension SNI pour les poignées de contact du serveur principal. À l'invite de commandes, tapez la commande suivante :

```
set vpn parameter  - backendServerSni ENABLED

set ssl parameter -denySSLReneg NONSECURE
<!--NeedCopy-->
```

> **Important**
>
> Pour les scénarios Home Realm Discovery (HRD) dans lesquels l'authentification doit être déchargée vers le serveur ADFS, Citrix vous recommande de désactiver à la fois l'authentification et le SSO sur l'appliance NetScaler.

Mécanisme d'authentification

Voici le flux d'événements de haut niveau pour l'authentification.

1. **Établir la confiance avec le serveur ADFS** : le serveur NetScaler établit la confiance avec le serveur ADFS en enregistrant un certificat client. Une fois la confiance établie, l'appliance NetScaler rétablit la confiance après le redémarrage sans intervention de l'utilisateur.

   À l'expiration du certificat, vous devez rétablir l'approbation en supprimant et en ajoutant à nouveau le profil proxy ADFS.

2. **Points de terminaison publiés** : l'appliance NetScaler récupère automatiquement la liste des points de terminaison publiés sur le serveur ADFS après l'établissement de la confiance. Ces points de terminaison publiés filtrent les demandes transmises au serveur ADFS.

3. **Insérer des en-têtes dans les demandes des clients** : lorsque l'appliance NetScaler tunnelise les demandes des clients, les en-têtes HTTP liés à ADFSPIP sont ajoutés au paquet lors de leur envoi au serveur ADFS. Vous pouvez implémenter un contrôle d'accès sur le serveur ADFS en fonction de ces valeurs d'en-tête. Les en-têtes suivants sont pris en charge.

- X-MS-Proxy
- X-MS-Endpoint-Absolute-Path
- X-MS-Forwarded-Client-IP
- X-MS-Proxy
- X-MS-Target-Role
- X-MS-ADFS-Proxy-Client-IP

4. **Gérer le trafic des utilisateurs finaux : le** trafic des utilisateurs finaux est acheminé en toute sécurité vers les ressources souhaitées.

> **Remarques :**
>
> - NetScaler utilise l'authentification basée sur des formulaires.
> - NetScaler ne prend pas en charge la publication d'une application conforme au protocole d'intégration du proxy Active Directory Federation Service.

Configurer NetScaler pour prendre en charge le serveur ADFS

Composants requis

- Configurez le serveur de commutation de contexte (CS) en tant que serveur frontal avec le serveur d'authentification, d'autorisation et d'audit derrière CS. À l'invite de commande, tapez :

```
1 add cs vserver <cs vserver name> SSL 10.220.xxx.xx 443
2 -cltTimeout 180 -AuthenticationHost <adfs server hostname> -
     Authentication OFF -persistenceType NONE
3 <!--NeedCopy-->
```

```
1 add cs action <action name1> -targetLBVserver <lb vserver name>
2 <!--NeedCopy-->
```

```
1 add cs action <action name2> -targetLBVserver <lb vserver name>
2 <!--NeedCopy-->
```

```
1 add cs policy <policy name1> -rule " http.req.url.contains("/adfs
     /services/trust") || http.req.url.contains("federationmetadata
     /2007-06/federationmetadata.xml")" -action <action name1>
2 <!--NeedCopy-->
```

```
1 add cs policy <policy name2> -rule "HTTP.REQ.URL.CONTAINS("/adfs/
     ls")" -action <action name2>
2 <!--NeedCopy-->
```



```
bind cs vserver <cs vserver name> -policyName <policy name1> -
   priority 100
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -policyName <policy name2> -
   priority 110
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -lbvserver <lb vserver name>
<!--NeedCopy-->
```

- Ajoutez un service ADFS. À l'invite de commande, tapez :

```
add service <adfs service name> <adfs server ip> SSL 443
<!--NeedCopy-->
```

```
set ssl service <adfs service name> -sslProfile
   ns_default_ssl_profile_backend
<!--NeedCopy-->
```

- Ajoutez un serveur virtuel à charge équilibrée. À l'invite de commande, tapez :

```
add lb vserver <lb vserver name> SSL 0.0.0.0 0
<!--NeedCopy-->
```

```
set ssl vserver <lb vserver name> -sslProfile
   ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

- Liez le service au serveur d'équilibrage de charge. À l'invite de commande, tapez :

```
bind lb vserver <lb vserver name> <adfs service name>
<!--NeedCopy-->
```

Pour configurer NetScaler afin qu'il fonctionne avec le serveur ADFS, vous devez procéder comme suit :

1. Créez une clé de profil SSL CertKey à utiliser avec le profil proxy ADFS
2. Création d'un profil proxy ADFS
3. Associez le profil proxy ADFS au serveur virtuel LB

Créez un certificat SSL avec clé privée à utiliser avec le profil proxy ADFS

À l'invite de commande, tapez :

```
1     add ssl certkey <certkeyname>  - cert <certificate path> -key <
         keypath>
2 <!--NeedCopy-->
```

Remarque : Le fichier de certificat et le fichier de clé doivent être présents dans l'appliance NetScaler. Créer un profil proxy ADFS à l'aide de la CLI

À l'invite de commande, tapez :

```
1 add authentication adfsProxyProfile  <profile name> -serverUrl <https:
     //<server FQDN or IP address>/> -username <adfs admin user name> -
     password <password for admin user> -certKeyName <name of the CertKey
      profile created above>
2 <!--NeedCopy-->
```

Où ?

Nom du profil : nom du profil proxy AFDS à créer

ServerURL : nom de domaine complet du service ADFS, y compris le protocole et le port. Par exemple, `https://adfs.citrix.com`

`Username` — Nom d'utilisateur d'un compte administrateur existant sur le serveur ADFS

Mot de passe : mot de passe du compte administrateur utilisé comme nom d'utilisateur

CertKeyName — Nom du profil CertKey SSL créé précédemment

Associez le profil proxy ADFS au serveur virtuel d'équilibrage de charge à l'aide de la CLI

Dans le déploiement ADFS, deux serveurs virtuels d'équilibrage de charge sont utilisés, l'un pour le trafic client et l'autre pour l'échange de métadonnées. Le profil proxy ADFS doit être associé au serveur virtuel d'équilibrage de charge qui est frontal au serveur ADFS.

À l'invite de commande, tapez :

```
1 set lb vserver <adfs-proxy-lb> -adfsProxyProfile <name of the ADFS
     proxy profile>
2 <!--NeedCopy-->
```

Soutien au renouvellement de confiance pour ADFSPIP

Vous pouvez renouveler l'approbation des certificats existants qui sont sur le point d'expirer ou si le certificat existant n'est pas valide. Le renouvellement de la confiance des certificats est effectué

uniquement lorsque la confiance est établie entre l'appliance NetScaler et le serveur ADFS. Pour renouveler l'approbation du certificat, vous devez fournir le nouveau certificat.

> **Important**
>
> Une intervention manuelle est requise pour le renouvellement de confiance des nouveaux certificats.

L'exemple suivant répertorie les étapes impliquées dans le renouvellement de l'approbation de certificat :

1. L'appliance NetScaler envoie les anciens certificats (SerializedTrustCertificate) et les nouveaux (SerializedReplacementCertificate) sous forme de requête POST au serveur ADFS pour le renouvellement de la confiance.
2. Le serveur ADFS répond avec un succès de 200 OK si l'approbation est renouvelée avec succès.
3. L'appliance NetScaler met à jour l'état sous la forme « ESTABLISHED_RENEW_SUCCESS » si le renouvellement de confiance est réussi. Si le renouvellement de la confiance échoue, l'état est mis à jour sous la forme « ESTABLISHED_RENEW_FAILED » et l'appliance NetScaler continue d'utiliser l'ancien certificat.

> **Remarque**
>
> Vous ne pouvez pas mettre à jour la clé de certification si elle est déjà liée à un profil proxy ADFS.

Pour configurer le renouvellement de confiance des certificats à l'aide de la CLI

À l'invite de commande, tapez :

```
set authentication adfsProxyProfile <name> [-CertKeyName <string>]
<!--NeedCopy-->
```

Exemple :

```
set authentication adfsProxyProfile adfs_2  - CertKeyName ca_cert1
<!--NeedCopy-->
```

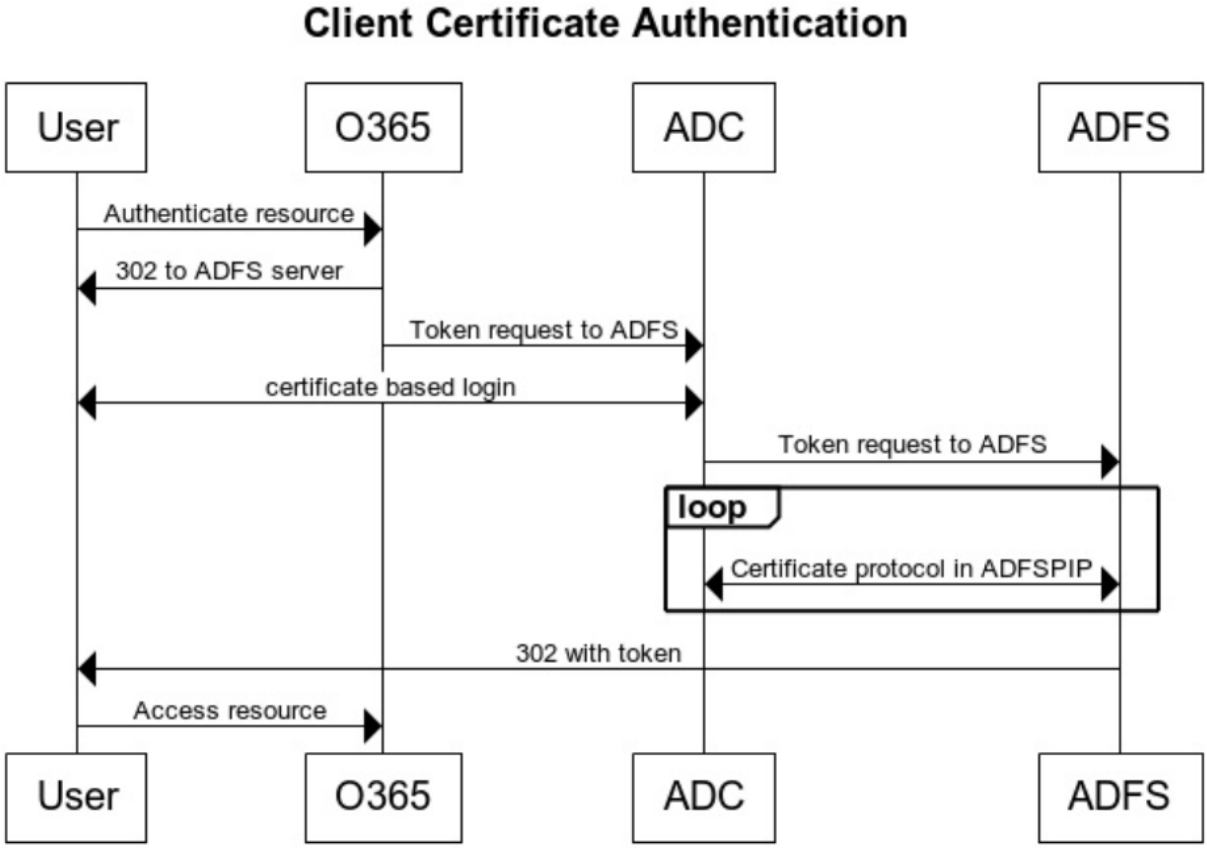
Authentification basée sur le certificat client sur le serveur ADFS

À partir de Windows Server 2016, Microsoft a introduit une nouvelle méthode d'authentification des utilisateurs lorsque l'accès à ADFS est effectué via des serveurs proxy. Désormais, les utilisateurs finaux peuvent se connecter avec leurs certificats, évitant ainsi l'utilisation d'un mot de passe.

Les utilisateurs finaux accèdent souvent à ADFS via un proxy, en particulier lorsqu'ils ne se trouvent pas sur place. Par conséquent, les serveurs proxy ADFS sont nécessaires pour prendre en charge l'authentification par certificat client via le protocole ADFSPIP.

Lorsque la charge d'ADFS est équilibrée à l'aide d'une appliance NetScaler, pour prendre en charge l'authentification basée sur un certificat sur le serveur ADFS, les utilisateurs doivent également se connecter à l'appliance NetScaler à l'aide du certificat. Cela permet à NetScaler de transmettre le certificat utilisateur à ADFS pour fournir une authentification unique au serveur ADFS.

Le schéma suivant illustre le flux d'authentification du certificat client.



Configurer l'authentification unique pour le serveur ADFS à l'aide d'un certificat client

Pour configurer le SSO pour le serveur ADFS à l'aide du certificat client, vous devez d'abord configurer l'authentification par certificat client sur l'appliance NetScaler. Vous devez ensuite lier la stratégie d'authentification par certificat au serveur virtuel d'authentification, d'autorisation et d'audit.

En outre, vous devez suivre les étapes suivantes.

- Un serveur virtuel de commutation de contexte supplémentaire avec le port 49443 doit être configuré et ce serveur virtuel de commutation de contexte doit pointer vers le même serveur virtuel d'équilibrage de charge ouvert pour tous les ports, que vous avez créé précédemment.
- Le port 49443 doit être ouvert sur l'appliance NetScaler pour l'authentification.
- La stratégie de commutation de contexte doit être liée au même serveur virtuel d'équilibrage de charge avec le port 443 ouvert que vous avez créé précédemment.

- Vous devez lier le même service SSL que vous avez créé précédemment au serveur virtuel d'équilibrage de charge.
- Si vous avez déjà créé un profil SSL pour le back-end, vous devez utiliser ce profil.

À l'invite de commandes, tapez ;

```
add cs vserver <name> <serviceType> <port>

bind cs vserver <name> (-lbvserver <string> | -vServer <string> | [-
    targetLBVserver <string>]

set ssl vserver <vServerName [-sslProfile <string>]

bind ssl vserver <vServerName -certkeyName <string>

add authentication certAction <action name>

add authentication Policy <policy name> -rule <expression> -action <
    action name>

add authentication policylable <label Name>

bind authentication policylabel <label Name> -policyName <name of the
    policy> -priority<integer>

<!--NeedCopy-->
```

Exemple :

```
add cs vserver srv123_adfsproxy_csvs_tls SSL $VIP_1 49443

bind cs vserver srv123_adfsproxy_csvs_tls -lbvserver
    srv123_adfs_lbvserver

set ssl vserver srv123_adfsproxy_csvs_tls -sslProfile
    ns_default_ssl_profile_frontend

bind ssl vserver srv123_adfsproxy_csvs_tls -certkeyName
    srv123_wildcardcert

add authentication certAction adfsproxy-cert

add authentication Policy cert1 -rule TRUE -action adfsproxy-cert

add authentication policylable certfactor
```



```
14
15 bind authentication policylabel certfactor -policyName cert1 -
      priority 100
16
17 <!--NeedCopy-->
```

Pour plus d'informations sur la configuration du certificat client sur l'appliance NetScaler, consultez la section Configurer l'authentification par certificat client à l'aide de stratégies avancées.

Utiliser un NetScaler Gateway local comme fournisseur d'identité pour Citrix Cloud

May 5, 2023

Citrix Cloud prend en charge l'utilisation d'un NetScaler Gateway local en tant que fournisseur d'identité pour authentifier les abonnés qui se connectent à leurs espaces de travail.

En utilisant l'authentification NetScaler Gateway, vous pouvez :

- Continuez à authentifier les utilisateurs via votre NetScaler Gateway existant afin qu'ils puissent accéder aux ressources de votre déploiement d'applications et de bureaux virtuels sur site via Citrix Workspace.
- Utilisez les fonctions d'authentification, d'autorisation et d'audit de NetScaler Gateway avec Citrix Workspace.
- Fournissez à vos utilisateurs l'accès aux ressources dont ils ont besoin via Citrix Workspace à l'aide de fonctionnalités telles que l'authentification pass-through, les cartes à puce, les jetons sécurisés, les stratégies d'accès conditionnel et la fédération.

L'authentification NetScaler Gateway est prise en charge pour une utilisation avec les versions de produit suivantes :

- NetScaler Gateway 13.0 41.20 Édition avancée ou version ultérieure
- NetScaler Gateway 12.1 54.13 Édition avancée ou ultérieure

Composants requis

- Cloud Connector : vous avez besoin d'au moins deux serveurs sur lesquels installer le logiciel Citrix Cloud Connector.
- Active Directory : effectuez les vérifications nécessaires.
- Configuration requise pour NetScaler Gateway

- Utilisez des stratégies avancées sur la passerelle locale en raison de la dépréciation des stratégies classiques.
- Lors de la configuration de la passerelle pour l'authentification des abonnés à Citrix Workspace, la passerelle agit en tant que fournisseur OpenID Connect. Les messages entre Citrix Cloud et Gateway sont conformes au protocole OIDC, qui inclut la signature numérique de jetons. Par conséquent, vous devez configurer un certificat pour signer ces jetons.
- Synchronisation de l'horloge - La passerelle doit être synchronisée à l'heure NTP.

Pour plus de détails, consultez la section Conditions préalables.

Création d'une politique d'IdP OAuth sur le NetScaler Gateway local

> **Important :**
>
> Vous devez avoir généré l'ID client, le code secret et l'URL de redirection dans l'onglet **Citrix Cloud > Gestion des identités et des accès > Authentification** . Pour plus de détails, consultez la section Connecter un NetScaler Gateway local à Citrix Cloud.

La création d'une stratégie d'authentification OAuth IdP implique les tâches suivantes :

1. Créer un profil d'authentification de fournisseur d'identité
2. Ajoutez une stratégie IdP OAuth.
3. Liez la stratégie IdP OAuth à un serveur virtuel d'authentification.
4. Liez le certificat globalement.

Création d'un profil IdP OAuth à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
add authentication OAuthIDPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <
    string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-action <
    string> [-undefAction <string>] [-comment <string>][-logAction <
    string>]

add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=aaa,
    dc=local"

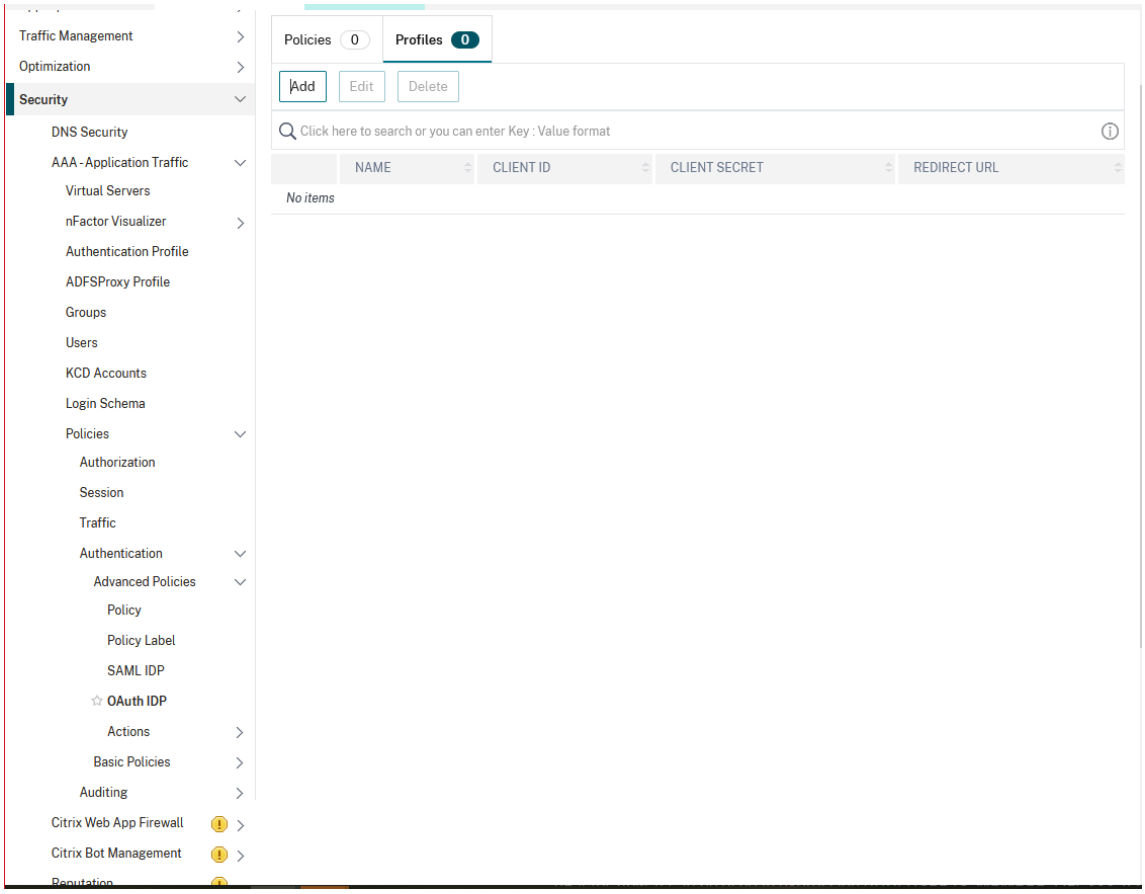
ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -
    ldapLoginName sAMAccountName
```



```
8
9  add authentication policy <name> -rule <expression> -action <string>
10
11 bind authentication vserver auth_vs -policy <ldap_policy_name> -
       priority <integer> -gotoPriorityExpression NEXT
12
13 bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -
       priority <integer> -gotoPriorityExpression END
14
15 bind vpn global -certkeyName <>
16 <!--NeedCopy-->
```

Création d'un profil IdP OAuth à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA — Trafic des applications > Stratégies > Authentification > Stratégies avancées > Fournisseur d'identités OAuth**.



2. Sur la page **IdP OAuth**, sélectionnez l'onglet **Profils** et cliquez sur **Ajouter**.
3. Configurez le profil IdP OAuth.

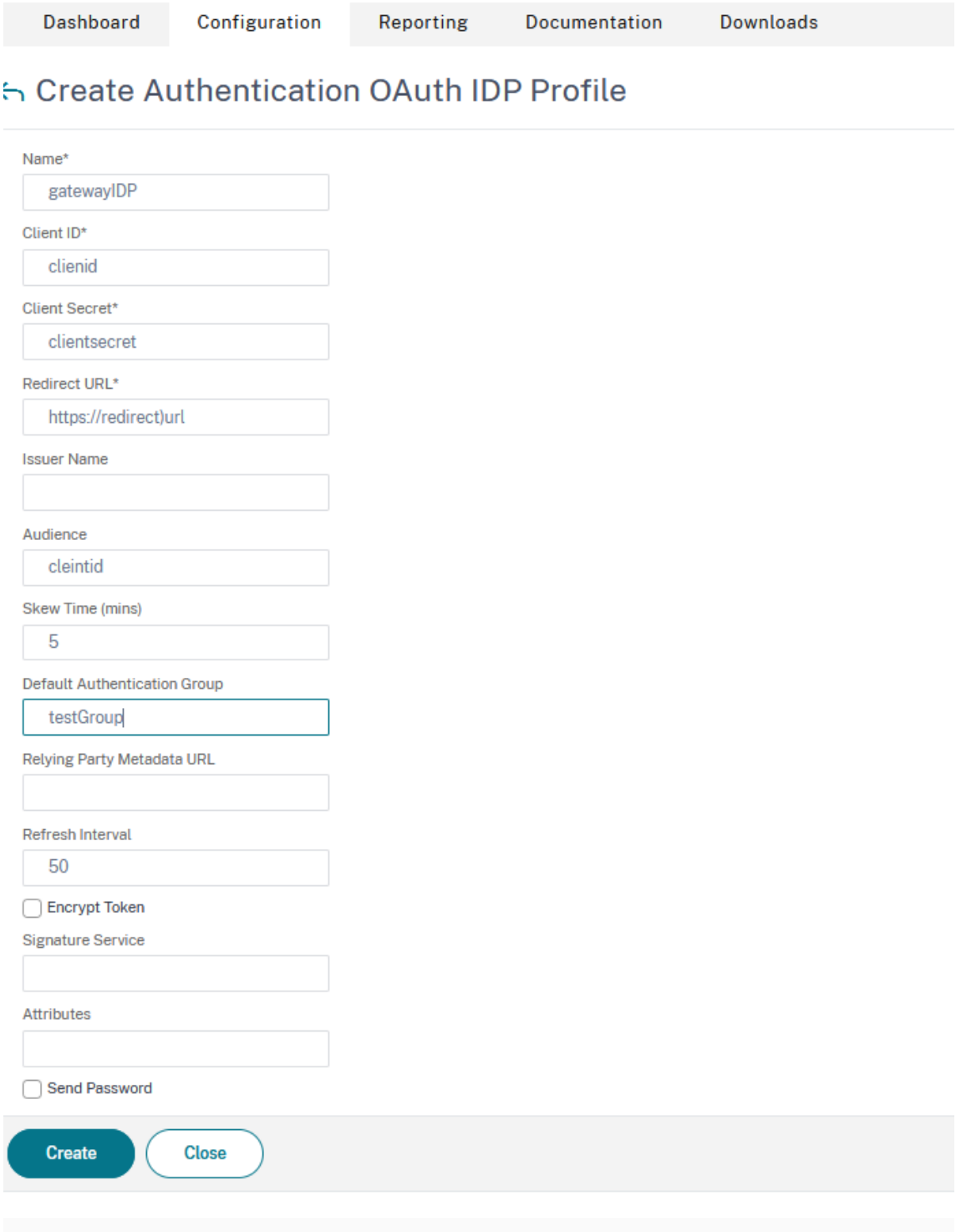
> **Remarque :**
>
> - Copiez et collez les valeurs de l'ID client, du secret et de l'URL de redirection à partir de l'onglet **Citrix Cloud > Gestion des identités et des accès > Authentification** pour établir la connexion à Citrix Cloud.
> - Entrez correctement l'URL de la passerelle dans l'exemple du **nom de l'émetteur** : https://GatewayFQDN.com
> - Copiez et collez également l'ID client dans le champ **Audience** .
> - **Envoyer le mot de passe** : activez cette option pour la prise en charge de l'authentification unique. Par défaut, cette option est désactivée.

4. Dans l'écran **Créer un profil de fournisseur d'identité OAuth d'authentification**, définissez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

   - **Nom** : nom du profil d'authentification. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_). Le nom ne doit contenir que des lettres, des chiffres et le trait d'union (-), point (.) livre (#), espace (), at (@), égal à (=), deux-points (:) et des caractères de soulignement. Impossible de modifier une fois le profil créé.
   - **Client ID** : chaîne unique qui identifie le fournisseur de services. Le serveur d'autorisation déduit la configuration du client en utilisant cet ID. Longueur maximale : 127.
   - **Client Secret** : chaîne secrète établie par l'utilisateur et le serveur d'autorisation. Longueur maximale : 239.
   - **URL de redirection** : point de terminaison sur le SP auquel le code/jeton doit être publié.
   - **Nom de l'émetteur** : identité du serveur dont les jetons doivent être acceptés. Longueur maximale : 127. Exemple : https://GatewayFQDN.com
   - **Audience** : destinataire cible du jeton envoyé par l'IdP. Ce jeton est vérifié par le destinataire.
   - **Temps d'inclinaison** : cette option spécifie le décalage d'horloge autorisé (en minutes) que NetScaler autorise sur un jeton entrant. Par exemple, si SkewTime est 10, le jeton sera valide de (heure actuelle - 10) min à (heure actuelle + 10) min, soit 20 min en tout. Valeur par défaut : 5.
   - **Groupe d'authentification par défaut** : groupe ajouté à la liste des groupes internes de session lorsque ce profil est choisi par IdP et peut être utilisé dans le flux nFactor. Il peut être utilisé dans l'expression (AAA.USER.IS_MEMBER_OF (« xxx »)) pour les stratégies d'authentification afin d'identifier le flux nFactor lié à la partie de confiance. Longueur maximale : 63

   Un groupe est ajouté à la session pour ce profil afin de simplifier l'évaluation des stratégies et

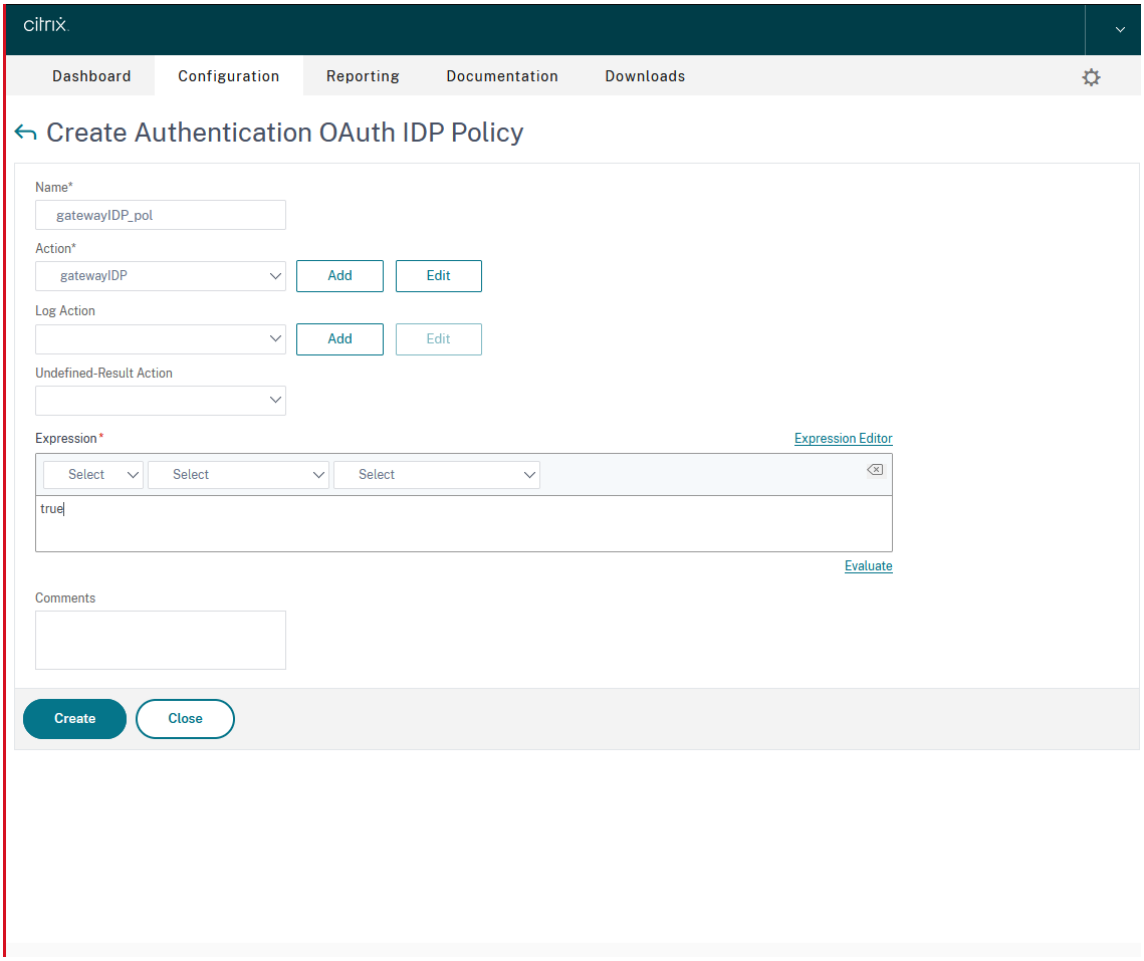
de faciliter la personnalisation des stratégies. Ce groupe est le groupe par défaut qui est choisi lorsque l'authentification réussit, en plus des groupes extraits. Longueur maximale : 63.



5. Cliquez sur **Stratégies** et cliquez sur **Ajouter.**
6. Dans l'écran **Créer une stratégie de fournisseur d'identité OAuth d'authentification**, définis-

sez des valeurs pour les paramètres suivants, puis cliquez sur **Créer**.

- **Nom** : nom de la stratégie d'authentification.
- **Action** : nom du profil créé précédemment.
- **Log Action** : nom de l'action du journal des messages à utiliser lorsqu'une demande correspond à cette stratégie. Ce n'est pas un dépôt obligatoire.
- **Action à résultat non défini** — Action à exécuter si le résultat de l'évaluation de la stratégie n'est pas défini (UNDEF). Ce champ n'est pas obligatoire.
- **Expression** : expression syntaxique par défaut utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, true.
- **Comments** : tout commentaire concernant la stratégie.



> **Remarque :**
>
> lorsque **SendPassword** est réglé sur ON (OFF par défaut), les informations d'identification de l'utilisateur sont chiffrées et transmises via un canal sécurisé à Citrix Cloud. La transmission des informations d'identification de l'utilisateur via un canal sécurisé vous permet d'activer l'authentification unique vers Citrix Virtual Apps and Desktops lors du lancement.

Liaison de la stratégie OAuthIDP et de la stratégie LDAP au serveur virtuel d'authentification

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Actions > LDAP**.
2. Dans l'écran **Actions LDAP**, cliquez sur **Ajouter**.
3. Dans l'écran **Créer un serveur LDAP d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer**.
    - **Nom :** nom de l'action LDAP
    - **ServerName/ServerIP :** fournit le nom de domaine complet ou l'adresse IP du serveur LDAP
    - Choisissez les valeurs appropriées **pour le type de sécurité, le port, le type de serveur et le délai d'expiration**
    - Assurez-vous que **l'authentification** est cochée
    - **DN de base :** base à partir de laquelle lancer la recherche LDAP. Par exemple, `dc=aaa,dc=local`.
    - **Administrator Bind DN :** nom d'utilisateur de la liaison au serveur LDAP. Par exemple, admin@aaa.local.
    - **Mot de passe administrateur/Confirmer le mot de passe : mot de passe pour lier LDAP**
    - Cliquez sur **Tester la connexion** pour tester vos paramètres.
    - **Attribut de nom d'ouverture de session du serveur :** choisissez **« SAMAccountName »**
    - Les autres champs ne sont pas obligatoires et peuvent donc être configurés comme requis.
4. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Stratégie.**
5. Dans l'écran **Stratégies d'authentification**, cliquez sur **Ajouter**.
6. Sur la page **Créer une stratégie d'authentification**, définissez les valeurs des paramètres suivants, puis cliquez sur **Créer.**
    - **Nom :** nom de la stratégie d'authentification LDAP.
    - **Type d'action :** choisissez **LDAP.**
    - **Action :** choisissez l'action LDAP.
    - **Expression —** Expression de syntaxe par défaut utilisée par la stratégie pour répondre à une demande spécifique. Par exemple, true**.

Support pour les déploiements GSLB actifs-actifs sur NetScaler Gateway

May 5, 2023

NetScaler Gateway configuré en tant que fournisseur d'identité (IdP) à l'aide du protocole OIDC peut prendre en charge les déploiements GSLB actifs et actifs.

Pour plus d'informations sur la configuration d'une installation GSLB, consultez Exemple d'installation et de configuration d'un GSLB.

> **Important :**
>
> Le GSLB actif-actif avec NetScaler Gateway en tant qu'IdP OAuth n'est pas pris en charge pour Citrix Cloud.

Prise en charge active-active GSLB pour l'authentification multifacteur à l'aide du proxy de connexion

À partir de la version 13.1 build 12.x de NetScaler, la prise en charge du déploiement actif-actif de GSLB est ajoutée pour l'authentification multifactorielle à l'aide d'un proxy de connexion. Ce support s'applique aux scénarios d'authentification, d'autorisation et d'audit NetScaler Gateway et NetScaler. Le proxy de connexion est utilisé pour acheminer les demandes vers les sites GSLB appropriés une fois l'authentification réussie. Pour plus d'informations sur la persistance du proxy de connexion, consultez Proxyde connexion

Fonctionnement

Le cookie de persistance du site GSLB est inséré dans la réponse d'authentification. À l'aide de ce cookie, l'appliance NetScaler ou NetScaler Gateway identifie si la demande concerne un site local ou un site distant. Les demandes sont ensuite acheminées en conséquence.

> **Important :**
>
> - Seul le déploiement de type actif-actif GSLB est pris en charge.
> - La topologie parent-enfant n'est pas prise en charge.
> - Le type de persistance dans le déploiement GSLB doit être configuré en tant que « ConnectionProxy ».

Prise en charge de la configuration de l'attribut de cookie SameSite

May 5, 2023

L'attribut SameSite indique au navigateur si le cookie peut être utilisé pour un contexte intersite ou uniquement pour un contexte de même site. De même, si une application a l'intention d'être accessible dans un contexte intersite, elle ne peut le faire que via la connexion HTTPS. Pour plus de détails, consultez la RFC6265.

Jusqu'en février 2020, l'attribut SameSite n'était pas défini de manière explicite dans NetScaler. Le navigateur a pris la valeur par défaut (Aucun). Le fait de ne pas définir l'attribut SameSite n'a eu aucune incidence sur NetScaler Gateway ni sur les déploiements d'authentification, d'autorisation et d'audit.

La mise à niveau de certains navigateurs, tels que Google Chrome 80, modifie le comportement par défaut des cookies entre domaines. L'attribut SameSite peut être défini sur l'une des valeurs suivantes. La valeur par défaut de Google Chrome est définie sur Lax. Pour certaines versions d'autres navigateurs, la valeur par défaut de l'attribut SameSite peut toujours être définie sur Aucun.

- **Aucun** : indique que le navigateur doit utiliser un cookie dans un contexte intersite uniquement sur des connexions sécurisées.
- **Lax** : indique que le navigateur doit utiliser un cookie pour les requêtes sur le même domaine et pour les intersites. Pour les sites intersites, seules les méthodes HTTP sécurisées telles que la requête GET peuvent utiliser le cookie. Par exemple, une requête GET d'un sous-domaine abc.example.com peut lire le cookie d'un autre sous-domaine xyz.exemple.com à l'aide d'un GET.
  Pour les sites intersites, seules les méthodes HTTP sécurisées sont utilisées, car les méthodes HTTP sécurisées ne modifient pas l'état du serveur. Pour plus de détails, consultez https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite#lax
- **Strict** : utilisez le cookie uniquement dans le même contexte de site.

S'il n'y a pas d'attribut SameSite dans le cookie, Google Chrome assume la fonctionnalité de SameSite = Lax.
Par conséquent, pour les déploiements au sein d'un iframe avec un contexte intersite qui nécessitent l'insertion de cookies par le navigateur, Google Chrome ne partage pas les cookies intersites. Par conséquent, il se peut que l'iframe du site Web ne se charge pas.

Configurer l'attribut de cookie SameSite

Un nouvel attribut de cookie nommé SameSite est ajouté au VPN et aux serveurs virtuels d'authentification, d'autorisation et d'audit. Cet attribut peut être défini au niveau global et au niveau du serveur virtuel.

Pour configurer l'attribut SameSite, vous devez effectuer les opérations suivantes :

1. Définissez l'attribut SameSite pour le serveur virtuel
2. Liez les cookies au jeu de brevets (si le navigateur supprime les cookies intersites)

Définition de l'attribut SameSite à l'aide de la CLI

Pour définir l'attribut SameSite au niveau du serveur virtuel, utilisez les commandes suivantes.

```
set vpn vserver VP1 -SameSite [STRICT | LAX | None]
set authentication vserver AV1 -SameSite [STRICT | LAX | None]
```



```
<!--NeedCopy-->
```

Pour définir l'attribut SameSite au niveau global, utilisez les commandes suivantes.

```
set aaa parameter -SameSite [STRICT | LAX | None]
set vpn parameter -SameSite [STRICT | LAX | None]
<!--NeedCopy-->
```

Remarque : Le paramètre de niveau du serveur virtuel est prioritaire sur le paramètre de niveau global. Citrix recommande de définir l'attribut de cookie SameSite au niveau du serveur virtuel.

Liaison des cookies au jeu de brevets à l'aide de la CLI

Si le navigateur supprime les cookies intersites, vous pouvez lier cette chaîne de cookie au patset NS_Cookies_SameSite existant afin que l'attribut SameSite soit ajouté au cookie.

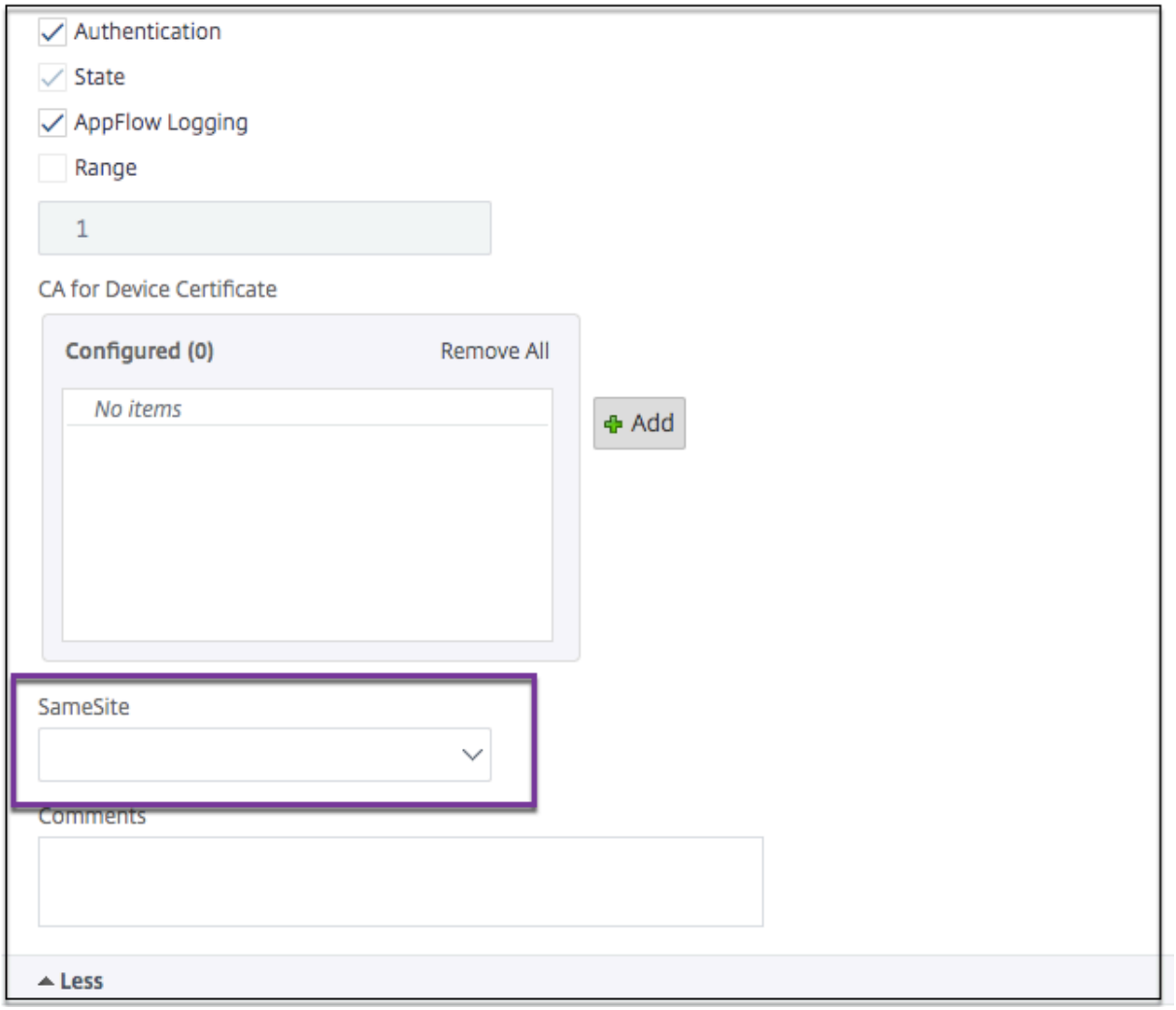
Exemple :

```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
<!--NeedCopy-->
```

Définition de l'attribut SameSite à l'aide de l'interface graphique

Pour définir l'attribut SameSite au niveau du serveur virtuel :

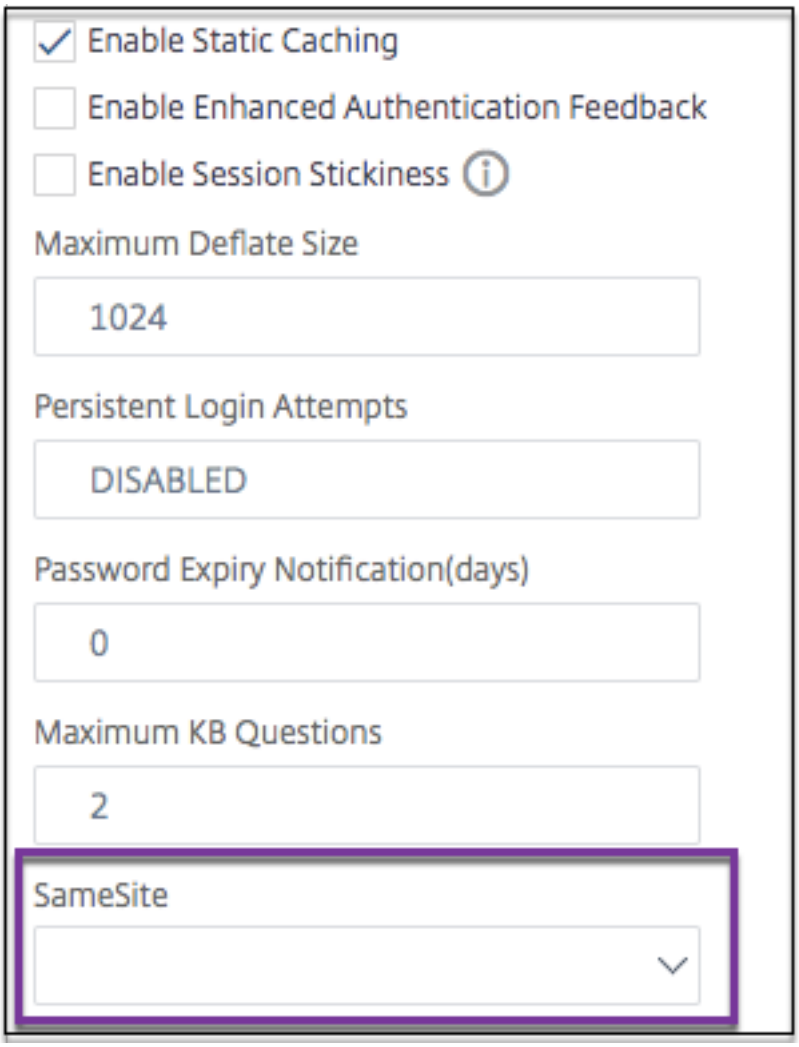
1. Accédez à **Sécurité > AAA — Trafic des applications > Serveurs virtuels.**
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.
3. Cliquez sur l'icône Modifier dans la section **Paramètres de base**, puis sur **Plus**.
4. Dans **SameSite**, sélectionnez l'option si nécessaire.



Pour définir l'attribut SameSite au niveau global :

1. Accédez à **Sécurité > AAA — Trafic des applications > Modifier les paramètres d'authentification.**

2. Dans la page **Configurer le paramètre AAA**, cliquez sur la liste **SameSite** et sélectionnez l'option requise.



Configuration de l'authentification, de l'autorisation et de l'audit pour les protocoles couramment utilisés

May 5, 2023

La configuration de l'appliance NetScaler pour l'authentification, l'autorisation et l'audit nécessite une configuration spécifique sur l'appliance NetScaler et les navigateurs des clients. La configuration varie selon le protocole utilisé pour l'authentification, l'autorisation et l'audit.

Pour plus d'informations sur la configuration de l'appliance NetScaler pour l'authentification Kerberos, consultez la section Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM.

Gestion de l'authentification, de l'autorisation et de l'audit avec Kerberos/NTLM

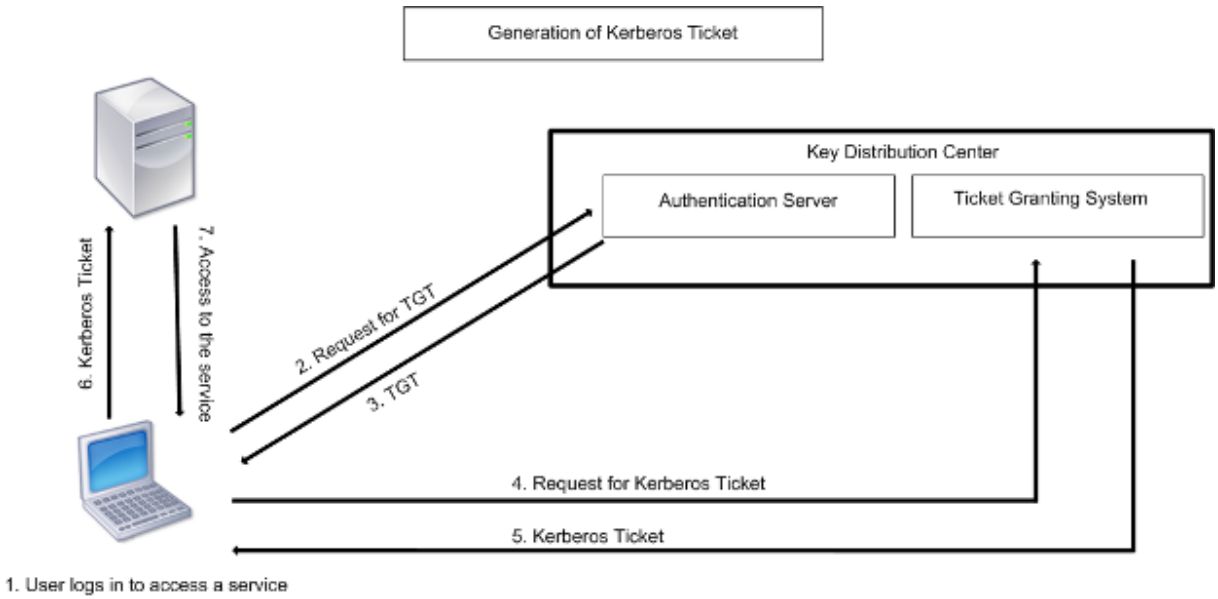
May 5, 2023

Kerberos, un protocole d'authentification de réseau informatique, fournit des communications sécurisées sur Internet. Conçu principalement pour les applications client-serveur, il fournit une authentification mutuelle grâce à laquelle le client et le serveur peuvent chacun garantir l'authenticité de l'autre. Kerberos fait appel à un tiers de confiance, appelé Key Distribution Center (KDC). Un KDC se compose d'un serveur d'authentification (AS), qui authentifie un utilisateur, et d'un serveur d'octroi de tickets (TGS).

Chaque entité du réseau (client ou serveur) possède une clé secrète qui n'est connue que d'elle-même et du KDC. La connaissance de cette clé implique l'authenticité de l'entité. Pour la communication entre deux entités du réseau, le KDC génère une clé de session, appelée ticket Kerberos ou ticket de service. Le client demande à l'AS des informations d'identification pour un serveur spécifique. Le client reçoit ensuite un ticket, appelé ticket d'octroi de tickets (TGT). Le client contacte ensuite le TGS, en utilisant le TGT qu'il a reçu de l'AS pour prouver son identité, et demande un service. Si le client est éligible au service, le TGS lui délivre un ticket Kerberos. Le client contacte ensuite le serveur hébergeant le service (appelé serveur de service) en utilisant le ticket Kerberos pour prouver qu'il est autorisé à recevoir le service. Le ticket Kerberos a une durée de vie configurable. Le client ne s'authentifie auprès de l'AS qu'une seule fois. S'il contacte le serveur physique à plusieurs reprises, il réutilise le ticket AS.

La figure suivante montre le fonctionnement de base du protocole Kerberos.

Figure 1. **Fonctionnement de Kerberos**



L'authentification Kerberos présente les avantages suivants :

- Authentification plus rapide. Lorsqu'un serveur physique reçoit un ticket Kerberos d'un client, le serveur dispose de suffisamment d'informations pour authentifier directement le client. Il n'est pas nécessaire de contacter un contrôleur de domaine pour l'authentification du client, ce qui accélère le processus d'authentification.
- Authentification mutuelle. Lorsque le KDC émet un ticket Kerberos à un client et que ce dernier utilise ce ticket pour accéder à un service, seuls les serveurs authentifiés peuvent déchiffrer le ticket Kerberos. Si le serveur virtuel de l'appliance NetScaler est capable de déchiffrer le ticket Kerberos, vous pouvez en conclure que le serveur virtuel et le client sont authentifiés. Ainsi, l'authentification du serveur se produit en même temps que l'authentification du client.
- Authentification unique entre Windows et les autres systèmes d'exploitation qui prennent en charge Kerberos.

L'authentification Kerberos peut présenter les inconvénients suivants :

- Kerberos impose des exigences temporelles strictes ; les horloges des hôtes concernés doivent être synchronisées avec l'horloge du serveur Kerberos pour garantir que l'authentification n'échoue pas. Vous pouvez atténuer cet inconvénient en utilisant les démons Network Time Protocol pour synchroniser les horloges des hôtes. Les tickets Kerberos ont une période de disponibilité que vous pouvez configurer.
- Kerberos a besoin que le serveur central soit disponible en permanence. Lorsque le serveur Kerberos est en panne, personne ne peut se connecter. Vous pouvez atténuer ce risque en utilisant plusieurs serveurs Kerberos et des mécanismes d'authentification de secours.
- Comme toutes les authentifications sont contrôlées par un KDC centralisé, toute compromission de cette infrastructure, telle que le vol du mot de passe d'un utilisateur pour un poste de travail local, peut permettre à un attaquant de se faire passer pour n'importe quel utilisateur. Vous pouvez atténuer ce risque dans une certaine mesure en utilisant uniquement un ordinateur de bureau ou un ordinateur portable auquel vous faites confiance, ou en appliquant la préauthentification au moyen d'un jeton matériel.

Pour utiliser l'authentification Kerberos, vous devez la configurer sur l'appliance NetScaler et sur chaque client.

Optimisation de l'authentification Kerberos en matière d'authentification, d'autorisation et d'audit

L'appliance NetScaler optimise et améliore désormais les performances du système lors de l'authentification Kerberos. Le démon d'authentification, d'autorisation et d'audit mémorise la requête Kerberos en attente pour le même utilisateur afin d'éviter de surcharger le Centre de distribution de clés (KDC), ce qui évitera les demandes dupliquées.

Comment NetScaler implémente Kerberos pour l'authentification des clients

May 5, 2023

> **Important**
>
> L'authentification Kerberos/NTLM n'est prise en charge que dans la version NetScaler 9.3 nCore ou ultérieure, et elle ne peut être utilisée que pour l'authentification, l'autorisation et l'audit des serveurs virtuels de gestion du trafic.

NetScaler gère les composants impliqués dans l'authentification Kerberos de la manière suivante :

Centre de distribution de clés (KDC)

Dans Windows 2000 Server ou versions ultérieures, le contrôleur de domaine et le KDC font partie de Windows Server. Si le Windows Server est opérationnel, cela indique que le contrôleur de domaine et le KDC sont configurés. Le KDC est également le serveur Active Directory.

> **Remarque**
>
> Toutes les interactions Kerberos sont validées avec le contrôleur de domaine Windows Kerberos.

Service d'authentification et négociation de protocoles

Une appliance NetScaler prend en charge l'authentification Kerberos sur les serveurs virtuels d'authentification, d'autorisation et d'audit de gestion du trafic. Si l'authentification Kerberos échoue, NetScaler utilise l'authentification NTLM.

Par défaut, Windows 2000 Server et les versions ultérieures de Windows Server utilisent Kerberos pour l'authentification, l'autorisation et l'audit. Si vous créez une politique d'authentification avec NEGOTIATE comme type d'authentification, NetScaler tente d'utiliser le protocole Kerberos pour l'authentification, l'autorisation et l'audit et si le navigateur du client ne reçoit pas de ticket Kerberos, NetScaler utilise l'authentification NTLM. Ce processus est appelé négociation.

Le client peut ne pas recevoir de ticket Kerberos dans les cas suivants :

- Kerberos n'est pas pris en charge sur le client.
- Kerberos n'est pas activé sur le client.
- Le client se trouve dans un domaine autre que celui du KDC.
- Le répertoire d'accès du KDC n'est pas accessible au client.

Pour l'authentification Kerberos/NTLM, NetScaler n'utilise pas les données présentes localement sur l'appliance NetScaler.

Authorization

Le serveur virtuel de gestion du trafic peut être un serveur virtuel d'équilibrage de charge ou un serveur virtuel de commutation de contenu.

Audit

L'appliance NetScaler prend en charge l'audit de l'authentification Kerberos grâce à la journalisation d'audit suivante :

- Piste d'audit complète de l'activité des utilisateurs finaux en matière de gestion du trafic
- SYSLOG et journalisation TCP à hautes performances
- Piste d'audit complète des administrateurs système
- Tous les événements du système
- Format de journal scriptable

Environnement pris en charge

L'authentification Kerberos ne nécessite aucun environnement spécifique sur NetScaler. Le client (navigateur) doit prendre en charge l'authentification Kerberos.

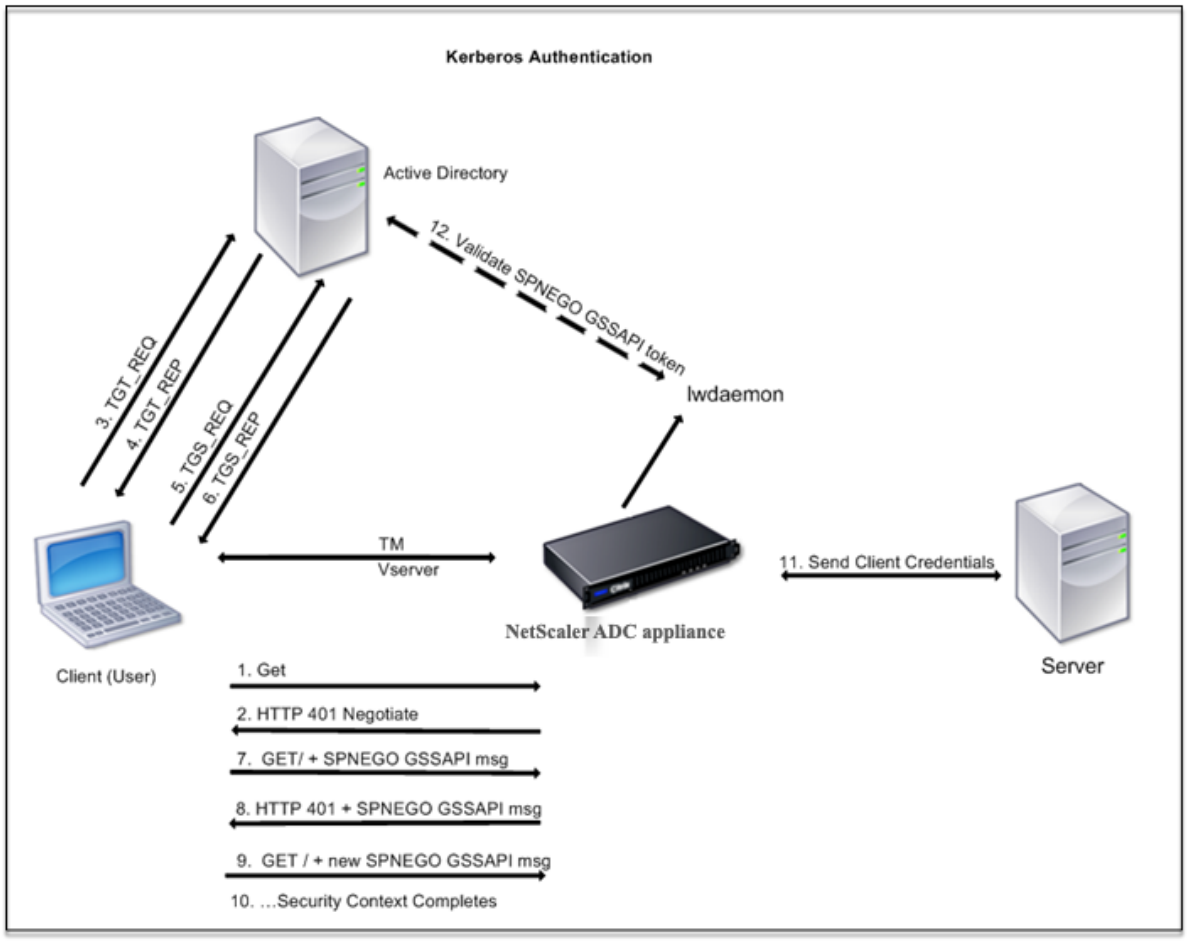
Haute disponibilité

Dans une configuration à haute disponibilité, seul le NetScaler actif rejoint le domaine. En cas de basculement, le démon NetScaler lwagent associe l'appliance NetScaler secondaire au domaine. Aucune configuration spécifique n'est requise pour cette fonctionnalité.

Processus d'authentification Kerberos

La figure suivante montre un processus typique d'authentification Kerberos dans l'environnement NetScaler.

Figure 1. Processus d'authentification Kerberos sur NetScaler



L'authentification Kerberos se déroule selon les étapes suivantes :

Le client s'authentifie auprès du KDC

1. L'appliance NetScaler reçoit une demande d'un client.
2. Le serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu) de l'appliance NetScaler envoie un défi au client.
3. Pour répondre à ce défi, le client reçoit un ticket Kerberos.
   - Le client envoie au serveur d'authentification du KDC une demande de ticket d'octroi de tickets (TGT) et reçoit le TGT. (Voir 3, 4 sur la figure, Processus d'authentification Kerberos.)
   - Le client envoie le TGT au serveur d'attribution de tickets du KDC et reçoit un ticket Kerberos. (Voir 5, 6 sur la figure, Processus d'authentification Kerberos.)

> **Remarque**
>
> Le processus d'authentification ci-dessus n'est pas nécessaire si le client possède déjà un ticket Kerberos dont la durée de vie n'a pas expiré. En outre, les clients tels que Web Services, .NET

> ou J2EE, qui prennent en charge SPNEGO, obtiennent un ticket Kerberos pour le serveur cible, créent un jeton SPNEGO et insèrent le jeton dans l'en-tête HTTP lorsqu'ils envoient une requête HTTP. Ils ne passent pas par le processus d'authentification du client.

Le client demande un service.

1. Le client envoie le ticket Kerberos contenant le jeton SPNEGO et la requête HTTP au serveur virtuel de gestion du trafic sur NetScaler. Le jeton SPNEGO contient les données GSSAPI nécessaires.
2. L'appliance NetScaler établit un contexte de sécurité entre le client et NetScaler. Si NetScaler ne peut pas accepter les données fournies dans le ticket Kerberos, le client est invité à obtenir un autre ticket. Ce cycle se répète jusqu'à ce que les données GSSAPI soient acceptables et que le contexte de sécurité soit établi. Le serveur virtuel de gestion du trafic sur NetScaler agit comme un proxy HTTP entre le client et le serveur physique.

L'appliance NetScaler termine l'authentification.

1. Une fois le contexte de sécurité terminé, le serveur virtuel de gestion du trafic valide le jeton SPNEGO.
2. À partir du jeton SPNEGO valide, le serveur virtuel extrait l'ID utilisateur et les informations d'identification GSS, puis les transmet au démon d'authentification.
3. Une authentification réussie termine l'authentification Kerberos.

Configuration de l'authentification Kerberos sur l'appliance NetScaler

May 9, 2023

Cette rubrique fournit les étapes détaillées pour configurer l'authentification Kerberos sur l'appliance NetScaler à l'aide de l'interface de ligne de commande et de l'interface graphique.

Configuration de l'authentification Kerberos sur la CLI

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit pour garantir l'authentification du trafic sur l'appliance.

   ns-cli-prompt> **enable ns feature** AAA

2. Ajoutez le fichier keytab à l'appliance NetScaler. Un fichier keytab est nécessaire pour déchiffrer le secret reçu du client lors de l'authentification Kerberos. Un seul fichier keytab contient les détails d'authentification de tous les services liés au serveur virtuel de gestion du trafic sur l'appliance NetScaler.

   Générez d'abord le fichier keytab sur le serveur Active Directory, puis transférez-le vers l'appliance NetScaler.

- Ouvrez une session sur le serveur Active Directory et ajoutez un utilisateur pour l'authentification Kerberos à l'aide de la commande suivante.

```
net user <username> <password> /add
```

> **Remarque**
>
> Dans la section **Propriétés de l'utilisateur**, assurez-vous que l'option « Modifier le mot de passe à la prochaine ouverture de session » n'est pas sélectionnée et que l'option « Le mot de passe n'expire pas » est sélectionnée.

- Mappez le service HTTP à l'utilisateur ci-dessus et exportez le fichier keytab. Par exemple, exécutez la commande suivante sur le serveur Active Directory :

```
ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM
   /pass <user password> /mapuser newacp\\dummy /ptype KRB5\
   _NT\_PRINCIPAL
```

> **Remarque**
>
> Vous pouvez mapper plusieurs services si l'authentification est requise pour plusieurs services. Si vous souhaitez mapper d'autres services, répétez la commande ci-dessus pour chaque service. Vous pouvez donner le même nom ou des noms différents au fichier de sortie.

- Transférez le fichier keytab vers l'appliance NetScaler à l'aide de la commande unix **ftp** ou de tout autre utilitaire de transfert de fichiers de votre choix. Téléchargez le fichier keytab dans le répertoire /nsconfig/krb/ de l'appliance NetScaler.

3. L'appliance NetScaler doit obtenir l'adresse IP du contrôleur de domaine à partir du nom de domaine complet (FQDN). Citrix recommande donc de configurer NetScaler avec un serveur DNS.

   ns-cli-prompt> **add dns nameserver** <ip-address>

   > **Remarque**
   >
   > Vous pouvez également ajouter des entrées d'hôte statiques ou utiliser tout autre moyen pour que l'appliance NetScaler puisse convertir le nom FQDN du contrôleur de domaine en adresse IP.

4. Configurez l'action d'authentification, puis associez-la à une stratégie d'authentification.

   - Configurez l'action de négociation.

     ns-cli-prompt> **add authentication negotiateAction** <name> -domain <domain name> -domainUser <domain user name> -domainUserPasswd <domain user password> -

defaultAuthenticationGroup <default authentication group> -keytab <string> -NTLMPath <string>

Remarque : Pour la configuration de l'utilisateur du domaine et du nom de domaine, accédez au client et utilisez la commande klist comme illustré dans l'exemple suivant :

Client: username @ AAA.LOCAL

Server: HTTP/onprem_idp.aaa.local @ AAA.LOCAL

add authentication negotiateAction <name> -domain -domainUser <HTTP/onprem_idp.aaa.local>

- Configurez la stratégie de négociation et associez l'action de négociation à cette stratégie.

  ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>

5. Créez un serveur virtuel d'authentification et associez-le à la stratégie de négociation.
   - Créez un serveur virtuel d'authentification.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>

   - Liez la stratégie de négociation au serveur virtuel d'authentification.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>

6. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu).

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

   > **Remarque**
   >
   > Des configurations similaires peuvent également être effectuées sur le serveur virtuel de commutation de contenu.

7. Vérifiez les configurations en procédant comme suit :
   - Accédez au serveur virtuel de gestion du trafic à l'aide du nom de domaine complet. Par exemple, Sample
   - Affichez les détails de la session sur l'interface de ligne de commande.

     ns-cli-prompt> **show aaa session**

Configuration de l'authentification Kerberos sur l'interface graphique

1. Activez la fonctionnalité d'authentification, d'autorisation et d'audit.

   Accédez à **Système** > **Paramètres**, cliquez sur **Configurer les fonctionnalités de base** et activez la fonctionnalité d'authentification, d'autorisation et d'audit.

2. Ajoutez le fichier keytab comme détaillé à l'étape 2 de la procédure CLI mentionnée ci-dessus.
3. Ajoutez un serveur DNS.

   Accédez à **Gestion du trafic > DNS > Serveurs de noms**et spécifiez l'adresse IP du serveur DNS.
4. Configurez l'action et la stratégie **Négocier** .

   Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégie**et créez une stratégie avec **Négocier** comme type d'action. Cliquez sur **AJOUTER** pour créer un nouveau serveur de négociation d'authentification ou sur **Modifier** pour configurer les détails existants.
5. Liez la stratégie de négociation au serveur virtuel d'authentification.

   Accédez à **Sécurité > AAA - Trafic des applications > Serveurs virtuels**et associez la stratégie de **négociation** au serveur virtuel d'authentification.
6. Associez le serveur virtuel d'authentification au serveur virtuel de gestion du trafic (équilibrage de charge ou commutation de contenu).

   Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et spécifiez les paramètres d'authentification appropriés.

   > **Remarque**
   >
   > Des configurations similaires peuvent également être effectuées sur le serveur virtuel de commutation de contenu.
7. Vérifiez les configurations décrites à l'étape 7 de la procédure CLI mentionnée ci-dessus.

Configuration de l'authentification Kerberos sur un client

May 5, 2023

La prise en charge de Kerberos doit être configurée sur le navigateur pour utiliser Kerberos pour l'authentification. Vous pouvez utiliser n'importe quel navigateur compatible Kerberos. Les instructions pour configurer la prise en charge de Kerberos sur Internet Explorer et Mozilla Firefox sont présentées ci-dessous. Pour les autres navigateurs, consultez la documentation du navigateur.

Pour configurer l'authentification Internet Explorer pour Kerberos

1. Dans le menu **Outils**, sélectionnez **Options Internet**.
2. Dans l'onglet **Sécurité**, cliquez sur **Intranet local**, puis sur **Sites**.
3. **Dans la boîte de dialogue**Intranet local**, assurez-vous que l'option Détecter automatiquement le réseau intranet est sélectionnée, puis cliquez sur Avancé.**

4. Dans la boîte de dialogue **Intranet local**, ajoutez les sites Web des domaines du serveur virtuel de gestion du trafic sur l'appliance NetScaler. Les sites spécifiés deviennent des sites intranet locaux.
5. Cliquez sur **Fermer** ou sur **OK** pour fermer les boîtes de dialogue.

Pour configurer l'authentification Mozilla Firefox pour Kerberos

1. Assurez-vous que Kerberos est correctement configuré sur votre ordinateur.
2. Tapez about:config dans la barre d'URL.
3. Dans la zone de texte du filtre, tapez network.negotiate.
4. Remplacez network.negotiate-auth.delegation-uris par le domaine que vous souhaitez ajouter.
5. Remplacez network.negotiate-auth.trusted-uris par le domaine que vous souhaitez ajouter.

> **Remarque :** Si vous exécutez Windows, vous devez également entrer sspi dans la zone de texte du filtre et changer l'option network.auth.use-sspi sur False.

Décharger l'authentification Kerberos des serveurs physiques

June 2, 2023

L'appliance NetScaler peut décharger les tâches d'authentification des serveurs. Au lieu que les serveurs physiques authentifient les demandes des clients, NetScaler authentifie toutes les demandes des clients avant de les transmettre à l'un des serveurs physiques qui lui sont liés. L'authentification de l'utilisateur est basée sur des jetons Active Directory.

Il n'existe aucune authentification entre NetScaler et le serveur physique, et le déchargement de l'authentification est transparent pour les utilisateurs finaux. Après l'ouverture de session initiale sur un ordinateur Windows, l'utilisateur final n'a pas besoin de saisir d'informations d'authentification supplémentaires dans une fenêtre contextuelle ou sur une page d'ouverture de session.

Dans la version actuelle de l'appliance NetScaler, l'authentification Kerberos n'est disponible que pour l'authentification, l'autorisation et l'audit des serveurs virtuels de gestion du trafic. L'authentification Kerberos n'est pas prise en charge pour le VPN SSL dans l'appliance NetScaler Gateway Advanced Edition ou pour la gestion de l'appliance NetScaler.

L'authentification Kerberos nécessite une configuration sur l'appliance NetScaler et sur les navigateurs clients.

Pour configurer l'authentification Kerberos sur l'appliance NetScaler

> **Remarque**
>
> Les mots de passe utilisés dans l'exemple de configuration suivant ne sont que des exemples et non les mots de passe de configuration réels.

1. Créez un compte utilisateur sur Active Directory. Lors de la création d'un compte utilisateur, vérifiez les options suivantes dans la section Propriétés de l'utilisateur :
   - Assurez-vous de ne pas sélectionner l'option Modifier le mot de passe lors de la prochaine connexion.
   - Assurez-vous de sélectionner l'option Le mot de passe n'expire pas.
2. Sur le serveur AD, à l'invite de commandes de l'interface de ligne de commande, tapez :
   - ktpass -princ HTTP/ kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass Citrix1 -out C:\kerbtabfile.txt

   > **Remarque**
   >
   > N'oubliez pas de taper la commande ci-dessus sur une seule ligne. La sortie de la commande ci-dessus est écrite dans le fichier C:\kerbtabfile.txt.
3. Téléchargez le fichier kerbtabfile.txt dans le répertoire /etc de l'appliance NetScaler à l'aide d'un client Secure Copy (SCP).
4. Exécutez la commande suivante pour ajouter un serveur DNS à l'appliance NetScaler.
   - add dns nameserver 1.2.3.4

   L'appliance NetScaler ne peut pas traiter les requêtes Kerberos sans le serveur DNS. Assurez-vous d'utiliser le même serveur DNS que celui utilisé dans le domaine Microsoft Windows.
5. Passez à l'interface de ligne de commande de NetScaler.
6. Exécutez la commande suivante pour créer un serveur d'authentification Kerberos :
   - add authentication negotiateAction KerberosServer -domain "crete.lab.net" -domainUser kerbuser -domainUserPasswd Citrix1 -keytab /var/mykcd.keytab

   > **Remarque**
   >
   > Si keytab n'est pas disponible, vous pouvez spécifier les paramètres suivants : domain, DomainUser et -DomainUserPasswd.
7. Exécutez la commande suivante pour créer une stratégie de négociation :
   - `add authentication negotiatePolicy Kerberos-Policy "REQ.IP.DESTIP == 192.168.17.200"KerberosServer<!--NeedCopy-->`
8. Exécutez la commande suivante pour créer un serveur virtuel d'authentification.
   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`

9. Exécutez la commande suivante pour lier la stratégie Kerberos au serveur virtuel d'authentification :
   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`
10. Exécutez la commande suivante pour lier un certificat SSL au serveur virtuel d'authentification. Vous pouvez utiliser l'un des certificats de test, que vous pouvez installer à partir de l'appliance GUI NetScaler. Exécutez la commande suivante pour utiliser l'exemple de certificat ServerTestCert.
    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`
11. Créez un serveur virtuel d'équilibrage de charge HTTP avec l'adresse IP 192.168.17.200.

    Assurez-vous de créer un serveur virtuel à partir de l'interface de ligne de commande pour les versions NetScaler 9.3 si elles sont antérieures à 9.3.47.8.
12. Exécutez la commande suivante pour configurer un serveur virtuel d'authentification :
    - `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy-->`
13. Entrez l' exemple de nom d'hôte dans la barre d'adresse du navigateur Web.

    Le navigateur Web affiche une boîte de dialogue d'authentification car l'authentification Kerberos n'est pas configurée dans le navigateur.

    > **Remarque**
    >
    > L'authentification Kerberos nécessite une configuration spécifique sur le client. Assurez-vous que le client peut résoudre le nom d'hôte, ce qui entraîne la connexion du navigateur Web à un serveur virtuel HTTP.
14. Configurez Kerberos sur le navigateur Web de l'ordinateur client.
    - Pour la configuration sur Internet Explorer, reportez-vous à la section Configuration de l'authentification Internet Explorer pour Kerberos.
    - Pour la configuration sur Mozilla Firefox, reportez-vous à la section Configuration de l'authentification Internet Explorer pour Kerberos.
15. Vérifiez si vous pouvez accéder au serveur physique principal sans authentification.

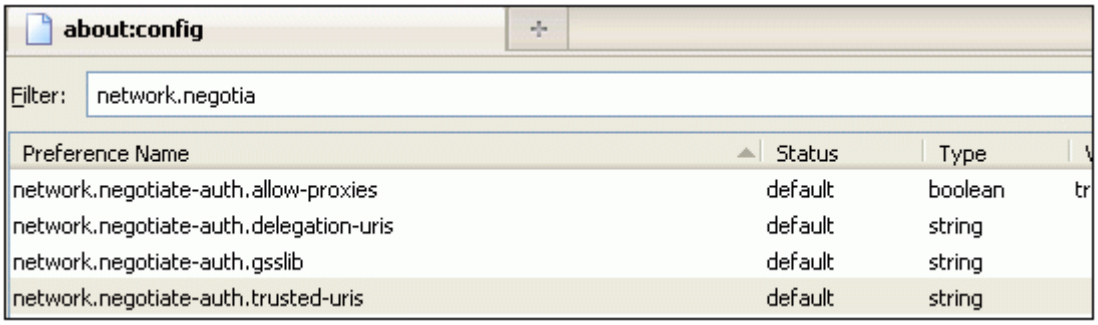
Pour configurer l'authentification Internet Explorer pour Kerberos

1. Sélectionnez **Options Internet** dans le menu **Outils** .
2. Activez l'onglet **Sécurité** .
3. Sélectionnez **Intranet local dans** la section Sélectionner une zone pour afficher les paramètres de sécurité des modifications.

4. Cliquez sur **Sites**.
5. Cliquez sur **Avancé**.
6. Spécifiez l'URL, Exemple, puis cliquez sur **Ajouter**.
7. Redémarrez **Internet Explorer**.

Pour configurer l'authentification Mozilla Firefox pour Kerberos

1. Entrez about:config dans la barre d'adresse du navigateur.
2. Cliquez sur l'avertissement de non-responsabilité.
3. Tapez **Network.Negotiate-Auth.Trusted-URIS** dans la zone **Filtre** .
4. Double-cliquez sur **Network.Negotiate-Auth.Trusted-URIS.** Un exemple d'écran est présenté ci-dessous.



5. Dans la boîte de dialogue Saisir une valeur de chaîne, spécifiez www.crete.lab.net.
6. Redémarrez Firefox.

Résoudre les problèmes liés à l'authentification et à l'autorisation

May 5, 2023

Localiser les messages d'erreur

Localiser les messages d'erreur générés par le système NetScaler nFactor

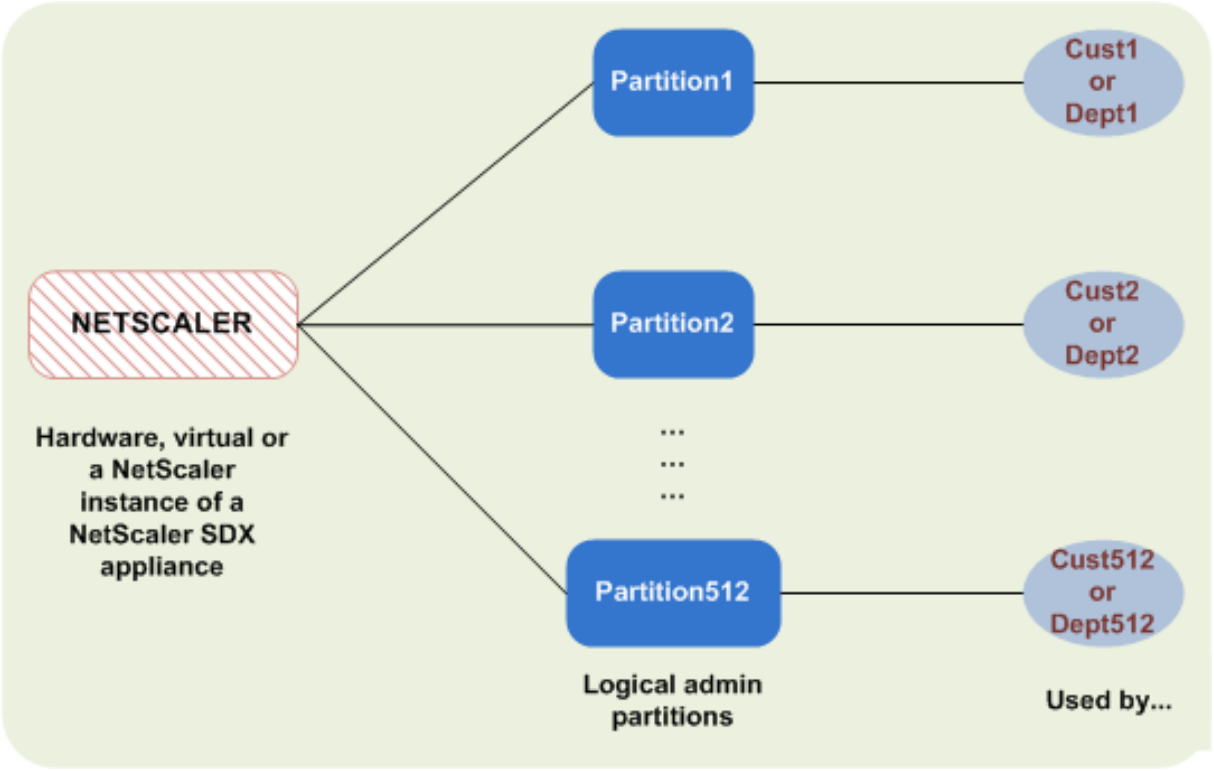
Résoudre les problèmes d'authentification avec le module aaad.debug

Résoudre les problèmes d'authentification dans NetScaler et NetScaler Gateway avec le module aaad.debug

Partition d'administration

May 5, 2023

Une appliance NetScaler peut être partitionnée en entités logiques appelées partitions d'administration. Chaque partition peut être configurée et utilisée comme une appliance NetScaler distincte. La figure suivante montre les partitions d'un NetScaler utilisées par différents clients et services :



Une appliance NetScaler partitionnée possède une seule partition par défaut et une ou plusieurs partitions d'administration. Le tableau suivant fournit des informations supplémentaires sur les deux types de partitions :

> **Remarque**
>
> Dans une appliance partitionnée, le mode BridgeBPDU ne peut être activé que dans la partition par défaut et non dans les partitions administratives.

Disponibilité :

L'appliance NetScaler est livrée avec une seule partition, appelée partition par défaut. La partition par défaut est conservée même après le partitionnement de l'appliance NetScaler.

Doit être créé explicitement comme décrit dans Configurer les partitions d'administration.

Nombre de partitions :

Un

Une appliance NetScaler peut comporter une ou plusieurs partitions d'administration (512 au maximum).

Accès et rôles des utilisateurs :

Tous les utilisateurs de NetScaler, qui ne sont pas associés à une politique de commande *spécifique à une partition*, peuvent accéder à la partition par défaut et la configurer. Comme toujours, la politique de commande associée restreint les opérations qu'un utilisateur peut effectuer.

L'accès et les rôles des utilisateurs sont créés par les superutilisateurs de NetScaler qui spécifient également les utilisateurs pour cette partition. Seuls les superutilisateurs et les utilisateurs associés de la partition peuvent accéder à la partition d'administration et la configurer.

> **Remarque**
>
> Les utilisateurs de partitions n'ont pas accès au shell.

Structure du fichier :

Tous les fichiers d'une partition par défaut sont stockés dans la structure de fichiers NetScaler par défaut.

Par exemple, le répertoire */nsconfig* stocke le fichier de configuration NetScaler et le répertoire */var/log/* stocke les journaux NetScaler.

Tous les fichiers d'une partition d'administration sont stockés dans des chemins de répertoire portant le nom de la partition d'administration.

Par exemple, le fichier de configuration NetScaler (ns.conf) est stocké dans le répertoire. `/nsconfig/partitions/<partitionName>` Les autres fichiers spécifiques à la partition sont stockés dans les `/var/partitions/<partitionName>` répertoires.

Quelques autres chemins dans une partition d'administration :

- Fichiers téléchargés : `/var/partitions/<partitionName>/download/`
- Fichiers journaux : `/var/partitions/<partitionName>/log/`

> **Remarque**
>
> Actuellement, la journalisation n'est pas prise en charge au niveau de la partition. Par conséquent, ce répertoire est vide et tous les journaux y sont stockés. `/var/log/`

- Fichiers relatifs au certificat SSL CRL : `/var/partitions/<partitionName>/netscaler/ssl`

Ressources disponibles :

Toutes les ressources NetScaler.

Ressources NetScaler qui sont explicitement attribuées à la partition d'administration.

Accès et rôles des utilisateurs

Lors de l'authentification et de l'autorisation d'une appliance NetScaler partitionnée, un administrateur root peut affecter un administrateur de partition à une ou plusieurs partitions. L'administrateur de partition peut autoriser les utilisateurs à accéder à cette partition sans affecter les autres partitions. Les utilisateurs de la partition sont autorisés à accéder uniquement à cette partition à l'aide de l'adresse SNIP. L'administrateur root et l'administrateur de partition peuvent configurer l'accès basé sur les rôles (RBA) en autorisant les utilisateurs à accéder à différentes applications.

Les rôles des administrateurs et des utilisateurs peuvent être décrits comme suit :

Administrateur root. Accède à l'appliance partitionnée via son adresse NSIP et peut accorder à l'utilisateur l'accès à une ou plusieurs partitions. L'administrateur peut également affecter des administrateurs de partition à une ou plusieurs partitions. L'administrateur peut créer un administrateur de partition à partir de la partition par défaut à l'aide d'une adresse NSIP ou passer à une partition, puis créer un utilisateur et attribuer un accès administrateur de partition à l'aide d'une adresse SNIP.

Administrateur de partition. Accède à la partition spécifiée via une adresse NSIP attribuée par l'administrateur root. L'administrateur peut attribuer un accès basé sur les rôles à l'accès utilisateur de la partition à cette partition et également configurer l'authentification du serveur externe à l'aide d'une configuration spécifique à la partition.

Utilisateur du système. Accède aux partitions via l'adresse NSIP. A accès aux partitions et aux ressources spécifiées par l'administrateur root.

Utilisateur de la partition. Accède à une partition via une adresse SNIP. Le compte utilisateur est créé par l'administrateur de la partition et l'utilisateur a accès aux ressources, uniquement au sein de la partition.

Points à retenir

Voici quelques points à retenir lorsque vous fournissez un accès basé sur les rôles à une partition.

1. Les utilisateurs de NetScaler accédant à l'interface graphique via l'adresse NSIP utilisent la configuration d'authentification de partition par défaut pour se connecter à l'appliance.
2. Les utilisateurs du système de partition accédant à l'interface graphique via une adresse SNIP de partition utilisent une configuration d'authentification spécifique à la partition pour se connecter à l'appliance.
3. L'utilisateur de la partition créé dans une partition ne peut pas se connecter à l'aide de l'adresse NSIP.
4. L'utilisateur NetScaler lié à une partition ne peut pas se connecter à l'aide de l'adresse SNIP de la partition.
5. Les utilisateurs du système qui s'authentifient via un serveur d'authentification externe (par exemple, LDAP, RADIUS, TACACS) doivent accéder à une partition via une adresse SNIP.

Cas d'utilisation pour la gestion de l'accès basé sur les rôles dans une configuration partitionnée

Imaginons un scénario dans lequel une entreprise, www.example.com, possède plusieurs unités commerciales et un administrateur centralisé qui gère toutes les instances de son réseau. Cependant, ils souhaitent fournir des privilèges utilisateur et un environnement exclusifs pour chaque unité commerciale.

Vous trouverez ci-dessous les administrateurs et les utilisateurs gérés par la configuration d'authentification de partition par défaut et la configuration spécifique à la partition dans une appliance partitionnée.

John : administrateur root

George : administrateur de partition

Adam : utilisateur du système

Jane : utilisateur de la partition

John est l'administrateur root d'une appliance NetScaler partitionnée. John gère tous les comptes utilisateurs et les comptes utilisateurs administratifs sur les partitions (par exemple, P1, P2, P3, P4 et P5) au sein de l'appliance. John fournit un accès granulaire basé sur les rôles aux entités depuis la partition par défaut de l'appliance. John crée des comptes utilisateurs et attribue un accès aux partitions à chaque compte. En tant qu'ingénieur réseau au sein de l'organisation, George préfère avoir un accès basé sur les rôles à quelques applications exécutées sur la partition P2. Sur la base de la gestion des utilisateurs, John crée un rôle d'administrateur de partition pour George et associe son compte utilisateur à une politique de commande partition-admin dans la partition P2. Adam étant un autre ingénieur réseau, il préfère accéder à une application s'exécutant sur P2. John crée un compte utilisateur système pour Adam et associe son compte utilisateur à une partition P2. Une fois le compte créé, Adam peut se connecter à l'appliance pour accéder à l'interface de gestion NetScaler via l'adresse NSIP et peut basculer vers la partition P2 en fonction de la liaison utilisateur/groupe.

Supposons que Jane, une autre ingénieure réseau, souhaite accéder directement à une application exécutée uniquement sur la partition P2. George (administrateur de partition) peut créer un compte utilisateur de partition pour elle et associer son compte à des politiques de commande pour les privilèges d'autorisation. Le compte utilisateur de Jane créé dans la partition est désormais directement associé à P2. Jane peut désormais accéder à l'interface de gestion NetScaler via l'adresse SNIP et ne peut passer à aucune autre partition.

> **Remarque**
>
> Si le compte utilisateur de Jane est créé par un administrateur de partition dans la partition P2, l'administrateur peut accéder à l'interface de gestion NetScaler uniquement via l'adresse SNIP (créée dans la partition). L'administrateur n'est pas autorisé à accéder à l'interface via l'adresse

> NSIP. De même, si le compte utilisateur d'Adam est créé par un administrateur root dans la partition par défaut et est lié à une partition P2. L'administrateur peut accéder à l'interface de gestion NetScaler uniquement via l'adresse NSIP ou l'adresse SNIP créée dans la partition par défaut (avec l'accès à la gestion activé). Et il n'est pas autorisé à accéder à l'interface de partition via l'adresse SNIP créée dans la partition administrative.

Configurer les rôles et les responsabilités des administrateurs de partition

Voici les configurations effectuées par un administrateur root dans une partition par défaut.

Création de partitions administratives et d'utilisateurs système : un administrateur root crée des partitions administratives et des utilisateurs système dans la partition par défaut de l'appliance. L'administrateur associe ensuite les utilisateurs à différentes partitions. Si vous êtes lié à une ou plusieurs partitions, vous pouvez passer d'une partition à l'autre en fonction des liaisons utilisateur. De plus, votre accès à une ou plusieurs partitions liées n'est autorisé que par l'administrateur root.

Autorisation de l'utilisateur système en tant qu'administrateur de partition pour une partition spécifique — Une fois qu'un compte utilisateur est créé, l'administrateur root bascule vers une partition spécifique et autorise l'utilisateur en tant qu'administrateur de partition. Cela se fait en attribuant la politique de commande partition-admin au compte utilisateur. L'utilisateur peut désormais accéder à la partition en tant qu'administrateur de partition et gérer les entités de la partition.

Voici les configurations effectuées par un administrateur de partition dans une partition administrative.

Configuration de l'adresse SNIP dans une partition administrative : l'administrateur de la partition se connecte à la partition, crée une adresse SNIP et fournit un accès de gestion à cette adresse.

Création et association d'un utilisateur du système de partition à la politique de commande de partition : l'administrateur de partition crée des utilisateurs de partition et définit l'étendue de l'accès des utilisateurs. Cela se fait en liant le compte utilisateur aux politiques de commande de partition.

Création et association de groupes d'utilisateurs d'un système de partition avec la politique de commande de partition - L'administrateur de partition crée des groupes d'utilisateurs de partition et définit l'étendue de l'accès aux groupes d'utilisateurs. Cela se fait en liant le compte du groupe d'utilisateurs aux politiques de commande de partition.

Configuration de l'authentification du serveur externe pour les utilisateurs externes (facultatif) - Cette configuration est effectuée pour authentifier les utilisateurs TACACS externes accédant à la partition à l'aide de l'adresse SNIP.

Les tâches suivantes sont effectuées lors de la configuration de l'accès basé sur les rôles pour les utilisateurs d'une partition administrative.

1. Création d'une partition administrative : avant de créer des utilisateurs dans une partition administrative, vous devez d'abord créer la partition. En tant qu'administrateur root, vous pouvez

créer une partition à partir de la partition par défaut à l'aide de l'utilitaire de configuration ou d'une interface de ligne de commande.

2. Changement de l'accès utilisateur de la partition par défaut vers la partition P2 — Si vous êtes un administrateur de partition accédant à l'appliance depuis la partition par défaut, vous pouvez passer de la partition par défaut à une partition spécifique. Par exemple, partitionnez P2 en fonction de la liaison utilisateur.
3. Ajouter une adresse SNIP au compte utilisateur de la partition avec l'accès à la gestion activé : une fois que vous avez transféré votre accès à une partition d'administration. Vous créez une adresse SNIP et vous fournissez un accès de gestion à cette adresse.
4. Création et association d'un utilisateur du système de partition à l'aide d'une politique de commande de partitionSi vous êtes administrateur de partition, vous pouvez créer des utilisateurs de partition et définir l'étendue de l'accès des utilisateurs. Cela se fait en liant le compte utilisateur aux politiques de commande de partition.
5. Création et association d'un groupe d'utilisateurs de partition à la politique de commande de partition : si vous êtes administrateur de partition, vous pouvez créer des groupes d'utilisateurs de partition et définir l'étendue du contrôle d'accès des utilisateurs. Cela se fait en liant le compte du groupe d'utilisateurs aux politiques de commande de partition.

Configuration de l'authentification du serveur externe pour les utilisateurs externes (facultatif) - Cette configuration est effectuée pour authentifier les utilisateurs TACACS externes accédant à la partition à l'aide d'une adresse SNIP.

Avantages de l'utilisation de partitions d'administration

Vous pouvez bénéficier des avantages suivants en utilisant des partitions d'administration pour votre déploiement :

- Permet de déléguer la propriété administrative d'une application au client.
- Réduit le coût de possession d'un ADC sans compromettre les performances et la facilité d'utilisation.
- Protège contre les modifications de configuration injustifiées. Dans une appliance NetScaler non partitionnée, les utilisateurs autorisés de l'autre application peuvent modifier intentionnellement ou non les configurations requises pour votre application. Cela peut entraîner un comportement indésirable. Cette possibilité est réduite dans une appliance NetScaler partitionnée.
- Isole le trafic entre différentes applications en utilisant des VLAN dédiés pour chaque partition.
- Accélère et permet l'évolutivité des déploiements d'applications.
- Permet une gestion et des rapports au niveau de l'application ou localisés.

Laissez-nous analyser quelques cas pour comprendre les scénarios dans lesquels vous pouvez utiliser des partitions d'administration.

Cas utilisateur 1 : Comment la partition d'administration est utilisée dans un réseau d'entreprise

Considérons un scénario auquel est confrontée une société nommée **Foo.com**.

- **Foo.com** possède un seul NetScaler.
- Il existe cinq départements et chaque département possède une application qui doit être déployée avec NetScaler.
- Chaque application doit être gérée indépendamment par un ensemble différent d'utilisateurs ou d'administrateurs.
- Les autres utilisateurs doivent être empêchés d'accéder aux configurations.
- L'application ou le back-end doit être en mesure de partager des ressources telles que des adresses IP.
- Le service informatique mondial doit être en mesure de contrôler les paramètres de niveau NetScaler qui doivent être communs à toutes les partitions.
- Les applications doivent être indépendantes les unes des autres. Une erreur dans la configuration d'une application ne doit pas affecter l'autre.

Un NetScaler non partitionné ne serait pas en mesure de répondre à ces exigences. Toutefois, vous pouvez satisfaire à toutes ces exigences en partitionnant un NetScaler.

Il suffit de créer une partition pour chacune des applications, d'attribuer les utilisateurs requis aux partitions, de spécifier un VLAN pour chaque partition et de définir les paramètres globaux sur la partition par défaut.

Cas d'utilisation 2 : comment une partition d'administration est utilisée par un fournisseur de services

Considérons un scénario auquel est confronté un fournisseur de services nommé **BigProvider** :

- BigProvider compte 5 clients : 3 petites entreprises et 2 grandes entreprises.
- **SmallBiz**, **SmallerBiz et**StartupBiz** n'ont besoin que des fonctionnalités NetScaler les plus élémentaires.
- **BigBiz** et **LargeBiz** sont de grandes entreprises dont les applications attirent un trafic important. Ils souhaiteraient utiliser certaines des fonctionnalités les plus complexes de NetScaler.

Dans une approche non partitionnée, l'administrateur NetScaler utilise généralement une appliance NetScaler SDX et provisionner une instance NetScaler pour chaque client.

La solution convient à **BigBiz et**LargeBiz**** car leurs applications ont besoin de la puissance intacte de l'ensemble de l'appliance NetScaler non partitionnée. **Toutefois, cette solution n'est peut-être pas aussi rentable pour la maintenance de **SmallBiz, SmallerBizet StartupBiz**.****

BigProvider opte donc pour la solution suivante :

- ****Utilisation d'une appliance NetScaler SDX pour créer des instances NetScaler dédiées pour BigBiz et LargeBiz.****
- **Utilisation d'un seul NetScaler partitionné en trois partitions, une pour**SmallBiz, **Smaller-Biz**et StartupBiz**.**

L'administrateur NetScaler (superutilisateur) crée une partition d'administration pour chacun de ces clients et indique les utilisateurs des partitions. Il spécifie également les ressources NetScaler pour les partitions et le VLAN à utiliser par le trafic destiné à chacune des partitions.

Prise en charge des configurations NetScaler dans la partition d'administration

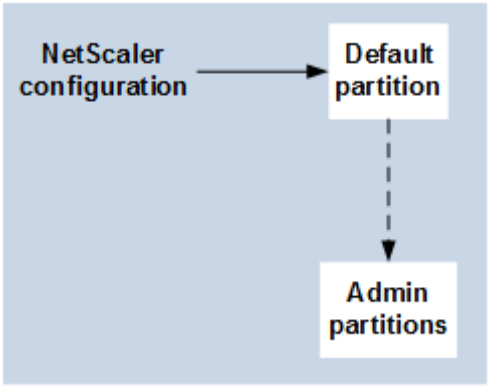
May 5, 2023

Les configurations NetScaler peuvent être classées selon les trois types de configurations suivants. Cela dépend de la configuration Citrix et de la partition dans laquelle la configuration est effectuée.

> **Remarque**
>
> - Les partitions d'administration ne peuvent pas être configurées sur un cluster NetScaler. Cela signifie qu'un cluster NetScaler ne peut pas être partitionné.
> - Les partitions d'administration ne peuvent pas être configurées sur une appliance NetScaler 14000 FIPS.
> - Lecas 3 répertorie les fonctionnalités de NetScaler qui ne sont pas prises en charge dans les partitions d'administration.
> - Les modèles d'équilibrage de charge ne sont pas pris en charge dans les partitions d'administration.

Cas 1 (configurations globales)

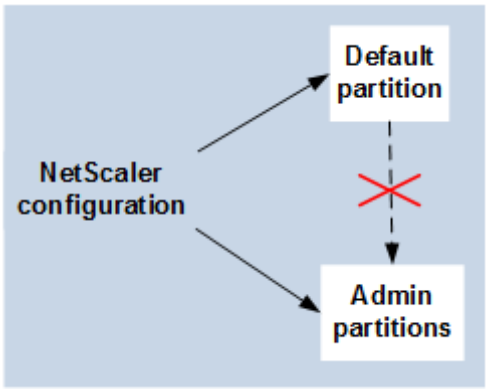
Configurations qui peuvent être exécutées UNIQUEMENT dans la partition par défaut et qui sont disponibles ou qui ont un impact sur toutes les partitions d'administration.



- Mises à jour des entités intégrées pour les moniteurs, les profils TCP, les profils HTTP, etc.
- Mises à jour des paramètres globaux pour syslog, NSLOG, weblog, commutation de contenu, IPSEC, SIP, DHCP, protection contre les surtensions, mise en mémoire tampon TCP et collecte de systèmes.
- Configurations haute disponibilité (HA)
- Modifications de l'interface et du VLAN
- Configurations utilisateur

Cas 2 (configurations spécifiques aux partitions)

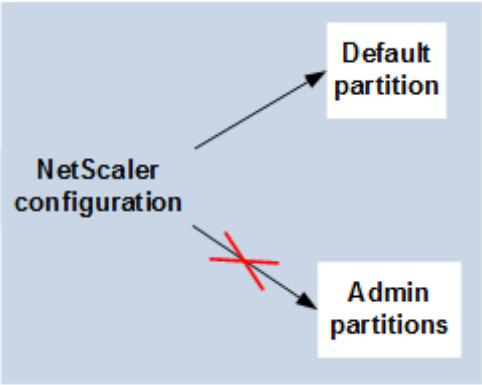
Configurations pouvant être exécutées indépendamment dans les partitions par défaut et d'administration. Ces configurations s'appliquent uniquement à la partition dans laquelle elles sont exécutées.



- Obtention des statistiques de niveau de trafic pour une partition.
- L'administrateur de partition peut mettre à jour les liaisons IP pour le VLAN qui est lié à cette partition. Mais il n'est pas possible de mettre à jour les liaisons d'interface.
- Effacement des configurations NetScaler.
- Paramètres spécifiques aux fonctionnalités pour les fonctionnalités suivantes : AppFlow, AppQoE, compression HTTP, DNS, TCP, HTTP, chiffrement, répondeur, réécriture et SSL.
- Configurations spécifiques aux fonctionnalités telles que les serveurs virtuels, les services et les moniteurs.

Cas 3

Configurations qui ne peuvent pas être exécutées sur les partitions d'administration. Ces fonctionnalités peuvent être configurées dans la partition par défaut, mais elles n'ont aucun impact sur les partitions d'administration.



> **Remarque :**
>
> Les configurations prises en charge sur les partitions d'administration pour une version particulière sont marquées comme **Oui**.

Composant caractéristique	Fonctionnalité NetScaler	NetScaler 11.1	NetScaler 12.0	NetScaler 12.1	NetScaler 13.0	NetScaler 13.1
Réseau	Domaine de trafic	Non (non pris en charge à partir de la version 60.13)	Non	Non	Non	Non
Stratégie	Extensibilité	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	Mise à l'Autoscale DBS	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	DNSSEC	Non	Non	Oui	Oui	Oui
Équilibrage de charge	Diameter	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	RTSP	Non	Non	Non	Non	Non

Composant caractéristique	Fonctionnalité NetScaler	NetScaler 11.1	NetScaler 12.0	NetScaler 12.1	NetScaler 13.0	NetScaler 13.1
Équilibrage de charge	Sure Connect	Oui	Oui	Obsolète	Obsolète	Supprimé
Équilibrage de charge	Groupe de services Autoscale	Oui	Oui	Oui	Oui	Oui
Facilité de gestion	Authentificati externe RBA	Oui	Oui	Oui	Oui	Oui
Facilité de gestion	Cisco RISE	Non	Non	Non	Oui	Oui
Facilité de gestion	ACI-Cisco	Oui	Oui	Oui	Oui	Oui
Facilité de gestion	AppExpert	Oui	Oui	Oui	Oui	Oui
Facilité de gestion	HDX Insight	Non	Non	Non	Non	Non
Facilité de gestion	Insight	Non	Non	Non	Non	Non
VPN	Connecteur Citrix Cloud-Bridge	Non	Non	Non	Non	Non
VPN	NetScaler Gateway ou VPN SSL	Non	Non	Non	Non	Non
VPN	Proxy ICA VPN SSL	Non	Non	Non	Non	Non
VPN	Interface Web sur NetScaler	Non	Non	Non	Non	Non
SSL	Profil SSL	Oui	Oui	Oui	Oui	Oui
SSL	SSL-FIPS	Non	Non	Non	Non	Non

Composant caractéristique	Fonctionnalité NetScaler	NetScaler 11.1	NetScaler 12.0	NetScaler 12.1	NetScaler 13.0	NetScaler 13.1
SSL	HSM externe	Non	Non	Non	Non	Non
Infra	Redirection de cache	Non	Non	Non	Non	Non
Infra	Mise en cache intégrée	Oui	Oui	Oui	Oui	Oui
Réseau	VXLAN	Oui	Oui	Oui	Oui	Oui
Réseau	Arrêt gracieux	Oui	Oui	Oui	Oui	Oui
Réseau	LSN	Non	Non	Non	Non	Non
Réseau	Logo IPv6 Ready	Oui	Oui	Oui	Oui	Oui
Réseau	vPath	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	flux de données	Oui	Oui	Oui	Oui	Oui
Journalisation	Journalisation Web	Oui	Oui	Oui	Oui	Oui
Réseau	Paramètre L2/L3	Oui	Oui	Oui	Oui	Oui
Réseau	Tunnel GRE	Oui	Oui	Oui	Oui	Oui
équilibrage de charge-ment	Surveillance scriptable	Oui	Oui	Oui	Oui	Oui
Équilibrage de charge	GSLB	Oui	Oui	Oui	Oui	Oui
Infra	Mise en miroir des connexions	Oui	Oui	Oui	Oui	Oui
Infra	FEO	Oui	Oui	Oui	Oui	Oui
Infra	Trace Ns	Oui	Oui	Oui	Oui	Oui

Composant caractéristique	Fonctionnalité NetScaler	NetScaler 11.1	NetScaler 12.0	NetScaler 12.1	NetScaler 13.0	NetScaler 13.1
Équilibrage de charge	File d'attente prioritaire	Oui	Oui	Obsolète	Obsolète	Supprimé
Réseau	HDOSP	Oui	Oui	Obsolète	Obsolète	Supprimé
Réseau	Profil net	Oui	Oui	Oui	Oui	Oui
Réseau	Mise en réseau (fonctionnalité restreinte)	Oui	Oui	Oui	Oui	Oui
Réseau	VRRP (fonctionnalité restreinte)	Oui	Oui	Oui	Oui	Oui
Journalisatio	Journalisatio d'audit (SYSLOG-TCP, LB de serveurs Syslog, prise en charge de SNIP et prise en charge du nom de domaine complet pour Syslog)	Oui	Oui	Oui	Oui	Oui
VPN	NetScaler Gateway	Non	Non	Non	Non	Non
VPN	AAA-TM	Oui	Oui	Oui	Oui	Oui

Composant caractéristique	Fonctionnalité NetScaler	NetScaler 11.1	NetScaler 12.0	NetScaler 12.1	NetScaler 13.0	NetScaler 13.1
AppFlow	AppFlow	Non	Oui (IPFIX uniquement)	Oui (IPFIX uniquement)	Oui	Oui
AppFW	Pare-feu d'application	Non	Non	Non	Non	Non
Transformation d'URL	Transformation d'URL	Non	Non	Non	Non	Non
Équilibrage de charge	Mise en mémoire tampon TCP	Non	Non	Non	Non	Non
Stratégies	Répondeur OCSP	Oui	Oui	Oui	Oui	Oui
Journal d'audit	SYSLOG-TCP	Non	Oui	Oui	Oui	Oui
Optimisation	Optimisation front-end	Non	Oui	Oui	Oui	Oui
AppQoE	AppQoE	Oui	Oui	Oui	Oui	Oui

Le tableau précédent répertorie certaines des fonctionnalités sous forme de **fonctionnalités restreintes** dans la configuration de la partition d'administration. La section suivante explique pourquoi certaines des fonctionnalités sont mentionnées comme des **fonctionnalités restreintes**.

- **VRRP**. Le VRRP est une fonctionnalité restreinte dans la partition d'administration en raison de ce qui suit :
  - L'ajout ou la suppression de VRID ne peuvent être effectués qu'à partir du contexte de partition par défaut. Toutefois, une fois qu'un VRID est créé, il peut être utilisé dans des partitions autres que par défaut.
  - La fonctionnalité VRRP est prise en charge uniquement sur les VLAN dédiés.
  - La fonctionnalité VRRP n'est pas prise en charge sur les VLAN partagés, utilisés par la partition d'administration. Il est bloqué en interne. Aucun message d'erreur n'est affiché pendant la configuration. Le protocole est bloqué sur un VLAN partagé (balisé ou non balisé) lié à une partition par défaut ou à n'importe quelle partition administrative.

> **Important**
>
> Pour prendre en charge le déploiement actif-actif à l'aide de VRRP, les VIP principal et de sauvegarde doivent utiliser le même VRID. Les différents VRID ne peuvent pas être utilisés.

- **Mise en réseau**. Certaines configurations réseau (L2 Param et L3 Param) ne sont pas prises en charge ou valides dans le contexte de la partition. Si vous rencontrez de telles configurations, le message d'erreur suivant s'affiche. « ERREUR : Cette option de configuration n'est pas prise en charge sur la partition autre que par défaut. «

Configuration des partitions d'administration

May 5, 2023

> **Important**
>
> - Seuls les superutilisateurs sont autorisés à créer et à configurer des partitions d'administration.
> - Sauf indication contraire, les configurations pour configurer une partition d'administration doivent être effectuées à partir de la partition par défaut.

En partitionnant une appliance NetScaler, vous créez plusieurs instances d'une seule appliance NetScaler. Chaque instance possède ses propres configurations et le trafic de chacune de ces partitions est isolé de l'autre. Cela se fait en attribuant à chaque partition un VLAN dédié ou un VLAN partagé.

Un NetScaler partitionné possède une partition par défaut et les partitions d'administration qui sont créées. Pour configurer une partition d'administration, vous devez d'abord créer une partition avec les ressources pertinentes (mémoire, bande passante maximale et connexions). Spécifiez ensuite les utilisateurs qui peuvent accéder à la partition et le niveau d'autorisation de chacun des utilisateurs de la partition.

L'accès à un NetScaler partitionné revient à accéder à un NetScaler non partitionné : via l'adresse NSIP ou toute autre adresse IP de gestion. En tant qu'utilisateur, une fois que vous avez fourni vos identifiants de connexion valides, vous êtes redirigé vers la partition à laquelle vous êtes lié. Toutes les configurations que vous créez sont enregistrées sur cette partition. Si vous êtes associé à plusieurs partitions, vous êtes redirigé vers la première partition à laquelle vous étiez associé. Si vous souhaitez configurer des entités sur l'une de vos autres partitions, vous devez explicitement passer à cette partition.

Après avoir accédé à la partition appropriée, les configurations que vous effectuez sont enregistrées sur cette partition et sont spécifiques à cette partition.

> **Remarque**
>
> - Les superutilisateurs de NetScaler et les autres utilisateurs ne disposant pas de partitions sont redirigés vers la partition par défaut.
> - Les utilisateurs de toutes les 512 partitions peuvent se connecter simultanément.

Conseil

Pour accéder à une appliance NetScaler partitionnée via HTTPS à l'aide du SNIP (avec l'accès à la gestion activé), assurez-vous que chaque partition possède le certificat de son administrateur de partition. Au sein de la partition, l'administrateur de la partition doit effectuer les opérations suivantes :

1. Ajoutez le certificat à NetScaler.

   ```
   add ssl certKey ns-server-certificate -cert ns-server.cert-key ns-server.key
   ```

2. Liez-le à un service nommé `nshttps-<SNIP>-3009`, où il `<SNIP>` doit être remplacé par l'adresse SNIP, dans ce cas 100.10.10.1.

   ```
   bind ssl service nshttps-100.10.10.1-3009 -certkeyName ns-server-certificate
   ```

Limitation des ressources de partition

Dans une appliance NetScaler partitionnée, un administrateur réseau peut créer une partition avec des ressources de partition telles que la mémoire, la bande passante et la limite de connexion configurées comme illimitées. Cela se fait en spécifiant Zero comme valeur de ressource de partition. Où zéro indique que la ressource est illimitée sur la partition et qu'elle peut être consommée dans les limites du système. La configuration des ressources de partition est utile lorsque vous migrez un déploiement de domaine de trafic vers une partition administrative ou si vous ne connaissez pas la limite d'allocation de ressources pour une partition dans un déploiement donné.

La limite de ressources pour une partition administrative est la suivante :

1. **Mémoire de partition**. Il s'agit de la mémoire maximale allouée pour une partition. Veillez à spécifier les valeurs lors de la création d'une partition.

   > **Remarque**
   >
   > À partir de NetScaler 12.0, lorsque vous créez une partition, vous pouvez définir la limite de mémoire sur zéro. Si une partition est déjà créée avec une limite de mémoire spécifique, vous pouvez réduire la limite à n'importe quelle valeur ou définir la limite sur zéro.

   Paramètre : MaxMemLimit

La mémoire maximale est allouée en Mo dans une partition. Une valeur nulle indique que la mémoire est illimitée sur la partition et qu'elle peut consommer jusqu'aux limites du système.

Valeur par défaut : 10

2. **Bande passante de partition**. Bande passante maximale allouée pour une partition. Si vous spécifiez une limite, assurez-vous qu'elle correspond au débit autorisé de l'appliance. Sinon, vous ne limitez pas la bande passante utilisée par la partition. La limite spécifiée dépend de la bande passante requise par l'application. Si la bande passante de l'application dépasse la limite spécifiée, les paquets sont supprimés.

   > **Remarque**
   >
   > À partir de NetScaler 12.0, lorsque vous pouvez créer une partition, vous pouvez définir la limite de bande passante de la partition sur zéro. Si une partition est déjà créée avec une bande passante spécifique, vous pouvez réduire la bande passante ou définir la limite sur zéro.

   Paramètre : MaxBandwidth

   La bande passante maximale est allouée en Kbit/s dans une partition. Une valeur nulle indique que la bande passante n'est pas restreinte. C'est-à-dire que la partition peut consommer jusqu'aux limites du système.

   Valeur par défaut : 10240

   Valeur maximale : 4294967295

3. **Connexion à une partition**. Nombre maximum de connexions simultanées pouvant être ouvertes dans une partition. La valeur doit tenir compte du débit simultané maximal attendu au sein de la partition. Les connexions aux partitions sont comptabilisées à partir de la mémoire à quota de partition. Auparavant, les connexions étaient comptabilisées à partir de la mémoire à quota de partition par défaut. Il est configuré uniquement côté client, pas sur les connexions TCP côté serveur principal. De nouvelles connexions ne peuvent pas être établies au-delà de cette valeur configurée.

   > **Remarque**
   >
   > À partir de NetScaler 12.0, vous pouvez créer une partition dont le nombre de connexions ouvertes est défini sur zéro. Si vous avez déjà créé une partition avec un nombre spécifique de connexions ouvertes, vous pouvez réduire la limite de connexions ou définir la limite sur zéro.

   Paramètre : MaxConnections

   Nombre maximum de connexions simultanées pouvant être ouvertes dans la partition. Une valeur nulle indique qu'il n'y a pas de limite quant au nombre de connexions ouvertes.

   Valeur par défaut : 1024

Valeur minimale : 0

Valeur maximale : 4294967295

Configurer une partition d'administration

Pour configurer une partition d'administration, effectuez les tâches suivantes.

Pour accéder à une partition d'administration à l'aide de l'interface de ligne de commande

1. Ouvrez une session sur l'appliance NetScaler.
2. Vérifiez si vous vous trouvez dans la bonne partition. L'invite de commande affiche le nom de la partition actuellement sélectionnée.
3. Si oui, passez à l'étape suivante.
4. Si ce n'est pas le cas, obtenez la liste des partitions auxquelles vous êtes associé et passez à la partition appropriée.
   - `show system user <username>`
   - `switch ns partition <partitionName>`
5. Vous pouvez désormais effectuer les configurations requises comme un NetScaler non partitionné.

Pour accéder à une partition d'administration à l'aide de l'interface graphique

1. Ouvrez une session sur l'appliance NetScaler.
2. Vérifiez si vous vous trouvez dans la bonne partition. La barre supérieure de l'interface graphique affiche le nom de la partition actuellement sélectionnée.
   - Si oui, passez à l'étape suivante.
   - Si ce n'est pas le cas, accédez à **Configuration > Système > Administration des partitions > Partitions**, cliquez avec le bouton droit sur la partition vers laquelle vous souhaitez basculer, puis sélectionnez **Commuter**.
3. Vous pouvez désormais effectuer les configurations requises comme un NetScaler non partitionné.

Ajouter une partition d'administration

L'administrateur racine ajoute une partition administrative à partir de la partition par défaut et lie la partition au VLAN 2.

Pour créer une partition administrative à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add partition <partitionname>
```

Basculer l'accès utilisateur de la partition par défaut vers une partition d'administration

Vous pouvez maintenant passer de l'accès utilisateur de la partition par défaut à la partition Par1.

Pour faire passer un compte utilisateur d'une partition par défaut à une partition d'administration à l'aide de l'interface de ligne de commande, procédez comme suit :

À l'invite de commande, tapez :

```
Switch ns partition <pname>
```

Ajout d'une adresse SNIP à un compte d'utilisateur de partition avec l'accès à la gestion activé

Dans la partition, créez une adresse SNIP avec l'accès de gestion activé.

Pour ajouter l'adresse SNIP au compte utilisateur de la partition avec l'accès de gestion activé à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
> add ns ip <ip address> <subnet mask> -mgmtAccess enabled
```

Création et liaison d'un utilisateur de partition à l'aide d'une politique de commande de partition

Dans partition, créez un utilisateur du système de partition et associez-le à l'aide des politiques de commande partition-admin.

Pour créer et lier un utilisateur du système de partition à une politique de commande de partition à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
> add system user <username> <password>

Done
```


Création et liaison d'un groupe d'utilisateurs de partition avec la politique de commande de partition

Dans Partition Par1, créez un groupe d'utilisateurs du système de partition et associez-le à une politique de commande de partition telle que partition admin, partition read-only, partition-operator ou partition-network.

Pour créer et lier un groupe d'utilisateurs de partition avec la stratégie de commande de partition à l'aide de l'interface de ligne de commande :

```
1 > add system group <groupName>
2 > bind system group <groupname> (-userName | -policyName <cmdpolicy> <
     priority> | -partitionName)
```

Configuration de l'authentification du serveur externe pour les utilisateurs externes

Dans la partition Par1, vous pouvez configurer une authentification de serveur externe pour authentifier les utilisateurs TACACS externes accédant à la partition via une adresse SNIP.

Pour configurer l'authentification du serveur externe pour les utilisateurs externes à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
1 > add authentication tacacsaction <name> -serverip <IP> -tacacsSecret <
     secret key> -authorization ON -accounting ON
2 > add authentication policy <policname> -rule true -action <name>
3 > bind system global <policyname> -priority <value>1
```

Configurer un compte utilisateur du système de partition dans une partition à l'aide de l'interface graphique

Pour configurer un compte utilisateur de partition dans une partition administrative, vous devez créer un utilisateur de partition ou un groupe d'utilisateurs de partition et le lier aux politiques de commande de partition. Vous pouvez également configurer l'authentification du serveur externe pour un utilisateur externe.

Pour créer un compte utilisateur de partition dans une partition à l'aide de l'interface graphique

Accédez à **Système > Administration**des utilisateurs, cliquez sur **Utilisateurs** pour ajouter un utilisateur du système de partition et lier l'utilisateur aux politiques de commande (partitionadmin/partitionread-only/partition-operator/partition-network).

Pour créer un compte de groupe d'utilisateurs de partition dans une partition à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs**, cliquez sur **Groupes** pour ajouter un groupe d'utilisateurs du système de partition et lier le groupe d'utilisateurs aux politiques de commande (partitionadmin/partitionread-only/partition-operator/partition-network).

Pour configurer l'authentification du serveur externe pour les utilisateurs externes à l'aide de l'interface graphique

Accédez à **Système > Authentification > Actions de base** et cliquez sur **TACACS** pour configurer un serveur TACACS afin d'authentifier les utilisateurs externes accédant à la partition.

Exemple de configuration

La configuration suivante montre comment créer un utilisateur de partition ou un groupe d'utilisateurs de partition et le lier à des politiques de commande de partition. De plus, comment configurer l'authentification du serveur externe pour l'authentification d'un utilisateur externe.

```
1  > add partition Par1
2  > switch ns partition Par1
3  > add ns ip 10.102.29.203 255.255.255.0 -mgmtAccessenabled
4  > add system user John Password
5  > bind system user Jane partition-read-only -priority 1
6  > add system group Retail
7  > bind system group Retail -policyname partition-network 1 (where 1 is
     the priority number)
8  > bind system group Retail  - username Jane
9  > add authentication tacacssaction tacuser  - serverip 10.102.29.200  -
     tacacsSecret Password  - authorization ON  - accounting ON
10 > add authentication policy polname  - rule true  - action tacacsAction
11 > bind system global polname  - priority 1
```

Stratégies de commande pour les utilisateurs de partition et les groupes d'utilisateurs de partition dans la partition d'administration

Commandes pour autoriser un compte utilisateur dans la partition administrative	Politiques de commande disponibles dans une partition administrative (politiques intégrées)	Type d'accès au compte utilisateur
ajouter un utilisateur au système	Administrateur de partitions	SNIP (avec accès de gestion activé)
ajouter un groupe de systèmes	Réseau de partitions	SNIP (avec accès de gestion activé)
ajouter une authentification `<action, policy>`, lier le système global `<policy name>`	Partition en lecture seule	SNIP (avec accès de gestion activé)
supprimer un utilisateur du système	Administrateur de partitions	SNIP (avec accès de gestion activé)
supprimer un groupe de systèmes	Administrateur de partitions	SNIP (avec accès de gestion activé)
`bind system cmdpolicy` à l'utilisateur du système ; `bind system cmdpolicy` au groupe de systèmes	Administrateur de partitions	SNIP (avec accès de gestion activé)

Configurer un canal Ethernet LACP sur la partition d'administration par défaut

Avec le protocole LACP (Link Aggregation Control Protocol), vous pouvez combiner plusieurs ports en une seule liaison haut débit (également appelée canal). Une appliance compatible LACP échange des unités de données LACP (LACPDU) sur le canal.

Il existe trois modes de configuration LACP que vous pouvez activer dans la partition par défaut d'une appliance NetScaler :

1. Actif. Un port en mode actif envoie des LACPDU. L'agrégation de liens est formée si l'autre extrémité de la liaison Ethernet est en mode LACP actif ou passif.
2. Passif. Un port en mode passif envoie des LACPDU uniquement lorsqu'il reçoit des LACPDU. L'agrégation de liens est formée si l'autre extrémité de la liaison Ethernet est en mode actif LACP.
3. Désactiver. L'agrégation de liens n'est pas créée.

> **Remarque**
>
> Par défaut, l'agrégation de liens est désactivée dans la partition par défaut de l'appliance.

Le LACP échange le LACPDU entre les appareils connectés par une liaison Ethernet. Ces appareils sont

généralement appelés acteurs ou partenaires.

Une unité de données LACPDU contient les paramètres suivants :

- Mode LACP. Actif, passif ou désactivé.
- Délai d'expiration du LACP. La période d'attente avant la fin du temps imparti au partenaire ou à l'acteur. Valeurs possibles : long et court. Par défaut : Long.
- Clé de port. Pour distinguer les différents canaux. Lorsque la clé vaut 1, LA/1 est créé. Lorsque la clé est 2, LA/2 est créé. Valeurs possibles : entier compris entre 1 et 8. 4 à 8 correspond au cluster CLAG.
- Priorité du port. Valeur minimale : 1. Valeur maximale : 65535. Valeur par défaut : 32768.
- Priorité du système. Utilise cette priorité avec le MAC du système pour former l'ID du système afin d'identifier de manière unique le système lors de la négociation LACP avec le partenaire. Définit la priorité du système entre 1 et 65535. La valeur par défaut est fixée à 32768.
- Interface. Prend en charge 8 interfaces par canal sur l'appliance NetScaler 10.1 et prend en charge 16 interfaces par canal sur les appliances NetScaler 10.5 et 11.0.

Après avoir échangé des LACPDU, l'acteur et le partenaire négocient les paramètres et décident d'ajouter ou non les ports à l'agrégation.

Configurer et vérifier le LACP

La section suivante explique comment configurer et vérifier le LACP dans la partition d'administration.

Pour configurer et vérifier le LACP sur une appliance NetScaler à l'aide de l'interface de ligne de commande

1. Activez LACP sur chaque interface.

   ```
   set interface <Interface_ID> -lacpMode PASSIVE -lacpKey 1<!--NeedCopy
   -->
   ```

   Lorsque vous activez le LACP sur une interface, les canaux sont créés dynamiquement. De plus, lorsque vous activez LACP sur une interface et que vous définissez LACPKey sur 1, l'interface est automatiquement liée au canal LA/1.

   > **Remarque**
   >
   > Lorsque vous liez une interface à un canal, les paramètres du canal ont priorité sur les paramètres de l'interface, de sorte que les paramètres d'interface sont ignorés. Si un canal est créé dynamiquement par LACP, vous ne pouvez pas effectuer les opérations d'ajout, de liaison, de dissociation ou de suppression sur le canal. Un canal créé dynamiquement par LACP est automatiquement supprimé lorsque vous désactivez le LACP sur toutes les interfaces du canal.

2. Définissez la priorité du système.

   ```
   set lacp -sysPriority <Positive_Integer><!--NeedCopy-->
   ```

3. Vérifiez que le LACP fonctionne comme prévu.

   “‘show interface

   ```
   ```show channel<!--NeedCopy-->
   ```

   ```
   show LACP<!--NeedCopy-->
   ```

   > **Remarque**
   >
   > Dans certaines versions du système d’exploitation interréseau Cisco (iOS), l’exécution de la <VLAN_ID>commande VLAN native switchport trunk amène le commutateur Cisco à étiqueter les PDU LACP. Cela entraîne la défaillance du canal LACP entre le commutateur Cisco et l’appliance NetScaler. Toutefois, ce problème n’affecte pas les canaux d’agrégation de liens statiques configurés dans la procédure précédente.

Enregistrer la configuration de toutes les partitions d’administration à partir de la partition par défaut

Les administrateurs peuvent enregistrer la configuration de toutes les partitions d’administration à la fois à partir de la partition par défaut.

Enregistrez toutes les partitions d’administration à partir de la partition par défaut à l’aide de l’interface de ligne de commande

À l’invite de commande, tapez :

```
save ns config -all
```

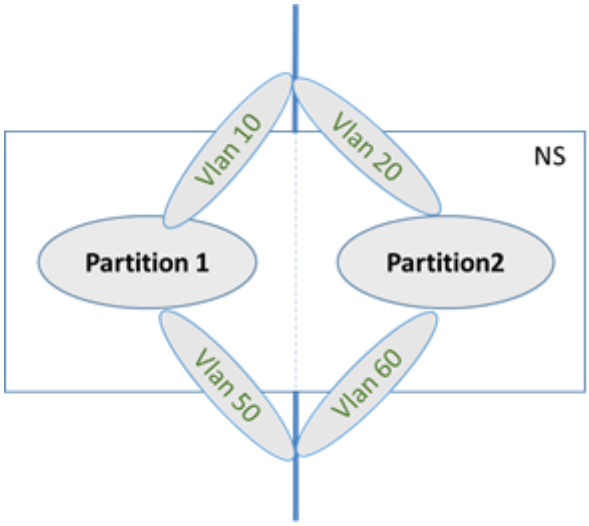
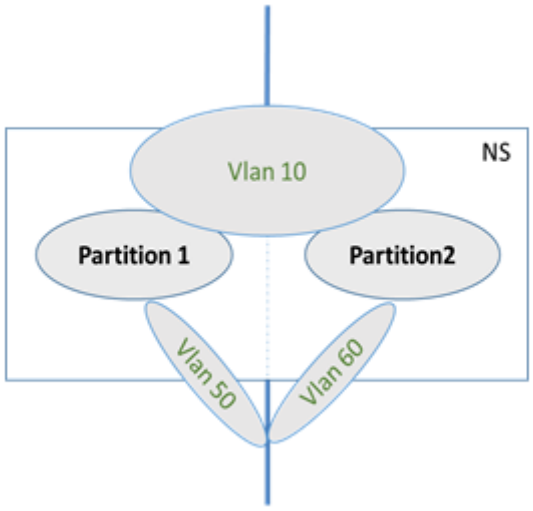
Prise en charge des rapports personnalisés basés sur des partitions et des clusters

L’interface graphique de NetScaler affiche uniquement les rapports personnalisés créés dans la partition d’affichage actuelle ou dans le cluster.

Auparavant, l’interface graphique de NetScaler stockait les noms des rapports personnalisés directement dans le fichier principal sans mentionner le nom de la partition ou du cluster pour les différencier.

Pour afficher les rapports personnalisés de la partition ou du cluster actuel dans l’interface graphique

- Accédez à l’onglet **Rapports** .


```

- Cliquez sur **Rapports personnalisés** pour afficher les rapports créés dans la partition actuelle ou dans le cluster.

### Prise en charge de la liaison des certificats mondiaux VPN dans une configuration partitionnée pour OAuth IdP

Dans une configuration partitionnée, vous pouvez désormais lier les certificats au VPN global pour les déploiements OAuth IdP.

#### Pour lier les certificats dans une configuration partitionnée à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind vpn global [-certkeyName <string>] [-userDataEncryptionKey <string
    >]
```

Configuration VLAN pour les partitions d'administration

May 5, 2023

Les VLAN peuvent être liés à une partition en tant que VLAN « dédié » ou VLAN « partagé ». En fonction de votre déploiement, vous pouvez lier un VLAN à une partition pour isoler son trafic réseau des autres partitions.

VLAN dédié — Un VLAN lié à une seule partition avec l'option « Partage » désactivée et doit être un VLAN balisé. Par exemple, dans un déploiement client-serveur, pour des raisons de sécurité, un administrateur système crée un VLAN dédié pour chaque partition côté serveur.

VLAN partagé : VLAN lié (partagé entre) à plusieurs partitions avec l'option « Partage » activée. Par exemple, dans un déploiement client-serveur, si l'administrateur système n'a pas le contrôle sur le réseau côté client, un VLAN est créé et partagé sur plusieurs partitions.

Le VLAN partagé peut être utilisé sur plusieurs partitions. Il est créé dans la partition par défaut et vous pouvez lier un VLAN partagé à plusieurs partitions. Par défaut, un VLAN partagé est implicitement lié à la partition par défaut et ne peut donc pas être lié explicitement.

> **Remarques**
>
> - Une appliance NetScaler déployée sur n'importe quelle plate-forme d'hyperviseur (ESX, KVM, Xen et Hyper-V) doit respecter les conditions suivantes dans la configuration d'une partition et dans le domaine de trafic :

  - Enable the promiscuous mode, MAC changes, MAC spoofing, or forged transmit for shared VLANs with partition.
  - Enable the VLAN with port group properties of the virtual switch, if the traffic is through a dedicated VLAN.
- Dans une appliance NetScaler partitionnée (multitenant), un administrateur système peut isoler le trafic circulant vers une ou plusieurs partitions particulières. Cela se fait en liant un ou plusieurs VLAN à chaque partition. Un VLAN peut être dédié à une partition ou partagé sur plusieurs partitions.
- Le routage interne entre des partitions hébergées sur la même appliance NetScaler n'est pas pris en charge.

VLAN dédiés

Pour isoler le trafic entrant dans une partition, créez un VLAN et associez-le à la partition. Le VLAN n'est alors visible que par la partition associée, et le trafic passant par le VLAN est classé et traité uniquement dans la partition associée.



Pour implémenter un VLAN dédié pour une partition particulière, procédez comme suit.

1. Ajoutez un VLAN (V1).
2. Liez une interface réseau au VLAN en tant qu'interface réseau balisée.
3. Créez une partition (P1).
4. Liez la partition (P1) au VLAN dédié (V1).

Configurez les éléments suivants à l'aide de la CLI

- Créer un VLAN


```
add vlan <id>
```

Exemple

```
1     add vlan 100
```

- Lier un VLAN

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple

```
1     bind vlan 100  - ifnum 1/8 -tagged
```

- Créer une partition

```
Add ns partition <partition name> [-maxBandwidth <positive_integer>][-
maxConn <positive_integer>] [-maxMemLimit <positive_integer>]
```

Exemple

```
1     Add ns partition P1  - maxBandwidth 200  - maxconn 50  - maxmemlimit
         90
2
3     Done
```

- Lier une partition à un VLAN

```
bind partition <partition-id> -vlan <id>
```

Exemple

```
1     bind partition P1  - vlan 100
```

Configurer un VLAN dédié à l'aide de l'interface graphique NetScaler

1. Accédez à **Configuration > Système > Réseau**VLAN* et cliquez sur **Ajouter** pour créer un VLAN.
2. Sur la page **Créer un VLAN**, définissez les paramètres suivants :
   - ID DE VLAN
   - Nom de l'alias
   - Unité de transmission maximale
   - Routage dynamique
   - Routage dynamique IPv6
   - Partage de partitions

3. Dans la section **Liaisons d'interface**, sélectionnez une ou plusieurs interfaces et liez-les au VLAN.
4. Dans la section **Liaisons IP**, sélectionnez une ou plusieurs adresses IP et liez le VLAN.
5. Cliquez sur **OK** et **Terminé**.

VLAN partagé

Dans une configuration de VLAN partagé, chaque partition possède une adresse MAC, et le trafic reçu sur le VLAN partagé est classé par adresse MAC. Seul un VLAN de couche 3 est recommandé car il peut restreindre le trafic de sous-réseau. Une adresse MAC de partition est applicable et importante uniquement pour un déploiement de VLAN partagé.

> **Remarque**
>
> À partir de NetScaler version 12.1 build 51.16, le VLAN partagé dans une appliance partitionnée prend en charge le protocole de routage dynamique.

Le diagramme suivant montre comment un VLAN (VLAN 10) est partagé entre deux partitions.



Pour déployer une configuration de VLAN partagé, procédez comme suit :

1. Créez un VLAN avec l'option de partage « activée » ou activez l'option de partage sur un VLAN existant. Par défaut, l'option est « désactivée ».
2. Liez l'interface de partition au VLAN partagé.
3. Créez les partitions, chacune avec sa propre adresse PartitionMac.
4. Liez les partitions au VLAN partagé.

Configurer un VLAN partagé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour ajouter un VLAN ou définir le paramètre de partage d'un VLAN existant :

```
add vlan <id> [-sharing (ENABLED | DISABLED)]

set vlan <id> [-sharing (ENABLED | DISABLED)]

add vlan 100  - sharing ENABLED

set vlan 100  - sharing ENABLED
```

Liez une partition à un VLAN partagé à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind partition <partition-id> -vlan <id>

bind partition P1  - vlan 100

add ns partition P1  - maxBandwidth 200  - maxconn 50    - maxmemlimit 90
   -partitionMAC<mac_addr

Done
```

Configurer une adresse MAC de partition à l'aide de l'interface de ligne de commande

```
set ns partition <partition name> [-partitionMAC<mac_addr>]

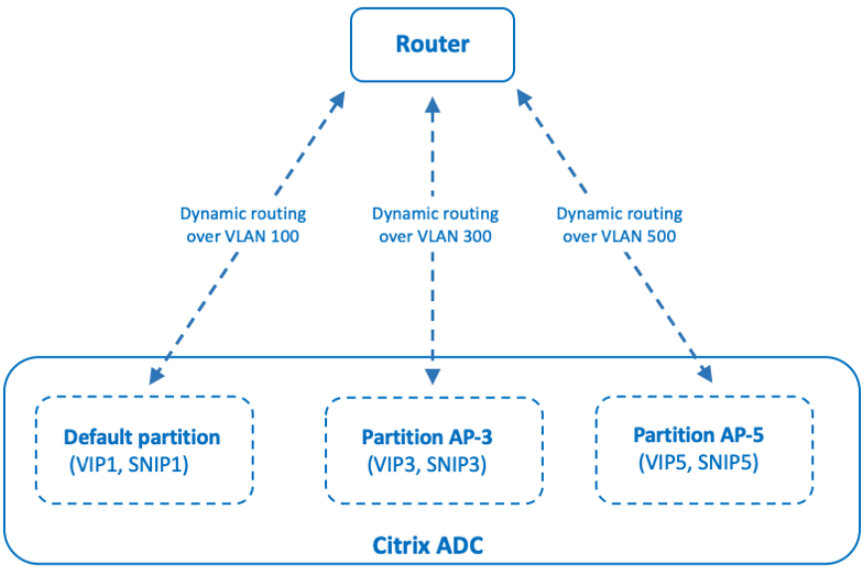
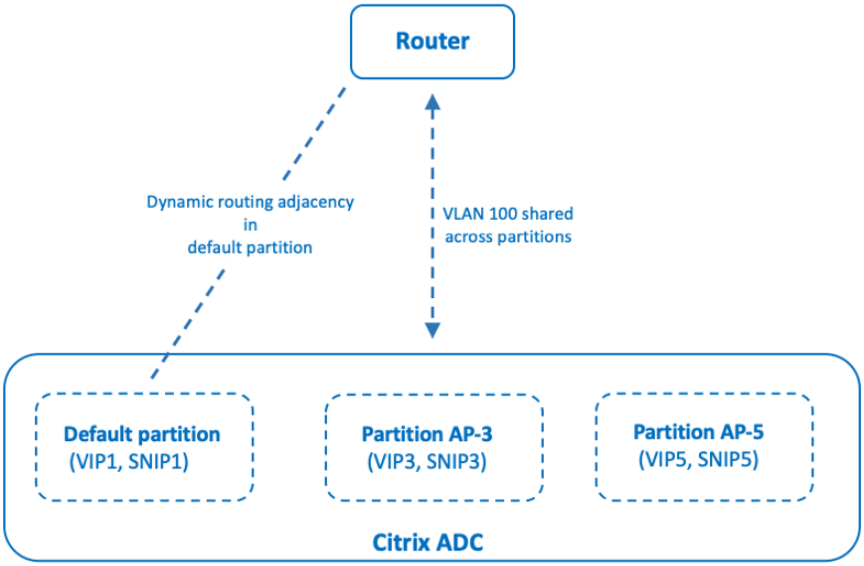
set ns partition P1  - partitionMAC 22:33:44:55:66:77
```

Lier des partitions à un VLAN partagé à l'aide de l'interface de ligne de commande

```
bind partition <partition-id> -vlan <id>

bind partition <partition-id> -vlan <id>

bind partition P1  - vlan 100

bind partition P2  - vlan 100

```



```
bind partition P3 -vlan 100

bind partition P4 -vlan 100
```

Configurer un VLAN partagé à l'aide de l'interface graphique NetScaler

1. Accédez à **Configuration > Système > Réseau > VLAN**, puis sélectionnez un profil **VLAN** et cliquez sur **Modifier** pour définir le paramètre de partage de partition.
2. Sur la page **Créer un VLAN**, cochez la case **Partage des partitions** .
3. Cliquez sur **OK**, puis sur **Terminé**.

Routage dynamique sur un VLAN partagé entre les partitions d'administration

Les partitions d'administration d'une appliance NetScaler permettent d'héberger plusieurs locataires.

À partir de NetScaler version 12.1 build 51.16, un VLAN partagé dans une appliance partitionnée prend en charge le protocole de routage dynamique. Le routage peut être configuré dans des VLAN dédiés ou partagés associés aux partitions d'administration.

VLAN dédié d'une partition d'administration. Dans un VLAN dédié, le chemin de données du locataire est identifié à l'aide d'un ou de plusieurs VLAN. Il en résulte une configuration stricte et une isolation des chemins de données pour le locataire. Pour annoncer la santé d'une adresse VIP, le routage dynamique est activé dans chaque partition et la contiguïté de routage est établie par partition.



Dynamic routing over a dedicated VLAN per partition

Un VLAN partagé entre les partitions d'administration. Dans un VLAN partagé, les adresses VIP configurées dans une partition autre que celle par défaut peuvent être publiées via une seule adjacence ou un appairage formé dans la partition par défaut. Une adresse SNIP dans la partition autre que celle par défaut est utilisée comme saut suivant pour toutes les adresses VIP (configurées avec l'option **AdvertiseOnDefaultPartition) de cette partition** autre que celle par défaut. L'adresse SNIP configurée est marquée comme adresse IP de saut suivant dans les annonces de routage.

Prenons un exemple de configuration de partitions d'administration dans une appliance NetScaler. Le VLAN 100 est partagé entre la partition par défaut et les partitions non par défaut : AP-3 et AP-5. Adresses SNIP SNIP1 est ajouté dans la partition par défaut, SNIP3 est ajouté dans AP-3 et SNIP5 est ajouté dans AP-5. SNIP1, SNIP3 et SNIP5 sont accessibles via le vlan-100. Les adresses VIP VIP1 sont ajoutées dans la partition par défaut, VIP3 dans AP-3 et VIP5 dans AP-5. VIP3 et VIP5 sont annoncés via l'adjacence ou l'appairage unique formé dans la partition par défaut.



Dynamic routing over a shared VLAN across partitions

Avant de commencer

Avant de configurer le routage dynamique sur un VLAN partagé dans une partition d'administration autre que celle par défaut, assurez-vous que :

- Le**routage dynamique est configuré sur le VLAN partagé dans la partition par défaut**. La configuration du routage dynamique sur le VLAN partagé dans la partition par défaut comprend les étapes suivantes :
  1. Activez le routage dynamique sur le VLAN partagé.
  2. Ajoutez une adresse IP SNIP avec le routage dynamique activé. Cette adresse IP SNIP est utilisée pour le routage dynamique avec l'amont.

3. Liez le sous-réseau IP SNIP au VLAN partagé.

- **Un ou plusieurs protocoles de routage dynamique sont configurés sur la partition par défaut**. Pour plus d'informations, voir Configurer les protocoles de routage dynamique.

Étapes de configuration

La configuration du routage dynamique sur un VLAN partagé dans une partition d'administration autre que celle par défaut comprend les étapes suivantes :

1. **Ajoutez une adresse IP SNIP dans la partition autre que celle par défaut**. Cette adresse IP SNIP doit se trouver dans le même sous-réseau de l'adresse IP SNIP utilisée pour le routage dynamique dans la partition par défaut.
2. **Définissez ou activez les paramètres suivants pour la publication d'une adresse VIP, dans une partition autre que celle par défaut, à l'aide du routage dynamique**.
   - Passerelle de route hôte (HostrTGW). Définissez ce paramètre sur l'adresse SNIP ajoutée à l'étape précédente.
   - Publicité sur la partition par défaut (AdvertiseOnDefaultPartition). Activez ce paramètre.

Exemple de configuration

Prenons un exemple de configuration d'une partition d'administration dans une appliance NetScaler. Une partition d'administration AP-3 autre que celle par défaut est configurée sur cette appliance. Un VLAN VLAN100 partagé est lié à AP-3. L'exemple de configuration suivant configure le routage dynamique, via VLAN100, dans AP-3.

Étapes	Exemple de configuration
Sur la partition d'administration par défaut	-
Activer le routage dynamique sur VLAN 100 partagé.	`set vlan 100 -dynamicRouting enabled`
Ajoutez l'adresse IP SNIP 192.0.2.10 avec le routage dynamique activé.Cette adresse IP SNIP est utilisée pour le routage dynamique avec l'amont.	`add ns ip 192.0.2.10 255.255.255.0 -type SNIP -dynamicRouting enabled`
Liez le sous-réseau 192.0.2.10 au VLAN 100 partagé.	`bind vlan 100 -IPAddress 192.0.2.10 255.255.255.0`
Sur la partition d'administration non par défaut AP-3	-

Étapes	Exemple de configuration
Ajouter l'adresse IP SNIP 192.0.2.30. Cette adresse IP SNIP se trouve dans le même sous-réseau que l'adresse IP SNIP 192.0.2.10 sur la partition par défaut.	`add ns ip 192.0.2.30 255.255.255.0 -type SNIP`
Pour la publicité de l'adresse VIP 203.0.113.300 utilisant le routage dynamique, activez le `advertiseOnDefaultPartition` paramètre et définissez le `hostRtGw`paramètre sur 192.0.2.30.	`set ns ip 203.0.113.300 255.255.255.255 -hostRoute enabled -advertiseOnDefaultPartition enabled -hostRtGw 192.0.2.30`

Routage dynamique d'IPv6 sur un VLAN partagé sur une partition d'administration

Les `set L3Param -ipv6DynamicRouting ENABLED` commandes `enable ns feature IPv6PT` et doivent être activées pour qu'une adresse IPv6 puisse router dynamiquement sur un VLAN partagé dans une partition d'administration. Les exemples de configurations suivants vous aident à configurer le routage dynamique d'IPv6 sur VLAN partagé.

Exemple de configuration

L'exemple de configuration suivant configure le routage dynamique, via le VLAN 100, dans AP-3.

Étapes	Exemple de configuration
Sur la partition d'administration par défaut	-
Activer le routage dynamique sur VLAN 100 partagé.	`set vlan 100 -dynamicRouting enabled`
Ajoutez l'adresse IP SNIP 2001:b:c:d 1/64 avec le routage dynamique activé. L'adresse IP SNIP est utilisée pour le routage dynamique avec l'amont.	`add ns ip6 2001:b:c:d::1/64 -type SNIP -dynamicRouting enabled`
Liez le sous-réseau 2001 : b:c:d 1/64 au VLAN 100 partagé.	`bind vlan 100 -IPAddress 2001:b:c:d::1/64`
Sur la partition d'administration non par défaut AP-3	-

Étapes	Exemple de configuration
Ajoutez l'adresse IP SNIP 2001:b:c:d 2/64. Cette adresse IP SNIP se trouve dans le même sous-réseau que l'adresse IP SNIP 2001:b:c:d 2/64 sur la partition par défaut.	`add ns ip6 2001:b:c:d::2/64 -type SNIP`
Pour la publicité de l'adresse VIP 2002 1/128 en utilisant le routage dynamique, activez le `advertiseOnDefaultPartition` paramètre et définissez le `ip6hostRtGw`paramètre sur 2001:b:c:d 2.	`set ns ip6 2002::1/128 -hostRoute enabled -advertiseOnDefaultPartition enabled -ip6hostRtGw 2001:b:c:d::2`

Le VIP présent dans la partition d'administration doit être vu sur VTYSH de la partition par défaut comme une route du noyau.

```
> switch partition default
Done

>vtysh
ns#

ns# sh ipv6 route kernel

IPv6 routing table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
   IA - OSPF inter area, E1 - OSPF external type 1,
   E2 - OSPF external type 2, I - IS-IS, B - BGP
Timers: Uptime

K      2002::1/128 via 2001:b:c:d::2, vlan0, 01:24:15
                                >> on Default Partition, VIP : 2002::1
    present in AP known via SNIP6 : 2001:b:c:d::2 is present in AP as a
    Kernel Route
```

Il peut être annoncé en amont en utilisant l'option « redistribuer le noyau » sous OSPFV3/BGP+ dans la partition par défaut.

```
ns# sh run router ipv6 ospf
!
router ipv6 ospf 1
redistribute kernel
!
```


VLAN partagé avec partition d'administration sur l'appliance NetScaler SDX

Sur une appliance SDX, vous devez générer et configurer l'adresse PMAC à l'aide de l'interface utilisateur du service de gestion, avant d'utiliser les partitions d'administration avec des VLAN partagés. Le service de gestion vous permet de générer des adresses MAC de partition en :

- Utilisation d'une adresse MAC de base
- Spécification d'adresses MAC personnalisées
- Adresses MAC générées aléatoirement

> **Remarques**
>
> - Les adresses MAC générées aléatoirement sont utilisées pour d'autres déploiements autres que la haute disponibilité.
> - Après avoir généré les adresses MAC des partitions, vous devez redémarrer l'instance NetScaler avant de configurer les partitions d'administration. Pour plus d'informations sur la génération d'adresses MAC de partition à partir de l'appliance SDX, consultez la section Génération d'adresses MAC de partition pour configurer la partition d'administration sur une instance NetScaler de l'appliance SDX.

Prise en charge de VXLAN pour les partitions d'administration

May 5, 2023

Dans une appliance NetScaler partitionnée, comme pour configurer un VLAN, vous pouvez configurer un VXLAN dans la partition par défaut. Après avoir configuré un VXLAN, vous pouvez le lier à une partition administrative ou, si un VXLAN étend un VLAN lié à une partition, l'appliance lie le VXLAN à la partition sous le même domaine de diffusion. Il est applicable pour dissocier un VLAN qui dissocie un VXLAN de la partition.

Pour plus d'informations sur le fonctionnement du VXLAN dans un dispositif NetScaler, consultez la section VXLAN.

Pour plus d'informations sur le fonctionnement du VLAN dans une appliance NetScaler partitionnée, consultez Partitionnement par administration.

Points à retenir avant de configurer un VXLAN

N'oubliez pas les points suivants avant de configurer un VXLAN dans une appliance NetScaler partitionnée :

- Lorsque vous étendez un VLAN sur un VXLAN, assurez-vous que le VLAN est lié à la partition.

- Seul un administrateur de partition doit configurer l'adresse IP et le routage dynamique du VXAN dans la partition administrative.

Un VXLAN partagé n'est pas pris en charge dans une appliance partitionnée. Par conséquent, un VXLAN ne peut pas être balisé sur un VLAN partagé ou vous ne pouvez pas faire d'un VLAN un VLAN partagé lorsqu'il est balisé sur un VXLAN.

Configurations VXLAN compatibles

Vous trouverez ci-dessous les configurations VXLAN compatibles.

Extension d'un VLAN sur un VXLAN dans le même domaine de diffusion

Les étapes suivantes de l'interface de ligne de commande vous aident à étendre un VLAN sur un VXLAN et inversement au sein du même domaine de diffusion.

1. Ajouter un VLAN dans la partition par défaut

```
1  add vlan <id>
```

2. Étendre le VLAN sur un VXLAN dans le même domaine de diffusion.

```
1 add vxlan <vxlan id>  - vlan <id>
```

3. Configurez un homologue `vtep` pour transporter tout le trafic BUM (diffusion inconnue de multidiffusion).

> **Remarque**
>
> L' adresse `vtep` peut être une adresse de multidiffusion.

```
1 add bridgetable -mac <mac_addr> -vxlan <positive_integer> -vtep <
     ip_addr> [-vni <positive_integer>][-deviceVlan <
     positive_integer>]
```

4. Liez les adresses IP au VXLAN.

```
1 bind vxlan <id> [-srcIP <ip_addr>][-IPAddress <ip_addr|ipv6_addr
     |*> [<netmask>]]
```

5. Liez un VLAN à une partition administrative.

```
1 bind partition <partition-id> -vxlan <id>
2
3 add vlan 3000
4
```



```
add vxlan 3000  -vlan 10

add bridgetable  -mac 00:00:00:00:00:00  -vxlan 3000 -vtep
    10.102.58.8  -vni 11

bind vxlan 3000  -  srcIP 10.102.101.15

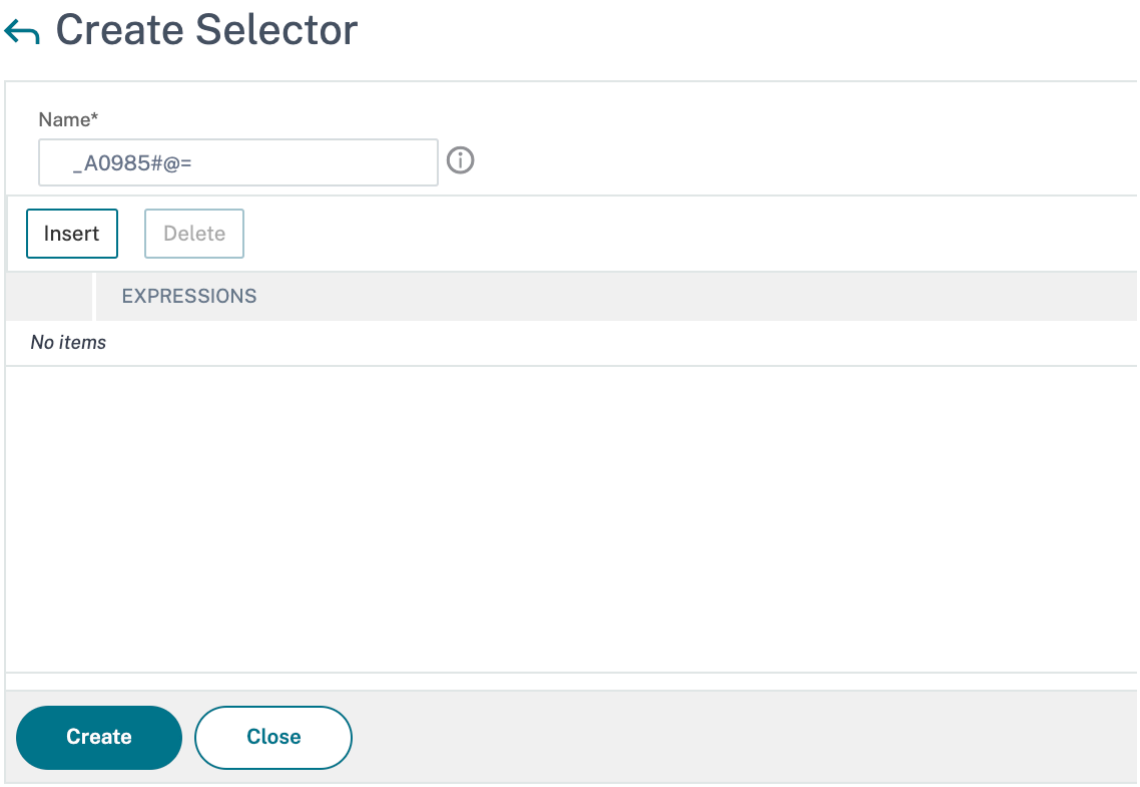
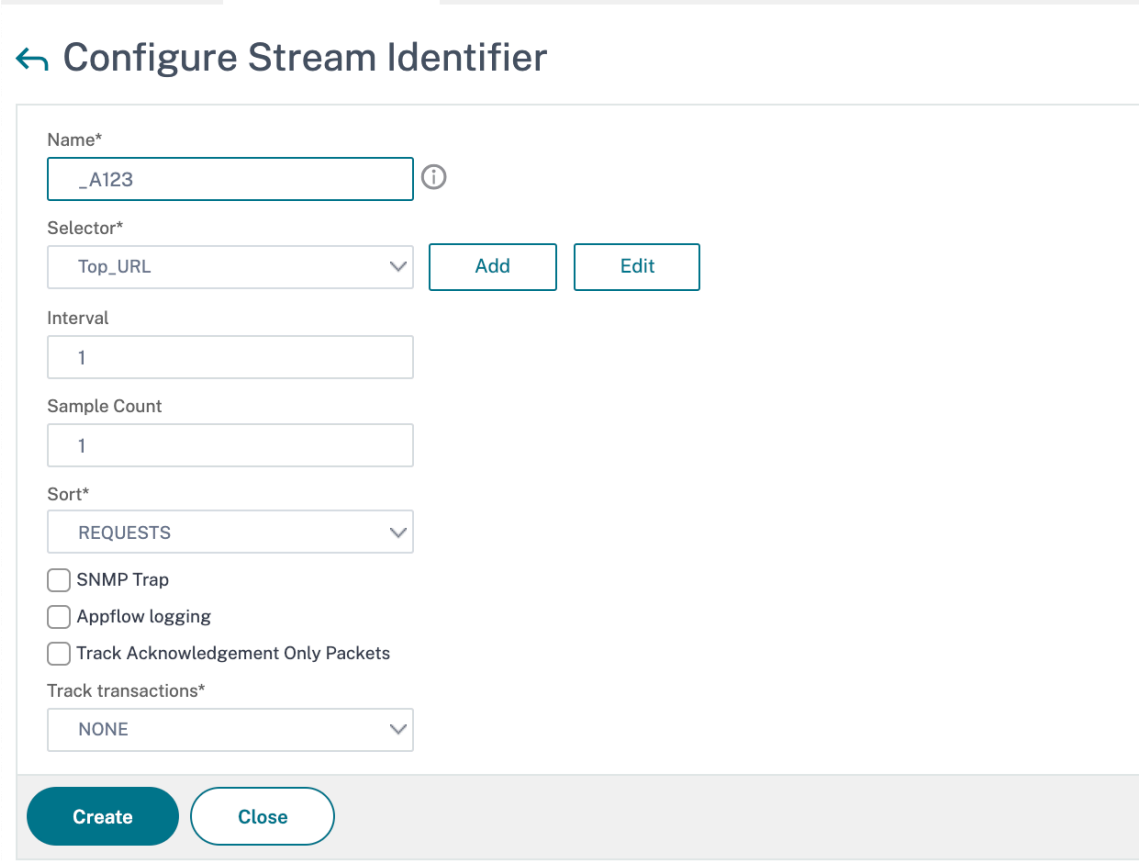
bind partition p1  -vlan 10
```

Prise en charge SNMP des partitions d'administration

May 5, 2023

Une appliance NetScaler partitionnée utilise l'infrastructure SNMP pour limiter le débit de partition et surveiller les détails d'utilisation des ressources de partition.

Interruptions SNMP pour limiter le débit de partition des administrateurs

Sur une appliance NetScaler partitionnée, une alarme PARTITION-RATE-LIMIT peut générer neuf interruptions SNMP pour signaler qu'une ressource de partition (telle que la bande passante, la connexion ou la mémoire) a atteint sa limite ou est revenue à la normale.

Les neuf interruptions SNMP suivantes sont générées lorsque :

- Le**seuil de partition**a été atteint. Le nombre de connexions actives pour une partition dépasse son pourcentage de seuil élevé.
- **PartitionConnThresholdNormal.** Le nombre de connexions actives est inférieur ou égal au pourcentage de seuil normal.
- Le**seuil de partition BW a été atteint.** L'utilisation de la bande passante de la partition atteint son seuil élevé en pourcentage.
- Le**seuil de partitionMemThreshold a été atteint.** L'utilisation actuelle de la mémoire de la partition dépasse son pourcentage de seuil élevé.
- **Partition MemThresholdNormal.** L'utilisation actuelle de la mémoire de la partition devient inférieure ou égale au pourcentage de seuil normal.
- **La limite de mémoire de partition a été dépassée.** L'utilisation actuelle de la mémoire de la partition dépasse son pourcentage de limite de mémoire.
- La**limite de partition Conn**a été dépassée. Le nombre de connexions actives pour une partition dépasse la limite configurée et de nouvelles connexions sont abandonnées.
- **PartitionConnLimitNormal.** Le nombre de connexions actives pour une partition est inférieur à la limite configurée et la partition peut désormais accepter une nouvelle connexion.

- La**limite BW de la partition**a été dépassée. L'utilisation actuelle de la bande passante d'une partition a dépassé la limite configurée.

Les valeurs de seuil pour les interruptions SNMP ne sont pas configurables et sont les suivantes :

- Seuil élevé = 80 % (applicable à tous les pièges à limite de débit de partage)
- Seuil bas = 60 % (applicable à tous les pièges à limite de débit de partage)
- Limite de mémoire = 95 % (applicable uniquement pour les interruptions de mémoire des partitions)

Configuration de l'alarme PARTITION-RATE-LIMIT

Pour configurer l'alarme PARTITION-RATE-LIMIT dans une partition spécifique et activer la génération des messages d'interruption SNMP.

1. Activer l'alarme PARTITION-RATE-LIMIT
2. Configurer l'alarme PARTITION-RATE-LIMIT
3. Configurer la destination des interruptions SNMP

Pour activer l'alarme PARTITION-RATE-LIMIT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
enable snmp alarm PARTITION-RATE-LIMIT

show snmp alarm PARTITION-RATE-LIMIT
```

Pour configurer l'alarme PARTITION-RATE-LIMIT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set snmp alarm PARTITION-RATE-LIMIT [-state ( ENABLED | DISABLED )] [-
    severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Pour configurer la destination des interruptions SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
add snmp trap <trapClass> <trapDestination> [-version <version>] [-td <
    positive_integer>] [-destPort <port>] [-communityName <string>] [-
    srcIP <ip_addr|ipv6_addr>] [-severity <severity>] [-allPartitions (
    ENABLED | DISABLED )]
```


Pour configurer l'alarme de limite de taux de partitionnement à l'aide de l'interface graphique

Accédez à **Système > SNMP > Alarmes, sélectionnez l'alarmePARTITION-RATE-LIMIT** et configurez les paramètres de l'alarme.

Pour configurer la destination des interruptions SNMP à l'aide de l'interface graphique

Accédez à **Système > SNMP > Trap**, puis spécifiez l'adresse IP du périphérique de destination.

Surveillance SNMP pour l'utilisation des ressources de partition

À l'aide du protocole SNMP, vous pouvez surveiller les détails d'utilisation des ressources d'une partition (telles que la bande passante, la connexion et la mémoire) en temps réel sur une appliance NetScaler. Cela se fait en envoyant une requête SNMP (telle que SNMP GET, SNMP GET BULK, SNMP GETNEXT ou SNMP WALK) depuis le gestionnaire SNMP.

> **Remarque**
>
> Pour surveiller les ressources des partitions, vous devez configurer la communauté SNMP dans la partition par défaut. Dans ce cas, la *PartitionTable* est conservée dans la partition par défaut et la communication SNMP s'effectue via l'adresse NSIP de l'appliance.

Imaginons un scénario dans lequel un administrateur NetScaler souhaite connaître l'utilisation de la bande passante de la partition P1 sur l'appliance. Le gestionnaire SNMP récupère ces informations en envoyant une requête SNMP GET sur l'OID correspondant (PartitionCurrentBandwidth) à l'adresse NSIP de l'appliance. L'agent SNMP sur la partition par défaut récupère et envoie l'utilisation actuelle de la bande passante de P1 au gestionnaire SNMP via l'adresse NSIP.

Le tableau suivant répertorie les compteurs SNMP qui font partie de *PartitionTable* et sa description :

Paramètre SNMP	IDENTIFIANT SNMP	Description
Nom de la partition	1.3.6.1.4.1.5951.4.1.1.88.1.1	Nom de la partition
Bande passante actuelle de la partition	1.3.6.1.4.1.5951.4.1.1.88.1.2	Utilisation actuelle de la bande passante de la partition.
Connexions actuelles de partitionnement	1.3.6.1.4.1.5951.4.1.1.88.1.3	Nombre actuel de connexions actives de la partition.
Utilisation de la mémoire de partition PCNT	1.3.6.1.4.1.5951.4.1.1.88.1.4	Utilisation actuelle de la mémoire (en pourcentage) de la partition.

Prise en charge du journal d'audit des partitions d'administration

May 5, 2023

Sur une appliance NetScaler partitionnée, pour améliorer la sécurité des données, vous pouvez configurer la journalisation des audits dans une partition administrative à l'aide de politiques avancées. Par exemple, vous souhaiterez peut-être consulter les journaux (états et informations d'état) d'une partition spécifique. Plusieurs utilisateurs accèdent à différents ensembles de fonctionnalités en fonction de leurs niveaux d'autorisation dans la partition.

Points à retenir

1. Les journaux d'audit générés à partir de la partition sont stockés dans un fichier journal unique (/var/log/ns.log).
2. Configurez l'adresse de sous-réseau du serveur du journal d'audit (syslog ou ns log) comme adresse IP source dans la partition pour envoyer les messages du journal d'audit.
3. La partition par défaut utilise le NSIP comme adresse IP source pour les messages du journal d'audit par défaut.
4. Vous pouvez afficher le message du journal d'audit à l'aide de la commande « Afficher les messages d'audit ».

Pour plus d'informations sur la configuration du journal d'audit, reportez-vous à la section Configuration du dispositif NetScaler Appliance for Audit Logging.

Configuration de la journalisation des audits dans l'appliance NetScaler partitionnée

Effectuez les tâches suivantes pour configurer la journalisation des audits dans une partition administrative.

1. Configurez l'adresse IP du sous-réseau de partition. Adresse SNIP IPv4 d'une partition administrative.
2. Configurez l'action audit-log (syslog et ns log). Une action d'audit est un ensemble d'informations qui spécifie les messages à enregistrer et la manière de les enregistrer sur le serveur de journalisation externe.
3. Configurez les politiques d'audit (syslog et ns log). Les politiques de journal d'audit définissent les messages de journal pour la partition source vers le serveur Syslog ou ns Log.
4. Liez la politique du journal d'audit à SysGlobal et à l'entité NSGlobal. Liez une politique de journal d'audit à une entité globale du système.
5. Passez en revue les statistiques du journal d'audit. Affichez les statistiques du journal d'audit et évaluez la configuration.

Configurez les éléments suivants à l'aide de la CLI

1. Création de l'adresse IP du sous-réseau d'une partition

   ```
   add ns ip <ip address> <subnet mask>
   ```

2. Création d'une action Syslog

   ```
   add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
    <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )] [-transport ( TCP |
   UDP )]
   ```

3. Création d'une action ns log

   ```
   add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
   <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )]
   ```

4. Création d'un journal d'audit Syslog : politiques

   ```
   add audit syslogpolicy syslog-pol1 true audit-action1
   ```

5. Création d'un journal d'audit et de règles de journal de bord

   ```
   add audit nslogpolicy nslog-pol1 true audit-action1
   ```

6. Lier une politique de journal d'audit à l'entité SyslogGlobal

   ```
   bind audit sysloggglobal -policyName <name> -priority <priority_integer>
    -globalBindType SYSTEM_GLOBAL
   ```

7. Lier une politique de journal d'audit à l'entité NSLogGlobal

   ```
   bind audit nsloggglobal -policyName <name> -priority <priority_integer>
   -globalBindType SYSTEM_GLOBAL
   ```

8. Afficher les statistiques d'un journal d'audit

   ```
   stat audit -detail
   ```

Exemple

```
1 add ns ip 10.102.1.1 255.255.255.0
2 add audit syslogAction syslog_action1 10.102.1.2 -logLevel
     INFORMATIONAL -dateFormat MMDDYYYY -transport UDP
3 add audit syslogpolicy syslog-pol1 true syslog_action1
4 bind audit sysloggglobal -policyName syslog-pol1 -priority 1 -
     globalBindType SYSTEM_GLOBAL
```


Stockage des journaux

Lorsque le serveur SYSLOG ou NSLOG collecte des informations de journal à partir de toutes les partitions, elles sont stockées sous forme de messages de journal dans le fichier ns.log. Les messages du journal contiennent les informations suivantes :

- Nom de la partition.
- L'adresse IP.
- Un horodatage.
- Le type de message
- Les niveaux de journalisation prédéfinis (critique, erreur, notification, avertissement, information, débogage, alerte et urgence)
- Les informations du message.

Afficher les adresses PMAC configurées pour la configuration de VLAN partagé

May 5, 2023

Pour utiliser une configuration de partition avec une configuration VLAN partagée, vous avez besoin d'une adresse MAC virtuelle appelée adresse MAC de partition (PMAC). La partition utilise l'adresse PMAC pour sa communication sur le VLAN partagé. Une adresse PMAC unique est configurée pour chaque partition et elle est utilisée sur tous les VLAN partagés liés à cette partition. Dans le cas d'une plate-forme non SDX (VPX ou MPX), l'adresse PMAC peut être spécifiée par l'utilisateur ou générée en interne par une appliance NetScaler. Si l'adresse PMAC n'est pas spécifiée pour une partition, elle est générée en interne lorsque la partition est liée au premier VLAN partagé. Dans le cas d'une plate-forme SDX, les adresses PMAC doivent toujours être configurées à partir de l'outil SVM, puis attribuées à une partition.

Pour afficher la liste des PMAC configurés, vous pouvez utiliser la commande **Show ns Partition-Mac** . La commande vous permet de vérifier les PMAC configurés via la CLI ou l'interface graphique NetScaler. La commande affiche toutes les adresses PMAC et les partitions correspondantes (si elles sont affectées). Dans le cas d'une plate-forme non SDX, la commande affiche toutes les adresses PMAC et leurs partitions correspondantes car l'adresse PMAC est attribuée à une partition uniquement en fonction des besoins (lorsqu'une partition est liée à un VLAN partagé). Toutefois, dans le cas d'une plate-forme SDX, vous pouvez avoir des PMAC non attribués dans la liste.

Pour plus d'informations sur la façon de générer un PMAC pour la plate-forme SDX, consultez la rubrique Génération d'adresses MAC de partition .

Afficher les PMAC à l'aide de l'interface de ligne de commande NetScaler

À l'invite de commandes, tapez la commande suivante :

```
show ns partitionMAC
```

```
Partition MAC Partition Name

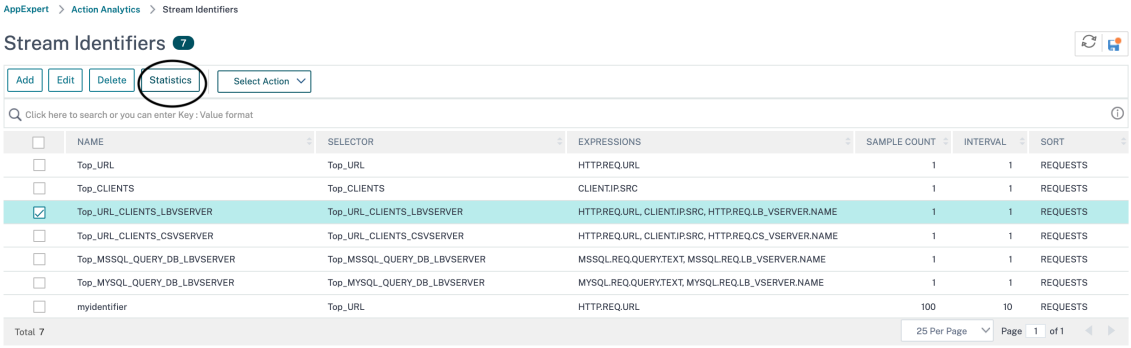
1) f2:0c:64:da:f6:d7

2) b4:0c:43:da:f6:d2

3) a6:e7:b2:6c:48:e0

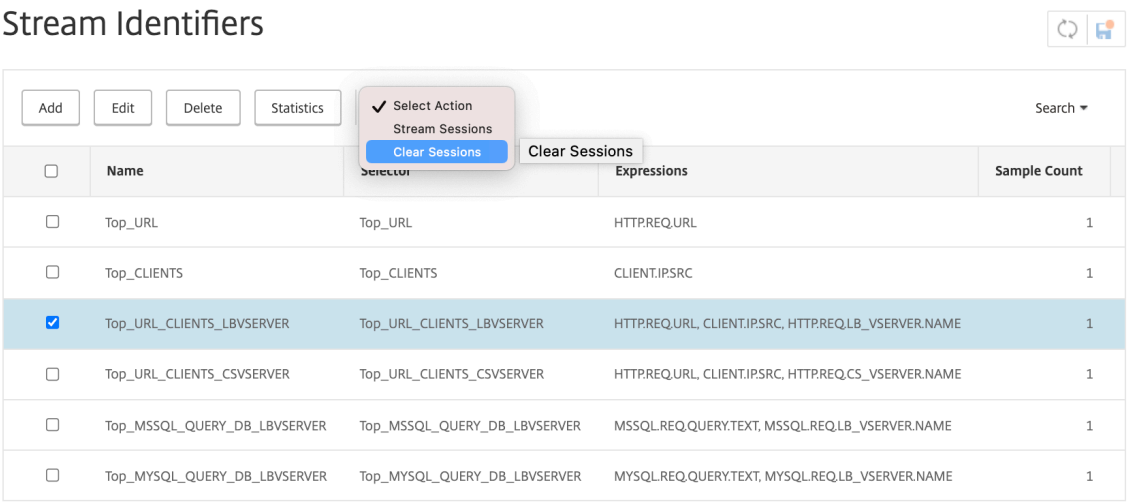
Done
```

Afficher les adresses PMAC à l'aide de l'interface graphique NetScaler

1. Connectez-vous à l'appliance NetScaler et accédez à **Configuration > Système > Partition MAC**.
2. La page Partition MAC affiche la liste des PMACs et de ses partitions.

AppExpert

May 5, 2023

Les rubriques suivantes fournissent une référence conceptuelle et des instructions de configuration pour AppExpert et d'autres fonctionnalités de l'appliance NetScaler.

> **Remarque**
>
> Pour plus d'informations sur les extensions de stratégie, voir Extensions de stratégie.

- Action Analytics : collecte des statistiques d'exécution sur la base de critères prédéfinis. Lorsqu'elle est utilisée avec des stratégies, la fonctionnalité vous fournit également l'infrastructure permettant d'optimiser automatiquement le trafic en temps réel.
- Applications et modèles AppExpert : simplifiez les étapes de configuration de l'appliance Citrix® NetScaler® en utilisant des applications, des modèles d'applications, des applications NetScaler Gateway et des modèles d'entités.
- AppQoE : La qualité d'expérience au niveau des applications (AppQoE) intègre plusieurs fonctionnalités de sécurité basées sur des politiques existantes de l'appliance NetScaler en une

seule fonctionnalité intégrée qui tire parti d'un nouveau mécanisme de mise en file d'attente, la mise en file d'attente équitable.

- Modèle d'entité : décrit comment utiliser des modèles d'entités pour configurer et configurer des entités NetScaler individuelles, telles qu'une politique ou un serveur virtuel. Un modèle d'entité fournit une spécification et un ensemble de valeurs par défaut pour l'objet.
- Légendes HTTP : requête HTTP que l'appliance NetScaler génère et envoie à une application externe lorsque certains critères sont remplis lors de l'évaluation des politiques.
- Jeux de motifs : autorise la correspondance de chaînes pendant l'évaluation d'une stratégie avancée.
- Politiques et expressions : règles qui déterminent les opérations que l'appliance NetScaler doit effectuer.
- Limitation du débit : définit la charge maximale pour une entité réseau ou une entité virtuelle donnée sur l'appliance NetScaler.
- Répondeur : base les réponses sur qui envoie la demande, d'où elle est envoyée et sur d'autres critères ayant des implications en matière de sécurité et de gestion du système.
- Réécriture : réécrit les informations contenues dans les demandes ou les réponses gérées par l'appliance NetScaler.
- String Maps : effectuez une correspondance de modèles dans toutes les fonctionnalités de NetScaler qui utilisent la syntaxe de politique par défaut.

Analyse des actions

May 5, 2023

Les performances de votre site Web ou de votre application dépendent de la façon dont vous optimisez la diffusion du contenu le plus fréquemment demandé. Des techniques telles que la mise en cache et la compression permettent d'accélérer la fourniture de services aux clients, mais vous devez être en mesure d'identifier les ressources les plus demandées, puis de mettre en cache ou de compresser ces ressources. Vous pouvez identifier les ressources les plus fréquemment utilisées en agrégeant des statistiques en temps réel sur le trafic du site Web ou des applications. Des statistiques telles que la fréquence d'accès à une ressource par rapport aux autres ressources et la quantité de bande passante consommée par ces ressources vous aident à déterminer si ces ressources doivent être mises en cache ou compressées pour améliorer les performances du serveur et l'utilisation du réseau. Des statistiques telles que les temps de réponse et le nombre de connexions simultanées à l'application vous aident à déterminer si vous devez améliorer les ressources côté serveur.

Si le site Web ou l'application ne change pas fréquemment, vous pouvez utiliser des produits qui collectent des données statistiques, puis analysent manuellement les statistiques et optimisent la diffusion du contenu. Toutefois, si vous ne souhaitez pas effectuer d'optimisations manuelles ou si votre site Web ou application est de nature dynamique, vous avez besoin d'une infrastructure capable non seulement de collecter des données statistiques, mais également d'optimiser automatiquement la fourniture de ressources sur la base des statistiques. Sur l'appliance NetScaler, cette fonctionnalité est fournie par la fonction d'analyse des actions. La fonctionnalité fonctionne sur une seule appliance NetScaler et collecte des statistiques d'exécution sur la base de critères que vous définissez. Lorsqu'elle est utilisée avec les politiques NetScaler, cette fonctionnalité vous fournit également l'infrastructure dont vous avez besoin pour optimiser automatiquement le trafic en temps réel.

Lors de la configuration de la fonctionnalité d'analyse des actions, vous spécifiez les attributs de demande pour lesquels vous souhaitez collecter des données statistiques, par exemple des URL et des méthodes HTTP, en configurant des expressions de stratégie avancées dans une entité appelée sélecteur. Ensuite, vous configurez un identificateur pour configurer des paramètres tels que l'intervalle d'échantillonnage et le nombre d'échantillons. Vous configurez également une stratégie qui permet à la solution matérielle-logicielle d'évaluer le trafic tel que spécifié par la paire sélecteur-identificateur. Enfin, vous liez la stratégie à un point de liaison pour commencer à collecter des statistiques.

La solution matérielle-logicielle vous fournit également un ensemble de sélecteurs, d'identificateurs et de stratégies de répondeur intégrés que vous pouvez utiliser pour commencer à utiliser cette fonctionnalité.

La solution matérielle-logicielle regroupe les statistiques suivantes :

- Le nombre de demandes.
- La bande passante consommée par les demandes.
- Le temps de réponse.
- Nombre de connexions simultanées.

Vous pouvez configurer la fonctionnalité pour effectuer le tri des enregistrements au moment de l'exécution sur un attribut de votre choix. Vous pouvez afficher les données statistiques à l'aide de l'interface de ligne de commande ou de l'outil Sessions en continu dans l'utilitaire de configuration.

Configurer un sélecteur

May 5, 2023

Un sélecteur est un filtre permettant d'identifier les demandes. Il comprend jusqu'à cinq expressions de stratégie avancée individuelles qui identifient les attributs de la demande tels que l'adresse IP du client et l'URL de la demande. Chaque expression est une expression de stratégie avancée non

composée et est considérée comme étant dans une relation AND avec les autres expressions. Voici quelques exemples d'expressions de sélecteur :

- `HTTP.REQ.URL`
- `CLIENT.IP.SRC`
- `HTTP.RES.BODY(1000).AFTER_STR("<string>").BEFORE_STR("<string>")"`
- `CLIENT.IP.SRC.SUBNET(24)`

Les sélecteurs sont utilisés dans les configurations de limitation de débit et d'analyse des actions. Un sélecteur est facultatif dans une configuration de limitation de débit, mais il est requis dans une configuration d'analyse des actions.

L'ordre dans lequel vous spécifiez les paramètres est significatif. Par exemple, si vous configurez une adresse IP et un domaine (dans cet ordre) dans un sélecteur, puis que vous spécifiez le domaine et l'adresse IP (dans l'ordre inverse) dans un autre sélecteur, NetScaler considère ces valeurs comme uniques. Cela peut entraîner le comptage deux fois de la même transaction. De plus, si plusieurs politiques invoquent le même sélecteur, NetScaler peut à nouveau compter la même transaction plusieurs fois.

Si vous modifiez une expression dans un sélecteur, une erreur peut s'afficher si une stratégie qui l'appelle est liée à une nouvelle étiquette de stratégie ou à un nouveau point de liaison. Par exemple, supposons que vous créiez un sélecteur nommé MyLimitSelector1, que vous l'appeliez à partir de MyLimitID1 et que vous invoquez l'identificateur à partir d'une stratégie DNS nommée DNSRateLimit1. Si vous modifiez l'expression dans MyLimitSelector1, vous risquez de recevoir une erreur lors de la liaison de DNSRateLimit1 à un nouveau point de liaison. La solution de contournement consiste à modifier ces expressions avant de créer les stratégies qui les invoquent.

L'appliance NetScaler fournit des sélecteurs PDF intégrés pour certains des cas d'utilisation les plus courants. Reportez-vous au pdf.

Vous pouvez également configurer un sélecteur avec des expressions qui identifient les attributs de demande de votre choix. Par exemple, vous pouvez créer un enregistrement pour une demande qui arrive avec un en-tête spécifique. Pour évaluer l'en-tête, vous pouvez l' `HTTP.REQ.HEADER("<header_name>")` ajouter au sélecteur que vous souhaitez utiliser.

Pour configurer un sélecteur à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer un sélecteur et vérifier la configuration :

- `add stream selector <name> <rule> ...`
- `show stream selector`

Exemple


```
> add stream selector myselector HTTP.REQ.URL CLIENT.IP.SRC
 Done
> show stream selector myselector
    Name: myselector
    Expressions:
        1) HTTP.REQ.URL
        2) CLIENT.IP.SRC
 Done
>
<!--NeedCopy-->
```

Pour modifier ou supprimer un sélecteur à l'aide de l'interface de ligne de commande :

- Pour modifier un sélecteur, tapez la commande set stream selector, le nom du sélecteur et le paramètre de règle avec les expressions. Saisissez les expressions existantes que vous souhaitez conserver, ainsi que les nouvelles expressions que vous souhaitez ajouter.
- Pour supprimer un sélecteur, tapez la commande rm stream selector et le nom du sélecteur.

Pour configurer un sélecteur à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Action Analytics** > **Selectors**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un sélecteur, cliquez sur **Ajouter**.
   - Pour modifier un sélecteur, sélectionnez-le, puis cliquez sur **Modifier**.
3. Dans la page **Créer un sélecteur** ou **Configurer le sélecteur**, définissez les paramètres suivants :
   - Nom. Pour ajouter un nom au sélecteur, entrez le nom dans le champ **Nom** . Le nom doit commencer par un caractère ASCII, alphanumérique ou de soulignement. Le nom doit contenir uniquement des caractères alphanumériques ASCII, soulignement, hachage, point, espace, deux-points, at, égal et trait d'union.
   - Expressions. Pour ajouter l'expression à la configuration du sélecteur, cliquez sur **Insérer**. Pour supprimer une expression de la configuration du sélecteur, dans la zone Expression, sélectionnez l'expression, puis cliquez sur **Supprimer**. Remarque : Dans la zone Expressions, saisissez un paramètre valide. Par exemple, saisissez HTTP. Ensuite, saisissez une période après ce paramètre. Un menu déroulant apparaît. Le contenu de ce menu fournit les mots-clés qui peuvent suivre le mot-clé initial que vous avez saisi. Pour sélectionner le mot-clé suivant dans ce préfixe d'expression, double-cliquez sur la sélection dans le menu déroulant. La zone de texte **Expressions** affiche les premier et deuxième mots-clés du préfixe d'expression, par exemple HTTP.REQ. Continuez à ajouter des composants d'expression jusqu'à ce que l'expression complète soit formée.
4. Cliquez sur **Insérer**.
5. Continuez à ajouter jusqu'à cinq expressions non composées.

6. Cliquez sur **Créer**, puis sur **Fermer**.



Configurer un identifiant de flux

May 5, 2023

Vous configurez un identifiant de flux pour spécifier les paramètres de collecte de données statistiques à partir des demandes identifiées par un sélecteur donné. Un identifiant spécifie le sélecteur à utiliser, l'intervalle de collecte des statistiques, le nombre d'échantillons et le champ sur lequel les enregistrements doivent être triés.

L'appliance NetScaler inclut les identifiants de flux intégrés suivants pour les cas d'utilisation courants. Tous les identificateurs intégrés spécifient un nombre d'échantillons de 1 et un intervalle d'une minute. En outre, ils trient les données sur l'attribut
REQUESTS. Ils ne diffèrent que par le fait qu'ils sont associés à différents sélecteurs intégrés. Chaque identifiant intégré est associé à un sélecteur intégré du même nom (par exemple, l'identifiant intégré Top_URL est associé au sélecteur
intégré Top_URL). Les identifiants intégrés sont les suivants :

- URL du haut

- Principaux clients
- Top_URL_Clients_LBVServer
- Clients_URL_Clients_Serveur_CSV
- Serveur Top_MSSQL_Query_DB_LBV
- Top_MYSQL_QUERY_DB_LBVSERVER

Pour plus d'informations sur les sélecteurs intégrés, voir Configuration d'un sélecteur.

Remarque : La longueur maximale pour stocker les résultats de chaîne des sélecteurs (par exemple, HTTP.REQ.URL) est de 60 caractères. Si la chaîne (URL, par exemple) comporte 1 000 caractères, dont 50 suffisent pour identifier une chaîne de manière unique, utilisez une expression pour extraire uniquement les 50 caractères requis.

Vous ne pouvez pas modifier la configuration d'un identifiant intégré. Vous pouvez toutefois créer un identifiant avec la configuration de votre choix.

Pour configurer un identifiant de flux à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un identifiant de flux et vérifier la configuration :

- `add stream identifier <name> <selectorName> [-interval <positive_integer>] [-SampleCount <positive_integer>] [-sort <sort>]`
- `show stream identifier <name>`

Exemple

```
1 > add stream identifier myidentifier Top_URL -interval 10 -sampleCount
     100
2  Done
3 <!--NeedCopy-->
```

Pour configurer un identifiant de flux à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Action Analytics** > **Identificateurs de flux**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer un identifiant de flux, cliquez sur **Ajouter**.
   - Pour modifier un identifiant de flux, sélectionnez-le, puis cliquez sur **Modifier**.
3. Sur la page Configurer l'identifiant de flux, définissez les paramètres suivants :
   - Nom
   - Sélecteur
   - Intervalle
   - Nombre d'échantillons
   - Trier

4. Cliquez sur **Créer**, puis sur **Fermer**.



Afficher les statistiques

August 20, 2021

Vous pouvez afficher les statistiques collectées au format tabulaire dans l'interface de ligne de commande et au format graphique dans l'utilitaire de configuration.

Le tableau suivant décrit les statistiques collectées :

Statistiques	Nom de colonne dans la sortie de la commande <identifier name> stat stream identifier	Description
Nombre de demandes	**Req**	Nombre de demandes pour lesquelles des enregistrements ont été créés au cours des<interval> dernières minutes.
Bande passante consommée	**BandW**	Bande passante totale consommée par les demandes reçues au cours des<interval> dernières minutes. La bande passante totale d'une demande est la bande passante consommée par la demande et sa réponse. La valeur est arrondie à la valeur entière supérieure ou inférieure suivante. Il peut donc être légèrement différent de la valeur attendue. Par exemple, si la consommation totale de bande passante d'une demande est de 2,2 Ko. Une instance de la demande peut être affichée comme ayant consommé 2 Ko. Deux instances peuvent être affichées comme ayant consommé 4 Ko, mais trois instances peuvent être affichées comme ayant consommé 7 Ko.

Statistiques	Nom de colonne dans la sortie de la commande <identifier name> stat stream identifier	Description
Temps de réponse	**RspTime**	Temps de réponse moyen pour toutes les demandes reçues au cours des<interval> dernières minutes.
Connexions simultanées	**Conn**	Nombre total de connexions simultanées actuellement ouvertes.

Pour afficher les données statistiques collectées pour un identifiant de flux à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
stat stream identifier <name> [<pattern> ...] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-sortBy <sortBy> [<sortOrder>]
```

Exemples

Exemple 1 trie la sortie de la colonne BandW, dans l'ordre décroissant. Exemple 2 trie la sortie dans l'exemple 1, dans la colonne **Req** et dans l'ordre croissant

Exemple 1

```
> stat stream identifier myidentifier -sortBy BandW Descending -fullValues
Stream Session statistics
                    Req                BandW
User1               508               125924
User2              5020                12692
User3              2025                 4316

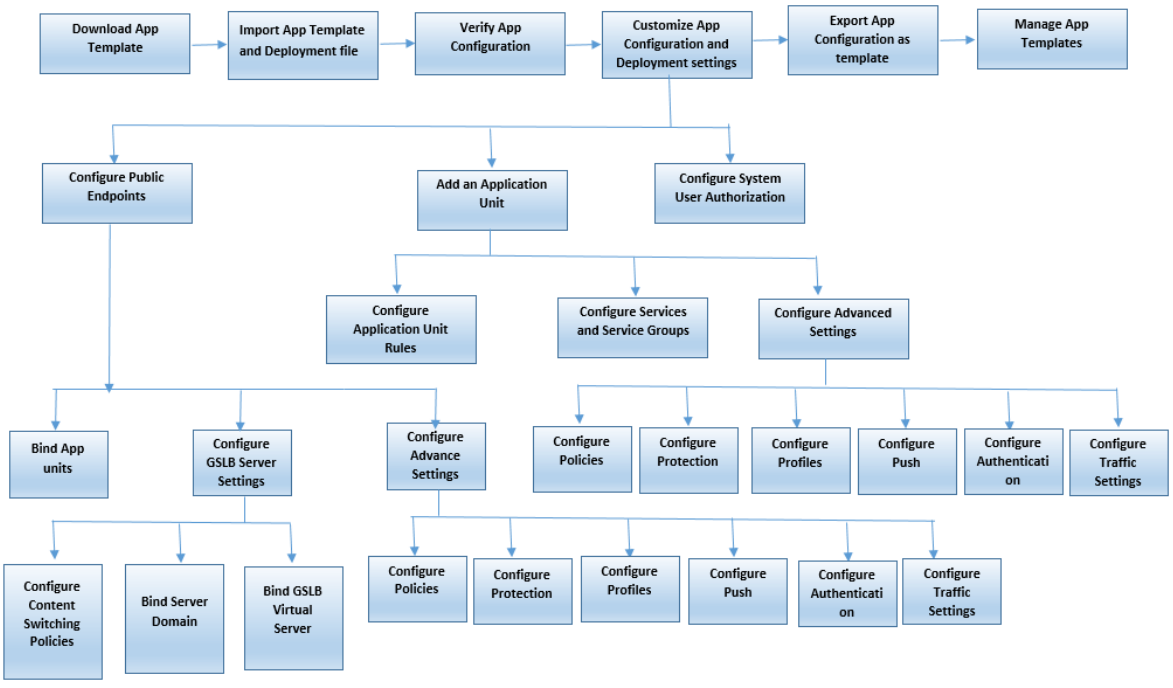
                RspTime                Conn
User1              5694                   0
User2               109                   0
User3                 3                   0
 Done
```



```
<!--NeedCopy-->
```

Exemple 2

```
> stat stream identifier myidentifier -sortBy Req Ascending -
    fullValues
Stream Session statistics
                    Req                 BandW
User1               508                125924
User3              2025                  4316
User2              5020                 12692

                RspTime                  Conn
User1              5694                     0
User3                 3                     0
User2               109                     0
 Done
<!--NeedCopy-->
```

Pour afficher les données statistiques collectées pour un identifiant de flux à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Analytics** > **Identificateurs de flux**.
2. Sélectionnez l'identificateur de flux dont vous souhaitez afficher les sessions, puis cliquez sur Statistiques Pour plus d'informations sur la façon de regrouper la sortie sur la base des valeurs collectées pour diverses expressions de sélecteur.



Regroupement des enregistrements sur les valeurs d'attribut

August 20, 2021

Des informations statistiques telles que le nombre de fois qu'une URL particulière a été accédé globalement et par client, et le nombre total de demandes GET et POST par client peuvent fournir des

informations précieuses pour savoir si l'une de vos ressources doit être développée pour répondre à la demande ou être optimisée pour la livraison. Pour obtenir de telles statistiques, vous devez utiliser un ensemble approprié d'expressions de sélection, puis utiliser le paramètre pattern dans la commande stat stream identifier. Le regroupement est basé sur le modèle spécifié dans la commande. Le regroupement peut être effectué simultanément sur les valeurs de plusieurs expressions.

Dans l'interface de ligne de commande, vous pouvez regrouper la sortie en utilisant les modèles de votre choix. Dans l'utilitaire de configuration, le motif dépend des choix que vous effectuez lors de l'exploration vers le bas des valeurs de diverses expressions de sélecteur. Par exemple, considérez un sélecteur qui a les expressions `HTTP.REQ.URL`, `CLIENT.IP.SRC`, et `HTTP.REQ.LB_VSERVER.NAME`, dans cet ordre. La page d'accueil des statistiques affiche des icônes pour chacune de ces expressions. Si vous cliquez sur l'icône pour `CLIENT.IP.SRC`, la sortie est basée sur les motifs *?*. La sortie affiche des statistiques pour chaque adresse IP du client. Si vous cliquez sur une adresse IP, la sortie est basée sur les modèles * `<IP address>` ? et ? `<IP address>` * où `<IP address>` est l'adresse IP que vous avez sélectionnée. Dans la sortie résultante, si vous cliquez sur une URL, le modèle utilisé est `<URL> <IP address> ?`.

Pour regrouper les enregistrements sur les valeurs des expressions de sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, entrez la commande suivante pour regrouper les enregistrements sur la base d'une expression de sélecteur :

```
stat stream identifier <name> [<pattern> ...]
```

Les exemples suivants utilisent un modèle différent pour démontrer l'effet du motif sur la sortie de la commande stat stream identifier. Les expressions sélectrices sont HTTP.REQ.URL et HTTP.REQ.HEADER (« UserHeader »), dans cet ordre. Les requêtes contiennent un en-tête personnalisé dont le nom est UserHeader. Notez que dans les exemples, une valeur statistique donnée change selon le regroupement, mais la somme totale des valeurs pour un champ donné reste la même.

Exemple 1

Dans la commande suivante, le modèle utilisé est ? ?. L'appliance regroupe la sortie sur les valeurs collectées pour les deux expressions de sélecteur. Les en-têtes de ligne sont constitués des valeurs d'expression séparées par un point d'interrogation (?). La ligne avec l'en-tête /mysite/mypage1.html? Ed affiche les statistiques des requêtes faites par l'utilisateur Ed pour l'URL /mysite/mypage1.html.

> **Remarque :**
>
> Vous devez vous assurer de taper la commande suivante avec "?" au lieu de "?". Par exemple, Si sélecteur utilise une expression - client.ip.src et client.tcp.srcport. La commande Stat pour

> regrouper la sortie sur les valeurs collectées pour le sélecteur est ‘stat stream identifier myidentifier ? ? -fullValues’ comme indiqué ci-dessous.

```
> stat stream identifier myidentifier ? ? -fullValues
Stream Session statistics
                                          Req                  BandW
/mysite/mypage2.html?Grace                  1                   2553
/mysite/mypage1.html?Grace                  2                      4
/mysite/mypage1.html?Ed                     8                     16
/mysite/mypage2.html?Joe                    1                   2554
/mysite/mypage1.html?Joe                    5                     10
/mysite/?Joe                                1                      4

                                       RspTime                  Conn
/mysite/mypage2.html?Grace                  0                      0
/mysite/mypage1.html?Grace                  0                      0
/mysite/mypage1.html?Ed                     0                      0
/mysite/mypage2.html?Joe                    0                      0
/mysite/mypage1.html?Joe                    0                      0
/mysite/?Joe                                6                      0
 Done
<!--NeedCopy-->
```

Exemple 2

Dans la commande suivante, le motif utilisé est * ?. L’appliance regroupe la sortie sur les valeurs accumulées pour la deuxième expression HTTP.REQ.HEADER (« userHeader »). Les lignes affichent des statistiques pour toutes les demandes faites par les utilisateurs Grace, Ed et Joe.

> **Remarque :**
>
> Assurez-vous de taper la commande suivante avec “?” au lieu de “?”.

```
> stat stream identifier myidentifier * ?
Stream Session statistics
                  Req    BandW  RspTime     Conn
Grace               3     2557        0        0
Ed                  8       16        0        0
Joe                 7     2568        6        0
 Done
<!--NeedCopy-->
```

Exemple 3

Dans la commande suivante, le modèle utilisé est ? *, qui est le modèle par défaut. La sortie est groupée sur les valeurs collectées pour la première expression de sélecteur. Chaque ligne affiche des statistiques pour une URL.

> **Remarque :**
>
> Assurez-vous de taper la commande suivante avec “?” au lieu de “?”.

```
> stat stream identifier myidentifier ? * -fullValues
Stream Session statistics

                                          Req                  BandW
/mysite/mypage2.html                        2                   5107
/mysite/mypage1.html                       15                     30
/mysite/                                    1                      4

                                       RspTime                  Conn
/mysite/mypage2.html                          0                      0
/mysite/mypage1.html                          0                      0
/mysite/                                      6                      0
 Done
<!--NeedCopy-->
```

Exemple 4

Dans la commande suivante, le modèle utilisé est `* *`. L’appliance affiche un ensemble de statistiques collectives pour toutes les demandes reçues, sans titre de ligne.

```
> stat stream identifier myidentifier * *
Stream Session statistics
                  Req     BandW  RspTime      Conn
                   18      5141         6         0
 Done
<!--NeedCopy-->
```

Exemple 5

Dans la commande suivante, le modèle est /mysite/mypage1.html *. L’appliance affiche un ensemble de statistiques collectives pour toutes les demandes reçues pour l’URL /mysite/mypage1.html, sans titre de ligne.

```
> stat stream identifier myidentifier /mysite/mypage1.html *
Stream Session statistics
                  Req     BandW  RspTime      Conn
                   15        30         0         0
 Done
<!--NeedCopy-->
```


Effacement d'une session de flux

August 20, 2021

Vous pouvez vider tous les enregistrements qui ont été accumulés pour un identifiant de flux.

Pour effacer une session de flux à l'aide de l'interface de ligne de commande

À l'invite de commandes, entrez les commandes suivantes pour effacer une session de flux et vérifier les résultats :

- session de flux effacer
- identificateur de flux stat

Exemple

Cet exemple utilise d'abord la commande stat stream identifier, de sorte qu'une comparaison peut être effectuée avec la commande stat stream identifier utilisée pour vérifier le résultat de la commande clear stream session.

```
1  >stat stream identifier myidentifier
2  Stream Session statistics
3                   Req    BandW  RspTime     Conn
4  /aed....html       2        0        0        0
5  /                636      303       12        0
6   Done
7  >clear stream session myidentifier
8   Done
9  >stat stream identifier myidentifier
10  Done
11 <!--NeedCopy-->
```

Pour effacer une session de flux à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Analytics** > **Identificateurs de flux**.
2. Sélectionnez l'identificateur de flux dont vous souhaitez effacer les sessions, puis cliquez sur **Effacer les sessions**.



Configurer la stratégie d'optimisation du trafic

May 5, 2023

Pour que la paire sélecteur-identificateur de votre configuration d'analyse des actions entre en vigueur, vous devez associer la paire au point du flux de trafic auquel vous souhaitez collecter des statistiques. Vous pouvez le faire en configurant une stratégie avancée et en référençant l'identificateur de flux à partir de la règle de stratégie. Vous pouvez utiliser des stratégies de compression, des stratégies de mise en cache, des stratégies de réécriture, des stratégies de pare-feu d'application, des stratégies de répondeur et toute autre stratégie dont l'action est basée sur une expression booléenne.

La fonctionnalité d'analyse des actions introduit un ensemble d'expressions de stratégie avancées et de fonctions de collecte et d'évaluation des données. L'expression `ANALYTICS.STREAM(<identifier_name>)` est utilisée pour référencer l'identificateur que vous souhaitez utiliser. L'expression COLLECT_STATS est utilisée pour collecter des données statistiques. Des fonctions telles que `IS_TOP(<uint>)` et `IS_TOP_FREQUENTS(<uint>)` sont utilisées pour prendre des décisions automatiques et en temps réel en matière d'optimisation du trafic.

- **IS_TOP (<number>).** Trouve si un objet donné se trouve en haut <number>des éléments. Par exemple, l'élément figure parmi les 10 premiers éléments. Lorsque plusieurs éléments sont comptés, ils sont considérés comme étant de nature similaire. La fonction de tri doit être activée pour éviter une condition undef.
- **IS_TOP_FREQUENTS(<frequency>).** Recherche si un objet donné se trouve au top de <frequency> des éléments qui se trouvent dans les éléments supérieurs. Par exemple, l'élément se situe parmi les 50 % les plus importants de tous les éléments les plus importants

maintenus. Les éléments ayant les mêmes valeurs sont considérés comme similaires par nature. La fonction de tri doit être activée pour éviter une condition undef.

C'est la configuration de votre politique qui détermine si l'appliance NetScaler doit uniquement collecter des données à partir du trafic ou également effectuer une action. Si la solution matérielle-logicielle doit uniquement collecter des données statistiques, vous pouvez configurer une stratégie avec la règle `ANALYTICS.STREAM(<identifier_name>).COLLECT_STATS` et l'action NOOP. La stratégie NOOP doit être la stratégie ayant la priorité la plus élevée au point de liaison. Cette stratégie est suffisante si vous ne collectez que des statistiques. Les décisions d'optimisation du trafic, telles que les éléments à compresser ou à mettre en cache, doivent être basées sur une évaluation manuelle et périodique des données statistiques.

Si, en plus de collecter des statistiques, l'appliance doit également effectuer une action sur le trafic, vous devez configurer le paramètre GoToPriorityExpression de la stratégie NOOP de sorte qu'une autre stratégie comportant la règle et l'action souhaitées soit évaluée ultérieurement. Cette deuxième stratégie doit comporter une règle commençant par le `ANALYTICS.STREAM(<identifier_name>)` préfixe et une fonction qui évalue les données.

Voici un exemple de deux stratégies de répondeur configurées et liées globalement. La stratégie responder_stat_collection permet à la solution matérielle-logicielle de collecter des statistiques basées sur l'identificateur myidentifier. La stratégie responder_notify évalue les données collectées.

Exemple

```
> add responder action send_notification respondwith '"You are in the Top 10 list for bandwidth consumption"'
 Done
> add responder policy responder_stat_collection' ANALYTICS.STREAM("myidentifier").COLLECT_STATS' NOOP
Done
> add responder policy responder_notify 'ANALYTICS.STREAM("myidentifier").BANDWIDTH.IS_TOP(10)' send_notification
 Done
> bind responder global responder_stat_collection 10 NEXT
 Done
> bind responder global responder_notify 20 END
 Done
<!--NeedCopy-->
```


Comment limiter la consommation de bande passante par utilisateur ou périphérique client

August 20, 2021

Votre site Web, application ou service d'hébergement de fichiers dispose de ressources réseau et serveur limitées pour servir tous ses utilisateurs. L'une des ressources les plus importantes est la bande passante. Une consommation importante de bande passante par seulement un sous-ensemble de la base d'utilisateurs peut entraîner une congestion du réseau et une réduction de la disponibilité des ressources pour les autres utilisateurs. Pour éviter la congestion réseau, vous devrez peut-être limiter la consommation de bande passante d'un client en utilisant des techniques de déni de service temporaires telles que la réponse à une demande client avec une page HTML si elle a dépassé une valeur de bande passante préconfigurée sur une période de temps fixe précédant la demande.

En général, vous pouvez réguler la consommation de bande passante par appareil client ou par utilisateur. Ce cas d'utilisation montre comment vous pouvez limiter la consommation de bande passante par client à 100 Mo sur une période d'une heure. Le cas d'utilisation montre également comment vous pouvez réguler la consommation de bande passante par utilisateur à 100 Mo sur une période d'une heure, à l'aide d'un en-tête personnalisé qui fournit le nom d'utilisateur. Dans les deux cas, le suivi de la consommation de bande passante sur une période de déplacement d'une heure est réalisé en définissant le paramètre d'intervalle dans l'identificateur de flux sur 60 minutes. Les cas d'utilisation montrent également comment importer une page HTML à envoyer à un client qui a dépassé la limite. L'importation d'une page HTML simplifie non seulement la configuration de l'action du répondeur dans ces cas d'utilisation, mais simplifie également la configuration de toutes les actions du répondeur qui nécessitent la même réponse.

Pour limiter la consommation de bande passante par utilisateur ou par périphérique client à l'aide de l'interface de ligne de commande

Dans l'interface de ligne de commande, effectuez les tâches suivantes pour configurer l'analyse des actions afin de limiter la consommation de bande passante d'un client ou d'un utilisateur. Chaque étape comprend des exemples de commandes et leur sortie.

1. **Configurez votre configuration d'équilibrage de charge.** Configurez le serveur virtuel d'équilibrage de charge mysitevip, puis configurez tous les services dont vous avez besoin. Liez les services au serveur virtuel. L'exemple suivant crée dix services et lie les services à mysitevip.

```
> add lb vserver mysitevip HTTP 192.0.2.17 80
 Done
> add service service[1-10] 192.0.2.[240-249] HTTP 80
service "service1" added
service "service2" added
```



```
service "service3" added
.
.
.
service "service10" added
 Done
> bind lb vserver vserver1 service[1-10]
service "service1" bound
service "service2" bound
service "service3" bound
.
.
.
service "service10" bound
 Done
<!--NeedCopy-->
```

2. **Configurez le sélecteur de flux.** Configurez l'un des sélecteurs de flux suivants :

   - Pour limiter la consommation de bande passante par client, configurez un sélecteur de flux qui identifie l'adresse IP du client.

     ```
     > add stream selector myselector CLIENT.IP.SRC
      Done
     <!--NeedCopy-->
     ```

   - Pour limiter la consommation de bande passante par utilisateur sur la base de la valeur d'un en-tête de demande qui fournit le nom d'utilisateur, configurez un sélecteur de flux qui identifie l'en-tête. Dans l'exemple suivant, le nom de l'en-tête est UserHeader.

     ```
     > add stream selector myselector HTTP.REQ.HEADER( "UserHeader
        " )
      Done
     <!--NeedCopy-->
     ```

3. **Configurez un identifiant de flux.** Configurez un identificateur de flux qui utilise le sélecteur de flux. Définissez le paramètre d'intervalle sur 60 minutes.

   ```
   > add stream identifier myidentifier myselector -interval 60 -
      sampleCount 1 -sort BANDWIDTH
    Done
   <!--NeedCopy-->
   ```

4. **Configurez l'action du répondeur.** Importez la page HTML que vous souhaitez envoyer aux utilisateurs ou aux clients qui ont dépassé la limite de consommation de bande passante, puis

utilisez la page dans l'action répondeur crossed_limits.

```
> import responder htmlpage http://.1.1.1/stdpages/wait.html
   crossed-limits.html
This operation may take some time, Please wait...

 Done
> add responder action crossed_limits respondwithhtmlpage crossed-
   limits.html
 Done
<!--NeedCopy-->
```

5. **Configurez les stratégies de répondeur.** Configurez la stratégie de répondeur myrespol1 avec la règle ANALYTICS.STREAM (« myidentifier ») .COLLECT_STATS et l'action NOOP. Ensuite, configurez la stratégie myrespol2 pour déterminer si un client ou un utilisateur a dépassé la limite de 100 Mo. La stratégie myrespol2 est configurée avec l'action du répondeur crossed_limits.

```
> add responder policy myrespol1 'ANALYTICS.STREAM("myidentifier")
   .COLLECT_STATS' NOOP
 Done
> add responder policy myrespol2 'ANALYTICS.STREAM("myidentifier")
   .BANDWIDTH.GT(104857600)' crossed_limits
 Done
<!--NeedCopy-->
```

6. **Liez les stratégies du répondeur au serveur virtuel d'équilibrage de charge.** La stratégie myrespol1, qui ne recueille que des données statistiques, doit avoir la priorité la plus élevée et une expression GOTO de NEXT.

```
> bind lb vserver mysitevip -policyName myrespol1 -priority 1 -
   gotoPriorityExpression NEXT
 Done
> bind lb vserver mysitevip -policyName myrespol2 -priority 2 -
   gotoPriorityExpression END
 Done
<!--NeedCopy-->
```

7. **Testez la configuration.** Testez la configuration en envoyant des requêtes HTTP de test, provenant de plusieurs clients ou utilisateurs, au serveur virtuel d'équilibrage de charge et en utilisant la commande stat stream identifier pour afficher les statistiques collectées pour l'identificateur spécifié. La sortie suivante affiche des statistiques pour les clients.

```
> stat stream identifier myidentifier -sortBy BandW  - fullValues
Stream Session statistics
```



```
3                                Req           BandW
4  192.0.2.30                    5000          3761
5  192.0.2.31                    29            2602
6  192.0.2.32                    25            51
7
8                                RspTime       Conn
9  192.0.2.30                    2             0
10 192.0.2.31                    0             0
11 192.0.2.32                    0             0
12  Done
13 >
14 <!--NeedCopy-->
```

Applications AppExpert

> **Avertissement**
>
> La fonctionnalité de modèle d'application est obsolète. Comme alternative, vous pouvez utiliser StyleBooks. Pour plus d'informations, consultez StyleBooks et le pare-feu d'applications Web StyleBook.

Une application AppExpert est un ensemble de configurations que vous configurez sur l'appliance NetScaler. La gestion des applications AppExpert est simplifiée par une interface graphique (GUI) qui vous permet de spécifier des sous-ensembles de trafic d'applications et un ensemble distinct de stratégies de sécurité et d'optimisation pour le traitement de chaque sous-ensemble de trafic. En outre, il consolide les étapes de déploiement dans une seule vue, ce qui vous permet de configurer rapidement les adresses IP cibles pour les clients et de spécifier des serveurs hôtes.

Une fois l'application AppExpert configurée, vous devez vérifier que l'application fonctionne correctement. Si nécessaire, vous pouvez personnaliser la configuration en fonction de vos besoins.

Périodiquement, vous pouvez vérifier et surveiller la configuration en affichant les compteurs de divers composants d'application, statistiques et Application Visualizer. Vous pouvez également configurer des stratégies d'authentification, d'autorisation et d'audit (authentification, autorisation et audit) pour l'application.

Terminologie de l'application AppExpert

Voici les termes utilisés dans la fonctionnalité AppExpert AppExpert et les descriptions des entités pour lesquelles ils sont utilisés :

Point de terminaison public. Combinaison d'adresse IP et de port par laquelle l'appliance NetScaler reçoit les demandes des clients pour l'application Web associée. Un point de terminaison public

peut être configuré pour recevoir du trafic HTTP ou HTTP sécurisé (HTTPS). Toutes les demandes du client pour l'application Web doivent être envoyées à un point de terminaison public. Il est possible d'attribuer plusieurs points de terminaison à une application AppExpert.

Unité d'application. Entité d'application AppExpert qui traite un sous-ensemble du trafic des applications Web et équilibre la charge d'un ensemble de services qui hébergent le contenu associé. Le sous-ensemble du trafic qu'une unité d'application doit gérer est défini par une règle. Chaque unité d'application définit également son propre ensemble de stratégies d'optimisation du trafic et de sécurité pour les demandes et les réponses qu'elle gère. Les services NetScaler associés à ces politiques sont la compression, la mise en cache, la réécriture, le répondeur et le pare-feu d'applications.

Par défaut, chaque application AppExpert comportant au moins une unité d'application inclut une unité d'application par défaut, qui ne peut pas être supprimée. L'unité d'application par défaut n'est pas associée à une règle d'identification des demandes et est toujours placée en dernier dans l'ordre des unités d'application. Il définit un ensemble de stratégies pour le traitement de toute demande qui ne correspond pas aux règles configurées pour les autres unités d'application. Ainsi, toutes les demandes des clients sont traitées.

Service. Combinaison de l'adresse IP du serveur qui héberge l'instance d'application Web et du port auquel l'application est mappée sur le serveur, au format `\<IP address\>:\<Port\>`. Une application Web qui répond à de nombreuses demandes est hébergée sur plusieurs serveurs. Chaque serveur est censé héberger une instance de l'application Web, et chacune de ces instances de l'application Web est représentée par un service sur l'appliance NetScaler.

Règle de l'unité d'application. Expression de stratégie avancée qui définit les caractéristiques d'un sous-ensemble de trafic pour une unité d'application. L'exemple de règle suivant est une expression de stratégie avancée qui identifie un sous-ensemble de trafic composé de quatre types d'images :

```
HTTP.REQ.URL.SUFFIX.EQ("bmp")|| HTTP.REQ.URL.SUFFIX.EQ("gif")|| HTTP.REQ.
URL.SUFFIX.EQ("png")|| HTTP.REQ.URL.SUFFIX.EQ("jpg")
```

Pour plus d'informations sur les expressions de stratégie avancées, consultez la section Stratégies et expressions.

Sous-ensemble de trafic. Ensemble de demandes client qui nécessitent un ensemble commun de stratégies d'optimisation du trafic et de sécurité. Un sous-ensemble de trafic est géré par une unité d'application et est défini par une règle.

Fonctionnement de l'application AppExpert

May 5, 2023

Lorsque le point de terminaison reçoit une demande client, l'appliance NetScaler évalue la demande par rapport à la règle configurée pour l'unité d'application la plus haute. Si la demande satisfait à cette

règle, elle est traitée par les stratégies qui sont configurées pour l'unité d'application, puis transmise à un service. Le choix du service dépend des services configurés pour l'application et de paramètres tels que l'algorithme d'équilibrage de charge et la méthode de persistance configurés pour l'unité d'application.

Si la demande ne satisfait pas la règle, elle est évaluée par rapport à la règle de l'unité d'application supérieure suivante. Dans cet ordre, la demande est évaluée par rapport à chaque règle d'unité d'application jusqu'à ce que la demande satisfasse à une règle. Si la demande ne satisfait aucune des règles configurées, elle est traitée par l'unité d'application par défaut, qui est toujours la dernière unité d'application.

Vous pouvez configurer plusieurs points de terminaison publics pour une application AppExpert. Dans une telle configuration, par défaut, chaque unité d'application traite les demandes reçues par tous les points de terminaison publics et équilibre la charge de tous les services configurés pour l'application. Toutefois, vous pouvez spécifier qu'une unité d'application traite le trafic provenant uniquement d'un sous-ensemble de points de terminaison publics et n'équilibre la charge qu'un sous-ensemble des services configurés pour l'application AppExpert.

Le diagramme de flux suivant illustre la séquence de flux de l'application AppExpert pour l'utilisation d'un modèle d'application intégré.



Si vous préférez créer une application personnalisée sans utiliser de modèle, procédez comme suit :

1. Créez une application personnalisée.
2. Configurez les paramètres de déploiement et d'application
3. Exportez la configuration vers de nouveaux fichiers modèles (facultatif).

4. Importez les fichiers modèles vers d'autres appliances NetScaler qui nécessitent une configuration d'application AppExpert similaire

Personnalisation de la configuration

May 5, 2023

Après avoir vérifié que l'application AppExpert fonctionne correctement, vous pouvez personnaliser la configuration en fonction de vos besoins.

Après avoir vérifié que la configuration de l'application AppExpert fonctionne correctement, vous pouvez configurer l'application et les paramètres de déploiement en fonction de vos besoins. Lorsque vous importez un modèle d'application et un fichier de déploiement, le système renseigne automatiquement l'application cible avec les paramètres de configuration disponibles (tels que les unités d'application, les règles d'unité d'application, les stratégies, les paramètres de persistance, les méthodes d'équilibrage de charge, les profils et les paramètres de trafic). Dans cette application, vous pouvez configurer les paramètres de déploiement tels que les points de terminaison publics, les services et les groupes de services pour chaque sous-ensemble de trafic. Si vous souhaitez que l'application AppExpert gère un sous-ensemble de trafic qui n'est pas inclus dans le modèle, vous pouvez ajouter une unité d'application pour un sous-ensemble de trafic ou modifier l'unité d'application existante. Après avoir personnalisé la configuration, vous pouvez également spécifier l'ordre d'évaluation pour chaque sous-ensemble de trafic géré par l'application.

La configuration d'une application AppExpert comprend les étapes suivantes :

1. Configuration de points de terminaison publics
2. Configuration des unités d'application
3. Spécification de l'ordre d'évaluation
4. Visualisation de la configuration de l'application à l'aide

Vous pouvez également configurer les stratégies fournies par le modèle. Si le modèle d'application AppExpert n'inclut pas de politiques pour une fonctionnalité particulière de NetScaler, telle que la réécriture ou le pare-feu d'applications, vous pouvez configurer vos propres politiques.

Configuration des points de terminaison publics

June 23, 2022

Si vous n'avez pas spécifié de point de terminaison public lors de l'importation d'une application AppExpert, vous pouvez spécifier des points de terminaison publics après avoir créé l'application. Vous

pouvez configurer un point de terminaison public de type HTTP et un point de terminaison public de type HTTPS pour votre application AppExpert.

Si les points de terminaison sont déjà configurés pour l'application, vous pouvez dissocier les points de terminaison de l'application AppExpert et supprimer les points de terminaison dont vous n'avez plus besoin. Notez que lorsque vous dissociez un point de terminaison public de l'application AppExpert, le point de terminaison est automatiquement dissocié de l'unité d'application associée, mais il n'est pas supprimé du système.

Pour configurer des points de terminaison publics pour une application AppExpert :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez avec le bouton droit sur l'application pour laquelle vous souhaitez configurer des points de terminaison publics, puis cliquez sur Modifier.
3. Dans la page **Applications**, accédez à la section **Public Endpoint** et cliquez sur l'icône en forme de crayon.
4. Dans le curseur **Public Endpoint**, définissez les paramètres suivants.
    a) Type de point de terminaison public. Sélectionnez le bouton radio pour définir le type de point final.
    b) Nom. Nom du point de terminaison public.
    c) Adresse IP. Adresse IP du point de terminaison public.
    d) Port. Numéro de port du point de terminaison public.
    e) Protocole. Sélectionnez un type de protocole comme HTTP ou HTTPS.
5. Cliquez sur **Continuer.**
6. Dans la section **Unités d'application**, sélectionnez une unité d'application dans la liste.
7. Cliquez sur **Continuer** pour définir la stratégie et les détails du serveur.
8. Cliquez sur **OK**, puis sur Terminé.
9. Cliquez sur Fermer.

Pour plus d'informations sur les paramètres de la boîte de dialogue **Configurer le point de terminaison public**, voir Commutation de contenu.

Configuration des services et des groupes de services pour une unité d'application

June 23, 2022

Lorsque vous configurez un service ou un groupe de services, vous modifiez un service ou un groupe de services existant, ou vous ajoutez de nouveaux services à l'application AppExpert. Vous ajoutez des services ou des groupes de services si vous ne les avez pas spécifiés lors de l'importation du modèle d'application. Vous ajoutez également des services et des groupes de services lorsque vous aug-

mentez le nombre de serveurs hébergeant des instances de l'application. Vous pouvez configurer un service et un groupe de services pour une unité d'application uniquement après avoir configuré le service ou le groupe de services pour l'application AppExpert.

Pour configurer un service ou un groupe de services pour l'application AppExpert :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez avec le bouton droit sur l'application, puis cliquez sur **Modifier.**
3. Sur la page **Applications**, sélectionnez une unité d'application, puis cliquez sur **Continuer**.
4. Dans la section **Services et groupes de services**, procédez comme suit :
    a) Dans le curseur Service Binding, définissez les paramètres suivants.
        i. Service. Sélectionnez un service d'équilibrage de charge dans la liste ou créez un nouveau service.
        ii. Poids. Fournissez une valeur pondérale pour le service.
    b) Cliquez sur **Lier**, puis sur **Terminé.**
    c) Dans le curseur ServiceGroup Binding, définissez les paramètres suivants :
        i. Nom du groupe de services. Sélectionnez un groupe de services d'équilibrage de charge ou créez un nouveau groupe de services.
        ii. Cliquez sur **Lier**, puis sur **Terminé**.
    d) Cliquez sur **Terminé**.
5. Cliquez sur **Continuer** pour définir d'autres configurations.

Créer des unités d'application

June 23, 2022

Il se peut que vous deviez ajouter des unités d'application pour les sous-ensembles de trafic qui sont spécifiques à votre implémentation d'application Web ou qui ne sont pas définis dans le modèle. Lorsque vous créez une unité d'application, vous devez configurer une règle pour cette unité d'application.

Pour créer une unité d'application pour l'application AppExpert, procédez comme suit :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit de la souris sur l'application pour laquelle vous souhaitez ajouter une unité d'application, puis cliquez sur **Ajouter**.
3. Dans la page **Applications**, accédez à la section **Unités d'application** et cliquez sur l'icône en forme de **crayon** .

Pour configurer les expressions de stratégie pour une unité d'application :

1. Accédez à **AppExpert** > **Applications**.

2. Dans le volet d'informations, cliquez avec le bouton droit de la souris sur l'application pour laquelle vous souhaitez ajouter une unité d'application, puis cliquez sur **Ajouter**.
3. Dans la page **Applications**, accédez à la section **Unités d'application** et cliquez sur l'icône **+** pour créer une unité et ajouter des expressions de stratégie.
4. Pour spécifier le format de la nouvelle expression, effectuez l'une des opérations suivantes :
   a) Pour spécifier que vous souhaitez configurer une expression de stratégie dans la zone Règle, cliquez sur Syntaxe classique.
   b) Pour spécifier que vous souhaitez configurer une expression avancée dans la zone Règle, cliquez sur Stratégie avancée.
   c) Dans la zone Règle, configurez l'expression.
5. Cliquez sur **OK**.

Configuration des règles d'unité d'application

June 23, 2022

Vous souhaiterez peut-être configurer une règle d'unité d'application pour inclure ou exclure certains types de trafic. Lorsque vous configurez la règle, vous pouvez également définir la syntaxe de l'expression.

Pour configurer une règle d'unité d'application :

1. Dans le volet de navigation de l'interface graphique, développez AppExpert, puis cliquez sur **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit de la souris sur l'unité d'application pour laquelle vous souhaitez modifier la règle, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue Configurer l'unité d'application, procédez comme suit :
   a) Pour spécifier le format de la nouvelle expression, effectuez l'une des opérations suivantes :
      - Pour spécifier que vous souhaitez configurer une expression de stratégie avancée dans la zone Règle, cliquez sur **Syntaxe classique**.
      - Pour spécifier que vous souhaitez configurer une expression avancée dans la zone Règle, cliquez sur **Stratégie avancée**.
   b) Dans la zone Règle, configurez l'expression.
4. Cliquez sur **OK**.

Configuration des stratégies pour les unités d'application

June 23, 2022

Pour une application AppExpert, vous pouvez configurer des stratégies de compression, de mise en cache, de réécriture, de répondeur et de pare-feu d'application. Les modèles que vous téléchargez à partir du site Web de la Citrix Community vous fournissent un ensemble de stratégies qui répondent aux exigences de gestion des applications les plus courantes. Vous souhaiterez peut-être peaufiner ou personnaliser ces stratégies. Si l'ensemble de stratégies fourni pour une unité d'application donnée n'inclut pas de stratégies pour une fonctionnalité particulière, vous pouvez créer et lier vos propres stratégies pour cette fonctionnalité.

Si vous créez une application AppExpert sans utiliser de modèle, vous devez configurer toutes les stratégies dont l'application Web a besoin.

L'interface graphique utilise diverses icônes pour indiquer si des stratégies sont configurées pour une fonctionnalité. Pour une unité d'application, si une stratégie est configurée pour une fonctionnalité donnée, une icône représentant la fonctionnalité s'affiche. Par exemple, si une stratégie de compression est configurée pour une unité d'application, une icône de compression s'affiche dans la colonne Compression de l'unité d'application. Pour les fonctionnalités pour lesquelles aucune stratégie n'est configurée, une icône représentant un signe plus (+) s'affiche.

Remarque : Lorsque vous configurez des stratégies pour les unités d'application, vous devrez peut-être configurer des stratégies et des expressions qui se trouvent dans la stratégie classique ou avancée. En outre, lorsque vous configurez des stratégies de stratégie avancées, vous devrez peut-être spécifier des paramètres tels que les expressions Goto et invoquer des banques de stratégies.

Pour plus d'informations sur la configuration des stratégies et des expressions dans les deux formats, voir Stratégies et expressions.

Configuration des stratégies de compression

Vous pouvez utiliser des stratégies classiques ou avancées pour configurer la compression, mais vous ne pouvez pas lier des stratégies de compression des deux types à la même unité d'application.

Pour configurer une stratégie de compression pour une unité d'application, procédez comme suit :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne Compression.
3. Dans la boîte de dialogue Configurer les stratégies de compression, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :
    - Cliquez sur Basculer vers la stratégie avancée si vous souhaitez configurer une stratégie de compression de stratégie avancée. Si vous souhaitez lier ou configurer des stratégies de compression classiques, et si vous êtes dans la vue des stratégies avancées, vous pouvez cliquer sur Basculer vers la syntaxe classique pour revenir à la vue de stratégie classique et

commencer à modifier les stratégies classiques liées ou créer et lier de nouvelles stratégies de compression classiques.

Important : Ce paramètre détermine également les stratégies qui s'affichent lorsque vous souhaitez insérer une stratégie. Par exemple, si vous êtes dans la vue des stratégies avancées, lorsque vous cliquez sur Insérer une stratégie, la liste qui apparaît dans la colonne Nom de la stratégie inclut uniquement les stratégies de stratégie avancées. Vous ne pouvez pas lier des stratégies des deux types à une unité d'application.

- Si vous souhaitez configurer des stratégies classiques, cliquez sur Demande ou Réponse, selon que vous souhaitez que la stratégie soit évaluée au moment de la demande ou au moment de la réponse.

  Vous pouvez configurer des stratégies de compression classiques de temps de demande et de temps de réponse pour une unité d'application. Après avoir évalué toutes les stratégies de temps de demande, si aucune correspondance n'est trouvée, l'appliance évalue les stratégies de temps de réponse.
- Pour modifier une stratégie de compression déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur Modifier la stratégie. Ensuite, dans la boîte de dialogue Configurer la stratégie de compression, modifiez la stratégie, puis cliquez sur OK.

  Pour plus d'informations sur la modification d'une stratégie de compression, voir Compression.
- Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur Délier la stratégie.
- Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
- Pour régénérer les priorités affectées, cliquez sur Régénérer les priorités.
- Pour insérer une nouvelle stratégie, cliquez sur **Insérer une stratégie** et, dans la liste affichée dans la colonne Nom de la stratégie, cliquez sur **Nouvelle stratégie**. Ensuite, dans la boîte de dialogue Créer une stratégie de compression, configurez la stratégie, puis cliquez sur **Créer**.

  Pour plus d'informations sur la modification d'une stratégie de compression, voir Compression.
- Si vous configurez une expression de stratégie avancée, procédez comme suit :
  - Dans la colonne Expression Goto, sélectionnez une expression Goto.
  - Dans la colonne Invoke (Invoke), spécifiez la banque de stratégies que vous souhaitez appeler si la stratégie actuelle est évaluée à TRUE.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies de mise en cache

Vous ne pouvez utiliser que des stratégies et expressions avancées pour configurer les stratégies de mise en cache.

Pour configurer les stratégies de mise en cache pour une unité d'application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne Mise en cache.
3. Dans la boîte de dialogue Configurer les stratégies de cache, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :
   - Cliquez sur Demande ou Réponse, selon que vous souhaitez que la stratégie soit évaluée au moment de la demande ou au moment de la réponse.
     Vous pouvez configurer des stratégies de mise en cache de temps de demande et de temps de réponse pour une unité d'application. Après avoir évalué toutes les stratégies de temps de demande, si aucune correspondance n'est trouvée, l'appliance évalue les stratégies de temps de réponse.
   - Pour modifier une stratégie de mise en cache déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur Modifier la stratégie. Ensuite, dans la boîte de dialogue **Configurer la stratégie de cache**, modifiez la stratégie, puis cliquez sur **OK** .
     Pour plus d'informations sur la modification d'une stratégie de mise en cache, reportez-vous à la section Mise en cache intégrée.
   - Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur **Délier la stratégie**.
   - Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
   - Pour régénérer les priorités attribuées, cliquez sur **Régénérer les priorités**.
   - Pour insérer une nouvelle stratégie, cliquez sur **Insérer une stratégie** et, dans la liste affichée dans la colonne Nom de la stratégie, cliquez sur **Nouvelle stratégie**. Ensuite, dans la boîte de dialogue **Créer une stratégie de cache**, configurez la stratégie, puis cliquez sur **Créer** .
     Pour plus d'informations sur la modification d'une stratégie de mise en cache, reportez-vous à la section Mise en cache intégrée.
   - Dans la colonne Expression Goto, sélectionnez une expression Goto.
   - Dans la colonne Invoke (Invoke), spécifiez la banque de stratégies que vous souhaitez appeler si la stratégie actuelle est évaluée à TRUE.
4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies de réécriture

Vous ne pouvez utiliser que des stratégies et expressions avancées pour configurer des stratégies de réécriture.

Pour configurer des stratégies de réécriture pour une unité d'application, procédez comme suit :

1. Accédez à **AppExpert** > **Applications**.

2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne Réécriture.
3. Dans la boîte de dialogue **Configurer les stratégies de réécriture**, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :
   - Cliquez sur Demande ou Réponse, selon que vous souhaitez que la stratégie soit évaluée au moment de la demande ou au moment de la réponse.
     Vous pouvez configurer des stratégies de réécriture en temps de demande et en temps de réponse pour une unité d'application. Après avoir évalué toutes les stratégies de temps de demande, si aucune correspondance n'est trouvée, l'appliance évalue les stratégies de temps de réponse.
   - Pour modifier une stratégie de réécriture déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur **Modifier la stratégie**. Ensuite, dans la boîte de dialogue Configurer la stratégie de réécriture, modifiez la stratégie, puis cliquez sur **OK**.
     Pour plus d'informations sur la modification d'une stratégie de réécriture, voir Réécriture.
   - Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur **Délier la stratégie**.
   - Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
   - Pour régénérer les priorités attribuées, cliquez sur **Régénérer les priorités**.
   - Pour insérer une nouvelle stratégie, cliquez sur **Insérer une stratégie** et, dans la liste qui s'affiche dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie.** Ensuite, dans la boîte de dialogue **Créer une stratégie de réécriture**, configurez la stratégie, puis cliquez sur **Créer** .
     Pour plus d'informations sur la modification d'une stratégie de réécriture, voir Réécriture.
   - Dans la colonne Expression Goto, sélectionnez une expression Goto.
   - Dans la colonne Invoke (Invoke), spécifiez la banque de stratégies que vous souhaitez appeler si la stratégie actuelle est évaluée à TRUE.
4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies de répondeur

Vous ne pouvez utiliser que des stratégies et expressions avancées pour configurer les stratégies de répondeur.

Pour configurer les stratégies de répondeur pour une unité d'application, procédez comme suit :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne Répondeur.
3. Dans la boîte de dialogue **Configurer les stratégies de répondeur**, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :

- Pour modifier une stratégie de filtre déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur **Modifier la stratégie**. Ensuite, dans la boîte de dialogue Configurer la stratégie de répondeur, modifiez la stratégie, puis cliquez sur **OK**.
  Pour plus d'informations sur la modification d'une stratégie de répondeur, voir Répondeur.
- Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur **Délier la stratégie**.
- Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
- Pour régénérer les priorités attribuées, cliquez sur **Régénérer les priorités**.
- Pour insérer une nouvelle stratégie, cliquez sur Insérer une stratégie et, dans la liste qui s'affiche dans la colonne Nom de la stratégie, cliquez sur Nouvelle stratégie. Ensuite, dans la boîte de dialogue Créer une stratégie de répondeur, configurez la stratégie, puis cliquez sur Créer.
  Pour plus d'informations sur la modification d'une stratégie de répondeur, voir Répondeur.
- Dans la colonne Expression Goto, sélectionnez une expression Goto.
- Dans la colonne Invoke (Invoke), spécifiez la banque de stratégies que vous souhaitez appeler si la stratégie actuelle est évaluée à TRUE.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des stratégies de pare-feu d'application

Vous pouvez configurer des stratégies et expressions classiques et avancées pour le pare-feu d'application. Toutefois, si une stratégie d'un type est déjà liée globalement ou à un serveur virtuel configuré sur l'appliance, vous ne pouvez pas lier une stratégie de l'autre type à une unité d'application. Par exemple, si une stratégie avancée est déjà liée globalement ou à un serveur virtuel, vous ne pouvez pas lier une stratégie classique à une unité d'application.

Pour configurer des stratégies de pare-feu d'application pour une unité d'application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, dans la ligne de l'unité d'application que vous souhaitez configurer, cliquez sur l'icône fournie dans la colonne **Pare-feu d'application** .
3. Dans la boîte de dialogue **Configurer les stratégies de pare-feu d'application**, effectuez une ou plusieurs des opérations suivantes, en fonction des tâches de configuration que vous souhaitez effectuer :
   - Cliquez sur Expression classique ou Expression avancée en fonction du type d'expression que vous souhaitez configurer pour la stratégie de pare-feu d'application.
     Important : Ce paramètre détermine également les stratégies affichées lorsque vous souhaitez insérer une stratégie. Par exemple, si vous sélectionnez Expression avancée,

lorsque vous cliquez sur **Insérer une stratégie**, la liste qui apparaît dans la colonne **Nom de la stratégie** inclut uniquement les stratégies de stratégie avancées. Vous ne pouvez pas lier des stratégies des deux types à une unité d'application. Cette option n'est pas disponible si une stratégie de l'un ou l'autre type est déjà liée globalement ou à un serveur virtuel.

- Pour modifier une stratégie de pare-feu d'application déjà liée à l'unité d'application, cliquez sur le nom de la stratégie, puis sur Modifier la stratégie. Ensuite, dans la boîte de dialogue Configurer la stratégie de pare-feu d'application, modifiez la stratégie, puis cliquez sur OK.
  Pour plus d'informations sur la modification d'une stratégie de pare-feu d'application, voir Stratégies.
- Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur Délier la stratégie.
- Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
- Pour régénérer les priorités affectées, cliquez sur Régénérer les priorités.
- Pour insérer une nouvelle stratégie, cliquez sur **Insérer une stratégie** et, dans la liste affichée dans la colonne **Nom de la stratégie**, cliquez sur Nouvelle stratégie. Ensuite, dans la boîte de dialogue **Créer une stratégie de pare-feu d'application**, configurez la stratégie, puis cliquez sur **Créer** .
  Pour plus d'informations sur la modification d'une stratégie de pare-feu d'application, voir Stratégies.

4. Cliquez sur **Appliquer les modifications**, puis cliquez sur **Fermer**.

Configuration des unités d'application

May 5, 2023

Pour configurer une unité d'application à l'aide de l'interface utilisateur graphique :

1. Accédez à la section **AppExpert** > **Applications** > **Unité d'application**, puis cliquez sur l'icône plus pour ajouter une nouvelle unité d'application pour un sous-ensemble de trafic.
2. Dans le curseur **Unité d'application**, définissez les paramètres suivants :
   - Nom
   - Expression

   Vous pouvez insérer une expression en ajoutant les composants de l'expression manuellement ou en utilisant le lien Éditeur d'expression. Pour ajouter manuellement une expression, entrez un composant de sélection, puis tapez un point (.) pour afficher une liste dans laquelle vous

pouvez sélectionner le composant suivant. Par exemple, tapez HTTP, puis saisissez un point. Un menu déroulant apparaît. Le contenu de ce menu fournit les mots-clés qui peuvent suivre le mot-clé initial que vous avez saisi. Sélectionnez un composant dans le menu déroulant. La zone de texte Expression* affiche désormais les composants que vous avez ajoutés à l'expression (par exemple, HTTP.REQ). Continuez à ajouter des composants jusqu'à ce que l'expression complète soit formée.

Si vous préférez obtenir de l'aide pour créer l'expression, vous pouvez utiliser le lien Editeur d'expression. Sur la page Éditeur d'expression, vous pouvez créer une expression en sélectionnant des composants dans les zones déroulantes. Sélectionnez les composants et cliquez sur Terminé pour insérer l'expression dans la page Unité d'application.

3. Cliquez sur **Continuer** pour lier les services et les groupes de services.
4. Cliquez sur la section **Service** pour sélectionner ou ajouter un service virtuel et le lier à l'unité d'application.
5. Cliquez sur **Continuer**, puis sur la section **Groupe de services** pour sélectionner ou ajouter un groupe de services virtuel et le lier à l'unité d'application.
6. Cliquez sur **Lier** et **continuer** pour configurer les paramètres avancés (tels que les stratégies, la méthode, la persistance, la protection, les profils, la transmission, l'authentification et les paramètres de trafic) pour l'unité d'application.
7. Cliquez sur l'icône **plus** dans chaque section pour définir les paramètres de configuration.
8. Cliquez sur **OK**, puis sur **Terminé**.

Pour modifier une unité d'application pour une application à l'aide de l'interface utilisateur graphique :

Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier**. Dans la section **Unité d'application**, sélectionnez une entité, cliquez sur l'icône Modifier et modifiez les paramètres de l'unité d'application.

Remarque : Vous ne pouvez pas modifier le nom et l'expression de règle d'une unité d'application existante.

Les didacticiels vidéo de NetScaler vous permettent de comprendre les fonctionnalités de NetScaler de manière simple et facile. Regardez la https://www.youtube.com/watch?v=bJ5_i8fV2hc vidéo pour découvrir comment configurer une unité d'application.

Configuration de points de terminaison publics pour une application

May 5, 2023

Pour configurer des points de terminaison publics pour une application à l'aide de l'interface utilisateur graphique :

1. Accédez à **AppExpert** > **Applications**, sélectionnez une entité d'application, puis cliquez sur **Modifier**.
2. Dans la section **Public Endpoint**, cliquez sur **+** pour configurer un nouveau point de terminaison public.
3. Dans le curseur **Public Endpoint**, effectuez l'une des opérations suivantes :
   a) Cliquez sur **Nouveau** pour créer un nouveau point de terminaison.
   b) Cliquez sur **Endpoint public existant** pour sélectionner un point de terminaison dans la liste déroulante.
4. Définissez les paramètres de point de terminaison suivants :
   a) Nom
   b) Adresse IP
   c) Protocole
   d) Port
5. Cliquez sur **Continuer** pour configurer des paramètres supplémentaires tels que les unités d'application, les liaisons de serveur GSLB, les stratégies, les profils, les push, les paramètres de trafic et l'authentification.
6. Cliquez sur **OK**, puis sur **Terminé**.
7. Cliquez sur **Continuer**, puis **Terminé**.

Pour modifier un point de terminaison public pour une application à l'aide de l'interface utilisateur graphique :

Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier**. Dans la section **Point de terminaison public**, sélectionnez un point de terminaison, cliquez sur l'icône en forme de stylo et modifiez les paramètres du point de terminaison.

Pour supprimer un point de terminaison public pour une application à l'aide de l'interface utilisateur graphique :

Accédez à **AppExpert** > **Applications** > **Public Endpoint,** cliquez sur l'icône en forme de stylo pour afficher l'icône de suppression en regard de l'entité.

Les didacticiels vidéo de NetScaler vous permettent de comprendre les fonctionnalités de NetScaler de manière simple et facile. Regardez la https://www.youtube.com/watch?v=z4v-edQiVpw vidéo pour savoir comment configurer un point de terminaison public.

Spécification de l'ordre d'évaluation des unités d'application

June 23, 2022

Les règles d'unité d'application sont évaluées dans l'ordre dans lequel elles sont placées dans l'interface utilisateur graphique. La règle configurée pour l'unité d'application la plus haute est toujours configurée en premier, suivie de la règle configurée pour la deuxième unité d'application la plus haute, et ainsi de suite. L'unité d'application par défaut est toujours évaluée en dernier.

Lorsqu'une demande correspond à la règle configurée pour une unité d'application, la demande est traitée par l'unité d'application et aucune autre correspondance n'est effectuée. Par conséquent, l'ordre d'évaluation des unités d'application devient un facteur important si les sous-ensembles de trafic pour deux unités d'application ou plus se chevauchent. Si les sous-ensembles de trafic pour deux unités d'application ou plus se chevauchent, vous devez spécifier l'ordre dans lequel une demande entrante est mise en correspondance avec les règles d'unité d'application.

Pour spécifier l'ordre d'évaluation des unités d'application :

1. Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier**. Dans la section **Unité d'application**, cliquez sur l'icône en forme de **crayon**, puis placez le curseur sur la case à cocher située à gauche du nom de l'unité d'application. Cliquez sur l'icône qui apparaît en regard de la case à cocher et maintenez la souris enfoncée pour faire glisser l'application vers le haut ou vers le bas vers un nouvel emplacement dans la liste des priorités.

Configuration de groupes de persistance pour les unités d'application

May 5, 2023

Vous pouvez configurer un groupe de persistance pour les unités de l'application dans une application AppExpert. Dans le contexte d'une application AppExpert, un groupe de persistance est un groupe d'unités d'application que vous pouvez traiter comme une entité unique dans le but d'appliquer des paramètres de persistance courants. Lorsque l'application est exportée vers un fichier de modèle d'application, les paramètres du groupe de persistance sont inclus et ils sont automatiquement appliqués aux unités de l'application lorsque vous importez l'application AppExpert.

Pour configurer un groupe de persistance pour une application à l'aide de l'interface utilisateur graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans la boîte de dialogue **Affichage des applications**, cliquez sur le nom de l'application pour laquelle vous souhaitez configurer un groupe de persistance, puis cliquez sur Configurer les **groupes de persistance**.
3. Dans la boîte de dialogue **Configurer les groupes de persistance**, effectuez l'une des opérations suivantes :
    - Pour ajouter un groupe de persistance, cliquez sur **Ajouter**.
    - Pour modifier un groupe de persistance, cliquez sur **Ouvrir**.

4. Dans la boîte de dialogue **Créer un groupe** de **persistance ou Configurer un groupe** de persistance, définissez les paramètres suivants :
   - Nom du groupe : nom du groupe de persistance. Pour que l'appliance NetScaler reconnaisse le groupe de persistance dans le cadre de la configuration de l'application, le nom de l'application AppExpert doit être inclus dans le nom du groupe de persistance, sous forme de préfixe. Par conséquent, par défaut, l'appliance affiche le préfixe dans la zone Nom du groupe, et vous ne pouvez pas supprimer ce préfixe. Entrez le nom de votre choix après le préfixe.
   - Persistance : type de persistance pour le serveur virtuel. Si vous sélectionnez SOURCEIP, dans la zone Masque réseau IPv4, entrez un masque réseau qui spécifie le nombre de bits que l'appliance doit prendre en compte lors de la création de sessions de persistance. Si vous sélectionnez COOKIEINSERT, dans les zones Domaine du cookie et Nom du cookie, spécifiez un attribut de domaine à envoyer dans la directive Set-Cookie, et un nom pour le cookie, respectivement.
   - Timeout : période pendant laquelle une session de persistance est en vigueur.
   - Persistance de sauvegarde : type de persistance de sauvegarde pour le groupe.
   - Backup Timeout : période, en minutes, pendant laquelle la persistance des sauvegardes est en vigueur.
   - Unités d'application : pour ajouter une unité d'application au groupe de persistance, dans la zone Unités d'application disponibles, cliquez sur l'unité d'application, puis sur Ajouter. Pour supprimer une unité d'application du groupe de persistance, dans la zone Unités d'application configurées, cliquez sur l'unité d'application, puis sur **Supprimer**.
5. Cliquez sur **OK**.

Affichage des applications AppExpert et configuration des entités à l'aide du visualiseur d'applications

June 23, 2022

La fonction Visualizer vous montre une représentation graphique de la configuration d'une application. Il inclut le nom du point de terminaison public, les unités d'application attribuées au point de terminaison public et le nombre de stratégies et de services liés à l'application. Vous pouvez utiliser le visualiseur pour obtenir un aperçu visuel de la configuration d'une application AppExpert et configurer certaines des entités affichées. Par défaut, le visualiseur affiche les unités d'application, les services et les moniteurs pour l'application sélectionnée.

Pour afficher une application AppExpert à l'aide du visualiseur d'applications :

1. Accédez à **AppExpert** > **Applications**, sélectionnez une entité d'application et cliquez sur **Visualizer**.

Configuration de l'authentification, de l'autorisation et de l'audit utilisateur

June 23, 2022

Vous pouvez configurer l'autorisation pour les utilisateurs et les groupes afin de leur permettre d'accéder à une application AppExpert. Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer des autorisations n'a pas encore été créé, vous pouvez le créer à partir d'AppExpert, puis configurer les autorisations pour l'accès aux applications.

Pour configurer des utilisateurs AAA et des groupes d'utilisateurs AAA pour une application à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Applications**, sélectionnez une entité d'application, puis cliquez sur **Modifier**.
2. Dans la section **Paramètres avancés**, cliquez sur **Autorisation**et configurez les utilisateurs et les groupes d'utilisateurs autorisés.
3. Cliquez sur la section Utilisateur **AAA** pour lier les utilisateurs autorisés à l'application.
4. Dans le curseur **Utilisateur AAA**, définissez les paramètres.
5. Cliquez sur **Continuer**, puis sur **Stratégies d'autorisation** dans la section **Paramètres avancés** .
6. Dans le curseur **Stratégie d'autorisation**, liez une stratégie d'autorisation à l'application.
7. Cliquez sur **Continuer**, puis sur la section **Groupe d'autorisation** dans la section **Paramètres avancés** .
8. Dans le curseur **Liaison de groupe AAA**, liez un groupe d'utilisateurs d'autorisation à l'application.
9. Cliquez sur **Continuer**, puis sur **Stratégies** dans la section **Paramètres avancés** .
10. Dans le curseur **Stratégies**, liez une stratégie **Audit Syslog** ou **Audit NSLog** à l'application.
11. Cliquez sur **Continuer**, puis **Terminé**.

Pour modifier les utilisateurs AAA et les groupes d'utilisateurs AAA pour une application à l'aide de l'interface utilisateur graphique :

Accédez à **AppExpert** > **Applications** > **Paramètres avancés** et cliquez sur **Autorisation**. Cliquez ensuite sur l'icône Modifier et spécifiez des valeurs pour les paramètres d'autorisation de l'utilisateur ou du groupe d'utilisateurs.

Pour supprimer des utilisateurs AAA et des groupes d'utilisateurs AAA à l'aide de l'interface utilisateur graphique :

Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier**. Dans la page **Applications**, cliquez sur **Paramètres avancés**, puis sur **Autorisation**. Cliquez sur l'icône Supprimer en regard de l'entité.

Surveillance d'une application NetScaler

May 5, 2023

Après avoir personnalisé l'application AppExpert, vous pouvez afficher les statistiques de l'application pour vous assurer que l'application et toutes ses entités fonctionnent correctement. Vous pouvez également utiliser le visualiseur d'applications pour surveiller les statistiques associées à certaines entités telles que les stratégies et les serveurs virtuels.

Vous pouvez également afficher les compteurs de succès de différentes entités à intervalles réguliers pour vous assurer que les compteurs sont mis à jour.

Afficher les statistiques des applications

Dans le nœud **Applications**, vous pouvez sélectionner une application et afficher la page Statistiques de l'application. Sur la page Statistiques, vous pouvez surveiller l'état et l'état des terminaux publics et des unités d'application, et afficher les informations statistiques suivantes :

- Demandes et réponses par seconde pour chacun des points de terminaison publics et unités d'application.
- Octets par seconde, à chaque point de terminaison, pour le trafic entrant et sortant.
- Compteurs d'accès des unités d'application et nombre de connexions client et serveur pour chaque unité d'application.
- Statistiques pour les services liés aux unités de l'application.

Sur la page Statistiques, vous pouvez également afficher l'utilisation du processeur, l'utilisation de la mémoire et les journaux système.

Pour consulter les statistiques d'une application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez sur l'application pour laquelle vous souhaitez afficher les statistiques, puis cliquez sur **Statistiques**.

Surveillance d'une application à l'aide du visualiseur d'applications

Vous pouvez utiliser le visualiseur d'application pour surveiller le nombre de requêtes reçues par seconde à un moment donné par les serveurs virtuels et le nombre d'accès par seconde à un moment donné pour les stratégies de réécriture, de réponse et de cache.

Pour afficher des informations statistiques sur les serveurs virtuels, les stratégies de réécriture, les stratégies de répondeur et les stratégies de cache dans le visualiseur :

1. Accédez à **AppExpert** > **Applications**.

2. Dans le volet de détails, sélectionnez l'application pour laquelle vous souhaitez afficher des informations statistiques, puis cliquez sur **Visualizer**.
3. Dans la fenêtre **Application Visualizer**, procédez comme suit :
    - Pour afficher les statistiques, cliquez sur **Afficher les statistiques**.
      Les informations statistiques sont affichées sur les nœuds respectifs du visualiseur. Ces informations ne sont pas mises à jour en temps réel et doivent être actualisées manuellement.
    - Pour actualiser les informations statistiques, cliquez sur **Actualiser les statistiques**.

Affichage des hits

Les compteurs d'accès fournis pour diverses entités d'application AppExpert vous permettent de surveiller le fonctionnement des points de terminaison publics et des unités d'application. Pour une application, la boîte de dialogue Hits affiche le nombre total de demandes reçues par chaque point de terminaison public configuré. Pour une unité d'application, la boîte de dialogue Résultats affiche le nombre de demandes traitées par l'unité d'application à partir de chacun des points de terminaison publics et le nombre total d'appels. Pour obtenir des instructions sur l'affichage des compteurs d'accès, reportez-vous à la section Vérification et test de la configuration.

Supprimer une application

June 23, 2022

Si vous n'avez plus besoin d'une application et de ses unités d'application, vous pouvez la supprimer. Lorsque vous supprimez une application AppExpert, les services backend ne sont pas supprimés et tous les points de terminaison publics utilisés par l'application deviennent disponibles pour être utilisés par d'autres applications.

Lorsque vous supprimez une application, vous êtes également invité à indiquer si vous souhaitez supprimer les stratégies et actions liées qui ne sont pas utilisées ailleurs.

Pour supprimer une unité d'application pour une application à l'aide de l'interface utilisateur graphique :

Accédez à **AppExpert** > **Applications**, sélectionnez une application et cliquez sur **Modifier**. Dans la section **Unité d'application**, cliquez sur l'icône Supprimer en regard de l'entité

Configuration de l'authentification, de l'autorisation et de l'audit des applications

June 23, 2022

Vous pouvez configurer Authentification, autorisation et audit (AAA) pour les applications que vous configurez sur l'appliance. Une stratégie d'authentification configurée pour une application définit le type d'authentification à appliquer lorsqu'un utilisateur ou un groupe tente d'accéder à l'application. Si l'authentification externe est utilisée, la stratégie spécifie également le serveur d'authentification externe. Les stratégies d'autorisation configurées pour une application spécifient si un utilisateur ou un groupe spécifique peut accéder à l'application. Les stratégies d'audit définissent le type de journal d'audit, le niveau auquel la journalisation est effectuée et d'autres paramètres du serveur d'audit. Les stratégies d'authentification et d'audit utilisent le format de stratégie classique.

Les stratégies d'authentification, d'autorisation et d'audit peuvent être configurées dans n'importe quel ordre. Toutefois, avant de configurer AAA pour une application, vous devez configurer un point de terminaison public pour l'application.

La configuration de l'authentification pour une application implique la spécification d'un nom de domaine complet d'authentification, d'un serveur virtuel d'authentification, d'un certificat de serveur et de stratégies d'authentification et de session. Les stratégies d'authentification sont automatiquement liées au serveur virtuel d'authentification spécifié pour l'application.

Pour configurer l'authentification pour une application AppExpert :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   a) Cliquez sur Ajouter pour ajouter une authentification pour une nouvelle application.
   b) Cliquez sur Modifier pour modifier une application existante.
3. Sur la page **Applications**, sélectionnez une unité d'application.
4. Dans la page du curseur **Unité d'application**, cliquez sur Authentification dans la section **Paramètres avancés** .
5. Dans la section **Authentification**, sélectionnez le type d'authentification comme suit :
   a) Authentification par formulaire
   b) Authentification basée sur 401
   c) Aucun
6. Cliquez sur **OK**, puis sur **Terminé**.

Configurer l'autorisation des applications

Vous pouvez configurer l'autorisation pour les utilisateurs et les groupes afin de leur permettre d'accéder à une application AppExpert. Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez

configurer des autorisations n'a pas encore été créé, vous pouvez le créer à partir d'AppExpert, puis configurer les autorisations pour l'accès aux applications.

Pour configurer les autorisations permettant à un utilisateur ou à un groupe AAA d'accéder à une application AppExpert :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez sur l'application AppExpert pour laquelle vous souhaitez configurer l'accès d'un utilisateur ou d'un groupe.
3. Dans la page **Applications**, puis cliquez sur Autorisation dans la section **Paramètres avancés** .
4. Procédez comme suit :
    - Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer des autorisations se trouve déjà dans l'arborescence Groups/Users, faites glisser l'utilisateur ou le groupe de l'arborescence Groups/Users vers le nœud Users or Groups dans l'arborescence des applications. Cliquez ensuite avec le bouton droit sur l'utilisateur ou le groupe et cliquez sur Autoriser
    - Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer des autorisations n'est pas configuré sur l'appliance, dans l'arborescence des applications, cliquez avec le bouton droit sur Utilisateurs ou Groupes, puis cliquez sur Ajouter. Dans la boîte de dialogue Créer un groupe AAA ou Créer un utilisateur AAA, renseignez les valeurs, cliquez sur Créer, puis sur Fermer.
      L'utilisateur ou le groupe est créé avec l'autorisation définie sur Autoriser. Pour modifier le paramètre d'autorisation, cliquez avec le bouton droit sur le groupe ou l'utilisateur, puis cliquez sur le paramètre d'autorisation.
5. Cliquez sur **Terminé**, puis cliquez sur **Fermer**.

Configurer l'audit des applications

Lorsque vous configurez des stratégies d'audit pour une application, vous devez spécifier le serveur vers lequel les messages de journal doivent être dirigés, le format des messages enregistrés et le niveau de journalisation. Vous pouvez éventuellement configurer d'autres paramètres, tels que la fonction de journalisation et le format de date. Les stratégies d'audit sont automatiquement liées à tous les points de terminaison publics de l'application AppExpert.

Pour configurer les stratégies d'audit pour une application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez sur l'application pour laquelle vous souhaitez configurer les stratégies d'audit.
3. Dans la page du curseur Unité d'application, cliquez sur l'icône+dans la section **Stratégies** pour configurer les stratégies d'audit.

4. Dans la page du curseur **Stratégies**, sélectionnez le type de stratégie Audit Syslog ou Audit Nslog et cliquez sur **Continuer**.
5. Dans la section Liaison de stratégie, définissez les paramètres suivants.
   a) Sélectionnez une stratégie pour la liaison. Si vous n'avez pas de stratégie de liaison, cliquez sur + pour créer une nouvelle stratégie.
   b) Pour créer une nouvelle stratégie d'audit, sous Nom de la stratégie, cliquez sur **Nouvelle stratégie,** puis, dans la page **Stratégie**, procédez comme suit :
      i. Dans la zone Nom, tapez le nom de la stratégie.
      ii. La zone Nom contient déjà la chaîne requise au début du nom du serveur. Vous ne pouvez pas modifier la chaîne.
      iii. Dans la liste Type d'audit, sélectionnez le type d'audit (SYSLOG ou NSLOG).
      iv. Si le serveur d'audit que vous souhaitez spécifier figure déjà dans la liste des serveurs, sélectionnez-le dans la liste, puis, si vous souhaitez modifier les paramètres du serveur, cliquez sur Modifier. Dans la boîte de dialogue Configurer le serveur d'audit, modifiez les paramètres le cas échéant, puis cliquez sur OK. Pour plus d'informations sur les paramètres de la boîte de dialogue Configurer le serveur d'Auditing, consultez Audit des sessions authentifiées.
      v. Si vous souhaitez configurer un nouveau serveur d'audit, cliquez sur Nouveau, puis, dans la boîte de dialogue Créer un serveur d'audit, tapez un nom pour le serveur, spécifiez l'adresse IP du serveur, le numéro de port et les autres paramètres appropriés. Lorsque vous avez terminé, cliquez sur **OK**.
      vi. Cliquez sur **Créer**.
   c) Pour modifier les priorités des nouvelles stratégies d'audit que vous avez créées, sous Priorité, pour chaque stratégie dont vous souhaitez modifier la priorité, double-cliquez sur la valeur de priorité et saisissez une nouvelle valeur de priorité.
   d) Pour régénérer les priorités, cliquez sur **Régénérer les priorités**.
   e) Pour délier une stratégie, cliquez sur la stratégie, puis cliquez sur **Délier la stratégie**.
   f) Pour modifier une stratégie, cliquez sur la stratégie, puis sur **Modifier la stratégie.**
6. Cliquez sur **Appliquer les modifications,** puis sur **Fermer**.

Désactiver AAA pour une application

Après avoir configuré AAA pour une application, vous pouvez désactiver la configuration AAA pour cette application. Lorsque vous désactivez AAA pour une application, la configuration n'est pas perdue. Vous pouvez activer AAA pour l'application lorsque vous souhaitez réappliquer la configuration.

Pour activer ou désactiver AAA pour une application :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez sur l'application pour laquelle vous souhaitez activer ou désactiver AAA, puis effectuez l'une des opérations suivantes :

3. Pour désactiver AAA pour l'application, cliquez sur **Désactiver AAA.**
4. Pour activer AAA pour l'application, cliquez **sur Activer AAA**.

Configuration d'une application NetScaler personnalisée

May 5, 2023

Si aucun modèle d'application AppExpert n'est disponible pour l'application Web que vous souhaitez gérer via l'appliance NetScaler, ou si les modèles d'application AppExpert disponibles ne répondent pas à vos besoins, vous pouvez créer une application AppExpert sans modèle.

Pour créer une application AppExpert sans modèle, vous devez d'abord créer une application et des unités d'application. Ensuite, vous configurez les points de terminaison publics, les services et les groupes de services. Enfin, vous configurez les stratégies qui déterminent la façon dont le trafic des applications est évalué et traité.

Après avoir créé l'application et les unités d'application et configuré les stratégies, vous devez vérifier la configuration et la tester pour vous assurer qu'elle fonctionne correctement, comme vous le feriez lorsque vous configurez une application à l'aide d'un modèle d'application AppExpert prédéfini. Ensuite, vous devez surveiller l'application pour vous assurer que l'application et ses entités fonctionnent correctement.

Création d'une application

Lorsque vous créez une application AppExpert, l'appliance crée un conteneur auquel vous pouvez ajouter des unités d'application. L'unité d'application par défaut n'est pas créée tant que vous n'avez pas créé la première unité d'application.

Pour créer une application AppExpert à l'aide de l'interface utilisateur graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez avec le bouton droit sur **Applications**, puis cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une application**, dans Nom, entrez un nom pour l'application, puis cliquez sur **OK**.

Création d'unités d'application

Pour chaque sous-ensemble de trafic associé à votre application Web, vous devez créer une unité d'application.

Pour créer une unité d'application pour l'application AppExpert à l'aide de l'interface utilisateur graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet d'informations, cliquez avec le bouton droit de la souris sur l'application pour laquelle vous souhaitez ajouter une unité d'application, puis cliquez sur **Ajouter**.
3. Cliquez sur **Create**.

Configuration de points de terminaison publics pour une application AppExpert

Après avoir créé toutes les unités d'application dont vous avez besoin, vous devez configurer un ou plusieurs points de terminaison publics pour permettre aux clients d'accéder à l'application Web via l'appliance NetScaler.

Pour configurer des points de terminaison publics pour une application AppExpert à l'aide de l'interface utilisateur graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez avec le bouton droit sur l'application pour laquelle vous souhaitez configurer des points de terminaison publics, puis cliquez sur **Configurer les points de terminaison publics**.
3. Dans la boîte de dialogue Choisir les points de terminaison publics de l'application, effectuez l'une des opérations suivantes :
   - Si les points de terminaison souhaités sont répertoriés dans la boîte de dialogue, cliquez sur les cases à cocher correspondantes.
   - Si vous souhaitez spécifier tous les points de terminaison publics, cliquez sur **Activer tout**.
   - Si vous souhaitez dissocier les points de terminaison de l'application AppExpert, désactivez les cases à cocher correspondantes.
   - Si vous souhaitez créer un nouveau point de terminaison public, cliquez sur **Ajouter**. Ensuite, dans la boîte de dialogue Créer un point de terminaison public, configurez les paramètres du point de terminaison, puis cliquez sur **OK**.
     Dans la boîte de dialogue **Créer un point de terminaison public**, vous ne pouvez spécifier que le nom, l'adresse IP, le port et le protocole du point de terminaison. Vous pouvez spécifier des paramètres de point de terminaison supplémentaires après avoir créé le point de terminaison public. Pour spécifier des paramètres de point de terminaison supplémentaires, après avoir créé le point de terminaison, dans la boîte de dialogue Choisir des points de terminaison publics, cliquez sur le point de terminaison, puis sur **Ouvrir**. Ensuite, dans la boîte de dialogue **Configurer le point de terminaison public**, fournissez des paramètres supplémentaires, puis cliquez sur **OK** .
     Pour plus d'informations sur les paramètres des boîtes de dialogue **Créer un point de terminaison public** et **Configurer un point de terminaison public**, voir Commutation de contenu.
   - Si vous souhaitez modifier un point de terminaison public, cliquez sur le point de terminaison, puis cliquez sur **Ouvrir**. Ensuite, dans la boîte de dialogue **Configurer le point**

de terminaison public, modifiez les paramètres du point de terminaison, puis cliquez sur **OK**.

Pour plus d'informations sur les paramètres de la boîte de dialogue Configurer un point de terminaison public, consultez la section Commutation de contenu.

4. Cliquez sur **Fermer**.

Configuration de points de terminaison publics pour une unité d'application

Pour une unité d'application, vous spécifiez les points de terminaison publics de la même manière que les points de terminaison publics pour une application créée à partir d'un modèle d'application AppExpert. Pour plus d'informations sur la spécification d'un sous-ensemble de points de terminaison pour une unité d'application, voir Configuration des points de terminaison pour une unité d'application.

Pour configurer les points de terminaison d'une unité d'application à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez avec le bouton droit sur l'unité d'application pour laquelle vous souhaitez spécifier des points de terminaison publics, puis cliquez sur **Configurer les points de terminaison publics**.
3. Dans la boîte de dialogue **Choisir les points de terminaison publics** de l'unité de l'application, effectuez l'une des opérations suivantes :
   - Si vous spécifiez des points de terminaison pour l'unité d'application pour la première fois, désactivez les cases à cocher correspondant aux points de terminaison que vous ne souhaitez pas être lié à l'unité d'application.
   - Si vous souhaitez spécifier des points de terminaison répertoriés dans la boîte de dialogue mais qui ne sont pas actuellement liés à l'unité de l'application, cochez les cases correspondantes.
4. Cliquez sur **OK**.

Configuration des services et des groupes de services pour une application AppExpert

Les services et les groupes de services sont disponibles pour les unités d'application uniquement après avoir configuré les services et les groupes de services pour l'application AppExpert. Par conséquent, vous devez configurer les services et les groupes de services pour l'application AppExpert avant de configurer les services pour les unités de l'application. Tous les services et groupes de services que vous configurez pour une application AppExpert doivent utiliser le même protocole (HTTP ou HTTPS). La procédure de configuration des services et des groupes de services pour une application AppExpert qui n'est pas créée à partir d'un modèle est la même que pour une application créée à partir d'un modèle.

Pour configurer un service ou un groupe de services pour l'application AppExpert à l'aide de l'interface utilisateur graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez avec le bouton droit sur l'application pour laquelle vous souhaitez configurer des services ou des groupes de services, puis cliquez sur **Configurer les services backend**.
3. Dans la boîte de dialogue Configurer les services backend, effectuez l'une des opérations suivantes :
   - Pour configurer les services, cliquez sur l'onglet **Services** .
   - Pour configurer des groupes de services, cliquez sur l'onglet **Groupes** de **services** .
4. Dans l'onglet **Serviceou Groupes** de services, effectuez l'une des opérations suivantes :
   - Si les services ou groupes de services souhaités sont répertoriés dans l'onglet, cochez les cases correspondantes.
   - Si vous souhaitez spécifier tous les services ou groupes de services, cliquez sur **Tout activer**.
   - Si vous souhaitez créer un nouveau service ou un nouveau groupe de services, cliquez sur **Ajouter**. Ensuite, dans la boîte de dialogue **Créerun service ou Créer un groupe**de services, configurez les paramètres du service ou du groupe de services, respectivement, puis cliquez sur**Créer**.
   - Si vous souhaitez modifier un service, cliquez sur le service, puis sur Ouvrir. Ensuite, dans la boîte de dialogue **Configurer** le **service ou Créer un groupe** de services boîte de dialogue, configurez les paramètres du service ou du groupe de services, respectivement, puis cliquez sur **OK** .

Pour plus d'informations sur les paramètres des boîtes de dialogue Créer un service, Configurer **un service et Créer un groupe** de services, voir Équilibrage de charge.

Configuration des services et des groupes de services pour une unité d'application

Après avoir configuré les services et les groupes de services, vous devez configurer les services et les groupes de services pour chaque unité d'application. Toutefois, cette étape n'est pas nécessaire si chaque service backend héberge tout le contenu associé à l'application Web. Vous configurez des services et des groupes de services pour une unité d'application si le contenu associé à l'unité d'application est hébergé uniquement sur un sous-ensemble des serveurs principaux.

Pour configurer des services ou des groupes de services pour une unité d'application à l'aide de l'interface utilisateur graphique :

1. Accédez à **AppExpert** > **Applications**.
2. Dans le volet de détails, cliquez avec le bouton droit sur l'unité d'application pour laquelle vous souhaitez configurer un service ou un groupe de services, puis cliquez sur **Configurer les services backend**.
3. Dans la boîte de dialogue **Configurer les services backend**, effectuez l'une des opérations suivantes :

- Pour configurer les services, cliquez sur l'onglet **Services** .
- Pour configurer des groupes de services, cliquez sur l'onglet **Groupes de services** .

4. Dans l'onglet **Services** ou **Groupes de services**, effectuez l'une des opérations suivantes :
   - Décochez les cases correspondant aux services ou groupes de services que vous ne souhaitez pas configurer pour l'unité d'application. Assurez-vous que les cases à cocher correspondant aux services ou groupes de services que vous souhaitez configurer pour l'unité d'application sont cochées. Ensuite, dans la colonne Poids, spécifiez le poids que vous souhaitez attribuer à chaque service configuré.
   - Pour spécifier tous les services ou groupes de services, cliquez sur **Tout activer**.
5. Dans les onglets **Méthode** et **Persistance** et **Avancé**, spécifiez les paramètres souhaités.
6. Cliquez sur **OK**.

Configuration des stratégies

Les procédures de configuration des stratégies pour une application AppExpert créée sans utiliser de modèle sont les mêmes que celles pour une application AppExpert créée à partir d'un modèle. Pour plus d'informations, voir Configuration des stratégies pour les unités d'application.

Applications NetScaler Gateway

May 5, 2023

Lorsque vous configurez une application AppExpert pour gérer une application Web via l'appliance Citrix® NetScaler®, vous créez également un ensemble d'unités d'application et configurez un ensemble de politiques d'optimisation du trafic et de sécurité pour chaque unité. Les stratégies que vous configurez pour chaque unité d'application (stratégies pour des fonctionnalités telles que la compression, la mise en cache et la réécriture) évaluent le trafic destiné uniquement à cette unité. Outre ces stratégies, vous pouvez configurer des stratégies Access Gateway pour l'application dans son ensemble afin d'optimiser le trafic de l'application lors de l'accès via Access Gateway. La fonction Applications Access Gateway vous permet de configurer des stratégies Access Gateway (autorisation, trafic, accès sans client et compression TCP) pour une application AppExpert. Après avoir configuré les politiques NetScaler Gateway pour les applications AppExpert, vous pouvez inclure la configuration des politiques dans les modèles d'applications AppExpert que vous créez.

Vous pouvez également configurer les politiques de NetScaler Gateway pour les sous-réseaux intranet, les partages de fichiers et d'autres ressources réseau. Enfin, vous pouvez créer des signets pour les applications AppExpert et certaines ressources si vous souhaitez que les utilisateurs puissent y accéder depuis la page d'accueil de NetScaler Gateway.

Vous pouvez configurer les entités dans la fonctionnalité NetScaler Gateway Applications uniquement à l'aide de l'interface graphique.

Fonctionnement d'une application NetScaler Gateway

Lorsque vous créez une application AppExpert dans le nœud Applications de l'interface utilisateur graphique, une application Access Gateway correspondante est automatiquement créée dans le nœud Applications Access Gateway. De plus, une règle qui utilise le point de terminaison public configuré de l'application AppExpert est automatiquement créée pour l'entrée de l'application Access Gateway. Si plusieurs points de terminaison sont configurés pour l'application AppExpert, la règle inclut tous les points de terminaison publics configurés. L'appliance NetScaler utilise cette règle pour appliquer toutes les politiques Access Gateway configurées au trafic reçu sur le point de terminaison public de l'application AppExpert. Le trafic reçu sur le point de terminaison public de l'application AppExpert est d'abord évalué par rapport aux politiques NetScaler Gateway, puis par rapport aux politiques configurées pour les unités d'application de l'application AppExpert.

La règle qui est créée pour les stratégies d'accès sans client pour une application Access Gateway est une expression avancée qui utilise également le point de terminaison public configuré pour l'application AppExpert. Par conséquent, avant de configurer les politiques NetScaler Gateway pour une application AppExpert, vous devez configurer des points de terminaison publics pour l'application AppExpert.

Lorsque vous incluez la configuration de NetScaler Gateway dans un modèle d'application, les informations spécifiques au déploiement, telles que l'adresse IP et les informations de port, ainsi que la règle créée à partir de ces informations ne sont pas incluses dans le modèle.

Comment fonctionne une configuration NetScaler pour un partage de fichiers

Sur l'appliance NetScaler, vous pouvez configurer des politiques d'autorisation pour un partage de fichiers hébergé sur le réseau de votre organisation.

Lorsque vous créez un partage de fichiers, vous spécifiez un nom pour le partage de fichiers et le chemin réseau vers le partage de fichiers. Dans le chemin réseau, vous pouvez spécifier le nom du serveur ou l'adresse IP du serveur. Une règle qui utilise les composants du chemin du partage de fichiers est automatiquement créée pour le partage de fichiers. Cette règle permet à l'appliance d'identifier les demandes de fichiers hébergés sur le serveur de partage de fichiers. Toutes les stratégies d'autorisation configurées pour le partage de fichiers sont appliquées aux demandes entrantes.

La configuration NetScaler pour un partage de fichiers ne peut pas être enregistrée dans les modèles d'applications AppExpert.

Fonctionnement d'une configuration NetScaler pour un sous-réseau intranet

Pour les sous-réseaux intranet qui font partie de votre réseau, vous pouvez configurer des politiques d'autorisation, de trafic et de compression TCP sur l'appliance NetScaler. Lorsque vous ajoutez un sous-réseau intranet, vous spécifiez l'adresse IP et le masque de réseau du sous-réseau intranet. Une règle qui utilise ces deux paramètres est automatiquement créée pour le sous-réseau intranet. L'appliance applique les stratégies configurées à toute demande dont l'adresse IP de destination et le masque réseau sont définis respectivement sur l'adresse IP et le masque réseau du sous-réseau.

La configuration NetScaler pour un sous-réseau intranet ne peut pas être enregistrée dans les modèles d'applications AppExpert.

Fonctionnement de la catégorie Autres ressources

La catégorie Autres ressources vous permet de configurer des stratégies Access Gateway pour n'importe quelle ressource réseau à l'aide de la règle de votre choix. Lorsque vous configurez l'appliance NetScaler pour traiter les demandes relatives à la ressource réseau, vous configurez une expression classique pour identifier les demandes associées à la ressource réseau. Vous pouvez configurer les stratégies d'autorisation, de trafic, d'accès sans client et de compression TCP pour une ressource réseau dans Autres ressources. L'appliance NetScaler applique les politiques NetScaler Gateway configurées à toutes les demandes qui correspondent à la règle configurée.

La configuration NetScaler pour une ressource réseau dans Autres ressources ne peut pas être enregistrée dans les modèles d'application AppExpert.

Conventions de dénomination des entités

La fonctionnalité NetScaler Gateway Applications applique une convention de dénomination pour certaines des entités que vous créez dans cette fonctionnalité. Par exemple, les noms des profils que vous créez pour les stratégies de trafic d'un sous-réseau intranet commencent toujours par une chaîne composée du nom du sous-réseau intranet suivi d'un trait de soulignement (_). Le nom que vous fournissez pour l'entité est ajouté à cette chaîne. Si le nom d'un sous-réseau est « subnet1 », le nom du profil commence par « subnet1_. » Lorsqu'une telle convention de dénomination est requise (dans la zone de texte dans laquelle vous tapez le nom d'une entité, par exemple), l'interface utilisateur insère automatiquement la chaîne avec laquelle le nom de l'entité doit commencer et ne vous permet pas de le modifier.

Ajout de sous-réseaux Intranet

June 23, 2022

Vous pouvez spécifier les stratégies d'autorisation et de trafic pour le trafic qui est destiné aux sous-réseaux intranet configurés dans votre réseau. Les règles de ces stratégies sont automatiquement créées à l'aide des paramètres que vous spécifiez pour le sous-réseau.

Pour configurer un sous-réseau intranet à l'aide de l'interface utilisateur graphique :

1. Dans le volet de navigation de l'interface utilisateur, développez **AppExpert**, puis cliquez sur Access Gateway Applications.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour ajouter un sous-réseau Intranet, cliquez sur **Sous-réseaux Intranet**, puis sur **Ajouter**.
   - Pour modifier un sous-réseau intranet, cliquez sur un sous-réseau intranet, puis sur **Ouvrir**.
3. Dans la boîte de dialogue **Créer un sous-réseauIntranet ou Configurer un sous-réseau** Intranet, procédez comme suit :
   a) Dans la zone Nom, tapez le nom du sous-réseau intranet que vous ajoutez. Ce paramètre ne peut pas être modifié pour un sous-réseau intranet existant.
   b) Dans la zone Adresse IP, tapez l'adresse IP du sous-réseau intranet.
   c) Dans la zone Masque réseau, tapez le masque de réseau qui sera utilisé pour le sous-réseau intranet.
   d) Cliquez sur **Créer** ou **sur OK**, puis sur **Fermer**.

Ajout d'autres ressources

June 23, 2022

Pour une ressource réseau que vous ajoutez aux autres ressources, vous devez configurer l'expression de stratégie avancée qui identifie le sous-ensemble du trafic associé à la ressource.

Pour configurer une ressource dans d'autres ressources à l'aide de l'interface graphique :

1. Dans le volet de navigation de l'interface utilisateur, développez AppExpert, puis cliquez sur **Access Gateway Applications**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour ajouter une ressource, cliquez sur **Autres ressources**, puis sur **Ajouter**.
   - Pour modifier une ressource, cliquez sur une ressource, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Créer une ressourceou Configurer** une ressource, procédez comme suit :
   a) Dans la zone Nom, tapez le nom de la ressource que vous ajoutez. Ce paramètre ne peut pas être modifié pour une ressource existante.

b) Dans la zone Règle, tapez la règle qui identifiera le sous-ensemble du trafic associé à la ressource que vous ajoutez.
Vous pouvez également cliquer sur **Configurer**, puis créer la règle dans la boîte de dialogue **Créer une expression** .
c) Cliquez sur **Créer** ou **sur OK**, puis sur **Fermer**.

Configuration des stratégies d'autorisation

May 5, 2023

Vous pouvez configurer les politiques d'autorisation de NetScaler Gateway pour que les utilisateurs et les groupes AAA accèdent à une ressource.

Pour configurer les autorisations permettant à un utilisateur ou un groupe AAA d'accéder à une ressource à l'aide de l'interface utilisateur graphique :

1. Dans le volet de navigation de l'interface utilisateur, développez AppExpert, puis cliquez sur **Access Gateway Applications**.
2. Dans le volet de détails, dans la colonne Autorisation, cliquez sur l'icône de l'application, du partage de fichiers, du sous-réseau intranet ou de la ressource pour laquelle vous souhaitez configurer des stratégies d'autorisation pour les utilisateurs et les groupes AAA.
3. Procédez comme suit :
   - Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer des autorisations se trouve déjà dans l'arborescence Groups/Users, faites glisser l'utilisateur ou le groupe de l'arborescence Groups/Users vers le nœud Users or Groups dans l'arborescence < `application name`>. Cliquez ensuite avec le bouton droit sur l'utilisateur ou le groupe, puis cliquez sur **Autoriser**.
   - Si l'utilisateur ou le groupe AAA pour lequel vous souhaitez configurer des autorisations n'est pas configuré sur l'appliance, dans l'arborescence <`application name`>, cliquez avec le bouton droit sur Utilisateurs ou Groupes, puis cliquez sur **Ajouter**. Dans la boîte de dialogue Créer un **groupe AAAou Créer un utilisateur AAA**, renseignez les valeurs, cliquez sur**Créer**, puis sur**Fermer**.
     L'utilisateur ou le groupe est créé avec l'autorisation définie sur Autoriser. Pour modifier le paramètre d'autorisation, cliquez avec le bouton droit sur le groupe ou l'utilisateur, puis cliquez sur le paramètre d'autorisation.
4. Cliquez sur **Fermer**.

Configuration des stratégies de trafic

May 5, 2023

Les politiques de trafic que vous configurez pour les ressources du nœud NetScaler Gateway Applications contrôlent les connexions des clients à l'application. Il n'est pas nécessaire de configurer une règle pour la ressource. La règle est créée automatiquement lorsque vous créez la ressource. Il suffit d'associer un profil de demande à la stratégie de trafic. Dans le profil de trafic, vous spécifiez des paramètres tels que le protocole, le délai d'expiration de l'application et l'association des types de fichiers.

Pour configurer les stratégies de trafic pour une ressource

1. Dans le volet de navigation de l'interface utilisateur, développez AppExpert, puis cliquez sur Access Gateway Applications.
2. Dans le volet d'informations, dans la colonne Trafic, cliquez sur l'icône fournie pour l'application, le partage de fichiers, le sous-réseau intranet ou la ressource pour laquelle vous souhaitez configurer des stratégies de trafic.
3. Dans la boîte de dialogue **Configurer les stratégies de trafic**, procédez comme suit :
   - Pour spécifier une stratégie de trafic existante, cliquez sur **Insérer une stratégie**, puis, dans la colonne Nom de la stratégie, cliquez sur le nom de la stratégie.
   - Pour configurer une nouvelle stratégie, cliquez sur Insérer une stratégie, puis, dans la colonne Nom de la stratégie, cliquez sur Nouvelle stratégie. Dans la boîte de dialogue Créer une stratégie de trafic, dans la zone Nom, après le trait de soulignement (_), tapez un nom pour la stratégie. Ensuite, dans Profil de demande, sélectionnez un profil de demande existant ou cliquez sur Nouveau pour configurer un nouveau profil de demande. Vous pouvez également sélectionner un profil existant, puis cliquer sur Modifier pour modifier le profil.
     Pour plus d'informations sur la configuration d'une politique ou d'un profil de trafic, consultez NetScalerGateway.
   - Pour modifier une stratégie que vous avez insérée, dans la colonne Nom de la stratégie, cliquez sur le nom de la stratégie, puis sur Modifier la stratégie. Pour modifier uniquement le profil associé, dans la colonne Profil, cliquez sur le nom du profil, puis sur **Modifier le profil**.
   - Pour régénérer les priorités attribuées aux stratégies, cliquez sur **Régénérer les priorités**.
   - Pour spécifier une nouvelle valeur de priorité pour une stratégie, dans la colonne Priorité, double-cliquez sur la priorité attribuée, puis entrez la valeur souhaitée.
   - Pour délier une stratégie, cliquez sur la stratégie, puis cliquez sur **Délier la stratégie**.
4. Cliquez sur **Appliquer les modifications**, puis sur **Fermer**.

Configuration des stratégies d'accès sans client

May 5, 2023

L'accès sans client, lorsqu'il est configuré pour une ressource sur l'appliance NetScaler, permet aux utilisateurs finaux d'accéder à la ressource sans utiliser le logiciel client NetScaler Gateway. Les utilisateurs peuvent utiliser des navigateurs Web pour accéder à des ressources telles qu'Outlook Web Access. Vous configurez l'accès sans client pour une ressource en configurant une stratégie d'accès sans client associée à un profil d'accès sans client.

Pour configurer une politique d'accès sans client pour une ressource dans le nœud NetScaler Gateway Applications :

1. Dans le volet de navigation de l'interface graphique, développez **AppExpert**, puis cliquez sur **Access Gateway Applications**.
2. Dans le volet d'informations, dans la colonne **Accès sans client**, cliquez sur l'icône de l'application, du partage de fichiers, du sous-réseau intranet ou de la ressource pour laquelle vous souhaitez configurer une stratégie d'accès sans client.
3. Dans la boîte de dialogue **Configurer les stratégies d'accès sans client**, procédez comme suit :
   - Pour spécifier une stratégie d'accès sans client existante, cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur le nom de la stratégie.
   - Pour configurer une nouvelle stratégie d'accès sans client, cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**. Dans la boîte de dialogue **Créer une stratégie d'accès sans client**, dans la zone Nom, après le trait de soulignement (_), tapez un nom pour la stratégie. Ensuite, dans Profil, sélectionnez un profil existant ou cliquez sur Nouveau pour configurer un nouveau profil. Vous pouvez également sélectionner un profil existant, puis cliquer sur **Modifier** pour modifier le profil.
     Pour plus d'informations sur la configuration d'une politique ou d'un profil d'accès sans client, consultez NetScalerGateway.
   - Pour modifier une stratégie que vous avez insérée, dans la colonne Nom de la stratégie, cliquez sur le nom de la stratégie, puis sur **Modifier la stratégie**. Pour modifier uniquement le profil associé, dans la colonne Profil, cliquez sur le nom du profil, puis sur Modifier le profil.
   - Pour spécifier une nouvelle valeur de priorité pour une stratégie, dans la colonne Priorité, double-cliquez sur la priorité attribuée, puis entrez la valeur souhaitée.
   - Pour délier une stratégie, cliquez sur la stratégie, puis cliquez sur **Délier la stratégie**.
4. Cliquez sur **Appliquer les modifications**, puis sur **Fermer**.

Configuration des stratégies de compression TCP

May 5, 2023

Vous pouvez configurer des stratégies de compression TCP pour une application afin d'augmenter ses performances. La compression TCP réduit la latence du réseau, réduit les besoins en bande passante et augmente la vitesse de transmission. Lorsque vous configurez une stratégie de compression TCP, vous associez une action de compression à la stratégie. L'action de compression spécifie Compress, GZIP, Deflate, ou NoCompress comme type de compression. Pour plus d'informations sur les politiques de compression et les actions de compression, consultez NetScalerGateway.

Pour configurer une politique de compression TCP pour une ressource dans le nœud NetScaler Gateway Applications

1. Dans le volet de navigation de l'interface graphique, développez **AppExpert**, puis cliquez sur **Access Gateway Applications**.
2. Dans le volet d'informations, dans la colonne Compression TCP, cliquez sur l'icône de l'application, du partage de fichiers, du sous-réseau intranet ou de la ressource pour laquelle vous souhaitez configurer une stratégie de compression TCP.
3. Dans la boîte de dialogue **Configurer les stratégies de compression TCP**, procédez comme suit :
   - Pour spécifier une stratégie de compression TCP existante, cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur le nom de la stratégie.
   - Pour créer une nouvelle stratégie de compression TCP, cliquez sur Insérer une stratégie, puis, dans la colonne Nom de la stratégie, cliquez sur Nouvelle stratégie. Dans la boîte de dialogue Créer une stratégie de compression TCP, dans la zone Nom de la stratégie, après le trait de soulignement (« _ »), tapez un nom pour la stratégie. Ensuite, dans Action, sélectionnez une action existante ou cliquez sur Nouveau et configurez une nouvelle action. Vous pouvez également cliquer sur Affichage pour afficher le type de compression configuré.
     Pour plus d'informations sur la configuration d'une politique ou d'une action de compression TCP, consultez NetScaler Gateway, Advanced Edition sur NetScaler Gateway.
   - Pour modifier une stratégie que vous avez insérée, dans la colonne Nom de la stratégie, cliquez sur le nom de la stratégie, puis sur **Modifier la stratégie**.
   - Pour régénérer les priorités attribuées aux stratégies, cliquez sur **Régénérer les priorités**.
   - Pour spécifier une nouvelle valeur de priorité pour une stratégie, dans la colonne Priorité, double-cliquez sur la priorité attribuée, puis entrez la valeur souhaitée.
   - Pour délier une stratégie, cliquez sur la stratégie, puis cliquez sur **Délier la stratégie**.
4. Cliquez sur **Appliquer les modifications,** puis sur **Fermer**.

Configuration des signets

June 23, 2022

Vous pouvez configurer des signets pour les applications internes ou les ressources disponibles pour un utilisateur autorisé. Vous pouvez ensuite lier le signet à un utilisateur, un groupe d'utilisateurs ou un serveur virtuel globalement et l'activer pour l'utilisateur dans l'interface d'accès. Les liens de signet que vous créez apparaissent dans les volets des sites Web sous les sites Web d'entreprise.

Pour plus d'informations, consultez la rubrique Création et application de liens Web .

AppQoE

May 5, 2023

La qualité d'expérience au niveau des applications (AppQoE) intègre plusieurs fonctionnalités de sécurité basées sur des politiques existantes de l'appliance NetScaler en une seule fonctionnalité intégrée qui tire parti d'un nouveau mécanisme de mise en file d'attente, la mise en file d'attente équitable. La mise en file d'attente pondérée gère les demandes vers des serveurs Web et des applications à charge équilibrée au niveau du serveur virtuel plutôt qu'au niveau du service, ce qui lui permet de gérer la file d'attente de toutes les demandes vers un site Web ou une application en tant que groupe avant l'équilibrage de charge, plutôt que comme des flux distincts après l'équilibrage de charge.

- **Surcharge simple.** Tout serveur, quelle que soit sa robustesse, ne peut accepter qu'un nombre limité de connexions en même temps. Lorsqu'un site Web ou une application protégé reçoit trop de demandes en même temps, la fonction Protection contre les surtensions détecte la surcharge et met en file d'attente les connexions excédentaires jusqu'à ce que le serveur puisse les accepter. La fonctionnalité AppQoE affiche une autre page Web qui avertit les utilisateurs que la ressource demandée n'est pas disponible.
- **Attaques par déni de service (DOS).** Toute ressource destinée au public est vulnérable aux attaques dont le but est de faire tomber ce service et d'en interdire l'accès aux utilisateurs légitimes. La fonction de protection contre les surtensions permet de gérer les attaques DOS en plus des autres types de charge élevée. En outre, la fonctionnalité de protection par déni de service HTTP cible les attaques DOS contre vos sites Web, en envoyant des défis aux attaquants suspects et en abandonnant les connexions si les clients n'envoient pas de réponse appropriée.

Jusqu'à la version actuelle du système d'exploitation NetScaler, ces fonctionnalités étaient implémentées au niveau du service, ce qui signifie que chaque service se voyait attribuer ses propres files d'attente. Bien que les files d'attente au niveau de service fonctionnent, elles présentent également certains inconvénients, dont la plupart sont dus au fait que l'appliance NetScaler doit équilibrer la charge des demandes avant de mettre en œuvre l'une des fonctionnalités de protection qui reposent

sur la mise en file d'attente. L'implémentation de fonctions de protection avant la mise en file d'attente présente divers avantages, dont certains sont énumérés ci-dessous :

- Les connexions ne sont pas vidé si un service transitions état, comme elles le sont dans une file d'attente de niveau service.
- Pendant les périodes de charge élevée, telles qu'une attaque par déni de service, et les déni de service HTTP entrent en jeu avant l'équilibrage de charge, ce qui permet à ces fonctionnalités de détecter et de détourner le trafic indésirable ou de priorité inférieure de l'équilibreur de charge avant que l'équilibreur de charge ne puisse y faire face.

En plus de mettre en œuvre une file d'attente équitable, AppQoE intègre un ensemble de fonctionnalités qui fournissent chacun un ensemble d'outils différents pour atteindre un objectif commun : protéger vos ressources réseau contre une demande excessive ou inappropriée. L'intégration de ces fonctionnalités dans un cadre commun vous permet de les configurer et de les implémenter plus facilement.

Activation d'AppQoE

August 20, 2021

Pour configurer AppQoE, vous devez d'abord activer la fonctionnalité.

Pour activer AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- activer la fonction ns appqoe
- show ns feature

Exemple :

```
> enable ns feature appqoe
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 ...
 1)     AppQoE                          AppQoE              ON
 Done
```



```
<!--NeedCopy-->
```

Pour activer AppQoE à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet d'informations, cliquez sur **Configurer les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, activez la case à cocher **AppQoE** .
4. Cliquez sur **OK**.

Actions AppQoE

May 5, 2023

Après avoir activé la fonctionnalité AppQoE, vous devez configurer une ou plusieurs actions pour la gestion des demandes.

> **Important :**
>
> Aucun paramètre individuel spécifique n'est requis pour créer une action, mais vous devez inclure au moins un paramètre, sinon vous ne pouvez pas créer l'action.

Pour configurer une action AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appqoe action <name> [-priority <priority>] [-respondWith (ACS|NS)[<customfile>] [-altContentSvcName <string>] [-altContentPath <string>] [-maxConn <positive_integer>] [-delay <usecs>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-dosAction (**SimpleResponse** | **HICResponse**)]`
- `show appqoe action`

Exemple

Pour configurer la mise en file d'attente prioritaire avec des profondeurs de file d'attente de politiques de 10 et 1 000 pour les files d'attente de priorité moyenne et faible, respectivement :

```
> add appqoe action appqoe-act-basic-prhigh -priority HIGH
 Done

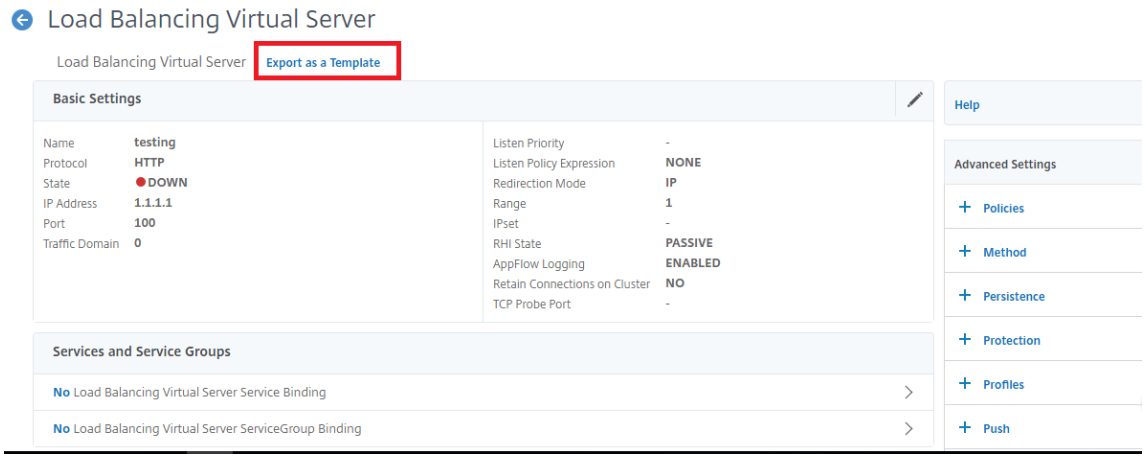
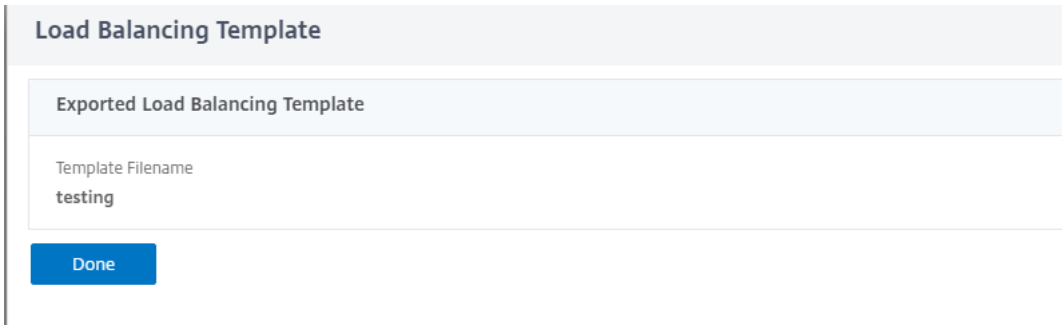
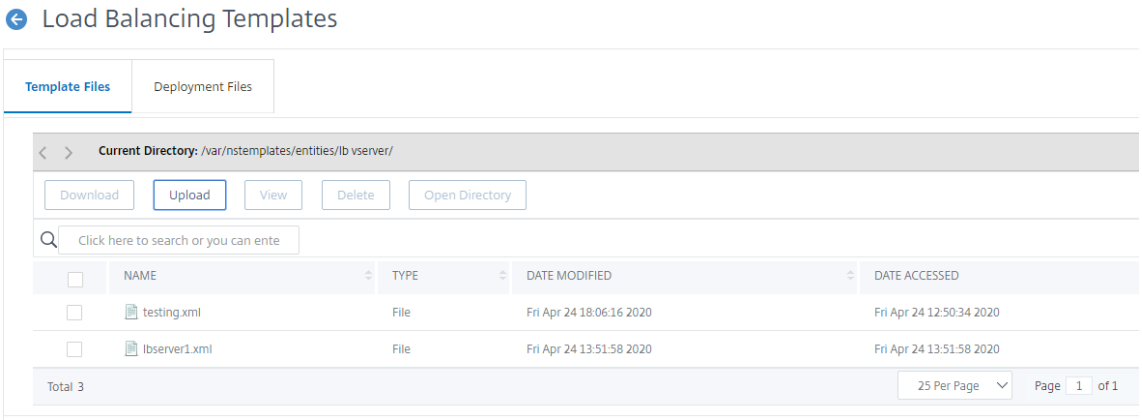
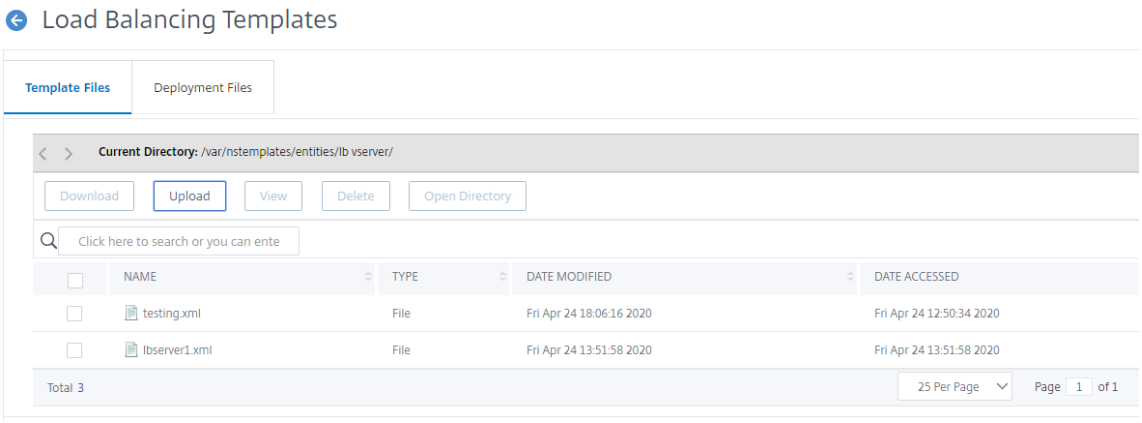
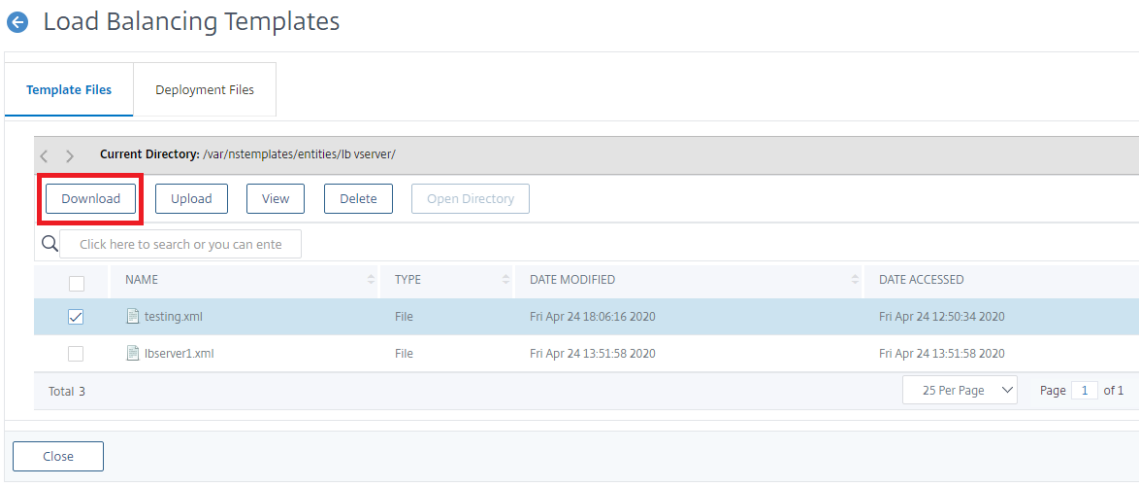
```



```
> add appqoe action appqoe-act-basic-prmedium -priority MEDIUM -
   polqDepth 10
 Done

> add appqoe action appqoe-act-basic-prlow -priority LOW -polqDepth
   1000
 Done

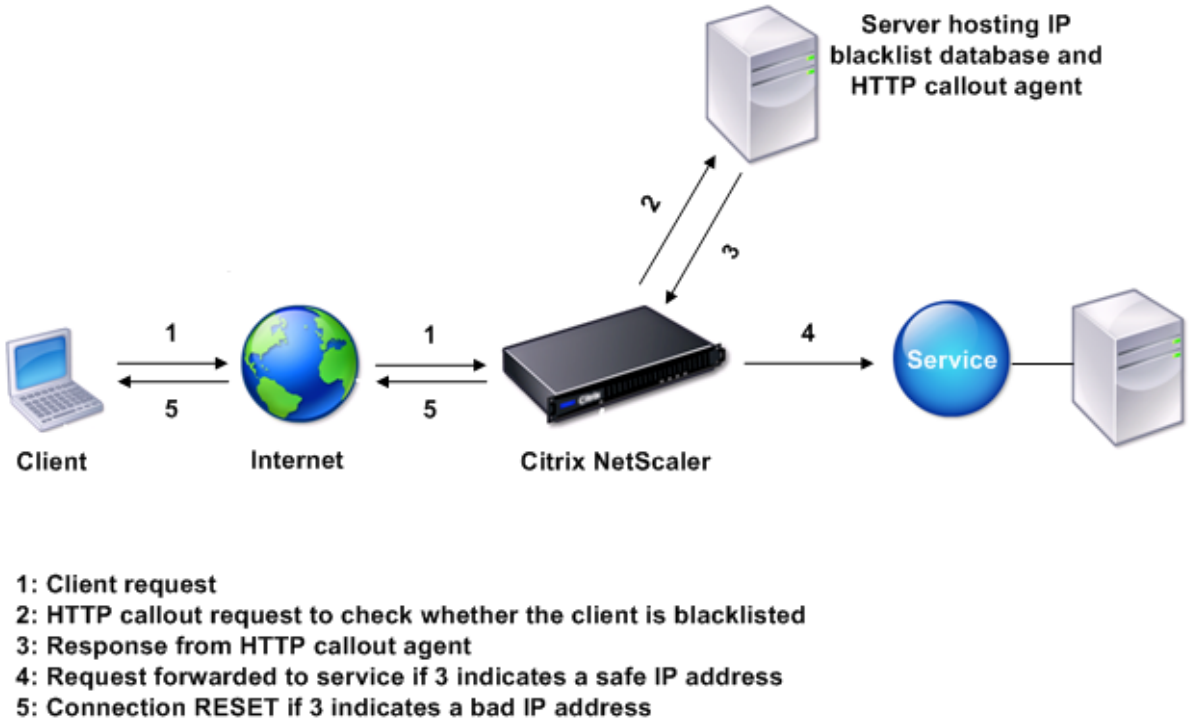
> show appqoe action

1.       Name: appqoe-act-basic-prhigh
        ActionType: PRIORITY_QUEUING
        Priority: HIGH
        PolicyQdepth: 0
        Qdepth: 0

1.      Name: appqoe-act-basic-prmedium
        ActionType: PRIORITY_QUEUING
        Priority: MEDIUM
        PolicyQdepth: 10
        Qdepth: 0

1.      Name: appqoe-act-basic-prlow
        ActionType: PRIORITY_QUEUING
        Priority: LOW
        PolicyQdepth: 1000
        Qdepth: 0
Done
<!--NeedCopy-->
```

Pour modifier une action AppQoE existante à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appqoe action <name> [-priority <priority>] [-altContentSvcName <string>] [-altContentPath <string>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-maxConn <positive_integer>] [-delay <usecs>] [-dosTrigExpression <expression>] [-dosAction ( SimpleResponse | HICResponse )]`
- `show appqoe action`

Pour supprimer une action AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `rm appqoe action <name>`
- `show appqoe action`

Paramètres de configuration d'une action AppQoE

- de l'utilisateur. Le nom de la nouvelle action ou le nom de l'action existante que vous souhaitez modifier. Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement et peut se composer de 1 à 3 lettres, de chiffres et du tiret (-), du point (.), de la livre (#), de l'espace (), du signe arobase (@), des égaux (=), des deux-points (:) et du trait de soulignement (_).
- priorité. La file d'attente prioritaire à laquelle la demande est affectée. Lorsqu'un serveur Web ou une application protégée est fortement chargé et ne peut pas accepter de demandes supplémentaires, spécifie l'ordre dans lequel les demandes en attente doivent être traitées lorsque les ressources sont disponibles. Les choix sont les suivants :

1. **HAUT.** Répond à la demande dès que les ressources sont disponibles.
2. **MOYEN.** Répond à la demande après avoir traité toutes les demandes de la file d'attente hautement prioritaire.
3. **FAIBLE.** Répond à la demande après avoir traité toutes les demandes figurant dans les files d'attente de priorité HAUTE et MOYENNE.
4. **LE PLUS BAS.** Répond à la demande uniquement après avoir traité toutes les demandes dans les files d'attente de priorité supérieure.

Si la priorité n'est pas configurée, l'appliance NetScaler attribue la demande à la file d'attente de priorité la plus BASSE par défaut.

- Répondez avec. Configure NetScaler pour qu'il exécute l'action du répondeur spécifiée lorsque le seuil spécifié est atteint. Doit être utilisé avec l'un des paramètres suivants :
  - **ACS :** diffuse du contenu à partir d'un service de contenu alternatif. Seuil : MaxConn (nombre maximum de connexions) ou délai.
  - **NS :** fournit une réponse intégrée à partir de NetScaler. Seuil : MaxConn (nombre maximum de connexions) ou délai.
  - **AUCUNE ACTION :** ne diffuse aucun contenu alternatif. Assigne les connexions à la file d'attente de priorité la plus BASSE si le seuil MaxConn (nombre maximal de connexions) ou de délai est atteint.
- AltContentSvcName. Si -responseWith ACS est spécifié, le nom du service de contenu alternatif, généralement une URL absolue vers le serveur Web qui héberge le contenu alternatif.
- AltContentPath. Si -responseWith (ACS | NS) est spécifié, le chemin vers le contenu alternatif.

- Profondeur OLQ. Valeur du seuil de profondeur de file d'attente de politiques pour la file d'attente de politiques associée à cette action. Lorsque le nombre de connexions dans la file d'attente de politiques associée à cette action atteint le nombre spécifié, les demandes suivantes sont affectées à la file d'attente de politiques LA PLUS FAIBLE. Valeur minimale : 1 Valeur maximale : 4 294 967 294
- PriqDepth. Valeur du seuil de profondeur de file d'attente de politiques pour la file d'attente prioritaire spécifiée. Si le nombre de demandes dans la file d'attente spécifiée sur le serveur virtuel auquel la politique associée à l'action en cours est liée augmente jusqu'au nombre spécifié, les demandes suivantes sont affectées à la file d'attente de priorité la plus BASSE. Valeur minimale : 1 Valeur maximale : 4 294 967 294
- Max Conn. Le nombre maximum de connexions pouvant être ouvertes pour les demandes qui correspondent à la règle de politique. Valeur minimale : 1 Valeur maximale : 4 294 967 294
- retard. Le seuil de délai, en microsecondes, pour les demandes qui correspondent à la règle de politique. Si une demande correspondante a été retardée au-delà du seuil, l'appliance NetScaler exécute l'action spécifiée. Si AUCUNE ACTION n'est spécifiée, l'appliance attribue les demandes à la file d'attente ayant la priorité la plus BASSE. Valeur minimale : 1 Valeur maximale : 599999 999
- DoStrigExpression. Ajoute une vérification de second niveau facultative pour déclencher des actions DoS.
- DoS Action. Action à prendre lorsque l'appliance détermine qu'elle ou qu'un serveur protégé fait l'objet d'une attaque DoS. Valeurs possibles : SimpleResponse, HicResponse.

Ces valeurs spécifient les méthodes de question-réponse HTTP permettant de valider l'authenticité des demandes entrantes afin d'atténuer une attaque HTTP-DDoS.

Dans le processus de génération et de validation des réponses aux défis HTTP, AppQoe utilise des cookies pour valider la réponse du client et vérifier que le client semble authentique. Lors de l'envoi d'un défi, une appliance NetScaler génère deux cookies :

cookie d'en-tête (_DOSQ). Contient des informations spécifiques au client, afin que l'appliance NetScaler puisse vérifier la réponse.

Biscuit corporel (_DOSH). Informations utilisées pour valider la machine cliente. Le navigateur du client (ou l'utilisateur, dans le cas de HIC) calcule une valeur pour ce cookie. L'appliance NetScaler compare cette valeur à la valeur attendue pour vérifier le client.

Les informations que l'appliance envoie au client pour le calcul de la valeur _DOSH sont basées sur la configuration de l'action DoS.

1. SimpleResponse : Dans ce cas, une appliance NetScaler divise la valeur et génère un code JavaScript pour combiner la valeur finale. Une machine cliente capable de calculer la valeur d'origine est considérée comme authentique.

2. HICResponse : dans ce cas, une appliance NetScaler génère deux nombres à un chiffre et génère des images pour ces numéros. Ensuite, à l'aide d'un framework backpatch, l'appliance insère ces images sous forme de chaînes base64.

Limitations

1. Il ne s'agit pas d'une implémentation triviale du CAPTCHA, c'est pourquoi ce terme n'est pas utilisé.
2. Le numéro de validation est basé sur un numéro généré par Netscaler qui ne change pas pendant 120 secondes. Ce numéro doit être dynamique ou spécifique au client.

Pour configurer une action AppQoE à l'aide de l'utilitaire de configuration

1. **Accédez à**App-Expert**>**AppQoE > Actions**.**
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle action, cliquez sur **Ajouter**.
   - Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Modifier**.
3. Dans l'écran **Créer une action AppQoE** ou **Configurer une action AppQoE**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres de configuration de l'action AppQoE » comme suit (un astérisque indique un paramètre obligatoire) :
   - Nom—nom
   - Type d'action : répondre par
   - Priorité : priorité
   - Profondeur de la file d'attente des politiques : PolqDepth
   - Profondeur de la file d'attente : PriqDepth
   - Action DOS : action DOS
4. Cliquez sur **Créer** ou **sur OK**.

Paramètres AppQoE

January 21, 2021

Dans les paramètres AppQoE, vous configurez la durée de vie de session d'une session AppQoE, le nom du fichier contenant la réponse personnalisée et le nombre de connexions clientes pouvant être placées dans une file d'attente.

Pour configurer les paramètres AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appqoe parameter [-sessionLife <secs>] [-avgwaitingclient <positive_integer>] [-MaxAltRespBandWidth <positive_integer>] [-dosAttackThresh <positive_integer>]`
- `show appqoe parameter`

Paramètres de configuration des paramètres AppQoE

- sessionLife

  Nombre de secondes à attendre après l'affichage du contenu alternatif avant que l'appliance affiche à nouveau le même contenu. Valeur par défaut : 300 Valeur minimale maximale : 1 Valeur maximale : 4,294,967,294

- avgwaitingclient

  Nombre moyen de demandes client pouvant se trouver dans la file d'attente de service. Valeur par défaut : 1000000 Valeur maximale : 4,294,967,294

- MaxAltrespBandwidth

  Bande passante maximale à consommer lors de l'envoi de réponses alternatives. Si le maximum est atteint, l'appliance quitte l'envoi du contenu alternatif jusqu'à ce que la consommation de bande passante diminue. Valeur par défaut : 100 Valeur minimale : 1 Valeur maximale : 4,294,967,294

- dosAtckThrsh

  Seuil d'attaque par déni de service. Nombre de connexions qui doivent être en attente dans les files d'attente avant que l'appliance ne réponde par des mesures de protection DoS. Valeur par défaut : 2000 Valeur minimale : 0 Valeur maximale : 4,294,967,294

Pour configurer les paramètres AppQoE à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **AppQoE** .
2. Dans le volet d'informations, cliquez sur **Configurer les paramètres AppQoE**.
3. Dans l'écran **Configurer les paramètres AppQoE**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres pour la configuration des paramètres AppQoE » comme suit (un astérisque indique un paramètre requis) :
   - Vie de session (secondes)
   - sessionLife

- Client en attente moyenne—avgwaitingclient
- Limite de bande passante de réponse alternative (Mbps) —MaxAltrespBandwidth
- Seuil d'attaque DOS —DosAttackThresh

4. Cliquez sur **OK**.

Politiques AppQoE

May 5, 2023

Pour implémenter AppQoE, vous devez configurer au moins une politique indiquant à votre NetScaler comment distinguer les connexions à mettre en file d'attente dans une file d'attente spécifique.

Pour configurer une politique AppQoE à l'aide de la ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
add appqoe policy <name> -rule <expression> -action <string>
```

Exemple :

L'exemple suivant sélectionne les requêtes dont l'en-tête User-Agent contient « Android » et les affecte à la file d'attente de priorité moyenne. Ces demandes proviennent de smartphones et de tablettes qui exécutent le système d'exploitation Google Android.

```
1  > add appqoe action appqoe-act-primd -priority MEDIUM
2  Done
3  > add appqoe policy appqoe-pol-primd -rule "HTTP.REQ.HEADER("User-Agent
       ").CONTAINS("Android")" -action appqoe-act-primd
4  Done
5  > sh appqoe policy appqoe-pol-primd
6          Name: appqoe-pol-primd
7          Rule: HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")
8          Action: appqoe-act-primd
9          Hits: 0
10
11 Done
12 <!--NeedCopy-->
```

Paramètres de configuration d'une politique AppQoE

- de l'utilisateur. Nom de la politique AppQoE. Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement et peut comprendre de 1 à 127 lettres, chiffres et le tiret (-), le

point (.), la livre (#), l'espace (), le signe arobase (@), l'égal (=), les deux points (:) et le trait de soulignement (_). Vous devez choisir un nom qui permet d'identifier le type d'action.
- règle. Expression NetScaler qui indique à l'appliance les connexions qu'elle doit gérer.
- action. L'action AppQoE à effectuer lorsqu'une connexion correspond à la politique.

Pour configurer une politique AppQoE à l'aide de l'utilitaire de configuration

1. **Accédez à**App-Expert > AppQoE****> Politiques**.**
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une stratégie, cliquez sur **Ajouter**.
   - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Modifier**.
3. Si vous créez une politique, dans la boîte de dialogue **Créer une politique AppQoE**, dans la zone de texte Nom, tapez le nom de votre nouvelle politique.

   Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement et peut comprendre de 1 à 127 lettres, chiffres et le tiret (-), le point (.), la livre (#), l'espace (), le signe arobase (@), l'égal (=), les deux points (:) et le trait de soulignement (_). Vous devez choisir un nom qui permet d'identifier l'objectif et l'effet de cette politique.

   Si vous modifiez une politique existante, ignorez cette étape. Vous ne pouvez pas modifier le nom d'une politique existante.
4. Dans la liste déroulante **Action**, choisissez l'action AppQoE à exécuter lorsque la politique correspond à une connexion. Cliquez sur le signe plus (+) pour ouvrir la boîte de dialogue **Ajouter une action AppQoE** et ajouter une nouvelle action.
5. Dans la zone de texte **Règle**, entrez directement l'expression de politique ou cliquez sur Nouveau pour créer une expression de politique. Si vous cliquez sur Nouveau, procédez comme suit :

   a) Dans la boîte de dialogue **Créer une expression**, cliquez sur **Ajouter**.
   1 Dans la boîte de dialogue **Ajouter une expression**, sélectionnez une expression courante dans la liste déroulante **Expressions fréquemment utilisées** ou utilisez les listes déroulantes **Construire une expression** pour créer l'expression qui définit le trafic à filtrer.
   Si vous choisissez de créer votre propre expression, vous devez commencer par sélectionner le premier terme dans la première liste déroulante sur le côté gauche de la zone Construire une expression. Les choix proposés dans cette liste sont les suivants :

   - HTTP
   - SYS
   - CLIENT

- SERVEUR
- ANALYTIQUE
- TEXTE

Le choix par défaut est HTTP. Après avoir fait un choix dans la première liste déroulante (ou accepté le terme par défaut), vous pouvez choisir le terme suivant de votre expression dans la liste déroulante située à droite de celle-ci. Les termes de cette liste et des autres listes qui suivent changent en fonction de vos choix précédents. Les listes ne proposent que des termes qui constituent des choix valides. Continuez à sélectionner des termes jusqu'à ce que vous ayez terminé l'expression.

a) Lorsque vous avez créé l'expression souhaitée, cliquez sur **OK**. L'expression est ajoutée dans la zone de texte **Expression** .

6. Cliquez sur **Create**. L'expression apparaît dans la zone de texte de la **règle** .

Modèle d'entité pour l'équilibrage de charge du serveur virtuel

May 5, 2023

> **Avertissement**
>
> La fonctionnalité de modèle d'entité est obsolète à partir de NetScaler 13.0 build 82.x et Citrix vous recommande d'utiliser les livres de style comme alternative. Pour plus d'informations, consultez la rubrique Livres de style .

Un modèle d'entité est un ensemble d'informations permettant de créer un modèle de serveur virtuel d'équilibrage de charge sur une appliance NetScaler. Il fournit une spécification et un ensemble de valeurs par défaut à configurer pour un serveur virtuel d'équilibrage de charge. À l'aide d'un modèle qui définit un ensemble de valeurs par défaut, vous pouvez rapidement configurer plusieurs serveurs virtuels nécessitant une configuration similaire tout en éliminant plusieurs étapes de configuration.

Vous pouvez créer un modèle d'entité en exportant les détails du serveur virtuel d'équilibrage de charge vers un fichier modèle. Cela ne peut être fait que via l'interface graphique de NetScaler. Vous utilisez l'interface graphique de NetScaler pour exporter, importer et gérer des modèles d'entités. Vous pouvez partager des modèles d'entités avec d'autres administrateurs et gérer les modèles enregistrés localement sur votre appliance ou votre machine. Vous pouvez également importer des modèles d'entités depuis l'appliance ou votre ordinateur local.

Avant de créer un modèle, vous devez vous familiariser avec la configuration du serveur virtuel d'équilibrage de charge.

Modèle de serveur virtuel d'équilibrage de charge

Les modèles d'entités d'équilibrage de charge sont créés de la même manière que les modèles d'applications NetScaler. Lorsque vous exportez un serveur virtuel d'équilibrage de charge vers un fichier modèle, les deux fichiers suivants sont automatiquement créés :

- Fichier modèle de serveur virtuel d'équilibrage de charge. Contient des éléments XML qui stockent les valeurs des paramètres configurés pour le serveur virtuel d'équilibrage de charge. Le fichier contient également des éléments XML permettant de stocker des informations sur les politiques liées.
- Fichier de déploiement. Contient des éléments XML qui stockent des informations spécifiques au déploiement, telles que des services, des groupes de services et des variables configurées. Dans les fichiers de modèle et de déploiement, chaque unité d'informations de configuration est encapsulée dans un élément XML spécifique destiné à ce type d'unité. Par exemple, le paramètre de méthode d'équilibrage de charge, LBMethod, est encapsulé dans les balises <lbmethod> et </lbmethod> .

> **Remarque :**
>
> Après avoir exporté un serveur virtuel d'équilibrage de charge, vous pouvez ajouter des éléments, supprimer des éléments et modifier des éléments existants avant d'importer les informations de configuration dans un dispositif NetScaler.

Fonctionnement d'un modèle de serveur virtuel d'équilibrage de charge

Lorsque vous créez un modèle pour un serveur virtuel d'équilibrage de charge, vous spécifiez des valeurs par défaut pour le serveur. Vous spécifiez les valeurs qui doivent être en lecture seule, celles qui ne doivent pas être affichées et les valeurs que les utilisateurs peuvent configurer. Vous configurez également les pages qui composent l'assistant d'importation de modèles. Toutes les informations et tous les paramètres que vous fournissez sont enregistrés dans le fichier modèle.
Lorsqu'un utilisateur importe le modèle dans une appliance NetScaler, l'interface graphique le guide à travers les différentes pages que vous avez configurées pour le modèle. L'interface graphique affiche les valeurs des paramètres en lecture seule et invite l'utilisateur à spécifier des valeurs pour les paramètres configurables. Une fois que l'utilisateur a suivi les instructions, l'appliance crée l'entité avec les valeurs configurées.
Vous pouvez créer ou modifier un modèle d'entité pour un serveur virtuel d'équilibrage de charge à partir du nœud Gestion du trafic.
Pour exporter les détails du serveur virtuel vers un modèle, vous devez spécifier les options et paramètres suivants pour le modèle :

- La valeur par défaut d'un paramètre.
- Si les valeurs par défaut sont visibles pour les utilisateurs.
- Si les valeurs par défaut peuvent être modifiées par les utilisateurs.

- Le nombre de pages dans l'assistant d'importation d'entités, y compris les noms de page, le texte et les paramètres disponibles.
- Les entités qui doivent être liées à l'entité pour laquelle le modèle est créé.

Par exemple, lorsque vous créez un modèle de serveur virtuel d'équilibrage de charge, vous pouvez spécifier les politiques que vous souhaitez lier au serveur virtuel que vous créez à partir du modèle. Toutefois, seules les informations contraignantes sont incluses dans le modèle. Les entités liées ne sont pas incluses. Si le modèle d'entité est importé vers une autre appliance NetScaler, les entités liées doivent exister sur l'appliance au moment de l'importation pour que la liaison réussisse. Si aucune des entités liées n'existe sur l'appliance cible, l'entité (pour laquelle le modèle a été configuré) est créée sans aucune liaison. Si seul un sous-ensemble des entités liées existe sur l'appliance cible, elles sont liées à l'entité créée à partir du modèle.
Lorsque vous exportez un modèle pour le serveur virtuel d'équilibrage de charge, les paramètres de configuration de l'entité apparaissent dans le modèle. Toutes les entités liées sont sélectionnées par défaut, mais vous pouvez modifier les liaisons si nécessaire. Comme dans le cas d'un modèle qui n'est pas basé sur une entité existante, seules les informations contraignantes sont incluses et non les entités. Vous pouvez enregistrer le modèle avec les paramètres de configuration existants ou utiliser les paramètres comme base pour créer une nouvelle configuration pour un modèle.

Configurer des variables dans le modèle de serveur virtuel d'équilibrage de charge

Les modèles de serveurs virtuels d'équilibrage de charge prennent en charge la déclaration de variables dans les paramètres d'équilibrage de charge configurés et dans les politiques et actions liées. La possibilité de déclarer des variables vous permet de remplacer des valeurs préconfigurées par des valeurs adaptées à l'environnement dans lequel vous importez le modèle.

À titre d'exemple, considérez l'expression suivante configurée pour une politique liée à un serveur virtuel d'équilibrage de charge pour lequel vous créez un modèle. L'expression évalue la valeur de l'en-tête accept-language dans une requête HTTP.

```
HTTP.REQ.HEADER("Accept-Language").CONTAINS("en-us")
```

Si vous souhaitez que la valeur de l'en-tête soit configurable au moment de l'importation, vous pouvez spécifier la chaîne en-us en tant que variable.

Après avoir créé une variable, vous pouvez effectuer les opérations suivantes :

- Attribuez d'autres chaînes à une variable existante. Après avoir créé une variable pour une chaîne, vous pouvez sélectionner et affecter d'autres parties de la même expression ou d'une expression différente à la variable. Les chaînes que vous attribuez à une variable ne doivent pas nécessairement être les mêmes. Au moment de l'importation, toutes les chaînes affectées à la variable sont remplacées par la valeur que vous fournissez.
- Affichez la chaîne ou les chaînes qui sont affectées à la variable.
- Afficher la liste de toutes les entités et de tous les paramètres qui utilisent la variable

Pour configurer des variables dans un modèle de serveur virtuel d'équilibrage de charge

Suivez la procédure suivante pour configurer des variables pour un modèle de serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique NetScaler.

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**
2. Dans le volet d'informations, cliquez avec le bouton droit sur le serveur virtuel que vous souhaitez exporter vers un fichier modèle, puis cliquez sur **Ajouter**.
3. Dans la page **Créer un serveur virtuel d'équilibrage de charge**, définissez les paramètres du serveur virtuel. Pour plus d'informations sur la configuration d'un serveur virtuel d'équilibrage de charge, voir Fonctionnement de l'équilibrage de charge.
4. Une fois que vous avez défini les paramètres du serveur virtuel d'équilibrage de charge, cliquez sur **Terminé**.



5. Cliquez sur le lien **Exporter en tant que modèle** en haut pour exporter les détails du serveur sous forme de fichier modèle.
6. Sur la page **Créer un modèle d'équilibrage** de charge, entrez les paramètres du modèle.
7. Cliquez sur **Terminé**.



Modifier un modèle de serveur virtuel d'équilibrage de charge

Vous pouvez modifier uniquement les paramètres, les liaisons et les pages configurés pour un modèle. Le nom et l'emplacement du modèle spécifiés lors de sa création ne peuvent pas être modifiés. L'appliance NetScaler ne vous offre pas la possibilité de modifier un modèle de serveur virtuel d'équilibrage de charge.

Pour modifier un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique NetScaler

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sur la page **Serveur virtuel d'équilibrage** de charge, modifiez les paramètres de l'entité.
3. Cliquez sur Terminé.
4. Cliquez sur le lien **Exporter en tant que modèle** .
5. Les modifications modifiées sont désormais disponibles dans le fichier modèle de serveur virtuel d'équilibrage de charge.
6. Sur la page **Modèle d'équilibrage de charge exporté**, cliquez sur **Terminé**.

Gérer les modèles de serveurs virtuels d'équilibrage de charge

Vous pouvez organiser les fichiers modèles de serveur virtuel d'équilibrage de charge et les fichiers de déploiement à l'aide de l'interface graphique NetScaler.

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sur la page **Serveurs virtuels**, sélectionnez l' **action Gérer le modèle**.
3. Sur la page **Modèles d'équilibrage de** charge, cliquez sur l'onglet **Fichier modèle** .
4. Dans l'onglet **Fichiers modèles**, vous pouvez charger ou télécharger un modèle depuis et vers le dossier des modèles de l'appliance.



5. Cliquez sur **Fermer**.

Pour télécharger un modèle d'entité de serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique NetScaler

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sur la page **Serveurs virtuels**, cliquez sur **Sélectionner une action**, puis sélectionnez **Gérer le modèle**.
3. Dans la page Modèles d'équilibrage de charge, cliquez sur l'onglet **Fichiers de modèles** .
4. Dans l'onglet **Fichiers modèles**, cliquez sur **Charger** pour charger un modèle.
5. Cliquez sur **Fermer**.



Pour télécharger un modèle d'entité de serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique NetScaler

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sur la page **Serveurs virtuels**, cliquez sur **Sélectionner une action**, puis sélectionnez **Gérer le modèle**.
3. Sur la page **Modèles d'équilibrage de** charge, cliquez sur l'onglet **Fichiers modèles** .
4. Dans l'onglet Fichiers modèles, sélectionnez un fichier modèle et cliquez sur Télécharger.
5. Cliquez sur Fermer.



Exemple de modèle de serveur virtuel d'équilibrage de charge et de modèle de déploiement

Voici un exemple de fichier modèle créé à partir d'un serveur virtuel d'équilibrage de charge appelé « Lbvip » :

```
COPY

<?xml version="1.0" encoding="UTF-8" ?>
  <template>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <entitytemplate>
      <lbvserver_list>
        <lbvserver>
          <name>Lbvip</name>
          <servicetype>HTTP</servicetype>
          <ipv46>0.0.0.0</ipv46>
          <ipmask>*</ipmask>
          <port>0</port>
          <range>1</range>
          <persistencetype>NONE</persistencetype>
          <timeout>2</timeout>
          <persistencebackup>NONE</persistencebackup>
          <backuppersistencetimeout>2</backuppersistencetimeout>
          <lbmethod>LEASTCONNECTION</lbmethod>
          <persistmask>255.255.255.255</persistmask>
```



```
            <v6persistmasklen>128</v6persistmasklen>
            <pq>OFF</pq>
            <sc>OFF</sc>
            <m>IP</m>
            <datalength>0</datalength>
            <dataoffset>0</dataoffset>
            <sessionless>DISABLED</sessionless>
            <state>ENABLED</state>
            <connfailover>DISABLED</connfailover>
            <clttimeout>180</clttimeout>
            <somethod>NONE</somethod>
            <sopersistence>DISABLED</sopersistence>
            <sopersistencetimeout>2</sopersistencetimeout>
            <redirectportrewrite>DISABLED</redirectportrewrite>
            <downstateflush>DISABLED</downstateflush>
            <gt2gb>DISABLED</gt2gb>
            <ipmapping>0.0.0.0</ipmapping>
            <disableprimaryondown>DISABLED</disableprimaryondown>
            <insertvserveripport>OFF</insertvserveripport>
            <authentication>OFF</authentication>
            <authn401>OFF</authn401>
            <push>DISABLED</push>
            <pushlabel>none</pushlabel>
            <l2conn>OFF</l2conn>
            <appflowlog>DISABLED</appflowlog>
            <icmpvsrresponse>PASSIVE</icmpvsrresponse>
            <lbvserver_cmppolicy_binding_list>
              <lbvserver_cmppolicy_binding>
                <name>Lbvip</name>
                <policyname>NOPOLICY-COMPRESSION</policyname>
                <priority>100</priority>
                <gotopriorityexpression>END</gotopriorityexpression>
                <bindpoint>REQUEST</bindpoint>
              </lbvserver_cmppolicy_binding>
            </lbvserver_cmppolicy_binding_list>
          </lbvserver>
        </lbvserver_list>
      </entitytemplate>
    </template>
<!--NeedCopy-->
```

Exemple de fichier de déploiement

Le fichier de déploiement associé au serveur virtuel dans l'exemple précédent est le suivant :

COPY

```
<?xml version="1.0" encoding="UTF-8" ?>
  <template_deployment>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <service_list>
      <service>
      <ip>1.2.3.4</ip>
      <port>80</port>
      <servicetype>HTTP</servicetype>
      </service>
    </service_list>
    <servicegroup_list>
      <servicegroup>
        <name>svcgrp</name>
        <servicetype>HTTP</servicetype>
        <servicegroup_servicegroupmember_binding_list>
          <servicegroup_servicegroupmember_binding>
            <ip>1.2.3.90</ip>
            <port>80</port>
          </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.0</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.1</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.9.0</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
      </servicegroup_servicegroupmember_binding_list>
    </servicegroup>
  </servicegroup_list>
</template_deployment>

<!--NeedCopy-->
```


légendes HTTP

May 5, 2023

Pour certains types de demandes, ou lorsque certains critères sont remplis au cours de l'évaluation des stratégies, vous pouvez interrompre brièvement l'évaluation des stratégies, extraire des informations d'un serveur, puis effectuer une action spécifique qui dépend des informations récupérées. D'autres fois, lorsque vous recevez certains types de demandes, vous pouvez souhaiter mettre à jour une base de données ou le contenu hébergé sur un serveur Web. Les légendes HTTP vous permettent d'effectuer toutes ces tâches.

Une légende HTTP est une requête HTTP ou HTTPS que l'appliance NetScaler génère et envoie à une application externe lorsque certains critères sont remplis lors de l'évaluation des politiques. Les informations extraites du serveur peuvent être analysées par des expressions de stratégie avancées, et une action appropriée peut être effectuée. Vous pouvez configurer des légendes HTTP pour la commutation de contenu HTTP, la commutation de contenu TCP, la réécriture, le répondeur et pour la méthode d'équilibrage de charge basée sur des jetons.

Avant de configurer une légende HTTP, vous devez configurer une application sur le serveur auquel la légende sera envoyée. L'application, appelée *agent de légende HTTP*, doit être configurée pour répondre à la demande de légende HTTP avec les informations requises. L'agent de légende HTTP peut également être un serveur Web qui fournit les données pour lesquelles l'appliance NetScaler envoie la légende. Vous devez vous assurer que le format de la réponse à une légende HTTP ne change pas d'un appel à l'autre.

Après avoir configuré l'agent de légende HTTP, vous configurez la légende HTTP sur l'appliance NetScaler. Enfin, pour invoquer la légende, vous devez inclure la légende dans une politique avancée de la fonctionnalité NetScaler appropriée, puis vous liez la politique au point de liaison auquel vous souhaitez que la stratégie soit évaluée.

Après avoir configuré la légende HTTP, vous devez vérifier la configuration pour vous assurer que la légende fonctionne correctement.

Comment fonctionne une légende HTTP

May 5, 2023

Lorsque l'appliance NetScaler reçoit une demande client, elle évalue la demande par rapport aux politiques liées à différents points de liaison. Au cours de cette évaluation, si l'appliance rencontre l'expression de légende HTTP `SYS.HTTP_CALLOUT(<name>)`, elle bloque brièvement l'évaluation de la politique et envoie une demande à l'agent de légende HTTP à l'aide des paramètres configurés

pour la légende HTTP spécifiée. À la réception de la réponse, l'appliance inspecte la partie spécifiée de la réponse, puis exécute une action ou évalue la politique suivante, selon que l'évaluation de la réponse de l'agent de légende HTTP est vraie ou fausse, respectivement. Par exemple, si la légende HTTP est incluse dans une politique de répondeur, si l'évaluation de la réponse est vraie, l'appliance exécute l'action associée à la politique de répondeur.

Si la configuration de la légende HTTP est incorrecte ou incomplète, ou si la légende s'appelle elle-même de manière récursive, l'appliance déclenche une condition UNDEF et met à jour le compteur d'accès non défini.

La figure suivante illustre le fonctionnement d'une légende HTTP invoquée à partir d'une politique de réponse globale. La légende HTTP est configurée pour inclure l'adresse IP du client associée à une demande entrante. Lorsque l'appliance NetScaler reçoit une demande d'un client, elle génère la demande de légende et l'envoie au serveur de légende, qui héberge une base de données d'adresses IP sur liste noire et un agent de légende HTTP qui vérifie si l'adresse IP du client figure dans la base de données. L'agent de légende HTTP reçoit la demande de légende, vérifie si l'adresse IP du client est répertoriée et envoie une réponse que l'appliance NetScaler évalue. Si la réponse indique que l'adresse IP du client n'est pas sur liste noire, l'appliance transmet la réponse au service configuré. Si l'adresse IP du client figure sur la liste noire, l'appliance réinitialise la connexion du client

Figure 1. Modèle d'entité de légende HTTP



Remarques sur le format des requêtes et des réponses HTTP

May 5, 2023

L'appliance NetScaler ne vérifie pas la validité de la demande de légende HTTP. Par conséquent, avant de configurer les légendes HTTP, vous devez connaître le format d'une requête HTTP. Vous devez également connaître le format d'une réponse HTTP, car la configuration d'une légende HTTP implique la configuration d'expressions qui évaluent la réponse de l'agent de légende HTTP.

Cette section comprend les sections suivantes :

- Format d'une requête HTTP
- Format d'une réponse HTTP

Format d'une requête HTTP

Une requête HTTP contient une série de lignes qui se terminent chacune par un retour de transport et un début de ligne, représentés par l'une ou l'autre de ces deux manières `<CR><LF> or \r\n`.

La première ligne d'une requête (la *ligne de message*) contient la méthode HTTP et la cible. Par exemple, une ligne de message pour une requête GET contient le mot clé GET et une chaîne qui représente l'objet à récupérer, comme illustré dans l'exemple suivant :

```
GET /mysite/mydirectory/index.html HTTP/1.1\r\n
<!--NeedCopy-->
```

Le reste de la requête contient des en-têtes HTTP, y compris un en-tête Host obligatoire et, le cas échéant, le corps du message.

La demande se termine par une ligne bancaire (un supplément `<CR><LF> or \r\n`).

Voici un exemple de demande :

```
Get /mysite/index.html HTTP/1.1\r\n
Host: 10.101.101.10\r\n
Accept: \*/\*\r\n
\r\n
<!--NeedCopy-->
```

Format d'une réponse HTTP

Une réponse HTTP contient un message d'état, des en-têtes HTTP de réponse et l'objet demandé ou, si l'objet demandé ne peut pas être servi, un message d'erreur.

Voici un exemple de réponse :


```
HTTP/1.1 200 OK\r\n
Content-Length: 55\r\n
Content-Type: text/html\r\n
Last-Modified: Wed, 12 Aug 1998 15:03:50 GMT\r\n
Accept-Ranges: bytes\r\n
ETag:  “04f97692cbd1:377” \r\n
Date: Thu, 19 Jun 2008 19:29:07 GMT\r\n
\r\n
<55-character response>
<!--NeedCopy-->
```

Configuration d’une légende HTTP

May 5, 2023

Lorsque vous configurez une légende HTTP, vous spécifiez le type de demande (HTTP ou HTTPS), la destination et le format de la demande. Le format attendu de la réponse et, enfin, la partie de la réponse que vous souhaitez analyser.

Pour la destination, vous spécifiez soit l’adresse IP et le port de l’agent de légende HTTP. Vous pouvez également engager un serveur virtuel d’équilibrage de charge, de commutation de contenu ou de redirection de cache pour gérer les demandes de légende HTTP.

Dans le premier cas, les demandes de légende HTTP sont envoyées directement à l’agent de légende HTTP. Dans le second cas, les demandes de légende HTTP sont envoyées à l’adresse IP virtuelle (VIP) du serveur virtuel spécifié. Le serveur virtuel traite la demande de la même manière qu’il traite une demande client. Par exemple, si vous attendez à ce que de nombreuses légendes soient générées, vous pouvez configurer des instances de l’agent de légende HTTP sur plusieurs serveurs, lier ces instances (en tant que services) à un serveur virtuel d’équilibrage de charge, puis spécifier le serveur virtuel d’équilibrage de charge dans la configuration de légende HTTP. Le serveur virtuel d’équilibrage de charge équilibre ensuite la charge sur ces instances configurées comme déterminé par l’algorithme d’équilibrage de charge.

Pour le format de la demande de légende HTTP, vous pouvez spécifier les attributs individuels de la demande de légende HTTP (légende HTTP basée sur des attributs), ou vous pouvez spécifier l’intégralité de la demande de légende HTTP en tant qu’expression de stratégie avancée (légende HTTP basée sur une expression).

Pour le format de la demande de légende HTTP, vous pouvez spécifier les attributs individuels de la demande de légende HTTP (une légende HTTP basée sur des attributs) ou vous pouvez spécifier

l'intégralité de la demande de légende HTTP en tant qu'expression de stratégie avancée (une légende HTTP basée sur une expression).

Pour plus d'informations, voir Policy-HttpCallout

Paramètre	Description
Nom	Nom de la légende, 127 caractères maximum
Adresse IP et port (adresse *IP/port*) ou nom du serveur virtuel (vserver)	Adresse IPv4 ou IPv6 du serveur vers lequel la légende est envoyée, ou un caractère générique, et le port du serveur vers lequel la légende est envoyée, ou un caractère générique. Ou bien, le nom d'un serveur virtuel d'équilibrage de charge, de commutation de contenu ou de redirection de cache avec un type de service HTTP.
Méthode HTTP (HttpMethod)	Méthode HTTP (HttpMethod). Méthode utilisée dans la requête HTTP envoyée par cette légende. Valeurs valides : GET ou POST. Par défaut : GET.
Expression de l'hôte (HostexPR)	Expression de l'hôte (HosteXPR). Expression de texte avancée pour configurer l'en-tête Host. Longueur maximale : 255. L'expression peut être une valeur littérale ou une expression avancée qui dérive la valeur. Exemples : « 10.101.10.11 », « http.req.header (« hôte ») »
Expression de tige d'URL (URLStemExpr)	Expression de tige URL (URLSemExpr) Expression de chaîne avancée permettant de générer la souche d'URL. Longueur maximale : 8191. L'expression peut être une chaîne littérale ou une expression qui dérive la valeur. Exemples : « » /mysite/index.html « » « http.req.url »

Paramètre	Description
En-têtes HTTP (en-têtes)	En-têtes HTTP (en-têtes). Expression de texte avancée pour insérer des en-têtes HTTP et leurs valeurs dans la demande de légende HTTP. Spécifiez une valeur pour chaque en-tête. Vous spécifiez le nom de l'en-tête sous forme de chaîne et la valeur d'en-tête en tant qu'expression avancée. Spécifiez les en-têtes séparés par l'espace. Tels que -headers cip(client.ip.src) hdr(http.req.header("HDR")). Le nombre d'en-têtes peut être de 8
Demande d'envoi au serveur basée sur des expressions (FullReqExpr)	Requête HTTP exacte que NetScaler doit envoyer sous forme d'expression avancée de 8 191 caractères. Si vous spécifiez ce paramètre, vous devez omettre les arguments HttpMethod, HostexPR, URLStemExpr, en-têtes et paramètres. L'expression de requête est limitée par la fonction dans laquelle la légende est utilisée. Par exemple, une expression HTTP.RES ne peut pas être utilisée dans une banque de stratégies au moment de la demande ou dans une banque de stratégies de changement de contenu TCP.
Demande d'envoi au serveur basée sur des expressions (BodyExpr)	Expression de chaîne avancée permettant de générer le corps de la requête. L'expression peut contenir une chaîne littérale ou une expression qui dérive la valeur (par exemple, client.ip.src). S'exclut mutuellement avec -FullReqExpr.

Paramètre	Description
Paramètres	Expression avancée permettant d'insérer des paramètres de requête dans la requête HTTP envoyée par la légende. Spécifiez une valeur pour chaque paramètre que vous configurez. Si la demande de légende utilise la méthode GET, ces paramètres sont insérés dans l'URL. Si la demande de légende utilise la méthode POST, ces paramètres sont insérés dans le corps POST. Vous configurez le nom du paramètre de requête sous forme de chaîne et la valeur en tant qu'expression avancée. Les valeurs des paramètres sont codées par URL. Spécifiez les paramètres séparés par l'espace comme ⊠paramètres name1 (« name1") name2 (http.req.header (« hdr »)). Le maximum de 8 paramètres peut être configuré.
Type de retour (ReturnType)	Type de données renvoyées par l'application cible dans la réponse à la légende. Valeurs valides : TEXT : Traitez la valeur renvoyée comme une chaîne de texte. NUM : Traitez la valeur renvoyée comme un nombre. BOOL : Traitez la valeur renvoyée comme une valeur booléenne. Remarque : Vous ne pouvez pas modifier le type de retour une fois qu'il a été défini.

Paramètre	Description
Expression pour extraire des données de la réponse (ResultExpr)	Expression avancée qui extrait les objets HTTP.RES de la réponse à la légende HTTP. La longueur maximale est de 8191. Les opérations de cette expression doivent correspondre au type de retour. Par exemple, si vous configurez un type de texte renvoyé, l'expression de résultat doit être une expression textuelle. Si le type de retour est num, l'expression de résultat (ResultExpr) doit renvoyer une valeur numérique similaire à la suivante : « http.res.body (10000) .length » Remarque : Parfois, si vous définissez un type de retour TEXT et que le résultat envoyé par le serveur dépasse 16 Ko, l'expression de résultat peut renvoyer NULL. Par exemple, lorsque le résultat est une chaîne concaténée qui dépasse 16 Ko.
Modèle	Type de schéma pour le serveur de légende. Exemple : HTTP, https
Cache pour Secs	Durée, en secondes, pour laquelle la réponse de légende est mise en cache. Les réponses mises en cache sont stockées dans un groupe de contenu de mise en cache intégré appelé « CalloutContentGroup ». Si aucune durée n'est configurée, les réponses de légende ne sont pas mises en cache à moins qu'une configuration normale de mise en cache soit utilisée pour les mettre en cache. Ce paramètre prévaut sur toute configuration normale de mise en cache qui s'appliquerait autrement à ces réponses.

Remarque : L'appliance ne vérifie pas la validité de la demande. Vous devez vous assurer que la demande est valide et qu'elle ne contient aucune information confidentielle. Une configuration de légende HTTP incorrecte ou incomplète entraîne une condition UNDEF d'exécution qui n'est pas associée à une action. La condition UNDEF met simplement à jour le compteur d'accès non définis, ce qui vous permet de dépanner une légende HTTP mal configurée. Toutefois, l'appliance

analyse la demande de légende HTTP pour vous permettre de configurer certaines fonctionnalités de NetScaler pour la légende. Cela peut conduire à une légende HTTP qui s'appelle elle-même. Pour plus d'informations sur la récursion de légende et sur la façon de l'éviter, reportez-vous à la section Éviter la récursion des légendes HTTP.

Enfin, que vous utilisiez des attributs de requête HTTP ou une expression pour définir le format de la demande de légende HTTP, vous devez spécifier le format de la réponse à partir de l'agent de légende HTTP et la partie de la réponse que vous souhaitez évaluer. Le type de réponse peut être une valeur booléenne, un nombre ou un texte. En fonction de ce type de retour uniquement, vous pouvez utiliser les autres méthodes d'expression sur la réponse de légende. Si le type de retour est un nombre, vous pouvez utiliser l'expression basée sur le nombre sur la réponse de légende. La partie de la réponse que vous souhaitez évaluer est spécifiée par une expression. Par exemple, si vous spécifiez que la réponse contient du texte, vous pouvez utiliser `HTTP.RES.BODY(<unit>)` pour spécifier que l'appliance doit évaluer uniquement les premiers <unit>octets de la réponse de l'agent de légende.

Sur la ligne de commande, vous créez d'abord une légende HTTP à l'aide de la commande add. Lorsque vous ajoutez une légende, tous les paramètres sont définis sur la valeur par défaut NONE, à l'exception de la méthode HTTP, qui est définie sur la valeur par défaut GET. Vous configurez ensuite les paramètres de la légende à l'aide de la commande set. La commande set permet de configurer les deux types de légendes (basées sur l'attribut et sur l'expression). La différence réside dans les paramètres utilisés pour configurer les deux types de légendes. Ainsi, les instructions de ligne de commande suivantes incluent une commande set pour configurer une légende basée sur des attributs et une commande set pour configurer une légende basée sur une expression. Dans l'utilitaire de configuration, toutes ces tâches de configuration sont exécutées dans une seule boîte de dialogue.

Remarque : Avant de placer une légende HTTP dans une stratégie, vous pouvez modifier tous les paramètres configurés à l'exception du type de retour. Une fois qu'une légende HTTP est dans une stratégie, vous ne pouvez pas modifier complètement une expression configurée dans la légende. Par exemple, vous ne pouvez pas remplacer HTTP.REQ.HEADER (« myval ») par CLIENT.IP.SRC. Vous pouvez modifier les opérateurs et les arguments transmis à l'expression. Par exemple, vous pouvez changer `HTTP.REQ.HEADER("myVal1")` sur `HTTP.REQ.HEADER("myVal2")`, ou `HTTP.REQ.HEADER("myVal")` sur `HTTP.REQ.HEADER("myVal").AFTER_STR(<string>)`. Si la commande set échoue, créez une légende HTTP.

La configuration des légendes HTTP implique la configuration des expressions de stratégie avancées. Pour plus d'informations sur la configuration des expressions de stratégie avancées, consultez Configuration des expressions de stratégie avancées : mise en route.

Pour configurer une légende HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

Créez une légende HTTP.


```
add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port<
    port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (
    GET | POST )] [-hostExpr <expression>]  [-urlStemExpr <expression>]
    [-headers <name(value)> ...] [-parameters <name(value)> ...] [-
    bodyExpr <expression>] [-fullReqExpr <expression>] [-scheme ( http |
     https )] [-resultExpr <expression>] [-cacheForSecs <secs>] [-
    comment <string>]

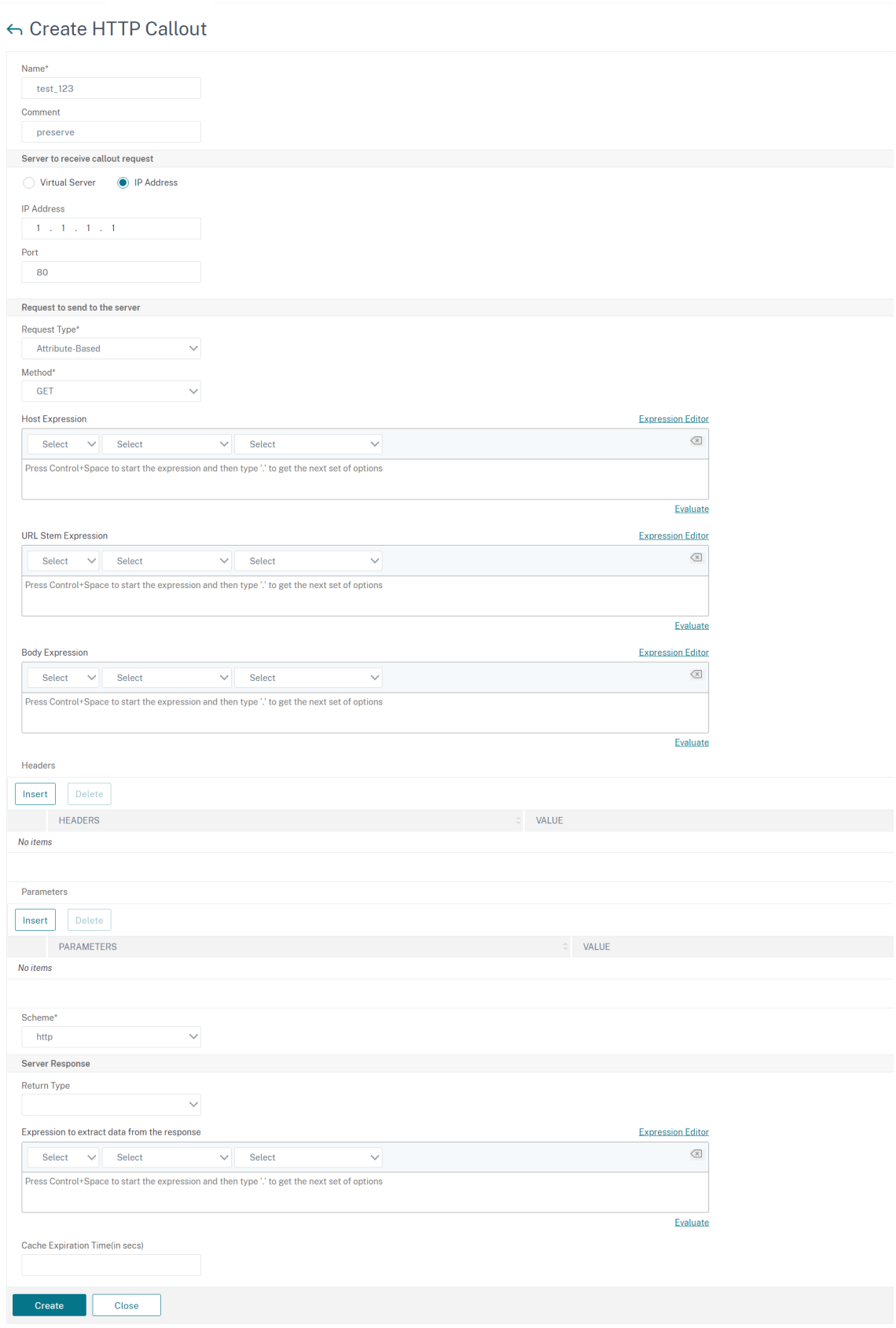
<!--NeedCopy-->
```

Exemple :

```
add policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader")-
    resultExpr "http.res.body(10000).length"

<!--NeedCopy-->
```

Modifiez la configuration de la légende HTTP.

```
set policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr|\*>] [-
    port <port|\*>] [-vServer <string>] [-returnType <returnType>] [-
    httpMethod ( GET | POST )] [-hostExpr <string>] [-urlStemExpr <
    string>] [-headers <name(value)> ...] [-parameters <name(value)>
    ...] [-resultExpr <string>]

<!--NeedCopy-->
```

Exemple :

```
> set policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader") -
    resultExpr "http.res.body(10000).length"
<!--NeedCopy-->
```

Configurez la légende HTTP à l'aide du paramètre FullReqExpr.

```
set policy httpCallout <name> [-vServer <string>] [-returnType <
    returnType>] [-fullReqExpr <string>] [-resultExpr <string>]
<!--NeedCopy-->
```

Exemple :


```
> set policy httpCallout mycallout1 -vserver lbv1 -returnType num
    fullReqExpr q{
 "GET " + http.req.url + "HTTP/" + http.req.version.major + "." + http.
    req.version.minor.sub(1) + "r\nHost:10.101.10.10\r\nAccept: \*/\*\r
    \n\r\n" }


<!--NeedCopy-->
```

Vérifiez les configurations de la légende HTTP.

```
show policy httpCallout `<name>`

sh policy httpCallout mycallout1
> Name: mycallout1
>Vserver: lbv1 (UP)
Effective Vserver state: UP
Return type: TEXT
Scheme: HTTP
Full REQ expr: "GET " + http.req.url + "HTTP/" + http.req.version.major
    + "." + http.req.version.minor.sub(1)+ "r\nHost:10.101.10.10\r\
   nAccept: \*/\*\r\n\r\n"
Result expr: http.res.body(100)
Hits: 0
Undef Hits: 0
Done
>

<!--NeedCopy-->
```

Pour configurer une légende HTTP à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert > AppExpert** > **AppAllets HTTP**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une légende HTTP**, configurez les paramètres de la légende HTTP. Pour obtenir une description du paramètre, placez le curseur de la souris sur la case à cocher.
4. Cliquez sur **Create**, puis cliquez sur **Close**.



Vérification de la configuration

May 5, 2023

Pour qu'une légende HTTP fonctionne correctement, tous les paramètres de légende HTTP et les entités associées à la légende doivent être correctement configurés. Bien que l'appliance NetScaler ne vérifie pas la validité des paramètres de légende HTTP, elle indique l'état des entités liées, à savoir le serveur ou le serveur virtuel auquel la légende HTTP est envoyée. Le tableau suivant répertorie les icônes et décrit les conditions dans lesquelles elles s'affichent.

Icône	Indique que
	L'état du serveur qui héberge l'agent de légende HTTP ou du serveur virtuel d'équilibrage de charge, de commutation de contenu ou de redirection de cache auquel la légende HTTP est envoyée est UP.
	L'état du serveur qui héberge l'agent de légende HTTP ou du serveur virtuel d'équilibrage de charge, de commutation de contenu ou de redirection de cache auquel la légende HTTP est envoyée est HORS SERVICE.
	L'état du serveur qui héberge l'agent de légende HTTP ou du serveur virtuel d'équilibrage de charge, de commutation de contenu ou de redirection de cache auquel la légende HTTP est envoyée est DOWN.

Tableau 1. Icônes indiquant l'état des entités liées à une légende HTTP

Pour qu'une légende HTTP fonctionne correctement, l'icône doit être verte à tout moment. Si l'icône n'est pas verte, vérifiez l'état du serveur de légende ou du serveur virtuel auquel la légende HTTP est envoyée. Si la légende HTTP ne fonctionne pas comme prévu alors que l'icône est verte, vérifiez les paramètres configurés pour la légende.

Vous pouvez également vérifier la configuration en envoyant des demandes de test qui correspondent à la politique à partir de laquelle la légende HTTP est invoquée, en vérifiant le compteur d'accès pour la politique et la légende HTTP, et en vérifiant les réponses que l'appliance NetScaler envoie au client.

Remarque : Une légende HTTP peut parfois s'invoquer de manière récursive une seconde fois. Dans ce cas, le compteur d'accès est incrémenté de deux fois pour chaque appel généré par l'appliance. Pour

que le compteur de hits affiche la valeur correcte, vous devez configurer la légende HTTP de telle sorte qu'elle ne s'invoque pas une seconde fois. Pour plus d'informations sur la façon d'éviter la récursion de légende HTTP, consultez la section Éviter la récursion des légendes HTTP.

Pour afficher le compteur d'accès d'une légende HTTP

1. Accédez à **AppExpert > AppExpert** > **AppAllets HTTP**.
2. Dans le volet d'informations, cliquez sur la légende HTTP pour laquelle vous souhaitez afficher le compteur de résultats, puis affichez les résultats dans la zone **Détails** .

Appel d'une légende HTTP

May 9, 2023

Après avoir configuré une légende HTTP, vous l'appelez en incluant l' `SYS.HTTP_CALLOUT(<name>)` expression dans une règle de stratégie avancée. Dans cette expression, `<name>` il s'agit du nom de la légende HTTP que vous souhaitez appeler.

Vous pouvez utiliser des opérateurs d'expression de stratégie avancée avec l'expression de légende pour traiter la réponse, puis effectuer une action appropriée. Le type de retour de la réponse de l'agent de légende HTTP détermine le jeu d'opérateurs que vous pouvez utiliser sur la réponse. Si la partie de la réponse que vous souhaitez analyser est du texte, vous pouvez utiliser un opérateur de texte pour analyser la réponse. Par exemple, vous pouvez utiliser l' <string> opérateur CONTAINS (\) pour vérifier si la partie spécifiée de la réponse contient une chaîne particulière, comme dans l'exemple suivant :

```
SYS.HTTP_CALLOUT(mycallout).contains("Good IP address")
<!--NeedCopy-->
```

Si vous utilisez l'expression précédente dans une stratégie de répondeur, vous pouvez configurer une action de répondeur appropriée.

De même, si la partie de la réponse que vous souhaitez évaluer est un nombre, vous pouvez utiliser un opérateur numérique tel que GT (int). Si la réponse contient une valeur booléenne, vous pouvez utiliser un opérateur booléen.

Remarque : Une légende HTTP peut s'appeler elle-même de manière récursive. La récursion des légendes HTTP peut être évitée en combinant l'expression de légende HTTP avec une expression de stratégie avancée qui empêche la récursion. Pour plus d'informations sur la façon d'éviter la récursion de légende HTTP, reportez-vous à la section Éviter la récursion des légendes HTTP.

Vous pouvez également mettre en cascade les légendes HTTP en configurant des stratégies qui appellent chacune une légende après avoir évalué les légendes générées précédemment. Dans ce scénario,

lorsqu'une politique appelle une légende, lorsque l'appliance NetScaler analyse la légende avant de l'envoyer au serveur de légende, un deuxième ensemble de politiques peut évaluer la légende et invoquer des légendes supplémentaires, qui peuvent à leur tour être évaluées par un troisième ensemble de politiques, et ainsi de suite. Une telle implémentation est décrite dans l'exemple suivant.

Tout d'abord, vous pouvez configurer une légende HTTP appelée MyCallout1, puis configurer une stratégie de répondeur, Pol1, pour appeler MyCallout1. Vous pouvez ensuite configurer une deuxième légende HTTP, MyCallout2, et une stratégie de répondeur, Pol2. Vous configurez Pol2 pour évaluer MyCallout1 et invoquer MyCallout2. Vous liez les deux stratégies de répondeur globalement.

Pour éviter la récursion des légendes HTTP, MyCallout1 est configuré avec un en-tête HTTP personnalisé unique appelé « Request1 ». « Pol1 est configuré pour éviter la récursion des légendes HTTP à l'aide de l'expression de stratégie avancée,

```
HTTP.REQ.HEADER("Request1").EQ("Callout Request").NOT.
<!--NeedCopy-->
```

Pol2 utilise la même expression de politique avancée, mais exclut l'opérateur .NOT afin que la politique évalue MyCallout1 lorsque l'appliance NetScaler l'analyse. Notez que MyCallout2 identifie son propre en-tête unique appelé « Request2 », et Pol2 inclut une expression de stratégie avancée pour empêcher MyCallout2 de s'appeler récursivement.

Exemple :

```
> add policy httpCallout myCallout1

Done

> set policy httpCallout myCallout1 -IPAddress 10.102.3.95 -port 80 -
   returnType TEXT -hostExpr
 ""10.102.3.95"" -urlStemExpr ""/cgi-bin/check_clnt_from_database.pl""
    -headers Request1
("Callout Request") -parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.
   RES.BODY(100)"

Done

> add responder policy Pol1 "HTTP.REQ.HEADER("Request1").EQ("Callout
   Request").NOT &&
SYS.HTTP_CALLOUT(myCallout1).CONTAINS("IP Matched")" RESET

Done

> bind responder global Pol1 100 END -type OVERRIDE

```



```
Done

> add policy httpCallout myCallout2

Done

> set policy httpCallout myCallout2 -IPAddress 10.102.3.96 -port 80 -
   returnType TEXT -hostExpr
""10.102.3.96"" -urlStemExpr ""/cgi-bin/
   check_clnt_location_from_database.pl"" -headers Request2
("Callout Request") -parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.
   RES.BODY(200)"

 Done

> add responder policy Pol2 "HTTP.REQ.HEADER("Request2").EQ("Callout
   Request").NOT &&
 HTTP.REQ.HEADER("Request1").EQ("Callout Request") && SYS.HTTP_CALLOUT(
    myCallout2).CONTAINS
("APAC")" RESET

 Done

> bind responder global Pol2 110 END -type OVERRIDE

Done
<!--NeedCopy-->
```

Éviter la récursion de légende HTTP

May 5, 2023

Même si l'appliance NetScaler ne vérifie pas la validité de la demande de légende HTTP, elle analyse la demande une fois avant de l'envoyer à l'agent de légende HTTP. Cette analyse permet à l'appliance de traiter la demande de légende comme n'importe quelle autre demande entrante, ce qui vous permet de configurer plusieurs fonctionnalités utiles de NetScaler (telles que la mise en cache intégrée) pour qu'elles fonctionnent sur la demande de légende.

Toutefois, au cours de cette analyse, la demande de légende HTTP peut sélectionner la même stratégie et donc s'invoquer de manière récursive. La solution matérielle-logicielle détecte l'appel récursif et déclenche une condition undefined (UNDEF). Toutefois, l'appel récursif entraîne l'incrémentation des compteurs de sélection de stratégie et de légende HTTP de deux points chacun au lieu d'un décompte

chacun.

Pour empêcher qu'une légende ne s'appelle elle-même, vous devez identifier au moins une caractéristique unique de la demande de légende HTTP, puis exclure toutes les demandes avec cette caractéristique du traitement par la règle de stratégie qui appelle la légende. Pour ce faire, vous pouvez inclure une autre expression de stratégie avancée dans la règle de stratégie. L'expression doit précéder l' `SYS.HTTP_CALLOUT(<name>)` expression de sorte qu'elle soit évaluée avant l'évaluation de l'expression de légende. Par exemple :

```
<Expression that prevents callout recursion> OR SYS.HTTP_CALLOUT(<name
    >)
<!--NeedCopy-->
```

Lorsque vous configurez une règle de stratégie de cette manière, lorsque la solution matérielle-logicielle génère la demande et l'analyse, la règle composée prend la valeur FALSE, la légende n'est pas générée une deuxième fois et les compteurs de sélection sont incrémentés correctement.

Une façon d'attribuer une caractéristique unique à une demande de légende HTTP consiste à inclure un en-tête HTTP personnalisé unique lorsque vous configurez la légende. Voici un exemple d'une légende HTTP appelée « MyCallout ». « La légende génère une requête HTTP qui vérifie si l'adresse IP d'un client est présente dans une base de données d'adresses IP sur liste noire. La légende inclut un en-tête personnalisé appelé « Demande », qui est défini sur la valeur « Demande de légende ». « Une stratégie de répondeur globalement liée, « Pol1 », appelle la légende HTTP mais exclut toutes les demandes dont l'en-tête Request est défini sur cette valeur, empêchant ainsi un second appel de MyCallout. L'expression qui empêche un deuxième appel est HTTP.REQ.HEADER (« Request ») .EQ (« Callout Request ») .NOT.

Exemple :

```
> add policy httpCallout myCallout
 Done

> set policy httpCallout myCallout -IPAddress 10.102.3.95 -port 80 -
    returnType TEXT -hostExpr ""10.102.3.95"" -urlStemExpr ""/cgi-bin/
    check_clnt_from_database.pl"" -headers Request("Callout Request") -
    parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.RES.BODY(100)"
Done

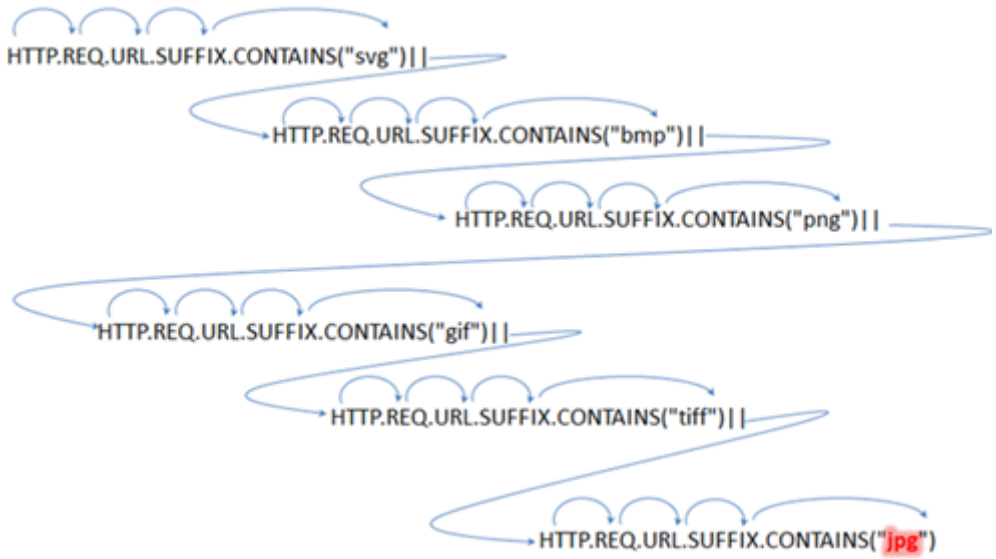
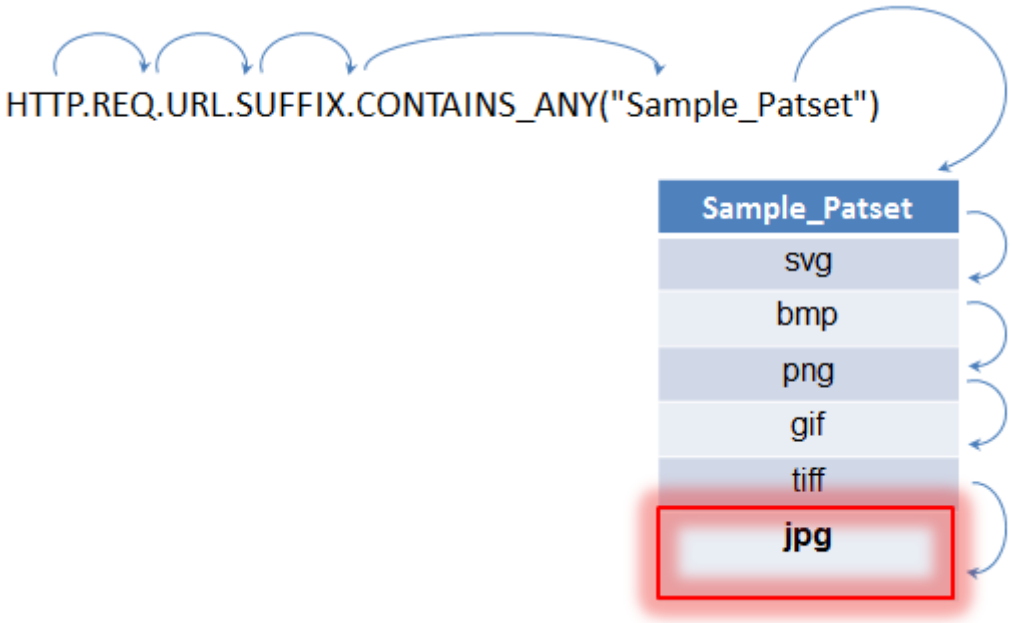
> add responder policy Pol1 "HTTP.REQ.HEADER("Request").EQ("Callout
    Request").NOT && SYS.HTTP_CALLOUT(myCallout).CONTAINS("IP Matched")"
     RESET
Done

> bind responder global Pol1 100 END -type OVERRIDE
Done
```



```
<!--NeedCopy-->
```

> **Remarque :**
> Vous pouvez également configurer une expression pour vérifier si l'URL de la demande inclut l'expression hampe configurée pour la légende HTTP. Pour implémenter la solution, assurez-vous que l'agent de légende HTTP ne peut répondre qu'aux appels HTTP et non aux autres requêtes dirigées via la solution matérielle-logicielle. Si l'agent de légende HTTP est une application ou un serveur Web qui répond à d'autres demandes client, une telle expression empêche la solution matérielle-logicielle de traiter ces demandes client. Utilisez plutôt un en-tête personnalisé unique comme décrit précédemment.

Mise en cache des réponses de légende HTTP

August 20, 2021

Pour améliorer les performances lors de l'utilisation des légendes, vous pouvez utiliser la fonction de mise en cache intégrée pour mettre en cache les réponses des légendes. Les réponses sont stockées dans un groupe de contenu de mise en cache intégré nommé CalloutContentGroup pour une durée spécifiée.

Remarque : Pour mettre en cache les réponses de légende, assurez-vous que la fonction de mise en cache intégrée est activée.

Pour définir la durée du cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set policy httpCallout <name> -cacheForSecs <secs>
```

Exemple :

```
> set httpcallout httpcallout1 -cacheForSecs 120
<!--NeedCopy-->
```

Pour définir la durée du cache à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert > Légendes HTTP**.
2. Dans le volet d'informations, sélectionnez la légende HTTP pour laquelle vous souhaitez définir la durée du cache et cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer la légende HTTP**, spécifiez l'**heure d'expiration du cache** .

4. Vérifiez que vous avez entré la durée correcte, puis cliquez sur **OK**.

Cas d'utilisation : filtrage des clients à l'aide d'une liste noire IP

May 5, 2023

Les appels HTTP peuvent être utilisés pour bloquer les demandes des clients qui sont mis sur liste noire par l'administrateur. La liste des clients peut être une liste noire connue du public, une liste noire que vous gérez pour votre organisation ou une combinaison des deux.

L'appliance NetScaler vérifie l'adresse IP du client par rapport à la liste noire préconfigurée et bloque la transaction si l'adresse IP figure sur la liste noire. Si l'adresse IP ne figure pas dans la liste, la solution matérielle-logicielle traite la transaction.

Pour implémenter cette configuration, vous devez effectuer les tâches suivantes :

1. Activez le répondeur sur l'appliance NetScaler.
2. Créez une légende HTTP sur l'appliance NetScaler et configurez-la avec des détails sur le serveur externe et les autres paramètres requis.
3. Configurez une stratégie de répondeur pour analyser la réponse à l'appel HTTP, puis liez la stratégie globalement.
4. Créez un agent de légende HTTP sur le serveur distant.

Activation du répondeur

Vous devez activer le répondeur avant de pouvoir l'utiliser.

Pour activer le répondeur à l'aide de l'interface graphique

1. Assurez-vous d'avoir installé la licence du répondeur.
2. Dans l'utilitaire de configuration, développez AppExpert, cliquez avec le bouton droit sur **Répondeur**, puis cliquez sur **Activer la fonctionnalité Répondeur** .

Création d'une légende HTTP sur l'appliance NetScaler

Créez une légende HTTP, HTTP_Callout, avec les paramètres indiqués dans le tableau suivant. Pour plus d'informations sur la création d'une légende HTTP, consultez Configuration d'une légende HTTP PDF.

Configuration d'une stratégie de répondeur et liaison globale

Après avoir configuré la légende HTTP, vérifiez la configuration de la légende, puis configurez une stratégie de répondeur pour appeler la légende. Bien que vous puissiez créer une stratégie de répondeur dans le sous-nœud
Stratégies, puis la lier globalement à l'aide du
Responder Policy Manager, cette démonstration utilise le
Responder Policy Manager pour créer la stratégie de répondeur et la lier globalement.

Pour créer une stratégie de répondeur et la lier globalement à l'aide de

1. Accédez à **AppExpert** > **Répondeur**.
2. Dans le volet d'informations, sous **Gestionnaire de stratégies**, cliquez sur **Gestionnaire de stratégies**.
3. Dans la boîte de dialogue **Responder Policy Manager**, cliquez sur **Remplacer la stratégie globale**.
4. Cliquez sur **Insérer une stratégie**, puis, sous **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**.
5. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :
   a) Dans Nom, saisissez **PolicyResponder1**.
   b) Dans **Action**, sélectionnez **RESET**.
   c) Dans Action de **résultat non défini, sélectionnez Actionglobale de résultat non défini** .
   d) Dans **Expression**, tapez l'expression de stratégie avancée suivante :

```
"HTTP.REQ.HEADER("Request").EQ("Callout Request").NOT && SYS.
   HTTP_CALLOUT(HTTP_Callout).CONTAINS("IP Matched")"
<!--NeedCopy-->
```

   e) Cliquez sur **Créer**, puis sur **Fermer**.
6. Cliquez sur **Appliquer les modifications**, puis sur **Fermer**.

Création d'un agent de légende HTTP sur le serveur distant

Vous devez maintenant créer un agent de légende HTTP sur le serveur de légende distant qui recevra les demandes de légende de l'appliance NetScaler et y répondra de manière appropriée. L'agent de légende HTTP est un script différent pour chaque déploiement et doit être écrit en tenant compte des spécifications du serveur, telles que le type de base de données et le langage de script pris en charge.

Voici un exemple d'agent de légende qui vérifie si l'adresse IP donnée fait partie d'une liste noire d'adresses IP. L'agent a été écrit dans le langage de script Perl et utilise une base de données MYSQL.

Le script CGI suivant vérifie la présence d'une adresse IP donnée sur le serveur de légendes.

```
#!/usr/bin/perl -w
print "Content-type: text/html\n\n";
        use DBI();
        use CGI qw(:standard);
#Take the Client IP address from the request query
        my $ip_to_check = param('cip');
# Where a MYSQL database is running
        my $dsn = 'DBI:mysql:BAD_CLIENT:localhost';
# Database username to connect with
        my $db_user_name =  'dbuser' ;
# Database password to connect with
        my $db_password = 'dbpassword';
        my ($id, $password);
# Connecting to the database
        my $dbh = DBI->connect($dsn, $db_user_name, $db_password);
        my $sth = $dbh->prepare(qq{
  select * from bad_clnt  }
 );
        $sth->execute();
        while (my ($ip_in_database) = $sth->fetchrow_array()) {

        chomp($ip_in_database);
# Check for IP match
        if ($ip_in_database eq $ip_to_check) {

              print "\n IP Matched\n";
                                                    $sth->finish();
                                               exit;
                 }

        }

       print "\n IP Failed\n";
       $sth->finish();
       exit;
<!--NeedCopy-->
```


Cas d'utilisation : prise en charge ESI pour la récupération et la mise à jour dynamique du contenu

May 9, 2023

Edge Side Includes (ESI) est un langage de balisage destiné à l'assemblage de contenu Web dynamique au niveau de la périphérie. Il aide à accélérer les applications Web dynamiques en définissant un langage de balisage simple pour décrire les composants de page Web pouvant être mis en cache et non mis en cache qui peuvent être agrégés, assemblés et fournis à la périphérie du réseau. En utilisant les légendes HTTP sur l'appliance NetScaler, vous pouvez lire les constructions ESI et agréger ou assembler le contenu de manière dynamique.

Pour implémenter cette configuration, vous devez effectuer les tâches suivantes :

1. Activez la réécriture sur l'appliance NetScaler.
2. Créez une légende HTTP sur la solution matérielle-logicielle et configurez-la avec des détails sur le serveur externe et d'autres paramètres requis.
3. Configurez une action de réécriture pour remplacer le contenu ESI par le corps de réponse de légende.
4. Configurez une stratégie de réécriture pour spécifier les conditions dans lesquelles l'action est exécutée, puis liez la stratégie de réécriture globalement.

Activation de la réécriture

La réécriture doit être activée avant d'être utilisée sur l'appliance NetScaler. La procédure suivante décrit les étapes à suivre pour activer la fonction de réécriture.

Pour activer la réécriture à l'aide de l'interface graphique

1. Assurez-vous d'avoir installé la licence de réécriture.
2. Dans l'utilitaire de configuration, développez AppExpert, cliquez avec le bouton droit de la souris sur Réécrire, puis cliquez sur Activer la fonction de réécriture.

Création d'une légende HTTP sur l'appliance NetScaler

Pour plus d'informations sur la création d'une légende HTTP, consultez Configuration d'une légende HTTP.
Pour plus d'informations sur les valeurs des paramètres, voir Paramètres et valeurs pour HTTP-Callout-2 pdf.

Configuration de l'action de réécriture

Créez une action de réécriture, Action-Rewrite-1, pour remplacer le contenu ESI par le corps de réponse de légende. Utilisez les paramètres affichés dans le tableau suivant.

Tableau 2 Paramètres et valeurs pour Action-Rewrite-1

Paramètre	Valeur
Nom	Action-Rewrite-1
Type	Remplacer
Expression pour choisir la référence du texte cible	"HTTP.RES.BODY(500).AFTER_STR (\" <example>\").BEFORE_STR (\"</example>\")"
Expression de chaîne pour le texte de remplacement	"SYS.HTTP_CALLOUT(HTTP-Callout-2)"

Pour configurer l'action de réécriture à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Réécrire** > **Actions**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action de réécriture**, dans Nom, tapez **Action-Rewrite-1**.
4. Dans Type, sélectionnez **REMPLACER**.
5. Dans **Expression** pour choisir une référence de texte cible, tapez l'expression de stratégie avancée suivante :

```
1 "HTTP.RES.BODY(500).AFTER_STR("<example>").BEFORE_STR("<example>")
     "
2 <!--NeedCopy-->
```

6. Dans l'expression String pour le texte de remplacement, tapez l'expression de chaîne suivante :

```
1 "SYS.HTTP_CALLOUT(HTTP-Callout-2)"
2 <!--NeedCopy-->
```

7. Cliquez sur **Créer**, puis sur **Fermer**.

Création de la stratégie de réécriture et liaison globale

Créez une stratégie de réécriture, Policy-Rewrite-1, avec les paramètres affichés dans le tableau suivant. Vous pouvez créer une stratégie de réécriture dans le sous-nœud

Policies, puis la lier globalement à l'aide du Gestionnaire de stratégies de réécriture. Vous pouvez également utiliser le Gestionnaire de stratégies de réécriture pour effectuer ces deux tâches simultanément. Cette démonstration utilise le Gestionnaire de stratégies de réécriture pour effectuer les deux tâches.

Tableau 3. Paramètres et valeurs pour Policy-Rewrite-1

Paramètre	Valeur
Nom	Policy-Rewrite-1
Action	Action_Rewrite-1
Action de résultat non définie	-Global undefined-result action-
Expression	"HTTP.REQ.HEADER("Name").CONTAINS ("Callout").NOT"

Pour configurer une stratégie de réécriture et la lier globalement à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Rewrite**.
2. Dans le volet d'informations, sous **Gestionnaire de stratégies**, cliquez sur **Réécrire le Gestionnaire de stratégies**.
3. Dans la boîte de dialogue **Gestionnaire de stratégies de réécriture**, cliquez sur **Remplacer la stratégie globale**.
4. Cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**.
5. Dans la boîte de dialogue **Créer une stratégie de réécriture**, procédez comme suit :
   1.Dans Nom, tapez Policy-Rewrite-1.
   a) Dans Action, sélectionnez Action-Rewrite-1.
   b) Dans Action de résultat non défini, sélectionnez Actionglobale de résultat non défini .
   c) Dans Expression, tapez l'expression de stratégie avancée suivante :

```
"HTTP.REQ.HEADER("Name").CONTAINS("Callout").NOT"
<!--NeedCopy-->
```

   a) Cliquez sur **Créer**, puis sur **Fermer**.
6. Cliquez sur **Appliquer les modifications**, puis sur **Fermer**.

Cas d'utilisation : contrôle d'accès et authentification

May 5, 2023

Dans les zones de haute sécurité, il est obligatoire d'authentifier l'utilisateur en externe avant que les clients n'accèdent à une ressource. Sur l'appliance NetScaler, vous pouvez utiliser des légendes HTTP pour authentifier l'utilisateur de manière externe en évaluant les informations d'identification fournies. Dans cet exemple, l'hypothèse est que le client envoie le nom d'utilisateur et le mot de passe via les en-têtes HTTP de la demande. Toutefois, les mêmes informations peuvent être récupérées à partir de l'URL ou du corps HTTP.

Pour implémenter cette configuration, vous devez effectuer les tâches suivantes :

1. Activez la fonctionnalité de répondeur sur l'appliance NetScaler.
2. Créez une légende HTTP sur la solution matérielle-logicielle et configurez-la avec des détails sur le serveur externe et d'autres paramètres requis.
3. Configurez une politique de répondeur pour analyser la réponse, puis liez-la globalement.
4. Créez un agent d'appel sur le serveur distant.

Activation du répondeur

La fonctionnalité de répondeur doit être activée avant d'être utilisée sur l'appliance NetScaler.

Pour activer le répondeur à l'aide de l'utilitaire de configuration

1. Assurez-vous que la licence du répondeur est installée.
2. Dans l'utilitaire de configuration, développez AppExpert, cliquez avec le bouton droit sur Responder, puis cliquez sur **Activer la fonctionnalité Responder**.

Création d'une légende HTTP sur l'appliance NetScaler

Créez une légende HTTP, HTTP-Callout-3, avec les paramètres indiqués dans le tableau suivant. Pour plus d'informations sur la création d'une légende HTTP, consultez Configuration d'une légende HTTP.

Tableau 1. Paramètres et valeurs pour HTTP-Callout-3

Paramètre	Valeur	Nom
Nom	Policy-Responder-3	

Paramètre

Valeur

Nom

HTTP-Callout-3

Serveur devant recevoir la demande d’appel :

Adresse IP

10.10.3.9.95

Port

80

Demande à envoyer au serveur :

Méthode

GET

Expression hôte

10.102.3.95

Expression racine d’URL

« /cgi-bin/authenticate.pl »

En-têtes :

Nom

Demander

Expression de valeur

Demande d’appel

Paramètres :

Nom

Nom d’utilisateur

Expression de valeur

HTTP.REQ.HEADER (« Nom d’utilisateur ») .VALUE (0)

Nom

Mot de passe

Expression de valeur

HTTP.REQ.HEADER (« Mot de passe ») .VALUE (0)

Réponse du serveur :

Type de retour

TEXTE

Expression pour extraire les données de la réponse

HTTP.RES.BODY (100)

Création d'une politique de réponse pour analyser la réponse

Créez une politique de réponse, Policy-Responder-3, qui vérifiera la réponse du serveur d'appel et réinitialisera la connexion si l'adresse IP source a été mise sur liste noire. Créez la politique avec les paramètres indiqués dans le tableau suivant. Bien que vous puissiez créer une politique de répondeur dans le sous-nœud
Politiques, puis la lier globalement à l'aide du
Responder Policy Manager, cette démonstration utilise le
Responder Policy Manager pour créer la politique de répondeur et lier la politique de manière globale.

Tableau 2 Paramètres et valeurs pour Policy-Responder-3

Paramètre	Valeur
Nom	Policy-Responder-3
Action	RÉINITIALISER
Action-résultat-action non défini	-Global undefined-result action-
Expression	« HTTP.REQ.HEADER (\" Request \ ») .EQ (\ "Demande d'appel \ ») .NOT && SYS.HTTP_CALLOUT (HTTP-Callout-3) .CONTAINS (\ "L'authentification a échoué \ ») »

Pour créer une politique de réponse et la lier globalement à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Répondeur**.
2. Dans le volet de détails, sous **Policy Manager**, cliquez sur **Responder Policy Manager**.
3. Dans la boîte de dialogue **Responder Policy Manager**, cliquez sur **Override Global**.
4. Cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**.
5. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :

a) Dans Nom, tapez Policy-Responder-3.
b) Dans Action, sélectionnez **RÉINITIALISER**.
c) Dans Action à résultat non défini, sélectionnez Action globale à résultat non défini.
d) Dans la zone de texte Expression, tapez :

```
"HTTP.REQ.HEADER("Request").EQ("Callout Request").NOT && SYS.
   HTTP_CALLOUT(HTTP-Callout-3).CONTAINS("Authentication Failed")"
<!--NeedCopy-->
```

a) Cliquez sur **Créer**, puis sur **Fermer**.

6. Cliquez sur **Appliquer les modifications**, puis sur **Fermer**.

Création d'un agent de légende HTTP sur le serveur distant

Vous devez maintenant créer un agent de légende HTTP sur le serveur de légende distant. L'agent de légende HTTP reçoit les demandes de légende de l'appliance NetScaler et y répond de manière appropriée. L'agent d'appel est un script différent pour chaque déploiement qui doit être écrit en tenant compte des spécifications du serveur, telles que le type de base de données et le langage de script pris en charge.

Vous trouverez ci-dessous un exemple de pseudo-code d'agent de rappel qui vérifie si le nom d'utilisateur et le mot de passe fournis sont valides. L'agent peut être implémenté dans le langage de programmation de votre choix. Le pseudo-code ne doit être utilisé que comme guide pour le développement de l'agent d'appel. Vous pouvez intégrer des fonctionnalités supplémentaires au programme.

Pour vérifier le nom d'utilisateur et le mot de passe fournis à l'aide d'un pseudo-code

1. Acceptez le nom d'utilisateur et le mot de passe fournis dans la demande et formatez-les de manière appropriée.
2. Connectez-vous à la base de données qui contient tous les noms d'utilisateur et mots de passe valides.
3. Vérifiez les informations d'identification fournies par rapport à votre base de données.
4. Formatez la réponse comme l'exige la légende HTTP.
5. Envoyez la réponse à l'appliance NetScaler.

Cas d'utilisation : filtrage du spam basé sur OWA

May 5, 2023

Le filtrage du spam est la capacité de bloquer de manière dynamique les e-mails qui ne proviennent pas d'une source connue ou fiable ou dont le contenu est inapproprié. Le filtrage du courrier indésirable nécessite une logique métier associée qui indique qu'un type particulier de message est du courrier indésirable. Lorsque l'appliance NetScaler traite les messages Outlook Web Access (OWA) en fonction du protocole HTTP, les légendes HTTP peuvent être utilisées pour filtrer le courrier indésirable.

Vous pouvez utiliser des légendes HTTP pour extraire n'importe quelle partie du message entrant et vérifier auprès d'un serveur de légende externe qui a été configuré avec des règles destinées à déterminer si un message est légitime ou s'il s'agit d'un courrier indésirable. En cas de courrier indésirable, pour des raisons de sécurité, l'appliance NetScaler n'informe pas l'expéditeur que l'e-mail est marqué comme spam.

L'exemple suivant effectue une vérification très basique des différents mots clés répertoriés dans l'objet de l'e-mail. Ces contrôles peuvent s'avérer plus complexes dans un environnement de production.

Pour implémenter cette configuration, vous devez effectuer les tâches suivantes :

1. Activez la fonctionnalité de répondeur sur l'appliance NetScaler.
2. Créez une légende HTTP sur l'appliance NetScaler et configurez-la avec des détails sur le serveur externe et les autres paramètres requis.
3. Créez une politique de répondeur pour analyser la réponse, puis liez-la globalement.
4. Créez un agent d'appel sur le serveur distant.

Activation du répondeur

La fonctionnalité de répondeur doit être activée avant de pouvoir être utilisée sur l'appliance NetScaler.

Pour activer le répondeur à l'aide de l'interface graphique

1. Assurez-vous que la licence du répondeur est installée.
2. Dans l'utilitaire de configuration, développez AppExpert, cliquez avec le bouton droit sur **Répondeur**, puis cliquez sur **Activer la fonctionnalité Répondeur** .

Création d'une légende HTTP sur l'appliance NetScaler

Créez une légende HTTP, HTTP-Callout-4, avec les paramètres indiqués dans le tableau suivant. Pour plus d'informations sur la création d'une légende HTTP, consultez Configuration d'une légende HTTP.

Pour plus d'informations, voir Paramètres et valeurs pour HTTP-Callout-4 pdf.

Création d'une action de répondeur

Créez une action de répondeur, Action-Responder-4. Créez l'action avec les paramètres indiqués dans le tableau suivant.

Paramètre	Valeur
Nom	Action-Responder-4
Type	Répondez avec
Target	« HTTP/1.1 200 OK \ r \ nServeur : Microsoft-IIS/6.0 \ r \ nX Alimenté par : ASP.NET \ r \ nLongueur du contenu : 0 \ r \ nStockage Web : 6.5.6944 \ r \ nCache-Control : no-cache \ r \ n \ r \ n" »

Tableau 2 Paramètres et valeurs pour Action-Responder-4

Pour créer une action de répondeur à l'aide de l'utilitaire de configuration

1. **Accédez à**AppExpert**>**Responder > Actions**.**
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action de répondeur**, dans Nom, tapez **Action-Responder-4**.
4. Dans Type, cliquez sur **Répondre par**.
5. Dans Target, tapez :

```
1 ""HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By:
     ASP.NET\r\nContent-Length: 0\r\nMS-WebStorage: 6.5.6944\r\
     nCache-Control: no-cache\r\n\r\n""
2 <!--NeedCopy-->
```

6. Cliquez sur **Créer**, puis sur **Fermer**.

Création d'une politique de répondeur pour invoquer la légende HTTP

Créez une politique de réponse, Policy-Responder-4, qui vérifiera le corps de la demande et, si le corps contient le mot «
objet », invoquera la légende HTTP pour vérifier l'e-mail. Créez la politique à l'aide des paramètres indiqués dans le tableau suivant. Bien que vous puissiez créer une politique de répondeur dans le

sous-nœud
Politiques, puis la lier globalement à l'aide du
Responder Policy Manager, cette démonstration utilise le
Responder Policy Manager pour créer la politique de répondeur et la lier globalement.

Paramètre	Valeur
Nom	Policy-Responder-4
Action	Action-Responder-4
Action-résultat-action non défini	-Global undefined-result action-
Expression	« HTTP.REQ.BODY (1000) .CONTAINS (« urn:schemas:httpmail:subject ») && SYS.HTTP_CALLOUT (HTTP-Callout-4) »

Pour créer une politique de réponse à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Répondeur**.
2. Dans le volet de détails, sous **Policy Manager**, cliquez sur **Responder Policy** Manager.
3. Dans la boîte de dialogue **Responder Policy Manager**, cliquez sur **Override Global**.
4. Cliquez sur **Insérer une stratégie**, puis, dans la colonne **Nom de la stratégie**, cliquez sur **Nouvelle stratégie**.
5. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :
   a) Dans Nom, tapez **Policy-Responder-4**.
   b) Dans Action, cliquez sur **Action-Responder-4**.
   c) Dans Action à résultat non défini, cliquez sur Action **globale** à résultat non défini.
   d) Dans la zone de texte **Expression**, tapez :

```
"HTTP.REQ.BODY(1000).CONTAINS("urn:schemas:httpmail:subject")
   && SYS.HTTP_CALLOUT(HTTP-Callout-4)"
<!--NeedCopy-->
```

   e) Cliquez sur **Créer**, puis sur **Fermer**.
6. Cliquez sur **Appliquer les modifications**, puis sur **Fermer**.

Création d'un agent de légende HTTP sur le serveur distant

Vous devez maintenant créer un agent de légende HTTP sur le serveur de légende distant. L'agent de légende HTTP reçoit les demandes de légende de l'appliance NetScaler et répond en conséquence. L'agent d'appel est un script différent pour chaque déploiement qui doit être écrit en tenant compte

des spécifications du serveur, telles que le type de base de données et le langage de script pris en charge.

Le pseudo-code suivant fournit des instructions pour créer un agent de légende qui vérifie une liste de mots généralement considérés comme désignant des courriers indésirables. L'agent peut être implémenté dans le langage de programmation de votre choix. Le pseudo-code ne doit être utilisé que comme guide pour le développement de l'agent d'appel. Vous pouvez intégrer des fonctionnalités supplémentaires au programme.

Pour identifier les spams à l'aide d'un pseudo-code

1. Acceptez l'objet de l'e-mail fourni par l'appliance NetScaler.
2. Connectez-vous à la base de données qui contient tous les termes par rapport auxquels l'objet de l'e-mail est vérifié.
3. Vérifiez que les mots figurant dans l'objet de l'e-mail correspondent à ceux figurant dans la liste des mots indésirables.
4. Formatez la réponse comme l'exige la légende HTTP.
5. Envoyez la réponse à l'appliance NetScaler.

Cas d'utilisation : Commutation de contenu dynamique

August 20, 2021

Ce cas d'utilisation fournit un changement de contenu dynamique à l'aide d'une légende HTTP pour obtenir le nom du serveur virtuel d'équilibrage de charge vers lequel la demande est transférée.

1. Ajouter un serveur virtuel de commutation de contenu.

```
add cs vserver cs_vserver1 HTTP 10.102.29.196 80
<!--NeedCopy-->
```

2. Créez une légende HTTP.

```
add policy httpCallout http_callout1
<!--NeedCopy-->
```

3. Configurez la légende HTTP pour qu'elle réponde avec le nom du serveur virtuel d'équilibrage de charge à partir d'une requête contenant l'adresse IP du client dans l'en-tête HTTP « X-CLIENT-IP ».


```
> set policy httpCallout http_callout1 -IPAddress 10.217.14.23 -
    port 80 -returnType TEXT -hostExpr ""www.get-lbvip.com"" -
    urlStemExpr ""/index.html"" -headers X-CLIENT-IP(CLIENT.IP.SRC)
     -resultExpr "HTTP.RES.BODY(1000).AFTER_STR("<lbvip>").
    BEFORE_STR("<lbvip")"
<!--NeedCopy-->
```

4. Configurez l'action de commutation de contenu pour récupérer la réponse de légende.

```
add cs action cs_action1 -targetVserverExpr 'SYS.HTTP_CALLOUT(
    http_callout1)'
<!--NeedCopy-->
```

> Remarque :
>
> Vous devez lier un serveur virtuel d'équilibrage de charge au serveur virtuel de commutation de contenu pour tenir compte des éléments suivants :

- Indisponibilité du serveur virtuel d'équilibrage de charge auquel la légende résout.
- Condition UNDEF résultant de l'exécution de la légende.

```
> bind cs vserver cs_vserver1 -lbvserver default_lbvip
<!--NeedCopy-->
```

5. Configurez la stratégie de changement de contenu.

```
add cs policy cs_policy1 -rule true -action cs_action1
<!--NeedCopy-->
```

6. Liaison de la stratégie de commutation de contenu au serveur virtuel de commutation de contenu.

```
bind cs vserver cs_vserver1 -policyName cs_policy1 -priority 10
<!--NeedCopy-->
```

Jeux de motifs et jeux de données

March 9, 2023

Les expressions de stratégie pour les opérations de correspondance de chaînes sur un grand nombre de modèles de chaînes ont tendance à devenir longues et complexes. Les ressources consommées par l'évaluation de ces expressions complexes sont importantes en termes de cycles de traitement,

de mémoire et de taille de configuration. Vous pouvez créer des expressions plus simples et moins gourmandes en ressources en utilisant la correspondance de motifs.

Selon le type de motifs que vous souhaitez faire correspondre, vous pouvez utiliser l'une des fonctions suivantes pour implémenter la correspondance de motifs :

- Un jeu de motifs est un tableau de motifs indexés utilisés pour la correspondance de chaînes lors de l'évaluation de la stratégie de syntaxe par défaut. Exemple de jeu de motifs : types d'images {svg, bmp, PNG, GIF, tiff, jpg}.
- Un ensemble de données est une forme spécialisée de jeu de motifs. Il s'agit d'un tableau de modèles de types nombre (entier), adresse IPv4 ou adresse IPv6.

La différence entre a `patset` et a `dataset` est que dans a, `dataset` nous comparons la condition aux limites. Par exemple, si la chaîne d'entrée est 1.1.1.11 et suppose que le modèle 1.1.1.1 est lié à a `patset` et a `dataset` de type IPv4, alors un ensemble de données `patset` et est configuré pour vérifier si l'adresse IP est présente dans la demande. Après évaluation, `patset` renvoie que le 1.1.1.1 est présent dans l'entrée, mais que `dataset` l'évaluation est fausse. Cela est dû à une vérification des limites dans laquelle l'adresse IP ne fait pas partie d'une autre adresse IP. Cela signifie qu'après le motif lié, il ne doit pas y avoir d'entier.

Dans la plupart des cas, vous pouvez utiliser des jeux de modèles ou des jeux de données. Toutefois, dans les cas où vous souhaitez des correspondances spécifiques pour des données numériques ou des adresses IPv4 et IPv6, vous devez utiliser des jeux de données.

> **Remarques :**
>
> - Les jeux de modèles et les ensembles de données ne peuvent être utilisés que dans les stratégies de syntaxe par défaut.
> - À partir de la version 13.1 build 42.x et des versions ultérieures, vous pouvez lier 50 000 modèles à un jeu de modèles. Avec le fichier de jeu de modèles, seuls 10 000 modèles peuvent être liés à un jeu de modèles. De plus, si le jeu de modèles est utilisé pour le streaming, seuls 5 000 modèles peuvent être liés à cet ensemble de modèles. Un modèle défini pour le streaming est utilisé dans le paramètre de recherche de l'action de réécriture, le corps HTTP ou l'expression basée sur la charge utile TCP.

Comment fonctionne la correspondance de chaînes avec les ensembles de modèles et les ensembles de données

May 5, 2023

Un ensemble de modèles ou un ensemble de données contient un ensemble de modèles, et un index unique est attribué à chaque modèle. Lorsqu'une politique est appliquée à un paquet, une expres-

sion identifie une chaîne à évaluer, et l'opérateur compare la chaîne aux modèles définis dans le jeu de modèles ou l'ensemble de données jusqu'à ce qu'une correspondance soit trouvée ou que tous les modèles aient été comparés. Ensuite, en fonction de sa fonction, l'opérateur renvoie soit une valeur booléenne qui indique si un modèle correspondant a été trouvé, soit l'indice du modèle qui correspond à la chaîne.

Remarque : Cette rubrique explique le fonctionnement d'un ensemble de modèles. Les ensembles de données fonctionnent de la même manière. La seule différence entre les ensembles de modèles et les ensembles de données réside dans le type de modèles définis dans l'ensemble.

Examinez le cas d'utilisation suivant pour comprendre comment les modèles peuvent être utilisés pour la mise en correspondance de chaînes.

Vous souhaitez déterminer si le suffixe d'URL (texte cible) contient l'une des extensions du fichier image. Sans utiliser d'ensembles de modèles, vous devez définir une expression complexe, comme suit :

```
1 HTTP.REQ.URL.SUFFIX.CONTAINS("svg") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("
    bmp") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("png") ¦¦
2 HTTP.REQ.URL.SUFFIX.CONTAINS("gif") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("
    tiff") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("jpg")
3 <!--NeedCopy-->
```

Si l'URL possède le suffixe « jpg », avec l'expression composée ci-dessus, l'appliance NetScaler doit parcourir l'ensemble de l'expression composée de manière séquentielle, d'une sous-expression à l'autre, pour déterminer que la demande fait référence à une image jpg. La figure suivante montre les étapes du processus.



Lorsqu'une expression composée inclut des centaines de sous-expressions, le processus ci-dessus est gourmand en ressources. Une meilleure alternative est une expression qui invoque un ensemble de modèles, comme le montre la figure suivante.



Lors de l'évaluation de la politique, comme indiqué ci-dessus, l'opérateur (CONTAINS_ANY) compare la chaîne identifiée dans la demande avec les modèles définis dans l'ensemble de modèles jusqu'à ce qu'une correspondance soit trouvée. Avec l'expression Sample_Patset, les multiples itérations de six sous-expressions sont réduites à une seule.

En éliminant la nécessité de configurer des expressions composées qui effectuent la correspondance de chaînes avec plusieurs opérations OR, les jeux de motifs ou les jeux de données simplifient la configuration et accélèrent le traitement des demandes et des réponses.

Configuration d'un jeu de modèles

May 5, 2023

Pour configurer un ensemble de modèles, vous devez spécifier les chaînes qui doivent servir de modèles. Vous pouvez attribuer manuellement une valeur d'indice unique à chacun de ces modèles ou autoriser l'attribution automatique des valeurs d'indice.

> **Remarque :**
>
> Les ensembles de modèles font la distinction entre majuscules et minuscules (sauf si vous spécifiez l'expression à ignorer). Par conséquent, le modèle de chaîne « product1 », par exemple, n'est pas le même que le modèle de chaîne « Product1 ». «

Points à retenir sur les valeurs d'index :

- Vous ne pouvez pas lier la même valeur d'indice à plusieurs modèles.

- Une valeur d'indice attribuée automatiquement est supérieure d'un chiffre à la valeur d'indice la plus élevée des modèles existants dans l'ensemble de modèles. Par exemple, si la valeur d'indice la plus élevée des modèles existants dans un ensemble de modèles est 104, la prochaine valeur d'indice automatiquement attribuée est 105.
- Si vous ne spécifiez pas d'indice pour le premier modèle, la valeur d'indice 1 est automatiquement attribuée à ce modèle.
- Les valeurs d'index ne sont pas régénérées automatiquement si un ou plusieurs modèles sont supprimés ou modifiés. Par exemple, si l'ensemble contient cinq modèles, avec des index compris entre 1 et 5, et si le modèle avec un indice de 3 est supprimé, les autres valeurs d'index du jeu de modèles ne sont pas automatiquement régénérées pour produire des valeurs de 1 à 4.
- La valeur d'indice maximale qui peut être attribuée à un modèle est 4294967290. Si cette valeur est déjà affectée à un modèle de l'ensemble, vous devez attribuer manuellement des valeurs d'index à tous les modèles nouvellement ajoutés. Une valeur d'indice inutilisée inférieure à une valeur actuellement utilisée ne peut pas être attribuée automatiquement.

Configurer un modèle défini à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

1. Créez un ensemble de motifs.

```
add policy patset <name>
```

Exemple :

```
add policy patset samplepatset
```

1. Liez les motifs à l'ensemble de motifs.

```
bind policy patset <name> <string> [-index <positive_integer>][-charset
 ( ASCII | UTF_8 )] [-comment <string>]
```

Exemple :

```
bind policy patset samplepatset product1 -index 1 -comment short description
 about the pattern bound to the pattern set
```

Remarque : Répétez cette étape pour tous les motifs que vous souhaitez lier au jeu de motifs.

1. Vérifiez la configuration.

```
show policy patset <name>
```

Configurer un ensemble de modèles à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Ensembles de modèles**.

2. Dans le volet d'informations, cliquez sur **Ajouter** pour ouvrir la boîte de dialogue **Create Pattern Set** .
3. Spécifiez un nom pour le modèle défini dans la zone de texte Nom.
4. Sous Spécifier le modèle, tapez le premier modèle et, éventuellement, spécifiez les valeurs des paramètres suivants :
   - Traiter la barre oblique inverse comme un caractère d'échappement : cochez cette case pour spécifier que tous les caractères de barre oblique inverse que vous pourriez inclure dans le modèle doivent être traités comme des caractères d'échappement.
   - Index : valeur d'index attribuée par l'utilisateur, comprise entre 1 et 4294967290.
5. Vérifiez que vous avez saisi les bons caractères, puis cliquez sur **Ajouter**.
6. Répétez les étapes 4 et 5 pour ajouter d'autres motifs, puis cliquez sur **Créer**.

Configurer des ensembles de modèles basés sur des fichiers

L'appliance NetScaler prend en charge les ensembles de modèles basés sur des fichiers.

Configurer des ensembles de modèles basés sur des fichiers à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- Importez un nouveau fichier d'ensemble de modèles dans l'appliance NetScaler.

```
import policy patsetfile <src> <name> -delimiter <char> -charset
   <ASCII | UTF_8>
<!--NeedCopy-->
```

Exemple :

```
import policy patsetfile local:test.csv clientids_list -
   delimiter ,
<!--NeedCopy-->
```

Vous pouvez importer un fichier depuis un appareil local, un serveur HTTP ou un serveur FTP. Pour ajouter le fichier depuis votre appareil local, le fichier doit être disponible sur `/var/tmp` place.

- Ajoutez un fichier de jeu de modèles au moteur de paquets.

```
add policy patsetfile <patset filename>
<!--NeedCopy-->
```

Exemple :


```
add policy patsetfile clientids_list
<!--NeedCopy-->
```

- Mettez à jour un fichier d'ensemble de modèles existant sur l'appliance NetScaler.

```
update policy patsetfile <patset filename>
<!--NeedCopy-->
```

Exemple :

```
update policy patsetfile clientids_list
<!--NeedCopy-->
```

- Liez les motifs à l'ensemble de motifs.

```
add policy patset <patset name> -patsetfile <patset filename>
<!--NeedCopy-->
```

Exemple :

```
add policy patset clientid_patset -patsetfile clientids_list
<!--NeedCopy-->
```

- Vérifiez la configuration.

```
show policy patsetfile clientids_list

Name: clientids_list
Patset Name: clientid_patset
Number of Imported Patterns: 8
Number of Bound Patterns: 8
(All the patterns bound successfully)

Done
<!--NeedCopy-->
```

Configurer des ensembles de modèles basés sur des fichiers à l'aide de l'interface graphique

1. Accédez à **AppExpert-> Pattern Set Files**.
2. Dans le volet **Importé**, cliquez sur **Importer**.
3. Sur la page **Configurer le fichier du jeu** de règles, sélectionnez le fichier que vous souhaitez importer, puis cliquez sur **OK.**

4. Sélectionnez le fichier importé, puis cliquez sur **Ajouter**.
5. Sur la page **Créer un fichier d'ensembles** de règles, entrez les détails, puis cliquez sur **Créer** pour ajouter un ensemble de modèles de stratégies.

Configuration d'un ensemble de données

September 23, 2022

Pour configurer un ensemble de données, vous devez spécifier les chaînes du serveur en tant que modèle, attribuer un type (numéro, adresse IPv4 ou adresse IPv6) et configurer la plage de jeux de données. Vous pouvez affecter manuellement une valeur d'index unique au modèle ou autoriser l'attribution automatique des valeurs d'index. Le jeu de données n'est pas lié au protocole HTTP ou à un protocole à 7 couches. Il ne fonctionne que sur du texte ou une chaîne de caractères. Il existe différents types de jeux de données tels que NUM, ULONG, IPv4, IPv6, MAC, DOUBLE. Vous pouvez sélectionner un type et définir la plage du jeu de données en fonction du type spécifié.

> **Remarque :**
>
> Les ensembles de données de stratégie sont sensibles à la casse (sauf si vous spécifiez l'expression à ignorer la casse). Par conséquent, l'adresse MAC ff:ff:ff:ff:ff:ff, par exemple, n'est pas la même que l'adresse MAC FF:FF:FF:FF:FF:FF.

Les règles appliquées aux valeurs d'index des ensembles de données sont similaires aux jeux de répétitifs. Pour plus d'informations sur les valeurs d'index, voir Configuration d'un jeu de modèles.

Configurer un ensemble de données

Procédez comme suit pour configurer un ensemble de données :

1. Ajouter un ensemble de données de stratégie
2. Modèle de liaison à un ensemble de données de stratégie
3. Ajouter une expression de stratégie
4. Vérifiez la configuration de la stratégie

Ajouter un ensemble de données de stratégie

À l'invite de commandes, procédez comme suit :

```
add policy dataset <name> <type>
```

Exemple :

```
add policy dataset ds1 ipv4 -comment numbers
```


Lier un modèle à l'ensemble de données

À l'invite de commandes, tapez :

```
bind policy dataset <name> <value> [-index <positive_integer>] [-endRange <
string>] [-comment <string>]
```

Exemple :

```
bind policy dataset ds1 1.1.1.1 -endRange 1.1.1.10 -comment short description
 about the pattern bound to the data set
```

> **Remarque :**
>
> Vous devez répéter cette étape pour tous les modèles que vous souhaitez lier à l'ensemble de données. Vous ne pouvez lier que 5 000 modèles maximum à un jeu de données.
>
> En outre, une plage de jeu de données ne doit pas chevaucher d'autres plages liées à un jeu de données et ne peut pas inclure de valeurs uniques liées au jeu de données. Si vous liez un jeu de données avec une plage superposée, une erreur se produit.

Exemple :

```
1 add policy dataset ip_set ipv4
2  Done
3 bind policy dataset ip_set 2.2.2.25
4  Done
5 bind policy dataset ip_set 2.2.2.20 -endRange 2.2.2.30
6 ERROR: The range overlaps an existing range or includes a value bound
     to the dataset.
7 <!--NeedCopy-->
```

Une valeur est considérée comme étant dans l'ensemble de données si elle est égale à une valeur unique liée à l'ensemble de données ou se situe entre la valeur inférieure et la valeur supérieure (valeur inférieure <= valeur && valeur <- valeur supérieure), pour une plage liée à l'ensemble de données.

Utiliser une expression de stratégie dans un ensemble de données de stratégie

À l'invite de commandes, tapez :

```
add policy expression exp1 http.req.body(100).contains_any("ds1")
```

Où,
L'expression vérifie s'il existe un motif (ou un motif dans la plage) lié à l'ensemble de données ds1 est présent dans les 100 premiers octets du corps de la requête HTTP.

Vérifiez la configuration du jeu

À l'invite de commandes, tapez :

```
show policy dataset ds1
> show policy dataset ds1
```

Exemple :

```
1         Dataset:        ds1
2          Type:   IPV4
3 1)       Bound Dataset Range from: 1.1.1.1       through: 1.1.1.10
            Index:  1
4 <!--NeedCopy-->
```

Configurer un ensemble de données à l'aide de l'utilitaire de configuration

Suivez les étapes ci-dessous pour configurer un ensemble de données de stratégie :

1. Accédez à **AppExpert > Ensembles de données**.
2. Dans le volet d'informations, sous Ensembles de données, cliquez sur **Ajouter**.
3. Sur la page **Configurer l'ensemble de données**, définissez les paramètres suivants.
   a) Nom. Nom de l'ensemble de données de stratégie.
   b) Type. Type de valeur à lier à l'ensemble de données.

   Configuration du jeu de données
4. Cliquez sur **Insérer** pour lier la valeur du jeu de données d'un type spécifique.
   a) Valeur. Valeur du type spécifié associé à l'ensemble de données.
   b) Indice. La valeur d'indice de l'ensemble de données.
   c) Fin de gamme. L'entrée du jeu de données. Il s"agit d"une gamme <value> pour <end_range>.
   d) Commentaires. Brève description de l'ensemble de données.

   Liaison d'ensemble
5. Cliquez sur **Insérer** et **fermer**.
6. Entrez les commentaires.
7. Cliquez sur **Créer** et **Fermer**.

Notation de sous-réseau CIDR dans les adresses IPv4 et IPv6 pour l'ensemble de données de stratégie

Les jeux de données de stratégie pour les adresses IPv4 et IPv6 autorisent la valeur liée à être des sous-réseaux en utilisant la notation CIDR. La notation CIDR spécifie l'adresse et la plage du sous-réseau. Notation CIDR <address>/<n>, où <address> est la première adresse du sous-réseau et <n> est un nombre entier spécifiant le nombre de bits les plus à gauche définis dans le masque de sous-réseau, qui définit la plage du sous-réseau.

Par exemple, 192.128.0.0/10 représente un sous-réseau IPv4 commençant à l'adresse 192.129.0.0 avec un masque 0xFFC0000 (255.192.0.0).

Exemple :

```
add policy dataset ds1 ipv4
bind policy dataset ds1 192.128.0.0/10
show policy dataset ds1
    Dataset: ds1
    Type: IPV4
Bound Dataset Value: 192.128.0.0/10 Index: 1 Comment: Subnet range from
    192.128.0.0 through 192.191.255.255

<!--NeedCopy-->
```

Voici un exemple d'utilisation de cet ensemble de données dans une expression :

```
add responder policy resp_ipv4_pol client.ip.src.typecast_text_t.
   equals_any("ds1") drop
<!--NeedCopy-->
```

Exemple de sous-réseau IPv6 :

Un exemple de sous-réseau IPv6 serait 2001:db 8:123::/56, qui commence à l'adresse 2001:db 8:123:: avec un masque FFFF:FFFF:FFFF:FF00::

```
add policy dataset ds2 ipv6
bind policy dataset ds2 2001:db8:123::/56
show policy dataset ds2
    Dataset: ds2
    Type: IPV61
Bound Dataset Value: 2001:db8:123::/56 Index: 1 Comment: Subnet range
   from 2001:db8:123:: through 2001:db8:123:ff:ffff:ffff:ffff:ffff

<!--NeedCopy-->
```

L'adresse de début du sous-réseau sera déterminée par l'adresse spécifiée masquée par le masque de

sous-réseau. Un avertissement est émis si l'adresse spécifiée ne correspond pas à l'adresse de départ résultante.

Exemple :

```
bind policy dataset ds1 192.168.0.0/10
Warning: Starting subnet address masked using subnet mask to create new
     starting address [192.128.0.0]
show policy dataset ds1
    Dataset: ds1
    Type: IPV4
Bound Dataset Value:192.168.0.0/10 Index: 1 Comment: Subnet range from
   192.128.0.0 through 192.191.255.255

<!--NeedCopy-->
```

Voici un exemple d'utilisation de cet ensemble de données dans une expression :

```
add responder policy resp_ipv6_pol client.ipv6.src.typecast_text_t.
   equals_any("ds2") drop
<!--NeedCopy-->
```

Utilisation de jeux de motifs et de jeux de données

October 5, 2021

Les expressions de stratégie avancées qui prennent des jeux de modèles ou des jeux de données comme argument peuvent être utilisées pour effectuer des opérations de mise en correspondance de chaînes.

L'utilisation est la suivante :

```
<text>.<operator>("<name>")
<!--NeedCopy-->
```

où,

- <text> est l'expression qui identifie une chaîne dans un paquet. Exemple : HTTP.REQ.HEADER("Host").
- <operator> est l'un des opérateurs décrits dans le tableau Types de jeux de modèles pdf.

Pour connaître l'utilisation des échantillons, voir Utilisation de l'échantillon.

Exemple d'utilisation

August 20, 2021

Pour comprendre l'utilisation des jeux de motifs dans les expressions, considérez l'exemple d'un jeu de motifs nommé "imagetypes."

Modèles	Valeur de l'indice
svg	1
bmp	2
png	3
gif	4
Tiff	5
jpg	6

Tableau 1. Jeu de motifs « imagetypes »

Exemple 1 : Déterminez si le suffixe d'une requête HTTP est l'une des extensions de fichier définies dans le jeu de motifs « imagetypes ».

- **Expression.** HTTP.REQ.URL.SUFFIX.EQUALS_ANY("imagetypes")
- **Exemple d'URL.** `http://www.example.com/homepageicon.jpg`
- **Résultat.** VRAI

Exemple 2 : Déterminez si le suffixe d'une requête HTTP est l'une des extensions de fichier définies dans le jeu de motifs « imagetypes » et renvoyez l'index de ce modèle.

- **Expression.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes")
- **Exemple d'URL.** `http://www.example.com/mylogo.png`
- **Résultat.** 4 (La valeur d'index du motif « gif ».)

Exemple 3 : Utilisez la valeur d'index d'un modèle pour déterminer si le suffixe d'URL se trouve dans une plage de valeurs d'index spécifiée.

- **Expression.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").GE(3) && HTTP.REQ.URL.SUFFIX.EQUALS
- **Exemple d'URL.** `http://www.example.com/mylogo.png`
- **Résultat.** TRUE (La valeur d'index des types de fichiers gif est 4.)

Exemple 4 : implémentez un ensemble de stratégies pour les extensions de fichiers bmp, jpg et png, et un autre ensemble de stratégies pour les fichiers gif, tiff et svg.

Une expression qui renvoie l'index d'un motif apparié peut être utilisée pour définir des sous-ensembles de trafic pour une application Web. Les deux expressions suivantes peuvent être utilisées dans les stratégies de commutation de contenu pour un serveur virtuel de commutation de contenu :

- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").LE(3)
- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX("imagetypes").GE(4)

Variables

May 5, 2023

Les variables sont des objets nommés qui stockent des informations sous forme de jetons. Ces jetons sont utilisés dans le cadre et entre différentes transactions sur l'appliance NetScaler pour le calcul interne et le traitement des politiques.

L'appliance NetScaler prend en charge la création de variables des types suivants :

- **Variables singleton.** Peut avoir une valeur unique de l'un des types suivants : ulong et text (taille maximale). Le type ulong est un entier de 64 bits non signé, le type de texte est une séquence d'octets et la taille maximale est le nombre maximum d'octets de la séquence.
- **Variables cartographiques.** Les cartes contiennent des valeurs associées à des clés : chaque paire clé-valeur est appelée une entrée de carte. La clé de chaque entrée est unique dans la carte. Les cartes sont spécifiées comme suit :

  carte (type_clé, type_valeur, valeurs maximales).

  où,

  - *key_type* est le type de données de la clé. Il est de type texte (taille maximale).
  - *value_type* est le type de données des valeurs de la carte. Il peut être de type ulong ou texte (taille maximale).
  - *max-values* est le nombre maximum d'entrées que la carte peut contenir. Il est de type ulong.

Les valeurs de ces variables sont définies à l'aide d'attributions qui doivent être invoquées lors des actions de stratégie.

Portée des variables

Une variable de carte ou une variable singleton peut avoir une portée globale. La portée d'une variable singleton peut également être limitée à une seule transaction.

- **Variable d'étendue globale** : une variable ayant une portée globale (valeur par défaut) ne possède qu'une seule instance, et cette instance possède les mêmes valeurs sur tous les cœurs d'une appliance NetScaler et sur tous les nœuds d'un cluster ou d'une configuration HA. Les valeurs des variables globales existent jusqu'à ce qu'elles soient explicitement supprimées, jusqu'à ce qu'elles expirent, ou jusqu'à ce qu'un dispositif autonome soit redémarré ou que tous les nœuds d'un cluster ou d'une configuration HA soient redémarrés.
- **Variable d'étendue de transaction** : une variable ayant une portée de transaction possède une instance distincte, avec sa propre valeur, pour chaque transaction traitée par l'appliance NetScaler. Lorsque le traitement de la transaction est terminé, la valeur de la variable de transaction est supprimée.

> **Remarque** : Les variables d'étendue des transactions sont disponibles dans NetScaler version 10.5.e ou ultérieure.

Configuration et utilisation des variables

May 5, 2023

Vous devez d'abord créer une variable, puis lui attribuer une valeur ou spécifier l'opération à effectuer sur la variable. Après avoir effectué ces opérations, vous pouvez utiliser l'affectation en tant qu'action de politique.

Remarque : Une fois configurés, les paramètres d'une variable ne peuvent pas être modifiés ou réinitialisés. Si la variable doit être modifiée, la variable et toutes les références à la variable (expressions et affectations) doivent être supprimées. La variable peut ensuite être ajoutée avec de nouveaux paramètres, et les références (expressions et affectations) peuvent être ajoutées à nouveau.

Pour configurer des variables à l'aide de l'interface de ligne de commande

1. Créez une variable.

```
1 add ns variable <name> -type <string> [-scope global] [-ifFull ( undef
     | lru )] [-ifValueTooBig ( undef | truncate )] [-ifNoValue ( undef |
      init )] [-init <string>] [-expires <positive_integer>] [-comment <
     string>]
2 <!--NeedCopy-->
```

Remarque : Reportez-vous à la page de manuel « man add ns variable » pour une description des paramètres de commande.

Exemple 1 : créez une variable ulong nommée « my_counter » et initialisez-la à 1.


```
add ns variable my_counter  - type ulong -init 1
<!--NeedCopy-->
```

Exemple 2 : créez une carte nommée « user_privilege_map ». La carte contiendra des clés d'une longueur maximale de 15 caractères et des valeurs de texte d'une longueur maximale de 10 caractères, avec un maximum de 10 000 entrées.

```
add ns variable user_privilege_map -type map(text(15),text(10),10000)
<!--NeedCopy-->
```

Remarque : Si la carte contient 10 000 entrées non expirées, les attributions des nouvelles clés réutilisent l'une des entrées les moins récemment utilisées. Par défaut, une expression qui essaie d'obtenir la valeur d'une clé inexistante initialise une valeur de texte vide.

Attribuez la valeur ou spécifiez l'opération à effectuer sur la variable. Cela se fait en créant une mission.

```
add ns assignment <name> -variable <expression> [-set <expression> | -
    add <expression> | -sub <expression> | -append <expression> | -clear
    ] [-comment <string>]
<!--NeedCopy-->
```

Remarque : Une variable est référencée à l'aide du sélecteur de variables ($). Par conséquent, **$variable1** est utilisé pour faire référence à du texte ou à des variables ulong. De même, **$variable2 [key-expression]** est utilisé pour faire référence à des variables cartographiques.

Exemple 1 : définissez une affectation nommée « inc_my_counter » qui ajoute automatiquement 1 à la variable « my_counter ».

```
add ns assignment inc_my_counter -variable $my_counter -add 1
<!--NeedCopy-->
```

Exemple 2 : définissez une affectation nommée « set_user_privilege » qui ajoute à la variable « user_privilege_map » une entrée pour l'adresse IP du client avec la valeur renvoyée par la légende HTTP « get_user_privilege ».

```
add ns assignment set_user_privilege -variable $user_privilege_map[
    client.ip.src.typecast_text_t] -set sys.http.callout(
    get_user_privilege)
<!--NeedCopy-->
```

Remarque : Si une entrée pour cette clé existe déjà, la valeur sera remplacée. Sinon, une nouvelle entrée pour la clé et la valeur sera ajoutée. Sur la base de la déclaration précédente pour user_privilege_map, si la carte contient déjà 10 000 entrées, l'une des entrées les moins récemment utilisées sera réutilisée pour la nouvelle clé et la nouvelle valeur.

1. Invoquez l'attribution de variables dans une politique.

   Deux fonctions peuvent fonctionner sur des variables cartographiques.

   - **$Name.valueExists (expression clé).** Renvoie la valeur true si la carte contient une valeur sélectionnée par l'expression clé. Dans le cas contraire, renvoie false. Cette fonction mettra à jour les informations d'expiration et de LRU si l'entrée de carte existe, mais ne créera pas de nouvelle entrée de carte si la valeur n'existe pas.
   - **$nom.valueCount.** Renvoie le nombre de valeurs actuellement détenues par la variable. Il s'agit du nombre d'entrées dans une carte. Pour une variable singleton, il s'agit de 0 si la variable n'est pas initialisée ou de 1 dans le cas contraire.

   Exemple : appelez l'attribution nommée « set_user_privilege » avec une politique de compression.

```
add cmp policy set_user_privilege_pol -rule $user_privilege_map.
    valueExists(client.ip.src.typecast_text_t).not -resAction
    set_user_privilege
<!--NeedCopy-->
```

Cas d'utilisation pour insérer un en-tête HTTP dans le côté réponse

L'exemple suivant montre un exemple de variable singleton.

Ajoutez une variable singleton de type text. Cette variable peut contenir au maximum 100 octets de données.

```
add ns variable http_req_data -type text(100) -scope transaction
<!--NeedCopy-->
```

Ajoutez une action d'attribution, qui sera utilisée pour stocker les données de la requête HTTP dans la variable.

```
add ns assignment set_http_req_data -variable $http_req_data -set http.
    req.body(100)
<!--NeedCopy-->
```

Ajoutez une action de réécriture pour insérer un en-tête HTTP, dont la valeur sera extraite de la variable.

```
add rewrite action act_ins_header insert_http_header user_name
    $http_req_data.after_str("user_name").before_str("password")
<!--NeedCopy-->
```


Ajoutez une politique de réécriture qui évaluera le délai de demande et prendra des mesures d'attribution pour stocker les données. Lorsque nous appliquerons cette politique, nous prendrons des mesures d'attribution et stockerons les données dans la variable ns (http_req_data)

```
add rewrite policy pol_set_variable true set_http_req_data

bind rewrite global pol_set_variable 10 -type req_dEFAULT
<!--NeedCopy-->
```

Ajoutez une politique de réécriture qui évaluera le temps de réponse, et ajoutez un en-tête HTTP dans la réponse.

```
add rewrite policy pol_ins_header true act_ins_header

bind rewrite global pol_ins_header 10 -type res_dEFAULT
<!--NeedCopy-->
```

Action d'affectation

Dans une appliance NetScaler, une action d'attribution liée à la politique est déclenchée lorsque la règle de politique est évaluée comme vraie. L'action met à jour la valeur de la variable qui peut être utilisée lors des évaluations ultérieures des règles de politique. Ainsi, la même variable peut être mise à jour et utilisée pour des évaluations ultérieures des politiques dans la même fonctionnalité. Auparavant, l'appliance exécutait des actions d'attribution uniquement après avoir évalué toutes les politiques de la fonctionnalité lorsque les politiques des actions d'attribution associées étaient considérées comme vraies. Par conséquent, la valeur variable définie par l'action d'attribution ne peut pas être utilisée dans les évaluations ultérieures des règles de politique au sein de la fonctionnalité.

Cette fonctionnalité peut être mieux comprise à l'aide d'un cas d'utilisation qui contrôle la liste d'accès des clients sur une appliance NetScaler. La décision d'accès est fournie par un service Web distinct, la demande `GET /client-access?<client-IP-address>` renvoyant une réponse avec « BLOCK » ou « ALLOW » dans le corps du message. La légende HTTP est configurée pour inclure l'adresse IP du client associée à une demande entrante. Lorsque l'appliance NetScaler reçoit une demande d'un client, elle génère la demande de légende et l'envoie au serveur de légende, qui héberge une base de données d'adresses IP sur liste noire et un agent de légende HTTP qui vérifie si l'adresse IP du client figure dans la base de données. L'agent de légende HTTP reçoit la demande de légende, vérifie si l'adresse IP du client est répertoriée et envoie une réponse. La réponse est un code d'état, 200, 302, suivi de « BLOCK » ou « ALLOW » dans le corps du message. Sur la base du code d'état, l'appliance effectue l'évaluation des politiques. Si l'évaluation de la politique est vraie, l'action d'affectation est déclenchée immédiatement et l'action définit la valeur de la variable. L'appliance utilise et définit cette valeur variable pour une évaluation ultérieure des politiques dans le même module.

Cas d'utilisation pour la configuration d'une action d'attribution

Suivez les étapes ci-dessous pour configurer l'action d'attribution et utiliser une variable pour les politiques suivantes :

1. La décision d'accès est fournie par un service Web distinct, la requête renvoyant une réponse avec BLOCK ou ALLOW dans le corps du message.

   ```
   GET /url-service>/url-allowed?<URL path>
   ```

2. Configurez une variable de carte pour contenir les décisions d'accès aux URL.

   ```
   add ns variable url_list_map -type 'map(text(1000),text(10),10000)'
   ```

3. Configurez une légende HTTP pour envoyer la demande d'accès au service Web.

   ```
   add policy httpCallout url_list_callout -vserver url_vs -returnType
   TEXT -urlStemExpr '"/url-allowed?" + HTTP.REQ.URL.PATH'-resultExpr '
   HTTP.RES.BODY(10)'
   ```

4. Configurez une action d'attribution pour appeler la légende afin d'obtenir la décision d'accès et de l'attribuer à l'entrée cartographique de l'URL.

   ```
   add ns assignment client_access_assn -variable '$client_access_map[
   CLIENT.IP.SRC.TYPECAST_TEXT_T]'-set SYS.HTTP_CALLOUT(client_access_callout
   )
   ```

5. Configurez une action de répondeur pour envoyer une réponse 403 si une demande d'URL est bloquée.

   ```
   add responder action url_list_block_act respondwith '"HTTP/1.1 403
   Forbidden\\r\\n\\r\\n"'
   ```

6. Configurez une politique de réponse pour définir l'entrée cartographique de l'URL si elle n'est pas déjà définie. Avec l'amélioration de l'action immédiate, la valeur d'entrée sur la carte est définie lors de l'évaluation de cette politique. Avant l'amélioration, l'attribution n'était effectuée qu'une fois que toutes les politiques de réponse avaient été évaluées. La décision est fournie par un service Web distinct.

   ```
   add responder policy url_list_assn_pol '!$url_list_map.VALUEEXISTS(HTTP
   .REQ.URL.PATH)'url_list_assn
   ```

7. Configurez une politique de réponse pour bloquer l'accès à une URL si sa valeur d'entrée dans la carte est BLOCK. Avec l'amélioration de l'action immédiate, l'entrée cartographique définie par la politique précédente peut être utilisée dans cette politique. Avant l'amélioration, l'entrée cartographique n'était toujours pas définie à ce stade.

   ```
   add responder policy client_access_block_pol '$client_access_map[CLIENT
   .IP.SRC.TYPECAST_TEXT_T] == "BLOCK"'client_access_block_act
   ```


8. Liez les politiques du répondeur au serveur virtuel. **Remarque** : Nous ne pouvons pas lier les politiques de manière globale car nous ne voulons pas les exécuter pour la légende HTTP sur un serveur virtuel distinct.

```
bind lb vserver vs -policyName client_access_assn_pol -priority 10 -
gotoPriorityExpression NEXT -type REQUEST
bind lb vserver vs -policyName client_access_block_pol -priority 20 -
gotoPriorityExpression END -type REQUEST
```

Pour configurer des variables à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert > Variables NS**pour créer une variable.
2. Accédez à **AppExpert > NS Assignments**pour attribuer des valeurs à la variable.
3. Accédez à la zone d'entités appropriée dans laquelle vous souhaitez configurer l'affectation en tant qu'action.

Cas d'utilisation : mise en cache des privilèges utilisateur

January 21, 2021

Dans ce cas d'utilisation, les privilèges utilisateur (« GOLD », « SILVER », etc.) doivent être récupérés à partir d'un service Web externe.

Pour réaliser ce cas d'utilisation, effectuez les opérations suivantes

Créez une légende HTTP pour récupérer les privilèges utilisateur à partir du service Web externe.

```
1 add policy httpcallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port <
     port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (
     GET | POST )] [-hostExpr <string>] [-urlStemExpr <string>] [-headers
      <name(value)> ...] [-parameters <name(value)> ...] [-bodyExpr <
     string>][-fullReqExpr <string>] [-scheme ( http | https )] [-
     resultExpr <string>] [-cacheForSecs <secs>] [-comment <string>]
2
3 add policy httpcallout get_user_privilege -ipaddress 10.217.193.84 -
     port 80 -returnType text -httpMethod GET -hostExpr '"/
     get_user_privilege"' -resultExpr 'http.res.body(5)'
4 <!--NeedCopy-->
```

Stockez les privilèges dans une variable.


```
add ns variable <name> -type <string> [-scope ( global | transaction )
    ][-ifFull ( undef | lru )] [-ifValueTooBig ( undef | truncate )][-
    ifNoValue ( undef | init )] [-init <string>] [-expires <
    positive_integer>] [-comment <string>]

add ns variable user_privilege_map -type map(text(15),text(10),10000) -
    expires 1200

add ns assignment set_user_privilege -variable $user_privilege_map[
    client.ip.src] -set sys.http_callout(get_user_privilege)
<!--NeedCopy-->
```

Créez une stratégie pour vérifier s'il existe déjà une entrée mise en cache pour l'adresse IP du client ; sinon, il appelle la légende HTTP pour définir une entrée de mappage pour le client.

```
add cmp policy <name> -rule <expression> -resAction <string>

add cmp policy set_user_privilege_pol -rule $user_privilege_map.
    valueExists(client.ip.src).not -resAction set_user_privilege>
<!--NeedCopy-->
```

Créez une stratégie qui compresse si l'entrée de privilège mise en cache pour le client est « GOLD ».

```
add cmp policy <name> -rule <expression> -resAction <string>

add cmp policy compress_if_gold_privilege_pol -rule '
    $user_privilege_map[client.ip.src].eq("GOLD")' -resAction compress
<!--NeedCopy-->
```

Liez les stratégies de compression globalement.

```
bind cmp global <policyName> [-priority <positive_integer>] [-state (
    ENABLED | DISABLED )] [-gotoPriorityExpression <expression>] [-type
    <type>] [-invoke (<labelType> <labelName>) ]

bind cmp global set_user_privilege_pol -priority 10 NEXT

bind cmp global compress_if_gold_privilege_pol -priority 20 END
<!--NeedCopy-->
```


Cas d'utilisation : limitation du nombre de sessions

June 7, 2022

Dans ce cas d'utilisation, il est nécessaire de limiter le nombre de sessions back-end actives. Dans le déploiement, chaque connexion de session possède un identifiant dans l'URL et chaque déconnexion de session possède une déconnexion dans l'URL. En cas de connexion réussie, le back-end définit un cookie d'identification de session avec une valeur unique de dix caractères.

Pour réaliser ce cas d'utilisation, effectuez les opérations suivantes :

1. Créez une variable cartographique qui peut stocker chaque session active. La clé de la carte est le sessionid. Le délai d'expiration de la variable est défini sur 600 secondes (10 minutes).

```
> add ns variable session_map -type map(text(10),ulong,100) -
    expires 600
<!--NeedCopy-->
```

2. Créez les affectations suivantes pour la variable de carte :

   - Créez une entrée pour l'identifiant de session et définissez cette valeur sur 1 (cette valeur n'est pas utilisée).

```
> add ns assignment add_session -variable '$session_map[http.
    req.cookie.value("sessionid")]' -set 1
<!--NeedCopy-->
```

   - Désallouez l'entrée pour un ID de session, ce qui décrémente implicitement le nombre de valeurs pour session_map.

```
> add ns assignment delete_session -variable '$session_map[
    http.req.cookie.value("sessionid")]' -clear
<!--NeedCopy-->
```

3. Créez des stratégies de répondeur pour les éléments suivants :

   - Pour vérifier si une entrée de carte existe pour cet ID de session dans la requête HTTP. L'affectation add_session est exécutée si l'entrée de map n'existe pas.

```
> add responder policy add_session_pol 'http.req.url.contains
    ("example") || $session_map.valueExists(http.req.cookie.
    value("abc"))' add_session
<!--NeedCopy-->
```

   Remarque : La fonction
   valueExists() de la stratégie

add_session_pol compte comme une référence à l'entrée de map de la session, de sorte que chaque requête réinitialise le délai d'expiration de sa session. Si aucune demande de session n'est reçue après 10 minutes, l'entrée de la session sera désallouée.

- Pour vérifier quand la session est déconnectée. L'affectation delete_session est exécutée.

```
add responder policy delete_session_pol "http.req.url.
   contains("Logout")" delete_session
<!--NeedCopy-->
```

- Pour vérifier les demandes de connexion et si le nombre de sessions actives dépasse 100. Si ces conditions sont remplies, afin de limiter le nombre de sessions, l'utilisateur est redirigé vers une page indiquant que le serveur est occupé.

```
add responder action redirect_too_busy redirect "/too_busy.
   html"
add responder policy check_login_pol "http.req.url.contains("
   example") && $session_map.valueCount > 100"
   redirect_too_busy
<!--NeedCopy-->
```

4. Liez les politiques du répondeur globalement.

```
bind responder global add_session_pol 30 next
bind responder global delete_session_pol 10
bind responder global check_login_pol 20
<!--NeedCopy-->
```

Stratégies et expressions

May 5, 2023

Les rubriques suivantes fournissent les informations conceptuelles et de référence dont vous avez besoin pour configurer des politiques avancées sur l'appliance Citrix® NetScaler®.

Pour en savoir plus sur toutes les expressions de politique avancées prises en charge par l'appliance NetScaler, consultez la section Expressions de politique

Introduction aux stratégies et expressions	Décrit l'objectif des expressions, des politiques et des actions, ainsi que la manière dont les différentes applications NetScaler les utilisent.

Configuration des stratégies avancées	Décrit la structure des stratégies avancées et la façon de les configurer individuellement et en tant que banques de stratégies.
Configuration des expressions avancées : mise en route	Décrit la syntaxe et la sémantique des expressions, et explique brièvement comment configurer les expressions et les stratégies.
Expressions avancées : évaluation du texte	Décrit les expressions que vous configurez lorsque vous souhaitez utiliser du texte (par exemple, le corps d'une demande HTTP POST ou le contenu d'un certificat utilisateur).
Expressions avancées : utilisation des dates, des heures et des nombres	Décrit les expressions que vous configurez lorsque vous souhaitez utiliser n'importe quel type de données numériques (par exemple, la longueur d'une URL, l'adresse IP d'un client ou la date et l'heure d'envoi d'une demande HTTP).
Expressions avancées : analyse des données HTTP, TCP et UDP	Décrit les expressions d'analyse des adresses IP et IPv6, des adresses MAC et des données spécifiques au trafic HTTP et TCP.
Expressions avancées : analyse des certificats SSL	Explique comment configurer des expressions pour le trafic SSL et les certificats clients, par exemple, comment récupérer la date d'expiration d'un certificat ou de l'émetteur du certificat.
Expressions avancées : adresses IP et MAC, débit, identifiants de VLAN	Décrit les expressions que vous pouvez utiliser pour travailler avec d'autres données relatives au client ou au serveur qui ne sont pas abordées dans les autres chapitres. |Données de typecasting	Décrit les expressions permettant de transformer des données d'un type en un autre. |Expressions régulaires| Décrit comment transmettre des expressions régulières en tant qu'arguments à des opérateurs dans des expressions avancées.	Référence des
expressions	Une référence pour les arguments d'expression avancés.	Exemples récapitulatifs d'expressions et de stratégies avancées	Exemples d'expressions et de stratégies avancées, sous forme de référence rapide et de didacticiel, que vous pouvez personnaliser pour votre propre usage.
Tutoriel Exemples de politiques avancées pour la réécriture	Exemples de stratégies avancées à utiliser dans la fonction de réécriture.
Tutoriel Exemples de politiques	Exemples de politiques pour les fonctionnalités de NetScaler telles que le pare-feu des applications et le protocole SSL.
Migration des règles mod_rewrite d'Apache vers des politiques avancées	Exemples de fonctions écrites à l'aide du moteur mod_rewrite du serveur HTTP Apache, avec des exemples de ces fonctions après traduction en politiques de réécriture et de réponse sur NetScaler.

Introduction aux politiques et expressions

May 5, 2023

Pour de nombreuses fonctionnalités de NetScaler, les politiques contrôlent la manière dont une fonc-

tionnalité évalue les données. Une stratégie utilise une expression logique, appelée en règle générale, pour évaluer les données et applique une ou plusieurs actions basées sur l'évaluation. Une stratégie peut également appliquer un profil, qui définit une action complexe.

Certaines fonctionnalités de NetScaler utilisent des politiques avancées, qui offrent des fonctionnalités supérieures à celles des anciennes stratégies classiques. Si vous avez migré vers une version plus récente du logiciel NetScaler et que vous avez configuré des politiques classiques pour les fonctionnalités qui utilisent des stratégies avancées, vous devez migrer manuellement les politiques vers une infrastructure de stratégies avancée.

Infrastructure de stratégie

July 12, 2023

> **Avertissement**
>
> Les expressions de stratégie classiques sont obsolètes à partir de NetScaler 12.0 build 56.20 et, comme alternative, Citrix vous recommande d'utiliser des stratégies avancées. Pour plus d'informations, consultez la section Stratégies avancées

L'infrastructure de stratégie avancée vous permet d'analyser de nombreux éléments de données (par exemple, le corps d'une requête HTTP) et de configurer de nombreuses opérations dans la règle de stratégie (par exemple, transformer les données du corps d'une demande en en-tête HTTP). Vous devez lier la stratégie à un point particulier du traitement associé aux fonctionnalités de NetScaler. Le point de liaison est l'un des facteurs qui déterminent le moment où la stratégie sera évaluée.

Avantages de l'utilisation de stratégies avancées

Les stratégies avancées utilisent un puissant langage d'expression basé sur un modèle class-objet et proposent plusieurs options qui améliorent votre capacité à configurer le comportement de diverses fonctionnalités de NetScaler. Grâce à une infrastructure de stratégies avancée, vous pouvez effectuer les opérations suivantes :

- Effectuer des analyses minces du trafic réseau des couches 2 à 7.
- Évaluez toute partie de l'en-tête ou du corps d'une requête ou réponse HTTP ou HTTPS.
- Liez les stratégies aux multiples points de liaison que l'infrastructure de stratégies avancée prend en charge au niveau du serveur par défaut, du serveur de remplacement et du serveur virtuel.
- Utilisez des outils spéciaux tels que des ensembles de modèles, des étiquettes de stratégie, des identificateurs de limite de débit, des légendes HTTP et des variables, qui vous permettent de configurer efficacement les stratégies pour des cas d'utilisation complexes.

En outre, l'utilitaire de configuration étend la prise en charge d'une interface graphique robuste pour l'infrastructure et les expressions de stratégies avancées et permet aux utilisateurs ayant une connaissance limitée des protocoles réseau de configurer rapidement et facilement des stratégies. L'utilitaire de configuration inclut également une fonction d'évaluation des stratégies avancées. Vous pouvez utiliser cette fonctionnalité pour évaluer une stratégie avancée et tester son comportement avant de la valider, réduisant ainsi le risque d'erreurs de configuration.

Composants de base d'une stratégie avancée

Voici quelques caractéristiques d'une stratégie avancée :

- Nom. Chaque stratégie possède un nom unique.
- Rule. La règle est une expression logique qui permet à la fonctionnalité NetScaler d'évaluer un élément de trafic ou un autre objet. Par exemple, une règle peut permettre à NetScaler de déterminer si une requête HTTP provient d'une adresse IP particulière ou si l'en-tête Cache-Control d'une requête HTTP possède la valeur « No-Cache ».
- Fixations. Pour vous assurer que NetScaler peut invoquer une stratégie lorsque cela est nécessaire, vous associez la stratégie, ou vous la liez, à un ou plusieurs points de liaison.

  Vous pouvez lier une stratégie globalement ou à un serveur virtuel. Pour plus d'informations, voir À propos des liaisons de stratégies.
- Une action associée. Une action est une entité distincte d'une stratégie. L'évaluation des stratégies aboutit finalement à l'exécution d'une action par NetScaler.

  Par exemple, une stratégie du cache intégré peut identifier les requêtes HTTP pour les fichiers .png ou .jpeg. Une action que vous associez à cette stratégie détermine que les réponses à ces types de demandes sont diffusées à partir du cache.

Pour certaines fonctionnalités, vous configurez des actions dans le cadre d'un ensemble d'instructions plus complexe appelé profil.

Comment les différentes fonctionnalités de NetScaler utilisent les stratégies

Le NetScaler prend en charge diverses fonctionnalités qui s'appuient sur des stratégies de fonctionnement. Le tableau suivant récapitule la manière dont les fonctionnalités de NetScaler utilisent les stratégies.

Nom de la fonctionnalité	Comment utiliser les stratégies de la fonctionnalité
Réécriture	Pour identifier les données que vous souhaitez modifier avant de les diffuser. Les stratégies fournissent des règles pour la modification des données. Par exemple, vous pouvez modifier les données HTTP pour rediriger une demande vers une nouvelle page d'accueil, un nouveau serveur ou un serveur sélectionné en fonction de l'adresse de la demande entrante, ou vous pouvez modifier les données pour masquer les informations du serveur dans une réponse à des fins de sécurité. La fonction URL Transformer identifie les URL dans les transactions HTTP et les fichiers texte afin d'évaluer si une URL doit être transformée.
Répondeur	Pour configurer le comportement de la fonction Responder. Une stratégie de répondeur est basée sur une règle, qui consiste en une ou plusieurs expressions. La règle est associée à une action, qui est exécutée si une demande correspond à la règle.
Commutation de contenu	Déterminer quel serveur ou groupe de serveurs est chargé de fournir les réponses, en fonction des caractéristiques d'une demande entrante. Les caractéristiques de la demande incluent le type de périphérique, la langue, les cookies, la méthode HTTP, le type de contenu et le serveur de cache associé.
Redirection de cache	Pour déterminer si les réponses sont diffusées à partir d'un cache ou d'un serveur d'origine.
Contrôle de la compression	Déterminer quel type de trafic doit être compressé.
DNS	Pour modifier diverses parties des requêtes et des réponses DNS

Nom de la fonctionnalité	Comment utiliser les stratégies de la fonctionnalité
Accès VPN sans client	Pour déterminer comment NetScaler Gateway exécute les fonctions d'authentification, d'autorisation, d'audit et autres, et pour définir des règles de réécriture pour l'accès Web général à l'aide de NetScaler Gateway.
Mettre en cache	Pour déterminer s'il faut envoyer une réponse depuis le cache ou le serveur d'origine.
Stratégie de transformation d'URL	Pour sélectionner les demandes et les réponses que NetScaler doit transformer à l'aide du profil de transformation d'URL.
Stratégie de pare-feu des applications	Attribuer différentes règles de filtrage à différents types de contenu Web.
Authorization	Fournir un accès au contenu demandé sans exposer de détails inutiles sur la configuration réelle du site Web.
Trafic TM	Pour définir les caractéristiques (telles que le délai d'expiration de la connexion, l'authentification unique et le lancement de la déconnexion) du trafic de l'application au moment de l'exécution.
Session TM	Pour personnaliser les sessions utilisateur une fois que l'utilisateur s'est connecté au serveur virtuel d'autorisation, d'autorisation et de comptabilité.
Stratégies SSL	Pour définir un contrôle ou une action sur les données à exécuter sur les demandes. Les stratégies SSL peuvent donc être classées en stratégies de contrôle et en stratégies de données. Une stratégie de contrôle utilise une action de contrôle, telle que forcer l'authentification du client. Une stratégie de données utilise une action de données, telle que l'insertion de certaines données dans la demande.

Nom de la fonctionnalité	Comment utiliser les stratégies de la fonctionnalité
Autoscale	Augmenter ou réduire le nombre de serveurs virtuels de manière fluide et automatique en fonction des conditions définies.
AppFlow	Permettre à NetScaler d'exporter les données de flux vers des outils de collecte, souvent utilisés pour l'analyse du réseau ou de la sécurité.
Optimisation du contenu	Pour réduire les temps de transaction entre les clients et les serveurs et réduire la consommation de bande passante. Également pour améliorer les performances du serveur en déchargeant certaines tâches et en rendant d'autres plus efficaces.
débordement	Utiliser une règle NetScaler pour spécifier les conditions d'un débordement. Les règles vous offrent la flexibilité nécessaire pour configurer le spillover en fonction de différentes conditions opérationnelles.
ICA	Pour générer dynamiquement une demande ICAP, recevez la réponse ICAP et enregistrez les données d'inspection du contenu.
Session VPN	Sur un NetScaler Gateway, pour configurer Endpoint Analysis (EPA) afin de vérifier si une machine utilisateur répond à certaines exigences de sécurité et, en conséquence, d'autoriser l'utilisateur à accéder aux ressources internes.
Trafic VPN	Sur un NetScaler Gateway, pour configurer Endpoint Analysis (EPA) afin de vérifier si une machine utilisateur répond à certaines exigences de sécurité et, en conséquence, d'autoriser l'utilisateur à accéder aux ressources internes.
syslog	Pour définir les messages à enregistrer sur le serveur Syslog spécifié.

Nom de la fonctionnalité	Comment utiliser les stratégies de la fonctionnalité
nslog	Pour définir les messages à enregistrer sur le serveur nslog spécifié.
Détection d'optimisation vidéo	Pour créer une étiquette de stratégie de détection d'optimisation vidéo définie par l'utilisateur, à laquelle vous pouvez lier des stratégies de détection. Une étiquette de stratégie est un outil permettant d'évaluer un ensemble de stratégies dans un ordre spécifique. À l'aide d'une étiquette de stratégie, vous pouvez configurer la fonction d'optimisation vidéo pour choisir la stratégie suivante, invoquer une étiquette de stratégie différente ou terminer complètement une évaluation de stratégie en vérifiant si la stratégie précédente avait la valeur VRAI ou FAUX.
Creusement de tunnels	Pour définir le type de compression à utiliser pour le trafic tunnelisé.
Inspection du contenu	Pour spécifier les demandes que le NetScaler ADC intercepte et exécute l'action spécifiée.
URL DU VPN	Créer un lien de signet vers une ressource externe ou interne qui apparaît sur l'interface d'accès, selon le type, sous forme de lien de site Web ou de lien de partage de fichiers.
Bot	Pour créer une étiquette de stratégie de bot définie par l'utilisateur, à laquelle vous pouvez lier des stratégies. Une étiquette de stratégie est un outil permettant d'évaluer un ensemble de stratégies dans un ordre spécifique. En utilisant une étiquette de stratégie, vous pouvez configurer la fonction de réponse pour choisir la stratégie suivante, invoquer une étiquette de stratégie différente ou terminer complètement une évaluation de stratégie en vérifiant si la stratégie précédente avait la valeur TRUE ou FALSE.

Nom de la fonctionnalité	Comment utiliser les stratégies de la fonctionnalité
Stratégie relative aux applications intranet VPN	Définir les applications intranet à rendre accessibles via NetScaler Gateway.
SmartAccess	Pour créer un profil d'accès ICA qui spécifie l'état des fonctionnalités (par défaut ou désactivé).
Équilibrage de charge	Pour définir comment répartir les connexions client entre les serveurs à charge équilibrée qu'il gère.

À propos des actions et des profils

Les stratégies n'agissent pas elles-mêmes sur les données. Les stratégies fournissent une logique en lecture seule pour évaluer le trafic. Pour permettre à une fonctionnalité d'effectuer une opération basée sur une évaluation de stratégie, vous configurez des actions ou des profils et vous les associez à des stratégies.

> **Remarque :**
>
> Les actions et les profils sont spécifiques à des fonctionnalités particulières. Pour plus d'informations sur l'affectation d'actions et de profils aux fonctionnalités, consultez la documentation relative aux fonctionnalités individuelles.

À propos des actions

Les actions sont des étapes que NetScaler exécute, en fonction de l'évaluation de l'expression dans la stratégie. Par exemple, si une expression d'une stratégie correspond à une adresse IP source particulière dans une demande, l'action associée à cette stratégie détermine si la connexion est autorisée.

Les types d'actions que NetScaler peut effectuer sont spécifiques aux fonctionnalités. Par exemple, dans Réécrire, les actions peuvent remplacer le texte d'une demande, modifier l'URL de destination d'une demande, etc. Dans Integrated Caching, les actions déterminent si les réponses HTTP sont diffusées à partir du cache ou d'un serveur d'origine.

Dans certaines fonctionnalités de NetScaler, les actions sont prédéfinies, tandis que dans d'autres, elles sont configurables. Dans certains cas (par exemple, Rewrite), vous configurez les actions à l'aide des mêmes types d'expressions que ceux que vous utilisez pour configurer la règle de stratégie associée.

> **Remarque :**
>
> Les combinaisons de fonction, de protocole, de direction et d'entité ne sont pas toutes valides.

À propos des profils

Certaines fonctionnalités de NetScaler vous permettent d'associer des profils, ou à la fois des actions et des profils, à une stratégie. Un profil est un ensemble de paramètres qui permettent à la fonctionnalité d'exécuter une fonction complexe. Par exemple, dans le pare-feu d'application, un profil de données XML peut effectuer plusieurs opérations de filtrage, telles que l'examen des données à la recherche d'une syntaxe XML illégale ou d'une preuve d'injection SQL.

À propos des liaisons de stratégie

Une stratégie est associée ou liée à une entité qui permet d'invoquer la stratégie. Par exemple, vous pouvez lier une stratégie à une évaluation au moment de la demande qui s'applique à tous les serveurs virtuels. Un ensemble de stratégies liées à un point de liaison particulier constitue une banque de stratégies.

Vous trouverez ci-dessous un aperçu des différents types de points de liaison d'une stratégie :

- Temps de demande global. Une stratégie peut être disponible pour tous les composants d'une fonctionnalité au moment de la demande.
- Temps de réponse global. Une stratégie peut être disponible pour tous les composants d'une fonctionnalité au moment de la réponse.
- Heure de la demande, spécifique au serveur virtuel. Une stratégie peut être liée au traitement au moment de la demande pour un serveur virtuel particulier. Par exemple, vous pouvez lier une stratégie de temps de demande à un serveur virtuel de redirection de cache pour vous assurer que des demandes particulières sont transférées vers un serveur virtuel d'équilibrage de charge pour le cache, et que les autres demandes sont envoyées à un serveur virtuel d'équilibrage de charge pour l'origine.
- Temps de réponse, spécifique au serveur virtuel. Une stratégie peut également être liée au traitement du temps de réponse pour un serveur virtuel particulier.
- Étiquette de stratégie définie par l'utilisateur. Pour une infrastructure de stratégies avancée, vous pouvez configurer des groupes personnalisés de stratégies (banques de stratégies) en définissant une étiquette de stratégie et en collectant un ensemble de stratégies associées sous cette étiquette.
- Autres points de liaison. La disponibilité de points de liaison supplémentaires dépend du type de stratégie avancée et des spécificités de la fonctionnalité NetScaler correspondante.

Pour plus d'informations sur les liaisons de stratégie avancées, consultez la rubrique Liaison de stratégies qui utilisent la rubrique Stratégies avancées .

À propos de l'ordre d'évaluation des stratégies

Les fonctionnalités de NetScaler sont traitées dans un certain ordre, ce qui inclut l'évaluation des stratégies relatives à la fonctionnalité et l'exécution des actions sélectionnées. Pour plus d'informations, consultez la section Flux de paquets.

À tout moment du traitement des messages, l'évaluation des stratégies est effectuée en fonction de la combinaison des éléments suivants :

- Protocole (tel que HTTP, SIP, TCP ou Diameter)
- Direction (demande ou réponse)
- Fonctionnalité (telle que Rewrite, Responder ou Bot)

Les combinaisons ne peuvent pas être mélangées. Les stratégies sont évaluées dans des groupes de stratégies appelés banques (également appelés étiquettes de stratégie ou points de liaison) dans l'ordre suivant :

1. Dépassement global
2. Serveur virtuel LB spécifique utilisé
3. Si un serveur virtuel CS spécifique est utilisé
4. Valeur par défaut globale

Au sein d'une banque, les stratégies sont évaluées de la priorité la plus faible à la plus élevée. Si une règle de stratégie est considérée comme fausse, l'évaluation passe automatiquement à la priorité numérotée la plus élevée suivante dans la même banque. S'il n'existe aucune règle de stratégie dans la même banque, l'évaluation porte sur la première stratégie de la banque suivante dans la commande. S'il n'y a plus de stratégies, l'évaluation des stratégies prend fin. Si une règle de stratégie est considérée comme vraie, l'action ou le profil correspondant est mémorisé en vue d'une éventuelle exécution ultérieure.

Si la stratégie est évaluée comme vraie, la valeur « GoToPriorityExpression » est vérifiée. Si « gotoPriorityExpression » a la valeur « END », l'évaluation de la stratégie s'arrête. Si « NEXT », la stratégie suivante (comme décrit ci-dessus) est évaluée. S'il s'agit d'une expression, cette expression est évaluée et la stratégie ayant cette priorité est ensuite sélectionnée.

> **Remarque**
>
> La valeur par défaut de « gotoPriorityExpression » est « END ». Toutefois, pour certaines fonctionnalités capables d'exécuter toutes les actions, il est recommandé de spécifier explicitement la valeur « gotoPriorityExpression ».

Une fois l'évaluation des stratégies terminée, la fonctionnalité exécute la liste ordonnée des actions ou des profils. Les fonctionnalités exécutent toutes les actions (par exemple, Rewrite) ou exécutent une seule action (par exemple, Responder ou Bot). Si plusieurs actions ou profils sont associés à une fonction qui ne peut en exécuter qu'une, la norme consiste à exécuter la dernière. Si aucune action ou aucun profil n'est sélectionné, la fonctionnalité exécute son action par défaut.

Order of evaluation based on traffic flow

Certaines stratégies influent sur le résultat d'autres stratégies. Voici des exemples :

- Si une réponse est fournie à partir du cache intégré, certaines autres fonctionnalités de NetScaler ne traitent pas la réponse ni la demande qui l'a initiée.
- Si le pare-feu d'application rejette une demande entrante, aucune autre fonctionnalité ne peut la traiter.
- La plupart des actions effectuées par Responder interrompent le traitement ultérieur.
- Les actions Drop et Reset effectuées par Rewrite interrompent le traitement ultérieur.

Expressions de stratégie avancées

May 5, 2023

L'une des composantes les plus fondamentales d'une politique est sa règle. Une règle de stratégie est une expression logique qui permet à la stratégie d'analyser le trafic. La plupart des fonctionnalités de la stratégie sont dérivées de son expression.

Une expression met en correspondance les caractéristiques du trafic ou d'autres données avec un ou plusieurs paramètres et valeurs. Par exemple, une expression peut permettre à NetScaler d'accomplir les tâches suivantes :

- Déterminez si une demande contient un certificat.
- Déterminez l'adresse IP d'un client qui a envoyé une demande TCP.
- Identifiez les données contenues dans une requête HTTP (par exemple, une feuille de calcul populaire ou une application de traitement de texte).
- Calculez la longueur d'une requête HTTP.

À propos des expressions de stratégie avancées

Toute fonctionnalité qui utilise une infrastructure de stratégie avancée utilise également des expressions avancées. Pour plus d'informations sur les fonctionnalités qui utilisent des politiques avancées, consultez le tableau Fonctionnalité de NetScaler, type de stratégie et Utilisation des politiques.

Les expressions de stratégie avancées ont d'autres utilisations. Outre la configuration des expressions avancées dans les règles de stratégie, vous configurez les
expressions avancées dans les situations suivantes :

- Mise en cache intégrée :

  Vous utilisez des expressions de stratégie avancées pour configurer un sélecteur pour un groupe de contenus dans le cache intégré.

- Équilibrage de charge :

  Vous utilisez des expressions de stratégie avancées pour configurer l'extraction de jetons pour un serveur virtuel d'équilibrage de charge qui utilise la méthode TOKEN pour l'équilibrage de charge.

- Réécriture :

  Vous utilisez des expressions de stratégie avancées pour configurer les actions de réécriture.

- Stratégies basées sur les taux :

  Vous utilisez des expressions de stratégie avancées pour configurer des sélecteurs de limite lorsque vous configurez une stratégie pour contrôler le taux de trafic vers différents serveurs.

Voici quelques exemples simples d'expressions de stratégie avancées :

- Une URL de requête HTTP ne contient pas plus de 500 caractères.

```
http.req.url.length \<= 500
```

- Une requête HTTP contient un cookie de moins de 500 caractères.

```
http.req.cookie.length \< 500
```

- Une URL de requête HTTP contient une chaîne de texte particulière.

```
http.req.url.contains(".html")
```

Conversion des expressions de stratégie à l'aide de l'outil NSPEPI

June 20, 2023

> **Remarque :**
>
> Vous pouvez télécharger l'outil de vérification NSPEPI et de pré-configuration depuis le GitHub public. Pour plus d'informations, consultez la page GitHub NEPEPI et la page README pour obtenir des instructions détaillées sur le téléchargement, l'installation et l'utilisation des outils. Nous recommandons aux clients d'utiliser les outils disponibles dans GitHub pour obtenir la version la plus complète et la plus récente.

Les fonctionnalités et fonctionnalités classiques basées sur des règles sont obsolètes à partir de NetScaler 12.0 build 56.20. Comme alternative, Citrix vous recommande d'utiliser l'infrastructure de stratégie avancée. Dans le cadre de cet effort, lorsque vous effectuez une mise à niveau vers NetScaler 12.1 build 56.20 ou version ultérieure, vous devez remplacer les fonctionnalités classiques basées sur des stratégies par les fonctionnalités et fonctionnalités non obsolètes correspondantes. Vous devez également convertir les stratégies et expressions classiques en stratégies et expressions

avancées. De plus, toutes les nouvelles fonctionnalités de NetScaler ne prennent en charge que l'infrastructure de stratégies avancées.

L'outil `nspepi` peut effectuer les opérations suivantes :

1. Convertissez les expressions de stratégie classiques en expressions de stratégie avancées.
2. Convertissez certaines stratégies classiques et leurs liaisons d'entités en stratégies et liaisons avancées.
3. Convertissez quelques autres entités obsolètes en fonctionnalités non dépréciées correspondantes.
4. Convertissez les commandes de filtre classiques en commandes de filtrage avancées.

> **Remarque :**
>
> Une fois que l'outil `nspepi` a réussi à convertir le fichier de configuration ns.conf, il affiche le fichier converti sous la forme d'un nouveau fichier avec le préfixe « new_ ». Si le fichier de configuration converti contient des erreurs ou des avertissements, vous devez les corriger manuellement dans le cadre du processus de conversion. Une fois converti, vous devez tester le fichier dans l'environnement de test, puis l'utiliser pour remplacer le fichier de configuration ns.conf actuel. Après le test, vous devez redémarrer l'appliance pour le fichier de configuration ns.conf nouvellement converti ou corrigé.

Les fonctionnalités qui ne prennent en charge que les stratégies ou expressions classiques sont obsolètes et peuvent être remplacées par les fonctionnalités non obsolètes correspondantes.

> **Remarque :**
>
> Les informations relatives à l'ancienne version de l'outil `nspepi` sont disponibles au format PDF. Pour plus d'informations, consultez la section Conversion de stratégie classique à l'aide de l'outil nspepi avant la version 12.1-51.16 PDF.

Avertissements de conversion et fichiers d'erreur

Avant d'utiliser l'outil pour votre conversion, il y a quelques avertissements à garder à l'esprit :

1. Tous les avertissements et erreurs sont affichés sur la console. Un fichier d'avertissement est créé dans lequel les fichiers de configuration sont stockés.
2. Le fichier d'avertissement et d'erreur porte le même nom que le fichier d'entrée, mais avec le préfixe « warn_» ajouté au nom du fichier. Lors de la conversion d'expression (avec l'option -e), les avertissements apparaissent dans le répertoire courant sous le nom « warn_expr ».

> **Remarque :**
>
> Ce fichier est au format de fichier journal standard, avec horodatage et niveau de journalisation. Les instances précédentes du fichier sont conservées avec des suffixes tels que ".1", ".2", etc., car

> l'outil est exécuté plusieurs fois. Au plus 10 instances seront conservées.

Format de fichier converti

Lors de la conversion d'un fichier de configuration (en utilisant « -f »), le fichier converti est placé dans le même répertoire que celui où existe le fichier de configuration d'entrée portant le même nom mais avec le préfixe « new_ ».

Commandes ou fonctionnalités gérées par l'outil de conversion nspepi

Voici les commandes gérées pendant le processus de conversion automatique.

- Les stratégies classiques suivantes et leurs expressions sont converties en stratégies et expressions avancées. La conversion inclut les liaisons d'entités et les liaisons globales.

1. add appfw policy
2. add cmp policy
3. add cr policy
4. add cs policy
5. add tm sessionPolicy
6. add filter action
7. add filter policy
8. liaison de stratégie de filtre à l'équilibrage de charge, à la commutation de contenu, à la redirection du cache et à la stratégie globale.

> **Remarque :**
>
> Toutefois, pour « add tm SessionPolicy », vous ne pouvez pas vous lier au remplacement global dans les stratégies avancées.

- Le paramètre de règle configuré dans « add lb virtual server » est converti de l'expression classique à l'expression avancée.
- Le paramètre SPDY configuré dans la commande « add ns HttpProfile » ou « set ns HttpProfile » est remplacé par « -http2 ENABLED ».
- Expressions nommées (commandes « add policy expression »). Chaque expression de stratégie nommée Classic est convertie en son expression nommée Advanced correspondante avec « nspepi_adv_ » défini comme préfixe. En outre, l'utilisation des expressions nommées pour les expressions classiques converties est remplacée par les expressions nommées avancées correspondantes. De plus, chaque expression nommée comporte deux expressions nommées, l'une étant classique et l'autre avancée (comme illustré ci-dessous).
- La conversion Tunnel TrafficPolicy est prise en charge.
- Gestion des liaisons de stratégie classiques intégrées dans CMP, CR et Tunnel.
- La fonction Patclass est convertie en fonction Pat set.

- Le paramètre « -pattern » de la commande « add rewrite action » est converti pour utiliser le paramètre « -search ».
- Les préfixes Q et S des expressions avancées sont convertis en expressions avancées non obsolètes équivalentes. Ces expressions sont visibles dans toutes les commandes où les expressions avancées sont autorisées.

Par exemple :

```
add policy expression classic_expr ns_true
Converts to:
add policy expression classic_expr ns_true
add policy expression nspepi_adv_classic_expr TRUE
<!--NeedCopy-->
```

- Le paramètre PolicyType configuré dans la commande « set cmp parameter » est supprimé. Par défaut, le type de stratégie est « Avancé ».

Convertir les commandes de filtre classiques en commandes de filtrage avancées

L' outil `nspepi` peut convertir des commandes basées sur des actions de filtre classiques telles que l'ajout, la liaison, etc. en commandes de filtrage avancées.

Toutefois, l'outil nepepi ne prend pas en charge les commandes de filtre suivantes.

1. add filter action <`action Name`> FORWARD <`service name`>
2. add filter action <`action name`> ADD prebody
3. add filter action <`action name`> ADD postbody

> **Remarque :**
>
> 1. S'il existe des fonctionnalités de réécriture ou de répondeur dans ns.conf et que leurs stratégies sont liées globalement à l'expression `GOTO` en tant que `END` ou `USER_INVOCATION_RESULT` et que le type de liaison est `REQ_X` ou `RES_X` alors l'outil convertit partiellement les commandes de filtre de liaison et les commente. Un message d'erreur s'affiche lors de la conversion manuelle.
> 2. S'il existe des fonctionnalités de réécriture ou de répondeur existantes et que leurs stratégies sont liées à des serveurs virtuels (par exemple, équilibrage de charge, changement de contenu ou redirection de cache) de type HTTPS avec `GOTO - END` ou `USER_INVOCATION_RESULT`, l'outil convertit partiellement les commandes de filtre de liaison, puis les commente. Un avertissement s'affiche pour la conversion manuelle.

Exemple

Voici un exemple d'entrée :


```
add lb vserver v1 http 1.1.1.1 80 -persistenceType NONE -cltTimeout
    9000
add cs vserver csv1 HTTP 1.1.1.2 80 -cltTimeout 180 -persistenceType
    NONE
add cr vserver crv1 HTTP 1.1.1.3 80 -cacheType FORWARD
add service svc1 1.1.1.4 http 80
add filter action fact_add add 'header:value'
add filter action fact_variable add 'H1:%%HTTP.TRANSID%%'
add filter action fact_prebody add prebody
add filter action fact_error_act1 ERRORCODE 200 "<HTML>Good URL</HTML>"
add filter action fact_forward_act1 FORWARD svc1
add filter policy fpol_add_res -rule ns_true -resAction fact_add
add filter policy fpol_error_res -rule ns_true -resAction
    fact_error_act1
add filter policy fpol_error_req -rule ns_true -reqAction
    fact_error_act1
add filter policy fpol_add_req -rule ns_true -reqAction fact_add
add filter policy fpol_variable_req -rule ns_true -reqAction
    fact_variable
add filter policy fpol_variable_res -rule ns_true -resAction
    fact_variable
add filter policy fpol_prebody_req -rule ns_true -reqAction
    fact_prebody
add filter policy fpol_prebody_res -rule ns_true -resAction
    fact_prebody
add filter policy fpol_forward_req -rule ns_true -reqAction
    fact_forward_act1
bind lb vserver v1 -policyName fpol_add_res
bind lb vserver v1 -policyName fpol_add_req
bind lb vserver v1 -policyName fpol_error_res
bind lb vserver v1 -policyName fpol_error_req
bind lb vserver v1 -policyName fpol_variable_res
bind lb vserver v1 -policyName fpol_variable_req
bind lb vserver v1 -policyName fpol_forward_req
bind cs vserver csv1 -policyName fpol_add_req
bind cs vserver csv1 -policyName fpol_add_res
bind cs vserver csv1 -policyName fpol_error_res
bind cs vserver csv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_add_req
bind cr vserver crv1 -policyName fpol_add_res
bind cr vserver crv1 -policyName fpol_error_res
bind cr vserver crv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_forward_req
bind filter global fpol_add_req
```



```
bind filter global fpol_add_res
bind filter global fpol_error_req
bind filter global fpol_error_res
bind filter global fpol_variable_req
bind filter global fpol_variable_res
bind filter global fpol_variable_res -state DISABLED
bind filter global fpol_prebody_req
bind filter global fpol_forward_req
After conversion, warning/error messages will be displayed for manual effort.
Warning files:
cat warn_<input file name>:
2019-11-07 17:13:34,724: ERROR - Conversion of [add filter action fact_prebody add prebody] not supported in this tool.
2019-11-07 17:13:34,739: ERROR - Conversion of [add filter action fact_forward_act1 FORWARD svc1] not supported in this tool.
2019-11-07 17:13:38,042: ERROR - Conversion of [add filter policy fpol_prebody_req -rule ns_true -reqAction fact_prebody] not supported in this tool.
2019-11-07 17:13:38,497: ERROR - Conversion of [add filter policy fpol_prebody_res -rule ns_true -resAction fact_prebody] not supported in this tool.
2019-11-07 17:13:39,035: ERROR - Conversion of [add filter policy fpol_forward_req -rule ns_true -reqAction fact_forward_act1] not supported in this tool.
2019-11-07 17:13:39,060: WARNING - Following bind command is commented out because state is disabled. Advanced expressions only have a fixed ordering of the types of bindings without interleaving, except that global bindings are allowed before all other bindings and after all bindings. If you have global bindings in the middle of non-global bindings or any other interleaving then you will need to reorder all your bindings for that feature and direction. Refer to nspepi documentation. If command is required please take a backup because comments will not be saved in ns.conf after triggering 'save ns config': bind filter global fpol_variable_res -state DISABLED


<!--NeedCopy-->
```

Voici un exemple de sortie. Toutes les commandes converties sont commentées.

```
cat new_<input file name>
add rewrite action fact_add insert_http_header header ""value""
add filter action fact_prebody add prebody
add filter action fact_forward_act1 FORWARD svc1
```



```
add filter policy fpol_prebody_req -rule ns_true -reqAction
    fact_prebody
add filter policy fpol_prebody_res -rule ns_true -resAction
    fact_prebody
add filter policy fpol_forward_req -rule ns_true -reqAction
    fact_forward_act1
bind lb vserver v1 -policyName fpol_forward_req
bind cr vserver crv1 -policyName fpol_forward_req
#bind filter global fpol_variable_res -state DISABLED
bind filter global fpol_prebody_req
bind filter global fpol_forward_req
add rewrite action nspepi_adv_fact_variable insert_http_header H1 HTTP.
    RES.TXID
add rewrite action fact_variable insert_http_header H1 HTTP.REQ.TXID
add responder action fact_error_act1 respondwith "HTTP.REQ.VERSION.
    APPEND(" 200 OK\r
nConnection: close\r
nContent-Length: 21\r\n\r
n<HTML>Good URL</HTML>")"
add rewrite action nspepi_adv_fact_error_act1 replace_http_res "HTTP.
    REQ.VERSION.APPEND(" 200 OK\r
nConnection: close\r
nContent-Length: 21\r\n\r
n<HTML>Good URL</HTML>")"
add rewrite policy fpol_add_res TRUE fact_add
add rewrite policy fpol_error_res TRUE nspepi_adv_fact_error_act1
add responder policy fpol_error_req TRUE fact_error_act1
add rewrite policy fpol_add_req TRUE fact_add
add rewrite policy fpol_variable_req TRUE fact_variable
add rewrite policy fpol_variable_res TRUE nspepi_adv_fact_variable
set cmp parameter -policyType ADVANCED
bind rewrite global fpol_add_req 100 NEXT -type REQ_DEFAULT
bind rewrite global fpol_variable_req 200 NEXT -type REQ_DEFAULT
bind rewrite global fpol_add_res 100 NEXT -type RES_DEFAULT
bind rewrite global fpol_error_res 200 NEXT -type RES_DEFAULT
bind rewrite global fpol_variable_res 300 NEXT -type RES_DEFAULT
bind responder global fpol_error_req 100 END -type REQ_DEFAULT
bind lb vserver v1 -policyName fpol_add_res -type RESPONSE -priority
    100 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_error_res -type RESPONSE -priority
    200 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_variable_res -type RESPONSE -
    priority 300 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_add_req -type REQUEST -priority 100
     -gotoPriorityExpression NEXT
```



```
bind lb vserver v1 -policyName fpol_variable_req -type REQUEST -priority 200 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_error_req -type REQUEST -priority 100 -gotoPriorityExpression END
bind cs vserver csv1 -policyName fpol_add_req -type REQUEST -priority 100 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_add_res -type RESPONSE -priority 100 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_error_res -type RESPONSE -priority 200 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_error_req -type REQUEST -priority 100 -gotoPriorityExpression END
bind cr vserver crv1 -policyName fpol_add_req -type REQUEST -priority 100 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_add_res -type RESPONSE -priority 100 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_error_res -type RESPONSE -priority 200 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_error_req -type REQUEST -priority 100 -gotoPriorityExpression END

<!--NeedCopy-->
```

Convertir les commandes de filtre classiques en commandes de fonctionnalités avancées si les liaisons de stratégie de réécriture ou de répondeur existantes ont atteint l'expression END ou USE_INNVOCATION

Dans cette conversion, si une stratégie de réécriture est liée à un ou plusieurs serveurs virtuels et si le serveur possède END ou USE_INVOCATION_RESULT, l'outil commente les commandes.

Exemple

Voici un exemple de commande d'entrée :

```
COPY
add filter policy fpol1 -rule ns_true -resAction reset
add filter policy fpol2 -rule ns_true -reqAction reset
add rewrite policy pol1 true NOREWRITE
add rewrite policylabel pl http_res
bind rewrite policylabel pl pol1 1
bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT -invoke policylabel pl
add responder policy pol2 true NOOP
```



```
add responder policylabel pl -policylabeltype HTTP
bind responder policylabel pl pol2 1
bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
   REQ_DEFAULT -invoke policylabel pl
bind lb vserver v1_tcp -policyName pol1 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind lb vserver v1_tcp -policyName pol2 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind lb vserver v1_http -policyName fpol1
bind cs vserver csv1_http -policyName fpol1
bind lb vserver v2_http -policyName fpol2
bind cs vserver csv2_http -policyName fpol2
bind cr vserver crv2_http -policyName fpol2
bind filter global fpol1 -priority 100
bind filter global fpol2 -priority 100
<!--NeedCopy-->
```

Voici un exemple de commande de sortie :

```
COPY
add rewrite policy pol1 true NOREWRITE
add rewrite policylabel pl http_res
bind rewrite policylabel pl pol1 1
add responder policy pol2 true NOOP
add responder policylabel pl -policylabeltype HTTP
bind responder policylabel pl pol2 1
add rewrite policy fpol1 TRUE RESET
add responder policy fpol2 TRUE RESET
#bind lb vserver v1_http -policyName fpol1 -type RESPONSE
#bind cs vserver csv1_http -policyName fpol1 -type RESPONSE
#bind rewrite global fpol1 100 -type RES_DEFAULT
#bind lb vserver v2_http -policyName fpol2 -type REQUEST
#bind cs vserver csv2_http -policyName fpol2 -type REQUEST
#bind cr vserver crv2_http -policyName fpol2 -type REQUEST
#bind responder global fpol2 100 -type REQ_DEFAULT
bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT
   -invoke policylabel pl
bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
   REQ_DEFAULT -invoke policylabel pl
```



```
19 bind lb vserver v1_tcp -policyName pol1 -priority 100 -
      gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
20 bind lb vserver v1_tcp -policyName pol2 -priority 100 -
      gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
21 bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
      gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
22 bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
      gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
23 bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
      gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST-
24
25 <!--NeedCopy-->
```

Commandes ou fonctionnalités non gérées par l'outil de conversion nspepi

Voici quelques commandes qui ne sont pas gérées dans le cadre du processus de conversion automatique.

- Certaines liaisons ne peuvent pas être converties s'il existe un certain entrelacement des priorités entre les points de liaison globaux et non globaux, entre les utilisateurs et les groupes, ainsi qu'entre les liaisons vers différentes entités. La configuration affectée est commentée et une erreur est générée. Ces configurations doivent être converties manuellement.
- Les stratégies Classic et Advanced peuvent être liées à cmp global. Dans de nombreux cas, la fonctionnalité change une fois que les stratégies classiques sont converties en stratégies avancées. Nous avons converti des commandes qui peuvent être résolues en commentant certaines stratégies. Certaines commandes ne peuvent cependant pas être converties. Dans ce cas, une erreur se produit et la conversion doit être effectuée manuellement.
- Les expressions nommées intégrées classiques ne sont pas toutes converties en expressions nommées Advanced équivalentes.
- Les expressions de sécurité client ne sont pas gérées.
- SureConnect (SC)
- Priority Queuing (PQ)
- HTTP Denial of Service (HDOS)
- HTML Injection
- Authentification
- Authorization
- VPN
- Syslog
- Nslog
- Les expressions classiques basées sur des fichiers ne sont pas gérées.

> **Remarque :**
>
> Pour certaines fonctionnalités telles que PatClass/Filter, la syntaxe de la commande est modifiée. S'il existe des stratégies cmd, les stratégies cmd peuvent devoir être modifiées en fonction des besoins du client.

Problèmes connus

Les scénarios suivants provoquent des erreurs dans l' `nspepi` outil

- En cas de problème lors de la conversion d'une expression
- Si une expression de stratégie nommée utilise le paramètre -ClientSecurityMessage parce que ce paramètre n'est pas pris en charge dans l'expression de stratégie avancée
- Si l'expression de la règle du serveur virtuel d'équilibrage de charge est une expression complexe comportant plusieurs expressions basées sur le CONTENU.
- Erreur lors de la conversion des fonctionnalités CMP
  - Lorsque les stratégies classiques et avancées sont liées à la mondialisation.
  - Lorsque les stratégies classiques sont liées et que le paramètre cmp est avancé.
  - Lorsque des stratégies avancées sont liées et que le paramètre cmp est classique.
  - Lorsque les stratégies classiques sont liées à un serveur virtuel et que les stratégies avancées sont liées à un serveur global.
  - Lorsque les stratégies avancées sont liées à un serveur virtuel alors que les stratégies classiques sont liées à un serveur global.
  - Lorsque les stratégies classiques sont liées à un serveur virtuel et que les stratégies classiques et avancées sont liées à un serveur global.
  - Lorsque les stratégies avancées sont liées à un serveur virtuel et que les stratégies classiques et avancées sont liées à un serveur global.
- Si l'expression nommée classique porte le même nom que le nom de l'entité de légende
- Si le nom de l'expression classique n'est pas valide pour l'expression avancée
- Si la longueur de l'expression convertie est supérieure à 1499 caractères
- Si l'expression classique comporte des expressions basées sur la sécurité du client ou des expressions basées sur des fichiers

Avertissement

Les scénarios suivants présentent les avertissements de l' `nspepi` outil

- Si l'expression de la règle du serveur virtuel d'équilibrage de charge est une expression booléenne, l'expression avancée équivalente génère une valeur booléenne au format chaîne. Cela entraîne une modification des fonctionnalités lorsque la règle est utilisée pour `persistenceType` ou `lbMethod`. Pour éviter le changement de fonctionnalité, la commande est modifiée en supprimant le `keywords rule` et `persistenceType`.

- Si le champ d'état de la commande de liaison est DÉSACTIVÉ. Si l'état est désactivé, la commande n'est pas utilisée. Le paramètre d'état n'est pas pris en charge par la configuration avancée. Donc, si nous convertissons cette configuration, la fonctionnalité change. Si la commande est requise, effectuez une sauvegarde car les commentaires ne seront pas enregistrés `ns.conf` après le déclenchement `save ns config`.

Avertissement lors de la conversion des fonctionnalités CMP :

- Si le type de stratégie d'un paramètre cmp global est défini sur CLASSIC et que les stratégies avancées sont liées au paramètre global. Sans conversion, les stratégies avancées limitées ne seront pas évaluées car le type de stratégie globale est défini sur CLASSIC. Après la conversion, le type de stratégie serait converti en AVANCÉ. Ainsi, si nous ne commentons pas les liaisons avancées globales existantes, ces liaisons sont évaluées et peuvent modifier les fonctionnalités.
- Si le type de stratégie du paramètre cmp global est défini sur ADVANCED et que les stratégies classiques sont liées au paramètre global. Sans conversion, ces liaisons classiques globales ne seraient pas évaluées car le type de stratégie globale est AVANCÉ. Pour préserver la fonctionnalité, nous commentons la configuration convertie. Dans le cas contraire, les stratégies avancées converties sont évaluées et peuvent modifier la fonctionnalité.

> **Remarque :**
>
> Toutes les liaisons de stratégie classiques avec l'option -state désactivée sont commentées. L'option -state n'est pas disponible pour les liaisons de stratégie avancées.

Exécution de l'outil nspepi

Voici un exemple de ligne de commande permettant d'exécuter l'outil `nspepi`. Cet outil est exécuté à partir de la ligne de commande du shell (vous devez taper la commande « shell » dans le « CLI » de NetScaler pour y accéder). « -f » ou « -e » doivent être spécifiés pour effectuer une conversion. L'utilisation de « -d » est destinée au personnel Citrix pour l'analyse à des fins de support.

```
1  usage: nspepi [-h] (-e <classic policy expression> | -f <path to ns
       config file>)[-d] [-v] [-V
2
3  Convert classic policy expressions to advanced policy expressions and
       deprecated commands to non-deprecated
4  commands.
5
6  optional arguments:
7  -h, --help show this help message and exit
8  -e <classic policy expression>, --expression <classic policy expression
       >
9  convert classic policy expression to advanced policy
10 expression (maximum length of 8191 allowed)
```



```
-f <path to ns config file>, --infile <path to ns config file>
convert netscaler config file
-d, --debug log debug output
-v, --verbose show verbose output
-V, --version show program's version number and exit
<!--NeedCopy-->
```

Exemples d'utilisation :

1. `nspepi -e "req.tcp.destport == 80"`
2. `nspepi -f /var/nsconfig/ns.conf`

Voici quelques exemples d'exécution de l'outil `nspepi` à l'aide de l'interface de ligne de commande :

Exemple de sortie pour le paramètre —e :

```
root@ns# nspepi -e "req.http.header foo == "bar""
"HTTP.REQ.HEADER("foo").EQ("bar")"
<!--NeedCopy-->
```

Exemple de sortie pour le paramètre -f :

```
root@ns# cat sample.conf
add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180 -
   originUSIP OFF
add cr policy cr_pol1 -rule ns_true
bind cr vserver cr_vs -policyName cr_pol1
<!--NeedCopy-->
```

Exécution de nspepi avec le paramètre -f :

```
nspepi -f sample.conf
<!--NeedCopy-->
```

La configuration convertie est disponible dans un nouveau fichier `new_sample.conf`.
Recherchez dans le fichier `warn_sample.conf` les avertissements ou erreurs qui ont pu être générés.

Exemple de sortie du paramètre -f avec le paramètre -v

```
nspepi -f sample.conf -v
INFO - add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180
    -originUSIP OFF
INFO - add cr policy cr_pol1 -rule TRUE -action ORIGIN
INFO - bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
   gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```


La configuration convertie est disponible dans un nouveau fichier `new_sample.conf`.
Recherchez dans le fichier `warn_sample.conf` les avertissements ou erreurs qui ont pu être générés.

Fichier de configuration converti :

```
root@ns# cat new_sample.conf
add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180 -
    originUSIP OFF
add cr policy cr_pol1 -rule TRUE -action ORIGIN
set cmp parameter -policyType ADVANCED
bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
    gotoPriorityExpression END -type REQUEST

<!--NeedCopy-->
```

Exemple de sortie d'un exemple de configuration sans erreur ni avertissement :

```
nspepi -f sample_2.conf
<!--NeedCopy-->
```

La configuration convertie est disponible dans un nouveau fichier `new_sample_2.conf`.
Recherchez dans le fichier `warn_sample_2.conf` les avertissements ou erreurs qui ont pu être générés.

Exemple de sortie d'un exemple de configuration avec des avertissements :

```
root@ns# cat sample_2.conf
add policy expression security_expr "req.tcp.destport == 80" -
    clientSecurityMessage "Not allowed"
set cmp parameter -policyType CLASSIC
add cmp policy cmp_pol1 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol2 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
bind cmp global cmp_pol1
bind cmp global cmp_pol2 -state DISABLED
bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
    RES_DEFAULT
bind lb vserver lb_vs -policyName cmp_pol2
root@ns#
<!--NeedCopy-->
```

Exemple d'exécution de nspepi avec le paramètre -f :

```
root@ns# nspepi -f sample_2.conf
ERROR - Error in converting expression security_expr : conversion of
    clientSecurityMessage based expression is not supported.
```



```
3 WARNING - Following bind command is commented out because state is
    disabled. Advanced expressions only have a fixed ordering of the
    types of bindings without interleaving, except that global bindings
    are allowed before all other bindings and after all bindings. If you
     have global bindings in the middle of non-global bindings or any
    other interleaving then you will need to reorder all your bindings
    for that feature and direction. Refer to nspepi documentation. If
    command is required please take a backup because comments will not
    be saved in ns.conf after triggering 'save ns config': bind cmp
    global cmp_pol2 -state DISABLED
4 Warning - Bindings of advanced CMP policies to cmp global are commented
     out, because initial global cmp parameter is classic but advanced
    policies are bound. Now global cmp parameter policy type is set to
    advanced. If commands are required please take a backup because
    comments will not be saved in ns.conf after triggering 'save ns
    config'. Advanced expressions only have a fixed ordering of the
    types of bindings without interleaving, except that global bindings
    are allowed before all other bindings and after all bindings. If you
     have global bindings in the middle of non-global bindings or any
    other interleaving then you will need to reorder all your bindings
    for that feature and direction. Refer to nspepi documentation.
5 root@ns#
6 <!--NeedCopy-->
```

Fichier converti :

```
1  root@ns# cat new_sample_2.conf
2  add policy expression security_expr "req.tcp.destport == 80" -
       clientSecurityMessage "Not allowed"
3  set cmp parameter -policyType ADVANCED
4  add cmp policy cmp_pol1 -rule TRUE -resAction COMPRESS
5  add cmp policy cmp_pol2 -rule TRUE -resAction COMPRESS
6  add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
7  #bind cmp global cmp_pol2 -state DISABLED
8  #bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
       RES_DEFAULT
9  bind cmp global cmp_pol1 -priority 100 -gotoPriorityExpression END -
       type RES_DEFAULT
10 bind lb vserver lb_vs -policyName cmp_pol2 -priority 100 -
       gotoPriorityExpression END -type RESPONSE
11 root@ns#
12 <!--NeedCopy-->
```

Fichier d'avertissement :


```
root@ns# cat warn_sample_2.conf
2019-02-28 06:20:10,590: ERROR - Error in converting expression
    security_expr : conversion of clientSecurityMessage based expression
     is not supported.
2019-02-28 06:20:12,187: WARNING - Following bind command is commented
    out because state is disabled. Advanced expressions only have a
    fixed ordering of the types of bindings without interleaving, except
     that global bindings are allowed before all other bindings and
    after all bindings. If you have global bindings in the middle of non
    -global bindings or any other interleaving then you will need to
    reorder all your bindings for that feature and direction. Refer to
    nspepi documentation. If command is required please take a backup
    because comments will not be saved in ns.conf after triggering 'save
     ns config': bind cmp global cmp_pol2 -state DISABLED
2019-02-28 06:20:12,191: WARNING - Bindings of advanced CMP policies to
     cmp global are commented out, because initial global cmp parameter
    is classic but advanced policies are bound. Now global cmp parameter
     policy type is set to advanced. If commands are required please
    take a backup because comments will not be saved in ns.conf after
    triggering 'save ns config'. Advanced expressions only have a fixed
    ordering of the types of bindings without interleaving, except that
    global bindings are allowed before all other bindings and after all
    bindings. If you have global bindings in the middle of non-global
    bindings or any other interleaving then you will need to reorder all
     your bindings for that feature and direction. Refer to nspepi
    documentation.
root@ns#
<!--NeedCopy-->
```

Priorités liées

Les stratégies avancées n'autorisent pas l'entrelacement arbitraire par priorité entre global et non global et entre différents types de liaison. Si vous vous fiez à un tel entrelacement des priorités de stratégie classique, vous devez ajuster les priorités pour qu'elles soient conformes aux règles de stratégie avancées et pour obtenir le comportement souhaité.
Les priorités des stratégies avancées sont locales à un point de liaison. Un point de liaison est une combinaison unique de protocole, de fonctionnalité, de direction et d'entité (les entités sont des serveurs virtuels spécifiques, des utilisateurs, des groupes, des services et soit un remplacement global, soit un défaut global). Les priorités stratégies ne sont pas suivies à travers les points de liaison.

Pour un protocole, une fonctionnalité et une direction donnés, l'ordre d'évaluation des stratégies avancées est le suivant :

- REMPLACEMENT GLOBAL.
- Authentification, autorisation et audit de l'utilisateur (actuel).
- Groupes d'authentification, d'autorisation et d'audit (dont l'utilisateur est membre) par ordre de pondération - l'ordre n'est pas défini si deux groupes ou plus ont le même poids.
- Serveur virtuel LB sur lequel la demande a été reçue ou que Content Switching a sélectionné.
- Serveur virtuel de commutation de contenu, serveur virtuel de redirection de cache sur lequel la demande a été reçue.
- Service sélectionné par l'équilibrage de charge.
- Valeur par défaut globale.

Pour l'évaluation de la stratégie d'autorisation, l'ordre est le suivant :

- Les systèmes sont priorisés.
- Serveur virtuel d'équilibrage de charge sur lequel la demande a été reçue ou sur lequel CS a été sélectionné.
- Serveur virtuel de commutation de contenu sur lequel la demande a été reçue.
- Valeur par défaut du système.

Dans chaque point de liaison, les stratégies sont évaluées par ordre de priorité, du numéro le plus bas au numéro le plus élevé. Les stratégies ne sont évaluées que pour le protocole utilisé et la direction d'où le message a été reçu.

Liaisons de stratégie classiques nécessitant une redéfinition manuelle des priorités

Voici quelques types de liaisons de stratégie classiques qui nécessitent une redéfinition manuelle des priorités pour répondre à vos besoins. Tous ces éléments sont destinés à un trait donné et à la direction.

- Priorités classiques dont le numéro de priorité augmente en sens inverse de la direction des listes de types d'entités ci-dessus. Par exemple, une liaison de serveur virtuel de commutation de contenu inférieure à une liaison de serveur virtuel d'équilibrage de charge.
- Priorités classiques qui entrelacent les groupes d'authentification, d'autorisation et d'audit. Une partie d'un groupe se trouve avant un autre groupe et une autre partie se trouve après une partie de cet autre groupe.
- Priorités classiques qui augmentent en nombre autre que l'ordre de pondération des groupes d'authentification, d'autorisation et d'audit.
- Les priorités mondiales classiques qui sont inférieures à certaines priorités non mondiales et les mêmes priorités mondiales sont supérieures à d'autres priorités non mondiales (en d'autres termes, tout segment de priorités non mondiales, suivi d'une ou de plusieurs priorités mondiales, suivi d'une ou de plusieurs priorités non mondiales).

Les outils NSPEPI et check_invalid_config peuvent être exécutés sur les systèmes CentOS et Ubuntu

Les modules suivants constituent les prérequis pour utiliser ces outils :

- Python
- Perl
- module Python Pip
- Module Play pour Python
- Switch.pm pour Perl

Outil de vérification de la préconfiguration

June 2, 2023

> **Remarque :**
>
> Vous pouvez télécharger l'outil de vérification NSPEPI et preconfig à partir de GitHub public. Pour plus d'informations, consultez la page NEPEPI de GitHubet la page de préconfiguration de GitHub pour obtenir des instructions détaillées sur le téléchargement des outils. Nous recommandons aux clients d'utiliser les outils disponibles dans GitHub pour obtenir la version la plus complète et la plus récente.

Un outil de pré-validation est disponible dans les versions NetScaler 12.1, 13.0 et 13.1 pour vérifier si des fonctionnalités non valides ou supprimées sont toujours utilisées dans une configuration de fonctionnalités. Les outils valident le `nsconfig` fichier s'il contient des commandes ou des paramètres dans une commande qui a été supprimée dans la version NetScaler 13.1. Si le résultat de la validation indique l'utilisation de commandes supprimées ou non valides, avant de mettre à niveau votre appliance, vous devez d'abord modifier la configuration en fonction de l'alternative recommandée par Citrix.

L'outil valide également l'utilisation des expressions de stratégie classiques utilisées dans la configuration des fonctionnalités qui ne prend pas en charge les stratégies classiques. Vous pouvez modifier manuellement ou utiliser l'outil `nspepi`.

L'outil valide l'utilisation suivante :

1. Expressions de stratégie classiques dans les fonctionnalités de commutation de contenu, de redirection de cache, d'AppFW, de SSL et de CMP.
2. Fonction de filtrage (également connue sous le nom de filtrage de contenu) : actions, stratégies et liaison
3. SPDY dans le profil HTTP, la connexion sûre (SC), la mise en file d'attente prioritaire (PQ), le déni de service HTTP (DoS) et les fonctionnalités d'injection HTML.

4. Expressions classiques dans les règles de persistance de l'équilibrage de charge.
5. Paramètres « Pattern » et « BypassSafetyCheck » dans les actions de réécriture.
6. Entité de configuration « patclass ».
7. « HTTP.REQ.BODY » sans argument dans les expressions avancées.
8. Préfixes Q et S dans les expressions avancées.
9. Paramètre « PolicyType » pour le paramètre cmp.

Exécution de l'outil de pré-revalidation dans UNIX Shell

À l'invite de commande, tapez :

```
check_invalid_config <config_file>
<!--NeedCopy-->
```

Exemple :

```
root@ns## check_invalid_config/nsconfig/ns.conf
```

Où, le fichier de configuration est le fichier de configuration NetScaler. Le fichier doit être issu d'une configuration enregistrée telle que `ns.conf`.

Exemple de sortie avec erreurs de validation

Voici un exemple de sortie du fichier de configuration contenant des erreurs dans la version 13.1 de NetScaler :

```
add cmp policy cmp_pol -rule ns_true -resAction GZIP
add cs policy cs_pol_2 -rule ns_true
add cs policy cs_pol_3 -domain www.abc.com
add cs policy cs_pol_4 -url "/abc"
add rewrite action act_1 replace_all "http.req.body(1000)" http.req.url
    -pattern abcd
add rewrite action act_123 replace_all http.req.url ""aaaa"" -pattern
   abcd
add responder action ract respondwith "Q.URL + Q.HEADER("abcd")"
add appfw policy aff_pol_1 "http.req.body.length.gt(10)" APPFW_BYPASS
add appfw policy aff_pol ns_true APPFW_BYPASS

<!--NeedCopy-->
```

Une fois ces erreurs détectées, vous pouvez utiliser l'outil de `nspepi` mise à niveau pour convertir votre configuration ou la convertir manuellement. Pour plus d'informations, consultez la rubrique de l'outil nspepi .

> **Remarque :**
>
> Vous pouvez exécuter l'outil `nspepi` uniquement sur les versions 12.1, 13.0 et ultérieures de NetScaler.

Exemple de sortie sans erreur de validation

Voici un exemple de sortie du fichier de configuration sans configuration supprimée ou non valide :

```
root@ns# check_invalid_config /var/tmp/new_ns.conf
No issue detected with the configuration.
root@ns#
<!--NeedCopy-->
```

FAQ sur la dépréciation des stratégies classiques

May 5, 2023

- **Quelles politiques classiques sont devenues obsolètes à partir de la version 12.0 de NetScaler ?**

  Toutes les fonctionnalités mentionnées dans le tableau des politiques obsolètes sont obsolètes à partir de la version 12.0 build 56.20 de NetScaler. Citrix vous recommande de consulter les tableaux suivants (au format PDF) pour obtenir des détails sur les fonctionnalités et les stratégies obsolètes.

  - Tableau 1 pour les politiques dépréciées et leur alternative.
  - Tableau 2 pour les fonctionnalités obsolètes de NetScaler et son alternative avec les détails de configuration.

- **Comment puis-je convertir les fonctionnalités et fonctionnalités basées sur des stratégies classiques en stratégie avancée ?**

  Vous pouvez utiliser l' `nspepi` outil propriétaire NetScaler pour convertir des commandes, des expressions et des configurations. `nspepi` L'outil permet de convertir toutes les expressions classiques de la configuration NetScaler en expressions de politique avancées. Pour plus d'informations sur `nspepi` cet outil, voir Conversion d'expressions de stratégie à l'aide de l'outil NSPEPI.

- **À partir de quelle version les fonctionnalités et fonctionnalités basées sur des stratégies classiques sont-elles obsolètes ?**

  NetScaler 12.0 build 56.20 et versions ultérieures.

- **À partir de quelle version les fonctionnalités et fonctionnalités classiques obsolètes basées sur des politiques ont-elles été supprimées de l'appliance NetScaler ?**

  NetScaler version 13.1 et versions ultérieures. Pour plus d'informations, consultez la section Tableau des stratégies dépréciées .

- **Quelles sont les étapes à suivre lorsque je mets à niveau mon appliance vers une version qui ne prend pas en charge les fonctionnalités classiques basées sur des stratégies ?**

  Citrix recommande d'utiliser des politiques avancées avant de mettre à niveau votre appliance vers des versions ultérieures à la version 13.0 de NetScaler. Pour plus d'informations, voir Stratégies avancées.

- **Pendant combien de temps les fonctionnalités obsolètes seront-elles prises en charge sur une appliance NetScaler ?**

  Citrix ne prendra pas en charge la politique classique et son utilisation dans les versions ultérieures à la version 13.0 de NetScaler.

  La stratégie et les expressions classiques sont déconseillées (leur utilisation est déconseillée et NON supprimée) à partir de 12.0 build 56.20. La stratégie et les expressions continuent de fonctionner partout de la même manière qu'elles fonctionnaient auparavant dans toutes les versions de la version 13.0. Toutefois, à partir de la version 13.1 de NetScaler, certaines fonctionnalités et fonctionnalités classiques basées sur des politiques ont été supprimées.

- **Dois-je redémarrer mon appliance après avoir converti le fichier de configuration ?**

  Oui, vous devez redémarrer l'instance NetScaler une fois la conversion du `ns.config` fichier réussie.

Avant de continuer

May 5, 2023

Avant de configurer des expressions et des politiques, assurez-vous de bien comprendre la fonctionnalité NetScaler pertinente et la structure de vos données, comme suit :

- Lisez la documentation sur la fonctionnalité concernée.
- Examinez le flux de données pour connaître le type de données que vous souhaitez configurer.

Vous souhaiterez peut-être exécuter un suivi sur le type de trafic ou de contenu que vous souhaitez configurer. Cela vous donnera une idée des paramètres et des valeurs, ainsi que des opérations sur ces paramètres et valeurs, que vous devez spécifier dans une expression.

Remarque : NetScaler prend en charge la politique avancée au sein d'une fonctionnalité. Les deux types ne peuvent pas figurer dans la même fonction. Au cours des dernières versions, certaines fonc-

tionnalités de NetScaler ont migré de l'utilisation de politiques et d'expressions vers des politiques et des expressions avancées. Si une fonctionnalité qui vous intéresse est passée au format de stratégie Avancé, il se peut que vous deviez migrer manuellement les informations plus anciennes. Vous trouverez ci-dessous des instructions pour décider si vous devez migrer vos stratégies :

- Si vous avez configuré des stratégies classiques dans une version de la fonctionnalité de mise en cache intégrée avant la version 9.0, puis que vous effectuez une mise à niveau vers la version 9.0 ou ultérieure, cela n'a aucun impact. Toutes les stratégies héritées sont migrées vers le format de stratégie avancé.
- Pour les autres fonctionnalités, vous devez migrer manuellement les stratégies et expressions classiques vers la syntaxe Avancée si la fonctionnalité a migré vers la stratégie Avancée.

Configuration d'une infrastructure de politiques avancée

May 5, 2023

Vous pouvez créer des politiques avancées pour diverses fonctionnalités de NetScaler, notamment le DNS, la réécriture, le répondeur et la mise en cache intégrée, ainsi que la fonction d'accès sans client dans NetScaler Gateway. Les politiques contrôlent le comportement de ces fonctionnalités.

Lorsque vous créez une politique, vous lui attribuez un nom, une règle (une expression), des attributs spécifiques à une fonctionnalité et une action à effectuer lorsque les données correspondent à la politique. Après avoir créé la politique, vous déterminez quand elle est invoquée en la liant globalement ou au traitement du temps de demande ou du temps de réponse pour un serveur virtuel.

Les politiques qui partagent le même point de liaison sont appelées *banque de stratégies*. Par exemple, toutes les politiques liées à un serveur virtuel constituent la banque de politiques du serveur virtuel. Lorsque vous liez la politique, vous lui attribuez un niveau de priorité afin de spécifier quand elle est invoquée par rapport aux autres politiques de la banque. Outre l'attribution d'un niveau de priorité, vous pouvez configurer un ordre d'évaluation arbitraire pour les politiques d'une banque en spécifiant des expressions Goto.

Outre les banques de politiques associées à un point de liaison intégré ou à un serveur virtuel, vous pouvez configurer des *étiquettes de stratégies*. Une étiquette de stratégie est une banque de stratégies identifiée par un nom arbitraire. Vous invoquez une étiquette de stratégie, ainsi que les politiques qu'elle contient, à partir d'une banque de stratégies globale ou spécifique à un serveur virtuel. Une étiquette de stratégie ou une banque de stratégies de serveur virtuel peuvent être appelées à partir de plusieurs banques de politiques.

Pour certaines fonctionnalités, vous pouvez utiliser le gestionnaire de stratégies pour configurer et lier des stratégies.

Règles relatives aux noms utilisés dans les identifiants utilisés dans les politiques

May 5, 2023

Les noms des identifiants contenus dans l'expression nommée, la légende HTTP, le jeu de modèles et les fonctionnalités de limitation de débit doivent commencer par un alphabet ASCII ou un trait de soulignement (_). Les autres caractères peuvent être des caractères alphanumériques ASCII ou des traits de soulignement (_).

Les noms de ces identifiants ne doivent pas commencer par les mots réservés suivants :

- Les mots ALT, TRUE ou FALSE ou l'identifiant à un caractère Q ou S.
- L'indicateur de syntaxe spéciale RE (pour les expressions régulières) ou XP (pour les expressions XPath).
- Les préfixes d'expression, qui sont actuellement les suivants :
  - CLIENT
  - ÉTENDRE
  - HTTP
  - SERVEUR
  - SYS
  - CIBLE
  - TEXTE
  - URL
  - MYSQL
  - MSSQL

En outre, les noms de ces identifiants ne peuvent pas être identiques à ceux des constantes d'énumération utilisées dans l'infrastructure des politiques. Par exemple, le nom d'un identifiant ne peut pas être IGNORECASE, YEAR ou LATIN2_CZECH_CS (un jeu de caractères MySQL).

Remarque : L'appliance NetScaler effectue une comparaison des identifiants sans distinction majuscules/minuscules avec ces mots et ces constantes d'énumération. Par exemple, les noms des identificateurs ne peuvent pas commencer par TRUE, True ou True.

Créer ou modifier une stratégie

June 2, 2023

Toutes les stratégies comportent des éléments communs. La création d'une stratégie consiste, au minimum, à nommer la stratégie et à configurer une règle. Les outils de configuration de stratégie pour les différentes entités présentent des zones de chevauchement, mais aussi des différences. Pour plus d'informations sur la configuration d'une stratégie pour une fonction particulière, y compris l'association d'une action à la stratégie, reportez-vous à la documentation de la fonction.

Pour créer une stratégie, commencez par déterminer l'objet de la stratégie. Par exemple, vous pouvez définir une stratégie qui identifie les requêtes HTTP pour les fichiers image ou les demandes client qui contiennent un certificat SSL. En plus de connaître le type d'informations avec lequel vous souhaitez que la stratégie fonctionne, vous devez connaître le format des données analysées par la stratégie.

Ensuite, déterminez si la stratégie est applicable globalement ou si elle concerne un serveur virtuel particulier. Tenez également compte de l'effet que l'ordre dans lequel vos stratégies sont évaluées (qui sera déterminé par la façon dont vous les liez) aura sur la stratégie que vous êtes sur le point de configurer.

Créer une stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une stratégie et vérifier la configuration :

```
- add responder|dns|cs|rewrite|cache policy <policyName> -rule <
    expression> [<feature-specific information>]

- show rewrite policy <name>
<!--NeedCopy-->
```

Exemple 1 :

```
add rewrite policy "pol_remove-ae" true "act_remove-ae"
Done
> show rewrite policy pol_remove-ae
            Name: pol_remove-ae
            Rule: true
            RewriteAction: act_remove-ae
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
            Bound to: GLOBAL RES_OVERRIDE
            Priority: 90
            GotoPriorityExpression: END
Done
<!--NeedCopy-->
```


Exemple 2 :

```
add cache policy BranchReportsCachePolicy -rule q{
 http.req.url.query.value("actionoverride").contains("branchReport s")
    }
  -action cache
Done
show cache policy BranchReportsCachePolicy
            Name: BranchReportsCachePolicy
            Rule: http.req.url.query.value("actionoverride").contains("
               branchReports")
            CacheAction: CACHE
            Stored in group: DEFAULT
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
Done
<!--NeedCopy-->
```

Remarque : Sur la ligne de commande, les guillemets dans une règle de stratégie (l'expression) doivent être échappés ou délimités avec le délimiteur q. Pour plus d'informations, voir Configurer les expressions de stratégie avancées : Pour commencer.

Créer ou modifier une stratégie à l'aide de l'interface graphique

1. Dans le volet de navigation, développez le nom de la fonctionnalité pour laquelle vous souhaitez configurer une stratégie, puis cliquez sur **Stratégies**. Par exemple, vous pouvez sélectionner **Commutation de contenu, Mise en cache intégrée, DNS, Réécriture ou Répondeur**.
2. Dans le volet d'informations, cliquez sur **Ajouter**ou sélectionnez une stratégie existante et cliquez sur **Ouvrir**. Une boîte de dialogue de configuration de stratégie s'affiche.
3. Spécifiez des valeurs pour les paramètres suivants. (Un astérisque indique un paramètre obligatoire. Pour un terme entre parenthèses, voir le paramètre correspondant dans "Paramètres pour la création ou la modification d'une stratégie.")
4. Cliquez sur **Créer**, puis sur **Fermer**.
5. Cliquez sur **Enregistrer**. Une stratégie est ajoutée.
   Remarque : Après avoir créé une stratégie, vous pouvez afficher les détails de la stratégie en cliquant sur l'entrée de stratégie dans le volet de configuration. Les détails qui sont mis en surbrillance et soulignés sont des liens vers l'entité correspondante (par exemple, une expression nommée).

Exemples de configuration de stratégie

August 20, 2021

Ces exemples montrent comment les stratégies et les actions associées sont entrées dans l'interface de ligne de commande. Dans l'utilitaire de configuration, les expressions s'affichent dans la fenêtre Expression de la boîte de dialogue Configuration de l'entité pour la fonction de mise en cache ou de réécriture intégrée.

Voici un exemple de création d'une stratégie de mise en cache. Notez que les actions pour les stratégies de mise en cache sont intégrées, vous n'avez donc pas besoin de les configurer séparément de la stratégie.

```
1   add cache policy BranchReportsCachePolicy -rule q{
2  http.req.url.query.value("actionoverride").contains("branchReports") }
3   -action cache
4 <!--NeedCopy-->
```

Voici un exemple de stratégie et d'action de réécriture :

```
1  add rewrite action myAction1 INSERT_HTTP_HEADER "myHeader" "
      valueForMyHeader"
2  add rewrite policy myPolicy1 "http.req.url.contains("myURLstring")"
      myAction1
3 <!--NeedCopy-->
```

Remarque : Sur la ligne de commande, les guillemets dans une règle de stratégie (l'expression) doivent être échappés ou délimités avec le délimiteur q. Pour plus d'informations, voir Configurer les expressions de stratégie avancées : Pour commencer.

Configurer et lier des stratégies avec le gestionnaire de stratégies

May 5, 2023

> **Avertissement :**
>
> Les expressions de politique classiques ne sont plus prises en charge à partir de NetScaler 12.0 build 56.20. Comme alternative, Citrix vous recommande d'utiliser des politiques avancées. Pour plus d'informations, voir Stratégies avancées.

Certaines applications fournissent un gestionnaire de politiques spécialisé dans l'utilitaire de configuration NetScaler afin de simplifier la configuration des banques de règles. Il vous permet également de rechercher et de supprimer des stratégies et des actions qui ne sont pas utilisées.

Le Gestionnaire de stratégies est actuellement disponible pour les fonctionnalités de réécriture, de mise en cache intégrée, de répondeur et de compression.

Voici les équivalents clavier des procédures décrites dans cette section :

- Pour modifier une cellule dans le Gestionnaire de stratégies, vous pouvez accéder à la cellule et cliquer sur F2 ou appuyer sur la barre d'espace du clavier.
- Pour sélectionner une entrée dans un menu déroulant, vous pouvez accéder à l'entrée avec la touche de tabulation, appuyer sur la barre d'espace pour afficher le menu déroulant, utiliser les touches FLÉCHÉES HAUT et BAS pour accéder à l'entrée souhaitée, puis appuyer à nouveau sur la barre d'espace pour sélectionner l'entrée.
- Pour annuler une sélection dans un menu déroulant, appuyez sur la touche Echap.
- Pour insérer une stratégie, appuyez sur la touche de tabulation jusqu'à la ligne au-dessus du point d'insertion et appuyez sur CtrL+Insérer, ou cliquez sur Insérer une stratégie.
- Pour supprimer une stratégie, appuyez sur la touche de tabulation jusqu'à la ligne qui contient la stratégie, puis appuyez sur Supprimer.

Remarque : Notez que lorsque vous supprimez la politique, NetScaler recherche les valeurs Goto Expression des autres politiques de la banque. Si l'une de ces valeurs Goto Expression correspond au niveau de priorité de la stratégie supprimée, elle est supprimée.

Configurez les liaisons de stratégie à l'aide du gestionnaire de stratégies

1. Dans le volet de navigation, cliquez sur la fonctionnalité pour laquelle vous souhaitez configurer des stratégies. Les choix sont Responder, Integrated Caching, Rewrite ou Compression.
2. Dans le volet d'informations, cliquez sur **Gestionnaire de stratégies**.
3. À tout moment avant de terminer la configuration des liaisons de stratégie, si vous souhaitez configurer les liaisons pour les stratégies qui utilisent la stratégie avancée, cliquez sur le bouton Basculer vers la stratégie avancée.
4. Pour les fonctionnalités autres que Responder, pour spécifier le point de liaison, cliquez sur Demande ou Réponse, puis sur l'un des points de liaison de temps de demande ou de réponse. Les options sont Override Global, LB Virtual Server, CS Virtual Server, Default Global ou Policy Label. Si vous configurez le répondeur, les types de flux Demande et Réponse ne sont pas disponibles.
5. Pour lier une stratégie à ce point de liaison, cliquez sur Insérer une stratégie, puis sélectionnez une stratégie précédemment configurée, une étiquette NOPOLICY ou l'option Nouvelle stratégie. Selon l'option que vous sélectionnez, vous avez les choix suivants :
    - **Nouvelle stratégie :** créez la stratégie comme décrit dans « Créer ou modifier une stratégie », puis configurez le niveau de priorité, l'expression GoTo et l'appel de stratégie comme décrit dans le tableau, « Format de chaque entrée d'une banque de stratégies. «

- **Stratégie existante**, **NOPOLICY**ou `NOPOLICY\<feature name\>` : Configurez le niveau de priorité, l'expression GoTo et l'appel de stratégie comme décrit dans le tableau, « Format de chaque entrée d'une banque de stratégies. « Les options `NOPOLICY\<feature name \>` ou les options **NOPOLICY** ne sont disponibles que pour les stratégies qui utilisent des stratégies avancées.

6. Répétez les étapes précédentes pour ajouter des entrées à cette banque de stratégies.
7. Pour modifier le niveau de priorité d'une entrée, vous pouvez effectuer l'une des opérations suivantes :

   - Double-cliquez sur le champ Priorité d'une entrée et modifiez la valeur.
   - Cliquez sur une stratégie et faites-la glisser vers une autre ligne du tableau.
   - Cliquez sur Régénérer les priorités.

   Dans les trois cas, les niveaux de priorité de toutes les autres politiques sont modifiés au besoin pour tenir compte de la nouvelle valeur. Les expressions Goto avec des valeurs entières sont également mises à jour automatiquement. Par exemple, si vous modifiez une valeur de priorité de 10 à 100, toutes les stratégies avec une valeur Goto Expression de 10 sont mises à jour avec la valeur 100.
8. Pour modifier l'appel de stratégie, d'action ou de banque de stratégies pour une ligne du tableau, cliquez sur la flèche vers le bas à droite de l'entrée et effectuez l'une des opérations suivantes :

   - Pour modifier la stratégie, sélectionnez un autre nom de stratégie ou sélectionnez Nouvelle stratégie et suivez les étapes de la section Créer ou modifier une stratégie.
   - Pour modifier l'expression Goto, sélectionnez Suivant, Fin, USE_INVOCATION_RESULT ou sélectionnez plus et entrez une expression dont le résultat renvoie le niveau de priorité d'une autre entrée de cette banque de stratégies.
   - Pour modifier un appel, sélectionnez une banque de stratégies existante ou cliquez sur Nouvelle étiquette de stratégie et suivez les étapes de la section Lier une stratégie à une étiquette de stratégie.
9. Pour dissocier une stratégie ou une invocation d'étiquette de stratégie de cette banque, cliquez sur n'importe quel champ de la ligne contenant l'étiquette de stratégie ou de stratégie, puis cliquez sur Annulation de la stratégie.
10. Lorsque vous avez terminé, cliquez sur Appliquer les modifications. Un message dans la barre d'état indique que la stratégie est liée avec succès.

Supprimer les stratégies inutilisées à l'aide du gestionnaire de stratégies

1. Dans le volet de navigation, cliquez sur la fonctionnalité pour laquelle vous souhaitez configurer la banque de stratégies. Les choix sont Responder, Integrated Caching ou Rewrite.

2. Dans le volet d'informations, cliquez sur Gestionnaire <Feature Name> de stratégies.
3. Dans la boîte de dialogue **Nom de la fonctionnalité** > **Gestionnaire des politiques**ou, cliquez sur **Configuration du nettoyage**.
4. Dans la boîte de dialogue **Configuration du nettoyage**, sélectionnez les éléments que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
5. Dans la boîte de dialogue Supprimer, cliquez sur **Oui**.
6. Cliquez sur **Fermer**. Un message dans la barre d'état indique que la stratégie a été supprimée avec succès.

Dissocier une stratégie

August 20, 2021

Si vous souhaitez réaffecter une stratégie ou la supprimer, vous devez d'abord supprimer sa liaison.

Dissocier globalement une stratégie avancée de mise en cache, de réécriture ou de compression intégrée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier globalement une stratégie avancée de mise en cache, de réécriture ou de compression intégrée et vérifier la configuration :

```
1 -  unbind cache|rewrite|cmp global <policyName> [-type req_override|
     req_default|res_override|res_default] [-priority <positiveInteger>]
2
3 -  show cache|rewrite|cmp global
4 <!--NeedCopy-->
```

Exemple :

```
1  > unbind cache global_nonPostReq
2  Done
3  > show cache global
4      1)      Global bindpoint: REQ_DEFAULT
5              Number of bound policies: 1
6
7      2)      Global bindpoint: RES_DEFAULT
8              Number of bound policies: 1
9
10 Done
11 <!--NeedCopy-->
```

La priorité n'est requise que pour la stratégie « factice » nommée NOPOLICY.

Dissocier globalement une stratégie de répondeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier globalement une stratégie de répondeur et vérifier la configuration :

```
1 - unbind responder global <policyName> [-type override|default] [-
    priority <positiveInteger>]
2
3 - show responder global
4 <!--NeedCopy-->
```

Exemple :

```
1 > unbind responder global pol404Error
2 Done
3 > show responder global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6 Done
7 <!--NeedCopy-->
```

La priorité n'est requise que pour la stratégie « factice » nommée NOPOLICY.

Dissocier globalement une stratégie DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier globalement une stratégie DNS et vérifier la configuration :

```
1 - unbind responder global <policyName>
2
3 - unbind responder global
4 <!--NeedCopy-->
```

Exemple :

```
1 unbind dns global dfgdfg
2 Done
3 show dns global
4     Policy name : dfgdfggfhg
5             Priority : 100
6             Goto expression : END
7 Done
8 <!--NeedCopy-->
```


Dissocier une stratégie avancée d'un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier une stratégie avancée d'un serveur virtuel et vérifier la configuration :

```
1 -  unbind cs vserver <name> -policyName <policyName> [-priority <
     positiveInteger>] [-type REQUEST|RESPONSE]
2
3 -  show lb vserver <name>
4 <!--NeedCopy-->
```

Exemple :

```
1  unbind cs vserver vs-cont-switch  -policyName pol1
2  Done
3  > show cs vserver vs-cont-switch
4              vs-cont-switch (10.102.29.10:80) - HTTP Type: CONTENT
5              State: UP
6              Last state change was at Wed Aug 19 08:56:55 2009 (+18 ms)
7              Time since last state change: 0 days, 02:47:55.750
8              Client Idle Timeout: 180 sec
9              Down state flush: ENABLED
10             Disable Primary Vserver On Down : DISABLED
11             Port Rewrite : DISABLED
12             State Update: DISABLED
13             Default:        Content Precedence: RULE
14             Vserver IP and Port insertion: OFF
15             Case Sensitivity: ON
16             Push: DISABLED  Push VServer:
17             Push Label Rule: none
18 Done
19 <!--NeedCopy-->
```

La priorité n'est requise que pour la stratégie « factice » nommée NOPOLICY.

Dissocier globalement une stratégie avancée de mise en cache, répondeur, réécriture ou compression intégrée à l'aide de l'interface graphique

1. Dans le volet de navigation, cliquez sur l'entité avec la stratégie que vous souhaitez dissocier (par exemple, mise en cache intégrée).
2. Dans le volet d'informations, cliquez sur Gestionnaire de stratégies <Feature Name>.
3. Dans la boîte de dialogue **Gestionnaire de stratégies**, sélectionnez le point de liaison avec la stratégie à dissocier, par exemple Advanced Global.

4. Cliquez sur le nom de la stratégie que vous souhaitez dissocier, puis cliquez sur Dissocier la stratégie.
5. Cliquez sur **Appliquer les modifications**.
6. Cliquez sur **Fermer**. Un message dans la barre d'état indique que la stratégie n'est pas liée avec succès.

Dissocier globalement une stratégie DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **DNS** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales**.
3. Dans la boîte de dialogue **Liaisons globales**, sélectionnez stratégie et cliquez sur **dissocier stratégie**.
4. Cliquez sur **OK**. Un message dans la barre d'état indique que la stratégie est dissociée avec succès.

Dissocier une stratégie avancée d'un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic,** développez Équilibrage de charge ou Changement de contenu, puis cliquez sur **Serveurs virtuels**.
2. Dans le volet d'informations, double-cliquez sur le serveur virtuel à partir duquel vous souhaitez dissocier la stratégie.
3. Sous l'onglet **Stratégies**, dans la colonne **Actif**, désactivez la case à cocher en regard de la stratégie à dissocier.
4. Cliquez sur **OK**. Un message dans la barre d'état indique que la stratégie est dissociée avec succès.

Création d'étiquettes de politique

May 5, 2023

Outre les points de liaison intégrés qui vous permettent de configurer des banques de stratégies, vous pouvez également configurer des étiquettes de stratégies définies par l'utilisateur et y associer des politiques.

Dans une étiquette de stratégie, vous liez des politiques et vous spécifiez l'ordre d'évaluation de chaque politique par rapport aux autres dans la banque de stratégies associée à l'étiquette de stratégie. NetScaler vous permet également de définir un ordre d'évaluation arbitraire comme suit :

- Vous pouvez utiliser des expressions « goto » pour pointer vers la prochaine entrée de la banque à évaluer après l'entrée en cours.
- Vous pouvez utiliser une entrée dans une banque de politiques pour appeler une autre banque.

Chaque fonctionnalité détermine le type de politique que vous pouvez lier à une étiquette de stratégie, le type de serveur virtuel d'équilibrage de charge auquel vous pouvez lier l'étiquette et le type de serveur virtuel de commutation de contenu à partir duquel l'étiquette peut être invoquée. Par exemple, une étiquette de politique TCP ne peut être liée qu'à un serveur virtuel d'équilibrage de charge TCP. Vous ne pouvez pas lier des politiques HTTP à une étiquette de politique de ce type. Et vous ne pouvez invoquer une étiquette de politique TCP qu'à partir d'un serveur virtuel de commutation de contenu TCP.

Après avoir configuré un nouveau libellé de politique, vous pouvez l'invoquer auprès d'une ou de plusieurs banques pour les points de liaison intégrés.

Créez une étiquette de politique de mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une étiquette de politique de mise en cache et vérifier la configuration :

```
1 -  add cache policylabel <labelName> -evaluates req|res
2
3 -  show cache policylabel<labelName>
4 <!--NeedCopy-->
```

Exemple :

```
1 > add cache policylabel lbl-cache-pol -evaluates req
2 Done
3
4 > show cache policylabel lbl-cache-pol
5             Label Name: lbl-cache-pol
6             Evaluates: REQ
7             Number of bound policies: 0
8             Number of times invoked: 0
9 Done
10 <!--NeedCopy-->
```


Créez une étiquette de politique de changement de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une étiquette de politique de commutation de contenu et vérifier la configuration :

```
- add cs policylabel <labelName> http|tcp|rtsp|ssl

- show cs policylabel <labelName>
<!--NeedCopy-->
```

Exemple :

```
> add cs policylabel lbl-cs-pol http
Done
> show cs policylabel lbl-cs-pol
            Label Name: lbl-cs-pol
            Label Type: HTTP
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Créez une étiquette de politique de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une étiquette de politique de réécriture et vérifier la configuration :

```
- add rewrite policylabel <labelName> http_req|http_res|url|text|
   clientless_vpn_req|clientless_vpn_res

- show rewrite policylabel <labelName>
<!--NeedCopy-->
```

Exemple :

```
> add rewrite policylabel lbl-rewrt-pol http_req
Done

> show rewrite policylabel lbl-rewrt-pol
            Label Name: lbl-rewrt-pol
            Transform Name: http_req
            Number of bound policies: 0
```



```
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Créez une étiquette de politique pour les répondeurs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une étiquette de politique du répondeur et vérifier la configuration :

```
-  add responder policylabel <labelName>

-  show responder policylabel <labelName>
<!--NeedCopy-->
```

Exemple :

```
> add responder policylabel lbl-respndr-pol
Done

> show responder policylabel lbl-respndr-pol
            Label Name: lbl-respndr-pol
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Remarque : invoquez cette étiquette de stratégie à partir d'une banque de stratégies. Pour plus d'informations, consultez la section « Lier une politique à un libellé de politique ».

Création d'une étiquette de politique à l'aide de l'interface graphique

1. Dans le volet de navigation, développez la fonctionnalité pour laquelle vous souhaitez créer une étiquette de stratégie, puis cliquez sur **Étiquettes de stratégie**. Vous avez le choix entre la mise en cache intégrée, la réécriture, la commutation de contenu ou le répondeur.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la zone Nom, entrez un nom unique pour cette étiquette de politique.
4. Entrez des informations spécifiques à la fonctionnalité pour l'étiquette de politique. Par exemple, pour la mise en cache intégrée, dans le menu déroulant Évaluations, vous devez sélectionner REQ si vous souhaitez que cette étiquette de politique contienne des politiques de temps de demande, ou sélectionnez RES si vous souhaitez que cette étiquette de stratégie contienne

des politiques de temps de réponse. Pour Réécrire, vous devez sélectionner un nom de transformation.

5. Cliquez sur **Create**.
6. Configurez l'une des banques de stratégies intégrées pour invoquer cette étiquette de stratégie. Pour plus d'informations, consultez la section « Lier une politique à un libellé de politique ». Un message dans la barre d'état indique que l'étiquette de politique a été créée avec succès.

Lier une politique à une étiquette de stratégie

Comme pour les banques de stratégies liées aux points de liaison intégrés, chaque entrée d'une étiquette de stratégie est une politique liée à l'étiquette de stratégie. Comme pour les politiques liées globalement ou à un vserver, chaque politique liée à l'étiquette de politique peut également invoquer une banque de politiques ou une étiquette de stratégie qui est évaluée après le traitement de l'entrée en cours. Le tableau suivant récapitule les entrées d'une étiquette de politique.

- **Nom**. Le nom d'une politique ou, pour appeler une autre banque de stratégies sans évaluer une politique, le nom de politique « fictif » NOPOLICY.

  Vous pouvez spécifier NOPOLICY plusieurs fois dans une banque de stratégies, mais vous ne pouvez spécifier une politique nommée qu'une seule fois.

- **Priorité**. Un entier. Ce paramètre peut fonctionner avec l'expression Goto.

- **Accédez à Expression**. Détermine la prochaine politique à évaluer dans cette banque. Vous pouvez fournir l'une des valeurs suivantes :

  - **SUIVANT**. Accédez à la politique dont la priorité est immédiatement supérieure.
  - **FIN**. Arrêtez l'évaluation.
  - **USE_INVOCATION_RESULT**. Applicable si cette entrée fait appel à une autre banque de politiques. Si le dernier Goto de la banque invoquée a la valeur END, l'évaluation s'arrête. Si le Goto final est autre que END, la banque de règles actuelle exécute un NEXT.
  - **Nombre positif :** le numéro de priorité de la prochaine politique à évaluer.
  - **Expression numérique**. Expression qui produit le numéro de priorité de la prochaine politique à évaluer.

  Le Goto ne peut aller de l'avant que dans une banque de polices.

  Si vous omettez l'expression Goto, cela revient à spécifier END.

- **Type d'invocation**. Désigne un type de banque de politiques. La valeur peut être l'une des suivantes :

  - **Demandez Vserver**. Invoque les politiques de temps de demande associées à un serveur virtuel.
  - **Serveur de réponse**. Invoque les politiques de temps de réponse associées à un serveur virtuel.

  - **Libellé de politique**. Appelle une autre banque de stratégies, telle qu'identifiée par l'étiquette de politiques de la banque.

- **Nom de l'invocation**. Nom d'un serveur virtuel ou d'une étiquette de stratégie, en fonction de la valeur que vous avez spécifiée pour le type d'appel.

Configuration d'une étiquette de stratégie ou d'une banque de règles de serveur virtuel

May 5, 2023

Après avoir créé des politiques et créé des banques de stratégies en liant les politiques, vous pouvez effectuer une configuration supplémentaire des politiques au sein d'une étiquette ou d'une banque de stratégies. Par exemple, avant de configurer l'invocation d'une banque de règles externe, vous pouvez attendre d'avoir configuré cette banque de stratégies.

Cette rubrique comprend les sections suivantes :

- Configuration d'une étiquette de politique
- Configuration d'une banque de politiques pour un serveur virtuel

Configuration d'une étiquette de politique

Une étiquette de stratégie se compose d'un ensemble de politiques et d'invocations d'autres étiquettes de politiques et de banques de stratégies spécifiques à un serveur virtuel. Un paramètre Invoke vous permet d'invoquer une étiquette de stratégie ou une banque de stratégies spécifique à un serveur virtuel à partir de n'importe quelle autre banque de stratégies. Une entrée NoPolicy spéciale vous permet d'appeler une banque externe sans traiter d'expression (une règle). L'entrée NoPolicy est une politique « fictive » qui ne contient pas de règle.

Pour configurer les étiquettes de politique à partir de la ligne de commande NetScaler, notez les élaborations suivantes de la syntaxe de commande :

- gotoPriorityExpression est configuré comme décrit dans le tableau 2. Format de chaque entrée dans une banque de politiques de la section « Entrées dans une banque de politiques » dans les stratégies de liaison utilisant une stratégie avancée.
- L'argument type est obligatoire. Cela n'est pas le cas d'une politique contraignante conventionnelle, où cet argument est facultatif.
- Vous pouvez invoquer la banque de politiques liées à un serveur virtuel en utilisant la même méthode que celle que vous utilisez pour appeler une étiquette de stratégie.

Configurer une étiquette de politique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une étiquette de politique et vérifier la configuration :

```
- bind cache|rewrite|responder policylabel <policylabelName> -
   policyName <policyName> -priority <priority> [-
   gotoPriorityExpression <gotoprioritыExpression>] [-invoke reqvserver
   |resvserver|policylabel <policyLabelName>|<vserverName>]

- show cache|rewrite|responder policylabel <policylabelName>
<!--NeedCopy-->
```

Exemple :

```
bind cache policylabel _reqBuiltinDefaults -policyName  _nonGetReq -
   priority 100
Done
show cache policylabel _reqBuiltinDefaults
            Label Name: _reqBuiltinDefaults
            Evaluates: REQ
            Number of bound policies: 3
            Number of times invoked: 0
    1)      Policy Name: _nonGetReq
            Priority: 100
            GotoPriorityExpression: END
    2)      Policy Name: _advancedConditionalReq
            Priority: 200
            GotoPriorityExpression: END

    3)      Policy Name: _personalizedReq
            Priority: 300
            GotoPriorityExpression: END
Done
<!--NeedCopy-->
```

Invoquer une étiquette de politique à partir d'une banque de règles de réécriture avec une entrée NOPOLICY à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une étiquette de politique à partir d'une banque de règles de réécriture avec une entrée NOPOLICY et vérifier la configuration :

```
- bind rewrite global <policyName> <priority> <gotoPriorityExpression>
   -type REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke
   reqvserver|resvserver|policylabel <policyLabelName>|<vserverName>
```



```
2
3 -  show rewrite global
4 <!--NeedCopy-->
```

Exemple :

```
1 > bind rewrite global NOPOLICY 100 -type REQ_DEFAULT -invoke
     policylabel lbl-rewrt-pol
2 Done
3 > show rewrite global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6
7     2)      Global bindpoint: REQ_OVERRIDE
8             Number of bound policies: 1
9 Done
10 <!--NeedCopy-->
```

Invoquer une étiquette de politique à partir d'une banque de politiques de mise en cache intégrée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une étiquette de politique à partir d'une banque de règles de mise en cache intégrée et vérifier la configuration :

```
1 -  bind cache global NOPOLICY -priority <priority> -
     gotoPriorityExpression <gotopriorityExpression> -type REQ_OVERRIDE|
     REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke reqvserver|resvserver|
     policylabel <policyLabelName>|<vserverName>
2
3 -  show cache global
4 <!--NeedCopy-->
```

Exemple :

```
1 bind cache global NOPOLICY -priority 100 -gotoPriorityExpression END -
     type REQ_DEFAULT -invoke policylabel lbl-cache-pol
2 Done
3 > show cache global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 2
6
7     2)      Global bindpoint: RES_DEFAULT
8             Number of bound policies: 1
9
```



```
Done
<!--NeedCopy-->
```

Invoquer une étiquette de politique à partir d'une banque de politiques Responder à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour appeler une étiquette de politique à partir d'une banque de règles Responder et vérifier la configuration :

```
- bind responder global NOPOLICY <priority> <gotoprioritыExpression> -
    type OVERRIDE|DEFAULT -invoke vserver|policylabel <policyLabelName
    >|<vserverName>

- show responder global
<!--NeedCopy-->
```

Exemple :

```
> bind responder global NOPOLICY 100 NEXT -type DEFAULT -invoke
    policylabel lbl-respndr-pol
Done
> show responder global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 2

Done
<!--NeedCopy-->
```

Configurer une étiquette de politique à l'aide de l'interface graphique

1. Dans le volet de navigation, développez la fonctionnalité pour laquelle vous souhaitez configurer une étiquette de stratégie, puis cliquez sur Étiquettes de stratégie. Vous avez le choix entre la mise en cache intégrée, la réécriture ou le répondeur.
2. Dans le volet d'informations, double-cliquez sur l'étiquette que vous souhaitez configurer.
3. Si vous ajoutez une nouvelle stratégie à cette étiquette de stratégie, cliquez sur Insérer une stratégie et, dans le champ Nom de la stratégie, sélectionnez Nouvelle stratégie. Pour plus d'informations sur l'ajout d'une stratégie, voir Créer ou modifier une stratégie. Notez que si vous appelez une banque de stratégies et que vous ne souhaitez pas qu'une règle soit évaluée avant l'invocation, cliquez sur Insérer une stratégie, puis dans le champ Nom de la stratégie, sélectionnez NOPOLICY.

4. Pour chaque entrée de cette étiquette de politique, configurez les éléments suivants :

   - **Nom de la politique :**

     Cela est déjà déterminé par le nom de la politique, la nouvelle politique ou l'entrée NOPOLICY que vous avez insérée dans cette banque.

   - **Priorité :**

     Valeur numérique qui détermine un ordre d'évaluation absolu au sein de la banque ou qui est utilisée conjointement avec une expression Goto.

   - **Expression :**

     La règle de politique. Les expressions de stratégie sont décrites en détail dans les chapitres suivants. Pour une introduction, reportez-vous à la section Configurer les expressions de stratégie avancées : Pour commencer.

   - **Action :**

     L'action à effectuer si cette politique est évaluée comme VRAI.

   - **Accédez à Expression :**

     Facultatif. Utilisé pour augmenter le niveau de priorité afin de déterminer la prochaine politique ou banque de politiques à évaluer. Pour plus d'informations sur les valeurs possibles d'une expression Goto, reportez-vous au tableau 2. Format de chaque entrée dans une banque de politiques de la section « Entrées dans une banque de politiques » dans les stratégies de liaison utilisant une stratégie avancée.

   - **Invoquer :**

     Facultatif. Invoque une autre banque de politiques.

5. Cliquez sur **OK**. Un message dans la barre d'état indique que l'étiquette de politique est correctement configurée.

Configuration d'une banque de politiques pour un serveur virtuel

Vous pouvez configurer une banque de politiques pour un serveur virtuel. La banque de stratégies peut contenir des politiques individuelles, et chaque entrée de la banque de stratégies peut éventuellement invoquer une étiquette de stratégies ou une banque de stratégies que vous avez configurée pour un autre serveur virtuel. Si vous invoquez un libellé ou une banque de stratégies, vous pouvez le faire sans déclencher d'expression (une règle) en sélectionnant une entrée « fictive » NOPOLICY au lieu d'un nom de politique.

Ajouter des politiques à une banque de règles de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter des politiques à une banque de stratégies de serveur virtuel et vérifier la configuration :

```
- bind lb|cs vserver <virtualServerName> <serviceType> [-policyName <
   policyName>] [-priority <positiveInteger>] [-gotoPriorityExpression
   <expression>] [-type REQUEST|RESPONSE]

- show lb|cs vserver <virtualServerName>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver vs-cont-sw TCP
Done
show lb vserver vs-cont-sw
            vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
            State: DOWN
            Last state change was at Wed Aug 19 10:04:02 2009 (+279 ms)
            Time since last state change: 0 days, 00:02:14.420
            Effective State: DOWN
            Client Idle Timeout: 9000 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Connection Failover: DISABLED
Done
<!--NeedCopy-->
```

Invoquer une étiquette de politique à partir d'une banque de règles de serveur virtuel avec une entrée NOPOLICY à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une étiquette de politique à partir d'une banque de règles de serveur virtuel avec une entrée NOPOLICY et vérifier la configuration :

```
- bind lb|cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
   NOPOLICY-CACHE|NOPOLICY-RESPONDER -priority <integer> -type REQUEST|
   RESPONSE -gotoPriorityExpression <gotopriorityExpression> -invoke
   reqVserver|resVserver|policyLabel <vserverName>|<labelName>
```



```
2
3 -  show lb vserver
4 <!--NeedCopy-->
```

Exemple :

```
1 > bind lb vserver vs-cont-sw -policyname NOPOLICY-REWRITE -priority 200
      -type REQUEST -gotoPriorityExpression NEXT -invoke policyLabel lbl-
    rewrt-pol
2 Done
3 <!--NeedCopy-->
```

Configuration d'une banque de règles de serveur virtuel à l'aide de l'interface graphique

1. **Dans le volet de navigation de gauche, ouvrez ** Gestion du trafic** > **Équilibrage de charge, Gestion du trafic** > **Commutation de contenu, Gestion du trafic** > **Déchargement SSL, Sécurité** > **AAA - Trafic applicatif**ou**0 NetScaler Gateway, selon le cas, puis cliquez sur Serveurs virtuels.****
2. Dans le volet de détails, sélectionnez le serveur virtuel que vous souhaitez configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le serveur virtuel**, cliquez sur l'onglet **Politiques** .
4. Pour créer une nouvelle politique dans cette banque, cliquez sur l'icône correspondant au type de politique ou d'étiquette de politique que vous souhaitez ajouter à la banque de politiques du serveur virtuel, puis cliquez sur **Insérer une politique**. Notez que si vous souhaitez invoquer une étiquette de politique sans évaluer une règle de politique, sélectionnez la politique « fictive » NOPOLICY.
5. Pour configurer une entrée existante dans cette banque de règles, entrez ce qui suit :
   - **Priorité :**

     Valeur numérique qui détermine un ordre d'évaluation absolu au sein de la banque ou qui est utilisée conjointement avec une expression Goto.
   - **Expression :**

     La règle de politique. Les expressions de stratégie sont décrites en détail dans les chapitres suivants. Pour une introduction, reportez-vous à la section Configuration des expressions de stratégie avancées : mise en route.
   - **Action :**

     L'action à effectuer si cette politique est évaluée comme VRAI.

- **Accédez à Expression :**

  Facultatif. Détermine la prochaine évaluation de la stratégie ou de la banque de stratégies. Pour plus d'informations sur les valeurs possibles d'une expression Goto, reportez-vous à la section « Entrées dans une banque de stratégies » de la section Règles de liaison utilisant une stratégie avancée.

- **Invoquer :**

  Facultatif. Pour appeler une autre banque de règles, sélectionnez le nom de l'étiquette de stratégies ou de la banque de stratégies du serveur virtuel que vous souhaitez appeler.

6. Cliquez sur **OK**. Un message dans la barre d'état indique que la politique est correctement configurée.

Invoquer ou supprimer une étiquette de stratégie ou une banque de politiques de serveur virtuel

March 9, 2023

Contrairement à une stratégie, qui ne peut être liée qu'une seule fois, vous pouvez utiliser une étiquette de stratégie ou la banque de politiques d'un serveur virtuel autant de fois que vous le souhaitez en l'invoquant. L'invocation peut être effectuée à partir de deux endroits :

- À partir de la reliure d'une police nommée dans une banque de politiques.
- À partir de la reliure d'une entrée « fictive » NOPOLICY dans une banque de politiques.

En général, l'étiquette de stratégie doit être du même type que la stratégie à partir de laquelle elle est invoquée. Par exemple, vous pouvez invoquer une étiquette de stratégie de répondeur à partir d'une politique de répondeur.

Remarque : Lorsque vous liez ou dissociez une entrée NOPOLICY globale dans une banque de politiques sur la ligne de commande, vous spécifiez une priorité pour distinguer une entrée NOPOLICY d'une autre.

Invoquez une étiquette de politique de mise en cache réécrite ou intégrée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour invoquer une étiquette de politique de réécriture ou de mise en cache intégrée et vérifier la configuration :

```
1 - bind cache global <policy> -priority <positive_integer> [-
    gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
```



```
    RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
    <label_name>

-  bind rewrite global<policy> -priority <positive_integer> [-
    gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
    RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
    <label_name>

-  show cache global|show rewrite global
<!--NeedCopy-->
```

Exemple :

```
> bind cache global _nonPostReq2 -priority 100 -type req_override -
    invoke
     policylabel lbl-cache-pol
Done
> show cache global
     1)      Global bindpoint: REQ_DEFAULT
             Number of bound policies: 2

     2)      Global bindpoint: RES_DEFAULT
             Number of bound policies: 1

     3)      Global bindpoint: REQ_OVERRIDE
             Number of bound policies: 1

Done
<!--NeedCopy-->
```

Invoquer une étiquette de politique de répondeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour invoquer une étiquette de politique de répondeur et vérifier la configuration :

```
-  bind responder global <policy_Name> <priority_as_positive_integer>
    [<gotoPriorityExpression>] -type REQ_OVERRIDE|REQ_DEFAULT|OVERRIDE|
    DEFAULT -invoke vserver|policylabel <label_name>

-  show responder global
<!--NeedCopy-->
```

Exemple :


```
> bind responder global pol404Error1 300 -invoke policylabel lbl-
    respndr-pol
Done
> show responder global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 2

Done
<!--NeedCopy-->
```

Invoquer une banque de politiques de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour appeler une banque de politiques de serveur virtuel et vérifier la configuration :

```
-  bind lb vserver <vserver_name> -policyName <policy_Name> -priority <
    positive_integer> [-gotoPriorityExpression <expression>] -type
    REQUEST|RESPONSE -invoke reqvserver|resvserver|policylabel <
    policy_Label_Name>

-  bind lb vserver <vserver_name>
<!--NeedCopy-->
```

Exemple :

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 100
Done

> show lb vserver lbvip
            lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
            State: DOWN
            Last state change was at Wed Jul 15 05:54:24 2009 (+166 ms)
            Time since last state change: 28 days, 06:37:49.250
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
```



```
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none

    1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority:
        100   Hits: 0

    2)      Policy : pol-ssl Priority:0
    3)      Policy : ns_cmp_msapp Priority:100
    4)      Policy : cf-pol Priority:1      Inherited
Done
<!--NeedCopy-->
```

Supprimer une étiquette de politique de mise en cache réécrite ou intégrée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour supprimer une étiquette de politique de réécriture ou de mise en cache intégrée et vérifier la configuration :

```
- unbind rewrite global <policyName> -priority <positiveInteger> -type
   REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT

- unbind cache global <policyName> -priority <positiveInteger> -type
  REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT

- show rewrite global|show cache global
<!--NeedCopy-->
```

Exemple :

```
> unbind rewrite global NOPOLICY -priority 100 -type REQ_OVERRIDE
> show rewrite global
Done
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 1

Done
<!--NeedCopy-->
```


Supprimer une étiquette de politique de répondeur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour supprimer l'étiquette de politique d'un répondeur et vérifier la configuration :

```
1 - unbind responder global <policyName> -priority <positiveInteger> -
    type OVERRIDE|DEFAULT
2
3 - show responder global
4 <!--NeedCopy-->
```

Exemple :

```
1 > unbind responder global NOPOLICY -priority 100 -type REQ_DEFAULT
2 Done
3 > show responder global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6
7 Done
8 <!--NeedCopy-->
```

Supprimer une étiquette de politique de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour supprimer une étiquette de politique de serveur virtuel et vérifier la configuration :

```
1 - unbind lb vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
    NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <
    positiveInteger>
2
3 - unbind cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
    NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <
    positiveInteger>
4
5 - show lb vserver|show cs vserver
6 <!--NeedCopy-->
```

Exemple :

```
1 > unbind lb vserver lbvip -policyName ns_cmp_msapp -priority 200
2 Done
```



```
> show lb vserver lbvip
            lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
            State: DOWN
            Last state change was at Wed Jul 15 05:54:24 2009 (+161 ms)
            Time since last state change: 28 days, 06:47:54.600
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none

    1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority:
       100   Hits: 0

    1)      Policy : pol-ssl Priority:0
    2)      Policy : cf-pol Priority:1      Inherited
Done
<!--NeedCopy-->
```

Appelez une étiquette de stratégie ou une banque de stratégies de serveur virtuel à l'aide de l'interface graphique

1. Liez une stratégie, comme décrit dans Lier une stratégie globalement, Lier une stratégie à un serveur virtuelou Lier une stratégie à une étiquette de stratégie. Vous pouvez également entrer une entrée « factice » NOPOLICY au lieu d'un nom de stratégie. Vous pouvez procéder ainsi si vous ne souhaitez pas évaluer une politique avant d'avoir évalué la banque de politiques.
2. Dans le champ Invoke, sélectionnez le nom de l'étiquette de stratégie ou de la banque de politiques du serveur virtuel dont vous souhaitez évaluer si le trafic correspond à la politique liée. Un message dans la barre d'état indique que l'étiquette de stratégie ou la banque de politiques du serveur virtuel a été invoquée avec succès.

Supprimer l'invocation d'une étiquette de politique à l'aide de l'interface graphique

1. Ouvrez la politique et effacez le champ Invoke. La suppression de la politique supprime également l'invocation de l'étiquette. Un message dans la barre d'état indique que l'étiquette de la politique a été supprimée avec succès.

Configuration d'une expression de politique avancée : mise en route

May 5, 2023

Les politiques avancées évaluent les données en fonction des informations que vous fournissez dans les expressions de stratégie avancées. Une expression de politique avancée analyse les éléments de données (par exemple, les en-têtes HTTP, les adresses IP source, l'heure du système NetScaler et les données du corps POST). Outre la configuration d'une expression de politique avancée dans une politique, certaines fonctionnalités de NetScaler vous permettent de configurer une expression de stratégie avancée en dehors du contexte d'une politique.

Pour créer une expression de politique avancée, vous sélectionnez un préfixe qui identifie une donnée que vous souhaitez analyser, puis vous spécifiez une opération à effectuer sur les données. Par exemple, une opération peut associer une donnée à une chaîne de texte que vous spécifiez ou transformer une chaîne de texte en en-tête HTTP. D'autres opérations font correspondre une chaîne renvoyée à un ensemble de chaînes ou à un modèle de chaîne. Vous configurez des expressions composées en spécifiant des opérateurs booléens et arithmétiques et en utilisant des parenthèses pour contrôler l'ordre d'évaluation.

L'expression de politique avancée peut également contenir des expressions classiques. Vous pouvez attribuer un nom à une expression fréquemment utilisée pour éviter d'avoir à créer l'expression à plusieurs reprises.

Les politiques et quelques autres entités incluent des règles que NetScaler utilise pour évaluer un paquet dans le trafic qui le traverse, pour extraire des données du système NetScaler lui-même, pour envoyer une demande (un « appel ») à une application externe ou pour analyser un autre élément de données. Une règle prend la forme d'une expression logique qui est comparée au trafic et renvoie finalement des valeurs TRUE ou FALSE.

Les éléments de la règle peuvent eux-mêmes renvoyer des valeurs TRUE ou FALSE, une chaîne ou des valeurs numériques.

Avant de configurer une expression de politique avancée, vous devez comprendre les caractéristiques des données que la politique ou une autre entité doit évaluer. Par exemple, lorsque vous utilisez la fonctionnalité de mise en cache intégrée, une politique détermine quelles données peuvent être stockées dans le cache. Avec la mise en cache intégrée, vous devez connaître les URL, les en-têtes

et les autres données contenues dans les requêtes et réponses HTTP que NetScaler reçoit. Grâce à ces connaissances, vous pouvez configurer des politiques qui correspondent aux données réelles et permettre à NetScaler de gérer la mise en cache du trafic HTTP. Ces informations vous aident à déterminer le type d'expression que vous devez configurer dans la stratégie.

Éléments de base d'une expression de stratégie avancée

May 8, 2023

Une expression de politique avancée se compose, au minimum, d'un préfixe (ou d'un seul élément utilisé à la place d'un préfixe). La plupart des expressions spécifient également une opération à effectuer sur les données identifiées par le préfixe. Vous pouvez formater une expression comportant jusqu'à 1 499 caractères comme suit :

```
<prefix>.<operation> [<compound-operator> <prefix>.<operation>. . .]
```

où

- \ <prefix>

  est un point d'ancrage pour démarrer une expression.

  Le préfixe est une clé délimitée par des points qui identifie une unité de données. Par exemple, le préfixe suivant examine les requêtes HTTP afin de détecter la présence d'un en-tête nommé Content-Type :

  http.req.header (« Type de contenu »)

  Les préfixes peuvent également être utilisés seuls pour renvoyer la valeur de l'objet que le préfixe identifie.

- \ <operation>

  identifie une évaluation à effectuer sur les données identifiées par le préfixe.

  Par exemple, considérez l'expression suivante :

  http.req.header (« Type de contenu ») .eq (« text/html »)

  Dans cette expression, le composant opérateur est le suivant :

  eq (« texte/html »)

  Cet opérateur amène NetScaler à évaluer toutes les requêtes HTTP contenant un en-tête Content-Type et, en particulier, à déterminer si la valeur de cet en-tête est égale à la chaîne « text/html ». Pour plus d'informations, voir « Opérations ». «

- <compound-operator>

  est un opérateur booléen ou arithmétique qui forme une expression composée à partir de plusieurs éléments de préfixe ou de préfixe.

  Par exemple, considérez l'expression suivante :

  http.req.header (« Type de contenu ») .eq (« text/html ») et http.req.url.contains (« .html »)

Préfixes

Un préfixe d'expression représente une donnée discrète. Par exemple, un préfixe d'expression peut représenter une URL HTTP, un en-tête de cookie HTTP ou une chaîne dans le corps d'une requête HTTP POST. Un préfixe d'expression peut identifier et renvoyer un large éventail de types de données, notamment les suivants :

- Adresse IP du client dans un paquet TCP/IP
- Heure du système NetScaler
- Une légende externe via HTTP
- Un type d'enregistrement TCP ou UDP

Dans la plupart des cas, le préfixe d'une expression commence par l'un des mots-clés suivants :

- CLIENT :
  - Identifie une caractéristique du client qui envoie une demande ou reçoit une réponse, comme dans les exemples suivants :
  - Le préfixe client.ip.dst désigne l'adresse IP de destination dans la demande ou la réponse.
  - Le préfixe client.ip.src désigne l'adresse IP source.
- HTTP :
  - Identifie un élément dans une requête ou une réponse HTTP, comme dans les exemples suivants :
  - Le préfixe http.req.body (entier) désigne le corps de la requête HTTP sous la forme d'un objet texte multiligne, jusqu'à la position du caractère indiquée en entier.
  - Le préfixe http.req.header (« header_name ») désigne un en-tête HTTP, tel que spécifié dans header_name.
  - Le préfixe http.req.url désigne une URL HTTP au format URL codé.
- SERVEUR :

  Identifie un élément du serveur qui traite une demande ou envoie une réponse.
- DIT :

  Identifie une caractéristique du NetScaler qui traite le trafic.

Remarque : Notez que les politiques DNS ne prennent en charge que les objets SYS, CLIENT et SERVER.

En outre, dans NetScaler Gateway, la fonction VPN sans client peut utiliser les types de préfixes suivants :

- TEXTE :

  Identifie tout élément de texte dans une demande ou une réponse.

- CIBLE :

  Identifie la cible d'une connexion.

- ADRESSE URL :

  Identifie un élément dans la partie URL d'une requête ou d'une réponse HTTP.

En règle générale, tout préfixe d'expression peut être une expression autonome. Par exemple, le préfixe suivant est une expression complète qui renvoie le contenu de l'en-tête HTTP spécifié dans l'argument de chaîne (entre guillemets) :

```
http.res.header.("myheader")
```

Vous pouvez également combiner des préfixes avec des opérations simples pour déterminer les valeurs VRAI et FAUX. Par exemple, la commande suivante renvoie la valeur TRUE ou FALSE :

```
http.res.header.("myheader").exists
```

Vous pouvez également utiliser des opérations complexes sur des préfixes individuels et sur plusieurs préfixes au sein d'une expression, comme dans l'exemple suivant :

```
http.req.url.length + http.req.cookie.length <= 500
```

Les préfixes d'expression que vous pouvez spécifier dépendent de la fonctionnalité NetScaler. Le tableau suivant décrit les préfixes d'expression qui présentent un intérêt pour chaque fonctionnalité.

Fonctionnalité	Types de préfixes d'expression utilisés dans la fonctionnalité
DNS	SYS, CLIENT, SERVEUR
Responder dans les fonctionnalités de protection	HTTP, SYS, CLIENT
Commutation de contenu	HTTP, SYS, CLIENT
Réécriture	HTTP, SYS, CLIENT, SERVEUR, URL, TEXTE, CIBLE, VPN
Mise en cache intégrée	HTTP, SYS, CLIENT, SERVEUR

Fonctionnalité	Types de préfixes d'expression utilisés dans la fonctionnalité
NetScaler Gateway, accès sans client	HTTP, SYS, CLIENT, SERVEUR, URL, TEXTE, CIBLE, VPN

Tableau 1. Types de préfixes d'expression autorisés dans diverses fonctionnalités de NetScaler

Remarque : Pour plus de détails sur les préfixes d'expression autorisés dans une fonctionnalité, consultez la documentation de cette fonctionnalité.

Expressions à élément unique

Le type le plus simple d'expression de politique avancée contient un seul élément. Cet élément peut être l'un des suivants :

- vrai. Une expression de politique avancée peut se composer simplement de la valeur true. Ce type d'expression renvoie toujours la valeur TRUE. Il est utile pour enchaîner les actions de politique et déclencher des expressions Goto.
- faux. Une expression de politique avancée peut simplement se composer de la valeur false. Ce type d'expression renvoie toujours la valeur FALSE.
- Préfixe d'une expression composée. Par exemple, le préfixe HTTP.REQ.HOSTNAME est une expression complète qui renvoie un nom d'hôte et HTTP.REQ.URL est une expression complète qui renvoie une URL. Le préfixe peut également être utilisé conjointement avec des opérations et des préfixes supplémentaires pour former une expression composée.

Opérations

Dans la plupart des expressions, vous spécifiez également une opération sur les données identifiées par le préfixe. Supposons, par exemple, que vous indiquiez le préfixe suivant :

```
http.req.url
```

Ce préfixe extrait les URL des requêtes HTTP. Ce préfixe d'expression ne nécessite pas l'utilisation d'opérateurs dans une expression. Toutefois, lorsque vous configurez une expression qui traite des URL de requête HTTP, vous pouvez spécifier des opérations qui analysent des caractéristiques particulières de l'URL. Voici quelques possibilités :

- Recherchez un nom d'hôte particulier dans l'URL.
- Recherchez un chemin particulier dans l'URL.
- Évaluez la longueur de l'URL.
- Dans l'URL, recherchez une chaîne indiquant un horodatage et convertissez-la en GMT.

Voici un exemple de préfixe qui identifie un en-tête HTTP nommé Server et une opération qui recherche la chaîne IIS dans la valeur de l'en-tête :

```
http.res.header("Server").contains("IIS")
```

Vous trouverez ci-dessous un exemple de préfixe identifiant les noms d'hôtes et d'opération de recherche de la chaîne « www.mycompany.com » comme valeur du nom :

```
http.req.hostname.eq("www.mycompany.com")
```

Opérations de base sur les préfixes d'expression

Le tableau suivant décrit quelques-unes des opérations de base qui peuvent être effectuées sur les préfixes d'expression.

Operation	Détermine si oui ou non
CONTIENT (\ <string>)	L'objet correspond à \ <string>. Voici un exemple : http.req.header (« Cache-Control ») .contains (« no-cache »)
EXISTE	Un élément particulier est présent dans un objet. Voici un exemple : http.res.header (« MyHDR ») .exists
<text>EQ (\)	Une valeur non numérique particulière est présente dans un objet. Voici un exemple : http.req.method.eq (post)
<integer>EQ (\)	Une valeur numérique particulière est présente dans un objet. Voici un exemple : client.ip.dst.eq (10.100.10.100)
LT (\ <integer>)	La valeur d'un objet est inférieure à une valeur particulière. Voici un exemple : http.req.content_length.lt (5000)
GT (\ <integer>)	La valeur d'un objet est supérieure à une valeur particulière. Voici un exemple : http.req.content_length.gt (5)

Le tableau suivant récapitule quelques-uns des types d'opérations disponibles.

Type d'opération	Description
Opérations sur le texte	Associez des chaînes individuelles et des ensembles de chaînes à n'importe quelle partie d'une cible. La cible peut être une chaîne entière, le début d'une chaîne ou n'importe quelle partie de texte située entre le début et la fin de la chaîne. Par exemple, vous pouvez extraire la chaîne « XYZ » de « XYZSomeText ». Vous pouvez également comparer la valeur d'un en-tête HTTP avec un tableau de chaînes différentes. Vous pouvez également transformer du texte en un autre type de données. Voici des exemples : transformez une chaîne en une valeur entière, créez une liste à partir des chaînes de requête d'une URL et transformez une chaîne en valeur temporelle.
Opérations numériques	Les opérations numériques incluent l'application d'opérateurs arithmétiques, l'évaluation de la longueur du contenu, le nombre d'éléments dans une liste, les dates, les heures et les adresses IP.

Expressions de stratégie avancées composées

May 5, 2023

Vous pouvez configurer une expression de stratégie avancée avec des opérateurs booléens ou arithmétiques et des opérations atomiques. L'expression composée suivante a un AND booléen :

```
http.req.hostname.eq("mycompany.com")&& http.req.method.eq(post)
```

L'expression suivante ajoute la valeur de deux cibles et compare le résultat à une troisième valeur :

```
http.req.url.length + http.req.cookie.length \<= 500
```

Une expression composée peut comporter un certain nombre d'opérateurs logiques et arithmétiques.

L'expression suivante évalue la longueur d'une requête HTTP. Cette expression est basée sur l'URL et le cookie.
Cette expression évalue le texte de l'en-tête. De plus, un AND booléen fait sur ces deux résultats :


```
http.req.url.length + http.req.cookie.length \<= 500 && http.req.header.
contains("some text")
```

Vous pouvez utiliser des parenthèses pour contrôler l'ordre d'évaluation dans une expression composée.

Booléens dans les expressions composées

Vous configurez des expressions composées à l'aide des opérateurs suivants :

- &&.

  Cet opérateur est un AND logique. Pour que l'expression soit évaluée à TRUE, tous les composants doivent être évalués à TRUE.

  Exemple :

  http.req.url.hostname.eq("myHost") && http.req.header("myHeader").exists

- ||.

  Cet opérateur est un OR logique. Si un composant de l'expression est évalué à TRUE, l'expression entière est TRUE.

- !.

  P N'est pas logique sur l'expression.

Parfois, l'utilitaire de configuration NetScaler propose les opérateurs AND, NOT et OR dans la boîte de dialogue **Ajouter une expression** . Toutefois, ces expressions composées sont d'une utilité limitée. Citrix vous recommande d'utiliser les opérateurs &&, || et ! Pour configurer des expressions composées utilisant la logique booléenne.

Parenthèses dans les expressions composées

Vous pouvez utiliser des parenthèses pour contrôler l'ordre d'évaluation d'une expression. Voici un exemple :

```
http.req.url.contains("myCompany.com")|| (http.req.url.hostname.eq("myHost"
)&& http.req.header("myHeader").exists)
```

Voici un autre exemple :

```
(http.req.header("Content-Type").exists && http.req.header("Content-Type").
eq("text/html"))|| (http.req.header("Transfer-Encoding").exists || http.req
.header("Content-Length").exists)
```


Opérations composées pour les chaînes

Le tableau suivant décrit les opérateurs que vous pouvez utiliser pour configurer des opérations composées sur des données de chaîne.

Opérations produisant une valeur de chaîne	Description
str +	Concatène la valeur de l'expression à gauche de l'opérateur avec la valeur à droite. Exemple : http.req.hostname + http.req.url.protocol
str + num	Concatène la valeur de l'expression à gauche de l'opérateur avec une valeur numérique à droite. Exemple : http.req.hostname + http.req.url.content_length
num + str	Concatène la valeur numérique de l'expression sur le côté gauche de l'opérateur avec une valeur de chaîne sur la droite. Exemple : http.req.url.content_length + http.req.url.hostname
str + ip	Concatène la valeur de chaîne de l'expression sur le côté gauche de l'opérateur avec une valeur d'adresse IP sur la droite. Exemple : http.req.hostname + 10.00.000.00
IP + str	Concatène la valeur de l'adresse IP de l'expression située à gauche de l'opérateur avec une valeur de chaîne à droite. Exemple : client.ip.dst + http.req.url.hostname
str1 ALT str2	Utilise string2 si l'évaluation de string1 entraîne une exception undef ou si le résultat est une chaîne nulle. Sinon, utilise string1 et n'évalue jamais string2. Exemple : ttp.req.hostname alt client.ip.src

Opérations sur les chaînes qui produisent un résultat de TRUE ou FALSE	Description
str == str	Évalue si les chaînes de chaque côté de l'opérateur sont identiques. Voici un exemple : http.req.header("myheader") == http.res.header("myheader")
str <= str	Évalue si la chaîne située à gauche de l'opérateur est identique à la chaîne de droite ou si elle la précède dans l'ordre alphabétique.
str >= str	Évalue si la chaîne située à gauche de l'opérateur est identique à la chaîne de droite ou si elle la suit dans l'ordre alphabétique.
str < str	Évalue si la chaîne située à gauche de l'opérateur précède la chaîne de droite dans l'ordre alphabétique.
str > str	Évalue si la chaîne située à gauche de l'opérateur suit la chaîne de droite dans l'ordre alphabétique.
str !!= str	Évalue si les chaînes de chaque côté de l'opérateur sont différentes.

Opérations logiques sur les chaînes	Description
bool && bool	Cet opérateur est un AND logique. Lors de l'évaluation des composants de l'expression composée, tous les composants qui sont joints par le AND doivent être évalués à TRUE. Voici un exemple : http.req.method.eq(GET) && http.req.url.query.contains("viewReport && my_pagelabel")

Opérations logiques sur les chaînes	Description
bool || bool	Cet opérateur est un OR logique. Lors de l'évaluation des composants de l'expression composée, si un composant de l'expression appartenant à OR est évalué à TRUE, l'expression entière est TRUE. Voici un exemple : http.req.url.contains(".js") || http.res.header.("Content-Type"). Contains("javascript")
Bool	Effectue une opération NOT logique sur l'expression.

Opérations composées pour les nombres

Vous pouvez configurer des expressions numériques composées. Par exemple, l'expression suivante renvoie une valeur numérique qui est la somme d'une longueur d'en-tête HTTP et d'une longueur d'URL :

```
http.req.header.length + http.req.url.length
```

Les tableaux suivants décrivent les opérateurs que vous pouvez utiliser pour configurer des expressions composées pour des données numériques.

Opérations arithmétiques sur les nombres	Description
num + num	Ajoutez la valeur de l'expression à gauche de l'opérateur à la valeur de l'expression de droite. Voici un exemple : http.req.content_length + http.req.url.length
num — num	Soustrayez la valeur de l'expression à droite de l'opérateur de la valeur de l'expression à gauche.
num*num	Multipliez la valeur de l'expression à gauche de l'opérateur par la valeur de l'expression à droite. Voici un exemple : client.interface.rxthroughput* 9
num / num	Divisez la valeur de l'expression à gauche de l'opérateur par la valeur de l'expression à droite.

Opérations arithmétiques sur les nombres	Description
num% num	Calculez le modulo, ou le reste numérique sur une division de la valeur de l'expression à gauche de l'opérateur par la valeur de l'expression à droite. Par exemple, les valeurs « 15 mod 4" sont égales à 3 et « 12 mod 4" sont égales à 0.
~number	Renvoie un nombre après avoir appliqué une négation logique bit à bit du nombre. L'exemple suivant suppose que numeric.expression renvoie 12 (binaire 1100) : ~numeric.expression. Le résultat de l'application de l'opérateur ~ est -11 (un binaire 1110011, 32 bits au total avec tous ceux à gauche). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.

Opérations arithmétiques sur les nombres	Description
number ^ number	Compare deux modèles de bits de même longueur et effectue une opération XOR sur chaque paire de bits correspondants dans chaque argument numérique, renvoyant 1 si les bits sont différents et 0 s'ils sont identiques. Renvoie un nombre après avoir appliqué un XOR bit à bit à l'argument entier et à la valeur numérique courante. Si les valeurs de la comparaison bit à bit sont identiques, la valeur renvoyée est 0. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 10 (binaire 1010) : numeric.expression1 ^ numeric.expression2Le résultat de l'application de l'opérateur ^ à l'ensemble de l'expression est 6 (binaire 0110). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.
number | number	Renvoie un nombre après avoir appliqué un OR bit à bit aux valeurs numériques. Si l'une des valeurs de la comparaison bit à bit est 1, la valeur renvoyée est 1. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 10 (binaire 1010) : numeric.expression1 | numeric.expression2 Le résultat de l'application de l'opérateur | à l'ensemble de l'expression est 14 (binaire 1110). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.

Opérations arithmétiques sur les nombres	Description
number & number	Compare deux modèles de bits de même longueur et effectue une opération AND bit à bit sur chaque paire de bits correspondants, renvoyant 1 si les deux bits contiennent une valeur de 1, et 0 si l'un des bits est égal à 0. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 10 (binaire 1010) : numeric.expression1 & numeric.expression2 L'expression entière est évaluée à 8 (binaire 1000). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.
num « num	Renvoie un nombre après un décalage vers la gauche de la valeur de nombre par le nombre d'arguments de droite nombre de bits. Notez que le nombre de bits décalés est un entier modulo 32. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 3 : numeric.expression1 « numeric.expression2 Le résultat de l'application de l'opérateur LSHIFT est 96 (un binaire 1100000) .Notez que toutes les valeurs renvoyées sont inférieures à 32 bits avant d'appliquer l'opérateur ont implicitement des zéros à gauche pour leur donner une largeur de 32 bits.

Opérations arithmétiques sur les nombres	Description
num » num	Retourne un nombre après un décalage vers la droite du bit de la valeur du nombre par le nombre entier d'argument de bits. Notez que le nombre de bits décalés est un entier modulo 32. L'exemple suivant suppose que numeric.expression1 renvoie 12 (binaire 1100) et numeric.expression2 renvoie 3 : numeric.expression1 » numeric.expression2 Le résultat de l'application de l'opérateur RSHIFT est 1 (un binaire 0001). Notez que toutes les valeurs renvoyées de moins de 32 bits avant l'application de l'opérateur ont implicitement des zéros à gauche pour les rendre larges de 32 bits.

Opérateurs numériques qui produisent un résultat de TRUE ou FALSE	Description
———–	———————————————————————————
num == num	Déterminez si la valeur de l'expression à gauche de l'opérateur est égale à la valeur de l'expression à droite.
num! = num	Déterminez si la valeur de l'expression située à gauche de l'opérateur n'est pas égale à la valeur de l'expression à droite.	
num > num	Déterminez si la valeur de l'expression située à gauche de l'opérateur est supérieure à la valeur de l'expression à droite.
num < num	Déterminez si la valeur de l'expression située à gauche de l'opérateur est inférieure à la valeur de l'expression à droite.
num >= num	Déterminez si la valeur de l'expression située à gauche de l'opérateur est supérieure ou égale à la valeur de l'expression à droite.
num <= num	Déterminez si la valeur de l'expression située à gauche de l'opérateur est inférieure ou égale à la valeur de l'expression à droite

Fonctions pour les types de données dans l'infrastructure de stratégie

L'infrastructure de politique NetScaler prend en charge les types de données numériques suivants :

- Entier (32 bits)
- Long non signé (64 bits)
- Double (64 bits)

Les expressions simples peuvent renvoyer tous ces types de données. Vous pouvez également créer des expressions composées qui utilisent des opérateurs arithmétiques et des opérateurs logiques pour évaluer ou renvoyer les valeurs de ces types de données. Vous pouvez également utiliser toutes ces valeurs dans des expressions de stratégie. Les constantes littérales de type unsigned long peuvent être spécifiées en ajoutant la chaîne ul au nombre. Les constantes littérales de type double contiennent un point (.), un exposant ou les deux.

Opérateurs arithmétiques, opérateurs logiques et promotion de type

Dans les expressions composées, les opérateurs arithmétiques et logiques standard suivants peuvent être utilisés pour les types de données longues doubles et non signées :

- +, -, * et/
- %, ~, ^, &, |, «, et » (ne s'appliquent pas au double)
- ==, ! =, >, <, >= et <=

Tous ces opérateurs ont la même signification que dans le langage de programmation C.

Dans tous les cas d'opérations mixtes entre des opérandes de type entier, long non signé et double. La promotion de type est effectuée pour effectuer l'opération sur les opérandes du même type. L'opération promeut un type de priorité inférieure à l'opérande ayant le type de priorité la plus élevée. L'ordre de priorité (supérieur à inférieur) est le suivant :

- Double
- Long non signé
- Nombre entier

Ainsi, une opération qui renvoie un résultat numérique renvoie un résultat du type le plus élevé impliqué dans l'opération.

Par exemple, si les opérandes sont de type entier et non signé long, l'opérande entier est automatiquement converti en type unsigned long. Cette conversion de type s'effectue dans des expressions simples. Le type de données identifié par le préfixe d'expression ne correspond pas au type de données transmises en tant qu'argument à la fonction. Dans l'opération HTTP.REQ.CONTENT_LENGTH.DIV (3ul), le préfixe HTTP.REQ.CONTENT_LENGTH.DIV renvoie un entier qui devient long non signé. Long non signé : le type de données transmis comme argument à la fonction DIV (), une division longue non signée est effectuée. De même, l'argument peut être promu dans une expression. Par exemple, HTTP.REQ.HEADER (« MyHeader ») .TYPECAST_DOUBLE_AT.DIV (5) promeut l'entier 5 à taper double et effectue une division à double précision.

Pour plus d'informations sur les expressions permettant de transférer des données d'un type vers des données d'un autre type, reportez-vous à la section Données de typage.

Spécifier le jeu de caractères dans les expressions

May 8, 2023

L'infrastructure de politiques de l'appliance NetScaler prend en charge les jeux de caractères ASCII et UTF-8. Le jeu de caractères par défaut est ASCII. Si le trafic pour lequel vous configurez une expression se compose uniquement de caractères ASCII, vous n'avez pas besoin de spécifier le jeu de caractères dans l'expression. L'appliance autorise toutes les chaînes et tous les caractères littéraux, y compris les caractères binaires. Cependant, les jeux de caractères UTF-8 nécessitent toujours que la chaîne et les littéraux de caractères soient un UTF-8 valide.

```
CLIENT.TCP.PAYLOAD(100).CONTAINS("\xff\x02")
```

Dans une expression, la fonction SET_CHAR_SET () doit être introduite au point de l'expression après lequel le traitement des données doit être effectué dans le jeu de caractères spécifié. <string>Par exemple, dans l'expression HTTP.REQ.BODY (1000) .AFTER_REGEX (re/following example/) .BEFORE_REGEX (re/dans l'exemple précédent/) .CONTAINS_ANY (« Alphabet grec »), si les chaînes stockées dans le jeu de modèles « GREEK_alphabet » sont en UTF-8, vous devez inclure la fonction SET_CHAR_SET (UTF_8) juste avant CONTAINS_ANY (« \ »), comme suit :

```
HTTP.REQ.BODY(1000).AFTER_REGEX(re/following example/).BEFORE_REGEX(re/In
the preceding example/).SET_CHAR_SET(UTF_8).CONTAINS_ANY("Greek_ alphabet")
```

La fonction SET_CHAR_SET () définit le jeu de caractères pour tous les traitements ultérieurs (c'est-à-dire pour toutes les fonctions suivantes) dans l'expression, à moins qu'il ne soit remplacé ultérieurement dans l'expression par une autre fonction SET_CHAR_SET () qui modifie le jeu de caractères. <int>Par conséquent, si toutes les fonctions d'une expression simple donnée sont destinées à l'UTF-8, vous pouvez inclure la fonction SET_CHAR_SET (UTF_8) immédiatement après les fonctions qui identifient du texte (par exemple, les fonctions HEADER (« \ <name> ») ou BODY (\)). Dans le deuxième exemple qui suit le premier paragraphe ci-dessus, si les arguments ASCII transmis aux fonctions AFTER_REGEX () et BEFORE_REGEX () sont remplacés par des chaînes UTF-8, vous pouvez inclure la fonction SET_CHAR_SET (UTF_8) immédiatement après la fonction BODY (1000), comme suit :

```
HTTP.REQ.BODY(1000).SET_CHAR_SET(UTF_8).AFTER_REGEX(re/Bücher/).BEFORE_REGEX
(re/Wörterbuch/).CONTAINS_ANY("Greek_alphabet")
```

Le jeu de caractères UTF-8 étant un sur-ensemble du jeu de caractères ASCII, les expressions configurées pour le jeu de caractères ASCII continuent de fonctionner comme prévu si vous remplacez le jeu de caractères par UTF-8.

Expressions composées avec différents jeux de caractères

Dans une expression composée, si un sous-ensemble d'expressions est configuré pour fonctionner avec des données du jeu de caractères ASCII et que les autres expressions sont configurées pour

fonctionner avec des données du jeu de caractères UTF-8, le jeu de caractères spécifié pour chaque expression individuelle est pris en compte lorsque les expressions sont évaluées individuellement. Toutefois, lors du traitement de l'expression composée, juste avant de traiter les opérateurs, l'appliance fait passer le jeu de caractères des valeurs ASCII renvoyées au format UTF-8. Par exemple, dans l'expression composée suivante, la première expression simple évalue les données du jeu de caractères ASCII tandis que la seconde expression simple évalue les données du jeu de caractères UTF-8 :

```
HTTP.REQ.HEADER("MyHeader")== HTTP.REQ.BODY(10).SET_CHAR_SET(UTF_8)
```

Toutefois, lors du traitement de l'expression composée, juste avant d'évaluer l'opérateur booléen « est égal à », l'appliance NetScaler transforme le jeu de caractères de la valeur renvoyée par HTTP.REQ.HEADER (« MyHeader ») en UTF-8.

La première expression simple de l'exemple suivant évalue les données du jeu de caractères ASCII. Toutefois, lorsque l'appliance NetScaler traite l'expression composée, juste avant de concaténer les résultats des deux expressions simples, elle transforme le jeu de caractères de la valeur renvoyée par HTTP.REQ.BODY (10) en UTF-8.

```
HTTP.REQ.BODY(10)+ HTTP.REQ.HEADER("MyHeader").SET_CHAR_SET(UTF_8)
```

Par conséquent, l'expression composée renvoie des données dans le jeu de caractères UTF-8.

Spécifiez le jeu de caractères en fonction du jeu de caractères du trafic

Vous pouvez définir le jeu de caractères sur UTF-8 en fonction des caractéristiques du trafic. Si vous n'êtes pas sûr que le jeu de caractères du trafic évalué est UTF-8, vous pouvez configurer une expression composée dans laquelle la première expression vérifie le trafic UTF-8 et les expressions suivantes définissent le jeu de caractères en UTF-8. Voici un exemple d'expression composée qui vérifie d'abord la valeur de « charset » dans l'en-tête Content-Type de la requête pour « UTF-8 » avant de vérifier si les 1 000 premiers octets de la requête contiennent la chaîne UTF-8 Bücher :

```
HTTP.REQ.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).TYPECAST_NVLIST_T
('=', '; ', '"').VALUE("charset").EQ("UTF-8")&& HTTP.REQ.BODY(1000).SET_CHAR_SET
(UTF_8).CONTAINS("Bücher")
```

Si vous êtes certain que le jeu de caractères du trafic évalué est UTF-8, la deuxième expression de l'exemple est suffisante.

Littéraux de caractères et de chaînes dans les expressions

Lors de l'évaluation d'une expression, même si le jeu de caractères actuel est ASCII, les littéraux de caractères et les littéraux de chaîne, qui sont placés respectivement entre guillemets simples (« ») et entre guillemets (« »), sont considérés comme des littéraux dans le jeu de caractères UTF-8. Dans une

expression donnée, si une fonction fonctionne sur des caractères ou des chaînes littéraux du jeu de caractères ASCII et que vous incluez un caractère non ASCII dans le littéral, une erreur est renvoyée.

> **Remarque** :
>
> Les littéraux de chaîne dans les expressions de stratégie avancées sont désormais aussi longs que l'expression de stratégie. La longueur de l'expression est autorisée à 1499 octets ou 8191 octets.

Valeurs aux formats hexadécimal et octal

Lorsque vous configurez une expression, vous pouvez entrer des valeurs aux formats octal et hexadécimal. Toutefois, chaque octet hexadécimal ou octal est considéré comme un octet UTF-8. Les octets UTF-8 non valides génèrent des erreurs, que la valeur soit saisie manuellement ou collée depuis le presse-papiers. Par exemple, « \ xce \ x20 » n'est pas un caractère UTF-8 non valide car « c8 » ne peut pas être suivi de « 20 » (chaque octet d'une chaîne UTF-8 multi-octets doit avoir le bit le plus élevé défini). Un autre exemple de caractère UTF-8 non valide est « \ xce \ xa9 », car les caractères hexadécimaux sont séparés par un espace blanc.

Fonctions renvoyant des chaînes UTF-8

Seules les `<text>.XPATH_JSON` fonctions `text>.XPATH` et renvoient toujours des chaînes UTF-8. Les routines MYSQL suivantes déterminent au moment de l'exécution le jeu de caractères à renvoyer, en fonction des données du protocole :

- `MYSQL_CLIENT_T.USER`
- `MYSQL_CLIENT_T.DATABASE`
- `MYSQL_REQ_QUERY_T.COMMAND`
- `MYSQL_REQ_QUERY_T.TEXT`
- `MYSQL_REQ_QUERY_T.TEXT(<unsigned int>)`
- `MYSQL_RES_ERROR_T.SQLSTATE`
- `MYSQL_RES_ERROR_T.MESSAGE`
- `MYSQL_RES_FIELD_T.CATALOG`
- `MYSQL_RES_FIELD_T.DB`
- `MYSQL_RES_FIELD_T.TABLE`
- `MSQL_RES_FIELD_T.ORIGINAL_TABLE`
- `MYSQL_RES_FIELD_T.NAME`
- `MYSQL_RES_FIELD_T.ORIGINAL_NAME`
- `MYSQL_RES_OK_T.MESSAGE`
- `MYSQL_RES_ROW_T.TEXT_ELEM(<unsigned int>)`

Paramètres de connexion du terminal pour UTF-8

Lorsque vous établissez une connexion à l'appliance NetScaler à l'aide d'une connexion terminal (à l'aide de PuTTY, par exemple), vous devez définir le jeu de caractères pour la transmission des données en UTF-8.

Fonctions minimales et maximales dans une expression de politique avancée

Les expressions de politique avancées prennent en charge les fonctions minimales et maximales ci-dessous.

1. (<expression1>.max(<expression2>) - renvoie le maximum des deux valeurs.
2. (<expression1>.min(<expression2>) - renvoie le minimum des deux valeurs.

Configuration des expressions de stratégie avancées dans une stratégie

October 5, 2021

Vous pouvez configurer une expression de stratégie avancée comportant jusqu'à 1 499 caractères dans une stratégie. L'interface utilisateur des expressions de stratégie avancées dépend dans une certaine mesure de la fonctionnalité pour laquelle vous configurez l'expression et de la configuration d'une expression pour une stratégie ou pour une autre utilisation.

Lorsque vous configurez des expressions sur la ligne de commande, vous les délimitez en utilisant des guillemets («.. » ou «.. »). Dans une expression, vous échappez les guillemets supplémentaires à l'aide d'une barre oblique inverse (). Par exemple, les méthodes standard suivantes permettent d'échapper les guillemets dans une expression :

```
"\"abc\""
```

```
'\"abc\"'
```

Vous devez également utiliser une barre oblique inverse pour échapper les points d'interrogation et autres barres obliques inverses sur la ligne de commande. Par exemple, l'expression http.req.url.contains (« ? ») nécessite une barre oblique inverse pour que le point d'interrogation soit analysé. Notez que la barre oblique inverse n'apparaîtra pas sur la ligne de commande après avoir tapé le point d'interrogation. En revanche, si vous échappez une barre oblique inverse (par exemple, dans l'expression 'http.req.url.contains (« \ \ http ») '), les caractères d'échappement sont repris en écho sur la ligne de commande.

Pour rendre une entrée plus lisible, vous pouvez échapper les guillemets pour une expression entière. Au début de l'expression, vous entrez la séquence d'échappement « q » plus l'un des caractères spéciaux suivants :/{<	~$^+=&%@‘ ?.

Vous n'entrez que le caractère spécial à la fin de l'expression, comme suit :

```
q@http.req.url.contains("sometext") && http.req.cookie.exists@

q~http.req.url.contains("sometext") && http.req.cookie.exists~
<!--NeedCopy-->
```

Notez qu'une expression qui utilise le délimiteur {est fermée par}.

Pour certaines fonctionnalités (par exemple, Integrated Caching and Responder), la boîte de dialogue de configuration de stratégie fournit une boîte de dialogue secondaire pour configurer les expressions. Cette boîte de dialogue vous permet de choisir parmi des listes déroulantes qui affichent les choix disponibles à chaque étape de la configuration de l'expression. Vous ne pouvez pas utiliser d'opérateurs arithmétiques lorsque vous utilisez ces boîtes de dialogue de configuration, mais la plupart des autres fonctionnalités avancées d'expression de stratégie sont disponibles. Pour utiliser des opérateurs arithmétiques, écrivez vos expressions au format libre.

Configurer une règle de syntaxe de stratégie avancée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une règle de stratégie avancée et vérifier la configuration :

1. `add cache|dns|rewrite|cs policyName **-rule** expression featureSpecificParameter **-action**`
2. `show cache|dns|rewrite|cs policyName`
   Voici un exemple de configuration d'une stratégie de mise en cache :

   Exemple :

```
> add cache policy pol-cache -rule http.req.content_length.le(5) -
    action INVAL
 Done

> show cache policy pol-cache
        Name: pol-cache
```



```
        Rule: http.req.content_length.le(5)
        CacheAction: INVAL
        Invalidate groups: DEFAULT
        UndefAction: Use Global
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```

Configurer une expression de stratégie avancée à l'aide de l'interface graphique

1. Dans le volet de navigation, cliquez sur le nom de l'entité pour laquelle vous souhaitez configurer une stratégie. Par exemple, vous pouvez sélectionner Mise en cache intégrée, Répondeur, DNS, Réécriture ou Changement de contenu, puis cliquez sur **Stratégies**.
2. Cliquez sur Ajouter.
3. Pour la plupart des fonctionnalités, cliquez sur dans le champ **Expression** . Pour le changement de contenu, cliquez sur **Configurer**.
4. Cliquez sur l'icône **Préfixe** (la maison) et sélectionnez le premier préfixe d'expression dans la liste déroulante. Par exemple, dans Responder, les options sont HTTP, SYS et CLIENT. Le prochain ensemble d'options applicables apparaît dans une liste déroulante.
5. Double-cliquez sur l'option suivante pour la sélectionner, puis tapez un point (.). Encore une fois, un ensemble d'options applicables apparaît dans une autre liste déroulante.
6. Continuez à sélectionner les options jusqu'à ce qu'un champ de saisie (signalé par des parenthèses) apparaisse. Lorsque vous voyez un champ de saisie, saisissez une valeur appropriée entre parenthèses. Par exemple, si vous sélectionnez GT (int) (format entier supérieur à), vous spécifiez un entier entre parenthèses. Les chaînes de texte sont délimitées par des guillemets. Voici un exemple :

   ```
   HTTP.REQ.BODY(1000).BETWEEN("this","that")
   ```

7. Pour insérer un opérateur entre deux parties d'une expression composée, cliquez sur l'icône Opérateurs (le sigma), puis sélectionnez le type d'opérateur. Voici un exemple d'expression configurée avec un OR booléen (signalé par des barres verticales doubles, ||) :

   ```
   HTTP.REQ.URL.EQ("www.mycompany.com")||HTTP.REQ.BODY(1000).BETWEEN("this
   ","that")
   ```

8. Pour insérer une expression nommée, cliquez sur la flèche vers le bas en regard de l'icône Ajouter (signe plus) et sélectionnez une expression nommée.

9. Pour configurer une expression à l'aide de menus déroulants et insérer des expressions intégrées, cliquez sur l'icône Ajouter (signe plus). La boîte de dialogue **Ajouter une expression** fonctionne de la même manière que la boîte de dialogue principale, mais elle fournit des listes déroulantes pour sélectionner des options et des champs de texte pour la saisie des données au lieu de parenthèses. Cette boîte de dialogue fournit également une liste déroulante Expressions fréquemment utilisées qui insère les expressions couramment utilisées. Lorsque vous avez terminé d'ajouter l'expression, cliquez sur **OK**.
10. Lorsque vous avez terminé, cliquez sur **Créer**. Un message dans la barre d'état indique que l'expression de stratégie est correctement configurée.

Test d'une expression de stratégie avancée à l'aide de l'interface graphique

1. Dans le volet de navigation, cliquez sur le nom de la fonctionnalité pour laquelle vous souhaitez configurer une stratégie (par exemple, vous pouvez sélectionner Mise en cache intégrée, Répondeur, DNS, Réécriture ou Changement de contenu), puis cliquez sur Stratégies.
2. Sélectionnez une stratégie, puis cliquez sur **Ouvrir**.
3. Pour tester l'expression, cliquez sur l'icône Evaluer (coche).
4. Dans la boîte de dialogue de l'évaluateur d'expression, sélectionnez le type de flux correspondant à l'expression.
5. Dans le champ **Données de demande HTTP** ou **Données de réponse HTTP**, collez la demande ou la réponse HTTP que vous souhaitez analyser avec l'expression, puis cliquez sur **Evaluer**. Notez que vous devez fournir une requête ou une réponse HTTP complète, et que l'en-tête et le corps doivent être séparés par une ligne vide. Certains programmes qui traquent les en-têtes HTTP ne traquent pas non plus la réponse. Si vous copiez et collez uniquement l'en-tête, insérez une ligne vide à la fin de l'en-tête pour former une requête ou une réponse HTTP complète.
6. Cliquez sur **Fermer** pour fermer cette boîte de dialogue.

Configuration des expressions de stratégie avancées nommées

October 5, 2021

Au lieu de retaper la même expression plusieurs fois dans plusieurs stratégies, vous pouvez configurer une expression nommée et faire référence au nom chaque fois que vous souhaitez utiliser l'expression dans une stratégie. Par exemple, vous pouvez créer les expressions nommées suivantes :

- Cette expression :

  ```
  http.req.body(100).contains("this")
  ```

- Cette expression :


```
http.req.body(100).contains("that")
```

Vous pouvez ensuite utiliser ces expressions nommées dans une expression de stratégie. Par exemple, voici une expression juridique basée sur les exemples précédents :

Cette expression	Cette expression

Vous pouvez utiliser le nom d'une expression de stratégie avancée comme préfixe d'une fonction. L'expression nommée peut être une expression simple ou une expression composée. La fonction doit être capable d'opérer sur le type de données renvoyé par l'expression nommée.

Exemple 1 : expression nommée simple en tant que préfixe

L'expression nommée simple suivante, qui identifie une chaîne de texte, peut être utilisée comme préfixe de la <string>fonction AFTER_STR (» «), qui fonctionne avec des données de texte :

```
HTTP.REQ.BODY(1000)
```

Si le nom de l'expression est Top1Ko, vous pouvez utiliser Top1KB.after_str (« username ») au lieu de HTTP.REQ.BODY (1000) .AFTER_STR (« username »).

Exemple 2 : expression nommée composée en tant que préfixe

Vous pouvez créer une expression nommée composée appelée basic_header_value pour concaténer le nom d'utilisateur dans une requête, un signe deux-points (:) et le mot de passe de l'utilisateur, comme suit :

```
add policy expression basic_header_value "HTTP.REQ.USER.NAME + \":\" + HTTP
.REQ.USER.PASSWD"
```

Vous pouvez ensuite utiliser le nom de l'expression dans une action de réécriture, comme illustré dans l'exemple suivant :

```
add rewrite action insert_b64encoded_authorization insert_http_header
authorization '"Basic " + basic_header_value.b64encode'
```

Dans cet exemple, dans l'expression utilisée pour construire la valeur de l'en-tête personnalisé, l'algorithme de codage B64 est appliqué à la chaîne renvoyée par l'expression nommée composée.

Vous pouvez également utiliser une expression nommée (seule ou comme préfixe d'une fonction) pour créer l'expression de texte de la cible de remplacement lors d'une réécriture.

Configurez une expression de stratégie avancée nommée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une expression nommée et vérifier la configuration :

```
1 -  add policy expression <name><value>
2
3 -  show policy expression <name>
4 <!--NeedCopy-->
```

Exemple :

```
1 > add policy expression myExp "http.req.body(100).contains("the other")
     "
2 Done
3
4 > show policy expression myExp
5     1)      Name: myExp  Expr: "http.req.body(100).contains("the other"
          )"  Hits: 0 Type : ADVANCED
6 Done
7 <!--NeedCopy-->
```

L'expression peut contenir jusqu'à 1 499 caractères.

Configurer une expression nommée à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **AppExpert**, puis cliquez sur **Expressions**.
2. Cliquez sur **Expressions avancées**.
3. Cliquez sur **Ajouter**.
4. Entrez un nom et une description pour l'expression.
5. Configurez l'expression à l'aide du processus décrit dans Configurer l'expression de stratégie avancée. Un message dans la barre d'état indique que l'expression de stratégie est correctement configurée.

Configurer des expressions de stratégie avancées en dehors du contexte d'une stratégie

August 20, 2021

Un certain nombre de fonctions, notamment les suivantes, peuvent nécessiter une expression de stratégie avancée qui ne fait pas partie d'une stratégie :

- Sélecteurs de mise en cache intégrés :

  Vous définissez plusieurs expressions non composées (sélections) dans la définition du sélecteur. Chaque sélecteur est dans une relation logique implicite ET avec les autres.

- Équilibrage de charge :

  Vous configurez une expression pour la méthode TOKEN d'équilibrage de charge pour un serveur virtuel d'équilibrage de charge.

- Actions de réécriture :

  Les expressions définissent l'emplacement de l'action de réécriture et le type de réécriture à effectuer, selon le type d'action de réécriture que vous configurez. Par exemple, une action DELETE utilise uniquement une expression cible. Une action REPLACE utilise une expression cible et une expression pour configurer le texte de remplacement.

- Stratégies basées sur des taux :

  Vous utilisez des expressions de stratégie avancées pour configurer les sélecteurs de limite. Vous pouvez utiliser ces sélecteurs lors de la configuration de stratégies pour étrangler le débit de trafic vers différents serveurs. Vous définissez jusqu'à cinq expressions non composées (sélections) dans la définition du sélecteur. Chaque sélecteur est dans un ET logique implicite avec les autres.

Configurer une expression de stratégie avancée en dehors d'une stratégie à l'aide de l'interface de ligne de commande (exemple de sélection de cache)

À l'invite de commandes, tapez les commandes suivantes pour configurer une expression de stratégie avancée en dehors d'une stratégie et vérifier la configuration :

```
1 -  add cache selector <selectorName> <rule>
2 -  show cache selector <selectorName>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add cache selector mainpageSelector "http.req.cookie.value("ABC_def")
     "
2     "http.req.url.query.value("_ghi")"selector "mainpageSelector" added
3 Done
4 > show cache selector mainpageSelector
5             Name: mainpageSelector
6             Expressions:
7                     1) http.req.cookie.value("ABC_def")
8                     2) http.req.url.query.value("_ghi")
```



```
Done
<!--NeedCopy-->
```

Voici une commande équivalente qui utilise le délimiteur q le plus lisible, comme décrit dans Configurer les expressions de stratégie avancées dans une stratégie :

```
> add cache selector mainpageSelector2 q~http.req.cookie.value("ABC_def
    ")~
    q~http.req.url.query.value("_ghi")~selector "mainpageSelector2"
       added
Done
> show cache selector mainpageSelector2
            Name: mainpageSelector2
            Expressions:
                    1) http.req.cookie.value("ABC_def")
                    2) http.req.url.query.value("_ghi")
Done
<!--NeedCopy-->
```

Expressions de stratégie avancées : évaluation du texte

January 21, 2021

Vous pouvez configurer une stratégie avec une expression de stratégie avancée qui évalue le texte d'une demande ou d'une réponse. Les expressions de texte de stratégie avancées peuvent aller des expressions simples qui effectuent la correspondance de chaînes dans les en-têtes HTTP aux expressions complexes qui encodent et décodent du texte. Vous pouvez configurer les expressions de texte pour qu'elles respectent la casse ou la casse et utiliser ou ignorer les espaces. Vous pouvez également configurer des expressions de texte complexes en combinant des expressions de texte avec des opérateurs booléens

Vous pouvez utiliser des préfixes d'expression et des opérateurs pour évaluer les requêtes HTTP, les réponses HTTP et les données VPN et VPN sans client. Toutefois, les préfixes d'expression de texte ne se limitent pas à évaluer ces éléments de votre trafic.

À propos des expressions de texte

May 5, 2023

Vous pouvez configurer différentes expressions pour travailler avec du texte qui circule dans l'appliance NetScaler. Voici quelques exemples de la façon dont vous pouvez analyser du texte à l'aide d'une expression de stratégie avancée :

- Déterminez qu'il existe un en-tête HTTP particulier.

  Par exemple, vous pouvez souhaiter identifier les requêtes HTTP qui contiennent un en-tête Accept-Language particulier afin de diriger la demande vers un serveur particulier.

- Déterminez qu'une URL HTTP particulière contient une chaîne particulière.

  Par exemple, vous pouvez souhaiter bloquer les demandes pour des URL particulières. Notez que la chaîne peut apparaître au début, au milieu ou à la fin d'une autre chaîne.

- Identifiez une demande POST qui est dirigée vers une application particulière.

  Par exemple, vous pouvez souhaiter identifier toutes les demandes POST qui sont dirigées vers une application de base de données dans le but d'actualiser les données d'application mises en cache.

Notez qu'il existe des outils spécialisés permettant de visualiser le flux de données des requêtes et réponses HTTP. Vous pouvez utiliser les outils pour afficher le flux de données.

À propos des opérations sur le texte

Une expression textuelle consiste en au moins un préfixe pour identifier un élément de données et généralement (mais pas toujours) une opération sur ce préfixe. Les opérations textuelles peuvent s'appliquer à n'importe quelle partie d'une demande ou d'une réponse. Les opérations de base sur le texte incluent différents types de correspondances de chaînes.

Par exemple, l'expression suivante compare une valeur d'en-tête à une chaîne :

```
http.req.header("myHeader").contains("some-text")
```

Les expressions suivantes sont des exemples de mise en correspondance d'un type de fichier dans une demande :

```
http.req.url.suffix.contains("jpeg")
```

```
http.req.url.suffix.eq("jpeg")
```

Dans les exemples précédents, l'opérateur contains autorise une correspondance partielle et l'opérateur eq recherche une correspondance exacte.

D'autres opérations sont disponibles pour formater la chaîne avant de l'évaluer. Par exemple, vous pouvez utiliser des opérations de texte pour supprimer les guillemets et les espaces blancs, pour convertir la chaîne en minuscules ou pour concaténer des chaînes.

> **Remarque** : Des opérations
>
> complexes sont disponibles pour effectuer des correspondances basées sur des motifs ou pour convertir un type de format de texte en un autre type.

Pour plus d'informations, consultez les rubriques suivantes :

- Jeux de modèles et jeux de données.
- Expressions régulières.
- Données de typographie.

Compilation et priorité dans les expressions de texte

Vous pouvez appliquer différents opérateurs pour combiner des préfixes de texte ou des expressions. Par exemple, l'expression suivante concatène les valeurs renvoyées pour chaque préfixe :

```
http.req.hostname + http.req.url
```

Voici un exemple d'expression de texte composé qui utilise un AND logique. Les deux composants de cette expression doivent avoir la valeur TRUE pour qu'une requête corresponde à l'expression :

```
http.req.method.eq(post)&& http.req.body(1024).startswith("destination=")
```

> **Remarque :**
>
> Pour plus d'informations sur les opérateurs de composition, voir Expressions avancées composées.

Catégories d'expressions de texte

Les principales catégories d'expressions de texte que vous pouvez configurer sont les suivantes :

- Informations dans les en-têtes HTTP, les URL HTTP et le corps POST dans les requêtes HTTP.

  Pour plus d'informations, voir Préfixes d'expression pour le texte dans les requêtes et réponses HTTP.

- Informations concernant un VPN ou un VPN sans client.

  Pour plus d'informations, consultez Préfixes d'expression pour les VPN et les VPN sans client.

- Informations sur la charge utile TCP.

  Pour plus d'informations sur les expressions de charge utile TCP, voir Expressions de stratégie avancées : analyse des données HTTP, TCP et UDP.

- Texte dans un certificat SSL (Secure Sockets Layer).

Pour plus d'informations sur les expressions de texte pour les données de certificat SSL et SSL, voir Expressions de stratégie avancées : Analyse des certificats SSL et Expressions pour les dates de certificat SSL.

> **Remarque :**
>
> L'analyse d'un corps de document, tel que le corps d'une requête POST, peut affecter les performances. Vous pouvez tester l'impact sur les performances des stratégies qui évaluent le corps d'un document.

Instructions relatives aux expressions de texte

Du point de vue des performances, il est généralement préférable d'utiliser des fonctions prenant en charge le protocole dans une expression. Par exemple, l'expression suivante utilise une fonction prenant en charge le protocole :

```
HTTP.REQ.URL.QUERY
```

L'expression précédente fonctionne mieux que l'expression équivalente suivante, qui est basée sur l'analyse de chaînes :

```
HTTP.REQ.URL.AFTER_STR("?")
```

Dans le premier cas, l'expression se penche spécifiquement sur la requête URL. Dans le second cas, l'expression analyse les données à la recherche de la première occurrence d'un point d'interrogation.

Il y a également un avantage de performance de l'analyse structurée du texte, comme dans l'expression suivante :

```
HTTP.REQ.HEADER("Example").TYPECAST_LIST_T(',').GET(1)
```

(Pour plus d'informations sur la typographie, voir Données de typographie. L'expression de typecasting, qui recueille des données délimitées par des virgules et les structure en une liste, fonctionnerait généralement mieux que l'équivalent non structuré suivant :

```
HTTP.REQ.HEADER("Example").AFTER_STR(",").BEFORE_STR(",")
```

Enfin, les expressions textuelles non structurées présentent généralement de meilleures performances que les expressions régulières. Par exemple, voici une expression de texte non structurée :

```
HTTP.REQ.HEADER("Example").AFTER_STR("more")
```

L'expression précédente fournirait généralement de meilleures performances que l'équivalent suivant, qui utilise une expression régulière :

```
HTTP.REQ.HEADER("Example").AFTER_REGEX(re/more/)
```

Pour plus d'informations sur les expressions régulières, voir Expressions régulières.

Préfixes d'expression pour le texte dans les requêtes et les réponses HTTP

May 5, 2023

Une requête ou une réponse HTTP contient généralement du texte, par exemple sous la forme d'en-têtes, de valeurs d'en-tête, d'URL et de corps de texte POST. Vous pouvez configurer des expressions pour qu'elles fonctionnent sur un ou plusieurs de ces éléments textuels dans une requête ou une réponse HTTP.

Pour plus d'informations sur les paramètres, consultez NetScaler Advanced Policy Expression Reference.

Reportez-vous aux rubriques suivantes pour obtenir plus de détails sur la configuration à l'aide de l'expression avancée.

- Expressions de stratégie avancées composées
- Expressions de stratégie avancées : adresses IP et MAC, débit, ID VLAN
- Expressions de stratégie avancées : analyse SSL
- Expressions de stratégie avancées : utilisation des dates, des heures et des nombres
- Éléments de base d'une expression de stratégie avancée
- Expressions de stratégie avancées : évaluation de texte
- Expressions de stratégie avancées : analyse des données HTTP, TCP et UDP
- Exemples récapitulatifs d'expressions de syntaxe et de stratégies par défaut

Préfixes d'expression pour les VPN et les VPN sans client

August 20, 2021

Le moteur de stratégie avancé fournit des préfixes spécifiques à l'analyse des données VPN ou VPN sans client. Ces données comprennent les éléments suivants :

- Noms d'hôte, domaines et URL dans le trafic VPN.
- Protocoles dans le trafic VPN.
- Requêtes dans le trafic VPN.

Ces éléments de texte sont souvent des URL et des composants d'URL. En plus d'appliquer les opérations textuelles sur ces éléments, vous pouvez analyser ces éléments à l'aide d'opérations spécifiques à l'analyse des URL. Pour plus d'informations, voir Expressions pour extraire des segments d'URL.

Pour plus d'informations sur les préfixes d'expression VPN, reportez-vous au tableau des expressions VPN.

Opérations de base sur le texte

October 5, 2021

Les opérations de base sur le texte incluent les opérations de correspondance de chaînes, de calcul de la longueur d'une chaîne et de contrôle de la sensibilité à la casse. Vous pouvez inclure des espaces blancs dans une chaîne passée en tant qu'argument à une expression, mais la chaîne ne peut pas dépasser 255 caractères.

Fonctions de comparaison de chaînes

Le tableau suivant répertorie les opérations de correspondance de chaînes de base dans lesquelles les fonctions renvoient une valeur booléenne TRUE ou FALSE.

Fonction	Description
`<text>.CONTAINS(<string>)`	Renvoie une valeur booléenne TRUE si la cible contient `<string>`. Exemple : `http.req.url.contains(".jpeg")`
`<text>.EQ(<string>)`	Renvoie une valeur booléenne TRUE si la cible correspond exactement à `<string>`. Par exemple, l'expression suivante renvoie une valeur booléenne TRUE pour une URL dont le nom d'hôte est « myhostabc » : `http.req.url.hostname.eq("myhostabc")`
`<text>.STARTSWITH(<string>)`	Renvoie une valeur booléenne TRUE si la cible commence par `<string>`. Par exemple, l'expression suivante renvoie une valeur booléenne TRUE pour une URL dont le nom d'hôte est « myhostabc » : `http.req.url.hostname.startswith("myhost")`
`<text>.ENDSWITH(<string>)`	Renvoie une valeur booléenne TRUE si la cible se termine par<string>. Par exemple, l'expression suivante renvoie une valeur booléenne TRUE pour une URL dont le nom d'hôte est « myhostabc » : `http.req.url.hostname.endswith("abc")`

Fonction	Description
`<text>.NE(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe n'est pas égal à l'argument de chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)or SET_TEXT_MODE(NOIGNORECASE)` et avec les jeux de caractères ASCII et UTF-8.
`<text>.GT(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe est alphabétiquement supérieur à l'argument de chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)` ou `SET_TEXT_MODE(NOIGNORECASE)`, et avec les jeux de caractères ASCII et UTF-8.
`<text>.GE(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe est alphabétiquement supérieur ou égal à l'argument de chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)` ou `SET_TEXT_MODE(NOIGNORECASE)`, et avec les jeux de caractères ASCII et UTF-8.

Fonction	Description
`<text>.LT(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe est alphabétiquement inférieur à l'argument chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)` ou `SET_TEXT_MODE(NOIGNORECASE)`, et avec les jeux de caractères ASCII et UTF-8.
`<text>.LE(<string>)`	Renvoie une valeur booléenne TRUE si le préfixe est alphabétiquement inférieur ou égal à l'argument chaîne. Si le préfixe renvoie une valeur qui n'est pas une chaîne, l'argument de la fonction est comparé à la représentation sous forme de chaîne de la valeur renvoyée par le préfixe. Vous pouvez utiliser les fonctions avec `SET_TEXT_MODE(IGNORECASE)` ou `SET_TEXT_MODE(NOIGNORECASE)`, et avec les jeux de caractères ASCII et UTF-8.

Calculer la longueur d'une chaîne

L' `<text>.LENGTH` opération renvoie une valeur numérique égale au nombre de caractères (et non d'octets) d'une chaîne :

```
<text>.LENGTH
```

Par exemple, vous pouvez souhaiter identifier les URL de demande qui dépassent une longueur particulière. Voici une expression qui implémente cet exemple :

```
HTTP.REQ.URL.LENGTH < 500
```

Après avoir compté les caractères ou les éléments d'une chaîne, vous pouvez leur appliquer des opérations numériques. Pour plus d'informations, consultez Expressions de stratégie avancées : utilisation des dates, des heures et des nombres.

Considérez, ignorez et modifiez la casse du texte

Les fonctions suivantes fonctionnent sur la casse (majuscule ou minuscule) des caractères de la chaîne.

Fonction	Description	
`<text>.SET_TEXT_MODE` (IGNORECASE	NOIGNORECASE)	Cette fonction active ou désactive la sensibilité à la casse pour toutes les opérations de texte.
`<text>.TO_LOWER`	Convertit la cible en minuscules pour un bloc de texte d'une taille maximale de 2 kilo-octets (Ko). Renvoie UNDEF si la cible dépasse 2 Ko. Par exemple, la chaîne « abCD : » est convertie en « abcd : » .	
`<text>.TO_UPPER`	Convertit la cible en majuscules. Renvoie UNDEF si la cible dépasse 2 Ko. Par exemple, la chaîne « AbCD : » est convertie en « ABCD : » .	

Dépouille des caractères spécifiques d'une chaîne

Vous pouvez utiliser la fonction STRIP_CHARS (`<string>`) pour supprimer des caractères spécifiques du texte renvoyé par un préfixe d'expression de stratégie avancée (la chaîne d'entrée). Toutes les instances des caractères spécifiés dans l'argument sont retirées de la chaîne d'entrée. Vous pouvez utiliser n'importe quelle méthode de texte sur la chaîne résultante, y compris les méthodes utilisées pour faire correspondre la chaîne à un jeu de motifs.

Par exemple, dans l'expression `CLIENT.UDP.DNS.DOMAIN.STRIP\\_CHARS(".-\\_")`, la fonction `STRIP\\_CHARS(<string>)` supprime tous les points (.), tirets (-) et traits de soulignement (_) du nom de domaine renvoyé par le préfixe CLIENT.UDP.DNS.DOMAIN. Si le nom de domaine renvoyé est « a.dom_ai_n-name », la fonction renvoie la chaîne « adomainname ».

Dans l'exemple suivant, la chaîne résultante est comparée à un jeu de motifs appelé « listofdomains » :

```
CLIENT.UDP.DNS.DOMAIN.STRIP_CHARS(".-_").CONTAINS_ANY("listofdomains")
```


Remarque : Vous ne pouvez pas effectuer de réécriture sur la chaîne renvoyée par la fonction `STRIP_CHARS(<string>)`.

Les fonctions suivantes enlève les caractères correspondants du début et de la fin d'une entrée de chaîne donnée.

Fonction	Description
`<text>.STRIP_START_CHARS(s)`	Enlève les caractères correspondants depuis le début de la chaîne d'entrée jusqu'à ce que le premier caractère non concordant soit trouvé et renvoie le reste de la chaîne. Vous devez spécifier les caractères que vous souhaitez supprimer sous la forme d'une chaîne unique entre guillemets. Par exemple, si le nom d'un en-tête est TestLang et que :*/en_us:est sa valeur, HTTP.RES.HEADER (« TestLang ») .STRIP_START_CHARS (« : «*) supprime les caractères spécifiés depuis le début de la valeur de l'en-tête jusqu'à ce que le premier caractère non correspondant e soit trouvé et renvoie sen_us : sous la forme d'un chaîne.
`<text>`.STRIP_END_CHARS(s)	Enlève les caractères correspondants depuis la fin de la chaîne d'entrée jusqu'au premier caractère non correspondant est trouvé et renvoie le reste de la chaîne. Vous devez spécifier les caractères que vous souhaitez supprimer sous la forme d'une chaîne unique entre guillemets. Par exemple, si le nom d'un en-tête est TestLang et que :*/en_us:is its value,HTTP.RES.HEADER("TestLang").STRIP_START_CHARS(":")* supprime les caractères spécifiés à partir de la fin de la valeur de l'en-tête jusqu'à ce que le premier caractère non correspondant s soit trouvé et renvoie : /_en_us sous forme de chaîne.

Ajouter une chaîne à une autre chaîne

Vous pouvez utiliser la fonction APPEND () pour ajouter la représentation sous forme de chaîne de l'argument à la représentation sous forme de chaîne de la valeur renvoyée par la fonction précédente. La fonction précédente peut être une fonction qui renvoie un nombre, un long non signé, un double, une valeur temporelle, une adresse IPv4 ou une adresse IPv6. L'argument peut être une chaîne de texte, un nombre, un long non signé, un double, une valeur temporelle, une adresse IPv4 ou une adresse IPv6. La valeur de chaîne résultante est la même valeur de chaîne que celle obtenue à l'aide de l'opérateur +.

Opérations complexes sur le texte

May 5, 2023

En plus de la simple correspondance de chaînes, vous pouvez configurer des expressions qui examinent la longueur des chaînes et les blocs de texte à la recherche de motifs plutôt que de chaînes spécifiques.

Pour toute opération basée sur du texte, prenez en compte les points suivants :

- Pour toute opération qui prend un argument de chaîne, la chaîne ne peut pas dépasser 255 caractères.
- Vous pouvez inclure des espaces blancs lorsque vous spécifiez une chaîne dans une expression.

Opérations sur la longueur d'une chaîne

Les opérations suivantes extraient les chaînes en fonction du nombre de caractères.

Opération de nombre de caractères	Description
`<text>.TRUNCATE(<count>)`	Renvoie une chaîne après avoir tronqué la fin de la cible du nombre de caractères dans `<count>`. Si la chaîne entière est plus courte que `<count>`, rien n'est renvoyé.
`<text>.TRUNCATE(<character>, <count>)`	Renvoie une chaîne après avoir tronqué le texte après `<character>` du nombre de caractères spécifié dans `<count>`.
`<text>.PREFIX(<character>, <count>)`	Sélectionne le préfixe le plus long de la cible dont le nombre d' `<count>` occurrences est le plus long `<character>`.

Opération de nombre de caractères	Description
<text>.SUFFIX(<character>, <count>)	Sélectionne le suffixe le plus long de la cible dont le nombre d' <count> occurrences est le plus long <character>. Par exemple, considérez le corps de réponse suivant : peninsula. L'expression suivante renvoie la valeur de sula: http.res.body(100).suffix('n',0). L'expression suivante renvoie insula: http.res.body(100).suffix('n',1). L'expression suivante renvoie la valeur de peninsula: http.res.body(100).suffix('n',2). L'expression suivante renvoie la valeur de peninsula: http.res.body(100).suffix('n',3).
<text>.SUBSTR(<starting_offset>, <length>)	Sélectionnez une chaîne contenant <length>le nombre de caractères de l'objet cible. Commencez à extraire la chaîne après le <starting_offset>. Si le nombre de caractères après le décalage est inférieur à la valeur de l'argument <length>, sélectionnez tous les caractères restants.
<text>.SKIP(<character>, <count>)	Sélectionnez une chaîne dans la cible après avoir ignoré le préfixe le plus long qui a au moins <count> occurrences de <character>.

Opérations sur une partie d'une chaîne

Reportez-vous à la table Opérations de chaîne pour savoir comment extraire un sous-ensemble d'une chaîne plus grande à l'aide de l'une des opérations.

Opérations de comparaison de l'ordre alphanumérique de deux chaînes

L'opération COMPARE examine le premier caractère non concordant de deux chaînes différentes. Cette opération est basée sur l'ordre lexicographique, qui est la méthode utilisée pour trier les termes dans les dictionnaires.

Cette opération renvoie la différence arithmétique entre les valeurs ASCII des premiers caractères non concordants des chaînes comparées. Les différences suivantes sont des exemples :

- La différence entre « abc » et « and » est de -1 (basé sur la troisième comparaison de caractères par paire).
- La différence entre « @ » et « abc » est de -33.
- La différence entre « 1 » et « abc » est de -47.

Voici la syntaxe de l'opération COMPARE.

```
<text>.COMPARE(<string>)
```

Extraire un entier d'une chaîne d'octets représentant du texte

Reportez-vous à la table d'extraction Integer pour savoir comment traiter une chaîne d'octets représentant du texte comme une séquence d'octets, extraire 8 bits, 16 bits ou 32 bits de la séquence, puis convertir les bits extraits en entier.

Convertir le texte en une valeur de hachage

Vous pouvez convertir une chaîne de texte en valeur de hachage à l'aide de la fonction HASH. Cette fonction renvoie un entier positif de 31 bits à la suite de l'opération. Voici le format de l'expression :

```
<text>.HASH
```

Cette fonction ne tient pas compte de la casse et des espaces blancs. Par exemple, après l'opération, les deux chaînes Ab c et a bc produiraient la même valeur de hachage.

Encodez et décodez du texte en appliquant l'algorithme de codage Base64

Les deux fonctions suivantes encodent et décodent une chaîne de texte en appliquant l'algorithme de codage Base64.

Fonction	Description
text.B64ENCODE	Encode la chaîne de texte (désignée par texte) en appliquant l'algorithme de codage Base64.
text.B64DECODE	Décode la chaîne codée en Base64 (désignée par du texte) en appliquant l'algorithme de décodage Base64. L'opération déclenche un UNDEF si le texte n'est pas au format B64.

Affinez la recherche dans une action de réécriture à l'aide de la fonction EXTEND

La fonction EXTEND est utilisée dans les actions de réécriture qui spécifient des motifs ou des jeux de motifs et ciblent le corps des paquets HTTP. Lorsqu'une correspondance de motif est trouvée, la fonction EXTEND étend la portée de la recherche d'un nombre prédéfini d'octets des deux côtés de la chaîne correspondante. Une expression régulière peut ensuite être utilisée pour effectuer une réécriture sur les correspondances dans cette région étendue. Les actions de réécriture configurées avec la fonction EXTEND effectuent des réécritures plus rapidement que les actions de réécriture qui évaluent des corps HTTP entiers à l'aide d'expressions régulières uniquement.

Le format de la fonction EXTEND est EXTEND (m, n), où m et n sont le nombre d'octets par lesquels la portée de la recherche est étendue avant et après le motif correspondant, respectivement. Lorsqu'une correspondance est trouvée, la nouvelle portée de recherche comprend m octets qui précèdent immédiatement la chaîne correspondante, la chaîne elle-même et les n octets qui suivent la chaîne. Une expression régulière peut ensuite être utilisée pour effectuer une réécriture sur une partie de cette nouvelle chaîne.

La fonction EXTEND ne peut être utilisée que si l'action de réécriture dans laquelle elle est utilisée remplit les conditions suivantes :

- La recherche est effectuée à l'aide de motifs ou de jeux de motifs (et non d'expressions régulières)
- L'action de réécriture évalue uniquement le corps des paquets HTTP.

De plus, la fonction EXTEND ne peut être utilisée qu'avec les types d'actions de réécriture suivants :

- replace_all
- insert_after_all
- delete_all
- insert_before_all

Par exemple, vous voudrez peut-être supprimer toutes les instances de http://exampleurl.com/ et http://exampleurl.au/ dans les 1000 premiers octets du corps. Pour ce faire, vous pouvez configurer une action de réécriture pour rechercher toutes les instances de la chaîne exampleurl, étendre la portée de la recherche des deux côtés de la chaîne lorsqu'une correspondance est trouvée, puis utiliser une expression régulière pour effectuer la réécriture dans la région étendue. L'exemple suivant étend la portée de la recherche de 20 octets à gauche et de 50 octets à droite de la chaîne correspondante :

```
add rewrite action delurl_example delete_all 'HTTP.REQ.BODY(1000)'-search
exampleurl -refineSearch 'extend(20,50).regex_select(re##http://exampleurl
.(com|au)##)'
```


Convertir du texte au format hexadécimal

La fonction suivante convertit le texte au format hexadécimal et extrait la chaîne résultante :

```
<text>.BLOB_TO_HEX(<string>)
```

Par exemple, cette fonction convertit la chaîne d'octets « abc » en « 61:62:63 ».

Crypter et déchiffrer du texte

Dans les expressions de stratégie avancées, vous pouvez utiliser les fonctions CRYPTER et DECRYPT pour chiffrer et déchiffrer du texte. Les données chiffrées par la fonction ENCRYPT sur une appliance NetScaler ou une paire haute disponibilité (HA) donnée sont destinées à être déchiffrées par la fonction DECRYPT sur la même appliance NetScaler ou la même paire HA. L'appliance prend en charge les méthodes de cryptage RC4, DES3, AES128, AES192 et AES256. La valeur de clé requise pour le chiffrement n'est pas spécifiable par l'utilisateur. Lorsqu'une méthode de chiffrement est définie, l'appliance génère automatiquement une valeur de clé aléatoire adaptée à la méthode spécifiée. La méthode par défaut est le chiffrement AES256, qui est la méthode de cryptage la plus sécurisée et celle recommandée par Citrix.

Vous n'avez pas besoin de configurer le chiffrement, sauf si vous souhaitez modifier la méthode de chiffrement ou si vous souhaitez que l'appliance génère une nouvelle valeur de clé pour la méthode de chiffrement actuelle.

Remarque : Vous pouvez également chiffrer et déchiffrer des charges utiles XML. Pour plus d'informations sur les fonctions de chiffrement et de déchiffrement des charges utiles XML, consultez Chiffrement et déchiffrement des charges utiles XML.

Configurer le chiffrement

Au démarrage, l'appliance exécute la commande set ns EncryptionParams avec, par défaut, la méthode de cryptage AES256, et utilise une valeur de clé générée aléatoirement qui convient au chiffrement AES256. L'appliance chiffre également la valeur de la clé et enregistre la commande, avec la valeur de la clé cryptée, dans le fichier de configuration NetScaler. Par conséquent, la méthode de cryptage AES256 est activée par défaut pour les fonctions ENCRYPT et DECRYPT. La valeur de clé enregistrée dans le fichier de configuration persiste lors des redémarrages, même si l'appliance exécute la commande chaque fois que vous la redémarrez.

Vous pouvez exécuter la commande set ns EncryptionParams manuellement ou utiliser l'utilitaire de configuration, si vous souhaitez modifier la méthode de chiffrement ou si vous souhaitez que l'appliance génère une nouvelle valeur de clé pour la méthode de chiffrement actuelle. Pour utiliser l'interface de ligne de commande pour modifier la méthode de chiffrement, définissez uniquement le paramètre de méthode, comme indiqué dans « **Exemple 1 : Modification de la méthode de chiffrement** ». Si vous souhaitez que l'appliance génère une nouvelle valeur de clé pour la méthode de

chiffrement actuelle, définissez le paramètre de méthode sur la méthode de chiffrement actuelle et le paramètre KeyValue sur une chaîne vide (« »), comme indiqué dans « **Exemple 2 : Génération d'une nouvelle valeur de clé pour la méthode de chiffrement actuelle**. » Après avoir généré une nouvelle valeur de clé, vous devez enregistrer la configuration. Si vous n'enregistrez pas la configuration, l'appliance utilise la valeur de clé nouvellement générée uniquement jusqu'au prochain redémarrage, après quoi elle revient à la valeur de clé dans la configuration enregistrée.

Configurer le chiffrement à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans la zone **Paramètres**, cliquez sur **Modifier les paramètres de chiffrement** .
3. Dans la boîte de dialogue **Modifier les paramètres de chiffrement**, effectuez l'une des opérations suivantes :
   - Pour modifier la méthode de chiffrement, dans la liste Méthode, sélectionnez la méthode de chiffrement souhaitée.
   - Pour générer une nouvelle valeur de clé pour la méthode de chiffrement actuelle, cliquez sur Générer une nouvelle clé pour la méthode sélectionnée.
4. Cliquez sur **OK**.

Utilisez les fonctions ENCRYPT et DECRYPT

Vous pouvez utiliser les fonctions ENCRYPT et DECRYPT avec n'importe quel préfixe d'expression qui renvoie du texte. Par exemple, vous pouvez utiliser les fonctions CRYPTER et DECRYPT dans les stratégies de réécriture pour le chiffrement des cookie. Dans l'exemple suivant, les actions de réécriture chiffrent un cookie nommé MyCookie, qui est défini par un service principal, et décryptent le même cookie lorsqu'il est renvoyé par un client :

```
1 add rewrite action my-cookie-encrypt-action replace "HTTP.RES.
     SET_COOKIE.COOKIE("MyCookie").VALUE(0)" "HTTP.RES.SET_COOKIE.COOKIE(
     "MyCookie").VALUE(0).ENCRYPT"
2
3 add rewrite action my-cookie-decrypt-action replace "HTTP.REQ.COOKIE.
     VALUE("MyCookie")" "HTTP.REQ.COOKIE.VALUE("MyCookie").DECRYPT"
4 <!--NeedCopy-->
```

Après avoir configuré les stratégies de chiffrement et de déchiffrement, enregistrez la configuration pour que les stratégies entrent en vigueur.

Configuration de la clé de chiffrement pour le chiffrement

Dans les expressions de stratégie avancées, vous pouvez utiliser les fonctions CRYPTER et DECRYPT pour chiffrer et déchiffrer le texte d'une demande ou d'une réponse. Les données chiffrées par la

fonction ENCRYPT sur une appliance (autonome, haute disponibilité ou cluster) sont destinées à être déchiffrées par la fonction DECRYPT par la même appliance. L'appliance prend en charge les méthodes de cryptage RC4, DES, Triple-DES, AES92 et AES256 et chacune de ces méthodes utilise une clé secrète pour le chiffrement et le déchiffrement des données. Vous pouvez utiliser l'une de ces méthodes pour chiffrer et déchiffrer les données de deux manières : l'autochiffrement et le cryptage tiers.

La fonctionnalité d'auto-chiffrement d'une appliance (autonome, haute disponibilité ou cluster) chiffre puis déchiffre les données en évaluant la valeur de l'en-tête. Un exemple pour comprendre cela est le cryptage des cookies HTTP. L'expression évalue l'en-tête, chiffre la valeur du cookie HTTP dans l'en-tête Set-Cookie dans la réponse sortante, puis déchiffre la valeur du cookie lorsqu'elle est renvoyée dans l'en-tête du cookie d'une demande entrante ultérieure du client. La valeur de la clé n'est pas configurable par l'utilisateur. En revanche, lorsqu'une méthode de chiffrement est configurée dans la commande set ns EncryptionParams, l'appliance génère automatiquement une valeur de clé aléatoire pour la méthode configurée. Par défaut, la commande utilise la méthode de cryptage AES256, qui est la méthode hautement sécurisée, et Citrix recommande cette méthode.

La fonctionnalité de chiffrement tiers chiffre ou déchiffre les données avec une application tierce. Par exemple, un client peut chiffrer les données d'une demande et l'appliance déchiffre les données avant de les envoyer au serveur principal ou vice versa. Pour ce faire, l'appliance et l'application tierce doivent partager une clé secrète. Sur l'appliance, vous pouvez configurer directement la clé secrète à l'aide d'un objet de clé de chiffrement et la valeur de clé est automatiquement générée par l'appliance pour un chiffrement renforcé. La même clé est configurée manuellement sur l'appliance tierce afin que l'appliance et l'application tierce puissent utiliser la même clé pour chiffrer et déchiffrer les données.

Remarque : En utilisant le chiffrement tiers, vous pouvez également chiffrer et déchiffrer les charges utiles XML. Pour plus d'informations sur les fonctions de chiffrement et de déchiffrement des charges utiles XML, reportez-vous à la section « Cryptage et déchiffrement des charges de traitement XML.

Méthodes de chiffrement

Une méthode de chiffrement fournit deux fonctions : une fonction de chiffrement qui transforme une séquence d'octets de texte brut en une séquence d'octets de texte chiffré, et une fonction de déchiffrement qui transforme le texte chiffré en texte brut. Les méthodes de chiffrement utilisent des séquences d'octets appelées clés pour effectuer le chiffrement et le déchiffrement. Les méthodes de chiffrement qui utilisent la même clé pour le chiffrement et le déchiffrement sont appelées symétriques. Les méthodes de chiffrement qui utilisent des clés différentes pour le chiffrement et le déchiffrement sont asymétriques. Les exemples les plus notables de chiffrement asymétrique se trouvent dans la cryptographie à clé publique, qui utilise une clé publique accessible à tous pour le chiffrement et une clé privée connue uniquement du décrypteur.

Une bonne méthode de chiffrement rend impossible le déchiffrement (« craquer ») du texte chiffré

si vous ne possédez pas la clé. « Infaisable » signifie vraiment que le déchiffrement du texte chiffré prendrait plus de temps et de ressources informatiques qu'il n'en vaut la peine. À mesure que les ordinateurs deviennent plus puissants et moins chers, les chiffrements qui étaient auparavant impossibles à déchiffrer deviennent de plus en plus réalisables. De plus, au fil du temps, des failles se retrouvent dans les méthodes de chiffrement (ou dans leurs implémentations), ce qui facilite le craquage. Les méthodes de chiffrement plus récentes sont donc préférées aux anciennes. En général, les clés de plus grande longueur offrent une meilleure sécurité que les clés plus courtes, au prix de temps de chiffrement et de déchiffrement plus longs.

Une méthode de chiffrement peut utiliser des chiffrements de flux ou des chiffrements par blocs. RC4 est le chiffrement de flux le plus sécurisé et il est utilisé uniquement pour les applications héritées. Les chiffrements par blocs peuvent inclure un remplissage.

Chiffrements de flux

Une méthode de chiffrement de flux fonctionne sur des octets individuels. Un seul chiffrement de flux est disponible sur les appliances NetScaler : RC4, qui utilise une longueur de clé de 128 bits (16 octets). Pour une clé donnée, RC4 génère une séquence pseudo-aléatoire d'octets, appelle un flux de clés, qui est oré X avec le texte brut pour produire le texte chiffré. RC4 n'est plus considéré comme sécurisé et ne doit être utilisé que si les applications héritées l'exigent.

Chiffrements par blocs

Une méthode de chiffrement par blocs fonctionne sur un bloc d'octets fixe. Une appliance NetScaler fournit deux chiffrements par blocs : Data Encryption Standard (DES) et Advanced Encryption Standard (AES). Le DES utilise une taille de bloc de 8 octets et (sur une appliance NetScaler) deux choix de longueur de clé : 64 bits (8 octets), dont 56 bits de données et 8 bits de parité, et Triple-DES, une longueur de clé de 192 bits (24 octets). AES a une taille de bloc de 16 octets et (sur NetScaler) trois choix de longueur de clé : 128 bits (16 octets), 192 bits (24 octets) et 256 bits (32 octets).

Padding

Si le texte brut d'un chiffrement par blocs n'est pas un nombre entier de blocs, un remplissage avec plus d'octets peut être nécessaire. Par exemple, supposons que le texte en clair soit « xyzzy » (hexadécimal 78797a7a79). Pour un bloc Triple-DES de 8 octets, cette valeur doit être complétée pour créer 8 octets. Le schéma de remplissage doit permettre à la fonction de déchiffrement de déterminer la longueur du texte brut original après le déchiffrement. Voici quelques schémas de remplissage actuellement utilisés (n est le nombre d'octets ajoutés) :

- PKCS7 : ajoute n octets de valeur n chacun. Par exemple, 78797a7a79030303. Il s'agit du schéma

de remplissage utilisé par OpenSSL et la fonction de stratégie ENCRYPT(). Le schéma de remplissage PKCS5 est le même que celui de PKCS7.
- ANSI X.923 : Ajoute n-1 zéro octet et un octet final de valeur n. Par exemple, 78797a7a79000003.
- ISO 10126 : Ajoute n-1 octets aléatoires et un octet final de valeur n. Par exemple, 78797a7a79xxxx03, où xx peut être n'importe quelle valeur d'octet. La fonction de stratégie DECRYPT() accepte ce schéma de remplissage, ce qui lui permet également d'accepter les schémas PKCS7 et ANSI X.923.
- ISO/IEC 7816-4 : Ajoute un octet 0x80 et n-1 zéro octet. Par exemple, 78797a7a79800000. C'est aussi ce que l'on appelle le padding OneAndZeros.
- Zéro : ajoute n zéro octet. Exemple : 78797a7a79000000. Cette option ne peut être utilisée qu'avec du texte brut qui n'inclut pas d'octets NUL.

Si le remplissage est utilisé et que le texte en clair est un nombre entier de blocs, un bloc supplémentaire est généralement ajouté afin que la fonction de déchiffrement puisse déterminer sans ambiguïté la longueur du texte brut d'origine. Pour PCKS7 et bloc de 8 octets, il s'agirait de 0808080808080808.

Modes de fonctionnement

Il existe différents modes de fonctionnement pour les chiffrements par blocs, qui spécifient comment plusieurs blocs de texte brut sont chiffrés. Certains modes utilisent un vecteur d'initialisation (IV), un bloc de données en dehors du texte brut utilisé pour démarrer le processus de chiffrement. Il est recommandé d'utiliser un IV différent pour chaque cryptage, de sorte qu'un même texte en clair produise un texte chiffré différent. Le IV n'a pas besoin d'être secret, c'est pourquoi il est ajouté au texte chiffré. Les modes incluent :

- Electronic Codebook (ECB) : Chaque bloc de texte en clair est crypté indépendamment. Aucun IV n'est utilisé. Le remplissage est requis si le texte en clair n'est pas un multiple de la taille du bloc de chiffrement. Le même texte brut et la même clé produisent toujours le même texte chiffré. Pour cette raison, ECB est considéré comme moins sécurisé que les autres modes et ne doit être utilisé que pour les applications héritées.
- Cipher Block Chaining (CBC) : Chaque bloc de texte brut est codé avec le bloc de texte chiffré précédent, ou l'IV du premier bloc, avant d'être chiffré. Le remplissage est requis si le texte en clair n'est pas un multiple de la taille du bloc de chiffrement. Il s'agit du mode utilisé avec la méthode NetScaler EncryptionParams.
- Retour de chiffrement (CFB) : Le bloc de texte chiffré précédent, ou l'IV du premier bloc, est chiffré et la sortie est codée avec le bloc de texte brut actuel pour créer le bloc de texte chiffré actuel. La rétroaction peut être de 1 bit, 8 bits ou 128 bits. Comme le texte en clair est codé avec le texte chiffré, le remplissage n'est pas nécessaire.
- Output Feedback (OFB) : Un flux de clés est généré en appliquant le chiffrement successivement au IV et en codant les blocs de flux de clés avec le texte brut. Le remplissage n'est pas nécessaire.

Configuration des clés de chiffrement pour le chiffrement tiers

Voici les tâches de configuration effectuées lors de la configuration de la clé de chiffrement.

1. Ajout d'une clé de chiffrement. Configure une clé de chiffrement pour une méthode de chiffrement spécifiée avec une valeur de clé spécifiée.
2. Modification d'une clé de chiffrement. Vous pouvez modifier les paramètres d'une clé de chiffrement configurée.
3. Désinstallation d'une clé de chiffrement. Définit les paramètres d'une clé de chiffrement configurée sur leurs valeurs par défaut. Une valeur EncryptionKey portant le nom doit exister. Définit le remplissage sur DEFAULT (déterminé par la méthode), supprime un IV existant, ce qui provoque la génération d'une IV aléatoire par ENCRYPT (). Supprime un commentaire existant. La méthode et la valeur de la clé ne peuvent pas être réinitialisées.
4. Suppression d'une clé de chiffrement. Supprime une clé de chiffrement configurée. La clé ne peut pas comporter de référence.
5. Afficher une clé de chiffrement. Affiche les paramètres de la clé de chiffrement configurée ou de toutes les clés configurées. Si le nom est omis, la valeur de la clé n'est pas affichée.

Ajouter une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ns encryptionKey <name> -method <method> [-keyValue <keyvalue>][-
padding (OFF | ON)] [-iv <hexstring>] -keyValue <keyvalue> [-comment <
string>]
```

Où,

```
1 <method> = ( NONE | RC4 | DES3 | AES128 | AES192 | AES256 | DES | DES-
     CBC | DES-CFB | DES-OFB | DES-ECB | DES3-CBC | DES3-CFB | DES3-OFB |
      DES3-ECB | AES128-CBC | AES128-CFB | AES128-OFB | AES128-ECB |
     AES192-CBC | AES192-CFB | AES192-OFB | AES192-ECB | AES256-CBC |
     AES256-CFB | AES256-OFB | AES256-ECB ) <hexstring> = hex-encoded
     byte sequence
2 <!--NeedCopy-->
```

Les méthodes de chiffrement ci-dessus spécifient le mode de fonctionnement avec CBC comme mode de fonctionnement par défaut. Par conséquent, les méthodes DES, DES2, AES128, AES192 et AES256 sont équivalentes aux méthodes DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC et AES256-CBC.

Modifier une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
set ns encryptionKey <name> [-method <method>] [-keyValue <keyvalue>] [-
padding ( OFF | ON )] [-iv <string>] [-comment <string>]
```

Désinstaller une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
unset ns encryptionKey <name> [-padding] [-iv] [-comment]
```

Supprimer une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm ns encryptionKey <name>
```

Afficher une clé de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

Exemple :

```
1  show ns encryptionKey [<name>]
2
3  add ns encryptionKey my_key -method aes256 -keyValue 26
       ea5537b7e0746089476e5658f9327c0b10c3b4778c673a5b38cee182874711  -iv
       c2bf0b2e15c15004d6b14bcdc7e5e365
4  set ns encryptionKey my_key -keyValue
       b8742b163abcf62d639837bbee3cef9fb5842d82d00dfe6548831d2bd1d93476
5  unset ns encryptionKey my_key -iv
6  rm ns encryptionKey my_key
7  show ns encryptionKey my_key
8  Name: my_key
9  Method: AES256
10 Padding: DEFAULT
11 Key Value: (not disclosed)
12 <!--NeedCopy-->
```

Ajouter une clé de chiffrement à l'aide de l'interface graphique

Accédez à **Système** > **Clés de chiffrement**, puis cliquez sur **Ajouter** pour créer une clé de chiffrement.

Modifier une clé de chiffrement à l'aide de l'interface graphique

Accédez à **Système** > **Clés de chiffrement**, puis cliquez sur **Modifier** pour modifier les paramètres d'une clé de chiffrement configurée.

Supprimer une clé de chiffrement à l'aide de l'interface graphique

Accédez à **Système** > **Clés de chiffrement**, puis cliquez sur **Supprimer**.

Fonctions ENCRYPT et DECRYPT pour le chiffrement tiers

Voici la fonction ENCRYPT utilisée pour le chiffrement tiers.

```
ENCRYPT (encryptionKey, out_encoding)
```

Où,

Les données d'entrée de l'appliance sont le texte à chiffrer

EncryptionKey : paramètre de chaîne facultatif qui spécifie l'objet clé de chiffrement configuré pour fournir la méthode de chiffrement, la valeur de la clé secrète et d'autres paramètres de chiffrement. Si elle n'est pas spécifiée, la méthode utilise la valeur de clé générée automatiquement associée à la commande set ns EncryptionParams.

out_encoding : Cette valeur spécifie le mode de codage de la sortie. S'il n'est pas spécifié, le codage BASE64 est utilisé.

Entrée :

```
BASE64: original PEM base64-encoding: 6 bits (0..63) encoded as one
    ASCII character:
                0..23 = 'A'..'Z', 24..51 = 'a'..'z', 52..61 = '0'..'9
                    ', 62 = '+', 63 = '/', '=' = pad byte.
      BASE64URL:  URL and Filename safe base64-encoding: same as BASE64
          except 62 = '-', 63 = '_'
      HEX_UPPER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
          '.
      HEX_LOWER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'a'..'f
          '.
      HEX_COLONS: Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
          '; ':' between each hex byte. Matches BLOB_TO_HEX() output
          format
      HEX:  For input, accepts HEX_UPPER, HEX_LOWER, and HEX_COLONS
          format. For output, produces HEX_LOWER format
<!--NeedCopy-->
```

Sortie : La sortie est un texte chiffré à l'aide de la méthode et de la clé spécifiées et codé à l'aide d'un codage de sortie spécifié. Il insère une IV générée avant le texte chiffré pour les méthodes de bloc et les modes nécessitant une IV, et soit aucune IV n'est spécifiée pour la clé de chiffrement, soit la clé de chiffrement est omise.

Voici la fonction DECRYPT utilisée pour le déchiffrement tiers.


```
DECRYPT(encryptionKey, in_encoding)
```

Où,

Les données d'entrée sont un texte chiffré à l'aide de la méthode spécifiée et une clé codée à l'aide du codage d'entrée spécifié. Ce texte est censé inclure une IV générée avant le texte chiffré pour les méthodes et modes de blocs qui nécessitent une IV, et soit aucune IV n'est spécifiée pour la clé de chiffrement, soit la clé de chiffrement est omise.

EncryptionKey : paramètre de chaîne facultatif qui spécifie l'objet EncryptionKey configuré pour fournir la méthode de chiffrement, la clé secrète et d'autres paramètres de chiffrement. En cas d'omission, la méthode et la clé générée automatiquement associées au paramètre Encryption-Params seront utilisées

IN_ENCODING : paramètre d'énumération facultatif qui spécifie comment l'entrée doit être codée. Les valeurs sont les mêmes que l'encodage sortant de ENCRYPT. S'il n'est pas spécifié, le codage BASE64 est attendu.

Les données de sortie sont un texte déchiffré non codé.

Variantes et paramètres facultatifs

Voici les variantes de ces fonctions avec les paramètres facultatifs :

Variante	Description
ENCRYPT	Utilisez la commande EncryptionParams et le paramètre de codage de sortie BASE64.
ENCRYPT(out_encoding)	Utilisez EncryptionParams et le paramètre de codage de sortie spécifié.
ENCRYPT(encryptionKey)	Utilisez les paramètres de codage de sortie EncryptionKey et BASE64 spécifiés.
ENCRYPT(encryptionKey, out_encoding)	Utilisez la clé de chiffrement et le paramètre de codage de sortie spécifiés.
DECRYPT	Utilisez la commande EncryptionParams et le paramètre de codage d'entrée BASE64.
DECRYPT(out_encoding)	Utilisez la commande EncryptionParams et le paramètre de codage d'entrée spécifié.
DECRYPT(encryptionKey)	Utilisez les paramètres de codage d'entrée EncryptionKey et BASE64 spécifiés.
DECRYPT(encryptionKey, out_encoding)	Utilisez la clé de chiffrement et le paramètre de codage d'entrée spécifiés.

Configurer les clés HMAC

Les appliances NetScaler prennent en charge une fonction HMAC (Hashed Message Authentication Code) qui calcule une méthode condensée ou un hachage du texte saisi à l'aide d'une clé secrète partagée entre l'expéditeur et le destinataire du message. La méthode de résumé (dérivée d'une technique RFC 2104) authentifie l'expéditeur et vérifie que le contenu du message n'a pas été modifié. Par exemple, lorsqu'un client envoie un message avec la clé HMAC partagée à une appliance NetScaler, les expressions de politique avancées (PI) utilisent la fonction HMAC pour calculer le code basé sur le hachage sur le texte sélectionné. Ensuite, lorsque le récepteur reçoit le message avec la clé secrète, il recalcule le HMAC en le comparant au HMAC d'origine pour déterminer si le message a été modifié. La fonction HMAC est prise en charge par les appliances autonomes et par les appliances dans une configuration haute disponibilité ou dans un cluster. Son utilisation est similaire à la configuration d'une clé de chiffrement.

Les commandes add ns hmackey et set ns hmackey incluent un paramètre qui spécifie la méthode de condensation et la clé secrète partagée à utiliser pour le calcul HMAC.

Pour configurer une clé HMAC, vous devez effectuer les opérations suivantes :

1. Ajout d'une clé HMAC. Configure une clé HMAC avec une valeur de clé spécifiée.
2. Modification d'une clé HMAC. Modifie les paramètres d'une clé HMAC configurée. La méthode de condensation peut être modifiée sans modifier la valeur de clé, car la longueur de la valeur de clé n'est pas déterminée par le condensé. Toutefois, il est conseillé de spécifier une nouvelle clé lors de la modification du résumé.
3. Désinstallation d'une clé HMAC. Définit les paramètres d'une clé HMAC configurée sur leurs valeurs par défaut. Un objet HMacKey portant le nom doit exister. Le seul paramètre qui peut être désactivé est le commentaire, qui est supprimé.
4. Suppression d'une clé HMAC. Supprime une clé configurée. La clé ne peut pas comporter de référence.
5. Afficher une clé HMAC. Affiche les paramètres de la clé AC HMAC configurée ou de toutes les clés configurées. Si le nom est omis, la valeur de la clé n'est pas affichée.

Configurer une clé HMAC unique et aléatoire

Vous pouvez générer automatiquement une clé HMAC unique. Si votre appliance est une configuration de cluster, la clé HMAC est générée au début du processus et distribuée à tous les nœuds et moteurs de paquets. Cela garantit que la clé HMAC est identique pour tous les moteurs de paquets et tous les nœuds du cluster.

À l'invite de commande, tapez :

```
add ns hmacKey <your_key> -digest <digest> -keyValue <keyvalue>
```

Exemple :


```
add ns hmacKey <name> -digest sha1 -keyValue AUTO
```

Où,

- La syntaxe du nom est correcte et ne duplique pas le nom d'une clé existante.
- La valeur de clé « AUTO » peut être utilisée dans les commandes set pour générer de nouvelles clés pour les objets EncrytionKey et HMacKey existants.

> **Remarque :**
>
> La génération automatique de clé est utile si l'appliance NetScaler chiffre et déchiffre des données à l'aide de la clé, ou si elle génère et vérifie une clé HMAC. Étant donné que la valeur de clé elle-même est déjà chiffrée lorsqu'elle est affichée, vous ne pouvez pas récupérer la valeur de clé générée à des fins d'utilisation par une autre partie.

Exemple :

```
add ns hmacKey my_hmac_key -digest sha1 -keyValue 0c753c6c5ef859189cacdf95b506d02c179
```

Les méthodes de chiffrement ci-dessus spécifient le mode de fonctionnement avec CBC comme mode de fonctionnement par défaut. Par conséquent, les méthodes DES, DES2, AES128, AES192 et AES256 sont équivalentes aux méthodes DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC et AES256-CBC.

Modifier une clé HMAC à l'aide de l'interface de ligne de commande

Cette commande modifie les paramètres configurés pour une clé HMAC. Vous pouvez modifier le résumé sans modifier la valeur de la clé, car la longueur de la valeur de clé n'est pas déterminée par le résumé. Toutefois, il est conseillé de spécifier une nouvelle clé lors de la modification du résumé. À l'invite de commande, tapez :

```
1 set ns hmacKey <name> [-digst <digest>] [-keyValue <keyvalue>]
2 [-comment <string>]
3
4 <!--NeedCopy-->
```

Désinstaller une clé HMAC à l'aide de l'interface de ligne de commande

Cette commande définit les paramètres configurés pour une clé HMAC avec leurs valeurs par défaut. Un objet HMacKey portant le nom doit exister. Le seul paramètre que vous pouvez annuler est l'option de commentaire, qui est supprimée. À l'invite de commande, tapez :

```
unset ns hmacKey <name> -comment
```


Supprimer une clé HMAC à l'aide de l'interface de ligne de commande

Cette commande supprime la clé hmac configurée. La clé ne peut pas contenir de références. À l'invite de commande, tapez :

```
rm ns hmacKey <name>
```

Afficher une clé HMAC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show ns encryptionKey [<name>]

add ns hmacKey my_hmac_key -digest sha1 -keyValue 0
    c753c6c5ef859189cacdf95b506d02c1797407d
set ns hmacKey my_hmac_key -keyValue
    f348c594341a840a1f641a1cf24aa24c15eb1317
rm ns hmacKey my_hmac_key
show ns hmacKey my_hmac_key
           Name: my_hmac_key
     Digest: SHA1
     Key Value: (not disclosed)
<!--NeedCopy-->
```

Expressions de stratégie avancées : utilisation des dates, des heures et des nombres

May 5, 2023

La plupart des données numériques traitées par l'appliance NetScaler sont des dates et des heures. Outre le traitement des dates et des heures, l'appliance traite d'autres données numériques, telles que la longueur des requêtes et des réponses HTTP. Pour traiter ces données, vous pouvez configurer des expressions de politique avancées qui traitent les nombres.

Une expression numérique se compose d'un préfixe d'expression qui renvoie un nombre et parfois, mais pas toujours, d'un opérateur capable d'effectuer une opération sur le nombre. Des exemples de préfixes d'expression qui renvoient des nombres sont `SYS.TIME.DAYHTTP.REQ.CONTENT_LENGTH`, et `HTTP.RES.BODY.LENGTH`. `Numeric` les opérateurs peuvent fonctionner avec n'importe quelle expression de préfixe qui renvoie des données au format numérique. L'`GT(<int>)` opérateur, par exemple, peut être utilisé avec n'importe quelle expression de préfixe, telle que HTTP.REQ.CONTENT_LENGTH, qui renvoie un entier.

Format des dates et des heures dans une expression

May 8, 2023

Lorsque vous configurez une expression de politique avancée dans une politique qui fonctionne avec des dates et des heures (par exemple, l'heure du système NetScaler ou une date dans un certificat SSL), vous spécifiez un format d'heure comme suit :

```
GMT|LOCAL [<yyyy>] [<month>] [<d>] [<h>] [<m>] [<s>]
```

Où :

- \ <yyyy> est une année à quatre chiffres après GMT ou LOCAL.
- \ <month> est une abréviation à trois caractères pour le mois, par exemple, janvier, décembre
- \ <d> est un jour de la semaine ou un nombre entier pour la date.

  Vous ne pouvez pas spécifier le jour comme lundi, mardi, etc. Vous spécifiez soit un entier pour un jour spécifique du mois, soit vous spécifiez une date comme le premier, le deuxième, le troisième jour de la semaine du mois, etc. Vous trouverez ci-dessous des exemples de spécification d'un jour de la semaine :

  - Sun_1 est le premier dimanche du mois.
  - Sun_3 est le troisième dimanche du mois.
  - Wed_3 est le troisième mercredi du mois.
  - 30 est un exemple de date exacte dans un mois.
- \ <h> est l'heure, par exemple 10h.
- \ <s> est le nombre de secondes, par exemple 30 secondes.

L'exemple d'expression suivant est vrai si la date se situe entre janvier 2008 et janvier 2009, selon l'heure GMT.

```
http.req.date.between(GMT 2008 Jan, GMT 2009 Jan)
```

L'exemple d'expression suivant est vrai pour le mois de mars et pour tous les mois qui suivent le mois de mars de l'année civile, sur la base de l'heure GMT :

```
sys.time.ge(GMT 2008 Mar)
```

Lorsque vous spécifiez une date et une heure, notez que le format respecte la casse et doit de conserver le nombre exact d'espaces vides entre les entrées.

```
1 **Note:**
2
3 In an expression that requires two time values, both must use GMT or
     both must use LOCAL. You cannot mix the two in an expression.
```



```
4
5 Unlike when you use the SYS.TIME prefix in an advanced policy
     expression, if you specify SYS.TIME in a rewrite action, the
     NetScaler returns a string in conventional date format (for example,
      Sun, 06 Nov 1994 08:49:37 GMT). For example, the following rewrite
     action replaces the http.res.date header with the NetScaler system
     time in a conventional date format:
6
7 add rewrite action sync_date replace http.res.date sys.time
```

Expressions relatives à l'heure du système NetScaler

May 8, 2023

Le préfixe d'expression SYS.TIME extrait l'heure du système NetScaler. Vous pouvez configurer des expressions qui déterminent si un événement particulier s'est produit à un moment donné ou dans un intervalle de temps spécifique en fonction de l'heure du système NetScaler.

Le tableau suivant décrit les expressions que vous pouvez créer à l'aide du préfixe SYS.TIME.

- **<time1> <time2>SYS.TIME.BETWEEN (\, \) :**

  <time2>Renvoie une valeur booléenne TRUE si la valeur renvoyée est ultérieure à \ <time1> et antérieure à \.

  Vous formatez les <time1> <time2> arguments \, \ comme suit :

  - Ils doivent être tous les deux GMT ou les deux LOCAUX.
  - \ <time2> doit être postérieur à \ <time1>.

  Par exemple, si l'heure actuelle est GMT 2005 du 1er mai à 10 h 15 min 30 s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit :

  - sys.time.between (GMT 2004, GMT 2006)
  - sys.time.between (GMT en janvier 2004, GMT en novembre 2006)
  - sys.time.between (GMT 2004 janvier, GMT 2006)
  - sys.time.between (GMT 2005 dimanche 1 mai, GMT dimanche 3 mai 2005)
  - sys.time.between (GMT le 1er mai 2005, GMT le 1er mai 2005)
  - sys.time.between (LOCAL 1er mai 2005, LOCAL 1er mai 2005 1)

- **SYS.TIME.DAY :**

  Renvoie le jour du mois en cours sous la forme d'un nombre compris entre 1 et 31.

- **<time>SYS.TIME.EQ (\) :**

<time>Renvoie une valeur booléenne TRUE si l'heure actuelle est égale à l'argument \.

Par exemple, si l'heure actuelle est GMT 2005 du 1er mai à 10 h 15 min 30 s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont indiqués entre parenthèses) :

- sys.time.eq (GMT 2005) (VRAI dans cet exemple.)
- sys.time.eq (GMT 2005 Dec) (FAUX dans cet exemple.)
- sys.time.eq (LOCAL 2005 May) (prend la valeur TRUE ou FALSE dans cet exemple, selon le fuseau horaire actuel.)
- sys.time.eq (GMT 10h) (VRAI dans cet exemple.)
- sys.time.eq (GMT 10h 30s) (VRAI dans cet exemple.)
- sys.time.eq (GMT le 10 mai) (VRAI dans cet exemple.)
- sys.time.eq (GMT Sun) (VRAI dans cet exemple.)
- sys.time.eq (GMT May Sun_1) (VRAI dans cet exemple.)

- **<time>SYS.TIME.NE (\) :**

<time>Renvoie une valeur booléenne TRUE si l'heure actuelle n'est pas égale à l'argument \.

- **<time>SYS.TIME.GE (\) :**

<time>Renvoie une valeur booléenne TRUE si l'heure actuelle est ultérieure ou égale à \.

Par exemple, si l'heure actuelle est GMT 2005 du 1er mai à 10 h 15 min 30 s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont indiqués entre parenthèses) :

- sys.time.ge (GMT 2004) (VRAI dans cet exemple.)
- sys.time.ge (GMT 2005 janvier) (VRAI dans cet exemple.)
- sys.time.ge (LOCAL 2005 May) (VRAI ou FAUX dans cet exemple, selon le fuseau horaire actuel.)
- sys.time.ge (GMT 8h) (VRAI dans cet exemple.)
- sys.time.ge (GMT 30m) (FAUX dans cet exemple.)
- sys.time.ge (GMT le 10 mai) (VRAI dans cet exemple.)
- sys.time.ge (GMT 10 h 00 min) (VRAI dans cet exemple.)
- sys.time.ge (GMT Sun) (VRAI dans cet exemple.)
- sys.time.ge (GMT May Sun_1) (VRAI dans cet exemple.)

- **<time>SYS.TIME.GT (\) :**

<time>Renvoie une valeur booléenne TRUE si la valeur temporelle est ultérieure à l'argument \.

Par exemple, si l'heure actuelle est GMT 2005 du 1er mai à 10 h 15 min 30 s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont indiqués entre parenthèses) :

- sys.time.gt (GMT 2004) (VRAI dans cet exemple.)
- sys.time.gt (GMT 2005 janvier) (VRAI dans cet exemple.)
- sys.time.gt (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
- sys.time.gt (GMT 8h) (VRAI dans cet exemple.)
- sys.time.gt (GMT 30m) (FAUX dans cet exemple.)
- sys.time.gt (GMT le 10 mai) (FAUX dans cet exemple.)
- sys.time.gt (GMT 10 h 00 min) (VRAI dans cet exemple.)
- sys.time.gt (GMT Sun) (FAUX dans cet exemple.)
- sys.time.gt (GMT May Sun_1) (FAUX dans cet exemple.)

- **SYS.TIME.HOURS :**

  Renvoie l'heure actuelle sous la forme d'un entier compris entre 0 et 23.

- **<time>SYS.TIME.LE (\) :**

  <time>Renvoie une valeur booléenne TRUE si la valeur de l'heure actuelle précède ou est égale à l'argument \.

  Par exemple, si l'heure actuelle est GMT 2005 du 1er mai à 10 h 15 min 30 s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont indiqués entre parenthèses) :

  - sys.time.le (GMT 2006) (VRAI dans cet exemple.)
  - sys.time.le (GMT 2005 Dec) (VRAI dans cet exemple.)
  - sys.time.le (LOCAL 2005, mai) (VRAI ou FAUX selon le fuseau horaire actuel.)
  - sys.time.le (GMT 8h) (FAUX dans cet exemple.)
  - sys.time.le (GMT 30m) (VRAI dans cet exemple.)
  - sys.time.le (GMT le 10 mai) (VRAI dans cet exemple.)
  - sys.time.le (GMT le 11 juin) (VRAI dans cet exemple.)
  - sys.time.le (GMT Wed) (VRAI dans cet exemple.)
  - sys.time.le (GMT May Sun_1) (VRAI dans cet exemple.)

- **<time>SYS.TIME.LT (\) :**

  <time>Renvoie une valeur booléenne TRUE si la valeur de l'heure actuelle précède l'argument \.

  Par exemple, si l'heure actuelle est GMT 2005 du 1er mai à 10 h 15 min 30 s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont indiqués entre parenthèses) :

  - sys.time.lt (GMT 2006) (VRAI dans cet exemple.)
  - sys.time.lt.time.lt (GMT 2005 Dec) (VRAI dans cet exemple.)
  - sys.time.lt (LOCAL 2005, mai) (VRAI ou FAUX selon le fuseau horaire actuel.)
  - sys.time.lt (GMT 8h) (FAUX dans cet exemple.)
  - sys.time.lt (GMT 30m) (VRAI dans cet exemple.)

- sys.time.lt (GMT le 10 mai) (FAUX dans cet exemple.)
- sys.time.lt (GMT le 11 juin) (VRAI dans cet exemple.)
- sys.time.lt (GMT Wed) (VRAI dans cet exemple.)
- sys.time.lt (GMT May Sun_1) (FAUX dans cet exemple.)

- **SYS.TIME.MINUTES :**

  Renvoie la minute en cours sous la forme d'un entier compris entre 0 et 59.

- **SYS.TIME.MONTH :**

  Extrait le mois en cours et renvoie un entier compris entre 1 (janvier) et 12 (décembre).

- **SYS.TIME.RELATIVE_BOOT :**

  Calcule le nombre de secondes avant le redémarrage précédent ou programmé le plus proche et renvoie un entier.

  Si l'heure de démarrage la plus proche se situe dans le passé, l'entier est négatif. Si c'est dans le futur, l'entier est positif.

- **SYS.TIME.RELATIVE_NOW :**

  Calcule le nombre de secondes entre l'heure actuelle du système NetScaler et l'heure spécifiée, et renvoie un entier indiquant la différence.

  Si l'heure indiquée est dans le passé, l'entier est négatif ; s'il est dans le futur, l'entier est positif.

- **SYS.TIME.SECONDS :**

  Extrait les secondes de l'heure actuelle du système NetScaler et renvoie cette valeur sous la forme d'un entier compris entre 0 et 59.

- **SYS.TIME.WEEK DAY :**

  Renvoie le jour de la semaine en cours sous la forme d'une valeur comprise entre 0 (dimanche) et 6 (samedi).

- **<time1> <time2>SYS.TIME.WITHIN (\, \) :**

  Si vous omettez un élément d'heure dans \ <time1>, par exemple le jour ou l'heure, il est supposé avoir la valeur la plus faible de sa plage. Si vous omettez un élément dans \ <time2>, il est supposé avoir la valeur la plus élevée de sa plage.

  Les plages des éléments temporels sont les suivantes : mois 1 à 12, jours 1 à 31, jours de semaine 0 à 6, heures 0 à 23, minutes 0 à 59 et secondes 0 à 59. Si vous spécifiez l'année, vous devez le faire à la fois dans \ <time1> et \ <time2>.

  Par exemple, si l'heure est GMT 2005 du 10 mai à 10 h 15 min 30 s et que c'est le deuxième mardi du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont indiqués entre parenthèses) :

- sys.time.within (GMT 2004, GMT 2006) (VRAI dans cet exemple.)
- sys.time.within (GMT 2004 janvier, GMT 2006 mars) (FAUX, le mois de mai n'est pas compris entre janvier et mars.)
- sys.time.within (GMT Feb, GMT) (VRAI, le mois de mai se situe entre février et décembre.)
- sys.time.within (GMT Sun_1, GMT Sun_3) (VRAI, le deuxième mardi se situe entre le premier dimanche et le troisième dimanche.)
- sys.time.within (GMT 2005 du 1er mai à 10h, GMT du 1er mai 2005 à 17h) (VRAI dans cet exemple.)
- sys.time.within (LOCAL 1er mai 2005, LOCAL 1er mai 2005) (VRAI ou FAUX, selon le fuseau horaire du système NetScaler.)

- **SYS.TIME.YEAR :**

  Extrait l'année de l'heure système actuelle et renvoie cette valeur sous la forme d'un entier à quatre chiffres.

Expressions pour les dates des certificats SSL

May 8, 2023

Vous pouvez déterminer la période de validité des certificats SSL en configurant une expression contenant le préfixe suivant :

```
CLIENT.SSL.CLIENT_CERT
```

L'exemple d'expression suivant fait correspondre une heure d'expiration particulière aux informations du certificat :

```
client.ssl.client_cert.valid_not_after.eq(GMT 2009)
```

Le tableau suivant décrit les opérations basées sur le temps sur les certificats SSL. Pour obtenir l'expression souhaitée, remplacez le *certificat* dans l'expression de la première colonne par le préfixe « CLIENT.SSL.CLIENT_CERT ».

- <certificate>.VALID_NOT_AFTER:

  Renvoie le dernier jour avant l'expiration du certificat. Le format de retour est le nombre de secondes écoulées depuis le 1er janvier 1970 GMT (0 heure, 0 minute, 0 seconde).

- **<certificate> <time1> <time2>.VALID_NOT_AFTER.BETWEEN (\, \) :**

  <time2>Renvoie une valeur booléenne TRUE si la validité du certificat se situe entre les arguments \ <time1> et \. \ <time1> et \ <time2> doivent tous deux être entièrement spécifiés. Voici des exemples :

  GMT 1995 Jan est entièrement spécifié.

GMT Jan n'est pas complètement spécifié

GMT 1995 20 n'est pas complètement spécifié.

GMT Jan Mon_2 n'est pas complètement spécifié.

Les <time1> <time2> arguments \ et \ doivent être à la fois GMT ou LOCAL, et \ <time2> doit être supérieur à \ <time1>.

Par exemple, si c'est GMT 2005 du 1er mai à 10 h 15 min 30 s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses).

- … entre (GMT 2004, GMT 2006) (VRAI)
- …. entre (GMT 2004 janvier, GMT 2006 novembre) (VRAI)
- …. entre (GMT 2004 janvier, GMT 2006) (VRAI)
- . .entre (GMT 2005 mai diman_1, GMT 2005 mai diman_3) (VRAI)
- . .between (GMT 2005 1er mai, GMT mai 2005 1) (VRAI)
- . .between (LOCAL 2005 1er mai 2005, LOCAL 1er mai 2005) (VRAI ou FAUX, selon le fuseau horaire du système NetScaler.)

- **<certificate>\.VALID_NOT_AFTER.DAY :**

  Extrait le dernier jour du mois pendant lequel le certificat est valide et renvoie un nombre compris entre 1 et 31, selon la date.

- **<certificate> <time>\.VALID_NOT_AFTER.EQ (\) :**

  <time>Renvoie une valeur booléenne TRUE si l'heure est égale à l'argument \.

  Par exemple, si l'heure actuelle est GMT 2005 du 1er mai à 10 h 15 min 30 s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation pour cet exemple figurent entre parenthèses) :

  - . .eq (GMT 2005) (VRAI)
  - . .eq (GMT décembre 2005) (FAUX)
  - . .eq (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel)
  - . .eq (GMT 10h) (VRAI)
  - . .eq (GMT 10h 30s) (VRAI)
  - . .eq (GMT le 10 mai) (VRAI)
  - . .eq (GMT Sun) (VRAI)
  - . .eq (GMT May Sun_1) (VRAI)

- **<certificate> <time>\.VALID_NOT_AFTER.GE (\) :**

  <time>Renvoie une valeur booléenne TRUE si la valeur temporelle est supérieure ou égale à l'argument \.

  Par exemple, si la valeur horaire est GMT 2005 du 1er mai à 10 h 15 min 30 s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de

l'évaluation pour cet exemple figurent entre parenthèses) :

- . .ge (GMT 2004) (VRAI)
- . .ge (GMT, janvier 2005) (VRAI)
- . .ge (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
- . .ge (GMT 8h) (VRAI)
- . .ge (GMT 30 m) (FAUX)
- . .ge (GMT le 10 mai) (VRAI)
- . .ge (GMT 10 mai à 0h) (VRAI)
- . .ge (GMT Sun) (VRAI)
- . .ge (GMT May Sun_1) (VRAI)

- **<certificate> <time>\.VALID_NOT_AFTER.GT (\) :**

  <time>Renvoie une valeur booléenne TRUE si la valeur temporelle est supérieure à l'argument \.

  Par exemple, si la valeur horaire est GMT 2005 du 1er mai à 10 h 15 min 30 s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation pour cet exemple figurent entre parenthèses) :

  - . .gt (GMT 2004) (VRAI)
  - . .gt (GMT, janvier 2005) (VRAI)
  - . .gt (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
  - . .gt (GMT 8h) (VRAI)
  - . .gt (GMT 30 m) (FAUX)
  - . .gt (GMT le 10 mai) (FAUX)
  - . .gt (GMT Sun) (FAUX)
  - . .gt (GMT May Sun_1) (FAUX)

- **<certificate>\.VALID_NOT_AFTER.HOURS :**

  Extrait la dernière heure pendant laquelle le certificat est valide et renvoie cette valeur sous la forme d'un entier compris entre 0 et 23.

- **<certificate> <time>\.VALID_NOT_AFTER.LE (\) :**

  <time>Renvoie une valeur booléenne TRUE si le temps précède ou est égal à l'argument \.

  Par exemple, si la valeur horaire est GMT 2005 du 1er mai à 10 h 15 min 30 s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation pour cet exemple figurent entre parenthèses) :

  - . .le (GMT 2006) (VRAI)
  - . .le (GMT décembre 2005) (VRAI)
  - . .le (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
  - . .le (GMT 8h) (FAUX)
  - . .le (GMT 30 m) (VRAI)

- . .le (GMT le 10 mai) (VRAI)
- . .le (GMT le 11 juin) (VRAI)
- . .le (GMT mercredi) (VRAI)
- . .le (GMT May Sun_1) (VRAI)

- **<certificate> <time>\.VALID_NOT_AFTER.LT (\) :**

  <time>Renvoie une valeur booléenne TRUE si l'heure précède l'argument \.

  Par exemple, si l'heure actuelle est GMT 2005 du 1er mai à 10 h 15 min 30 s et que c'est le premier dimanche du mois, vous pouvez spécifier ce qui suit :

  - . .lt (GMT 2006) (VRAI)
  - . .lt (GMT en décembre 2005) (VRAI)
  - . .lt (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
  - . .lt (GMT 8h) (FAUX)
  - . .lt (GMT 30 m) (VRAI)
  - . .lt (GMT le 10 mai) (FAUX)
  - . .lt (GMT le 11 juin) (VRAI)
  - . .lt (mercredi GMT) (VRAI)
  - . .lt (GMT May Sun_1) (FAUX)

- **<certificate>\.VALID_NOT_AFTER.MINUTES :**

  Extrait la dernière minute pendant laquelle le certificat est valide et renvoie cette valeur sous la forme d'un entier compris entre 0 et 59.

- **<certificate>\.VALID_NOT_AFTER.MONTH :**

  Extrait le dernier mois de validité du certificat et renvoie cette valeur sous forme d'entier compris entre 1 (janvier) et 12 (décembre).

- **<certificate>\.VALID_NOT_AFTER.RELATIVE_BOOT :**

  Calcule le nombre de secondes avant le redémarrage précédent ou programmé le plus proche et renvoie un entier. Si l'heure de démarrage la plus proche se situe dans le passé, l'entier est négatif. Si c'est dans le futur, l'entier est positif.

- **<certificate>\.VALID_NOT_AFTER.RELATIVE_NOW ;**

  Calcule le nombre de secondes entre l'heure actuelle du système et l'heure spécifiée et renvoie un entier. Si le temps est passé, l'entier est négatif ; s'il est dans le futur, il est positif.

- **<certificate>\.VALID_NOT_AFTER.SECONDES :**

  Extrait la dernière seconde pendant laquelle le certificat est valide et renvoie cette valeur sous la forme d'un entier compris entre 0 et 59.

- **<certificate>\.VALID_NOT_AFTER.JOUR DE SEMAINE :**

Extrait le dernier jour de la semaine pendant lequel le certificat est valide. Renvoie un nombre compris entre 0 (dimanche) et 6 (samedi) pour indiquer le jour de la semaine dans la valeur horaire.

- **<certificate> <time1> <time2>\.VALID_NOT_AFTER.WITHIN (\, \) :**

  <time2>Renvoie une valeur booléenne TRUE si l'heure se situe dans toutes les plages définies par les éléments entre \ <time1> et \.

  Si vous omettez un élément temporel dans \ <time1>, il est supposé avoir la valeur la plus faible de sa plage. Si vous omettez un élément dans \ <time2>, il est supposé avoir la valeur la plus élevée de sa plage. Si vous spécifiez une année dans \ <time1>, vous devez la spécifier dans \ <time2>.

  Les plages des éléments temporels sont les suivantes : mois 1 à 12, jours 1 à 31, jours de semaine 0 à 6, heures 0 à 23, minutes 0 à 59 et secondes 0 à 59. Pour que le résultat soit VRAI, chaque élément du temps doit exister dans la plage correspondante que vous avez spécifiée dans \ <time1>, \ <time2>.

  Par exemple, si l'heure est GMT 2005 du 10 mai à 10 h 15 min 30 s et que c'est le deuxième mardi du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses) :

  - . .within (GMT 2004, GMT 2006) (VRAI)
  - . .within (GMT 2004 janvier, GMT 2006 mars) (FAUX, le mois de mai n'est pas compris entre janvier et mars.)
  - . .within (GMT Feb, GMT) (VRAI, le mois de mai se situe entre février et décembre)
  - . .within (GMT Sun_1, GMT Sun_3) (VRAI, le deuxième mardi se situe entre le premier dimanche et le troisième dimanche)
  - . .within (GMT 2005 du 1er mai à 10h, GMT du 1er mai 2005 à 17h) (VRAI)
  - . .within (LOCAL 2005 1er mai 2005, LOCAL 1er mai 2005) (VRAI ou FAUX, selon le fuseau horaire du système NetScaler)

- **<certificate>\.VALID_NOT_AFTER.YEAR :**

  Extrait la dernière année de validité du certificat et renvoie un entier à quatre chiffres.

- **<certificate>\.VALID_NOT_AVANT :**

  Renvoie la date à laquelle le certificat client devient valide.

  Le format de retour est le nombre de secondes écoulées depuis le 1er janvier 1970 GMT (0 heure, 0 minute, 0 seconde).

- **<certificate> <time1> <time2>\.VALID_NOT_BEFORE.BETWEEN (\, \) :**

  Renvoie une valeur booléenne TRUE si la valeur temporelle se situe entre les deux arguments temporels. Les <time1> <time2> arguments \ et \ doivent être entièrement spécifiés.

  Voici des exemples :

GMT 1995 Jan est entièrement spécifié.
GMT Jan n'est pas complètement spécifié.
GMT 1995 20 n'est pas complètement spécifié.
GMT Jan Mon_2 n'est pas complètement spécifié.
Les arguments temporels doivent être à la fois GMT ou LOCAL, et \ <time2> doit être supérieur à \ <time1>.

Par exemple, si la valeur horaire est GMT 2005 du 1er mai à 10 h 15 min 30 s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation pour cet exemple figurent entre parenthèses) :

- … entre (GMT 2004, GMT 2006) (VRAI)
- …. entre (GMT 2004 janvier, GMT 2006 novembre) (VRAI)
- …. entre (GMT 2004 janvier, GMT 2006) (VRAI)
- . .entre (GMT 2005 mai diman_1, GMT 2005 mai diman_3) (VRAI)
- . .between (GMT 2005 1er mai, GMT mai 2005 1) (VRAI)
- . .between (LOCAL 2005 1er mai 2005, LOCAL 1er mai 2005) (VRAI ou FAUX, selon le fuseau horaire du système NetScaler.)

- **<certificate>\.VALID_NOT_BEFORE.DAY :**

  Extrait le dernier jour du mois pendant lequel le certificat est valide et renvoie cette valeur sous la forme d'un nombre compris entre 1 et 31 représentant ce jour.

- **<certificate> <time>\.VALID_PAT_AVANT .EQ (\) :**

  <time>Renvoie une valeur booléenne TRUE si l'heure est égale à l'argument \.

  Par exemple, si la valeur horaire est GMT 2005 du 1er mai à 10 h 15 min 30 s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation pour cet exemple figurent entre parenthèses) :

  - . .eq (GMT 2005) (VRAI)
  - . .eq (GMT décembre 2005) (FAUX)
  - . .eq (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
  - . .eq (GMT 10h) (VRAI)
  - . .eq (GMT 10h 30s) (VRAI)
  - . .eq (GMT le 10 mai) (VRAI)
  - . .eq (GMT Sun) (VRAI)
  - . .eq (GMT May Sun_1) (VRAI)

- **<certificate> <time>\.VALID_PAT_BEFORE.GE (\) :**

  <time>Renvoie une valeur booléenne TRUE si l'heure est supérieure à (après) ou égale à l'argument \.

Par exemple, si la valeur horaire est GMT 2005 du 1er mai à 10 h 15 min 30 s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses) :

- . .ge (GMT 2004) (VRAI)
- . .ge (GMT, janvier 2005) (VRAI)
- . .ge (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
- . .ge (GMT 8h) (VRAI)
- . .ge (GMT 30 m) (FAUX)
- . .ge (GMT le 10 mai) (VRAI)
- . .ge (GMT 10 mai à 0h) (VRAI)
- . .ge (GMT Sun) (VRAI)
- . .ge (GMT May Sun_1) (VRAI)

- **<certificate> <time>\.VALID_PAT_BEFOR.GT (\) :**

  <time>Renvoie une valeur booléenne TRUE si le temps s'écoule après l'argument \.

  Par exemple, si la valeur horaire est GMT 2005 du 1er mai à 10 h 15 min 30 s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses) :

  - . .gt (GMT 2004) (VRAI)
  - . .gt (GMT, janvier 2005) (VRAI)
  - . .gt (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
  - . .gt (GMT 8h) (VRAI)
  - . .gt (GMT 30 m) (FAUX)
  - . .gt (GMT le 10 mai) (FAUX)
  - . .gt (GMT 10 mai à 0h) (VRAI)
  - . .gt (GMT Sun) (FAUX)
  - . .gt (GMT May Sun_1) (FAUX)

- **<certificate>\.VALID_NOT_BEFORE.HOURS :**

  Extrait la dernière heure pendant laquelle le certificat est valide et renvoie cette valeur sous la forme d'un entier compris entre 0 et 23.

- **<certificate> <time>\.VALID_PAT_AVANT .LE (\)

  <time>Renvoie une valeur booléenne TRUE si le temps précède ou est égal à l'argument \.

  Par exemple, si la valeur horaire est GMT 2005 du 1er mai à 10 h 15 min 30 s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation pour cet exemple figurent entre parenthèses) :

  - . .le (GMT 2006) (VRAI)
  - . .le (GMT décembre 2005) (VRAI)

- . .le (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
- . .le (GMT 8h) (FAUX)
  . - . .le (GMT 30m) (VRAI)
- . .le (GMT le 10 mai) (VRAI)
- . .le (GMT le 11 juin) (VRAI)
- . .le (GMT mercredi) (VRAI)
- . .le (GMT May Sun_1) (VRAI)

- **<certificate> <time>\.VALID_NOT_BEFORE.LT (\) :**

  <time>Renvoie une valeur booléenne TRUE si l'heure précède l'argument \.

  Par exemple, si la valeur horaire est GMT 2005 du 1er mai à 10 h 15 min 30 s et qu'il s'agit du premier dimanche du mois de mai 2005, vous pouvez spécifier ce qui suit (les résultats de l'évaluation pour cet exemple figurent entre parenthèses) :

  - . .lt (GMT 2006) (VRAI)
  - . .lt (GMT en décembre 2005) (VRAI)
  - . .lt (LOCAL 2005, mai) (VRAI ou FAUX, selon le fuseau horaire actuel.)
  - . .lt (GMT 8h) (FAUX)
  - . .lt (GMT 30 m) (VRAI)
  - . .lt (GMT le 10 mai) (FAUX)
  - . .lt (GMT le 11 juin) (VRAI)
  - . .lt (mercredi GMT) (VRAI)
  - . .lt (GMT May Sun_1) (FAUX)

- **<certificate>\.VALID_PAT_BEFORE.MINUTES :**

  Extrait la dernière minute pendant laquelle le certificat est valide. Renvoie la minute en cours sous la forme d'un entier compris entre 0 et 59.

- **<certificate>\.VALID_PAT_BEFOR.MONTH :**

  Extrait le dernier mois de validité du certificat. Renvoie le mois en cours sous la forme d'un entier compris entre 1 (janvier) et 12 (décembre).

- **<certificate>\.VALID_NOT_BEFOR.RELATIVE_BOOT :**

  Calcule le nombre de secondes avant le redémarrage précédent ou programmé le plus proche de NetScaler et renvoie un entier. Si l'heure de démarrage la plus proche se situe dans le passé, l'entier est négatif ; s'il se situe dans le futur, l'entier est positif.

- **<certificate>\.VALID_NOT_BEFORE.RELATIVE_NOW :**

  Renvoie le nombre de secondes entre l'heure actuelle du système NetScaler et l'heure spécifiée sous forme d'entier. Si l'heure indiquée se trouve dans le passé, le nombre entier est négatif. Si c'est dans le futur, l'entier est positif.

- **<certificate>\.VALID_NOT_BEFORE.SECONDES :**

  Extrait la dernière seconde pendant laquelle le certificat est valide. Renvoie la seconde en cours sous la forme d'un entier compris entre 0 et 59.

- **<certificate>\.VALID_NOT_BEFORE.JOUR DE SEMAINE :**

  Extrait le dernier jour de la semaine pendant lequel le certificat est valide. Renvoie le jour de la semaine sous la forme d'un nombre compris entre 0 (dimanche) et 6 (samedi).

- **<certificate> <time1> <time2>\.VALID_NOT_BEFORE.WITHIN (\, \) :**

  <time2>Renvoie une valeur booléenne TRUE si chaque élément temporel se trouve dans la plage définie dans les arguments \ <time1>, \.

  Si vous omettez un élément temporel dans \ <time1>, il est supposé avoir la valeur la plus faible de sa plage. Si vous omettez un élément temporel dans \ <time2>, il est supposé avoir la valeur la plus élevée dans sa plage. Si vous spécifiez une année dans \ <time1>, elle doit être spécifiée dans \ <time2>. Les plages des éléments temporels sont les suivantes : mois 1 à 12, jours 1 à 31, jours de semaine 0 à 6, heures 0 à 23, minutes 0 à 59 et secondes 0 à 59.

  Par exemple, si l'heure est GMT 2005 du 10 mai à 10 h 15 min 30 s et que c'est le deuxième mardi du mois, vous pouvez spécifier ce qui suit (les résultats de l'évaluation sont entre parenthèses) :

  - . .within (GMT 2004, GMT 2006) (VRAI)
  - . .within (GMT 2004 janvier, GMT 2006 mars) (FAUX, le mois de mai n'est pas compris entre janvier et mars.)
  - . .within (GMT Feb, GMT) (VRAI, le mois de mai se situe entre février et décembre.)
  - . .within (GMT Sun_1, GMT Sun_3) (VRAI, le deuxième mardi se situe entre le premier dimanche et le troisième dimanche.)
  - . .within (GMT 2005 du 1er mai à 10h, GMT du 1er mai 2005 à 17h) (VRAI)
  - . .within (LOCAL 2005 1er mai 2005, LOCAL 1er mai 2005) (VRAI ou FAUX, selon le fuseau horaire du système NetScaler)

- **<certificate>\.VALID_PAT_BEFORE.YEAR :**

  Extrait la dernière année de validité du certificat. Renvoie l'année en cours sous la forme d'un entier à quatre chiffres.

Expressions pour les dates de requête et de réponse HTTP

October 5, 2021

Les préfixes d'expression suivants renvoient le contenu de l'en-tête Date HTTP sous forme de texte ou d'objet date. Ces valeurs peuvent être évaluées comme suit :

- En tant que numéro. La valeur numérique d'un en-tête HTTP Date est renvoyée sous la forme du nombre de secondes écoulées depuis le 1er janvier 1970.

  Par exemple, l'expression http.req.date.mod (86400) renvoie le nombre de secondes écoulées depuis le début de la journée. Ces valeurs peuvent être évaluées en utilisant les mêmes opérations que d'autres données numériques non liées à la date. Pour plus d'informations, voir Préfixes d'expression pour les données numériques autres que la date et l'heure.

- En tant qu'en-tête HTTP. Les en-têtes de date peuvent être évalués en utilisant les mêmes opérations que les autres en-têtes HTTP.

  Pour plus d'informations, consultez Expressions de stratégie avancées : analyse des données HTTP, TCP et UDP.

- Comme texte. Les en-têtes de date peuvent être évalués en utilisant les mêmes opérations que les autres chaînes.

Pour plus d'informations, voir Expressions de stratégie avancées : évaluation du texte.

Prefix	Description
HTTP.REQ.DATE	Renvoie le contenu de l'en-tête HTTP Date sous forme de texte ou d'objet date. Les formats de date reconnus sont : RFC822. Dim, 06 Jan 1980 08:49:37 GMT, RFC 850. Dimanche, 06-Jan-80 09:49:37 GMT, et ASCTIME. Dim. 6 janv. 08:49:37 1980.
HTTP.RES.DATE	Renvoie le contenu de l'en-tête HTTP Date sous forme de texte ou d'objet date. Les formats de date reconnus sont : RFC822. Dim, 06 Jan 1980 8:49:37 GMT, RFC 850. Dimanche 6 janvier 80 9 : 49 : 37 GMT, et ASCTIME. Dim. 6 janv. 08:49:37 1980.

Générer le jour de la semaine, sous forme de chaîne, en formats courts et longs

January 21, 2021

Les fonctions,`WEEKDAY_STRING_SHORT` et`WEEKDAY_STRING`, génèrent le jour de la semaine, sous forme de chaîne, en formats courts et longs, respectivement. Les chaînes renvoyées sont toujours

en anglais. Le préfixe utilisé avec ces fonctions doit renvoyer le jour de la semaine au format entier et la plage acceptable pour la valeur renvoyée par le préfixe est 0-6. Par conséquent, vous pouvez utiliser n'importe quel préfixe qui renvoie un entier dans la plage acceptable. Une condition UNDEF est déclenchée si la valeur renvoyée n'est pas dans cette plage ou si l'allocation de mémoire échoue.

Voici les descriptions des fonctions :

Fonction	Description
`<prefix>.WEEKDAY_STRING_SHORT`	Renvoie le jour de la semaine en format court. La forme abrégée est toujours de 3 caractères avec une majuscule initiale et les caractères restants en minuscules. Par exemple, SYS.TIME.WEEKDAY.WEEKDAY_STRING_SHORTrenvoie Sun si la valeur renvoyée par la fonction WEEKDAY est 0 et Sat si la valeur renvoyée par le préfixe est 6.
`<prefix>.WEEKDAY_STRING`	Renvoie le jour de la semaine en format long. La forme longue a toujours une majuscule initiale, avec les caractères restants en minuscules. Par exemple,`SYS.TIME.WEEKDAY.WEEKDAY_STRING` renvoie Sunday si la valeur renvoyée par la fonction WEEKDAY est 0 et Saturday si la valeur renvoyée par le préfixe est 6.

Préfixes d'expression pour les données numériques autres que la date et l'heure

August 20, 2021

Outre la configuration d'expressions fonctionnant à temps, vous pouvez configurer des expressions pour les types de données numériques suivants :

- La longueur des requêtes HTTP, le nombre d'en-têtes HTTP dans une requête, etc.

  Pour plus d'informations, consultez Expressions pour les données de charge utile HTTP numériques autres que les dates.

- Adresses IP et MAC.

Pour plus d'informations, voir Expressions pour adresses IP et sous-réseauxIP.

- Données client et serveur en ce qui concerne les ID d'interface et le débit de transaction.

  Pour plus d'informations, voir Expressions pour données numériques client et serveur.

- Données numériques dans les certificats clients autres que les dates.

  Pour plus d'informations sur ces préfixes, y compris le nombre de jours avant l'expiration du certificat et la taille de la clé de chiffrement, consultez Préfixes pour les données numériques dans les certificats SSL.

Conversion de nombres en texte

August 20, 2021

Les fonctions suivantes produisent des chaînes binaires à partir d'un nombre renvoyé par un préfixe d'expression. Ces fonctions sont particulièrement utiles dans la fonction de réécriture TCP en tant que chaînes de remplacement pour les données binaires. Pour plus d'informations sur la fonction de réécriture TCP, voir Réécriture.

Toutes les fonctions renvoient une valeur de type texte. L'endianness que certaines fonctions acceptent comme paramètre est LITTLE_ENDIAN ou BIG_ENDIAN.

Fonction	Description
<number>.SIGNED8_STRING	Produit une chaîne binaire signée de 8 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_SIGNED8(16).SUB(3).SIGNED8_STR
<number>.UNSIGNED8_STRING	Produit une chaîne binaire non signée de 8 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_UNSIGNED8(31).ADD(3).UNSIGNED
<number>.SIGNED16_STRING(<endianness>)	Produit une chaîne binaire signée de 16 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).SKIP(12).GET_SIGNED16(0, BIG_ENDIAN).SUB(4).SIGNED16_STRING(BIG_ENDIAN)

Fonction	Description
<number>.UNSIGNED16_STRING(<endianness>)	Produit une chaîne binaire non signée de 16 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_UNSIGNED16(47, LIT-TLE_ENDIAN).ADD(7).UNSIGNED16_STRING(LITTLE_ENDIAN)
<number>.SIGNED32_STRING (<endianness>)	Produit une chaîne binaire signée 32 bits représentant le nombre. Exemple : HTTP.REQ.BODY(100).AFTER_STR(“delim”).GET_SIGNED32(0, BIG_ENDIAN).SUB(1).SIGNED32_STRING(BIG_ENDIAN)
<unsigned_long_number>.UNSIGNED8_STRING	Produit une chaîne binaire non signée de 8 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_UNSIGNED8(24).TYPECAST_UNSIG
<unsigned_long_number>.UNSIGNED16_STRING	Produit une chaîne binaire non signée de 16 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).GET_UNSIGNED16(23, LIT-TLE_ENDIAN).TYPECAST_UNSIGNED_LONG_AT.ADD(10).UNSIG
<unsigned_long_number>.UNSIGNED32_STRING(<endianness>)	Produit une chaîne binaire non signée 32 bits représentant le nombre. Si la valeur est hors plage, une condition undef est déclenchée. Exemple : HTTP.REQ.BODY(100).AFTER_STR(“delim2”).GET_UNSIGNED3 BIG_ENDIAN).ADD(2).UNSIGNED32_STRING(BIG_ENDIAN)

Expressions basées sur un serveur virtuel

October 5, 2021

Le préfixe `SYS.VSERVER("<vserver-name>")` d’expression vous permet d’identifier un serveur

virtuel. Vous pouvez utiliser les fonctions suivantes avec ce préfixe pour récupérer des informations relatives au serveur virtuel spécifié :

- **DÉBIT.** Renvoie le débit du serveur virtuel en Mbps (mégabits par seconde). La valeur renvoyée est un nombre long non signé.

  Utilisation : SYS.VSERVER (« vserver ») .THROUGHPUT

- **CONNEXIONS.** Renvoie le nombre de connexions gérées par le serveur virtuel. La valeur renvoyée est un nombre long non signé.

  Utilisation : SYS.VSERVER (« vserver ») .CONNECTIONS

- **ÉTAT.** Renvoie l'état du serveur virtuel. La valeur renvoyée est UP, DOWN ou OUT_OF_SERVICE. L'une de ces valeurs peut donc être passée en argument à l'opérateur EQ () pour effectuer une comparaison qui aboutit à une valeur booléenne TRUE ou FALSE.

  Utilisation : SYS.VSERVER (« vserver ») .STATE

- **SANTÉ.** Renvoie le pourcentage de services en état UP pour le serveur virtuel spécifié. La valeur renvoyée est un nombre entier.

  Utilisation : SYS.VSERVER (« vserver ») .HEALTH

- **RESPTIME.** Renvoie le temps de réponse sous la forme d'un nombre entier représentant le nombre de microsecondes. Le temps de réponse est le TTFB (Time To First Byte) moyen de tous les services liés au serveur virtuel.

  Utilisation : SYS.VSERVER (« vserver ») .RESPTIME

- **SURGECOUNT.** Renvoie le nombre de demandes dans la file d'attente de surtension du serveur virtuel. La valeur renvoyée est un nombre entier.

  Utilisation : SYS.VSERVER (« vserver ») .SURGECOUNT

Exemple 1 :

La stratégie de réécriture suivante interrompt le traitement de réécriture si le nombre de connexions sur le serveur virtuel d'équilibrage de charge LBVServer dépasse 10 000 :

```
add rewrite policy norewrite_pol sys.vserver("LBvserver").connections.gt
(10000)norewrite
```

Exemple 2 :

L'action de réécriture suivante insère un en-tête personnalisé, TP, dont la valeur est le tout au long du serveur virtuel LBVServer :

```
add rewrite action tp_header insert_http_header TP SYS.VSERVER("LBvserver")
.THROUGHPUT
```

Exemple 3 :

L'action de message de journal d'audit suivante écrit le TTFB moyen des services liés à un serveur virtuel, dans le fichier journal newnslog :

```
add audit messageaction log_vserver_resptime_act INFORMATIONAL "\"NS
Response Time to Servers:\" + sys.vserver(\"ssllb\").resptime + \" millisec
\""-logtoNewnslog YES
```

Expressions de stratégie avancées : analyse des données HTTP, TCP et UDP

May 5, 2023

Vous pouvez configurer des expressions de stratégie avancées pour évaluer la charge utile dans une demande ou une réponse HTTP. La charge utile associée à une connexion HTTP inclut les en-têtes HTTP (en-têtes standard ou personnalisés), le corps et l'URL de connexion. Vous pouvez également évaluer et traiter la charge utile dans un paquet TCP ou UDP. Pour les connexions HTTP, par exemple, vous pouvez vérifier si un en-tête HTTP particulier est présent ou si l'URL inclut un paramètre de requête particulier.

Vous pouvez configurer des expressions pour transformer le codage URL et appliquer un codage HTML ou XML « sécurisé » pour une évaluation ultérieure. Vous pouvez également utiliser les préfixes XPATH et JSON pour évaluer la date dans les fichiers XML et JSON, respectivement.

Vous pouvez également utiliser des expressions de stratégie avancées basées sur le texte et numériques pour évaluer les données de requête et de réponse HTTP. Pour plus d'informations, consultez les sections Expressions de stratégie avancées : évaluation du texte et Expressions de stratégie avancées : utilisation des dates, des heures et des nombres.

Expressions permettant d'identifier le protocole dans un paquet IP entrant

May 5, 2023

Le tableau suivant répertorie les expressions que vous pouvez utiliser pour identifier le protocole dans un paquet entrant.

Expression	Description
CLIENT.IP.PROTOCOL	Identifie le protocole dans les paquets IPv4 envoyés par les clients.
CLIENT.IPV6.PROTOCOL	Identifie le protocole dans les paquets IPv6 envoyés par les clients.
PROTOCOLE SERVEUR.IP.	Identifie le protocole dans les paquets IPv4 envoyés par les serveurs.
SERVER.IPV6.PROTOCOL	Identifie le protocole dans les paquets IPv6 envoyés par les serveurs.

Arguments de la fonction PROTOCOL

Vous pouvez transmettre le numéro de protocole IANA (Internet Assigned Numbers Authority) à la fonction PROTOCOLE. Par exemple, si vous souhaitez déterminer si le protocole d'un paquet entrant est TCP, vous pouvez utiliser CLIENT.IP.PROTOCOL.EQ (6), où 6 est le numéro de protocole TCP attribué par l'IANA. Pour certains protocoles, vous pouvez transmettre une valeur d'énumération au lieu du numéro de protocole. Par exemple, au lieu de CLIENT.IP.PROTOCOL.EQ (6), vous pouvez utiliser CLIENT.IP.PROTOCOL.EQ (TCP). Le tableau suivant répertorie les protocoles pour lesquels vous pouvez utiliser des valeurs d'énumération, ainsi que les valeurs d'énumération correspondantes à utiliser avec la fonction PROTOCOL.

Protocole	Valeur d'énumération
Protocole de contrôle de transmission (TCP)	TCP
Protocole UDP (User Datagram Protocol)	UDP
Protocole ICMP (Internet Control Message Protocol)	ICMP
En-tête d'authentification IP (AH), pour fournir des services d'authentification en IPv4 et IPv6	AH
Protocole ESP (Encapsulating Security Payload)	ESP
Encapsulation générale du routage (GRE)	GRE
Protocole d'encapsulation IP-within-IP	IPIP
Protocole de message de contrôle Internet pour IPv6 (ICMPv6)	ICMPv6

Protocole	Valeur d'énumération
En-tête du fragment pour IPv6	FRAGMENT

Scénarios de cas d'utilisation

Les expressions de protocole peuvent être utilisées à la fois dans des politiques basées sur des demandes et des politiques basées sur des réponses. Vous pouvez utiliser les expressions dans diverses fonctionnalités de NetScaler, telles que l'équilibrage de charge, l'optimisation du WAN, la commutation de contenu, la réécriture et les politiques d'écoute. Vous pouvez utiliser les expressions avec des fonctions telles que EQ () et NE () pour identifier le protocole dans une politique et effectuer une action.

Voici quelques cas d'utilisation de ces expressions :

- Dans les configurations d'équilibrage de charge de Branch Repeater, vous pouvez utiliser les expressions dans une politique d'écoute pour le serveur virtuel générique. Par exemple, vous pouvez configurer le serveur virtuel générique à l'aide de la politique d'écoute CLIENT.IP.PROTOCOL.EQ (TCP) afin que le serveur virtuel traite uniquement le trafic TCP et relie simplement tout le trafic non TCP. Même si vous pouvez utiliser une liste de contrôle d'accès au lieu de la politique d'écoute, cette dernière permet de mieux contrôler le trafic traité.
- Pour les serveurs virtuels de commutation de contenu de type ANY, vous pouvez configurer des politiques de commutation de contenu qui commutent les demandes sur la base du protocole contenu dans les paquets entrants. Par exemple, vous pouvez configurer des politiques de commutation de contenu pour diriger tout le trafic TCP vers un serveur virtuel d'équilibrage de charge et tout le trafic non TCP vers un autre serveur virtuel d'équilibrage de charge.
- Vous pouvez utiliser les expressions basées sur le client pour configurer la persistance en fonction du protocole. Par exemple, vous pouvez utiliser CLIENT.IP.PROTOCOL pour configurer la persistance sur la base des protocoles dans les paquets IPv4 entrants.

Expressions pour les en-têtes HTTP et de contrôle de cache

August 20, 2021

Une méthode courante d'évaluation du trafic HTTP consiste à examiner les en-têtes d'une requête ou d'une réponse. Un en-tête peut effectuer un certain nombre de fonctions, notamment les suivantes :

- Fournissez des cookies qui contiennent des données sur l'expéditeur.
- Identifiez le type de données transmises.
- Identifiez l'itinéraire parcouru par les données (en-tête Via).

> **Remarque**
>
> Si une opération est utilisée pour évaluer les données d'en-tête et de texte, l'opération basée sur l'en-tête remplace toujours l'opération basée sur le texte. Par exemple, l'opération AFTER_STR, lorsqu'elle est appliquée à un en-tête, remplace les opérations AFTER_STR basées sur le texte pour toutes les instances du type d'en-tête actuel.

Préfixes pour les en-têtes HTTP

Le tableau Préfixes pour les en-têtes HTTP pour les préfixes d'expression qui extrait les en-têtes HTTP.

Opérations pour les en-têtes HTTP

Le tableau Opérations pour en-têtes HTTP pour les opérations que vous pouvez spécifier avec les préfixes des en-têtes HTTP.

Préfixes pour les en-têtes de contrôle de cache

Les préfixes suivants s'appliquent spécifiquement aux en-têtes Cache-Control.

Préfixe d'en-tête HTTP	Description
HTTP.REQ.CACHE_CONTROL	Renvoie un en-tête Cache-Control dans une requête HTTP.
HTTP.RES.CACHE_CONTROL	Renvoie un en-tête Cache-Control dans une réponse HTTP.

Opérations pour les en-têtes de contrôle de cache

Vous pouvez appliquer n'importe quelle opération pour les en-têtes HTTP aux en-têtes Cache-Control.

En outre, les opérations suivantes identifient des types spécifiques d'en-têtes Cache-Control. Reportez-vous à la section RFC 2616 pour plus d'informations sur ces types d'en-tête.

Opération d'en-tête HTTP	Description
`Cache-Control header.NAME(<integer>)`	Renvoie sous forme de valeur de texte le nom de l'en-tête Cache-Control qui correspond au nième composant d'une liste nom-valeur, comme spécifié par`<integer>`. L'index du composant nom-valeur est basé sur 0. Si le `<integer>` qui est spécifié par l'argument entier est supérieur au nombre de composants dans la liste, un objet texte de longueur nulle est renvoyé. Voici un exemple : `http.req.cache_control.name(3).contains("some_text")`
Cache-Control header.IS_INVALID	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control n'est pas présent dans la requête ou la réponse. Voici un exemple : `http.req.cache_control.is_invalid`
`Cache-Control header.IS_PRIVATE`	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Private. Voici un exemple : `http.req.cache_control.is_private`
Cache-Control header.IS_PUBLIC	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Private. Voici un exemple : http.req.cache_control.is_public
Cache-Control header.IS_NO_STORE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur No-Store. Voici un exemple : http.req.cache_control.is_no_store
Cache-Control header.IS_NO_CACHE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur No-Cache. Voici un exemple : http.req.cache_control.is_no_cache
Cache-Control header.IS_MAX_AGE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Max-Age. Voici un exemple : http.req.cache_control.is_max_age
Cache-Control header.IS_MIN_FRESH	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Min-Fresh. Voici un exemple : http.req.cache_control.is_min_fresh

Opération d'en-tête HTTP	Description
Cache-Control header.IS_MAX_STALE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Max-Stale. Voici un exemple : http.req.cache_control.is_max_stale
Cache-Control header.IS_MUST_REVALIDATE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Doit-Revalidate. Voici un exemple : http.req.cache_control.is_must_revalidate
Cache-Control header.IS_NO_TRANSFORM	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur No-Transform. Voici un exemple : http.req.cache_control.is_no_transform
Cache-Control header.IS_ONLY_IF_CACHED	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Only-If-Cached. Voici un exemple : http.req.cache_control.is_only_if_cached
Cache-Control header.IS_PROXY_REVALIDATE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur Proxy-Revalidate. Voici un exemple : http.req.cache_control.is_proxy_revalidate
Cache-Control header.IS_S_MAXAGE	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control a la valeur S-Maxage. Voici un exemple : http.req.cache_control.is_s_maxage
Cache-Control header.IS_UNKNOWN	Renvoie une valeur booléenne TRUE si l'en-tête Cache-Control est d'un type inconnu. Voici un exemple : http.req.cache_control.is_unknown
Cache-Control header.MAX_AGE	Renvoie la valeur de l'en-tête Cache-Control Max-Age. Si cet en-tête est absent ou non valide, 0 est renvoyé. Voici un exemple : http.req.cache_control.max_age.le(3)
Cache-Control header.MAX_STALE	Renvoie la valeur de l'en-tête Cache-Control Max-Stale. Si cet en-tête est absent ou non valide, 0 est renvoyé. Voici un exemple : http.req.cache_control.max_stale.le(3)

Opération d'en-tête HTTP	Description
Cache-Control header.MIN_FRESH	Renvoie la valeur de l'en-tête Cache-Control Min-Fresh. Si cet en-tête est absent ou non valide, 0 est renvoyé. Voici un exemple : http.req.cache_control.min_fresh.le (3)
Cache-Control header.S_MAXAGE	Renvoie la valeur de l'en-tête Cache-Control S-Maxage. Si cet en-tête est absent ou non valide, 0 est retourné.Folor est un exemple : http.req.cache_control.s_maxage.eq (2)

Expressions pour extraire des segments d'URL

August 20, 2021

Vous pouvez extraire des URL et des parties d'URL, telles que le nom d'hôte ou un segment du chemin d'URL. Par exemple, l'expression suivante identifie les requêtes HTTP pour les fichiers image en extrayant les suffixes de fichier image de l'URL :

```
http.req.url.suffix.eq("jpeg")|| http.req.url.suffix.eq("gif")
```

La plupart des expressions pour URL fonctionnent sur du texte et sont décrites dans Préfixes d'expression pour le texte dans les requêtes et réponses HTTP. Cette section traite de l'opération GET. L'opération GET extrait du texte lorsqu'elle est utilisée avec les préfixes suivants :

- HTTP.REQ.URL.PATH
- VPN.BASEURL.PATH
- VPN.CLIENTLESS_BASEURL.PATH

Le tableau suivant décrit les préfixes des URL HTTP.

Préfixe d'URL	Description
HTTP.REQ.URL.PATH.GET(<n>)	Renvoie une liste séparée par barre oblique (« / ») du chemin d'URL. Par exemple, considérez l'URL suivante :<`http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1`>. L'expression suivante renvoie dir1 à partir de cette URL :<`http.req.url.path.get(1)`>. L'expression suivante renvoie dir2 : http.req.url.path.get (2)
HTTP.REQ.URL.PATH.GET_REVERSE(<n>)	Retourne une liste slash- (« / ») séparée du chemin d'URL, à partir de la fin du chemin d'accès. Par exemple, considérez l'URL suivante :<`http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1`>. L'expression suivante renvoie index.html à partir de cette URL :<`http.req.url.path.get_reverse(0)`>. L'expression suivante renvoie dir3 : http.req.url.path.get_reverse(1)

Expressions pour les codes d'état HTTP et les données de charge utile HTTP numériques autres que les dates

January 21, 2021

Le tableau suivant décrit les préfixes pour les valeurs numériques dans les données HTTP autres que les dates.

Prefix	Description
HTTP.REQ.CONTENT_LENGTH	Renvoie la longueur d'une requête HTTP sous la forme d'un nombre. Voici un exemple : http.req.content_length < 500
HTTP.RES.CONTENT_LENGTH	Renvoie la longueur de la réponse HTTP sous la forme d'un nombre. Voici un exemple : http.res.content_length <= 1000
HTTP.RES.STATUS	Retourne le code d'état de la réponse

Prefix	Description
HTTP.RES.IS_REDIRECT	Renvoie une valeur booléenne TRUE si le code de réponse est associé à une redirection. Voici les codes de réponse de redirection : 300 (choix multiples), 301 (déplacement permanent), 302 (trouvé), 303 (voir autre), 305 (utilisation proxy) et 307 (redirection temporaire). Remarque : Le code d'état 304 n'est pas considéré comme un code d'état de la réponse HTTP de redirection. Le code d'état 306 n'est pas utilisé.

Expressions SIP

May 8, 2023

Le langage d'expressions de politique NetScaler Advanced contient un certain nombre d'expressions qui fonctionnent sur les connexions SIP (Session Initiation Protocol). Ces expressions sont destinées à être utilisées dans les politiques de tout protocole pris en charge qui fonctionne sur la base d'une demande/réponse. Ces expressions peuvent être utilisées dans les stratégies de commutation de contenu, de limitation de débit, de répondeur et de réécriture.

Certaines limitations s'appliquent aux expressions SIP utilisées avec les politiques de répondeur. Seules les actions DROP, NOOP ou RESPONDWITH sont autorisées sur un serveur virtuel d'équilibrage de charge SIP. Les politiques du répondeur peuvent être liées à un serveur virtuel d'équilibrage de charge, à un point de liaison global de remplacement, à un point de liaison global par défaut ou à une étiquette de politique sip_udp.

Le format d'en-tête utilisé par le protocole SIP est similaire à celui utilisé par le protocole HTTP, de sorte que la plupart des nouvelles expressions ressemblent et fonctionnent de manière très similaire à leurs analogues HTTP. Chaque en-tête SIP se compose d'une ligne qui inclut la méthode SIP, l'URL et la version, suivies d'une série de paires nom-valeur qui ressemblent à des en-têtes HTTP.

Voici un exemple d'en-tête SIP auquel il est fait référence dans les tableaux d'expressions situés en dessous :

```
1 INVITE sip:16@www.sip.com:5060;transport=udp SIP/2.0
2 Record-Route: <sip:200.200.100.22;lr=on>
3 Via: SIP/2.0/UDP 200.200.100.22;branch=z9hG4bK444b.c8e103d1.0;rport
     =5060;
4     received=10.102.84.18
```



```
Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;
    received=10.102.84.160
From: "12" <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53
   cc0185
To: "16" <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185
Call-ID: 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180
Max-Forwards: 69CSeq: 101 INVITE
User-Agent: Cisco-CP7940G/8.0
Contact: <sip:12@10.102.84.180:5060;transport=udp>
Expires: 180
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE
Supported: replaces,join,norefersub
Content-Length: 277
Content-Type: application/sdp
Content-Disposition: session;handling=optiona
<!--NeedCopy-->
```

Tableaux de référence SIP

Les tableaux suivants contiennent des listes d'expressions qui fonctionnent sur les en-têtes SIP. Le premier tableau contient des expressions qui s'appliquent aux en-têtes de requête. La plupart des expressions basées sur les réponses sont quasiment identiques aux expressions basées sur les requêtes correspondantes. Pour créer une expression de réponse à partir de l'expression de demande correspondante, vous modifiez les deux premières sections de l'expression de SIP.REQ en SIP.RES, et vous apportez d'autres ajustements évidents. Le deuxième tableau contient les expressions de réponse qui sont uniques aux réponses et qui n'ont aucun équivalent de demande. Vous pouvez utiliser n'importe quel élément des tableaux suivants comme expression complète à part entière, ou vous pouvez utiliser différents opérateurs pour combiner ces éléments d'expression avec d'autres afin de créer des expressions plus complexes.

Expressions de requête SIP

Expression	Description
MÉTHODE SIP.REQ.	Fonctionne selon la méthode de la requête SIP. Les méthodes de requête SIP prises en charge sont ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, REGISTER, SUBSCRIBE et UPDATE. Cette expression est une dérivée de la classe de texte, de sorte que toutes les opérations applicables au texte sont applicables à cette méthode. Par exemple, pour une requête SIP de type INVITE sip:16 @10 .102.84. 181:5060 ; transport=udp SIP/2.0, cette expression renvoie INVITE.
SIP.REQ.URL	Fonctionne sur l'URL de requête SIP. Cette expression est une dérivée de la classe de texte, de sorte que toutes les opérations applicables au texte sont applicables à cette méthode. Par exemple, pour une requête SIP de type INVITE sip:16 @10 .102.84. 181:5060 ; transport=udp SIP/2.0, cette expression renvoie ssip:16 @10 .102.84. 181:5060 ; transport=udp.
SIP.REQ.URL.PROTOCOL	Renvoie le protocole URL. Par exemple, pour une URL SIP de type sip : 16@www.sip.com:5060 ; transport=udp, cette expression renvoie sip.
SIP.REQ.URL.HOSTNAME	Renvoie la partie nom d'hôte de l'URL SIP. Par exemple, pour une URL SIP sip : 16@www.sip.com:5060 ; transport=udp, cette expression renvoie www.sip.com:5060.
SIP.REQ.URL.HOSTNAME.PORT	Renvoie la partie port du nom d'hôte de l'URL SIP. Si aucun port n'est spécifié, cette expression renvoie le port SIP par défaut, 5060. Par exemple, pour un nom d'hôte SIP www.sip.com:5060, cette expression renvoie 5060.

Expression	Description
SIP.REQ.URL.HOSTNAME.DOMAINE	Renvoie la partie nom de domaine du nom d'hôte de l'URL SIP. Si l'hôte est une adresse IP, cette expression renvoie un résultat incorrect. Par exemple, pour un nom d'hôte SIP www.sip.com:5060, cette expression renvoie sip.com. Pour un nom d'hôte SIP 192.168.43. 15:5060, cette expression renvoie une erreur.
SIP.REQ.URL.HOSTNAME.SERVER	Renvoie la partie serveur de l'hôte. Par exemple, pour un nom d'hôte SIP www.sip.com:5060, cette expression renvoie www.
SIP.REQ.URL.NOM D'UTILISATEUR	Renvoie le nom d'utilisateur qui précède le caractère @. Par exemple, pour une URL SIP de type sip : 16@www.sip.com:5060 ; transport=udp, cette expression renvoie 16.
SIP.REQ.VERSION	Renvoie le numéro de version SIP figurant dans la demande. Par exemple, pour une requête SIP de type INVITE sip:16 @10 .102.84. 181:5060 ; transport=udp SIP/2.0, cette expression renvoie SIP/2.0.
SIP.REQ.VERSION.MAJOR	Renvoie le numéro de version principal (le numéro situé à gauche du point). Par exemple, pour un numéro de version SIP SIP/2.0, cette expression renvoie 2.
SIP.REQ.VERSION.MINOR	Renvoie le numéro de version secondaire (le numéro situé à droite du point). Par exemple, pour un numéro de version SIP SIP/2.0, cette expression renvoie 0.
SIP.REQ.CONTENT_LENGTH	Renvoie le contenu de l'en-tête Content-Length. Cette expression est un dérivé de la classe thesip_header_t, de sorte que toutes les opérations disponibles pour les en-têtes SIP peuvent être utilisées. Par exemple, pour un en-tête SIP Content-Length de type Content-Length : 277, cette expression renvoie 277.

Expression	Description
SIP.REQ.TO	Renvoie le contenu de l'en-tête To. <sip:16@sip_example.com>Par exemple, pour un en-tête SIP To de type To : « 16 » ; tag=00127f54ec85a6d90cc14f45-53cc0185, cette <sip:16@sip_example.com> expression renvoie « 16 » ; tag=00127f54ec85a6d90cc14f45-53cc0185.
SIP.REQ.TO.ADDRESS	Renvoie l'URI SIP qui se trouve dans l'objet sip_url. Toutes les opérations disponibles pour les URI SIP peuvent être utilisées. Par exemple, pour un en-tête SIP To de type To : « 16 » <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, cette expression renvoie <sip:16@sip_example.com>.
SIP.REQ.TO.DISPLAY_NAME	Renvoie la partie du nom d'affichage de l'en-tête To. Par exemple, pour un en-tête SIP To de type To : « 16 » <sip:16@sip_example.com> ; tag=00127f54ec85a6d90cc14f45-53cc0185, cette expression renvoie 16.
SIP.REQ.TO.TAG	Renvoie la valeur « tag » issue de la paire nom-valeur « tag » dans l'en-tête TO. Par exemple, pour un en-tête SIP To de type To : « 16 » <sip:16@sip_example.com> ; tag=00127f54ec85a6d90cc14f45-53cc0185, cette expression renvoie 00127f54ec85a6d90cc14f45-53cc0185.
SIP.REQ.FROM	Renvoie le contenu de l'en-tête From. Par exemple, pour un en-tête SIP From de type From : « 12 » <sip:12@sip_example.com> ; tag=00127f54ec85a6d90cc14f45-53cc0185, cette expression renvoie <sip:12@sip_example.com>.

Expression	Description
SIP.REQ.FROM.ADDRESS	Renvoie l'URI SIP qui se trouve dans l'objet sip_url. Toutes les opérations disponibles pour les URI SIP peuvent être utilisées. Par exemple, pour un en-tête SIP From de type From : « 12 » <sip:12@sip_example.com> ; tag=00127f54ec85a6d90cc14f45-53cc0185, cette expression renvoie <sip:12@sip_example.com>.
SIP.REQ.FROM.DISPLAY_NAME	Renvoie la partie du nom d'affichage de l'en-tête To. Par exemple, pour un en-tête SIP From contenant la valeur From : « 12 » <sip:12@sip_example.com> ; tag=00127f54ec85a6d90cc14f45-53cc0185, cette expression renvoie 12.
SIP.REQ.FROM.TAG	Renvoie la valeur « tag » issue de la paire nom/valeur « tag » dans l'en-tête TO. Par exemple, pour un en-tête SIP From contenant la valeur From : « 12 » <sip:12@sip_example.com> ; tag=00127f54ec85a6d90cc14f45-53cc0185, cette expression renvoie 00127f54ec85a6d90cc14f45-53cc0185.
SIP.REQ.VIA	Renvoie l'en-tête Via complet. Si la requête contient plusieurs en-têtes Via, renvoie le dernier en-tête Via. Par exemple, pour les deux en-têtes Via de l'exemple d'en-tête SIP, cette expression renvoie Via : SIP/2.0/UDP 10.102.84. 180:5060 ; Branch=Z9HG4BK03E76D0B ; rport=5060 ; received=10.102.84.160.
SIP.REQ.VIA.SENTBY_ADDRESS	Renvoie l'adresse qui a envoyé la demande. Par exemple, pour l'en-tête Via Via : SIP/2.0/UDP 10.102.84. 180:5060 ; Branch=Z9hg4bk03e76d0b ; rport=5060 ; received=10.102.84.160, cette expression renvoie 10.102.84.180.

Expression	Description
SIP.REQ.VIA.SENTBY_PORT	Renvoie le port qui a envoyé la demande. Par exemple, pour l'en-tête Via Via : SIP/2.0/UDP 10.102.84. 180:5060 ; Branch=Z9HG4BK03E76D0B ; rport=5060 ; received=10.102.84.160, cette expression renvoie 5060.
SIP.REQ.VIA.RPORT	Renvoie la valeur de la paire nom/valeur du rapport. Par exemple, pour l'en-tête Via Via : SIP/2.0/UDP 10.102.84. 180:5060 ; Branch=Z9HG4BK03E76D0B ; rport=5060 ; received=10.102.84.160, cette expression renvoie 5060.
SIP.REQ.VIA.BRANCH	Renvoie la valeur de la paire nom/valeur de la branche. Par exemple, pour l'en-tête Via Via : SIP/2.0/UDP 10.102.84. 180:5060 ; Branch=Z9hg4bk03e76d0b ; rport=5060 ; received=10.102.84.160, cette expression renvoie Z9hg4bk03e76d0b.
SIP.REQ.VIA.RECEIVED	Renvoie la valeur de la paire nom/valeur reçue. Par exemple, pour l'en-tête Via Via : SIP/2.0/UDP 10.102.84. 180:5060 ; Branch=Z9hg4bk03e76d0b ; rport=5060 ; received=10.102.84.160, cette expression renvoie 10.102.84.160.
SIP.REQ.CALLLID	Renvoie le contenu de l'en-tête Callid. Cette expression est un dérivé de la classe thesip_header_t, de sorte que toutes les opérations disponibles pour les en-têtes SIP peuvent être utilisées. Par exemple, pour un en-tête SIP Callid dont l'ID d'appel est 00127f54-ec850017-0e46f5b9-5ec149c2 @10 .102.84.180, cette expression renvoie 00127f54-ec850017-0e46f5b9-5ec149c2 @10 .102.84.180.

Expression	Description
SIP.REQ.CSEQ	Renvoie le numéro CSEQ à partir du CSEQ, sous la forme d'un entier. Par exemple, pour un en-tête SIP CSEQ de type CSeq : 101 INVITE, cette expression renvoie 101.
<header_name>EN-TÊTE SIP.REQ.(\)	Renvoie l'en-tête SIP spécifié. <header_name>Remplacez par le nom de l'en-tête de votre choix. Par exemple, pour renvoyer l'en-tête SIP From, vous devez taper SIP.REQ.HEADER (« From »).
<line_number>SIP.REQ.HEADER (\ <header_name>) .INSTANCE (\)	Renvoie l'instance spécifiée de l'en-tête SIP spécifié. Plusieurs instances du même en-tête SIP peuvent se produire. Lorsque vous souhaitez obtenir une instance spécifique d'un tel en-tête SIP (par exemple, un en-tête Via spécifique), vous pouvez spécifier cet en-tête en saisissant un nombre sous la forme du<line_number>. Les instances d'en-tête sont mises en correspondance de la dernière (0) à la première. En d'autres termes, SIP.REQ.HEADER (« Via ») .INSTANCE (0) renvoie la dernière instance de l'en-tête Via, tandis que SIP.REQ.HEADER (« Via ») .INSTANCE (1) renvoie la dernière instance sauf une de l'en-tête Via, et ainsi de suite. Par exemple, s'il est utilisé dans l'exemple d'en-tête SIP, SIP.REQ.HEADER (« Via ») .INSTANCE (1) renvoie VIA : SIP/2.0/UDP 10.102.84. 180:5060 ; Branch=Z9HG4BK03E76D0B ; rport=5060.
<line_number>SIP.REQ.HEADER (\ <header_name>) .VALEUR (\)	Renvoie le contenu de l'instance spécifiée de l'en-tête SIP spécifié. L'utilisation est presque identique à celle de l'expression précédente. Par exemple, s'il est utilisé dans l'exemple d'en-tête SIP figurant dans l'entrée du tableau précédent, SIP.REQ.HEADER (« Via ») .VALUE (1) renvoie SIP/2.0/UDP 10.102.84. 180:5060 ; Branch=Z9HG4BK03E76D0B ; rport=5060.

Expression	Description
<header_name>SIP.REQ.HEADER (\) .COUNT	Renvoie le nombre d'instances d'un en-tête particulier sous forme d'entier. Par exemple, s'il est utilisé dans l'exemple d'en-tête SIP ci-dessus, SIP.REQ.HEADER (« Via ») .COUNT renvoie 2.
<header_name>SIP.REQ.HEADER (\) .EXISTS	Renvoie une valeur booléenne vraie ou fausse, selon que l'en-tête spécifié existe ou non. Par exemple, s'il est utilisé dans l'exemple d'en-tête SIP ci-dessus, SIP.REQ.HEADER (« Expires ») .existsRenvoie la valeur true, tandis que SIP.REQ.HEADER (« Caller-ID ») .EXISTS renvoie la valeur false.
<header_name>SIP.REQ.HEADER (\) .LISTE	Renvoie la liste des paramètres séparés par des virgules dans l'en-tête spécifié. Par exemple, s'il est utilisé dans l'exemple d'en-tête SIP ci-dessus, SIP.REQ.HEADER (« Allow ») .LIST renvoie ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER, UPDATE. Vous pouvez ajouter la chaîne .GET (<list_item_number>) pour sélectionner un élément de liste spécifique. Par exemple, pour obtenir le premier élément (ACK) de la liste ci-dessus, vous devez taper SIP.REQ.HEADER (« Allow ») .LIST.GET (0). Pour extraire le second élément (BYE), tapez SIP.REQ.HEADER (« Allow ») .LIST.GET (1). Remarque : Si l'en-tête spécifié contient une liste de paires nom/valeur, la paire nom/valeur complète est renvoyée.

Expression	Description
<in_header_name>SIP.REQ.HEADER (\ <header_name>) .TYPECAST_SIP_HEADER_T (« \ «)	<header_name><in_header_name>Typecast vers. N'importe quel texte peut être typé dans la classe sip_header_t, après quoi toutes les opérations basées sur les en-têtes peuvent être utilisées. Après avoir effectué cette opération, vous pouvez appliquer toutes les opérations pouvant être utilisées avec<in_header_name>. Par exemple, l'expression SIP.REQ.CONTENT_LENGTH.TYPECAST_SIP_HEADER_T classe toutes les instances de l'en-tête Content-Length. Après avoir effectué cette opération, vous pouvez appliquer toutes les opérations d'en-tête à toutes les instances de l'en-tête spécifié.
<string>SIP.REQ.HEADER (\ <header_name>) .CONTIENT (\).	Renvoie la valeur booléenne true si la chaîne de texte spécifiée est présente dans n'importe quelle instance de l'en-tête spécifié. Fonctionne sur toutes les instances de l'en-tête spécifié. Les instances d'en-tête sont mises en correspondance de la dernière (0) à la première.
<patset>SIP.REQ.HEADER (\ <header_name>) .EQUALS_ANY (\)	Renvoie la valeur booléenne true si un modèle associé à \ <patset> correspond à un contenu quelconque dans n'importe quelle instance de l'en-tête spécifié. Fonctionne sur toutes les instances de l'en-tête spécifié. Les instances d'en-tête sont mises en correspondance de la dernière (0) à la première.
<patset>SIP.REQ.HEADER (\ <header_name>) .CONTIENS_ANY (\)	Renvoie la valeur booléenne true si un modèle associé à \ <patset> correspond à un contenu quelconque dans n'importe quelle instance de l'en-tête spécifié. Fonctionne sur toutes les instances de l'en-tête spécifié. Les instances d'en-tête sont mises en correspondance de la dernière (0) à la première.

Expression	Description
<patset>SIP.REQ.HEADER (\ <header_name>) .CONTAINS_INDEX (\)	Renvoie l'index du modèle correspondant associé à \ <patset> si ce modèle correspond à n'importe quel contenu de n'importe quelle instance de l'en-tête spécifié. Fonctionne sur toutes les instances de l'en-tête spécifié. Les instances d'en-tête sont mises en correspondance de la dernière (0) à la première.
<patset>SIP.REQ.HEADER (\ <header_name>) .EQUALS_INDEX (\)	Renvoie l'index du modèle correspondant associé à \ <patset> si ce modèle correspond à n'importe quelle instance de l'en-tête spécifié. Fonctionne sur toutes les instances de l'en-tête spécifié. Les instances d'en-tête sont mises en correspondance de la dernière (0) à la première.
<string>SIP.REQ.HEADER (\ <header_name>) .SUBSTR (\)	Si la chaîne spécifiée est présente dans n'importe quelle instance de l'en-tête spécifié, cette expression renvoie cette chaîne. Par exemple, pour l'en-tête SIP Via : SIP/2.0/UDP 10.102.84. 180:5060 ; Branch=Z9HG4BK03E76D0B ; rport=5060 ; received=10.102.84.160", SIP.REQ.HEADER (« Via ») .SUBSTR (« rport=5060") renvoie « rport=5060". SIP.REQ.header (« Via ») .SUBSTR (« rport=5061") renvoie une chaîne vide.
<string>SIP.REQ.HEADER (\ <header_name>) .AFTER_STR (\)	Si la chaîne spécifiée est présente dans n'importe quelle instance de l'en-tête spécifié, cette expression renvoie la chaîne immédiatement après cette chaîne. Par exemple, pour l'en-tête SIP Via : SIP/2.0/UDP 10.102.84. 180:5060 ; branch=Z9hg4bk03e76d0b ; rport=5060 ; received=10.102.84.160, l'expression SIP.REQ.HEADER (« Via ») .AFTER_STR (« rport= ») renvoie 5060.

Expression	Description
<regex>SIP.REQ.HEADER (\ <header_name>) .REGEX_MATCH (\)	Renvoie la valeur booléenne true si l'expression régulière spécifiée (regex) correspond à n'importe quelle instance de l'en-tête spécifié. <same delimiter>Vous devez spécifier l'expression régulière au format suivant : re \regular <delimiter> expression \. La longueur de l'expression régulière ne peut pas dépasser 1 499 caractères. Il doit être conforme à la bibliothèque d'expressions régulières PCRE. Consultez http://www.pcre.org/pcre.txt la documentation sur la syntaxe des expressions régulières PCRE. La page de manuel pcrepattern contient également des informations utiles sur la spécification de modèles à l'aide d'expressions régulières PCRE. La syntaxe des expressions régulières prise en charge dans cette expression présente certaines différences par rapport au PCRE. Les références rétrospectivement ne sont pas autorisées. Vous devez éviter les expressions régulières récursives ; bien que certaines fonctionnent, d'autres ne le font pas. Le métacaractère point (.) correspond aux sauts de ligne. L'Unicode n'est pas pris en charge. set_text_mode (IGNORECASE) remplace le (? i) option interne spécifiée dans l'expression régulière.

Expression	Description
<regex>SIP.REQ.HEADER (\ <header_name>) .REGEX_SELECT (\)	Si la regex spécifiée correspond à n'importe quel texte dans n'importe quelle instance de l'en-tête spécifié, cette expression renvoie le texte. Par exemple, pour l'en-tête SIP Via : SIP/2.0/UDP 10.102.84. 180:5060 ; branch=Z9hg4bk03e76d0b ; rport=5060 ; received=10.102.84.160, l'expression SIP.REQ.HEADER (« Via ») .REGEX_SELECT (« received= [0-9] {1,3}. [0-9] {1,3}. [0-9] {1,3}. [0-9] {1,3}. [0-9] {1,3} ») renvoie received=10.102.84,160.
<regex>SIP.REQ.HEADER (\ <header_name>) .AFTER_REGEX (\)	Si la regex spécifiée correspond à n'importe quel texte dans n'importe quelle instance de l'en-tête spécifié, cette expression renvoie la chaîne immédiatement après ce texte. Par exemple, pour l'en-tête SIP Via : SIP/2.0/UDP 10.102.84. 180:5060 ; branch=Z9hg4bk03e76d0b ; rport=5060 ; received=10.102.84.160, l'expression SIP.REQ.HEADER (« Via ») .AFTER_REGEX (« received= ») renvoie 10.102.84.160.
<regex>SIP.REQ.HEADER (\ <header_name>) .BEFORE_REGEX (\)	Si la regex spécifiée correspond à n'importe quel texte dans n'importe quelle instance de l'en-tête spécifié, cette expression renvoie la chaîne juste avant ce texte. Par exemple, pour l'en-tête SIP Via : SIP/2.0/UDP 10.102.84. 180:5060 ; branch=Z9hg4bk03e76d0b ; rport=5060 ; received=10.102.84.160, l'expression SIP.REQ.HEADER (« Via ») .BEFORE_REGEX (« [0-9] {1,3}. [0-9] {1,3}. [0-9] {1,3}. [0-9] {1,3}. [0-9] {1,3} ») renvoie received=.
SIP.REQ.FULL_HEADER	Renvoie l'en-tête SIP complet, y compris le CR/LF de terminaison.
SIP.REQ.IS_VALID	Renvoie la valeur booléenne true si le format de demande est valide.

Expression	Description
<length>SIP.REQ.BODY (\)	Renvoie le corps de la requête, jusqu'à la longueur spécifiée. Si la longueur spécifiée est supérieure à la longueur du corps de la requête, cette expression renvoie le corps entier de la requête.
SIP.REQ.LB_VSERVER	Renvoie le nom du serveur virtuel d'équilibrage de charge (LB vserver) qui traite la demande en cours.
SIP.REQ.CS_VSERVER	Renvoie le nom du serveur virtuel de commutation de contenu (CS vserver) qui traite la demande en cours.

Expressions de réponse SIP

Expression	Description
SIP.RES.STATUS	Renvoie le code d'état de la réponse SIP. Par exemple, si la première ligne de la réponse est SIP/2.0 100 Trying, cette expression renvoie 100.
SIP.RES.STATUS_MSG	Renvoie le message d'état de la réponse SIP. Par exemple, si la première ligne de la réponse est SIP/2.0 100 Trying, cette expression renvoie Trying.
SIP.RES.IS_REDIRECT	Renvoie la valeur booléenne true si le code de réponse est une redirection.
MÉTHODE SIP.RES	Renvoie la méthode de réponse extraite de la chaîne de méthode request dans l'en-tête CSeq.

Opérations relatives au codage HTTP, HTML et XML et aux caractères « sécurisés »

May 8, 2023

Les opérations suivantes fonctionnent avec le codage des données HTML dans une requête ou une réponse et des données XML dans un corps POST.

- **\.HTML_XML_SAFE : transforme**
  <text> les caractères spéciaux en format sécurisé XML, comme dans les exemples suivants :

  Un support d'angle pointant vers la gauche (<) est converti en <
  Un support d'angle pointant vers la droite (>) est converti en
  Une esperluette (&) est convertie en &
  Cette opération protège contre les attaques de script intersites. La longueur maximale du texte transformé est de 2 048 octets. Il s'agit d'une opération en lecture seule.

  Après avoir appliqué la transformation, les opérateurs supplémentaires que vous spécifiez dans l'expression sont appliqués au texte sélectionné. Voici un exemple :

  http.req.url.query.html_xml_safe. contient (« MyQueryString »)

- **\.HTTP_HEADER_SAFE : convertit**
  <text> tous les nouveaux caractères de ligne ('\ n') du texte d'entrée en' A 'pour permettre à l'entrée d'être utilisée en toute sécurité dans les en-têtes HTTP.

  Cette opération permet de se prémunir contre les attaques par fractionnement des réponses.

  La longueur maximale du texte transformé est de 2 048 octets. Il s'agit d'une opération en lecture seule.

- **\.HTTP_URL_SAFE : convertit les caractères d'URL dangereux en**
  <text> valeurs « %xx », où « xx » est une représentation hexadécimale du caractère saisi. Par exemple, l'esperluette (&) est représentée par %26 dans le codage sécurisé pour les URL. La longueur maximale du texte transformé est de 2 048 octets. Il s'agit d'une opération en lecture seule.

  Vous trouverez ci-dessous les caractères sécurisés pour les URL. Tous les autres ne sont pas sûrs :

  - Caractères alphanumériques : a-z, A-Z, 0-9
  - Astérix : « * »
  - Espluette : « & »
  - Signe AT : « @ »
  - Deux points : « : »
  - Virgule : «, »
  - Dollar : « $ »
  - Point : ». «
  - Égal à : « = »
  - Point d'exclamation : « ! «
  - Trait d'union : « - »

- Ouvrez et fermez les parenthèses : « («, «) »
- Pourcentage : « % »
- Plus : « + »
- Point-virgule : « ; »
- Citation unique : « ’»
- barre oblique : «/»
- Point d’interrogation : « ? «
- Titre : « ~ »
- Souligner : « _ »

- **<text>\.MARK_SAFE :**

  Marque le texte comme sûr sans appliquer aucun type de transformation de données.

- **<text>\.SET_TEXT_MODE (URLENCODE|NOULENCODÉ)**

  Transforme tout le codage %HH du flux d’octets. Cette opération fonctionne avec des caractères (pas des octets). Par défaut, un seul octet représente un caractère dans le codage ASCII. Toutefois, si vous spécifiez le mode URLENCODED, trois octets peuvent représenter un caractère.

  Dans l’exemple suivant, une opération PREFIX (3) sélectionne les 3 premiers caractères d’une cible.

  ```
  http.req.url.hostname.prefix(3)
  ```

  Dans l’exemple suivant, NetScaler peut sélectionner jusqu’à 9 octets à partir de la cible :

  ```
  http.req.url.hostname.set_text_mode(urlencoded).prefix(3)
  ```

- **<text>\.SET_TEXT_MODE (PLUS_AS_SPACE|NO_PLUS_AS_SPACE) :**

  Spécifie comment traiter le caractère plus (+). L’option PLUS_AS_SPACE remplace le caractère plus par un espace blanc. Par exemple, le texte « bonjour+monde » devient « bonjour tout le monde ». « L’option NO_PLUS_AS_SPACE laisse les caractères plus tels quels.

- **<text>\.SET_TEXT_MODE (BACKSLASH_ENCODED|NO_BACKSLASH_ENCODED) :**

  <text>Spécifie si le décodage de la barre oblique inverse est effectué sur l’objet texte représenté par \.

  Si BACKSLASH_ENCODED est spécifié, l’opérateur SET_TEXT_MODE effectue les opérations suivantes sur l’objet texte :

  - Toutes les occurrences de « \ XXX » seront remplacées par le caractère « Y » (où XXX représente un nombre dans le système octal et Y représente l’équivalent ASCII de XXX). La plage de valeurs octales valide pour ce type de codage est comprise entre 0 et 377. Par exemple, les textes codés « http \ 72// » et http \ 072// » seront tous deux décodés <http**:**//>, où les deux points (:) sont l’équivalent ASCII de la valeur octale « 72 ».

- Toutes les occurrences de « \ xHH » seront remplacées par le caractère « Y » (HH représente un nombre dans le système hexadécimal et Y indique l'équivalent ASCII de HH. Par exemple, le texte codé « http \ x3a// » sera décodé <http://>, où les deux points (:) sont l'équivalent ASCII de la valeur hexadécimale « 3a ».
- Toutes les occurrences de « \ uWWxx » seront remplacées par la séquence de caractères « YZ » (où WW et XX représentent deux valeurs hexadécimales distinctes et Y et Z représentent leurs équivalents ASCII de WW et XX respectivement). Par exemple, les textes codés « http%u3a2f/ » et « http%u003a// » seront tous deux décodés <http://>, où « 3a » et « 2f » sont deux valeurs hexadécimales et les deux points (:) et la barre oblique («/») représentent leurs équivalents ASCII respectivement.
- Toutes les occurrences de « \ b », « \ n », « \ t », « \ f » et « \ r » sont remplacées par les caractères ASCII correspondants.

Si NO_BACKSLASH_ENCODED est spécifié, le décodage de la barre oblique inverse n'est pas effectué sur l'objet texte.

- **<text>\.SET_TEXT_MODE (BAD_ENCODE_RAISE_UNDEF|NO_BAD_ENCODE_RAISE_UNDEF) :**

  <text>Exécute l'action non définie associée si le mode URLENCODED ou BACKSLASH_ENCODED est défini et qu'un mauvais codage correspondant au mode de codage spécifié est détecté dans l'objet texte représenté par \.

  <text>Si NO_BAD_ENCODE_RAISE_UNDEF est spécifié, l'action non définie associée ne sera pas exécutée en cas de mauvais encodage dans l'objet texte représenté par \.

Expressions pour les données TCP, UDP et VLAN

May 8, 2023

Les données TCP et UDP prennent la forme d'une chaîne ou d'un nombre. Pour les préfixes d'expression qui renvoient des valeurs de chaîne pour les données TCP et UDP, vous pouvez appliquer toutes les opérations basées sur le texte. Pour plus d'informations, voir Expressions de stratégie avancées : évaluation du texte.

Pour les préfixes d'expression qui renvoient une valeur numérique, comme un port source, vous pouvez appliquer une opération arithmétique. Pour plus d'informations, voir Opérations de base sur les préfixes d'expression et Opérations composées pour les nombres.

Le tableau suivant décrit les préfixes qui extraient les données TCP et UDP du client.

Opération GET	Description
CLIENT.TCP.PAYLOAD ()<integer>	Renvoie les données de la charge utile TCP sous forme de chaîne, en commençant par le premier caractère de la charge utile et en continuant jusqu'au nombre de caractères de l'argument <integer>. Vous pouvez appliquer n'importe quelle opération textuelle à ce préfixe.
CLIENT.TCP.SRCPORT	Renvoie l'ID du port source du paquet actuel sous forme de nombre.
CLIENT.TCP.DSTPORT	Renvoie l'ID du port de destination du paquet actuel sous forme de nombre.
CLIENT.TCP.OPTIONS	Renvoie les options TCP définies par le client. Parmi les options TCP, citons la taille maximale des segments (MSS), l'échelle de fenêtre, les accusés de réception sélectifs (SACK) et l'option d'horodatage. Les opérateurs COUNT, TYPE (<type>), et TYPE_NAME (<m>) peuvent être utilisés avec ce préfixe. Pour les options TCP définies par le serveur, consultez le préfixe SERVER.TCP.OPTIONS.
CLIENT.TCP.OPTIONS.COUNT	Renvoie le nombre d'options TCP que le client a définies.
<type>CLIENT.TCP.OPTIONS.TYPE (\)	Renvoie la valeur de l'option TCP dont le type (ou le type d'option) est spécifié comme argument. La valeur est renvoyée sous la forme d'une chaîne d'octets au format Big Endian (ou ordre des octets du réseau). Paramètres : type - Valeur du type

Opération GET	Description
<m>CLIENT.TCP.OPTIONS.TYPE_NAME (\)	Renvoie la valeur de l'option TCP dont la constante d'énumération est spécifiée comme argument. Les constantes d'énumération que vous pouvez transmettre comme argument sont REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW et MAXSEG. Pour spécifier le type d'option TCP au lieu de ces constantes d'énumération, utilisez CLIENT.TCP.OPTIONS.TYPE(<type>). Pour les autres options TCP, vous devez utiliser CLIENT.TCP.OPTIONS.TYPE(<type>). Paramètres : m - Constante d'énumération des options TCP
CLIENT.TCP.REPEATER_OPTION.EXISTS	Renvoie une valeur booléenne TRUE si les options TCP du répéteur existent.
CLIENT.TCP.REPEATER_OPTION.IP	Renvoie l'adresse IPv4 du répéteur de branche à partir des options TCP du répéteur.
CLIENT.TCP.REPEATER_OPTION.MAC	Renvoie l'adresse MAC du répéteur de branche à partir des options TCP du répéteur.
CLIENT.UDP.DNS.DOMAIN	Renvoie le nom de domaine DNS.
CLIENT.UDP.DNS.DOMAIN.EQ("<hostname>")	Renvoie une valeur booléenne TRUE si le nom de domaine correspond à l'argument <hostname>. La comparaison ne tient pas compte des majuscules et des minuscules. Voici un exemple : client.udp.dns.domain.eq("www.mycompany.com")
CLIENT.UDP.DNS.IS_AAAAREC	Renvoie une valeur booléenne TRUE si le type d'enregistrement est AAAA. Ces types d'enregistrements indiquent une adresse IPv6 dans les recherches directes.
CLIENT.UDP.DNS.IS_ANYREC	Renvoie une valeur booléenne TRUE s'il s'agit d'un type d'enregistrement quelconque.
CLIENT.UDP.DNS.IS_AREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type A. Les enregistrements de type A fournissent l'adresse de l'hôte.

Opération GET	Description
CLIENT.UDP.DNS.IS_CNAMEREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type CNAME. Dans les systèmes qui utilisent plusieurs noms pour identifier une ressource, il existe un nom canonique et plusieurs alias. Le CNAME fournit le nom canonique.
CLIENT.UDP.DNS.IS_MXREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type MX (échangeur de courrier). Cet enregistrement DNS décrit une priorité et un nom d'hôte. Les enregistrements MX pour le même nom de domaine indiquent les serveurs de messagerie du domaine et la priorité de chaque serveur.
CLIENT.UDP.DNS.IS_NSREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type NS. Il s'agit d'un enregistrement de serveur de noms qui inclut un nom d'hôte et un enregistrement A associé. Cela permet de localiser le nom de domaine associé à l'enregistrement NS.
CLIENT.UDP.DNS.IS_PTRREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type PTR. Il s'agit d'un pointeur de nom de domaine qui est souvent utilisé pour associer un nom de domaine à une adresse IPv4.
CLIENT.UDP.DNS.IS_SOAREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type SOA. C'est le début d'un record d'autorité.
CLIENT.UDP.DNS.IS_SRVREC	Renvoie une valeur booléenne TRUE si l'enregistrement est de type SRV. Il s'agit d'une version plus générale de l'enregistrement MX.
CLIENT.UDP.DSTPORT	Renvoie l'identifiant numérique du port de destination UDP du paquet actuel.
CLIENT.UDP.SRCPORT	Renvoie l'identifiant numérique du port source UDP du paquet actuel.
CLIENT.UDP.LENGTH	Renvoie l'identifiant numérique de la longueur UDP du paquet actuel.

Opération GET	Description
CLIENT.UDP.CHECKSUM	Renvoie l'identifiant numérique de la somme de contrôle UDP du paquet actuel.
CLIENT.UDP.PAYLOAD	Renvoie la charge utile UDP du paquet actuel.
CLIENT.UDP.RADIUS	Renvoie les données RADIUS pour le paquet actuel.
<type>CLIENT.UDP.RADIUS.ATTR_TYPE (\)	Renvoie la valeur du type d'attribut spécifié comme argument.
CLIENT.UDP.RADIUS.USERNAME	Renvoie le nom d'utilisateur RADIUS.
CLIENT.TCP.MSS	Renvoie la taille de segment maximale (MSS) pour la connexion en cours sous forme de nombre.
CLIENT.VLAN.ID	Renvoie l'ID numérique du VLAN par lequel le paquet actuel est entré dans NetScaler.

Le tableau suivant décrit les préfixes qui extraient les données TCP et UDP du serveur.

Opération GET	Description
SERVER.TCP.DSTPORT	Renvoie l'identifiant numérique du port de destination du paquet actuel.
SERVEUR.TCP.SRCPORT	Renvoie l'identifiant numérique du port source du paquet actuel.
SERVER.TCP.OPTIONS	Renvoie les options TCP définies par le serveur. Parmi les options TCP, citons la taille maximale des segments (MSS), l'échelle de fenêtre, les accusés de réception sélectifs (SACK) et l'option d'horodatage. Les opérateurs COUNT, TYPE (<type>), et TYPE_NAME (<m>) peuvent être utilisés avec ce préfixe. Pour les options TCP définies par le client, consultez le préfixe CLIENT.TCP.OPTIONS.
SERVER.TCP.OPTIONS.COUNT	Renvoie le nombre d'options TCP définies par le serveur.

Opération GET	Description
<type>SERVEUR.TCP.OPTIONS.TYPE (\)	Renvoie la valeur de l'option TCP dont le type (ou le type d'option) est spécifié comme argument. La valeur est renvoyée sous la forme d'une chaîne d'octets au format Big Endian (ou ordre des octets du réseau). Paramètres : type - Valeur du type
<m>SERVEUR.TCP.OPTIONS.TYPE_NAME (\)	Renvoie la valeur de l'option TCP dont la constante d'énumération est spécifiée comme argument. Les constantes d'énumération que vous pouvez transmettre comme argument sont REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW et MAXSEG. Pour spécifier le type d'option TCP au lieu de ces constantes d'énumération, utilisez CLIENT.TCP.OPTIONS.TYPE(<type>). Pour les autres options TCP, vous devez utiliser CLIENT.TCP.OPTIONS.TYPE(<type>). Paramètres : m - Constante d'énumération des options TCP
SERVEUR.VLAN	Fonctionne sur le VLAN par lequel le paquet actuel est entré dans NetScaler.
SERVEUR.UDP.DSTPORT	Renvoie l'identifiant numérique du port de destination UDP du paquet actuel.
SERVEUR.UDP.SRCPORT	Renvoie l'identifiant numérique du port source UDP du paquet actuel.
SERVER.UDP.LENGTH	Renvoie l'identifiant numérique de la longueur UDP du paquet actuel.
SERVER.UDP.CHECKSUM	Renvoie l'identifiant numérique de la somme de contrôle UDP du paquet actuel.
SERVEUR.UDP.PAYLOAD	Renvoie la charge utile UDP du paquet actuel.
SERVER.VLAN.ID	Renvoie l'ID numérique du VLAN par lequel le paquet actuel est entré dans NetScaler.

Expressions pour évaluer un message DNS et identifier son protocole porteur

January 26, 2022

Vous pouvez évaluer les demandes et les réponses DNS à l'aide d'expressions commençant par DNS.REQ et DNS.RES, respectivement. Vous pouvez également identifier le protocole de la couche transport utilisé pour envoyer les messages DNS.

Les fonctions suivantes renvoient le contenu d'une requête DNS.

Fonction	Description
DNS.REQ.QUESTION.DOMAIN	Renvoie le nom de domaine (la valeur du champ QNAME) dans la section question de la requête DNS. Le nom de domaine est renvoyé sous forme de chaîne de texte, qui peut être transmise à EQ (), NE () et à toute autre fonction qui fonctionne avec du texte.
DNS.REQ.QUESTION.TYPE	Renvoie le type de requête (la valeur du champ QTYPE) dans la requête DNS. Le champ indique le type d'enregistrement de ressource (par exemple, A, NS ou CNAME) pour lequel le serveur de noms est interrogé. La valeur renvoyée peut être comparée à l'une des valeurs suivantes en utilisant les fonctions EQ () et NE () : A, AAAA, NS, SRV, PTR, CNAME, SOA, MX et ANY. Remarque : Vous ne pouvez utiliser que les fonctions EQ () et NE () avec la fonction TYPE. Exemple : DNS.REQ.QUESTION.TYPE.EQ (MX)

Les fonctions suivantes renvoient le contenu d'une réponse DNS.

Fonction	Description
DNS.RES.HEADER.RCODE	Renvoie le code de réponse (la valeur du champ RCODE) dans la section d'en-tête de la réponse DNS. Vous ne pouvez utiliser que les fonctions EQ () et NE () avec la fonction RCODE. Les valeurs possibles sont les suivantes : NOERROR, FORMERR, SERVFAIL, NXDOMAIN, NOTIMP et REFUSED.
DNS.RES.QUESTION.DOMAIN	Renvoie le nom de domaine (la valeur du champ QNAME) dans la section question de la réponse DNS. Le nom de domaine est renvoyé sous forme de chaîne de texte, qui peut être transmise à EQ (), NE () et à toute autre fonction qui fonctionne avec du texte.
DNS.RES.QUESTION.TYPE	Renvoie le type de requête (la valeur du champ QTYPE) dans la section question de la réponse DNS. Le champ indique le type d'enregistrement de ressource (par exemple, A, NS ou CNAME) contenu dans la réponse. La valeur renvoyée peut être comparée à l'une des valeurs suivantes en utilisant les fonctions EQ() et NE() : A, AAAA, NS, SRV, PTR, CNAME, SOA, MX et ANY. Vous ne pouvez utiliser que les fonctions EQ() et NE() avec la fonction TYPE. Exemple : DNS.RES.QUESTION.TYPE.EQ (SOA)

Les fonctions suivantes renvoient le nom du protocole de la couche transport.

Fonction	Description
DNS.REQ.TRANSPORT	Renvoie le nom du protocole de la couche transport qui a été utilisé pour envoyer la requête DNS. Les valeurs possibles renvoyées sont TCP et UDP. Vous ne pouvez utiliser que les fonctions EQ () et NE () avec la fonction TRANSPORT. Exemple : DNS.REQ.TRANSPORT.EQ (TCP)

Fonction	Description
DNS.RES.TRANSPORT	Renvoie le nom du protocole de la couche transport qui a été utilisé pour la réponse DNS. Les valeurs possibles renvoyées sont TCP et UDP. Vous ne pouvez utiliser que les fonctions EQ () et NE () avec la fonction TRANSPORT. Exemple : DNS.RES.TRANSPORT.EQ (TCP)

Les fonctions suivantes renvoient le nom de l'emplacement correspondant lorsque la requête contient ou ne contient pas l'option DNS ECS.

Fonction	Description
DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION	Renvoie le nom de l'emplacement correspondant qui a été utilisé dans la requête avec l'option DNS ECS. Exemple :(DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION(".CH…..")
client.IP.SRC.MATCHES_LOCATION	Renvoie le nom de l'emplacement correspondant qui a été utilisé dans la requête sans l'option DNS ECS. Exemple : (client.IP.SRC.MATCHES_LOCATION(".CH…..")
DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION OR client.IP.SRC.MATCHES_LOCATION	Expression commune à utiliser dans la stratégie lorsque le trafic DNS peut avoir ou non l'option ECS dans la requête. Exemple : "(((DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION(".CH…..").typec ALT (client.IP.SRC.MATCHES_LOCATION(".CH…..").typecast_text_t

Expressions XPath et HTML, XML ou JSON

August 20, 2021

L'infrastructure de stratégie avancée prend en charge les expressions permettant d'évaluer et de récupérer des données à partir de fichiers JSON (HTML, XML et JavaScript Object Notation). Cela vous permet de rechercher des nœuds spécifiques dans un document HTML, XML ou JSON, de déterminer si un nœud existe dans le fichier, de localiser des nœuds dans des contextes XML (par exemple,

des nœuds qui ont des parents spécifiques ou un attribut spécifique avec une valeur donnée) et de renvoyer le contenu de ces nœuds. En outre, vous pouvez utiliser les expressions XPath dans les expressions de réécriture.

L'implémentation de l'expression de stratégie avancée pour XPath comprend un préfixe d'expression de stratégie avancée (tel que « HTTP.REQ.BODY ») qui désigne du texte HTML ou XML, et l'opérateur XPATH qui prend l'expression XPath comme argument.

Les fichiers HTML sont une collection largement libre de balises et d'éléments de texte. Vous pouvez utiliser l'opérateur XPATH_HTML, qui prend une expression XPath comme argument, pour traiter les fichiers HTML. Les fichiers JSON sont soit une collection de paires nom/valeur, soit une liste ordonnée de valeurs. Vous pouvez utiliser l'opérateur XPATH_JSON, qui prend une expression XPath comme argument, pour traiter les fichiers JSON.

- **<text>.XPATH(xpathex):**

  Opérer sur un fichier XML et renvoyer une valeur booléenne.

  Par exemple, l'expression suivante renvoie une valeur booléenne TRUE si un nœud appelé « creator » existe sous le nœud « Book » dans les 1000 premiers octets du fichier XML.

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%boolean(//Book/creator)%)
  ```

  Paramètres :

  xpathex - Expression booléenne XPath

- **<text>.XPATH(xpathex):**

  Opérer sur un fichier XML et renvoyer une valeur de type de données “double.”

  Par exemple, l'expression suivante convertit la chaîne « 36” (une valeur de prix) en une valeur de type de données « double » si la chaîne se trouve dans les 1000 premiers octets du fichier XML :

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%number(/Book/price)%)
  ```

  Paramètres :

  xpathex - Expression numérique XPath

Exemple :

```
    <Book>
    <creator>
        <Person>
            <name>Milton</name>
        </Person>
    </creator>
    <title>Paradise Lost</title>
    </Book>
<!--NeedCopy-->
```


- **<text>.XPATH(xpathex):**

  Opérer sur un fichier XML et renvoyer un jeu de nœuds ou une chaîne. Les ensembles de nœuds sont convertis en chaînes correspondantes à l'aide de la routine de conversion de chaînes XPath standard.

  Par exemple, l'expression suivante sélectionne tous les nœuds qui sont entourés par « /book/creator » (un ensemble de nœuds) dans les 1000 premiers octets du corps :

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%/Book/creator%)
  ```

  Paramètres :

  xpathex - Expression XPath

- **<text>.XPATH_HTML(xpathex)**

  Fonctionnez sur un fichier HTML et renvoyez une valeur de texte.

  Par exemple, l'expression suivante fonctionne sur un fichier HTML et renvoie le texte enfermé dans les balises <title\></title\> si l'élément HTML titre se trouve dans les 1000 premiers octets :

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML(xp%/html/head/title%)
  ```

  Paramètres :

  xpathex - Expression de texte XPath

- **<text>.XPATH_HTML_WITH_MARKUP(xpathex)**

  Fonctionnez sur un fichier HTML et renvoyez une chaîne contenant la totalité de la partie sélectionnée du document, y compris le balisage, par exemple l'inclusion des balises d'élément englobant.

  L'expression suivante fonctionne sur le fichier HTML et sélectionne tout le contenu de la balise <\title> balise, y compris le balisage.

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML_WITH_MARKUP( xp%/html/head/title%)
  ```

  La partie du corps HTML sélectionnée par l'expression est marquée pour un traitement ultérieur.

  Paramètres :

  xpathex - Expression XPath

- **<text>.XPATH_JSON(xpathex)**

  Opérer sur un fichier JSON et renvoyer une valeur booléenne.

  Par exemple, considérez le fichier JSON suivant :

  { "Book":{ "creator":{ "person":{ "name":'<name>' } }, "title":'<title>' } }

L'expression suivante fonctionne sur le fichier JSON et renvoie une valeur booléenne TRUE si le fichier JSON contient un nœud nommé « creator », dont le nœud parent est « Book », dans les 1000 premiers octets :

```
HTTP.REQ.BODY(1000).XPATH_JSON(xp%boolean(/Book/creator)%)
```

Paramètres :

xpathex - Expression booléenne XPath

- **<text>.XPATH_JSON(xpathex)**

  Opérer sur un fichier JSON et renvoyer une valeur de type de données "double."

  Par exemple, considérez le fichier JSON suivant :

  { "Book":{ "creator":{ "person":{ "name":'<name>' } }, "title":'<title>', "price":"36" } }

  L'expression suivante fonctionne sur le fichier JSON et convertit la chaîne "36" en une valeur de type de données « double » si la chaîne est présente dans les 1000 premiers octets du fichier JSON.

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%number(/Book/price)%)
  ```

  Paramètres :

  xpathex - Expression numérique XPath

- **<text>.XPATH_JSON(xpathex)**

  Opérer sur un fichier JSON et renvoyer un jeu de nœuds ou une chaîne. Les ensembles de nœuds sont convertis en chaînes correspondantes à l'aide de la routine de conversion de chaînes XPath standard.

  Par exemple, considérez le fichier JSON suivant :

  { "Book":{ "creator":{ "person":{ "name":'<name>' } }, "title":'<title>' } }

  L'expression suivante sélectionne tous les nœuds qui sont entourés par « /Book » (un jeu de nœuds) dans les 1000 premiers octets du corps du fichier JSON et renvoie la valeur de chaîne correspondante, qui est »<name><title>":

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%/Book%)
  ```

  Paramètres :

  xpathex - Expression XPath

- **<text>.XPATH_JSON_WITH_MARKUP (xpathex)**

  Fonctionnez sur un fichier XML et renvoyez une chaîne contenant toute la partie du document pour le nœud de résultat, y compris le balisage comme l'inclusion des balises d'élément englobant.

Par exemple, considérez le fichier JSON suivant :

{”Book”:{ ”creator”:{ ”person”:{ ”name”:’<name>’ } }, ”title”:’<title>’ } }

L’expression suivante fonctionne sur le fichier JSON et sélectionne tous les nœuds qui sont entourés par « /book/creator » dans les 1000 premiers octets du corps, qui est “creator:{ person:{ name:’<name>’ } }.”

```
HTTP.REQ.BODY(1000).XPATH_JSON_WITH_MARKUP(xp%/Book/creator%)
```

La partie du corps JSON sélectionnée par l’expression est marquée pour un traitement ultérieur.

Paramètres :

xpathex - Expression XPath

- **<text>.XPATH_WITH_MARKUP (xpathex) :**

  Fonctionnez sur un fichier XML et renvoyez une chaîne contenant toute la partie du document pour le nœud de résultat, y compris le balisage comme l’inclusion des balises d’élément englobant.

  Par exemple, l’expression suivante fonctionne sur un fichier XML et sélectionne tous les nœuds entourés par « /book/creator » dans les 1000 premiers octets du corps.

  ```
  HTTP.REQ.BODY(1000).XPATH_WITH_MARKUP(xp%/Book/creator%)
  ```

  La partie du corps JSON sélectionnée par l’expression est marquée pour un traitement ultérieur.

  Paramètres :

  xpathex - Expression XPath

Crypter et décrypter les charges utiles XML

May 5, 2023

Vous pouvez utiliser les fonctions XML_ENCRYPT () et XML_DECRYPT () dans les expressions de stratégie avancées pour chiffrer et déchiffrer, respectivement, les données XML. Ces fonctions sont conformes à la norme W3C XML Encryption définie à l’adresse “http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/. « XML_ENCRYPT () et XML_DECRYPT () prennent en charge un sous-ensemble de la spécification XML Encryption. Dans le sous-ensemble, le chiffrement des données utilise une méthode de chiffrement en bloc (RC4, DES3, AES128, AES192 ou AES256), et une clé publique RSA est utilisée pour chiffrer la clé de chiffrement en bloc.

Remarque : Si vous souhaitez chiffrer et déchiffrer du texte dans une charge utile, vous devez utiliser les fonctions ENCRYPT et DECRYPT. Pour plus d’informations sur ces fonctions, voir Chiffrer et déchiffrer du texte.

Les fonctions XML_ENCRYPT () et XML_DECRYPT () ne dépendent pas du service de chiffrement et de déchiffrement utilisé par les commandes ENCRYPT et DECRYPT pour le texte. La méthode de chiffrement est spécifiée explicitement en tant qu'argument de la fonction XML_ENCRYPT (). La `XML_DECRYPT()` fonction obtient les informations relatives à la méthode de chiffrement spécifiée à partir de l' `<xenc:EncryptedData>` élément. Voici des synopsis des fonctions de chiffrement et de déchiffrement XML :

- `XML_ENCRYPT(<certKeyName>, <method> [, <flags>])**. Returns an <xenc:EncryptedData>` qui contient le texte d'entrée chiffré et la clé de chiffrement, qui est elle-même chiffrée à l'aide de RSA.
- `XML_DECRYPT(<certKeyName>)`. Renvoie le texte déchiffré de l' `<xenc:EncryptedData>` élément d'entrée, qui inclut la méthode de chiffrement et la clé chiffrée RSA.

Remarque : L' `<xenc:EncryptedData>` élément est défini dans la spécification W3C XML Encryption.

Voici une description des arguments :

- **CertKeyName :** sélectionne un certificat X.509 avec une clé publique RSA pour XML_ENCRYPT () ou une clé privée RSA pour XML_DECRYPT (). La clé de certificat doit avoir été créée au préalable par une `add ssl certKey` commande.
- **method :** spécifie la méthode de chiffrement à utiliser pour chiffrer les données XML. Valeurs possibles : RC4, DES3, AES128, AES192, AES256.
- **flags :** masque de bits spécifiant les informations clés facultatives suivantes (`<ds:KeyInfo>`) à inclure dans l' `<xenc:EncryptedData>` élément généré par `XML_ENCRYPT()` :
  - **1** - Incluez un élément KeyName avec le CertKeyName. L'élément est `<ds:KeyName>`.
  - **2** - Incluez un élément KeyValue avec la clé publique RSA du certificat. L'élément est `<ds:KeyValue>`.
  - **4** - Incluez un élément X509IssuerSerial avec le numéro de série du certificat et le nom unique de l'émetteur. L'élément est `<ds:X509IssuserSerial>`.
  - **8** - Inclut un élément X509SubjectName avec le nom unique de l'objet du certificat. L'élément est `<ds:X509SubjectName>`.
  - **16** - Incluez un élément X509Certificate avec l'intégralité du certificat. L'élément est `<ds:X509Certificate>`.

Utiliser les fonctions XML_ENCRYPT () et XML_DECRYPT () dans les expressions

La fonctionnalité de cryptage XML utilise des paires de clés de certificat SSL pour fournir des certificats X.509 (avec des clés publiques RSA) pour le chiffrement des clés et des clés privées RSA pour le déchiffrement des clés. Par conséquent, avant d'utiliser la fonction XML_ENCRYPT () dans une expression, vous devez créer une paire de clés de certificat SSL. La commande suivante crée une paire

de clés de certificat SSL, my-certkey, avec le certificat X.509, my-cert.pem et le fichier de clé privée, my-key.pem.

```
add ssl certKey my-certkey -cert my-cert.pem -key my-key.pem -passcrypt
kxPeMRYnitY=
```

Les commandes CLI suivantes créent des actions de réécriture et des stratégies de chiffrement et de déchiffrement du contenu XML.

```
1  add rewrite action my-xml-encrypt-action replace "HTTP.RES.BODY(10000).
       XPATH_WITH_MARKUP(xp%/%)" "HTTP.RES.BODY(10000).XPATH_WITH_MARKUP(xp
       %/%).XML_ENCRYPT("my-certkey", AES256, 31)"
2
3  add rewrite action my-xml-decrypt-action replace "HTTP.REQ.BODY(10000).
       XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%)" "HTTP.REQ.BODY(10000).
       XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%).XML_DECRYPT("my-certkey"
       )"
4
5  add rewrite policy my-xml-encrypt-policy "HTTP.REQ.URL.CONTAINS("xml-
       encrypt")" my-xml-encrypt-action
6
7  add rewrite policy my-xml-decrypt-policy "HTTP.REQ.BODY(10000).XPATH(xp
       %boolean(//xenc:EncryptedData)%)" my-xml-decrypt-action
8
9  bind rewrite global my-xml-encrypt-policy 30
10
11 bind rewrite global my-xml-decrypt-policy 30
12 <!--NeedCopy-->
```

Dans l'exemple ci-dessus, l'action de réécriture my-xml-encrypt-action chiffre l'intégralité du document XML (XPATH_WITH_MARKUP (xp%/%)) dans la demande à l'aide de la méthode de chiffrement en bloc AES-256 et de la clé publique RSA de my-certkey pour chiffrer la clé de chiffrement en bloc. L'action remplace le document par un <xenc:EncryptedData> élément contenant les données chiffrées et une clé chiffrée. Les drapeaux représentés par 31 incluent tous les <ds:KeyInfo> éléments facultatifs.

L'action my-xml-decrypt-action déchiffre le premier <xenc:EncryptedData> élément de la réponse (XPATH_WITH_MARKUP (XP%//XENC:EncryptedData%)). Cela nécessite l'ajout préalable de l'espace de noms XML xenc à l'aide de la commande CLI suivante :

```
add ns xmlnamespace xenc http://www.w3.org/2001/04/xmlenc##
```

L'action my-xml-decrypt-action utilise la clé privée RSA dans my-certkey pour déchiffrer la clé chiffrée, puis utilise la méthode de chiffrement en bloc spécifiée dans l'élément pour déchiffrer le contenu chiffré. Enfin, l'action remplace l'élément de données chiffré par le contenu déchiffré.

La stratégie de réécriture my-xml-encrypt-policy applique my-xml-encrypt-action aux demandes d'URL contenant xml-encrypt. L'action chiffre l'intégralité de la réponse à partir d'un service configuré sur l'appliance NetScaler.

La stratégie de réécriture my-xml-decrypt-policy applique my-xml-decrypt-action aux requêtes qui contiennent un <xenc:EncryptedData> élément (XPATH (XP%//XENC:EncryptedData%) renvoie une chaîne non vide). L'action déchiffre les données cryptées dans les demandes liées à un service configuré sur l'appliance NetScaler.

Expressions de stratégie avancées : analyse SSL

November 2, 2022

Il existe des expressions de stratégie avancées pour analyser les certificats SSL et les messages Hello du client SSL.

Analyse des certificats SSL

Vous pouvez utiliser des expressions de stratégie avancées pour évaluer les certificats clients SSL (Secure Sockets Layer) X.509. Un certificat client est un document électronique qui peut être utilisé pour authentifier l'identité d'un utilisateur. Un certificat client contient (au minimum) des informations de version, un numéro de série, un identifiant d'algorithme de signature, un nom d'émetteur, une période de validité, un nom de sujet (utilisateur), une clé publique et des signatures.

Vous pouvez examiner à la fois les connexions SSL et les données des certificats clients. Par exemple, vous pouvez envoyer des demandes SSL qui utilisent des chiffrements de faible puissance à une batterie de serveurs virtuels d'équilibrage de charge particulière. La commande suivante est un exemple de stratégie de commutation de contenu qui analyse la force de chiffrement dans une demande et fait correspondre des forces de chiffrement inférieures ou égales à 40 :

```
add cs policy p1 -rule "client.ssl.cipher_bits.le(40)"
```

Dans un autre exemple, vous pouvez configurer une stratégie qui détermine si une demande contient un certificat client :

```
add cs policy p2 -rule "client.ssl.client_cert exists"
```

Vous pouvez également configurer une stratégie qui examine des informations spécifiques d'un certificat client. Par exemple, la stratégie suivante vérifie que le certificat a un ou plusieurs jours avant son expiration :

```
add cs policy p2 -rule "client.ssl.client_cert exists && client.ssl.client_cert
.days_to_expire.ge(1)"
```


Exemple d'utilisation des empreintes digitales JA3 :

```
add ssl policy ja3_pol -rule "CLIENT.SSL.JA3_FINGERPRINT.EQ(bb4c15a90e93a25ddc1627439
)"-action reset
```

Ou, un exemple d'utilisation des empreintes digitales JA3 avec patset :

```
1 add policy patset pat1
2 bind policy patset pat1 bb4c15a90e93a25ddc16274395bce4c6 -index 1
3 bind policy patset pat1 cd3c15a90e93a25ddc16274395bce6b4 -index 2
4 add ssl policy ssl_ja3_pol -rule CLIENT.SSL.JA3_FINGERPRINT.
     contains_any("pat1") -action reset
5 <!--NeedCopy-->
```

> **Remarque**
>
> Pour plus d'informations sur l'analyse des dates et des heures dans un certificat, voir Format des dates et heures dans une expression et des expressions pour les dates de certificat SSL.

Préfixes pour les données SSL et de certificat basées sur le texte

Le tableau suivant décrit les préfixes d'expression qui identifient les éléments textuels dans les transactions SSL et les certificats clients.

Tableau 1. Préfixes qui renvoient du texte ou des valeurs booléennes pour les données de certificat SSL et client

Préfixe	Description
CLIENT.SSL.CLIENT_CERT	Renvoie le certificat client SSL dans la transaction SSL en cours.
CLIENT.SSL.CLIENT_CERT.TO_PEM	Renvoie le certificat client SSL au format binaire.
CLIENT.SSL.CIPHER_EXPORTABLE	Renvoie une valeur booléenne TRUE si le chiffrement cryptographique SSL est exportable.
CLIENT.SSL.CIPHER_NAME	Renvoie le nom du chiffrement SSL s'il est invoqué à partir d'une connexion SSL, et une chaîne NULL s'il est invoqué à partir d'une connexion non SSL.
CLIENT.SSL.IS_SSL	Renvoie une valeur booléenne TRUE si la connexion en cours est basée sur SSL.

Préfixe	Description
CLIENT.SSL.JA3_FINGERPRINT	Renvoie une valeur booléenne TRUE si l'empreinte digitale JA3 configurée correspond à l'empreinte digitale JA3 dans le message Hello du client. **Remarque :** Cette expression est disponible dans les versions 13.1 build 12.x et ultérieures.

Préfixes pour les données numériques dans les certificats SSL

Le tableau suivant décrit les préfixes qui évaluent des données numériques autres que les dates dans les certificats SSL. Ces préfixes peuvent être utilisés avec les opérations décrites dans Opérations de base sur les préfixes d'expression et Opérations composées pour les nombres.

Tableau 2. Préfixes qui évaluent les données numériques autres que les dates dans les certificats SSL

Préfixe	Description
CLIENT.SSL.CLIENT_CERT.DAYS_TO_EXPIRE	Renvoie le nombre de jours pendant lesquels le certificat est valide ou renvoie -1 pour les certificats expirés.
CLIENT.SSL.CLIENT_CERT.PK_SIZE	Renvoie la taille de la clé publique utilisée dans le certificat.
CLIENT.SSL.CLIENT_CERT.VERSION	Renvoie le numéro de version du certificat. Si la connexion n'est pas basée sur SSL, renvoie zéro (0).
CLIENT.SSL.CIPHER_BITS	Renvoie le nombre de bits de la clé cryptographique. Renvoie 0 si la connexion n'est pas basée sur SSL.
CLIENT.SSL.VERSION	Renvoie un nombre qui représente la version du protocole SSL, comme suit : 0. La transaction n'est pas basée sur SSL : 0x002. La transaction est SSLv2 : 0x300. La transaction est SSLv3 : 0x301. La transaction est TLSv1 : 0x302. La transaction est TLS 1.1 : 0x303. La transaction est TLS 1.2 : 0x304. La transaction est TLS 1.3.

> **Remarque**
>
> Pour les expressions liées aux dates d'expiration d'un certificat, voir Expressions pour les dates de certificat SSL.

Expressions pour les certificats SSL

Vous pouvez analyser les certificats SSL en configurant des expressions qui utilisent le préfixe suivant :

CLIENT.SSL.CLIENT_CERT

Cette section décrit les expressions que vous pouvez configurer pour les certificats, à l'exception des expressions qui examinent l'expiration du certificat. Les opérations temporelles sont décrites dans Expressions de stratégie avancées : utilisation des dates, des heures et des nombres.

Le tableau suivant décrit les opérations que vous pouvez spécifier pour le préfixe CLIENT.SSL.CLIENT_CERT.

Tableau 3. Opérations pouvant être spécifiées avec le préfixe CLIENT.SSL.CLIENT_CERT

Opération du certificat SSL	Description
`<certificate>.EXISTS`	Renvoie une valeur booléenne TRUE si le client possède un certificat SSL.
`<certificate>.ISSUER`	Renvoie le nom distinctif (DN) de l'émetteur dans le certificat sous forme de liste nom-valeur. Un signe égal (« = ») est le délimiteur du nom et de la valeur, et la barre oblique («/») est le délimiteur qui sépare les paires nom-valeur. Voici un exemple de DN renvoyé : `/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycompany.com`

Opération du certificat SSL	Description
<certificate>.ISSUER.IGNORE_EMPTY_ELEMENTS	Renvoie l'émetteur et ignore les éléments vides d'une liste nom-valeur. Par exemple, considérez ce qui suit : `Cert-Issuer: /c=in/st=kar//l=bangelore //o=mycompany/ou=sales/ /emailAddress=myuserid@mycompany.com`. L'action Réécriture suivante renvoie un nombre de 6 en fonction de la définition précédente de l'émetteur : `sh rewrite action insert_ssl_header Name: insert_ssl Operation: insert_http_header Target:Cert-Issuer Value:CLIENT.SSL.CLIENT_CERT.ISSUER.COUNT`. Toutefois, si vous modifiez la valeur suivante, le nombre retourné est 9 :`CLIENT.SSL.CLIENT_CERT.ISSUER.IGNORE_EMPTY_ELEMENTS.COUNT`
<certificate>. SERIALNUMBER	Renvoie le numéro de série du certificat sous la forme d'une chaîne hexadécimale en majuscule, sans zéro en début de chaîne. Par exemple, si le numéro de série du certificat est 04daa1e44bd2e7769638a0058b4964bd, l'expression suivante permet de faire correspondre le numéro de série `CLIENT.SSL.CLIENT_CERT.SERIALNUMBER.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"4daa1e44bd2e7769638a0058b4964bd\")`

Bonjour du client Parse SSL

Vous pouvez analyser le message Hello du client SSL en configurant des expressions qui utilisent le préfixe suivant :

Préfixe	Description
CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXC(	Correspond au code hexadécimal fourni dans l'expression avec les codes hexadécimaux des suites de chiffrement reçues dans le message Hello du client.
CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION	Version reçue dans l'en-tête du message Hello du client.
CLIENT.SSL.CLIENT_HELLO.IS_RENEGOTIATE	Renvoie la valeur true si un client ou un serveur lance une renégociation de session.
CLIENT.SSL.CLIENT_HELLO.IS_REUSE	Renvoie true si l'appliance réutilise la session SSL en fonction de l'ID de session différent de zéro reçu dans le message client-Hello.
CLIENT.SSL.CLIENT_HELLO.IS_SCSV	Renvoie true si la capacité SCSV (Signaling Cipher Suite Value) est annoncée dans le message Hello du client. Le code hexadécimal pour SCSV de secours est 0x5600.
CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET	Renvoie la valeur true si une extension de ticket de session dont la longueur est différente de zéro est annoncée dans le message client-hello.
CLIENT.SSL.CLIENT_HELLO.LENGTH	Longueur reçue dans l'en-tête du message Hello du client.
CLIENT.SSL.CLIENT_HELLO.SNI	Renvoie le nom du serveur reçu dans l'extension Nom du serveur du message Hello du client.
CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPRC	Renvoie true si le protocole d'application de l'extension ALPN reçu dans le message Hello du client correspond au protocole fourni dans l'expression.

Ces expressions peuvent être utilisées au niveau du point de liaison CLIENTHELLO_REQ. Pour plus d'informations, voir Liaison de stratégie SSL.

Expressions de stratégie avancées : adresses IP et MAC, débit, ID VLAN

May 5, 2023

Vous pouvez utiliser des préfixes d'expression de stratégie avancée qui renvoient des adresses IPv4 et IPv6, des adresses MAC, des sous-réseaux IP, des données client et serveur utiles telles que les débits aux ports d'interface (Rx, Tx et RxTx) et les ID des VLAN via lesquels les paquets sont reçus. Vous pouvez ensuite utiliser différents opérateurs pour évaluer les données renvoyées par ces préfixes d'expression.

Expressions pour adresses IP et sous-réseaux IP

Vous pouvez utiliser des expressions de stratégie avancées pour évaluer les adresses et les sous-réseaux qui sont au format IPv4 (Internet Protocol version 4) ou IPv6 (Internet Protocol version 6). Les préfixes d'expression des adresses et sous-réseaux IPv6 incluent IPv6 dans le préfixe. Les préfixes d'expression des adresses et sous-réseaux IPv4 incluent l'adresse IP dans le préfixe. Voici un exemple d'expression qui identifie si une demande provient d'un sous-réseau IPv4 particulier.

```
client.ip.src.in_subnet(147.1.0.0/16)
<!--NeedCopy-->
```

Voici deux exemples de stratégies de réécriture qui examinent le sous-réseau à partir duquel le paquet est reçu et effectuent une action de réécriture sur l'en-tête Host. Une fois ces deux stratégies configurées, l'action de réécriture effectuée dépend du sous-réseau de la demande. Ces deux stratégies évaluent les adresses IP au format d'adresse IPv4.

```
- add rewrite action URL1-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany1.com""
- add rewrite policy URL1-rewrite-policy "http.req.header("Host").
   contains("www.test1.com") && client.ip.src.in_subnet(147.1.0.0/16)"
   URL1-rewrite-action
- add rewrite action URL2-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany2.com""
- add rewrite policy URL2-rewrite-policy "http.req.header("Host").
   contains("www.test2.com") && client.ip.src.in_subnet(10.202.0.0/16)"
    URL2-rewrite-action
<!--NeedCopy-->
```

> **Remarque**
>
> Les exemples précédents sont des commandes que vous saisissez sur l'interface de ligne de commande (CLI) NetScaler. Par conséquent, chaque guillemet doit être précédé d'une barre oblique

> inverse (\). Pour plus d'informations, voir Configuration d'expressions de stratégie avancées dans une stratégie."

Préfixes pour les adresses IPV4 et les sous-réseaux IP

Le tableau suivant décrit les préfixes qui renvoient des adresses et des sous-réseaux IPv4, ainsi que des segments d'adresses IPv4. Vous pouvez utiliser des opérateurs numériques et des opérateurs spécifiques aux adresses IPv4 avec ces préfixes. Pour plus d'informations sur les opérations numériques, voir « Opérations debase sur les préfixes d'expression » et « Opérations composées pour les nombres ».

Tableau 1. Préfixes qui évaluent les adresses IP et MAC

Prefix	Description
CLIENT.IP.SRC	Renvoie l'adresse IP source du paquet actuel sous forme d'adresse IP ou de numéro.
CLIENT.IP.DST	Renvoie l'adresse IP de destination du paquet actuel sous forme d'adresse IP ou de numéro.
SERVEUR.IP.SRC	Renvoie l'adresse IP source du paquet actuel sous forme d'adresse IP ou de numéro.
SERVEUR.IP.DST	Renvoie l'adresse IP de destination du paquet actuel sous forme d'adresse IP ou de numéro.

Opérations pour les adresses IPV4

Le tableau Prefix for IPV4 Operations décrit les opérateurs pouvant être utilisés avec des préfixes renvoyant une adresse IPv4.

A propos des expressions IPv6

Le format d'adresse IPv6 offre plus de flexibilité que l'ancien format IPv4. Les adresses IPv6 sont au format hexadécimal (RFC 2373). Dans les exemples suivants, l'exemple 1 est une adresse IPv6, l'exemple 2 est une URL qui inclut l'adresse IPv6 et l'exemple 3 inclut l'adresse IPv6 et un numéro de port.

Exemple 1 :

```
9901:0ab1:22a2:88a3:3333:4a4b:5555:6666
<!--NeedCopy-->
```

Exemple 2 :


```
http://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]/
<!--NeedCopy-->
```

Exemple 3 :

```
https://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]:8080/
<!--NeedCopy-->
```

Dans l'exemple 3, les crochets séparent l'adresse IP du numéro de port (8080).

Notez que vous ne pouvez utiliser l'opérateur « + » que pour combiner des expressions IPv6 avec d'autres expressions. La sortie est une concaténation des valeurs de chaîne renvoyées par les expressions individuelles. Vous ne pouvez pas utiliser d'autres opérateurs arithmétiques avec une expression IPv6. La syntaxe suivante est un exemple :

```
client.ipv6.src + server.ip.dst
<!--NeedCopy-->
```

Par exemple, si l'adresse IPv6 source du client est `ABCD:1234::ABCD`, et que l'adresse IPv4 de destination du serveur est `10.100.10.100`, l'expression précédente renvoie `"ABCD:1234::ABCD10.100.10.100"`.

Notez que lorsque l'appliance NetScaler reçoit un paquet IPv6, elle attribue une adresse IPv4 temporaire à partir d'une plage d'adresses IPv4 non utilisée et remplace l'adresse source du paquet par cette adresse temporaire. Au moment de la réponse, l'adresse source du paquet sortant est remplacée par l'adresse IPv6 d'origine.

> **Remarque**
>
> Vous pouvez combiner une expression IPv6 avec n'importe quelle autre expression, à l'exception d'une expression qui produit un résultat booléen.

Préfixes d'expression pour les adresses IPv6

Les adresses IPv6 renvoyées par les préfixes d'expression du tableau suivant peuvent être traitées comme des données textuelles. Par exemple, le préfixe client.ipv6.dst renvoie l'adresse IPv6 de destination sous la forme d'une chaîne pouvant être évaluée en tant que texte.

Le tableau suivant décrit les préfixes d'expression qui renvoient une adresse IPv6.

Tableau 3. Préfixes d'expression IPv6 qui renvoient du texte

Prefix	Description
CLIENT.IPV6	Fonctionne sur l'adresse IPv6 avec le paquet actuel.
CLIENT.IPV6.DST	Renvoie l'adresse IPv6 dans le champ de destination de l'en-tête IP.
CLIENT.IPV6.SRC	Renvoie l'adresse IPv6 dans le champ source de l'en-tête IP. Voici des exemples : `client.ipv6.src.in_subnet(2007::2008/64)` `client.ipv6.src.get1.le(2008)`
SERVEUR.IPV6	Fonctionne sur l'adresse IPv6 avec le paquet actuel.
SERVER.IPV6.DST	Renvoie l'adresse IPv6 dans le champ de destination de l'en-tête IP.
SERVER.IPV6.SRC	Renvoie l'adresse IPv6 dans le champ source de l'en-tête IP. Voici des exemples : `server.ipv6.src.in_subnet(2007::2008/64)` `server.ipv6.src.get1.le(2008)`

Opérations pour les préfixes IPv6

Le tableau suivant décrit les opérateurs qui peuvent être utilisés avec des préfixes qui renvoient une adresse IPv6 :

Tableau 4. Opérations qui évaluent les adresses IPv6

Fonctionnement IPv6	Description
`<ipv6>.EQ(<IPv6_address>`	Renvoie une valeur booléenne TRUE si la valeur de l'adresse IP est identique à celle de l' `<IPv6_address>` argument. Voici un exemple : `client.ipv6.dst.eq(ABCD:1234::ABCD)`

Fonctionnement IPv6	Description
<ipv6>.GET1. . .GET8	Renvoie un segment d'une adresse IPv6 sous la forme d'un nombre. Les exemples d'expressions suivants récupèrent des segments à partir de l'adresse ipv6 1000:1001:CD 10:0000:0000:89 AB:4567:CDEF : `client.ipv6.dst.get5 extracts 0000`, qui est le cinquième ensemble de bits de l'adresse. `client.ipv6.dst.get6 extracts 89AB`. `client.ipv6.dst.get7 extracts 4567`. Vous pouvez effectuer des opérations numériques sur ces segments. Notez que vous ne pouvez pas effectuer d'opérations numériques lorsque vous récupérez une adresse IPv6 complète. En effet, les expressions qui renvoient une adresse IPv6 complète, comme CLIENT.IPV6.SRC, renvoient l'adresse au format texte.
<ipv6>.IN_SUBNET(<subnet>)	Renvoie une valeur booléenne TRUE si la valeur de l'adresse IPv6 se trouve dans le sous-réseau spécifié par l' <subnet> argument. Voici un exemple : `client.ipv6.dst.eq(1000:1001:CD10 :0000:0000:89AB:4567:CDEF/60)`
<ipv6>.IS_IPV4	Retourne une valeur booléenne TRUE s'il s'agit d'un client IPv4, et renvoie une valeur booléenne FALSE si ce n'est pas le cas.
<ipv6>.SUBNET(<n>)	Renvoie l'adresse IPv6 après avoir appliqué le masque de sous-réseau spécifié comme argument. Le masque de sous-réseau peut prendre des valeurs comprises entre 0 et 128. Pa exemple : `CLIENT.IPV6.SRC.SUBNET(24)`

Expressions pour adresses MAC

Une adresse MAC est constituée de valeurs hexadécimales délimitées par deux points au format ## : ## : ## : ## : ## : ##, où chaque « # » représente soit un nombre compris entre 0 et 9, soit une lettre de A à F. Des préfixes et opérateurs d'expression de stratégie avancés sont disponibles pour évaluer les adresses MAC source et cible.

Préfixes des adresses MAC

Le tableau suivant décrit les préfixes qui renvoient des adresses MAC.

Tableau 5. Préfixes qui évaluent les adresses MAC

Prefix	Description
`client.ether.dstmac`	Renvoie l'adresse MAC dans le champ de destination de l'en-tête Ethernet.
`client.ether.srcmac`	Renvoie l'adresse MAC dans le champ source de l'en-tête Ethernet.

Opérations pour les adresses MAC

Le tableau suivant décrit les opérateurs qui peuvent être utilisés avec des préfixes qui renvoient une adresse MAC.

Tableau 6. Opérations sur les adresses MAC

Prefix	Description
`<mac address>.EQ(<address>)`	Renvoie une valeur booléenne TRUE si la valeur de l'adresse MAC est identique à celle de l' `<address>` argument.
`<mac address>.GET1. . .GET4`	Renvoie une valeur numérique extraite du segment de l'adresse MAC spécifié dans l'opération GET. Par exemple, si l'adresse MAC est 12:34:56:78:9 a:bc, la valeur suivante renvoie 34 : `client.ether.dstmac.get2`

Expressions pour les données numériques du client et du serveur

Le tableau suivant décrit les préfixes pour l'utilisation des données numériques du client et du serveur, notamment le débit, les numéros de port et les ID de VLAN.

Tableau 7. Préfixes qui évaluent les données numériques du client et du serveur

Prefix	Description
Débit client.interface.rx	Renvoie un entier représentant le débit brut du trafic reçu en kilo-octets par seconde (Kbps) pendant les sept secondes précédentes.
débit client.interface.tx	Renvoie un entier représentant le débit brut du trafic transmis en Kbps pendant les sept secondes précédentes.
Débit client.interface.rxtx	Renvoie un entier représentant le débit brut du trafic reçu et transmis en Kbps pendant les sept secondes précédentes.
débit server.interface.rx	Renvoie un entier représentant le débit brut du trafic reçu en Kbps pendant les sept secondes précédentes.
débit server.interface.tx	Renvoie un entier représentant le débit brut du trafic transmis en Kbps pendant les sept secondes précédentes.
débit server.interface.rxtx	Renvoie un entier représentant le débit brut du trafic reçu et transmis en Kbps pendant les sept secondes précédentes.
server.vlan.id	Renvoie un ID numérique du VLAN par lequel le paquet actuel est entré dans NetScaler.
client.vlan.id	Renvoie un ID numérique pour le VLAN par lequel le paquet actuel est entré dans NetScaler.

Expressions de stratégie avancées : fonctions d'analyse de flux

January 21, 2021

Les expressions Stream Analytics commencent par le préfixe ANALYTICS.STREAM(<identifier_name>)

. La liste suivante décrit les fonctions qui peuvent être utilisées avec ce préfixe.

- **COLLECT_STATS**

  Recueillir des données statistiques à partir des demandes évaluées par rapport à la stratégie et créer un enregistrement pour chaque demande.

- **REQUESTS**

  Retourne le nombre de requêtes existant pour le regroupement d'enregistrements spécifié. La valeur renvoyée est de type unsigned long.

- **BANDWIDTH**

  Retourne la statistique de bande passante pour le regroupement d'enregistrements spécifié. La valeur renvoyée est de type unsigned long.

- **RESPTIME**

  Renvoie la statistique de temps de réponse pour le regroupement d'enregistrements spécifié. La valeur renvoyée est de type unsigned long.

- **CONNECTIONS**

  Renvoie le nombre de connexions simultanées existant pour le regroupement d'enregistrements spécifié. La valeur renvoyée est de type unsigned long.

- **IS_TOP (n)**

  Renvoie une valeur booléenne TRUE si la valeur statistique du regroupement d'enregistrements spécifié est l'un des n groupes les plus importants. Sinon, renvoyez une valeur booléenne FALSE.

- **CHECK_LIMIT**

  Renvoie une valeur booléenne TRUE si la statistique du regroupement d'enregistrements spécifié a atteint la limite préconfigurée. Sinon, renvoyez une valeur booléenne FALSE.

Expressions de politique avancées : DataStream

May 8, 2023

L'infrastructure de politiques de l'appliance NetScaler inclut des expressions que vous pouvez utiliser pour évaluer et traiter le trafic des serveurs de base de données lorsque l'appliance est déployée entre une batterie de serveurs d'applications et leurs serveurs de base de données associés.

Cette rubrique comprend les sections suivantes :

- Expressions pour le protocole MySQL
- Expressions pour évaluer les connexions Microsoft SQL Server

Expressions pour le protocole MySQL

Les expressions suivantes évaluent le trafic associé aux serveurs de base de données MySQL. Vous pouvez utiliser les expressions basées sur les demandes (expressions commençant par MYSQL.CLIENT et MYSQL.REQ) dans les politiques pour prendre des décisions de commutation de demandes au point de liaison du serveur virtuel de commutation de contenu et les expressions basées sur les réponses (expressions commençant par MYSQL.RES) pour évaluer les réponses du serveur aux moniteurs de santé configurés par l'utilisateur.

- **MYSQL.CLIENT.** Fonctionne sur les propriétés client d'une connexion MySQL.
- **MYSQL.CLIENT.CAPABILITIES.** Renvoie l'ensemble d'indicateurs que le client a défini dans le champ des fonctionnalités du paquet d'initialisation de l'établissement de la liaison lors de l'authentification. Les indicateurs définis sont par exemple CLIENT_FOUND_ROWS, CLIENT_COMPRESS et CLIENT_SSL.
- **MYSQL.CLIENT.CHAR_SET.** Renvoie la constante d'énumération affectée au jeu de caractères utilisé par le client. Les <m> <m> opérateurs EQ (\) et NE (\), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe. Les constantes d'énumération des jeux de caractères sont les suivantes :
  - LATIN2_CZECH_CS
  - DEC8_SWEDISH_CI
  - CP850_GENERAL_CI
  - GREEK_GENERAL_CI
  - LATIN1_GERMAN1_CI
  - HP8_ENGLISH_CI
  - KOI8R_GENERAL_CI
  - LATIN1_SWEDISH_CI
  - LATIN2_GENERAL_CI
  - SWE7_SWEDISH_CI
  - ASCII_GENERAL_CI
  - CP1251_BULGARIAN_CI
  - LATIN1_DANISH_CI
  - HEBREW_GENERAL_CI
  - LATIN7_ESTONIAN_CS
  - LATIN2_HUNGARIAN_CI
  - KOI8U_GENERAL_CI
  - CP1251_UKRAINIAN_CI
  - CP1250_GENERAL_CI
  - LATIN2_CROATIAN_CI
  - CP1257_LITHUANIAN_CI
  - LATIN5_TURKISH_CI

- LATIN1_GERMAN2_CI
- ARMSCII8_GENERAL_CI
- UTF8_GENERAL_CI
- CP1250_CZECH_CS
- CP866_GENERAL_CI
- KEYBCS2_GENERAL_CI
- MACCE_GENERAL_CI
- MACROMAN_GENERAL_CI
- CP852_GENERAL_CI
- LATIN7_GENERAL_CI
- LATIN7_GENERAL_CS
- MACCE_BIN
- CP1250_CROATIAN_CI
- LATIN1_BIN
- LATIN1_GENERAL_CI
- LATIN1_GENERAL_CS
- CP1251_BIN
- CP1251_GENERAL_CI
- CP1251_GENERAL_CS
- MACROMAN_BIN
- CP1256_GENERAL_CI
- CP1257_BIN
- CP1257_GENERAL_CI
- ARMSCII8_BIN
- ASCII_BIN
- CP1250_BIN
- CP1256_BIN
- CP866_BIN
- DEC8_BIN
- CORBEILLE GRECQUE
- HEBREW_BIN
- HP8_BIN
- KEYBCS2_BIN
- KOI8R_BIN
- KOI8U_BIN
- LATIN2_BIN
- LATIN5_BIN
- LATIN7_BIN
- CP850_BIN

  - CP852_BIN
  - SWE7_BIN
  - UTF8_BIN
  - GEOSTD8_GENERAL_CI
  - GEOSTD8_BIN
  - LATIN1_SPANISH_CI
  - UTF8_UNICODE_CI
  - UTF8_ICELANDIC_CI
  - UTF8_LATVIAN_CI
  - UTF8_ROMANIAN_CI
  - UTF8_SLOVENIAN_CI
  - UTF8_POLISH_CI
  - UTF8_ESTONIAN_CI
  - UTF8_SPANISH_CI
  - UTF8_SWEDISH_CI
  - UTF8_TURKISH_CI
  - UTF8_CZECH_CI
  - UTF8_DANISH_CI
  - UTF8_LITHUANIAN_CI
  - UTF8_SLOVAK_CI
  - UTF8_SPANISH2_CI
  - UTF8_ROMAN_CI
  - UTF8_PERSIAN_CI
  - UTF8_ESPERANTO_CI
  - UTF8_HUNGARIAN_CI
  - CHARSET NON VALIDE

- **MYSQL.CLIENT.DATABASE.** Renvoie le nom de la base de données spécifiée dans le paquet d'authentification que le client envoie au serveur de base de données. Il s'agit de l'attribut databasename.
- MYSQL.CLIENT.USER. Renvoie le nom d'utilisateur (dans le paquet d'authentification) avec lequel le client tente de se connecter à la base de données. Il s'agit de l'attribut utilisateur.
- **MYSQL.REQ.** Fonctionne sur une requête MySQL.
- **MYSQL.REQ.COMMAND.** Identifie la constante d'énumération affectée au type de commande dans la demande. Les <m> <m> opérateurs EQ (\) et NE (\), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe. Les valeurs constantes d'énumération sont les suivantes :

  - DORMIR
  - ARRÊTER

  - INIT_DB
  - REQUÊTE
  - LISTE_DE_CHAMP
  - CREATE_DB
  - DROP_DB
  - RAFRAÎCHIR
  - ARRÊT
  - STATISTIQUES
  - INFORMATION_PROCESSUS
  - SE CONNECTER
  - PROCESS_KILL
  - DEBUG
  - PING
  - HEURE
  - INSERTION_DIFFÉRÉE
  - CHANGE_UTILISATEUR
  - BINLOG_DUMP
  - TABLE_DUMP
  - CONNEXION_OUT
  - ENREGISTRER_ESCLAVE
  - STMT_PREPARE
  - STMT_EXECUTE
  - STMT_SEND_LONG_DATA
  - STMT_CLOSE
  - STMT_RESET
  - SET_OPTION
  - STMT_FETCH

- **MYSQL.REQ.QUERY.** Identifie la requête dans la requête MySQL.
- **MYSQL.REQ.QUERY.COMMAND.** Renvoie le premier mot clé de la requête MySQL.
- **MYSQL.REQ.QUERY.SIZE.** Renvoie la taille de la requête au format entier. La méthode SIZE est similaire à la méthode CONTENT_LENGTH qui renvoie la longueur d'une requête ou d'une réponse HTTP.
- **MYSQL.REQ.QUERY.TEXT.** Renvoie une chaîne couvrant l'intégralité de la requête.
- **<n>MYSQL.REQ.QUERY.TEXT (\).** Renvoie les n premiers octets de la requête MySQL sous forme de chaîne. <n>Ceci est similaire à HTTP.BODY (\).

  Paramètres :

  n - Nombre d'octets à renvoyer

- **MYSQL.RES.** Fonctionne sur une réponse MySQL.
- **<i>MYSQL.RES.ATLEAST_ROWS_COUNT (\).** Vérifie si la réponse comporte au moins un nombre de lignes et renvoie une valeur booléenne TRUE ou FALSE pour indiquer le résultat.

  Paramètres :

  i - Nombre de lignes
- **MYSQL.RES. ERREUR.** Identifie l'objet d'erreur MySQL. L'objet d'erreur inclut le numéro d'erreur et le message d'erreur.
- **MYSQL.RES.ERROR.MESSAGE.** Renvoie le message d'erreur extrait de la réponse d'erreur du serveur.
- **MYSQL.RES.ERROR.NUM.** Renvoie le numéro d'erreur extrait de la réponse d'erreur du serveur.
- **MYSQL.RES.ERROR.SQLSTATE.** Renvoie la valeur du champ SQLSTATE dans la réponse d'erreur du serveur. Le serveur MySQL traduit les valeurs des numéros d'erreur en valeurs SQLSTATE.
- **<i>MYSQL.RES.FIELD (\).** ^{Identifie le paquet qui correspond à la valeur i \th} champ individuel dans la réponse du serveur. Chaque paquet de champ décrit les propriétés de la colonne associée. Le nombre de paquets (i) commence à 0.

  Paramètres :

  i - Numéro du paquet
- **<i>MYSQL.RES.FIELD (\) .CATALOG.** Renvoie la propriété de catalogue du paquet de champs.
- **<i>MYSQL.RES.FIELD (\) .CHAR_SET.** Renvoie le jeu de caractères de la colonne. Les <m> <m> opérateurs EQ (\) et NE (\), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe.
- **<i>MYSQL.RES.FIELD (\) .TYPE DE DONNÉES.** Renvoie une constante d'énumération qui représente le type de données de la colonne. Il s'agit de l'attribut type (également appelé enum_field_type) de la colonne. Les <m> <m> opérateurs EQ (\) et NE (\), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe. Les valeurs possibles pour les différents types de données sont les suivantes :
  - DÉCIMAL
  - MINUSCULE
  - COURT
  - LONG
  - FLOTTER
  - DOUBLE
  - NULL
  - HORODATAGE

  - LONGLONG
  - INT24
  - DATE
  - HEURE
  - DATE/HEURE
  - ANNÉE
  - NOUVELLE DATE
  - VARCHAR (nouveau dans MySQL 5.0)
  - BIT (nouveau dans MySQL 5.0)
  - NEWDECIMAL (nouveau dans MySQL 5.0)
  - ENUM
  - ENSEMBLE
  - TINY_BLOB
  - MEDIUM_BLOB
  - LONG_BLOB
  - BLOB
  - VAR_STRING
  - FICELLE
  - GÉOMÉTRIE

- **<i>MYSQL.RES.FIELD (\) .DB.** Renvoie l'attribut d'identifiant de base de données (db) du paquet de champs.
- **<i>MYSQL.RES.FIELD (\) .DECIMALS.** Renvoie le nombre de positions après la virgule décimale si le type est DECIMAL ou NUMERIC. Il s'agit de l'attribut décimal du paquet de champs.
- **<i>MYSQL.RES.FIELD (\) .FLAGS.** Renvoie la propriété flags du paquet de champs. Les valeurs d'indicateur hexadécimales possibles sont les suivantes :
  - 0001 : NOT_NULL_FLAG
  - 0002 : PRI_KEY_FLAG
  - 0004 : UNIQUE_KEY_FLAG
  - 0008 : MULTIPLE_KEY_FLAG
  - 0010 : BLOB_FLAG
  - 0020 : DRAPEAU_NON SIGNÉ
  - 0040 : ZEROFILL_FLAG
  - 0080 : DRAPEAU BINAIRE
  - 0100 : ENUM_FLAG
  - 0200 : AUTO_INCREMENT_FLAG
  - 0400 : TIMESTAMP_FLAG
  - 0800 : SET_FLAG
- **<i>MYSQL.RES.FIELD (\) .LENGTH.** Renvoie la longueur de la colonne. Il s'agit de la valeur de

l'attribut de longueur du paquet de champs. La valeur renvoyée peut être supérieure à la valeur réelle. Par exemple, une instance d'une colonne VARCHAR (2) peut renvoyer la valeur 2 même si elle ne contient qu'un seul caractère.

- **<i>MYSQL.RES.FIELD (\) .NOM.** Renvoie l'identifiant de colonne (le nom suivant la clause AS, le cas échéant). Il s'agit de l'attribut de nom du paquet de champs.
- **<i>MYSQL.RES.FIELD (\) .NOM_ORIGINAL.** Renvoie l'identifiant de colonne d'origine (avant la clause AS, le cas échéant). Il s'agit de l'attribut org_name du paquet de champs.
- **<i>MYSQL.RES.FIELD (\) .TABLE_ORIGINALE.** Renvoie l'identifiant de table d'origine de la colonne (avant la clause AS, le cas échéant). Il s'agit de l'attribut org_table du paquet de champs.
- **<i>MYSQL.RES.FIELD (\) .TABLEAU.** Renvoie l'identifiant de table de la colonne (après la clause AS, le cas échéant). Il s'agit de l'attribut de table du paquet de champs.
- **MYSQL.RES.FIELDS_COUNT.** Renvoie le nombre de paquets de champs contenus dans la réponse (l'attribut field_count du paquet OK).
- **MYSQL.RES.OK.** Identifie le paquet OK envoyé par le serveur de base de données.
- **MYSQL.RES.OK.AFFECTED_ROWS.** Renvoie le nombre de lignes affectées par une requête INSERT, UPDATE ou DELETE. Il s'agit de la valeur de l'attribut affected_rows du paquet OK.
- **MYSQL.RES.OK.INSERT_ID.** Identifie l'attribut unique_id du paquet OK. Si aucune identité d'incrémentation automatique n'est générée par l'instruction ou la requête MySQL en cours, la valeur de unique_id, et donc la valeur renvoyée par l'expression, est 0.
- **MYSQL.RES.OK.MESSAGE.** Renvoie la propriété de message du paquet OK.
- **MYSQL.RES.OK.STATUS.** Identifie la chaîne de bits dans l'attribut server_status du paquet OK. Les clients peuvent utiliser l'état du serveur pour vérifier si la commande en cours fait partie d'une transaction en cours. Les bits de la chaîne de bits server_status correspondent aux champs suivants (dans l'ordre indiqué) :
  - EN TRANSACTION
  - AUTO_COMMIT
  - PLUS DE RÉSULTATS
  - REQUÊTE MULTIPLE
  - MAUVAIS INDEX UTILISÉ
  - AUCUN INDICE UTILISÉ
  - LE CURSEUR EXISTE
  - DERNIÈRE LIGNE VUE
  - BASE DE DONNÉES SUPPRIMÉE
  - AUCUNE BARRE OBLIQUE INVERSE NE S'ÉCHAPPE

- **MYSQL.RES.OK.WARNING_COUNT.** Renvoie l'attribut warning_count du paquet OK.
- **<i>MYSQL.RES.ROW (\).** ^{Identifie le paquet qui correspond à la valeur i \th} ligne individuelle dans la réponse du serveur de base de données.

  Paramètres :

  i - Numéro de ligne
- **<j>MYSQL.RES.ROW (\ <i>) .DOUBLE_ELEM (\).** ^{Vérifie si le fichier j \ th} ^{colonne du fichier i \th} la ligne de la table est NULL. Conformément aux conventions C, les index i et j commencent tous deux à 0. ^{Par conséquent, la ligne i et la colonne j sont en fait le (i+1) \th} ^{ligne et le (j+1) \th} colonne, respectivement.

  Paramètres :

  i - Numéro de ligne

  j - Numéro de colonne
- **MYSQL.RES.ROW (\ <i>) .IS_NULL_ELEM (j).** ^{Vérifie si le fichier j \ th} ^{colonne du fichier i \th} la ligne de la table est NULL. Conformément aux conventions C, les index i et j commencent tous deux à 0. ^{Par conséquent, la ligne i et la colonne j sont en fait le (i+1) \th} ^{ligne et le (j+1) \th} colonne, respectivement.

  Paramètres :

  i - Numéro de ligne

  j - Numéro de colonne
- **<j>MYSQL.RES.ROW (\ <i>) .NUM_ELEM (\).** ^{Renvoie une valeur entière à partir de j \th} ^{colonne du fichier i \th} rangée du tableau. Conformément aux conventions C, les index i et j commencent tous deux à 0. ^{Par conséquent, la ligne i et la colonne j sont en fait le (i+1) \th} ^{ligne et le (j+1) \th} colonne, respectivement.

  Paramètres :

  i - Numéro de ligne

  j - Numéro de colonne
- **MYSQL.RES.ROW (\ <i>) .TEXT_ELEM (j).** ^{Renvoie une chaîne à partir du fichier j \th} ^{colonne du fichier i \th} rangée du tableau. Conformément aux conventions C, les index i et j commencent tous deux à 0. ^{Par conséquent, la ligne i et la colonne j sont en fait le (i+1) \th} ^{ligne et le (j+1) \th} colonne, respectivement.

  Paramètres :

  i - Numéro de ligne

  j - Numéro de colonne

- **MYSQL.RES.TYPE.** Renvoie une constante d'énumération pour le type de réponse. Ses valeurs peuvent être ERROR, OK et RESULT_SET. Les <m> <m> opérateurs EQ (\) et NE (\), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec ce préfixe.

Expressions permettant d'évaluer les connexions au serveur Microsoft SQL

Les expressions suivantes évaluent le trafic associé aux serveurs de base de données Microsoft SQL Server. Vous pouvez utiliser les expressions basées sur les demandes (expressions commençant par MSSQL.CLIENT et MSSQL.REQ) dans les politiques pour prendre des décisions de commutation de demandes au point de liaison du serveur virtuel de commutation de contenu et les expressions basées sur les réponses (expressions commençant par MSSQL.RES) pour évaluer les réponses du serveur aux moniteurs de santé configurés par l'utilisateur.

Expression	Description
MSSQL.CLIENT.CAPABILITIES	Renvoie les champs OptionFlags1, OptionFlags2, OptionFlags3 et TypeFlags du paquet d'authentification Login7Authentication, dans cet ordre, sous la forme d'un entier de 4 octets. Chaque champ a une longueur d'un octet et spécifie un ensemble de fonctionnalités du client.
MSSQL.CLIENT.DATABASE	Renvoie le nom de la base de données client. La valeur renvoyée est de type texte.
MSSQL.CLIENT.USER	Renvoie le nom d'utilisateur avec lequel le client s'est authentifié. La valeur renvoyée est de type texte.
COMMANDE MSSQL.REQ.COMMAND	Renvoie une constante d'énumération qui identifie le type de commande figurant dans la demande envoyée à un serveur de base de données Microsoft SQL Server. La valeur renvoyée est de type texte. Les valeurs de la constante d'énumération sont QUERY, RESPONSE, RPC et ATTENTION. Les <m> <m> opérateurs EQ (\) et NE (\), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec cette expression.

Expression	Description
MSSQL.REQ.QUERY.COMMAND	Renvoie le premier mot clé de la requête SQL. La valeur renvoyée est de type texte.
MSSQL.REQ.QUERY.SIZE	Renvoie la taille de la requête SQL contenue dans la requête. La valeur renvoyée est un nombre.
MSSQL.REQ.QUERY.TEXT	Renvoie l'intégralité de la requête SQL sous forme de chaîne. La valeur renvoyée est de type texte.
<n>MSSQL.REQ.QUERY.TEXT (\)	Renvoie les n premiers octets de la requête SQL. La valeur renvoyée est de type texte. Paramètres : n - Nombre d'octets
MSSQL.REQ.RPC.NOM	Renvoie le nom de la procédure appelée dans une demande d'appel de procédure distante (RPC). Le nom est renvoyé sous forme de chaîne.
MSSQL.REQ.RPC.IS_PROCID	Renvoie une valeur booléenne qui indique si la demande d'appel de procédure distante (RPC) contient un ID de procédure ou un nom RPC. La valeur de retour Trueindique que la demande contient un ID de procédure et la valeur de retour FALSE indique que la demande contient un nom RPC.
MSSQL.REQ.RPC.PROCID	Renvoie l'ID de procédure de la demande d'appel de procédure distant (RPC) sous forme d'entier.
MSSQL.REQ.RPC.BODY **Remarque** : Non disponible pour les versions antérieures à la version 10.1.	Renvoie le corps de la requête SQL sous forme de chaîne sous forme de paramètres représentés par des clauses « a=b » séparées par des virgules, où « a » est le nom du paramètre RPC et « b » sa valeur.

Expression	Description
MSSQL.REQ.RPC.BODY (n) **Remarque** : Non disponible pour les versions antérieures à la version 10.1.	Renvoie une partie du corps de la requête SQL sous forme de chaîne sous forme de paramètres représentés par des clauses « a=b » séparées par des virgules, où « a » est le nom du paramètre RPC et « b » sa valeur. Les paramètres sont renvoyés uniquement à partir des « n » premiers octets de la requête, sans tenir compte de l'en-tête SQL. Seules les paires nom-valeur complètes sont renvoyées.
MSSQL.RES.ATLEAST_ROWS_COUNT (i)	Vérifie si la réponse comporte au moins un nombre de lignes. La valeur renvoyée est une valeur booléenne TRUE ou FalseValue. Paramètres : i - Nombre de lignes
MSSQL.RES.DONE.ROWCOUNT	Renvoie le nombre de lignes affectées par une requête INSERT, UPDATE ou DELETE. La valeur renvoyée est de type long non signé.
MSSQL.RES.DONE.STATUS	Renvoie le champ d'état à partir du jeton DONE envoyé par un serveur de base de données Microsoft SQL Server. La valeur renvoyée est un nombre.
MSSQL.RES. ERREUR. MESSAGE	Renvoie le message d'erreur provenant du jeton ERROR envoyé par un serveur de base de données Microsoft SQL Server. Il s'agit de la valeur du champ MsgText dans le jeton ERROR. La valeur renvoyée est de type texte.
MSSQL.RES.ERROR.NUM	Renvoie le numéro d'erreur du jeton ERROR envoyé par un serveur de base de données Microsoft SQL Server. Il s'agit de la valeur du champ Numéro du jeton ERROR. La valeur renvoyée est un nombre.
MSSQL.RES.ERROR.STATE	Renvoie l'état d'erreur à partir du jeton ERROR envoyé par un serveur de base de données Microsoft SQL Server. Il s'agit de la valeur du champ State dans le jeton ERROR. La valeur renvoyée est un nombre.

Expression	Description
<i>MSSQL.RES.FIELD (\) .TYPE DE DONNÉES	Renvoie le type de données du dernier champ de la réponse du serveur. Les <m> <m> fonctions EQ (\) et NE (\), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisées avec ce préfixe. <2>Par exemple, l'expression suivante renvoie une valeur booléenne TRUE si la fonction DATATYPE renvoie la valeur date/heure pour le troisième champ de la réponse : MSSQL.RES.FIELD (\) .DATATYPE.EQ (datetime) Paramètres : i - Numéro de ligne
<i>MSSQL.RES.FIELD (\) .LONGUEUR	Renvoie la longueur maximale possible du ième champ de la réponse du serveur. La valeur renvoyée est un nombre. Paramètres : i - Numéro de ligne
<i>MSSQL.RES.FIELD (\) .NOM	Renvoie le nom du dernier champ de la réponse du serveur. La valeur renvoyée est de type texte. Paramètres : i - Numéro de ligne
<i> <j>MSSQL.RES.ROW (\) .DOUBLE_ELEM (\)	Renvoie une valeur de type double à partir de la jème colonne de la ième ligne du tableau. Si la valeur n'est pas une valeur double, une condition UNDEF est déclenchée. Conformément aux conventions C, les index i et j commencent tous deux à 0 (zéro). Par conséquent, la ligne i et la colonne j sont en fait la (i + 1) ème ligne et la (j + 1) ème colonne, respectivement. Paramètres : i - Numéro de ligne j - Numéro de colonne

Expression	Description
<i>MSSQL.RES.ROW (\) .NUM_ELEM (j)	Renvoie une valeur entière à partir de la jème colonne de la dernière ligne du tableau. Si la valeur n'est pas un entier, une condition UNDEF est déclenchée. Conformément aux conventions C, les index i et j commencent tous deux à 0 (zéro). Par conséquent, la ligne i et la colonne j sont en fait la (i + 1) ème ligne et la (j + 1) ème colonne, respectivement. Paramètres : i - Numéro de ligne j - Numéro de colonne
<i>MSSQL.RES.ROW (\) .IS_NULL_ELEM (j)	Vérifie si la jème colonne de la ième ligne du tableau est NULL et renvoie une valeur booléenne TRUE ou FALSE pour indiquer le résultat. Conformément aux conventions C, les index i et j commencent tous deux à 0 (zéro). Par conséquent, la ligne i et la colonne j sont en fait la (i + 1) ème ligne et la (j + 1) ème colonne, respectivement. Paramètres : i - Numéro de ligne j - Numéro de colonne
<i>MSSQL.RES.ROW (\) .TEXT_ELEM (j)	Renvoie une chaîne de texte à partir de la jème colonne de la ligne Ith du tableau. Conformément aux conventions C, les index i et j commencent tous deux à 0 (zéro). Par conséquent, la ligne i et la colonne j sont en fait la (i + 1) ème ligne et la (j + 1) ème colonne, respectivement. Paramètres : i - Numéro de ligne j - Numéro de colonne
MSSQL.RES.TYPE	Renvoie une constante d'énumération qui identifie le type de réponse. Les valeurs de retour possibles sont les suivantes : ERROR, OK et RESULT_SET. Les <m> <m> opérateurs EQ (\) et NE (\), qui renvoient des valeurs booléennes pour indiquer le résultat d'une comparaison, sont utilisés avec cette expression.

Données de typecasting

August 20, 2021

Vous pouvez extraire des données d'un type (par exemple, du texte ou un entier) des demandes et des réponses et les transformer en données d'un autre type. Par exemple, vous pouvez extraire une chaîne et la transformer en format temporel. Vous pouvez également extraire une chaîne d'un corps de requête HTTP et la traiter comme un en-tête HTTP ou extraire une valeur d'un type d'en-tête de requête et l'insérer dans un en-tête de réponse d'un type différent.

Après avoir tapé les données, vous pouvez appliquer n'importe quelle opération appropriée au nouveau type de données. Par exemple, si vous tapez du texte dans un en-tête HTTP, vous pouvez appliquer toute opération applicable aux en-têtes HTTP à la valeur renvoyée.

Pour plus d'informations sur les données de typographie, consultez le fichier PDF Typecasting Operations .

Expressions régulières

May 5, 2023

Lorsque vous souhaitez effectuer des opérations de correspondance de chaînes plus complexes que celles effectuées avec les opérateurs CONTIENS (`"<string>"`) ou EQ (`"<string>"`), vous utilisez des expressions régulières. L'infrastructure de politiques de l'appliance Citrix® NetScaler® inclut des opérateurs auxquels vous pouvez transmettre des expressions régulières en tant qu'arguments pour la mise en correspondance du texte. Les noms des opérateurs qui travaillent avec les expressions régulières incluent la chaîne REGEX. Les expressions régulières que vous transmettez en tant qu'arguments doivent être conformes à la syntaxe des expressions régulières décrite dans `"<http://www.pcre.org/pcre.txt>."` Pour en savoir plus sur les expressions régulières, consultez `"<http://www.regular-expressions.info/quickstart.html>"` et à `"<http://www.silverstones.com/thebat/Regex.html>."`

Le texte cible d'un opérateur qui travaille avec des expressions régulières peut être du texte ou la valeur d'un en-tête HTTP. Voici le format d'une expression de stratégie avancée qui utilise un opérateur d'expression régulière pour opérer sur du texte :

```
<text>.<regex_operator>(re<delimiter><regex_pattern><delimiter>)
```

La chaîne `<text>` représente le préfixe d'expression de stratégie avancée qui identifie une chaîne de texte dans un paquet (par exemple, HTTP.REQ.URL). La chaîne `<regex_operator>` représente l'opérateur d'expression régulière. L'expression régulière commence toujours par la chaîne re.

Une paire de délimiteurs correspondants, représentés par `<delimiter>`, entoure la chaîne `<regex_pattern>`, qui représente l'expression régulière.

L'exemple d'expression suivant vérifie si l'URL d'un paquet HTTP contient la chaîne `*.jpeg` (où * est un caractère générique) et renvoie une valeur booléenne TRUE ou FALSE pour indiquer le résultat. L'expression régulière est entourée d'une paire de barre oblique (/), qui servent de délimiteurs.

```
http.req.url.regex_match(re/.<asterisk>\.jpeg/)
```

Les opérateurs d'expression régulière peuvent être combinés pour définir ou affiner la portée d'une recherche. Par exemple, `<text>.AFTER_REGEX(reregex_pattern1).BEFORE_REGEX(reregex_pattern2)` spécifie que la cible de la correspondance de chaîne est le texte entre les motifs regex_pattern1 et regex_pattern2. Vous pouvez utiliser un opérateur de texte sur la portée définie par les opérateurs d'expression régulière. Par exemple, vous pouvez utiliser l'opérateur CONTAINS (`"<string>"`) pour vérifier si la portée définie contient la chaîne abc :

```
<text>.AFTER_REGEX(re/regex_pattern1).BEFORE_REGEX(re/regex_pattern2/).
CONTAINS("abc")
```

> **Remarque**
>
> Le processus d'évaluation d'une expression régulière prend plus de temps que celui d'un opérateur tel que CONtains (`"<string>"`) ou EQ (`"<string>"`), qui fonctionnent avec des arguments de chaîne simples. Vous devez utiliser des expressions régulières uniquement si votre exigence dépasse le champ d'application des autres opérateurs.

Caractéristiques de base des expressions régulières

May 8, 2023

Voici les principales caractéristiques des expressions régulières telles que définies sur l'appliance NetScaler :

- Une expression régulière commence toujours par la chaîne « re » suivie d'une paire de caractères de délimitation (appelés délimiteurs) qui entourent l'expression régulière que vous souhaitez utiliser.

Par exemple, re# \# <regex_pattern> utilise le signe numérique (#) comme délimiteur.

- Une expression régulière ne peut pas dépasser 1 499 caractères.
- La correspondance des chiffres peut être effectuée à l'aide de la chaîne \ d (une barre oblique inverse suivie de d).
- Les espaces blancs peuvent être représentés à l'aide de \ s (une barre oblique inverse suivie de s).

- Une expression régulière peut contenir des espaces blancs.

Les différences entre la syntaxe NetScaler et la syntaxe PCRE sont les suivantes :

- NetScaler n'autorise pas les références rétrospectives dans les expressions régulières.
- Vous ne devez pas utiliser d'expressions régulières récursives.
- Le méta-caractère point correspond également au caractère de saut de ligne.
- L'Unicode n'est pas pris en charge.
- L'opération SET_TEXT_MODE (IGNORECASE) remplace l'opération (? i) option interne dans l'expression régulière.

Opérations pour les expressions régulières

October 5, 2021

Le tableau suivant décrit les opérateurs qui utilisent des expressions régulières. L'opération effectuée par un opérateur d'expression régulière dans une expression de stratégie avancée donnée dépend du fait que le préfixe d'expression identifie du texte ou des en-têtes HTTP. Les opérations qui évaluent les en-têtes remplacent toutes les opérations textuelles pour toutes les instances du type d'en-tête spécifié. Lorsque vous utilisez un opérateur, remplacez-le <text>par le préfixe d'expression de stratégie avancée que vous souhaitez configurer pour identifier le texte.

Opération d'expression régulière	Description
<text>.BEFORE_REGEX (<regular expression>)	Sélectionne le texte qui précède la chaîne correspondant à l'<regular expression>argument. Si l'expression régulière ne correspond à aucune donnée de la cible, elle renvoie un objet texte de longueur 0. L'expression suivante sélectionne la chaîne « text » dans « text/plain ». http.res.header (« content-type ») .before_regex (re#/#)
<text>.AFTER_REGEX (<regular expression>)	Sélectionne le texte qui suit la chaîne qui correspond à l'<regular expression>argument. Si l'expression régulière ne correspond à aucun texte de la cible, elle renvoie un objet texte de longueur 0. L'expression suivante extrait « Example » de « MyExample » : http.req.header (« etag ») .after_regex (re/my/)

Opération d'expression régulière	Description
<text>.REGEX_SELECT (<regular expression>)	Sélectionne une chaîne qui correspond à l'<regular expression>argument. Si l'expression régulière ne correspond pas à la cible, un objet texte de longueur 0 est renvoyé. L'exemple suivant extrait la chaîne « NS-CACHE-9.0 : 90 » d'un en-tête Via : http.req.header (« via ») .regex_select (re ! NS-CACHE- \ d. \ d : \ s* \ d {1,3} !)

Opération d'expression régulière	Description
<text>.REGEX_MATCH (<regular expression>)	Renvoie TRUE si la cible correspond à un <regular expression>argument de 1499 caractères maximum. L'expression régulière doit avoir le format suivant : re <delimiter>expression régulière< delimiter> Les deux délimiteurs doivent être identiques. En outre, l'expression régulière doit être conforme à la syntaxe de la bibliothèque d'expressions rationnelles compatible PERL (PCRE). Pour plus d'informations, accédez à http://www.pcre.org/pcre.txt. En particulier, consultez la page de manuel pcrepattern. Toutefois, notez ce qui suit : Les références antécédentes ne sont pas autorisées. Les expressions régulières récursives ne sont pas recommandées. Le métacaractère de point correspond également au caractère de saut de ligne. Le jeu de caractères Unicode n'est pas pris en charge. SET_TEXT_MODE (IGNORECASE) remplace le (? i) option interne spécifiée dans l'expression régulière. Voici des exemples : http.req.hostname.regex_match (re/[[:alpha :]] + (abc) {2,3}/) et http.req.url.set_text_mode (code URL) .regex_match (re# (a*b*+c*) #) L'exemple suivant correspond à ab et aB : http.req.url.regex_match (re/a (re/a (re/a (? i) b/) L'exemple suivant correspond à ab, ab, Ab et AB : http.req.url.set_text_mode (ignorecase) .regex_match (re/ab/) L'exemple suivant effectue une correspondance multiligne insensible à la casse dans laquelle le méta-caractère du point correspond également à un caractère de saut de ligne : http.req.body.regex_match (re/ (? ixm) (^ab (.*) cd$)/)

Exemples récapitulatifs d'expressions de stratégie et de stratégies avancées

May 5, 2023

Le tableau suivant fournit des exemples d'expressions de stratégie avancées que vous pouvez utiliser comme base pour vos propres expressions de stratégie avancée.

Tableau 1. Exemples d'expressions de stratégie avancées

Type d'expression	Exemples d'expressions
Examinez la méthode utilisée dans la requête HTTP.	`http.req.method.eq(post)http.req.method.eq(get)`

Vérifiez la valeur de l'en-tête Cache-Control ou Pragma dans une requête (req) ou une réponse HTTP (res).	`http.req.header("Cache-Control").contains("no-store")`
	`http.req.header("Cache-Control").contains("no-cache")`
	`http.req.header("Pragma").contains("no-cache")`
	`http.res.header("Cache-Control").contains("private")`
	`http.res.header("Cache-Control").contains("public")`
	`http.res.header("Cache-Control").contains("must-revalidate")http.res.header("Cache-Control").contains ("proxy-revalidate")`
	`http.res.header("Cache-Control").contains("max-age")`

Vérifiez la présence d'un en-tête dans une requête (req) ou une réponse (res).	`http.req.header("myHeader").exists` `http.res.header("myHeader").exists`

Type d'expression	Exemples d'expressions
Recherchez un type de fichier particulier dans une requête HTTP en fonction de l'extension de fichier.	`http.req.url.contains(".html")http.req.url.contains(".cgi")http.req.url.contains(".asp")http.req.url.contains(".exe")http.req.url.contains(".cfm")http.req.url.contains(".ex")http.req.url.contains(".shtml")http.req.url.contains(".htx")http.req.url.contains("/cgi-bin/")http.req.url.contains("/exec/")http.req.url.contains("/bin/")`
Recherchez tout élément autre qu'un type de fichier particulier dans une requête HTTP.	`http.req.url.contains(".png").not; http.req.url.contains(".jpeg").not`
Vérifiez le type de fichier envoyé dans une réponse HTTP en fonction de l'en-tête Content-Type.	`http.res.header("Content-Type").contains("text")http.res.header("Content-Type").contains "application/msword")http.res.header("Content-Type").contains("vnd.ms-excel")http.res.header("Content-Type").contains("application/vnd.ms-powerpoint"); http.res.header("Content-Type").contains("text/css"); http.res.header("Content-Type").contains("text/xml"); http.res.header("Content-Type").contains("image/")`
Vérifiez si cette réponse contient un en-tête d'expiration.	`http.res.header("Expires").exists`
Recherchez un en-tête Set-Cookie dans une réponse.	`http.res.header("Set-Cookie").exists`
Vérifiez l'agent qui a envoyé la réponse.	`http.res.header("User-Agent").contains("Mozilla/4.7")http.res.header("User-Agent").contains("MSIE")`

Type d'expression	Exemples d'expressions
Vérifiez si les 1024 premiers octets du corps d'une requête commencent par la chaîne « du texte ».	`http.req.body(1024).contains("some text")`

Le tableau suivant présente des exemples de configurations de stratégie et de liaisons pour les fonctions couramment utilisées.

Tableau 2 Exemples d'expressions et de stratégies avancées

Motif	Exemple
Utilisez la fonction de réécriture pour remplacer les occurrences de `http://with https://` dans le corps d'une réponse HTTP.	`add rewrite action httpRewriteAction replace_all http.res.body(50000)"\"https://\""-search http://add rewrite policy demo_rep34312 "http.res.body(50000).contains(\"http://\")" httpRewriteAction`
Remplacez toutes les occurrences de « abcd » par « 1234 » dans les 1000 premiers octets du corps HTTP.	`add rewrite action abcdTo1234Action replace_all "http.req.body(1000)""\"1234\""-search abcd add rewrite policy abcdTo1234Policy "http.req.body(1000).contains(\"abcd\")" abcdTo1234Action bind rewrite global abcdTo1234Policy 100 END -type REQ_OVERRIDE`
Réduisez la version HTTP vers la version 1.0 pour empêcher le serveur de répartir les réponses HTTP.	`add rewrite action downgradeTo1.0Action replace http.req.version.minor "\"0\""add rewrite policy downgradeTo1.0Policy "http.req.version.minor.eq(1)"downgradeTo1.0Action bind lb vserver myLBVserver -policyName downgradeTo1.0Policy -priority 100 -gotoPriorityExpression NEXT -type REQUEST`

Motif	Exemple
Supprimez les références au protocole HTTP ou HTTPS dans toutes les réponses, de sorte que si la connexion de l'utilisateur est HTTP, le lien soit ouvert à l'aide de HTTP, et si la connexion de l'utilisateur est HTTPS, le lien soit ouvert à l'aide du protocole HTTPS.	`add rewrite action remove_http_https replace_all "http.res.body(1000000).set_text_mode(ignorecase)""\"//\""-search "re~https?://|HTTPS?://~"add rewrite policy remove_http_https true remove_http_https bind lb vserver test_vsvr -policyName remove_http_https -priority 20 -gotoPriorityExpression NEXT -type RESPONSE`
Réécrivez les instances de http : en https : dans toutes les URL.	`add responder action httpToHttpsAction redirect "\"https://\" + http.req.hostname + http.req.url"add responder policy httpToHttpsPolicy "!CLIENT.SSL.IS_SSL"httpToHttpsAction bind responder global httpToHttpsPolicy 1 END -type OVERRIDE`
Modifiez une URL pour rediriger de l'URL A vers l'URL B. Dans cet exemple, « file5.html » est ajouté au chemin d'accès.	`add responder action appendFile5Action redirect \"http://\" + http.req.hostname + http.req.url + \"/file5.html\""add responder policy appendFile5Policy "http.req.url.eq(\"/testsite\")" appendFile5Action bind responder global appendFile5Policy 1 END -type OVERRIDE`

Motif	Exemple
Redirigez une URL externe vers une URL interne.	`add rewrite action act_external_to_internal REPLACE 'http.req.hostname.server'"www.my.host.com"'add rewrite policy pol_external_to_internal 'http.req.hostname.server.eq("www.external.host.com")'act_external_to_internal bind rewrite global pol_external_to_internal 100 END -type REQ_OVERRIDE`
Redirigez les demandes vers www.example.com qui ont une chaîne de requête vers www.webn.example.com. La valeur n est dérivée d'un paramètre de serveur dans la chaîne de requête, par exemple, server=5.	`add rewrite action act_redirect_query REPLACE q##http.req.header("Host").before_str(".example.com")'"Web"+ http.req.url.query.value("server")## add rewrite policy pol_redirect_query q##http.req.header("Host").eq("www.example.com")&& http.req.url.contains("?")'act_redirect_query##`
Limitez le nombre de demandes par seconde à partir d'une URL.	`add ns limitSelector ip_limit_selector http.req.url "client.ip.src"add ns limitIdentifier ip_limit_identifier -threshold 4 -timeSlice 3600 -mode request_rate -limitType smooth -selectorName ip_limit_selector add responder action my_Web_site_redirect_action redirect "\"http://www.mycompany.com/\""add responder policy ip_limit_responder_policy "http.req.url.contains(\"myasp.asp\")&& sys.check_limit (\"ip_limit_identifier\")"my_Web_site_redirect_action bind responder global ip_limit_responder_policy 100 END -type default`

Motif	Exemple
Vérifiez l'adresse IP du client, mais transmettez la demande sans modifier la demande.	`add rewrite policy check_client_ip_policy 'HTTP.REQ.HEADER ("x-forwarded-for").EXISTS HTTP.REQ.HEADER ("client-ip").EXISTS'NOREWRITE bind rewrite global check_client_ip_policy 100 END`
Supprimez les anciens en-têtes d'une demande et insérez un en-tête NS-Client.	`add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for add rewrite action del_client_ip delete_http_header client-ip add rewrite policy check_x_forwarded_for_policy 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS'del_x_forwarded_for add rewrite policy check_client_ip_policy 'HTTP.REQ.HEADER("client-ip").EXISTS' del_client_ip add rewrite action insert_ns_client_header insert_http_header NS-Client 'CLIENT.IP.SRC'add rewrite policy insert_ns_client_policy 'HTTP.REQ.HEADER("x-forwarded-for").EXISTS HTTP.REQ.HEADER("client-ip").EXISTS 'insert_ns_client_header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 END`

Motif	Exemple
Supprimez les anciens en-têtes d'une demande, insérez un en-tête NS-Client, puis modifiez l'action « Insérer un en-tête » de sorte que la valeur de l'en-tête inséré contienne les valeurs IP du client issues des anciens en-têtes et l'adresse IP de connexion de l'appliance NetScaler. Notez que cet exemple répète l'exemple précédent, à l'exception de l'action de réécriture du jeu final.	'ajouter une action de réécriture del_x_forwarded_for delete_http_header x-forwarded-for ajouter une action de réécriture del_client_ip delete_http_header client-ip ajouter une politique de réécriture check_x_forwarded_for_policy 'HTTP.REQ.HEADER (« x-forwarded-for ») .EXISTS' del_x_forwarded_for ajouter une politique de réécriture check_client_ip_policy 'HTTP.REQ. HEADER (« client-ip ») .EXISTS 'del_client_ip ajouter l'action de réécriture insert_ns_client_header insert_http_header NS-Client 'CLIENT.IP.SRC' ajouter la stratégie de réécriture insert_ns_client_policy 'HTTP.REQ.HEADER (« x-forwarded-for ») .EXISTS HTTP.REQ.HEADER (« client-ip ») .EXISTS' insert_ns_ns__client_ header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 FIN définir l'action de réécriture insert_ns_client_header -StringBuilderExpr 'HTTP.REQ.HEADER (« x-forwarded-for ») .VALUE (0) + "" + HTTP.REQ. EN-TÊTE (« client-ip ») .VALUE (0) + "" + CLIENT.IP.SRC'

Exemples de stratégies de stratégie avancées pour la réécriture

July 31, 2023

Avec la fonction de réécriture, vous pouvez modifier n'importe quelle partie d'un en-tête HTTP et, pour les réponses, vous pouvez modifier le corps HTTP. Vous pouvez utiliser cette fonctionnalité pour effectuer plusieurs tâches utiles, telles que la suppression d'en-têtes HTTP inutiles, le masquage d'URL internes, la redirection de pages Web et la redirection de requêtes ou de mots clés.

Dans les exemples suivants, vous créez d'abord une action de réécriture et une stratégie de réécriture.

Ensuite, vous liez la stratégie à l'échelle mondiale.

Ce document comprend les détails suivants :

- Redirection d'une URL externe vers une URL interne
- Redirection d'une requête
- Réécriture d'HTTP en HTTPS
- Suppression des en-têtes indésirables
- Réduction des redirections de serveur Web
- Masquage de l'en-tête du serveur
- Conversion de texte brut en chaîne codée par URL et de la manière inverse

Pour plus d'informations sur les commandes et les descriptions de syntaxe, consultez la page Réécriture de la référence des commandes .

Redirection d'une URL externe vers une URL interne

Cet exemple décrit comment créer une action de réécriture et une stratégie de réécriture qui redirige une URL externe vers une URL interne. Vous créez une action, appelée act_external_to_internal, qui effectue la réécriture. Ensuite, vous créez une stratégie appelée pol_external_to_internal.

Pour rediriger une URL externe vers une URL interne à l'aide de l'interface de ligne de commande

- Pour créer l'action de réécriture, à l'invite de commandes, tapez :

```
add rewrite action act_external_to_internal REPLACE "http.req.hostname.
server" "\" host_name_of_internal_Web_server\" "
```

- Pour créer la politique de réécriture, à l'invite de commande NetScaler, tapez :

```
add rewrite policy pol_external_to_internal "http.req.hostname.server.eq(\"
host_name_of_external_Web_server\")"act_external_to_internal
```

- Liez la stratégie à l'échelle mondiale.

Pour rediriger une URL externe vers une URL interne à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert** > **Réécrire** > **Actions**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action de réécriture**, entrez le nom act_external_to_internal.
4. Pour remplacer le nom d'hôte du serveur HTTP par le nom du serveur interne, choisissez **Remplacer** dans la zone de liste Type.
5. Dans le champ Nom de l'en-tête, tapez **Hôte**.

6. Dans l'expression chaîne d'un champ de texte de remplacement, saisissez le nom d'hôte interne de votre serveur Web.
7. Cliquez sur **Create**, puis cliquez sur **Close**.
8. Dans le volet de navigation, cliquez sur **Stratégies**.
9. Dans le volet de détails, cliquez sur **Ajouter**.
10. Dans le champ Nom, tapez pol_external_to_internal. Cette stratégie détecte les connexions au serveur Web.
11. Dans le menu déroulant **Action**, choisissez l'action act_external_to_internal.
12. Dans l'éditeur d'expressions, construisez l'expression suivante :

```
HTTP.REQ.HOSTNAME.SERVER.EQ("www.example.com")
<!--NeedCopy-->
```

1. Liez votre nouvelle stratégie à l'échelle mondiale.

Redirection d'une requête

Cet exemple décrit comment créer une action de réécriture et une stratégie de réécriture qui redirige une requête vers l'URL appropriée. L'exemple suppose que la requête contient un en-tête Host défini sur **www.example.com** et une méthode GET avec la **chaîne /query.cgi ? serveur=5**. La redirection extrait le nom de domaine de l'en-tête de l'hôte et le numéro de la chaîne de requête, puis redirige la requête de l'utilisateur vers le serveur **Web5.example.com**, où le reste de la requête de l'utilisateur est traité.

> **Remarque :**
>
> Bien que les commandes suivantes apparaissent sur plusieurs lignes, vous devez les saisir sur une seule ligne sans sauts de ligne.

Pour rediriger une requête vers l'URL appropriée à l'aide de l'interface de ligne de commande

- Pour créer une action de réécriture nommée act_redirect_query qui remplace le nom d'hôte du serveur HTTP par le nom du serveur interne, tapez :

```
add rewrite action act_redirect_query REPLACE http.req.header("Host").
before_str(".example.com")'"Web" + http.req.url.query.value("server")'
```

- Pour créer une politique de réécriture nommée pol_redirect_query, tapez les commandes suivantes à l'invite de commande NetScaler. Cette stratégie détecte les connexions au serveur Web qui contiennent une chaîne de requête. N'appliquez pas cette stratégie aux connexions qui ne contiennent pas de chaîne de requête :

```
add rewrite policy pol_redirect_query 'http.req.header("Host").eq(www.
example.com)&& http.req.url.contains("?")'act_redirect_query
```


- Liez votre nouvelle stratégie à l'échelle mondiale.

Étant donné que cette stratégie de réécriture est très spécifique et doit être exécutée avant toute autre stratégie de réécriture, il est conseillé de lui attribuer une priorité élevée. Si vous lui attribuez une priorité de 1, elle est évaluée en premier.

Réécriture d'HTTP en HTTPS

Cet exemple explique comment réécrire les réponses du serveur Web pour rechercher toutes les URL commençant par la chaîne « HTTP » et remplacer cette chaîne par « https ». Vous pouvez l'utiliser pour éviter de devoir mettre à jour des pages Web après avoir déplacé un serveur de HTTP vers HTTPS.

Pour rediriger les URL HTTP vers HTTPS à l'aide de l'interface de ligne de commande

- Pour créer une action de réécriture nommée act_replace_http_with_https qui remplace toutes les instances de la chaîne « HTTP » par la chaîne « https », entrez la commande suivante :

```
add rewrite action act_replace_http_with_https replace_all 'http.res.body
(100)''"https"'-search text("http")
```

- Pour créer une stratégie de réécriture nommée pol_replace_http_with_https qui détecte les connexions au serveur Web, entrez la commande suivante :

```
add rewrite policy pol_replace_http_with_https TRUE act_replace_http_with_https
 NOREWRITE
```

- Liez votre nouvelle stratégie à l'échelle mondiale.

Pour résoudre cette opération de réécriture, reportez-vous à la section « Étude de cas : Politique de réécriture pour la conversion des liens HTTP en HTTPS ne fonctionne pas. «

Suppression des en-têtes indésirables

Cet exemple explique comment utiliser une stratégie de réécriture pour supprimer les en-têtes indésirables. Plus précisément, l'exemple montre comment supprimer les en-têtes suivants :

- **Acceptez l'en-tête Encoding.** La suppression de l'en-tête Accept Encoding des réponses HTTP empêche la compression de la réponse.
- **En-tête Emplacement du contenu.** La suppression de l'en-tête Content Location des réponses HTTP empêche votre serveur de fournir à un pirate des informations susceptibles de permettre une faille de sécurité.

Pour supprimer des en-têtes des réponses HTTP, vous créez une action de réécriture et une stratégie de réécriture, et vous liez la stratégie globalement.

Pour créer l'action de réécriture appropriée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour supprimer l'en-tête Accepter l'encodage et empêcher la compression des réponses ou supprimer l'en-tête Emplacement de contenu :

- `add rewrite action "act_remove-ae"delete_http_header "Accept-Encoding"`
- `add rewrite action "act_remove-cl"delete_http_header "Content-Location"`

Pour créer la stratégie de réécriture appropriée à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour supprimer l'en-tête Accepter l'encodage ou l'en-tête Emplacement de contenu :

- `add rewrite policy "pol_remove-ae"true "act_remove-ae"`
- `add rewrite policy "pol_remove-cl"true "act_remove-cl"`

Pour lier la stratégie globalement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes, le cas échéant, pour lier globalement la stratégie que vous avez créée :

- `bind rewrite global pol_remove_ae 100`
- `bind rewrite global pol_remove_cl 200`

Réduction des redirections de serveur Web

Cet exemple explique comment utiliser une stratégie de réécriture pour modifier les connexions à votre page d'accueil et à d'autres URL qui se terminent par une barre oblique (/) vers la page d'index par défaut de votre serveur, empêchant les redirections et réduisant la charge sur votre serveur.

Pour modifier les requêtes HTTP au niveau du répertoire afin d'inclure la page d'accueil par défaut à l'aide de l'interface de ligne de commande

- Pour créer une action de réécriture nommée action-default-homepage qui modifie les URL qui se terminent par une barre oblique pour inclure la page d'accueil par défaut index.html, tapez :

```
add rewrite action "action-default-homepage"replace http.req.url.path "\"/
index.html\""
```

- Pour créer une stratégie de réécriture nommée policy-default-homepage qui détecte les connexions à votre page d'accueil et applique votre nouvelle action, tapez :

```
add rewrite policy "policy-default-homepage"q\##http.req.url.path.EQ("/")"
action-default-homepage"\##
```


- Liez globalement votre nouvelle politique pour la mettre en œuvre.

Masquage de l'en-tête du serveur

Cet exemple explique comment utiliser une stratégie de réécriture pour masquer les informations contenues dans l'en-tête du serveur dans les réponses HTTP de votre serveur Web. Cet en-tête contient des informations que les pirates peuvent utiliser pour compromettre votre site Web. Bien que le masquage de l'en-tête n'empêche pas un hacker qualifié de trouver des informations sur votre serveur, cela rend le piratage de votre serveur Web plus difficile et encourage les pirates à choisir des cibles moins protégées.

Pour masquer l'en-tête du serveur dans les réponses de l'interface de ligne de commande

1. Pour créer une action de réécriture nommée act_mask-server qui remplace le contenu de l'en-tête Server par une chaîne non informative, tapez :

```
add rewrite action "act_mask-server"replace "http.RES.HEADER(\"Server\")""
\"Web Server 1.0\""
```

1. Pour créer une stratégie de réécriture nommée pol_mask-server qui détecte toutes les connexions, tapez :

```
add rewrite policy "pol_mask-server"true "act_mask-server"
```

1. Liez globalement votre nouvelle politique pour la mettre en œuvre.

Comment convertir du texte brut en chaîne encodée par URL et de la manière inverse

Les expressions suivantes convertissent le texte brut en chaîne encodée par URL et de la manière inverse :

1. URL_RESERVED_CHARS_SAFE (chaîne vers URL ENCODED).

Exemple :

```
("abc def&123").URL_RESERVED_CHARS_SAFE
Output will be
 “abc%20def%26123”  which is url encoded.
<!--NeedCopy-->
```

1. SET_TEXT_MODE (URLENCODED) .DECODE_USING_TEXT_MODE. (URL ENCODÉE en chaîne)

Exemple :

```
("abc%20def%26123").SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE
Output will be
```



```
 “abc def&123”
<!--NeedCopy-->
```

Exemples de stratégies de réécriture et de répondeur

October 5, 2021

Voici quelques exemples de stratégies de réécriture et de répondeur :

Exemple 1 : Pour ajouter un en-tête Client-IP local à l’aide de l’interface de ligne de commande

```
add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.
   IP.SRC'
add rewrite policy pol_ins_client http.req.is_valid act_ins_client
bind rewrite global pol_ins_client 300 END

namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:06:48 GMT
* Server Apache/2.2.15 (CentOS) is not blacklisted
< Server: Apache/2.2.15 (CentOS)
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: "816c5-5-58bbc1e73cdd3"
< Accept-Ranges: bytes
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
< NS-Client: 10.102.1.98
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_namem@obelix:~$

<!--NeedCopy-->
```


Exemple 2 : masquer le type de serveur HTTP

```
add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("Server") ""Web Server 1.0""
add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:15:42 GMT
* Server Web Server 1.0 is not blacklisted
< Server: Web Server 1.0
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: "816c5-5-58bbc1e73cdd3"
< Accept-Ranges: bytes
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_namem@obelix:~$
<!--NeedCopy-->
```

Exemple 3 : Répondez en redirigeant vers une autre URL lorsqu'une URL est reçue

```
> add responder action act1 redirect ""www.google.com""
 Done
> add responder policy pol1 'HTTP.REQ.URL.CONTAINS("file")' act1
 Done
> bind responder global pol1 1
 Done
>

name:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
```



```
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 302 Found : Moved Temporarily
< Location: www.google.com
< Connection: close
< Cache-Control: no-cache
< Pragma: no-cache
<
* Closing connection 0
name@obelix:~$
<!--NeedCopy-->
```

Exemple 4 : Répondez avec un message qui peut être n'importe quelle expression ou un texte

```
add responder action act123 respondwith ""Please reach out to
   administrator""
add responder policy pol1 "HTTP.REQ.URL.CONTAINS("file")" act123
bind responder global pol1 100 END

name@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10..Responder Action and Policy:

>add responder action Redirect-Action redirect ""https://xyz.abc.com/
   dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302

>add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc"
   )" Redirect-Action

Binding to LB Virtual Server:

>bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -
   gotoPriorityExpression END -type REQUEST.
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
* Connection #0 to host 10.10.10.10 left intact
```



```
Please reach out to administratort_name@obelix:~$
<!--NeedCopy-->
```

Exemple 5 : répondre avec une page HTML importée

```
import responder htmlpage http://10.10.10.10)/testsite/file5.html
   page112
add responder action act1 respondwithHtmlpage page1
add responder policy pol1 true act1
bind responder global pol1 100

name@obelix:~$ curl -v http://10.10.10.10)/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10)) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.102.58.140
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Content-Length: 5
< Content-Type: text/html
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_name@obelix:~$
<!--NeedCopy-->
```

Exemple 6 : URL de redirection basée sur HOSTNAME à l'aide de la stratégie de répondeur

```
Responder Action and Policy:

>add responder action Redirect-Action redirect ""https://xyz.abc.com/
   dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302

>add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc"
   )" Redirect-Action

Binding to LB Virtual Server:

```



```
>bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Limitation de débit

May 5, 2023

La fonction de limitation de débit vous permet de définir la charge maximale pour une entité réseau ou une entité virtuelle donnée sur l'appliance NetScaler. Cette fonctionnalité vous permet de configurer la solution matérielle-logicielle pour surveiller le taux de trafic associé à l'entité et prendre des mesures préventives, en temps réel, en fonction du taux de trafic. Cette fonctionnalité est particulièrement utile lorsque le réseau est attaqué par un client hostile qui envoie un flot de requêtes à la solution matérielle-logicielle. Vous pouvez atténuer les risques qui affectent la disponibilité des ressources pour les clients et améliorer la fiabilité du réseau et des ressources que l'appliance gère.

Vous pouvez surveiller et contrôler le taux de trafic associé aux entités virtuelles et définies par l'utilisateur, y compris les serveurs virtuels, les URL, les domaines et les combinaisons d'URL et de domaines. Vous pouvez limiter le taux de trafic s'il est trop élevé, baser la mise en cache des informations sur le débit de trafic et rediriger le trafic vers un serveur virtuel d'équilibrage de charge donné si le débit de trafic dépasse une limite prédéfinie. Vous pouvez appliquer une surveillance basée sur le débit aux requêtes HTTP, TCP et DNS.

Pour surveiller le taux de trafic pour un scénario donné, vous devez configurer un *identificateur de limite de débit*. Un identificateur de limite de débit spécifie des seuils numériques tels que le nombre maximal de demandes ou de connexions (d'un type particulier) autorisées dans une période spécifiée appelée *tranche de temps*.

Vous pouvez également configurer des filtres, appelés *sélecteurs de flux*, et les associer à des identificateurs de limite de débit lorsque vous configurez les identificateurs. Après avoir configuré le sélecteur de flux facultatif et l'identificateur de limite, vous devez appeler l'identificateur de limite à partir d'une stratégie avancée. Vous pouvez appeler des identificateurs à partir de n'importe quelle fonctionnalité dans laquelle l'identifiant peut être utile, y compris la réécriture, le répondeur, le DNS et la mise en cache intégrée.

Vous pouvez activer et désactiver globalement les interruptions SNMP pour les identificateurs de limite de débit. Chaque interruption contient des données cumulatives pour l'intervalle de collecte de données configuré de l'identificateur de limite de débit (tranche de temps), sauf si vous avez spécifié plusieurs interruptions à générer par tranche de temps. Pour plus d'informations sur la configuration des interruptions et des gestionnaires SNMP, consultez SNMP.

Configuration d'un sélecteur de flux

May 5, 2023

Un sélecteur de flux de trafic est un filtre facultatif permettant d'identifier une entité pour laquelle vous souhaitez limiter l'accès. Le sélecteur est appliqué à une demande ou à une réponse et sélectionne des points de données (clés) qui peuvent être analysés par un identifiant de flux de débit. Ces points de données peuvent être basés sur presque toutes les caractéristiques du trafic, y compris les adresses IP, les sous-réseaux, les noms de domaine, les identifiants TCP ou UDP, et des chaînes ou extensions particulières dans les URL.

Un sélecteur de flux se compose d'expressions de stratégie avancées individuelles appelées selectlets. Chaque selectlet est une expression de stratégie avancée non composée. Un sélecteur de flux de trafic peut contenir jusqu'à cinq expressions non composées appelées selectlets. Chaque selectlet est considéré comme étant en relation AND avec les autres expressions. Voici quelques exemples de selectlets :

```
http.req.url
http.res.body(1000>after_str("car_model").before_str("made_in")"
"client.ip.src.subnet(24)"
<!--NeedCopy-->
```

L'ordre dans lequel vous spécifiez les paramètres est significatif. Par exemple, si vous configurez une adresse IP et un domaine (dans cet ordre) dans un sélecteur, puis que vous spécifiez le domaine et l'adresse IP (dans l'ordre inverse) dans un autre sélecteur, NetScaler considère ces valeurs comme uniques. Cela peut entraîner le comptage deux fois de la même transaction. De plus, si plusieurs politiques invoquent le même sélecteur, NetScaler peut à nouveau compter la même transaction plusieurs fois.

Remarque : Si vous modifiez une expression dans un sélecteur de flux, une erreur peut s'afficher si une stratégie qui l'appelle est liée à une nouvelle étiquette de stratégie ou à un nouveau point de liaison. Par exemple, supposons que vous créiez un sélecteur de flux nommé MyStreamSelector1, que vous l'appeliez à partir de MyLimitid1 et que vous invoquez l'identificateur à partir d'une stratégie DNS nommée DNSRateLimit1. Si vous modifiez l'expression dans MyStreamSelector1, vous risquez de recevoir une erreur lors de la liaison de DNSRateLimit1 à un nouveau point de liaison. La solution de contournement consiste à modifier ces expressions avant de créer les stratégies qui les invoquent.

Pour configurer un sélecteur de flux de trafic à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add stream selector <name> <rule> ...
<!--NeedCopy-->
```

Exemple :

```
add stream selector myStreamSel HTTP.REQ.URL CLIENT.IP.SRC
<!--NeedCopy-->
```

Pour configurer un sélecteur de flux à l'aide de l'utilitaire de configuration

Accédez à AppExpert > Limitation de débit > Sélecteurs, cliquez sur Ajouter et spécifiez les détails pertinents.

Configuration d'un identificateur de limite de débit de trafic

May 5, 2023

Un identificateur de limite de débit vérifie si la quantité de trafic dépasse une valeur spécifiée, dans un intervalle de temps particulier. L'identificateur renvoie un « Boolean TRUE » si la quantité de trafic dépasse une limite dans un intervalle de temps particulier. Lorsque vous incluez un identificateur de limite dans l'expression de stratégie DAvanced composée d'une règle de stratégie, vous devez inclure un sélecteur de flux. Si vous ne le spécifiez pas, l'identificateur de limite est appliqué à toutes les demandes ou réponses identifiées par les expressions composées.

> **Remarque :**
>
> La longueur maximale de stockage des résultats de chaîne (par exemple, HTTP.REQ.URL) est de 60 caractères. Si la chaîne (par exemple, URL) comporte 1 000 caractères, dont 50 sont suffisants pour identifier une chaîne de manière unique, vous pouvez utiliser une expression pour extraire les 50 caractères requis.

Pour configurer un identificateur de limite de trafic à partir de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ns limitIdentifier <limitIdentifier> -threshold <positive_integer>
    -timeSlice <positive_integer> -mode <mode> -limitType ( BURSTY |
    SMOOTH ) -selectorName <string> -maxBandwidth <positive_integer> -
    trapsInTimeSlice <positive_integer>
<!--NeedCopy-->
```


Description de l'argument

Identificateur de limite. Nom d'un identificateur de limite de taux. Doit commencer par une lettre ASCII ou un caractère de soulignement (_) et ne doit être composé que de caractères alphanumériques ou de soulignement ASCII. Les mots réservés ne doivent pas être utilisés. Il s'agit d'un argument obligatoire. Longueur maximale : 31

seuil. Nombre maximal de demandes autorisées dans la tranche de temps donnée lorsque les demandes (le mode est défini sur REQUEST_RATE) sont suivies par tranche de temps. Lorsque les connexions (le mode est défini sur CONNECTION) sont suivies, il s'agit du nombre total de connexions qui seraient laissées passer. Valeur par défaut : 1 Valeur minimale : 1 Valeur maximale : 4294967295

TimeSlice. Intervalle de temps, en millisecondes, spécifié en multiples de 10, pendant lequel les demandes sont suivies pour vérifier si elles dépassent le seuil. Cet argument n'est nécessaire que lorsque le mode est défini sur REQUEST_RATE. Valeur par défaut : 1000 Valeur minimale : 10 Valeur maximale : 4294967295

mode. Définit le type de trafic à suivre.

1. REQUEST_RATE. Effectue le suivi des demandes/tranche de temps.
2. CONNEXION. Suivi des transactions actives.

LimitType. Type de demande lisse ou éclatante.

NomSelector. Nom du sélecteur de limite de taux. Si cet argument est NULL, la limitation du débit sera appliquée à tout le trafic reçu par le serveur virtuel ou NetScaler (selon que l'identifiant de limite est lié à un serveur virtuel ou globalement) sans aucun **filtrage. Longueur maximale : 31**

Bande passante maximale. Bande passante maximale autorisée, en kbps. Valeur minimale : 0 Valeur maximale : 4294967287

Exemple :

Configuration de l'identificateur de limite de débit de trafic en mode BURSTY :

```
1 add ns limitIdentifier 100_request_limit -threshold 100 -timeSlice 1000
      -mode REQUEST_RATE -limitType BURSTY -selectorName
     limit_100_requests_selector -trapsInTimeSlice 30
2 <!--NeedCopy-->
```

Configuration de l'identificateur de limite de débit de trafic en mode SMOOTH :

```
1 add ns limitidentifier limit_req -mode request_rate -limitType smooth -
     timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200
2 <!--NeedCopy-->
```


Pour configurer un identificateur de limite de trafic à l'aide de l'utilitaire de configuration

Accédez à AppExpert > Limitation de débit > Identificateurs de limite, cliquez sur Ajouter et spécifiez les détails pertinents.

Configuration et liaison d'une stratégie de débit de trafic

May 5, 2023

Vous implémentez le comportement des applications basé sur le taux en configurant une politique dans une fonctionnalité NetScaler appropriée. La fonctionnalité doit prendre en charge les stratégies avancées. L'expression de stratégie doit contenir le préfixe d'expression suivant pour permettre à la fonctionnalité d'analyser le taux de trafic :

```
sys.check_limit(<limit_identifier>)
<!--NeedCopy-->
```

Où limit_identifier est le nom d'un identificateur de limite.

L'expression de stratégie doit être une expression composée qui contient au moins deux composants :

- Expression qui identifie le trafic auquel l'identificateur de limite de débit est appliqué. Par exemple :

```
    http.req.url.contains("my_aspx.aspx").
<!--NeedCopy-->
```

- Expression qui identifie un identificateur de limite de taux, par exemple, sys.check_limit (« my_limit_identifier »). Il doit s'agir de la dernière expression de l'expression de stratégie.

Pour configurer une stratégie basée sur les taux à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer une stratégie basée sur les taux et vérifier la configuration :

```
add cache|dns|rewrite|responder policy <policy_name> -rule expression
    && sys.check_limit("<LimitIdentifierName>") [<feature-specific
    information>]
<!--NeedCopy-->
```


Voici un exemple complet de règle de stratégie basée sur le taux. Notez que cet exemple suppose que vous avez configuré l'action du répondeur, send_direct_url, qui est associée à la stratégie. Notez que le paramètre sys.check_limit doit être le dernier élément de l'expression de stratégie :

```
1 add responder policy responder_threshold_policy "http.req.url.contains(
     "myindex.html") && sys.check_limit("my_limit_identifier")"
     send_direct_url
2 <!--NeedCopy-->
```

Pour plus d'informations sur la liaison d'une stratégie globalement ou à un serveur virtuel, reportez-vous à la section « Liaison de stratégies avancées ». «

Pour configurer une stratégie basée sur les taux à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez la fonctionnalité dans laquelle vous souhaitez configurer une stratégie (par exemple, Mise en cache intégrée, Réécriture ou Répondeur), puis cliquez sur Stratégies.
2. Dans le volet de détails, cliquez sur Ajouter. Dans Nom, saisissez un nom unique pour la stratégie.
3. Sous Expression, entrez la règle de stratégie et assurez-vous d'inclure le paramètre sys.check_limit en tant que composant final de l'expression. Par exemple :

   ```
   1 http.req.url.contains("my_aspx.aspx") && sys.check_limit("
        my_limit_identifier")
   2 <!--NeedCopy-->
   ```

4. Saisissez des informations spécifiques à la fonctionnalité concernant la stratégie.

   Par exemple, vous devrez peut-être associer la stratégie à une action ou à un profil. Pour plus d'informations, consultez la documentation spécifique aux fonctionnalités.
5. Cliquez sur Créer, puis sur Fermer.
6. Cliquez sur Enregistrer.

Affichage du débit de trafic

August 20, 2021

Si le trafic via un ou plusieurs serveurs virtuels correspond à une stratégie basée sur les taux, vous pouvez afficher le débit de ce trafic. Les statistiques de taux sont conservées dans l'identificateur de limite que vous avez nommé dans la règle pour la stratégie basée sur le taux. Si plusieurs stratégies

utilisent le même identificateur de limite, vous pouvez afficher le taux de trafic tel que défini par les accès à toutes les stratégies qui utilisent cet identificateur de limite particulier.

Pour afficher le débit de trafic à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour afficher le débit de trafic :

```
show ns limitSessions <limitIdentifier>
<!--NeedCopy-->
```

Exemple :

```
sh limitsession myLimitSession
<!--NeedCopy-->
```

Pour afficher le débit de trafic à l'aide de l'utilitaire de configuration

1. Accédez à AppExpert > Limitation de débit > Identificateurs de limite.
2. Sélectionnez un identificateur de limite dont vous souhaitez afficher le taux de trafic.
3. Cliquez sur le bouton Afficher les sessions. Si le trafic via un ou plusieurs serveurs virtuels correspond à une stratégie de limitation de débit qui utilise cet identificateur de limite (et que les accès se trouvent dans la tranche de temps configurée pour cet identificateur), la boîte de dialogue Détails de la session apparaît. Sinon, vous recevez un message « Aucune session n'existe ».

Test d'une stratégie basée sur les taux

May 5, 2023

Pour tester une politique basée sur le débit, vous pouvez envoyer du trafic vers n'importe quel serveur virtuel auquel une politique basée sur le débit est liée.

Présentation des tâches : Tester une politique basée sur les taux

1. Configurez un sélecteur de flux (facultatif) et un identifiant de limite de débit (obligatoire). Par exemple :

```
add stream selector sel_subnet Q.URL "CLIENT.IP.SRC.SUBNET(24)"
add ns limitIdentifier k_subnet -Threshold 4 -timeSlice 3600 -mode
    REQUEST_RATE  -limittype smooth  -selectorName sel_subnet  -
   trapsInTimeSlice 8
<!--NeedCopy-->
```


2. Configurez l'action que vous souhaitez associer à la politique qui utilise l'identifiant de limite de débit. Par exemple :

```
add responder action resp_redirect redirect ""http://response_site.com/""
<!--NeedCopy-->
```

3. Configurez une politique qui utilise le préfixe de l'expression sys.check_limit pour appeler l'identifiant de limite de débit. Par exemple, la politique peut appliquer un identifiant de limite de débit à toutes les demandes provenant d'un sous-réseau particulier, comme suit :

```
add responder policy resp_subnet "SYS.CHECK_LIMIT("k_subnet")" resp_redirect
<!--NeedCopy-->
```

4. Liez la politique globalement ou à un serveur virtuel. Par exemple :

```
bind responder global resp_subnet 6 END -type DEFAULT
<!--NeedCopy-->
```

5. Dans la barre d'adresse d'un navigateur, envoyez une requête HTTP de test à un serveur virtuel. Par exemple :

```
http://<IP of a vserver>/testsite/test.txt
<!--NeedCopy-->
```

6. À l'invite de commande NetScaler, tapez :

```
show ns limitSessions \<limitIdentifier\>
<!--NeedCopy-->
```

Exemple

```
> sh limitsession k_subnet
1)      Time Remaining:       98 secs  Hits: 2
                            Action Taken: 0
        Total Hash:    1718618  Hash String: /test.txt
        IPs gathered:
                1) 10.217.253.0
        Active Transactions: 0
 Done
>
<!--NeedCopy-->
```


7. Répétez la requête et vérifiez à nouveau les statistiques de l'identificateur de limite pour vérifier que les statistiques sont mises à jour correctement.

Exemples de politiques basées sur les taux

May 5, 2023

Cette rubrique répertorie quelques exemples de politiques basées sur les taux.

Limiter le nombre de requêtes provenant d'une URL

Exécutez les commandes suivantes pour limiter le nombre de requêtes par seconde à partir d'une URL :

```
add stream selector ipStreamSelector http.req.url "client.ip.src" add ns limitIdentifier ipLimitIdentifier -threshold 4 -timeSlice 1000 -mode request_rate -limitType smooth -selectorName ipStreamSelector

add responder action myWebSiteRedirectAction redirect ""http: //www.mycompany .com/""

add responder policy ipLimitResponderPolicy "http.req-url.contains("myasp.asp") && sys.check_limit("ipLimitIdentifier")" myWebSiteRedirectaction

bind responder global ipLimitResponderPolicy 100 END -type default
<!--NeedCopy-->
```

Mettre en cache une réponse pour l'URL de la demande

Exécutez les commandes suivantes pour mettre en cache une réponse si le taux d'URL de la demande dépasse 5 toutes les 20 000 millisecondes :

```
add stream selector cacheStreamSelector http.req.url add ns limitidentifier cacheRateLimitIdentifier -threshold 5 -timeSlice 2000 -selectorName cacheStreamSelector

add cache policy cacheRateLimitPolicy -rule "http req.method.eq(get) && sys.check_limit "cacheRateLimitIdentifier")" -action cache

bind cache global cacheRateLimitPolicy -priority 10
<!--NeedCopy-->
```


Supprimer une connexion basée sur les cookies

Exécutez les commandes suivantes pour interrompre une connexion en fonction des cookies reçus dans les requêtes `www.mycompany.com` dont les demandes dépassent la limite de débit :

```
add stream selector reqCookieStreamSelector "http req.cookie «value("
    mycookie")" "client.ip.src.subnet(24)"

add ns limitIdentifier myLimitIdentifier -Threshold 2 -timeSlice 3000 -
    selectorName reqCookieStreamSelector

add responder action sendRedirectUrl redirect '"http://www.mycompany.
    com" + http.req.url' -bypassSafetyCheck YES

add responder policy rateLimitCookiePolicy "http. req.url.contains("www
    .yourcompany.com") && sys check_limit("myLimitIdentifier")"
    sendRedirectUrl
<!--NeedCopy-->
```

Supprimer un paquet DNS depuis une adresse IP particulière

Exécutez les commandes suivantes pour supprimer un paquet DNS si les requêtes provenant d'une adresse IP client et d'un domaine DNS spécifiques dépassent la limite de débit :

```
add stream selector dropDNSStreamSelector client udp.dns.domain client.
    ip.src
add ns limitIdentifier dropDNSRateIdentifier -timeslice 20000 -mode
    request_rate -selectorName dropDNSStreamSelector -maxBandwidth 1 -
    trapsintimeslice 20

add dns policy dnsDropOnClientRatePolicy "sys check_limit ("
    dropDNSRateIdentifier")" -drop yes
<!--NeedCopy-->
```

Limiter le nombre de requêtes HTTP provenant du même hôte

Exécutez les commandes suivantes pour limiter le nombre de requêtes HTTP provenant du même hôte avec un masque de sous-réseau de 32 et ayant la même adresse IP de destination :

```
add stream selector ipv6_sel "CLIENT.IPv6.src.subne (32)" CLIENT.IPv6.
    dst Q.URL
add ns limitIdentifier ipvé_id -imeSlice 20000 -selectorName ipvé_sel
add lb vserver ipv6é_vip HTTP 3ffe::209 80 -persistenceType NONE -
    cltTimeout 180
```



```
add responder action redirect_page redirect ""http://redirectpage.com/""
add responder policy ipvé_resp_pol "SYS.CHECK_LIMIT("ipv6_id")" redirect_page
bind responder global ipv6_resp_pol 5 END -type DEFAULT
<!--NeedCopy-->
```

Exemples de cas d'utilisation pour les stratégies basées sur les taux

May 5, 2023

Les scénarios suivants décrivent deux utilisations des politiques basées sur le débit dans le cadre de l'équilibrage global de la charge des serveurs (GSLB) :

- Le premier scénario décrit l'utilisation d'une politique basée sur le débit qui envoie le trafic vers un nouveau centre de données si le taux de requêtes DNS dépasse 1 000 par seconde.
- Dans le second scénario, si plus de cinq demandes DNS arrivent pour un client DNS local (LDNS) au cours d'une période donnée, les demandes supplémentaires sont supprimées.

Redirection du trafic en fonction du débit de trafic

Dans ce scénario, vous configurez une méthode d'équilibrage de charge basée sur la proximité et une politique de limitation de débit qui identifie les demandes DNS pour une région particulière. Dans la politique de limitation du débit, vous spécifiez un seuil de 1 000 requêtes DNS par seconde. Une politique DNS applique la politique de limitation du débit aux demandes DNS pour la région « Europe.gb.17.london.uk-East.ISP-UK ». « Dans la politique DNS, les demandes DNS qui dépassent le seuil de limite de débit, en commençant par la demande 1001 et en continuant jusqu'à la fin de l'intervalle d'une seconde, doivent être transmises aux adresses IP associées à la région « Amérique du Nord.US.TX.Dallas.us-East.ISP-US ». «

La configuration suivante illustre ce scénario :

```
add stream selector DNSSelector1 client.udp.dns.domain

add ns limitIdentifier DNSLimitIdentifier1 -threshold 5 -timeSlice 1000 -selectorName DNSSelector1

add dns policy DNSLimitPolicy1 "client.ip.src.matches_location("Europe.GB.17.London.\*.\*") &&
sys.check_limit("DNSLimitIdentifier1")" -preferredLocation "North America.US.TX.Dallas.\*.\*"

```



```
bind dns global DNSLimitPolicy1 5
<!--NeedCopy-->
```

Suppression des requêtes DNS en fonction du débit de trafic

Dans l'exemple suivant d'équilibrage de charge global des serveurs, vous configurez une politique de limitation de débit qui permet de diriger un maximum de cinq requêtes DNS dans un intervalle donné, par domaine, vers un client LDNS pour résolution. Toutes les demandes dépassant ce taux sont abandonnées. Ce type de politique peut aider à protéger NetScaler contre l'exploitation des ressources. Par exemple, dans ce scénario, si la durée de vie (TTL) d'une connexion est de cinq secondes, cette politique empêche le LDNS de demander un domaine. Il utilise plutôt des données mises en cache sur NetScaler.

```
add stream selector LDNSSelector1 client.udp.dns.domain client.ip.src

add ns limitIdentifier LDNSLimitIdentifier1 -threshold 5 -timeSlice
    1000 -selectorName LDNSSelector1

add dns policy LDNSPolicy1 "client.udp.dns.domain.contains(".") && sys.
    check_limit("LDNSLimitIdentifier1")" -drop YES

bind dns global LDNSPolicy1 6

show gslb vserver gvip

gvip - HTTP     State: UP
Last state change was at Mon Sep  8 11:50:48 2008 (+711 ms)
Time since last state change: 1 days, 02:55:08.830
Configured Method: STATICPROXIMITY
BackupMethod: ROUNDROBIN
No. of Bound Services :  3 (Total)       3 (Active)
Persistence: NONE       Persistence ID: 100
Disable Primary Vserver on Down: DISABLED       Site Persistence: NONE
Backup Session Timeout: 0
Empty Down Response: DISABLED
Multi IP Response: DISABLED Dynamic Weights: DISABLED
Cname Flag: DISABLED
Effective State Considered: NONE
1.     site11_svc(10.100.00.00: 80)- HTTP State: UP    Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: Europe.GB.17.London.UK-East.ISP-UK
```



```
2.      site12_svc(10.101.00.100: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: North America.US.TX.Dallas.US-East.ISP-US
3.      site13_svc(10.102.00.200: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: North America.US.NJ.Salem.US-Mid.ISP-US
4.      www.gslbindia.com        TTL: 5 secn
Cookie Timeout: 0 min   Site domain TTL: 3600 sec
Done
<!--NeedCopy-->
```

Limitation de débit pour les domaines de trafic

May 5, 2023

Vous pouvez configurer la limitation du débit pour les domaines de trafic. L'expression suivante dans le langage d'expressions NetScaler identifie le trafic associé aux domaines de trafic.

- client.traffic_domain.id

Vous pouvez configurer la limitation du débit pour le trafic associé à un domaine de trafic particulier, à un ensemble de domaines de trafic ou à tous les domaines de trafic.

Pour configurer la limitation du débit pour les domaines de trafic, vous devez effectuer les étapes suivantes sur une appliance NetScaler à l'aide de l'utilitaire de configuration ou de la ligne de commande NetScaler :

1. Configurez un sélecteur de flux qui utilise l'expression client.traffic_domain.id pour identifier le trafic, associé aux domaines de trafic, dont le débit doit être limité.
2. Configurez un identifiant de limite de débit qui spécifie des paramètres tels que le seuil maximum pour le trafic à limiter. Vous associez également un sélecteur de flux au limiteur de débit à cette étape.
3. Configurez une action que vous souhaitez associer à la politique qui utilise l'identifiant de limite de débit.
4. Configurez une politique qui utilise le préfixe de l'expression sys.check_limit pour appeler l'identifiant de limite de débit et associez l'action à cette politique.
5. Liez la stratégie à l'échelle mondiale.

Prenons un exemple dans lequel deux domaines de trafic, avec les ID 10 et 20, sont configurés sur NetScaler NS1. Sur le domaine de trafic 10, LB1-TD-1 est configuré pour équilibrer la charge des serveurs S1 et S2 ; LB2-TD1 est configuré pour équilibrer la charge des serveurs S3 et S4.

Sur le domaine de trafic 20, LB1-TD-2 est configuré pour équilibrer la charge des serveurs S5 et S6 ; LB2-TD2 est configuré pour équilibrer la charge des serveurs S7 et S8.

Le tableau suivant répertorie quelques exemples de politiques de limitation de débit pour les domaines de trafic dans l'exemple de configuration.

Motif	Commandes CLI
Limitez le nombre de requêtes à 10 par seconde pour chacun des domaines de trafic.	ajouter un sélecteur de flux tdratelimit-1 CLIENT.TRAFFIC_DOMAIN.ID add ns LimitIdentifier limitidf-1 -threshold 10 -SelectorName tdratelimit-1 -TrapsInTimeSlice 0 ajouter une politique de répondeur ratelimit-pol « sys.check_limit (\" limitidf-1 \ ») » DROP bind responder global ratelimit-pol 1
Limitez le nombre de demandes à 5 par client et par seconde pour chacun des domaines de trafic.	ajouter un sélecteur de flux tdandclientip CLIENT.IP.SRC, CLIENT.TRAFFIC_DOMAIN.ID add ns LimitIdentifier td_limitidf -threshold 5 -SelectorName tdandclientip -TrapsInTimeslice 5 ajouter une politique de répondeur tdratelimit-pol « sys.check_limit (\" td_limitidf \ ») » DROP bind responder global tdratelimit-pol 2
Limitez le nombre de demandes envoyées pour un domaine de trafic particulier (par exemple, le domaine de trafic 10) à 30 demandes toutes les 3 secondes.	ajouter un sélecteur de flux tdratelimit CLIENT.TRAFFIC_DOMAIN.ID ajouter ns LimitIdentifier td10_limitidf -threshold 30 -TimeSlice 3000 -SelectorName tdratelimit -TrapsInTimeslice 5 ajouter une politique de réponse td10ratelimit « client.traffic_domain.id ==10 && sys.check_limit (\" td10_limitidf \ ») » DROP bind responder global td10ratelimit 3

Motif	Commandes CLI
Limitez le nombre de connexions à 5 par client et par seconde pour un domaine de trafic particulier (par exemple, le domaine de trafic 20).	ajouter un sélecteur de flux tdandclientip CLIENT.IP.SRC CLIENT.TRAFFIC_DOMAIN.ID ajouter ns LimitIdentifier td20_limitidf -threshold 5 -mode CONNECTION -SelectorName tdandclientip -TrapsInTimeslice 5 ajouter une politique de répondeur td20_ratelimit « client.traffic_domain.id ==20 && sys.check_limit (\" td20_limitidf \ ») » DROP bind répondeur global td20_ratelimit 4

Configurer la limite de débit au niveau des paquets

January 26, 2022

Vous pouvez configurer un sélecteur de flux et une stratégie de répondeur pour collecter des statistiques au niveau des paquets passant par toutes les connexions identifiées par le sélecteur. Si le nombre de paquets par seconde dépasse le seuil configuré, la stratégie applique l'action configurée (RESET ou DROP). Vous pouvez configurer ces stratégies pour tous les types de serveurs virtuels. Les paquets de toutes tailles sont pris en compte.

Pour configurer la limitation de débit au niveau des paquets, effectuez les tâches suivantes

1. Activer l'équilibrage de charge
2. Ajout d'un sélecteur
3. Ajouter un identifiant de flux
4. Ajouter une stratégie de répondeur
5. Ajouter un serveur virtuel d'équilibrage de charge
6. Stratégie de répondeur Bind

Pour activer la fonction d'équilibrage de charge

À l'invite de commandes, tapez :

```
enable ns feature lb
<!--NeedCopy-->
```


Pour ajouter un sélecteur de flux

À l'invite de commandes, tapez :

```
add stream selector packetlimitselector client.ip.src client.tcp.
   srcport client.ip.dst client.tcp.dstport
<!--NeedCopy-->
```

Pour ajouter un identifiant de flux

À l'invite de commandes, tapez :

```
add stream identifier packetlimitidentifier packetlimitselector -
   interval 1
<!--NeedCopy-->
```

Pour activer le suivi des paquets ACK uniquement

À l'invite de commandes, tapez :

```
set stream identifier packetlimitidentifier  -trackAckOnlyPackets
   ENABLED
<!--NeedCopy-->
```

Pour ajouter une stratégie de répondeur

À l'invite de commandes, tapez :

```
add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
   packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", <
   max_threshold_PPS>, ACTION, 0/1)" NOOP
<!--NeedCopy-->
```

Où,

- <max_threshold_PPS>est le nombre maximum de paquets autorisés par seconde via la connexion.
- L'ACTION peut être DROP ou RESET.
- 0 ou 1 représente le type de limite ; 0 représente le type de limite BURSTY et 1 représente le type de limite SMOOTH.

Exemple :


```
add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
    packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", 40, RESET, 0)"
     NOOP
<!--NeedCopy-->
```

Pour ajouter un serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez :

```
add lb vserver <name> <serviceType> <ip> <port>

add lb vserver Vserver-lb-1 HTTP 10.102.20.200 80
<!--NeedCopy-->
```

Pour lier une stratégie de répondeur

Une fois le sélecteur et la stratégie de répondeur configurés, la stratégie peut être liée globalement ou au serveur virtuel spécifique.

À l'invite de commandes, tapez l'une des commandes suivantes :

```
bind responder global <policyName> <priority> [<gotoPriorityExpression
    >] [-type <type>] [-invoke  (<labelType>  <labelName>) ]
<!--NeedCopy-->
```

OU

```
bind lb vserver <name>@  (-policyName <string>@ [-priority <
    positive_integer>]
<!--NeedCopy-->
```

Exemples :

```
bind responder global packet_rate_sessionpolicy 101 END -type
    REQ_DEFAULT

bind responder global packet_rate_sessionpolicy 102 END -type

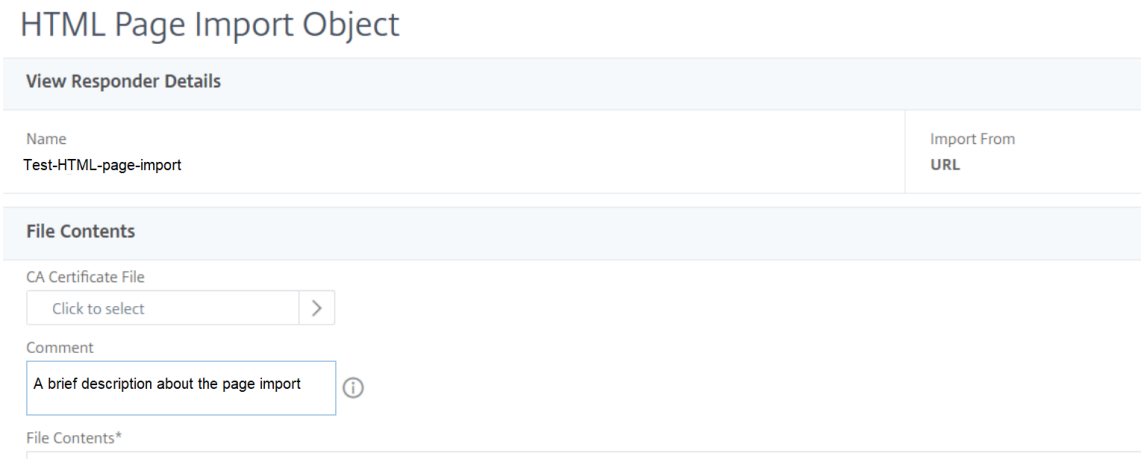
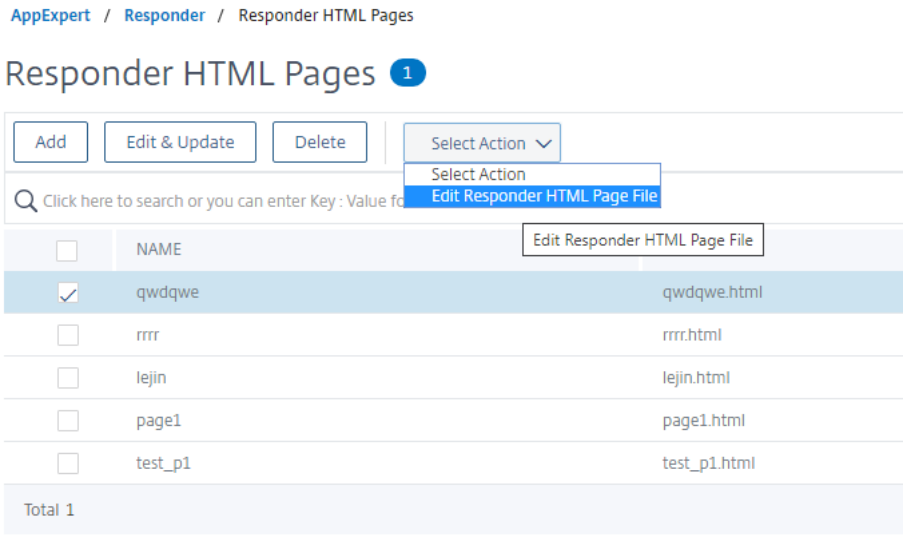
bind lb vserver v1 -policyname packet_rate_sessionpolicy -priority 10
<!--NeedCopy-->
```


Répondeur

May 5, 2023

> **Avertissement**
>
> Les fonctionnalités de filtrage utilisant des stratégies classiques sont obsolètes et Citrix vous recommande d'utiliser les fonctionnalités de réécriture et de répondeur avec une infrastructure de stratégie avancée.

Les configurations Web complexes d'aujourd'hui nécessitent souvent des réponses différentes aux requêtes HTTP qui semblent, à première vue, similaires. Lorsque les utilisateurs demandent une page Web, vous pouvez souhaiter fournir une page différente en fonction de la situation géographique de l'utilisateur, des spécifications du navigateur ou des langues acceptées par le navigateur et de l'ordre de préférence. Vous souhaiterez peut-être interrompre la connexion si la demande provient d'une plage d'adresses IP qui a généré des attaques DDoS ou initié des tentatives de piratage.

Responder prend en charge des protocoles tels que TCP, DNS (UDP) et HTTP. Lorsque le répondeur est activé sur votre appliance, les réponses du serveur peuvent être basées sur l'expéditeur de la demande, son origine et d'autres critères ayant des implications en matière de sécurité et de gestion du système. La fonctionnalité est simple et rapide à utiliser. En évitant l'invocation de fonctionnalités plus complexes, il réduit les cycles CPU et le temps passé à traiter les demandes qui ne nécessitent pas de traitement complexe.

Pour gérer des données sensibles telles que des informations financières, si vous voulez vous assurer que le client utilise une connexion sécurisée pour parcourir un site, vous pouvez rediriger la demande vers une connexion sécurisée en utilisant `https://` au lieu de `http://`.

Pour utiliser un répondeur, procédez comme suit :

- Activez une fonction de répondeur sur l'appliance.
- Configurez une action de répondeur. L'action peut consister à générer une réponse personnalisée, à rediriger une demande vers une autre page Web ou à réinitialiser une connexion.
- Configurez une politique de réponse. La politique détermine les demandes (trafic) sur lesquelles une action doit être entreprise.
- Liez chaque politique à un point de liaison pour la mettre en œuvre. Un point de liaison fait référence à une entité au niveau de laquelle l'appliance NetScaler examine le trafic pour voir s'il correspond à une politique. Par exemple, un point de liaison peut être un serveur virtuel d'équilibrage de charge.

Vous pouvez spécifier une action par défaut pour les demandes qui ne correspondent à aucune politique, et vous pouvez contourner le contrôle de sécurité pour les actions qui, autrement, généreraient des messages d'erreur.

La fonctionnalité de réécriture de NetScaler permet de réécrire certaines informations dans les demandes ou les réponses gérées par NetScaler. La section suivante présente certaines différences entre les deux fonctionnalités.

Comparaison entre les options Réécriture et Répondeur

La principale différence entre la fonction de réécriture et la fonction répondeur est la suivante :

Le répondeur ne peut pas être utilisé pour les expressions de réponse ou basées sur le serveur. Le répondeur ne peut être utilisé que pour les scénarios suivants, en fonction des paramètres du client :

- Redirection d'une requête HTTP vers de nouveaux sites Web ou pages Web
- Répondre avec une réponse personnalisée
- Dépose ou réinitialisation d'une connexion au niveau de la demande

S'il existe une politique de réponse, NetScaler examine la demande du client, prend des mesures conformément aux politiques applicables, envoie la réponse au client et ferme la connexion avec le client.

S'il existe une politique de réécriture, NetScaler examine la demande du client ou la réponse du serveur, prend des mesures conformément aux politiques applicables et transmet le trafic au client ou au serveur.

En général, il est recommandé d'utiliser un répondeur si vous souhaitez que l'appliance réinitialise ou abandonne une connexion en fonction d'un paramètre basé sur une demande. Utilisez un répondeur pour rediriger le trafic ou répondez par des messages personnalisés. Utilisez la réécriture pour manipuler les données des requêtes et réponses HTTP.

Activation de la fonction Responder

May 5, 2023

Pour utiliser la fonction Répondeur, vous devez d'abord l'activer.

Pour activer la fonctionnalité de répondeur à l'aide de l'interface de ligne de commande NetScaler :

À l'invite de commandes, tapez les commandes suivantes pour activer la fonction de répondeur et vérifier la configuration :

- `enable ns feature <feature>`
- `show ns feature`

Exemple :

```
enable ns feature Responder
 Done
```



```
> show ns feature

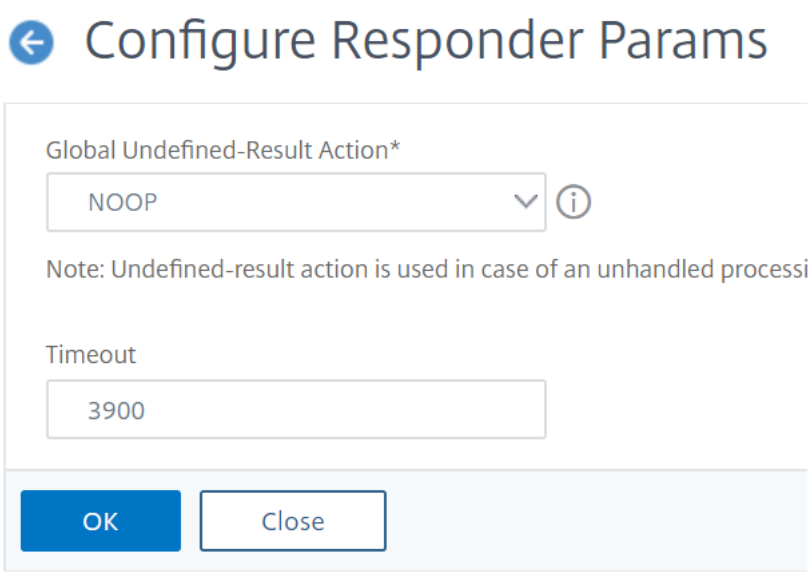
        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 .
 .
 .
 19)     Responder                       RESPONDER           ON
 20)     NetScaler Push                  push                OFF
 Done
>
<!--NeedCopy-->
```

Pour activer la fonctionnalité de répondeur à l'aide de l'interface graphique :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Dans le volet d'informations, sous **Modes** et **fonctionnalités**, cliquez sur **Modifier les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, activez la case à cocher **Répondeur**, puis cliquez sur **OK**.
4. Dans la ou les **fonctions Activer/Désactiver ?**, cliquez sur **OUI**. Un message apparaît dans la barre d'état indiquant que la fonction a été activée.

Configurer l'action du répondeur

June 2, 2023

Après avoir activé la fonction de répondeur, vous devez configurer une ou plusieurs actions de traitement des demandes. Le répondeur prend en charge les types d'actions suivants :

- **Répondez avec**. Envoie la réponse définie par l'expression Target sans transférer la demande à un serveur Web. (L'appliance NetScaler remplace un serveur Web et fait office de serveur Web.) Utilisez ce type d'action pour définir manuellement une réponse HTML simple. Normalement, le texte d'une action Répondre avec consiste en un code d'erreur de serveur Web et une brève page HTML.
- **Répondez avec SQL OK**. Envoie la réponse SQL OK désignée définie par l'expression Target. Utilisez ce type d'action pour envoyer une réponse SQL OK à une requête SQL.
- **Répondez avec une erreur SQL**. Envoie la réponse d'erreur SQL désignée définie par l'expression Target. Utilisez ce type d'action pour envoyer une réponse d'erreur SQL à une

requête SQL.

- **Répondez avec une page HTML**. Envoie la page HTML désignée en tant que réponse. Vous pouvez choisir dans une liste déroulante de pages HTML précédemment chargées ou charger une nouvelle page HTML. Utilisez ce type d'action pour envoyer une page HTML importée en tant que réponse. L'appliance répond avec un en-tête personnalisé dans l'action Responder responsewithhtmlpage. Vous pouvez configurer jusqu'à huit en-têtes personnalisés. La page HTML importée est stockée dans le répertoire `/var/download/responder`.
- **Redirection**. Redirige la demande vers une autre page Web ou un autre serveur Web. Une action de redirection peut rediriger les demandes initialement envoyées vers un site Web « fictif » qui existe dans le DNS, mais pour lequel il n'existe pas de serveur Web réel, vers un site Web réel. Il peut également rediriger les demandes de recherche vers une URL appropriée. Normalement, la cible de redirection d'une action de redirection consiste en une URL complète.

Configurez une action de répondeur à l'aide de l'interface de ligne de commande :

Affiche les paramètres actuels de l'action de répondeur spécifiée. Si aucun nom d'action n'est fourni, affichez la liste de toutes les actions du répondeur actuellement configurées sur l'appliance NetScaler, avec des paramètres abrégés.

À l'invite de commandes, tapez les commandes suivantes pour configurer une action de répondeur et vérifier la configuration :

- `add responder action <name> <type> <target>`
- `show responder action`

Paramètres :

- **Nom**. Nom de l'action du répondeur. Longueur maximale : 127
- **type**. Type d'action du répondeur. Il peut s'agir de : (répondez avec).
- **target**. Expression indiquant par quoi répondre.
- **htmlpage**. Option spécifiant de répondre par une page HTML.
- **hits**. Le nombre de fois où l'action a été effectuée.
- **referenceCount**. Nombre de références à l'action.
- **undefHits**. Le nombre de fois où l'action a abouti dans UNDEF.
- **comment**. Tout type d'informations concernant cette action de répondeur.
- **builtin**. Indicateur permettant de déterminer si l'action du répondeur est intégrée ou non.

Exemple :

```
1 Create a responder action that displays a "Not Found" error page for
     URLs that do not exist:
```



```
2
3 > add responder action act404Error respondWith '"HTTP/1.1 404 Not Found
     \r\n\r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web
     server."'
4 Done
5
6 > show responder action
7
8 1) Name: act404Error
9 Operation: respondwith
10 Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE + " does
     not exist on the web server."
11 Hits: 0
12 Undef Hits: 0
13 Action Reference Count: 0
14 Done
15
16 Create a responder action that displays a  “Not Found”  error page for
     URLs that do not exist:
17
18 add responder action act404Error respondWith '"HTTP/1.1 404 Not Found\r
     \n\r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web
     server."'
19 Done
20 > show responder action
21
22 1) Name: act404Error
23 Operation: respondwith
24 Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE + " does
     not exist on the web server."
25 Hits: 0
26 Undef Hits: 0
27 Action Reference Count: 0
28 Done
29
30 <!--NeedCopy-->
```

Modifiez une action de répondeur existante à l’aide de l’interface de ligne de commande :

À l’invite de commandes, tapez la commande suivante pour modifier une action de répondeur existante et vérifier la configuration :

- `set responder action <name> -target <string>`
- `show responder action`

Exemple :


```
set responder action act404Error  -target '"HTTP/1.1 404 Not Found\r\n\
    r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web
    server."'
 Done
> show responder action

1)      Name: act404Error
        Operation: respondwith
        Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE +
            " does not exist on the web server."
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
 Done

<!--NeedCopy-->
```

Supprimez une action de répondeur à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante pour supprimer une action de répondeur et vérifier la configuration :

- `rm responder action <name>`
- `show responder action`

Exemple :

```
rm responder action act404Error
 Done

> show responder action
 Done

<!--NeedCopy-->
```

Ajoutez des en-têtes personnalisés dans l'action responsewithhtmlpage responder à l'aide de la CLI :

Une appliance NetScaler peut désormais répondre avec des en-têtes personnalisés dans l'action du répondeur responsewithhtmlpage. Vous pouvez configurer jusqu'à huit en-têtes personnalisés. Auparavant, l'appliance répondait uniquement avec des en-têtes statiques `Content-type:text/html` et `Content-Length:<value>`.

> **Remarque :**
>
> Dans la configuration d'en-tête personnalisée, vous pouvez également écraser la valeur de l'en-

> tête « Content-Type ».

À l'invite de commandes, tapez la commande suivante :

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string
>] [-responseStatusCode <positive_integer>] [-reasonPhrase <expression>] [-
headers <name(value)> ...]
```

Où,

name : nom de l'action du répondeur. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), le hachage (#), l'espace (), à (@), égal (=), deux-points (:) et les caractères de soulignement. Peut être modifié après l'ajout de la stratégie de répondeur.

Type : type d'action du répondeur. Les paramètres disponibles fonctionnent comme suit :

1. **respondwith <target>** - Répondez à la demande avec l'expression spécifiée comme cible.
2. **respondwithhtmlpage** - Répondez à la demande en utilisant l'objet de page HTML chargé spécifié comme cible.
3. **redirect** - Redirige la demande vers l'URL spécifiée comme cible.
4. **sqlresponse_ok** - Envoie une réponse SQL OK
5. **sqlresponse_error** - Envoie une réponse d'erreur SQL. Il s'agit d'un argument obligatoire. Valeurs possibles : `noop`, `respondwith`, `redirect`, `respondwithhtmlpage`, `sqlresponse_ok`, `sqlresponse_error`

Cible : expression indiquant par quoi répondre. En général, une URL pour les stratégies de redirection ou une expression de syntaxe par défaut. Outre les expressions de syntaxe par défaut de NetScaler qui font référence aux informations contenues dans la demande, une expression de générateur de chaînes peut contenir du texte et du code HTML, ainsi que de simples codes d'échappement qui définissent de nouvelles lignes et de nouveaux paragraphes. Placez chaque élément d'expression du générateur de chaînes (une expression de syntaxe par défaut NetScaler ou une chaîne) entre guillemets doubles. Utilisez le signe plus (+) pour joindre les éléments.

htmlpage : pour les stratégies `respondwithhtmlpage`, nom de l'objet de page HTML à utiliser comme réponse. Vous devez d'abord importer l'objet de page. Longueur maximale : 31

Commentaire : tout type d'information concernant cette action du répondeur. Longueur maximale : 255

responseStatusCode : code d'état de réponse HTTP, par exemple 200, 302, 404, etc. La valeur par défaut pour le type `redirect action` est 302 et pour `respondwithhtmlpage` est 200 Valeur minimale : 100 Valeur maximale : 599

ReasonPhrase : expression spécifiant la phrase de raison de la réponse HTTP. La phrase de raison peut être un littéral de chaîne avec des guillemets ou une expression PI. Pa exemple : `"Invalid URL : "+ HTTP.REQ.URL Maximum Length: 8191`

En-têtes : un ou plusieurs en-têtes à insérer dans la réponse HTTP. Chaque en-tête est spécifié comme `"name(expr),"` ou expr est une expression qui est évaluée lors de l'exécution pour fournir la valeur de l'en-tête nommé. Vous pouvez configurer un maximum de huit en-têtes pour une action de répondeur.

Configurez une action de répondeur à l'aide de l'interface graphique :

1. Accédez à **AppExpert > Répondeur > Actions**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une action, cliquez sur **Ajouter**.
   - Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
3. Cliquez sur **Créer** ou sur **OK**, selon que vous créez une action ou modifiez une action existante.
4. Cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que la fonction a été activée.
5. Pour supprimer une action de répondeur, sélectionnez-la, puis cliquez sur **Supprimer**. Un message apparaît dans la barre d'état, indiquant que la fonctionnalité a été désactivée.

Ajouter une expression à l'aide de la boîte de dialogue **Ajouter une expression**

1. Dans la boîte de dialogue **Créer une action de répondeur** ou **Configurer une action de répondeur**, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Ajouter une expression**, dans la première zone de liste, choisissez le premier terme de votre expression.
   - HTTP. Le protocole HTTP. Choisissez cette option si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP.
   - SYS. Un ou plusieurs sites Web protégés. Sélectionnez cette option si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
   - CLIENT. L'ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.
   - ANALYTICS. Les données analytiques associées à la demande. Sélectionnez cette option si vous souhaitez examiner les métadonnées de la demande.
   - SIP. Une demande SIP. Choisissez cette option si vous souhaitez examiner certains aspects d'une demande SIP. Lorsque vous faites votre choix, la zone de liste la plus à droite répertorie les termes appropriés pour la partie suivante de votre expression.
3. Dans la deuxième zone de liste, choisissez le deuxième terme de votre expression. Les choix dépendent du choix que vous avez effectué à l'étape précédente et sont adaptés au contexte. Une fois que vous avez fait votre deuxième choix, la fenêtre d'aide située sous la fenêtre Construire une expression (qui était vide) affiche de l'aide décrivant le but et l'utilisation du terme que vous venez de choisir.
4. Continuez à choisir des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente, ou à taper des chaînes ou des nombres dans les zones de texte qui s'affichent

pour vous inviter à entrer une valeur, jusqu'à ce que votre expression soit terminée.

Configuration de l'action HTTP globale

Vous pouvez configurer l'action HTTP globale pour qu'elle invoque une action de répondeur lorsqu'une requête HTTP arrive à son heure d'attente. Pour configurer cette fonctionnalité, vous devez d'abord créer l'action de répondeur que vous souhaitez appeler. Configurez ensuite l'action de temporisation HTTP globale pour répondre à un délai d'expiration avec cette action de répondeur.

Configurez l'action HTTP globale à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

- `set ns httpProfile -reqTimeoutAction <responder action name>`
- `save ns config`

Pour `<responder action name>`, remplacez le nom de l'action du répondeur.

Configurer l'importation d'une page HTML

Lorsqu'une appliance NetScaler répond par un message personnalisé, nous pouvons répondre par un fichier HTML. Vous pouvez importer le fichier à l'aide de la commande **`import`** `responder htmlpage`, puis utiliser ce fichier dans la commande `add responder action <act name> respondwithhtmlpage <file name>`. Vous pouvez également importer le fichier via l'interface graphique de NetScaler. Vous pouvez importer la page HTML souhaitée dans le dossier de l'appliance et la télécharger pendant l'exécution du répondeur.

Importer une page HTML à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
import responder htmlpage [<src>] <name> [-comment <string>] [-overwrite][-CAcertFile <string>]
```

Exemple :

```
import responder htmlpage http://www.example.com/page.html my-responder-page -CAcertFile my_root_ca_cert
```

Où,
un certificat CA est utilisé pour vérifier le certificat client. Le certificat doit être importé à l'aide de la commande CLI **`import`** `ssl certfile` ou d'une commande équivalente via une API ou une interface graphique. Si aucun nom de certificat n'est configuré, les certificats CA racine par défaut sont utilisés pour la vérification du certificat.

Importer une page HTML depuis le système de fichiers local

Vous pouvez également importer une page HTML depuis le système de fichiers local. Pour importer, copiez le fichier à l'aide de SCP ou de toute autre manière dans le répertoire /var/tmp/, puis importez-le à l'aide du mot clé « local : ». Par exemple :

```
import responder htmlpage local:my_local_file.html my_local_file
```

Où `my_local_file.html` se trouve dans le répertoire « /var/tmp/ ».

> **Remarque**
>
> : le mot clé « local : » recherche uniquement le fichier dans le répertoire « /var/tmp/ ». Pour les partitions autres que celles par défaut, vous devez copier le fichier dans le répertoire tmp spécifique à la partition qui se trouve dans `/var/partitions/<partition name>/tmp`.

Importer une page HTML à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Répondeur** > **Importations de pages HTML**.
2. Dans le volet de détails **Importations HTML du répondeur**, cliquez sur **Ajouter**.
3. Dans la **page Objet d'importation de page HTML**, définissez les paramètres suivants :
   a) Nom. Nom de la page HTML.
   b) Importer depuis. Importé à partir d'un fichier, d'un texte ou d'un texte.
   c) URL. Sélectionnez cette option pour entrer l'emplacement URL du fichier HTML.
   d) Dossier. Sélectionnez le fichier HTML dans le répertoire de l'appliance.
   e) Texte. Sélectionnez le fichier HTML sous forme de texte.
4. Cliquez sur **Continuer**.
5. Vérifiez les détails de la page HTML du répondeur.
6. Cliquez sur **Terminé**.



Pour modifier une page HTML, vous pouvez sélectionner un fichier et cliquer sur **Modifier le fichier de page HTML du répondeur** dans la liste déroulante **Sélectionner une action** .



Configuration d'une stratégie de répondeur

May 5, 2023

Après avoir configuré une action de répondeur, vous devez ensuite configurer une politique de répondeur pour sélectionner les demandes auxquelles l'appliance NetScaler doit répondre. Une stratégie de répondeur est basée sur une règle, qui consiste en une ou plusieurs expressions. La règle est associée à une action, qui est exécutée si une demande correspond à la règle.

Remarque : pour la création et la gestion des politiques de réponse, l'interface graphique fournit une assistance qui n'est pas disponible à l'invite de commande NetScaler.

Pour configurer une politique de répondeur à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction <actionName>`
- `show responder policy <name>`

Exemple :

```
1  > add responder policyThree "CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)"
     RESET
2   Done
3  > show responder policyThree
```



```
4
5          Name: policyThree
6          Rule: CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)
7          Responder Action: RESET
8          UndefAction: Use Global
9          Hits: 0
10         Undef Hits: 0
11  Done
12 <!--NeedCopy-->
```

Pour modifier une politique de répondeur existante à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `set responder policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>]`
- `show responder policy <name>`

Pour supprimer une politique de répondeur à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `rm responder policy <name>`
- `show responder policy`

Exemple :

```
1  >rm responder policy pol404Error
2   Done
3
4  > show responder policy
5   Done
6  <!--NeedCopy-->
```

Pour configurer une stratégie de répondeur à l'aide de l'interface graphique :

1. Accédez à **AppExpert > Responder > Politiques**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle stratégie, cliquez sur **Ajouter**.
   - Pour modifier une politique existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
3. Cliquez sur **Créer** ou sur **OK**, selon que vous créez une nouvelle stratégie ou modifiez une stratégie existante.
4. Cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que la fonction a été configurée.

Liaison d'une stratégie de répondeur

May 5, 2023

Pour mettre en œuvre une politique, vous devez la lier soit globalement, afin qu'elle s'applique à tout le trafic qui passe par NetScaler, soit à un serveur virtuel spécifique, afin que la politique s'applique uniquement aux demandes dont l'adresse IP de destination est le VIP de ce serveur virtuel.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel nombre entier positif.

Dans le système d'exploitation NetScaler, les priorités des politiques fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible. Par exemple, si vous avez trois stratégies avec des priorités de 10, 100 et 1000, la stratégie affectée d'une priorité de 10 est exécutée en premier, puis la stratégie attribuée une priorité de 100 et enfin la stratégie affectée d'un ordre de 1000. La fonctionnalité de répondeur implémente uniquement la première stratégie à laquelle une demande correspond, pas les stratégies supplémentaires auxquelles elle pourrait également correspondre. La priorité de la stratégie est donc importante pour obtenir les résultats souhaités.

Vous pouvez vous laisser suffisamment de place pour ajouter d'autres stratégies dans n'importe quel ordre, tout en les définissant pour qu'elles soient évaluées dans l'ordre de votre choix, en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous la liez globalement. Vous pouvez ensuite ajouter d'autres stratégies à tout moment sans avoir à réaffecter la priorité d'une stratégie existante.

Pour plus d'informations sur les politiques de liaison sur NetScaler, consultez Politiques et expressions.

> **Remarque :**
>
> Les stratégies de répondeur sont liées à des serveurs virtuels basés sur TCP.

Pour lier globalement une politique de répondeur à l'aide de la ligne de commande NetScaler :

À l'invite de commandes, tapez la commande suivante pour lier globalement une stratégie de répondeur et vérifier la configuration :

- `bind responder global <policyName> <priority> [<gotoPriorityExpression> [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show responder global`

Exemple :

```
1 > bind responder global poliError 100
2  Done
3 > show responder global
```



```
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

 Done
<!--NeedCopy-->
```

Pour lier la politique du répondeur à un serveur virtuel spécifique à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `bind lb vserver <name> -policyname <policy_name> -priority <priority>`
- `show lb vserver vs-loadbal <name>`

Exemple :

```
> bind lb vserver vs-loadbal -policyName policyTwo -priority 100
 Done
> show lb vserver
1)      vs-loadbal (10.102.29.20:80) - HTTP     Type: ADDRESS
        State: OUT OF SERVICE
        Last state change was at Wed Aug 19 09:05:47 2009 (+211 ms)
        Time since last state change: 2 days, 00:58:03.260
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
2)      vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
        State: DOWN
        Last state change was at Wed Aug 19 10:03:46 2009 (+213 ms)
        Time since last state change: 2 days, 00:00:04.260
        Effective State: DOWN
        Client Idle Timeout: 9000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
```



```
31          Mode: IP
32          Persistence: NONE
33          Connection Failover: DISABLED
34   Done
35  <!--NeedCopy-->
```

Pour lier globalement une stratégie de répondeur à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Répondeur** > **Stratégies**.
2. Sur la page **Stratégies du répondeur**, sélectionnez une stratégie de répondeur, puis cliquez sur **Gestionnaire de stratégies**.
3. Dans le menu Points de liaison de la boîte de dialogue **Responder Policy Manager**, sélectionnez Global par défaut.
4. Cliquez sur **Insérer une stratégie** pour insérer une nouvelle ligne et afficher une liste déroulante de toutes les stratégies de répondeur indépendant.
5. Cliquez sur l'une des stratégies de la liste. Cette stratégie est insérée dans la liste des stratégies de répondeur liées globalement.
6. Cliquez sur **Appliquer les modifications**.
7. Cliquez sur **Fermer**. Un message s'affiche dans la barre d'état, indiquant que la configuration s'est terminée avec succès.

Pour lier une stratégie de répondeur à un serveur virtuel spécifique à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sur la page **Serveurs virtuels d'équilibrage de charge**, sélectionnez le serveur virtuel auquel vous souhaitez lier la stratégie de répondeur, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le serveur virtuel** (équilibrage de charge), sélectionnez l'onglet **Politiques**, qui affiche la liste de toutes les politiques configurées sur votre appliance NetScaler.
4. Cochez la case en regard du nom de la stratégie que vous souhaitez lier à ce serveur virtuel.
5. Cliquez sur **OK**. Un message s'affiche dans la barre d'état, indiquant que la configuration s'est terminée avec succès.

Définition de l'action par défaut pour une stratégie de répondeur

May 5, 2023

L'appliance NetScaler génère un événement non défini (événement UNDEF) lorsqu'une demande ne correspond pas à une politique de réponse. L'appliance exécute ensuite l'action par défaut attribuée aux événements non définis. Par défaut, l'action transmet la demande à la fonctionnalité suivante, telle que l'équilibrage de charge, le filtrage du contenu, etc. Ce comportement par défaut garantit que

les demandes ne nécessitent aucune action de réponse spécifique pour être envoyées à vos serveurs Web. Les clients ont également accès au contenu qu'ils ont demandé.

Toutefois, si un ou plusieurs sites Web protégés par votre appliance NetScaler reçoivent un nombre important de demandes non valides ou malveillantes, vous pouvez modifier l'action par défaut pour réinitialiser la connexion client ou supprimer la demande. Dans ce type de configuration, vous devez écrire une ou plusieurs politiques de réponse qui correspondent à toutes les demandes légitimes, et vous redirigerez simplement ces demandes vers leurs destinations d'origine. Votre appliance NetScaler bloquera alors toutes les autres demandes, comme spécifié par l'action par défaut que vous avez configurée.

Vous pouvez attribuer l'une des actions suivantes à un événement non défini :

- **NOOP.** L'action NOOP interrompt le traitement du répondeur mais ne modifie pas le flux de paquets. Ainsi, l'appliance continue à traiter les demandes qui ne correspondent à aucune politique de réponse et les transfère finalement vers l'URL demandée à moins qu'une autre fonctionnalité n'intervienne pour bloquer ou rediriger la demande. Cette action est appropriée pour les requêtes normales adressées à vos serveurs Web et constitue le paramètre par défaut.
- **RÉINITIALISER**. Si l'action non définie est définie sur RESET, l'appliance réinitialise la connexion client, informant le client qu'il doit rétablir sa session avec le serveur Web. Cette action est appropriée pour les demandes répétées concernant des pages Web qui n'existent pas ou pour les connexions qui peuvent être des tentatives de piratage ou d'exploration de vos sites Web protégés.
- **LAISSER TOMBER**. Si l'action non définie est définie sur DROP, l'appliance abandonne silencieusement la demande sans répondre au client de quelque manière que ce soit. Cette action est appropriée pour les demandes qui semblent faire partie d'une attaque DDoS ou d'une autre attaque soutenue sur vos serveurs.

Remarque : Les événements UNDEF sont déclenchés uniquement pour les demandes des clients. Aucun événement UNDEF n'est déclenché pour les réponses.

Pour définir l'action non définie à l'aide de la ligne de commande NetScaler :

À l'invite de commandes, tapez la commande suivante pour définir l'action non définie et vérifier la configuration :

- `set responder param -undefAction (RESET|DROP|NOOP)[-timeout <msecs>]`
- `show responder param`

Où,

timeout : durée maximale en millisecondes pour permettre le traitement de toutes les politiques et de leurs actions sélectionnées sans interruption. Si le délai d'attente est atteint, l'évaluation provoque le déclenchement d'un UNDEF et aucun autre traitement n'est effectué.

Valeur minimale : 1

Valeur maximale : 5000

Exemple :

```
>set responder param -undefAction RESET -timeout 3900
 Done
> show responder param
Action Name: RESET
Timeout: 3900
 Done
>
<!--NeedCopy-->
```

Définissez l'action non définie à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Répondeur**, puis sous **Paramètres**, cliquez sur le lien **Modifier les paramètres du répondeur** .
2. Sur la page **Définir les paramètres du répondeur**, définissez les paramètres suivants :
   a) Action globale dont le résultat n'est pas défini. Une action à résultat non défini est préférée en cas d'exception de traitement non gérée dans les politiques et actions du répondeur. Sélectionnez **NOOP**, **RESET**ou **DROP**.
   b) Délai d'expiration. Durée maximale en millisecondes pour permettre le traitement de toutes les politiques et de leurs actions sélectionnées sans interruption. Si le délai d'attente est atteint, l'évaluation provoque le déclenchement d'un UNDEF et aucun autre traitement n'est effectué.
3. Cliquez sur **OK**.



Exemples d'actions et de stratégies de répondeur

May 5, 2023

Les actions et les politiques des intervenants sont puissantes et complexes, mais vous pouvez démarrer avec des applications relativement simples.

Exemple : blocage de l'accès depuis des adresses IP spécifiées

Les procédures suivantes bloquent l'accès à vos sites Web protégés par les clients provenant du CIDR 222.222.0.0/16. Le répondeur envoie un message d'erreur indiquant que le client n'est pas autorisé à accéder à l'URL demandée.

Pour bloquer l'accès à l'aide de la ligne de commande NetScaler :

À l'invite de commandes, tapez les commandes suivantes pour bloquer l'accès :

- add responder action act_unauthorized respond with "HTTP/1.1 403 Forbidden\r\n\r\n" + "Client: " + CLIENT.IP.SRC + " is not authorized to access URL:" + "HTTP.REQ.URL.HTTP_URL_SAFE"'
- add responder policy pol_un "CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)" act_unauthorized
- bind responder global pol_un 10

Pour bloquer l'accès à l'aide de l'interface graphique :

1. Dans le volet de navigation, développez **Répondeur**, puis cliquez sur **Actions**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action de répondeur**, procédez comme suit :

a) Dans la zone **de texte Nom**, saisissez act_unauthorized.
b) Sous Type, sélectionnez Répondre par.
c) Dans la zone de texte Cible, tapez la chaîne suivante : “HTTP/1.1 403 Forbidden\r\n\r\n” + “Client: “ + CLIENT.IP.SRC + “ is not authorized to access URL:” + HTTP.REQ.URL.HTTP_URL_SAFE
d) Cliquez sur **Créer**, puis sur **Fermer**.
L’action du répondeur que vous avez configurée, nommée act_unauthorized, apparaît désormais dans la page **Actions du répondeur** .

4. Dans le volet de navigation, cliquez sur **Stratégies**.
5. Dans le volet de détails, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :
a) Dans la zone de texte Nom, saisissez pol_unauthorized.
b) Sous **Action**, sélectionnez act_unauthorized.
c) Dans la fenêtre **Expression**, tapez la règle suivante : CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)
d) Cliquez sur **Créer**, puis sur **Fermer**.
La stratégie de répondeur que vous avez configurée, nommée pol_unauthorized, apparaît désormais dans la page **Stratégies de répondeur** .
7. Liez globalement votre nouvelle stratégie, pol_unauthorized, comme décrit dans Liaison d’une stratégie de répondeur.

Exemple : Redirection d’un client vers une nouvelle URL

Les procédures suivantes redirigent les clients qui accèdent à votre (vos) site (s) Web protégé (s) à partir du CIDR 222.222.0.0/16 vers une URL spécifiée.

Pour rediriger les clients à l’aide de la ligne de commande NetScaler :

À l’invite de commandes, tapez les commandes suivantes pour rediriger les clients et vérifier la configuration :

- add responder action act_redirect redirect "<http://www.example.com/404.html>"
- show responder action act_redirect
- add responder policy pol_redirect “CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)” act_redirect
- show responder policy pol_redirect
- bind responder global pol_redirect 10

Exemple :

```
1 > add responder action act_redirect redirect `" http ://www.example.com
    /404.html "`
2 Done
3
```



```
> add responder policy pol_redirect "CLIENT.IP.SRC.IN_SUBNET
   (222.222.0.0/16)" act_redirect
Done
<!--NeedCopy-->
```

Pour rediriger les clients à l'aide de l'interface graphique :

1. **Accédez à**AppExpert**>**Responder > Actions**.**
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une action de répondeur**, procédez comme suit :
   a) Dans la zone **de texte Nom**, saisissez act_redirect.
   b) Sous Type, sélectionnez **Redirection**.
   c) Dans la zone de texte **Cible**, saisissez la chaîne suivante : `"<http://www.example.com/404.html>"`
   d) Cliquez sur **Créer**, puis sur **Fermer**.
   L'action du répondeur que vous avez configurée, nommée act_redirect, apparaît désormais dans la page **Actions du répondeur** .
4. Dans le volet de navigation, cliquez sur **Stratégies**.
5. Dans le volet de détails, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Créer une stratégie de répondeur**, procédez comme suit :
   a) Dans la zone **de texte Nom**, saisissez pol_redirect.
   b) Sous **Action**, sélectionnez act_redirect.
   c) Dans la fenêtre **Expression**, tapez la règle suivante : CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)
   d) Cliquez sur **Créer**, puis sur **Fermer**.
   La stratégie de répondeur que vous avez configurée, nommée pol_redirect, apparaît désormais dans la page **Stratégies de répondeur** .
7. Liez globalement votre nouvelle stratégie, pol_redirect, comme décrit dans Liaison d'une stratégie de répondeur.

Support de diamètre pour répondeur

May 5, 2023

La fonction Responder prend désormais en charge le protocole Diameter. Vous pouvez configurer Responder pour qu'il réponde aux demandes Diameter de la même manière qu'il répond aux requêtes HTTP et TCP. Par exemple, vous pouvez configurer Responder pour qu'il réponde aux demandes provenant d'une source Diameter spécifique avec une redirection vers une page Web optimisée pour les appareils mobiles. Un certain nombre d'expressions NetScaler ont été ajoutées pour prendre en charge l'examen de l'en-tête Diameter et des paires attribut-valeur (AVP). Ces expressions permettent

de rechercher des AVP spécifiques par index, ID ou nom, d'examiner les informations de chaque AVP et d'envoyer une réponse appropriée.

Pour configurer Responder afin qu'il réponde à une demande Diameter :

À l'invite de commandes, tapez les commandes suivantes :

- `add responder action <actname> RESPONDWITH "DIAMETER.NEW_REDIRECT(\"aaa://host.example.com\")"`

  Pour <actname>, remplacez votre nouvelle action par un nom. Le nom peut comporter de 1 à 127 caractères et peut contenir des lettres, des chiffres ainsi que les symboles de tiret (-) et de trait de soulignement (_). Remplacez par l'URL de l'hôte diameter vers lequel vous souhaitez rediriger les connexions. `aaa://host.example.com`

- ajouter une politique de répondeur <polname> « diameter.req.avp (264) .value.eq (« host1.example.net ») » <actname>

  Par <polname>, remplacez votre nouvelle politique par un nom. Comme c'est le cas <actname>, le nom peut comporter de 1 à 127 caractères et peut contenir des lettres, des chiffres ainsi que les symboles de tiret (-) et de trait de soulignement (_). Pour host1.example.net, remplacez le nom de l'hôte d'origine des requêtes que vous souhaitez rediriger. Remplacez par le nom de l'action que vous venez de créer. <actname>

- `bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST`

  Par <vservername>, remplacez le nom du serveur virtuel d'équilibrage de charge auquel vous souhaitez lier la politique. Remplacez par le nom de la politique que vous venez de créer. <polname> Par <priority>, remplacez la politique par une priorité.

Exemple :

Pour créer une action et une politique Responder afin de répondre aux demandes Diameter provenant de « host1.example.net » avec une redirection vers « host.example.com », vous pouvez ajouter l'action et la politique suivantes, puis lier la politique comme indiqué.

```
1 > add responder action act_resp-dm-redirect RESPONDWITH "DIAMETER.
     NEW_REDIRECT("aaa://host.example.com")"
2 Done
3
4 > add responder pol_resp-dm-redirect "diameter.req.avp(264).value.eq("
     host1.example.net")" act_resp-dm-redirect
5 Done
6
7 > bind lb vserver vs1 -policyName pol_resp-dm-redirect -priority 10 -
     type REQUEST
8 Done
```



```
<!--NeedCopy-->
```

Prise en charge de RADIUS pour Responder

May 5, 2023

Le langage d'expressions NetScaler contient des expressions permettant d'extraire des informations à partir de requêtes RADIUS et de les manipuler. Ces expressions vous permettent d'utiliser la fonctionnalité Répondeur pour répondre aux demandes RADIUS. Les politiques et actions de votre répondeur peuvent utiliser n'importe quelle expression appropriée ou pertinente pour une demande RADIUS. Les expressions disponibles vous permettent d'identifier le type de message RADIUS, d'extraire toute paire attribut-valeur (AVP) de la connexion et d'envoyer différentes réponses sur la base de ces informations. Vous pouvez également créer des étiquettes de politique qui invoquent toutes les politiques de répondeur pour les connexions RADIUS.

Vous pouvez utiliser des expressions RADIUS pour créer des réponses simples qui ne nécessitent pas de communication avec le serveur RADIUS auquel la demande a été envoyée. Lorsqu'une politique de répondeur correspond à une connexion, NetScaler construit et envoie la réponse RADIUS appropriée sans contacter le serveur d'authentification RADIUS. Par exemple, si l'adresse IP source d'une demande RADIUS provient d'un sous-réseau spécifié dans la politique de réponse, NetScaler peut répondre à cette demande par un message de rejet d'accès ou peut simplement supprimer la demande.

Vous pouvez également créer des étiquettes de politique pour acheminer des types spécifiques de demandes RADIUS par le biais d'une série de politiques adaptées à ces demandes.

Remarque : Les expressions RADIUS actuelles ne fonctionnent pas avec les attributs IPv6 de RADIUS.

La documentation de NetScaler relative aux expressions qui prennent en charge RADIUS suppose une connaissance de la structure et de l'objectif de base des communications RADIUS. Si vous avez besoin de plus amples informations sur RADIUS, consultez la documentation de votre serveur RADIUS ou recherchez en ligne une introduction au protocole RADIUS.

Configuration des politiques de répondeur pour RADIUS

La procédure suivante utilise la ligne de commande NetScaler pour configurer une action et une politique de répondeur, et lier la politique à un point de liaison global spécifique à RADIUS.

Pour configurer une action et une politique de répondeur, et lier la politique, procédez comme suit :

À l'invite de commandes, tapez les commandes suivantes :

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`

- `bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>` où `<bindPoint>` représente l'un des points de liaison globaux spécifiques à RADIUS.

Expressions RADIUS pour Responder

Dans une configuration de répondeur, vous pouvez utiliser les expressions NetScaler suivantes pour faire référence à différentes parties d'une demande RADIUS.

Identification du type de connexion :

- RADIUS.IS_CLIENT. Renvoie TRUE si la connexion est un message client RADIUS (demande).
- RADIUS.IS_SERVER. Renvoie TRUE si la connexion est un message de serveur RADIUS (réponse).

Expressions de demande :

- `RADIUS.REQ.CODE`. Renvoie le numéro qui correspond au type de demande RADIUS. Un dérivé de la classe num_at. Par exemple, une demande d'accès RADIUS renverrait 1 (un). Une demande de comptabilité RADIUS renverrait 4.
- `RADIUS.REQ.LENGTH`. Renvoie la longueur de la requête RADIUS, y compris l'en-tête. Un dérivé de la classe num_at.
- `RADIUS.REQ.IDENTIFIER`. Renvoie l'identifiant de demande RADIUS, un numéro attribué à chaque demande qui permet de faire correspondre la demande à la réponse correspondante. Un dérivé de la classe num_at.
- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`. Renvoie la valeur de la première occurrence de cet AVP sous la forme d'une chaîne de type text_t.
- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`. Renvoie l'instance spécifiée de l'AVP sous la forme d'une chaîne de type RAVP_t. Un AVP RADIUS spécifique peut apparaître plusieurs fois dans un message RADIUS. INSTANCE (0) renvoie la première instance, INSTANCE (1) renvoie la deuxième instance, et ainsi de suite, jusqu'à seize instances.
- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`. Renvoie la valeur de l'instance spécifiée de l'AVP sous forme de chaîne de type text_t.
- `RADIUS.REQ.AVP(<AVP code no>).COUNT`. Renvoie le nombre d'instances d'un AVP spécifique dans une connexion RADIUS, sous forme d'entier.
- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`. Renvoie TRUE si le type d'AVP spécifié existe dans le message, ou FALSE dans le cas contraire.

Expressions de réponse :

Les expressions de réponse RADIUS sont identiques aux expressions de demande RADIUS, sauf que RES remplace REQ.

Types de valeurs AVP :

L'ADC prend en charge les expressions permettant de convertir les valeurs RADIUS AVP sous forme de texte, d'entier, d'entier non signé, de type long, de type long non signé, d'adresse ipv4, d'adresse

ipv6, de préfixe ipv6 et de types de données temporelles. La syntaxe est la même que pour les autres expressions NetScaler typecast.

Exemple :

L'ADC prend en charge les expressions permettant de convertir les valeurs RADIUS AVP sous forme de texte, d'entier, d'entier non signé, de type long, de type long non signé, d'adresse ipv4, d'adresse ipv6, de préfixe ipv6 et de types de données temporelles. La syntaxe est la même que pour les autres expressions NetScaler typecast.

```
RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
<!--NeedCopy-->
```

Expressions de type AVP :

NetScaler prend en charge les expressions permettant d'extraire les valeurs RADIUS AVP à l'aide des codes entiers assignés décrits dans les RFC2865 et RFC2866. Vous pouvez également utiliser des alias de texte pour effectuer la même tâche. Voici quelques exemples.

- RADIUS.REQ.AVP (1) .VALUE ou RADIUS.req.UserName.Value. Extrait la valeur du nom d'utilisateur RADIUS.
- RADIUS.REQ.AVP (4). VALUE ou RADIUS.REQ. ACCT_SESSION_ID.VALEUR. Extrait le Acct-Session-ID AVP (code 44) du message.
- RADIUS.REQ.AVP (26). VALUE ou RADIUS.REQ.VENDOR_SPECIFIC.VALUE. Extrait la valeur spécifique au fournisseur.

Les valeurs des AVP RADIUS les plus couramment utilisées peuvent être extraites de la même manière.

Points de liaison RADIUS :

Quatre points de liaison globaux sont disponibles pour les politiques contenant des expressions RADIUS.

- RADIUS_REQ_OVERRIDE. File d'attente des politiques relatives aux demandes de priorité/de dérogation.
- RADIUS_REQ_DEFAULT. File d'attente de règles de demande standard.
- RADIUS_RES_OVERRIDE. File d'attente des politiques de priorité/d'annulation des réponses.
- RADIUS_RES_DEFAULT. File d'attente de politiques de réponse standard.

Expressions spécifiques au répondeur RADIUS :

- RADIUS_RESPONDWITH. Répondez avec la réponse RADIUS spécifiée. La réponse est créée à l'aide d'expressions NetScaler, à la fois des expressions RADIUS et toute autre expression applicable.
- RADIUS.NEW_ANSWER. Envoie une nouvelle réponse RADIUS à l'utilisateur.
- RADIUS.NEW_ACCESSREJECT. Rejette la demande RADIUS.
- RADIUS.NEW_AVP. Ajoute le nouvel AVP spécifié à la réponse.

Cas d'utilisation

Vous trouverez ci-dessous des cas d'utilisation de RADIUS avec répondeur.

Blocage des requêtes RADIUS provenant d'un réseau spécifique

Pour configurer la fonction de répondeur afin de bloquer les demandes d'authentification provenant d'un réseau spécifique, commencez par créer une action de répondeur qui rejette les demandes. Utilisez cette action dans une politique qui sélectionne les demandes provenant des réseaux que vous souhaitez bloquer. Liez la politique du répondeur à un point de liaison global spécifique à RADIUS, en spécifiant :

- La priorité
- END comme valeur NextExr, pour garantir que l'évaluation de la politique s'arrête lorsque cette politique correspond
- RADIUS_REQ_OVERRIDE comme file d'attente à laquelle vous attribuez la politique, afin qu'elle soit évaluée avant que les politiques ne soient attribuées à la file d'attente par défaut

Pour configurer Responder afin de bloquer les connexions à partir d'un réseau spécifique**

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`
- `bind responder global <polName> <priority> <nextExpr> -type <bindPoint>`

Exemple :

```
1 > add responder action rspActRadiusReject respondwith radius.
     new_accessreject
2 Done
3
4 > add responder policy rspPolRadiusReject client.ip.src.in_subnet
     (10.224.85.0/24) rspActRadiusReject
5 Done
6
7 > bind responder global rspPolRadiusReject 1 END -type
     RADIUS_REQ_OVERRIDE
8 <!--NeedCopy-->
```

Prise en charge DNS de la fonction Responder

May 5, 2023

Vous pouvez configurer la fonction de répondeur pour qu'elle réponde aux requêtes DNS de la même manière qu'aux requêtes HTTP et TCP. Par exemple, vous pouvez le configurer pour envoyer des réponses DNS via UDP et vous assurer que les demandes DNS du client sont envoyées via TCP. Un certain nombre d'expressions NetScaler prennent en charge l'examen de l'en-tête DNS de la requête. Ces expressions examinent des champs d'en-tête spécifiques et envoient une réponse appropriée.

- **Expressions DNS**. Dans la configuration d'un répondeur, vous pouvez utiliser les expressions NetScaler suivantes pour faire référence à différentes parties d'une requête DNS :

Expressions	Description
DNS.NEW_RESPONSE	Crée une nouvelle réponse DNS vide en fonction de la demande.
DNS.NEW_RESPONSE <AA, TC, rcode>	Crée une nouvelle réponse DNS en fonction des paramètres spécifiés.

- Points de**liaison DNS**. Les points de liaison globaux suivants sont disponibles pour les politiques qui contiennent des expressions DNS.

Points de liaison	Description
DNS_REQ_OVERRIDE	File d'attente des politiques relatives aux demandes de priorité/de dérogation.
DNS_REQ_DEFAULT	File d'attente de règles de demande standard.

Outre les points de liaison par défaut, vous pouvez créer des étiquettes de politique de type DNS et y lier des politiques DNS.

Configuration des politiques de répondeur pour le DNS

La procédure suivante utilise la ligne de commande NetScaler pour configurer une action et une politique du répondeur et lier la politique à un point de liaison global spécifique au répondeur.

Pour configurer Responder afin qu'il réponde à une demande DNS :

À l'invite de commandes, tapez les commandes suivantes :

1. `add responder action <actName> <actType>`

   Pour <actname>, remplacez votre nouvelle action par un nom. Le nom peut comporter entre 1 et 127 caractères et peut contenir des lettres, des chiffres, des traits d'union (-) et des traits de soulignement (_). Remplacez par un type d'action de répondeur, *RespondWith*. <actType>

2. `add responder policy <polName> <rule> <actName>`

   Par `<polname>`, remplacez votre nouvelle politique par un nom. Car `<actname>`, le nom peut comporter entre 1 et 127 caractères et peut contenir des lettres, des chiffres, des traits d'union (-) et des traits de soulignement (_). Remplacez par le nom de l'action que vous venez de créer. `<actname>`

3. `bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>`

   Pour `<bindPoint>`, spécifiez l'un des points de liaison globaux spécifiques au répondeur. Remplacez par le nom de la politique que vous venez de créer. `<polName>` Pour `<priority>`, spécifiez la priorité de la politique.

Exemple de configuration : appliquez toutes les requêtes DNS via TCP :

Pour appliquer toutes les requêtes DNS sur TCP, créez une action de répondeur qui définira le bit TC et rcode comme NOERROR.

```
1 > add responder action resp_act_set_tc_bit respondwith DNS.NEW_RESPONSE
     (true, true, NOERROR)
2 Done
3
4 > add responder policy enforce_tcp  dns.REQ.TRANSPORT.EQ(udp)
     resp_act_set_tc_bit
5 Done
6
7 >bind lb vserver dns_udp  - policyName  enforce_tcp   -type request  -
     priority 100
8 Done
9 <!--NeedCopy-->
```

Prise en charge de MQTT pour répondeur

May 5, 2023

La fonction Responder prend en charge le protocole MQTT. Vous pouvez configurer les politiques du répondeur pour effectuer une action en fonction des paramètres du message MQTT entrant.

L'action répond par l'un des éléments suivants à une nouvelle connexion :

- ABANDONNER
- RÉINITIALISER
- NOOP
- Une action du répondeur pour initier une nouvelle réponse MQTT CONNACK.

Configuration des politiques de répondeur pour MQTT

Après avoir activé la fonctionnalité de répondeur, vous devez configurer une ou plusieurs actions pour gérer les requêtes MQTT. Configurez ensuite une politique de réponse. Vous pouvez lier les politiques du répondeur de manière globale ou à un serveur virtuel d'équilibrage de charge ou à un serveur virtuel de commutation de contenu spécifique.

Les points de liaison suivants sont disponibles pour lier les politiques du répondeur de manière globale :

- MQTT_REQ_DEFAULT
- MQTT_REQ_OVERRIDE
- MQTT_JUMBO_REQ_DEFAULT
- MQTT_JUMBO_REQ_OVERRIDE

Les points de liaison suivants sont disponibles pour lier les politiques du répondeur à un serveur virtuel de commutation de contenu ou d'équilibrage de charge :

- REQUEST
- MQTT_JUMBO_REQ (ce point de liaison est utilisé uniquement pour les paquets Jumbo)

Pour configurer le répondeur afin qu'il réponde à une demande MQTT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

Configurez une action de répondeur.

```
add responder action <actName> <actType>
<!--NeedCopy-->
```

- Pour `actname`, remplacez votre nouvelle action par un nom. Le nom peut comporter entre 1 et 127 caractères et peut contenir des lettres, des chiffres, des traits d'union (-) et des traits de soulignement (_).
- Remplacez `actType`le type d'action du répondeur par respondwith.

Exemple :

```
add responder action mqtt_connack_unsup_ver respondwith MQTT.
   NEW_CONNACK(132)
<!--NeedCopy-->
```

Configurez une politique de réponse. L'appliance NetScaler répond aux demandes MQTT sélectionnées par cette politique de réponse.

```
add responder policy <polName> <rule> <actname>
```



```
<!--NeedCopy-->
```

- Par `polname`, remplacez votre nouvelle politique par un nom.
- Remplacez par le nom de l'action que vous avez créée. `actname`

Exemple :

```
add responder policy reject_lower_version "MQTT.HEADER.COMMAND.EQ(
    CONNECT) && MQTT.VERSION.LT(3)" mqtt_connack_unsup_ver
<!--NeedCopy-->
```

Liez la politique du répondeur à un serveur virtuel d'équilibrage de charge ou à un serveur virtuel de commutation de contenu spécifique. La politique s'applique uniquement aux requêtes MQTT dont l'adresse IP de destination est le VIP de ce serveur virtuel.

```
bind lb vserver <name> -policyName <policy_name> -priority <priority>

bind cs vserver <name> -policyName <policy_name> -priority <priority>
<!--NeedCopy-->
```

- Remplacez par le nom de la politique que vous avez créée. `policy_name`
- Pour `priority`, spécifiez la priorité de la politique.

Exemple :

```
bind lb vserver lb1 -policyName reject_lower_version -priority 50

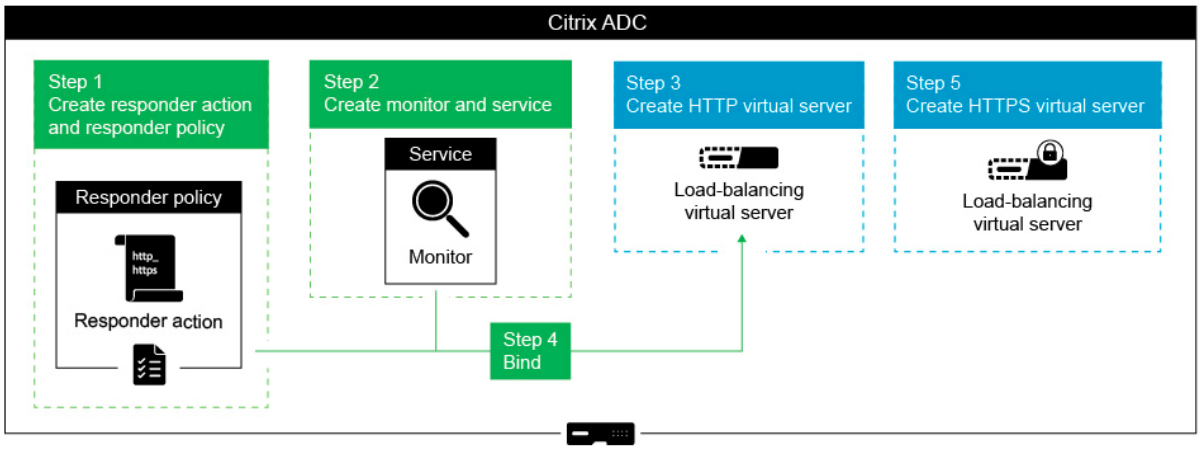
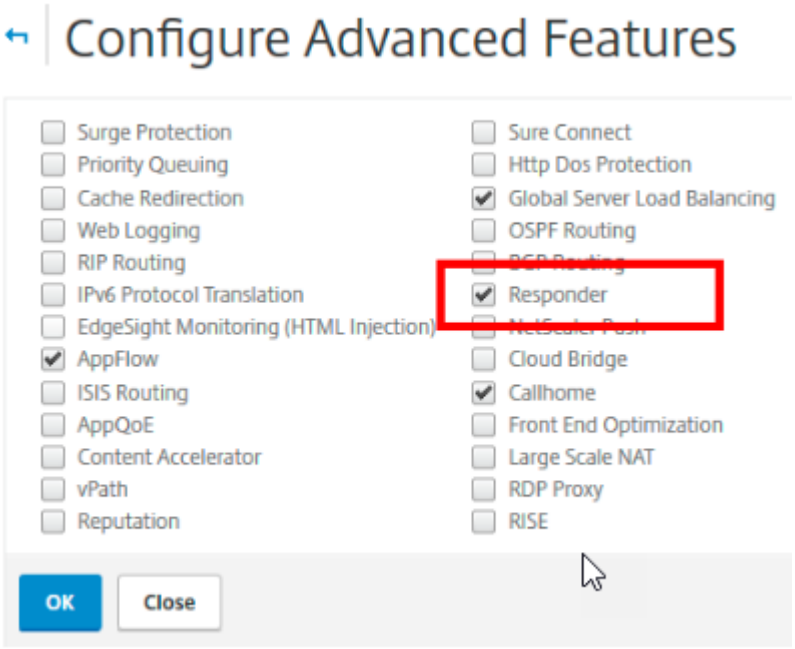
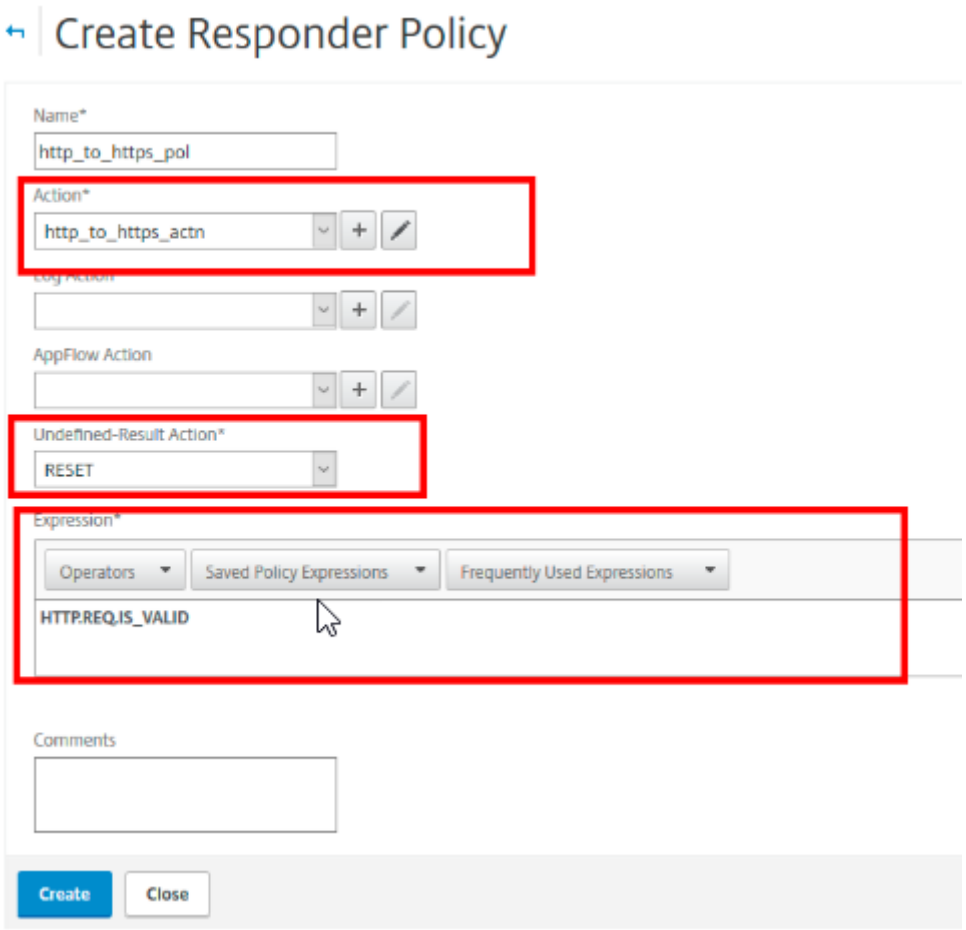
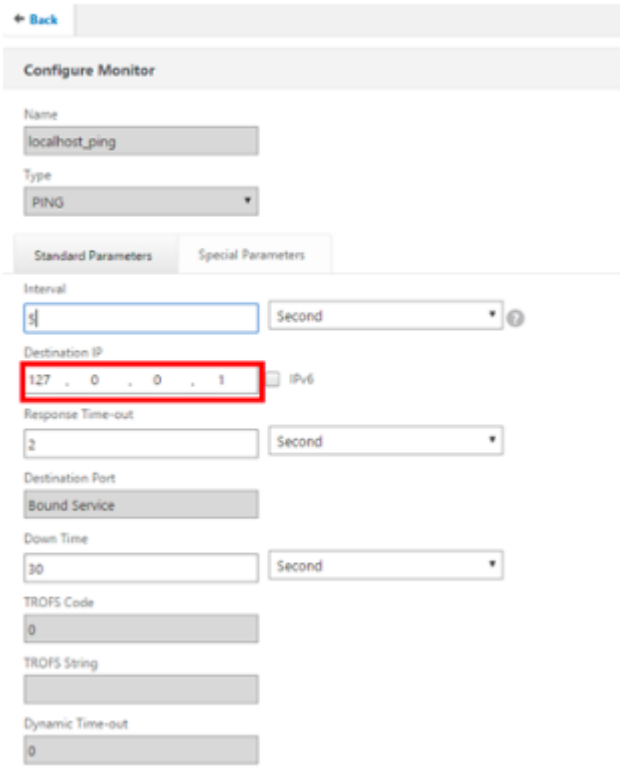
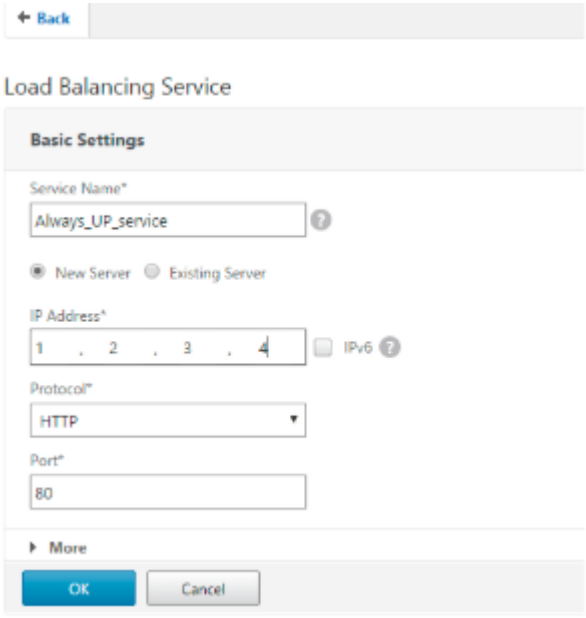
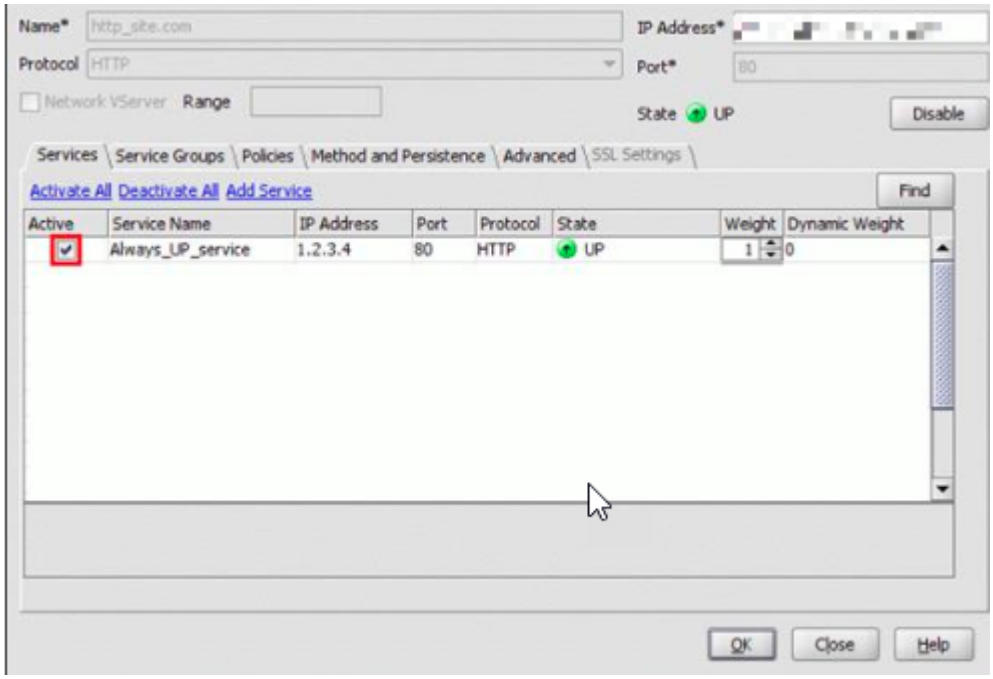
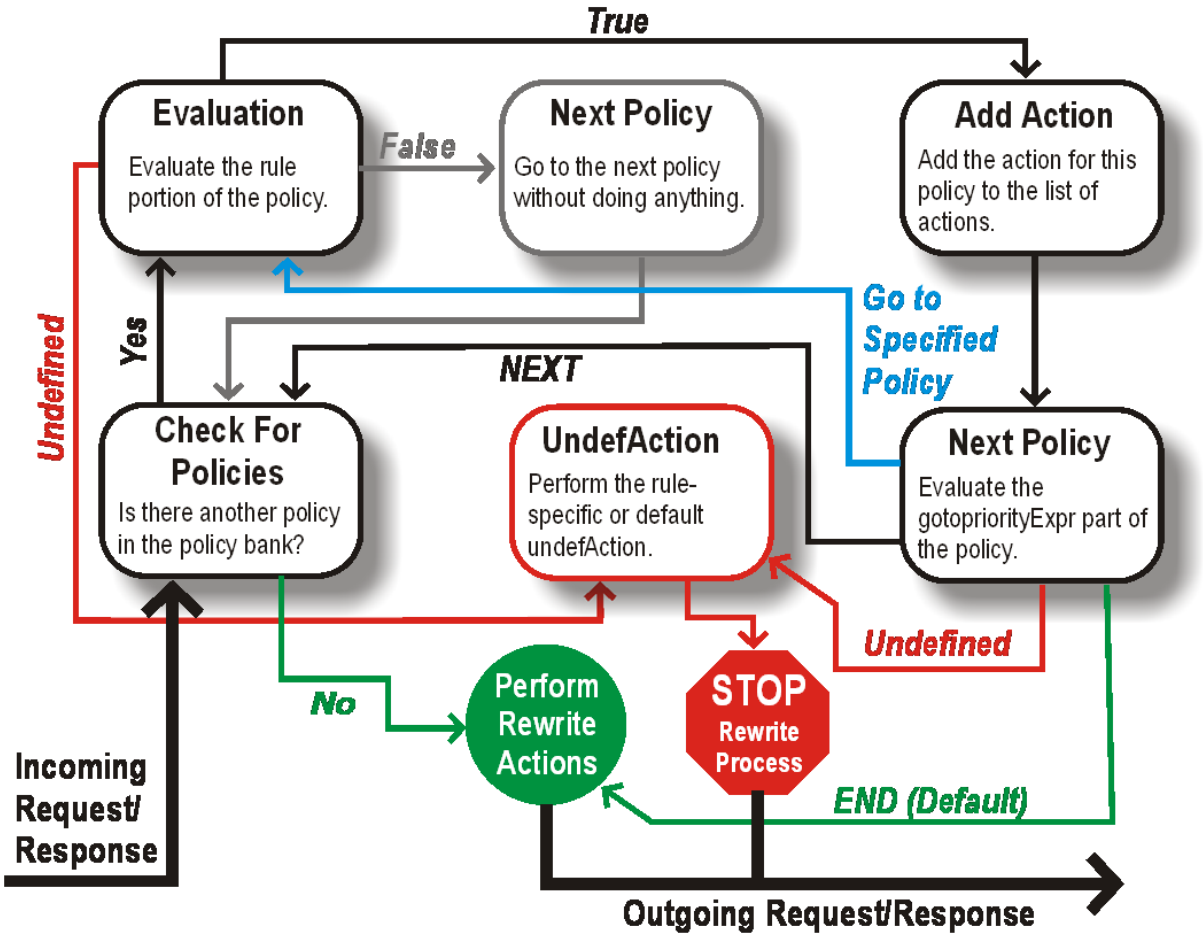
bind cs vserver mqtt_frontend_cs -policyName reject_lower_version -
    priority 5
<!--NeedCopy-->
```

Cas d'utilisation 1 : Filtrer les clients en fonction du nom d'utilisateur ou de l'ID client

L'administrateur peut configurer une politique de répondeur MQTT pour rejeter la connexion en fonction du nom d'utilisateur ou de l'ID client figurant dans le message MQTT CONNECT.

Exemple de configuration pour filtrer les clients en fonction de l'ID client

```
add policy patset filter_clients
bind policy patset filter_clients client1

add responder action mqtt_connack_invalid_client respondwith MQTT.
    NEW_CONNACK(2)

```



```
add responder policy reject_clients "MQTT.HEADER.COMMAND.EQ(CONNECT) &&
     mqtt.connect.clientid.equals_any("filter_clients")"
    mqtt_connack_invalid_client

bind cs vserver mqtt_frontend_cs -policyName reject_clients -priority 5
<!--NeedCopy-->
```

Cas d'utilisation 2 : Limiter la longueur maximale des messages MQTT pour gérer les paquets Jumbo

L'administrateur peut configurer une politique de réponse MQTT pour interrompre la connexion client si la longueur du message dépasse un certain seuil, ou prendre les mesures nécessaires en fonction des besoins.

Pour gérer les paquets Jumbo, les politiques du répondeur présentant l'un des modèles de règles suivants sont liées au point de liaison Jumbo :

- MQTT.MESSAGE_LENGTH
- MQTT.COMMAND
- MQTT.FROM_CLIENT
- MQTT.FROM_SERVER

Les politiques liées aux points de liaison Jumbo sont évaluées uniquement pour les paquets Jumbo.

Exemple de configuration pour limiter la longueur maximale des messages MQTT

```
set lb parameter -dropmqttjumbomessage no

add responder policy drop_large_message MQTT.MESSAGE_LENGTH.GT(100000)
    reset

bind cs vserver mqtt_frontend_cs -policyName drop_large_message -
    priority 10
<!--NeedCopy-->
```

Dans cet exemple, le `dropmqttjumbomessage` paramètre est défini sur NON. Par conséquent, l'appliance ADC traite les messages dont la longueur est supérieure à 64 000 octets et inférieure à 1 000 000 octets. Les messages dont la longueur est supérieure à 1 000 000 octets sont réinitialisés.

Comment rediriger une requête HTTP vers HTTPS à l'aide d'un répondeur

May 5, 2023

Cet article explique comment configurer la fonctionnalité de répondeur avec un équilibrage de charge des adresses IP de serveur virtuel et rediriger les demandes des clients de HTTP vers HTTPS.

Imaginons un scénario dans lequel un utilisateur pourrait tenter d'accéder à un site Web sécurisé en envoyant une requête HTTP. Au lieu de supprimer la demande, vous pouvez la rediriger vers un site Web sécurisé. Vous pouvez utiliser la fonction de répondeur pour rediriger la demande vers le site Web sécurisé sans modifier le chemin et la requête URL auxquels l'utilisateur tente d'accéder.

Comment le répondeur NetScaler redirige une requête de HTTP vers HTTPS

L'illustration suivante montre étape par étape comment l'appliance redirige une demande.



> **Remarque** : Les chemins de navigation et les captures d'écran sont dérivés de NetScaler 11.0.

Pour configurer la fonctionnalité Responder ainsi que les adresses VIP d'équilibrage de charge d'une appliance NetScaler afin de rediriger les demandes des clients de HTTP vers HTTPS, procédez comme suit.

1. Activez la fonction de répondeur sur l'appliance. Accédez à **Système** > **Paramètres** > **Configurer les fonctionnalités avancées** > **Répondeur.**



2. Créez une action de répondeur et spécifiez un nom approprié, tel que http_to_https_actn, dans le champ Nom.
3. **Pour créer une action de répondeur, dans le volet de navigation, ouvrez**AppExpert**>**Répondeur**, cliquez sur**Actions**, puis sur Ajouter.**
4. Sélectionnez Rediriger comme type.
5. Dans le champ **Expression**, saisissez l'expression suivante :

   ```
   "https://"+ HTTP.REQ.HOSTNAME.HTTP_URL_SAFE + HTTP.REQ.URL.PATH_AND_QUERY
   .HTTP_URL_SAFE.
   ```

6. Dans les versions 9.0 et 10.0 de NetScaler, assurez-vous que l'option **Contourner le contrôle de sécurité** est désactivée.

   Remarque : Cette option n'est pas présente à partir de NetScaler 11.0.
7. Créez une **politique de réponse** et spécifiez un nom approprié, tel que http_to_https_pol, dans le champ Nom.
8. **Pour créer une politique de répondeur, dans le volet de navigation, ouvrez**AppExpert**>**Répondeur**, cliquez sur**Politiques**, puis sur Ajouter.**
9. Dans la liste des actions, sélectionnez le nom de l'action que vous avez créée.
10. Dans la liste des actions non définies, sélectionnez RÉINITIALISER.
11. Tapez l'expression **HTTP.REQ.IS_VALID** dans le champ **Expression** comme indiqué dans la capture d'écran suivante.



1. Créez un moniteur dont l'état est toujours marqué comme UP et spécifiez un nom approprié, tel que localhost_ping, dans le champ Nom.
2. Pour créer un moniteur, dans le volet de navigation, ouvrez **Load Balancing**, cliquez sur **Moniteurs**, puis sur **Ajouter**.
3. Dans le champ **IP de destination**, spécifiez l'adresse IP 127.0.0.1, comme indiqué dans la capture d'écran suivante.



4. **Créez un service et spécifiez un nom approprié, tel que Always_up_Service, dans le champ Nom.**
5. Pour créer un service, dans le volet de navigation, développez **Load Balancing**, cliquez sur **Services**, puis sur **Ajouter**.
6. Spécifiez une adresse IP inexistante dans le champ **Serveur** .



7. Spécifiez 80 dans le champ **Port** .
8. Ajoutez le moniteur créé à partir de la liste des **moniteurs disponibles** .
9. Créez un serveur virtuel d'équilibrage de charge et spécifiez un nom approprié dans le champ **Nom** .
10. Pour créer un serveur virtuel d'équilibrage de charge, dans le volet de navigation, développez **Équilibrage de charge**, cliquez sur **Services**, puis sur **Ajouter**.
11. Spécifiez l'adresse IP du site Web dans le champ Adresse IP.
12. Sélectionnez HTTP dans la liste des protocoles.
13. Tapez 80 dans le champ Port.
14. Sur NetScaler versions 9.0 et 10.0, sélectionnez l'option Active pour le service que vous avez créé dans l'onglet Services, comme illustré dans la capture d'écran suivante. Cette option est obsolète dans la version 11.0 de NetScaler.



15. Cliquez sur l'onglet **Stratégies**.
16. Liez la politique de répondeur que vous avez créée à l'adresse VIP d'équilibrage de charge HTTP du site Web.
17. Créez un serveur virtuel d'équilibrage de charge sécurisé dont l'adresse IP du site Web et le port sont 443.

Pour créer une configuration similaire à la procédure précédente à partir de l'interface de ligne de commande de l'appliance, exécutez les commandes suivantes :

```
1  enable ns feature responder
2  add responder action http_to_https_actn redirect ""https://" + http.req
       .hostname.HTTP_URL_SAFE + http.REQ.URL.PATH_AND_QUERY.HTTP_URL_SAFE"
3  add responder policy http_to_https_pol HTTP.REQ.IS_VALID
       http_to_https_actn RESET
4  add lb monitor localhost_ping PING -LRTM ENABLED -destIP 127.0.0.1
5  add service Always_UP_service 1.2.3.4 HTTP 80 -gslb NONE -maxClient 0 -
       maxReq 0 -cip ENABLED dummy -usip NO -sp OFF -cltTimeout 180 -
       svrTimeout 360 -CKA NO -TCPB NO -CMP YES
6  bind lb monitor localhost_ping Always_UP_service
7  add lb vserver http_site.com HTTP 10.217.96.238 80 -persistenceType
       COOKIEINSERT -timeout 0 -cltTimeout 180
8  bind lb vserver http_site.com Always_UP_service
9  bind lb vserver http_site.com -policyName http_to_https_pol -priority 1
        -gotoPriorityExpression END
10 <!--NeedCopy-->
```


Remarques :

- L'état du serveur virtuel de redirection d'équilibrage de charge du port 80 doit être ACTIF pour que la redirection fonctionne.
- Les navigateurs Web risquent de ne pas rediriger correctement si le serveur virtuel HTTPS n'est pas actif.
- Cette configuration de redirection permet de faire face aux situations dans lesquelles plusieurs domaines sont liés à la même adresse IP.
- Si le client envoie une requête HTTP non valide au serveur virtuel de redirection, l'appliance envoie un code de message RESET.

Dépannage

May 5, 2023

Si la fonctionnalité de répondeur ne fonctionne pas comme prévu une fois que vous l'avez configurée, vous pouvez utiliser certains outils courants pour accéder aux ressources NetScaler et diagnostiquer le problème.

Ressources pour la résolution des problèmes

Pour de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème de cache intégré sur une appliance NetScaler :

- Le fichier ns.conf
- Les fichiers de trace pertinents provenant du client et de l'appliance NetScaler

Outre les ressources ci-dessus, les outils suivants accélèrent le dépannage :

- Le iehttpheaders ou un utilitaire similaire
- L'application Wireshark personnalisée pour les fichiers de trace NetScaler

Résolution des problèmes liés au répondeur

- **Problème**

  La fonctionnalité Répondeur est configurée, mais l'action du répondeur ne fonctionne pas.

  Résolution

  - Vérifiez que la fonctionnalité est activée.
  - Vérifiez les compteurs de visites de l'une des politiques pour voir si les compteurs sont incrémentés.

- Vérifiez que les politiques et les actions sont correctement configurées.
- Vérifiez que les actions et les politiques sont liées de manière appropriée.
- Enregistrez les traces des paquets sur le client et sur l'appliance NetScaler, puis analysez-les pour obtenir des indications sur le problème.
- Enregistrez les traces des paquets IEHTTPHeaters sur le client et vérifiez les requêtes et les réponses HTTP pour obtenir des indications sur le problème.

- **Problème**

  Vous devez créer une page de maintenance.

  Résolution

1. Configurez les services et le serveur virtuel.
2. Configurez un serveur virtuel de sauvegarde auquel un service est lié. Cela garantit que l'état du site Web est toujours affiché comme UP.
3. Configurez le serveur virtuel principal pour utiliser le serveur virtuel de sauvegarde comme sauvegarde.
4. Créez une action de répondeur avec une cible appropriée. Voici un exemple à titre de référence :

   ```
   add responder action sorry_page respondwith q{ "HTTP/1.0 200 OK"+"\r\n\
   r\n"+ "<html><body>Sorry, this page is not available\</body>\</html>"+
   "\r\n"}
   ```

5. Créez une politique de réponse et liez-y l'action.
6. Liez la stratégie de répondeur au serveur virtuel de sauvegarde.

Réécriture

July 7, 2023

> **Avertissement :**
>
> Les fonctionnalités de filtrage utilisant des stratégies classiques sont obsolètes et Citrix vous recommande d'utiliser les fonctionnalités de réécriture et de répondeur avec une infrastructure de stratégie avancée.

La réécriture fait référence à la réécriture de certaines informations contenues dans les demandes ou les réponses gérées par l'appliance NetScaler. La réécriture peut aider à fournir l'accès au contenu demandé sans exposer des détails inutiles sur la configuration réelle du site Web. Voici quelques situations dans lesquelles la fonction de réécriture est utile :

- Pour améliorer la sécurité, NetScaler peut réécrire tous les `http://links` vers `https://` dans corps de la réponse.
- Dans le déploiement de déchargement SSL, les liens non sécurisés de la réponse doivent être convertis en liens sécurisés. À l'aide de l'option de réécriture, vous pouvez réécrire tous les `http://links` vers `https://` pour vous assurer que les réponses sortantes de NetScaler au client contiennent des liens sécurisés.
- Si un site Web doit afficher une page d'erreur, vous pouvez afficher une page d'erreur personnalisée au lieu de la page d'erreur 404 par défaut. Par exemple, si vous affichez la page d'accueil ou le plan du site Web au lieu d'une page d'erreur, le visiteur reste sur le site au lieu de s'éloigner du site Web.
- Si vous souhaitez lancer un nouveau site Web, mais utiliser l'ancienne URL, vous pouvez utiliser l'option Réécrire.
- Lorsqu'une rubrique d'un site comporte une URL compliquée, vous pouvez la réécrire avec une URL simple et facile à retenir (également appelée « URL cool »).
- Vous pouvez ajouter le nom de page par défaut à l'URL d'un site Web. Par exemple, si la page par défaut du site Web d'une entreprise est `http://www.abc.com/index.php`, lorsque l'utilisateur tape « abc.com » dans la barre d'adresse du navigateur, vous pouvez réécrire l'URL en « abc.com/index.php ».

Lorsque vous activez la fonctionnalité de réécriture, NetScaler peut modifier les en-têtes et le corps des requêtes et réponses HTTP.

Pour réécrire les requêtes et les réponses HTTP, vous pouvez utiliser des expressions de stratégie NetScaler sensibles aux protocoles dans les stratégies de réécriture que vous configurez. Les serveurs virtuels qui gèrent les demandes et réponses HTTP doivent être de type
HTTP ou
SSL. Dans le trafic HTTP, vous pouvez effectuer les actions suivantes :

- Modifier l'URL d'une demande
- Ajouter, modifier ou supprimer des en-têtes
- Ajoutez, remplacez ou supprimez une chaîne spécifique dans le corps ou les en-têtes.

Pour réécrire des charges utiles TCP, considérez la charge utile comme un flux brut d'octets. Chacun des serveurs virtuels qui gèrent les connexions TCP doit être de type TCP ou SSL_TCP. Le terme réécriture TCP est utilisé pour désigner la réécriture de charges utiles TCP qui ne sont pas des données HTTP. Dans le trafic TCP, vous pouvez ajouter, modifier ou supprimer n'importe quelle partie de la charge utile TCP.

Pour obtenir des exemples d'utilisation de la fonction de réécriture, consultez Exemples d'actions de réécriture et de stratégie.

Comparaison entre les options Réécriture et Répondeur

La principale différence entre la fonction de réécriture et la fonction répondeur est la suivante :

Le répondeur ne peut pas être utilisé pour les expressions de réponse ou basées sur le serveur. Le répondeur ne peut être utilisé que pour les scénarios suivants, en fonction des paramètres du client :

- Redirection d'une requête HTTP vers de nouveaux sites Web ou pages Web
- Répondre avec une réponse personnalisée
- Dépose ou réinitialisation d'une connexion au niveau de la demande

S'il existe une stratégie de répondeur, NetScaler examine la demande du client, prend des mesures conformément aux stratégies applicables, envoie la réponse au client et ferme la connexion avec le client.

S'il existe une stratégie de réécriture, NetScaler examine la demande du client ou la réponse du serveur, prend les mesures nécessaires conformément aux stratégies applicables et transmet le trafic au client ou au serveur.

En général, il est recommandé d'utiliser un répondeur si vous souhaitez que NetScaler réinitialise ou abandonne une connexion en fonction d'un client ou d'un paramètre basé sur une demande. Utilisez le répondeur pour rediriger le trafic ou répondez avec des messages personnalisés. Utilisez la réécriture pour manipuler les données des requêtes et réponses HTTP.

Comment fonctionne la réécriture

Une stratégie de réécriture consiste en une règle et une action. La règle détermine le trafic auquel la réécriture est appliquée et l'action détermine l'action à effectuer par NetScaler. Vous pouvez définir plusieurs stratégies de réécriture. Pour chaque stratégie, spécifiez le point de liaison et la priorité.

Un point de liaison fait référence à un point du flux de trafic auquel le NetScaler examine le trafic pour vérifier si une stratégie de réécriture peut lui être appliquée. Vous pouvez lier une stratégie à un serveur virtuel d'équilibrage de charge ou de commutation de contenu spécifique, ou définir la stratégie globale si vous souhaitez qu'elle soit appliquée à l'ensemble du trafic géré par NetScaler. Ces stratégies sont appelées stratégies globales.

Outre les stratégies définies par l'utilisateur, NetScaler possède certaines stratégies par défaut. Vous ne pouvez pas modifier ou supprimer une stratégie par défaut.

Pour évaluer les stratégies, NetScaler suit l'ordre suivant :

- Stratégies mondiales
- Stratégies liées à des serveurs virtuels spécifiques
- Stratégies par défaut

> **Remarque :**
>
> NetScaler ne peut appliquer une stratégie de réécriture que lorsqu'elle est liée à un point.

NetScaler implémente la fonctionnalité de réécriture selon les étapes suivantes :

- L'appliance NetScaler vérifie les stratégies globales, puis vérifie les stratégies aux points de liaison individuels.
- Si plusieurs stratégies sont liées à un point de liaison, NetScaler les évalue dans l'ordre de leur priorité. La stratégie ayant la priorité la plus élevée est évaluée en premier. Après avoir évalué chaque stratégie, si la stratégie est évaluée à TRUE, elle ajoute l'action associée à la stratégie à laquelle l'action associée est exécutée. Une correspondance se produit lorsque les caractéristiques spécifiées dans la règle de stratégie correspondent aux caractéristiques de la demande ou de la réponse en cours d'évaluation.
- Pour n'importe quelle stratégie, en plus de l'action, vous pouvez spécifier la stratégie qui doit être évaluée après l'évaluation de la stratégie actuelle. Cette stratégie est appelée « Aller à l'expression ». Pour n'importe quelle stratégie, si une stratégie Go to Expression (GoToPriorityExpr) est spécifiée, NetScaler évalue la stratégie Go to Expression. Il ne tient pas compte de la stratégie qui a la priorité la plus élevée.

  Vous pouvez spécifier la priorité de la stratégie pour indiquer la stratégie Atteindre l'expression. Vous ne pouvez pas utiliser le nom de la stratégie. Si vous souhaitez que NetScaler arrête d'évaluer d'autres stratégies après avoir évalué une stratégie particulière, vous pouvez définir l'expression Go to sur « END ».
- Une fois que toutes les stratégies ont été évaluées ou lorsque l'option Go to Expression est définie sur END, le NetScaler commence à exécuter les actions en fonction de la liste d'actions.

Pour plus d'informations sur la configuration des stratégies de réécriture, voir Configuration d'une stratégie de réécriture et sur la liaison des stratégies de réécriture, voir Liaison d'une stratégie de réécriture.

La figure suivante montre comment NetScaler traite une demande ou une réponse lorsque la fonctionnalité de réécriture est utilisée.

Figure 1. Le processus de réécriture



Évaluation des stratégies

La stratégie ayant la priorité la plus élevée est évaluée en premier. NetScaler n'arrête pas l'évaluation des stratégies de réécriture lorsqu'il trouve une correspondance. Il évalue toutes les stratégies de réécriture configurées sur NetScaler.

- Si une stratégie obtient la valeur TRUE, NetScaler suit la procédure ci-dessous :
  - Si l'option Go to Expression est définie sur END, NetScaler arrête d'évaluer toutes les autres stratégies et commence à effectuer la réécriture.
  - L'expression GoToPriorityExpression peut être définie sur « NEXT », « END », un nombre entier ou « INVOCATION_LIST ». La valeur détermine la stratégie avec la priorité suivante. Le tableau suivant montre l'action entreprise par NetScaler pour chaque valeur de l'expression.

Valeur de l'expression	Action
SUIVANT	La stratégie avec la priorité suivante est évaluée.
END	L'évaluation des stratégies s'arrête.
<an integer>	La stratégie avec une priorité spécifiée est évaluée.
INVOCATION_LIST	Goto NEXT ou END est appliqué en fonction du résultat de la liste d'appels.

- Si une stratégie donne la valeur FALSE, NetScaler poursuit l'évaluation dans l'ordre de priorité.
- Si une stratégie est évaluée comme NON DÉFINIE (ne peut pas être évaluée sur le trafic reçu en raison d'une erreur), NetScaler exécute l'action affectée à la condition UNDEFINED (appelée UNDEFaction) et arrête toute évaluation ultérieure des stratégies.

NetScaler ne commence la réécriture proprement dite qu'une fois l'évaluation terminée. Il fait référence à la liste des actions identifiées par les stratégies évaluées à TRUE et démarre la réécriture. Après avoir implémenté toutes les actions de la liste, NetScaler transfère le trafic selon les besoins.

> **Remarque :**
>
> Assurez-vous que les stratégies ne spécifient pas d'actions conflictuelles ou superposées sur la même partie de l'en-tête ou du corps HTTP, ou de la charge utile TCP. Lorsqu'un tel conflit se produit, NetScaler rencontre une situation indéfinie et abandonne la réécriture.

Actions de réécriture

Sur l'appliance NetScaler, spécifiez les actions à effectuer, telles que l'ajout, le remplacement ou la suppression de texte dans le corps, ou l'ajout, la modification ou la suppression d'en-têtes, ou toute modification de la charge utile TCP sous forme d'actions de réécriture. Pour plus d'informations sur les actions de réécriture, voir Configuration d'une action de réécriture.

Le tableau suivant décrit les étapes que NetScaler peut suivre lorsqu'une stratégie obtient la valeur TRUE.

Action	Résultat
Insérer	L'action de réécriture spécifiée pour la stratégie est exécutée.
NOREWRITE	La demande ou la réponse n'est pas réécrite. NetScaler transfère le trafic sans réécrire aucune partie du message.

Action	Résultat
RESET	La connexion est interrompue au niveau TCP.
ABANDONNER	Le message est supprimé.

> **Remarque** :
>
> Pour n'importe quelle stratégie, vous pouvez configurer la sous-action (action à effectuer lorsque la stratégie est évaluée à UNDEFINED) en tant que NOREWRITE, RESET ou DROP.

Pour utiliser la fonction de
réécriture, procédez comme suit :

- Activez la fonctionnalité sur NetScaler.
- Définissez les actions de réécriture.
- Définissez des stratégies de réécriture.
- Liez les stratégies à un point de liaison pour mettre en œuvre une stratégie.

Activer la réécriture

Activez la fonctionnalité de réécriture sur l'appliance NetScaler si vous souhaitez réécrire les demandes ou réponses HTTP ou TCP. Si la fonctionnalité est activée, NetScaler effectue une action de réécriture conformément aux stratégies spécifiées. Pour plus d'informations, voir Comment fonctionne la réécriture.

Pour activer la fonction de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la fonction de réécriture et vérifier la configuration :

- enable ns feature REWRITE
- show ns feature

Exemple :

```
> enable ns feature REWRITE
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 .
 .
```



```
11   .
12   1)     Rewrite                         REWRITE             ON
13   .
14   .
15   1)     NetScaler Push                  push                OFF
16   Done
17 <!--NeedCopy-->
```

Pour activer la fonction de réécriture à l'aide de l'interface graphique

1. Dans le volet de navigation, cliquez sur **Système**, puis sur **Paramètres**.
2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur **Configurer les fonctionnalités de base**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités de base**, activez la case à cocher Réécrire, puis cliquez sur **OK**.
4. Dans la boîte de dialogue **Activer/Désactiver les fonctionnalités**, cliquez sur **Oui**. Un message apparaît dans la barre d'état, indiquant que la fonctionnalité sélectionnée a été activée.

Configuration d'une action de réécriture

> **Avertissement**
>
> La fonction Pattern dans une action de réécriture est obsolète à partir de NetScaler 12.0 build 56.20 et, comme alternative, Citrix vous recommande d'utiliser le paramètre d'action de réécriture Search.

Une action de réécriture indique les modifications apportées à une demande ou à une réponse avant de l'envoyer à un serveur ou à un client.

Les expressions définissent les éléments suivants :

- Type d'action de réécriture.
- Emplacement de l'action de réécriture.
- Type de configuration de l'action de réécriture.

Par exemple, une action DELETE utilise uniquement une expression cible. Une action REMPLACER utilise une expression cible et une expression pour configurer le texte de remplacement.

Après avoir activé la fonction de réécriture, vous devez configurer une ou plusieurs actions, à moins qu'une action de réécriture intégrée ne soit suffisante. Toutes les actions intégrées ont des noms commençant par la chaîne ns_cvpn, suivie d'une chaîne de lettres et de caractères de soulignement. Les actions intégrées effectuent des tâches utiles et complexes telles que le décodage de parties d'une demande ou d'une réponse VPN sans client ou la modification de données JavaScript ou XML. Les actions intégrées peuvent être affichées, activées et désactivées, mais elles ne peuvent pas être modifiées ou supprimées.

> Remarque :
>
> Les types d'action qui peuvent être utilisés uniquement pour la réécriture HTTP sont identifiés dans la colonne **Type d'action de réécriture** .

Pour plus d'informations, consultez la section **Paramètre de type**.

Créer une action de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une action de réécriture et vérifier la configuration :

- `add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-search <expression>] [refineSearch <expression>] [-comment<string>]`
- `show rewrite action <name>`

Pour plus d'informations, consultez le tableau Types d'actions de réécriture et leurs arguments .

La fonction de réécriture comporte les actions intégrées suivantes :

- NoRewrite-envoie la demande ou la réponse à l'utilisateur sans la réécrire.
- RESET - Réinitialise la connexion et informe le navigateur de l'utilisateur, afin que l'utilisateur puisse renvoyer la demande.
- DROP - Permet de supprimer la connexion sans envoyer de réponse à l'utilisateur.

L'un des types de flux suivants est implicitement associé à chaque action :

- Demande - L'action s'applique à la demande.
- Réponse - L'action s'applique à la réponse.
- Neutre - L'action s'applique à la fois aux demandes et aux réponses.

Nom

Nom de l'action de réécriture définie par l'utilisateur. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), le hachage (#), l'espace (), à (@), égal (=), deux-points (:) et les caractères de soulignement. Peut être modifié après l'ajout de la stratégie de réécriture.

Paramètre de type

Le paramètre **Type** indique le type d'action de réécriture définie par l'utilisateur.

Voici les valeurs du paramètre **Type** :

- `REPLACE <target> <string_builder_expr>`. Remplace la chaîne cible par l'expression string-builder.

Exemple :

```
> add rewrite action replace_http_act replace http.res.body(100) '"new_replaced_data"'
Done
> sh rewrite action replace_http_act
Name: replace_http_act
Operation: replace
Target:http.res.body(100)
Value:"new_replaced_data"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `REPLACE_ALL <target> <string_builder_expr1> -(search)<s>` - Dans la demande ou la réponse spécifiée par `<target>`, remplace toutes les occurrences de la chaîne définie par `<pattern_to_search>` avec la chaîne définie par `<string_builder_expr>`. Vous pouvez utiliser l'option de recherche pour trouver les chaînes à remplacer.

Exemple :

```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 "www.abc.com"
Done
> bind policy patset pat_list_2 "www.def.com"
Done
> add rewrite action refineSearch_act_31 replace_all "HTTP.RES.BODY(100000)" ""https://""-search "patset("pat_list_2")" -refineSearch "EXTEND(7,0).REGEX_SELECT(re#http://#)"
Done

> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:"https://"
Search: patset("pat_list_2")
Hits: 0
```



```
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_HTTP_RES <string_builder_expr>. Remplace la réponse HTTP complète par la chaîne définie par l'expression string-builder.

Exemple :

```
> add rewrite action replace_http_res_act replace_http_res '"HTTP/1.1
   200 OK\r\n\r\nSending from ADC"'
 Done
> sh rewrite action replace_http_res_act
Name: replace_http_res_act
Operation: replace_http_res
Target:"HTTP/1.1 200 OK
Sending from ADC"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_SIP_RES <target>. Remplace la réponse SIP complète par la chaîne spécifiée par <target>.

Exemple :

```
> add rewrite action replace_sip_res_act replace_sip_res '"HTTP/1.1 200
    OK\r\n\r\nSending from ADC"'
Done
> sh rewrite action replace_sip_res_act
Name: replace_sip_res_act
Operation: replace_sip_res
Target:"HTTP/1.1 200 OK
Sending from ADC"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```


- INSERT_HTTP_HEADER <header_string> <contents_string_builder_expr>. Insère l'en-tête HTTP spécifié par header_string et le contenu de l'en-tête spécifié par contents_string_builder_expr.

Exemple :

```
> add rewrite action ins_cip_header insert_http_header "CIP" "CLIENT.IP.SRC"
Done
> sh rewrite action ins_cip_header
Name: ins_cip_header
Operation: insert_http_header
Target:CIP
Value:CLIENT.IP.SRC
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_HTTP_HEADER <target>. Supprime l'en-tête HTTP spécifié par <target>

Exemple :

```
> add rewrite action del_true_client_ip_header delete_http_header "True-Client-IP"
Done
> sh rewrite action del_true_client_ip_header
Name: del_true_client_ip_header
Operation: delete_http_header
Target:True-Client-IP
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CORRUPT_HTTP_HEADER <target>. Remplace le nom d'en-tête de toutes les occurrences de l'en-tête HTTP spécifié <target> par un nom corrompu, de sorte qu'il ne soit pas reconnu par le destinataire Exemple : MY_HEADER est remplacé par MHEY_ADER.

Exemple :


```
> add rewrite action corrupt_content_length_hdr corrupt_http_header "
    Content-Length"
Done
> sh rewrite action corrupt_content_length_hdr
Name: corrupt_content_length_hdr
Operation: corrupt_http_header
Target:Content-Length
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_BEFORE <string_builder_expr1> <string_builder_expr1>. Recherche la chaîne spécifiée dans <string_builder_expr1> et insère la chaîne <string_builder_expr2 > avant.

```
> add rewrite action insert_before_ex_act insert_before http.res.body
    (100) '"Add this string in the starting"'
Done
> sh rewrite action insert_before_ex_act
Name: insert_before_ex_act
Operation: insert_before
Target:http.res.body(100)
Value:"Add this string in the starting"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_BEFORE_ALL <target> <string_builder_expr1> -(search)<string_builder_expr2 >. Dans la demande ou la réponse spécifiée par <target>, localise toutes les occurrences de la chaîne spécifiée dans et insère la chaîne spécifiée dans avant celle-ci. Vous pouvez utiliser l'option de recherche pour trouver les chaînes.

Exemple :

```
> add policy patset pat
 Done
> bind policy patset pat abcd
 Done
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
```



```
      (10) 'target.prefix(10) + "refineSearch_testing"' -search patset("
      pat") -refineSearch extend(10,10)
 Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + "refineSearch_testing"
Search: patset("pat")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER <string_builder_expr1> <string_builder_expr2>. Insère la chaîne spécifiée par string_builder_expr2 après la chaîne string_builder_expr1.

Exemple :

```
> add rewrite action insert_after_act insert_after http.req.body(100) '
   "add this string after 100 bytes"'
Done
> sh rewrite action insert_after_act
Name: insert_after_act
Operation: insert_after
Target:http.req.body(100)
Value:"add this string after 100 bytes"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER_ALL <target> <string_builder_expr1> -(search)<string_builder_expr2>. Dans la demande ou la réponse spécifiée par <target>, localise toutes les occurrences de la chaîne spécifiée par <string_builder_expr2> et insère la chaîne spécifiée par <string_builder_expr1> après celle-ci. Vous pouvez utiliser la fonction de recherche pour trouver les chaînes.

Exemple :


```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
    (100) '"refineSearch_testing"' -search text("abc") -refineSearch
    extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:"refineSearch_testing"
Search: text("abc")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE <target>. Supprime la chaîne spécifiée par la cible.

Exemple :

```
> add rewrite action delete_ex_act delete http.req.header("HDR")
Done
> sh rewrite action delete_ex_act
Name: delete_ex_act
Operation: delete
Target:http.req.header("HDR")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_ALL <target> -(search)<string_builder_expr>. Dans la demande ou la réponse spécifiée par <target>, recherche et supprime toutes les occurrences de la chaîne spécifiée par <string_builder_expr>. Vous pouvez utiliser la fonction de recherche pour trouver les chaînes.

Exemple :

```
>add rewrite action refineSearch_act_4 delete_all "HTTP.RES.BODY(50000)
    " -search text("Windows Desktops") -refineSearch "EXTEND(40,40).
    REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s`\*`<\\/AppData>#)"
Done
```



```
> show REWRITE action refineSearch_act_4
Name: refineSearch_act_4
Operation: delete_all
Target:HTTP.RES.BODY(50000)
Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s
    `\*`</AppData>#)
Search: text("Windows Desktops")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_DIAMETER_HEADER_FIELD <target> <field value>. Dans la ou les réponses, modifiez le champ d'en-tête spécifié par <target>. Utilisez Diameter.req.flags.SET (<flag>) ou Diameter.req.flags.UNSET<flag> comme stringbuilderexpression pour définir ou annuler les indicateurs.

Exemple :

```
> add rewrite action replace_diameter_field_ex_act
    replace_diameter_header_field diameter.req.flags diameter.req.flags.
    set(PROXIABLE)
Done
> sh rewrite action replace_diameter_field_ex_act
Name: replace_diameter_field_ex_act
Operation: replace_diameter_header_field
Target:diameter.req.flags
Value:diameter.req.flags.set(PROXIABLE)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_DNS_HEADER_FIELD <target>. Dans la demande ou la réponse, modifie le champ d'en-tête spécifié par <target>.

Exemple :

```
> add rewrite action replace_dns_hdr_act replace_dns_header_field dns.
    req.header.flags.set(AA)
Done
```



```
> sh rewrite action replace_dns_hdr_act
Name: replace_dns_hdr_act
Operation: replace_dns_header_field
Target:dns.req.header.flags.set(AA)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `REPLACE_DNS_ANSWER_SECTION <target>`. Remplacez la section de réponse DNS dans la réponse. Cela s'applique uniquement aux enregistrements A et AAAA. Utilisez `DNS.NEW_RRSET_A` les `NS.NEW_RRSET_AAAA` expressions et pour configurer la nouvelle section de réponses.

Exemple :

```
> add rewrite action replace_dns_ans_act replace_dns_answer_section
   DNS.NEW_RRSET_A("1.1.1.1", 10)
Done
> sh rewrite action replace_dns_ans_act
Name: replace_dns_ans_act
Operation: replace_dns_answer_section
Target:DNS.NEW_RRSET_A("1.1.1.1", 10)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `CLIENTLESS_VPN_DECODE<target>`. Décode le modèle spécifié par la cible au format VPN sans client.

Exemple :

```
> add rewrite action cvpn_decode_act_1 clientless_vpn_decode http.req.
   body(100)
Done
> sh rewrite action cvpn_decode_act_1
Name: cvpn_decode_act_1
Operation: clientless_vpn_decode
Target:http.req.body(100)
Hits: 0
```



```
8  Undef Hits: 0
9  Action Reference Count: 0
10 Done
11
12 <!--NeedCopy-->
```

- CLIENTLESS_VPN_DECODE_ALL<target>-search<expression>. Décode TOUS les modèles spécifiés par le paramètre de recherche au format VPN sans client.

Exemple :

```
1  > add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
      -search text("abcd")
2  Done
3  > sh rewrite action act1
4  Name: act1
5  Operation: clientless_vpn_decode_all
6  Target:http.req.body(100)
7  Search: text("abcd")
8  Hits: 0
9  Undef Hits: 0
10 Action Reference Count: 0
11 Done
12
13 <!--NeedCopy-->
```

- CLIENTLESS_VPN_ENCODE<target>. Encode le modèle spécifié par la cible au format VPN sans client.

Exemple :

```
1  > add rewrite action cvpn_encode_act_1 clientless_vpn_encode http.req.
      body(100)
2  Done
3  > sh rewrite action cvpn_encode_act_1
4  Name: cvpn_encode_act_1
5  Operation: clientless_vpn_encode
6  Target:http.req.body(100)
7  Hits: 0
8  Undef Hits: 0
9  Action Reference Count: 0
10 Done
11
12 <!--NeedCopy-->
```


- CLIENTLESS_VPN_ENCODE_ALL<target>-search<expression>. Encode TOUS les paramètres de recherche spécifiés dans le format VPN sans client.

Exemple :

```
> add rewrite action act2 clientless_vpn_encode_all http.req.body(100)
   -search text("abcd")
Done
> sh rewrite action act2
Name: act1
Operation: clientless_vpn_encode_all
Target:http.req.body(100)
Search: text("abcd")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CORRUPT_SIP_HEADER<target>. Remplace le nom d'en-tête de toutes les occurrences de l'en-tête SIP spécifié par <target> par un nom corrompu, de sorte que le destinataire ne le reconnaisse pas.

Exemple :

```
> add rewrite action corrupt_sip_hdr_act corrupt_sip_header SIP_HDR
Done
> sh rewrite action corrupt_sip_hdr_act
Name: corrupt_sip_hdr_act
Operation: corrupt_sip_header
Target:SIP_HDR
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_SIP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Insère l'en-tête SIP spécifié par <header_string_builder_expr> et le contenu de l'en-tête spécifié par <contents_string_builder_expr>.

Exemple :


```
> add rewrite action insert_sip_hdr_act insert_sip_header SIP_HDR '"
    inserting_sip_header"'
 Done
>sh rewrite action insert_sip_hdr_act
Name: insert_sip_hdr_act
Operation: insert_sip_header
Target:SIP_HDR
Value:"inserting_sip_header"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_SIP_HEADER<target>. Supprime l'en-tête SIP spécifié par <target>

Exemple :

```
> add rewrite action delete_sip_hdr delete_sip_header  SIP_HDR
Done
> sh rewrite action delete_sip_hdr
Name: delete_sip_hdr
Operation: delete_sip_header
Target:SIP_HDR
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Paramètre Target

Le paramètre Target est une expression qui spécifie la partie de la demande ou de la réponse à réécrire.

StringBuilderExpr

StringBuilderExpr est une expression qui spécifie le contenu qui doit être inséré dans la demande ou la réponse à l'emplacement spécifié. Cette expression remplace une chaîne spécifiée.

Exemple 1. Insertion d'un en-tête HTTP avec l'adresse IP du client :

```
> add rewrite action insertact INSERT_HTTP_HEADER "client-IP" CLIENT.IP
    .SRC
```



```
Done
> show rewrite action insertact
Name: insertact
Operation: insert_http_header
Target:Client-IP
Value:CLIENT.IP.SRC
BypassSafetyCheck : NO
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Exemple 2. Remplacement des chaînes dans une charge utile TCP (réécriture TCP) :

```
> add rewrite action client_tcp_payload_replace_all REPLACE_ALL
  'client.tcp.payload(1000)' '"new-string"' -search text("old-string")
Done
> show rewrite action client_tcp_payload_replace_all
Name: client_tcp_payload_replace_all
Operation: replace_all
Target:client.tcp.payload(1000)
Value:"new-string"
Search: text("old-string")
BypassSafetyCheck : NO
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Rechercher une partie de la demande ou de la réponse à réécrire

La fonctionnalité de recherche permet de trouver toutes les instances du modèle requis dans la demande ou la réponse.

La fonctionnalité de recherche doit être utilisée dans les types d'action suivants :

- INSERT_BEFORE_ALL
- INSERT_AFTER_ALL
- REPLACE_ALL
- DELETE_ALL

- CLIENTLESS_VPN_ENCODE_ALL
- CLIENTLESS_VPN_DECODE_ALL

La fonctionnalité de recherche ne peut pas être utilisée avec les types d'action suivants :

- INSERT_HTTP_HEADER
- INSERT_BEFORE
- INSERT_AFTER
- REMPLACER
- SUPPRIMER
- DELETE_HTTP_HEADER
- CORRUPT_HTTP_HEADER
- REPLACE_HTTP_RES
- CLIENTLESS_VPN_ENCODE
- CLIENTLESS_VPN_DECODE
- INSERT_SIP_HEADER
- DELETE_SIP_HEADER
- CORRUPT_SIP_HEADER
- REPLACE_DIAMETER_HEADER_FIELD
- REPLACE_DNS_ANSWER_SECTION
- REPLACE_DNS_HEADER_FIELD
- REPLACE_SIP_RES

Les types de recherche suivants sont pris en charge :

- Texte - une chaîne littérale
  Exemple recherche de texte (« bonjour »)
- Expression régulière - modèle utilisé pour faire correspondre plusieurs chaînes dans la requête ou la réponse
  Exemple search regex (re~^bonjour*~)
- XPATH - Expression XPATH pour effectuer une recherche XML.
  Exemple search xpath (xp%/a/b%)
- JSON : expression XPATH permettant de rechercher JSON.
  Exemple search xpath_json (xp%/a/b%)
  HTML - Une expression XPATH pour rechercher du HTML
  Exemple search xpath_html (xp%/html/body%)
  Patset - Ceci recherche tous les motifs liés à l'entité patset.
  Exemple -search patset("patset1")
- Jeu de données - Cette option recherche tous les modèles liés à l'entité du jeu de données.
  Exemple : -search dataset("dataset1")
- AVP - Numéro AVP utilisé pour faire correspondre plusieurs AVP dans un message Diameter/Radius

Exemple ⊠search avp (999)

Affiner les résultats de la recherche

Vous pouvez utiliser la fonctionnalité Affiner la recherche pour spécifier les critères supplémentaires permettant d'affiner les résultats de la recherche. La fonctionnalité Affiner la recherche ne peut être utilisée que si la fonctionnalité de recherche est utilisée.
Le paramètre Affiner la recherche commence toujours par l'opération « extend (m, n) », où 'm' indique quelques octets à gauche du résultat de la recherche et 'n' indique plusieurs octets à droite du résultat de la recherche pour étendre la zone sélectionnée.

Si l'action de réécriture configurée est la suivante :

```
> add rewrite action test_refine_search replace_all http.res.body(10) '
    " testing_refine_search" ' -search text("abc") -refineSearch extend
    (1,1)
And the HTTP response body is abcxxxx456.

<!--NeedCopy-->
```

Ensuite, le paramètre de recherche trouve le motif « abc » et puisque le paramètre RefineSearch est également configuré pour vérifier un octet supplémentaire à gauche et un octet supplémentaire à droite du motif correspondant. Le texte remplacé qui en résulte est : abcx. Le résultat de cette action est donc `testing_refine_searchxxx456`.

Exemple 1 : Utilisation de la fonctionnalité Affiner la recherche dans le type d'action INSERT_BEFORE_ALL.

```
> add policy patset pat
Done
> bind policy patset pat abcd
Done
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
    (10) 'target.prefix(10) + "refineSearch_testing"' -search patset("
    pat") -refineSearch extend(10,10)
Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + "refineSearch_testing"
Search: patset("pat")
Hits: 0
Undef Hits: 0
```



```
Action Reference Count: 0
Done

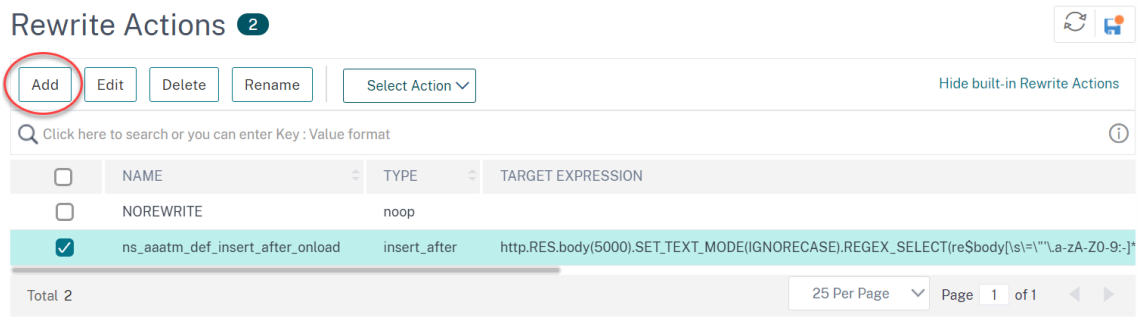
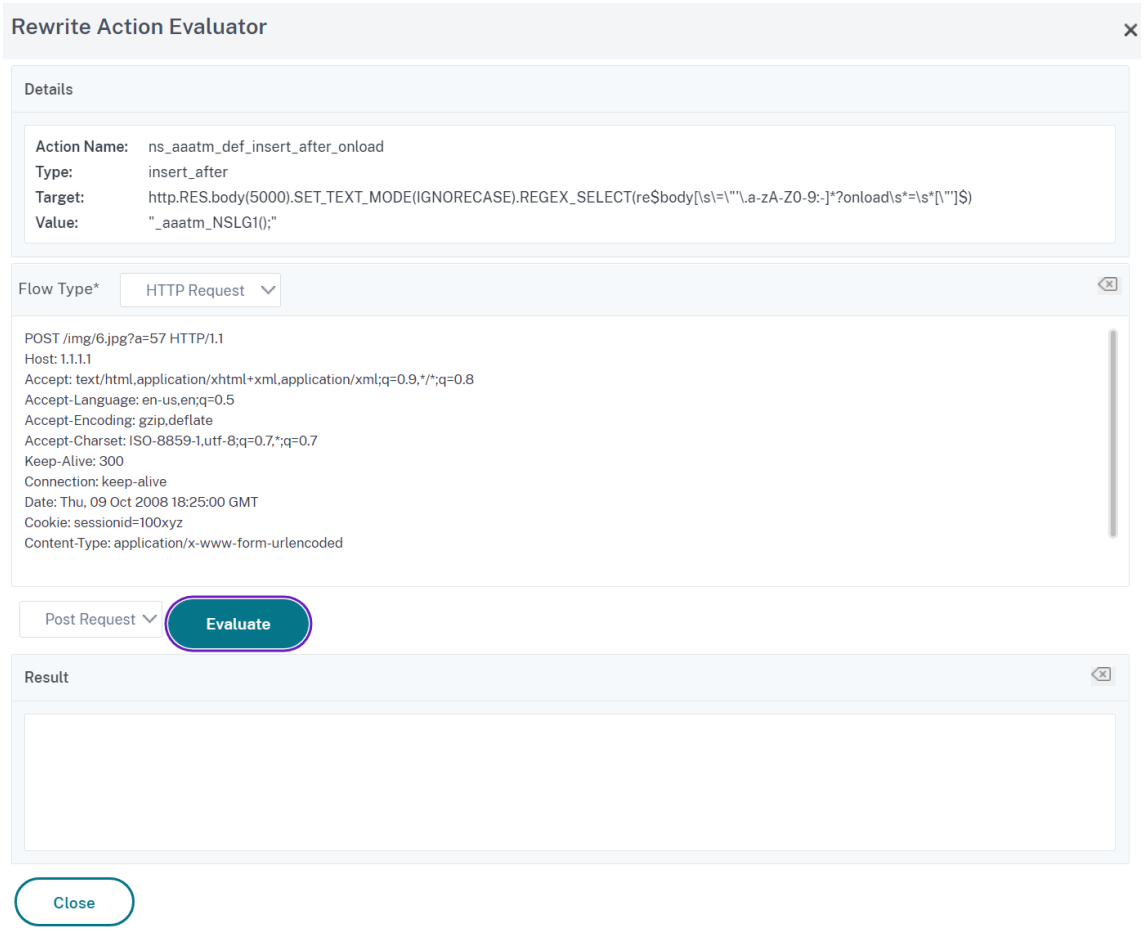
<!--NeedCopy-->
```

Exemple 2 : utilisation de la fonctionnalité Affiner la recherche dans le type d'action INSERT_AFTER_ALL.

```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
   (100) '"refineSearch_testing"' -search text("abc") -refineSearch
   extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:"refineSearch_testing"
Search: text("abc")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Exemple 3 : utilisation de la fonctionnalité Affiner la recherche dans le type d'action REPLACE_ALL.

```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 "www.abc.com"
Done
> bind policy patset pat_list_2 "www.def.com"
Done
> add rewrite action refineSearch_act_31 replace_all "HTTP.RES.BODY
   (100000)" ""https://"" -search "patset("pat_list_2")" -refineSearch
   "EXTEND(7,0).REGEX_SELECT(re#http://#)"
Done
> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:"https://"
```



```
Search: patset("pat_list_2")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Exemple 4 : utilisation de la fonctionnalité Affiner la recherche dans le type d'action DELETE_ALL.

```
>add rewrite action refineSearch_act_4 delete_all "HTTP.RES.BODY(50000)
   " -search text("Windows Desktops") -refineSearch "EXTEND(40,40).
   REGEX_SELECT(re#\s*<AppData>.\*\s\*<\\/AppData>#)"
> show REWRITE action refineSearch_act_4
Name: refineSearch_act_4
Operation: delete_all
Target:HTTP.RES.BODY(50000)
Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s*<AppData>.\*\s\*</
   AppData>#)
Search: text("Windows Desktops")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Exemple 5 : utilisation de la fonctionnalité Affiner la recherche dans le type d'action CLIENTLESS_VPN_ENCODE_ALL.

"'

> ajout de l'action de réécriture act2 clientless_vpn_encode_all http.req.body (100) -search text (« abcd »)
> Effectuée action de réécriture
> sh act2
> Nom : act1
> Opération : clientless_vpn_encode_all
> Cible : http.req.body (100)
> Recherche : text (« abcd »)
> Hits : 0
> Undef Hits : 0
> Action Nombre de références : 0

> Terminé
>
> ”’

Exemple 6 : utilisation de la fonctionnalité Affiner la recherche dans le type d’action CLIENTLESS_VPN_DECODE_ALL.

```
> add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
   -search text("abcd")
Done
> sh rewrite action act1
Name: act1
Operation: clientless_vpn_decode_all
Target:http.req.body(100)
Search: text("abcd")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Modifier une action de réécriture existante à l’aide de l’interface de ligne de commande

À l’invite de commandes, tapez les commandes suivantes pour modifier une action de réécriture existante et vérifier la configuration :

- `set rewrite action <name> [-target <expression>] [-stringBuilderExpr <expression>] [-search <expression>] [-refineSearch <expression>] [-comment <string>]`

À l’invite de commandes, tapez les commandes suivantes pour vérifier la configuration modifiée

- `show rewrite action <name>`

Exemple :

```
> set rewrite action insertact -target "Client-IP"
 Done
> show rewrite action insertact

Name: insertact
Operation: insert_http_header   Target:Client-IP
Value:CLIENT.IP.SRC
Hits: 0
```



```
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Supprimer une action de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour supprimer une action de réécriture :

```
rm rewrite action <name>
```

Exemple :

```
> rm rewrite action insertact
Done

<!--NeedCopy-->
```

Configurez une action de réécriture à l'aide de l'utilitaire de configuration

1. Accédez à **AppExpert > Rewrite > Actions**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une action, cliquez sur **Ajouter**.
   - Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Modifier**.
3. Cliquez sur **Créer** ou **sur OK**. Un message apparaît dans la barre d'état, indiquant que l'action a été correctement configurée.
4. Répétez les étapes 2 à 4 pour créer ou modifier autant d'actions de réécriture que vous le souhaitez.
5. Cliquez sur **Fermer**.



Ajouter une expression à l'aide de la boîte de dialogue Ajouter une expression

1. Dans la boîte de dialogue **Créer une action** de **réécriture ou Configurer une action** de réécriture, sous la zone de texte de l'argument de type que vous souhaitez entrer, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Ajouter une expression**, dans la première zone de liste, choisissez le premier terme de votre expression.
   - HTTP. Le protocole HTTP. Choisissez cette option si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP.
   - SYS. Les sites Web protégés. Sélectionnez cette option si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
   - CLIENT. L'ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.

Lorsque vous faites votre choix, la zone de liste la plus à droite répertorie les termes appropriés pour la partie suivante de votre expression.

1. Dans la deuxième zone de liste, choisissez le deuxième terme de votre expression. Les choix dépendent du choix que vous avez effectué à l'étape précédente et sont adaptés au contexte. Une fois que vous avez fait votre deuxième choix, la fenêtre d'aide située sous la fenêtre Construire une expression (qui était vide) affiche de l'aide décrivant le but et l'utilisation du terme que vous venez de choisir.
2. Continuez à choisir des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente, ou à taper des chaînes ou des nombres dans les zones de texte qui s'affichent pour vous inviter à entrer une valeur, jusqu'à ce que votre expression soit terminée.
   Pour plus d'informations sur le langage des expressions PI et la création d'expressions pour les stratégies de répondeur, voir « Policies and Expressions ».

Si vous souhaitez tester l'effet d'une action de réécriture lorsqu'elle est utilisée sur des exemples de données HTTP, vous pouvez utiliser l'évaluateur de réécriture d'expression.

Réécriture des charges utiles TCP

Les expressions cibles des actions de réécriture TCP doivent commencer par l'un des préfixes d'expression suivants :

- **CLIENT.TCP.PAYLOAD.** Pour réécrire les charges utiles TCP dans les demandes des clients. Par exemple, CLIENT.TCP.PAYLOAD(10000).AFTER_STR("string1").
- **SERVER.TCP.PAYLOAD.** Pour réécrire les charges utiles TCP dans les réponses du serveur. Par exemple, SERVER.TCP.PAYLOAD(1000).B64DECODE.BETWEEN("string1","string2").

Évaluez une action de réécriture à l'aide de la boîte de dialogue Evaluateur d'actions de réécriture

1. Dans le volet de détails **Actions de réécriture**, sélectionnez l'action de réécriture que vous souhaitez évaluer, puis cliquez sur **Evaluer**.
2. Dans la boîte de dialogue Rewrite Expression Evaluator, spécifiez les valeurs des paramètres suivants. (Un astérisque indique un paramètre obligatoire.)

   Action de réécriture : si l'action de réécriture que vous souhaitez évaluer n'est pas déjà sélectionnée, sélectionnez-la dans la liste déroulante. Une fois que vous avez sélectionné une action de réécriture, la section Détails affiche les détails de l'action de réécriture sélectionnée.
   Nouveau : sélectionnez Nouveau pour ouvrir la boîte de dialogue Créer une action de réécriture et créer une action de réécriture.
   Modifier : sélectionnez Modifier pour ouvrir la boîte de dialogue Configurer l'action de réécriture et modifier l'action de réécriture sélectionnée.
   Type de flux : spécifie si l'action de réécriture sélectionnée doit être testée avec des données de demande HTTP ou de réponse HTTP. La valeur par défaut est Request. Si vous souhaitez effectuer un test avec les données de réponse, sélectionnez Réponse.
   Données de requête/réponse HTTP* : fournit un espace vous permettant de fournir les données HTTP que l'évaluateur d'action de réécriture est utilisé pour tester. Vous pouvez coller les données directement dans la fenêtre ou cliquer sur Exemple pour insérer des exemples d'en-têtes HTTP.
   Afficher la fin de ligne : spécifie si les caractères de fin de ligne de style UNIX (\ n) doivent être affichés à la fin de chaque ligne d'exemple de données HTTP.
   Exemple : insère des données HTTP d'exemple dans la fenêtre Données de requête/réponse HTTP. Vous pouvez choisir les données GET ou POST.
   Parcourir (Browse) : ouvre une fenêtre de navigation locale qui vous permet de choisir un fichier contenant des exemples de données HTTP à partir d'un emplacement local ou réseau.

Effacer (Clear) : efface les exemples de données HTTP actuels de la fenêtre Données de requête/réponse HTTP.

3. Cliquez sur Evaluer. L' **évaluateur d'action de réécriture** évalue l'effet de l'action Réécrire sur les données d'exemple que vous avez choisies et affiche les résultats tels que modifiés par l'action de **réécriture** sélectionnée dans la fenêtre **Résultats** . Les ajouts et suppressions sont mis en surbrillance comme indiqué dans la légende dans le coin inférieur gauche de la boîte de dialogue.
4. Continuez à évaluer les actions de réécriture jusqu'à ce que vous ayez déterminé que toutes vos actions ont l'effet souhaité.
    - Vous pouvez modifier l'action de réécriture sélectionnée et tester la version modifiée en cliquant sur **Modifier** pour ouvrir la boîte de dialogue **Configurer l'action de réécriture**, en effectuant et en enregistrant vos modifications, puis en cliquant à nouveau sur Evaluer.
    - Vous pouvez évaluer une action de réécriture différente à l'aide des mêmes données de demande ou de réponse en la sélectionnant dans la liste déroulante **Action de réécriture**, puis en cliquant à nouveau sur **Evaluer** .
5. Cliquez sur **Fermer** pour fermer l' **évaluateur d'expression de réécriture** et revenir au volet **Actions de réécriture** .
6. Pour supprimer une action de réécriture, sélectionnez l'action de réécriture à supprimer, puis cliquez sur **Supprimer** et, lorsque vous y êtes invité, confirmez votre choix en cliquant sur **OK**.



Configurer la stratégie de réécriture

Après avoir créé les actions de réécriture nécessaires, vous devez créer au moins une stratégie de réécriture pour sélectionner les demandes que vous souhaitez que l'appliance NetScaler réécrive.

Une stratégie de réécriture se compose d'une règle, elle-même composée d'une ou de plusieurs expressions, et d'une action associée qui est exécutée si une demande ou une réponse correspond à la règle. Les règles de stratégie d'évaluation des requêtes et réponses HTTP peuvent être basées sur presque n'importe quelle partie d'une demande ou d'une réponse.

Même si vous ne pouvez pas utiliser les actions de réécriture TCP pour réécrire des données autres que la charge utile TCP, vous pouvez baser les règles de stratégie pour les stratégies de réécriture TCP sur les informations de la couche de transport et des couches situées sous la couche de transport.

Si une règle configurée correspond à une demande ou à une réponse, la stratégie correspondante est déclenchée et l'action qui lui est associée est exécutée.

> **Remarque :**
>
> Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique pour créer et con-

> figurer des stratégies de réécriture. Les utilisateurs qui ne sont pas parfaitement familiarisés avec l'interface de ligne de commande et le langage d'expression NetScaler Policy trouveront généralement l'interface utilisateur beaucoup plus facile à utiliser.

Pour ajouter une nouvelle stratégie de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une nouvelle stratégie de réécriture et vérifier la configuration :

- `<add rewrite policy <name> <expression> <action> [<undefaction>]`
- `<show rewrite policy <name>`

Exemple 1. Réécriture du contenu HTTP

```
> add rewrite policyNew "HTTP.RES.IS_VALID" insertact NOREWRITE
 Done
> show rewrite policyNew
        Name: policyNew
        Rule: HTTP.RES.IS_VALID
        RewriteAction: insertact
        UndefAction: NOREWRITE
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```

Exemple 2. Réécriture d'une charge utile TCP (réécriture TCP) :

```
> add rewrite policy client_tcp_payload_policy CLIENT.IP.SRC.EQ
   (172.168.12.232) client_tcp_payload_replace_all
 Done
> show rewrite policy client_tcp_payload_policy
        Name: client_tcp_payload_policy
        Rule: CLIENT.IP.SRC.EQ(172.168.12.232)
        RewriteAction: client_tcp_payload_replace_all
        UndefAction: Use Global
        LogAction: Use Global
        Hits: 0
        Undef Hits: 0

 Done
>
<!--NeedCopy-->
```

Pour modifier une stratégie de réécriture existante à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier une stratégie de réécriture existante et vérifier la configuration :

- `<set rewrite policy <name> -rule <expression> -action <action> [<undefaction>]`
- `<show rewrite policy <name>`

Exemple :

```
> set rewrite policyNew -rule "HTTP.RES.IS_VALID" -action insertaction
 Done

> show rewrite policyNew
        Name: policyNew
        Rule: HTTP.RES.IS_VALID
        RewriteAction: insertaction
        UndefAction: NOREWRITE
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```

Pour supprimer une stratégie de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour supprimer une stratégie de réécriture :

```
rm rewrite policy <name>
```

Exemple :

```
> rm rewrite policyNew
Done
<!--NeedCopy-->
```

Pour configurer une stratégie de réécriture à l'aide de l'interface graphique

1. Accédez à **AppExpert > Rewrite > Policies**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une stratégie, cliquez sur Ajouter.
   - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur Ouvrir.
3. Cliquez sur **Créer** ou **sur OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.
4. Répétez les étapes 2 à 4 pour créer ou modifier autant d'actions de réécriture que vous le souhaitez.

5. Cliquez sur **Fermer**. Pour supprimer une stratégie de réécriture, sélectionnez la stratégie de réécriture à supprimer, puis cliquez sur **Supprimer** et, lorsque vous y êtes invité, confirmez votre choix en cliquant sur **OK**.

Lier une stratégie de réécriture

Après avoir créé une stratégie de réécriture, vous devez la lier pour la mettre en œuvre. Vous pouvez lier votre stratégie à Global si vous souhaitez l'appliquer à tout le trafic qui passe par votre NetScaler, ou vous pouvez lier votre stratégie à un serveur virtuel ou à un point de liaison spécifique pour diriger uniquement ce serveur virtuel ou lier le trafic entrant du point à cette stratégie. Si une demande entrante correspond à une stratégie de réécriture, l'action associée à cette stratégie est exécutée.

Les stratégies de réécriture pour l'évaluation des requêtes et réponses HTTP peuvent être liées à des serveurs virtuels de type HTTP ou SSL, ou elles peuvent être liées aux points de liaison REQ_OVERRIDE,
REQ_DEFAULT, RES_OVERRIDE et RES_DEFAULT. Les stratégies de réécriture pour la réécriture TCP peuvent être liées uniquement aux serveurs virtuels de type TCP ou SSL_TCP, ou aux points de liaison OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE et OTHERTCP_RES_DEFAULT.

> **Remarque :**
>
> Le terme OTHERTCP est utilisé dans le contexte de l'appliance NetScaler pour désigner toutes les demandes et réponses TCP ou SSL_TCP que vous souhaitez traiter comme un flux brut d'octets, quels que soient les protocoles encapsulés par les paquets TCP.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel nombre entier positif.

Dans le système d'exploitation NetScaler, les priorités des stratégies fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible. Par exemple, si vous avez trois stratégies avec des priorités de 10, 100 et 1000, la stratégie affectée d'une priorité de 10 est appliquée en premier, puis la stratégie affectée une priorité de 100 et enfin la stratégie affectée d'un ordre de 1000.

Contrairement à la plupart des autres fonctionnalités du système d'exploitation NetScaler, la fonction de réécriture continue d'évaluer et de mettre en œuvre des stratégies une fois qu'une demande correspond à une stratégie. Toutefois, l'effet d'une stratégie d'action particulière sur une demande ou une réponse sera souvent différent selon qu'elle est exécutée avant ou après une autre action. La priorité est importante pour obtenir les résultats escomptés.

Vous pouvez vous laisser suffisamment de place pour ajouter d'autres stratégies dans n'importe quel ordre, tout en les définissant pour qu'elles soient évaluées dans l'ordre souhaité, en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous la liez. Dans ce cas, vous

pouvez ajouter d'autres stratégies à tout moment sans avoir à réattribuer la priorité d'une stratégie existante.

Lorsque vous liez une stratégie de réécriture, vous avez également la possibilité d'affecter une expression goto (GoToPriorityExpression) à la stratégie. Une expression goto peut être n'importe quel entier positif correspondant à la priorité attribuée à une autre stratégie dont la priorité est supérieure à celle qui contient l'expression goto. Si vous attribuez une expression goto à une stratégie et qu'une demande ou une réponse correspond à cette stratégie, NetScaler accède immédiatement à la stratégie dont la priorité correspond à l'expression goto. Il ignore toutes les stratégies dont les numéros de priorité sont inférieurs à ceux de la stratégie actuelle, mais supérieurs au numéro de priorité de l'expression goto, et n'évalue pas ces stratégies.

Pour lier globalement une stratégie de réécriture à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier globalement une stratégie de réécriture et vérifier la configuration :

- `bind rewrite global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show rewrite global`

Exemple :

```
>bind rewrite global policyNew 10
 Done

> show rewrite global
1)      Global bindpoint: RES_DEFAULT
        Number of bound policies: 1

2)      Global bindpoint: REQ_OVERRIDE
        Number of bound policies: 1

 Done
<!--NeedCopy-->
```

Pour lier la stratégie de réécriture à un serveur virtuel spécifique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier la stratégie de réécriture à un serveur virtuel spécifique et vérifier la configuration :

- `bind lb vserver <name>@ (<serviceName>@ [-weight <positive_integer>])| <serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>)] )`

- show lb vserver <name>

Exemple :

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 50
 Done
>
> show lb vserver lbvip
        lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jul 15 05:54:24 2009 (+226 ms)
        Time since last state change: 28 days, 01:57:26.350
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1)      Policy : ns_cmp_msapp Priority:50
2)      Policy : cf-pol Priority:1      Inherited
 Done
<!--NeedCopy-->
```

Pour lier une stratégie de réécriture à un point de liaison à l'aide de l'interface graphique

1. Accédez à **AppExpert** >**Réécriture** > **Stratégies**.
2. Dans le volet d'informations, sélectionnez la stratégie de réécriture que vous souhaitez lier globalement, puis cliquez sur **Gestionnaire de stratégies**.
3. Dans la boîte de dialogue **Gestionnaire de stratégies de réécriture**, dans le menu **Points de liaison**, effectuez l'une des opérations suivantes :
   a) Si vous souhaitez configurer des liaisons pour les stratégies de réécriture HTTP, cliquez sur **HTTP**, puis sur **Demande** ou **Réponse**, selon que vous souhaitez configurer des stratégies de réécriture basées sur les demandes ou des stratégies de réécriture basées sur les réponses.
   b) Si vous souhaitez configurer des liaisons pour les stratégies de réécriture TCP, cliquez sur **TCP**, puis sur **Client** ou **Serveur**, selon que vous souhaitez configurer des stratégies de

réécriture TCP côté client ou des stratégies de réécriture TCP côté serveur.

4. Cliquez sur le point de liaison auquel vous souhaitez lier la stratégie de réécriture. La boîte de dialogue **Gestionnaire de stratégies** de réécriture affiche toutes les stratégies de réécriture liées au point de liaison sélectionné.
5. Cliquez sur **Insérer une stratégie** pour insérer une nouvelle ligne et afficher une liste déroulante contenant toutes les stratégies de réécriture disponibles et non liées.
6. Cliquez sur la stratégie que vous souhaitez lier au point de liaison. La stratégie est insérée dans la liste des stratégies de réécriture liées au point de liaison.
7. Dans la colonne **Priorité**, vous pouvez modifier la priorité par n'importe quel entier positif. Pour plus d'informations sur ce paramètre, reportez-vous à la section Priorité dans « Paramètres de liaison d'une stratégie de réécriture. »
8. Si vous souhaitez ignorer les stratégies et accéder directement à une stratégie spécifique si la stratégie actuelle est appariée, modifiez la valeur de la colonne Goto Expression pour qu'elle corresponde à la priorité de la prochaine stratégie à appliquer. Pour plus d'informations sur ce paramètre, consultez GoToPriorityExpression dans « Paramètres de liaison d'une stratégie de réécriture ».
9. Pour modifier une stratégie, cliquez sur la stratégie, puis sur **Modifier la stratégie**.
10. Pour délier une stratégie, cliquez sur la stratégie, puis cliquez sur **Délier la stratégie**.
11. Pour modifier une action, dans la colonne Action, cliquez sur l'action que vous souhaitez modifier, puis cliquez sur **Modifier l'action**.
12. Pour modifier une étiquette d'appel, dans la colonne **Invoke**, cliquez sur l'étiquette d'appel que vous souhaitez modifier, puis cliquez sur **Modifier le libellé d'appel**.
13. Pour régénérer les priorités de toutes les stratégies liées au point de liaison que vous configurez actuellement, cliquez sur **Régénérer les priorités**. Les stratégies conservent leurs priorités existantes par rapport aux autres stratégies, mais les priorités sont renumérotées par multiples de 10.
14. Cliquez sur **Appliquer les modifications**.
15. Cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.

Pour lier une stratégie de réécriture à un serveur virtuel spécifique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans la liste des serveurs virtuels du volet d'informations, sélectionnez le serveur virtuel auquel vous souhaitez lier la stratégie de réécriture, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le serveur virtuel (équilibrage de charge)**, sélectionnez l'onglet **Stratégies** . Toutes les stratégies configurées sur votre NetScaler apparaissent dans la liste.
4. Cochez la case en regard du nom de la stratégie que vous souhaitez lier à ce serveur virtuel.
5. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.

Configuration des étiquettes de stratégie de réécriture

Si vous souhaitez créer une structure de stratégie plus complexe que celle prise en charge par des stratégies uniques, vous pouvez créer des étiquettes de stratégie, puis les lier comme vous le feriez pour les stratégies. Une étiquette de stratégie est un point défini par l'utilisateur auquel les stratégies sont liées. Lorsqu'une étiquette de stratégie est appelée, toutes les stratégies qui lui sont liées sont évaluées dans l'ordre de priorité que vous avez configuré. Un libellé de stratégie peut inclure une ou plusieurs stratégies, chacune pouvant se voir attribuer son propre résultat. Une correspondance sur une stratégie dans l'étiquette de stratégie peut entraîner la poursuite de la stratégie suivante, l'appel d'un autre libellé de stratégie ou d'une ressource appropriée, ou la fin immédiate de l'évaluation de la stratégie et le retour du contrôle à la stratégie qui a appelé l'étiquette de stratégie.

Une étiquette de stratégie de réécriture se compose d'un nom, d'un nom de transformation qui décrit le type de stratégie inclus dans l'étiquette de stratégie et d'une liste de stratégies liées à l'étiquette de stratégie. Chaque stratégie liée à l'étiquette de stratégie contient tous les éléments décrits dans Configuration d'une stratégie de réécriture.

Remarque : Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique pour créer et configurer des étiquettes de stratégie de réécriture. Les utilisateurs qui ne sont pas parfaitement familiarisés avec l'interface de ligne de commande et le langage NetScaler Policy Infrastructure (PI) trouvent généralement l'interface utilisateur beaucoup plus facile à utiliser.

Pour configurer une étiquette de stratégie de réécriture à l'aide de l'interface de ligne de commande

Pour ajouter une étiquette de stratégie de réécriture, à l'invite de commandes, tapez la commande suivante :

```
add rewrite policylabel <labelName> <transform>
```

Par exemple, pour ajouter une étiquette de stratégie de réécriture nommée PollabelHttpResponses afin de regrouper toutes les stratégies qui fonctionnent sur les réponses HTTP, vous devez taper ce qui suit :

```
add rewrite policy label polLabelHTTPResponses http_res
```

Pour modifier une étiquette de stratégie de réécriture existante, à l'invite de commande **NetScaler**, tapez la commande suivante :

```
set rewrite policy <name> <transform>
```

> **Remarque :**
>
> La commande set rewrite policy utilise les mêmes options que la commande add rewrite policy.

Pour supprimer une étiquette de stratégie de réécriture, à l'invite de commande **NetScaler**, tapez la commande suivante :

```
rm rewrite policy<name>
```


Par exemple, pour supprimer une étiquette de stratégie de réécriture nommée PollabelHttpResponses, vous devez taper ce qui suit :

```
rm rewrite policy polLabelHTTPResponses
```

Pour configurer une étiquette de stratégie de réécriture à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Réécriture** > **Étiquettes de stratégie**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une étiquette de stratégie, cliquez sur **Ajouter**.
   - Pour modifier une étiquette de stratégie existante, sélectionnez la stratégie, puis cliquez sur **Ouvrir**.
3. Ajoutez ou supprimez des stratégies de la liste liée à l'étiquette de stratégie.
   - Pour ajouter une stratégie à la liste, cliquez sur **Insérer une stratégie**, puis choisissez une stratégie dans la liste déroulante. Vous pouvez créer une stratégie et l'ajouter à la liste en choisissant Nouvelle stratégie dans la liste, puis en suivant les instructions de la section Configuration d'une stratégie de réécriture.
   - Pour supprimer une stratégie de la liste, sélectionnez-la, puis cliquez sur Annuler la stratégie.
4. Modifiez la priorité de chaque stratégie en modifiant le nombre dans la colonne Priorité.
   Vous pouvez également renuméroter automatiquement les stratégies en cliquant sur Régénérer les priorités.
5. Cliquez sur **Créer** ou sur **OK**, puis sur **Fermer**.
   Pour supprimer une étiquette de stratégie, sélectionnez-la, puis cliquez sur **Supprimer**. Pour renommer une étiquette de stratégie, sélectionnez-la, puis cliquez sur **Renommer**. Modifiez le nom de la stratégie, puis cliquez sur **OK** pour enregistrer vos modifications.

Comportement de la longueur du contenu de l'en-tête dans une action de réécriture en continu

June 20, 2023

L'en-tête Content-Length est l'un des moyens d'indiquer la longueur du message (en octets) dans une requête ou une réponse HTTP. Outre l'en-tête Content-Length, vous pouvez également spécifier la longueur du message en utilisant l'une des méthodes suivantes :

- Codage fragmenté
- Arrêt FIN

Dans un processus de streaming, NetScaler envoie des données en continu après le traitement de l'action de réécriture. Comme les données sont envoyées en continu et ne sont pas conservées par

NetScaler, la longueur réelle du message qui serait envoyé au client est inconnue. Par conséquent, la valeur correcte de l'en-tête Content-Length ne peut pas être mentionnée dans la réponse.

Pour faciliter le processus de diffusion, la fonction de réécriture de NetScaler convertit la manière d'indiquer la longueur du message entre l'en-tête Content-Length et la fin FIN. Dans le cadre de la conversion, NetScaler corrompt l'en-tête Content-Length en réorganisant les quatre premiers caractères du nom de l'en-tête.

En HTTP, le client est censé ignorer les en-têtes qu'il ne comprend pas. Le client ne comprend donc pas le nom d'en-tête Content-Length corrompu et ignore donc l'en-tête. Pour améliorer les performances de NetScaler, l'en-tête est endommagé au lieu d'être supprimé. Corriger le nom de l'en-tête au lieu de le supprimer évite de recalculer la somme de contrôle car la somme de contrôle n'est pas modifiée si les mêmes octets se trouvent dans un ordre différent.

Par exemple, considérez la requête HTTP suivante :

```
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml,
     image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-
    excel, application/vnd.ms-powerpoint, application/msword, /
Accept-Language: en-GB
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
    Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
     3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; CMDTDF; MS-RTC
    LM 8)
Accept-Encoding: gzip, deflate
Host: test.example.net
Connection: Keep-Alive
<!--NeedCopy-->
```

Dans un scénario fonctionnel, la réponse entre NetScaler et le serveur principal pour cette requête HTTP est la suivante :

```
HTTP/1.1 200 OK
Content-Length: 10967
Connection: close
var SERVER_URL = 'https\x3a\x2f\x2ftest.example.net\x2f';
var WEB_SERVER_HOST = 'test.example.net';
<!--NeedCopy-->
```

Mais la réponse reçue par le client de NetScaler dans un scénario non fonctionnel est la suivante. L'en-tête `Content-Length` est renommé en `ntcoent-Length`.

```
HTTP/1.1 200 OK
ntCoent-Length: 10967
```



```
nnCoection: close
var SERVER_URL = 'https\x3a\x2f\x2ftest.example.net\x2f';
var WEB_SERVER_HOST = 'test.example.net';
<!--NeedCopy-->
```

En général, les applications clientes prennent en charge les trois méthodes de transaction : en-tête de longueur du contenu, codage par blocs et terminaison FIN. Ainsi, la conversion de l'en-tête Content-Length en Fin Termination ne doit pas poser de problème. Mais si l'application ne fonctionne pas à cause de cette modification, vous devez désactiver le processus de streaming.

Comment désactiver le processus de streaming dans une stratégie de réécriture

Vous pouvez désactiver le processus de diffusion dans une stratégie de réécriture de l'une des manières suivantes :

1. Ajoutez une action non liée au streaming associée à une stratégie de réécriture associée à une priorité plus élevée. L'action doit être telle qu'elle ne modifie pas la réponse.

   Par exemple :

   ```
   add rewrite action non_stream_act replace_all HTTP.RES.BODY(1000000)
   HTTP.RES.FULL_HEADER -search text("pattern_which_will_not_match_in_body
   ")
   ```

   La valeur du corps dans cette action de réécriture doit être supérieure à la valeur sur laquelle fonctionne l'action de diffusion en cours.

2. Au lieu de la configuration de diffusion, utilisez la configuration non de diffusion.

   > **Remarque :**
   >
   > Le passage d'un traitement en streaming à un traitement sans diffusion peut avoir un impact sur les performances de NetScaler.

   Par exemple, une configuration de diffusion peut être convertie en une configuration non de diffusion comme suit :

   Configuration du streaming :

   ```
   add rewrite action rw_act_1 replace_all HTTP.RES.BODY(1000) ""http
       "" -search text("http")

   add policy patset pat_list
   bind policy patset pat_list abcd
   bind policy patset pat_list defg

   ```



```
add rewrite action rw_act_2 replace_all HTTP.RES.BODY(1000) ""
    replaced_data"" -search patset("pat_list")
<!--NeedCopy-->
```

Configuration sans diffusion en continu :

```
add rewrite action rw_act_1 replace_all HTTP.RES.BODY(1000) ""http
    "" -search regex(re/http/)

add rewrite action rw_act_1 replace_all HTTP.RES.BODY(1000) ""http
    "" -search regex(re/abcd|defg/)
<!--NeedCopy-->
```

Exemples d'actions et de stratégies de réécriture

May 5, 2023

Les exemples de cette section montrent comment configurer la réécriture pour effectuer diverses tâches utiles. Les exemples se trouvent dans la salle des serveurs d'Example Manufacturing Inc., une entreprise de fabrication de taille moyenne qui utilise son site Web pour gérer une part considérable de ses ventes, de ses livraisons et de son support client.

Example Manufacturing possède deux domaines : example.com pour son site Web et ses e-mails destinés aux clients, et example.net pour son intranet. Les clients utilisent le site Web Example pour passer des commandes, demander des devis, rechercher des produits et contacter le service client et le support technique.

En tant que partie importante du flux de revenus d'Example, le site Web doit répondre rapidement et préserver la confidentialité des données des clients. Example possède donc plusieurs serveurs Web et utilise des appliances NetScaler pour équilibrer la charge du site Web et gérer le trafic à destination et en provenance de ses serveurs Web.

Les administrateurs système de l'exemple utilisent les fonctionnalités de réécriture pour effectuer les tâches suivantes :

Exemple 1 : Supprimer les anciens en-têtes X-Forwarded-For et Client-IP

Example Inc. supprime les anciens en-têtes HTTP X-Forwarded-For et Client-IP des requêtes entrantes.

Exemple 2 : Ajout d'un en-tête Client-IP local

Example Inc. ajoute un nouvel en-tête Client-IP local aux demandes entrantes.

Exemple 3 : Balisage des connexions sécurisées et non sécurisées

Example Inc. étiquette les demandes entrantes avec un en-tête qui indique si la connexion est sécurisée.

Exemple 4 : masquer le type de serveur HTTP

Example Inc. modifie l'en-tête HTTP Server : afin que les utilisateurs non autorisés et les codes malveillants ne puissent pas utiliser cet en-tête pour déterminer le logiciel du serveur HTTP qu'il utilise.

Exemple 5 : rediriger une URL externe vers une URL interne

Example Inc. masque aux utilisateurs les informations concernant les noms réels de ses serveurs Web et la configuration de sa salle de serveurs, afin de raccourcir les URL de son site Web et d'en faciliter la mémorisation et d'améliorer la sécurité de son site.

Exemple 6 : migration des règles du module de réécriture Apache

Example Inc. a transféré ses règles de réécriture Apache vers une appliance NetScaler, traduisant la syntaxe du script basé sur Apache Perl en syntaxe des règles de réécriture NetScaler.

Exemple 7 : Redirection de mots clés marketing

Le service marketing d'Example Inc. définit des URL simplifiées pour certaines recherches par mot clé prédéfinies sur le site Web de l'entreprise.

Exemple 8 : rediriger les requêtes vers le serveur interrogé

Example Inc. redirige certaines requêtes vers le serveur approprié.

Exemple 9 : Redirection de la page d'accueil

Example Inc. a récemment acquis un petit concurrent et redirige désormais les demandes vers la page d'accueil de la société acquise vers une page de son propre site Web.

Exemple 10 : Cryptage RSA basé sur une stratégie

Exemple : cryptez le contenu d'en-tête ou de corps HTTP prédéfini et défini par l'utilisateur à l'aide de la clé publique PEM RSA.

Chacune de ces tâches nécessite que les administrateurs système créent des actions et des politiques de réécriture et les lient à un point de liaison valide sur NetScaler.

Exemple 1 : Supprimer les anciens en-têtes X-Forwarded-For et Client-IP

May 5, 2023

Example Inc. souhaite supprimer les anciens en-têtes HTTP X-Forwarded-For et Client-IP des requêtes entrantes, afin que les seuls en-têtes X-Forwarded-For qui apparaissent soient ceux ajoutés par le serveur local. Cette configuration peut être effectuée via la ligne de commande NetScaler

ou l'utilitaire de configuration. L'administrateur système d'Example Inc. est un ingénieur réseau de la vieille école qui préfère utiliser une CLI dans la mesure du possible, mais il souhaite s'assurer qu'il comprend l'interface de l'utilitaire de configuration afin de pouvoir montrer aux nouveaux administrateurs système de l'équipe comment l'utiliser.

Les exemples ci-dessous montrent comment effectuer chaque configuration à la fois à l'aide de l'interface de ligne de commande et de l'utilitaire de configuration. Les procédures sont abrégées en supposant que les utilisateurs connaissent déjà les bases de la création d'actions de réécriture, de la création de stratégies de réécriture et des stratégies de liaison.

- Pour plus d'informations sur la création d'actions de réécriture, voir Configuration d'une action de réécriture.
- Pour plus d'informations sur la création de stratégies de réécriture, voir Configuration d'une stratégie de réécriture.
- Pour plus d'informations sur les stratégies de réécriture de liaison, voir Liaison d'une stratégie de réécriture.

Pour supprimer les anciens en-têtes X-Forwarded et Client-IP d'une requête à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes dans l'ordre indiqué :

```
add rewrite action act_del_xfor delete_http_header x-forwarded-for
add rewrite action act_del_cip delete_http_header client-ip
add rewrite policy pol_check_xfor 'HTTP.REQ.HEADER("x-forwarded-for").
    EXISTS' act_del_xfor
add rewrite policy pol_check_cip 'HTTP.REQ.HEADER("client-ip").EXISTS'
    act_del_cip
bind rewrite global pol_check_xfor 100 200
bind rewrite global pol_check_cip 200 300
<!--NeedCopy-->
```

Pour supprimer les anciens en-têtes X-ForWARDED et Client-IP d'une requête à l'aide de l'utilitaire de configuration

Dans la boîte de dialogue Créer une action de réécriture, créez deux actions de réécriture avec les descriptions suivantes.

Nom	Type	Argument (s)
act_del_xpour	delete_http_header	x-forwarded-pour
act_del_cip	delete_http_header	adresse IP du client

Dans la boîte de dialogue Créer une politique de réécriture, créez deux politiques de réécriture avec les descriptions suivantes.

Nom	Expression	Action
pol_check_xpour	« HTTP.REQ.HEADER (« x-forwarded-for ») .EXISTE »	act_del_xpour
pol_check_cip	« HTTP.REQ.HEADER (« client-ip ») .EXISTE »	act_del_cip

Liez les deux politiques à une politique globale, en attribuant les priorités et les valeurs d'expression goto indiquées ci-dessous.

Nom	Priority	Aller à Expression
pol_check_xpour	100	200
pol_check_cip	200	300

Tous les anciens en-têtes HTTP X-Forwarded-For et Client-IP sont désormais supprimés des requêtes entrantes.

Exemple 2 : Ajout d'un en-tête IP client local

August 20, 2021

Example Inc. souhaite ajouter un en-tête HTTP Client-IP local aux requêtes entrantes. Cet exemple contient deux versions légèrement différentes de la même tâche de base.

Pour ajouter un en-tête Client-IP local à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes dans l'ordre indiqué :

```
1 add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.
     IP.SRC'
2 add rewrite policy pol_ins_client 'HTTP.REQ.HEADER("x-forwarded-for").
     EXISTS || HTTP.REQ.HEADER("client-ip").EXISTS' act_ins_client
3 bind rewrite global pol_ins_client 300 END
4 <!--NeedCopy-->
```


Pour ajouter un en-tête Client-IP local à l'aide de l'utilitaire de configuration

Dans la boîte de dialogue Créer une action de réécriture, créez une action de réécriture avec la description suivante.

Nom	Type	Argument(s)
act_ins_client	insert_http_header	NS-Client 'CLIENT .IP.SRC'

Dans la boîte de dialogue Créer une stratégie de réécriture, créez une stratégie de réécriture avec la description suivante.

Nom	Expression.	Action
pol_ins_client	'HTTP.REQ.HEADER (« x-forwarded-for ») .EXISTS || HTTP.REQ.HEADER (« client-ip ») .EXISTS'	act_ins_client

Liez la stratégie à globale, en affectant les priorités et les valeurs d'expression goto indiquées ci-dessous.

Nom	Priority	Goto Expression
pol_ins_client	100	Suivant

Exemple 3 : Balisage des connexions sécurisées et non sécurisées

May 5, 2023

Example Inc. souhaite baliser les demandes entrantes avec un en-tête indiquant si la connexion est sécurisée ou non. Cela permet au serveur de suivre les connexions sécurisées une fois que NetScaler les a déchiffrées.

Pour implémenter cette configuration, vous devez commencer par créer des actions de réécriture avec les valeurs indiquées dans les tableaux suivants. Ces actions qualifient les connexions au port 80 de connexions non sécurisées et les connexions au port 443 de connexions sécurisées.

Nom de l'action	Type d'action de réécriture	Nom de l'en-tête	Valeur
Action-Rewrite-SSL_Oui	INSERT_HTTP_HEADER	SSL	OUI

Nom de l'action	Type d'action de réécriture	Nom de l'en-tête	Valeur
Action-Rewrite-SSL_Non	INSERT_HTTP_HEADER	SSL	NON

Vous devez ensuite créer une politique de réécriture avec les valeurs indiquées dans les tableaux suivants. Ces politiques vérifient les demandes entrantes afin de déterminer quelles demandes sont dirigées vers le port 80 et lesquelles sont dirigées vers le port 443. Les politiques ajoutent ensuite l'en-tête SSL approprié.

Nom de la stratégie	Nom de l'action	Action non définie	Expression
Policy-Rewrite-SSL_Yes	Action-Rewrite-SSL_Oui	NOREWRITE	CLIENT.TCP.DSTPORT.EQ (443)
Policy-Rewrite-SSL_NO	Action-Rewrite-SSL_Non	NOREWRITE	CLIENT.TCP.DSTPORT.EQ (80)

Enfin, vous devez lier les politiques de réécriture à NetScaler, en attribuant à la première politique une priorité de 200 et à la seconde une priorité de 300, et en définissant l'expression goto des deux politiques sur END.

Chaque connexion entrante au port 80 a maintenant un en-tête HTTP SSL:NO ajouté et chaque connexion entrante au port 443 a un en-tête HTTP SSL:YES ajouté.

Exemple 4 : masquer le type de serveur HTTP

October 5, 2021

Example Inc. souhaite modifier l'en-tête HTTP Server : afin que les utilisateurs non autorisés et le code malveillant ne puissent pas utiliser cet en-tête pour identifier le logiciel utilisé par le serveur HTTP.

Pour modifier l'en-tête HTTP Server :, vous devez créer une action de réécriture et une stratégie de réécriture avec les valeurs des tableaux suivants.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Masque_serveur Action-Réécriture	REMPLACER	HTTP.RES.HEADER (« Serveur »)	« Serveur Web 1.0 »

Nom de la stratégie	Nom de l'action	Action non définie	Expression.
Policy-Rewrite-Server_Mask	Masque_serveur Action-Réécriture	NOREWRITE	HTTP.RES.IS_VALID

Exemples de commandes :

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("Server")"\"Web Server 1.0\""
```

```
> add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
```

Vous liez ensuite globalement la stratégie de réécriture, en attribuant une priorité de 100 et en définissant l'expression de priorité Goto de la stratégie sur END.

L'en-tête HTTP Server : est maintenant modifié pour lire « Web Server 1.0 », masquant le logiciel de serveur HTTP utilisé par le site Web Example Inc.

Exemple 5 : rediriger une URL externe vers une URL interne

January 31, 2022

Example Inc. souhaite masquer la configuration de sa salle de serveurs aux utilisateurs afin d'améliorer la sécurité de ses serveurs Web.

Pour améliorer la sécurité, vous devez créer une action de réécriture avec les valeurs indiquées dans les tableaux suivants. Pour les en-têtes de demande, l'action de la table est modifiée `www.example.com` en web.hq.example.net. Pour les en-têtes de réponse, l'action fait l'inverse, en se traduisant par `web.hq.example.netwww.example.com`.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Action-Réécriture-Request_Server_Repla	REMPLACER	HTTP.REQ.HOSTNAME.S	« Web.HQ.Example.net »
Action-Réécriture-Response_Server_Replace	REMPLACER	HTTP.RES.HEADER (« Serveur »)	« www.example.com »

La première stratégie vérifie les demandes entrantes pour voir si elles sont valides. S'ils sont valides, il exécute l'action Action-Rewrite-Request_Server_Replace. La deuxième stratégie vérifie les réponses pour vérifier si elles proviennent du serveur `web.hq.example.net`. Si tel est le cas, il exécute l'action Action-Rewrite-Response_Server_Replace.

Exemples d'actions de réécriture et de stratégie de redirection d'une URL externe.

```
add rewrite action Action-Rewrite-Request_Server_Replace REPLACE HTTP.REQ.
HOSTNAME.SERVER '"Web.hq.example.net"'

add rewrite action Action-Rewrite-Response_Server_Replace REPLACE HTTP.RES.
HEADER("Server")'"www.example.com"'

add rewrite policy Rewrite-Request_Server_Replace HTTP.REQ.HOSTNAME.SERVER.
EQ("www.example.com")Action-Rewrite-Request_Server_Replace NOREWRITE

add rewrite policy Rewrite-Response_Server_Replace HTTP.REQ.HEADER("Server"
).EQ("Web.hq.example.net")Action-Rewrite-Response_Server_Replace
```

Enfin, vous devez lier les stratégies de réécriture, en attribuant à chacune une priorité de 500, car elles se trouvent dans des banques de stratégies différentes et ne sont pas en conflit. Définissez l'expression goto sur NEXT pour les deux liaisons.

```
bind rewrite global Policy-Rewrite-Request_Server_Replace 500 END -type
REQ_DEFAULT

bind rewrite global Policy-Rewrite-Response_Server_Replace 500 END -type
RES_DEFAULT
```

Toutes les instances de `www.example.com` dans les en-têtes de requête sont désormais remplacées par `web.hq.example.net`, et toutes les instances `web.hq.example.net` des en-têtes de réponse sont désormais remplacées par `www.example.com`.

Exemple 6 : migration des règles du module de réécriture Apache

May 5, 2023

Example Inc. utilise actuellement le module de réécriture d'Apache pour traiter les demandes de recherche envoyées à ses serveurs Web et rediriger ces demandes vers le serveur approprié sur la base des informations contenues dans l'URL de la demande. Example Inc. souhaite simplifier sa configuration en migrant ces règles vers la plateforme NetScaler.

Plusieurs règles de réécriture d'Apache utilisées actuellement par Example sont présentées ci-dessous. Ces règles redirigent les demandes de recherche vers une page de résultats spéciale si elles ne comportent pas de chaîne SiteID ou si la chaîne SiteID est égale à zéro (0), ou vers la page de résultats standard si ces conditions ne s'appliquent pas.

Voici les règles de réécriture Apache actuelles :

- RewriteCond % {REQUEST_FILENAME} ^/search$ [NC]
- Réécrivez % {QUERY_STRING} ! SiteID= [OU]
- RewriteCond %{QUERY_STRING} SiteId=0
- RewriteCond % {QUERY_STRING} callName=DisplayResults [NC]
- Règle de réécriture ^.*$ results2.html [P, L]
- RewriteCond % {REQUEST_FILENAME} ^/search$ [NC]
- RewriteCond % {QUERY_STRING} callName=DisplayResults [NC]
- Règle de réécriture ^.*$ /results.html [P, L]

Pour implémenter ces règles de réécriture Apache sur NetScaler, vous devez créer des actions de réécriture avec les valeurs des tableaux suivants.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Action-Rewrite-Display_Results_Nulsit	REMPLACER	HTTP.REQ.URL	"/results2.html"
Action-Réécriture-Afficher_Résultats	REMPLACER	HTTP.REQ.URL	"/results2.html"

Vous devez ensuite créer des politiques de réécriture avec les valeurs indiquées dans les tableaux ci-dessous.

Nom de la stratégie	Nom de l'action	Action non définie	Expression
Réécriture de la politique Display_Results_NulSiteID	Action-Rewrite-Display_Results_Nulsit	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MOD (IGNORECASE) .EQ (« /search ») && (! HTTP.REQ.URL.QUERY.CONTAINS (« SiteId= ») || HTTP.REQ.URL.QUERY.CONTAINS (« SiteId=0") || HTTP.REQ.URL.QUERY.SET_TEXT_MO (IGNORECASE) .CONTAINS (« Call-Name=DisplayResults »))
Réécriture des politiques - Affichage des résultats	Action-Réécriture-Afficher_Résultats	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MOD (IGNORECASE) .EQ (« /search ») || HTTP.REQ.URL.QUERY.SET_TEXT_MO (IGNORECASE) .CONTAINS (« Call-Name=DisplayResults »))

Enfin, vous devez lier les politiques de réécriture en attribuant à la première une priorité de 600 et à la seconde une priorité de 700, puis en définissant l'expression goto sur NEXT pour les deux liaisons.

NetScaler gère désormais ces demandes de recherche exactement comme le faisait le serveur Web avant la migration des règles du module de réécriture Apache.

Exemple 7 : Redirection de mots clés marketing

May 5, 2023

Le service marketing d'Example Inc. souhaite configurer des URL simplifiées pour certaines recherches par mot clé prédéfinies sur le site Web de l'entreprise. Pour ces mots clés, il souhaite redéfinir l'URL comme indiqué ci-dessous.

- URL externe :

```
http://www.example.com/\<marketingkeyword\>
```

- URL interne :


```
http://www.example.com/go/kwsearch.asp?keyword=\<marketingkeyword\>
```

Pour configurer la redirection pour les mots clés marketing, vous devez créer une action de réécriture avec les valeurs du tableau suivant.

Nom de l'action	Type d'action de réécriture	Expression pour choisir l'emplacement cible	Expression de chaîne pour le texte de remplacement
Action-Rewrite-Modify_URL	INSERT_BEFORE	HTTP.REQ.URL.PATH.GE (1)	« go/k-search.aspkeyword = »

Vous devez ensuite créer une stratégie de réécriture avec les valeurs du tableau suivant.

Nom de la stratégie	Nom de l'action	Action non définie	Expression
Réécriture-Modify_URL de la politique	Action-Rewrite-Modify_URL	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ (« www.exemple.com »)

Enfin, vous liez la stratégie de réécriture en lui attribuant une priorité de 800. Contrairement aux politiques de réécriture précédentes, cette politique doit être la dernière à être appliquée à une demande correspondant à ses critères. C'est pourquoi l'administrateur de NetScaler définit son expression de priorité Goto sur END.

Toute demande utilisant un mot clé marketing est redirigée vers la page CGI de recherche par mot clé, après quoi une recherche est effectuée et toutes les politiques restantes sont ignorées.

Exemple 8 : Redirection des requêtes vers le serveur interrogé

October 5, 2021

Example Inc. souhaite rediriger les demandes de requête vers le serveur approprié, comme illustré ici.

- `<Request: GET /query.cgi?server=5HOST: www.example.com`
- `<Redirect URL: <http://web-5.example.com/>`

Pour implémenter cette redirection, vous devez d'abord créer une action de réécriture avec les valeurs du tableau suivant.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Action-Réécriture-Replace_Hostheader	REMPLACER	HTTP.REQ.HEADER (« Hôte ») .BEFORE_STR (« .example.com »)	« serveur- » + HTTP.REQ.URL.QUERY.VALUE (« web »)

Vous devez ensuite créer une stratégie de réécriture avec les valeurs du tableau suivant.

Nom de la stratégie	Nom de l'action	Action non définie	Expression.
`Policy-Rewrite-Replace_Hostheader`	`Action-Rewrite-Replace_Hostheader`	NOREWRITE	`HTTP.REQ.HEADER("Host").EQ("www.example.com")`

Exemples de commandes :

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("Server")"\"Web Server 1.0\""
Done
```

```
> add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
Done
```

Enfin, vous liez la stratégie de réécriture en lui attribuant une priorité de 900. Comme cette stratégie doit être la dernière stratégie appliquée à une demande qui correspond à ses critères, vous définissez l'expression goto sur END.

Les demandes entrantes vers n'importe quelle URL commençant par `<http://www.example.com/query.cgi?server>=` sont redirigées vers le numéro de serveur figurant dans la requête.

Exemple 9 : Redirection de la page d'accueil

May 5, 2023

New Company, Inc. a récemment acquis un concurrent plus petit, Purchased Company, et souhaite rediriger la page d'accueil de Purchased Company vers une nouvelle page de son propre site Web, comme indiqué ici.

- Ancienne URL : http://www.purchasedcompany.com/*
- Nouvelle URL : http://www.newcompany.com/products/page.htm

Pour rediriger les demandes vers la page d'accueil de la société achetée, vous devez créer des actions de réécriture avec les valeurs du tableau suivant.

Nom de l'action	Type d'action de réécriture	Expression pour choisir la référence cible	Expression de chaîne pour le texte de remplacement
Action-Rewrite-Replace_URLR	REMPLACER	HTTP.REQ.URL.PATH_A	« /products/-page.htm »
Action-Réécriture-Remplacer_Host	REMPLACER	HTTP.REQ.HOSTNAME	« www.newcompany.com »

```
1 add rewrite action action-Rewrite-Replace_URLr REPLACE HTTP.REQ.URL.
    PATH_AND_QUERY  "/products/page.htm"
2
3 add rewrite action action-Rewrite-Replace_Host REPLACE HTTP.REQ.
    HOSTNAME  "www.newcompany.com"
4 <!--NeedCopy-->
```

Vous devez ensuite créer des politiques de réécriture avec les valeurs du tableau suivant.

Nom de la stratégie	Nom de l'action	Action non définie	Expression
Réécriture de la politique, remplacement, aucune	Action-Réécriture-Remplace-Aucun	NOREWRITE	! HTTP.REQ.HOSTNAME.SERVER.EQ (« www.purchasedcompany.com »)
Réécriture des politiques, remplacement de l'hôte	Action-Réécriture-Remplacer_Host	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ (« www.purchasedcompany.com »)

```
1 add rewrite policy Policy-Rewrite-Replace-None !HTTP.REQ.HOSTNAME.
    SERVER.EQ( "www.purchasedcompany.com" ) Action-Rewrite-Replace-None
    NOREWRITE
2
3 add rewrite policy Policy-Rewrite-Replace-Host HTTP.REQ.HOSTNAME.SERVER
    .EQ( "www.purchasedcompany.com" ) Action-Rewrite-Replace_Host
```



```
    NOREWRITE
<!--NeedCopy-->
```

Enfin, vous devez lier les politiques de réécriture de manière globale, en attribuant à la première une priorité de 100 et à la seconde une priorité de 200.

```
bind rewrite global Policy-Rewrite-Replace-None 100

bind rewrite global Policy-Rewrite-Replace-Host 200
<!--NeedCopy-->
```

Les demandes adressées à l'ancien site Web de la société acquise sont désormais redirigées vers la bonne page sur la page d'accueil de la nouvelle société.

Exemple 10 : Cryptage RSA basé sur une stratégie

May 5, 2023

L'algorithme RSA utilise la fonction PKEY_ENCRYPT_PEM () pour chiffrer le contenu d'en-tête ou de corps HTTP prédéfini et défini par l'utilisateur. La fonction accepte uniquement les clés publiques RSA (pas les clés privées) et les données cryptées ne peuvent pas dépasser la longueur de la clé publique. Lorsque les données cryptées sont inférieures à la longueur de la clé, l'algorithme utilise la méthode de remplissage RSA_PKCS1.

Dans un exemple de scénario, la fonction peut être utilisée avec la fonction B64ENCODE () dans une action de réécriture visant à remplacer une valeur d'en-tête HTTP par une valeur cryptée par une clé publique RSA. Les données chiffrées sont ensuite décryptées par le destinataire à l'aide de la clé privée RSA.

Vous pouvez implémenter cette fonctionnalité à l'aide d'une politique de réécriture. Pour ce faire, vous devez effectuer les tâches suivantes :

1. Ajoutez la clé publique RSA en tant qu'expression de politique.
2. Créez une action de réécriture.
3. Créez une politique de réécriture.
4. Liez la politique de réécriture comme globale.
5. Vérifiez le chiffrement RSA

Chiffrement RSA basé sur des règles à l'aide de l'interface de commande NetScaler

Effectuez les tâches suivantes pour configurer le chiffrement RSA basé sur des règles à l'aide de l'interface de commande NetScaler.

Pour ajouter une clé publique RSA en tant qu'expression de politique à l'aide de l'interface de commande NetScaler :

```
add policy expression pubkey '"-----BEGIN RSA PUBLIC KEY-----
   MIGJAoGBAKl5vgQEj73Kxp+9
   yn1v5gPR1pnc4oLM2a0kaWwBOsB6rzCIy6znwnvwCY1xRvQhRlJSAyJbloL7wZFIJ2FOR8Cz
   +8ZQWXU2syG+udi4EnWqLgFYowF9zK+o79az597eNPAjsHZ/C2oL/+6qY5a/
   f1z8bQPrHC4GpFfAEJhh/+NnAgMBAAE=-----END RSA PUBLIC KEY-----"'
<!--NeedCopy-->
```

Pour ajouter une action de réécriture visant à chiffrer une demande d'en-tête HTTP à l'aide de l'interface de commande NetScaler :

```
add rewrite action encrypt_act insert_http_header encrypted_data

HTTP.REQ.HEADER("data_to_encrypt").PKEY_ENCRYPT_PEM(pubkey).B64ENCODE
```

Pour ajouter une politique de réécriture à l'aide de l'interface de commande NetScaler :

```
add rewrite policy encrypt_pol 'HTTP.REQ.HEADER("data_to_encrypt").
   EXISTS' encrypt_act
<!--NeedCopy-->
```

Pour lier une politique de réécriture globale à l'aide de l'interface de commande NetScaler :

```
bind rewrite global encrypt_pol 10 -type RES_DEFAULT
```

Pour vérifier le chiffrement RSA à l'aide de l'interface de commande NetScaler :

```
>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/`

* About to connect() to 10.217.24.7 port 80 (#0)

*  Trying 10.217.24.7...

*  connected

*  Connected to 10.217.24.7 (10.217.24.7) port 80 (#0)

> GET / HTTP/1.1
> User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0
   OpenSSL/0.9.8y zlib/1.2.3
> Host: 10.217.24.7
> Accept: \*/\*
> data_to_encrypt: Now is the time that tries men's souls
>
```



```
< HTTP/1.1 200 OK
< Date: Mon, 09 Oct 2017 05:22:37 GMT
< Server: Apache/2.2.24 (FreeBSD) mod_ssl/2.2.24 OpenSSL/0.9.8y DAV/2
< Last-Modified: Thu, 20 Feb 2014 20:29:06 GMT
< ETag: "6bd9f2-2c-4f2dc5b570880"
< Accept-Ranges: bytes
< Content-Length: 44
< Content-Type: text/html
< encrypted_data: UliegKBJqZd7JdaC49XMLEK1+eQN2rEfevypW91gKvBVlaKM9N9/
   C2BKuztS99SE0xQaisidzN5IgeIcpQMn+
   CiKYVlLzPG1RuhGaqHYzIt6C8A842da7xE4OlV5SHwScqkqZ5aVrXc3EwtUksna7jOLr40aLeXnnB
   /DB11pUAE=
<
* Connection #0 to host 10.217.24.7 left intact
<html><body><h1>It works!</h1></body></html>* Closing connection #0

<!--NeedCopy-->
```

L'exécution ultérieure de cette commande curl avec les mêmes données à chiffrer montre que les données cryptées sont différentes à chaque exécution. Cela est dû au fait que le remplissage insère des octets aléatoires au début des données à chiffrer, ce qui fait que les données cryptées sont différentes à chaque fois.

```
>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/`

< encrypted_data:
   DaOjtl1Pl4DlQKf58MMeL4cFwFvZwhjMqv5aUYM5Iyzk4UpwIYhpRvgTNu2lXEVc1H0tcR1EGC
   /ViQncLc4EbTurCWLbzjce3+fknnMmzF0lRT6ZZXWbMvsNFOxDA1SnuAgwxWXy/
   ooe9Wy6SYsL2oi1sr5wTG+RihDd9zP+P14=

>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/

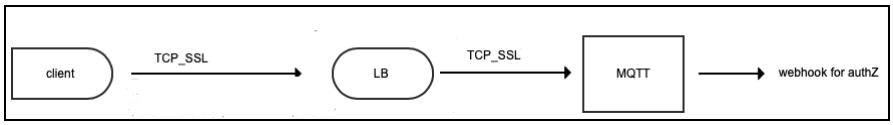
. . .

< encrypted_data: eej6YbGP68yHn48qFUvi+fkG+OiO8j3yYLScrRBU+
   TPQ8WeDVaWnDNAVLvL0ZYHHAU1W2YDRYb+8
   cdKHLpW36QbI6Q5FfBuWKZSI2hSyUvypTpCoAYcHXFv0ns+tRtg0EPNNj+
   lyGjKQWtFi6K8IXXISoDy42FblKIlaA7gEriY=
<!--NeedCopy-->
```


Chiffrement RSA basé sur des règles à l'aide de l'interface graphique

L'interface graphique vous permet d'effectuer les tâches suivantes :

Pour ajouter une clé publique RSA en tant qu'expression de politique à l'aide de l'interface graphique :

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configurations**>**AppExpert > Expressions avancées**.**
2. Dans le volet de détails, cliquez sur **Ajouter** pour définir une clé publique RSA en tant qu'expression de politique avancée.
3. Dans la page Créer une expression, définissez les paramètres suivants :
   a) Nom de l'expression. Nom de l'expression avancée.
   b) Expression : Définissez la clé publique RSA en tant qu'expression avancée à l'aide de l'éditeur d'expressions.
   c) Commentaires. Brève description de l'expression.
4. Cliquez sur **Create**.

Pour ajouter une action de réécriture afin de chiffrer une demande d'en-tête HTTP à l'aide de l'interface graphique :

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configurations**>**AppExpert > **Réécrire**** > Actions.**
2. Dans le volet de détails, cliquez sur **Ajouter** pour ajouter une action de réécriture.
3. Dans l'écran **Créer une action de réécriture**, définissez les paramètres suivants :
   a) Nom. Nom de l'action de réécriture.
   b) Tapez. Sélectionnez le type d'action INSERT_HTTP_HEADER.
   c) Utilisez le type d'action pour insérer un en-tête. Entrez le nom de l'en-tête HTTP qui doit être réécrit.
   d) Expression : Nom de l'expression de politique avancée associée à l'action.
   e) Commentaires. Brève description de l'action de réécriture.
4. Cliquez sur **Create**.

Pour ajouter une politique avancée de réécriture à l'aide de l'interface graphique :

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configurations**>**AppExpert**>**Réécrire**> Politiques.**
2. Sur la page **Politiques de réécriture**, cliquez sur **Ajouter** pour ajouter une politique de réécriture.
3. Sur la page **Créer une politique de réécriture**, définissez les paramètres suivants :
   a) Nom. Nom de la politique de réécriture.
   b) Action. Nom de l'action de réécriture à effectuer si la demande ou la réponse correspond à cette politique de réécriture.
   c) Action de journalisation. Nom de l'action du journal des messages à utiliser lorsqu'une

demande correspond à cette politique.
   d) Action dont le résultat n'est pas défini. Action à effectuer si le résultat de l'évaluation de la politique n'est pas défini.
   e) Expression : Nom de l'expression de politique avancée qui déclenche l'action.
   f) Commentaires. Brève description de l'action de réécriture.
4. Cliquez sur **Create**.

Pour lier une politique de réécriture globale à l'aide de l'interface graphique :

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configurations**>**AppExpert**>**Réécrire**>** **Politiques.**
2. Dans l'écran **Politiques de réécriture**, sélectionnez la politique de réécriture que vous souhaitez lier et cliquez sur Gestionnaire de **stratégies**.
3. Sur la page Rewrite Policy Manager, dans la section Bind Points, définissez les paramètres suivants :
   a) Point de liaison. Sélectionnez le point de liaison comme Global par défaut.
   b) Protocole. Sélectionnez le type de protocole HTTP.
   c) Type de connexion. Sélectionnez le type de connexion comme Demande.
   d) Cliquez sur **Continuer** pour afficher la section **Politique contraignante** .
   e) Dans la section **Liaison des politiques**, sélectionnez la politique de réécriture et définissez les paramètres de liaison.
4. Cliquez sur **Bind**.

Exemple 11 : chiffrement RSA basé sur des règles sans opération de remplissage

May 5, 2023

La fonction de politique PKEY_ENCRYPT_PEM_NO_PADDING () utilise l'algorithme RSA sans opération de remplissage avant d'effectuer le chiffrement RSA. La fonction de politique fonctionne exactement comme la fonction PKEY_ENCRYPT_PEM (), sauf qu'elle utilise la méthode RSA_NO_PADDING au lieu de RSA_PKCS1_PADDING. Le paramètre pkey est une chaîne de texte contenant une clé publique RSA codée au format PEM. Comme pour PKEY_ENCRYPT_PEM (), vous pouvez utiliser une expression de politique pour la clé.

Vous pouvez implémenter cette fonctionnalité à l'aide d'une politique de réécriture. Pour ce faire, vous devez effectuer les tâches suivantes :

1. Ajoutez la clé publique RSA en tant qu'expression de politique.
2. Créez une action de réécriture.

Chiffrement RSA basé sur des règles à l'aide de l'interface de commande NetScaler

Effectuez les tâches suivantes pour configurer le chiffrement RSA basé sur des règles à l'aide de l'interface de commande NetScaler.

Pour ajouter une clé publique RSA sans expression de politique de remplissage à l'aide de l'interface de commande NetScaler :

```
1 add expression rsa_pub_key_4096 '"-----BEGIN RSA PUBLIC KEY-----" + "
    MIICCgKCAgEArrwBldKd48xrpOSRPMrg+eNAO0ODU6t5b/WYQLdElqNv7WpefBrA" +
    "nwI2s619gEU1r4zoLqL7l5ALtt5Z+F0JBYfOzBzOky0GtEJ5iX5GP4QxT65J3nHH" +
     "4MTF3acmjvXxclmaKXEFlaVIzW7FTr3Luw/CnOjflAB403Q6F9VBVvQmOVYWnqoI"
    + "+0q1VIg6Q1pAcvdKBiOf85BBofE5EIbZ/1Jt0CdbsV568l+8ve7BnSUncFHoRR3O"
     + "/VfSsDuNWZf7n3RNMzxEuIA72UGPzNYFQzvcPOdzd0aN7jAXw0mgC/NSvKzGKHlo
    " + "mUYYBzlVQdDMZWnd6jSzsBRXSXxsNEy/
    RuXwplrA5epo7JdCoMkfeI4vUXm6MNr8" + "
    TQdFqIc1pdnOsbRf9ec62XbcfR7P8CDTsmLSaagx3rjenPdB+LTWKw2VUF+YONIg" +
    "jM3fyFef9ovVhLhS5HvMqFGs8P75W+d7BOIbIu3EngACiEJOpYSsETD4WgPK6Iyv" +
     "j6cxsLeYMtElTb0fBIIqysCHdmjF3M1lqdqp4dKs3+W798GJZYM5MxZKUzrBi0Xu"
    + "e7GtSh2aimsfQureUD+0z0RN2umeDsYcA1ghXMclDP+jLS1lnrv0Yvo+TKcm9b8G"
     + "uR/drbCrCsGyWFW+bsAu3AWz9S6TePurP5unRmNNvXpH5DRgsYl3d50CAwEAAQ
    ==" + "-----END RSA PUBLIC KEY-----"
2 <!--NeedCopy-->
```

Pour ajouter une action de réécriture pour une expression de politique sans remplissage à l'aide de l'interface de commande NetScaler :

```
add rewrite action rsa_encrypt_act insertHttpHeader encrypted 'HTTP.REQ.
HEADER("plaintext").PKEY_ENCRYPT_PEM_NO_PADDING(rsa_pub_key_4096)
```

Chiffrement RSA basé sur des règles sans option de remplissage à l'aide de l'interface graphique

L'interface graphique vous permet d'effectuer les tâches suivantes :

Pour ajouter une clé publique RSA sans opération de remplissage en tant qu'expression de politique à l'aide de l'interface graphique :

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configurations**>**AppExpert > Expressions avancées**.**
2. Dans le volet de détails, cliquez sur **Ajouter** pour définir une clé publique RSA en tant qu'expression de politique avancée.
3. Dans la page Créer une expression, définissez les paramètres suivants :
   a) Nom de l'expression. Nom de l'expression avancée.

b) Expression : Définissez la clé publique RSA en tant qu'expression avancée à l'aide de l'éditeur d'expressions.
Remarque : La longueur de chaîne maximale est de 255 caractères dans une expression de politique. Pour toute clé de plus de 1024 bits, vous devez la diviser en petits morceaux et les concaténer sous la forme « chunk1" + « chunk2" +…
c) Commentaires. Brève description de l'expression.

4. Cliquez sur **Create**.

Pour ajouter une action de réécriture à l'aide de l'interface graphique :

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configurations**>**AppExpert > **Réécrire**** > Actions.**
2. Dans le volet de détails, cliquez sur **Ajouter** pour ajouter une action de réécriture.
3. Dans l'écran **Créer une action de réécriture**, définissez les paramètres suivants :
   a) Nom. Nom de l'action de réécriture.
   b) Tapez. Sélectionnez le type d'action INSERT_HTTP_HEADER.
   c) Utilisez le type d'action pour insérer un en-tête. Entrez le nom de l'en-tête HTTP qui doit être réécrit.
   d) Expression : Nom de l'expression de politique avancée associée à l'action.
   e) Commentaires. Brève description de l'action de réécriture.
4. Cliquez sur **Create**.

Exemple 12 : configurer la réécriture pour modifier le nom d'hôte et l'URL dans la demande du client sur l'appliance NetScaler

May 5, 2023

La fonctionnalité de réécriture d'une appliance NetScaler est utilisée pour convertir l'URL disponible dans la demande du client en une autre URL que le serveur principal peut comprendre. Vous pouvez bénéficier des avantages suivants en utilisant la fonction de réécriture :

- Améliore la sécurité en masquant l'URL réelle de la ressource demandée par le client.
- Empêche les utilisateurs non autorisés d'accéder aux ressources du réseau.

Prenons un exemple où votre organisation actuelle est rachetée par une autre organisation. Il devient difficile pour les administrateurs d'informer chaque utilisateur de l'organisation acquise de la nouvelle adresse Web. Dans ce scénario, l'utilisation de la fonction de réécriture devient pratique pour modifier le nom d'hôte et l'URL dans les demandes du client pour le site Web de l'organisation acquise. Vous pouvez utiliser la réécriture pour modifier temporairement les URL de la demande du client lorsque le site Web est en cours de maintenance.

La section suivante décrit la procédure permettant de modifier le nom d'hôte et l'URL dans une demande client à l'aide de la fonction de réécriture.

Prenons l'exemple d'un utilisateur qui saisit une `http://www.example.com` URL dans le navigateur Web. L'administrateur du site Web souhaite que l'appliance NetScaler convertisse l'URL précédente de la demande du client en. `http://myexample.example.net.in/resource/inventory/s?t=112`

Dans l'exemple précédent, l'administrateur du site Web souhaite que l'appliance NetScaler remplace le nom de domaine « example.com » par « myexample.example.net.in » et l'URL par « resource/inventory/s ? t = 112 pouces.

Effectuez les opérations suivantes à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'appliance NetScaler via SSH.
2. Ajoutez des actions de réécriture.
   - `add rewrite action rewrite_doman_url_repalce_act replace HTTP.REQ.URL "\"http://myexample.example.net.in/resource/inventory/s?t=112\""`
3. Ajoutez des stratégies de réécriture pour les actions de réécriture.
   - `add rewrite policy rewrite_domain_url_pol HTTP.REQ.HOSTNAME.EQ("www.example.com")rewrite_doman_url_repalce_act`
4. Liez les stratégies de réécriture à un serveur virtuel.
   - `bind lb vserver rewrite_LB -policyName rewrite_domain_url_pol -priority 100 -gotoPriorityExpression END -type REQUEST`

Transformation d'URL

March 1, 2022

La fonction de transformation d'URL fournit une méthode pour modifier toutes les URL des demandes désignées à partir d'une version externe vue par des utilisateurs externes vers une URL interne visible uniquement par vos serveurs Web et votre personnel informatique. Vous pouvez rediriger les demandes des utilisateurs de manière transparente, sans exposer la structure de votre réseau aux utilisateurs. Vous pouvez également modifier des URL internes complexes dont les utilisateurs peuvent avoir du mal à se souvenir en URL externes plus simples et plus facilement mémorisées.

> **Remarque**
>
> Avant de pouvoir utiliser la fonction de transformation d'URL, vous devez activer la fonction Réécriture. Pour activer la fonction de réécriture, reportez-vous à la section Activation de la fonction de réécriture.
>
> La fonction de transformation d'URL réécrit les URL dans le corps de réponse HTML et n'est pas appliquée à JavaScript et à d'autres variables.

Pour commencer à configurer la transformation d'URL, vous créez des profils, chacun décrivant une transformation spécifique. Dans chaque profil, vous créez une ou plusieurs actions décrivant en détail la transformation. Ensuite, vous créez des stratégies, chacune identifiant un type de requête HTTP à transformer, et vous associez chaque stratégie à un profil approprié. Enfin, vous liez globalement chaque stratégie pour la mettre en œuvre.

Configuration des profils de transformation d'URL

May 5, 2023

Un profil décrit une transformation d'URL spécifique sous la forme d'une série d'actions. Le profil fonctionne principalement comme un conteneur pour les actions, déterminant l'ordre dans lequel les actions sont exécutées. La plupart des transformations transforment un nom d'hôte externe et un chemin facultatif en un nom d'hôte et un chemin internes différents. La plupart des transformations utiles sont simples et ne nécessitent qu'une seule action, mais vous pouvez utiliser plusieurs actions pour effectuer des transformations complexes.

Vous ne pouvez pas créer d'actions puis les ajouter à un profil. Vous devez d'abord créer le profil, puis y ajouter des actions. Dans l'interface de ligne de commande, la création d'une action et sa configuration sont des étapes distinctes. La création d'un profil et sa configuration sont des étapes distinctes à la fois dans l'interface de ligne de commande et dans l'utilitaire de configuration.

Pour créer un profil de transformation d'URL à l'aide de la ligne de commande NetScaler

À l'invite de commandes NetScaler, tapez les commandes suivantes, dans l'ordre indiqué, pour créer un profil de transformation d'URL et vérifier la configuration. Vous pouvez ensuite répéter les deuxième et troisième commandes pour configurer des actions supplémentaires :

- `add transform profile <profileName> -type URL [-onlyTransformAbsURLinBody (ON|OFF)] \[-comment <comment>]`
- `add transform action <name> <profileName> <priority>`

- set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainFrom <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]
- show transform profile <name>

Exemple :

```
> add transform profile shoppingcart -type URL
 Done
> add transform action actshopping shoppingcart 1000
 Done
> set transform action actshopping -priority 1000 -reqUrlFrom 'shopping
   .example.com' -reqUrlInto 'www.example.net/shopping' -resUrlFrom '
   www.example.net/shopping' -resUrlInto 'shopping.example.com' -
   cookieDomainFrom 'example.com' -cookieDomainInto 'example.net' -
   state ENABLED -comment 'URL transformation for shopping cart.'
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
 Done
<!--NeedCopy-->
```

Pour modifier un profil ou une action de transformation d'URL existant à l'aide de la ligne de commande NetScaler

À l'invite de commandes NetScaler, tapez les commandes suivantes pour modifier un profil ou une action de transformation d'URL existant et vérifier la configuration :

Remarque : Utilisez respectivement un profil de transformation défini ou une commande d'action de transformation. La commande set transform profile utilise les mêmes arguments que la commande add transform profile, et set transform action est la même commande que celle utilisée pour la configuration initiale.

- set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]
- show transform profile <name>

Exemple :

```
> set transform action actshopping -priority 1000 -reqUrlFrom '
    searching.example.net' -reqUrlInto 'www.example.net/searching' -
    resUrlFrom 'www.example.net/searching' -resUrlInto 'searching.
    example.com' -cookieDomainInto 'example.net' -state ENABLED -comment
     'URL transformation for searching cart.'
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
 Done
<!--NeedCopy-->
```

Pour supprimer un profil de transformation d'URL et des actions à l'aide de la ligne de commande NetScaler

Supprimez d'abord toutes les actions associées à ce profil en saisissant la commande suivante une fois pour chaque action :

- action de transformation rm <name> Après avoir supprimé toutes les actions associées à un profil, supprimez le profil comme indiqué ci-dessous.
- profil de transformation rm <name>

Pour créer un profil de transformation d'URL à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez **Réécrire**, développez Transformation d'URL, puis cliquez sur **Profils**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un profil de transformation d'URL**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres de configuration des profils de transformation d'URL » comme suit (un astérisque indique un paramètre obligatoire) :
    - Nom* : nom
    - Commentaire : commentaire
    - Transformez uniquement les URL absolues dans le corps de la réponse : OnlyTransformAbsurlinBody

4. Cliquez sur **Créer**, puis sur **Fermer**. Un message s'affiche dans la barre d'état, indiquant que le profil a été correctement configuré.

Pour configurer un profil de transformation d'URL et des actions à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez **Réécrire**, développez Transformation d'URL, puis cliquez sur **Profils**.
2. Dans le volet de détails, sélectionnez le profil que vous souhaitez configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le profil de transformation d'URL**, effectuez l'une des opérations suivantes.
   - Pour créer une nouvelle action, cliquez sur **Ajouter**.
   - Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
4. Remplissez la boîte de dialogue **Créer une action de transformation d'URL ou Modifier une action de transformation d'** URL en saisissant ou en sélectionnant des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres de configuration des profils de transformation d'URL » comme suit (un astérisque indique un paramètre obligatoire) :
   - Nom de l'action* : nom
   - Commentaires : commentaire
   - Priorité*—Priorité
   - Demander une URL à partir de : requrlFrom
   - Demande d'URL dans : RequrLinto
   - URL de réponse de : ResurlFrom
   - URL de réponse dans : URL de retour
   - Domaine du cookie From—CookieDomainFrom
   - Cookie Domain Into—CookieDomainInto
   - Activé : État
5. Enregistrez vos modifications.
   - Si vous créez une nouvelle action, cliquez sur **Créer**, puis sur **Fermer**.
   - Si vous modifiez une action existante, cliquez sur **OK**.
     Un message s'affiche dans la barre d'état, indiquant que le profil a été correctement configuré.
6. Répétez les étapes 3 à 5 pour créer ou modifier des actions supplémentaires.
7. Pour supprimer une action, sélectionnez-la, puis cliquez sur Supprimer. Lorsque vous y êtes invité, cliquez sur OK pour confirmer la suppression.
8. Cliquez sur **OK** pour enregistrer vos modifications et fermer la boîte de dialogue Modifier le profil de transformation d'URL.
9. Pour supprimer un profil, sélectionnez le profil dans le volet d'informations, puis cliquez sur

Supprimer. Lorsque vous y êtes invité, cliquez sur **OK** pour confirmer la suppression.

Configuration des stratégies de transformation d'URL

May 5, 2023

Après avoir créé un profil de transformation d'URL, vous créez ensuite une politique de transformation d'URL pour sélectionner les demandes et les réponses que NetScaler doit transformer à l'aide du profil. La transformation d'URL considère chaque demande et la réponse à celle-ci comme une seule unité, de sorte que les politiques de transformation d'URL ne sont évaluées que lorsqu'une demande est reçue. Si une politique correspond, NetScaler transforme à la fois la demande et la réponse.

Remarque : Les fonctionnalités de transformation et de réécriture d'URL ne peuvent pas toutes deux fonctionner sur le même en-tête HTTP lors du traitement de la demande. Pour cette raison, si vous souhaitez appliquer une transformation d'URL à une demande, vous devez vous assurer qu'aucun des en-têtes HTTP qu'elle modifiera n'est manipulé par une action de réécriture.

Pour configurer une politique de transformation d'URL à l'aide de la ligne de commande NetScaler

Vous devez créer une nouvelle politique. Sur la ligne de commande, une politique existante peut uniquement être supprimée. À l'invite de commandes NetScaler, tapez les commandes suivantes pour configurer une politique de transformation d'URL et vérifier la configuration :

- `<add transform policy <name> <rule> <profileName>`
- `<show transform policy <name>`

Exemple :

```
1  > add transform policy polsearch  HTTP.REQ.URL.SUFFIX.EQ("Searching")
       prosearching
2   Done
3  > show transform policy polsearch
4  1)      Name: polsearch
5          Rule: HTTP.REQ.URL.SUFFIX.EQ("Searching")
6          Profile: prosearching
7          Priority: 0
8          Hits: 0
9   Done
10 <!--NeedCopy-->
```


Pour supprimer une politique de transformation d'URL à l'aide de la ligne de commande NetScaler

À l'invite de commande NetScaler, tapez la commande suivante pour supprimer une politique de transformation d'URL :

```
rm transform policy <name>
```

Exemple :

```
1 > rm transform policy polsearch
2 Done
3 <!--NeedCopy-->
```

Pour configurer une politique de transformation d'URL à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez **Réécrire**, développez Transformation d'URL, puis cliquez sur **Politiques**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle stratégie, cliquez sur **Ajouter**.
   - Pour modifier une politique existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Créer une politique de transformation** d' **URL ou Configurer une politique de transformation** d'URL, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres de configuration des politiques de transformation d'URL » comme suit (un astérisque indique un paramètre obligatoire) :
   - Nom* : nom (ne peut pas être modifié pour une politique précédemment configurée.)
   - profil* : nom du profil
   - Expression—règle

   Si vous avez besoin d'aide pour créer une expression pour une nouvelle politique, vous pouvez soit maintenir la touche Ctrl enfoncée, soit appuyer sur la barre d'espace lorsque votre curseur se trouve dans la zone de texte Expression. Pour créer l'expression, vous pouvez la saisir directement comme décrit ci-dessous ou utiliser la boîte de dialogue Ajouter une expression.
4. Cliquez sur **Préfixe**, puis choisissez le préfixe de votre expression.

   Vos choix sont les suivants :
   - HTTP : le protocole HTTP. Choisissez cette option si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP.

- SYS : le ou les sites Web protégés. Sélectionnez cette option si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
- Client : ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.
- Serveur : ordinateur auquel la demande a été envoyée. Choisissez cette option si vous souhaitez examiner certains aspects du destinataire de la demande.
- URL : URL de la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'URL à laquelle la demande a été envoyée.
- Texte : n'importe quelle chaîne de texte contenue dans la demande. Choisissez cette option si vous souhaitez examiner une chaîne de texte dans la demande.
- Cible : cible de la demande. Choisissez cette option si vous souhaitez examiner certains aspects de la cible de la demande.

Une fois que vous avez choisi un préfixe, NetScaler affiche une fenêtre d'invite en deux parties qui affiche les choix suivants possibles en haut et une brève explication de la signification du choix sélectionné en bas. Les choix dépendent du préfixe que vous avez choisi.

5. Sélectionnez votre prochain terme.

Si vous avez choisi HTTP comme préfixe, vos choix sont REQ, qui spécifie les requêtes HTTP, et RES, qui spécifie les réponses HTTP. Si vous choisissez un autre préfixe, vos choix sont plus variés. Pour obtenir de l'aide sur un choix spécifique, cliquez une fois sur ce choix pour afficher les informations le concernant dans la fenêtre contextuelle inférieure.

Lorsque vous êtes certain du choix souhaité, double-cliquez dessus pour l'insérer dans la fenêtre Expression.

1. Tapez un point, puis continuez à sélectionner des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente. Vous tapez les chaînes de texte ou les nombres appropriés dans les zones de texte qui s'affichent pour vous demander de saisir une valeur, jusqu'à ce que votre expression soit terminée.
2. Cliquez sur **Créer** ou sur **OK**, selon que vous créez une nouvelle stratégie ou modifiez une stratégie existante.
3. Cliquez sur **Fermer**. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.

Pour ajouter une expression à l'aide de la boîte de dialogue Ajouter une expression

1. Dans la boîte de dialogue **Créer une action de répondeur** ou **Configurer une action de répondeur**, cliquez sur **Ajouter**.

2. Dans la boîte de dialogue **Ajouter une expression**, dans la première zone de liste, choisissez le premier terme de votre expression.

    - HTTP. Le protocole HTTP. Choisissez cette option si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP.
    - SYS. Le ou les sites Web protégés. Sélectionnez cette option si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
    - CLIENT. L'ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.
    - SERVEUR. L'ordinateur auquel la demande a été envoyée. Choisissez cette option si vous souhaitez examiner certains aspects du destinataire de la demande.
    - URL. URL de la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'URL à laquelle la demande a été envoyée.
    - TEXTE. N'importe quelle chaîne de texte contenue dans la demande. Choisissez cette option si vous souhaitez examiner une chaîne de texte dans la demande.
    - CIBLE. La cible de la demande. Choisissez cette option si vous souhaitez examiner certains aspects de la cible de la demande.
      Lorsque vous faites votre choix, la zone de liste la plus à droite répertorie les termes appropriés pour la partie suivante de votre expression.

3. Dans la deuxième zone de liste, choisissez le deuxième terme de votre expression. Les choix dépendent du choix que vous avez effectué à l'étape précédente et sont adaptés au contexte. Une fois que vous avez fait votre deuxième choix, la fenêtre d'aide située sous la fenêtre Construire une expression (qui était vide) affiche de l'aide décrivant le but et l'utilisation du terme que vous venez de choisir.

4. Continuez à choisir des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente, ou à taper des chaînes ou des nombres dans les zones de texte qui s'affichent pour vous inviter à entrer une valeur, jusqu'à ce que votre expression soit terminée.

Liaison globale des stratégies de transformation d'URL

May 5, 2023

Après avoir configuré vos politiques de transformation d'URL, vous les liez à Global ou à un point de liaison pour les mettre en œuvre. Après la liaison, toute demande ou réponse correspondant à une politique de transformation d'URL est transformée par le profil associé à cette politique.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe

quel nombre entier positif. Dans le système d'exploitation NetScaler, les priorités des politiques fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible.

Étant donné que la fonctionnalité de transformation d'URL met en œuvre uniquement la première politique à laquelle une demande correspond, et non les politiques supplémentaires auxquelles elle pourrait également correspondre, la priorité de la politique est importante pour obtenir les résultats souhaités. Si vous attribuez à votre première politique une faible priorité (par exemple 1000), vous demandez à NetScaler de ne l'exécuter que si d'autres politiques ayant une priorité plus élevée ne correspondent pas à une demande. Si vous accordez à votre première politique une priorité élevée (par exemple, 1), vous demandez à NetScaler de l'exécuter en premier et vous ignorez toutes les autres politiques qui pourraient également correspondre. Vous pouvez vous laisser suffisamment de marge de manœuvre pour ajouter d'autres politiques dans n'importe quel ordre, sans avoir à réattribuer des priorités, en définissant des priorités avec des intervalles de 50 ou 100 entre chaque politique lorsque vous liez vos politiques de manière globale.

Remarque : Les politiques de transformation d'URL ne peuvent pas être liées à des serveurs virtuels basés sur TCP.

Pour lier une politique de transformation d'URL à l'aide de la ligne de commande NetScaler

À l'invite de commandes NetScaler, tapez les commandes suivantes pour lier globalement une politique de transformation d'URL et vérifier la configuration :

- `bind transform global <policyName> <priority>`
- `show transform global`

Exemple :

```
1 > bind transform global polisearching 100
2  Done
3 > show transform global
4 1)      Policy Name: polisearching
5         Priority: 100
6
7  Done
8 <!--NeedCopy-->
```

Pour lier une politique de transformation d'URL à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez Réécrire, puis développez Transformation d'URL, puis cliquez sur **Politiques.
2. Dans le volet d'informations, cliquez sur **Gestionnaire de stratégies**.

3. Dans la boîte de dialogue **Transform Policy Manager**, choisissez le point de liaison auquel vous souhaitez lier la politique**. Les choix sont les suivants :
    - **Remplacez Global.** Les politiques liées à ce point de liaison traitent l'ensemble du trafic provenant de toutes les interfaces de l'appliance NetScaler et sont appliquées avant toute autre politique.
    - **Serveur virtuel LB.** Les politiques liées à un serveur virtuel d'équilibrage de charge sont appliquées uniquement au trafic traité par ce serveur virtuel d'équilibrage de charge et sont appliquées avant toute politique globale par défaut. Après avoir sélectionné le serveur virtuel LB, vous devez également sélectionner le serveur virtuel d'équilibrage de charge spécifique auquel vous souhaitez lier cette politique.
    - **Serveur virtuel CS.** Les politiques liées à un serveur virtuel de commutation de contenu sont appliquées uniquement au trafic traité par ce serveur virtuel de commutation de contenu et sont appliquées avant toute politique globale par défaut. Après avoir sélectionné CS Virtual Server, vous devez également sélectionner le serveur virtuel de commutation de contenu spécifique auquel vous souhaitez lier cette politique.
    - **Global par défaut.** Les politiques liées à ce point de liaison traitent l'ensemble du trafic provenant de toutes les interfaces de l'appliance NetScaler.
    - **Libellé de politique.** Les politiques liées à une étiquette de stratégie traitent le trafic que l'étiquette de stratégie leur achemine. L'étiquette de politique contrôle l'ordre dans lequel les politiques sont appliquées à ce trafic.
4. Sélectionnez Insérer une politique pour insérer une nouvelle ligne et afficher une liste déroulante répertoriant toutes les politiques de transformation d'URL indépendantes disponibles.
5. Sélectionnez la politique que vous souhaitez lier ou sélectionnez Nouvelle stratégie pour créer une nouvelle politique. La politique que vous avez sélectionnée ou créée est insérée dans la liste des politiques de transformation d'URL liées globalement.
6. Apportez tous les ajustements supplémentaires à la reliure.
    - Pour modifier la priorité de la stratégie, cliquez sur le champ pour l'activer, puis tapez une nouvelle priorité. Vous pouvez également sélectionner Régénérer les priorités pour renuméroter les priorités uniformément.
    - Pour modifier l'expression de politique, double-cliquez sur ce champ pour ouvrir la boîte de dialogue Configurer la politique de transformation, dans laquelle vous pouvez modifier l'expression de politique.
    - Pour définir l'expression Goto, double-cliquez sur le champ dans l'en-tête de colonne Goto Expression pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression.
    - Pour définir l'option Invoquer, double-cliquez sur le champ dans l'en-tête de la colonne Invoquer pour afficher la liste déroulante dans laquelle vous pouvez choisir une expression.
7. Répétez les étapes 3 à 6 pour ajouter les politiques de transformation d'URL supplémentaires

que vous souhaitez lier globalement.

8. Cliquez sur **OK** pour enregistrer vos modifications. Un message apparaît dans la barre d'état indiquant que la stratégie a été configurée avec succès.

Support RADIUS pour la fonctionnalité de réécriture

May 5, 2023

Le langage d'expressions NetScaler inclut des expressions permettant d'extraire des informations des messages RADIUS et de les manipuler dans les requêtes et les réponses. Ces expressions vous permettent d'utiliser la fonction de réécriture pour modifier des parties d'un message RADIUS avant de l'envoyer à sa destination. Vos politiques et actions de réécriture peuvent utiliser n'importe quelle expression appropriée ou pertinente pour un message RADIUS. Les expressions disponibles vous permettent d'identifier le type de message RADIUS, d'extraire toute paire attribut-valeur (AVP) de la connexion et de modifier les AVP RADIUS. Vous pouvez également créer des étiquettes de politique pour les connexions RADIUS.

Vous pouvez utiliser les nouvelles expressions RADIUS dans les règles de réécriture à différentes fins. Par exemple, vous pouvez :

- Supprimez la partie domaine \ du nom d'utilisateur RADIUS AVP pour simplifier l'authentification unique (SSO).
- Insérez un AVP spécifique au fournisseur, tel que le champ MSISDN utilisé dans les opérations de la compagnie de téléphone pour contenir les informations sur les abonnés.

Vous pouvez également créer des étiquettes de politique pour acheminer des types spécifiques de demandes RADIUS par le biais d'une série de politiques adaptées à ces demandes.

> **Remarque** :
>
> RADIUS for Rewrite présente les limites suivantes :

- NetScaler ne signe pas à nouveau les demandes ou réponses RADIUS réécrites. Si le serveur d'authentification RADIUS requiert des messages RADIUS signés, l'authentification échouera.
- Les expressions RADIUS actuellement disponibles ne fonctionnent pas avec les attributs IPv6 de RADIUS.

La documentation de NetScaler relative aux expressions qui prennent en charge RADIUS suppose une connaissance de la structure et de l'objectif de base des communications RADIUS. Si vous avez besoin de plus amples informations sur RADIUS, consultez la documentation de votre serveur RADIUS ou recherchez en ligne une introduction au protocole RADIUS.

Configuration des politiques de réécriture pour RADIUS

La procédure suivante utilise la ligne de commande NetScaler pour configurer une action et une politique de réécriture et lier la politique à un point de liaison global spécifique à la réécriture.

Pour configurer une action et une politique de réécriture, et lier la politique,procédez comme suit :

À l'invite de commandes, tapez les commandes suivantes :

- `add rewrite action <actName> <actType>`
- `add rewrite policy <polName> <rule> <actName>`
- `bind rewrite policy <polName> <priority> <nextExpr> -type <bindPoint>` où `<bindPoint>` représente l'un des points de liaison globaux spécifiques à la réécriture.

Expressions RADIUS pour la réécriture

Dans une configuration de réécriture, vous pouvez utiliser les expressions NetScaler suivantes pour faire référence à différentes parties d'une demande ou d'une réponse RADIUS.

Identification du type de connexion :

- `RADIUS.IS_CLIENT`

  Renvoie TRUE si la connexion est un message client RADIUS (demande).

- `RADIUS.IS_SERVER`

  Renvoie TRUE si la connexion est un message de serveur RADIUS (réponse).

Expressions de demande :

- `RADIUS.REQ.CODE`

  Renvoie le numéro qui correspond au type de demande RADIUS. Un dérivé de la classe num_at. Par exemple, une demande d'accès RADIUS renverrait 1 (un). Une demande de comptabilité RADIUS renverrait 4.

- `RADIUS.REQ.LENGTH`

  Renvoie la longueur de la requête RADIUS, y compris l'en-tête. Un dérivé de la classe num_at.

- `RADIUS.REQ.IDENTIFIER`

  Renvoie l'identifiant de demande RADIUS, un numéro attribué à chaque demande qui permet de faire correspondre la demande à la réponse correspondante. Un dérivé de la classe num_at.

- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`

Renvoie la valeur de la première occurrence de cet AVP sous la forme d'une chaîne de type text_t.

- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`

  Renvoie l'instance spécifiée de l'AVP sous la forme d'une chaîne de type RAVP_t. Un AVP RADIUS spécifique peut apparaître plusieurs fois dans un message RADIUS. INSTANCE (0) renvoie la première instance, INSTANCE (1) renvoie la deuxième instance, et ainsi de suite, jusqu'à seize instances.

- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`

  Renvoie la valeur de l'instance spécifiée de l'AVP sous forme de chaîne de type text_t.

- `RADIUS.REQ.AVP(<AVP code no>).COUNT`

  Renvoie le nombre d'instances d'un AVP spécifique dans une connexion RADIUS, sous forme d'entier.

- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`

  Renvoie TRUE si le type d'AVP spécifié existe dans le message, ou FALSE dans le cas contraire.

Expressions de réponse :

Les expressions de réponse RADIUS sont identiques aux expressions de demande RADIUS, sauf que RES remplace REQ.

Typecasts des valeurs AVP :

L'ADC prend en charge les expressions permettant de convertir les valeurs RADIUS AVP sous forme de texte, d'entier, d'entier non signé, de type long, de type long non signé, d'adresse ipv4, d'adresse ipv6, de préfixe ipv6 et de types de données temporelles. La syntaxe est la même que pour les autres expressions NetScaler typecast.

Exemple :

L'ADC prend en charge les expressions permettant de convertir les valeurs RADIUS AVP sous forme de texte, d'entier, d'entier non signé, de type long, de type long non signé, d'adresse ipv4, d'adresse ipv6, de préfixe ipv6 et de types de données temporelles. La syntaxe est la même que pour les autres expressions NetScaler typecast.

```
1 RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
2 <!--NeedCopy-->
```

Expressions de type AVP :

NetScaler prend en charge les expressions permettant d'extraire les valeurs RADIUS AVP à l'aide des codes entiers assignés décrits dans les RFC2865 et RFC2866. Vous pouvez également utiliser des alias de texte pour effectuer la même tâche. Voici quelques exemples.

- `RADIUS.REQ.AVP (1).VALUE or RADIUS.REQ.USERNAME.value`

  Extrait la valeur du nom d'utilisateur RADIUS.

- `RADIUS.REQ.AVP (4). VALUE or RADIUS.REQ. ACCT\\_SESSION\\_ID.value`

  Extrait le Acct-Session-ID AVP (code 44) du message.

- `RADIUS.REQ.AVP (26). VALUE or RADIUS.REQ.VENDOR\\_SPECIFIC.VALUE`

  Extrait la valeur spécifique au fournisseur.

Les valeurs des AVP RADIUS les plus couramment utilisées peuvent être extraites de la même manière.

Points de liaison RADIUS :

Quatre points de liaison globaux sont disponibles pour les politiques contenant des expressions RADIUS.

- `RADIUS_REQ_OVERRIDE`

  File d'attente des politiques relatives aux demandes de priorité/de dérogation.

- `RADIUS_REQ_DEFAULT`

  File d'attente de règles de demande standard.

- `RADIUS_RES_OVERRIDE`

  File d'attente des politiques de priorité/d'annulation des réponses.

- `RADIUS_RES_DEFAULT`

  File d'attente de politiques de réponse standard.

Expressions spécifiques à la réécriture RADIUS :

- `RADIUS.NEW_AVP`

  Renvoie le RADIUS AVP spécifié sous forme de chaîne.

- `RADIUS.NEW_AVP_INTEGER32`

  Renvoie le RADIUS AVP spécifié sous la forme d'un entier.

- `RADIUS.NEW_AVP_UNSIGNED32`

  Renvoie le RADIUS AVP spécifié sous la forme d'un entier non signé.

- `RADIUS.NEW_VENDOR_SPEC_AVP(<ID>, <definition>)`

  Ajoute les AVP étendus spécifiques au fournisseur à la connexion. Remplacez par un nombre long. `<ID>` Remplacez par une chaîne contenant les données de l'AVP. `<definition>`

- `RADIUS.REQ.AVP_START`

Renvoie l'emplacement entre la fin de l'en-tête RADIUS et le début des AVP. Utilisé dans les actions de réécriture.

Exemple :

```
1     add rewrite action insert1 insert_after radius.req.avp_start radius
          .new_avp(33, "NEW AVP")
2 <!--NeedCopy-->
```

- RADIUS.REQ.AVP_END

  Renvoie l'emplacement à la fin du message Radius (ou en d'autres termes, fin de tous les AVP) dans le message Radius. Utilisé lors de l'exécution d'actions de réécriture.

  Exemple :

```
1     add rewrite action insert2 insert_before radius.req.avp_end "radius
          .new_avp(33, "NEW AVP")"
2 <!--NeedCopy-->
```

- RADIUS.REQ.AVP_LIST

  Renvoie l'emplacement au début des AVP dans un message RADIUS, ainsi que la longueur du message RADIUS, à l'exclusion de l'en-tête. En d'autres termes, renvoie tous les AVP dans un message RADIUS. Utilisé pour effectuer des actions de réécriture.

  Exemple :

```
1     add rewrite action insert3 insert_before_all radius.req.avp_list "
          radius.new_avp(33, "NEW AVP")" -search "avp(33)"
2 <!--NeedCopy-->
```

Types d'actions de réécriture valides pourRADIUS :

Les types d'actions de réécriture qui peuvent être utilisés avec les expressions RADIUS sont les suivants :

- INSERT_AFTER
- INSERT_BEFORE
- INSERT_AFTER_ALL
- INSERT_BEFORE_ALL
- SUPPRIMER
- DELETE_ALL
- REMPLACER
- REPLACE_ALL

Tous `INSERT_ actions` peuvent être utilisés pour insérer un RADIUS AVP dans une connexion RADIUS.

Cas d'utilisation

Vous trouverez ci-dessous des cas d'utilisation de RADIUS avec réécriture.

Réécriture du nom d'utilisateur AVP

Pour configurer la fonctionnalité de réécriture afin de supprimer le domaine \ string du nom d'utilisateur RADIUS AVP, commencez par créer une action de réécriture REPLACE comme indiqué dans l'exemple ci-dessous. Utilisez cette action dans une politique de réécriture qui sélectionne toutes les demandes RADIUS. Liez la politique à un point de liaison global. Pour ce faire, définissez le niveau de priorité approprié pour permettre aux politiques de blocage ou de rejet d'entrer en vigueur en premier, tout en veillant à ce que toutes les demandes qui ne sont pas bloquées ou rejetées soient réécrites. Définissez l'expression Goto (GoToPriorityExpr) sur NEXT pour poursuivre l'évaluation de la politique et attachez la politique à la file d'attente RADIUS_REQ_DEFAULT.

Exemple :

```
1 add rewrite action rwActRadiusDomainDel replace radius.req.user_name q/
     RADIUS.NEW_AVP(1,RADIUS.REQ.USER_NAME.VALUE.AFTER_STR(" "))/
2 add rewrite policy RadiusRemoveDomainPol true rwActRadiusDomainDel
3 <!--NeedCopy-->
```

> **Remarque** :
>
> La politique de réécriture pour RADIUS ne s'applique pas à un serveur virtuel de passerelle. Si un serveur virtuel de passerelle est utilisé comme équilibrage de charge, RADIUS doit être configuré et la politique de réécriture doit être liée à un serveur virtuel d'équilibrage de charge RADIUS.

Insertion d'un AVP spécifique au fournisseur

Pour configurer l'action de réécriture afin d'insérer un AVP spécifique au fournisseur contenant le contenu du champ MSISDN, commencez par créer une action de réécriture INSERT qui insère le champ MSISDN dans la demande. Utilisez l'action dans une politique de réécriture qui sélectionne toutes les demandes RADIUS. Liez la politique à globale, en définissant la priorité à un niveau approprié et les autres paramètres, comme indiqué dans l'exemple suivant.

Exemple :

```
1 add rewrite action rwActRadiusInsMSISDN insert_after radius.req.
     avp_start RADIUS.NEW_VENDOR_SPEC_AVP(<VENDOR ID>, "RADIUS.NEW_AVP(<
     Attribute Code>, <MSISDN>)")
2 add rewrite policy rwPolRadiusInsMSISDN true rwActRadiusInsMSISDN
3 bind rewrite global rwPolRadiusInsMSISDN 100 NEXT -type
     RADIUS_REQ_DEFAULT
```



```
<!--NeedCopy-->
```

Prise en charge de Diameter pour la réécriture

May 8, 2023

La fonction de réécriture prend désormais en charge le protocole Diameter. Vous pouvez configurer Rewrite pour modifier les requêtes et les réponses Diameter comme vous le feriez pour les requêtes et réponses HTTP ou TCP, ce qui vous permet d'utiliser Rewrite pour gérer le flux des demandes Diameter et apporter les modifications nécessaires. Par exemple, si la valeur « Origin-Host » d'une requête Diameter n'est pas appropriée, vous pouvez utiliser Rewrite pour la remplacer par une valeur acceptable pour le serveur Diameter.

Pour configurer Rewrite afin de modifier une demande Diameter

Pour configurer la fonction de réécriture afin de remplacer l'hôte d'origine dans une demande de diamètre par une valeur différente, à l'invite de commandes, tapez les commandes suivantes :

- <actname><add rewrite action \ <actname> replace « DIAMETER.REQ.AVP (264, \ \" Netscaler.example.net \ \ ») » Par \, remplacez « DIAMETER.REQ.AVP (264, \ \" Netscaler.example.net \ \ ») » par \, remplacez votre nouvelle action par un nom.
  Le nom peut comporter de 1 à 127 caractères et peut contenir des lettres, des chiffres ainsi que les symboles de tiret (-) et de trait de soulignement (\ _). Pour Netscaler.example.net, remplacez le nom d'hôte d'origine par le nom d'hôte d'origine.
- <actname> <polname>ajoutez une politique de réécriture \ <polname> « diameter.req.avp (264) .value.eq (\ \" host.example.com \ \ ») » \ Pour \, remplacez votre nouvelle politique par un nom. Comme pour \ <actname>, le nom peut comporter de 1 à 127 caractères et peut contenir des lettres, des chiffres ainsi que les symboles de tiret (-) et de trait de soulignement (\ _). Pour host.example.com, remplacez le nom de l'origine de l'hôte que vous souhaitez modifier. Par \ <actname>, remplacez le nom de l'action que vous venez de créer.
- bind lb vserver \ <vservername> -PolicyName \ <polname> -priority \ <priority> -type REQUEST Pour \ <vservername>, remplacez le nom du serveur virtuel d'équilibrage de charge auquel vous souhaitez lier la politique. Par \ <polname>, remplacez le nom de la politique que vous venez de créer. Pour \ <priority>, remplacez la politique par une priorité.

Exemple :

Pour créer une action et une politique de réécriture afin de modifier toutes les origines d'hôtes Diameter de « host.example.com » en « Netscaler.example.net », vous pouvez ajouter l'action et la politique suivantes, puis lier la politique comme indiqué.


```
> add rewrite action rw_act_replace_avp replace "diameter.req.avp(264)"
    "diameter.new.avp(264,"NetScaler.example.net")"
> add rewrite policy rw_diam_pol "diameter.req.avp(264).value.eq("
    client.realm2.net")" rw_act_replace_avp
> bind lb vserver vs1 -policyName rw_diam_pol -priority 10 -type
    REQUEST

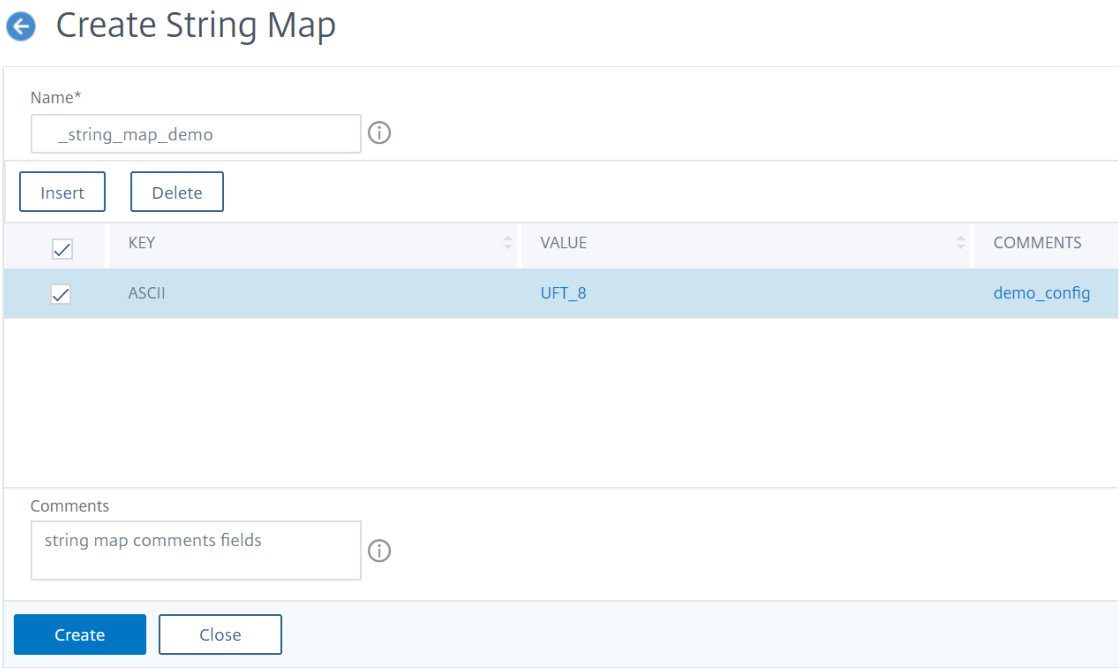
Done
<!--NeedCopy-->
```

Prise en charge DNS de la fonction de réécriture

May 5, 2023

Vous pouvez configurer la fonctionnalité de réécriture pour modifier les requêtes et les réponses DNS, comme vous le feriez pour les requêtes et les réponses HTTP ou TCP. Vous pouvez utiliser la réécriture pour gérer le flux des requêtes DNS et apporter les modifications nécessaires à l'en-tête ou à la section des réponses. Par exemple, si le bit AA de la réponse DNS n'est pas défini dans l'indicateur d'en-tête, vous pouvez utiliser la réécriture pour définir le bit AA dans la réponse DNS et l'envoyer au client.

Expressions DNS

Dans une configuration de réécriture, vous pouvez utiliser les expressions NetScaler suivantes pour faire référence à différentes parties d'une demande ou d'une réponse DNS :

Voir Expressions et descriptions

Points de liaison DNS

Les points de liaison globaux suivants sont disponibles pour les politiques qui contiennent des expressions DNS.

Points de liaison	Description
DNS_REQ_OVERRIDE	Ignorez la file d'attente des politiques de demande.
DNS_REQ_DEFAULT	File d'attente de règles de demande standard.
DNS_RES_OVERRIDE	Ignorez la file d'attente des politiques de réponse.

Points de liaison	Description
DNS_RES_DEFAULT	File d'attente de politiques de réponse standard.

Outre les points de liaison par défaut, vous pouvez créer des étiquettes de politique de type DNS_REQ ou DNS_RES et y lier des politiques DNS.

Types d'actions de réécriture pour le DNS

- **replace_dns_answer_section —Cette action remplace la section**des réponses DNS par l'expression définie dans la politique DNS.
- **replace_dns_header_field —Vérifie**le type d'opcode dans la requête DNS. Renvoie True ou False, indiquant si le type d'opcode dans la requête DNS correspond au type d'opcode spécifié. Cette action remplace la section d'en-tête DNS par l'expression définie dans la politique DNS.

Configuration des politiques de réécriture pour le DNS

La procédure suivante utilise la ligne de commande NetScaler pour configurer une action et une politique de réécriture et lier la politique à un point de liaison global spécifique à la réécriture.

Configurer l'action et la politique de réécriture, et lier la politique au DNS

À l'invite de commandes, tapez les commandes suivantes :

1. `add rewrite action <actName> <actType>`

   Pour `<actname>`, remplacez votre nouvelle action par un nom. Le nom peut comporter entre 1 et 127 caractères et peut contenir des lettres, des chiffres, des traits d'union (-) et des traits de soulignement (_). Pour `<actType>`, spécifiez les types d'actions de réécriture fournis pour les expressions DNS.

2. `add rewrite policy <polName> <rule> <actName>`

   Par `<polname>`, remplacez votre nouvelle politique par un nom. Car `<actname>`, le nom peut comporter entre 1 et 127 caractères et peut contenir des lettres, des chiffres, des traits d'union (-) et des traits de soulignement (_). Remplacez par le nom de l'action que vous venez de créer. `<actname>`

3. `bind rewrite global <polName> <priority> <gotoPriorityExpression> -type <bindPoint>`

Remplacez par le nom de la politique que vous venez de créer. <polName> Pour <priority>, spécifiez la priorité de la politique. Par <bindPoint>, remplacez l'un des points de liaison globaux spécifiques à la réécriture.

Exemple :

Définissez le bit AA de la requête DNS pour équilibrer la charge du serveur virtuel.

Les commandes suivantes configurent l'appliance NetScaler pour qu'elle agisse en tant que serveur DNS faisant autorité pour toutes les requêtes qu'elle traite.

```
1 add rewrite action set_aa replace_dns_header_field dns.req.header.flags
     .set(aa)
2 add rewrite policy pol !dns.req.header.flags.is_set(aa)  set_aa
3 bind rewrite global  pol  100  -type dns_res_override
4 <!--NeedCopy-->
```

Modifiez la réponse et la section d'en-tête.

Si le serveur répond avec un domaine NX, vous pouvez définir l'action de réécriture pour remplacer la réponse par l'adresse IP spécifiée. Un NOPOLICY-REWRITE vous permet d'appeler une banque externe sans traiter d'expression (une règle). Cette entrée est une politique fictive qui ne contient pas de règle mais dirige l'entrée vers une étiquette de politique ou des banques de politiques spécifiques à un serveur virtuel.

```
1 add rewrite action set_aa_res replace_dns_header_field "dns.res.header.
     flags.set(aa)"
2 add rewrite action modify_nxdomain_res replace_dns_answer_section "dns.
     new_rrset_a("10.102.218.160",300)"
3 add rewrite policy set_res_aa true set_aa_res
4 add add rewrite policy modify_answer "dns.RES.HEADER.RCODE.EQ(nxdomain)
      && dns.RES.QUESTION.TYPE.EQ(A)"
5 modify_nxdomain_res
6 add rewrite policylabel MODIFY_NODATA dns_res
7 bind rewrite policylabel MODIFY_NODATA modify_answer 10 END
8 bind rewrite policylabel MODIFY_NODATA set_res_aa 11 END
9 bind lb vserver v1 -policyName NOPOLICY-REWRITE -priority 11 -
     gotoPriorityExpression END -type
10 RESPONSE -invoke policylabel MODIFY_NODATA
11 <!--NeedCopy-->
```

Limites :

- Les politiques de réécriture ne sont évaluées que si l'appliance NetScaler est configurée en tant que serveur proxy DNS et qu'il y a un échec de cache.

- Si l'indicateur de récursivité disponible (RA) dans l'en-tête est défini sur OUI, l'indicateur RA ne sera pas modifié lors des réécritures.
- Si l'indicateur RA dans l'en-tête est défini sur YES, l'indicateur CD dans l'en-tête est modifié indépendamment de toute action de réécriture.

Prise en charge MQTT pour la réécriture

May 5, 2023

La fonction de réécriture prend en charge le protocole MQTT. Vous pouvez configurer des stratégies de réécriture pour effectuer des actions en fonction des paramètres des demandes du client MQTT et des réponses du serveur.

Action de réécriture pour MQTT

L'action de réécriture pour MQTT indique les modifications apportées à la demande ou à la réponse MQTT avant de l'envoyer à un serveur ou un client.

Expression :

```
add rewrite action <name> <rewrite_type> <target> <rewrite_action>
```

Type de réécriture pour MQTT

Selon le type de règle d'expression de réécriture utilisé, les types de réécriture MQTT suivants sont pris en charge :

- `replace_mqtt`
- `insert_before_mqtt`
- `insert_after_mqtt`
- `delete_mqtt`
- `insert_mqtt`

Cible de réécriture pour MQTT

Dans les exemples suivants, la fonctionnalité de réécriture MQTT utilise des expressions de stratégie pour indiquer la partie de la demande à modifier (cible) et la modification à effectuer (expression chaîne) :

- Réécrivez un ID client dans le paquet de connexion à l'aide du type `replace_mqtt` d'action.

  ```
  add rewrite action rwact1 replace_mqtt MQTT.CONNECT.CLIENTID "\"xyz\""
  ```


- Réécrivez une rubrique dans la demande de publication à l'aide du type `replace_mqtt` d'action.

  ```
  add rewrite action rwact1 replace_mqtt MQTT.PUBLISH.TOPIC "\"testing/
  test123\""
  ```

- Réécrivez pour insérer une propriété à l'aide du type d'action insert_mqtt.

  ```
  add rewrite action rwact1 insert_mqtt MQTT.NEW_PROPERTY("prop1", "test"
  )
  ```

- Supprimez une rubrique à l'aide du type d'action delete_mqtt.

  ```
  add rewrite action rwact2 delete_mqtt MQTT.SUBSCRIBE.TOPIC_FILTERS.
  TOPIC(1)
  ```

Action de réécriture pour MQTT

Voici les actions de réécriture prédéfinies pour MQTT :

- `MQTT.NEW_KEEPALIVE(interval)`
- `MQTT.NEW_PACKET_IDENTIFIER(packetID)`
- `MQTT.NEW_REASON_CODE(retCode)`
- `MQTT.NEW_PUBLISH(topic_name, payload)`
- `MQTT.NEW_CONNECT_USERNAME(username)`
- `MQTT.NEW_CONNECT_WILL_MESSAGE(will_topic, will_payload, will_Qos, will_retain)`
- `MQTT.NEW_TOPIC(topic, qos)`
- `MQTT.NEW_TOPIC(topic)`
- `MQTT.NEW_PROPERTY(key, value)`

Exemple pour l'action de réécriture prédéfinie :

```
add rewrite action rwact1 replace_mqtt MQTT.CONNECT.KEEPALIVE MQTT.NEW_KEEPALIVE
(90)
```

Exemple d'action de réécriture définie par l'utilisateur :

```
add rewrite action rwact1 replace_mqtt MQTT.CONNECT.USERNAME "\"user1\""
```

Politique de réécriture pour MQTT

Une stratégie de réécriture pour MQTT se compose d'une règle et d'une action. La règle détermine le trafic MQTT auquel la réécriture est appliquée et l'action détermine l'action à effectuer par l'appliance NetScaler.

Expression :


```
add rewrite policy <name> <rewrite_rule> <rewrite_action>
```

Exemple :

```
add rewrite action insert_mqtt_username insert_mqtt MQTT.NEW_CONNECT_USERNAME
("user1")

add rewrite policy rewrite_mqtt_username "MQTT.COMMAND.EQ(CONNECT)&& MQTT.
CONNECT.USERNAME.LENGTH.EQUALS(0)insert_mqtt_username
```

Points de liaison pour MQTT

Vous pouvez lier une stratégie de réécriture globalement ou à un serveur virtuel d'équilibrage de charge ou à un serveur virtuel de commutation de contenu spécifique.
Les points de liaison globaux sont les suivants :

- MQTT_REQ_DEFAULT
- MQTT_REQ_OVERRIDE
- MQTT_RES_DEFAULT
- MQTT_RES_OVERRIDE

Expression :

- `bind rewrite global <policyName> <priority> [-type MQTT_REQ_OVERRIDE | MQTT_REQ_DEFAULT | MQTT_RES_OVERRIDE | MQTT_RES_DEFAULT]`
- `bind lb|cs vserver <virtualServerName> -policyName <policyName> -priority <positiveInteger> -type REQUEST|RESPONSE`

Exemple :

- `bind rewrite global pol1 10 -type MQTT_REQ_DEFAULT`
- `add/bind lb vserver v1 -policyName pol1 -type reqUEST -priority 10`

Configurer une stratégie de réécriture pour MQTT

Pour configurer une stratégie de réécriture, suivez les étapes et tapez les commandes à l'invite de commandes :

1. Activez la fonctionnalité de réécriture sur l'appliance NetScaler.

   ```
   enable ns feature REWRITE
   ```

2. Ajoutez une action de réécriture.

   ```
   add rewrite action rwact1 replace_mqtt MQTT.CONNECT.KEEPALIVE MQTT.
   NEW_KEEPALIVE(10)
   ```


3. Ajoutez une stratégie de réécriture.

   ```
   add rewrite policy pol1 MQTT.COMMAND.EQ(CONNECT)rwact1
   ```

4. Configurez un serveur virtuel d'équilibrage de charge MQTT.

   ```
   add lb vserver v1 MQTT 1.1.1.1 1883
   ```

5. Liez la stratégie de réécriture globalement ou à un serveur virtuel d'équilibrage de charge spécifique.

   ```
   bind rewrite global pol1 10 -type MQTT_REQ_DEFAULT
   ```

   ```
   add/bind lb vserver v1 -policyName pol1 -type REQUEST -priority 10
   ```

Cas d'utilisation 1 : remplacez le nom d'utilisateur dans le message MQTT CONNECT par le nom du certificat

L'administrateur peut configurer une stratégie de réécriture MQTT pour remplacer le nom d'utilisateur par le nom du certificat du client.

Prenons un exemple. La demande du client contient un `MQTT CONNECT` message contenant le nom d'utilisateur « admin ». Ce nom d'utilisateur doit être remplacé par le numéro de série (16 chiffres) extrait du certificat client (nom du certificat).

La figure suivante montre le flux de travail :



1. Une demande TCP (Transport Control Protocol) est envoyée à l'équilibreur de charge.
2. Dans l'équilibreur de charge, le nom d'utilisateur est remplacé par le nom du certificat.
3. La demande est transmise au courtier MQTT.
4. Ce nouveau nom d'utilisateur est utilisé pour l'autorisation via la charge utile du webhook.

Exemple de configuration :

```
add rewrite action mqtt_rw_unameact1 replace_mqtt MQTT.CONNECT.USERNAME
CLIENT.SSL.CLIENT_CERT.SERIALNUMBER
```

```
add rewrite policy mqtt_rw_uname_pol1 "MQTT.COMMAND.EQ(CONNECT)"mqtt_rw_unameact1
```

```
bind cs vserver mqtt_frontend_cs -policyName mqtt_rw_uname_pol1 -priority
10 -gotoPriorityExpression END -type REQUEST
```


Cas d'utilisation 2 : Fournir un abonnement à un nouveau TOPIC

L'administrateur peut fournir un abonnement à un nouveau TOPIC. Prenons un exemple. Une demande client est associée à un abonnement au TOPIC 1. L'administrateur peut configurer une stratégie de réécriture pour fournir un abonnement à un nouveau TOPIC 2. L'abonnement peut être inséré avant ou après.

Exemple de configuration :

- `add rewrite action act2 insert_before_mqtt MQTT.TOPIC_FILTERS.TOPIC(1) MQTT.NEW_TOPIC(topic2, 2)`
- `add rewrite policy policy2 "MQTT.COMMAND.EQ(SUBSCRIBE)&& MQTT.SUBSCRIBE. TOPIC_FILTERS.TOPIC.CONTAINS(\"test\")"act2`

Cartes à cordes

May 5, 2023

Vous pouvez utiliser des mappages de chaînes pour effectuer la mise en correspondance de modèles dans toutes les fonctionnalités de NetScaler qui utilisent la syntaxe de politique par défaut. Une carte de chaînes est une entité NetScaler composée de paires clé-valeur. Les clés et les valeurs sont des chaînes au format ASCII ou UTF-8. La comparaison de chaînes utilise deux nouvelles fonctions, `MAP_STRING(<string_map_name>)` et `IS_STRINGMAP_KEY(<string_map_name>)`.

Une configuration de stratégie qui utilise des mappages de chaînes fonctionne mieux qu'une configuration qui effectue une correspondance de chaînes via des expressions de stratégie, et vous avez besoin de moins de stratégies pour effectuer une correspondance de chaînes avec un grand nombre de paires clé-valeur. Les String Maps sont également intuitifs, simples à configurer et se traduisent par une configuration plus petite.

Fonctionnent les String Maps

Les mappages de chaînes ont une structure similaire aux jeux de motifs (un jeu de motifs définit un mappage des valeurs d'index avec des chaînes ; un mappage de chaînes définit un mappage de chaînes avec des chaînes de caractères) et les commandes de configuration des mappages de chaînes (commandes telles que add, bind, unbind, remove et show) sont syntaxiquement similaires à la configuration commandes pour les jeux de motifs. De plus, comme pour les valeurs d'index d'un jeu de motifs, chaque clé d'une carte de chaînes doit être unique sur la carte. Le tableau suivant illustre un mappage de chaînes appelé url_string_map, qui contient des URL sous forme de clés et de valeurs.

Clé	Valeur
/url_1.html	http://www.redirect_url_1.com/url_1.html
/url_2.html	http://www.redirect_url_2.com/url_2.html
/url_3.html	http://www.redirect_url_1.com/url_1.html

Tableau 1. String Map « url_string_map »

Le tableau suivant décrit les deux fonctions qui ont été introduites pour activer la correspondance de chaînes avec des clés dans un mappage de chaînes. La correspondance des chaînes est toujours effectuée avec les clés. En outre, les fonctions suivantes effectuent une comparaison entre les clés du mappage de chaînes et la chaîne complète renvoyée par le préfixe d'expression. Les exemples dans les descriptions se réfèrent à l'exemple précédent.

Pour obtenir des informations complètes sur les deux fonctions introduites pour activer la correspondance de chaînes avec des clés dans une carte de chaînes, reportez-vous au tableau des fonctions de carte de chaînes pdf.

Configuration d'un mappage de chaînes

Vous créez d'abord une carte de chaînes, puis vous y liez des paires clé-valeur. Vous pouvez créer un mappage de chaînes à partir de l'interface de ligne de commande (CLI) ou de l'utilitaire de configuration.

Pour configurer un mappage de chaînes à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

1. Créez une carte de chaînes.

```
add policy stringmap <name> -comment <string>
```

1. Liez une paire clé-valeur à la carte de chaînes.

```
bind policy stringmap <name> <key> <value> [-comment <string>]
```

Exemple :

```
1 bind policy stringmap url_string_map1 "/url_1.html" "http://www.
     redirect_url_1.com/url_1.html"
2 <!--NeedCopy-->
```


Pour configurer une carte de chaînes à l'aide de l'interface graphique NetScaler

Accédez à **AppExpert** > **String Maps**, cliquez sur **Ajouter** et spécifiez les détails pertinents.

Exemple : stratégie de répondeur avec une action de redirection

Le cas d'utilisation suivant implique une stratégie de répondeur avec une action de redirection. Dans l'exemple ci-dessous, les quatre premières commandes créent la carte de chaînes url_string_map et lient les trois paires clé-valeur utilisées dans l'exemple précédent. Après avoir créé la carte et lié les paires clé-valeur, vous créez une action de répondeur (act_url_redirects) qui redirige le client vers l'URL correspondante dans la carte de chaînes ou vers www.default.com. Vous configurez également une stratégie de répondeur (pol_url_redirects) qui vérifie si les URL demandées correspondent à l'une des clés de url_string_map, puis exécute l'action configurée. Enfin, vous liez la stratégie de répondeur au serveur virtuel de commutation de contenu qui reçoit les demandes des clients qui doivent être évaluées.

```
add stringmap url_string_map

bind stringmap url_string_map /url_1.html http://www.redirect_url_1.com/
url_1.html

bind stringmap url_string_map /url_2.html http://www.redirect_url_2.com/
url_2.html

bind stringmap url_string_map /url_3.html http://www.redirect_url_1.com/
url_1.html
```

'Ajouter l'action du répondeur act_url_redirects rediriger 'HTTP.REQ.URL.MAP_STRING (« url_string_map ») ALT « www.default.com"'

```
add responder policy pol_url_redirects TRUE act_url_redirects

bind cs vserver csw_redirect -policyname pol_url_redirects -priority 1 -
type request
```

Pour configurer une carte de chaînes à l'aide de l'interface graphique NetScaler

Suivez la procédure ci-dessous pour configurer un mappage de chaînes.

1. Dans le volet de navigation, développez **AppExpert** et cliquez sur **String Maps**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Create String Map**, définissez les paramètres suivants :
   - Nom. Nom de la carte de chaînes.
   - Configurez la valeur de clé. Entrée de valeur de clé ASCII liée au mappage de chaînes

- Commentaires. Une brève description des valeurs clés liées à la carte de chaînes.

4. Cliquez sur **Créer** et **Fermer**.



Jeux d'URL

January 21, 2021

Cette fonctionnalité vous permet de mettre en liste noire un million d'URL. La section comprend les rubriques suivantes :

- Mise en route
- Utilisation des expressions de stratégie avancées pour l'évaluation d'URL
- Configuration d'un jeu d'URL
- Sémantique des modèles d'URL
- Catégories d'URL sur la liste noire

Mise en route

June 20, 2023

Pour empêcher l'accès à des sites Web restreints, une appliance NetScaler utilise un algorithme de correspondance d'URL spécialisé. L'algorithme utilise un ensemble d'URL qui peut contenir une liste

d'URL contenant jusqu'à 1 million (1 000 000) d'entrées bloquées. La limite globale est de 1 million d'entrées. Vous pouvez ajouter un ensemble d'URL contenant 1 million d'entrées ou plusieurs ensembles d'URL contenant un million d'entrées au total.

> **Remarque :**
>
> évitez d'utiliser de nombreux ensembles d'URL. Nous vous recommandons d'utiliser un nombre limité d'ensembles d'URL en fonction de la mémoire disponible pour le jeu d'URL.

Chaque entrée peut inclure des métadonnées qui définissent les catégories d'URL et les groupes de catégories en tant que modèles indexés. L'appliance peut également télécharger régulièrement des ensembles d'URL hautement sensibles gérés par les agences chargées de l'application des lois sur Internet (avec des sites Web gouvernementaux) ou des organisations Internet. Une fois que l'ensemble d'URL est téléchargé depuis un site Web et importé dans l'appliance, l'appliance chiffre les ensembles d'URL (comme l'exigent ces agences). Les ensembles d'URL cryptés restent confidentiels et les entrées ne sont pas altérées.

L'appliance NetScaler utilise des stratégies avancées pour déterminer si une URL entrante doit être bloquée, autorisée ou redirigée. Ces stratégies utilisent des expressions avancées pour évaluer les URL entrantes par rapport aux entrées figurant sur la liste noire. Une entrée peut inclure des métadonnées. Pour les entrées dépourvues de métadonnées, vous pouvez utiliser une expression qui évalue l'URL en fonction d'une correspondance de chaîne exacte. Pour les autres URL, vous pouvez utiliser une expression qui évalue les métadonnées de l'URL, en plus d'une expression qui vérifie la correspondance exacte de la chaîne.

Cas d'utilisation des stratégies d'accès Internet sécurisé pour les FAI et les opérateurs de télécommunications

Un ensemble d'URL permet à un fournisseur d'accès Internet (ISP) ou à un client de télécommunications de faire appliquer les stratégies d'accès Internet sécurisé imposées par le gouvernement, telles que :

1. Bloquer l'accès à des sites Internet illégaux (maltraitance d'enfants, drogues, etc.)
2. Navigation sécurisée pour les enfants

Une appliance NetScaler vous permet de télécharger régulièrement des ensembles d'URL gérés par les agences chargées de l'application des lois sur Internet ou par des organisations Internet indépendantes. L'appliance télécharge régulièrement la liste et la met à jour en toute sécurité. La liste est stockée sous forme d'ensembles d'URL confidentiels afin qu'elle ne soit pas falsifiée ou lisible par l'homme. L'ensemble d'URL téléchargé régulièrement fonctionne comme un ensemble sur liste noire à des fins d'évaluation des URL.

Si vous avez défini une URL privée et que le contenu de la liste reste confidentiel et que l'administrateur réseau ne connaît pas les URL figurant sur la liste noire présentes dans la liste. Pour vous assurer que

la stratégie est correctement configurée et que la bonne liste est référencée, vous devez configurer l'URL Canary et l'ajouter à l'ensemble d'URL. À l'aide de l'URL Canary, l'administrateur peut effectuer une demande via l'appliance et utilise l'URL privée définie pour s'assurer qu'elle est recherchée pour chaque demande d'URL.

Expressions de stratégie avancées pour l'évaluation d'URL

August 20, 2021

Le tableau suivant décrit les expressions que vous pouvez utiliser pour évaluer les URL entrantes avec des entrées dans un jeu d'URL.

Remarque : HTTP.REQ.URL est généralisé pour être utilisé comme <URL expression>

Expression.	Opération
<URL expression>.URLSET_MATCHES_ANY	Value TRUE si l'URL correspond exactement à n'importe quelle entrée du jeu d'URL.
<URL expression> .GET_URLSET_METADATA(<URLSET>)	L'expression GET_URLSET_METADATA() renvoie les métadonnées associées si l'URL correspond exactement à n'importe quel motif dans le jeu d'URL. Une chaîne vide est renvoyée s'il n'y avait pas de correspondance.
<URL expression> .GET_URLSET_METADATA(<URLSET>).EQ(<METADATA>	Evalue à TRUE si les métadonnées correspondantes sont égales à <METADATA>.
<URL expression> .GET_URLSET_METADATA(<URLSET>).TYPECAST_LIST_T(',').GET(0).EQ(<CATEGORY>)	Value TRUE si les métadonnées correspondantes sont au début de la catégorie. Ce modèle peut être utilisé pour encoder des champs distincts dans les métadonnées, mais correspondre uniquement au 1er champ.
HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)	Joigne les paramètres hôte et URL, qui peuvent ensuite être utilisés comme un <URL expression> pour la correspondance.

Configuration du jeu d'URL

May 5, 2023

Vous pouvez effectuer les tâches suivantes pour configurer un ensemble d'URL et restreindre les URL sur une plate-forme NetScaler :

1. Importez un ensemble d'URL (téléchargez-le et chiffrez-le). L'importation d'un ensemble d'URL dans une appliance NetScaler vous permet de :

- Pour télécharger le fichier URL.
- Pour ajouter le fichier à l'appliance.
- Pour crypter le fichier.
  Tant que vous n'avez pas ajouté l'URL définie au système, elle n'est pas visible pour l'utilisateur.

Vous pouvez télécharger un set des manières suivantes :

- Téléchargez un ensemble d'URL une fois depuis un serveur distant et spécifiez-le comme `http://myserver.com/file_with_urlset.csv`
- ajoutez un fichier sous le `/var/tmp/` chemin dans ADC et utilisez la commande, comme dans l'exemple :

```
> shell cat /var/tmp/test_urlset.csv
example.com
google.com
> import policy urlset top10
k -url local:test_urlset.csv -delimiter "," -rowSeparator "n" -interval
    10 -privateSet -canaryUrl http://www.in.gr
Done

<!--NeedCopy-->
```

L'ensemble d'URL importé est ensuite classé en différentes catégories et groupes de catégories dans la base de données. Cela n'est valable que si des catégories existent dans les métadonnées du fichier d'ensemble d'URL.

Remarque : Il est possible que vous ayez des modèles d'URL sans métadonnées.

Une fois que vous avez importé le fichier, vous pouvez mettre à jour, supprimer ou afficher les propriétés du fichier. Une fois le fichier introduit dans l'appliance, vous pouvez modifier les entrées en ajoutant d'autres lignes.

L'ensemble importé est ensuite stocké dans un format de fichier crypté dans le répertoire NetScaler. La liste importée contient des millions d'entrées d'URL. À la liste suivante : « La liste importée peut contenir jusqu'à 1 million d'entrées d'URL. Dans le cas contraire, l'appliance renvoie un message d'erreur

indiquant que la valeur dépasse la limite. Si l'ensemble d'URL importé contient des entrées sur liste noire contenant des métadonnées, celles-ci sont détectées par l'appliance lors de son importation.

Une fois que vous avez importé un ensemble d'URL et que vous l'avez ajouté à l'appliance, celui-ci est disponible pour les politiques avancées afin d'identifier le bon ensemble d'URL lors de l'évaluation des URL entrantes. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY(<URL set name>)`

1. Mise à jour d'une URL définie sur l'appliance NetScaler. Une fois que vous avez introduit le fichier dans l'appliance, vous pouvez, à cet intervalle, mettre à jour manuellement un fichier URL à l'aide de l'interface de ligne de commande.
2. Exportation d'un ensemble d'URL. Si vous préférez sauvegarder l'ensemble d'URL, vous pouvez exporter la liste des modèles d'URL et en enregistrer une copie dans une URL de destination. Avant d'exporter, vérifiez si l'ensemble d'URL est marqué comme privé. S'il est marqué comme privé, l'ensemble d'URL ne peut pas être exporté. La fonctionnalité d'exportation ne fonctionne pas avec un set privé. Ainsi, un nouvel ensemble d'URL `myurl` serait importé sans définition d'ensemble privé, puis il serait exporté vers un autre fichier dans un chemin local, comme ci-dessous :

```
> shell touch /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset.csv
example.com
google.com
Done
> export urlset myurl -url local:test_urlset_export.csv

> import urlset myurl -url local:test_urlset.csv
Done
(a non-private urlset is imported)

<!--NeedCopy-->
```

1. Suppression d'un ensemble d'URL. Si vous souhaitez supprimer un ensemble d'URL contenant des entrées sur liste noire, vous pouvez utiliser la commande remove pour supprimer l'ensemble d'URL de l'appliance NetScaler.
2. Affichage d'un ensemble d'URL. Vous pouvez afficher les propriétés d'un ensemble d'URL à l'aide de la commande show.

> **Remarque :** Les URL contenant une partie de requête sont supprimées lors de l'importation.

Exemple :


```
show urlset
Name: top100 PatternCount: 100 Delimiter:  RowSeparator: Interval: 0
Done
<!--NeedCopy-->
```

Importer un ensemble d'URL avec méta à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
import urlset <name> [-overwrite] [ - delimiter <character>] [-
    rowSeparator <character>] [-url] <url> [-interval <seconds>] [-
    privateSet] [-canaryUrl <URL>]
<!--NeedCopy-->
```

Où,

Le délimiteur est un enregistrement de fichier CSV dont la valeur par défaut est 44.

RowSeparator est un séparateur de lignes de fichier CSV dont la valeur par défaut est 10.

L'intervalle est l'intervalle de temps en secondes, arrondi aux 15 minutes les plus proches pendant lesquelles la mise à jour de l'ensemble d'URL a lieu.

CanaryURL est une URL utilisée pour tester lorsque le contenu de l'ensemble d'URL reste confidentiel.

Exemple

```
import policy urlset -url local:test_urlset.csv -delimiter ","-rowSeparator
 "n"-interval 10 -privateSet -canaryUrl http://www.in.gr
```

Effectuer une correspondance explicite entre les sous-domaines pour un ensemble d'URL importé

Vous pouvez désormais effectuer une correspondance de sous-domaine explicite pour un ensemble d'URL importé. Un nouveau paramètre, « SubdomainExactMatch », est ajouté à la commande « import policy URLSet ». Lorsque vous activez le paramètre, l'algorithme de filtrage d'URL effectue une correspondance explicite entre les sous-domaines. Par exemple, si l'URL entrante est « news.example.com » et si l'entrée du jeu d'URL est « example.com », l'algorithme ne correspond pas aux URL.

À l'invite de commande, tapez :

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator
 <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch]
[-canaryUrl <URL>]
```


Exemple :

```
import policy urlset forth_urlset -url local:test_urlset.csv -interval 3600
 -subdomainExactMatch
```

Pour afficher l'URL définie à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show urlset <name>
```

Exemple :

À l'invite de commande, tapez :

```
1          URLset     Count
2          ------     -----
3  1)      top1k      100
4   Done
5
6  > show urlset top1k
7          Count      Delimiter  Interval   RowSeparator
8          -----      ---------  --------   ------------
9          100              ,        0         0x0a
10  Done
11 >
12
13 <!--NeedCopy-->
```

Pour afficher le jeu d'URL importé à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show urlset -imported
```

Exemple :

À l'invite de commande, tapez :

```
1          URLset
2          ------
3  1)      top1k
4   Done
5  <!--NeedCopy-->
```


Pour afficher le jeu d'URL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show urlset <name>
```

Pour exporter un ensemble d'URL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
export urlset <name> <url>
```

Pour ajouter un ensemble d'URL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add urlset <urlset_name>
```

Pour mettre à jour un ensemble d'URL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
update urlset <name>
```

Pour supprimer une commande de définition d'URL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
remove urlset <name>
```

Exemple :

> Remarque :
>
> Avant d'importer ou d'exporter un ensemble d'URL, vous devez vous assurer que les `test_urlset.csv` fichiers `test_urlset_export.csv` et sont créés et disponibles dans le `/var/tmp` répertoire.

```
1 import policy urlset -url local:test_urlset.csv -delimiter "," -
     rowSeparator "n" -interval 10 -privateSet -overwrite  - canaryUrl
     http://www.in.gr
2
3 add policy urlset top10k
4
5 update policy urlset top10k
6
```



```
sh policy urlset

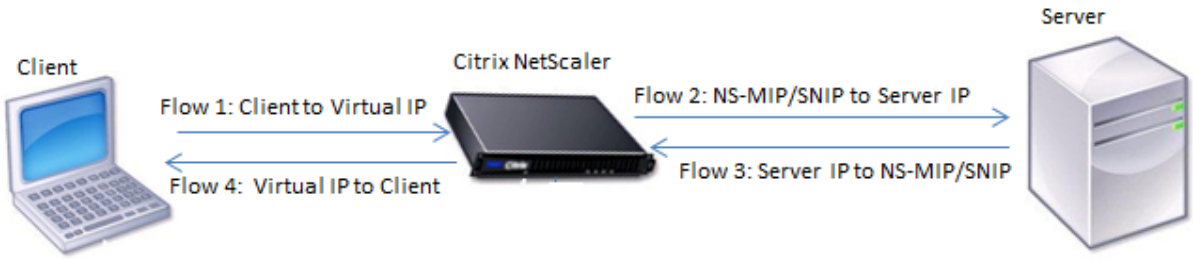
sh policy urlset top10k

export policy urlset urlset1 -url local:test_urlset_export.csv

import policy urlset top10k -url local:test_urlset.csv  - privateSet

add policy urlset top10k

update policy urlset top10k

show policy urlset top10k
<!--NeedCopy-->
```

Afficher les ensembles d'URL importés

Vous pouvez désormais afficher les ensembles d'URL importés en plus des ensembles d'URL ajoutés. Pour ce faire, un nouveau paramètre « importé » est ajouté à la commande « show url set ». Si vous activez cette option, l'appliance affiche tous les ensembles d'URL importés et distingue les jeux d'URL importés des ensembles d'URL ajoutés.

À l'invite de commande, tapez :

```
show policy urlset [<name>] [-imported]
```

Exemple :

```
show policy urlset -imported
```

Pour importer un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert** > **Ensembles d'URL**, cliquez sur **Importer** pour télécharger l'ensemble d'URL.

Pour ajouter un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert** > **Ensembles d'URL**, cliquez sur **Ajouter** pour créer un fichier d'ensemble d'URL pour l'ensemble d'URL téléchargé.

Pour modifier un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert** > **Ensembles d'URL**, sélectionnez un ensemble d'URL et cliquez sur **Modifier** pour le modifier.

Pour mettre à jour un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert** > **Ensembles d'URL,** sélectionnez un jeu d'URL et cliquez sur **Mettre à jour le jeu** d'URL pour mettre à jour le jeu d'URL avec les dernières modifications apportées au fichier.

Pour exporter un ensemble d'URL à l'aide de l'interface graphique

Accédez à **AppExpert > Ensembles d'URL**, sélectionnez un ensemble d'URL, puis cliquez sur **Exporter le jeu** d'URL pour exporter les modèles d'URL d'un ensemble vers une URL de destination et l'enregistrer à cet emplacement.

Sémantique des modèles d'URL

August 20, 2021

Le tableau suivant présente les modèles d'URL utilisés pour spécifier la liste des pages que vous souhaitez filtrer. Par exemple, le modèle d'URL `http://www.example.com/bar` correspond à une seule page `http://www.example.com/bar`. Pour couvrir toutes les pages où l'URL commence par www.example.com/bar, vous devez ajouter explicitement un « * » à la fin.

Pour plus d'informations, voir Tableau de mappage des métadonnées de modèle d'URL .

Catégories d'URL

August 20, 2021

Voici une liste des catégories sur la liste noire.

S.non	Catégories sur la liste noire
1	Activités illégales
2	Drogues illicites
3	Médicaments
4	Marijuana
5	Terrorisme/extrémistes
6	Armes
7	Haine/calomnie

S.non	Catégories sur la liste noire
8	Violence/suicide
9	Défense d’intérêts en général
10	Adulte/pornographie
11	Nudité
12	Services sexuels
13	Recherche/liens pour adultes
14	Piratage/décodage
15	Malware
16	Proxies distants
17	Caches du moteur de recherche
18	Traducteurs
19	Rencontres
20	Mariage
21	Taux du marché
22	Négoce en ligne
23	Assurance
24	Produits financiers
25	Jeux d’argent en général
26	Loterie
27	Jeux en ligne
28	Jeux
29	Enchères
30	Shopping/vente au détail
31	Immobilier
32	Achats informatiques en ligne
33	Chat en ligne
34	Messages instantanés
35	Courrier basé sur le Web
36	Abonnements par e-Mail

S.non	Catégories sur la liste noire
37	Bulletins électroniques
38	Bulletins informatiques
39	Pages Web personnelles/blogs
40	Téléchargements
41	Téléchargements de programmes
42	Services de stockage
43	Streaming de multimédia
44	Emploi
45	Avancement professionnel
46	Activités parallèles
47	Grotesque
48	Événements spéciaux
49	Sujets populaires
50	Magazine/actualités pour adultes
51	Fumer
52	Boissons
53	Produits alcoolisés
54	Fétiche
55	Expression sexuelle (texte)
56	Costume/divertissement
57	Occulte
58	Maison et famille
59	Sports professionnels
60	Sports en général
61	Événements de la vie
62	Voyage et tourisme
63	Agence publique de tourisme
64	Transport public
65	Hébergement

S.non	Catégories sur la liste noire
66	Musique
67	Horoscope /astrologie/voyance
68	Artiste/célébrité
69	Restaurant/gastronomie
70	Divertissements/lieux/activités
71	Religions traditionnelles
72	Religions
73	Politique
74	Publicités/bannières
75	Concours/prix
76	SPAM
77	Actualités
78	Automobile
79	Affaires et Commercial
80	Informatique et Internet
81	Éducation
82	Gouvernement
83	Intégrité
84	Téléphonie Internet
85	Militaire
86	Peer to Peer/Torrents
87	Loisirs et hobbies
88	Référence
89	Moteurs de recherche et portails
90	Éducation sexuelle
91	Services de SMS et de téléphonie mobile
92	Applications mobiles et éditeurs
93	Spyware

S.non	Catégories sur la liste noire
94	Réseaux de distribution de contenu et infrastructure
95	Sites pour enfants
96	Maillots de bain et lingerie
97	Événements artistiques et culturels
98	Sites d’hébergement
99	Organisations philanthropiques à but non lucratif
100	Sites de recherche et de partage de photos
101	Sonneries
102	Mode et beauté
103	App Stores pour mobiles
104	Domaines parqués
105	Émoticônes
106	Opérateurs mobiles
107	Botnets
108	Sites infectés
109	Sites de phishing
110	Keyloggers
111	Malware sur mobiles
112	Aucun contenu
113	Agriculture
114	Architecture
115	Associations/groupements d’affiliation/syndicats
116	Livres/eBooks
117	Bot de type rappel (phone home)
118	DDNS
119	URL non prise en charge
120	Loi

S.non	Catégories sur la liste noire
121	Communautés locales
122	Divers
123	Magazines en ligne
124	Animaux/vétérinaire
125	Piratage et usurpation de droits d'auteur
126	Adresses IP privées
127	Recyclage/environnement
128	Science
129	Société et culture
130	Services de transport et de fret
131	Photographie et film
132	Musées et histoire
133	Formation en ligne
134	Réseaux sociaux en général
135	Facebook
136	Facebook : Publication
137	Facebook : Commenter
138	Facebook : Amis
139	Facebook : Charger des photos
140	Facebook : Événements
141	Facebook : Applications
142	Facebook : Chat
143	Facebook : Questions
144	Facebook : Chargement de vidéos
145	Facebook : Groupes
146	Facebook : Jeux
147	LinkedIn
148	LinkedIn : Mises à jour
149	LinkedIn : Messages

S.non	Catégories sur la liste noire
150	LinkedIn : Connexions
151	LinkedIn : Emplois
152	Twitter
153	Twitter : Publication
154	Twitter : Messages
155	Twitter : Suivre
156	Youtube
157	YouTube : Commenter
158	YouTube : Chargement de vidéos
159	YouTube : Partage
160	Instagram
161	Instagram : Charger
162	Instagram : Commenter
163	Instagram : Message privé
164	Tumblr
165	Tumblr : Publication
166	Tumblr : Commenter
167	Tumblr : Chargement de photos ou de vidéos
168	Google+
169	Google+ : Publication
170	Google+ : Commenter
171	Google+ : Chargement de photos
172	Google+ : Chargement de vidéos
173	Google+ : chat vidéo
174	Pinterest
175	Pinterest : Code PIN
176	Vine : Charger
177	Vine : Commenter
178	Vine : Message

S.non	Catégories sur la liste noire
179	Ask.fm
180	Ask.fm : Demander
181	Ask.fm : Répondre
182	YikYak
183	YikYak : Publication
184	YikYak : Commenter
185	Wordpress
186	Wordpress : Publication
187	Wordpress : Charger

AppFlow

May 5, 2023

L'appliance NetScaler est un point de contrôle central pour tout le trafic des applications dans le centre de données. Il collecte des informations de flux et de session utilisateur utiles pour la surveillance des performances des applications, l'analyse et les applications de Business Intelligence. Il collecte également des données sur les performances des pages Web et des informations de base de données. AppFlow transmet les informations en utilisant le format IPFIX (Internet Protocol Flow Information Export), qui est une norme ouverte de l'Internet Engineering Task Force (IETF) définie dans la RFC 5101. IPFIX (la version normalisée de NetFlow de Cisco) est largement utilisé pour surveiller les informations de flux réseau. AppFlow définit de nouveaux éléments d'information pour représenter des informations au niveau de l'application, des données de performances de page Web et des informations de base de données.

En utilisant UDP comme protocole de transport, AppFlow transmet les données collectées, appelées *enregistrements de flux*, à un ou plusieurs collecteurs IPv4. Les collecteurs regroupent les enregistrements de flux et génèrent des rapports en temps réel ou historiques.

AppFlow offre une visibilité au niveau des transactions pour les flux HTTP, SSL, TCP, SSL_TCP et HDX Insight. Vous pouvez échantillonner et filtrer les types de flux que vous souhaitez surveiller.

> **Remarque**
>
> Pour plus d'informations sur HDX Insight, consultez HDX Insight.

AppFlow utilise des actions et des stratégies pour envoyer des enregistrements pour un flux sélectionné à un ensemble de collecteurs spécifique. Une action AppFlow spécifie quel ensemble de collecteurs reçoit les enregistrements AppFlow. Les stratégies basées sur des expressions avancées peuvent être configurées pour sélectionner les flux pour lesquels des enregistrements de flux sont envoyés aux collecteurs spécifiés par l'action AppFlow associée.

Pour limiter les types de flux, vous pouvez activer AppFlow pour un serveur virtuel. AppFlow peut également fournir des statistiques pour le serveur virtuel.

Vous pouvez également activer AppFlow pour un service spécifique, représentant un serveur d'applications, et surveiller le trafic vers ce serveur d'applications.

Remarque : Cette fonctionnalité n'est prise en charge que sur les versions NetScaler nCore.

Fonctionnement d'AppFlow

Dans le scénario de déploiement le plus courant, le trafic entrant est acheminé vers une adresse IP virtuelle (VIP) sur l'appliance NetScaler et la charge est équilibrée vers un serveur. Le trafic sortant circule du serveur vers une adresse IP mappée ou de sous-réseau sur NetScaler et du VIP vers le client. Un flux est un ensemble unidirectionnel de paquets IP identifiés par les cinq n-uplets suivants : SourceIP, SourcePort, DEStip, DestPort et protocole.

La figure suivante décrit le fonctionnement de la fonctionnalité AppFlow.

Figure 1. Séquence NetScaler Flow



Comme le montre la figure, les identificateurs de flux réseau pour chaque segment d'une transaction dépendent de la direction du trafic.

Les différents flux qui forment un enregistrement de flux sont les suivants :

Flux 1 : <Client-IP, Client-Port, VIP-IP, VIP-port, Protocol>

Débit 2 : <NS-MIP/SNIP, NS-port, Server-IP, Server-Port, Protocol>

Flux 3 : <Server-IP, Server-Port, NS-MIP/SNIP, NS-Port, Protocol>

Flux 4 : <VIP-IP, VIP-port, Client-IP, Client-Port, Protocol>

Pour aider le collecteur à lier les quatre flux d'une transaction, AppFlow ajoute un élément TransactionID personnalisé à chaque flux. Pour la commutation de contenu au niveau de l'application, telle que HTTP, il est possible d'équilibrer la charge d'une connexion TCP client unique sur différentes connexions TCP dorsales pour chaque demande. AppFlow fournit un ensemble d'enregistrements pour chaque transaction.

Enregistrements de flux

Les enregistrements AppFlow contiennent des informations NetFlow ou IPFIX standard, telles que les horodatages pour le début et la fin d'un flux, le nombre de paquets et le nombre d'octets. Les enregistrements AppFlow contiennent également des informations au niveau de l'application (telles que les URL HTTP, les méthodes de requête HTTP et les codes d'état de réponse, le temps de réponse du serveur et la latence). Données de performances de la page Web (telles que le temps de chargement de la page, le temps de rendu de la page et le temps passé sur la page). Et les informations de base de données (telles que le protocole de base de données, l'état de la réponse de base de données et la taille de la réponse Les enregistrements de flux IPFIX sont basés sur des modèles qui doivent être envoyés avant d'envoyer des enregistrements de flux.

Modèles

AppFlow définit un ensemble de modèles, un pour chaque type de flux. Chaque modèle contient un ensemble d'éléments d'information (IE) standard et d'éléments d'information spécifiques à l'entreprise (EIE). Les modèles IPFIX définissent l'ordre et la taille des éléments d'information (Internet Explorer) dans l'enregistrement de flux. Les modèles sont envoyés aux collecteurs à intervalles réguliers, comme décrit dans la RFC 5101.

Un modèle peut inclure les EIE suivants :

- transactionID

  Numéro 32 bits non signé identifiant une transaction au niveau de l'application. Pour HTTP, il correspond à une paire requêtes et réponses. Tous les enregistrements de flux qui correspondent à cette paire demande et réponse ont le même ID de transaction. Dans le cas le plus courant, quatre `uniflow` enregistrements correspondent à cette transaction. Si NetScaler génère lui-même la réponse (fournie à partir du cache intégré ou par une politique de sécurité), il se peut qu'il n'y ait que deux enregistrements de flux pour cette transaction.

- connectionID

  Numéro 32 bits non signé identifiant une connexion de couche 4 (TCP ou UDP). Les flux NetScaler sont bidirectionnels, avec deux enregistrements de flux distincts pour chaque direction du flux. Cet élément d'information peut être utilisé pour relier les deux flux.

Pour NetScaler, un ConnectionID est un identifiant de la structure de données de connexion permettant de suivre la progression d'une connexion. Dans une transaction HTTP, par exemple, un ConnectionID donné peut comporter plusieurs éléments TransactionID correspondant à plusieurs requêtes effectuées sur cette connexion.

- TCPRTT

  Temps aller-retour, en millisecondes, mesuré sur la connexion TCP. Il peut être utilisé comme mesure pour déterminer la latence du client ou du serveur sur le réseau.

- httpRequestMethod

  Numéro 8 bits indiquant la méthode HTTP utilisée dans la transaction. Un modèle d'options avec le mappage number-to-method est envoyé avec le modèle.

- httpRequestSize

  Numéro 32 bits non signé indiquant la taille de la charge utile de la demande.

- httpRequestURL

  URL HTTP demandée par le client.

- httpUserAgent

  Source des demandes entrantes adressées au serveur Web.

- httpResponseStatus

  Numéro 32 bits non signé indiquant le code d'état de la réponse.

- httpResponseSize

  Un numéro 32 bits non signé indiquant la taille de la réponse.

- httpResponseTimeToFirstByte

  Un numéro 32 bits non signé indiquant le temps nécessaire à la réception du premier octet de la réponse.

- httpResponseTimeToLastByte

  Numéro 32 bits non signé indiquant le temps nécessaire à la réception du dernier octet de la réponse.

- flowFlags

  Indicateur 64 bits non signé utilisé pour indiquer différentes conditions de flux.

EIE pour les données de performance des pages Web

- clientInteractionStartTime

  Heure à laquelle le navigateur reçoit le premier octet de la réponse pour charger les objets de la page tels que les images, les scripts et les feuilles de style.

- clientInteractionEndTime

  Heure à laquelle le navigateur a reçu le dernier octet de réponse pour charger tous les objets de la page tels que les images, les scripts et les feuilles de style.

- clientRenderStartTime

  Heure à laquelle le navigateur commence à afficher la page.

- clientRenderEndTime

  Heure à laquelle un navigateur a terminé le rendu de la page entière, y compris les objets incorporés.

EIE pour les informations de base de données

- dbProtocolName

  Numéro 8 bits non signé indiquant le protocole de base de données. Les valeurs valides sont 1 pour MS SQL et 2 pour MySQL.

- dbReqType

  Numéro 8 bits non signé indiquant la méthode de demande de base de données utilisée dans la transaction. Pour MS SQL, les valeurs valides sont 1 pour QUERY, 2 pour TRANSACTION et 3 pour RPC. Pour connaître les valeurs valides pour MySQL, consultez la documentation MySQL.

- dbReqString

  Indique la chaîne de requête de base de données sans l'en-tête.

- dbRespStatus

  Numéro 64 bits non signé indiquant l'état de la réponse de base de données reçue du serveur Web.

- dbRespLength

  Nombre 64 bits non signé indiquant la taille de la réponse.

- dbRespStatString

  Chaîne d'état de réponse reçue du serveur Web.

Configuration de la fonctionnalité AppFlow

May 5, 2023

Vous pouvez configurer AppFlow de la même manière que la plupart des autres fonctionnalités basées sur des règles. Tout d'abord, vous devez activer la fonctionnalité AppFlow. Vous spécifiez ensuite les collecteurs auxquels les enregistrements de flux sont envoyés. Ensuite, vous définissez des actions, qui sont des ensembles de collecteurs configurés. Vous configurez ensuite une ou plusieurs stratégies et associez une action à chaque stratégie. La politique indique à l'appliance NetScaler de sélectionner les demandes dont les enregistrements de flux sont envoyés à l'action associée. Enfin, vous liez chaque stratégie soit globalement, soit au serveur virtuel spécifique pour la mettre en œuvre.

Vous pouvez également définir les paramètres AppFlow pour spécifier l'intervalle d'actualisation du modèle et pour activer l'exportation des informations HttpURL, HttpCookie et HttpPreferer. Sur chaque collecteur, vous devez spécifier l'adresse IP NetScaler comme adresse de l'exportateur.

> **Remarque**
>
> Pour plus d'informations sur la configuration de NetScaler en tant qu'exportateur sur le collecteur, consultez la documentation du collecteur spécifique.

L'utilitaire de configuration fournit des outils qui aident les utilisateurs à définir les stratégies et les actions. Il détermine exactement comment l'appliance NetScaler exporte les enregistrements d'un flux particulier vers un ensemble de collecteurs (action). L'interface de ligne de commande fournit un ensemble correspondant de commandes basées sur l'interface de ligne de commande pour les utilisateurs expérimentés qui préfèrent utiliser la ligne de commande.

Activation d'AppFlow

Pour pouvoir utiliser la fonctionnalité AppFlow, vous devez d'abord l'activer.

> **Remarque**
>
> AppFlow ne peut être activé que sur les appliances nCore NetScaler.

Activez la fonctionnalité AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
1 enable ns feature AppFlow
2
3 <!--NeedCopy-->
```


Activez la fonctionnalité AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres**, cliquez sur **Configurer les fonctionnalités avancées**et sélectionnez l'option **AppFlow** .

Spécifier un collecteur

Un collecteur reçoit les enregistrements AppFlow générés par l'appliance NetScaler. Pour envoyer les enregistrements AppFlow, vous devez spécifier au moins un collecteur. Par défaut, le collecteur écoute les messages IPFIX sur le port UDP 4739. Vous pouvez modifier le port par défaut lors de la configuration du collecteur. De même, par défaut, NSIP est utilisé comme adresse IP source pour le trafic AppFlow. Vous pouvez remplacer cette adresse IP source par défaut par une adresse SNIP lors de la configuration d'un collecteur. Vous pouvez également supprimer des collecteurs inutilisés.

Spécifiez un collecteur à l'aide de l'interface de ligne de commande

> **Important**
>
> À partir de NetScaler version 12.1 build 55.13, vous pouvez spécifier le type de collecteur que vous souhaitez utiliser. Un nouveau paramètre « Transport » est introduit dans la commande `add appflow collector`. Par défaut, le collecteur écoute les messages IPFIX. Vous pouvez modifier le type de collecteur `logstream` ou `ipfix` ou rest en utilisant le paramètre « Transport ». Pour plus d'informations sur la configuration, consultez l'exemple.

À l'invite de commandes, tapez les commandes suivantes pour ajouter un collecteur et vérifier la configuration :

```
1 -  add appflow collector <name> -IPAddress <ipaddress> -port <
     port_number> -netprofile <netprofile_name> -Transport <Transport>
2
3 -  show appflow collector <name>
4
5 <!--NeedCopy-->
```

Exemple

```
1 add appflow collector col1 -IPaddress 10.102.29.251 -port 8000 -
     netprofile n2 -Transport ipfix
2
3 <!--NeedCopy-->
```


Spécifier plusieurs collecteurs en utilisant l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter et envoyer les mêmes données à plusieurs collecteurs :

```
add appflow collector <collector1> -IPAddress <IP>

add appflow collector <collector2> -IPAddress <IP>

add appflow action <action> -collectors <collector1> <collector2>

add appflow policy <policy> true <action>

bind lbvserver <lbvserver> -policy <policy> -priority <priority>
<!--NeedCopy-->
```

Spécifiez un ou plusieurs collecteurs à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow > Collectors**et créez le collecteur AppFlow.

Configurer une action AppFlow

Une action AppFlow est un collecteur d'ensembles auquel les enregistrements de flux sont envoyés si la stratégie AppFlow associée correspond.

Configurer une action AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une action AppFlow et vérifier la configuration :

```
add appflow action <name> --collectors <string> ... [-
    clientSideMeasurements (Enabled|Disabled) ] [-comment <string>]

show appflow action

<!--NeedCopy-->
```

Exemple

```
add appflow action apfl-act-collector-1-and-3 -collectors collector-1
    collecter-3

```



```
<!--NeedCopy-->
```

Configurer une action AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow > Actions**et créez l'action AppFlow.

Configurer une stratégie AppFlow

Après avoir configuré une action AppFlow, vous devez ensuite configurer une stratégie AppFlow. Une stratégie AppFlow est basée sur une règle, qui consiste en une ou plusieurs expressions.

> **Remarque**
>
> Pour la création et la gestion des stratégies AppFlow, l'utilitaire de configuration fournit une assistance qui n'est pas disponible sur l'interface de ligne de commande.

Configurer une stratégie AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour ajouter une stratégie AppFlow et vérifier la configuration :

```
add appflow policy <name> <rule> <action>

show appflow policy <name>

<!--NeedCopy-->
```

Exemple

```
add appflow policy apfl-pol-tcp-dsprt client.TCP.DSTPORT.EQ(22) apfl-
    act-collector-1-and-3

<!--NeedCopy-->
```

Configurer une stratégie AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow > Stratégies**et créez la stratégie AppFlow.

Ajouter une expression à l'aide de la boîte de dialogue Ajouter une expression

1. Dans la boîte de dialogue Ajouter une expression, dans la première zone de liste, choisissez le premier terme de votre expression.

   -

   HTTP
   Le protocole HTTP. Choisissez cette option si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP.

   -

   SSL

   ```
   Les sites Web protégés. Choisissez cette option si vous souhaitez
      examiner certains aspects de la demande qui concernent le
      destinataire de la demande. -
   CLIENT

   The computer that sent the request. Choose the option if you want
      to examine some aspect of the sender of the request. Lorsque
      vous faites votre choix, la zone de liste la plus à droite ré
      pertorie les termes appropriés pour la partie suivante de votre
       expression.
   ```

2. Dans la deuxième zone de liste, choisissez le deuxième terme de votre expression. Les choix dépendent du choix que vous avez effectué à l'étape précédente et sont adaptés au contexte. Une fois que vous avez fait votre deuxième choix, la fenêtre d'aide située sous la fenêtre Construire une expression (qui était vide) affiche de l'aide décrivant le but et l'utilisation du terme que vous venez de choisir.
3. Continuez à choisir des termes dans les zones de liste qui apparaissent à droite de la zone de liste précédente, ou à taper des chaînes ou des nombres dans les zones de texte qui s'affichent pour vous inviter à entrer une valeur, jusqu'à ce que votre expression soit terminée.

Lier une stratégie AppFlow

Pour mettre en œuvre une politique, vous devez la lier soit globalement, afin qu'elle s'applique à tout le trafic qui passe par NetScaler, soit à un serveur virtuel spécifique, de sorte que la politique s'applique uniquement au trafic lié à ce serveur virtuel.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel nombre entier positif.

Dans le système d'exploitation NetScaler, les priorités des politiques fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible. Par exemple, si vous avez trois stratégies

avec des priorités de 10, 100 et 1 000, la stratégie affectée d'une priorité de 10 est exécutée en premier. Plus tard, la stratégie affectée avec une priorité de 100, et enfin la stratégie a attribué un ordre de 1000.

Vous pouvez vous laisser suffisamment de place pour ajouter d'autres stratégies dans n'importe quel ordre, tout en les configurant pour qu'elles soient évaluées dans l'ordre de votre choix. Vous pouvez y parvenir en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous la liez globalement. Vous pouvez ensuite ajouter d'autres stratégies à tout moment sans avoir à modifier la priorité d'une stratégie existante.

Liez globalement une stratégie AppFlow à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez la commande suivante pour lier globalement une stratégie AppFlow et vérifier la configuration :

```
bind appflow global <policyName> <priority> [<gotoPriorityExpression [-
    type <type>] [-invoke (<labelType> <labelName>)]

show appflow global

<!--NeedCopy-->
```

Exemple

```
bind appflow global af_policy_lb1_10.102.71.190 1 NEXT -type
    REQ_OVERRIDE -invoke vserver google

<!--NeedCopy-->
```

Liez une stratégie AppFlow à un serveur virtuel spécifique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez la commande suivante pour lier une stratégie AppFlow à un serveur virtuel spécifique et vérifier la configuration :

```
bind lb vserver <name> -policyname <policy_name> -priority <priority>

<!--NeedCopy-->
```

Exemple


```
bind lb vserver google -policyname af_policy_google_10.102.19.179 -
    priority 251

<!--NeedCopy-->
```

Liez globalement une stratégie AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow**, cliquez sur **Gestionnaire de stratégies AppFlow**, sélectionnez le point de liaison (global par défaut) et le type de connexion appropriés, puis liez la stratégie AppFlow.

Liez une stratégie AppFlow à un serveur virtuel spécifique à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, sélectionnez le serveur virtuel, cliquez sur **Stratégies**, puis liez la stratégie AppFlow.

Activer AppFlow pour les serveurs virtuels

Si vous souhaitez surveiller uniquement le trafic via certains serveurs virtuels, activez AppFlow spécifiquement pour ces serveurs virtuels. Vous pouvez activer AppFlow pour l'équilibrage de charge, la commutation de contenu, la redirection de cache, le VPN SSL, le GSLB et les serveurs virtuels d'authentification.

Activer AppFlow pour un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cs vserver <name> <protocol> <IPAddress> <port> -appflowLog ENABLED

<!--NeedCopy-->
```

Exemple

```
set cs vserver Vserver-CS-1 HTTP 10.102.29.161 80 -appflowLog ENABLED

<!--NeedCopy-->
```


Activez AppFlow pour un serveur virtuel à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez le serveur virtuel et activez l'option Journalisation AppFlow.

Activer AppFlow pour un service

Vous pouvez activer AppFlow pour les services qui doivent être liés aux serveurs virtuels d'équilibrage de charge.

Activer AppFlow pour un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -appflowLog ENABLED

<!--NeedCopy-->
```

Exemple

```
set service ser -appflowLog ENABLED

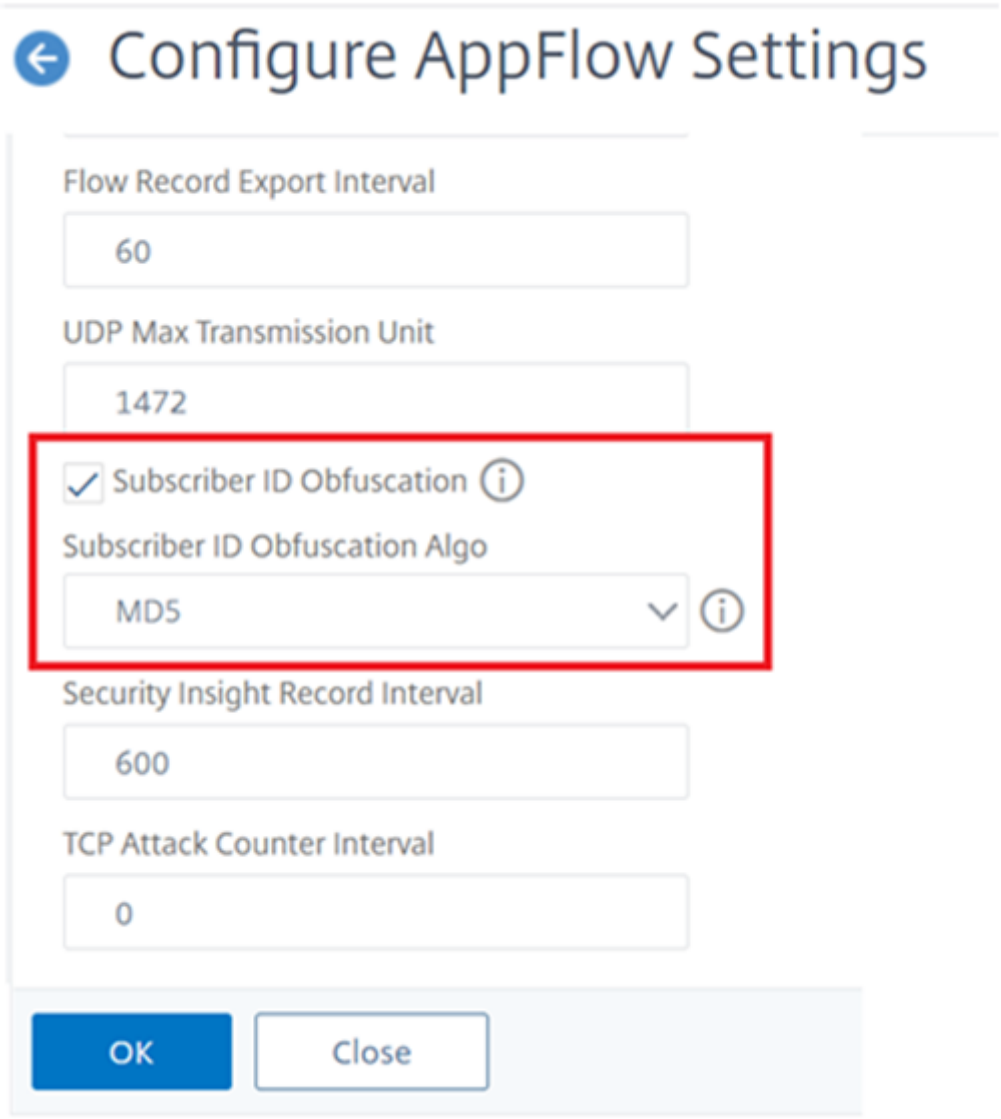
<!--NeedCopy-->
```

Activer AppFlow pour un service à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, sélectionnez le service et activez l'option Journalisation AppFlow.

Définir les paramètres AppFlow

Vous pouvez définir des paramètres AppFlow pour personnaliser l'exportation des données vers les collecteurs.

Définissez les paramètres AppFlow à l'aide de l'interface de ligne de commande

> **Important**
>
> - À partir de NetScaler version 12.1 build 55.13, vous pouvez utiliser le NSIP pour envoyer `Logstream` des enregistrements au lieu du SNIP. Un nouveau paramètre « LogStreaMovern-SIP » est introduit dans la `set appflow param` commande. Par défaut, le paramètre

> « LogStreamoVernSip » est DÉSACTIVÉ, vous devez « ACTIVER ». Pour plus d'informations sur la configuration, consultez l'exemple.
>
> - À partir de la version 13.0 build 58.x de NetScaler, vous pouvez activer l'option d'application Web SaaS dans la fonctionnalité AppFlow. Il peut être activé pour recevoir l'utilisation des données des applications Web ou SaaS à partir du service Citrix Gateway. Pour plus d'informations sur la configuration, consultez l'exemple.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres AppFlow et vérifier les paramètres :

```
- set appflow param [-templateRefresh <secs>] [-appnameRefresh <secs>]
   [-flowRecordInterval <secs>] [-udpPmtu <positive_integer>] [-
  httpUrl ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-httpCookie ( \*\*
  ENABLED\*\* | \*\*DISABLED\*\* )] [-httpReferer ( \*\*ENABLED\*\* |
  \*\*DISABLED\*\* )] [-httpMethod ( \*\*ENABLED\*\* | \*\*DISABLED
  \*\* )] [-httpHost ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
  httpUserAgent ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
  httpXForwardedFor ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )][-
  clientTrafficOnly ( \*\*YES\*\* | \*\*NO\*\*)] [-
  webSaaSAppUsageReporting ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
  logstreamOverNSIP ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )]

- show appflow Param

<!--NeedCopy-->
```

Exemple

```
set appflow Param -templateRefresh 240 -udpPmtu 128 -httpUrl enabled -
   webSaaSAppUsageReporting ENABLED -logstreamOverNSIP ENABLED

<!--NeedCopy-->
```

Définissez les paramètres AppFlow à l'aide de l'utilitaire de configuration

Accédez à **Système > AppFlow**, cliquez sur **Modifier les paramètres AppFlow**et spécifiez les paramètres AppFlow pertinents.

Prise en charge du masquage de l'identifiant d'abonné

À partir de la version 13.0 build 35.xx de NetScaler, la configuration d'AppFlow est améliorée pour prendre en charge l'algorithme « SubscriberidObfuscation » destiné à masquer le MSISDN dans les

enregistrements AppFlow de couche 4 ou de couche 7. Toutefois, avant de configurer l'algorithme en tant que MD5 ou SHA256, vous devez d'abord l'activer en tant que paramètre AppFlow. Le paramètre est désactivé par défaut.

Configuration de l'algorithme d'obscurcissement de l'ID d'abonné à l'aide de l'interface

À l'invite de commande, tapez :

```
set appflow param [-subscriberIdObfuscation ( ENABLED | DISABLED )  [-
    subscriberIdObfuscationAlgo ( MD5 | SHA256 )]]

<!--NeedCopy-->
```

Exemple

```
set appflow param  -subscriberIdObfuscation ENABLED  -
    subscriberIdObfuscationAlgo SHA256

<!--NeedCopy-->
```

Configurer l'algorithme d'obscurcissement de l'ID d'abonné à l'aide de l'interface graphique

1. Accédez à **Système > AppFlow**.
2. Dans le volet détaillé AppFlow, cliquez sur **Modifier le paramètre AppFlow** sous **Paramètres**.
3. Dans la page Configurer les paramètres AppFlow, définissez les paramètres suivants :
   - **Obfuscation de l'identifiant d'abonné.** Activez l'option d'obscurcissement MSISDN dans les enregistrements AppFlow L4/L7.
   - **Algo d'obscurcissement de l'identifiant d'abonné.** Sélectionnez le type d'algorithme MD5 ou SHA256.
4. Cliquez sur **OK** et sur **Fermer**.



Exemple : configurer AppFlow pour DataStream

L'exemple suivant illustre la procédure de configuration d'AppFlow pour DataStream à l'aide de l'interface de ligne de commande.

```
enable feature appflow

add db user sa password freebsd

add lbvserver lb0 MSSQL 10.102.147.97 1433 -appflowLog ENABLED

add service sv0 10.103.24.132 MSSQL 1433 -appflowLog ENABLED

```



```
bind lbvserver lb0 sv0

add appflow collector col0 -IPAddress 10.102.147.90

add appflow action act0 -collectors col0

add appflow policy pol0 "mssql.req.query.text.contains("select")" act0

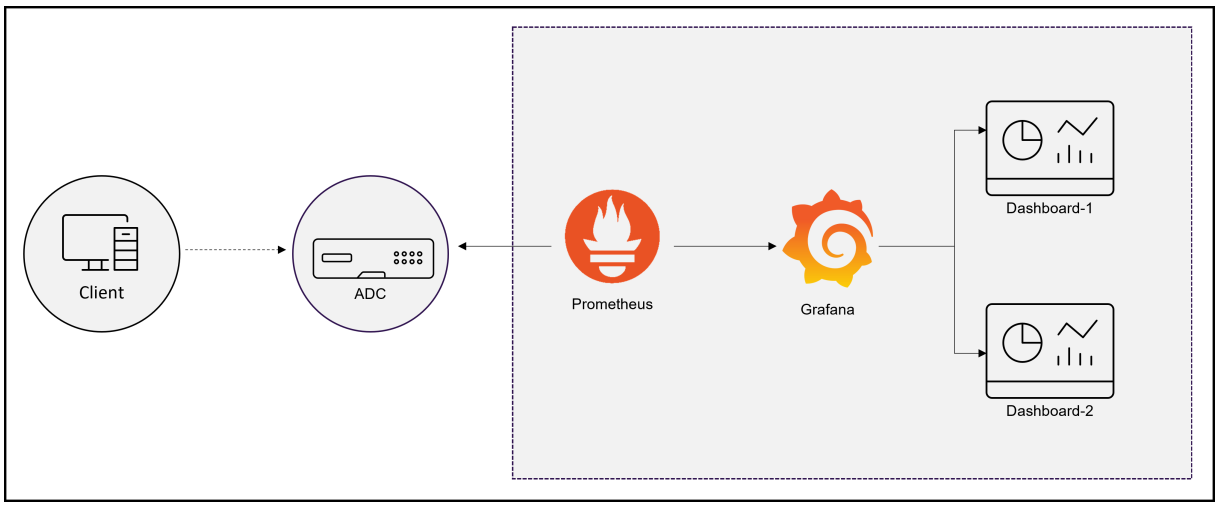
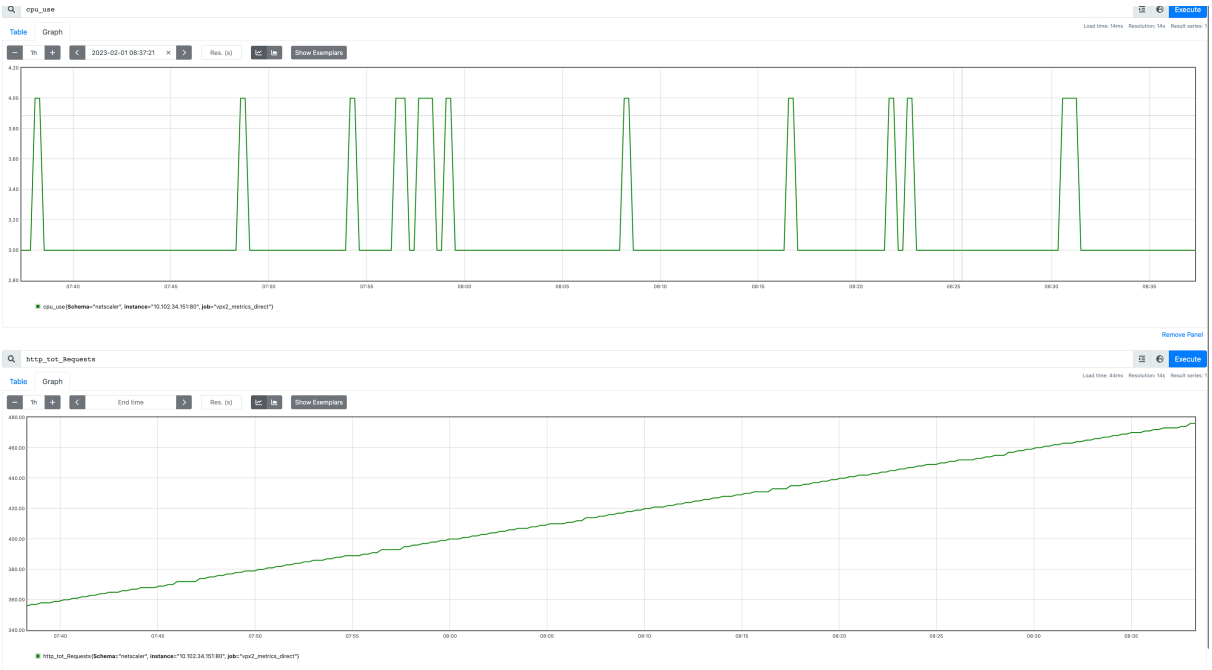
bind lbvserver lb0 -policyName pol0 -priority 10

<!--NeedCopy-->
```

Lorsque l'appliance NetScaler reçoit une demande de base de données, elle évalue la demande par rapport à une politique configurée. Si une correspondance est trouvée, les détails sont envoyés au collecteur AppFlow configuré dans la stratégie.

Configurer le collecteur de métriques

Le collecteur de métriques est un service que vous pouvez activer sur NetScaler pour collecter et exporter des métriques depuis NetScaler vers différents points de terminaison. Vous pouvez exporter des métriques dans deux formats : Avro et Prometheus. Les mesures exportées peuvent être traitées et visualisées pour obtenir des informations pertinentes. Par défaut, le collecteur de métriques prend en charge l'exportation de données analytiques de séries chronologiques toutes les 30 secondes. Vous pouvez toutefois le configurer sous la forme d'une valeur comprise entre 30 et 300 secondes afin de pouvoir décider de l'intervalle d'exportation des données du profil d'analyse des séries chronologiques.

Procédez comme suit pour configurer un collecteur de métriques à l'aide de l'interface de ligne de commande.

1. Configurez un service de collecteur avec adresse IP, protocole et port à l'aide de la commande suivante.

   ```
   add service <metrics_service_name> <ip-address> <protocol> <port>
   ```

   Exemple :

   ```
   add service metrics_service1 192.168.1.1 HTTP 5563
   ```

2. Configurez le profil de série chronologique d'analyse pour envoyer des données de mesures au service de collecte. Spécifiez le service de collecte, la fréquence d'exportation des métriques et le mode de sortie.


```
set analytics profile ns_analytics_time_series_profile -collectors
     <metrics_service_name> -type timeseries -metrics ENABLED
    metricsExportFrequency <30-300> -outputMode <avro/prometheus>
```

Exemple :

```
set analytics profile ns_analytics_time_series_profile -collectors
     metrics_service1 -type timeseries -metrics Enabled
    metricsExportFrequency 90 -outputMode prometheus --serveMode
    PUSH
```

> **Remarque :**
>
> Cet exemple utilise le profil de série chronologique par défaut `ns_analytics_time_series_profile`. Si vous souhaitez créer un profil de série chronologique, vous pouvez utiliser la `add analytics profile` commande.

Dans cet exemple, la fréquence d'exportation des métriques est définie sur 90 secondes et le mode d'exportation est spécifié comme Prometheus.

Vérifiez la configuration du collecteur de métriques à l'aide de la `show analytics profile <analytics-profile-name>` commande :

```
show analytics profile ns_analytics_time_series_profile

    Name: ns_analytics_time_series_profile
    Collector: metrics_service1
    Profile-type: timeseries
        Output Mode: Prometheus
        Metrics: ENABLED
          Schema File: schema.json
          Metrics Export Frequency: 90
        Events: DISABLED
        Auditlog: DISABLED
        Serve mode: Pull
    Reference Count: 0
```

Collecteur de métriques de débug

Les journaux de débogage requis sont stockés sur `/var/nslog/metricscollector.log` place.

Génération de fichiers métriques

Les `metrics_<format>_log.*` fichiers sont générés sous l'emplacement du `/var/nslog/` dossier.

Support dynamique des schémas dans le collecteur de métriques

À l'aide de compteurs de schémas dynamiques, un fichier de schéma contenant une liste de compteurs peut être mis à jour au moment de l'exécution en fonction des besoins. Par défaut, `/var/metrics_conf/schema.json` le fichier est configuré avec une liste de compteurs.

> **Remarque :**
>
> Le fichier de schéma par défaut du collecteur de métriques `/var/metrics_conf/schema.json` peut être installé sur une appliance NetScaler à l'aide de la procédure installns.

Configurer le collecteur de metrics pour souscrire des compteurs à l'aide de l'interface

Démarrez l'exportation des métriques en configurant un service Collector.

À l'invite de commande, tapez :

```
1 set analytics profile ns_analytics_time_series_profile -metrics ENABLED
      -collectors <collector_name> -schemaFile  schema.json -outputMode <
     avro | prometheus>
2
3 <!--NeedCopy-->
```

> **Remarque :**
>
> `schema.json` est la configuration SchemaFile par défaut.

Un nouveau fichier de schéma avec un ensemble de compteurs requis peut être configuré à l'aide de la commande CLI pour que le collecteur de metrics exporte. Le fichier de schéma doit être présent dans l'emplacement `/var/metrics_conf/`.

Le fichier de schéma contenant toutes les listes de compteurs (reference_schema.json) pris en charge par stats infra est présent dans l'emplacement `/var/metrics_conf/`. Ce fichier peut être utilisé comme référence pour créer une liste personnalisée de compteurs.

Configurer un fichier de schéma à l'aide de l'interface

```
1 set analytics profile ns_analytics_time_series_profile -metrics ENABLED
      -collectors <collector name> -schemaFile <schema file_name> -
     outputMode <avro | prometheus>
2
3 <!--NeedCopy-->
```

Un nouveau fichier de schéma avec les compteurs requis peut être ajouté et configuré à l'aide de la commande CLI précédente pour que le collecteur de métriques puisse être exporté.

Le fichier de schéma de référence contenant toutes les listes de compteurs (reference_schema.json) pris en charge par stats infra est présent dans l' `/var/metrics_conf/` emplacement. Ce fichier peut être utilisé comme référence pour créer une liste personnalisée de compteurs.

Vérifiez la sortie de configuration CLI à l'invite de commande :

```
show analytics profile ns_analytics_time_series_profile

    Name: ns_analytics_time_series_profile
    Collector: <collector_name>
    Profile-type: timeseries
    Output Mode: avro
    Metrics: ENABLED
    Schema File: schema.json
    Events: ENABLED
    Auditlog: DISABLED
    Serve mode: Push
    Reference Count: 0

<!--NeedCopy-->
```

Étapes pour mettre à jour la liste des compteurs exportés

La procédure suivante décrit les étapes à suivre pour mettre à jour la liste des compteurs exportés :

1. Mettez à jour le fichier de schéma personnalisé/nouveau.
2. Désactivez ou activez les métriques à l'aide de l' `-metrics` option indiquée dans la configuration de la CLI pour le fichier de schéma mis à jour à utiliser.

Prise en charge de plusieurs profils chronologiques

Le collecteur de métriques prend en charge jusqu'à trois configurations de profils de séries chronologiques sur l'appliance NetScaler.
Vous pouvez configurer chaque série chronologique pour qu'elle comporte les éléments suivants.

- Collectionneur.
- Fichier de schéma contenant l'ensemble de compteurs requis à exporter.
- Format de données dans lequel les métriques doivent être exportées.
- Possibilité d'activer ou de désactiver les métriques, les journaux d'audit et les événements.

Grâce à la prise en charge de plusieurs profils de séries chronologiques, le collecteur de métriques peut exporter simultanément un ensemble différent (en fonction du fichier de schéma configuré) de mesures vers différents collecteurs dans différents formats (AVRO, Prometheus, Influx).

Ajouter un profil de série chronologique via l'interface de ligne

À l'invite de commande, tapez :

```
add analytics profile <profile_name> -type timeseries
<!--NeedCopy-->
```

Configurer le profil des séries chronologiques à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set analytics profile <profile_name> -metrics <DISABLED|ENABLED> -
    auditlogs <DISABLED|ENABLED> -events <DISABLED|ENABLED> -collectors
    <collector_name> -schemaFile schema.json -outputMode <avro | influx
    | prometheus>

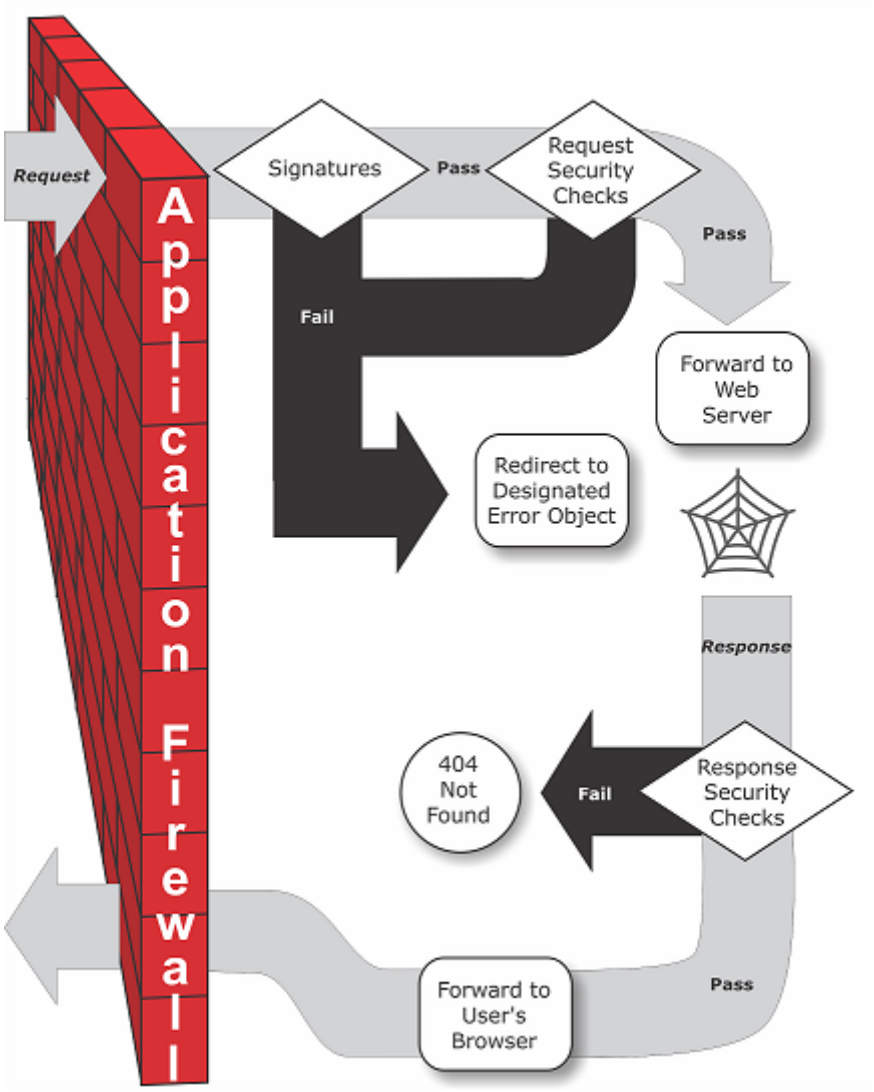
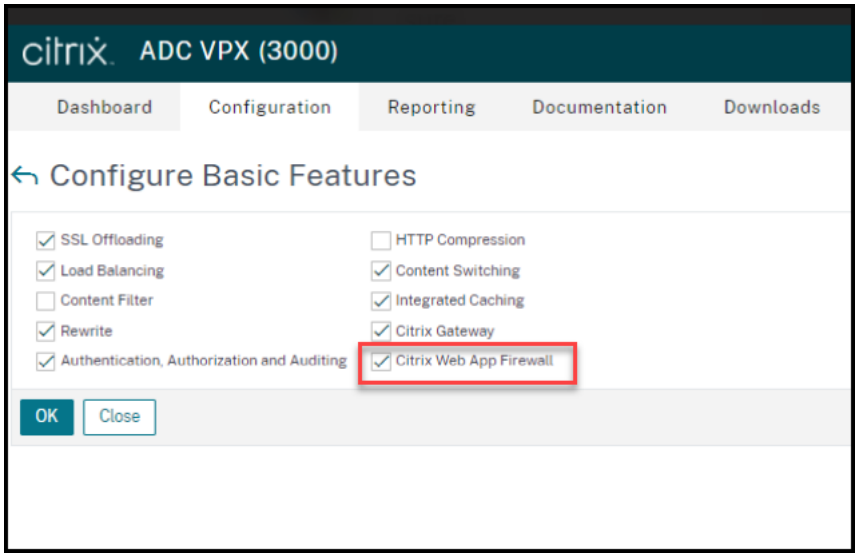
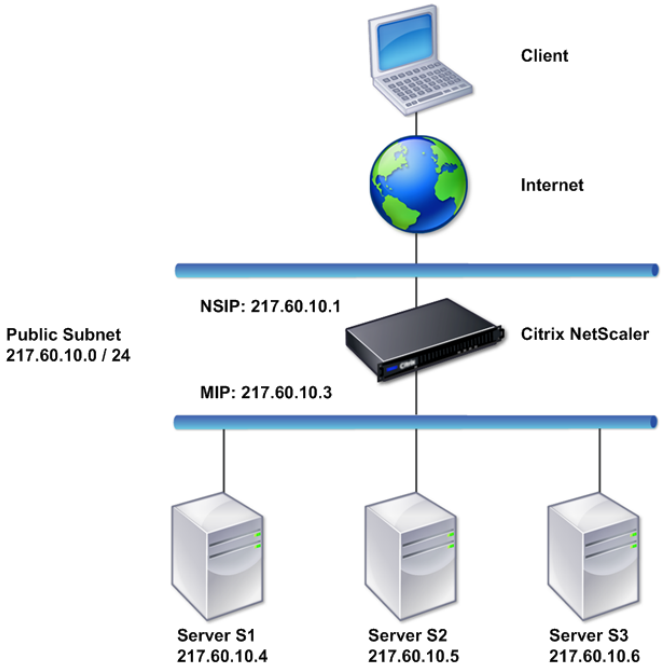
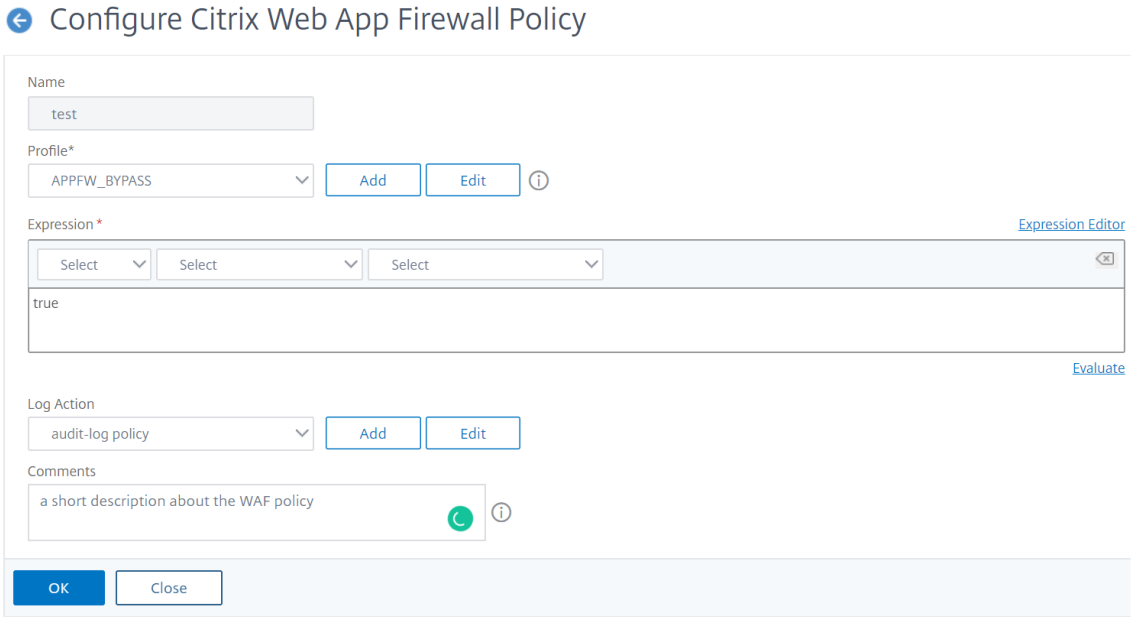
<!--NeedCopy-->
```

Conventions de dénomination des fichiers journaux avec prise en charge de plusieurs profils de séries chronologiques

- Les fichiers journaux Avro sont générés au format `metrics_avro_<profile_name>_log.*`.
- Les fichiers journaux de Prometheus sont générés au format `metrics_prom_<profile_name>.log`.

> **Remarques :**
>
> - Même si les métriques peuvent être activées sur tous les profils de séries chronologiques configurés, les événements et les journaux d'audit ne peuvent être activés que sur un seul profil.
> - La fonctionnalité de schéma dynamique est prise en charge à partir de la version 13.1 build 23.16.
> - Le profil de séries chronologiques multiples est pris en charge à partir de la version 13.1 build 33.6.

Exportation des données de performances des pages Web vers AppFlow Collector

May 5, 2023

L'application EdgeSight Monitoring fournit des données de surveillance des pages Web qui vous permettent de surveiller les performances de diverses applications Web proposées dans un environnement NetScaler. Vous pouvez désormais exporter ces données vers des collecteurs AppFlow pour obtenir une analyse approfondie des applications de page Web. AppFlow, basé sur la norme IPFIX, fournit des informations plus spécifiques sur les performances des applications Web que la seule surveillance EdgeSight.

Vous pouvez configurer des serveurs virtuels d'équilibrage de charge et de commutation de contenu pour exporter des données EdgeSight Monitoring vers des collecteurs AppFlow. Avant de configurer un serveur virtuel pour l'exportation AppFlow, associez une action AppFlow à la stratégie de réponse EdgeSight Monitoring.

Les données de performances de la page Web suivantes sont exportées vers AppFlow :

- **Temps de chargement de la page**. Temps écoulé, en millisecondes, entre le moment où le navigateur commence à recevoir le premier octet d'une réponse et celui où l'utilisateur commence à interagir avec la page. À ce stade, tout le contenu de la page peut ne pas être chargé.
- **Heure de rendu de la page**. Temps écoulé, en millisecondes, entre le moment où le navigateur reçoit le premier octet de réponse jusqu'à ce que tout le contenu de la page ait été rendu ou que l'action de chargement de page ait expiré.
- **Temps passé sur la page**. Temps passé par les utilisateurs sur une page. Représente le temps écouler entre une demande de page et la suivante.

AppFlow transmet les données de performances à l'aide du format IPFIX (Internet Protocol Flow Information Export), qui est un standard ouvert Internet Engineering Task Force (IETF) défini dans la RFC 5101. Les modèles AppFlow utilisent les éléments d'information (EIS) spécifiques à l'entreprise suivants pour exporter les informations :

- **Heure de fin du chargement du client**. Heure à laquelle le navigateur a reçu le dernier octet d'une réponse pour charger tous les objets de la page tels que les images, les scripts et les feuilles de style.
- **Heure de début du chargement du client**. Heure à laquelle le navigateur reçoit le premier octet de la réponse pour charger tous les objets de la page tels que des images, des scripts et des feuilles de style.
- **Heure de fin du rendu client**. Heure à laquelle un navigateur a terminé le rendu de la page entière, y compris les objets incorporés.
- **Heure de début du rendu client**. Heure à laquelle le navigateur a commencé à rendre la page.

Conditions préalables à l'exportation des données de performances des pages Web vers des collecteurs AppFlow

Avant d'associer l'action AppFlow à la stratégie AppFlow, vérifiez que les conditions préalables suivantes ont été remplies :

- La fonctionnalité AppFlow a été activée et configurée.
- La fonction Répondeur a été activée.
- La fonctionnalité de surveillance EdgeSight a été activée.
- La surveillance EdgeSight a été activée sur les serveurs virtuels d'équilibrage de charge ou de commutation de contenu liés aux services des applications pour lesquelles vous souhaitez collecter les données de performances.

Association d'une action AppFlow à la stratégie de réponse EdgeSight monitoring

Pour exporter les données de performances de la page Web vers le collecteur AppFlow, vous devez associer une action AppFlow à la stratégie de réponse EdgeSight Monitoring. Une action AppFlow spécifie quel ensemble de collecteurs reçoit le trafic.

Pour associer une action AppFlow à la stratégie EdgeSight Monitoring Responder à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set responder policy <name> -appflowAction <action_Name>
<!--NeedCopy-->
```

Exemple

```
set responder policy pol -appflowAction actn
<!--NeedCopy-->
```

Pour associer une action AppFlow à la stratégie EdgeSight Monitoring Responder à l'aide de l'interface graphique

1. Accédez à **AppExpert** > **Répondeur** > **Stratégies**.
2. Dans le volet d'informations, sélectionnez une stratégie de répondeur EdgeSight Monitoring, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer la stratégie de répondeur**, dans la liste déroulante **Action AppFlow**, sélectionnez l'action AppFlow associée aux collecteurs auxquels vous souhaitez envoyer les données de performances de la page Web.
4. Cliquez sur **OK**.

Configuration d'un serveur virtuel pour exporter les statistiques EdgeSight vers des collecteurs AppFlow

Pour exporter les informations statistiques EdgeSight d'un serveur virtuel vers le collecteur AppFlow, vous devez associer une action AppFlow au serveur virtuel.

Pour associer une action AppFlow à un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**. Vous pouvez également accéder à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels**.
2. Dans le volet de détails, sélectionnez un serveur virtuel ou plusieurs serveurs virtuels, puis cliquez sur **Activer la surveillance EdgeSight**.
3. Dans la boîte de dialogue Activer la surveillance EdgeSight, activez la case à cocher **Exporter les statistiques EdgeSight vers Appflow** .
4. Dans la liste déroulante Action AppFlow, sélectionnez l'action **AppFlow** . L'action AppFlow définit la liste des collecteurs AppFlow vers lesquels elle exporte les statistiques EdgeSight Monitoring. Si vous avez sélectionné plusieurs serveurs virtuels d'équilibrage de charge, la même action AppFlow est associée aux stratégies de répondeur qui leur sont liées. Vous pouvez modifier ultérieurement l'action AppFlow configurée pour chacun des serveurs virtuels d'équilibrage de charge sélectionné individuellement, si nécessaire.
5. Cliquez sur **OK**.

Fiabilité des sessions sur la paire haute disponibilité de NetScaler

May 5, 2023

Lorsqu'une interruption du réseau ou un basculement de périphérique se produit pendant une session ICA, la reconnexion de session peut utiliser l'un des deux mécanismes suivants : la fiabilité de session ou la reconnexion automatique des clients.

Fiabilité des sessions. Le mode préféré est une expérience fluide pour l'utilisateur. La perturbation est à peine perceptible lors de brèves interruptions de réseau.

Reconnexion automatique des clients. L'option de secours implique le redémarrage du client. Ce mécanisme perturbe l'utilisateur et n'est pas toujours pris en charge.

Les récepteurs peuvent reconnecter leurs sessions ICA de manière transparente à l'aide de la fonctionnalité de fiabilité de session ICA, lorsque HDX Insight est activé.
Cette fonctionnalité fonctionne à la fois en mode autonome et dans une configuration par paire NetScaler HA, et même en cas de basculement NetScaler.

Remarque :

- Les appliances NetScaler doivent s'exécuter sur la version logicielle 11.1 build 49.16 ou ultérieure.
- Vous ne devez ni activer ni désactiver le mode de fiabilité de session lorsque les appliances NetScaler disposent de connexions actives.
- L'activation ou la désactivation de la fonctionnalité lorsque les connexions sont toujours actives entraîne l'arrêt de l'analyse de ces sessions par HDX Insight après un basculement. Cela entraîne la perte d'informations sur les sessions.
- La fiabilité des sessions sur une configuration haute disponibilité est désactivée par défaut pour la version 11.1 49.16 ou ultérieure du logiciel NetScaler. La fiabilité de session n'est prise en charge sur une configuration haute disponibilité que si les deux nœuds de l'installation exécutent la même version (par exemple, la version 11.1 build 53). En d'autres termes, la fiabilité de session n'est pas prise en charge dans une configuration haute disponibilité si les deux nœuds exécutent des versions différentes (par exemple, un nœud possède la version 11.1 build 53 tandis que l'autre possède la version 11.1 build 56). La fiabilité de session pour SSL VDA est prise en charge si les conditions suivantes sont remplies :
  - The "EnableSRonHAFailover" parameter in the `set ica parameter` command must be YES.
  - The HTTPS must be used instead of HTTP while configuring the virtual server.
- Lorsque HDX Insight est activé, les applications de chiffrement de base et les postes de travail se reconnectent après basculement haute disponibilité, même si le paramètre EnableSronhaFailover est désactivé.

Pour configurer la fiabilité de session à l'aide de la CLI :

1. Sur la ligne de commande, utilisez les informations d'identification de l'administrateur système par défaut pour ouvrir une session sur le système.
2. Pour activer la fiabilité de session en cas de basculement HA, à l'invite, tapez : `set ica parameter EnableSRonHAFailover YES`
3. Pour désactiver la fiabilité de session en cas de basculement HA, à l'invite, tapez : `set ica parameter EnableSRonHAFailover NO`

Pour activer la fiabilité de session en cas de basculement HA à l'aide de l'interface graphique :

1. Dans un navigateur Web, tapez l'adresse IP de l'instance principale de NetScaler dans la paire HA (par exemple, http://192.168.100.1).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Dans l'onglet **Configuration**, accédez à **Système** > **Paramètres**, puis cliquez sur **Modifier les paramètres ICA**.
4. Dans la section **Change ICA Parameters**, sélectionnez **Session Reliability on HA Failover**.

5. Cliquez sur **OK**.

Limitations

- L'activation de cette fonctionnalité entraîne une augmentation de la consommation de bande passante due à la désactivation de la compression ICA par la fonctionnalité. Et le trafic supplémentaire entre les nœuds principal et secondaire pour les maintenir synchronisés.
- Cette fonctionnalité est prise en charge uniquement en mode actif-passif. Le mode actif-actif n'est actuellement pas pris en charge.
- Lorsque HDX Insight est activé et que la fiabilité des sessions sur le bouton HA est définie sur NON, seul le mode de reconnexion ACR est pris en charge dans le scénario de basculement haute disponibilité de NetScaler. Le bouton HA ne désactive pas la fiabilité de session si HDX Insight est désactivé.

La table **Sémantique de reconnexion** de session est la suivante :

Session reconnecte la sémantique

État	EnableSRonHAFailover Yes	EnableSRonHAFailover No (Défaut)
HDX Insight activé	Reconnexion de session pour les travaux de session ICA	La reconnexion de session pour les sessions ICA ne fonctionne pas
HDX Insight désactivé	Reconnexion de session pour les travaux de session ICA	La reconnexion de session pour les sessions ICA fonctionne

Points à noter

- La fiabilité des sessions ICA fonctionne de manière immédiate avec NetScaler Gateway.
- La fiabilité de session pour les sessions ICA ne fonctionne pas lorsque les deux conditions suivantes sont remplies :
  - HDX Insight est activé
  - EnableSRonHAFailover est défini sur NO
- La définition du bouton EnableSRonHAFailover sur OUI ou NON ne fait aucune différence lorsque HDX Insight est désactivé.

Surveillance de NetScaler, des applications et de la sécurité des applications à l'aide de Prometheus

May 5, 2023

Les métriques sont une représentation numérique de données mesurées sur une certaine période. Les données métriques sont utiles pour suivre l'
état de santé d'un système au fil du temps. Prometheus est un outil de surveillance open source qui collecte des données métriques et stocke ces données avec un horodatage auquel les données ont été enregistrées.

En surveillant et en analysant les indicateurs, vous pouvez suivre l'état de santé de vos applications, détecter toute anomalie, créer des alertes et prendre les mesures correctives nécessaires pour garantir une fourniture logicielle robuste.

NetScaler prend désormais en charge l'exportation directe des métriques vers Prometheus. Vous pouvez utiliser le riche ensemble de mesures fourni par NetScaler ADC pour surveiller l'état de NetScaler ainsi que celui des applications. Par exemple, vous pouvez collecter des mesures sur l'utilisation du processeur et de la mémoire pour connaître l'état de santé de NetScaler. De même, vous pouvez utiliser des mesures telles que le nombre de requêtes HTTP reçues par seconde ou le nombre de clients actifs pour surveiller l'état de santé des applications.

Exportation de métriques depuis NetScaler vers Prometheus

NetScaler prend en charge le mode pull de Prometheus ainsi que le mode push. En mode extraction, vous devez configurer un profil de série chronologique que Prometheus interroge à intervalles réguliers et extrait les données métriques directement sans aucune ressource d'exportation intermédiaire. Avec le mode pull, vous pouvez autoriser l'accès en lecture seule à un utilisateur ne disposant pas de privilèges de superutilisateur pour exporter des métriques vers Prometheus. À l'aide de Grafana, vous pouvez visualiser les métriques NetScaler exportées vers Prometheus pour faciliter l'interprétation et la compréhension.

Le schéma suivant montre une intégration de Prometheus et Grafana avec NetScaler.



Configurer l'exportation des métriques de NetScaler vers Prometheus et la visualisation à l'aide de Grafana

Vous devez suivre les étapes suivantes pour configurer l'exportation des métriques de NetScaler vers Prometheus et la visualiser à l'aide de Grafana.

1. Configurez NetScaler avec un profil d'analyse de séries chronologiques pour exporter des métriques vers Prometheus.
2. Installez Prometheus et configurez-le avec les paramètres spécifiques à NetScaler.
3. Ajoutez Prometheus comme source de données dans Grafana.
4. Créer une visualisation dans Grafana

Configurer un profil d'analyse de séries chronologiques sur NetScaler pour prendre en charge le mode d'extraction de Prometheus

Procédez comme suit pour configurer le mode pull à l'aide de l'interface de ligne de commande NetScaler :

1. Créez un profil d'analyse dont le type est une série chronologique. Spécifiez le fichier de schéma avec les métriques NetScaler requises.

```
1 add analytics profile <timeseries_profile_name> -type timeseries -
     schemaFile <name_of_schema_file>
2 -outputMode Prometheus -serveMode PULL -metrics ENABLED
```

   Dans cette commande :

   - `timeseries_profile_name`: Spécifiez le nom du profil de la série chronologique.
   - `schemaFile`: Spécifiez le nom du fichier de schéma avec les compteurs NetScaler. Par défaut, un fichier de schéma `/var/metrics_conf/schema.json` contenant une liste de

compteurs est configuré. Un fichier de schéma de référence `reference_schema.json` avec tous les compteurs pris en charge est également disponible sous le chemin `/var/metrics_conf/`. Ce fichier de schéma peut être utilisé comme référence pour créer une liste personnalisée de compteurs. Lorsque vous spécifiez le fichier de schéma, le chemin du fichier de schéma `/var/metrics_conf/` est automatiquement ajouté et vous devez uniquement mentionner le nom du fichier de schéma. Par exemple, si vous avez créé un fichier de schéma `schema1.json` avec une liste personnalisée de compteurs à l'adresse `/var/metrics_conf/`, vous devez uniquement spécifier le nom du fichier sous la forme `schema1.json`.

- `outputMode`: définissez le mode de sortie comme Prometheus.
- `serveMode`: Spécifiez le mode d'extraction de Prometheus.
- `metrics`: Activez la collecte de métriques à partir de NetScaler.

> **Remarque :**
>
> Vous pouvez configurer un profil d'analyse avec tous les paramètres nécessaires à l'aide de la commande add. Si vous devez apporter des modifications après avoir créé le profil, vous pouvez utiliser la commande set pour prendre les mesures appropriées, telles que désactiver les métriques et modifier le mode serveur. Vous pouvez configurer l'accès en lecture seule à Prometheus pour un utilisateur qui n'est pas un superutilisateur. Pour plus d'informations, consultez la section Configurer l'accès en lecture seule à Prometheus pour un utilisateur qui n'est pas un superutilisateur.

Installation et configuration de Prometheus pour l'exportation de métriques depuis NetScaler

Vous pouvez télécharger Prometheus à partir de référentiels tels que DockerHub ou Quay ou du référentiel officiel Prometheus.

Pour exécuter Prometheus en tant que conteneur Docker, utilisez la commande suivante :

```
1    docker run -dp 39090:9090 -v /tmp/prometheus.yml:/etc/prometheus/
        prometheus.yml --name native_prom prom/prometheus:latest  > **
        Remarque :** > > Ici, `/tmp/prometheus.yml` est utilisé comme
        chemin d'accés au `prometheus.yml` fichier. Au lieu de cela,
        vous pouvez spécifier le chemin sur votre machine virtuelle.
```

Vous devez modifier le `prometheus.yml` avec les paramètres NetScaler.

Pour exporter des métriques depuis NetScaler, vous devez spécifier les paramètres spécifiques à NetScaler suivants dans la section de configuration de **Prometheus** YAML scrape. La section de configuration du scrape spécifie un ensemble de cibles et de paramètres de configuration décrivant comment les récupérer.

- `metrics_path` : Spécifiez le chemin de la ressource HTTP dans NetScaler (/nitro/v1/config/systemfile) pour récupérer les métriques.
- `username`: Spécifiez le nom d'utilisateur NetScaler.
- `password`: Spécifiez le mot de passe NetScaler.
- `targets`: Spécifiez l'adresse IP du NetScaler à partir duquel vous devez exporter les métriques, les métriques et le port que vous souhaitez exposer.
- `filename` : Spécifiez le nom du profil de série chronologique configuré `timeseries_profile_name` à la place du `metrics_prom_<timeseries_profile_name>.log` fichier.
- `filelocation`: spécifiez l'emplacement du fichier sous la forme `/var/nslog`.

Vous trouverez ci-dessous la section de configuration de rebut du fichier YAML de Prometheus permettant d'ajouter l'adresse IP NetScaler en tant que cible sur Prometheus pour exporter des métriques. Ici, le protocole HTTP est utilisé comme schéma. Vous pouvez utiliser HTTP ou HTTPS.

```
scrape_configs:
  - job_name: 'vpx2_metrics_direct'
    metrics_path: /nitro/v1/config/systemfile
    params:
      args: ['filename:metrics_prom_ns_analytics_time_series_profile.
         log,filelocation:/var/nslog']
      format: ['prometheus']
    basic_auth:
     username: 'prom_user'
     password: 'user_password'
    scheme: http
    scrape_interval: 30s
    static_configs:
     - targets: ['10.102.34.231:80']
<!--NeedCopy-->
```

Ajouter Prometheus comme source de données dans Grafana

Si vous avez besoin de visualiser les métriques à l'aide des tableaux de bord Grafana, vous devez ajouter Prometheus en tant que source de données dans Grafana. Pour plus d'informations, voir Ajouter Prometheus en tant que source de données dans Grafana.

Créez la visualisation des métriques dans Grafana

Vous pouvez créer un tableau de bord Grafana et sélectionner les indicateurs clés et le type de visualisation approprié.

La procédure suivante montre comment ajouter une métrique au panneau Grafana et créer un exemple de tableau de bord de visualisation.

1. Spécifiez le titre du panneau.
2. Dans l'onglet Requête, pour la requête A, spécifiez la métrique requise.
3. Dans l'onglet Paramètres, sélectionnez le type de visualisation.

Vous pouvez modifier les données et leur représentation dans Grafana. Pour plus d'informations, consultez la documentation Grafana.

Voici un exemple de tableau de bord Grafana avec quelques métriques NetScaler :

Dans ce tableau de bord, vous pouvez consulter des graphiques pour différentes métriques NetScaler, telles que :

- `vsvr_tot_Hits`: indique le nombre de demandes reçues par le serveur virtuel.
- `cc_cpu_use`: affiche le pourcentage d'utilisation du processeur.
- `http_tot_Requests`: affiche les requêtes HTTP reçues.
- `serv_tot_serviced`: affiche la demande en cours de traitement.
- `mem_cur_used_size`: affiche la mémoire actuellement utilisée par l'appliance NetScaler.

Exemples de graphes de Prometheus

À l'aide du navigateur d'expressions Prometheus, vous pouvez afficher les métriques de séries chronologiques collectées par le serveur Prometheus. Vous pouvez accéder au navigateur d'expressions en le pointant `prometheu-server-ip-address/graph` dans votre navigateur. Vous pouvez saisir une expression et voir le résultat sous forme de tableau ou de graphique au fil du temps. Spécifiez la métrique exacte que vous souhaitez afficher en saisissant le nom de la métrique dans le champ Expression. Vous pouvez spécifier plusieurs compteurs à l'aide de différents panneaux.

Le diagramme suivant montre les graphes de Prometheus pour deux métriques NetScaler et. `cpu_usehttp_tot_requests`



Exemple de tableau de bord Grafana

Vous pouvez télécharger les exemples de tableaux de bord depuis la page de téléchargement de NetScaler.

Vous trouverez ci-dessous un exemple de tableau de bord Grafana avec la possibilité de consulter les différentes mesures de l'infrastructure globale en un seul endroit, telles que l'état de NetScaler, l'état du serveur virtuel, l'état des applications (applications HTTP et TCP) et la sécurité des applications (applications SSL).

Vous pouvez développer la section correspondante dans le tableau de bord pour afficher la visualisation détaillée de chaque section, telle que les applications HTTP, les applications SSL, les applications TCP, les statistiques des serveurs virtuels (vStats) et les statistiques NetScaler.

Le schéma suivant montre un exemple de tableau de bord Grafana avec des statistiques NetScaler étendues :

Informations supplémentaires

Schéma avec les compteurs NetScaler requis pour l'exportation

Le collecteur de métriques exporte les compteurs présents dans le fichier de schéma configuré. Le `/var/metrics_conf/schema.json` fichier est le fichier de schéma par défaut configuré dans le profil d'analyse.

Le fichier de schéma est une liste de types d'entités et de compteurs associés. Dans le schéma, tous les compteurs globaux ou au niveau du système sont regroupés sous le type `netscaler`d'entité. Certains des compteurs globaux sont l'utilisation du processeur (`cpu_use`), l'utilisation du processeur de gestion (`mgmt_cpu_use`) et le nombre total de requêtes HTTP reçues (`http_tot_Requests`). Les compteurs spécifiques aux groupes de services `lbvserver`, `csvserver`, etc. sont répertoriés sous les types d'entités respectifs.

Vous trouverez ci-dessous un exemple de compteurs contenus dans le `schema.json` fichier pour l'entité serveur virtuel d'authentification (`vserver_authn`).

```
1  "vserver_authn":
2    [
```



```
      {
"name":"si_tot_Requests","rate":"True" }
,
      {
"name":"si_tot_Responses","rate":"True" }
,
      {
"name":"si_tot_RequestBytes","rate":"True" }
,
      {
"name":"si_cur_state","rate":"False" }
,
      {
"name":"si_tot_ResponseBytes","rate":"True" }
,
      {
"name":"si_peer_port","rate":"True" }
,
      {
"name":"vsvr_Protocol","rate":"False" }

 ]
```

Le tableau suivant explique les compteurs mentionnés dans cet exemple :

Nom du compteur	Description
`si_tot_Requests`	Nombre total de demandes reçues sur ce service ou ce serveur virtuel.
`si_tot_Responses`	Nombre total de réponses reçues sur ce service ou ce serveur virtuel.
`si_tot_RequestBytes`	Nombre total d'octets de demande reçus sur ce service ou serveur virtuel.
`si_cur_state`	État actuel du serveur virtuel.
`si_tot_ResponseBytes`	Nombre total d'octets de réponse reçus sur ce service ou ce serveur virtuel.
`si_peer_port`	Port sur lequel le service s'exécute.
`vsvr_Protocol`	Protocole associé au serveur virtuel.

Le `rate` champ peut être défini comme `True` s'il s'agissait de la valeur du taux qu'un compteur doit

exporter. Par exemple, le taux de `si_tot_Requests` est exporté si le `rate` est défini sur `True` pour `si_tot_Requests`.

Vous trouverez ci-dessous un exemple de compteurs de l' `netscaler` entité.

```
 "netscaler":
   [
       {
"name":"cpu_use","rate":"False" }
,
       {
"name":"mgmt_cpu_use","rate":"False" }
,
       {
"name":"tcp_tot_rxpkts","rate":"True" }
,
       {
"name":"tcp_tot_rxbytes","rate":"True" }
,
       {
"name":"tcp_tot_txpkts","rate":"True" }
,
       {
"name":"tcp_tot_txbytes","rate":"True" }
,
       {
"name":"tcp_cur_ClientConnEst","rate":"False" }
,
       {
"name":"tcp_cur_ServerConnEst","rate":"False" }
,
       {
"name":"tcp_cur_ClientConn","rate":"False" }
,
       {
"name":"tcp_cur_ClientConnClosing","rate":"False" }
,
       {
"name":"tcp_tot_ClientOpen","rate":"True" }
,
       {
"name":"tcp_cur_ServerConn","rate":"False" }
,
       {
"name":"tcp_cur_ServerConnClosing","rate":"False" }
```



```
41  ,
42          {
43  "name":"http_tot_Requests","rate":"True" }
44  ,
45          {
46  "name":"http_tot_Responses","rate":"True" }
47  ,
48          {
49  "name":"http_tot_Gets","rate":"True" }
50  ,
51          {
52  "name":"http_tot_Posts","rate":"True" }
53  ,
54          {
55  "name":"http_tot_Others","rate":"True" }
56  ,
57     ]
```

Le tableau suivant explique les compteurs mentionnés dans cet exemple :

Nom du compteur	Description
cpu_use	Suit le pourcentage d'utilisation du processeur (pourcentage d'utilisation du processeur * 10).
tcp_tot_rxpkts	Paquets TCP reçus.
tcp_tot_rxbytes	Octets de données TCP reçus.
tcp_tot_txpkts	Paquets TCP transmis.
tcp_tot_txbytes	Octets de données TCP transmis.
tcp_cur_ClientConnEst	Les connexions client actuelles sont dans l'état Établi, ce qui indique qu'un transfert de données peut avoir lieu entre l'appliance NetScaler et le client.
tcp_cur_ServerConnEst	Les connexions au serveur en cours sont dans l'état Établi, ce qui indique qu'un transfert de données peut avoir lieu entre l'appliance NetScaler et le serveur.
tcp_cur_ClientConn	Connexions client, y compris les connexions à l'état Ouvrir, Établi et Fermer. Connexions au serveur, y compris les connexions à l'état Ouvrir, Établi et Fermer.

Nom du compteur	Description
tcp_cur_ClientConnClosing	Les connexions client sont dans l'état de fermeture, ce qui indique que le processus de fin de connexion a débuté mais n'est pas terminé.
tcp_cur_ServerConn	Connexions au serveur, y compris les connexions à l'état Ouvrir, Établi et Fermer.
tcp_cur_ServerConnClosing	Les connexions au serveur sont en cours de fermeture, ce qui indique que le processus de fin de connexion a débuté mais n'est pas terminé.
http_tot_Requests	Ce compteur assure le suivi des requêtes HTTP reçues à l'aide de la méthode GET.
http_tot_Responses	Ce compteur assure le suivi des requêtes HTTP reçues à l'aide de la méthode POST.
http_tot_Gets	Ce compteur assure le suivi des requêtes HTTP reçues à l'aide de la méthode GET.
http_tot_Posts	Ce compteur assure le suivi des requêtes HTTP reçues.
http_tot_Others	Ce compteur suit les requêtes HTTP reçues à l'aide de méthodes autres que GET et POST.

Vous trouverez ci-dessous un exemple de compteurs de l' vserver_ssl entité.

```
"vserver_ssl":
[
    {
 "name":"ssl_ctx_tot_session_hits","rate":"True" }
 ,
    {
 "name":"ssl_ctx_tot_session_new","rate":"True" }
 ,
    {
 "name":"ssl_ctx_tot_enc_bytes","rate":"True" }
 ,
    {
 "name":"ssl_ctx_tot_dec_bytes","rate":"True" }
 ,
]
```


Le tableau suivant explique les compteurs SSL mentionnés dans cet exemple :

Nom du compteur	Description
ssl_ctx_tot_session_hits	Ce compteur enregistre le nombre d'accès à la session.
ssl_ctx_tot_session_new	Ce compteur enregistre le nombre de nouvelles sessions créées.
ssl_ctx_tot_enc_bytes	Ce compteur suit le nombre d'octets chiffrés par serveur virtuel SSL.
ssl_ctx_tot_dec_bytes	Ce compteur suit le nombre d'octets déchiffrés par serveur virtuel SSL.

Configurer l'accès en lecture seule à Prometheus pour un utilisateur qui n'est pas un superutilisateur

Procédez comme suit pour configurer l'accès en lecture seule à Prometheus pour un utilisateur qui n'est pas un superutilisateur.

1. Ajoutez un nouvel utilisateur à l'appliance NetScaler.

```
add system user <ns_user_name> <ns_user's_password> -externalAuth
    enabled -promptString user-%u-at-%T logging enaBLED
```

   Exemple :

```
add system user nspaul nspaul -externalAuth enabled -promptString
    user-%u-at-%T logging enaBLED
```

2. Créez une stratégie de commande pour un utilisateur en lecture seule. Cette stratégie de commande autorise l'accès en lecture seule à partir de n'importe quel fichier sous le `/var/nslog/` `directory`.

```
add system cmdPolicy read-only-prometheus ALLOW "(^man.*)|(^show\\
    s+(?!system)(?!configstatus)(?!ns ns\\.conf)(?!ns savedconfig)
    (?!ns runningConfig)(?!gslb runningConfig)(?!audit messages)(?!
    techsupport).*)|(^stat.*)|(show system file .* -filelocation
    \"/var/nslog\")"
```

3. Si les métriques ne sont écrites que dans un certain fichier, vous pouvez même limiter l'accès des utilisateurs de telle sorte qu'ils ne puissent accéder qu'à ce fichier spécifique.


```
add system cmdPolicy read-only-prometheus ALLOW "(^man.*)|(^show\\
    s+(!system)(!configstatus)(!ns ns\\.conf)(!ns savedconfig)
(!ns runningConfig)(!gslb   runningConfig)(!audit messages)(!
    techsupport).*)|(^stat.*)
|(show system file metrics_prom_<name_of_timeseries_profile>.log -
    filelocation \"/var/nslog\")"
```

> **Remarque :**
>
> Dans la `show system file` commande, spécifiez le nom du profil de série chronologique que vous avez configuré à la place `name_of_ timeseries_profile`.

4. Liez un utilisateur à la stratégie de commande.

```
bind system user <userName> ((<policyName> <priority>) | -
    partitionName <string>)
```

Par exemple :

```
bind system user user1 read-only-prometheus 0
```

Pour dissocier et supprimer un utilisateur de la stratégie de commande, utilisez les commandes suivantes :

1. Dissociez un utilisateur configuré de la stratégie de commande du système.

```
unbind system user <userName> (<policyName> | -partitionName <
    string>
```

Par exemple :

```
unbind system user user1 read-only-prometheus
```

2. Supprimez la commande Policy de NetScaler.

```
rm system cmdPolicy read-only-prometheus
```

Abonnement de compteurs pour plusieurs profils de séries chronologiques

NetScaler prend désormais en charge la création de plusieurs profils de séries chronologiques et spécifie un ensemble de compteurs différent pour chaque profil. Vous pouvez également exporter uniquement les compteurs en fonction de vos besoins.

Vous devez créer plusieurs `schema.json` fichiers contenant les compteurs nécessaires avec des noms uniques et l' `.json` extension pour configurer plusieurs profils de séries chronologiques. Un

fichier de schéma de référence `reference_schema.json` est disponible sous le chemin `/var/metrics_conf/`. Vous pouvez modifier le schéma de référence selon vos besoins et l'utiliser en conséquence.

La configuration des deux nouveaux profils de séries chronologiques est la suivante :

```
add analytics profile ns_analytics_timeseries_profile_1   -type timeseries -schemaFile schema1.json

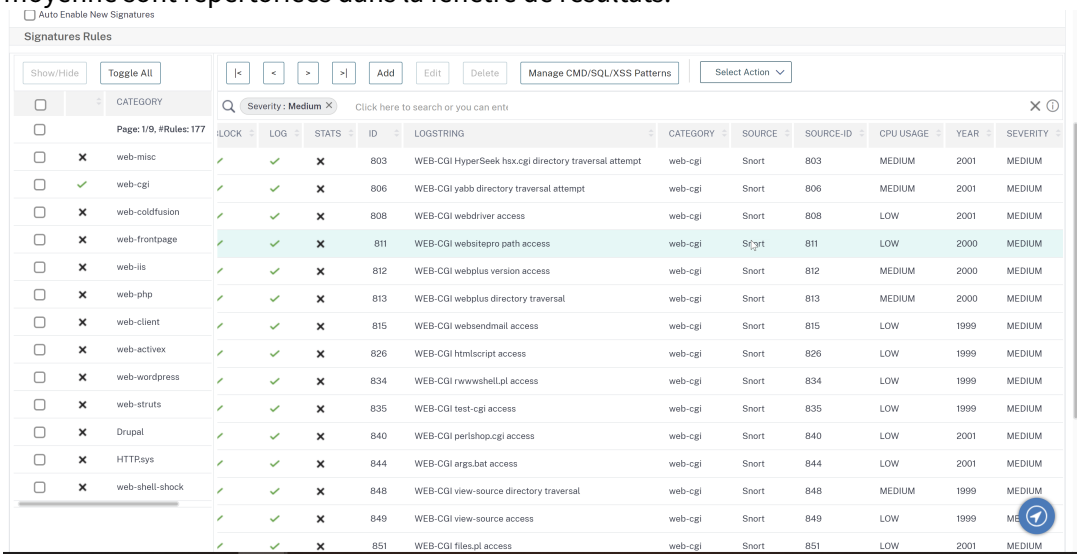
set analytics profile  ns_analytics_timeseries_profile_1 -outputMode prometheus -serveMode PULL -metrics ENABLED

add analytics profile ns_analytics_timeseries_profile_2   -type timeseries -schemaFile schema2.json

set analytics profile  ns_analytics_timeseries_profile_2 -outputMode prometheus -serveMode PULL -metrics ENABLED
```

Dans cet exemple, `schema1.json` et `schema2.json` possèdent différents ensembles de compteurs.

Configuration de Prometheus

La configuration d'un fichier `prometheus.yml` d'exemple est la suivante :

```
scrape_configs:
  - job_name: 'vpx2_metrics_direct'
    metrics_path: /nitro/v1/config/systemfile
    params:
      args: ['filename:metrics_prom_ns_analytics_time_series_profile.log,filelocation:/var/nslog']
      format: ['prometheus']
    basic_auth:
     username: 'prom_user'
     password: 'user_password'
    scheme: https
    scrape_interval: 30s
    static_configs:
     - targets: ['<ADC1-ip>:<port>', '<ADC2-ip>:<port>']
<!--NeedCopy-->
```


Exportation des journaux d'audit et des événements directement depuis NetScaler vers Splunk

May 5, 2023

La journalisation des audits vous permet de consigner les états de NetScaler et les informations d'état collectées par les différents modules de NetScaler. En consultant les journaux, vous pouvez résoudre les problèmes ou les erreurs et les corriger.

Vous pouvez désormais exporter des journaux d'audit et des événements depuis NetScaler vers des plateformes d'agrégation de journaux standard telles que Splunk et obtenir des informations pertinentes.

Il existe plusieurs manières d'exporter les journaux d'audit de NetScaler vers Splunk. Vous pouvez configurer Splunk en tant que serveur syslog ou en tant que serveur HTTP. Cette rubrique fournit des informations sur la configuration de Splunk en tant que serveur HTTP à l'aide du collecteur d'événements HTTP Splunk. À l'aide du collecteur d'événements HTTP, vous pouvez envoyer des journaux d'audit via HTTP (ou HTTPS) directement à la plateforme Splunk depuis votre NetScaler.

Configurer l'exportation des journaux d'audit de NetScaler vers Splunk

Pour configurer l'exportation des journaux d'audit, vous devez suivre les étapes suivantes :

1. Configurez le collecteur d'événements HTTP sur Splunk.
2. Créez un service de collecte et un profil d'analyse de séries chronologiques sur NetScaler.

Configurer le collecteur d'événements HTTP sur Splunk

Vous pouvez transmettre les journaux d'audit à Splunk en configurant un collecteur d'événements HTTP.

Consultez la documentation de Splunk pour savoir comment configurer le collecteur d'événements HTTP.

Une fois que vous avez configuré le collecteur d'événements HTTP, copiez le jeton d'authentification et enregistrez-le pour référence. Vous devez spécifier ce jeton lors de la configuration du profil d'analyse sur NetScaler.

Configurer le profil d'analyse des séries chronologiques sur NetScaler

Procédez comme suit pour exporter les journaux d'audit NetScaler vers Splunk.

1. Créez un service de collecte pour Splunk.


```
add service <collector> <splunk-server-ip-address> <protocol> <
    port>
```

Exemple :

```
add service splunk_service 10.102.34.155 HTTP 8088
```

Dans cette configuration :

- `ip-address`: Spécifiez l'adresse IP du serveur Splunk.
- `collector-name`: Spécifiez le collecteur.
- `protocol`: Spécifiez le protocole HTTP ou HTTPS
- `port`: Spécifiez le numéro de port.

2. Créez un profil d'analyse de séries chronologiques.

```
add analytics profile <profile-name> -type time series -
    auditlog enabled -collectors <collector-name>  -
    analyticsAuthToken <"auth-tocken">
-analyticsEndpointContentType <"Application/json"> -
    analyticsEndpointMetadata <"meta-data-for-endpoint:"> -
    analyticsEndpointUrl <"endpoint-url">
```

Exemple :

```
add analytics profile audit_profile -type timeseries -auditlog
     enabled -collectors splunk -analyticsAuthToken "
    1234-5678-12345" -analyticsEndpointContentType "Application
    /json" -analyticsEndpointMetadata "Event:" -
    analyticsEndpointUrl "/services/collector/event"
```

Dans cette configuration :

- `auditlog`: Spécifiez la valeur `enabled` pour activer la journalisation des audits.
- `analyticsAuthToken`: Spécifiez le jeton d'authentification à inclure dans l'en-tête d'autorisation lors de l'envoi des journaux à Splunk. Ce jeton est le jeton d'authentification créé sur le serveur Splunk lors de la configuration du collecteur d'événements HTTP.
- `analyticsEndpointContentType`: Spécifiez le format des journaux.
- `analyticsEndpointMetadata`: Spécifiez les métadonnées spécifiques au point de terminaison.
- `analyticsEndpointUrl`: Spécifiez l'emplacement sur le point de terminaison pour exporter les journaux.

> **Remarque :**
>
> Vous pouvez modifier les paramètres du profil d'analyse des séries chronologiques à l'aide de la `set analytics profile` commande.

3. Vérifiez la configuration du profil d'analyse à l'aide de la commande show analytics profile.

```
# show analytics profile audit_profile

1)    Name: audit_profile
      Collector: splunk
      Profile-type: timeseries
            Output Mode: avro
            Metrics: DISABLED
              Schema File: schema.json
              Metrics Export Frequency: 30
            Events: DISABLED
            Auditlog: ENABLED
            Serve mode: Push
       Authentication Token: <auth-tocken>
       Endpoint URL: /services/collector/event
       Endpoint Content-type: Application/json
       Endpoint Metadata: Event:
       Reference Count: 0
```

Une fois la configuration réussie, les journaux d'audit sont envoyés sous forme de charges utiles HTTP à Splunk et vous pouvez les consulter sur l'interface utilisateur de l'application Splunk.

Configurer l'exportation d'événements depuis NetScaler vers Splunk

Pour configurer l'exportation des événements, vous devez suivre les étapes suivantes :

1. Configurez le collecteur d'événements HTTP sur Splunk en suivant les étapes décrites dans Configurer le collecteur d'événements HTTP sur Splunk.
2. Créez un service de collecteur sur NetScaler en suivant l'étape 1 de la section Configurer le profil d'analyse des séries chronologiques surNetScaler.
3. Créez un profil d'analyse de séries chronologiques sur NetScaler à l'aide de la `add analytics profile` commande. Vous devez spécifier l' `-events enabled` option au lieu de l' `-auditlog enabled` option lors de la création du profil d'analyse.

   Exemple :

```
add analytics profile event_profile -type timeseries -events
    enabled -collectors splunk -analyticsAuthToken "1234-5678-12345
```



```
" -analyticsEndpointContentType "Application/json" -
analyticsEndpointMetadata "Event:" -analyticsEndpointUrl "/
services/collector/event"
```

Web App Firewall NetScaler

June 20, 2023

Le pare-feu NetScaler Web App Firewall propose des options faciles à configurer pour répondre à un large éventail d'exigences de sécurité des applications. Les profils Web App Firewall, qui consistent en des ensembles de contrôles de sécurité, peuvent être utilisés pour protéger à la fois les demandes et les réponses en effectuant des inspections approfondies au niveau des paquets. Chaque profil inclut une option permettant de sélectionner des protections de base ou des protections avancées. Certaines protections peuvent nécessiter l'utilisation d'autres fichiers. Par exemple, les contrôles de validation XML peuvent nécessiter des fichiers WSDL ou de schéma. Les profils peuvent également utiliser d'autres fichiers, tels que des signatures ou des objets d'erreur. Ces fichiers peuvent être ajoutés localement ou importés à l'avance et enregistrés sur l'appliance pour une utilisation ultérieure.

Chaque stratégie identifie un type de trafic et ce trafic est inspecté pour détecter les violations de contrôle de sécurité spécifiées dans le profil associé à la stratégie. Les stratégies peuvent avoir différents points de liaison, qui déterminent la portée de la stratégie. Par exemple, une stratégie liée à un serveur virtuel spécifique est invoquée et évaluée uniquement pour le trafic transitant par ce serveur virtuel. Les stratégies sont évaluées dans l'ordre de leurs priorités désignées, et la première qui correspond à la demande ou à la réponse est appliquée.

- Déploiement rapide de la protection par pare-feu des applications Web

  Vous pouvez utiliser la procédure suivante pour déployer rapidement la sécurité du Web App Firewall :

  1. Ajoutez un profil de Web App Firewall et sélectionnez le type approprié (html, xml, JSON) en fonction des exigences de sécurité de l'application.
  2. Sélectionnez le niveau de sécurité requis (de base ou avancé).
  3. Ajoutez ou importez les fichiers requis, tels que des signatures ou WSDL.
  4. Configurez le profil pour qu'il utilise les fichiers et apportez toute autre modification nécessaire aux paramètres par défaut.
  5. Ajoutez une stratégie de Web App Firewall pour ce profil.
  6. Liez la stratégie au point de liaison cible et spécifiez la priorité.

- Entités de Web App Firewall

  Profil : un profil Web App Firewall spécifie ce qu'il faut rechercher et ce qu'il faut faire. Il examine à la fois la demande et la réponse afin de déterminer quelles violations potentielles de sécurité

doivent être vérifiées et quelles mesures doivent être prises lors du traitement d'une transaction. Un profil peut protéger une charge utile HTML, XML ou HTML et XML. En fonction des exigences de sécurité de l'application, vous pouvez créer un profil de base ou un profil avancé. Un profil de base peut protéger contre les attaques connues. Si une sécurité accrue est requise, vous pouvez déployer un profil avancé pour permettre un accès contrôlé aux ressources de l'application et bloquer les attaques Zero Day. Cependant, un profil de base peut être modifié pour offrir des protections avancées, et inversement. Plusieurs choix d'actions (par exemple, bloquer, enregistrer, apprendre et transformer) sont disponibles. Les contrôles de sécurité avancés peuvent utiliser des cookies de session et des balises de formulaire masquées pour contrôler et surveiller les connexions des clients. Les profils de Web App Firewall peuvent apprendre les violations déclenchées et suggérer les règles de relaxation.

Protections de base : un profil de base inclut un ensemble préconfiguré de règles de relaxation d'URL de démarrage et de refus d'URL. Ces règles d'assouplissement déterminent quelles demandes doivent être autorisées et celles qui doivent être refusées. Les demandes entrantes sont comparées à ces listes et les actions configurées sont appliquées. Cela permet à l'utilisateur de sécuriser les applications avec une configuration minimale pour les règles de relaxation. Les règles d'URL de démarrage protègent contre la navigation forcée. Les vulnérabilités connues des serveurs Web exploitées par des pirates peuvent être détectées et bloquées en activant un ensemble de règles de refus d'URL par défaut. Les attaques lancées couramment, telles que Buffer Overflow, SQL ou cross-site scripting peuvent également être facilement détectées.

Protections avancées : comme son nom l'indique, les protections avancées sont utilisées pour les applications qui présentent des exigences de sécurité plus élevées. Les règles de relaxation sont configurées pour autoriser l'accès à des données spécifiques et bloquer le reste. Ce modèle de sécurité positif atténue les attaques inconnues, qui peuvent ne pas être détectées par les contrôles de sécurité de base. Outre toutes les protections de base, un profil avancé permet de suivre la session d'un utilisateur en contrôlant la navigation, en vérifiant la présence de cookies, en spécifiant les exigences de saisie pour les différents champs de formulaire et en protégeant contre la falsification des formulaires ou les attaques de falsification de demandes intersites. L'apprentissage, qui observe le trafic et déploie les relaxations appropriées, est activé par défaut pour de nombreux contrôles de sécurité. Bien que faciles à utiliser, les protections avancées nécessitent une attention particulière, car elles offrent une sécurité plus étroite, mais nécessitent également plus de traitement et ne permettent pas l'utilisation de la mise en cache, ce qui peut affecter les performances.

Importer—La fonctionnalité d'importation est utile lorsque les profils Web App Firewall doivent utiliser des fichiers externes, c'est-à-dire des fichiers hébergés sur un serveur Web externe ou interne, ou qui doivent être copiés à partir d'une machine locale. Il est utile d'importer un fichier et de le stocker sur l'appliance, en particulier dans les situations où vous devez contrôler l'accès à des sites Web externes, ou lorsque la compilation prend beaucoup de temps, que des fichiers

volumineux doivent être synchronisés sur des déploiements HA ou vous pouvez réutiliser un fichier en le copiant sur plusieurs périphériques. Par exemple :

- Les WSDL hébergés sur des serveurs Web externes peuvent être importés localement avant de bloquer l'accès à des sites Web externes.
- Les fichiers de signature volumineux générés par un outil d'analyse externe tel que Cenzic peuvent être importés et précompilés à l'aide du schéma de l'appliance NetScaler ADC.
- Une page d'erreur HTML ou XML personnalisée peut être importée à partir d'un serveur Web externe ou copiée à partir d'un fichier local.

Signatures—Les signatures sont puissantes, car elles utilisent la correspondance de motifs pour détecter les attaques malveillantes et peuvent être configurées pour vérifier à la fois la demande et la réponse d'une transaction. Ils sont une option privilégiée lorsqu'une solution de sécurité personnalisable est nécessaire. Plusieurs choix (par exemple, bloquer, enregistrer, apprendre et transformer) sont disponibles pour l'action à effectuer lorsqu'une correspondance de signature est détectée. Le Web App Firewall possède un objet de signature par défaut intégré composé de plus de 1 300 règles de signature, avec une option permettant d'obtenir les règles les plus récentes à l'aide de la fonction de mise à jour automatique. Les règles créées par d'autres outils d'analyse peuvent également être importées. L'objet de signature peut être personnalisé en ajoutant de nouvelles règles, qui peuvent fonctionner avec les autres contrôles de sécurité spécifiés dans le profil Web App Firewall. Une règle de signature peut comporter plusieurs modèles et ne peut signaler une violation que lorsque tous les modèles correspondent, évitant ainsi les faux positifs. Une sélection minutieuse d'un `fastmatch` motif littéral pour une règle peut considérablement optimiser le temps de traitement.

Stratégies—Les stratégies de pare-feu Web App sont utilisées pour filtrer et séparer le trafic en différents types. Cela offre la flexibilité nécessaire pour implémenter différents niveaux de protection de sécurité pour les données de l'application. L'accès à des données très sensibles peut être dirigé vers des inspections de sécurité avancées, tandis que les données moins sensibles sont protégées par des inspections de sécurité de base. Des stratégies peuvent également être configurées pour contourner les contrôles de sécurité en cas de trafic inoffensif. Une sécurité accrue nécessite davantage de traitement. Une conception soignée des stratégies peut donc fournir la sécurité souhaitée ainsi que des performances optimisées. La priorité de la stratégie détermine l'ordre dans lequel elle est évaluée, et son point de référence détermine la portée de son application.

Résumé

1. Possibilité de sécuriser un large éventail d'applications en protégeant différents types de données, en mettant en œuvre le niveau de sécurité approprié pour différentes ressources, tout en obtenant des performances optimales.

2. Possibilité d'ajouter ou de modifier une configuration de sécurité. Vous pouvez renforcer ou assouplir les contrôles de sécurité en activant ou en désactivant les protections de base et avancées.
3. Possibilité de convertir un profil HTML en profil XML ou Web2.0 (HTML+XML) et inversement, offrant la flexibilité nécessaire pour renforcer la sécurité pour différents types de charge utile.
4. Des actions faciles à déployer pour bloquer les attaques, les surveiller dans des journaux, collecter des statistiques ou même transformer certaines chaînes d'attaques pour les rendre inoffensives.
5. Possibilité de détecter les attaques en inspectant les demandes entrantes et de prévenir les fuites de données sensibles en inspectant les réponses envoyées par les serveurs.
6. Possibilité d'apprendre à partir du modèle de trafic pour obtenir des recommandations concernant des règles de relaxation facilement modifiables qui peuvent être déployées pour autoriser les exceptions.
7. Modèle de sécurité hybride qui applique la puissance des signatures personnalisables pour bloquer les attaques correspondant à des modèles spécifiques, et qui offre la flexibilité nécessaire pour utiliser les contrôles du modèle de sécurité positif pour des protections de sécurité de base ou avancées.
8. Disponibilité de rapports de configuration complets, y compris des informations sur la conformité à la norme PCI-DSS.

FAQ et guide de déploiement

June 20, 2023

Q : Pourquoi le pare-feu NetScaler Web App Firewall est-il le choix préféré pour sécuriser les applications ?

Avec les fonctionnalités suivantes, le NetScaler Web App Firewall offre une solution de sécurité complète :

- **Modèle de sécurité hybride : le modèle** de sécurité hybride de NetScaler vous permet de tirer parti à la fois d'un modèle de sécurité positif et d'un modèle de sécurité négatif pour créer une configuration parfaitement adaptée à vos applications.
  - Le**modèle de sécurité positif** protège contre le Buffer Overflow, la manipulation de paramètres CGI-BIN, la manipulation de formulaires et de champs cachés, la navigation forcée, l'empoisonnement des cookies ou des sessions, les listes de contrôle d'accès brisées, les scripts intersites (script intersite), l'injection de commandes, l'injection SQL, le déclenchement d'erreur sensible Fuite d'informations, utilisation non sécurisée de la cryptographie, mauvaise configuration du serveur, portes dérobées et options de

débogage, application de la stratégie basée sur les taux, vulnérabilités bien connues de la plate-forme, exploits zero-day, falsification des demandes intersites (CSRF) et fuite de cartes de crédit et d'autres données sensibles.

- **Le modèle de sécurité négatif** utilise un ensemble de signatures enrichies pour se protéger contre les vulnérabilités des applications L7 et HTTP. Le Web App Firewall est intégré à plusieurs outils d'analyse tiers, tels que ceux proposés par Cenzic, Qualys, Whitehat et IBM. Les fichiers XSLT intégrés permettent d'importer facilement des règles, qui peuvent être utilisées conjointement avec les règles Snort au format natif. Une fonctionnalité de mise à jour automatique obtient les dernières mises à jour des nouvelles vulnérabilités.

Le modèle de sécurité positif peut être le choix privilégié pour protéger les applications qui ont un besoin élevé de sécurité, car il vous donne la possibilité de contrôler entièrement qui peut accéder à quelles données. Vous n'autorisez que ce que vous voulez et bloquez le reste. Ce modèle inclut une configuration de vérification de sécurité intégrée, qui peut être déployée en quelques clics. Cependant, gardez à l'esprit que plus la sécurité est renforcée, plus la surcharge de traitement est importante.

Le modèle de sécurité négative peut être préférable pour les applications personnalisées. Les signatures vous permettent de combiner plusieurs conditions, et une correspondance et l'action spécifiée sont déclenchées uniquement lorsque toutes les conditions sont remplies. Vous ne bloquez que ce que vous ne voulez pas et vous autorisez le reste. Un modèle de correspondance rapide spécifique dans un emplacement spécifié peut réduire considérablement la surcharge de traitement afin d'optimiser les performances. La possibilité d'ajouter vos propres règles de signature, en fonction des besoins de sécurité spécifiques de vos applications, vous donne la possibilité de concevoir vos propres solutions de sécurité personnalisées.

- **Détection et protection côté demande et réponse :** Vous pouvez inspecter les demandes entrantes pour détecter tout comportement suspect et prendre les mesures appropriées, et vous pouvez vérifier les réponses pour détecter et protéger contre les fuites de données sensibles.
- **Ensemble complet de protections intégrées pour les charges utiles HTML, XML et JSON :** le Web App Firewall offre 19 contrôles de sécurité différents. Six d'entre eux (tels que Start URL et Deny URL) s'appliquent aux données HTML et XML. Cinq vérifications (telles que la cohérence des champs et le format des champs) sont spécifiques au HTML, et huit (telles que le format XML et l'interopérabilité des services Web) sont spécifiques aux charges utiles XML. Cette fonctionnalité inclut un ensemble complet d'actions et d'options. Par exemple, la fermeture d'URL vous permet de contrôler et d'optimiser la navigation sur votre site Web, pour vous protéger contre une navigation forcée sans avoir à configurer des règles de relaxation pour autoriser chaque URL légitime. Vous avez la possibilité de supprimer ou de supprimer les données sensibles, telles que les numéros de carte de crédit, dans la réponse. Que ce soit la protection contre les attaques SOAP Array, le déni de service XML (XDoS), la prévention de l' analyse WSDL, la vérification des pièces jointes ou tout autre type d'attaques XML, vous avez le confort de savoir que vous

disposez d'un bouclier inébranlable protégeant vos données lorsque vos applications sont protégées par le Web App Firewall. Les signatures vous permettent de configurer des règles à l'aide d'expressions XPath pour détecter les violations dans le corps ainsi que dans l'en-tête d'une charge utile JSON.

- **GWT :** prise en charge de la protection des applications Google Web Toolkit pour se protéger contre les violations de SQL, de script intersite et de vérification de la cohérence des champs de formulaire.
- **Interface utilisateur graphique (GUI) conviviale et sans Java : Une interface** graphique intuitive et des contrôles de sécurité préconfigurés facilitent le déploiement de la sécurité en cliquant sur quelques boutons. Un assistant vous invite et vous guide pour créer les éléments requis, tels que des profils, des stratégies, des signatures et des liaisons. L'interface graphique basée sur HTML5 est exempte de toute dépendance Java. Les performances sont nettement supérieures à celles des anciennes versions Java.
- **CLI facile à utiliser et automatisable :** La plupart des options de configuration disponibles dans l'interface graphique sont également disponibles dans l'interface de ligne de commande (CLI). Les commandes CLI peuvent être exécutées par un fichier de commandes et sont faciles à automatiser.
- **Support pour l'API REST :** le protocole NetScaler NITRO prend en charge un ensemble complet d'API REST pour automatiser la configuration du Web App Firewall et collecter des statistiques pertinentes pour une surveillance continue des violations de sécurité.
- **Apprentissage :** La capacité du Web App Firewall à apprendre en surveillant le trafic pour affiner la sécurité est très conviviale. Le moteur d'apprentissage recommande des règles, ce qui facilite le déploiement de relaxations sans maîtrise des expressions régulières.
- **Prise en charge de l'éditeur RegEx :** Les expressions régulières offrent une solution élégante au dilemme de la volonté de consolider les règles tout en optimisant la recherche. Vous pouvez tirer parti de la puissance des expressions régulières pour configurer des URL, des noms de champs, des modèles de signature, etc. L'éditeur RegEx intégré riche vous offre une référence rapide pour les expressions et fournit un moyen pratique de valider et de tester la précision de votre RegEx.
- **Page d'erreur personnalisée :** les demandes bloquées peuvent être redirigées vers une URL d'erreur. Vous avez également la possibilité d'afficher un objet d'erreur personnalisé qui utilise des variables prises en charge et la stratégie avancée de NetScaler (expressions PI avancées) pour intégrer les informations de dépannage destinées au client.
- Rapports**PCI-DSS, statistiques et autres rapports de violation :** le riche ensemble de rapports facilite le respect des exigences de conformité PCI-DSS, la collecte de statistiques sur les compteurs de trafic et l'affichage des rapports de violation pour tous les profils ou un seul profil.

- **Logging and click-to-rule from log :** La journalisation détaillée est prise en charge pour les formats natif et CEF. Le Web App Firewall vous offre la possibilité de filtrer les messages de journal ciblés dans la visionneuse Syslog. Vous pouvez sélectionner un message de journal et déployer une règle de relaxation correspondante en cliquant simplement sur un bouton. Vous avez la flexibilité de personnaliser les messages de journal et également la prise en charge de la génération de journaux Web. Pour plus de détails, consultez la rubrique Journaux du Web App Firewall .
- **Inclure les journaux de violation dans les enregistrements de trace :** la possibilité d'inclure des messages de journal dans les enregistrements de trace facilite le débogage d'un comportement inattendu tel que la réinitialisation et le blocage.
- **Clonage :** l'option utile de profil d'importation/exportation vous permet de cloner la configuration de sécurité d'une appliance NetScaler vers d'autres. Les options d'exportation des données apprises facilitent l'exportation des règles apprises vers un fichier Excel. Vous pouvez ensuite les faire examiner et approuver par le propriétaire de l'application avant de les appliquer.
- **Un modèle AppExpert** (un ensemble de paramètres de configuration) peut être conçu pour fournir une protection appropriée à vos sites Web. Vous pouvez simplifier et accélérer le déploiement d'une protection similaire sur d'autres appliances en exportant ces modèles de découpe vers un modèle.

Pour plus de détails, consultez la rubrique sur le modèle AppExpert.

- **Vérifications de sécurité sans session :** le déploiement de vérifications de sécurité sans session peut vous aider à réduire l'empreinte mémoire et à accélérer le traitement.
- **Interopérabilité avec les autres fonctionnalités de NetScaler :** le Web App Firewall fonctionne parfaitement avec les autres fonctionnalités de NetScaler, telles que la réécriture, la transformation d'URL, la mise en cache intégrée, le CVPN et la limitation du débit.
- **Prise en charge des expressions PI dans les stratégies :** vous pouvez tirer parti de la puissance des expressions PI avancées pour concevoir des stratégies afin d'implémenter différents niveaux de sécurité pour différentes parties de votre application.
- **Prise en charge d'IPv6 :** le Web App Firewall prend en charge les protocoles IPv4 et IPv6.
- **Protection de sécurité basée sur la géolocalisation :** vous pouvez utiliser la stratégie avancée NetScaler (PI Expressions) pour configurer des stratégies basées sur la localisation, qui peuvent être utilisées conjointement avec une base de données de localisation intégrée pour personnaliser la protection par pare-feu. Vous pouvez identifier les emplacements d'où proviennent les demandes malveillantes et appliquer le niveau d'inspection de sécurité souhaité pour les demandes provenant d'un emplacement géographique spécifique.
- **Performances :** la **diffusion en continu** côté demande améliore considérablement les performances. Dès qu'un champ est traité, les données résultantes sont transférées vers le back-end tandis que l'évaluation se poursuit pour les champs restants. L'amélioration du temps de traitement est particulièrement importante lorsque l'on manipule de gros poteaux.
- **Autres fonctionnalités de sécurité :** Le Web App Firewall comporte plusieurs autres

paramètres de sécurité qui peuvent contribuer à assurer la sécurité de vos données. Par exemple, le **champ confidentiel** vous permet de bloquer les fuites d'informations sensibles dans les messages de journal, et **Strip HTML Comment** vous permet de supprimer les commentaires HTML de la réponse avant de la transmettre au client. **Les types de champs** peuvent être utilisés pour spécifier les entrées autorisées dans les formulaires envoyés à votre application.

Q : Que dois-je faire pour configurer le Web App Firewall ?

Procédez comme suit :

- Ajoutez un profil de Web App Firewall et sélectionnez le type approprié (html, xml, web2.0) pour les exigences de sécurité de l'application.
- Sélectionnez le niveau de sécurité requis (de base ou avancé).
- Ajoutez ou importez les fichiers requis, tels que des signatures ou WSDL.
- Configurez le profil pour qu'il utilise les fichiers et apportez toute autre modification nécessaire aux paramètres par défaut.
- Ajoutez une stratégie de Web App Firewall pour ce profil.
- Liez la stratégie au point de liaison cible et spécifiez la priorité.

Q : Comment savoir quel type de profil choisir ?

Le profil Web App Firewall offre une protection pour les charges utiles HTML et XML. Selon les besoins de votre application, vous pouvez choisir un profil HTML ou un profil XML. Si votre application prend en charge les données HTML et XML, vous pouvez choisir un profil Web2.0.

Q : Quelle est la différence entre un profil de base et un profil avancé ? Comment puis-je choisir celui dont j'ai besoin ?

La décision d'utiliser un profil de base ou un profil avancé dépend des besoins de sécurité de votre application. Un profil de base inclut un ensemble préconfiguré de règles de relaxation URL de démarrage et Refuser l'URL. Ces règles de relaxation déterminent quelles demandes sont autorisées et lesquelles sont refusées. Les demandes entrantes sont mises en correspondance avec les règles préconfigurées et les actions configurées sont appliquées. L'utilisateur peut sécuriser les applications avec une configuration minimale des règles de relaxation. Les règles d'URL de démarrage protègent contre la navigation forcée. Les vulnérabilités connues des serveurs Web exploitées par des pirates peuvent être détectées et bloquées en activant un ensemble de règles de refus d'URL par défaut. Les attaques couramment lancées, telles que Buffer Overflow, SQL ou Cross-Site Scripting, peuvent également être facilement détectées.

Comme son nom l'indique, les protections avancées sont destinées aux applications qui ont des exigences de sécurité plus élevées. Les règles de relaxation sont configurées pour autoriser l'accès à

des données spécifiques et bloquer le reste. Ce modèle de sécurité positif atténue les attaques inconnues, qui peuvent ne pas être détectées par les contrôles de sécurité de base. En plus de toutes les protections de base, un profil avancé assure le suivi d'une session utilisateur en contrôlant la navigation, en vérifiant les cookies, en spécifiant les exigences de saisie pour divers champs de formulaire et en protégeant contre la falsification des formulaires ou les attaques Cross-Site Request Forgery. L'apprentissage, qui observe le trafic et recommande les assouplissements appropriés, est activé par défaut pour de nombreux contrôles de sécurité. Bien qu'elles soient faciles à utiliser, les protections avancées nécessitent une attention particulière, car elles offrent une sécurité plus stricte mais nécessitent également un traitement plus important. Certaines vérifications de sécurité avancées n'autorisent pas l'utilisation de la mise en cache, ce qui peut affecter les performances.

Gardez à l'esprit les points suivants lorsque vous décidez d'utiliser des profils de base ou avancés :

- Les profils de base et avancés ne font que commencer les modèles. Vous pouvez toujours modifier le profil de base pour déployer des fonctionnalités de sécurité avancées, et vice versa.
- Les contrôles de sécurité avancés nécessitent davantage de traitement et peuvent affecter les performances. À moins que votre application n'ait besoin d'une sécurité avancée, vous pouvez commencer par un profil de base et resserrer la sécurité selon les besoins de votre application.
- Vous ne souhaitez pas activer toutes les vérifications de sécurité, sauf si votre application en a besoin.

Q : Qu'est-ce qu'une stratégie ? Comment sélectionner le point de liaison et définir la priorité ?

Les stratégies de Web App Firewall peuvent vous aider à trier votre trafic en groupes logiques afin de configurer différents niveaux de mise en œuvre de la sécurité. Sélectionnez soigneusement les points de liaison des stratégies afin de déterminer quel trafic est mis en correspondance avec quelle stratégie. Par exemple, si vous souhaitez que chaque requête entrante soit vérifiée pour détecter les attaques de script SQL/intersite, vous pouvez créer une stratégie générique et la lier globalement. Si vous souhaitez appliquer des contrôles de sécurité plus stricts au trafic d'un serveur virtuel hébergeant des applications contenant des données sensibles, vous pouvez lier une stratégie à ce serveur virtuel.

Une affectation minutieuse des priorités peut améliorer le traitement du trafic. Vous souhaitez attribuer des priorités plus élevées à des stratégies plus spécifiques et des priorités plus faibles aux stratégies génériques. Notez que plus le nombre est élevé, plus la priorité est faible. Une stratégie avec une priorité de 10 est évaluée avant une stratégie qui a une priorité de 15.

Vous pouvez appliquer différents niveaux de sécurité pour différents types de contenus, par exemple les demandes d'objets statiques tels que les images et le texte peuvent être contournées à l'aide d'une stratégie et les demandes pour d'autres contenus sensibles peuvent être soumises à un contrôle très rigoureux à l'aide d'une deuxième stratégie.

Q : Comment puis-je configurer les règles pour sécuriser mon application ?

Le Web App Firewall permet de concevoir très facilement le niveau de sécurité approprié pour votre site Web. Vous pouvez avoir plusieurs stratégies de Web App Firewall, liées à différents profils de Web App Firewall, afin de mettre en œuvre différents niveaux d'inspections de vérification de sécurité pour vos applications. Vous pouvez d'abord surveiller les journaux pour savoir quelles menaces de sécurité sont détectées et quelles violations sont déclenchées. Vous pouvez ajouter manuellement les règles de relaxation ou tirer parti des règles apprises recommandées par le Web App Firewall pour déployer les assouplissements requis afin d'éviter les faux positifs.

Le NetScaler Web App Firewall prend en charge les **visualiseurs** dans l'interface graphique, ce qui facilite grandement la gestion des règles. Vous pouvez facilement afficher toutes les données sur un seul écran et agir sur plusieurs règles en un seul clic. Le plus grand avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de règles, en vous basant sur le délimiteur et l'URL de l'action. La prise en charge de Visualizer est disponible pour visualiser 1) les règles apprises et 2) les règles de relaxation.

1. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer sous forme d'assouplissements. Vous pouvez également ignorer (ignorer) les règles.
2. Le visualiseur des relaxations déployées vous offre la possibilité d'ajouter une nouvelle règle ou de modifier une règle existante. Vous pouvez également activer ou désactiver un groupe de règles en sélectionnant un nœud et en cliquant sur le bouton **Activer** ou **Désactiver** dans le visualiseur de relaxation.

Q : Que sont les signatures ? Comment savoir quelles signatures utiliser ?

Une signature est un objet qui peut comporter plusieurs règles. Chaque règle se compose d'un ou de plusieurs modèles pouvant être associés à un ensemble d'actions spécifié. Le Web App Firewall comporte un objet de signature par défaut intégré composé de plus de 1 300 règles de signature, avec une option permettant d'obtenir les dernières règles à l'aide de la fonctionnalité de **mise à jour automatique** pour obtenir une protection contre les nouvelles vulnérabilités. Les règles créées par d'autres outils d'analyse peuvent également être importées.

Les signatures sont très puissantes car elles utilisent la correspondance de motifs pour détecter les attaques malveillantes et peuvent être configurées pour vérifier à la fois la demande et la réponse d'une transaction. Ils sont une option privilégiée lorsqu'une solution de sécurité personnalisable est nécessaire. Plusieurs choix d'actions (par exemple, bloquer, consigner, apprendre et transformer) sont disponibles lorsqu'une correspondance de signature est détectée. Les signatures par défaut couvrent les règles pour protéger différents types d'applications, telles que web-cgi, web-coldfusion, web-frontpage, web-iis, web-php, web-client, web-activex, web-shell-shock et web-struts. Pour répondre aux besoins de votre application, vous pouvez sélectionner et déployer les règles appartenant à une catégorie spécifique.

Conseils d'utilisation des signatures :

- Vous pouvez simplement créer une copie de l'objet de signature par défaut et le modifier pour activer les règles dont vous avez besoin et configurer les actions souhaitées.
- L'objet de signature peut être personnalisé en ajoutant de nouvelles règles, qui peuvent fonctionner conjointement avec d'autres règles de signature.
- Les règles de signature peuvent également être configurées pour fonctionner conjointement avec les vérifications de sécurité spécifiées dans le profil de Web App Firewall. Si une correspondance indiquant une violation est détectée par une signature et un contrôle de sécurité, l'action la plus restrictive est celle qui est appliquée.
- Une règle de signature peut comporter plusieurs modèles et être configurée pour signaler une violation uniquement lorsque tous les modèles sont appariés, évitant ainsi les faux positifs.
- La sélection rigoureuse d'un modèle de correspondance rapide littéral pour une règle peut considérablement optimiser le temps de traitement.

Q : Le Web App Firewall fonctionne-t-il avec d'autres fonctionnalités de NetScaler ?

Le Web App Firewall est entièrement intégré à l'appliance NetScaler et fonctionne parfaitement avec d'autres fonctionnalités. Vous pouvez configurer une sécurité maximale pour votre application en utilisant d'autres fonctionnalités de sécurité NetScaler associées au Web App Firewall. Par exemple, **AAA-TM** peut être utilisé pour authentifier l'utilisateur, vérifier l'autorisation de l'utilisateur à accéder au contenu et consigner les accès, y compris les tentatives de connexion non valides. La**réécriture** peut être utilisée pour modifier l'URL ou pour ajouter, modifier ou supprimer des en-têtes, et **Responder** peut être utilisé pour fournir du contenu personnalisé à différents utilisateurs. Vous pouvez définir la charge maximale de votre site Web en utilisant la **limitation de débit** pour surveiller le trafic et limiter le taux s'il est trop élevé. La protection par**déni de service (DoS) HTTP** peut aider à faire la distinction entre les clients HTTP réels et les clients DoS malveillants. Vous pouvez réduire la portée de l'inspection de vérification de sécurité en liant les stratégies de Web App Firewall aux serveurs virtuels, tout en optimisant l'expérience utilisateur en utilisant la fonctionnalité d' **équilibrage de charge** pour gérer les applications très utilisées. Les demandes d'objets statiques tels que des images ou du texte peuvent contourner l'inspection des contrôles de sécurité, en tirant parti de la **mise en cache intégrée** ou de la **compression** pour optimiser l'utilisation de la bande passante pour ce contenu.

Q : Comment la charge utile est-elle traitée par le Web App Firewall et les autres fonctionnalités de NetScaler ?

Un diagramme présentant les détails du flux de paquets L7 dans une appliance NetScaler est disponible dans la section Ordre de traitement des fonctionnalités .

Q : Quel est le flux de travail recommandé pour le déploiement du Web App Firewall ?

Maintenant que vous connaissez les avantages de l'utilisation des protections de sécurité de pointe du NetScaler Web App Firewall, vous souhaiterez peut-être collecter des informations supplémentaires qui peuvent vous aider à concevoir la solution optimale pour vos besoins de sécurité. Citrix vous recommande d'effectuer les opérations suivantes :

- **Connaître votre environnement :** La connaissance de votre environnement vous aidera à identifier la meilleure solution de protection de sécurité (signatures, contrôles de sécurité ou les deux) pour vos besoins. Avant de commencer la configuration, vous devez collecter les informations suivantes.
  - Système d'**exploitation :** Quel type de système d'exploitation (MS Windows, Linux, BSD, Unix, autres) avez-vous ?
  - Serveur**Web :** quel serveur Web (IIS, Apache ou NetScaler Enterprise Server) exécutez-vous ?
  - **Application :** Quels types d'applications sont en cours d'exécution sur votre serveur d'applications (par exemple, ASP.NET, PHP, Cold Fusion, ActiveX, FrontPage, Struts, CGI, Apache Tomcat, Domino et WebLogic) ?
  - Avez-vous des applications personnalisées ou des applications prêtes à l'emploi (par exemple, Oracle, SAP) ? Quelle version utilisez-vous ?
  - **SSL :** Avez-vous besoin de SSL ? Dans l'affirmative, quelle taille de clé (512, 1024, 2048, 4096) est utilisée pour la signature des certificats ?
  - **Volume du trafic :** Quel est le taux de trafic moyen via vos applications ? Avez-vous des pics de trafic saisonniers ou temporels ?
  - **Ferme de serveurs :** Combien de serveurs disposez-vous ? Avez-vous besoin d'utiliser l'équilibrage de charge ?
  - **Base de données :** Quel type de base de données (MS-SQL, MySQL, Oracle, Postgres, SQLite, nosql, Sybase, Informix, etc.) utilisez-vous ?
  - **Connectivité DB :** Quel type de connectivité de base de données disposez-vous (DSN, chaîne de connexion par fichier, chaîne de connexion à un seul fichier) et quels pilotes sont utilisés ?
- **Identifiez vos besoins en matière de sécurité :** Vous voudrez peut-être évaluer quelles applications ou données spécifiques nécessitent une protection de sécurité maximale, lesquelles sont les moins vulnérables et celles pour lesquelles l'inspection de sécurité peut être contournée en toute sécurité. Cela vous aidera à trouver une configuration optimale et à concevoir des stratégies et des points de liaison appropriés pour séparer le trafic. Par exemple, vous pouvez configurer une stratégie pour contourner l'inspection de sécurité des demandes de contenu Web statique, tels que des images, des fichiers MP3 et des films, et configurer une autre stratégie pour appliquer des contrôles de sécurité avancés aux demandes de contenu dynamique. Vous pouvez utiliser plusieurs stratégies et profils pour protéger différents contenus d'une même application.

- **Exigence de licence :** NetScaler propose une solution unifiée pour optimiser les performances de votre application en tirant parti d'un ensemble complet de fonctionnalités telles que l'équilibrage de charge, la commutation de contenu, la mise en cache, la compression, le répondeur, la réécriture et le filtrage de contenu, pour n'en nommer que quelques-unes. L'identification des fonctionnalités souhaitées peut vous aider à choisir la licence dont vous avez besoin.
- **Installez et configurez une appliance NetScaler :** créez un serveur virtuel et testez le trafic via celui-ci pour avoir une idée du débit et de la quantité de trafic qui transite par votre système. Ces informations vous aideront à identifier vos besoins en capacité et à sélectionner le bon matériel (VPX, MPX ou SDX).
- **Déployer le pare-feu des applications Web :** utilisez l'assistant Web App Firewall pour procéder à une configuration de sécurité simple. L'Assistant vous guide à travers plusieurs écrans et vous invite à ajouter un profil, une stratégie, une signature et des vérifications de sécurité.
  - **Profil :** sélectionnez un nom significatif et le type approprié (HTML, XML ou WEB 2.0) pour votre profil. La stratégie et les signatures seront générées automatiquement sous le même nom.
  - **Stratégie :** La stratégie générée automatiquement possède l'expression par défaut (true), qui sélectionne tout le trafic et est liée globalement. C'est un bon point de départ, sauf si vous avez en tête une stratégie spécifique que vous souhaitez utiliser.
  - **Protections :** l'assistant vous aide à tirer parti du modèle de sécurité hybride, dans lequel vous pouvez utiliser les signatures par défaut offrant un ensemble complet de règles pour protéger différents types d'applications. Le mode d'édition**simple** vous permet de visualiser les différentes catégories (CGI, Cold Fusion, PHP, etc.). Vous pouvez sélectionner une ou plusieurs catégories pour identifier un ensemble spécifique de règles applicables à votre application. Utilisez l'option **Action** pour activer toutes les règles de signature dans les catégories sélectionnées. Assurez-vous que le blocage est désactivé afin de pouvoir surveiller le trafic avant de renforcer la sécurité. Cliquez sur **Continuer**. Dans le volet **Spécifier les protections approfondies**, vous pouvez apporter les modifications nécessaires pour déployer les protections de vérification de sécurité. Dans la plupart des cas, les protections de base sont suffisantes pour la configuration initiale de la sécurité. Exécutez le trafic pendant un certain temps pour collecter un échantillon représentatif des données d'inspection de sécurité.
  - **Renforcer la sécurité :** après avoir déployé Web App Firewall et observé le trafic pendant un certain temps, vous pouvez commencer à renforcer la sécurité de vos applications en déployant des assouplissements, puis en activant le blocage. Les règles**Learning**, **Visualizer** et **Click to deploy** sont des fonctionnalités utiles qui facilitent la modification de votre configuration pour trouver le bon niveau de relaxation. À ce stade, vous pouvez également modifier l'expression de la stratégie et/ou configurer des stratégies et des profils supplé-

mentaires pour mettre en œuvre les niveaux de sécurité souhaités pour différents types de contenu.

- **Débogage :** si vous constatez un comportement inattendu de votre application, le Web App Firewall offre différentes options pour faciliter le débogage :
  - **Journal**. Si des demandes légitimes sont bloquées, la première étape consiste à vérifier le fichier ns.log pour voir si une violation inattendue des contrôles de sécurité est déclenchée.
  - **Désactiver la fonction.** Si vous ne constatez aucune violation, mais que vous constatez toujours un comportement inattendu, comme la réinitialisation d'une application ou l'envoi de réponses partielles, vous pouvez désactiver la fonctionnalité Web App Firewall pour le débogage. Si le problème persiste, il exclut le Web App Firewall en tant que suspect.
  - **Trace les enregistrements avec des messages de journal.** Si le problème semble être lié au Web App Firewall et doit être examiné de plus près, vous avez la possibilité d'inclure des messages de violation de sécurité dans une nstrace. Vous pouvez utiliser « Suivre le flux TCP » dans la trace pour afficher les détails de la transaction individuelle, y compris les en-têtes, la charge utile et le message de journal correspondant, ensemble sur le même écran. Des détails sur l'utilisation de cette fonctionnalité sont disponibles dans les annexes.

Présentation de NetScaler Web App Firewall

May 5, 2023

Le pare-feu NetScaler Web App Firewall prévient les failles de sécurité, les pertes de données et les éventuelles modifications non autorisées des sites Web qui accèdent à des informations commerciales ou clients sensibles. Pour ce faire, il filtre à la fois les demandes et les réponses, en les examinant pour détecter des preuves d'activité malveillante et en bloquant les demandes présentant une telle activité. Votre site est protégé non seulement contre les types d'attaques courants, mais également contre les nouvelles attaques encore inconnues. En plus de protéger les serveurs Web et les sites Web contre tout accès non autorisé, le Web App Firewall protège contre les vulnérabilités du code ou des scripts CGI existants, des frameworks Web, des logiciels de serveur Web et d'autres systèmes d'exploitation sous-jacents.

Le NetScaler Web App Firewall est disponible en tant qu'appliance autonome ou en tant que fonctionnalité sur une appliance virtuelle NetScaler (VPX). Dans la documentation du Web App Firewall, le terme NetScaler fait référence à la plate-forme sur laquelle le Web App Firewall s'exécute, qu'il s'agisse d'une appliance de pare-feu dédiée, d'un NetScaler sur lequel d'autres fonctionnalités ont également été configurées ou d'un NetScaler VPX.

Pour utiliser le Web App Firewall, vous devez créer au moins une configuration de sécurité afin de bloquer les connexions qui enfreignent les règles que vous avez définies pour vos sites Web protégés. Le nombre de configurations de sécurité que vous souhaiterez peut-être créer dépend de la complexité de votre site Web. Parfois, une seule configuration suffit. Dans d'autres cas, notamment ceux qui incluent des sites Web interactifs, des sites Web qui accèdent à des serveurs de base de données, des boutiques en ligne avec des paniers d'achat, vous pouvez avoir besoin de plusieurs configurations différentes pour protéger au mieux les données sensibles sans gaspiller d'efforts importants sur du contenu non vulnérable à certains types d'attaques. Vous pouvez souvent laisser inchangées les valeurs par défaut des paramètres globaux, qui affectent toutes les configurations de sécurité. Vous pouvez toutefois modifier les paramètres généraux s'ils entrent en conflit avec d'autres parties de votre configuration ou si vous préférez les personnaliser.

Sécurité des applications Web

La sécurité des applications Web est la sécurité réseau des ordinateurs et des programmes qui communiquent à l'aide des protocoles HTTP et HTTPS. Il s'agit d'un vaste domaine dans lequel les failles et les faiblesses de sécurité abondent. Les systèmes d'exploitation des serveurs et des clients présentent des problèmes de sécurité et sont vulnérables aux attaques. Les logiciels de serveur Web et les technologies d'activation des sites Web telles que CGI, Java, JavaScript, PERL et PHP présentent des vulnérabilités sous-jacentes. Les navigateurs et autres applications clientes qui communiquent avec des applications Web présentent également des vulnérabilités. Les sites Web qui utilisent n'importe quelle technologie à l'exception du langage HTML le plus simple, y compris tout site permettant une interaction avec les visiteurs, présentent souvent leurs propres vulnérabilités.

Dans le passé, une faille de sécurité n'était souvent qu'une gêne, mais aujourd'hui, c'est rarement le cas. Par exemple, les attaques au cours desquelles un pirate informatique accédait à un serveur Web et apportait des modifications non autorisées (dégradant) un site Web étaient monnaie courante. Ils étaient généralement lancés par des pirates informatiques qui n'avaient d'autre motivation que de démontrer leurs compétences à d'autres pirates informatiques ou d'embarrasser la personne ou l'entreprise ciblée. La plupart des failles de sécurité actuelles sont toutefois motivées par un désir d'argent. La majorité d'entre eux tentent d'atteindre l'un ou l'autre des objectifs suivants, voire les deux : obtenir des informations privées sensibles et potentiellement précieuses, ou obtenir un accès non autorisé à un site Web ou à un serveur Web et le contrôle de celui-ci.

Certaines formes d'attaques Web visent à obtenir des informations privées. Ces attaques sont souvent possibles même contre des sites Web suffisamment sécurisés pour empêcher un attaquant d'en prendre le contrôle total. Les informations qu'un attaquant peut obtenir à partir d'un site Web peuvent inclure les noms des clients, des adresses, des numéros de téléphone, des numéros de sécurité sociale, des numéros de carte de crédit, des dossiers médicaux et d'autres informations privées. L'attaquant peut ensuite utiliser ces informations ou les vendre à d'autres personnes. La plupart des informations obtenues par de telles attaques sont protégées par la loi, et toutes par les coutumes et les attentes.

Une violation de ce type peut avoir de graves conséquences pour les clients dont les informations privées sont compromises. Au mieux, ces clients doivent faire preuve de vigilance pour empêcher d'autres personnes d'utiliser leurs cartes de crédit à mauvais escient, d'ouvrir des comptes de crédit non autorisés à leur nom ou de s'approprier purement et simplement leur identité (vol d'identité). Dans le pire des cas, les clients risquent d'être confrontés à des cotes de crédit ruinées ou même d'être accusés d'activités criminelles auxquelles ils n'ont pas participé.

D'autres attaques Web visent à prendre le contrôle (ou à *compromettre*) un site Web ou le serveur sur lequel il fonctionne, ou les deux. Un pirate informatique qui prend le contrôle d'un site Web ou d'un serveur peut l'utiliser pour héberger du contenu non autorisé, agir en tant que proxy pour le contenu hébergé sur un autre serveur Web, fournir des services SMTP pour envoyer des e-mails en masse non sollicités ou fournir des services DNS pour prendre en charge de telles activités sur d'autres serveurs Web compromis. La plupart des sites Web hébergés sur des serveurs Web compromis font la promotion d'entreprises douteuses ou carrément frauduleuses. Par exemple, la plupart des sites Web de phishing et d'exploitation d'enfants sont hébergés sur des serveurs Web compromis.

La protection de vos sites Web et services Web contre ces attaques nécessite une défense à plusieurs niveaux capable à la fois de bloquer les attaques connues présentant des caractéristiques identifiables et de vous protéger contre les attaques inconnues, qui peuvent souvent être détectées car leur apparence est différente du trafic normal vers vos sites Web et services Web.

Attaques Web connues

La première ligne de défense de vos sites Web est la protection contre le grand nombre d'attaques connues qui ont été observées et analysées par des experts en sécurité Web. Les types d'attaques les plus courants contre les sites Web HTML sont les suivants :

- **Attaques par débordement de la mémoire tampon.** L'envoi d'une URL longue, d'un cookie long ou de longues informations à un serveur Web entraîne le blocage, le blocage du système ou l'accès non autorisé au système d'exploitation sous-jacent. Une attaque par débordement de la mémoire tampon peut être utilisée pour accéder à des informations non autorisées, pour compromettre un serveur Web, ou les deux.
- **Attaques de sécurité liées aux cookies.** Envoi d'un cookie modifié à un serveur Web, généralement dans l'espoir d'accéder à un contenu non autorisé en utilisant des informations d'identification falsifiées.
- **Navigation musclée.** Accès direct aux URL d'un site Web, sans accéder aux URL contenant des hyperliens sur la page d'accueil ou à d'autres URL de démarrage courantes sur le site Web. Des cas individuels de navigation forcée peuvent indiquer qu'un utilisateur a ajouté une page à ses favoris sur votre site Web, mais les tentatives répétées d'accès à un contenu inexistant, ou à un contenu auquel les utilisateurs ne doivent jamais accéder directement, constituent souvent une atteinte à la sécurité du site Web. La navigation forcée est généralement utilisée pour accéder

à des informations non autorisées, mais elle peut également être associée à une attaque par débordement de la mémoire tampon dans le but de compromettre votre serveur.

- **Attaques contre la sécurité des formulaires Web.** Envoi de contenu inapproprié à votre site Web dans un formulaire Web. Le contenu inapproprié peut inclure des champs masqués modifiés, du code HTML ou du code dans un champ destiné uniquement à des données alphanumériques, une chaîne trop longue dans un champ qui n'accepte qu'une chaîne courte, une chaîne alphanumérique dans un champ qui n'accepte qu'un entier et une grande variété d'autres données que votre site Web ne s'attend pas à recevoir dans ce formulaire Web. Une attaque de sécurité par formulaire Web peut être utilisée soit pour obtenir des informations non autorisées à partir de votre site Web, soit pour compromettre purement et simplement le site Web, généralement lorsqu'elle est associée à une attaque par débordement de la mémoire tampon.

Deux types d'attaques spécifiques visant la sécurité des formulaires Web méritent une mention spéciale :

- **Attaques par injection SQL.** Envoi d'une ou de plusieurs commandes SQL actives dans un formulaire Web ou dans le cadre d'une URL, dans le but de faire en sorte qu'une base de données SQL exécute la ou les commandes. Les attaques par injection SQL sont généralement utilisées pour obtenir des informations non autorisées.
- **Attaques par script intersites.** Utilisation d'une URL ou d'un script sur une page Web pour enfreindre la politique d'origine identique, qui interdit à tout script d'obtenir des propriétés ou de modifier le contenu d'un autre site Web. Étant donné que les scripts peuvent obtenir des informations et modifier des fichiers sur votre site Web, autoriser un script à accéder au contenu d'un autre site Web peut fournir à un attaquant le moyen d'obtenir des informations non autorisées, de compromettre un serveur Web, ou les deux.

Les attaques contre les services Web basés sur XML appartiennent généralement à au moins l'une des deux catégories suivantes : tentatives d'envoi de contenu inapproprié à un service Web ou tentatives de violation de la sécurité d'un service Web. Les types d'attaques les plus courants contre les services Web basés sur XML sont les suivants :

- **Code ou objets malveillants.** Requêtes XML contenant du code ou des objets susceptibles d'obtenir directement des informations sensibles ou de permettre à un attaquant de contrôler le service Web ou le serveur sous-jacent.
- **Requêtes XML mal formées.** Demandes XML qui ne sont pas conformes à la spécification XML du W3C et qui peuvent donc porter atteinte à la sécurité d'un service Web non sécurisé
- **Attaques par déni de service (DoS).** Requêtes XML qui sont envoyées à plusieurs reprises et en grand volume, dans le but de surcharger le service Web ciblé et de refuser aux utilisateurs légitimes l'accès au service Web.

Outre les attaques XML standard, les services Web XML et les sites Web 2.0 sont également vulnérables aux attaques par injection SQL et par script intersite, comme décrit ci-dessous :

- **Attaques par injection SQL.** Envoi d'une ou de plusieurs commandes SQL actives dans une requête XML, dans le but de faire en sorte qu'une base de données SQL exécute cette ou ces commandes. Comme les attaques par injection HTML SQL, les attaques par injection XML SQL sont généralement utilisées pour obtenir des informations non autorisées.
- **Attaques par script intersites.** Utilisation d'un script inclus dans une application XML pour enfreindre la politique d'origine identique, qui interdit à tout script d'obtenir des propriétés ou de modifier le contenu d'une autre application. Étant donné que les scripts peuvent obtenir des informations et modifier des fichiers à l'aide de votre application XML, autoriser un script à accéder au contenu appartenant à une autre application peut permettre à un attaquant d'obtenir des informations non autorisées, de compromettre l'application, ou les deux

Les attaques Web connues peuvent généralement être bloquées en filtrant le trafic du site Web en fonction de caractéristiques spécifiques (signatures) qui apparaissent toujours pour une attaque spécifique et ne doivent jamais apparaître dans le trafic légitime. Cette approche présente l'avantage de nécessiter relativement peu de ressources et de présenter relativement peu de risques de faux positifs. Il s'agit donc d'un outil précieux pour lutter contre les attaques contre les sites Web et les services Web et pour configurer la protection de base des signatures.

Attaques Web inconnues

La plus grande menace contre les sites Web et les applications ne provient pas d'attaques connues, mais d'attaques inconnues. La plupart des attaques inconnues se classent dans l'une des deux catégories suivantes : les attaques récemment lancées pour lesquelles les entreprises de sécurité n'ont pas encore développé de défense efficace (attaques de type « zero-day »), et les attaques soigneusement ciblées visant un site Web ou un service Web spécifique plutôt que de nombreux sites Web ou services Web (attaques de type spear). Ces attaques, comme les attaques connues, visent à obtenir des informations privées sensibles, à compromettre le site Web ou le service Web et à permettre leur utilisation pour d'autres attaques, ou à ces deux objectifs.

Les attaques zero-day constituent une menace majeure pour tous les utilisateurs. Ces attaques sont généralement du même type que les attaques connues ; les attaques zero-day impliquent souvent du SQL injecté, un script intersite, une falsification de requêtes intersites ou un autre type d'attaque similaire aux attaques connues. Ils ciblent généralement des vulnérabilités que les développeurs du logiciel, du site Web ou du service Web ciblé ignorent ou ont découvert. Les entreprises de sécurité n'ont donc pas développé de moyens de défense contre ces attaques et, même si c'est le cas, les utilisateurs n'ont pas obtenu et installé les correctifs ni mis en œuvre les solutions de contournement nécessaires pour se protéger contre ces attaques. Le délai entre la découverte d'une attaque de type « jour zéro » et la mise en place d'une défense (la fenêtre de vulnérabilité) est de plus en plus court, mais les auteurs peuvent toujours compter sur des heures, voire des jours, pendant lesquels de nombreux sites Web et services Web ne disposent pas d'une protection spécifique contre l'attaque.

Les attaques à la lance constituent une menace majeure, mais elles concernent un groupe

d'utilisateurs plus restreint. Un type courant d'attaque au harpon, le hameçonnage, vise les clients d'une banque ou d'une institution financière spécifique, ou (moins fréquemment) les employés d'une entreprise ou d'une organisation spécifique. Contrairement aux autres hameçonnage, qui sont souvent des contrefaçons rédigées de manière grossière et qu'un utilisateur familiarisé avec les communications de cette banque ou institution financière peut reconnaître, les hameçonnages sont parfaits et convaincants. Ils peuvent contenir des informations spécifiques à l'individu que, à première vue, aucun étranger ne doit connaître ou être en mesure d'obtenir. Le spécialiste de l'hameçonnage est donc en mesure de convaincre la cible de fournir les informations demandées, que le phisher peut ensuite utiliser pour piller des comptes, traiter de l'argent obtenu illégitimement d'autres sources ou accéder à d'autres informations encore plus sensibles.

Ces deux types d'attaques présentent certaines caractéristiques qui peuvent généralement être détectées, mais pas en utilisant des modèles statiques qui recherchent des caractéristiques spécifiques, comme le font les signatures standard. La détection de ces types d'attaques nécessite des approches plus sophistiquées et plus gourmandes en ressources, telles que le filtrage heuristique et les systèmes de modèles de sécurité positifs. Le filtrage heuristique ne recherche pas des modèles spécifiques, mais des modèles de comportements. Les systèmes à modèle de sécurité positif modélisent le comportement normal du site Web ou du service Web qu'ils protègent, puis bloquent les connexions qui ne correspondent pas à ce modèle d'utilisation normale. Les contrôles de sécurité basés sur des URL et des formulaires Web évaluent l'utilisation normale de vos sites Web, puis contrôlent la manière dont les utilisateurs interagissent avec vos sites Web, en utilisant à la fois des heuristiques et une sécurité positive pour bloquer le trafic anormal ou inattendu. La sécurité heuristique et positive, correctement conçue et déployée, permet de détecter la plupart des attaques que les signatures passent inaperçues. Cependant, elles nécessitent beaucoup plus de ressources que les signatures, et vous devez passer un certain temps à les configurer correctement pour éviter les faux positifs. Ils sont donc utilisés, non pas comme ligne de défense principale, mais comme sauvegarde des signatures ou d'autres approches moins gourmandes en ressources.

En configurant ces protections avancées en plus des signatures, vous créez un modèle de sécurité hybride, qui permet au Web App Firewall de fournir une protection complète contre les attaques connues et inconnues.

Comment fonctionne NetScaler Web App Firewall

Lorsque vous installez le Web App Firewall, vous créez une configuration de sécurité initiale composée d'une politique, d'un profil et d'un objet de signatures. La politique est une règle qui identifie le trafic à filtrer, et le profil identifie les modèles et les types de comportement à autoriser ou à bloquer lorsque le trafic est filtré. Les modèles les plus simples, appelés signatures, ne sont pas spécifiés dans le profil, mais dans un objet de signatures associé au profil.

Une signature est une chaîne ou un modèle qui correspond à un type d'attaque connu. Le Web App Firewall contient plus d'un millier de signatures réparties en sept catégories, chacune dirigée contre

des attaques contre des types spécifiques de serveurs Web et de contenu Web. NetScaler met à jour la liste avec de nouvelles signatures à mesure que de nouvelles menaces sont identifiées. Lors de la configuration, vous spécifiez les catégories de signatures adaptées aux serveurs Web et au contenu que vous devez protéger. Les signatures fournissent une bonne protection de base avec une faible charge de traitement. Si vos applications présentent des vulnérabilités particulières ou si vous détectez une attaque contre laquelle aucune signature n'existe, vous pouvez ajouter vos propres signatures.

Les protections les plus avancées sont appelées contrôles de sécurité. Un contrôle de sécurité est une inspection algorithmique plus rigoureuse d'une demande visant à détecter des modèles ou des types de comportements spécifiques susceptibles d'indiquer une attaque ou de constituer une menace pour vos sites Web et services Web protégés. Il peut, par exemple, identifier une demande visant à effectuer un certain type d'opération susceptible de porter atteinte à la sécurité, ou une réponse contenant des informations privées sensibles telles qu'un numéro de sécurité sociale ou un numéro de carte de crédit. Lors de la configuration, vous spécifiez les contrôles de sécurité adaptés aux serveurs Web et au contenu que vous devez protéger. Les contrôles de sécurité sont restrictifs. Nombre d'entre eux peuvent bloquer les demandes et les réponses légitimes si vous n'ajoutez pas les exceptions (assouplissements) appropriées lors de leur configuration. Identifier les exceptions nécessaires n'est pas difficile si vous utilisez la fonction d'apprentissage adaptatif, qui observe l'utilisation normale de votre site Web et crée des exceptions recommandées.

Le Web App Firewall peut être installé en tant que périphérique réseau de couche 3 ou en tant que pont réseau de couche 2 entre vos serveurs et vos utilisateurs, généralement derrière le routeur ou le pare-feu de votre entreprise. Il doit être installé à un endroit où il peut intercepter le trafic entre les serveurs Web que vous souhaitez protéger et le hub ou le commutateur par lequel les utilisateurs accèdent à ces serveurs Web. Vous configurez ensuite le réseau pour envoyer des demandes au Web App Firewall plutôt que directement à vos serveurs Web, et des réponses au Web App Firewall plutôt que directement à vos utilisateurs. Le Web App Firewall filtre ce trafic avant de le transférer vers sa destination finale, en utilisant à la fois son ensemble de règles internes et vos ajouts et modifications. Il bloque ou rend inoffensif toute activité qu'il détecte comme nuisible, puis transfère le trafic restant au serveur Web. La figure suivante donne une vue d'ensemble du processus de filtrage.

> **Remarque :**
>
> La figure omet l'application d'une politique au trafic entrant. Il illustre une configuration de sécurité dans laquelle la stratégie est de traiter toutes les demandes. De plus, dans cette configuration, un objet signatures a été configuré et associé au profil, et des vérifications de sécurité ont été configurées dans le profil.

Figure 1. Organigramme du filtrage du Web App Firewall



Comme le montre la figure, lorsqu'un utilisateur demande une URL sur un site Web protégé, le Web App Firewall examine d'abord la demande pour s'assurer qu'elle ne correspond pas à une signature. Si la demande correspond à une signature, NetScaler Web App Firewall affiche l'objet d'erreur (une page Web située sur l'appliance Web App Firewall et que vous pouvez configurer à l'aide de la fonctionnalité d'importation) ou transmet la demande à l'URL d'erreur désignée (la page d'erreur). Les signatures ne nécessitent pas autant de ressources que les contrôles de sécurité. Par conséquent, la détection et l'arrêt des attaques détectées par une signature avant d'exécuter l'un des contrôles de sécurité réduisent la charge sur le serveur.

Si une demande passe l'inspection des signatures, le Web App Firewall applique les contrôles de sécurité des demandes qui ont été activés. Les contrôles de sécurité des demandes vérifient que la demande est appropriée pour votre site Web ou service Web et qu'elle ne contient aucun élément susceptible de constituer une menace. Par exemple, les vérifications de sécurité examinent la demande pour détecter des signes indiquant qu'elle peut être d'un type inattendu, demander du contenu inat-

tendu ou contenir des données de formulaire Web, des commandes SQL ou des scripts inattendus et éventuellement malveillants. Si la demande échoue à un contrôle de sécurité, le Web App Firewall nettoie la demande puis la renvoie à l'appliance NetScaler (ou à l'appliance virtuelle NetScaler) ou affiche l'objet d'erreur. Si la demande passe les contrôles de sécurité, elle est renvoyée à l'appliance NetScaler, qui termine tout autre traitement et transmet la demande au serveur Web protégé.

Lorsque le site Web ou le service Web envoie une réponse à l'utilisateur, le Web App Firewall applique les contrôles de sécurité des réponses qui ont été activés. Les contrôles de sécurité des réponses examinent la réponse pour détecter les fuites d'informations privées sensibles, les signes de dégradation du site Web ou tout autre contenu qui ne doit pas être présent. Si la réponse échoue à un contrôle de sécurité, le Web App Firewall supprime le contenu qui ne doit pas être présent ou bloque la réponse. Si la réponse passe les contrôles de sécurité, elle est renvoyée à l'appliance NetScaler, qui la transmet à l'utilisateur.

Fonctionnalités du pare-feu NetScaler Web App

Les fonctionnalités de base du Web App Firewall sont les stratégies, les profils et les signatures, qui fournissent un modèle de sécurité hybride tel que décrit dans Attaques Web connues, Attaques Web inconnueset Fonctionnement du pare-feu Web App. Il convient de noter la fonctionnalité d'apprentissage, qui observe le trafic vers vos applications protégées et recommande les paramètres de configuration appropriés pour certaines vérifications de sécurité.

La fonctionnalité d'importation gère les fichiers que vous chargez sur le Web App Firewall. Ces fichiers sont ensuite utilisés par le Web App Firewall lors de divers contrôles de sécurité ou lorsqu'il répond à une connexion qui correspond à un contrôle de sécurité.

Vous pouvez utiliser les fonctionnalités de journaux, de statistiques et de rapports pour évaluer les performances du Web App Firewall et identifier les besoins éventuels en matière de protections supplémentaires.

Comment NetScaler Web App Firewall modifie le trafic des applications

Le pare-feu NetScaler Web App affecte le comportement d'une application Web qu'il protège en modifiant les éléments suivants :

- Cookies
- En-têtes HTTP
- Formulaires/Données

cookie de session NetScaler Web App Firewall

Pour maintenir l'état de la session, NetScaler Web App Firewall génère son propre cookie de session. Ce cookie est transmis uniquement entre le navigateur Web et le pare-feu d'application Web

NetScaler, et non au serveur Web. Si un pirate informatique tente de modifier le cookie de session, le pare-feu de l'application supprime le cookie avant de transmettre la demande au serveur et traite la demande comme une nouvelle session utilisateur. Le cookie de session est présent tant que le navigateur Web est ouvert. Lorsque le navigateur Web est fermé, la durée de validité du cookie de session Application Firewall est prolongée. L'état de la session conserve les informations relatives aux URL et aux formulaires visités par le client.

Le cookie de session configurable du Web App Firewall est `citrix_ns_id`.

À partir des versions 12.1 54 et 13.0 de NetScaler, la cohérence des cookies s'effectue sans session et n'impose pas l'ajout d'un cookie de session généré par l'appliance. `citrix_ns_id`

Cookies du pare-feu NetScaler Web App

De nombreuses applications Web génèrent des cookies pour suivre les informations spécifiques à l'utilisateur ou à la session. Ces informations peuvent être les préférences de l'utilisateur ou les articles du panier. Un cookie d'application Web peut être de l'un des deux types suivants :

- **Cookies persistants** - Ces cookies sont stockés localement sur l'ordinateur et réutilisés lors de votre prochaine visite sur le site. Ce type de cookie contient généralement des informations sur l'utilisateur, telles que son identifiant, son mot de passe ou ses préférences.
- **Cookies de session ou transitoires** - Ces cookies ne sont utilisés que pendant la session et sont détruits après la fin de la session. Ce type de cookie contient des informations sur l'état de l'application, telles que les articles du panier ou les informations d'identification de session.

Les pirates informatiques peuvent tenter de modifier ou de voler des cookies d'applications pour pirater la session d'un utilisateur ou se faire passer pour un utilisateur. Le pare-feu d'application empêche de telles tentatives en hachant les cookies de l'application, puis en ajoutant d'autres cookies avec les signatures numériques. En suivant les cookies, le pare-feu d'application garantit que les cookies ne sont pas modifiés ou compromis entre le navigateur client et le pare-feu d'application. Le pare-feu d'application ne modifie pas les cookies de l'application.

Le pare-feu NetScaler Web App Firewall génère les cookies par défaut suivants pour suivre les cookies de l'application :

- **Cookies persistants** : `citrix_ns_id_wlf`. Remarque : wlf est l'abréviation de Will Live Forever.
- **Cookies de session ou transitoires** : `citrix_ns_id_wat`. Remarque : ce qui signifie agira de manière transitoire.
  Pour suivre les cookies d'application, le pare-feu d'application regroupe les cookies d'application persistants ou de session, puis hache et signe tous les cookies ensemble. Ainsi, le pare-feu d'application génère un `wlf` cookie pour suivre tous les cookies d'application persistants et un `wat` cookie pour suivre tous les cookies de session de l'application.

Le tableau suivant indique le nombre et les types de cookies générés par le pare-feu d'application en fonction des cookies générés par l'application Web :

Avant NetScaler Web App Firewall	À
Un cookie persistant	cookie persistant : `citix_ns_id_wlf`
Un cookie temporaire	Cookie temporaire : `citix_ns_id_wat`
Plusieurs cookies persistants, plusieurs cookies transitoires	Un cookie persistant : `citrix_ns_id_wlf`, Un cookie transitoire : `citix_ns_id_wat`

NetScaler Web App Firewall permet de crypter le cookie de l'application. Le pare-feu d'application fournit également une option permettant de transmettre par proxy le cookie de session envoyé par l'application, en le stockant avec le reste des données de session du pare-feu d'application et en ne l'envoyant pas au client. Lorsqu'un client envoie à l'application une demande qui inclut un cookie de session Application Firewall, Application Firewall réinsère le cookie envoyé par l'application dans la demande avant de l'envoyer à l'application d'origine. Le pare-feu d'application permet également d'ajouter les indicateurs HttpOnly et/ou Secure aux cookies.

Comment le pare-feu de l'application affecte les en-têtes HTTP

Les requêtes HTTPs et les réponses HTTPs utilisent des en-têtes pour envoyer des informations sur un ou plusieurs messages HTTPS. Un en-tête est une série de lignes dont chaque ligne contient un nom suivi de deux points, d'un espace et d'une valeur. Par exemple, l'en-tête Host a le format suivant :

```
Host: www.citrix.com
```

Certains champs d'en-tête sont utilisés à la fois dans les en-têtes de demande et de réponse, tandis que d'autres ne conviennent qu'à une demande ou à une réponse. Le pare-feu d'application peut ajouter, modifier ou supprimer certains en-têtes dans une ou plusieurs demandes ou réponses HTTPS afin de maintenir la sécurité de l'application.

En-têtes de requête supprimés par le NetScaler Web App Firewall

La plupart des en-têtes de demande liés à la mise en cache sont supprimés pour afficher chaque demande dans le contexte d'une session. De même, si la demande inclut un en-tête de codage permettant au serveur Web d'envoyer des réponses compressées, le pare-feu des applications supprime cet en-tête afin que le contenu de la réponse non compressée du serveur soit inspecté par le Web App Firewall afin d'empêcher toute fuite de données sensibles vers le client.

Le pare-feu d'applications supprime les en-têtes de requête suivants :

- Plage : utilisée pour récupérer des données après un échec ou un transfert partiel de fichiers.

- If-Range — Permet à un client de récupérer un objet partiel lorsqu'il contient déjà une partie de cet objet dans son cache (GET conditionnel).
- If-Modified-Since — Si l'objet demandé n'est pas modifié depuis l'heure spécifiée dans ce champ, aucune entité n'est renvoyée par le serveur. Vous obtenez une erreur HTTP 304 non modifiée.
- If-None-Match : permet des mises à jour efficaces des informations mises en cache avec un minimum de surcharge.
- Accept-Encoding — Quelles méthodes de codage sont autorisées pour un objet particulier, tel que gzip.

En-tête de demande modifié par le NetScaler Web App Firewall

Si un navigateur Web utilise le protocole HTTP/1.0 ou une version antérieure, le navigateur ouvre et ferme continuellement la connexion au socket TCP après avoir reçu chaque réponse. Cela augmente la charge du serveur Web et empêche le maintien de l'état de la session. Le protocole HTTP/1.1 permet à la connexion de rester ouverte pendant la session. Le pare-feu d'application modifie l'en-tête de demande suivant pour utiliser le protocole HTTP/1.1 entre le pare-feu d'applications et le serveur Web, quel que soit le protocole utilisé par le navigateur Web :
Connexion : keep-alive

En-têtes de requête ajoutés par le NetScaler Web App Firewall

Le pare-feu d'application agit comme un proxy inverse et remplace l'adresse IP source d'origine de la session par l'adresse IP du pare-feu d'application. Par conséquent, toutes les demandes enregistrées dans le journal du serveur Web indiquent qu'elles sont envoyées depuis le pare-feu d'applications.

En-tête de réponse déposé par le NetScaler Web App Firewall

Le pare-feu des applications peut bloquer ou modifier du contenu, par exemple en supprimant des numéros de carte de crédit ou en supprimant des commentaires, ce qui peut entraîner une différence de taille. Pour éviter un tel scénario, le pare-feu d'applications supprime l'en-tête suivant :

Longueur du contenu : indique la taille du message envoyé au destinataire.
En-têtes de réponse modifiés par le pare-feu de l'application

La plupart des en-têtes de réponse modifiés par le pare-feu d'applications sont liés à la mise en cache. Les en-têtes de mise en cache des réponses HTTP (S) doivent être modifiés pour obliger le navigateur Web à toujours envoyer une demande au serveur Web pour obtenir les données les plus récentes et à ne pas utiliser le cache local. Toutefois, certaines applications ASP utilisent des plug-ins distincts pour afficher des contenus dynamiques et peuvent nécessiter la possibilité de mettre temporairement les données en cache dans le navigateur. Pour autoriser la mise en cache temporaire des données lorsque des protections de sécurité avancées telles que la FFC, la fermeture d'URL ou les contrôles CSRF sont

activées, Application Firewall ajoute ou modifie les en-têtes de contrôle du cache dans la réponse du serveur en utilisant la logique suivante :

- Si le serveur envoie Pragma : no-cache, le pare-feu des applications n'apporte aucune modification.
- Si la demande du client est HTTP 1.0, Application Firewall insère Pragma : no-cache.
- Si la demande du client est HTTP 1.1 et que le contrôle du cache est défini comme suit : no-store, Application Firewall n'apporte aucune modification.
- Si la demande du client est HTTP 1.1 et que la réponse du serveur comporte un en-tête Cache-Control sans directive de stockage ou sans cache, alors Application Firewall n'apporte aucune modification.
- Si la demande du client est HTTP 1.1 et que la réponse du serveur comporte un en-tête No Cache-Control ou que l'en-tête Cache-Control ne comporte aucune directive store ou no-cache, le pare-feu applicatif effectue les tâches suivantes :

1. Inserts Cache-control: max-age=3, must-revalidate,private.
2. Inserts X-Cache-Control-orig = Original value of Cache-Control Header.
3. Supprime l'en-tête de dernière modification.
4. Remplace Etag.
5. Insère X-Expires-Orig=Valeur d'origine de l'en-tête Expire envoyé par le serveur.
6. Modifie l'en-tête Expires et fixe la date d'expiration de la page Web au passé, afin qu'elle soit toujours reprise.
7. Modifie Accept-Ranges et le définit sur None.

Pour remplacer les données temporairement mises en cache dans le navigateur client lorsque Application Firewall modifie la réponse, par exemple, pour StripComments, X-out/Remove SafeObject, xout ou remove Credit Card ou URL Transform, Application Firewall prend les mesures suivantes :

1. Supprime la dernière modification du serveur avant de la transférer au client.
2. Remplace Etag par une valeur déterminée par Application Firewall.

En-têtes de réponse ajoutés par le NetScaler Web App Firewall

- `Transfer-Encoding` : Chunked. Cet en-tête renvoie des informations à un client sans avoir à connaître la longueur totale de la réponse avant de l'envoyer. Cet en-tête est obligatoire car l'en-tête de longueur de contenu est supprimé.
- `Set-Cookie`: les cookies ajoutés par le pare-feu de l'application.
- `Xet-Cookie`: Si la session est valide et si la réponse n'a pas expiré dans le cache, vous pouvez servir à partir du cache sans avoir à envoyer de nouveau cookie car la session est toujours valide. Dans un tel scénario, le Set-Cookie est remplacé par Xet-Cookie. Pour le navigateur Web.

Comment les données du formulaire sont-elles affectées

Le pare-feu d'application protège contre les attaques visant à modifier le contenu du formulaire original envoyé par le serveur. Il peut également vous protéger contre les attaques de falsification de requêtes intersites. Le pare-feu d'application y parvient en insérant la balise de formulaire masquée as_fid dans la page.

Exemple : `<input type="hidden"name="as_fid"value="VRgWq0I196Jmg/+LOY7C"/>`

Le champ masqué as_fid est utilisé pour la cohérence des champs. Ce champ est utilisé par Application Firewall pour suivre tous les champs du formulaire, y compris les paires nom/valeur de champ masquées, et pour s'assurer qu'aucun des champs du formulaire envoyé par le serveur n'est modifié côté client. La vérification CSRF utilise également cette balise de formulaire unique as_fid pour s'assurer que les formulaires soumis par l'utilisateur lui ont été servis au cours de cette session et qu'aucun pirate informatique ne tente de pirater la session utilisateur.

Vérification des formulaires sans session

Application Firewall propose également une option pour protéger les données des formulaires grâce à la cohérence des champs sans session. Cela est utile pour les applications où les formulaires peuvent contenir un grand nombre de champs cachés dynamiques, ce qui entraîne une allocation de mémoire élevée par session par le pare-feu des applications. Le contrôle de cohérence des champs sans session est effectué en insérant un autre champ masqué as_ffc_field uniquement pour les requêtes POST ou pour les requêtes GET et POST en fonction du paramètre configuré. Le pare-feu d'application remplace la méthode GET par POST lorsqu'il transmet le formulaire au client. L'appliance rétablit ensuite la méthode en GET lorsqu'elle la renvoie au serveur. La valeur as_ffc_field peut être importante car elle contient le résumé crypté du formulaire diffusé. Voici un exemple de vérification de formulaire sans session :

```
1 <input type="hidden" name="as_ffc_field" value="CwAAAAVIGLD/
     luRRi1Wu1rbYrFYargEDcO5xVAxsEnMP1megXuQfiDTGbwk0fpgndMHqfMbzfAFdjwR+
     TOm1oT
2 +u+Svo9+NuloPhtnbkxGtNe7gB/o8GlxEcK9ZkIIVv3oIL/
     nIPSRWJljgpWgafzVx7wtugNwnn8/
     GdnhneLCJTaYU7ScnC6LexJDLisI1xsEeONWt8Zm
3 +vJTa3mTebDY6LVyhDpDQfBgI1XLgfLTexAUzSNWHYyloqPruGYfnRPw+
     DIGf6gGwn1BYLEsRHKNbjJBrKpOJo9JzhEqdtZ1g3bMzEF9PocPvM1Hpvi5T6VB
4 /YFunUFM4f+bD7EAVcugdhovzb71CsSQX5+qcC1B8WjQ==" />
5 <!--NeedCopy-->
```

Suppression des commentaires HTML

Le pare-feu d'application offre également la possibilité de supprimer tous les commentaires HTML contenus dans les réponses avant de les envoyer au client. Cela concerne non seulement les formulaires, mais également toutes les pages de réponses. Le pare-feu d'application localise et supprime tout texte intégré entre « < ! balises de commentaire « - » et « -> ». Les balises sont conservées pour indiquer qu'un commentaire existait à cet emplacement du code source HTML. Tout texte intégré dans d'autres balises HTML ou JavaScript est ignoré.
Certaines applications risquent de ne pas fonctionner correctement si le code JavaScript est incorrectement intégré dans les balises de commentaire. Une comparaison du code source de la page avant et après la suppression des commentaires par Application Firewall peut aider à déterminer si le code JavaScript requis était intégré à l'un des commentaires supprimés.

Protection par carte de crédit

Le pare-feu des applications offre la possibilité d'inspecter les en-têtes et le corps de la réponse et de supprimer ou de supprimer les numéros de carte de crédit avant de transmettre la réponse au client. À l'heure actuelle, Application Firewall protège les principales cartes de crédit suivantes : American Express, Diners Club, Discover, JCB, MasterCard et Visa. L'action x-out fonctionne indépendamment de l'action Bloquer.

Protection sûre des objets

À l'instar des numéros de carte de crédit, la fuite d'autres données sensibles peut également être évitée en utilisant le contrôle de sécurité Safe Object d'Application Firewall pour supprimer ou masquer le contenu sensible de la réponse.

Les scripts intersites transforment l'action

Lorsque la transformation est activée pour les scripts intersites, le Web App Firewall modifie `"<"into "%26lt;"and ">"into "%26gt;"` les demandes. Si le paramètre CheckRequestHeaders dans le Web App Firewall est activé, le Web App Firewall inspecte les en-têtes de demande et transforme également ces caractères en en-tête et en cookies. L'action de transformation ne bloque ni ne transforme les valeurs initialement envoyées par le serveur. Le Web App Firewall autorise un ensemble d'attributs et de balises par défaut pour les scripts intersites. Une liste par défaut des modèles de scripts intersites refusés est également fournie. Vous pouvez les personnaliser en sélectionnant l'objet de signatures et en cliquant sur la boîte de **dialogue Gérer les modèles de script SQL/cross-site** dans l'interface graphique.

Transformation de caractères spéciaux SQL

Application Firewall applique les règles de transformation par défaut suivantes pour les caractères spéciaux SQL :

De	À	Transformation
‘(guillemet simple, c’est-à-dire %27)	”	Une autre citation
\ (barre oblique inverse égale à %5C)	|Une autre barre oblique inverse a été ajoutée	
; (point-virgule qui est « %B »)		Lâché

Lorsque la transformation des caractères spéciaux est activée et que le CheckRequestHeaders est défini sur ON, la transformation des caractères spéciaux se produit également dans les en-têtes et les cookies.
Remarque : Certains en-têtes de requête tels que User-Agent, Accept-Encoding contiennent généralement des points-virgules et peuvent être affectés par la transformation SQL.

Comportement du pare-feu NetScaler Web App qui altère l’en-tête EXPECT

1. Chaque fois que NetScaler reçoit une requête HTTP contenant l’en-tête EXPECT, NetScaler envoie la réponse EXPECT : 100 -continue au client au nom du serveur principal.
2. Ce comportement est dû au fait que les protections du pare-feu d’application doivent être exécutées sur l’intégralité de la demande avant de la transmettre au serveur. NetScaler doit obtenir l’intégralité de la demande du client.
3. À la réception d’une `100 continue` réponse, le client envoie la partie restante de la demande qui complète la demande.
4. NetScaler exécute ensuite toutes les protections, puis transmet la demande au serveur.
5. Maintenant que NetScaler transmet la requête complète, l’en-tête EXPECT qui figurait dans la demande initiale devient obsolète, car NetScaler corrompt cet en-tête et l’envoie au serveur.
6. Lors de la réception de la demande, le serveur ignore tout en-tête endommagé.

Configuration de Web App Firewall

June 2, 2023

Vous pouvez configurer le NetScaler Web App Firewall (Web App Firewall) à l’aide de l’une des méthodes suivantes :

- **Assistant de Web App Firewall.** Une boîte de dialogue composée d’une série d’écrans qui vous guident tout au long du processus de configuration.

- **Modèle AppExpert de l'interface Web NetScaler.** Un modèle AppExpert (un ensemble de paramètres de configuration) conçu pour fournir une protection appropriée aux sites Web. Ce modèle AppExpert contient les paramètres de configuration du Web App Firewall appropriés pour protéger de nombreux sites Web.
- **Interface graphique NetScaler.** L'interface de configuration Web.
- **Interface de ligne de commande NetScaler.** L'interface de configuration en ligne de commande.

Citrix vous recommande d'utiliser l'assistant Web App Firewall. La plupart des utilisateurs trouveront que c'est la méthode la plus simple pour configurer le Web App Firewall, et elle est conçue pour éviter les erreurs. Si vous possédez un nouveau NetScaler ou VPX que vous utiliserez principalement pour protéger les sites Web, vous trouverez peut-être que le modèle AppExpert de l'interface Web est une meilleure option car il fournit une bonne configuration par défaut, non seulement pour le Web App Firewall, mais pour l'ensemble de l'appliance. L'interface graphique et l'interface de ligne de commande sont toutes deux destinées aux utilisateurs expérimentés, principalement pour modifier une configuration existante ou utiliser des options avancées.

Assistant Web App Firewall

L'assistant Web App Firewall est une boîte de dialogue composée de plusieurs écrans qui vous invitent à configurer chaque partie d'une configuration simple. Le Web App Firewall crée ensuite les éléments de configuration appropriés à partir des informations que vous lui donnez. Il s'agit de la méthode la plus simple et, dans la plupart des cas, la meilleure pour configurer le Web App Firewall.

Pour utiliser l'assistant, connectez-vous à l'interface graphique avec le navigateur de votre choix. Lorsque la connexion est établie, vérifiez que le Web App Firewall est activé, puis exécutez l'assistant Web App Firewall, qui vous demande des informations de configuration. Vous n'êtes pas obligé de fournir toutes les informations demandées la première fois que vous utilisez l'assistant. Vous pouvez plutôt accepter les paramètres par défaut, effectuer quelques tâches de configuration relativement simples pour activer des fonctionnalités importantes, puis autoriser le Web App Firewall à collecter des informations importantes pour vous aider à terminer la configuration.

Par exemple, lorsque l'assistant vous invite à spécifier une règle pour sélectionner le trafic à traiter, vous pouvez accepter la règle par défaut, qui sélectionne tout le trafic. Lorsqu'il vous présente une liste de signatures, vous pouvez activer les catégories de signatures appropriées et activer la collecte de statistiques pour ces signatures. Pour cette configuration initiale, vous pouvez ignorer les protections avancées (contrôles de sécurité). L'assistant crée automatiquement la politique, l'objet de signature et le profil appropriés (collectivement, la configuration de sécurité), et lie la politique au niveau global. Le Web App Firewall commence alors à filtrer les connexions vers vos sites Web protégés, à enregistrer toutes les connexions qui correspondent à une ou plusieurs des signatures que vous avez activées et à collecter des statistiques sur les connexions auxquelles chaque signature correspond. Une fois que le Web App Firewall a traité une partie du trafic, vous pouvez réexécuter l'assistant et examiner

les journaux et les statistiques pour voir si l'une des signatures que vous avez activées correspond au trafic légitime. Après avoir déterminé quelles signatures identifient le trafic que vous souhaitez bloquer, vous pouvez activer le blocage de ces signatures. Si votre site Web ou service Web n'est pas complexe, n'utilise pas SQL et n'a pas accès à des informations privées sensibles, cette configuration de sécurité de base fournira probablement une protection adéquate.

Vous pouvez avoir besoin d'une protection supplémentaire si, par exemple, votre site Web est dynamique. Le contenu qui utilise des scripts peut avoir besoin d'une protection contre les attaques par script intersites. Les contenus Web qui utilisent SQL, tels que les paniers d'achat, de nombreux blogs et la plupart des systèmes de gestion de contenu, peuvent avoir besoin d'une protection contre les attaques par injection SQL. Les sites Web et les services Web qui collectent des informations privées sensibles telles que des numéros de sécurité sociale ou de carte de crédit peuvent nécessiter une protection contre l'exposition involontaire de ces informations. Certains types de logiciels de serveur Web ou de serveur XML peuvent nécessiter une protection contre des types d'attaques adaptés à ces logiciels. Il faut également tenir compte du fait que des éléments spécifiques de vos sites Web ou services Web peuvent nécessiter une protection différente de celle d'autres éléments. L'examen des journaux et des statistiques du Web App Firewall peut vous aider à identifier les protections supplémentaires dont vous pourriez avoir besoin.

Après avoir décidé quelles protections avancées sont nécessaires pour vos sites Web et services Web, vous pouvez exécuter à nouveau l'assistant pour configurer ces protections. Certains contrôles de sécurité nécessitent que vous saisissiez des exceptions (assouplissements) pour empêcher le contrôle de bloquer le trafic légitime. Vous pouvez le faire manuellement, mais il est généralement plus facile d'activer la fonction d'apprentissage adaptatif et de lui permettre de recommander la relaxation nécessaire. Vous pouvez utiliser l'assistant autant de fois que nécessaire pour améliorer votre configuration de sécurité de base et/ou créer des configurations de sécurité supplémentaires.

L'assistant automatise certaines tâches que vous devriez effectuer manuellement si vous ne l'utilisiez pas. Il crée automatiquement une politique, un objet de signature et un profil, et leur attribue le nom que vous avez indiqué lorsque vous avez été invité à entrer le nom de votre configuration. L'assistant ajoute également vos paramètres de protection avancés au profil, lie l'objet de signatures au profil, associe le profil à la politique et met la politique en vigueur en la liant à Global.

Certaines tâches ne peuvent pas être effectuées dans l'assistant. Vous ne pouvez pas utiliser l'assistant pour lier une politique à un point de liaison autre que Global. Si vous souhaitez que le profil s'applique uniquement à une partie spécifique de votre configuration, vous devez configurer manuellement la liaison. Vous ne pouvez pas configurer les paramètres du moteur ni certaines autres options de configuration globale dans l'assistant. Bien que vous puissiez configurer l'un des paramètres de protection avancés de l'Assistant, si vous souhaitez modifier un paramètre spécifique dans une seule vérification de sécurité, il peut être plus facile de le faire sur les écrans de configuration manuelle de l'interface graphique.

Pour plus d'informations sur l'utilisation de l'assistant Web App Firewall Wizard, consultez l'assistant

Web App Firewall Wizard.

Modèle AppExpert de l'interface Web NetScaler

Les modèles AppExpert constituent une approche différente et plus simple de la configuration et de la gestion d'applications d'entreprise complexes. L'affichage d'AppExpert dans l'interface graphique se compose d'un tableau. Les applications sont répertoriées dans la colonne la plus à gauche, et les fonctionnalités NetScaler applicables à cette application apparaissent chacune dans sa propre colonne à droite. (Dans l'interface AppExpert, les fonctionnalités associées à une application sont appelées *unités d'application*.) Dans l'interface AppExpert, vous configurez le trafic intéressant pour chaque application et activez les règles de compression, de mise en cache, de réécriture, de filtrage, de répondeur et de Web App Firewall, au lieu d'avoir à configurer chaque fonctionnalité individuellement.

Le modèle AppExpert Interface Web contient des règles pour les signatures de Web App Firewall et les vérifications de sécurité suivantes :

- **Refuser la vérification d'URL.** Détecte les connexions au contenu qui pose un risque de sécurité ou à toute autre URL que vous désignez.
- **Vérification du dépassement de tampon.** Détecte les tentatives de provoquer un dépassement de tampon sur un serveur Web protégé.
- **Vérification de la cohérence des cookies.** Détecte les modifications malveillantes des cookies définis par un site Web protégé.
- **Vérification de la cohérence des champs de formulaire.** Détecte les modifications apportées à la structure d'un formulaire Web sur un site Web protégé.
- **Vérification du marquage de formulaire CSRF.** Détecte les attaques de falsification de requêtes intersites.
- **Vérification des formats de champ.** Détecte les informations inappropriées téléchargées dans les formulaires Web sur un site Web protégé.
- **Vérification HTML SQL Injection.** Détecte les tentatives d'injection de code SQL non autorisé.
- **Contrôle HTML Cross-Site Scripting.** Détecte les attaques de script inter-sites.

Pour plus d'informations sur l'installation et l'utilisation d'un modèle AppExpert, consultez Applications et modèles AppExpert.

L'interface graphique

L'interface graphique est une interface Web qui permet d'accéder à toutes les options de configuration de la fonctionnalité Web App Firewall, y compris des options de configuration et de gestion avancées qui ne sont disponibles dans aucun autre outil ou interface de configuration. Plus précisément, de nombreuses options de signature avancées ne peuvent être configurées que dans l'interface graphique. Vous pouvez consulter les recommandations générées par la fonctionnalité

d'apprentissage uniquement dans l'interface graphique. Vous pouvez lier des stratégies à un point de liaison autre que Global uniquement dans l'interface graphique.

Pour obtenir une description de l'interface graphique, reportez-vous à la section Interfaces de configuration du Web App Firewall. Pour plus d'informations sur l'utilisation de l'interface graphique pour configurer le Web App Firewall, voir Configuration manuelle à l'aide de l'interface graphique.

Pour obtenir des instructions sur la configuration du Web App Firewall à l'aide de l'interface graphique, voir Configuration manuelle à l'aide de l'interface graphique. Pour plus d'informations sur l'interface graphique de citrix-adc, reportez-vous à la section Interfaces de configuration du Web App Firewall.

L'interface de ligne de commande NetScaler

L'interface de ligne de commande NetScaler est un shell UNIX modifié basé sur le shell bash de FreeBSD. Pour configurer le Web App Firewall à partir de l'interface de ligne de commande, vous tapez des commandes à l'invite et vous appuyez sur la touche Entrée, comme vous le faites avec n'importe quel autre shell Unix. Vous pouvez configurer la plupart des paramètres et options du Web App Firewall à l'aide de la ligne de commande NetScaler. Les exceptions sont la fonctionnalité de signatures, dont la plupart des options peuvent être configurées uniquement à l'aide de l'interface graphique ou de l'assistant de Web App Firewall, et la fonctionnalité d'apprentissage, dont les recommandations ne peuvent être examinées que dans l'interface graphique.

Pour obtenir des instructions sur la configuration du Web App Firewall à l'aide de la ligne de commande NetScaler, voir Configuration manuelle à l'aide de l'interface de ligne de commande.

Activer le pare-feu NetScaler Web App

May 5, 2023

Avant de pouvoir créer une configuration de sécurité, vous devez activer la fonctionnalité NetScaler Web App Firewall sur l'appliance.

Points à retenir

- Si vous configurez une appliance NetScaler Web App Firewall dédiée ou si vous mettez à niveau une appliance existante, la fonctionnalité est déjà activée. Vous n'êtes pas obligé d'effectuer l'une ou l'autre des procédures décrites ici.
- Si vous possédez un nouveau NetScaler ou VPX, vous devez activer la fonctionnalité NetScaler Web App Firewall avant de le configurer.
- Si vous mettez à niveau un NetScaler ou un VPX à partir d'une version précédente, vous devez d'abord activer la fonctionnalité NetScaler Web App Firewall avant de la configurer.

> **Remarque :**
>
> Si vous mettez à niveau un NetScaler ou un VPX à partir d'une version précédente, vous devrez peut-être mettre à jour les licences de votre appliance avant d'activer NetScaler Web App Firewall. Renseignez-vous auprès de votre représentant ou revendeur NetScaler pour obtenir la licence appropriée.

Activez le pare-feu NetScaler Web App à l'aide de l'interface de commande

À l'invite de commandes, tapez la commande suivante :

```
enable ns feature AppFW
```

Activez le Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet de détails, cliquez sur **Configurer les fonctionnalités avancées**.
3. Sur la page **Configurer les fonctionnalités avancées**, sélectionnez **NetScaler Web App Firewall**.
4. Cliquez sur **OK**.



L'assistant de Web App Firewall

May 5, 2023

Contrairement à la plupart des assistants, l'assistant NetScaler Web App Firewall est conçu non seulement pour simplifier le processus de configuration initial, mais également pour modifier les configu-

rations créées précédemment et pour maintenir la configuration de votre Web App Firewall. Un utilisateur type exécute l'assistant plusieurs fois en sautant certains écrans à chaque fois.

L'assistant Web App Firewall crée automatiquement des profils, des politiques et des signatures.

Ouverture de l'assistant

Pour exécuter l'assistant Web App Firewall, ouvrez l'interface graphique et procédez comme suit :

1. Accédez à **Sécurité** > **Pare-feu d'applications**.
2. Dans le volet d'informations, sous **Mise en route**, cliquez sur **Application Firewall Wizard**. L'Assistant s'ouvre.

Pour plus d'informations sur l'interface graphique, consultez les interfaces de configuration du Web App Firewall.

Les écrans de l'Assistant

L'assistant Web App Firewall affiche les écrans suivants sur une page tabulaire :

1. Spécifiez le nom : sur cet écran, lorsque vous créez une nouvelle configuration de sécurité, spécifiez un nom significatif et le type approprié (HTML, XML ou WEB 2.0) pour votre profil. La politique et les signatures par défaut sont générées automatiquement en utilisant le même nom.

Nom du profil

Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement et peut comprendre de 1 à 31 lettres, des chiffres et les symboles tiret (-), point (.), livre (#), espace (), at (@), égal (=), deux-points (:) et trait de soulignement (_). Choisissez un nom qui permet aux autres utilisateurs de déterminer facilement le contenu protégé par votre nouvelle configuration de sécurité.

> **Remarque :**
>
> Comme l'assistant utilise ce nom à la fois pour la politique et pour le profil, il est limité à 31 caractères. Les politiques créées manuellement peuvent avoir des noms d'une longueur maximale de 127 caractères.

Lorsque vous modifiez une configuration existante, vous sélectionnez Modifier la configuration existante puis, dans la liste déroulante Nom, sélectionnez le nom de la configuration existante que vous souhaitez modifier.

> **Remarque :**
>
> Seules les politiques liées à une stratégie globale ou à un point de liaison apparaissent dans cette liste ; vous ne pouvez pas modifier une politique indépendante à l'aide de l'assistant Application Firewall. Vous devez soit le lier manuellement à Global ou à un point de liaison, soit le modifier manuellement. (Pour une modification manuelle, dans l'interface graphique) **Pare-feu**

> **d'application** > **Politiques** > volet **Pare-feu**, sélectionnez la politique et cliquez sur **Ouvrir**.

Type de profil

Vous pouvez également sélectionner un type de profil sur cet écran. Le type de profil détermine les types de protection avancée (contrôles de sécurité) qui peuvent être configurés. Comme certains types de contenu ne sont pas vulnérables à certains types de menaces de sécurité, la limitation de la liste des vérifications disponibles permet de gagner du temps lors de la configuration. Les types de profils de Web App Firewall sont les suivants :

- Application Web (HTML). Tout site Web HTML qui n'utilise pas les technologies XML ou Web 2.0.
- Application XML (XML, SOAP). Tout service Web basé sur XML.
- Application Web 2.0 (HTML, XML, REST). Tout site Web 2.0 qui combine du contenu HTML et XML, tel qu'un site Atom, un blog, un flux RSS ou un wiki.

Remarque : Si vous ne savez pas quel type de contenu est utilisé sur votre site Web, vous pouvez choisir l'application Web 2.0 pour vous assurer de protéger tous les types de contenu d'applications Web.

2. Spécifier la règle : dans cet écran, vous pouvez spécifier la règle de politique (expression) qui définit le trafic examiné par la configuration actuelle. Si vous créez une configuration initiale pour protéger vos sites Web et services Web, vous pouvez accepter la valeur par défaut, **true**, qui sélectionne tout le trafic Web.

Si vous souhaitez que cette configuration de sécurité examine non pas l'ensemble du trafic HTTP acheminé via l'appliance, mais un trafic spécifique, vous pouvez rédiger une règle de politique spécifiant le trafic que vous souhaitez qu'elle examine. Les règles sont écrites dans le langage d'expressions NetScaler, qui est un langage de programmation orienté objet entièrement fonctionnel.

Remarque : Outre la syntaxe des expressions par défaut, pour des raisons de rétrocompatibilité, le système d'exploitation NetScaler prend en charge la syntaxe des expressions classiques NetScaler sur les appliances NetScaler Classic et nCore et les appliances virtuelles. Les expressions classiques ne sont pas prises en charge sur les appliances NetScaler Cluster et les appliances virtuelles. Les utilisateurs actuels qui souhaitent migrer leurs configurations existantes vers le cluster NetScaler doivent migrer toutes les politiques contenant des expressions classiques vers la syntaxe des expressions par défaut.

- Pour une description simple de l'utilisation de la syntaxe des expressions NetScaler pour créer des règles de Web App Firewall, ainsi qu'une liste de règles utiles, voir Politiques de pare-feu.
- Pour une explication détaillée de la création de règles de politique dans la syntaxe des expressions NetScaler, consultez Politiques etexpressions.

4. Sélectionnez Signatures : sur cet écran, vous sélectionnez les catégories de signatures que vous souhaitez utiliser pour protéger vos sites Web et services Web.

Cette étape n'est pas obligatoire et vous pouvez l'ignorer si vous le souhaitez et accéder à l'écran **Spé-**

cifier les protections approfondies . Si l'écran Sélectionner les signatures est ignoré, seuls un profil et les politiques associées sont créés, mais les signatures ne sont pas créées.

Vous pouvez sélectionner **Créer une nouvelle signature** ou **Sélectionner une signature existante**.

Si vous créez une nouvelle configuration de sécurité, les catégories de signatures que vous sélectionnez sont activées et, par défaut, elles sont enregistrées dans un nouvel objet de signature. Le nouvel objet de signatures se voit attribuer le même nom que celui que vous avez saisi dans l'écran Spécifier le nom comme nom de la configuration de sécurité.

Si vous avez déjà configuré des objets de signature et que vous souhaitez utiliser l'un d'entre eux comme objet de signature associé à la configuration de sécurité que vous créez, cliquez sur **Sélectionner une signature existante** et sélectionnez un objet de signature dans la liste des signatures.

Si vous modifiez une configuration de sécurité existante, vous pouvez cliquer sur Sélectionner une signature existante et attribuer un objet de signature différent à la configuration de sécurité.

Si vous cliquez sur Créer une nouvelle signature, vous pouvez choisir le mode d'édition **simple** ou **avancé**.

1. **Spécifier les protections de signature (mode simple)**

Le mode simple permet de configurer facilement la signature, avec une liste prédéfinie de définitions de protection pour les applications courantes telles que IIS (Internet Information Server), PHP et ActiveX. Les catégories par défaut en mode Simple sont les suivantes :

- CGI. Protection contre les attaques contre les sites Web qui utilisent des scripts CGI dans n'importe quel langage, y compris les scripts PERL, les scripts shell Unix et les scripts Python.
- Fusion à froid. Protection contre les attaques visant les sites Web qui utilisent la plateforme de développement Web Adobe Systems® ColdFusion®.
- Page d'accueil. Protection contre les attaques visant les sites Web qui utilisent la plateforme de développement Web Microsoft® FrontPage®.
- PHP. Protection contre les attaques contre les sites Web qui utilisent le langage de script de développement Web open source PHP.
- Côté client. Protection contre les attaques visant les outils côté client utilisés pour accéder à vos sites Web protégés, tels que Microsoft Internet Explorer, Mozilla Firefox, le navigateur Opera et Adobe Acrobat Reader.
- Microsoft IIS. Protection contre les attaques contre les sites Web qui exécutent Microsoft Internet Information Server (IIS)
- Divers. Protection contre les attaques visant d'autres outils côté serveur, tels que les serveurs Web et les serveurs de base de données.

Sur cet écran, vous sélectionnez les actions associées aux catégories de signatures que vous avez sélectionnées sur l'écran Sélectionner les signatures. Les actions que vous pouvez configurer sont les suivantes :

- Bloquer
- Journal
- Statistiques

Par défaut, les actions Journal et Statistiques sont activées, mais pas l'action Bloquer. Pour configurer les actions, cliquez sur **Paramètres**. Vous pouvez modifier les paramètres d'action de toutes les catégories sélectionnées à l'aide de la liste déroulante **Action** .

1. **Spécifier les protections de signature (mode avancé)**

Le mode avancé permet un contrôle plus précis des définitions de signature et fournit beaucoup plus d'informations. Utilisez le mode avancé si vous souhaitez contrôler complètement la définition de signature.

Le contenu de cet écran est identique au contenu de la boîte de dialogue Modifier un objet Signatures, comme décrit dans Configuration ou modification d'un objet Signatures. Dans cet écran, vous pouvez configurer des actions en cliquant sur la liste déroulante **Actions** ou sur le menu Actions, qui apparaît sous la forme d'un cercle avec trois points.

7. Spécifiez les protections approfondies : sur cet écran, vous choisissez les protections avancées (également appelées contrôles de sécurité ou simplement contrôles) que vous souhaitez utiliser pour protéger vos sites Web et services Web. Les vérifications disponibles dépendent du type de profil que vous avez choisi sur l'écran Spécifier le nom. Toutes les vérifications sont disponibles pour les profils d'application Web 2.0.

Pour plus d'informations, voir Vue d'ensemble des contrôles de sécuritéet voir Contrôles avancés de protection des formulaires.

Vous configurez les actions pour les protections avancées que vous avez activées.Les actions que vous pouvez configurer sont les suivantes :

- Bloquer : bloque les connexions qui correspondent à la signature. Désactivé par défaut.
- Journal : enregistre les connexions qui correspondent à la signature pour une analyse ultérieure. Activé par défaut.
- Statistiques : conserve des statistiques, pour chaque signature, qui indiquent le nombre de connexions correspondantes et fournissent certaines autres informations sur les types de connexions bloquées. Désactivé par défaut.
- Apprenez. Observez le trafic vers ce site Web ou ce service Web et utilisez les connexions qui enfreignent régulièrement cette vérification pour générer des exceptions recommandées à la vérification ou de nouvelles règles pour la vérification. Disponible uniquement pour certains chèques. Pour plus d'informations sur la fonctionnalité d'apprentissage, voir Configuration et

utilisation de la fonctionnalité d'apprentissage, et comment l'apprentissage fonctionne et comment configurer des exceptions (relaxations) ou déployer des règles apprises pour une vérification, voir Configuration manuelle à l'aide de l'interface graphique.

Pour configurer des actions, activez la protection en cochant la case à cocher, puis cliquez sur **Paramètres d'action** pour sélectionner les actions requises. Sélectionnez d'autres paramètres, si nécessaire, puis cliquez sur **OK** pour fermer la fenêtre Paramètres d'action.

Pour afficher tous les journaux d'une vérification spécifique, sélectionnez-la, puis cliquez sur **Journaux** pour afficher la visionneuse Syslog, comme décrit dans Journaux du Web App Firewall. Si une vérification de sécurité bloque l'accès légitime à votre site Web ou service Web protégé, vous pouvez créer et implémenter une relaxation pour cette vérification de sécurité en sélectionnant un journal affichant le blocage indésirable, puis en cliquant sur **Déployer**.

Après avoir défini les paramètres d'action, cliquez sur **Terminer** pour terminer l'assistant.

Les quatre procédures suivantes montrent comment effectuer des types de configuration spécifiques à l'aide de l'assistant Web App Firewall.

Création d'une nouvelle configuration

Procédez comme suit pour créer une nouvelle configuration de pare-feu et des objets de signature à l'aide de l'assistant de pare-feu d'application.

1. Accédez à **Sécurité** > **Pare-feu d'applications**.
2. Dans le volet d'informations, sous **Mise en route**, cliquez sur Pare-feu **d'applications. L'Assistant s'ouvre.



3. Sur l'écran **Spécifier le nom**, sélectionnez **Créer une nouvelle configuration.
4. Dans le champ **Nom**, saisissez un nom, puis cliquez sur **Suivant**.
5. Dans l'écran **Spécifier la règle**, cliquez à nouveau sur **Suivant** .
6. Dans l'écran **Sélectionner les signatures**, sélectionnez **Créer une nouvelle signature** et **Simple** comme mode d'édition, puis cliquez sur **Suivant**.
7. Dans l'écran **Spécifier les protections de signature**, configurez les paramètres requis. Pour plus d'informations sur les signatures à bloquer et sur la manière de déterminer quand vous pouvez activer le blocage d'une signature en toute sécurité, consultez la section Signatures.
8. Dans l'écran **Spécifier les protections approfondies**, configurez les actions et les paramètres requis dans **Paramètres d'action**.
9. Lorsque vous avez terminé, cliquez sur **Terminer** pour fermer l'assistant de pare-feu d'applications.

Modifier une configuration existante

Suivez ces étapes pour modifier une configuration existante et des catégories de signatures existantes.

1. Accédez à **Sécurité** > **Pare-feu d'applications**.

2. Dans le volet d'informations, sous **Mise en route**, cliquez sur **Application Firewall Wizard**. L'Assistant s'ouvre.
3. Sur l'écran **Spécifier le nom**, sélectionnez Modifier la configuration existante et, dans la liste déroulante **Nom**, choisissez la configuration de sécurité que vous avez créée lors de la nouvelle configuration, puis cliquez sur **Suivant**.
4. Dans l'écran **Spécifier la règle**, cliquez sur Suivant pour conserver la valeur par défaut « true ». Si vous souhaitez modifier la règle, suivez les étapes décrites dans Configurer une expression de stratégie personnalisée.
5. Dans l'écran **Sélectionner les signatures**, cliquez sur **Sélectionner une signature existante**. Dans la liste déroulante **Signature existante**, sélectionnez l'option appropriée, puis cliquez sur **Suivant**. L'écran de protection avancée des signatures s'affiche.
   Remarque : Si vous sélectionnez une signature existante, le mode d'édition par défaut pour la protection des signatures est avancé.
6. Dans l'écran Spécifier les protections de signature, configurez les paramètres requis et cliquez sur **Suivant**. Pour plus d'informations sur les signatures à prendre en compte pour le blocage et sur la manière de déterminer quand vous pouvez activer le blocage d'une signature en toute sécurité, consultez la section Signatures.
7. Dans l'écran **Spécifier les protections profondes**, configurez les paramètres et cliquez sur **Suivant**.
8. Une fois que vous avez terminé, cliquez sur **Terminer** pour fermer l' **assistant Web App Firewall**.

Création d'une nouvelle configuration sans signatures

Suivez ces étapes pour utiliser l'assistant de pare-feu des applications afin d'ignorer l'écran de sélection des signatures et de créer une nouvelle configuration avec uniquement le profil et les politiques associées, mais sans aucune signature.

1. Accédez à **Sécurité** > **Pare-feu d'applications**.
2. Dans le volet d'informations, sous **Mise en route**, cliquez sur **Application Firewall Wizard**. L'Assistant s'ouvre.
3. Sur l'écran **Spécifier le nom**, sélectionnez **Créer une nouvelle configuration**.
4. Dans le champ **Nom**, saisissez un nom, puis cliquez sur **Suivant**.
5. **Dans l'écran**Spécifier une règle**, cliquez à nouveau sur Suivant.**
6. Dans l'écran **Sélectionner les signatures**, cliquez sur **Ignorer.**
7. Dans l'écran **Spécifier les protections approfondies**, configurez les actions et les paramètres requis dans **Paramètres d'action**.
8. Lorsque vous avez terminé, cliquez sur **Terminer** pour fermer l'assistant de pare-feu d'application.

Configuration d'une expression de politique personnalisée

Suivez ces étapes pour utiliser l'assistant de pare-feu d'application afin de créer une configuration de sécurité spécialisée afin de protéger uniquement un contenu spécifique. Dans ce cas, vous créez une nouvelle configuration de sécurité au lieu de modifier la configuration initiale. Ce type de configuration de sécurité nécessite une règle personnalisée, de sorte que la politique applique la configuration uniquement au trafic Web sélectionné.

1. Accédez à **Sécurité** > **Pare-feu d'applications**.
2. Dans le volet d'informations, sous **Mise en route**, cliquez sur **Application Firewall Wizard**.
3. Sur l'écran Spécifier le nom, tapez le nom de votre nouvelle configuration de sécurité dans la zone de texte Nom, sélectionnez le type de configuration de sécurité dans la liste déroulante Type, puis cliquez sur **Suivant**.
4. Dans l'écran **Spécifier la règle**, entrez une règle qui correspond uniquement au contenu que vous souhaitez que cette application Web protège. Utilisez la liste déroulante **Expressions fréquemment utilisées** et l' **éditeur d'** expressions pour créer une expression personnalisée. Lorsque vous avez terminé, cliquez sur **Suivant**.
5. Dans l'écran **Sélectionner les signatures**, sélectionnez le mode d'édition, puis cliquez sur **Suivant**.
6. Dans l'écran **Spécifier les protections de signature**, configurez les paramètres requis.
7. Dans l'écran **Spécifier les protections approfondies**, configurez les actions et les paramètres requis dans **Paramètres d'action**.
8. Lorsque vous avez terminé, cliquez sur **Terminer** pour fermer l' **assistant de pare-feu d'applications**.

Configuration manuelle

August 20, 2021

Si vous souhaitez lier un profil à un point de liaison autre que Global, vous devez configurer manuellement la liaison. En outre, certaines vérifications de sécurité exigent que vous saisissez manuellement les exceptions nécessaires ou que la fonctionnalité d'apprentissage génère les exceptions dont vos sites Web et services Web ont besoin. Certaines de ces tâches ne peuvent pas être effectuées à l'aide de l'Assistant Web App Firewall.

Si vous connaissez bien le fonctionnement du Web App Firewall et que vous préférez une configuration manuelle, vous pouvez configurer manuellement un objet signatures et un profil, associer l'objet signatures au profil, créer une stratégie avec une règle qui correspond au trafic Web que vous souhaitez configurer et associer la stratégie avec le profil. Vous liez ensuite la stratégie à Global, ou à un point de liaison, pour la mettre en œuvre, et vous avez créé une configuration de sécurité complète.

Pour la configuration manuelle, vous pouvez utiliser l'interface graphique (interface graphique) ou la ligne de commande. Citrix vous recommande d'utiliser l'interface graphique. Toutes les tâches de configuration ne peuvent pas être exécutées sur la ligne de commande. Certaines tâches, telles que l'activation des signatures et l'examen des données apprises, doivent être effectuées dans l'interface graphique. La plupart des autres tâches sont plus faciles à effectuer dans l'interface graphique.

Réplication de la configuration

Lorsque vous utilisez l'interface graphique (GUI) ou l'interface de ligne de commande (CLI) pour configurer manuellement le Web App Firewall, la configuration est enregistrée dans le fichier /nsconfig/ns.conf. Vous pouvez utiliser les commandes de ce fichier pour répliquer la configuration sur une autre appliance. Vous pouvez couper et coller les commandes dans l'interface de ligne de commande une par une, ou enregistrer plusieurs commandes dans un fichier texte dans le dossier /var/tmp et les exécuter en tant que fichier batch. Voici un exemple d'exécution d'un fichier batch contenant des commandes copiées à partir du fichier /nsconfig/ns.conf d'une autre appliance :

```
> batch -f /var/tmp/appfw_add.txt
```

> **Avertissement :**
>
> Les commandes d'importation ne sont pas enregistrées dans le fichier ns.conf. Avant d'exécuter des commandes à partir du fichier ns.conf pour répliquer la configuration sur une autre appliance, vous devez importer tous les objets utilisés dans la configuration (par exemple, signatures, page d'erreur, WSDL et schéma) vers l'appliance sur laquelle vous répliquez la configuration. La commande add permettant d'ajouter un profil Web App Firewall enregistré dans un fichier ns.conf peut inclure le nom d'un objet importé, mais cette commande peut échouer lorsqu'elle est exécutée sur une autre appliance si l'objet référencé n'existe pas sur cette appliance.

Pour plus d'informations sur les détails d'importation ou d'exportation pour la réplication de la configuration, consultez les rubriques Exportation de signatureset Export d'importation commune .

Configuration manuelle à l'aide de l'interface graphique NetScaler

May 5, 2023

Si vous devez configurer manuellement la fonctionnalité Web App Firewall, Citrix vous recommande d'utiliser la procédure de l'interface graphique NetScaler.

Pour créer et configurer un objet de signatures

Avant de configurer les signatures, vous devez créer un objet de signatures à partir du modèle d'objet de signatures par défaut approprié. Attribuez un nouveau nom à la copie, puis configurez la copie.

Vous ne pouvez pas configurer ou modifier directement les objets de signatures par défaut. La procédure suivante fournit des instructions de base pour configurer un objet signatures. Pour obtenir des instructions plus détaillées, voir Configuration manuelle de la fonctionnalité Signatures.

1. Accédez à **Sécurité > NetScaler Web App Firewall > Signatures**.
2. Dans le volet de détails, sélectionnez l'objet de signatures que vous souhaitez utiliser comme modèle, puis cliquez sur **Ajouter**.

   Vos choix sont les suivants :

   - **Signatures par défaut.** Contient les règles de signature, les règles d'injection SQL et les règles de script intersite.
   - **Injection XPath.** Contient tous les éléments des signatures par défaut et contient également les règles d'injection XPath.
3. Dans la boîte de dialogue **Ajouter un objet de signature**, tapez le nom de votre nouvel objet de signature, cliquez sur OK, puis sur **Fermer**. Le nom peut commencer par une lettre, un chiffre ou le symbole du trait de soulignement et peut être composé de 1 à 31 lettres, chiffres et tiret (-), point (.) livre (#), espace (), at (@), égal (=) et trait de soulignement (_).
4. Sélectionnez l'objet de signatures que vous avez créé, puis cliquez sur **Ouvrir**.
5. Dans la boîte de dialogue **Modifier l'objet des signatures**, définissez les options **Afficher les critères de filtre** sur la gauche pour afficher les éléments de filtre que vous souhaitez configurer.

   Lorsque vous modifiez ces options, les résultats que vous spécifiez sont affichés dans la fenêtre Résultats filtrés située à droite. Pour plus d'informations sur les catégories de signatures, voir Signatures.
6. Dans la zone **Résultats filtrés**, configurez les paramètres d'une signature en cochant et en désactivant les cases à cocher appropriées.
7. Lorsque vous avez terminé, cliquez sur **Fermer**.

Pour créer un profil de Web App Firewall à l'aide de l'interface graphique

Pour créer un profil de Web App Firewall, vous ne devez spécifier que quelques détails de configuration.

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un profil de Web App Firewall**, tapez le nom de votre profil.

Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement et peut comprendre de 1 à 31 lettres, chiffres et le tiret (-), le point (.), la livre (#), l'espace (), l'arobase (@), l'égal (=), les deux points (:) et le trait de soulignement (_).

4. Choisissez le type de profil dans la liste déroulante.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour configurer un profil Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez le profil que vous souhaitez configurer, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Configurer le profil de Web App Firewall**, sous l'onglet **Vérifications de sécurité**, configurez les contrôles de sécurité.
   - Pour activer ou désactiver une action pour une vérification, dans la liste, activez ou désactivez la case à cocher correspondant à cette action.
   - Pour configurer d'autres paramètres pour les contrôles qui en disposent, dans la liste, cliquez sur le chevron bleu situé à l'extrême droite de cette vérification. Dans la boîte de dialogue qui s'affiche, configurez les paramètres. Celles-ci varient d'un chèque à l'autre.

     Vous pouvez également sélectionner une coche et, au bas de la boîte de dialogue, cliquer sur Ouvrir pour afficher la boîte de dialogue Configurer la relaxation ou Configurer la règle pour cette vérification. Ces boîtes de dialogue varient également d'une vérification à l'autre. La plupart d'entre eux incluent un onglet Vérifications et un onglet Général . Si la vérification prend en charge les assouplissements ou les règles définies par l'utilisateur, l'onglet Vérifications inclut un bouton Ajouter, qui ouvre une autre boîte de dialogue, dans laquelle vous pouvez spécifier un assouplissement ou une règle pour la vérification. (Un assouplissement est une règle visant à exempter du contrôle le trafic spécifié.) Si les relaxations ont déjà été configurées, vous pouvez en sélectionner une et cliquer sur Ouvrir pour la modifier.
   - Pour consulter les exceptions ou les règles apprises pour une vérification, sélectionnez-la, puis cliquez sur Violations apprises. Dans la boîte de dialogue Gérer les règles apprises, sélectionnez chaque exception ou règle apprise à tour de rôle.
     - Pour modifier l'exception ou la règle, puis l'ajouter à la liste, cliquez sur **Modifier et déployer**.
     - Pour accepter l'exception ou la règle sans modification, cliquez sur **Déployer**.
     - Pour supprimer l'exception ou la règle de la liste, cliquez sur **Ignorer**.
   - Pour actualiser la liste des exceptions ou des règles à examiner, cliquez sur **Actualiser**.

- Pour ouvrir le **visualiseur d'apprentissage** et l'utiliser pour consulter les règles apprises, cliquez sur **Visualiseur**.
- Pour consulter les entrées du journal pour les connexions qui correspondent à une vérification, sélectionnez la vérification, puis cliquez sur **Journaux**. Vous pouvez utiliser ces informations pour déterminer quels contrôles correspondent à des attaques afin de pouvoir activer le blocage de ces contrôles. Vous pouvez également utiliser ces informations pour déterminer quelles vérifications correspondent au trafic légitime, de sorte que vous pouvez configurer une exemption appropriée pour autoriser ces connexions légitimes. Pour plus d'informations sur les journaux, consultez Journaux, statistiques et rapports.
- Pour désactiver complètement une coche, dans la liste, désactivez toutes les cases à droite de cette coche.

4. Dans l'onglet **Paramètres**, configurez les paramètres du profil.
   - Pour associer le profil à l'ensemble de signatures que vous avez créé et configuré précédemment, sous **Paramètres communs**, sélectionnez cet ensemble de signatures dans la liste déroulante Signatures.

     > **Remarque :**
     >
     > Vous pouvez utiliser la barre de défilement située à droite de la boîte de dialogue pour faire défiler vers le bas et afficher la section Paramètres communs.

   - Pour configurer un objet d'erreur HTML ou XML, sélectionnez-le dans la liste déroulante appropriée.

     > **Remarque :**
     >
     > Vous devez d'abord charger l'objet d'erreur que vous souhaitez utiliser dans le volet Importer.

   - Pour configurer le type de contenu XML par défaut, saisissez la chaîne du type de contenu directement dans les zones de texte Demande par défaut et Réponse par défaut, ou cliquez sur Gérer les types de contenu autorisés pour gérer la liste des types de contenu autorisés.
5. Si vous souhaitez utiliser la fonctionnalité d'apprentissage, cliquez sur Formation et configurez les paramètres d'apprentissage du profil. Pour plus d'informations, voir Fonctionnalité Configurer et apprendre.
6. Cliquez sur **OK** pour enregistrer vos modifications et revenir au volet Profils.

Configuration d'une règle ou d'une relaxation du Web App Firewall

Vous pouvez configurer deux types d'informations différents dans cette boîte de dialogue, en fonction du contrôle de sécurité que vous configurez. Dans la plupart des cas, vous configurez une exception

(ou une relaxation) au contrôle de sécurité. Si vous configurez la vérification de l'URL refusée ou la vérification des formats de champs, vous configurez un ajout (ou une règle). Le processus pour l'un ou l'autre est le même.

Pour configurer une règle de relaxation à l'aide de l'interface graphique NetScaler

1. **Accédez à**Sécurité**>**NetScaler Web App Firewall > Profils**.**
2. Dans le volet **Profils**, sélectionnez le profil que vous souhaitez configurer, puis cliquez sur **Modifier**.
3. Sur la page **Configurer le profil du Web App Firewall**, cliquez sur **Règle de relaxationdans la section Paramètres avancés**. La section**Règles de relaxation** contient la liste complète des règles de relaxation du Web App Firewall.
4. Cliquez sur la règle de sécurité que vous souhaitez configurer, puis cliquez sur **Modifier**.
5. La page Règles de relaxation des URL contient une liste d'actions que vous pouvez configurer pour cette règle ainsi qu'une liste d'assouplissements ou de règles existants. La liste est peut-être vide si vous n'avez pas ajouté manuellement de relaxations ni approuvé de relaxations recommandées par le moteur d'apprentissage. Sous la liste se trouve une rangée de boutons qui vous permettent d'ajouter, de modifier, de supprimer, d'activer ou de désactiver les relaxations de la liste.
6. Pour ajouter ou modifier un assouplissement ou une règle, effectuez l'une des opérations suivantes :

   - Pour ajouter une nouvelle relaxation, cliquez sur **Ajouter**.
   - Pour modifier une relaxation existante, sélectionnez la relaxation que vous souhaitez modifier, puis cliquez sur **Ouvrir**.

   La page **Start URL Relaxation Rule** s'affiche. À l'exception du titre, ces boîtes de dialogue sont identiques.
7. Remplissez la boîte de dialogue comme décrit ci-dessous. Les boîtes de dialogue de chaque vérification sont différentes. La liste ci-dessous couvre tous les éléments qui peuvent apparaître dans n'importe quelle boîte de dialogue.

   - Case à**cocher activée : cochez**cette case pour activer cette relaxation ou cette règle ; désactivez-la pour la désactiver.
   - **Type de contenu de pièce jointe** : attribut de type de contenu d'une pièce jointe XML. Dans la zone de texte, entrez une expression régulière qui correspond à l'attribut Content-Type des pièces jointes XML à autoriser.
   - **URL de l'action**—Dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL vers laquelle les données saisies dans le formulaire Web sont envoyées.

- **Cookie**—Dans la zone de texte, entrez une expression régulière au format PCRE qui définit le cookie.
- **Nom du champ** : un élément de nom de champ de formulaire Web peut être intitulé Nom du champ, Champ du formulaire ou un autre nom similaire. Dans la zone de texte, entrez une expression régulière au format PCRE qui définit le nom du champ de formulaire.
- **À partir de l'URL d'origine** : dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL qui héberge le formulaire Web.
- **À partir de l'URL de l'action** : dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL vers laquelle les données saisies dans le formulaire Web sont envoyées.
- **Nom**—Un nom d'élément ou d'attribut XML. Dans la zone de texte, entrez une expression régulière au format PCRE qui définit le nom de l'élément ou de l'attribut.
- **URL** : un élément d'URL peut être intitulé URL d'action, URL de refus, URL d'action du formulaire, URL d'origine du formulaire, URL de début ou simplement URL. Dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL.
- **Format** : la section Format contient plusieurs paramètres, notamment des zones de liste et des zones de texte. L'un des éléments suivants peut apparaître :
  - **Type**—Sélectionnez un type de champ dans la liste déroulante Type. Pour ajouter une nouvelle définition de type de champ, cliquez sur Gérer—
  - **Longueur minimale**—Entrez un entier positif qui représente la longueur minimale en caractères si vous souhaitez obliger les utilisateurs à remplir ce champ. Par défaut : 0 (permet de laisser le champ vide.)
  - **Longueur maximale**—Pour limiter la longueur des données dans ce champ, tapez un entier positif qui représente la longueur maximale en caractères. Par défaut : 65535
- **Lieu**—Choisissez l'élément de la demande auquel s'applique votre relaxation dans la liste déroulante. Pour les contrôles de sécurité HTML, les choix sont les suivants :
  - FormField : champs de formulaire dans des formulaires Web.
  - En-tête : en-têtes de demande.
  - Cookie : définissez les en-têtes des cookies.

  Pour les contrôles de sécurité XML, les choix sont les suivants :
  - ELEMENT : élément XML.
  - ATTRIBUT : attribut XML.
- **Taille maximale de la pièce jointe** : taille maximale en octets autorisée pour une pièce jointe XML.
- **Commentaires**—Dans la zone de texte, tapez un commentaire. Facultatif.

Remarque : Pour tout élément nécessitant une expression régulière, vous pouvez saisir l'expression régulière, utiliser le menu Regex Tokens pour insérer des éléments d'expression régulière et des symboles directement dans la zone de texte, ou cliquer sur **Regex Editor** pour ouvrir la boîte de dialogue **Ajouter une expression régulière** et l'utiliser pour créer l'expression.

8. Pour supprimer une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Supprimer**.
9. Pour activer une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Activer**.
10. Pour désactiver une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Désactiver**.
11. Pour configurer les paramètres et les relations de toutes les relaxations existantes dans un affichage graphique interactif intégré, cliquez sur **Visualizer**et utilisez les outils d'affichage.

    > **Remarque :**
    >
    > Le bouton **Visualiseur** n'apparaît pas dans toutes les boîtes de dialogue de relaxation de vérification.

12. Pour consulter les règles apprises pour cette vérification, cliquez sur Apprentissage et effectuez les étapes de la section Pour configurer et utiliser la fonctionnalité d'apprentissage.
13. Cliquez sur **OK**.

Pour configurer les règles apprises à l'aide de l'interface graphique NetScaler

1. **Accédez à**Sécurité**>**NetScaler Web App Firewall > Profils**.**
2. Dans le volet **Profils**, sélectionnez le profil, puis cliquez sur **Modifier**.
3. Sur la page de **profil du Web App Firewall NetScaler**, cliquez sur **Règles apprises à partir des** paramètres **avancés**. Dans la section **Règles apprises**, vous pouvez voir une liste des contrôles de sécurité disponibles dans le profil actuel et compatibles avec la fonctionnalité d'apprentissage.
4. Pour configurer les seuils d'apprentissage, sélectionnez un contrôle de sécurité, puis cliquez sur **Paramètres**.
5. Dans la page **Paramètres des règles de profilage dynamique et d'apprentissage**, vous pouvez définir les paramètres. Pour plus d'informations, voir Paramètres de profil dynamique.

    - **Seuil de nombre minimum.** Selon les paramètres d'apprentissage du contrôle de sécurité que vous configurez, le seuil minimal peut faire référence au nombre minimum de sessions utilisateur totales qui doivent être observées, au nombre minimum de demandes à respecter ou au nombre minimum de fois qu'un champ de formulaire spécifique doit être observé, avant qu'une relaxation apprise ne soit générée. Par défaut : 1

- **Pourcentage de fois le seuil.** Selon les paramètres d'apprentissage du contrôle de sécurité que vous configurez, le seuil de pourcentage de fois peut faire référence au pourcentage du nombre total de sessions utilisateur observées qui ont enfreint le contrôle de sécurité, au pourcentage de demandes ou au pourcentage de fois qu'un champ de formulaire correspondait à un type de champ particulier, avant un une relaxation apprise est générée. Par défaut : 0

6. Pour supprimer toutes les données apprises et réinitialiser la fonction d'apprentissage afin qu'elle doive recommencer ses observations depuis le début, sélectionnez l'action **Supprimer toutes les données apprises** .

   > **Remarque :**
   >
   > Ce bouton supprime uniquement les recommandations apprises qui n'ont pas été examinées, approuvées ou ignorées. Il ne supprime pas les relaxations apprises qui ont été acceptées et déployées.

7. Pour limiter le moteur d'apprentissage au trafic provenant d'un ensemble spécifique d'adresses IP, cliquez sur **Trusted Learning Clients**, puis ajoutez les adresses IP que vous souhaitez utiliser à la liste.

   a) Pour ajouter une adresse IP ou une plage d'adresses IP à la liste Trusted Learning Clients, cliquez sur **Ajouter**.
   b) **Sur la page Associant le**profil AppFirewall à Trusted Clint**, cliquez sur Ajouter.**
   c) Cochez la case **Activé** pour activer la fonctionnalité.
   d) Dans la zone Trusted Learning Client,** tapez l'adresse IP ou une plage d'adresses IP au format CIDR.
   e) Dans la zone de texte **Commentaires**, tapez un commentaire qui décrit cette adresse IP ou cette plage.
   f) Cliquez sur **Créer** et **Fermer**.

8. Pour modifier une adresse IP ou une plage existante, cliquez sur l'adresse IP ou la plage, puis cliquez sur **Modifier**. À l'exception du nom, la boîte de dialogue qui s'affiche est identique à la boîte de dialogue Ajouter des clients de formation approuvés .

9. Pour désactiver ou activer une adresse IP ou une plage, tout en la laissant dans la liste, cliquez sur l'adresse IP ou la plage, puis sur **Désactiver** ou **Activer**, selon le cas.

10. Pour supprimer complètement une adresse IP ou une plage, cliquez sur l'adresse IP ou la plage, puis sur **Supprimer**.

11. Cliquez sur **Fermer** pour revenir à la page de **profil de NetScaler Web App Firewall** .

Pour créer une politique de pare-feu NetScaler Web App à l'aide de l'interface graphique de NetScaler

1. **Accédez à**Sécurité**>**NetScaler Web App Firewall > Politiques**.**
2. Sur la page **Politiques**, cliquez sur le lien **Stratégie de pare-feu NetScaler Web App** .
3. **Sur la page Politiques de NetScaler Web App Firewall, cliquez sur Ajouter.**
4. Sur la page Créer une politique de pare-feu NetScaler Web App, définissez les paramètres suivants.
   a) Nom. Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement et peut comprendre de 1 à 128 lettres, chiffres et le tiret (-), le point (.), la livre (#), l'espace (), l'arobase (@), l'égal (=), les deux points (:) et le trait de soulignement (_).
   b) Profil. Sélectionnez le profil que vous souhaitez associer à cette politique dans la liste déroulante Profil. Vous pouvez créer un profil à associer à votre politique en cliquant sur Nouveau, et vous pouvez modifier un profil existant en cliquant sur **Modifier**.
   c) Expression : Dans la zone de texte Expression, créez une règle pour votre politique.
   d) Action de journalisation. Ajoutez une action de journal ou vous pouvez modifier une action de journal existante.
   e) Commentaires. Brève description de la politique.
5. Cliquez sur **Créer** ou **sur OK**, puis sur **Fermer**.



Pour créer ou configurer une règle de Web App Firewall (expression)

La règle de politique, également appelée *expression*, définit le trafic Web que le Web App Firewall filtre à l'aide du profil associé à la politique. Comme les autres règles (ou *expressions*) de politique

NetScaler, les règles du Web App Firewall utilisent la syntaxe des expressions NetScaler. Cette syntaxe est puissante, flexible et extensible. C'est trop complexe pour être décrit complètement dans cet ensemble d'instructions. Vous pouvez utiliser la procédure suivante pour créer une règle de politique de pare-feu simple, ou vous pouvez la lire comme une vue d'ensemble du processus de création de la politique.

1. Si ce n'est pas déjà fait, accédez à l'emplacement approprié dans l'assistant Web App Firewall ou dans l'interface graphique de NetScaler pour créer votre règle de politique :

   - Si vous configurez une politique dans l'assistant Web App Firewall, dans le volet de navigation, cliquez sur **NetScaler Web App Firewall Wizard**, puis dans le volet de détails, cliquez sur **NetScaler Web App Firewall Wizard**, puis accédez à l'onglet **Spécifier** une règle.
   - Sur la page **Spécifier une règle**, choisissez le préfixe de votre expression dans la liste déroulante. Vos choix sont les suivants :
   - **HTTP.** Le protocole HTTP. Choisissez cette option si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP.
   - **SYS.** Un ou plusieurs sites Web protégés. Sélectionnez cette option si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
   - **CLIENT.** L'ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.
   - **SERVEUR.** L'ordinateur auquel la demande a été envoyée. Choisissez cette option si vous souhaitez examiner certains aspects du destinataire de la demande.

   Une fois que vous avez choisi un préfixe, le Web App Firewall affiche une fenêtre d'invite en deux parties qui affiche les choix suivants possibles en haut et une brève explication de la signification du choix sélectionné en bas.

2. Choisissez votre prochain mandat.

   Si vous avez choisi HTTP comme préfixe, votre seul choix est REQ, qui spécifie la paire Requête/Réponse. (Le Web App Firewall fonctionne sur la demande et la réponse comme une unité plutôt que séparément.) Si vous choisissez un autre préfixe, vos choix sont plus variés. Pour obtenir de l'aide sur un choix spécifique, cliquez une fois sur ce choix pour afficher les informations le concernant dans la fenêtre contextuelle inférieure.

   Lorsque vous avez choisi le terme que vous souhaitez utiliser, double-cliquez dessus pour l'insérer dans la fenêtre Expression.

3. Tapez un point après le terme que vous venez de choisir. Vous êtes ensuite invité à choisir votre prochain terme, comme décrit à l'étape précédente. Lorsqu'un terme nécessite que vous saisissiez une valeur, renseignez la valeur appropriée. Par exemple, si vous choisissez HTTP.REQ.HEADER (« »), saisissez le nom de l'en-tête entre guillemets.

4. Continuez à choisir des termes à partir des instructions et à saisir les valeurs nécessaires jusqu'à ce que votre expression soit terminée.

   Vous trouverez ci-dessous quelques exemples d'expressions destinées à des fins spécifiques.

   - **Hébergeur Web spécifique.** Pour faire correspondre le trafic provenant d'un hébergeur en particulier :

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Pour shopping.example.com, remplacez le nom de l'hébergeur auquel vous souhaitez faire correspondre le nom.

- **Dossier ou répertoire Web spécifique.** Pour faire correspondre le trafic provenant d'un dossier ou d'un répertoire spécifique sur un hôte Web, procédez comme suit :

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
```

Pour www.example.com, remplacez le nom de l'hébergeur Web. Par dossier, remplacez le dossier ou le chemin d'accès au contenu auquel vous souhaitez faire correspondre. Par exemple, si votre panier se trouve dans un dossier nommé /solutions/orders, vous remplacez cette chaîne par dossier.

- **Type de contenu spécifique : images GIF.** Pour faire correspondre des images au format GIF :

```
HTTP.REQ.URL.ENDSWITH(".png")
```

Pour faire correspondre des images d'un autre format, remplacez .png par une autre chaîne.

- **Type de contenu spécifique : scripts.** Pour faire correspondre tous les scripts CGI situés dans le répertoire CGI-BIN :

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
```

Pour faire correspondre tous les Javascripts avec les extensions .js :

```
HTTP.REQ.URL.ENDSWITH(".js")
```

Pour plus d'informations sur la création d'expressions de stratégie, voir Stratégies et expressions.

> **Remarque :**
>
> Si vous utilisez la ligne de commande pour configurer une politique, pensez à éviter les guillemets doubles dans les expressions NetScaler. Par exemple, l'expression suivante est correcte si elle est saisie dans l'interface graphique :

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Toutefois, si vous le saisissez sur la ligne de commande, vous devez plutôt taper ceci :

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

```
1 ![Policy expression configuration](/en-us/citrix-adc/media/waf-rule.png
     )
```


Pour ajouter une règle de pare-feu (expression) à l'aide de la boîte de dialogue Ajouter une expression

La boîte de dialogue **Ajouter une expression** (également appelée éditeur d'expressions) aide les utilisateurs qui ne sont pas familiarisés avec le langage d'expressions NetScaler à élaborer une politique correspondant au trafic qu'ils souhaitent filtrer.

1. Si ce n'est pas déjà fait, accédez à l'emplacement approprié dans l'assistant Web App Firewall ou dans l'interface graphique de NetScaler :
   - Si vous configurez une politique dans l'assistant **Web App Firewall**, dans le volet de navigation, cliquez sur **Web App Firewall**, puis dans le volet de détails, cliquez sur Assistant **Web App Firewall**, puis accédez à l'écran **Spécifier la règle** .
   - Si vous configurez une politique manuellement, dans le volet de navigation, développez **Web App Firewall**, puis **Politiques**, puis **Firewall**. Dans le volet d'informations, pour créer une politique, cliquez sur **Ajouter**. Pour modifier une politique existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
2. Sur l'écran **Spécifier une règle**, dans la boîte de dialogue **Créer un profil de Web App Firewall** ou dans la boîte de dialogue de **configuration du profil de Web App Firewall**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une expression**, dans la zone Construire une expression, dans la première zone de liste, choisissez l'un des préfixes suivants :
   - **HTTP.** Le protocole HTTP. Choisissez cette option si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP. Le choix par défaut.
   - **SYS.** Un ou plusieurs sites Web protégés. Sélectionnez cette option si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
   - **CLIENT.** L'ordinateur qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.
   - **SERVEUR.** L'ordinateur auquel la demande a été envoyée. Choisissez cette option si vous souhaitez examiner certains aspects du destinataire de la demande.
4. Dans la deuxième zone de liste, choisissez votre prochain terme. Les termes disponibles varient en fonction du choix que vous avez fait à l'étape précédente, car la boîte de dialogue ajuste automatiquement la liste pour ne contenir que les termes qui sont valides pour le contexte. Par exemple, si vous avez sélectionné HTTP dans la zone de liste précédente, le seul choix est REQ, pour les requêtes. Étant donné que le Web App Firewall traite les demandes et les réponses associées comme une seule unité et filtre les deux, vous n'avez pas besoin de réponses spécifiques séparément. Une fois que vous avez choisi votre deuxième terme, une troisième zone de liste apparaît à droite du second. La fenêtre d'aide affiche la description du deuxième terme et la fenêtre Aperçu de l'expression affiche votre expression.
5. Dans la troisième zone de liste, choisissez le terme suivant. Une nouvelle zone de liste apparaît sur la droite et la fenêtre d'aide change pour afficher la description du nouveau terme. La fenêtre Aperçu de l'expression se met à jour pour afficher l'expression telle que vous l'avez spécifiée

jusqu'à présent.

6. Continuez à choisir des termes et, lorsque vous y êtes invité, à saisir des arguments, jusqu'à ce que votre expression soit complète. Si vous faites une erreur ou souhaitez modifier votre expression alors que vous avez déjà sélectionné un terme, vous pouvez simplement en choisir un autre. L'expression est modifiée et tous les arguments ou autres termes que vous avez ajoutés après le terme que vous avez modifié sont effacés.
7. Lorsque vous avez fini de créer votre expression, cliquez sur OK pour fermer la boîte de dialogue Ajouter une expression. Votre expression est insérée dans la zone de texte Expression.

Pour lier une politique de Web App Firewall à l'aide de l'interface graphique NetScaler

1. Procédez comme suit :
   - Accédez à **Sécurité** > **Web App Firewall**, puis dans le volet de détails, cliquez sur le **gestionnaire de politiques de pare-feu d'applications**.
   - **Accédez à**Sécurité**>**NetScaler Web App Firewall > **Politiques** > **Pare-feu, puis dans le volet « Politiques de NetScaler Web App Firewall », cliquez sur Policy Manager.**
2. Dans la boîte de dialogue **Application Firewall Policy Manager**, choisissez le point de liaison auquel vous souhaitez lier la politique dans la liste déroulante. Les choix sont les suivants :
   - **Remplacez Global.** Les politiques liées à ce point de liaison traitent l'ensemble du trafic provenant de toutes les interfaces de l'appliance NetScaler et sont appliquées avant toute autre politique.
   - **Serveur virtuel LB.** Les politiques liées à un serveur virtuel d'équilibrage de charge sont appliquées uniquement au trafic traité par ce serveur virtuel d'équilibrage de charge et sont appliquées avant toute politique globale par défaut. Après avoir sélectionné le serveur virtuel LB, vous devez également sélectionner le serveur virtuel d'équilibrage de charge spécifique auquel vous souhaitez lier cette politique.
   - **Serveur virtuel CS.** Les politiques liées à un serveur virtuel de commutation de contenu sont appliquées uniquement au trafic traité par ce serveur virtuel de commutation de contenu et sont appliquées avant toute politique globale par défaut. Après avoir sélectionné CS Virtual Server, vous devez également sélectionner le serveur virtuel de commutation de contenu spécifique auquel vous souhaitez lier cette politique.
   - **Global par défaut.** Les politiques liées à ce point de liaison traitent l'ensemble du trafic provenant de toutes les interfaces de l'appliance NetScaler.
   - **Libellé de politique.** Les politiques liées à une étiquette de stratégie traitent le trafic que l'étiquette de stratégie leur achemine. L'étiquette de politique contrôle l'ordre dans lequel les politiques sont appliquées à ce trafic.
   - **None.** Ne liez la politique à aucun point de liaison.
3. Cliquez sur **Continuer**. La liste des politiques de Web App Firewall existantes s'affiche.
4. Sélectionnez la politique que vous souhaitez lier en cliquant dessus.
5. Apportez tous les ajustements supplémentaires à la reliure.

- Pour modifier la priorité de la stratégie, cliquez sur le champ pour l'activer, puis tapez une nouvelle priorité. Vous pouvez également sélectionner **Régénérer les priorités** pour renuméroter les priorités de manière uniforme.
- Pour modifier l'expression de politique, double-cliquez sur ce champ pour ouvrir la boîte de dialogue **Configurer la politique de Web App Firewall**, dans laquelle vous pouvez modifier l'expression de stratégie.
- Pour définir l'expression Goto, double-cliquez sur le champ dans l'en-tête de la colonne **Goto Expression** pour afficher la liste déroulante dans laquelle vous pouvez choisir une expression.
- Pour définir l'option Invoquer, double-cliquez sur le champ dans l'en-tête de la colonne Invoquer pour afficher la liste déroulante dans laquelle vous pouvez choisir une expression.

6. Répétez les étapes 3 à 6 pour ajouter les politiques de Web App Firewall supplémentaires que vous souhaitez lier globalement.
7. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été liée avec succès.

Configuration manuelle à l'aide de l'interface de ligne de commande

May 5, 2023

> **Remarque :**
>
> Si vous devez configurer manuellement la fonctionnalité Web App Firewall, Citrix vous recommande d'utiliser la procédure de l'interface graphique NetScaler.

Vous pouvez configurer les fonctionnalités du Web App Firewall à partir de l'interface de commande **NetScaler.** Il existe toutefois d'importantes exceptions. Vous ne pouvez pas activer les signatures depuis l'interface de commande. Il existe environ 1 000 signatures par défaut réparties en sept catégories et la tâche est trop complexe pour l'interface de commande. Vous pouvez activer ou désactiver des fonctionnalités et configurer des paramètres à partir de la ligne de commande, mais vous ne pouvez pas configurer des relaxations manuelles. Bien que vous puissiez configurer la fonctionnalité d'apprentissage adaptatif et activer l'apprentissage à partir de la ligne de commande, vous ne pouvez pas consulter les relaxations apprises ou les règles apprises et les approuver ou les ignorer. L'interface de ligne de commande est destinée aux utilisateurs avancés qui sont familiarisés avec l'appliance NetScaler et le Web App Firewall.

Pour configurer manuellement le Web App Firewall à l'aide de la ligne de commande NetScaler, utilisez un client telnet ou Secure Shell de votre choix pour vous connecter à la ligne de commande NetScaler.

Pour créer un profil à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw profile <name> [-defaults ( basic | advanced )]`
- `set appfw profile <name> -type ( HTML | XML | HTML XML )`
- `save ns config`

Exemple

L'exemple suivant ajoute un profil nommé pr-basic, avec des valeurs par défaut de base, et affecte un type de profil HTML. Il s'agit de la configuration initiale appropriée pour un profil afin de protéger un site Web HTML.

```
1 add appfw profile pr-basic -defaults basic
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```

Pour configurer un profil à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> <arg1> [<arg2> ...]` où `<arg1>` représente un paramètre et `<arg2>` représente un autre paramètre ou la valeur à affecter au paramètre représenté par `<arg1>`. Pour obtenir des descriptions des paramètres à utiliser lors de la configuration de contrôles de sécurité spécifiques, consultez Protections avancées et ses sous-rubriques. Pour obtenir une description des autres paramètres, reportez-vous à la section « Paramètres pour la création d'un profil ».
- `save ns config`

Exemple

L'exemple suivant montre comment configurer un profil HTML créé avec des valeurs par défaut de base pour commencer à protéger un site Web HTML simple. Cet exemple active la journalisation et la gestion des statistiques pour la plupart des contrôles de sécurité, mais active le blocage uniquement pour les contrôles présentant un faible taux de faux positifs et ne nécessitant aucune configuration particulière. Il active également la transformation du code HTML non sécurisé et du code SQL non sécurisé, ce qui empêche les attaques mais ne bloque pas les requêtes adressées à vos sites Web. Lorsque la journalisation et les statistiques sont activées, vous pouvez consulter ultérieurement les journaux pour déterminer s'il convient d'activer le blocage pour un contrôle de sécurité spécifique.


```
set appfw profile -startURLAction log stats
set appfw profile -denyURLAction block log stats
set appfw profile -cookieConsistencyAction log stats
set appfw profile -crossSiteScriptingAction log stats
set appfw profile -crossSiteScriptingTransformUnsafeHTML ON
set appfw profile -fieldConsistencyAction log stats
set appfw profile -SQLInjectionAction log stats
set appfw profile -SQLInjectionTransformSpecialChars ON
set appfw profile -SQLInjectionOnlyCheckFieldsWithSQLChars ON
set appfw profile -SQLInjectionParseComments checkall
set appfw profile -fieldFormatAction log stats
set appfw profile -bufferOverflowAction block log stats
set appfw profile -CSRFtagAction log stats
save ns config
<!--NeedCopy-->
```

Pour créer et configurer une politique

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw policy <name> <rule> <profile>`
- `save ns config`

Exemple

L'exemple suivant ajoute une politique nommée pl-blog, avec une règle qui intercepte tout le trafic à destination ou en provenance de l'hôte blog.example.com, et associe cette politique au profil pr-blog.

```
add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com
    ")" pr-blog
<!--NeedCopy-->
```

Pour lier une politique de Web App Firewall

À l'invite de commandes, tapez les commandes suivantes :

- `bind appfw global <policyName> <priority>`
- `save ns config`

Exemple

L'exemple suivant lie la politique nommée pl-blog et lui attribue une priorité de 10.


```
bind appfw global pl-blog 10
save ns config
<!--NeedCopy-->
```

Pour configurer la limite de session par PE

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw settings <session limit>`

Exemple

L'exemple suivant configure la limite de session par PE.

```
> set appfw settings -sessionLimit 500000`

Done

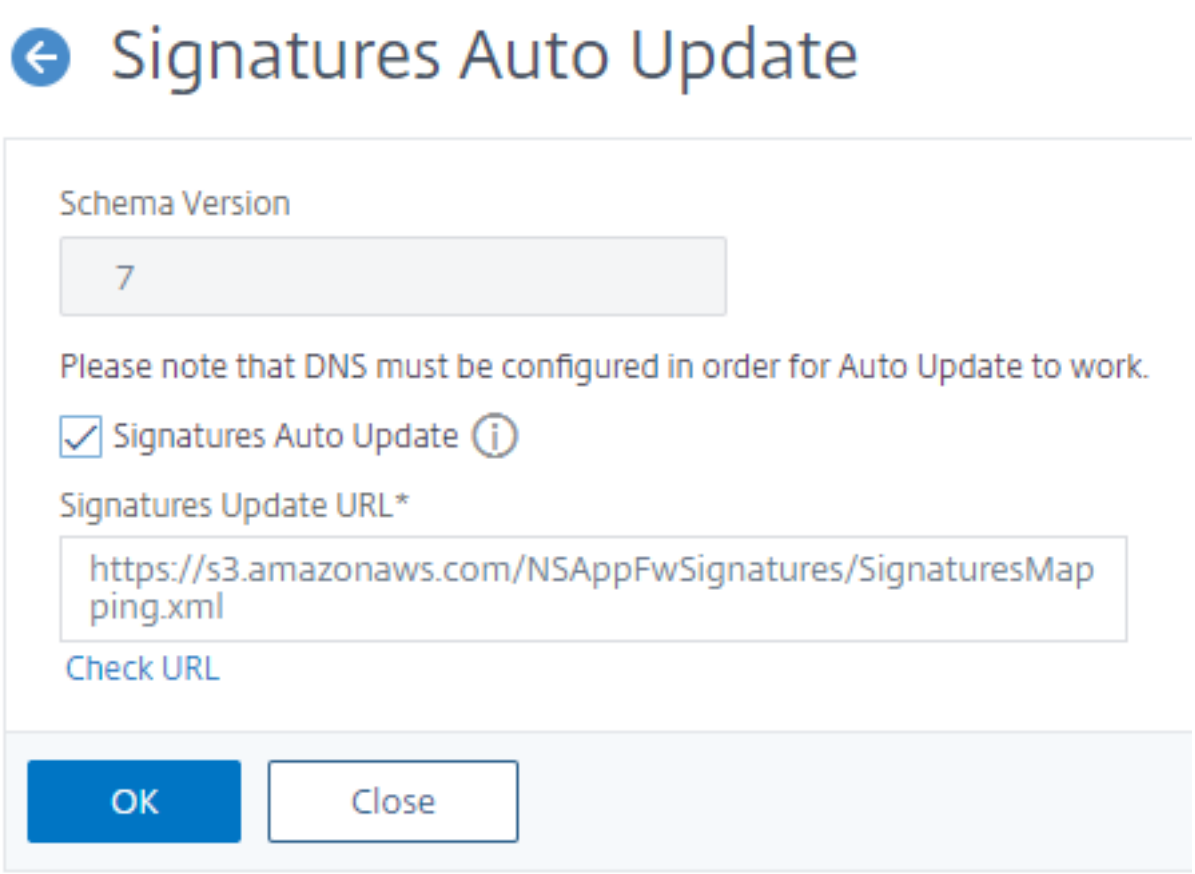
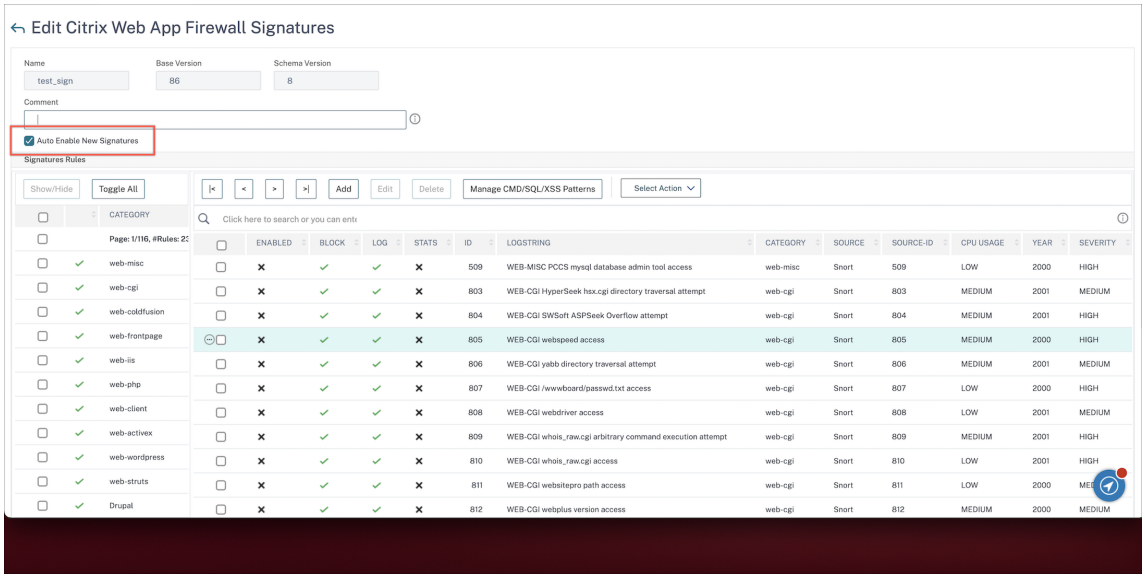
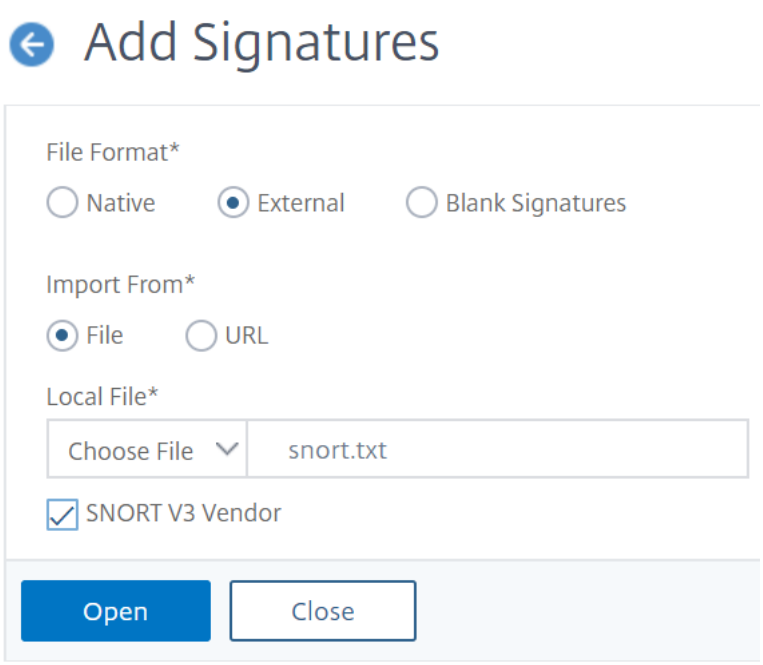
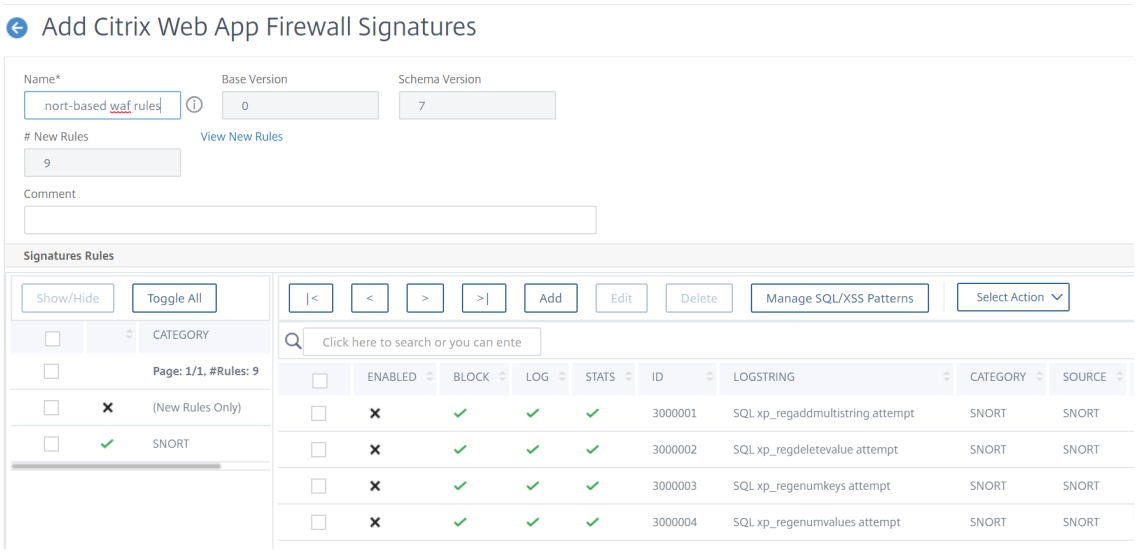
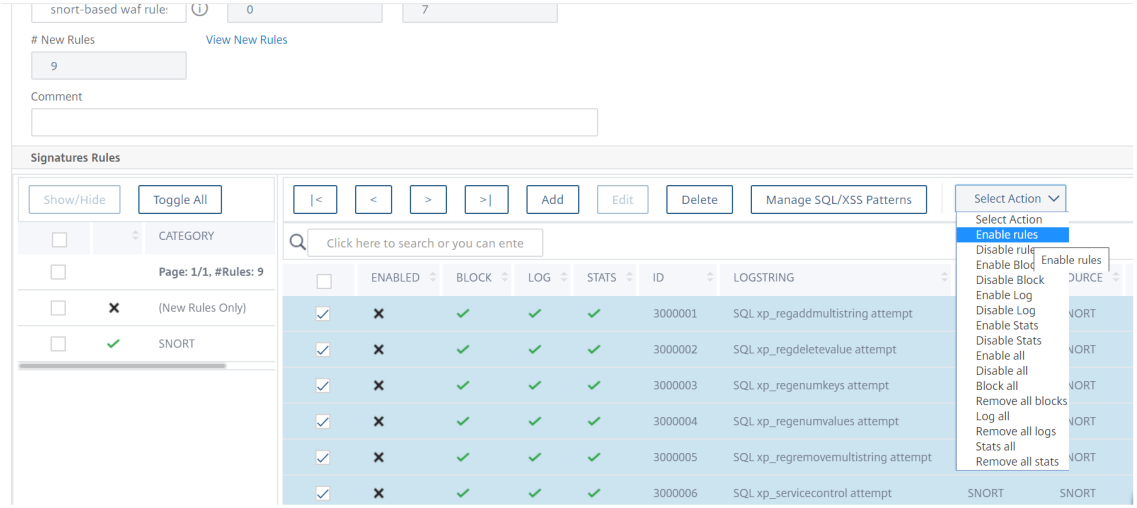
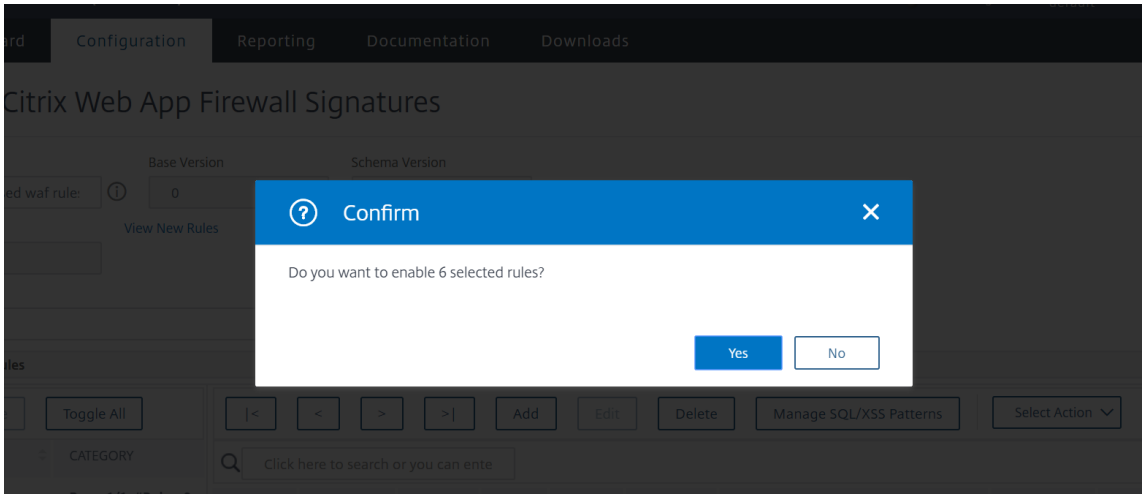
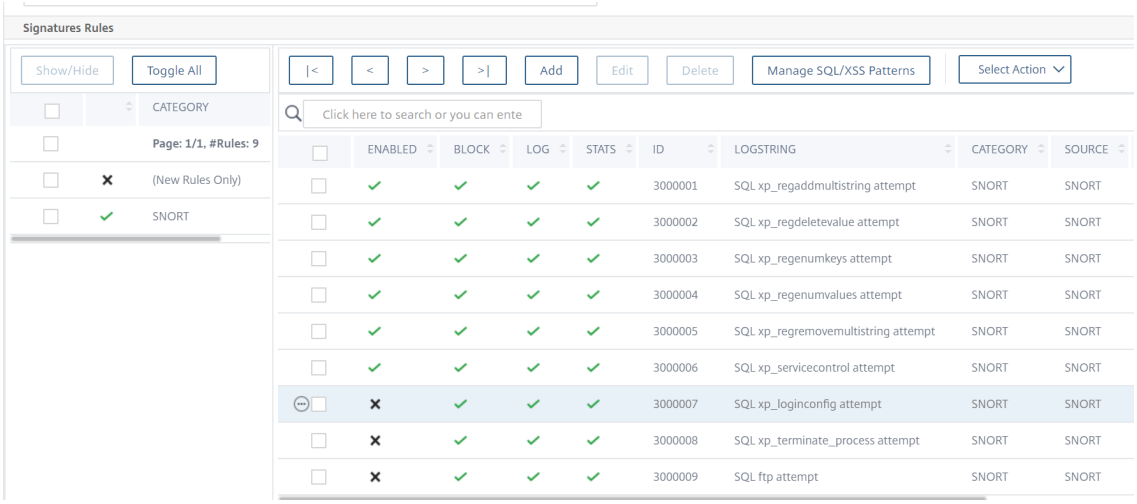
Default value:100000   Max value:500000 per PE
<!--NeedCopy-->
```

Signatures

May 5, 2023

Les signatures du Web App Firewall fournissent des règles spécifiques configurables pour simplifier la tâche de protection de vos sites Web contre les attaques connues. Une signature représente un modèle qui est un composant d'une attaque connue contre un système d'exploitation, un serveur Web, un site Web, un service Web XML ou une autre ressource. Un ensemble complet de règles préconfigurées intégrées ou natives du Web App Firewall constitue une solution de sécurité facile à utiliser qui utilise la puissance de la mise en correspondance des modèles pour détecter les attaques et protéger les applications contre les vulnérabilités.

Vous pouvez créer vos propres signatures ou utiliser des signatures dans les modèles intégrés. Le Web App Firewall possède deux modèles intégrés :

- **Signatures par défaut** : ce modèle contient une liste préconfigurée de plus de 1 300 signatures, en plus d'une liste complète de mots-clés d'injection SQL, de chaînes spéciales SQL, de règles de transformation SQL et de caractères génériques SQL. Il contient également des modèles refusés pour les scripts intersites, ainsi que des attributs et des balises autorisés pour les scripts

intersites. Il s'agit d'un modèle en lecture seule. Vous pouvez consulter le contenu, mais vous ne pouvez rien ajouter, modifier ou supprimer dans ce modèle. Pour l'utiliser, vous devez en faire une copie. Dans votre propre copie, vous pouvez activer les règles de signature que vous souhaitez appliquer à votre trafic et spécifier les actions à entreprendre lorsque les règles de signature correspondent au trafic.

Les signatures du Web App Firewall sont dérivées des règles publiées par Snort, un système open source de prévention des intrusions capable d'effectuer une analyse du trafic en temps réel pour détecter diverses attaques et sondes.

- ***Modèles d'injection Xpath** : ce modèle contient un ensemble préconfiguré de mots-clés littéraux et PCRE ainsi que des chaînes spéciales utilisées pour détecter les attaques par injection XPath (XML Path Language).

Signatures vierges : Outre la copie du modèle *Default Signatures intégré, vous pouvez utiliser un modèle de signatures vierge pour créer un objet de signature. L'objet de signature que vous créez à l'aide de l'option de signatures vierges ne possède aucune règle de signature native, mais, tout comme le modèle *Default, il possède toutes les entités intégrées de script SQL/intersite.

Signatures au format externe : le Web App Firewall prend également en charge les signatures au format externe. Vous pouvez importer le rapport d'analyse tiers à l'aide des fichiers XSLT pris en charge par NetScaler Web App Firewall. Un ensemble de fichiers XSLT intégrés est disponible pour les outils de numérisation suivants afin de traduire des fichiers au format externe au format natif :

- Cenzic
- Sécurité approfondie pour les applications Web
- IBM AppScan Enterprise
- Norme IBM AppScan.
- Qualys
- Qualys Cloud
- Chapeau blanc
- Hewlett Packard Enterprise WebInspect
- Rapid7 AppSpider
- Acunétix

Protection de sécurité pour votre application

Le renforcement de la sécurité augmente les frais de traitement. Les signatures fournissent les options de déploiement suivantes pour vous aider à optimiser la protection de vos applications :

- **Modèle de sécurité négatif : avec le modèle**de sécurité négatif, vous utilisez un ensemble complet de règles de signature préconfigurées pour appliquer la puissance de la mise en correspondance des modèles afin de détecter les attaques et de vous protéger contre les vulnérabilités des applications. Vous ne bloquez que ce que vous ne voulez pas et vous autorisez le reste.

Vous pouvez ajouter vos propres règles de signature, en fonction des besoins de sécurité spécifiques de vos applications, afin de concevoir vos propres solutions de sécurité personnalisées.

- **Modèle de sécurité hybride** : Outre l'utilisation de signatures, vous pouvez utiliser des contrôles de sécurité positifs pour créer une configuration parfaitement adaptée à vos applications. Utilisez des signatures pour bloquer ce que vous ne voulez pas et utilisez des contrôles de sécurité positifs pour faire respecter ce qui est autorisé.

Pour protéger votre application à l'aide de signatures, vous devez configurer un ou plusieurs profils pour utiliser votre objet de signatures. Dans une configuration de sécurité hybride, les modèles d'injection SQL et de script intersite, ainsi que les règles de transformation SQL, de votre objet de signatures sont utilisés non seulement par les règles de signature, mais également par les contrôles de sécurité positifs configurés dans le profil Web App Firewall qui utilise l'objet de signatures.

Le Web App Firewall examine le trafic vers vos sites Web et services Web protégés afin de détecter le trafic correspondant à une signature. Une correspondance n'est déclenchée que lorsque chaque motif de la règle correspond au trafic. Lorsqu'une correspondance se produit, les actions spécifiées pour la règle sont appelées. Vous pouvez afficher une page d'erreur ou un objet d'erreur lorsqu'une demande est bloquée. Les messages de journal peuvent vous aider à identifier les attaques lancées contre votre application. Si vous activez les statistiques, le Web App Firewall conserve les données relatives aux demandes qui correspondent à une signature ou à un contrôle de sécurité du Web App Firewall.

Si le trafic correspond à la fois à une signature et à un contrôle de sécurité positif, la plus restrictive des deux actions est appliquée. Par exemple, si une demande correspond à une règle de signature pour laquelle l'action de blocage est désactivée, mais que la demande correspond également à une vérification de sécurité positive SQL Injection pour laquelle l'action est bloquée, la demande est bloquée. Dans ce cas, la violation de signature peut être enregistrée sous forme `<not blocked>`, bien que la demande soit bloquée par le contrôle de l'injection SQL.

Personnalisation : si nécessaire, vous pouvez ajouter vos propres règles à un objet de signatures. Vous pouvez également personnaliser les modèles de script SQL/cross-site. La possibilité d'ajouter vos propres règles de signature, en fonction des besoins de sécurité spécifiques de vos applications, vous donne la possibilité de concevoir vos propres solutions de sécurité personnalisées. Vous ne bloquez que ce que vous ne voulez pas et vous autorisez le reste. Un modèle de correspondance rapide spécifique dans un emplacement spécifié peut réduire considérablement la surcharge de traitement afin d'optimiser les performances. Vous pouvez ajouter, modifier ou supprimer des modèles d'injection SQL et de script intersite. Les éditeurs RegEx et d'expressions intégrés vous aident à configurer vos modèles et à vérifier leur précision.

Mise à jour automatique : vous pouvez mettre à jour manuellement l'objet de signature pour obtenir les dernières règles de signature, ou vous pouvez appliquer la fonctionnalité de mise à jour automatique afin que le Web App Firewall puisse automatiquement mettre à jour les signatures à partir du service de mise à jour du Web App Firewall basé sur le cloud.

> **Remarque :**
>
> Si de nouvelles règles de signature sont ajoutées lors de la mise à jour automatique, elles sont désactivées par défaut. Vous devez vérifier régulièrement les signatures mises à jour et activer les règles récemment ajoutées qui sont pertinentes pour protéger vos applications.
>
> Vous devez configurer CORS pour héberger les signatures sur les serveurs IIS.
>
> La fonctionnalité de mise à jour automatique des signatures ne fonctionne pas sur le serveur Web local lorsque vous accédez à l'URL depuis l'interface graphique de NetScaler.

Mise en route

L'utilisation des signatures Citrix pour protéger votre application est simple et peut être réalisée en quelques étapes simples :

1. Ajoutez un objet de signature.

- Vous pouvez utiliser l'assistant qui vous invite à créer l'intégralité de la configuration du Web App Firewall, notamment en ajoutant le profil et la politique, en sélectionnant et en activant les signatures, et en spécifiant des actions pour les signatures et les contrôles de sécurité positifs. L'objet de signatures est créé automatiquement.
- Vous pouvez créer une copie de l'objet de signatures à partir du modèle *Signatures par défaut, utiliser un modèle vierge pour créer une signature avec vos propres règles personnalisées ou ajouter une signature au format externe. Activez les règles et configurez les actions que vous souhaitez appliquer.

1. Configurez le profil Web App Firewall cible pour utiliser cet objet de signatures.
2. Envoyez du trafic pour valider la fonctionnalité

Résumé

- L'objet de signatures par défaut est un modèle. Il ne peut être ni modifié ni supprimé. Pour l'utiliser, vous devez en créer une copie. Dans votre propre copie, vous pouvez activer les règles et l'action souhaitée pour chaque règle selon les besoins de votre application. Pour protéger l'application, vous devez configurer le profil cible afin qu'il utilise cette signature.
- Le traitement des modèles de signature entraîne des frais supplémentaires. Essayez d'activer uniquement les signatures applicables à la protection de votre application, plutôt que d'activer toutes les règles de signature.
- Chaque modèle de la règle doit correspondre pour déclencher une correspondance de signature.
- Vous pouvez ajouter vos propres règles personnalisées pour inspecter les demandes entrantes afin de détecter différents types d'attaques, tels que les attaques par injection SQL ou par script

intersite. Vous pouvez également ajouter des règles pour inspecter les réponses afin de détecter et de bloquer les fuites d'informations sensibles telles que les numéros de cartes de crédit.
- Vous pouvez copier un objet de signature existant et le modifier en ajoutant ou en modifiant des règles et des modèles de script SQL/intersites, afin de protéger une autre application.
- Vous pouvez utiliser la mise à jour automatique pour télécharger la dernière version des règles par défaut du Web App Firewall sans avoir à effectuer une surveillance continue pour vérifier la disponibilité de la nouvelle mise à jour.
- Un objet de signature peut être utilisé par plusieurs profils. Même après avoir configuré un ou plusieurs profils pour utiliser un objet de signature, vous pouvez toujours activer ou désactiver les signatures ou modifier les paramètres d'action. Vous pouvez créer et modifier manuellement vos propres règles de signature personnalisées. Les modifications s'appliquent à tous les profils actuellement configurés pour utiliser cet objet de signature.
- Vous pouvez configurer des signatures pour détecter les violations dans différents types de charges utiles, telles que HTML, XML, JSON et GWT.
- Vous pouvez exporter un objet de signature configuré et l'importer vers une autre appliance NetScaler pour répliquer facilement vos règles de signature personnalisées.

Les signatures sont des modèles associés à une vulnérabilité connue. Vous pouvez utiliser la protection des signatures pour identifier le trafic qui tente d'exploiter ces vulnérabilités et prendre des mesures spécifiques.

Les signatures sont organisées en catégories. Vous pouvez optimiser les performances et réduire les frais de traitement en activant uniquement les règles dans les catégories appropriées à la protection de votre application.

Configuration manuelle de la fonction de signatures

August 20, 2021

Pour utiliser des signatures pour protéger vos sites Web, vous devez examiner les règles et activer et configurer celles que vous souhaitez appliquer. Les règles sont désactivées par défaut. Citrix vous recommande d'activer toutes les règles applicables au type de contenu utilisé par votre site Web.

Pour configurer manuellement la fonction de signatures, utilisez un navigateur pour vous connecter à l'interface graphique. Ensuite, créez un objet signatures à partir d'un modèle intégré, d'un objet signatures existant ou en important un fichier. Ensuite, configurez le nouvel objet signatures comme expliqué dans Configuration ou modification d'un objet Signatures.

Ajouter ou supprimer un objet de signature

May 5, 2023

Vous pouvez ajouter un nouvel objet de signature au Web App Firewall en :

- Copie d'un modèle intégré.
- Copie d'un objet de signatures existant.
- Importation d'un objet signatures à partir d'un fichier externe.

Le fichier de signature inclut l'utilisation de l'UC, la dernière année applicable et les détails du niveau de gravité. Vous pouvez consulter l'utilisation du processeur, l'année dernière et le niveau de gravité CVE chaque fois qu'un fichier de signature est modifié et téléchargé régulièrement. Après avoir observé ces valeurs, vous pouvez décider d'activer ou de désactiver la signature sur l'appliance.

Vous devez utiliser l'interface graphique pour copier un modèle ou un objet de signatures existant. Vous pouvez utiliser l'interface graphique ou la ligne de commande pour importer un objet signatures. Vous pouvez également utiliser l'interface graphique ou la ligne de commande pour supprimer un objet signatures.

Pour créer un objet signatures à partir d'un modèle

1. Accédez à **Sécurité > NetScaler Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures que vous souhaitez utiliser comme modèle.

   Vos choix sont les suivants :

   - **Signatures par défaut.** Contient les règles de signature, les règles d'injection SQL et les règles de script intersite.
   - **Injection XPath.** Contient les modèles d'injection XPath.
   - **Tout objet de signatures existant.**

   > **Attention :**
   >
   > Si vous ne choisissez pas de type de signature à utiliser comme modèle, le Web App Firewall vous invite à créer des signatures à partir de zéro.

3. Cliquez sur **Ajouter**.
4. Dans la boîte de dialogue Ajouter un objet Signatures, tapez un nom pour votre nouvel objet de signatures, puis cliquez sur OK. Le nom peut commencer par une lettre, un chiffre ou le symbole du trait de soulignement et peut être composé de 1 à 31 lettres, chiffres et tiret (-), point (.) livre (#), espace (), at (@), égal (=) et trait de soulignement (_).
5. Cliquez sur **Fermer**.

Pour créer un objet signatures en important un fichier

1. Accédez à **Sécurité > NetScaler Web App Firewall > Signatures**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un objet Signatures**, sélectionnez le format des signatures que vous souhaitez importer.
   - Pour importer un fichier de signatures au format NetScaler, sélectionnez l'onglet **Format natif** .
   - Pour importer un fichier de format de signature externe, sélectionnez l'onglet **Format externe** .
4. Choisissez le fichier que vous souhaitez utiliser pour créer votre objet signatures.
   - Pour importer un fichier de signatures au format NetScaler natif, dans la section Importer, sélectionnez Importer depuis un fichier local ou Importer depuis une URL, puis tapez ou accédez au chemin ou à l'URL du fichier.
   - Pour importer un fichier au format Cenzic, IBM AppScan, Qualys ou Whitehat, dans la section XSLT, sélectionnez Utiliser un fichier XSLT intégré, Utiliser un fichier local ou Référence à partir d'une URL. Ensuite, si vous avez choisi Utiliser le fichier XSLT intégré, sélectionnez le format de fichier approprié dans la liste. Si vous avez choisi Utiliser un fichier local ou une référence à partir d'une URL, saisissez ou recherchez le chemin d'accès ou l'URL du fichier.
5. Cliquez sur **Ajouter**, puis sur **Fermer**.

Pour créer un objet signatures en important un fichier à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `import appfw signatures <src> <name> [-xslt <string>] [-comment <string>] [-overwrite] [-merge] [-sha1 <string>]`
- `save ns config`

Exemple #1

L'exemple suivant crée un objet signatures à partir d'un fichier nommé signatures.xml et lui attribue le nom MySignatures.

```
import appfw signatures local:signatures.xml MySignatures
save ns config
<!--NeedCopy-->
```


Pour ajouter des signatures individuelles à l'aide de l'interface de ligne de commande

Vous pouvez sélectionner les signatures en fonction de leur identifiant ou de leur catégorie, puis définir des actions. À l'invite de commandes, exécutez la commande suivante :

```
import appfw signature <source> <name> [-sigRuleId| -sigCategory] [Rule
   -IDs | Category name] -Enabled [ON | OFF] [-Action LOG BLOCK]
<!--NeedCopy-->
```

- **Exemples d'utilisation des identifiants de signature**

  L'exemple suivant active les signatures en fonction de leurs identifiants de règle et définit les actions de journalisation et de blocage :

  ```
  import appfw signature DEFAULT object_name -sigRuleId 1001 9882
     2000 1250 810 -Enabled ON -Action LOG BLOCK
  <!--NeedCopy-->
  ```

  L'exemple suivant ajoute la signature à l'aide de son identifiant sans l'activer :

  ```
  import appfw signature DEFAULT object_name -sigRuleId 810 -
     Enabled OFF
  <!--NeedCopy-->
  ```

- **Exemples d'utilisation de la catégorie de signature**

  L'exemple suivant active les signatures par `web-misc` catégorie et définit les actions de journalisation et de blocage :

  ```
  import appfw signature DEFAULT object_name -sigCategory web-misc
     -Enabled ON -Action LOG BLOCK
  <!--NeedCopy-->
  ```

  L'exemple suivant ajoute les signatures par `web-misc` catégorie sans l'activer :

  ```
  import appfw signature DEFAULT object_name -sigCategory web-misc
     -Enabled OFF
  <!--NeedCopy-->
  ```

Pour supprimer un objet signatures à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez l'objet signatures que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.

Pour supprimer un objet signatures à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `rm appfw signatures <name>`
- `save ns config`

Configuration ou modification d'un objet de signatures

June 20, 2023

Vous configurez un objet de signatures après l'avoir créé, ou vous modifiez un objet de signatures existant pour activer ou désactiver des catégories de signatures ou des signatures spécifiques, et vous configurez la façon dont le Web App Firewall répond lorsqu'une signature correspond à une connexion.

Pour configurer ou modifier un objet de signatures

1. Accédez à **Sécurité > NetScaler Web App Firewall > Signatures**.
2. Dans le volet de détails, sélectionnez l'objet de signatures que vous souhaitez configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Modifier l'objet des signatures**, définissez les options **Afficher les critères de filtre** sur la gauche pour afficher les éléments de filtre que vous souhaitez configurer.

   Lorsque vous modifiez ces options, les résultats que vous avez demandés s'affichent dans la fenêtre Résultats filtrés sur la droite.

   - Pour afficher uniquement certaines catégories de signatures, cochez ou décochez les cases correspondant à la catégorie de signature appropriée. À partir de la version 13.1 build 48.x, vous pouvez utiliser CVE dans le panneau de gauche pour afficher les vulnérabilités publiées pour l'année sélectionnée.
     Les catégories de signatures sont les suivantes :

Nom	Type d'attaque contre lequel cette signature protège
cgi	Des scripts CGI. Inclut des scripts shell Perl et UNIX.
client	Navigateurs et autres clients.

Nom	Type d'attaque contre lequel cette signature protège
coldfusion	sites Web qui utilisent le serveur d'applications Adobe Systems ColdFusion.
frontpage	sites Web qui utilisent le serveur FrontPage de Microsoft.
iis	sites Web qui utilisent le serveur Microsoft Internet Information Server (IIS).
misc	Attaques diverses.
php	sites Web qui utilisent PHP
web-activex	sites Web contenant des contrôles ActiveX.
web-struts	sites Web contenant des applets Apache Struts, qui sont des applets basés sur Java-ee.
CVE	Répertorie les CVE publiés pour l'année sélectionnée.

- Pour afficher uniquement les signatures pour lesquelles des actions de vérification spécifiques sont activées, cochez la case ON pour chacune de ces actions, désactivez les cases ON pour les autres actions et désactivez toutes les cases à cocher OFF. Pour afficher uniquement les signatures dont une action de vérification spécifique est désactivée, cochez les cases correspondantes et désactivez toutes les cases à cocher ACTIVÉES. Pour afficher les signatures, qu'une action de vérification soit activée ou désactivée, cochez ou décochez les cases ON et OFF pour cette action. Les actions de vérification sont les suivantes :

Critère	Description
Activé	La signature est activée. Le Web App Firewall vérifie uniquement les signatures activées lorsqu'il traite le trafic.
Bloquer	Les connexions qui correspondent à cette signature sont bloquées.
Journal	Une entrée de journal est produite pour toute connexion qui correspond à cette signature.

Critère	Description
Statistiques	Le Web App Firewall inclut toute connexion qui correspond à cette signature dans les statistiques qu'il génère pour cette vérification.

- Pour filtrer davantage les détails affichés dans la fenêtre de résultats, utilisez la barre de recherche située au-dessus de la fenêtre de résultats. Sélectionnez les propriétés que vous souhaitez filtrer dans la barre de recherche, saisissez la valeur et appuyez sur le bouton Entrée. Il filtre davantage le contenu déjà affiché dans la fenêtre de résultats et répertorie les détails en fonction de la valeur saisie.
  Exemple : Dans l'image suivante, Web-CGI est sélectionné en tant que catégorie dans les options des critères de filtre d'affichage sur la gauche. Les détails de la signature Web-CGI sont répertoriés dans la fenêtre de résultats à droite. Pour filtrer davantage les détails en fonction de la gravité, dans la barre de recherche, la gravité est sélectionnée en tant que propriété et le moyen est saisi en tant que valeur. Les signatures Web-CGI de gravité moyenne sont répertoriées dans la fenêtre de résultats.



- Pour rétablir les paramètres par défaut de tous les critères de filtre d'affichage et afficher toutes les signatures, cliquez sur Afficher tout.

> **Remarque**
>
> Le nombre d'éléments répertoriés dans la fenêtre de résultats filtrée est de 20. La pagination est disponible au-dessus des options Afficher les critères de filtre sur la gauche.

1. Pour plus d'informations sur une signature spécifique, sélectionnez la signature, puis cliquez sur la double flèche bleue dans le champ Plus. La boîte de message Détail de la vulnérabilité relative à la règle de signature s'affiche. Elle contient des informations sur l'objectif de la signa-

ture et fournit des liens vers des informations Web externes concernant la vulnérabilité ou les vulnérabilités que cette signature corrige. Pour accéder à un lien externe, cliquez sur la double flèche bleue à gauche de la description de ce lien.

2. Configurez les paramètres d'une signature en cochant les cases appropriées.
3. Si vous souhaitez ajouter une règle de signature locale à l'objet signatures ou modifier une règle de signature locale existante, consultez The Signatures Editor.
4. Si vous n'avez pas besoin d'injection SQL, de script intersite ou de modèles d'injection Xpath, cliquez sur OK, puis sur Fermer. Sinon, dans le coin inférieur gauche du volet de détails, cliquez sur Gérer les modèles de script SQL/cross-site.
5. Dans la boîte de dialogue Gérer les modèles de script SQL/inter-sites, fenêtre Résultats filtrés, accédez à la catégorie et au modèle de répétition que vous souhaitez configurer. Pour plus d'informations sur les modèles d'injection SQL, reportez-vous à la section Vérification des injections HTML SQL. Pour plus d'informations sur les modèles de script intersite, consultez Vérification des scripts intersites HTML.
6. Pour ajouter un nouveau motif :
   a) Sélectionnez la branche à laquelle vous souhaitez ajouter le nouveau motif.
   b) Cliquez sur le bouton **Ajouter** directement en dessous de la section inférieure de la fenêtre **Résultats filtrés** .
   c) Dans la boîte de dialogue Créer un élément de signature, renseignez la zone de texte de l'élément avec le modèle que vous souhaitez ajouter. Si vous ajoutez un modèle de transformation à la branche des règles de transformation, sous Éléments, remplissez la zone de texte De avec le modèle que vous souhaitez modifier et la zone de texte Vers avec le modèle selon lequel vous souhaitez modifier le modèle précédent.
   d) Cliquez sur **OK**.
7. Pour modifier un modèle existant :
   a) Dans la fenêtre **Résultats filtrés**, sélectionnez la branche qui contient le modèle que vous souhaitez modifier.
   b) Dans la fenêtre détaillée située sous la fenêtre **Résultats filtrés**, sélectionnez le modèle que vous souhaitez modifier.
   c) Cliquez sur **Modifier**.
   d) Dans la boîte de dialogue **Modifier l'**élément**de signature**, zone de texte de l'élément, modifiez le modèle. Si vous modifiez un modèle de transformation, vous pouvez modifier l'un ou les deux modèles sous Éléments, dans les zones de texte De et À.
   e) Cliquez sur **OK**.
8. Pour supprimer un modèle, sélectionnez le modèle que vous souhaitez supprimer, puis cliquez sur le bouton **Supprimer** situé sous le volet de détails sous la fenêtre **Résultats filtrés** . Lorsque vous y êtes invité, confirmez votre choix en cliquant sur **Fermer**.

9. Pour ajouter la catégorie patterns à la branche de script intersite :
    a) Sélectionnez la branche à laquelle vous souhaitez ajouter la catégorie de modèles.
    b) Cliquez sur le bouton **Ajouter** directement en dessous de la fenêtre **Résultats filtrés** .

    > **Remarque :** Actuellement, vous ne pouvez ajouter qu'une seule catégorie, nommée patterns, à la branche de script intersite. Après avoir cliqué sur **Ajouter**, vous devez accepter le choix par défaut, à savoir les modèles.

    c) Cliquez sur **OK**.
10. Pour supprimer une branche, sélectionnez-la, puis cliquez sur le bouton Supprimer situé juste en dessous de la fenêtre **Résultats filtrés** . Lorsque vous y êtes invité, confirmez votre choix en cliquant sur **OK**.

    > **Remarque :** Si vous supprimez une branche par défaut, vous supprimez tous les modèles de cette branche. Cela peut désactiver les contrôles de sécurité qui utilisent ces informations.

11. Lorsque vous avez terminé de modifier les modèles d'injection SQL, de script intersite et d'injection XPath, cliquez sur **OK**, puis sur **Fermer** pour revenir à la boîte de dialogue **Modifier l'objet de signatures** .
12. Cliquez sur **OK** à tout moment pour enregistrer vos modifications, puis lorsque vous avez terminé de configurer l'objet de signatures, cliquez sur **Fermer**.

Protection des applications JSON à l'aide de signatures

May 9, 2023

JavaScript Object Notation (JSON) est un standard ouvert basé sur du texte dérivé du langage de script JavaScript. Le format JSON est préférable pour la représentation lisible par l'homme de structures de données simples et de tableaux associatifs, appelés objets. Il constitue une alternative au XML et est principalement utilisé pour transmettre des structures de données sérialisées pour communiquer avec des applications Web. Les fichiers JSON sont généralement enregistrés avec une extension .json.

La charge utile JSON est généralement envoyée avec le type MIME spécifié comme application/json. Les autres types de contenu « standard » pour JSON sont les suivants :

- **application/x-javascript**
- **texte/javascript**
- **texte/x-javascript**
- **text/x-json**

Utilisation des signatures du NetScaler Web App Firewall pour protéger les applications JSON

Pour autoriser les requêtes JSON, l'appliance est préconfigurée avec le type de contenu JSON, comme indiqué dans la sortie show-command suivante :

```
> sh appfw jsonContentType
1)      JSONContenttypevalue:  "^application/json$" IsRegex:  REGEX
Done
<!--NeedCopy-->
```

Le pare-feu NetScaler Web App traite le corps du message uniquement pour les types de contenu suivants :

- **application/x-www-form-urlencoded**
- **données multipart/formulaire**
- **texte/x-gwt-rpc**

Les demandes reçues avec d'autres en-têtes de type de contenu, y compris application/json (ou tout autre type de contenu autorisé) sont transmises au backend après inspection des en-têtes. Le corps de publication de ces requêtes n'est pas inspecté pour détecter toute violation des contrôles de sécurité, même lorsque les contrôles de sécurité du profil, tels que le SQL ou les scripts intersites, sont activés.

Afin de protéger les applications JSON et de détecter les violations, les signatures du Web App Firewall peuvent être utilisées. Toutes les demandes contenant l'en-tête du type de contenu autorisé sont traitées par le Web App Firewall pour la correspondance des signatures. Vous pouvez ajouter vos propres règles de signature personnalisées pour traiter la charge utile JSON afin d'effectuer diverses inspections de sécurité (par exemple, des scripts intersites, du SQL et de la cohérence des champs), de détecter les violations dans les en-têtes ainsi que dans le corps du message, et de prendre des mesures spécifiques.

> **Conseil**
>
> Contrairement aux autres valeurs par défaut intégrées, le type de contenu JSON préconfiguré peut être modifié ou supprimé à l'aide de l'interface de ligne de commande ou de l'interface graphique (GUI). Si des requêtes légitimes pour des applications JSON sont bloquées et déclenchent des violations de type de contenu, vérifiez que la valeur du type de contenu est configurée avec précision. Pour plus d'informations sur la façon dont Web App Firewall traite l'en-tête de type de contenu, voir Protection du type de contenu.

Pour ajouter ou supprimer le type de contenu JSON à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :


```
add appfw jsonContentType ^application/json$ IsRegEx REGEX

rm appfw JSONContentType "^application/json$"
```

Pour gérer les types de contenu JSON à l'aide de l'interface graphique

Accédez à **Sécurité** > **Web App Firewall** et, dans la section **Paramètres**, sélectionnez **Gérer les types de contenu JSON**.

Dans le panneau **Configurer le type de contenu JSON du Web App Firewall**, ajoutez, modifiez ou supprimez des types de contenu JSON en fonction des besoins de vos applications.

Configuration de la protection des signatures pour détecter les attaques dans la charge utile JSON

Outre un type de contenu JSON valide, vous devez configurer des signatures pour spécifier le ou les modèles qui, lorsqu'ils sont détectés dans une requête JSON, indiquent une faille de sécurité. Les actions spécifiées, telles que le blocage et l'enregistrement, sont effectuées lorsqu'une demande entrante déclenche une correspondance pour tous les modèles cibles de la règle de signature.

Pour ajouter une règle de signature personnalisée, Citrix vous recommande d'utiliser l'interface graphique. Accédez à **Système** > **Sécurité** > **Web App Firewall** > **Signatures**. Double-cliquez sur l'objet de signature cible pour accéder au panneau **Modifier les signatures du Web App Firewall** . Cliquez sur le bouton **Ajouter** pour configurer les actions, la catégorie, la chaîne de journal, les modèles de règles, etc. Bien que le Web App Firewall inspecte toutes les charges utiles de type de contenu autorisées pour détecter la correspondance des signatures, vous pouvez optimiser le traitement en spécifiant l'expression JSON dans la règle. Lorsque vous **ajoutez** un nouveau modèle de règle, sélectionnez **Expression** dans les options déroulantes de **Match** et indiquez l'expression de correspondance cible à partir de votre charge utile JSON pour identifier les demandes spécifiques qui doivent être inspectées. Une expression doit commencer par un **TEXTE.** préfixe. Vous pouvez ajouter d'autres modèles de règles pour spécifier des modèles de correspondance supplémentaires afin d'identifier l'attaque.

L'exemple suivant montre une règle de signature. Si une balise de script intersite est détectée dans le corps POST de la charge utile JSON qui correspond à l'expression XPATH_JSON spécifiée, une correspondance de signature est déclenchée.

Exemple de signature pour détecter les scripts intersites dans la charge utile JSON

```
1 <SignatureRule actions="log,stats" category="JSON" enabled="ON" id="
     1000001" severity="" source="" type="" version="1">
2
3   <PatternList>
```



```
4
5       <RequestPatterns>
6
7         <Pattern>
8
9           <Location area="HTTP_POST_BODY"/>
10
11          <Match type="Expression">TEXT.XPATH_JSON(xp%/glossary/title%).
                CONTAINS("example glossary")</Match>
12
13        </Pattern>
14
15        <Pattern>
16
17          <Location area="HTTP_METHOD"/>
18
19          <Match type="LITERAL">POST</Match>
20
21        </Pattern>
22
23        <Pattern>
24
25          <Location area="HTTP_POST_BODY"/>
26
27          <Match type="CrossSiteScripting"/>
28
29         </Pattern>
30
31      </RequestPatterns>
32
33    </PatternList>
34
35    <LogString>Cross-site scripting violation detected in json payload</
         LogString>
36
37    <Comment/>
38
39  </SignatureRule>
40  <!--NeedCopy-->
```

Exemple de charge utile

La charge utile suivante déclenche la correspondance des signatures, car elle inclut la balise de script intersite **<Gotcha!!>**.


```
{
 "glossary": {
 "title": "example glossary","GlossDiv": {
 "title": "S","GlossList": {
 "GlossEntry": {
 "ID": "SGML","SortAs": "SGML","GlossTerm": "Standard Generalized
    Markup Language","Acronym": "SGML","Abbrev": "ISO 8879:1986","
    GlossDef": {
 "para": "A meta-markup language, used to create markup languages \*\*<
    Gotcha!!>\*\* such as DocBook.","GlossSeeAlso": ["GML", "XML"] }
 ,"GlossSee": "markup" }
  }
  }
  }
  }

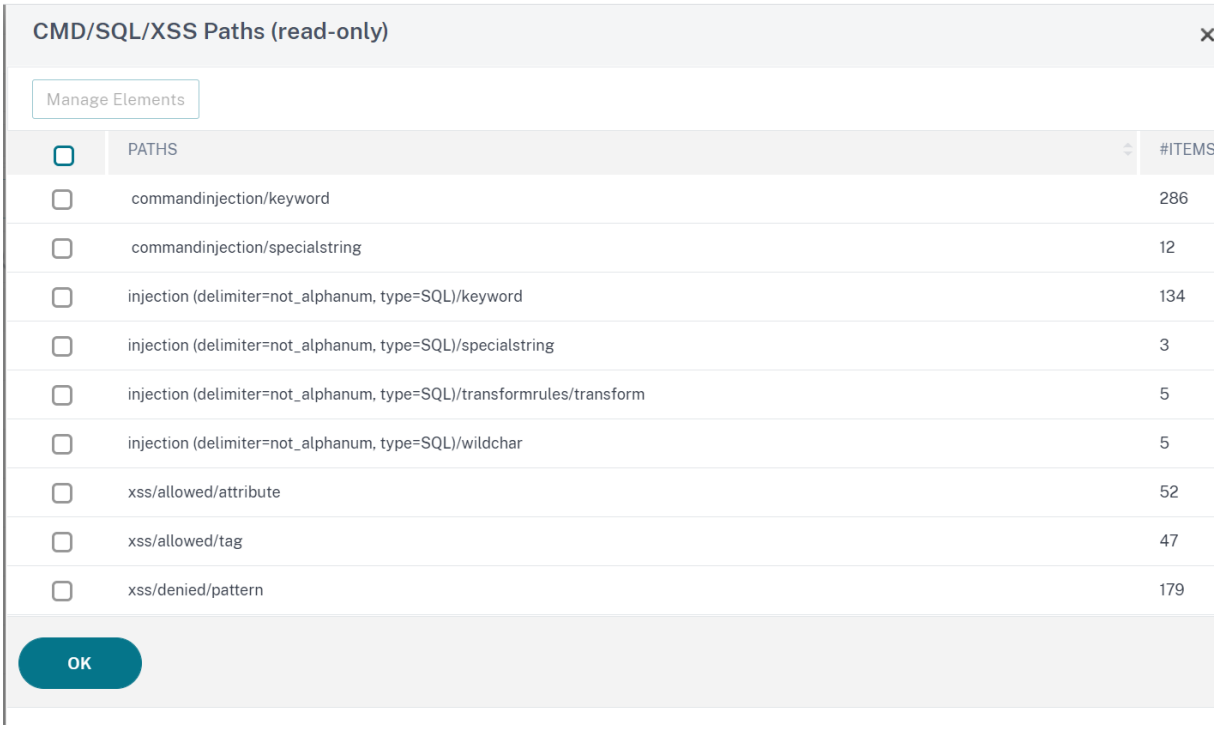
<!--NeedCopy-->
```

Exemple de message de journal

```
Aug 21 12:21:42 <local0.info> 10.217.31.239 08/21/2015:23:21:42 GMT ns
    0-PPE-1 : APPFW APPFW_SIGNATURE_MATCH 1471 0 :  10.217.253.62 990-
    PPE0 NtJnVMNnvPeQJnaUzXYW/GTvAQsA010 prof1 http://10.217.31.212/FFC/
    login_post.php Signature violation rule ID 1000001: cross-site
    scripting violation detected in json payload  <not blocked>
<!--NeedCopy-->
```

> **Remarque**
>
> Si vous envoyez la même charge utile après avoir supprimé la balise de script intersite (**<Gotcha!!>**), la correspondance entre les règles de signature n'est pas déclenchée.

Résumé

- Pour protéger la charge utile JSON, utilisez les signatures du Web App Firewall pour détecter les violations liées aux scripts intersites, au SQL et à d'autres violations.
- Vérifiez que le type de contenu JSON est configuré sur l'appliance en tant que type de contenu autorisé.
- Assurez-vous que le type de contenu de la charge utile correspond au type de contenu JSON configuré.
- Assurez-vous que tous les modèles configurés dans la règle de signature correspondent pour que la violation de signature soit déclenchée.

- Lorsque vous ajoutez une règle de signature, elle DOIT comporter au moins un modèle de règle correspondant à l'expression de la charge utile JSON. Toutes les expressions PI figurant dans les règles de signature doivent commencer par le préfixe TEXT et doivent être booléennes.

Protégez le type de contenu d'application ou JSON à l'aide de SQL et de la charge utile codée par script intersite à l'aide de politiques et de signatures

NetScaler Web App Firewall peut protéger les applications ou les types de contenu JSON à l'aide de politiques et de signatures.

Inspectez le type de contenu d'application ou JSON pour l'injection SQL à l'aide de politiques

Vous devez ajouter les stratégies suivantes et les lier au serveur virtuel globalement pour prendre en charge l'injection SQL.

```
add appfw policy sqli_1 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((((\\A)
|(?<=[^a-zA-Z0-9_])))(select|insert|delete|update|drop|create|alter|grant
|revoke|commit|rollback|shutdown|union|intersect|minus|case|decode|where
|group|begin|join|exists|distinct|add|modify|constraint|null|like|exec|
execute|char|or|and|sp_sdidebug)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK

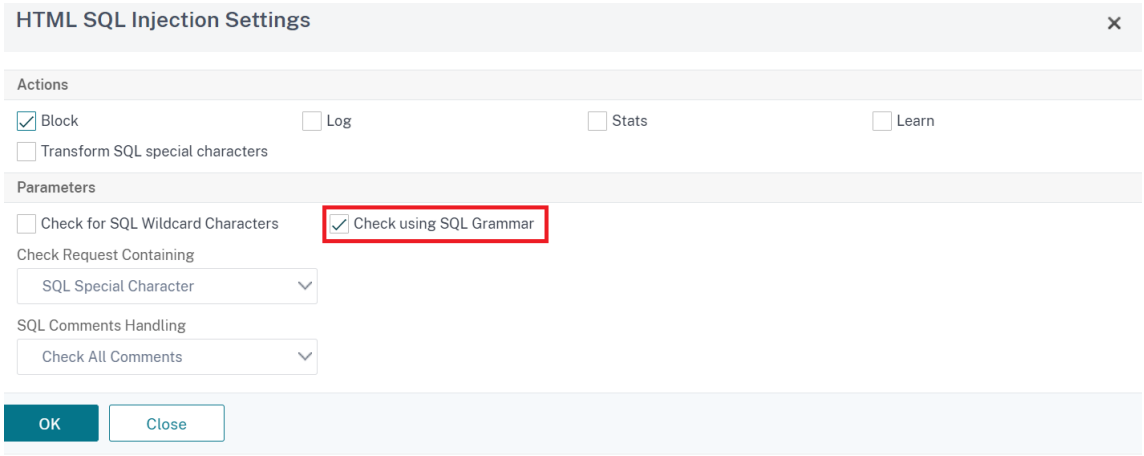
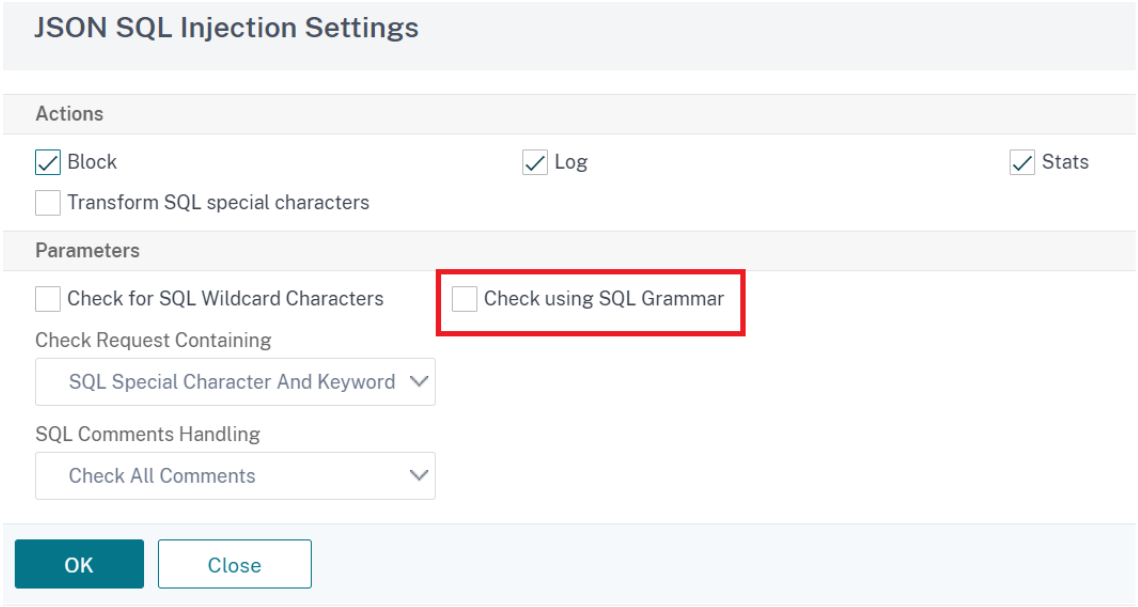
add appfw policy sqli_2 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_]))(xp_availablemedia|xp_cmdshell|xp_deletemail|xp_dirtree
|xp_dropwebtask|xp_dsninfo|xp_enumdsn|xp_enumerrorlogs|xp_enumgroups|
xp_enumqueuedtasks|xp_eventlog|xp_findnextmsg|xp_fixeddrives|xp_getfiledetails
|xp_getnetname|xp_grantlogin|xp_logevent|xp_loginconfig|xp_logininfo|
xp_makewebtask|xp_msver|xp_regread|xp_perfend|xp_perfmonitor|xp_perfsample
|xp_perfstart|xp_readerrorlog|xp_readmail|xp_revokelogin|xp_runwebtask|
xp_schedulersignal|xp_sendmail|xp_servicecontrol|xp_snmp_getstate|xp_snmp_raisetrap
|xp_sprintf|xp_sqlinventory|xp_sqlregister|xp_sqltrace|xp_sscanf|xp_startmail
|xp_stopmail|xp_subdirs|xp_unc_to_drive)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK


add appfw policy sqli_3 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_]))(sysobjects|syscolumns|MSysACEs|MSysObjects|MSysQueries
|MSysRelationships)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK

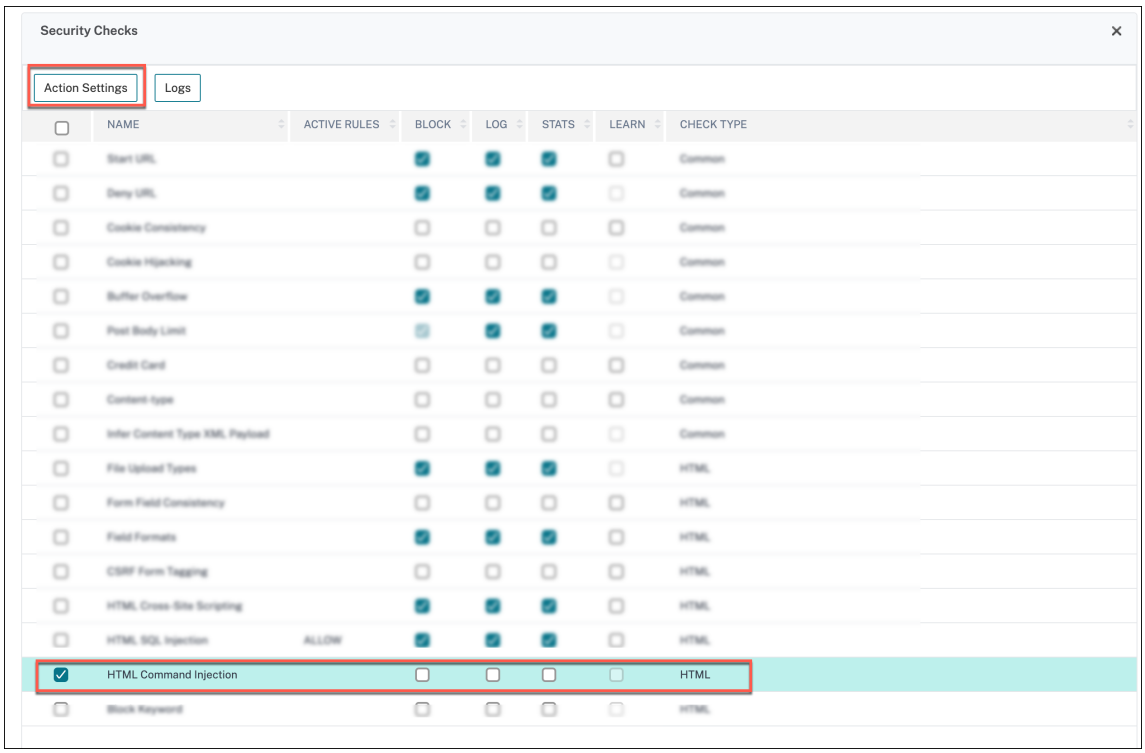
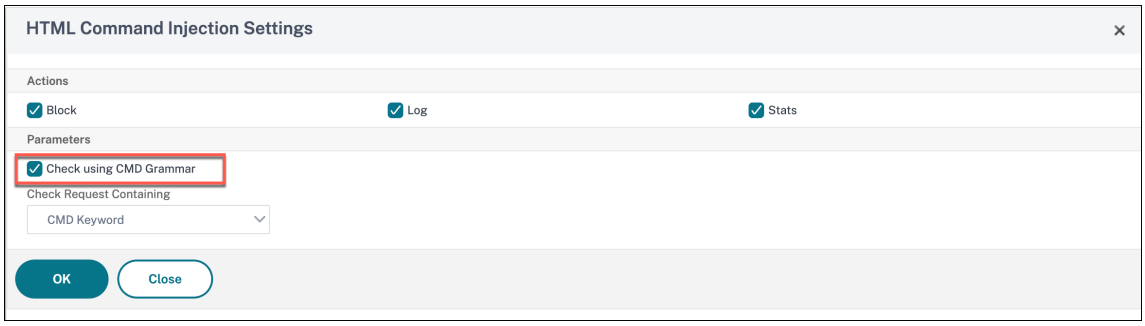
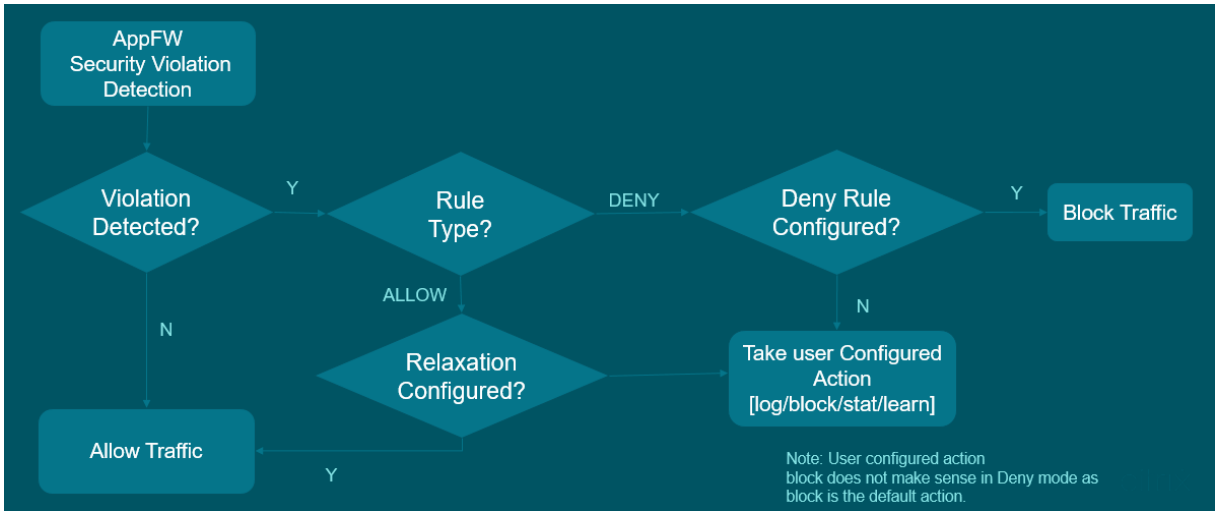
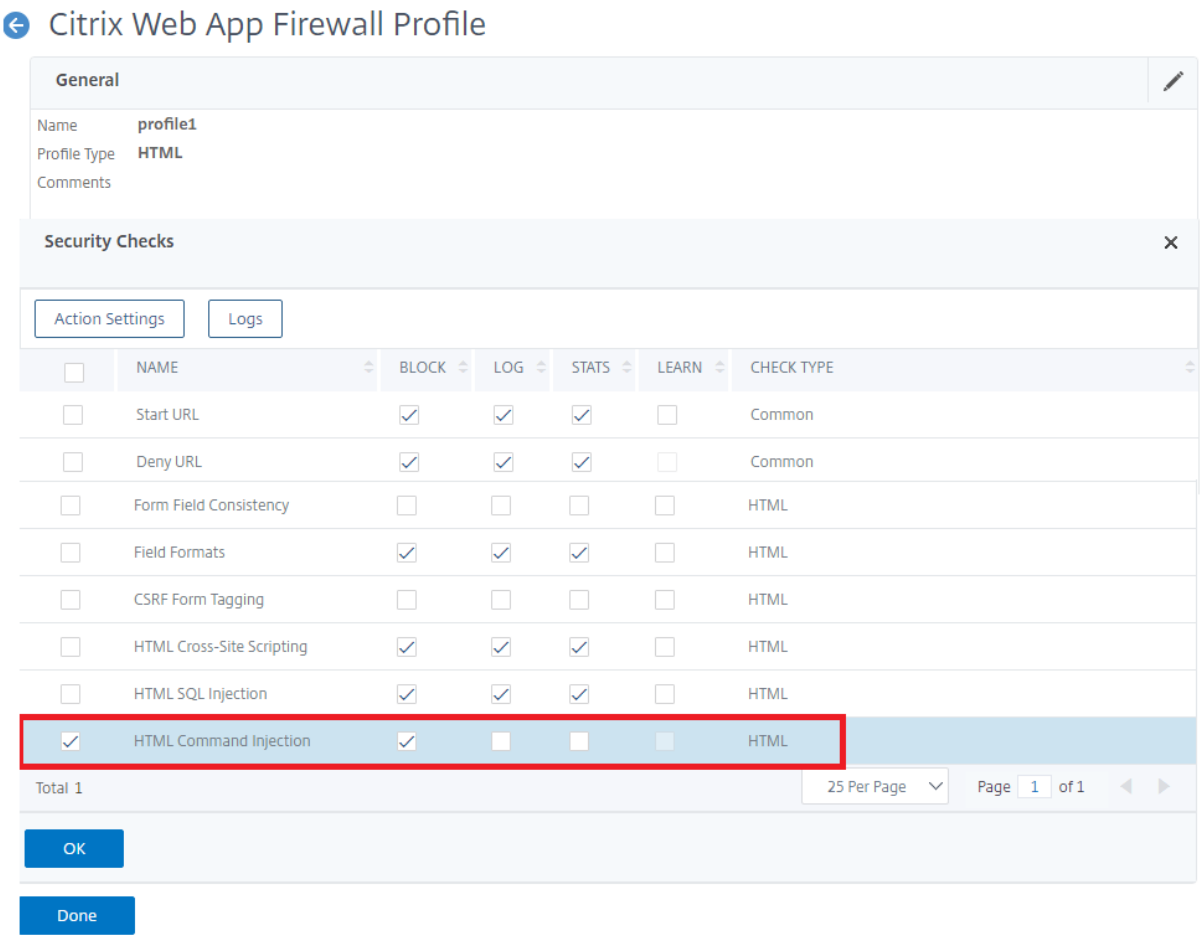
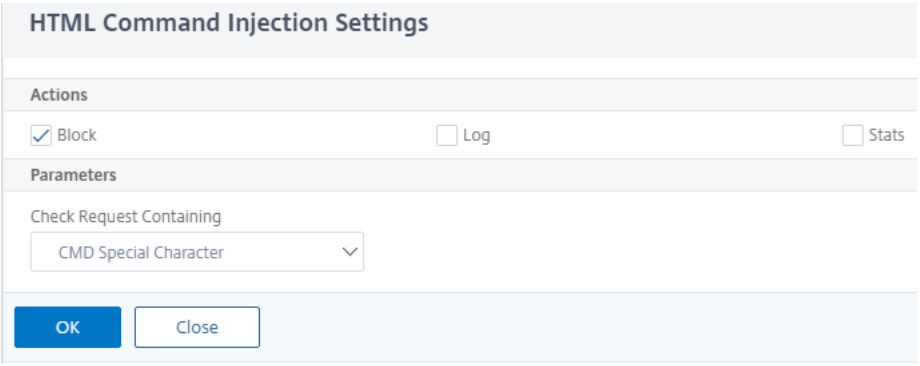
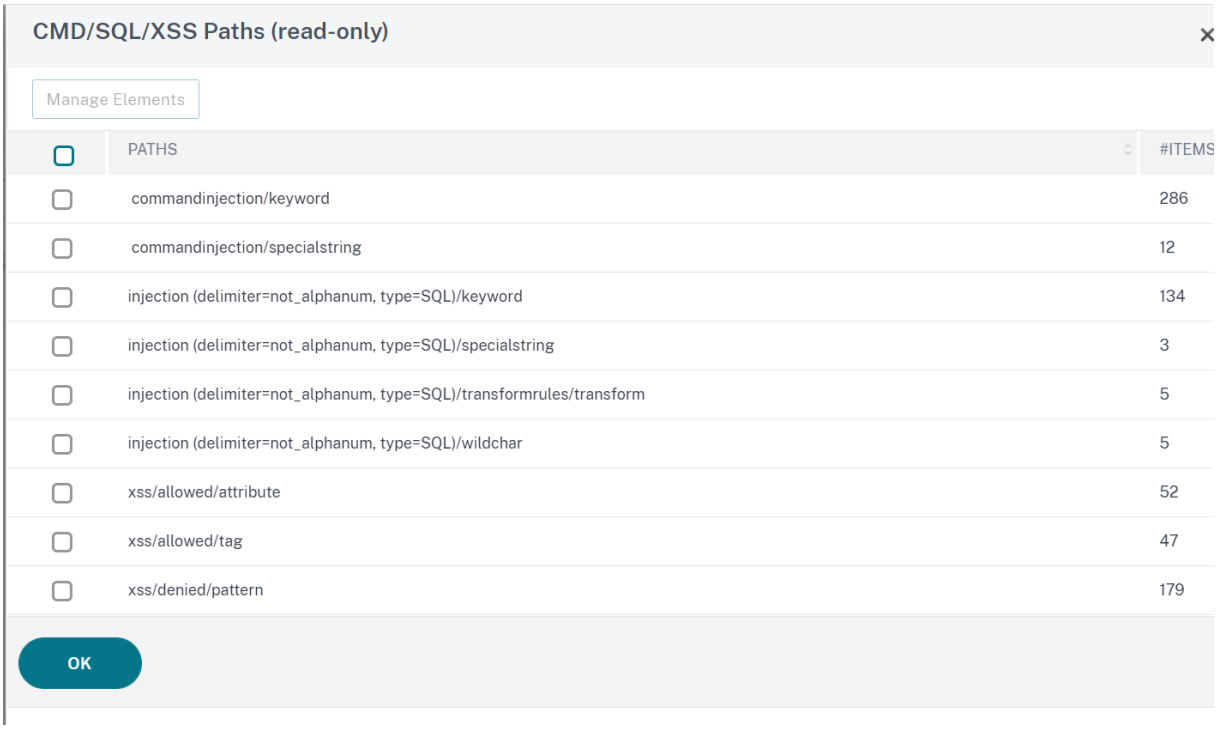
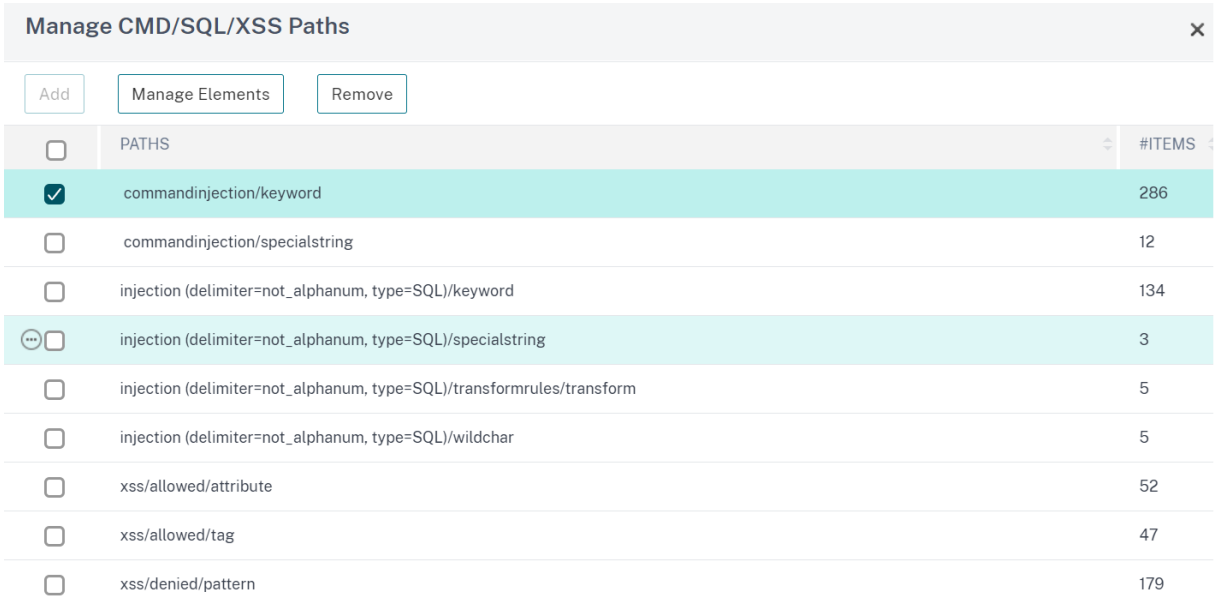
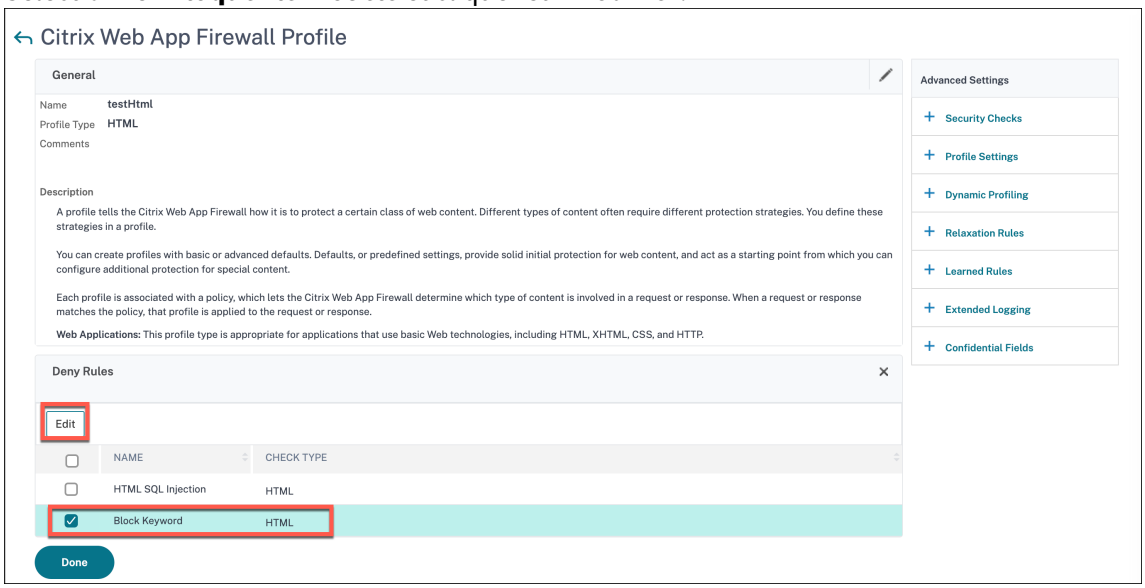
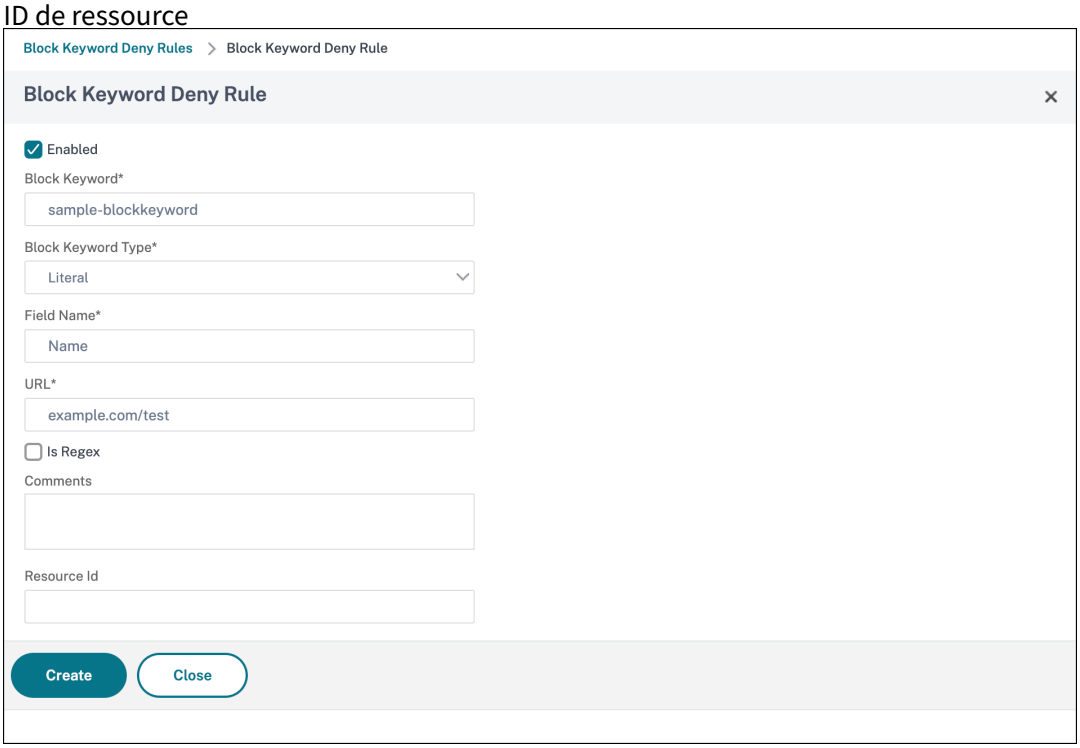
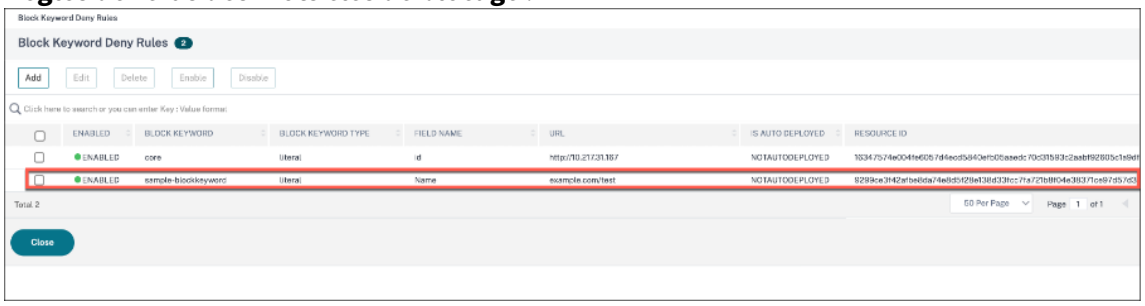
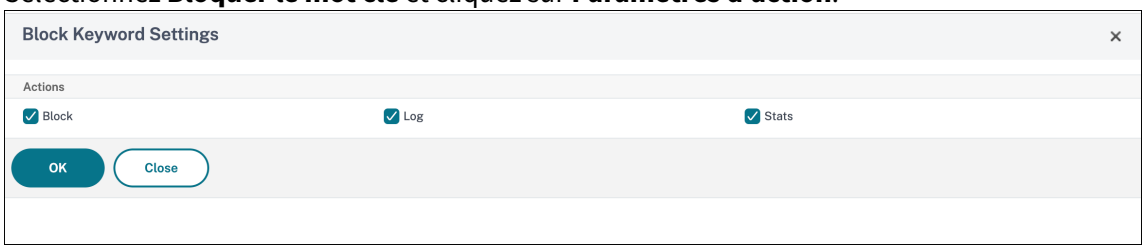
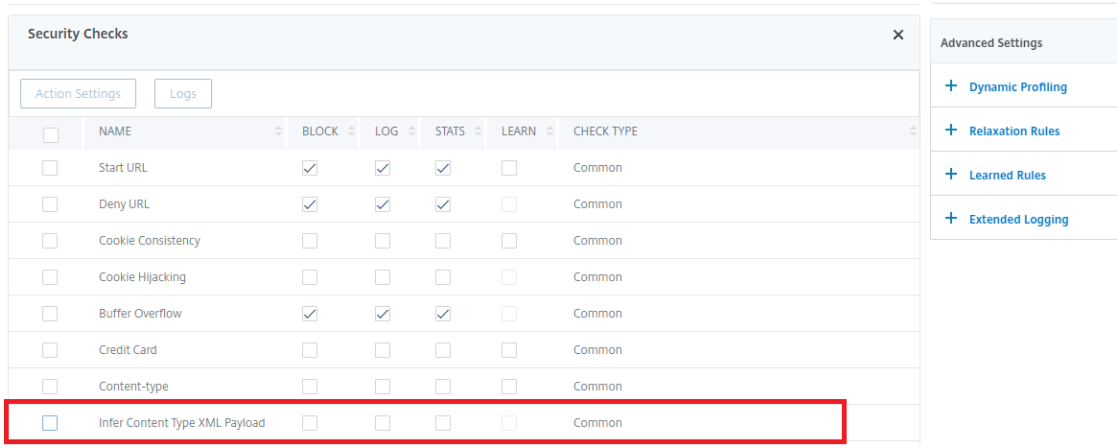
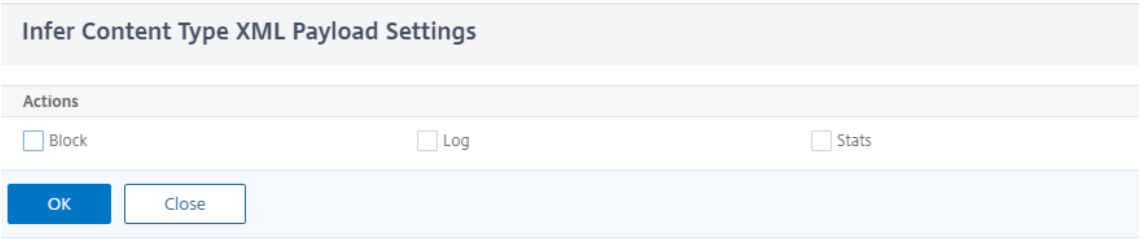
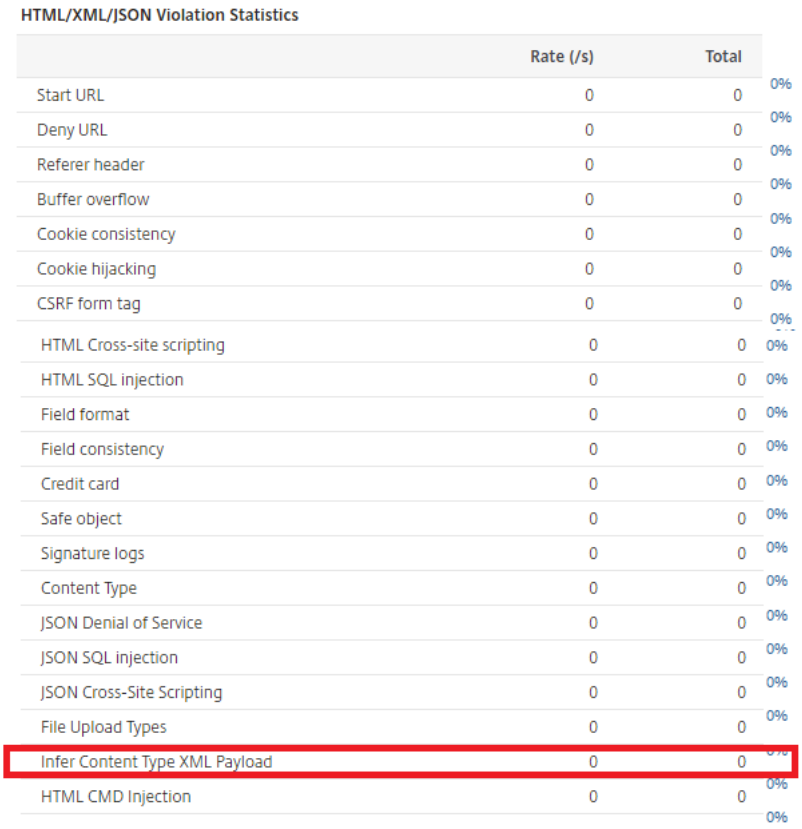
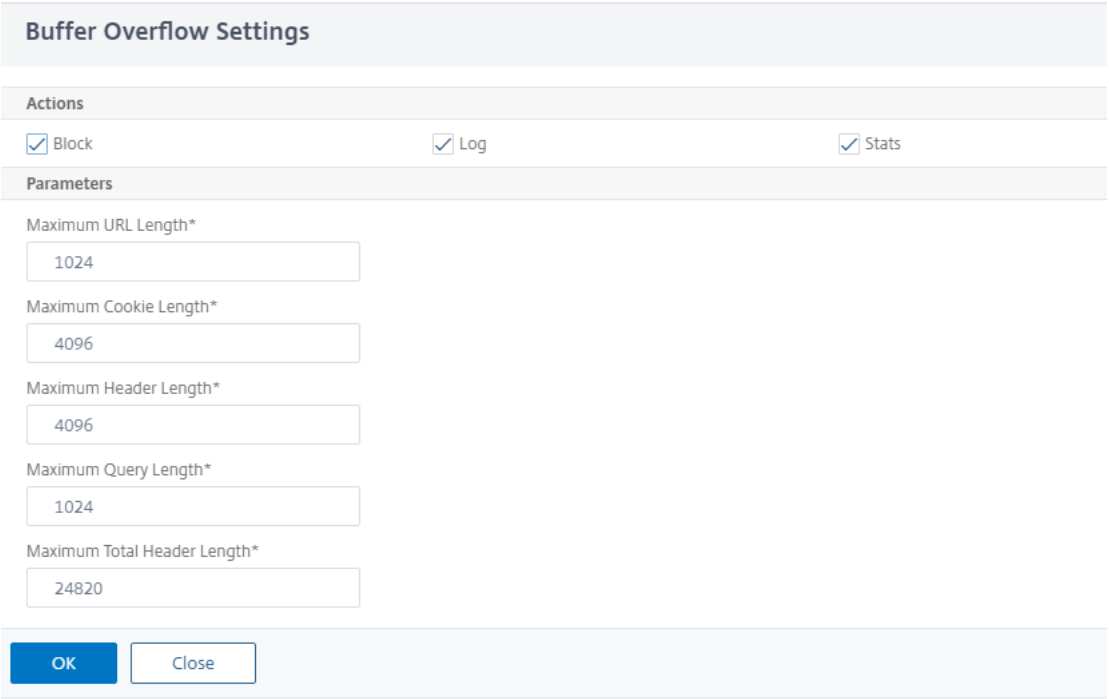
add appfw policy sqli_4 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A
```



```
)|(?<=[^a-zA-Z0-9_]))(SYS\.USER_OBJECTS|SYS\.TAB|SYS\.USER_TABLES|SYS\.
USER_VIEWS|SYS\.ALL_TABLES|SYS\.USER_TAB_COLUMNS|SYS\.USER_CONSTRAINTS|SYS
\.USER_TRIGGERS|SYS\.USER_CATALOG|SYS\.ALL_CATALOG|SYS\.ALL_CONSTRAINTS|SYS
\.ALL_OBJECTS|SYS\.ALL_TAB_COLUMNS|SYS\.ALL_TAB_PRIVS|SYS\.ALL_TRIGGERS|SYS
\.ALL_USERS|SYS\.ALL_VIEWS|SYS\.USER_ROLE_PRIVS|SYS\.USER_SYS_PRIVS|SYS\.
USER_TAB_PRIVS)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

Inspecter l'application ou le type de contenu JSON à l'aide de signatures

Vous pouvez ajouter les règles de signature suivantes à l'objet de signature dans le profil du pare-feu de l'application afin de prendre en charge l'injection SQL pour le type de contenu JSON.

> **Remarque :**
>
> Les signatures postérieures sont gourmandes en CPU.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2013-2018 Citrix Systems, Inc. All rights reserved. -->
<SignaturesFile schema_version="6" version="0" minor_schema_version="0"
    >
     <Signatures>
         <SignatureRule id="4000000" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
             <PatternList>
                 <RequestPatterns>
                     <Pattern>
                         <Location area="HTTP_POST_BODY"/>
                         <Match type="Expression">TEXT.SET_TEXT_MODE(
                            IGNORECASE).SET_TEXT_MODE(URLENCODED).
                            DECODE_USING_TEXT_MODE.REGEX_MATCH(re#(((\A)
                            |(?<=[^a-zA-Z0-9_])))(select|insert|delete|
                            update|drop|create|alter|grant|revoke|commit
                            |rollback|shutdown|union|intersect|minus|
                            case|decode|where|group|begin|join|exists|
                            distinct|add|modify|constraint|null|like|
                            exec|execute|char|or|and|sp_sdidebug)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                     </Pattern>
                     <Pattern type="fastmatch">
                         <Location area="HTTP_METHOD"/>
                         <Match type="LITERAL">T</Match>
                     </Pattern>
                 </RequestPatterns>
             </PatternList>
```



```
            <LogString>sql Injection</LogString>
            <Comment/>
        </SignatureRule>
        <SignatureRule id="4000001" enabled="ON" actions="log,block"
           category="sql" source="" severity="" type="" version="1"
           sourceid="" harmscore="">
            <PatternList>
                <RequestPatterns>
                    <Pattern>
                        <Location area="HTTP_POST_BODY"/>
                        <Match type="Expression">TEXT.SET_TEXT_MODE(
                           IGNORECASE).SET_TEXT_MODE(URLENCODED).
                           DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                           |(?<=[^a-zA-Z0-9_]))(xp_availablemedia|
                           xp_cmdshell|xp_deletemail|xp_dirtree|
                           xp_dropwebtask|xp_dsninfo|xp_enumdsn|
                           xp_enumerrorlogs|xp_enumgroups|
                           xp_enumqueuedtasks|xp_eventlog|
                           xp_findnextmsg|xp_fixeddrives|
                           xp_getfiledetails|xp_getnetname|
                           xp_grantlogin|xp_logevent|xp_loginconfig|
                           xp_logininfo|xp_makewebtask|xp_msver|
                           xp_regread|xp_perfend|xp_perfmonitor|
                           xp_perfsample|xp_perfstart|xp_readerrorlog|
                           xp_readmail|xp_revokelogin|xp_runwebtask|
                           xp_schedulersignal|xp_sendmail|
                           xp_servicecontrol|xp_snmp_getstate|
                           xp_snmp_raisetrap|xp_sprintf|xp_sqlinventory
                           |xp_sqlregister|xp_sqltrace|xp_sscanf|
                           xp_startmail|xp_stopmail|xp_subdirs|
                           xp_unc_to_drive)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                    </Pattern>
                    <Pattern type="fastmatch">
                        <Location area="HTTP_METHOD"/>
                        <Match type="LITERAL">T</Match>
                    </Pattern>
                </RequestPatterns>
            </PatternList>
            <LogString>sql Injection</LogString>
            <Comment/>
        </SignatureRule>
        <SignatureRule id="4000002" enabled="ON" actions="log,block"
           category="sql" source="" severity="" type="" version="1"
           sourceid="" harmscore="">
```



```
40              <PatternList>
41                  <RequestPatterns>
42                      <Pattern>
43                          <Location area="HTTP_POST_BODY"/>
44                          <Match type="Expression">TEXT.SET_TEXT_MODE(
                                IGNORECASE).SET_TEXT_MODE(URLENCODED).
                                DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                                |(?<=[^a-zA-Z0-9_]))(sysobjects|syscolumns|
                                MSysACEs|MSysObjects|MSysQueries|
                                MSysRelationships)((
45  Z)|(?=[^a-zA-Z0-9_]))#)</Match>
46                      </Pattern>
47                      <Pattern type="fastmatch">
48                          <Location area="HTTP_METHOD"/>
49                          <Match type="LITERAL">T</Match>
50                      </Pattern>
51                  </RequestPatterns>
52              </PatternList>
53              <LogString>sql Injection</LogString>
54              <Comment/>
55          </SignatureRule>
56          <SignatureRule id="4000003" enabled="ON" actions="log,block"
               category="sql" source="" severity="" type="" version="1"
               sourceid="" harmscore="">
57              <PatternList>
58                  <RequestPatterns>
59                      <Pattern>
60                          <Location area="HTTP_POST_BODY"/>
61                          <Match type="Expression">TEXT.SET_TEXT_MODE(
                                IGNORECASE).SET_TEXT_MODE(URLENCODED).
                                DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                                |(?<=[^a-zA-Z0-9_]))(SYS.USER_OBJECTS|SYS.
                                TAB|SYS.USER_TABLES|SYS.USER_VIEWS|SYS.
                                ALL_TABLES|SYS.USER_TAB_COLUMNS|SYS.
                                USER_CONSTRAINTS|SYS.USER_TRIGGERS|SYS.
                                USER_CATALOG|SYS.ALL_CATALOG|SYS.
                                ALL_CONSTRAINTS|SYS.ALL_OBJECTS|SYS.
                                ALL_TAB_COLUMNS|SYS.ALL_TAB_PRIVS|SYS.
                                ALL_TRIGGERS|SYS.ALL_USERS|SYS.ALL_VIEWS|SYS
                                .USER_ROLE_PRIVS|SYS.USER_SYS_PRIVS|SYS.
                                USER_TAB_PRIVS)((
62  Z)|(?=[^a-zA-Z0-9_]))#)</Match>
63                      </Pattern>
64                      <Pattern type="fastmatch">
65                          <Location area="HTTP_METHOD"/>
```



```
66                          <Match type="LITERAL">T</Match>
67                       </Pattern>
68                    </RequestPatterns>
69                </PatternList>
70                <LogString>sql Injection</LogString>
71                <Comment/>
72             </SignatureRule>
73        </Signatures>
74  </SignaturesFile>
75
76  <!--NeedCopy-->
```

Mettre à jour un objet de signature

May 5, 2023

Vous devez régulièrement mettre à jour vos objets de signature pour vous assurer que votre Web App Firewall fournit une protection contre les menaces actuelles. Vous devez régulièrement mettre à jour les signatures par défaut du Web App Firewall et toutes les signatures que vous importez à partir d'un outil d'analyse des vulnérabilités compatible.

NetScaler met régulièrement à jour les signatures par défaut du Web App Firewall. Vous pouvez mettre à jour les signatures par défaut manuellement ou automatiquement. Dans les deux cas, demandez à votre représentant NetScaler ou à votre revendeur NetScaler l'URL permettant d'accéder aux mises à jour. Vous pouvez activer les mises à jour automatiques des signatures au format natif NetScaler dans les boîtes de dialogue « Paramètres du moteur » et « Paramètres de mise à jour automatique des signatures ».

La plupart des fabricants d'outils d'analyse des vulnérabilités les mettent régulièrement à jour. La plupart des sites Web changent également fréquemment. Vous devez mettre à jour votre outil et réanalyser régulièrement vos sites Web, en exportant les signatures obtenues dans un fichier et en les important dans la configuration de votre Web App Firewall.

> **Conseil**
>
> Lorsque vous mettez à jour les signatures du Web App Firewall à partir de la ligne de commande NetScaler, vous devez d'abord mettre à jour les signatures par défaut, puis émettre d'autres commandes de mise à jour pour mettre à jour chaque fichier de signatures personnalisées basé sur les signatures par défaut. Si vous ne mettez pas d'abord à jour les signatures par défaut, une erreur d'incompatibilité de version empêche la mise à jour des fichiers de signatures personnalisés.

> **Remarque**
>
> Ce qui suit s'applique à la fusion d'un objet de signature tiers avec un objet de signature défini par l'utilisateur avec des règles natives et des règles ajoutées par l'utilisateur :
>
> Lorsque des signatures de version 0 sont fusionnées avec un nouveau fichier importé, les signatures résultantes restent en tant que version 0.
>
> Cela signifie que toutes les règles natives (ou intégrées) du fichier importé seront ignorées après la fusion. Cela permet de garantir que les signatures de la version 0 sont conservées telles quelles après une fusion.
>
> Pour inclure les règles natives dans le fichier importé pour la fusion, vous devez d'abord mettre à jour les signatures existantes à partir de la version 0 avant la fusion. Cela signifie que vous devez abandonner le caractère de version 0 des signatures existantes.
>
> Lors d'une mise à niveau de NetScaler, le fichier « default_signatures.xml » est ajouté à la nouvelle version et le fichier « updated_signature.xml » est supprimé de l'ancienne version. Après la mise à niveau, si la fonctionnalité de mise à jour automatique des signatures est activée, l'appliance met à jour la signature existante vers la dernière version de la version et génère le fichier « updated_signature.xml ».

Pour mettre à jour les signatures du Web App Firewall à partir de la source à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `update appfw signatures <name> [-mergedefault]`
- `save ns config`

Exemple

L'exemple suivant met à jour l'objet de signatures nommé MySignatures à partir de l'objet de signatures par défaut, en fusionnant les nouvelles signatures de l'objet de signatures par défaut avec les signatures existantes. Cette commande ne remplace aucune signature créée par l'utilisateur ni aucune signature importée depuis une autre source, telle qu'un outil d'analyse des vulnérabilités approuvé.

```
1 update appfw signatures MySignatures -mergedefault
2 save ns config
3 <!--NeedCopy-->
```


Mettre à jour un objet de signatures à partir d'un fichier au format NetScaler

NetScaler met régulièrement à jour les signatures du Web App Firewall. Vous devez régulièrement mettre à jour les signatures de votre Web App Firewall pour vous assurer que votre Web App Firewall utilise la liste la plus récente. Demandez à votre représentant NetScaler ou à votre revendeur NetScaler l'URL permettant d'accéder aux mises à jour.

Pour mettre à jour un objet de signatures à partir d'un fichier au format NetScaler à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `update appfw signatures <name> [-mergeDefault]`
- `save ns config`

Pour mettre à jour un objet de signatures à partir d'un fichier au format NetScaler à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Signatures**.
2. Dans le volet de détails, sélectionnez l'objet de signatures que vous souhaitez mettre à jour.
3. Dans la liste déroulante **Action**, sélectionnez **Fusionner**.
4. Dans la boîte de dialogue **Mettre à jour l'objet de signatures**, choisissez l'une des options suivantes.
   - **Importer depuis une URL** : choisissez cette option si vous téléchargez les mises à jour des signatures à partir d'une URL Web.
   - **Importer à partir d'un fichier local** : choisissez cette option si vous importez des mises à jour de signature à partir d'un fichier sur votre disque dur local, sur votre disque dur réseau ou sur un autre périphérique de stockage.
5. Dans la zone de texte, tapez l'URL, ou saisissez le fichier local ou naviguez jusqu'à celui-ci.
6. Cliquez sur **Update**. Le fichier de mise à jour est importé et le format de la boîte de dialogue Mettre à jour les signatures est quasiment identique à celui de la boîte de dialogue **Modifier l'objet des signatures** . La boîte de dialogue **Mettre à jour les signatures d'objet** affiche toutes les branches avec des règles de signature nouvelles ou modifiées, des modèles de script d'injection SQL ou intersite et des modèles d'injection XPath, le cas échéant.
7. Vérifiez et configurez les signatures nouvelles et modifiées.
8. Lorsque vous avez terminé, cliquez sur **OK**, puis sur **Fermer**.

Mise à jour d'un objet de signatures à partir d'un outil d'analyse des vulnérabilités compatible

> **Remarque :**
>
> Avant de mettre à jour un objet de signatures à partir d'un fichier, vous devez créer le fichier en exportant les signatures à partir de l'outil d'analyse des vulnérabilités.

Pour importer et mettre à jour des signatures à partir d'un outil d'analyse des vulnérabilités

1. Accédez à **Sécurité** > **Web App Firewall** > **Signatures**.
2. Dans le volet de détails, sélectionnez l'objet de signatures que vous souhaitez mettre à jour, puis cliquez sur **Fusionner**.
3. Dans la boîte de dialogue **Mettre à jour l'objet de signatures**, **sous l'onglet Format externe**, section Importer, choisissez l'une des options suivantes.
   - **Importer depuis une URL** : choisissez cette option si vous téléchargez les mises à jour des signatures à partir d'une URL Web.
   - **Importer à partir d'un fichier local** : choisissez cette option si vous importez des mises à jour de signature à partir d'un fichier sur votre disque dur local ou réseau ou sur un autre périphérique de stockage.
4. Dans la zone de texte, tapez l'URL, parcourez le fichier local ou saisissez son chemin.
5. Dans la section XSLT, choisissez l'une des options suivantes.
   - **Utiliser un fichier XSLT intégré**—Choisissez cette option si vous souhaitez utiliser un fichier XSLT intégré.
   - **Utiliser un fichier XSLT local**—Choisissez cette option pour utiliser un fichier XSLT sur votre ordinateur local.
   - **Référence XSLT à partir d'une URL**—Choisissez cette option pour importer un fichier XSLT à partir d'une URL Web.
6. Si vous avez choisi Utiliser le fichier XSLT intégré, dans la liste déroulante XSLT intégré, sélectionnez le fichier que vous souhaitez utiliser parmi les options suivantes :
   - **Cenzic.**
   - **Sécurité approfondie pour les applications Web.**
   - **Hewlett_Packard_Enterprise_WebInspect.**
   - **IBM-AppScan-Entreprise.**
   - **Norme IBM AppScan.**
   - **Qualys.**
   - **Chapeau blanc.**
7. Cliquez sur **Update**. Le fichier de mise à jour est importé et la boîte de dialogue Mettre à jour les signatures passe à un format presque identique à celui de la boîte de dialogue Modifier un objet Signatures, décrite dans Configuration ou modification d'un objet Signatures. La boîte de dialogue **Mettre à jour les signatures d'objet** affiche toutes les branches avec des règles de signature nouvelles ou modifiées, des modèles de script d'injection SQL ou intersite et des modèles d'injection XPath, le cas échéant.

8. Vérifiez et configurez les signatures nouvelles et modifiées.
9. Lorsque vous avez terminé, cliquez sur **OK**, puis sur **Fermer**.

Mise à jour automatique de signature

May 5, 2023

La fonctionnalité Signature Auto Update du pare-feu d'application Web permet à l'utilisateur d'obtenir les dernières signatures pour protéger l'application Web contre les nouvelles vulnérabilités. La fonction de mise à jour automatique offre une meilleure protection sans intervention manuelle continue pour obtenir les dernières mises à jour.

Les signatures sont mises à jour automatiquement toutes les heures et ne nécessitent pas de vérification régulière de la disponibilité de la dernière mise à jour. Une fois que vous avez activé la mise à jour automatique des signatures, l'appliance NetScaler se connecte au serveur hébergeant les signatures pour vérifier si une version plus récente est disponible.

Emplacement personnalisable

Les dernières signatures d'Application Firewall sont hébergées sur Amazon, qui est configurée comme URL de signature par défaut pour vérifier la dernière mise à jour.

Toutefois, l'utilisateur a la possibilité de télécharger ces fichiers de mappage de signatures sur son serveur interne. L'utilisateur peut ensuite configurer un chemin d'URL de signature différent pour télécharger les fichiers de mappage de signatures à partir d'un serveur local. Pour que la fonctionnalité de mise à jour automatique fonctionne, vous devrez peut-être configurer le serveur DNS pour accéder au site externe.

Signatures de

Tous les objets de signature définis par l'utilisateur qui sont créés à l'aide de l'objet signature par défaut appfw ont une version supérieure à zéro. Si vous activez la mise à jour automatique des signatures, toutes les signatures sont automatiquement mises à jour.

Si l'utilisateur a importé des signatures au format externe tel que Cenzic ou Qualys, les signatures sont importées avec la version zéro. De même, si l'utilisateur a créé un objet signature à l'aide du modèle vide, il est créé en tant que signature de version zéro. Ces signatures ne sont pas automatiquement mises à jour, car l'utilisateur peut ne pas être intéressé par la surcharge de gestion des signatures par défaut qui ne sont pas utilisées.

Toutefois, le pare-feu d'application Web permet également à l'utilisateur de sélectionner manuellement ces signatures et de les mettre à jour pour ajouter les règles de signature par défaut aux règles

existantes. Une fois les signatures mises à jour manuellement, la version change, puis les signatures seront automatiquement mises à jour avec les autres signatures.

Configurer la mise à jour automatique des signatures

Pour configurer la fonctionnalité de mise à jour automatique des signatures à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set appfw settings SignatureAutoUpdate on
set appfw settings SignatureUrl https://s3.amazonaws.com/
   NSAppFwSignatures/SignaturesMapping.xml
<!--NeedCopy-->
```

Pour configurer la mise à jour automatique des signatures à l'aide de l'interface graphique :

1. Accédez à **Sécurité > NetScaler Web App Firewall > Signatures**.
2. Sélectionnez **Paramètres de mise à jour automatique** dans **Action**.
3. Activez l'option **Mise à jour automatique des signatures** .
4. Vous pouvez spécifier un chemin personnalisé pour l'URL de mise à jour de la signature, si nécessaire. Cliquez sur **Réinitialiser** pour réinitialiser la valeur par défaut `s3.amazonaws.com server`.
5. Cliquez sur **OK**.



Mettre à jour manuellement les signatures

Pour mettre à jour manuellement une signature de version zéro ou toute autre signature définie par l'utilisateur, vous devez d'abord obtenir la dernière mise à jour des signatures par défaut, puis l'utiliser pour mettre à jour la signature définie par l'utilisateur cible.

Exécutez les commandes suivantes à partir de l'interface de ligne de commande pour mettre à jour un fichier de signatures :

```
update appfw signatures "*Default Signatures"
update appfw signatures cenzic  -mergedefault
<!--NeedCopy-->
```

> **Remarque :**
>
> `Default Signatures` Il est sensible à la casse. Cenzic dans la commande précédente est le nom du fichier de signatures mis à jour.

Importer des signatures par défaut sans accès Internet

Il est recommandé de configurer un serveur proxy pour qu'il pointe vers le serveur Amazon (AWS) pour obtenir la dernière mise à jour. Toutefois, si l'appliance NetScaler n'a pas de connexion Internet vers les sites externes, l'utilisateur peut stocker les fichiers de signatures mis à jour sur un serveur local. L'appliance peut ensuite télécharger les signatures à partir du serveur local. Dans ce scénario, l'utilisateur doit constamment vérifier le **site Amazon** pour obtenir les dernières mises à jour. Vous pouvez télécharger et vérifier le fichier de signature par rapport au fichier sha1 correspondant créé à l'aide de la clé **publique Citrix** pour vous protéger contre la falsification.

Pour copier les fichiers Signatures sur un serveur local, procédez comme suit :

1. Créez un répertoire local tel que <MySignatures> sur un serveur local.
2. Ouvrez le site AWS.
3. Copiez le fichier SignaturesMapping.xml dans le dossier <MySignatures>.

Si vous ouvrez le SignaturesMapping.xml fichier, vous pouvez voir tous les fichiers XML pour les signatures et leurs fichiers sha1 correspondants pour les différentes versions prises en charge. Une de ces paires est mise en surbrillance dans la capture d'écran suivante :

1. Créez un sous-répertoire <sigs> dans le <MySignatures> dossier.
2. Copiez toutes les paires de *.xml files listed in the <file> balises et les *.xml.sha1 fichiers répertoriés dans les <sha1> balises correspondantes du SignaturesMapping.xml fichier dans le <sigs> dossier. Voici quelques exemples de fichiers copiés <sigs> dans le dossier :

```
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml.sha1
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml.sha1
```

> **Remarque :**
>
> Vous pouvez donner n'importe quel nom au <MySignatures> dossier et il peut se trouver à n'importe quel emplacement, mais le sous-répertoire <sigs> doit être un sous-répertoire du <MySignatures> dossier dans lequel le fichier de mappage est copié. En outre, assurez-vous que, comme indiqué dans le fichier SignaturesMapping.xml, le nom du sous-répertoire <sigs> doit porter le nom exact et est sensible à la casse. Tous les fichiers Signature et leurs fichiers sha1 correspondants doivent être copiés <sigs> dans ce répertoire.

Après avoir mis en miroir le contenu du serveur Web Amazon hébergé vers le serveur local, modifiez le chemin d'accès au nouveau serveur Web local pour le définir comme URL de signature pour la mise à jour automatique. Par exemple, exécutez la commande suivante à partir de l'interface de ligne de commande de l'appliance :


```
set appfw settings SignatureUrl https://myserver.example.net/
    MySignatures/SignaturesMapping.xml
<!--NeedCopy-->
```

L'opération de mise à jour peut prendre plusieurs minutes, en fonction du nombre de signatures à mettre à jour. Prévoyez suffisamment de temps pour que l'opération de mise à jour soit terminée.

Si vous rencontrez une erreur « Erreur lors de l'accès à l'URL ! » lors de la configuration, suivez les étapes pour le résoudre.

1. Ajoutez l'URL `https://myserver.example.net` pour `/netscaler/ns_gui/admin_ui/php/application/controllers/common/utils.php` que la sécurité CSP (Content Security Policy) ne bloque pas l'accès à l'URL. Veuillez noter que ces paramètres ne persistent pas lors d'une mise à niveau. L'utilisateur doit l'ajouter à nouveau après la mise à niveau.

```
$configuration_view_connect_src = "connect-src 'self' https://app.pendo
    .io https://s3.amazonaws.comhttps://myserver.example.net;";
<!--NeedCopy-->
```

1. L'utilisateur doit configurer le serveur Web de `https://myserver.example.net` manière à ce qu'il réponde aux en-têtes CORS suivants pour `https://myserver.example.net/MySignatures/SignaturesMapping.xml`

```
Access-Control-Allow-Methods: GET
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 3000
<!--NeedCopy-->
```

Directives pour mettre à jour les signatures

Les directives suivantes sont utilisées lors de la mise à jour des signatures :

- Les signatures sont mises à jour lorsque l'URL de mise à jour Signature comporte un objet Signature ayant la même version ou une version plus récente.
- Chaque règle de signature est associée à un ID de règle et à un numéro de version. Pa exemple : `<SignatureRule id="803"version="16"···>`
- La règle de signature du fichier Signatures entrantes portant le même ID et le même numéro de version que le fichier existant est ignorée même si elle comporte des modèles ou une chaîne de journal différents.
- Une règle de signature avec un nouvel identifiant est ajoutée. Toutes les actions et l'indicateur activé sont utilisés à partir du nouveau fichier.

> **Remarque :**
>
> Vous devez consulter régulièrement les signatures mises à jour pour activer les règles récemment ajoutées et modifier les autres paramètres d'action conformément aux exigences de l'application.

- Les règles portant le même ID mais avec un numéro de version plus récent remplacent celui existant. Toutes les actions et l'indicateur activé de la règle existante sont conservés.

> **Conseil :**
>
> Lorsque vous mettez à jour les signatures de l'interface de ligne de commande, vous devez d'abord mettre à jour les signatures par défaut. Vous devez ensuite ajouter des commandes de mise à jour pour mettre à jour chaque fichier de signatures personnalisé basé sur les signatures par défaut. Si vous ne mettez pas à jour les signatures par défaut en premier, une erreur de non-correspondance de version empêche la mise à jour du fichier de signatures personnalisées.

Activation automatique des nouvelles signatures

À partir de la version 13.1 buid 27.x et versions ultérieures, vous pouvez sélectionner **Activer automatiquement les nouvelles signatures** pour autoriser l'activation automatique des nouvelles règles de signature WAF par défaut après une mise à jour.

Activation automatique des nouvelles signatures via l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Signatures**.
2. Sélectionnez une signature et cliquez sur **Modifier**.
3. Sélectionnez **Activer automatiquement les nouvelles signatures**.



Activer automatiquement les nouvelles signatures à l'aide de l'interface

À l'invite de commande, tapez :

```
import appfw signatures <src> <name> [-xslt <string>] [-comment <string>]
[-overwrite] [-merge [-preservedefactions]] [-sha1 <string>] [-VendorType
Snort] [-autoEnableNewSignatures ( ON | OFF )]
```

Exemple :

```
import signatures http://www.example.com/ns/signatures.xml my-signature -
autoEnableNewSignatures ON
```

Intégration des règles Snort

May 5, 2023

Face aux attaques malveillantes visant les applications Web, il est important de protéger votre réseau interne. Les données malveillantes affectent non seulement vos applications Web au niveau de l'interface, mais les paquets malveillants atteignent également la couche application. Pour surmonter ces attaques, il est important de configurer un système de détection et de prévention des intrusions qui examine votre réseau interne.

Les règles Snort sont intégrées à l'appliance pour examiner les attaques malveillantes dans les paquets de données au niveau de la couche application. Vous pouvez télécharger les règles de sniffage et les convertir en règles de signature WAF. Les signatures sont configurées selon des règles capables de détecter les activités malveillantes telles que les attaques DOS, les dépassements de mémoire tampon, les scans furtifs des ports, les attaques CGI, les sondes SMB et les tentatives d'empreinte digitale du système d'exploitation. En intégrant les règles Snort, vous pouvez renforcer votre solution de sécurité au niveau de l'interface et de l'application.

Configurer les règles de raccourcissement

La configuration commence par le téléchargement des règles Snort, puis par leur importation dans les règles de signature WAF. Une fois que vous avez converti les règles en signatures WAF, elles peuvent être utilisées comme contrôles de sécurité WAF. Les règles de signature basées sur Snort examinent le paquet de données entrant afin de détecter toute attaque malveillante sur votre réseau.

Un nouveau paramètre, « VendorType », est ajouté à la commande d'importation pour convertir les règles Snort en signatures WAF.

Le paramètre « VendorType » est défini sur SNORT uniquement pour les règles Snort.

Téléchargez les règles Snort à l'aide de l'interface de commande

Vous pouvez télécharger les règles de Snort sous forme de fichier texte à partir de l'URL ci-dessous :

```
https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
```

Importez les règles Snort à l'aide de l'interface de commande

Après le téléchargement, vous pouvez importer les règles Snort dans votre appliance.

À l'invite de commande, tapez :

```
import appfw signatures <src> <name> [-xslt <string>] [-comment <string>]
[-overwrite] [-merge [-preservedefactions]] [-sha1 <string>] [-VendorType
Snort]
```

Exemple :

```
import appfw signatures http://www.example.com/ns/signatures.xml sig-snort -
comment "signatures from snort rules" -VendorType snort
```

Arguments :

Src. URL (protocole, hôte, chemin et nom de fichier) correspondant à l'emplacement où stocker l'objet de signatures importé.

> **Remarque :**
>
> L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite une authentification par certificat client pour y accéder. Argument obligatoire de longueur maximale : 2047

Nom. Nom à attribuer à l'objet de signatures sur NetScaler. Argument obligatoire de longueur maximale : 31

Commentaire. Description de la manière de conserver les informations relatives à l'objet de signatures. Longueur maximale : 255
réécritures. Remplacez tous les objets de signatures existants portant le même nom.

Fusionner. Fusionne la signature existante avec les nouvelles règles de signature.

Défactions préservées. Préserve les actions définies des règles de signature.

Type de fournisseur. Fournisseur tiers chargé de générer les signatures WAF. Valeurs possibles : Snort.

Configuration des règles de sniffage à l'aide de l'interface graphique NetScaler

La configuration de l'interface graphique pour les règles Snort est similaire à celle d'autres scanners d'applications Web externes tels que Cenzic, Qualys, Whitehat.

Suivez les étapes ci-dessous pour configurer Snort :

1. Accédez à **Configuration > Sécurité > NetScaler Web App Firewall > Signatures**.
2. Sur la page **Signatures**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter des signatures**, définissez les paramètres suivants pour configurer les règles de Snort.
   a) Format de fichier. Sélectionnez le format de fichier comme externe.
   b) Importer depuis. Sélectionnez l'option d'importation sous forme de fichier de sniff ou d'URL pour saisir l'URL.
   c) Fournisseur de Snort V3. Cochez la case pour importer les règles Snort à partir d'un fichier ou d'une URL.
4. Cliquez sur **Ouvrir**.



L'appliance importe les règles Snort sous forme de règles de signature WAF basées sur Snort.



La meilleure pratique consiste à utiliser des actions de filtrage pour activer les règles de sniffage que vous préférez importer sous forme de règles de signature WAF sur l'appliance.



5. Pour confirmer, cliquez sur **Yes**.



6. Les règles sélectionnées sont activées sur l'appliance.



7. Cliquez sur **OK**.

Exportation d'un objet de signatures vers un fichier

May 5, 2023

Vous exportez un objet de signatures vers un fichier afin de pouvoir l'importer dans un autre NetScaler.

Pour exporter un objet de signatures vers un fichier

1. Accédez à **Sécurité > NetScaler Web App Firewall > Signatures**.
2. Dans le volet de détails, sélectionnez l'objet de signatures que vous souhaitez configurer.
3. Dans la liste déroulante **Actions**, sélectionnez **Exporter**.

4. Dans la boîte de dialogue **Exporter l'objet de signatures**, zone de texte **Fichier local**, tapez le chemin et le nom du fichier vers lequel vous souhaitez exporter l'objet de signatures, ou utilisez la boîte de dialogue **Parcourir** pour désigner un chemin et un nom.
5. Cliquez sur **OK**.

Modifier les signatures pour ajouter ou modifier des règles

May 5, 2023

Vous pouvez modifier les signatures définies par l'utilisateur pour ajouter ou modifier une règle. Une règle de signature locale possède les mêmes attributs qu'une règle de signature par défaut de Citrix, et elle fonctionne de la même manière. Vous l'activez ou la désactivez et configurez les actions de signature pour elle, comme vous le faites pour une signature par défaut.

Ajoutez une règle locale si vous devez protéger vos sites Web et services contre une attaque connue à laquelle les signatures existantes ne correspondent pas. Par exemple, vous pouvez découvrir un nouveau type d'attaque et déterminer ses caractéristiques en examinant les journaux de votre serveur Web, ou vous pouvez obtenir des informations tierces sur un nouveau type d'attaque.

Au cœur d'une règle de signature se trouvent les *modèles*de règles, qui décrivent collectivement les caractéristiques de l'attaque auxquelles la règle est censée correspondre. Chaque modèle peut consister en une chaîne simple, une expression régulière au format PCRE ou les modèles intégrés d'injection SQL ou de script intersite.

Vous souhaiterez peut-être modifier une règle de signature en ajoutant un nouveau modèle ou en modifiant un modèle existant pour qu'il corresponde à une attaque. Par exemple, vous pouvez découvrir les modifications apportées à une attaque, ou vous pouvez déterminer un meilleur modèle en examinant les journaux de votre serveur Web ou en consultant des informations provenant de tiers.

Ajouter ou modifier une règle de signature locale

1. Accédez à **Sécurité > NetScaler Web App Firewall > Signatures**.
2. Dans le volet d'informations, sélectionnez les signatures définies par l'utilisateur que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la section **Règles de signature**, cliquez sur **Ajouter**. Le volet **Règle de signature** s'affiche.
4. Configurez les actions relatives à une signature en cochant les cases appropriées.
    - **Activé.** Active la nouvelle règle de signature. Si vous ne sélectionnez pas cette option, cette nouvelle règle de signature est ajoutée à votre configuration, mais elle est inactive.
    - **Bloquer.** Bloque les connexions qui enfreignent cette règle de signature.

- **Bûche.** Consigne les violations de cette règle de signature dans le journal NetScaler.
- **État.** Inclut les violations de cette règle de signature dans les statistiques.
- **Remove.** Supprime de la réponse les informations qui correspondent à la règle de signature. (S'applique uniquement aux règles de réponse.)
- **Sortie X.** Masque les informations qui correspondent à la règle de signature par la lettre X. (S'applique uniquement aux règles de réponse.)
- **Autorisez les doublons.** Autorise les doublons de cette règle de signature dans cet objet de signature.

5. Choisissez une catégorie pour la nouvelle règle de signature dans la liste déroulante **Catégorie**.

   Si vous souhaitez créer une catégorie, cliquez sur **Ajouter**. Pour plus d'informations, voir Ajouter une catégorie de règles de signature.

6. Dans la zone de texte **LogString**, tapez une brève description de la règle de signature à utiliser dans les journaux.

7. Dans la zone de texte **Commentaire**, tapez un commentaire. (Facultatif)

8. Cliquez sur **Plus** pour modifier les options avancées.

   a) Pour supprimer les commentaires HTML avant d'appliquer cette règle de signature, dans la liste déroulante Slot Commentaires, choisissez Tout ou Exclure la balise de script.
   b) Pour configurer la vérification de l'en-tête de référence CSRF, dans le tableau de boutons radio de vérification de l'en-tête de référence CSRF, sélectionnez le bouton radio Si présent ou Toujours.
   c) Pour modifier manuellement l'ID de règle affecté à cette règle de signature locale, modifiez le numéro dans la zone de texte ID de règle. L'ID doit être un entier positif compris entre 1000000 et 1999999 qui n'a pas encore été attribué à une règle de signature locale.
   d) Pour attribuer un numéro de version à la nouvelle règle de signature, modifiez le numéro dans la zone de texte Numéro de version.
   e) Pour attribuer un identifiant source, modifiez la chaîne dans la zone de texte ID source.
   f) Pour spécifier la source, choisissez Local ou Snort dans la liste déroulante Source, ou cliquez sur l'icône Ajouter à droite de la liste et ajoutez une nouvelle source.
   g) Pour attribuer un score de préjudice aux violations de cette règle de signature locale, tapez un nombre compris entre 1 et 10 dans la zone de texte Harm Score.
   h) Pour attribuer un niveau de gravité à cette règle de signature locale, dans la liste déroulante Gravité, choisissez Élevé, Moyen ou Faible, ou cliquez sur l'icône Ajouter à droite de la liste et ajoutez un nouveau niveau de gravité.
   i) Pour attribuer un type de violation à cette règle de signature locale, dans la liste déroulante Type, choisissez Vulnérable ou Avertissement, ou cliquez sur l'icône Ajouter à droite de la liste et ajoutez un nouveau type de violation.

9. Dans **Modèles de règles**, cliquez sur **Ajouter** pour ajouter un modèle. Vous pouvez également

modifier les modèles existants. Pour ce faire, cliquez sur **Modifier**.

Pour plus d'informations sur l'ajout ou la modification de modèles, voir Modèles de règles de signature.

10. Cliquez sur **OK**.

Ajouter une catégorie de règles de signature

Le classement des règles de signature dans une catégorie vous permet de configurer les actions pour un groupe de signatures plutôt que pour chaque signature individuelle. Vous souhaiterez peut-être le faire pour les raisons suivantes :

- **Facilité de sélection** Supposons, par exemple, que toutes les règles de signature d'un groupe particulier protègent contre les attaques visant un type spécifique de logiciel ou de technologie de serveur Web. Si vos sites Web protégés utilisent ce logiciel ou cette technologie, vous devez tous les activer. Si ce n'est pas le cas, vous ne souhaitez activer aucun d'entre eux.
- **Facilité de configuration initiale.** Il est plus facile de définir les valeurs par défaut pour un groupe de signatures en tant que catégorie, plutôt qu'une par une. Vous pouvez ensuite apporter les modifications nécessaires aux signatures individuelles.
- **Facilité de configuration continue.** Il est plus facile de configurer les signatures si vous pouvez afficher uniquement celles qui répondent à des critères spécifiques, tels que l'appartenance à une catégorie spécifique.

Ajouter des modèles de règles de signature

May 5, 2023

Vous pouvez ajouter un modèle ou modifier un modèle existant pour spécifier une chaîne ou une expression qui caractérise une attaque si la signature correspond. Pour détecter les tendances d'une attaque, vous pouvez consulter les journaux de votre serveur Web. Vous pouvez utiliser un outil pour observer les données de connexion en temps réel, ou obtenir la chaîne ou l'expression à partir d'un rapport tiers concernant l'attaque.

> **Important**
>
> Un nouveau modèle que vous ajoutez à une règle de signature est dans une relation ET avec les modèles existants. N'ajoutez pas de modèle à une règle de signature existante si vous ne souhaitez pas qu'une attaque potentielle doive correspondre à tous les modèles correspondant à la signature.

Chaque modèle peut consister en une chaîne simple, une expression régulière au format PCRE ou le modèle intégré d'injection SQL ou de script intersite. Avant d'essayer d'ajouter un modèle basé sur

une expression régulière, vous devez vous assurer que vous comprenez les expressions régulières au format PCRE. Les expressions PCRE sont complexes et puissantes. Si vous ne comprenez pas comment ils fonctionnent, vous pouvez créer involontairement un modèle qui correspond à quelque chose que vous ne vouliez pas (un *faux positif*) ou qui ne correspond pas à ce que vous vouliez (un *faux négatif*).

Modèle de signature personnalisé pour les types de contenu autres que ceux par défaut

Le NetScaler Web App Firewall (WAF) prend désormais en charge un nouvel emplacement pour inspecter le contenu canonisé. Par défaut, WAF ne bloque pas la charge utile codée avec des types de contenu autres que ceux par défaut. Lorsque ces types de contenu figurent sur la liste blanche et qu'aucune action configurée n'est appliquée, le contrôle de protection contre les scripts SQL et intersites ne filtre pas les attaques par script SQL ou intersite dans les charges utiles codées. Pour résoudre ce problème, un utilisateur peut créer une règle de signature personnalisée avec ce nouvel emplacement (HTTP_CANON_POST_BODY) qui examine les charges utiles codées pour les types de contenu autres que ceux par défaut et, en cas d'attaque SQL ou de script intersite, bloque le trafic après la canonisation du corps de la publication.

> **Remarque :**
>
> Cette prise en charge s'applique uniquement aux requêtes HTTP.

Si vous n'êtes pas déjà familiarisé avec les expressions régulières au format PCRE, vous pouvez utiliser les ressources suivantes pour en savoir plus ou pour obtenir de l'aide concernant un problème spécifique :

- « Mastering Regular Expressions », troisième édition. Copyright (c) 2006 par Jeffrey Friedl. O'Reilly Media, ISBN : 9780596528126.
- « Livre de recettes sur les expressions régulières ». Copyright (c) 2009 par Jan Goyvaerts et Steven Levithan. O'Reilly Media, ISBN : 9780596520687
- Page de manuel/Spécification du PCRE
- Page d'accueil/spécification PCRE
- Entrée PCRE de Wikipédia
- Liste de diffusion PCRE

Si vous devez coder des caractères non ASCII dans une expression régulière au format PCRE, la plateforme NetScaler prend en charge le codage de codes UTF-8 hexadécimaux. Pour plus d'informations, voir Format de codage de caractères PCRE.

Configuration d'un modèle de règles de signature

Lorsque vous modifiez une signature, vous pouvez ajouter ou modifier le modèle de règles. Pour ajouter ou modifier les règles de signature, voir Modifier les signatures pour ajouter ou modifier des règles.

- **Type** : sélectionnez le type de connexion auquel le modèle est censé correspondre.
  - **Requête** : elle correspond aux éléments ou fonctionnalités de la demande tels que le code SQL injecté, les attaques contre les formulaires Web, les scripts intersites ou les URL inappropriées.
  - **Réponse** : elle correspond aux éléments ou caractéristiques de la réponse tels que les numéros de carte de crédit ou les objets sécurisés.
- **Emplacement** - Sélectionnez une **zone** à examiner à l'aide de ce modèle. La zone décrit les éléments de la requête ou de la réponse HTTP à examiner pour ce modèle. En fonction du type de motif sélectionné, les options apparaissent dans la liste des **zones**. Elles dépendent du type de motif choisi.

  Pour le type de modèle de **demande**, les éléments relatifs aux requêtes HTTP apparaissent.
  - **HTTP_N' IMPORTE QUEL**. Toutes les parties de la connexion HTTP.
  - **HTTP_COOKIE**. Tous les cookies figurant dans les en-têtes de requête HTTP après toute transformation de cookie.

    > **Remarque**
    >
    > Ne recherche pas les en-têtes « Set-Cookie : » de la réponse HTTP.
  - **CHAMP HTTP_FORM_FIELD**. Les champs de formulaire et leur contenu, après le décodage de l'URL, le pourcentage de décodage et la suppression des espaces blancs excédentaires. Vous pouvez utiliser la `<Location>` balise pour restreindre davantage la liste des noms de champs de formulaire dans lesquels la recherche doit être effectuée.
  - **HTTP_HEADER**. Portions de valeur de l'en-tête HTTP après toute transformation de script intersite ou de décodage d'URL.
  - **HTTP_METHODE**. La méthode de requête HTTP.
  - **URL HTTP**. Portion de valeur de l'URL dans les en-têtes HTTP, à l'exclusion de tout port de requête ou de fragment, après conversion au jeu de caractères UTF-*, décodage de l'URL, suppression des espaces et conversion des URL relatives en URL absolues. N'inclut pas le décodage des entités HTML.
  - URL D'**ORIGINE HTTP.** URL d'origine d'un formulaire Web.
  - **HTTP_POST_BODY**. Le corps du message HTTP et les données du formulaire Web qu'il contient.

- **HTTP_RAW_COOKIE**. Tous les cookie de requête HTTP, y compris la partie du nom « Cookie : ».
  Remarque : ne recherche pas les en-têtes « Set-Cookie : » des réponses HTTP.
- **HTTP_RAW_HEADER**. L'en-tête HTTP complet, avec les en-têtes individuels séparés par des caractères de ligne (\ n) ou des chaînes de retour/d'alimentation en ligne (\ r \ n).

Pour le type de **réponse**, les éléments relatifs aux réponses HTTP apparaissent.

- **HTTP_RAW_RESP_HEADER**. L'intégralité de l'en-tête de réponse, y compris les parties nom et valeur de l'en-tête de réponse une fois la transformation de l'URL effectuée, et l'état complet de la réponse. Comme pour HTTP_RAW_HEADER, les en-têtes individuels sont séparés par des caractères d'entrée de ligne (\ n) ou des chaînes de retour de carrière/d'alimentation en ligne (\ r \ n).
- **HTTP_RAW_SET_COOKIE**. L'intégralité de l'en-tête Set-Cookie après toute transformation d'URL

  > **Remarque**
  >
  > La transformation d'URL peut modifier à la fois les parties de domaine et de chemin de l'en-tête Set-Cookie.

- **HTTP_RAW_URL**. L'URL complète de la demande avant toute transformation d'URL, y compris les parties de la requête ou du fragment.
- **HTTP_RESP_HEADER**. La partie valeur des en-têtes de réponse complets après toute transformation d'URL.
- **HTTP_RESP_BODY**. Le corps de la réponse HTTP
- **HTTP_SET_COOKIE**. Tous les en-têtes « Set-Cookie » dans les en-têtes de réponse HTTP.
- **HTTP_STATUS_CODE**. Le code d'état HTTP.
- **MESSAGE D'ÉTAT HTTP**. Le message d'état HTTP.

Lorsque vous sélectionnez une option **dans la liste des zones**, les options de la zone sélectionnée sont modifiées de manière dynamique.

- **N'importe lequel.** Vérifie les noms de champs ou les URL.
- **Littéral**. Vérifie les noms de champs ou les URL qui contiennent une chaîne littérale. Une fois que vous avez sélectionné Literal, une zone de texte s'affiche. Tapez la chaîne littérale souhaitée dans la zone de texte.
- **PCRE.** Vérifie les noms de champs ou les URL qui correspondent à une expression régulière au format PCRE. Une fois que vous avez sélectionné ce choix, la fenêtre d'expression régulière s'affiche. Tapez l'expression régulière dans la fenêtre. Vous pouvez utiliser les **jetons Regex** pour insérer des éléments d'expression régulière courants au niveau du curseur, ou vous pouvez cliquer sur Regex Editor pour afficher la boîte de

dialogue de l'éditeur d'expressions régulières, qui fournit une assistance supplémentaire pour créer l'expression régulière souhaitée.

- **Expression** : Vérifie les noms de champs ou les URL qui correspondent à une expression par défaut de NetScaler.

- **Motif** : un modèle est une chaîne littérale ou une expression régulière au format PCRE qui définit le modèle auquel vous souhaitez faire correspondre. Sélectionnez le type de **correspondance** dans la liste.
  - **Littéral**. Une chaîne littérale.
  - **PCRE.** Expression régulière au format PCRE.

    > **Remarque**
    >
    > Lorsque vous choisissez PCRE, les outils d'expression régulière situés sous la fenêtre Pattern sont activés. Ces outils ne sont pas utiles pour la plupart des autres types de motifs.

  - **Expression** : Une expression dans le langage d'expressions par défaut de NetScaler est le même langage d'expression que celui utilisé pour créer des politiques de Web App Firewall sur l'appliance NetScaler. Bien que le langage d'expressions NetScaler ait été initialement développé pour les règles de politique, il s'agit d'un langage à usage général très flexible qui peut également être utilisé pour définir un modèle de signature.

    Lorsque vous choisissez Expression, l'éditeur d'expressions NetScaler apparaît sous la fenêtre Pattern. Pour plus d'informations sur l'éditeur d'expression et des instructions sur son utilisation, reportez-vous à la section Pour ajouter une règle de pare-feu (expression) à l'aide de la boîte de dialogue Ajouter une expression.
  - **Injection SQL**. Indique au Web App Firewall de rechercher le code SQL injecté à l'emplacement spécifié.
  - **Scripting intersite**. Demande au Web App Firewall de rechercher des scripts intersites à l'emplacement spécifié.
  - **Injection de commandes.** Demande au NetScaler Web App Firewall de rechercher toutes les commandes malveillantes injectées à l'emplacement spécifié.
  - Grammaire de l'**injection SQL.** Demande au NetScaler Web App Firewall de rechercher la grammaire SQL injectée à l'emplacement spécifié. Surtout lorsque des mots couramment utilisés tels que `Select` et `From` sont utilisés dans une requête HTTP.
  - Grammaire de l'injection de**commandes.** Demande au NetScaler Web App Firewall de rechercher la grammaire des commandes malveillantes injectées à l'emplacement spécifié. Surtout lorsqu'un mot couramment utilisé tel que « Exit » est utilisé dans une requête HTTP.

Si vous souhaitez configurer d'autres paramètres, spécifiez les éléments suivants :

- **Décalage**. Le nombre de caractères à ignorer avant de commencer à correspondre sur ce modèle. Vous utilisez ce champ pour commencer à examiner une chaîne à un moment autre que le premier caractère.
- **Profondeur**. Combien de caractères à partir du point de départ doivent être examinés pour trouver des correspondances. Ce champ permet de limiter les recherches d'une grande chaîne à un certain nombre de caractères.
- **Longueur minimale**. La chaîne à rechercher doit avoir au moins le nombre d'octets spécifié. Les chaînes plus courtes ne correspondent pas.
- **Longueur maximale**. La chaîne à rechercher ne doit pas dépasser le nombre d'octets spécifié. Les chaînes plus longues ne correspondent pas.
- **Méthode de recherche**. Une case à cocher étiquetée `fastmatch`. Vous ne pouvez l'activer `fastmatch` que pour un modèle littéral, afin d'améliorer les performances.

> **Remarque**
>
> Vos modifications ne sont pas enregistrées tant que vous n'avez pas cliqué sur **OK** dans le volet **Signature Rule Pattern** . Ne fermez aucune de ces boîtes de dialogue sans cliquer sur **OK**, sauf si vous souhaitez annuler vos modifications.

Pour importer et fusionner des règles

May 5, 2023

Lorsque vous utilisez l'éditeur de signature pour effectuer une opération d'importation et de fusion à partir de l'interface graphique, vous pouvez désormais voir les règles nouvelles, mises à jour, dupliquées et non valides.

L'éditeur de signature affiche les quatre nouvelles lignes suivantes :

1. Nouvelles règles
2. Règles mises à jour
3. Règles dupliquées
4. Règles non valides

Le résultat des filtres Nouvelles règles uniquement et Règles mises à jour uniquement apparaît également dans le volet des filtres de catégorie de la fenêtre d'édition de l'éditeur de signatures.

Vous devrez importer les fichiers depuis l'interface graphique pour voir les liens correspondants aux règles nouvelles, dupliquées, non valides et mises à jour.

Procédure d'importation des règles de signature :

1. Dans l'interface graphique Web de NetScaler, accédez à **Configuration > Sécurité > Signatures du pare-feu NetScaler Web App.** Dans la fenêtre Signatures, cliquez sur **Ajouter**. Ensuite, sélectionnez **Format de fichier** > **Natif**, **Importer de** > **URL** et dans le champ URL, ajoutez le lien ci-dessus. Si vous ne parvenez pas à accéder à l'URL, vous pouvez télécharger les données XML.
2. Après avoir cliqué sur **Ouvrir**, le fichier de signature s'ouvre et vous pouvez voir des liens pour la nouvelle règle et les règles non valides.
3. Si vous importez une règle de signature de3rd partie, vous pouvez voir 90 nouvelles règles et 9 règles en double dans le fichier .xml importé. Si vous ne parvenez pas à accéder à l'URL, vous pouvez télécharger les données XML.

Mises à jour de signature dans le déploiement et les mises à niveau de génération haute disponibilité

January 21, 2021

La mise à jour de signature se produit sur le nœud principal. Pendant que les signatures sont mises à jour sur le nœud principal, les fichiers mis à jour sont simultanément synchronisés avec le nœud secondaire.

La signature par défaut est toujours mise à jour en premier, puis le reste des signatures définies par l'utilisateur est mis à jour.

Connexion à Amazon AWS

La route par défaut NSIP est utilisée pour se connecter à Amazon AWS. S'il existe un scénario d'utilisation spécifique dans lequel SNIP est utilisé, et s'il existe plusieurs SNIP, le premier à recevoir la réponse ARP du site d'hébergement contiendra l'itinéraire.

Mises à jour de signature pendant les mises à niveau de version

Dans le cas d'une mise à niveau, si le NS dispose d'une version de base plus ancienne pour les signatures, *La signature par défaut est automatiquement mise à jour si une version de signature plus récente est disponible.

Si le schéma a changé, la version de schéma de tous les objets de signature est mise à jour lors de la mise à niveau de la version.

Toutefois, pour la version de base des signatures définies par l'utilisateur, le comportement est différent dans la version 10.5 par rapport à la version 11.0.

Dans la version 10.5, seule la signature par défaut a été mise à jour et la version de base du reste des signatures est restée inchangée après la mise à niveau de génération.

Dans la version 11.0, ce comportement a changé. Lorsque l'appliance est mise à niveau pour installer une nouvelle version, non seulement l'objet signature *Default, mais toutes les autres signatures définies par l'utilisateur qui existent actuellement dans l'appliance sont également mises à jour et auront la même version après la mise à niveau de la version.

Dans les versions 10.5 et 11.0, si la mise à jour automatique est configurée, les signatures *Default ainsi que toutes les signatures de version non nulle sont automatiquement mises à jour vers la dernière version de signature publiée et auront la même version de base.

Vue d'ensemble des contrôles de sécurité

August 20, 2021

Les protections avancées du pare-feu Web App Firewall (contrôles de sécurité) sont un ensemble de filtres conçus pour détecter les attaques complexes ou inconnues sur vos sites Web et services Web protégés. Les contrôles de sécurité utilisent des techniques heuristiques, une sécurité positive et d'autres techniques pour détecter les attaques qui ne peuvent pas être détectées uniquement par les signatures. Vous configurez les vérifications de sécurité en créant et en configurant un profil de Web App Firewall, qui est un ensemble de paramètres définis par l'utilisateur qui indiquent au pare-feu Web App les vérifications de sécurité à utiliser et comment gérer une demande ou une réponse qui échoue une vérification de sécurité. Un profil est associé à un objet signatures et à une stratégie pour créer une configuration de sécurité.

Le pare-feu des applications Web fournit vingt contrôles de sécurité, qui diffèrent considérablement par le type d'attaque qu'ils ciblent et la complexité de leur configuration. Les contrôles de sécurité sont organisés selon les catégories suivantes :

- **Contrôles de sécurité communs.** Les contrôles qui s'appliquent à tout aspect de la sécurité Web qui n'implique pas de contenu ou s'appliquent également à tous les types de contenu.
- **Vérifications de sécurité HTML.** Vérifications qui examinent les demandes et les réponses HTML. Ces vérifications s'appliquent aux sites Web HTML et aux parties HTML des sites Web 2.0, qui contiennent des contenus HTML et XML mixtes.
- **Vérifications de sécurité XML.** Vérifications qui examinent les demandes et les réponses XML. Ces vérifications s'appliquent aux services Web XML et aux parties XML des sites Web 2.0.

Les contrôles de sécurité protègent contre un large éventail de types d'attaques, y compris les attaques contre les vulnérabilités logicielles du système d'exploitation et du serveur Web, les vulnérabilités de base de données SQL, les erreurs dans la conception et le codage des sites Web et des services Web, et les échecs de sites sécurisés qui hébergent ou peuvent accéder à des informations sensibles.

Toutes les vérifications de sécurité ont un ensemble d'options de configuration, les actions de vérification, qui contrôlent la façon dont le Web App Firewall gère une connexion correspondant à une vérification. Trois actions de vérification sont disponibles pour toutes les vérifications de sécurité. Ils sont :

- **Bloc.** Bloquer les connexions qui correspondent à la signature. Désactivé par défaut.
- **Journal.** Enregistrer les connexions qui correspondent à la signature, pour une analyse ultérieure. Activé par défaut.
- **Statistiques.** Tenir à jour des statistiques, pour chaque signature, indiquant le nombre de connexions correspondant et fournissant d'autres informations sur les types de connexions bloquées. Désactivé par défaut.

Une quatrième action de vérification, **Apprendre**, est disponible pour plus de la moitié des actions de vérification. Il observe le trafic vers un site Web protégé ou un service Web et utilise des connexions qui violent à plusieurs reprises la vérification de sécurité pour générer des exceptions recommandées (relaxations) à la vérification, ou de nouvelles règles pour la vérification. Outre les actions de vérification, certaines vérifications de sécurité ont des paramètres qui contrôlent les règles utilisées par la vérification pour déterminer quelles connexions ne respectent pas cette vérification ou qui configurent la réponse du pare-feu Web App aux connexions qui violent la vérification. Ces paramètres sont différents pour chaque vérification, et ils sont décrits dans la documentation de chaque vérification.

Pour configurer les contrôles de sécurité, vous pouvez utiliser l'assistant Web App Firewall, comme décrit dans l'Assistant Web App Firewall, ou vous pouvez configurer les contrôles de sécurité manuellement, comme décrit dans Configuration manuelle à l'aide de l'interface graphique. Certaines tâches, telles que la saisie manuelle de relaxations ou de règles ou l'examen des données apprises, ne peuvent être effectuées qu'à l'aide de l'interface graphique, et non de la ligne de commande. L'utilisation de l'assistant est généralement la meilleure méthode de configuration, mais dans certains cas, la configuration manuelle peut être plus facile si vous êtes bien familier avec lui et que vous voulez simplement ajuster la configuration pour une seule vérification de sécurité.

Quelle que soit la méthode que vous utilisez pour configurer les vérifications de sécurité, chaque vérification de sécurité nécessite l'exécution de certaines tâches. De nombreuses vérifications nécessitent que vous spécifiez des exceptions (relaxations) pour empêcher le blocage du trafic légitime avant d'activer le blocage pour cette vérification de sécurité. Vous pouvez le faire manuellement, en observant les entrées du journal après un certain volume de trafic a été filtré, puis en créant les exceptions nécessaires. Cependant, il est généralement beaucoup plus facile d'activer la fonctionnalité d'apprentissage et de la laisser observer le trafic et recommander les exceptions nécessaires.

Le Web App Firewall utilise des moteurs de paquets (PE) pendant le traitement des transactions. Chaque moteur de paquets a une limite de 100 000 sessions, ce qui est suffisant pour la plupart des scénarios de déploiement. Toutefois, lorsque le Web App Firewall traite un trafic important et que le délai d'expiration de session est configuré à une valeur plus élevée, les sessions peuvent être accumulées. Si le nombre de sessions actives de Web App Firewall dépasse la limite de 100 000 par PE, les viola-

tions de vérification de sécurité du pare-feu Web App peuvent ne pas être envoyées à l'appliance Security Insight. La réduction du délai d'expiration de session à une valeur plus petite, ou l'utilisation du mode sans session pour les vérifications de sécurité avec fermeture d'URL sans session ou cohérence de champ sans session peut aider à empêcher l'accumulation des sessions. Si cette option n'est pas viable dans les scénarios où les transactions peuvent nécessiter des sessions plus longues, la mise à niveau vers une plate-forme supérieure avec plus de moteur de paquets est recommandée.

La prise en charge de AppFirewall mis en cache est ajoutée, et le paramètre de session maximale via l'interface de ligne de commande par cœur est défini sur 50 000 sessions.

Protections de haut niveau

May 5, 2023

Quatre des protections du Web App Firewall sont particulièrement efficaces contre les types courants d'attaques Web et sont donc plus couramment utilisées que les autres. Ils sont :

- **Scripting intersite HTML.** Examine les demandes et les réponses des scripts qui tentent d'accéder au contenu ou de le modifier sur un site Web différent de celui sur lequel se trouve le script. Lorsque cette vérification détecte un tel script, elle le rend inoffensif avant de transférer la requête ou la réponse à sa destination, ou elle bloque la connexion.
- **Injection HTML SQL.** Examine les demandes contenant des données de champs de formulaire pour les tentatives d'injection de commandes SQL dans une base de données SQL. Lorsque cette vérification détecte du code SQL injecté, elle bloque la requête ou rend le code SQL injecté inoffensif avant de transférer la demande au serveur Web.

  Remarque : Si les deux conditions suivantes s'appliquent à votre configuration, vous devez vous assurer que votre Web App Firewall est correctement configuré :

  - Si vous activez la vérification des scripts intersites HTML ou la vérification de l'injection SQL HTML (ou les deux), et
  - Vos sites Web protégés acceptent les téléchargements de fichiers ou contiennent des formulaires Web qui peuvent contenir des données corporelles POST volumineuses.

  Pour plus d'informations sur la configuration du Web App Firewall pour gérer ce cas, reportez-vous à la section Configuration du pare-feu d'application.
- **Dépassement de mémoire tampon.** Examine les demandes visant à détecter les tentatives visant à provoquer un dépassement de la mémoire tampon sur le serveur Web.
- **Cohérence des cookies.** Examine les cookies renvoyés avec les demandes des utilisateurs afin de vérifier qu'ils correspondent aux cookies que votre serveur Web a définis pour cet utilisateur.

Si un cookie modifié est trouvé, il est retiré de la demande avant que la demande soit transférée au serveur Web.

La vérification du Buffer Overflow est simple ; vous pouvez généralement activer son blocage immédiatement. Les trois autres contrôles de haut niveau sont considérablement plus complexes et nécessitent une configuration avant de pouvoir les utiliser en toute sécurité pour bloquer le trafic. NetScaler recommande vivement, plutôt que d'essayer de configurer ces vérifications manuellement, d'activer la fonctionnalité d'apprentissage et de lui permettre de générer les exceptions nécessaires.

Vérification des scripts intersites HTML

May 5, 2023

La vérification Script intersite HTML (script intersite) examine à la fois les en-têtes et les corps POST des requêtes utilisateur pour détecter d'éventuelles attaques de script intersite. S'il trouve un script intersite, il modifie (*transforme*) la demande pour rendre l'attaque inoffensive ou bloque la demande.

> **Remarque :**
>
> La vérification Script intersite HTML (script intersite) fonctionne uniquement pour le type de contenu, la longueur du contenu, etc. Assurez-vous également que l'option « CheckRequestHeaders » est activée dans votre profil de pare-feu d'application Web.

Vous pouvez empêcher l'utilisation abusive des scripts sur vos sites Web protégés en utilisant les scripts de script intersite HTML qui enfreignent la *même règle d'origine*, qui stipule que les scripts ne doivent pas accéder au contenu ni le modifier sur aucun serveur, sauf le serveur sur lequel ils se trouvent. Tout script qui enfreint la même règle d'origine est appelé script intersite, et la pratique consistant à utiliser des scripts pour accéder ou modifier du contenu sur un autre serveur est appelée script intersite. La raison pour laquelle les scripts intersites constituent un problème de sécurité est qu'un serveur Web qui autorise le script intersite peut être attaqué à l'aide d'un script qui ne se trouve pas sur ce serveur Web, mais sur un autre serveur Web, tel qu'un serveur détenu et contrôlé par l'attaquant.

Malheureusement, de nombreuses entreprises disposent d'une importante base installée de contenu Web amélioré par JavaScript qui enfreint la même règle d'origine. Si vous activez la vérification de script intersite HTML sur un tel site, vous devez générer les exceptions appropriées afin que la vérification ne bloque pas les activités légitimes.

Le Web App Firewall propose diverses options d'action pour mettre en œuvre la protection par script intersite HTML. Outre les actions **Bloquer**, **Consigner**, **Statistiques** et **Apprendre**, vous avez également la possibilité de **Transformer les scripts intersites** afin de neutraliser une attaque par l'entité encodant les balises de script dans la demande soumise. Vous pouvez configurer le paramètre Vérifier les URL complètes pour le script intersite afin de spécifier si vous souhaitez inspecter non seulement

les paramètres de requête, mais également l'URL complète pour détecter une attaque de script intersite. Vous pouvez configurer le paramètre **InspectQueryContentTypes** pour inspecter la partie requête de demande pour l'attaque de script intersite pour les types de contenu spécifiques.

Vous pouvez déployer des relaxations pour éviter les faux positifs. Le moteur d'apprentissage du Web App Firewall peut fournir des recommandations pour la configuration des règles de relaxation.

Pour configurer une protection par script intersite HTML optimisée pour votre application, configurez l'une des actions suivantes :

- **Bloquer** : si vous activez le blocage, l'action de blocage est déclenchée si les balises de script intersite sont détectées dans la demande.
- **Journal** : si vous activez la fonctionnalité de journal, la vérification de script intersite HTML génère des messages de journal indiquant les actions qu'elle entreprend. Si le blocage est désactivé, un message de journal distinct est généré pour chaque en-tête ou champ de formulaire dans lequel la violation de script intersite a été détectée. Toutefois, un seul message est généré lorsque la demande est bloquée. De même, 1 message de journal par demande est généré pour l'opération de transformation, même lorsque les balises de script intersite sont transformées dans plusieurs champs. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.
- **Stats** : si elle est activée, la fonctionnalité de statistiques collecte des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si des demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer les nouvelles règles de relaxation ou modifier celles existantes.
- **Learn**—Si vous n'êtes pas sûr des règles de relaxation qui conviennent le mieux à votre application, vous pouvez utiliser la fonction d'apprentissage pour générer des recommandations de règles de script intersite HTML basées sur les données apprises. Le moteur d'apprentissage du Web App Firewall surveille le trafic et fournit des recommandations d'apprentissage basées sur les valeurs observées. Pour obtenir des avantages optimaux sans compromettre les performances, vous pouvez activer l'option d'apprentissage pendant une courte période afin d'obtenir un exemple représentatif des règles, puis déployer les règles et désactiver l'apprentissage.
- **Transformer les scripts intersites** : si cette option est activée, le Web App Firewall apporte les modifications suivantes aux demandes qui correspondent à la vérification de script intersite HTML :
  - Crochet angulaire gauche (<) en équivalent d'entité de caractères HTML (<)
  - Crochet droit (>) en équivalent d'entité de caractères HTML (>)

Cela garantit que les navigateurs n'interprètent pas les balises HTML non sécurisées, telles que < `script`>, et exécutent ainsi du code malveillant. Si vous activez à la fois la vérification et la transfor-

mation des en-têtes de demande, tous les caractères spéciaux présents dans les en-têtes de demande sont également modifiés. Si les scripts de votre site Web protégé contiennent des fonctionnalités de script intersite, mais que votre site Web ne dépend pas de ces scripts pour fonctionner correctement, vous pouvez désactiver le blocage et activer la transformation en toute sécurité. Cette configuration garantit qu'aucun trafic Web légitime n'est bloqué, tout en arrêtant toute attaque de script intersite potentielle.

- **Vérifiez les URL complètes pour les scripts intersites**. Si la vérification des URL complètes est activée, le Web App Firewall examine les URL entières à la recherche d'attaques de script intersite HTML au lieu de vérifier uniquement les parties de requête des URL.
- **Vérifiez les en-têtes de demande**. Si la vérification des en-têtes de demande est activée, le Web App Firewall examine les en-têtes des demandes d'attaques de script intersite HTML, au lieu de simplement les URL. Si vous utilisez l'interface graphique, vous pouvez activer ce paramètre dans l'onglet Paramètres du profil Web App Firewall.
- **InspectQueryContentTypes**. Si l'inspection des requêtes par requête est configurée, App Firewall examine la requête des demandes d'attaques de script intersite pour les types de contenu spécifiques. Si vous utilisez l'interface graphique, vous pouvez configurer ce paramètre dans l'onglet Paramètres du profil App Firewall.

> **Important :**
>
> Dans le cadre des modifications apportées à la diffusion en continu, le traitement des balises de script intersite par le Web App Firewall a changé. Cette modification s'applique aux versions 11.0 et ultérieures. Cette modification est également pertinente pour les versions d'amélioration de la version 10.5.e qui prennent en charge la diffusion côté demande. Dans les versions précédentes, la présence d'un crochet ouvert (<), or close bracket (>) ou des deux crochets ouverts et fermants (<>) était signalée comme Violation de script intersite. Le comportement a changé dans les versions qui incluent la prise en charge du streaming côté demande. Seul le caractère de crochet fermé (>) n'est plus considéré comme une attaque. Les demandes sont bloquées même lorsqu'un caractère entre crochets ouverts (<) est présent, et sont considérées comme une attaque. L'attaque par script intersite est signalée.

Script intersite Relaxations affinées

Le Web App Firewall vous donne la possibilité d'exempter un champ de formulaire, un en-tête ou un cookie spécifique de la vérification d'inspection des scripts intersites. Vous pouvez complètement contourner l'inspection pour un ou plusieurs de ces champs en configurant les règles de relaxation.

Le Web App Firewall vous permet d'implémenter une sécurité plus stricte en affinant les règles de relaxation. Une application peut avoir besoin de flexibilité pour autoriser des modèles spécifiques, mais la configuration d'une règle d'assouplissement pour contourner l'inspection de sécurité peut rendre l'application vulnérable aux attaques, car le champ cible est exempté d'inspection pour tout

modèle d'attaque par script intersite. La relaxation affinée des scripts intersites offre la possibilité d'autoriser des attributs, des balises et des modèles spécifiques. Les autres attributs, balises et modèles sont bloqués. Par exemple, le Web App Firewall possède actuellement un ensemble par défaut de plus de 125 modèles refusés. Étant donné que les pirates informatiques peuvent utiliser ces modèles dans des attaques de script intersites, le Web App Firewall les signale comme des menaces potentielles. Vous pouvez détendre un ou plusieurs modèles considérés comme sûrs pour un endroit spécifique. Les autres modèles de script intersite potentiellement dangereux sont toujours vérifiés pour l'emplacement cible et continuent de déclencher les violations du contrôle de sécurité. Vous avez maintenant un contrôle beaucoup plus serré.

Les commandes utilisées dans les relaxations comportent des paramètres facultatifs pour le **type de valeur** et **l'expression de valeur**. Le type de valeur peut être laissé vide ou vous avez la possibilité de sélectionner **Balise**, **Attribut** ou **Motif**. Si vous laissez le type de valeur vide, le champ configuré de l'URL spécifiée est exempté de l'inspection de vérification de script intersite. Si vous sélectionnez un type de valeur, vous devez fournir une expression de valeur. Vous pouvez spécifier si l'expression de valeur est une expression régulière ou une chaîne littérale. Lorsque l'entrée est mise en correspondance avec la liste autorisée et refusée, seules les expressions spécifiées configurées dans les règles de relaxation sont exemptées.

Le Web App Firewall possède les listes intégrées de script intersite suivantes :

1. **Attributs autorisés : 52 attributs**par défaut sont autorisés, tels que, **abbr**, **accesskey**, **align**, **alt**, **axis**, **bgcolor**, **border**, **remplissage de cellule**, **cell**spacing, **char**, **charoff**, **charset** et ainsi de suite
2. **Balises autorisées : Il y a 47 balises**autorisées par défaut, telles que, **address**, **basefont**, **bgsound**, **big**, **blockquote**, **bg**, **br**, **caption**, **center**, ****cite, ****dd**, **del** et ainsi de suite
3. **Modèles refusés de script intersite** : Il existe 129 modèles refusés par défaut, tels que **FSCommand**, **javascript :**, **OnAbort**, **OnActivate** et ainsi de suite

> **Avertissement**
>
> Les URL d'action du Web App Firewall sont des expressions régulières. Lorsque vous configurez des règles de relaxation de script intersite HTML, vous pouvez spécifier **Name**et **Value Expression** comme étant littéral ou RegEx. Les expressions régulières sont puissantes. Surtout si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement la règle que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation imprudente de caractères génériques, et en particulier du métacaractère point-astérisque (.*) ou de la combinaison de caractères génériques, peut avoir des résultats indésirables, tels que le blocage de l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou l'autorisation d'une attaque que la vérification de script intersite HTML aurait autrement bloquée.

Points à considérer :

- L'expression de valeur est un argument facultatif. Le nom d'un champ peut ne pas comporter d'expression de valeur.
- Un nom de champ peut être lié à plusieurs expressions de valeur.
- Les expressions de valeur doivent se voir attribuer un type de valeur. Le type de valeur de script intersite peut être : 1) Balise, 2) Attribut ou 3) Modèle.
- Vous pouvez avoir plusieurs règles de relaxation par combinaison nom de champ/URL
- Les noms des champs de formulaire et les URL d'action ne sont pas sensibles à la casse.

Utilisation de la ligne de commande pour configurer la vérification de script intersite HTML

Pour configurer le script intersite HTML, les actions de vérification et d'autres paramètres à l'aide de la ligne de commande

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer les commandes suivantes pour configurer la vérification de script inter-site HTML :

- définir le sujet du profil appfw .
- <name> -crossSiteScriptingAction (([block] [learn] [log] [stats])| [** none**])
- [Définir le sujet du profil appfw.
- <name> **-crossSiteScriptingTransformUnsafeHTML** (ON | OFF)
- définir le sujet du profil appfw.
- <name> -crossSiteScriptingCheckCompleteURLs (ON | OFF)
- définir le sujet du profil appfw.
- ' - CheckRequestHeaders (Activé \| Désactivé)
- <name> - CheckRequestQueryNonHtml (ON | OFF)

Pour configurer une règle de relaxation de script intersite HTML, vérifiez la règle de relaxation à l'aide de la ligne de commande

Utilisez la commande bind ou unbind pour ajouter ou supprimer une liaison, comme suit :

- bind appfw profile <name> -crossSiteScripting <String> [isRegex (REGEX | NOTREGEX)] <formActionURL> [-location <location>] [-valueType (Tag| Attribute|Pattern)[<valueExpression>] [-isValueRegex (REGEX | NOTREGEX)]]
- unbind appfw profile <name> -crossSiteScripting <String> <formActionURL > [-location <location>] [-valueType (Tag |Attribute|Pattern)[<valueExpression >]]

Utilisation de l'interface graphique pour configurer la vérification de script intersite HTML

Dans l'interface graphique, vous pouvez configurer la vérification de script intersite HTML dans le volet pour le profil associé à votre application.

Pour configurer ou modifier la vérification de script intersite HTML à l'aide de l'interface graphique

1. Accédez à **Application Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Contrôles de sécurité**.

Le tableau de contrôle de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Deux options de configuration s'offrent à vous :

a. Si vous souhaitez activer ou désactiver les actions **Bloquer**, **Consigner**, **Statistiques**et **Apprendre** pour le script intersite HTML, vous pouvez activer ou désactiver les cases à cocher dans le tableau, cliquer sur **OK**, puis sur **Enregistrer et fermer** pour fermer le **Volet de contrôle de sécurité** .

b. Si vous souhaitez configurer d'autres options pour cette vérification de sécurité, double-cliquez sur **Script intersite HTML**, ou sélectionnez la ligne et cliquez sur **Paramètres d'action**, pour afficher les options suivantes :

Transformer les scripts intersites : transforme les balises de script non sécurisées.

Vérifier les URL complètes pour les scripts intersites : au lieu de vérifier uniquement la partie requête de l'URL, vérifiez que l'URL complète ne contient pas de violations de script intersite.

Après avoir modifié l'un des paramètres ci-dessus, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau Contrôles de sécurité. Vous pouvez procéder à la configuration d'autres contrôles de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section **Contrôles de sécurité**, puis cliquez sur **Enregistrer et fermer** pour fermer le volet **Contrôle de sécurité** .

Pour activer ou désactiver le paramètre **En-tête de demande de vérification**, dans le volet **Paramètres avancés**, cliquez sur **Paramètres du profil**. Dans **Paramètres communs**, activez ou désactivez la case à **cocher Vérifier les en-têtes de demande** . Cliquez sur **OK**. Vous pouvez soit utiliser l'icône **X** en haut à droite du volet **Paramètres du profil** pour fermer cette section, soit, si vous avez fini de configurer ce profil, vous pouvez cliquer sur **Terminé** pour revenir à **Application Firewall** > **Profil**.

Pour activer ou désactiver le paramètre **Requête de demande de vérification non HTML**, dans le volet **Paramètres avancés**, cliquez sur **Paramètres du profil**. Dans **Paramètres communs**, activez ou désactivez la **case à cocher Requête de demande de vérification non HTML** . Cliquez sur **OK**. Vous pouvez soit utiliser l'icône X en haut à droite du volet **Paramètres du profil** pour fermer cette section, soit, si vous avez fini de configurer ce profil, vous pouvez cliquer sur **Terminé** pour revenir à **App Firewall > Profil**.

Pour configurer une règle de relaxation de script intersite HTML à l'aide de l'interface graphique

1. Accédez à **Application Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
3. Dans le tableau Règles de relaxation, double-cliquez sur l'entrée **Script intersite HTML**, ou sélectionnez-la et cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Règles de relaxation des scripts intersites HTML**, effectuez des opérations **Ajouter**, **Modifier**, **Supprimer**, **Activer**ou **Désactiver** pour les règles de relaxation.

> **Remarque**
>
> Lorsque vous ajoutez une nouvelle règle, le champ **Expression de valeur** ne s'affiche pas, sauf si vous sélectionnez l'option **Balise**, **Attribut** ou **Modèle** dans le champ **Type de valeur** .

Pour gérer les règles de relaxation du script intersite HTML à l'aide du visualiseur

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez mettre en surbrillance la ligne **Script intersite HTML** dans le tableau Règles de relaxation, puis cliquer sur **Visualiseur**. Le visualiseur pour les relaxations déployées vous offre la possibilité d' **ajouter** une nouvelle règle ou de **modifier** une règle existante. Vous pouvez également **activer** ou **désactiver** un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Pour afficher ou personnaliser les modèles de script intersite à l'aide de l'interface graphique

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser la liste par défaut des attributs autorisés ou des balises autorisées pour les scripts intersites. Vous pouvez également afficher ou personnaliser la liste par défaut des modèles refusés par script intersite.

Les listes par défaut sont spécifiées dans **Pare-feu d'application** > **Signatures > Signaturespar défaut**. Si vous ne liez aucun objet de signature à votre profil, la liste des scripts intersites autorisés et refusés par défaut spécifiée dans l'objet Signatures par défaut sera utilisée par le profil pour le traitement du contrôle de sécurité du script intersite. Les balises, les attributs et les modèles, spécifiés dans l'objet signatures par défaut, sont en lecture seule. Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez les modifier ou les modifier, faites une copie de l'objet Signatures par défaut pour créer un objet signature défini par l'utilisateur. Apportez des modifications aux listes autorisées ou refusées du nouvel objet de signature défini par l'utilisateur et utilisez cet objet de signature dans votre profil qui traite le trafic pour lequel vous souhaitez utiliser ces listes d'autorisation et de refus personnalisées.

1. Pour afficher les modèles de script intersite par défaut :

a. Accédez à **Pare-feu d'application** > **Signatures**, sélectionnez **Signatures par défaut**, puis cliquez sur **Modifier**. Cliquez ensuite sur **Gérer les modèles de script SQL/intersite**.

Le tableau **Gérer les chemins de script SQL/intersite** affiche les trois lignes suivantes relatives au script intersite :


```
xss/allowed/attribute

xss/allowed/tag

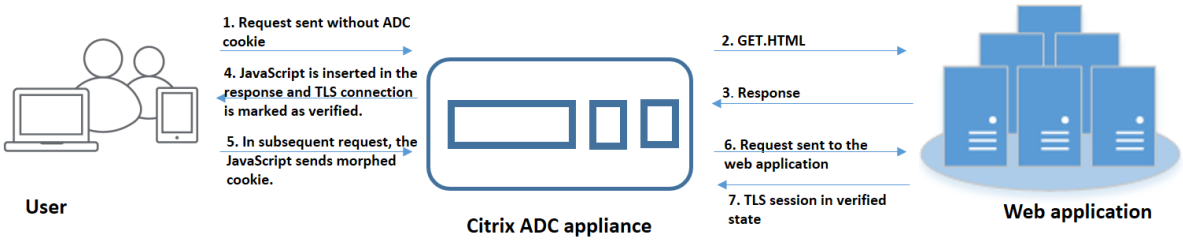
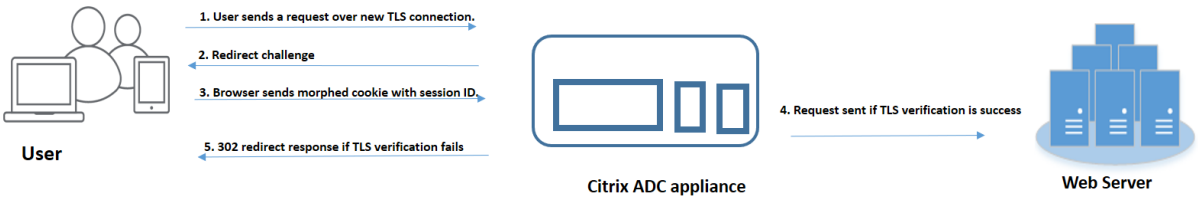
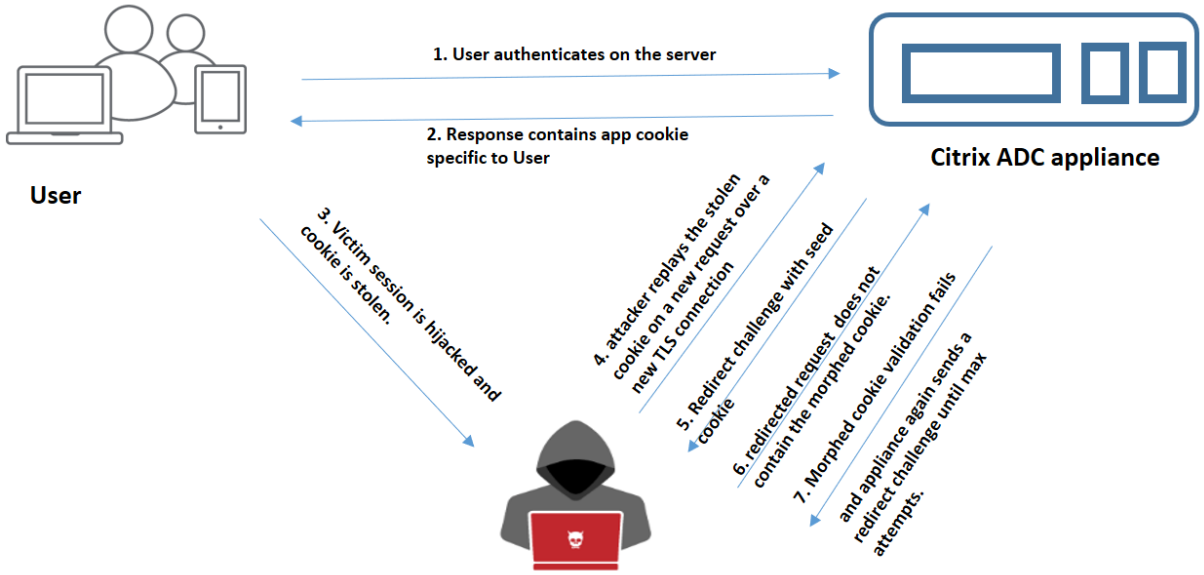
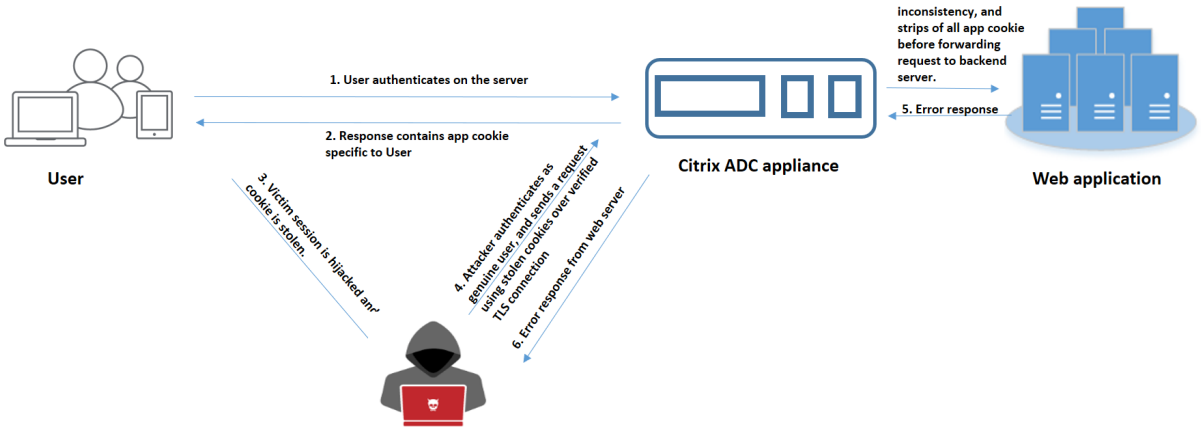
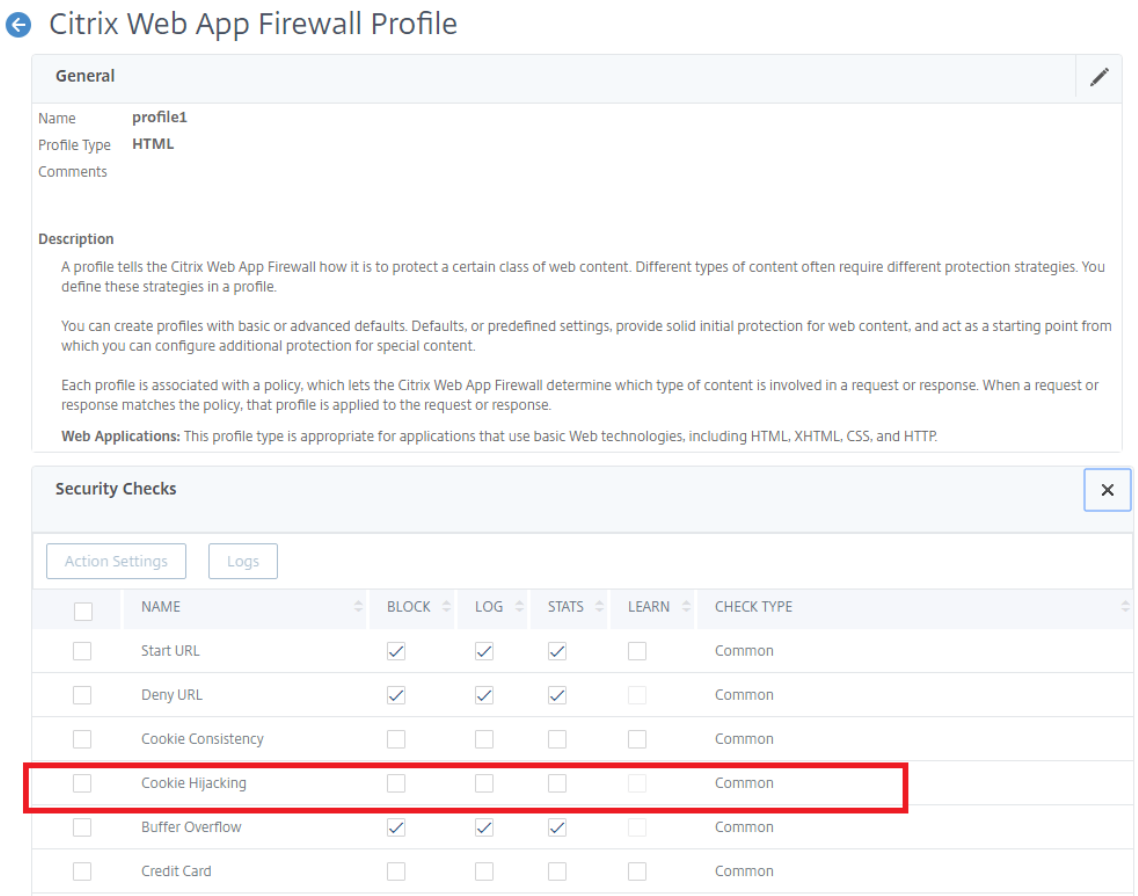
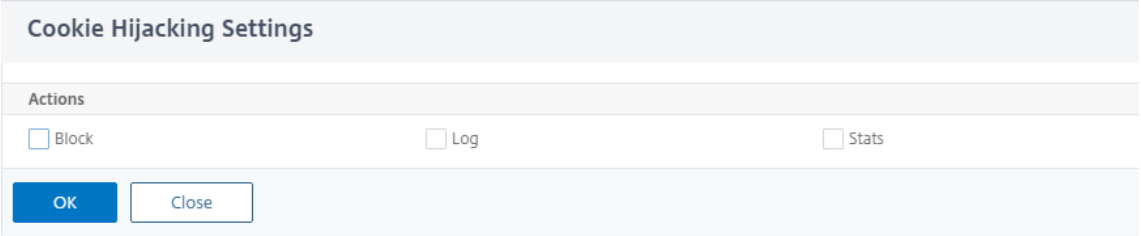
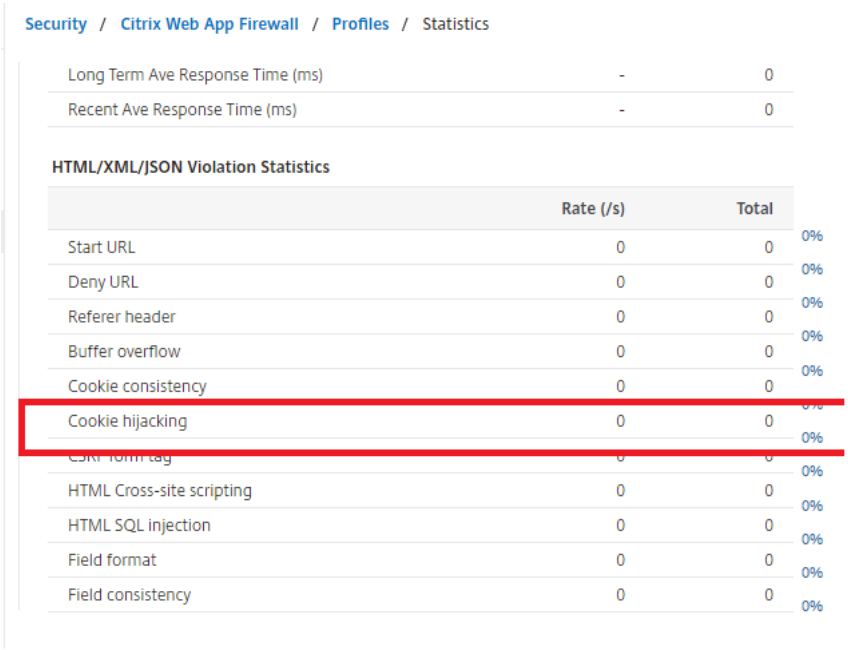
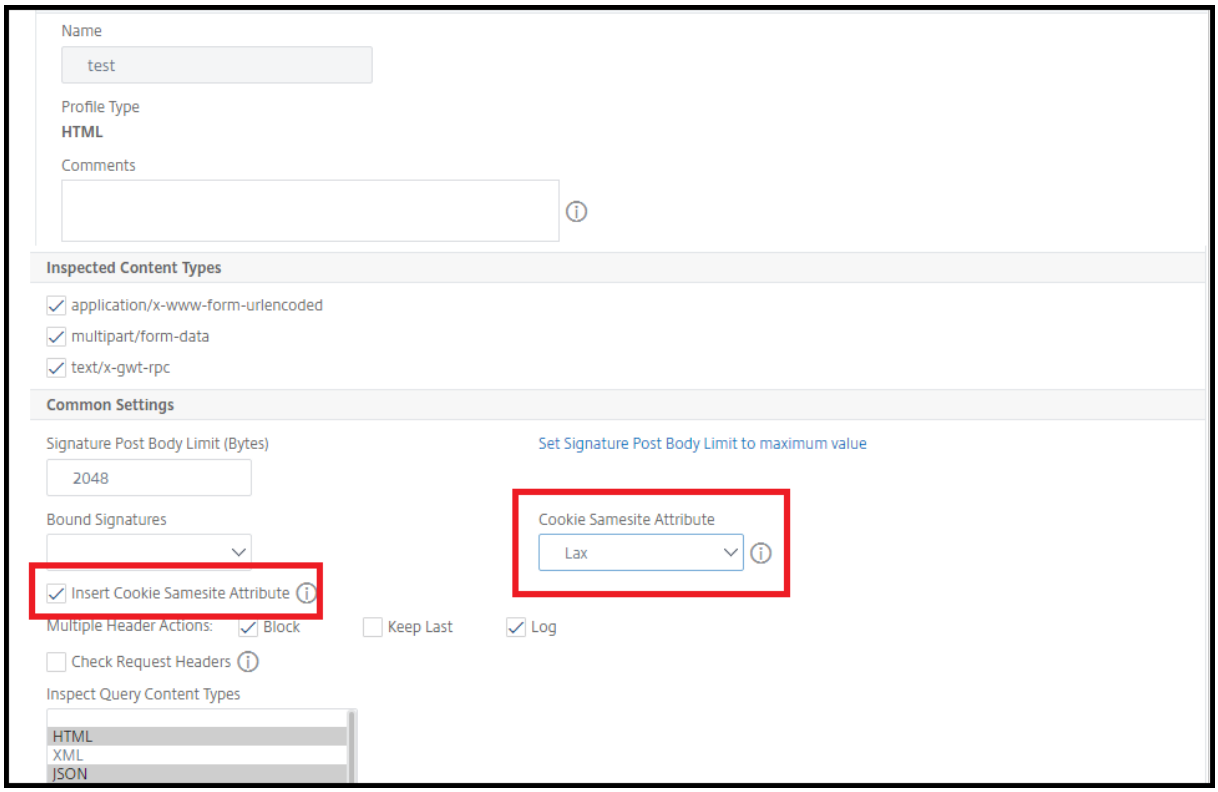
xss/denied/pattern
```

b. Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les éléments de script intersite correspondants (balise, attribut, modèle) utilisés par la vérification de **script intersite du** Web App Firewall.

1. **Pour personnaliser les éléments de script intersite** : vous pouvez modifier l'objet de signature défini par l'utilisateur pour personnaliser la balise autorisée, les attributs autorisés et les modèles refusés. Vous pouvez ajouter de nouvelles entrées ou supprimer celles qui existent déjà.

a. Accédez à **Pare-feu d'application** > **Signatures**, mettez en surbrillance la signature définie par l'utilisateur cible, puis cliquez sur **Modifier**. Cliquez sur **Gérer les modèles de script SQL/intersite** pour afficher le tableau **Gérer les chemins de script SQL/intersite** .

b. Sélectionnez la ligne de script intersite cible.

i. Cliquez sur **Gérer les éléments**pour **ajouter**, **modifier** ou **supprimer** l'élément de script intersite correspondant.

ii. Cliquez sur **Supprimer** pour supprimer la ligne sélectionnée.

> **Avertissement :**
>
> Vous devez être prudent avant de supprimer ou de modifier un élément de script intersite par défaut, ou de supprimer le chemin de script intersite pour supprimer la ligne entière. Les règles de signature et le contrôle de sécurité du script intersite s'appuient sur ces éléments pour détecter les attaques afin de protéger vos applications. Personnalisation des scripts intersites Les éléments peuvent rendre votre application vulnérable aux attaques de script intersite si le modèle requis est supprimé pendant la modification.

Apprendre les violations de script intersite HTML (script intersite)

Lorsque l'apprentissage est activé, le moteur d'apprentissage de NetScaler Web App Firewall surveille le trafic et détecte les violations d'URL liées aux scripts intersites. Vous pouvez inspecter régulièrement les règles d'URL de script intersite et les déployer en cas de faux positifs.

> **Remarque :**
>
> Dans une configuration de cluster, tous les nœuds doivent être de la même version pour déployer les règles d'URL de script intersite.

Dans le cadre de la configuration de l'apprentissage, le Web App Firewall propose un apprentissage détaillé du script intersite HTML. Le moteur d'apprentissage fait des recommandations concernant le

type de valeur observé (balise, attribut, modèle) et l'expression de valeur correspondante observée dans les champs de saisie. En plus de vérifier les demandes bloquées pour déterminer si la règle actuelle est trop restrictive et doit être assouplie, vous pouvez consulter les règles générées par le moteur d'apprentissage pour déterminer quels types de valeur et expressions de valeur déclenchent des violations et doivent être traitées dans les règles de relaxation.

> **Remarque :**
>
> Le moteur d'apprentissage du pare-feu Web App Firewall ne peut distinguer que les 128 premiers octets du nom. Si un formulaire comporte plusieurs champs dont les noms correspondent aux 128 premiers octets, le moteur d'apprentissage peut ne pas être en mesure de les distinguer. De même, la règle d'assouplissement déployée peut par inadvertance relâcher tous ces champs de l'inspection de script intersite HTML.
>
> **Conseil :**
>
> Les balises de script intersite de plus de 12 caractères ne sont pas apprises ou consignées correctement.
>
> Si vous avez besoin d'une longueur de balise plus grande pour l'apprentissage, vous pouvez ajouter une grande balise non apparaissant dans la liste **AS_Cross-site scripting_allowed_tags_List** pour la longueur « x ».

Le processus d'apprentissage du script intersite HTML réduit les faux positifs dans les attaques par script intersite. Lorsque l'apprentissage est activé, vous pouvez apprendre toutes les violations d'une demande et éventuellement appliquer un assouplissement à plusieurs balises, attributs ou modèles sans avoir besoin de les répéter.

Par exemple, s'il y a 15 balises personnalisées dans une charge utile entraînant chacune une violation, vous pouvez appliquer la relaxation fine pour toutes les balises signalées comme violation, au lieu de répéter le processus pour appliquer la relaxation pour une balise à la fois.

Scénario 1 : apprentissage activé et blocage activé :
Dans ce scénario, l'appliance NetScaler apprend toutes les violations dans des balises/attributes/-modèles personnalisés, puis la demande est bloquée et chaque violation est enregistrée. Le comportement est cohérent pour les violations identifiées dans le champ de formulaire, l'en-tête ou le cookie.

Scénario 2 : apprentissage activé et blocage désactivé :
Dans ce scénario, l'appliance NetScaler apprend les violations sous forme de balises/attributes/modèles personnalisés et chacune des violations est enregistrée. La demande n'est pas bloquée. Le comportement est cohérent pour les violations identifiées dans le champ de formulaire, l'en-tête ou le cookie.

Pour afficher ou utiliser les données apprises à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `show appfw learningdata <profilename> crossSiteScripting`
- `rm appfw learningdata <profilename> -crossSiteScripting <string> <formActionURL> [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> **crossSiteScripting*`

Configurer la relaxation fine du script intersite pour contourner les balises personnalisées

Vous pouvez configurer la relaxation des scripts intersites dans le profil de pare-feu de l'application Web pour contourner les balises/attributs/modèles personnalisés qui ne figurent pas dans la liste verte.
À l'invite de commande, tapez :

```
bind appfw profile p1 -crossSiteScripting <string> <formActionURL> -valueType
 <valueType> <value expression>
```

Exemple :

```
bind appfw profile profile1 -crossSiteScripting formfield1 http://1.1.1.1 -
valueType Tag tag1
```

Pour afficher ou utiliser les données apprises à l'aide de l'interface graphique

1. Accédez à **Application Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles apprises**. Vous pouvez sélectionner l'entrée **Script intersite HTML** dans le tableau Règles apprises et double-cliquer dessus pour accéder aux règles apprises. Le tableau affiche les colonnes **Nom de champ**,**URL d'action**, **Type**de **valeur, Valeur**et **Résultats** . Vous pouvez déployer les règles apprises ou modifier une règle avant de la déployer en tant que règle de relaxation. Pour annuler une règle, vous pouvez la sélectionner et cliquer sur le bouton **Ignorer** . Vous ne pouvez modifier qu'une règle à la fois, mais vous pouvez sélectionner plusieurs règles à déployer ou à ignorer.

Vous pouvez également afficher un résumé des relaxations apprises en sélectionnant l'entrée **Script intersite HTML** dans le tableau Règles apprises et en cliquant sur **Visualiseur** pour obtenir une vue consolidée de toutes les violations apprises. Le visualiseur facilite la gestion des règles apprises. Il présente une vue complète des données sur un seul écran et facilite la prise de mesures sur un groupe de règles en un seul clic. Le principal avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de ces règles, en fonction du délimiteur et de l'URL d'action. Vous pouvez afficher 25, 50 ou 75 règles dans le visualiseur, en sélectionnant le nombre dans une liste déroulante. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer sous forme d'assouplissements. Vous pouvez également ignorer les règles pour les ignorer.

Utilisation de la fonction de journalisation avec la vérification du script intersite HTML

Lorsque l'action de journalisation est activée, les violations de contrôle de sécurité du script intersite HTML sont consignées dans le journal d'audit en tant que violations de **script intersite AppFW_intersite** . Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur Syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Passez au shell et terminez les fichiers ns.logs dans le dossier /var/log/ pour accéder aux messages de journal relatifs aux violations de script intersite HTML :

```
Shell
tail -f /var/log/ns.log | grep APPFW_cross-site scripting
```

Exemple de message de journal de violation de vérification de sécurité de script intersite au format journal CEF :

```
1 Jul 11 00:45:51 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|\*\*APPFW_cross-site scripting\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=4840 method=GET request=http://aaron.
    stratum8.net/FFC/CreditCardMind.html?abc=%3Cdef%3E msg=\*\*Cross-
    site script check failed for field abc="Bad tag: def"\*\* cn1=133
    cn2=294 cs1=pr_ffc cs2=PPE1 cs3=eUljypvLa0BbabwfGVE52Sewg9U0001 cs4=
    ALERT cs5=2015 act=\*\*not blocked\*\*
2 <!--NeedCopy-->
```

Exemple de message de journal de violation de vérification de sécurité de script intersite au format journal natif indiquant l'action de transformation

```
1 Jul 11 01:00:28 <local0.info> 10.217.31.98 07/11/2015:01:00:28 GMT ns
    0-PPE-0 : default APPFW \*\*APPFW_cross-site scripting\*\* 132 0 :
    10.217.253.62 392-PPE0 eUljypvLa0BbabwfGVE52Sewg9U0001 pr_ffc http:
    //aaron.stratum8.net/FFC/login.php?login_name=%3CBOB%3E&passwd=&
    drinking_pref=on &text_area=&loginButton=ClickToLogin&as_sfid=
    AAAAAAVFqmYL68IGvkrcn2pzehjfIkm5E6EZ9FL8YLvIW_41AvAATuKYe9N7uGThSpEAxbb0iBx55j
    -FC4llF \*\*Cross-site script special characters seen in fields <
    transformed>\*\*
2 <!--NeedCopy-->
```

Accédez aux messages du journal à l'aide de l'interface graphique

L'interface graphique inclut un outil utile (Syslog Viewer) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **Pare-feu des applications** > **Profils**, sélectionnez le profil cible, puis cliquez sur **Contrôles de sécurité**. Mettez en surbrillance la ligne **Script intersite HTML** et cliquez sur **Journaux**. Lorsque vous accédez aux journaux directement à partir de la vérification de script intersite HTML du profil, l'interface graphique filtre les messages du journal et affiche uniquement les journaux relatifs à ces violations de contrôle de sécurité.
- ****Vous pouvez également accéder à la visionneuse Syslog en accédant à **NetScaler** > Système > Audit.**** Dans la section **Messages d'audit**, cliquez sur le lien **des messages Syslog** pour afficher le visualiseur Syslog, qui affiche tous les messages du journal, y compris les autres journaux de violations des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de contrôle de sécurité peuvent être déclenchées pendant le traitement des demandes.
- Accédez à **Pare-feu des applications** > **Stratégies** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation de vérification de sécurité.

La visionneuse Syslog basée sur HTML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour sélectionner les messages de journal pour la vérification de **script intersite HTML**, filtrez en sélectionnant **APPFW** dans les options de la liste déroulante pour **Module**. La liste **Type d'événement** offre un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **Script intersite AppFW_Cross-site** et que vous cliquez sur le bouton **Appliquer**, seuls les messages de journal relatifs aux violations de contrôle de **sécurité du script intersite HTML** apparaissent dans la visionneuse Syslog.

Si vous placez le curseur sur la ligne d'un message de journal spécifique, plusieurs options, telles que le **module**, le **type d'événement**, l'**ID d'événement**, l'**adresse IP du client**, etc., apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

La fonctionnalité**Cliquer pour déployer** n'est disponible que dans l'interface graphique. Vous pouvez utiliser la visionneuse Syslog non seulement pour afficher les journaux, mais également pour déployer les règles de relaxation du script intersite HTML en fonction des messages de journal pour les violations de contrôle de sécurité du Web App Firewall. Les messages de journal doivent être au format de journal CEF pour cette opération. La fonctionnalité Cliquer pour déployer n'est disponible que pour les messages de journal générés par l'action Bloquer (ou ne pas bloquer). Vous ne pouvez pas déployer de règle de relaxation pour un message de journal concernant l'opération de transformation.

Pour déployer une règle de relaxation à partir de la visionneuse Syslog, sélectionnez le message de journal. Une case à cocher apparaît dans le coin supérieur droit de la case **Syslog Viewer** de la ligne sélectionnée. Activez la case à cocher, puis sélectionnez une option dans la liste **Action** pour déployer la règle de relaxation. Les options**Modifier et déployer**, **Déployer**et **Tout déployer** sont disponibles en tant qu'options **d'action** .

Les règles de script intersite HTML qui sont déployées à l'aide de l'option **Cliquez pour déployer**

n'incluent pas les recommandations de relaxation fine.

Configurer la fonctionnalité Cliquer pour déployer à l'aide de l'interface graphique

1. Dans la visionneuse Syslog, sélectionnez **APPFW** dans les options du **module** .
2. Sélectionnez le **script App_Cross-site** comme **Type d'événement** pour filtrer les messages de journal correspondants.
3. Cochez la case pour identifier la règle à déployer.
4. Utilisez la liste déroulante d'options **Action** pour déployer la règle de relaxation.
5. Vérifiez que la règle apparaît dans la section de règle de relaxation correspondante.

Statistiques relatives aux violations de script intersite HTML

Lorsque l'action de statistiques est activée, le compteur de la vérification de script intersite HTML est incrémenté lorsque le Web App Firewall effectue une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, la demande d'une page contenant 3 violations de script intersite HTML incrémente le compteur de statistiques d'un, car la page est bloquée lorsque la première violation est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente de trois le compteur de statistiques pour les violations et les journaux, car chaque violation génère un message de journal distinct.

Pour afficher les statistiques de vérification du script intersite HTML à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
> sh appfw stats
```

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> **stat appfw profile** <profile name>
```

Afficher les statistiques de script intersite HTML à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Pare-feu des applications > Profils > Statistiques**.
2. Dans le volet droit, accédez au lien **Statistiques** .
3. Utilisez la barre de défilement pour afficher les statistiques relatives aux violations de script intersite HTML et aux journaux. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Résumé

- **Support intégré pour la protection contre les attaques par script intersite HTML** : NetScaler Web App Firewall protège contre les attaques par script intersite en surveillant une combinaison d'attributs et de balises autorisés, ainsi que les modèles refusés dans la charge utile reçue. Toutes les balises autorisées par défaut intégrées, les attributs autorisés et les modèles refusés utilisés par la vérification de script intersite sont spécifiés dans le fichier /netscaler/default_custom_settings.xml.
- **Personnalisation** : vous pouvez modifier la liste par défaut des balises, des attributs et des modèles afin de personnaliser l'inspection du contrôle de sécurité du script intersite en fonction des besoins spécifiques de votre application. Effectuez une copie de l'objet signature par défaut, modifiez les entrées existantes ou ajoutez de nouvelles entrées. Liez cet objet de signature à votre profil pour utiliser la configuration personnalisée.
- **Modèle de sécurité hybride** : les signatures et les protections de sécurité avancées utilisent les modèles de script SQL/intersite spécifiés dans l'objet de signature lié au profil. Si aucun objet de signature n'est lié au profil, les modèles de script SQL/intersite présents dans l'objet de signature par défaut sont utilisés.
- **Transform**—Notez les points suivants concernant l'opération de transformation :

L'opération de transformation fonctionne indépendamment des autres paramètres d'action de script intersite. Si la transformation est activée et que le blocage, le journal, les statistiques et l'apprentissage sont tous désactivés, les balises de script intersite sont transformées.

Si l'action de blocage est activée, elle a priorité sur l'action de transformation.

- **Relaxation et apprentissage à grains fins**. Affinez la règle de relaxation pour assouplir un sous-ensemble d'éléments de script intersite issus de l'inspection du contrôle de sécurité, mais détectez le reste. Le moteur d'apprentissage recommande un type de valeur spécifique et des expressions de valeur basées sur les données observées.
- **Cliquez pour déployer** : sélectionnez un ou plusieurs messages de journal de violation de script intersite dans la visionneuse Syslog et déployez-les en tant que règles de relaxation.
- **Charset**—Le jeu de caractères par défaut du profil doit être défini en fonction des besoins de l'application. Par défaut, le jeu de caractères du profil est défini sur Anglais américain (ISO-8859-1). Si une demande est reçue sans le jeu de caractères spécifié, le Web App Firewall traite la demande comme s'il s'agissait de la norme ISO-8859-1. Le caractère de crochet ouvert (<) or the close bracket character (>) ne sera pas interprété comme des balises de script intersite si ces caractères sont codés dans d'autres jeux de caractères. Par exemple, si une demande contient une chaîne de caractères UTF-8 « **%uff1cscript%uff1e** » mais que le jeu de caractères n'est pas spécifié sur la page de demande, la violation de script intersite peut ne pas être déclenchée à moins que le jeu de caractères par défaut du profil ne soit spécifié comme Unicode.

Vérification par injection HTML SQL

May 5, 2023

De nombreuses applications Web possèdent des formulaires Web qui utilisent SQL pour communiquer avec des serveurs de bases de données relationnelles. Un code malveillant ou un pirate informatique peut utiliser un formulaire Web non sécurisé pour envoyer des commandes SQL au serveur Web. La vérification par injection SQL HTML de Web App Firewall fournit des défenses spéciales contre l'injection de code SQL non autorisé susceptible de compromettre la sécurité. Si le Web App Firewall détecte un code SQL non autorisé dans une demande utilisateur, il transforme la demande, pour rendre le code SQL inactif, ou bloque la demande. Le Web App Firewall examine la charge utile de la requête pour le code SQL injecté à trois emplacements : 1) corps POST, 2) en-têtes et 3) cookies. Pour examiner une partie de requête dans les demandes de code SQL injecté, configurez un paramètre de profil de pare-feu d'application « InspectQueryContentTypes » pour les types de contenu spécifiques.

Un ensemble par défaut de mots-clés et de caractères spéciaux fournit des mots-clés connus et des caractères spéciaux couramment utilisés pour lancer des attaques SQL. Vous pouvez ajouter de nouveaux modèles et modifier le jeu par défaut pour personnaliser l'inspection des vérifications SQL. Le Web App Firewall propose différentes options d'action pour mettre en œuvre la protection par injection SQL. Outre les actions **Bloquer**, **Log**, **Stats** et **Learn**, le profil Web App Firewall offre également la possibilité de **transformer les caractères spéciaux SQL** pour rendre une attaque inoffensive.

Outre les actions, plusieurs paramètres peuvent être configurés pour le traitement par injection SQL. Vous pouvez vérifier la présence de **caractères génériques SQL**. Vous pouvez modifier le type d'injection SQL et sélectionner l'une des 4 options (**SQLKeyword**, **SqlsplChar**, **SqlsplCharAndKeyword**, **SQLSplCharOrKeyword**) pour indiquer comment évaluer les mots-clés SQL et les caractères spéciaux SQL lors du traitement de la charge utile. Le **paramètre Gestion des commentaires SQL** vous permet de spécifier le type de commentaires qui doivent être inspectés ou exemptés lors de la détection par injection SQL.

Vous pouvez déployer des relaxations pour éviter les faux positifs. Le moteur d'apprentissage du Web App Firewall peut fournir des recommandations pour la configuration des règles de relaxation.

Les options suivantes sont disponibles pour configurer une protection SQL Injection optimisée pour votre application :

Block—L'action de bloc n'est déclenchée que si l'entrée correspond à la spécification de type d'injection SQL. Par exemple, si **SQLSplCharANDKeyword** est configuré comme type d'injection SQL, une requête n'est pas bloquée si elle ne contient pas de mots-clés, même si des caractères spéciaux SQL sont détectés dans l'entrée. Une telle demande est bloquée si le type d'injection SQL est défini sur **SqlsplChar**ou **SqlsplCharOrKeyword**.

Log—Si vous activez la fonction de journal, la vérification SQL Injection génère des messages de jour-

nal indiquant les actions qu'elle effectue. Si l'action de blocage est désactivée, un message de journal distinct est généré pour chaque champ de saisie dans lequel la violation SQL a été détectée. Toutefois, un seul message est généré lorsque la demande est bloquée. De même, un message de journal par demande est généré pour l'opération de transformation, même lorsque des caractères spéciaux SQL sont transformés dans plusieurs champs. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.

Stats : si elle est activée, la fonctionnalité de statistiques collecte des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si des demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer de nouvelles règles de relaxation ou modifier celles existantes.

Apprendre : si vous n'êtes pas sûr des règles de relaxation SQL qui conviennent le mieux à votre application, vous pouvez utiliser la fonctionnalité d'apprentissage pour générer des recommandations basées sur les données apprises. Le moteur d'apprentissage du Web App Firewall surveille le trafic et fournit des recommandations d'apprentissage SQL en fonction des valeurs observées. Pour obtenir des avantages optimaux sans compromettre les performances, vous pouvez activer l'option d'apprentissage pendant une courte période afin d'obtenir un exemple représentatif des règles, puis déployer les règles et désactiver l'apprentissage.

Caractères spéciaux Transform SQL : le Web App Firewall considère trois caractères, les guillemets simples (‘), les barres obliques `(\)` inverses et les points-virgules (;) comme des caractères spéciaux pour le traitement des vérifications de sécurité SQL. La fonction Transformation SQL modifie le code d'injection SQL dans une requête HTML afin de garantir que la demande est rendue inoffensive. La demande HTML modifiée est ensuite envoyée au serveur. Toutes les règles de transformation par défaut sont spécifiées dans le fichier /netscaler/default_custom_settings.xml.

L'opération de transformation rend le code SQL inactif en apportant les modifications suivantes à la demande :

- Guillemets simples (‘) vers guillemets droits doubles («).
- Barre oblique inverse `(\)` pour double barre oblique inverse `(\)`.
- Le point-virgule (;) est complètement supprimé.

Ces trois caractères (chaînes spéciales) sont nécessaires pour émettre des commandes vers un serveur SQL. À moins qu'une commande SQL ne soit préfacée par une chaîne spéciale, la plupart des serveurs SQL ignorent cette commande. Par conséquent, les modifications que le Web App Firewall effectue lorsque la transformation est activée empêchent un attaquant d'injecter du code SQL actif. Une fois ces modifications apportées, la demande peut être transmise en toute sécurité à votre site Web protégé. Lorsque les formulaires Web de votre site Web protégé peuvent légitimement contenir des chaînes spéciales SQL, mais que les formulaires Web ne dépendent pas des chaînes spéciales pour fonctionner correctement, vous pouvez désactiver le blocage et activer la transformation

pour empêcher le blocage des données de formulaire Web légitimes sans réduire la protection que l'application Web Le pare-feu fournit à vos sites Web protégés.

L'opération de transformation fonctionne indépendamment du paramètre du **type d'injection SQL** . Si la transformation est activée et que le type d'injection SQL est spécifié comme mot-clé SQL, les caractères spéciaux SQL sont transformés même si la requête ne contient aucun mot-clé.

> **Conseil**
>
> Vous activez normalement la transformation ou le blocage, mais pas les deux. Si l'action de blocage est activée, elle a priorité sur l'action de transformation. Si le blocage est activé, l'activation de la transformation est redondante.

Vérifier les caractères génériques SQL —Lescaractères génériques peuvent être utilisés pour élargir les sélections d'une instruction SQL (SQL-SELECT). Ces opérateurs de caractères génériques peuvent être utilisés avec des opérateurs **LIKEet NOT** LIKE pour comparer une valeur à des valeurs similaires. Le pourcentage (%) et le trait de soulignement (_) sont fréquemment utilisés comme caractères génériques. Le signe pour cent est analogue au caractère générique astérisque (*) utilisé avec MS-DOS et pour faire correspondre zéro, un ou plusieurs caractères dans un champ. Le trait de soulignement est similaire au point d'interrogation MS-DOS (?) caractère générique. Il correspond à un seul nombre ou caractère dans une expression.

Par exemple, vous pouvez utiliser la requête suivante pour effectuer une recherche de chaîne afin de rechercher tous les clients dont le nom contient le caractère D.

SELECT * from customer WHERE name like "%D%":

L'exemple suivant combine les opérateurs pour rechercher les valeurs de salaire dont la deuxième et la troisième position sont égales à 0.

SELECT * from customer WHERE salary like '_00%':

Différents fournisseurs de SGBD ont étendu les caractères génériques en ajoutant des opérateurs supplémentaires. Le pare-feu NetScaler Web App peut protéger contre les attaques lancées en injectant ces caractères génériques. Les 5 caractères génériques par défaut sont le pourcentage (%), le trait de soulignement (_), le signe d'insertion (^), le crochet ouvrant ([) et le crochet fermant (]). Cette protection s'applique aux profils HTML et XML.

Les caractères génériques par défaut sont une liste de littéraux spécifiés dans ***Signatures par défaut** :

- `<wildchar type="LITERAL">%</wildchar>`
- `<wildchar type="LITERAL">_</wildchar>`
- `<wildchar type="LITERAL">^</wildchar>`
- `<wildchar type="LITERAL">[</wildchar>`
- `<wildchar type="LITERAL">]</wildchar>`

Les caractères génériques d'une attaque peuvent être PCRE, comme [^A-F]. Le Web App Firewall prend également en charge les caractères génériques PCRE, mais les caractères génériques littéraux ci-dessus sont suffisants pour bloquer la plupart des attaques.

> **Remarque :**
>
> La vérification des caractères génériques SQL est différente de la vérification des caractères spéciaux SQL. Cette option doit être utilisée avec précaution afin d'éviter les faux positifs.

Demande de vérification contenant le type d'injection SQL : le Web App Firewall propose 4 options pour mettre en œuvre le niveau de rigueur souhaité pour l'inspection par injection SQL, en fonction des besoins individuels de l'application. La demande est vérifiée par rapport à la spécification du type d'injection pour détecter les violations SQL. Les 4 options de type d'injection SQL sont les suivantes :

- **Caractère spécial et mot-clé**SQL : un mot-clé SQL et un caractère spécial SQL doivent être présents dans l'entrée pour déclencher une violation SQL. Ce paramètre le moins restrictif est également le paramètre par défaut.
- **Caractère spécial SQL** : au moins un des caractères spéciaux doit être présent dans l'entrée pour déclencher une violation SQL.
- **Mot clé SQL** : au moins un des mots-clés SQL spécifiés doit être présent dans l'entrée pour déclencher une violation SQL. Ne sélectionnez pas cette option sans avoir dûment pris en considération. Pour éviter les faux positifs, assurez-vous qu'aucun des mots-clés n'est attendu dans les entrées.
- **Caractère spécial ou mot clé SQL** : le mot clé ou la chaîne de caractères spéciaux doit être présent dans l'entrée pour déclencher la violation du contrôle de sécurité.

> **Conseil :**
>
> Si vous configurez le Web App Firewall pour rechercher les entrées contenant un caractère spécial SQL, le pare-feu Web App ignore les champs de formulaire Web qui ne contiennent pas de caractères spéciaux. Étant donné que la plupart des serveurs SQL ne traitent pas les commandes SQL qui ne sont pas précédées d'un caractère spécial, l'activation de cette option peut réduire considérablement la charge sur le Web App Firewall et accélérer le traitement sans mettre en danger vos sites Web protégés.

Gestion des commentaires SQL : par défaut, le Web App Firewall vérifie tous les commentaires SQL à la recherche de commandes SQL injectées. Cependant, de nombreux serveurs SQL ignorent tout élément d'un commentaire, même s'il est précédé d'un caractère spécial SQL. Pour un traitement plus rapide, si votre serveur SQL ignore les commentaires, vous pouvez configurer le Web App Firewall pour ignorer les commentaires lors de l'examen des demandes de SQL injecté. Les options de gestion des commentaires SQL sont les suivantes :

- **ANSI**—Ignorez les commentaires SQL au format ANSI, qui sont normalement utilisés par les bases de données SQL basées sur UNIX. Par exemple :

- — (Deux traits d'union) - Il s'agit d'un commentaire qui commence par deux traits d'union et se termine par la fin de la ligne.
- {} - Accolades (Les accolades enferment le commentaire. Le {précède le commentaire, et le} le suit. Les accolades peuvent délimiter les commentaires sur une ou plusieurs lignes, mais les commentaires ne peuvent pas être imbriqués)
- `/**/: C style comments (Does not allow nested comments). Please note /*! <comment that begin with slash followed by asterisk and exclamation mark is not a comment > */`
- MySQL Server prend en charge certaines variantes de commentaires de style C. Ceux-ci vous permettent d'écrire du code qui inclut des extensions MySQL, mais qui est toujours portable, en utilisant les commentaires de la forme suivante : `/*! MySQL-specific code */`
- . # : Commentaires Mysql : Il s'agit d'un commentaire qui commence par # caractère.

- **Imbriqué**—Ignorer les commentaires SQL imbriqués, qui sont normalement utilisés par Microsoft SQL Server. Par exemple ; — (Deux traits d'union) et **/* */** (Autorise les commentaires imbriqués)
- **ANSI/imbriqué**—Ignorer les commentaires qui respectent les normes ANSI et SQL de commentaires imbriqués. Les commentaires qui correspondent uniquement à la norme ANSI, ou uniquement à la norme imbriquée, sont toujours vérifiés pour détecter le code SQL injecté.
- **Vérifier tous les commentaires** : permet de vérifier l'intégralité de la demande de code SQL injecté sans rien ignorer. C'est le réglage par défaut.

> **Conseil**
>
> Habituellement, vous ne devez pas choisir l'option imbriquée ou l'option ANSI/imbriquée, sauf si votre base de données principale s'exécute sur Microsoft SQL Server. La plupart des autres types de logiciels SQL Server ne reconnaissent pas les commentaires imbriqués. Si des commentaires imbriqués apparaissent dans une demande dirigée vers un autre type de serveur SQL, ils peuvent indiquer une tentative de violation de la sécurité sur ce serveur.

Vérifier les en-têtes de demande : activez cette option si, en plus d'examiner l'entrée dans les champs du formulaire, vous souhaitez examiner les en-têtes de demande pour des attaques par injection HTML SQL. Si vous utilisez l'interface graphique, vous pouvez activer ce paramètre dans le volet **Paramètres avancés -> Paramètres** de **profil** du profil Pare-feu de l'application Web.

> **Remarque :**
>
> Si vous activez l'indicateur d'en-tête Check Request, vous devrez peut-être configurer une règle de relaxation pour l'en-tête **User-Agent** . La présence du mot-clé SQL **like** et du caractère spécial SQL point-virgule (**;**) peut déclencher des requêtes fausses positives et bloquer qui contiennent cet en-tête.
> **Avertissement**

> Si vous activez à la fois la vérification et la transformation des en-têtes de requête, tous les caractères spéciaux SQL présents dans les en-têtes sont également transformés. Les en-têtes Accept, Accept-Charset, Accept-Encoding, Accept-Language, Expect et User-Agent contiennent normalement des points-virgules (;). L'activation simultanée de la vérification et de la transformation des en-têtes de demande peut entraîner des erreurs

InspectQueryContentTypes : configurez cette option si vous souhaitez examiner la partie requête de requête pour les attaques par injection SQL pour les types de contenu spécifiques. Si vous utilisez l'interface graphique, vous pouvez configurer ce paramètre dans le volet **Paramètres avancés** -> **Paramètres du profil** du profil App Firewall.

SQL Relaxations à grain fin

Le Web App Firewall vous permet d'exempter un champ de formulaire, un en-tête ou un cookie spécifique de la vérification d'inspection SQL Injection. Vous pouvez complètement contourner l'inspection d'un ou de plusieurs de ces champs en configurant les règles de relaxation pour la vérification SQL Injection.

Le Web App Firewall vous permet d'implémenter une sécurité plus stricte en affinant les règles de relaxation. Une application peut nécessiter la flexibilité nécessaire pour autoriser des modèles spécifiques, mais la configuration d'une règle de relaxation pour contourner l'inspection de sécurité peut rendre l'application vulnérable aux attaques, car le champ cible est exempté de l'inspection pour tout modèle d'attaque SQL. La relaxation fine SQL fournit la possibilité d'autoriser des modèles spécifiques et de bloquer le reste. Par exemple, le Web App Firewall possède actuellement un ensemble par défaut de plus de 100 mots-clés SQL. Étant donné que les pirates peuvent utiliser ces mots-clés dans des attaques SQL Injection, le Web App Firewall les signale comme des menaces potentielles. Vous pouvez détendre un ou plusieurs mots-clés considérés comme sûrs pour un emplacement spécifique. Le reste des mots-clés SQL potentiellement dangereux sont toujours vérifiés pour l'emplacement cible et continuent de déclencher les violations de vérification de sécurité. Vous avez maintenant un contrôle beaucoup plus serré.

Les commandes utilisées dans les relaxations comportent des paramètres facultatifs pour le **type de valeur** et **l'expression de valeur**. Vous pouvez spécifier si l'expression de valeur est une expression régulière ou une chaîne littérale. Le type de valeur peut être laissé vide ou vous avez une option pour sélectionner **Mot-clé** ou **SpecialString** ou **WildChar**.

> **Avertissement :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation imprudente des caractères génériques, et en

> particulier du métacaractère d'astérisque de points (.*) ou de la combinaison de caractères génériques, peut avoir des résultats que vous ne souhaitez pas, tels que le blocage de l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification d'injection HTML SQL aurait autrement bloquée.

Points à considérer :

- L'expression de valeur est un argument facultatif. Le nom d'un champ peut ne pas comporter d'expression de valeur.
- Un nom de champ peut être lié à plusieurs expressions de valeur.
- Les expressions de valeur doivent se voir attribuer un type de valeur. Le type de valeur SQL peut être : 1) Mot-clé, 2) SpecialString ou 3) WildChar.
- Vous pouvez définir plusieurs règles de relaxation par combinaison nom de champ/URL.

Utilisation de la ligne de commande pour configurer le contrôle d'injection SQL

Pour configurer les actions d'injection SQL et d'autres paramètres à l'aide de la ligne de commande :

Dans l'interface de ligne de commande, vous pouvez utiliser la commande **set appfw profile** ou la commande **add appfw profile** pour configurer les protections SQL Injection. Vous pouvez activer les actions de blocage, d'apprentissage, de journalisation et de statistiques et spécifier si vous souhaitez transformer les caractères spéciaux utilisés dans les chaînes d'attaque SQL Injection pour désactiver l'attaque. Sélectionnez le type de modèle d'attaque SQL (mots-clés, caractères génériques, chaînes spéciales) que vous souhaitez détecter dans les charges utiles et indiquez si vous souhaitez que le Web App Firewall inspecte également les en-têtes de requête pour les violations SQL Injection. Utilisez la commande **unset appfw profile** pour rétablir les paramètres configurés à leurs valeurs par défaut. Chacune des commandes suivantes ne définit qu'un seul paramètre, mais vous pouvez inclure plusieurs paramètres dans une seule commande :

- set application firewall profile "Parameter descriptions provided at the bottom of the page."
- `<name> -SQLInjectionAction ([block] [learn] [log] [stats])| [none])`
- set application firewall profile "Parameter descriptions provided at the bottom of the page."
- `<name> -SQLInjectionTransformSpecialChars (**ON** | OFF)`
- set application firewall profile "Parameter descriptions provided at the bottom of the page."
- `<name> -**SQLInjectionCheckSQLWildChars** (**ON** |**OFF**)`
- set application firewall profile "Parameter descriptions provided at the bottom of the page."
- `**<name> -**SQLInjectionType** ([**SQLKeyword**] | [**SQLSplChar**] | [**SQLSplCharANDKeyword**] | [**SQLSplCharORKeyword**])`
- **set application firewall profile** "Parameter descriptions provided at the bottom of the page."
- `<name> -**SQLInjectionParseComments** ([**checkall**] | [**ansi|nested **] | [**ansinested**])`
- **set application firewall profile "Parameter descriptions provided at the bottom of the page."

- <name> -CheckRequestHeaders (ON | OFF) Les descriptions des paramètres sont fournies en bas de la page.
- <name> - CheckRequestQueryNonHtml (ON | OFF) Les descriptions des paramètres sont fournies en bas de la page.

Pour configurer une règle de relaxation SQL Injection à l'aide de l'interface de commande

Utilisez la commande bind ou unbind pour ajouter ou supprimer une liaison, comme suit :

- bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX|NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor |SpecialString|Wildchar)[<valueExpression>][-isValueRegex (REGEX | NOTREGEX)]]
- unbind appfw profile <name> -SQLInjection <String> <formActionURL> [-location <location>] [-valueTyp (Keyword|SpecialString|Wildchar)[<valueExpression>]]

> **Remarque :**
>
> Vous pouvez trouver la liste des mots-clés SQL à partir du contenu du fichier de signatures par défaut en affichant l'objet de signature de vue, qui contient la liste des mots-clés SQL et des caractères spéciaux SQL.

Utilisation de l'interface graphique pour configurer la vérification de sécurité SQL Injection

Dans l'interface graphique, vous pouvez configurer le contrôle de sécurité Injection SQL dans le volet du profil associé à votre application.

Pour configurer ou modifier la vérification d'injection SQL à l'aide de l'interface graphique

1. Accédez à **Pare-feu d'application > Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Contrôles de sécurité**.

Le tableau de contrôle de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Deux options de configuration s'offrent à vous :

a. Si vous souhaitez activer ou désactiver les actions Block, Log, Stats et Learn pour HTML SQL Injection, vous pouvez sélectionner ou désactiver des cases à cocher dans le tableau, cliquer sur **OK**, puis cliquer sur **Enregistrer et fermer** pour fermer le volet de **contrôle de sécurité** .

b. Si vous souhaitez configurer d'autres options pour cette vérification de sécurité, double-cliquez sur Injection HTML SQL, ou sélectionnez la ligne et cliquez sur **Paramètres d'action**, pour afficher les options suivantes :

Transformer le caractère spécial SQL—Transformez tous les caractères spéciaux SQL dans la requête.

Rechercher les caractères génériques SQL : considérez les caractères génériques SQL dans la charge utile comme des modèles d'attaque.

Check Request Containing : type d'injection SQL (SQLKeyword, SQLSplChar, SQLSplCharAndKeyword ou SQLSplCharOrKeyword) à vérifier.

Gestion des commentaires SQL : type de commentaires (cocher tous les commentaires, ANSI, imbriqué ou ANSI/imbriqué) à vérifier.

Après avoir modifié l'un des paramètres ci-dessus, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau Contrôles de sécurité. Vous pouvez procéder à la configuration d'autres contrôles de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur **Enregistrer et fermer** pour fermer le volet Contrôle de sécurité.

Pour configurer une règle de relaxation d'injection SQL à l'aide de l'interface graphique

- Accédez à **Application Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Modifier**.
- Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
- Dans le tableau Règles de relaxation, double-cliquez sur l'entrée **Injection HTML SQL** ou sélectionnez-la et cliquez sur **Modifier**.
- **Dans la boîte de dialogue**Règles de relaxation pour injection SQL HTML**, effectuez des opérations d'**ajout**, de**modification**, de**suppression**, d'**activation ou de désactivation**des règles de relaxation.**

> **Remarque**
>
> Lorsque vous ajoutez une nouvelle règle, le champ **Expression de la valeur** n'est pas affiché, sauf si vous sélectionnez l'option **Mot-clé** ou **SpecialString** ou **WildChar** dans le champ **Type de valeur**.

Pour gérer les règles de relaxation par injection SQL à l'aide du visualiseur

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez mettre en surbrillance la ligne **HTML SQL Injection** et cliquer sur **Visualizer**. Le visualiseur pour les relaxations déployées vous offre la possibilité d' **ajouter** une nouvelle règle ou de **modifier** une règle existante. Vous pouvez également **activer** ou **désactiver** un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Afficher ou personnaliser les modèles d'injection à l'aide de l'interface graphique

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser les modèles d'injection.

Les modèles SQL par défaut sont spécifiés dans le fichier de signatures par défaut. Si vous ne liez aucun objet signature à votre profil, les modèles d'injection par défaut spécifiés dans l'objet signatures par défaut seront utilisés par le profil pour le traitement du contrôle de sécurité par injection de commandes. Les règles et les motifs, spécifiés dans l'objet signatures par défaut, sont en lecture seule. Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez modifier ou modifier ces modèles, effectuez une copie de l'objet sSignatures par défaut pour créer un objet Signature défini par l'utilisateur. Apportez des modifications aux modèles d'injection de commandes dans le nouvel objet Signature défini par l'utilisateur et utilisez cet objet signature dans votre profil qui traite le trafic pour lequel vous souhaitez utiliser ces modèles personnalisés.

Pour plus d'informations, voir Signatures.

Pour afficher les schémas d'injection par défaut à l'aide de l'interface graphique :

1. Accédez à **Application Firewall > Signatures**, sélectionnez ***Signatures par défaut**, puis cliquez sur **Modifier**.

1. Cliquez sur **Gérer les modèles CMD/SQL/XSS**. Le tableau **Gérer les chemins de script SQL/inter-sites** affiche les modèles relatifs à l'injection CMD/SQL/XS :



1. Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les modèles d'injection correspondants (mots-clés, chaînes spéciales, règles de transformation ou caractères génériques) utilisés par la vérification d'injection de la commande Web App Firewall.

Utilisation de la fonctionnalité d'apprentissage avec la vérification d'injection SQL

Lorsque l'action d'apprentissage est activée, le moteur d'apprentissage du Web App Firewall surveille le trafic et apprend les violations déclenchées. Vous pouvez inspecter périodiquement ces règles apprises. Après mûre réflexion, vous pouvez déployer la règle apprise en tant que règle de relaxation d'injection SQL.

Amélioration de**l'apprentissage par injection SQL : une amélioration**de l'apprentissage du Web App Firewall a été introduite dans la version 11.0 du logiciel NetScaler. Pour déployer une relaxation fine par injection SQL, le Web App Firewall propose un apprentissage précis de l'injection SQL. Le moteur d'apprentissage formule des recommandations concernant le type de valeur observé (mot-clé, SpecialString, Wildchar) et l'expression de valeur correspondante observée dans les champs d'entrée. En plus de vérifier les demandes bloquées pour déterminer si la règle actuelle est trop restrictive et doit être assouplie, vous pouvez consulter les règles générées par le moteur d'apprentissage pour déterminer quels types de valeur et expressions de valeur déclenchent des violations et doivent être traitées dans les règles de relaxation.

> **Important**
>
> Le moteur d'apprentissage du pare-feu Web App Firewall ne peut distinguer que les 128 premiers

> octets du nom. Si un formulaire comporte plusieurs champs dont les noms correspondent aux 128 premiers octets, le moteur d'apprentissage peut ne pas être en mesure de les distinguer. De même, la règle de relaxation déployée peut par inadvertance relâcher tous ces champs de l'inspection SQL Injection.
>
> **Remarque** Pour contourner l'enregistrement SQL de l'en-tête User-Agent, utilisez la règle de relaxation suivante :
>
> ```
> bind appfw profile your_profile_name -SQLInjection User-Agent ".*"-
> location HEADER
> ```

Pour afficher ou utiliser les données apprises à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `show appfw learningdata <profilename> SQLInjection`
- `rm appfw learningdata <profilename> -SQLInjection <string> <formActionURL > [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> SQLInjection`

Pour afficher ou utiliser les données apprises à l'aide de l'interface graphique

1. Accédez à **Pare-feu d'application > Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles apprises**. Vous pouvez sélectionner l'entrée **Injection HTML SQL** dans le tableau Règles apprises et double-cliquer dessus pour accéder aux règles apprises. Vous pouvez déployer les règles apprises ou modifier une règle avant de la déployer en tant que règle de relaxation. Pour annuler une règle, vous pouvez la sélectionner et cliquer sur le bouton **Ignorer** . Vous ne pouvez modifier qu'une règle à la fois, mais vous pouvez sélectionner plusieurs règles à déployer ou à ignorer.

Vous avez également la possibilité d'afficher une vue résumée des relaxations apprises en sélectionnant l'entrée **HTML SQL Injection** dans le tableau Règles apprises et en cliquant sur **Visualizer** pour obtenir une vue consolidée de toutes les violations apprises. Le visualiseur facilite la gestion des règles apprises. Il présente une vue complète des données sur un seul écran et facilite la prise de mesures sur un groupe de règles en un seul clic. Le principal avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de ces règles, en fonction du délimiteur et de l'URL d'action. Vous pouvez afficher 25, 50 ou 75 règles dans le visualiseur, en sélectionnant le nombre dans une liste déroulante. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer sous forme d'assouplissements. Vous pouvez également ignorer les règles pour les ignorer.

Utilisation de la fonctionnalité de journal avec le contrôle d'injection SQL

Lorsque l'action de journalisation est activée, les violations du contrôle de sécurité d'injection SQL HTML sont consignées dans le journal d'audit en tant que violations **APPFW_SQL** . Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur Syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Passez à l'interpréteur de commandes et repérez ns.logs dans le dossier **/var/log/** pour accéder aux messages de journal relatifs aux violations SQL Injection :

```
> Shell

## tail -f /var/log/ns.log | grep APPFW_SQL
```

Exemple de message de journal HTML SQL Injection lorsque la demande est transformée

```
1 Jun 26 21:08:41 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
      .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=54001
       method=GET request=http://aaron.stratum8.net/FFC/login.php?
      login_name=%27+or&passwd=and+%3B&drinking_pref=on&text_area=select
      +*+from+%5C+%3B&loginButton=ClickToLogin&as_sfid=AAAAAAXjnGN5gLH-
      hvhTOpIySEIqES7BjFRs5Mq0fwPp-3ZHDi5yWlRWByj0cVbMyy-
      Ens2vaaiULKOcUri4OD4kbXWwSY5s7I3QkDsrvIgCYMC9BMvBwY2wbNcSqCwk52lfE0k
      %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c msg= Special
      characters seen in fields cn1=74 cn2=762 cs1=pr_ffc cs2=PPE1 cs3=9
      ztIlf9p1H7p6Xtzn6NMygTv/QM0002 cs4=ALERT cs5=2015 act=transformed
2 <!--NeedCopy-->
```

Exemple de message de journal HTML SQL Injection lorsque la demande de publication est bloquée

```
1 Jun 26 21:30:34 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
      .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=9459
      method=POST request=http://aaron.stratum8.net/FFC/login_post.php msg
      =SQL Keyword check failed for field text_area="(')" cn1=78 cn2=834
      cs1=pr_ffc cs2=PPE1 cs3=eVJMMPtZ2XgylGrHjkx3rZLfBCI0002 cs4=ALERT
      cs5=2015 act=blocked
2 <!--NeedCopy-->
```

> **Remarque**
>
> Dans le cadre des modifications apportées au streaming dans la version 10.5.e (versions d'amélioration) et la version 11.0 ultérieure, nous traitons maintenant les données d'entrée en blocs. La correspondance de motifs RegEx est désormais limitée à 4K pour la correspondance de chaînes de caractères contiguës. Avec cette modification, les messages du journal des violations

> SQL peuvent inclure des informations différentes par rapport aux versions précédentes. Le mot-clé et le caractère spécial de l'entrée peuvent être séparés par de nombreux octets. Nous gardons maintenant une trace des mots-clés SQL et des chaînes spéciales lors du traitement des données, au lieu de mettre en mémoire tampon toute la valeur d'entrée. Outre le nom du champ, le message de journal inclut désormais le mot-clé SQL ou le caractère spécial SQL, ou à la fois le mot-clé SQL et le caractère spécial SQL, tels que déterminés par le paramètre configuré. Le reste de l'entrée n'est plus inclus dans le message de journal, comme illustré dans l'exemple suivant :
>
> **Exemple :**
>
> Dans 10.5, lorsque le Web App Firewall détecte la violation SQL, la chaîne d'entrée entière peut être incluse dans le message de journal, comme indiqué ci-dessous :
>
> ```
> SQL Keyword check failed for field text=\"select a name from testbed1
> ;(;)\".*<blocked>
> ```
>
> Dans les versions d'amélioration de 10.5.e prenant en charge le streaming côté demande et la version 11.0 ultérieure, nous consignons uniquement le nom du champ, le mot-clé et le caractère spécial (le cas échéant) dans le message de journal, comme indiqué ci-dessous :
>
> ```
> SQL Keyword check failed for field **text="select(;)"<blocked>
> ```
>
> Cette modification s'applique aux demandes contenant des types de contenu application/x-www-form-urlencoded, multipart/form-data ou text/x-gwt-rpc . Les messages de journal générés lors du traitement des charges utiles **JSON** ou **XML** ne sont pas affectés par cette modification.

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique inclut un outil utile (**Syslog Viewer**) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **Pare-feu des applications** > **Profils**, sélectionnez le profil cible, puis cliquez sur **Contrôles de sécurité**. Mettez en surbrillance la ligne **Injection HTML SQL** et cliquez sur **Journaux**. Lorsque vous accédez aux journaux directement à partir de la vérification par injection HTML SQL du profil, l'interface graphique filtre les messages de journal et affiche uniquement les journaux relatifs à ces violations de vérification de sécurité.
- ****Vous pouvez également accéder à la visionneuse Syslog en accédant à **NetScaler** > Système > Audit.**** Dans la section Messages d'audit, cliquez sur le lien **des messages Syslog** pour afficher le visualiseur Syslog, qui affiche tous les messages du journal, y compris les autres journaux de violations des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de contrôle de sécurité peuvent être déclenchées pendant le traitement des demandes.
- Accédez à **Pare-feu des applications** > **Stratégies** > **Audit**. Dans la section Messages d'audit,

cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation de vérification de sécurité.

La visionneuse Syslog basée sur HTML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour sélectionner les messages de journal pour la vérification **HTML SQL Injection**, filtrez en sélectionnant **APPFW** dans la liste déroulante Options du **module**. La liste **Type d'événement** offre un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **APPFW_SQL** et que vous cliquez sur le bouton **Appliquer**, seuls les messages de journal relatifs aux violations de vérification de sécurité **d'injection SQL** apparaissent dans la visionneuse Syslog.

Si vous placez le curseur sur la ligne d'un message de journal spécifique, plusieurs options, telles que **Module**, **Type d'événement, ID**d'événement,**IP du client**, etc. apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

La fonctionnalité**Cliquer pour déployer** n'est disponible que dans l'interface graphique. Vous pouvez utiliser la visionneuse Syslog non seulement pour afficher les journaux, mais également pour déployer des règles de relaxation d'injection SQL HTML basées sur les messages de journal pour les violations de vérification de sécurité du Web App Firewall. Les messages de journal doivent être au format de journal CEF pour cette opération. La fonctionnalité Cliquer pour déployer n'est disponible que pour les messages de journal générés par l'action Bloquer (ou ne pas bloquer). Vous ne pouvez pas déployer de règle de relaxation pour un message de journal concernant l'opération de transformation.

Pour déployer une règle de relaxation à partir de la visionneuse Syslog, sélectionnez le message de journal. Une case à cocher apparaît dans le coin supérieur droit de la case **Syslog Viewer** de la ligne sélectionnée. Activez la case à cocher, puis sélectionnez une option dans la liste Action pour déployer la règle de relaxation. Les options**Modifier et déployer**, **Déployer**et **Tout déployer** sont disponibles en tant qu'options **d'action** .

Les règles d'injection SQL déployées à l'aide de l'option Cliquer pour déployer n'incluent pas les recommandations de relaxation du grain fin.

Pour utiliser la fonctionnalité Cliquer pour déployer dans l'interface graphique :

1. Dans la visionneuse Syslog, sélectionnez **Pare-feu d'application** dans les options du **module** .
2. Sélectionnez **APP_SQL** comme **type d'événement** pour filtrer les messages de journal correspondants.
3. Cochez la case pour identifier la règle à déployer.
4. Utilisez la liste déroulante d'options **Action** pour déployer la règle de relaxation.
5. Vérifiez que la règle apparaît dans la section de règle de relaxation correspondante.

Statistiques relatives aux violations d'injection SQL

Lorsque l'action de statistiques est activée, le compteur pour la vérification d'injection SQL est incrémenté lorsque le Web App Firewall effectue une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, la demande d'une page contenant 3 violations SQL Injection incrémente le compteur de statistiques d'un, car la page est bloquée dès que la première violation est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente de trois le compteur de statistiques pour les violations et les journaux, car chaque violation génère un message de journal distinct.

Pour afficher les statistiques de vérification SQL Injection à l'aide de la ligne de commande :

À l'invite de commande, tapez :

> **sh appfw stats**

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> stat appfw profile <profile name>
```

Pour afficher les statistiques d'injection HTML SQL à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Pare-feu d'application**.
2. Dans le volet droit, accédez au lien **Statistiques** .
3. Utilisez la barre de défilement pour afficher les statistiques relatives aux violations et aux journaux d'injection SQL HTML. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Résumé

Notez les points suivants concernant la vérification par injection SQL :

- **Support intégré pour la protection par injection SQL** : NetScaler Web App Firewall protège contre l'injection SQL en surveillant une combinaison de mots clés SQL et de caractères spéciaux dans les paramètres du formulaire. Tous les mots-clés SQL, caractères spéciaux, caractères génériques et règles de transformation par défaut sont spécifiés dans le fichier /netscaler/default_custom_settings.xml.
- **Personnalisation** : vous pouvez modifier les mots-clés, les caractères spéciaux, les caractères génériques et les règles de transformation par défaut pour personnaliser l'inspection du contrôle de sécurité SQL en fonction des besoins spécifiques de votre application. Effectuez une copie de l'objet signature par défaut, modifiez les entrées existantes ou ajoutez de nouvelles entrées. Liez cet objet de signature à votre profil pour utiliser la configuration personnalisée.

- **Modèle de sécurité hybride** : les signatures et les protections de sécurité avancées utilisent les modèles de script SQL/intersite spécifiés dans l'objet de signature lié au profil. Si aucun objet de signature n'est lié au profil, les modèles de script SQL/intersite présents dans l'objet de signature par défaut sont utilisés.
- **Transform**—Notez les points suivants concernant l'opération de transformation :
  - L'opération de transformation fonctionne indépendamment des autres paramètres d'action SQL Injection. Si la transformation est activée et que le bloc, le journal, les statistiques et l'apprentissage sont tous désactivés, les caractères spéciaux SQL sont transformés.
  - Lorsque la transformation SQL est activée, les demandes des utilisateurs sont envoyées aux serveurs principaux après la transformation des caractères spéciaux SQL en mode non bloqué. Si l'action de blocage est activée, elle a priorité sur l'action de transformation. Si le type d'injection est spécifié en tant que caractère spécial SQL et que le bloc est activé, la demande est bloquée malgré l'action de transformation.
- **Relaxation et apprentissage à grains fins** : affinez la règle de relaxation pour détendre un sous-ensemble d'éléments SQL de l'inspection des contrôles de sécurité, mais détecter le reste. Le moteur d'apprentissage recommande un type de valeur spécifique et des expressions de valeur basées sur les données observées.
- **Cliquez pour déployer** : sélectionnez un ou plusieurs messages de journal des violations SQL dans la visionneuse syslog et déployez-les en tant que règles de relaxation.

Protection basée sur la grammaire SQL pour les charges utiles HTML et JSON

May 5, 2023

NetScaler Web App Firewall utilise une approche de correspondance de modèles pour détecter les attaques par injection SQL dans les charges utiles `HTTP` et `JSON` les charges utiles. L'approche utilise un ensemble de mots-clés prédéfinis et (ou) de caractères spéciaux pour détecter une attaque et la signaler comme une violation. Bien que cette approche soit efficace, elle peut entraîner de nombreux faux positifs, entraînant l'ajout d'une ou de plusieurs règles de relaxation. Surtout lorsque des mots couramment utilisés tels que « Sélectionner » et « De » sont utilisés dans une requête HTTP ou JSON. Nous pouvons réduire les faux positifs en implémentant la vérification de la protection de la grammaire SQL `HTML` et la `JSON` charge utile.

Dans l'approche de correspondance de modèles existante, une attaque par injection SQL est identifiée si un mot-clé prédéfini et/ou un caractère spécial sont présents dans une requête HTTP. Dans ce cas, il n'est pas nécessaire que l'instruction soit une instruction SQL valide. Toutefois, dans l'approche basée sur la grammaire, une attaque par injection SQL n'est détectée que si un mot-clé ou un caractère

spécial est présent dans une instruction SQL ou fait partie d'une instruction SQL, réduisant ainsi les scénarios faux positifs.

scénario d'utilisation de la protection basée sur la grammaire SQL

Considérez une déclaration intitulée « Sélectionnez mes billets et rencontrons à la station Union » présente dans une demande HTTP. Bien que l'instruction ne soit pas une instruction SQL valide, l'approche de correspondance de modèle existante détecte la demande comme une attaque par injection SQL car l'instruction utilise des mots-clés tels que « Select », « and » et « Union ». Toutefois, dans le cas de l'approche grammaire SQL, l'instruction n'est pas détectée comme une attaque de violation car les mots-clés ne sont pas présents dans une instruction SQL valide ou ne font pas partie d'une instruction SQL valide.

L'approche basée sur la grammaire peut également être configurée pour détecter les attaques par injection SQL dans les `JSON` charges utiles. Pour ajouter une règle de relaxation, vous pouvez réutiliser les règles de relaxation existantes. Les règles de relaxation à grains fins sont également applicables à la grammaire SQL, aux règles avec « mot clé » « ValueType ». Dans la grammaire `JSON` SQL, la méthode basée sur URL existante peut être réutilisée.

Configurez la protection basée sur la grammaire SQL à l'aide de l'interface de ligne

Pour implémenter la détection basée sur la grammaire SQL, vous devez configurer le paramètre « SQLInjectionGrammar » dans le profil Web App Firewall. Par défaut, le paramètre est désactivé. Toutes les actions SQL Injection existantes sont prises en charge, sauf l'apprentissage. Tout nouveau profil créé après une mise à niveau prend en charge la grammaire d'injection SQL et le type par défaut reste « caractère spécial ou mot-clé » et il doit être explicitement activé.

À l'invite de commande, tapez :

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Exemple :

```
add appfw profile profile1 -SQLInjectionAction Block -SQLInjectionGrammar ON
```

Configurer la protection de correspondance de motifs SQL et la protection basée sur la grammaire à l'aide de l'interface de ligne de commande

Si vous avez activé les approches grammaticales et les approches de correspondance de modèle, l'appliance effectue d'abord une détection grammaire et s'il existe une détection par injection SQL

avec le type d'action défini sur bloquer, la demande est bloquée (sans vérifier la détection à l'aide de la correspondance de modèle).

À l'invite de commande, tapez :

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
      SQLInjectionGrammar ON  - SQLInjectionType <Any action other than  '
      None' : SQLSplCharANDKeyword/ SQLSplCharORKeyword/ SQLSplChar/
      SQLKeyword>
2 <!--NeedCopy-->
```

Exemple :

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType SQLSplChar
```

Configurer la vérification SQL Injection uniquement avec une protection grammaire à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
      SQLInjectionGrammar ON  - SQLInjectionType None
2 <!--NeedCopy-->
```

Exemple :

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType None
```

Liez les règles de relaxation pour la protection basée sur la grammaire SQL à l'aide de l'interface de ligne de commande

Si votre application exige que vous contourniez le contrôle d' SQL injection pour un « ELEMENT » ou un « ATTRIBUT » spécifique dans la charge utile, vous devez configurer une règle de relaxation.

> **Remarque :**
>
> Les règles de relaxation avec « mot-clé » ValueType sont évaluées uniquement lorsque l'appliance effectue une détection à l'aide de la SQL grammaire.

Les règles de relaxation de l'inspection par injection de SQL commandes ont la syntaxe suivante. À l'invite de commande, tapez :


```
bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX|
    NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor
    |SpecialString|Wildchar) [<valueExpression>][-isValueRegex (REGEX |
    NOTREGEX) ]]
<!--NeedCopy-->
```

Exemple :

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```

Configurer la protection basée sur la grammaire SQL pour la charge utile JSON à l'aide de l'interface de ligne de commande

Pour implémenter la détection basée sur la grammaire SQL pour la charge utile JSON, vous devez configurer le paramètre « JSONSQLInjectionGrammar » dans le profil Web App Firewall. Par défaut, le paramètre est désactivé. Toutes les actions SQL Injection existantes sont prises en charge, sauf l'apprentissage. Tout nouveau profil créé après une mise à niveau prend en charge la grammaire d'injection SQL et le type par défaut reste « caractère spécial ou mot-clé » et vous devez l'activer explicitement.

À l'invite de commande, tapez :

```
add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
    action-name> -JSONSQLInjectionGrammar ON/OFF
<!--NeedCopy-->
```

Exemple :

```
add appfw profile profile1 -type JSON -JSONSQLInjectionAction Block -JSONSQLInjectionG
 ON
```

Configurer la protection de correspondance de motifs SQL et la protection grammaire à l'aide de l'interface de ligne de commande

Si vous avez activé les vérifications de grammaire et de correspondance de modèle, l'appliance effectue d'abord une détection grammaire et s'il existe une détection par injection SQL avec le type d'action bloqué, la demande est bloquée (sans vérifier la détection à l'aide de la correspondance de modèle).

> **Remarque :**
>
> Les règles de relaxation avec « mot-clé » ValueType sont évaluées uniquement lorsque l'appliance effectue une détection à l'aide de la grammaire SQL.

À l'invite de commande, tapez :

```
add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
    action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType <Any
     action other than  'None' : SQLSplCharANDKeyword/
    SQLSplCharORKeyword/ SQLSplChar/ SQLKeyword>
<!--NeedCopy-->
```

Exemple :

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType SQLSplChar
```

Configurer la protection basée sur la grammaire SQL pour la charge utile JSON à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
    action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType None
    `\
<!--NeedCopy-->
```

Exemple :

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType None
```

Lier des règles de relaxation basées sur des URL pour une protection grammaire JSON SQL à l'aide de l'interface de ligne de commande

Si votre application exige que vous contourniez l'inspection par injection de `JSON` commandes pour un « ELEMENT » ou « ATTRIBUTE » spécifique dans la charge utile, vous pouvez configurer une règle de relaxation.
La `JSON` commande Règles de relaxation de l'inspection par injection a la syntaxe suivante. À l'invite de commande, tapez :

```
bind appfw profile <profile name>  - JSONCMDURL <expression> -comment <
    string> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED ) -state (
    ENABLED | DISABLED )
```



```
<!--NeedCopy-->
```

Exemple :

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```

Configurer la protection basée sur la grammaire SQL à l'aide de l'interface graphique

Effectuez la procédure GUI pour configurer la détection d'injection HTML SQL basée sur la grammaire.

1. Dans le volet de navigation, accédez à **Sécurité > Profils**.
2. Sur la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Contrôles de sécurité** sous Paramètres **avancés**.
4. Dans la section **Vérification de sécurité**, accédez aux paramètres **HTML SQL Injection** .
5. Cliquez sur l'icône exécutable située près de la case à cocher.
6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres d'injection SQL HMTL** .



7. Activez la **case à cocher Vérifier l'utilisation de la grammaire SQL** .
8. Cliquez sur **OK**.

Configurer la protection basée sur la grammaire SQL pour la charge utile JSON à l'aide de l'interface graphique

Effectuez la procédure GUI pour configurer la détection d'injection JSON SQL basée sur la grammaire.

1. Dans le volet de navigation, accédez à **Sécurité > Profils**.
2. Sur la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Contrôles de sécurité** sous Paramètres **avancés**.
4. Dans la section **Vérifications de sécurité**, accédez aux paramètres **d'injection SQL JSON** .
5. Cliquez sur l'icône exécutable située près de la case à cocher.
6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres d'injection JSON SQL**.
7. Activez la **case à cocher Vérifier l'utilisation de la grammaire SQL** .
8. Cliquez sur **OK**.



Protection basée sur la grammaire par injection de commandes pour la charge utile HTML

May 5, 2023

NetScaler Web App Firewall utilise une approche de correspondance de modèles pour détecter les attaques par injection de commandes dans les charges utiles HTML. L'approche utilise un ensemble de mots-clés prédéfinis et (ou) de caractères spéciaux pour détecter une attaque et la signaler comme une violation. Bien que cette approche soit efficace, elle peut entraîner de nombreux faux positifs qui conduisent à l'ajout d'une ou de plusieurs règles d'assouplissement. Surtout lorsqu'un mot couramment utilisé tel que « Exit » est utilisé dans une requête HTTP. Nous pouvons réduire les faux positifs

en implémentant la vérification de protection basée sur la grammaire par injection de commandes pour la charge utile HTML.

Dans l'approche de correspondance de modèles, une attaque par injection de commande est identifiée si un mot-clé prédéfini et/ou (ou) un caractère spécial sont présents dans une requête HTTP. Dans ce cas, il n'est pas nécessaire que l'instruction soit une instruction d'injection de commande valide. Mais dans l'approche basée sur la grammaire, une attaque par injection de commande n'est détectée que si un mot-clé ou un caractère spécial est présent dans une instruction d'injection de commande. Par conséquent, les scénarios de faux positifs sont réduits.

Scénario d'utilisation de la protection basée sur la grammaire de

Prenons une déclaration : « Rush to the exit ! » présent dans une requête HTTP. Bien que l'instruction ne soit pas une instruction d'injection de commande valide, l'approche de correspondance de modèle détecte la demande comme une attaque par injection de commande en raison du mot-clé « exit ». Mais dans l'approche basée sur la grammaire d'injection de commandes, l'instruction n'est pas détectée comme une attaque de violation car les mots-clés ne sont pas présents dans une instruction d'injection de commande valide.

Configuration du paramètre de protection basé sur la grammaire d'injection de commandes à l'aide

Pour implémenter la détection basée sur la grammaire par injection de commandes, vous devez configurer le paramètre « CmdInjectionGrammar » dans le profil Web App Firewall. Par défaut, le paramètre est désactivé. Toutes les actions d'injection de commandes existantes sont prises en charge sauf l'apprentissage. Tout nouveau profil créé après une mise à niveau prend en charge la grammaire d'injection de commandes Le nouveau profil conserve le type par défaut « caractère spécial ou mot-clé » et la grammaire d'injection de commandes doit être explicitement activée.

À l'invite de commande, tapez :

```
1 add appfw profile <profile-name>  - CMDInjectionAction <action-name> -
     CMDInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Exemple :

```
1 add appfw profile profile1  - CMDInjectionAction Block  -
     CMDInjectionGrammar ON
2 <!--NeedCopy-->
```


Configurer la protection par correspondance de modèle d'injection de commandes et la protection basée sur la grammaire à l'aide

Si vous avez activé les approches basées sur la grammaire et la correspondance de modèles, l'appliance effectue d'abord une détection basée sur la grammaire. Si une injection de commande est détectée avec le type d'action défini sur « bloquer », la demande est bloquée (sans vérification de la détection à l'aide de la correspondance de motifs).

À l'invite de commande, tapez :

```
1 add appfw profile <profile-name> -CMDInjectionAction <action-name> -
    CMDInjectionGrammar ON -CMDInjectionType <Any action other than 'None' : CMDSplCharANDKeyword/ CMDSplCharORKeyword/ CMDSplChar/
    CMDKeyword>
2 <!--NeedCopy-->
```

Exemple :

```
1 add appfw profile p1 -CMDInjectionAction block - CMDInjectionGrammar
    ON -CMDInjectionType CMDSplChar
2 <!--NeedCopy-->
```

Configurer la vérification d'injection de commandes uniquement avec une protection basée sur la grammaire à l'aide

À l'invite de commande, tapez :

```
1 add appfw profile <profile-name> -CMDInjectionAction <action-name> -
    CMDInjectionGrammar ON -CMDInjectionType None
2 <!--NeedCopy-->
```

Exemple :

```
1 add appfw profile p1 -CMDInjectionAction block - CMDInjectionGrammar
    ON -CMDInjectionType None
2 <!--NeedCopy-->
```

Règles de relaxation de liaison pour la protection basée sur la grammaire par injection de commandes à l'aide

Si votre application exige que vous contourniez la vérification d'injection de commande pour un « ELEMENT » ou un « ATTRIBUTE » spécifique dans la charge utile HTML, vous devez configurer une règle de relaxation.

> **Remarque :**
>
> les règles de relaxation avec le ValueType comme « mot-clé » ne sont évaluées que lorsque l'appliance effectue une détection à l'aide de la grammaire d'injection de commandes.

Les règles de relaxation de l'inspection par injection de commandes ont la syntaxe suivante. À l'invite de commande, tapez :

```
bind appfw profile <name> -CMDInjection <String> [isRegex(REGEX|
    NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor
    |SpecialString|Wildchar) [<valueExpression>][-isValueRegex (REGEX |
    NOTREGEX) ]]
<!--NeedCopy-->
```

Exemple :

```
bind appfw profile p1 -cmdinjection abc http://10.10.10.10/

bind appfw profile p1  - cmdinjection 'abc[0-9]+' http://10.10.10.10/ -
    isregex regEX

bind appfw profile p1  - cmdinjection 'name' http://10.10.10.10/ -
    valueType Keyword 'exi[a-z]+' -isvalueRegex regEX
<!--NeedCopy-->
```

Configuration de la protection basée sur la grammaire par injection de commandes à l'aide

Effectuez les étapes suivantes pour configurer la détection par injection de commandes HTML basée sur la grammaire.

1. Accédez à**Sécurité > Profil du Web App Firewall NetScaler > Profils**.
2. Sélectionnez un profil et cliquez sur **Modifier**.
3. Accédez à la section**Paramètres avancés**et cliquez sur**Contrôles de sécurité**.
4. Activez la case à cocher **Injection de commandes HTML** et cliquez sur**Paramètres d'action**.



5. Activez la case à cocher **Vérifier en utilisant la grammaire CMD**.
6. Sélectionnez **Aucun** dans **Demande de vérification contenant**.



7. Cliquez sur**OK**.

Règles de relaxation et de refus pour gérer les attaques par injection HTML SQL

August 20, 2021

En cas de trafic entrant, la logique de détection des violations vérifie les violations de la circulation. Si aucune attaque par injection HTML SQL n'est détectée, le trafic est autorisé à passer. Mais si une violation est détectée, les règles de relaxation (autorisation) et de refus définissent comment gérer les

violations. Si le contrôle de sécurité est configuré en mode Autoriser (mode par défaut), la violation détectée est bloquée à moins que l'utilisateur n'ait explicitement configuré une règle de relaxation ou d'autorisation.

En plus du mode Autoriser, le contrôle de sécurité peut également être configuré en mode Refuser et utiliser des règles de refus pour gérer les violations. Si le contrôle de sécurité est configuré dans ce mode, les violations détectées sont bloquées si un utilisateur a explicitement configuré une règle de refus. Si aucune règle de refus n'est configurée, l'action configurée par l'utilisateur est appliquée.

L'illustration suivante explique comment autoriser et refuser les modes de fonctionnement :



1. Lorsqu'une violation est détectée, les règles de relaxation (autorisation) et de refus définissent la façon de gérer les violations.
2. Si le contrôle de sécurité est configuré en mode Refuser (s'il est configuré en mode Autoriser, passez à l'étape 5), la violation est bloquée sauf si vous avez explicitement configuré une règle de refus.
3. Si la violation correspond à une règle de refus, l'appliance bloque le trafic.
4. Si la violation du trafic ne correspond pas à une règle, l'appliance applique une action définie par l'utilisateur (bloquer, réinitialiser ou supprimer).
5. Si le contrôle de sécurité est configuré en mode Autoriser, le module Web App Firewall vérifie si une règle d'autorisation est configurée.
6. Si la violation correspond à une règle d'autorisation, l'appliance autorise le trafic à contourner autrement, il est bloqué.

Configurer le mode de relaxation et d'application de l'enregistrement de sécurité

À l'invite de commandes, tapez :

```
set appfw profile <name>   - SQLInjectionAction [block stats learn]  -
    SQLInjectionRuleType [ALLOW DENY]
```



```
<!--NeedCopy-->
```

Exemple :

```
set appfw profile prof1 sqlInjectionAction block -sqlInjectionRuleType
ALLOW DENY
```

Lier les règles de relaxation et d'application au profil Web Application Firewall

À l'invite de commandes, tapez :

```
bind appfw profile <name> -SQLInjection <string> <formActionURL>
<!--NeedCopy-->
```

Exemple :

```
bind appfw profile p1 -SQLInjection field_f1 "/login.php"-RuleType ALLOW
bind appfw profile p2 -SQLInjection field_f1 "/login.php"-RuleType ALLOW
```

Contrôle de protection par injection de commandes HTML

May 5, 2023

La vérification d'injection de commandes **HTML** examine si le trafic entrant comporte des commandes non autorisées qui enfreignent la sécurité du système ou modifient le système. Si le trafic contient des commandes malveillantes lorsqu'il est détecté, l'appliance bloque la demande ou exécute l'action configurée.

Le profil NetScaler Web App Firewall est désormais amélioré grâce à un nouveau contrôle de sécurité pour les attaques par injection de commandes. Lorsque le contrôle de sécurité par injection de commandes examine le trafic et détecte des commandes malveillantes, l'appliance bloque la demande ou exécute l'action configurée.

Lors d'une attaque par injection de commandes, l'attaquant vise à exécuter des commandes non autorisées sur le système d'exploitation NetScaler. Pour ce faire, l'attaquant injecte des commandes du système d'exploitation à l'aide d'une application vulnérable. Une appliance NetScaler est vulnérable aux attaques par injection si l'application transmet des données dangereuses (formulaires, cookies ou en-tête) au shell du système.

Comment fonctionne la protection par injection de commande

1. Pour une demande entrante, WAF examine le trafic à la recherche de mots-clés ou de caractères spéciaux. Si la demande entrante ne comporte aucun modèle correspondant à l'un des mots clés ou caractères spéciaux refusés, la demande est autorisée. Sinon, la demande est bloquée, abandonnée ou redirigée en fonction de l'action configurée.
2. Si vous préférez exclure un mot clé ou un caractère spécial de la liste, vous pouvez appliquer une règle d'assouplissement pour contourner le contrôle de sécurité dans certaines conditions.
3. Vous pouvez activer la journalisation pour générer des messages de journal. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.
4. Vous pouvez également activer la fonctionnalité de statistiques pour collecter des données statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si des demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer la nouvelle règle de relaxation ou modifier celle existante.

Mots clés et caractères spéciaux refusés pour la vérification de l'injection de commande

Pour détecter et bloquer les attaques par injection de commandes, l'appliance dispose d'un ensemble de modèles (mots-clés et caractères spéciaux) définis dans le fichier de signature par défaut. Voici une liste de mots-clés bloqués lors de la détection d'injection de commande.

```
    <commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
…
</commandinjection>
<!--NeedCopy-->
```

Les caractères spéciaux définis dans le fichier de signature sont les suivants :

```
| ; & $ > < '\ ! >> ##
```

Configuration de la vérification de l'injection de commandes à l'aide de l'interface de ligne de commande

Dans l'interface de ligne de commande, vous pouvez utiliser la commande set the profile ou la commande add the profile pour configurer les paramètres d'injection de commandes. Vous pouvez activer

les actions de blocage, de journalisation et de statistiques. Vous devez également définir les mots clés et les chaînes de caractères que vous souhaitez détecter dans les charges utiles.

À l'invite de commande, tapez :

```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Remarque :**
>
> Par défaut, l'action d'injection de commande est définie sur « Aucune ». En outre, le type d'injection de commande par défaut est défini comme `CmdSplCharANDKeyWord`.

Exemple :

```
set appfw profile profile1 -cmdInjectionAction block -CMDInjectionType
CmdSplChar
```

Où, les actions d'injection de commandes disponibles sont les suivantes :

- Aucun : désactive la protection par injection de commandes.
- Log - Consigne les violations d'injection de commande pour le contrôle de sécurité.
- Bloquer : bloque le trafic qui enfreint le contrôle de sécurité de l'injection de commande.
- Stats - Génère des statistiques sur les violations de sécurité liées à l'injection

Où, les types d'injection de commandes disponibles sont les suivants :

- Cmd SplChar. Vérifie les caractères spéciaux
- Mot-clé CMD. Vérifie les mots-clés d'injection de commandes
- CmdSplCharandKeyword. Vérifie les caractères spéciaux et l'injection de commandes. Mots clés et blocs uniquement si les deux sont présents.
- cmdsplcharorMot-clé. Vérifie les caractères spéciaux et les mots-clés d'injection de commandes et bloque si l'un d'entre eux est trouvé.

Configuration des règles de relaxation pour le contrôle de la protection par injection de commandes

Si votre application exige que vous contourniez l'inspection par injection de commandes pour un ÉLÉMENT ou UN ATTRIBUT spécifique de la charge utile, vous pouvez configurer une règle de relaxation.

Les règles de relaxation de l'inspection par injection de commandes ont la syntaxe suivante :

```
bind appfw profile <profile name> -cmdInjection <string> <URL> -isregex <
REGEX/NOTREGEX>
```


Exemple de règle de relaxation pour Regex dans l'en-tête

```
bind appfw profile sample -CMDInjection hdr "http://10.10.10.10/"-location
heaDER -valueType Keyword '[a-z]+grep'-isvalueRegex REGEX
```

Par conséquent, l'injection exempte la vérification d'injection de commande autorise l'en-tête `hdr` contenant des variantes de « grep ». «

Exemple de règle de relaxation avec ValueType en tant que regex dans le cookie

```
bind appfw profile sample -CMDInjection ck_login "http://10.10.10.10/"-
location cookie -valueType Keyword 'pkg[a-z]+'-isvalueRegex REGEX
```

Configuration du contrôle d'injection de commandes à l'aide de l'interface graphique NetScaler

Procédez comme suit pour configurer le contrôle d'injection de commandes.

1. Accédez à **Sécurité > NetScaler Web App Firewall and Profiles**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page de **profil du Web App Firewall NetScaler**, accédez à la section **Paramètres avancés** et cliquez sur Contrôles **de sécurité**.



1. Dans la section **Contrôles de sécurité**, sélectionnez **Injection de commandes HTML** et cliquez sur Paramètres **d'action** .
2. Sur la page **Paramètres d'injection de commandes HTML**, définissez les paramètres suivants :
   a) Des actions. Sélectionnez une ou plusieurs actions à effectuer pour le contrôle de sécurité par injection de commandes.
   b) Demande de contrôle contenant. Sélectionnez un modèle d'injection de commande pour vérifier si la demande entrante possède le modèle.
3. Cliquez sur **OK**.



Afficher ou personnaliser les modèles d'injection de commandes à l'aide de l'interface graphique

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser les modèles d'injection de commandes **HTML** .

Les modèles d'injection de commandes par défaut sont spécifiés dans le fichier de signatures par défaut. Si vous ne liez aucun objet signature à votre profil, les modèles d'injection de commandes HTML par défaut spécifiés dans l'objet signatures par défaut seront utilisés par le profil pour le traitement du contrôle de sécurité des injections de commandes. Les règles et les motifs, spécifiés dans l'objet signatures par défaut, sont en lecture seule. Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez modifier ou modifier ces modèles, effectuez une copie de l'objet sSignatures par défaut pour créer un objet Signature défini par l'utilisateur. Apportez des modifications aux modèles d'injection de commandes dans le nouvel objet Signature défini par l'utilisateur et utilisez cet objet signature dans votre profil qui traite le trafic pour lequel vous souhaitez utiliser ces modèles personnalisés.

Pour plus d'informations, voir Signatures.

Pour afficher les modèles d'injection de commandes par défaut à l'aide de l'interface graphique :

1. Accédez à **Application Firewall > Signatures**, sélectionnez ***Signatures par défaut**, puis cliquez sur **Modifier**.

1. Cliquez sur **Gérer les modèles CMD/SQL/XSS**. Le tableau **Chemins CMD/SQL/XSS (lecture seule)** présente les schémas relatifs à l' `CMD`/`SQL`/`XSS` injection :



1. Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les modèles d'injection de commandes correspondants (mots-clés, chaînes spéciales, règles de transformation ou caractères génériques) utilisés par la vérification d'injection de commande Web App Firewall.

Pour personnaliser un modèle d'injection de commandes à l'aide de l'interface graphique

Vous pouvez modifier l'objet signature défini par l'utilisateur pour personnaliser les mots-clés **CMD**, les chaînes spéciales et les caractères génériques. Vous pouvez ajouter de nouvelles entrées ou sup-

primer celles qui existent déjà. Vous pouvez modifier les règles de transformation des chaînes spéciales d'injection de commandes.

1. **Accédez à Application Firewall > Signatures**, mettez en surbrillance la signature définie par l'utilisateur cible, puis cliquez sur **Ajouter**. Cliquez sur **Gérer les modèles CMD/SQL/XSS**.
2. Dans la page **Gérer les chemins CMD/SQL/XSS**, sélectionnez la ligne d'injection CMD cible.
3. Cliquez sur **Gérer les éléments**, **Ajouter**ou **supprimer** un élément d'injection de commande.

> **Avertissement :**
>
> Vous devez être prudent avant de supprimer ou de modifier un élément d'injection de commande par défaut, ou de supprimer le chemin CMD pour supprimer la ligne entière. Les règles de signature et le contrôle de sécurité de l'injection de commandes reposent sur ces éléments pour détecter les attaques par injection de commandes afin de protéger vos applications. La personnalisation des modèles SQL peut rendre votre application vulnérable aux attaques par injection de commandes si le modèle requis est supprimé pendant la mise à jour.



Affichage des statistiques sur le trafic d'injection de commandes et les violations

La page des **statistiques du Web App Firewall NetScaler** affiche les détails du trafic de sécurité et des violations de sécurité sous forme de tableau ou de graphique.

Pour afficher les statistiques de sécurité à l'aide de l'interface de commande.

À l'invite de commande, tapez :

```
stat appfw profile profile1
```


Statistiques de trafic du profil Appfw	Taux (/s)	Total :
Demandes	0	0
Bytes de requête	0	0
Réponses	0	0
octets de réponse	0	0
Abandons	0	0
Redirections	0	0
Temps de réponse moyen à long terme (ms)	–	0
Temps de réponse de l’avenue récente (ms)	–	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
URL de démarrage	0	0
Refuser URL	0	0
En-tête de référence	0	0
débordement de tampon	0	0
Cohérence des cookies	0	0
Détournement de cookies	0	0
Balise de formulaire CSRF	0	0
Script intersite HTML	0	0
Injection HTML SQL	0	0
Format de champ	0	0
cohérence sur le terrain	0	0
Carte de crédit	0	0
Objet sûr	0	0
Violations de signature	0	0
Type de contenu	0	0
Déni de service JSON	0	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
Injection SQL JSON	0	0
Script intersite JSON	0	0
Types de téléchargement de fichiers	0	0
Déduire la charge utile XML du type de contenu	0	0
Injection de CMD HTML	0	0
Format XML	0	0
Déni de service XML (XDoS)	0	0
Validation des messages XML	0	0
Interopérabilité des services	0	0
Injection SQL XML	0	0
Script intersite XML	0	0
Pièce jointe XML	0	0
Violations d'erreur SOAP	0	0
Violations génériques XML	0	0
Nombre total de violations	0	0

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
Journaux d'URL de démarrage	0	0
Journaux d'URL refusées	0	0
Journaux d'en-tête Referer	0	0
Logs de débordement	0	0
Journaux de cohérence des cookies	0	0
Journaux de détournement de cookies	0	0

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
CSRF à partir des journaux de balises	0	0
Journaux de script intersite HTML	0	0
Journaux de transformation de script intersite HTML	0	0
Journaux d'injection HTML SQL	0	0
Journaux de transformation HTML SQL	0	0
Journaux de format de champ	0	0
Journaux de cohérence des champs	0	0
Cartes de crédit	0	0
Journaux de transformation des cartes de crédit	0	0
Journaux des objets sécurisés	0	0
Journaux de signature	0	0
Journaux du type de contenu	0	0
Journaux de déni de service JSON	0	0
Journaux d'injection JSON SQL	0	0
Journaux de script intersite JSON	0	0
Journaux des types de téléchargement de fichiers	0	0
Déduire la charge utile XML du type de contenu L	0	0
Journaux d'injection de commandes HTML	0	0
Journaux au format XML	0	0

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
Journaux de déni de service XML (XDoS)	0	0
Journaux de validation des messages XML	0	0
Journaux WSI	0	0
Journaux d'injection SQL XML	0	0
Journaux de script intersite XML	0	0
Journaux des pièces jointes XML	0	0
Journaux d'erreurs SOAP	0	0
Journaux génériques XML	0	0
Nombre total de messages journaux	0	0

Taux de statistiques de réponse aux erreurs du serveur (/s) > Total |
|—|–|–|
Erreurs client HTTP (4xx Resp) | 0 | 0| Erreurs serveur
HTTP (5xx Resp) | 0 | 0 |

Affichage des statistiques d'injection de commandes HTML à l'aide de l'interface graphique NetScaler

Procédez comme suit pour afficher les statistiques d'injection de commandes :

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet de détails, sélectionnez un profil de Web App Firewall et cliquez sur **Statistiques**.
3. La page des **statistiques du pare-feu NetScaler Web App** affiche le trafic d'injection de commandes HTML et les détails des violations.
4. Vous pouvez sélectionner **Vue tabulaire** ou passer en mode Affichage **graphique pour afficher** les données sous forme de tableau ou de graphique.

Statistiques du trafic d'injection de commandes HTML

HTML SQL Injection logs	0	0
HTML SQL transform logs	0	0
Field format logs	0	0
Field consistency logs	0	0
Credit cards	0	0
Credit card transform logs	0	0
Safe object logs	0	0
Signature logs	0	0
Content Type logs	0	0
JSON Denial of Service logs	0	0
JSON SQL injection logs	0	0
JSON Cross-Site Scripting logs	0	0
File upload types logs	0	0
Infer Content Type XML Payload Logs	0	0
HTML Command Injection logs	0	0
XML Format logs	0	0
XML Denial of Service(XDoS) logs	0	0
XML Message Validation logs	0	0
WSI logs	0	0
XML SQL Injection logs	0	0
XML XSS logs	0	0
XML Attachment logs	0	0

Statistiques sur les violations liées à l'injection de commandes HTML

HTML/XML/JSON Violation Statistics

	Rate (/s)	Total	
Start URL	0	0	0%
Deny URL	0	0	0%
Referer header	0	0	0%
Buffer overflow	0	0	0%
Cookie consistency	0	0	0%
Cookie hijacking	0	0	0%
CSRF form tag	0	0	0%
HTML Cross-site scripting	0	0	0%
HTML SQL injection	0	0	0%
Field format	0	0	0%
Field consistency	0	0	0%
Credit card	0	0	0%
Safe object	0	0	0%
Signature logs	0	0	0%
Content Type	0	0	0%
JSON Denial of Service	0	0	0%
JSON SQL injection	0	0	0%
JSON Cross-Site Scripting	0	0	0%
File Upload Types	0	0	0%
Infer Content Type XML Payload	0	0	0%
HTML CMD Injection	0	0	0%
XML Format	0	0	0%
XML Denial of Service (XDoS)	0	0	
XML Message Validation	0	0	
Web Services Interoperability	0	0	

Support de mots clés personnalisé pour la charge utile HTML

May 5, 2023

À partir de la version 13.1 build 27.xx de NetScaler, vous pouvez ajouter les mots clés de votre choix et vérifier si ces mots clés configurés sont présents dans la charge utile HTML.

L'injection SQL et l'injection de commandes ont un ensemble prédéfini de mots-clés ou de modèles qu'elles recherchent dans les demandes entrantes. Ces ensembles prédéfinis de mots clés peuvent ne pas couvrir tous les mots clés selon vos besoins et peuvent entraîner une augmentation du nombre de faux positifs. Grâce à cette fonctionnalité, vous pouvez ajouter des mots-clés qui ne sont pas couverts par les contrôles d'injection SQL et d'injection de commandes et ainsi réduire les faux positifs.

Après avoir ajouté les mots clés, vous pouvez configurer l'appliance NetScaler pour vérifier si les mots clés ajoutés sont détectés dans les demandes entrantes. Vous pouvez ensuite configurer l'appliance NetScaler pour effectuer l'une des actions suivantes :

- **Aucune** — Aucune mesure n'est prise. Cette action est la valeur par défaut.
- **Journal** - Consigne toutes les demandes qui correspondent à l'URL et dont les mots-clés sont configurés.
- **Bloquer** : bloque toutes les demandes qui correspondent à l'URL et dont les mots-clés sont configurés.
- **Stats** — Incrémente le compteur de journaux pour chaque demande qui correspond à l'URL et possède les mots-clés configurés.

Ajoutez des mots clés personnalisés à l'aide de la

L'ajout d'un mot clé personnalisé à l'aide de la CLI implique les étapes suivantes :

1. Configurez un profil de pare-feu d'application Web et définissez une action lorsque le mot-clé personnalisé est détecté dans la demande entrante.

   ```
   set appfw profile <profile-name>  -blockKeywordAction (block | log
       | stats | none)
   <!--NeedCopy-->
   ```

   Par défaut, -BlockKeywordAction est défini sur none.

   Exemple :

   ```
   set appfw profile test_profile -blockKeywordAction none
   <!--NeedCopy-->
   ```

2. Liez le profil de pare-feu de l'application Web à vos mots clés personnalisés.


```
bind appfw profile <profile_name> -blockKeyword <keyword_name> -
    BlockKeywordType <literal|PCRE > -fieldName <field_name> -
    formURL <URL> -isFieldNameRegex <REGEX|NOTREGEX> -state <enable
    /disable> -comment <text>
<!--NeedCopy-->
```

Exemple :

Pour ajouter **blockword** en tant que mot-clé personnalisé et le lier à **test_profile**, exécutez la commande suivante :

```
bind appfw profile test_profile -blockKeyword "blockword"
    BlockKeywordType literal -fieldName "firstname" -formURL "/
    signup.php" -state enable
<!--NeedCopy-->
```

Ajoutez des mots clés personnalisés à l'aide de l'

1. Accédez à**Sécurité > Profil du Web App Firewall NetScaler > Profils**.
2. Sélectionnez un profil et cliquez sur **Modifier**.
3. Accédez à la section**Paramètres avancés**et cliquez sur **Refuser les règles**.
4. Sélectionnez **Bloquer le mot clé** et cliquez sur **Modifier**.



5. Cliquez sur **Ajouter** et définissez les paramètres suivants :
   - Activer
   - Mot clé Block
   - Type de mot-clé de bloc
   - Nom du champ

- URL
- Est Regex
- Commentaires
- ID de ressource



6. Cliquez sur **Create**. Le mot clé personnalisé que vous avez ajouté est répertorié dans la page **Règles de refus des mots clés de blocage** .



7. Accédez à la section**Paramètres avancés**et cliquez sur**Contrôles de sécurité**.
8. Sélectionnez **Bloquer le mot clé** et cliquez sur **Paramètres d'action**.



9. Sélectionnez les actions requises et cliquez sur **OK**.

Afficher des statistiques personnalisées sur les mots clés à l'aide

Pour afficher les statistiques personnalisées sur les mots clés, tapez la commande suivante à l'invite de commandes :

```
stat appfw profile <profile name>
<!--NeedCopy-->
```

Exemple

```
stat appfw profile test_profile
<!--NeedCopy-->
```

Afficher les statistiques de mots clés personnalisées dans l'interface

1. Accédez à**Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un **profil Web App Firewall** et cliquez sur**Statistiques**. La page des**statistiques du pare-feu NetScaler Web App**affiche le trafic de mots clés personnalisés et les détails des violations.
3. Vous pouvez sélectionner la**vue tabulaire**ou passer à la**vue graphique**pour afficher les données dans un format tabulaire ou graphique.

Entités externes XML (XXE) Protection contre les attaques

May 5, 2023

La protection contre les attaques contre les entités externes XML (XXE) examine si une charge utile entrante contient des entrées XML non autorisées concernant des entités situées en dehors du domaine de confiance dans lequel réside l'application Web. L'attaque XXE se produit si vous disposez d'un analyseur XML faible qui analyse une charge utile XML dont l'entrée contient des références à des entités externes.

Dans une appliance NetScaler, si l'analyseur XML n'est pas correctement configuré, l'exploitation de la vulnérabilité peut avoir des conséquences dangereuses. Il permet à un attaquant de lire des données sensibles sur le serveur Web. Effectuez l'attaque par déni de service, etc. Par conséquent, il est important de protéger l'appliance contre les attaques XXE. Web Application Firewall est capable de protéger l'appliance contre les attaques XXE tant que le type de contenu est identifié comme XML. Pour empêcher un utilisateur malveillant de contourner ce mécanisme de protection, WAF bloque une demande entrante si le type de contenu « inféré » dans les en-têtes HTTP ne correspond pas au

type de contenu du corps. Ce mécanisme empêche le contournement de la protection contre les attaques XXE lorsqu'un type de contenu par défaut ou non par défaut est utilisé sur liste blanche.

Certaines des menaces XXE potentielles qui affectent une appliance NetScaler sont les suivantes :

- Fuites de données confidentielles
- Attaques par déni de service (DOS)
- demandes de falsification côté serveur
- Analyse des ports

Configurer la protection par injection d'entités externes XML (XXE)

Pour configurer les entités externes XML (XXE), vérifiez à l'aide de l'interface de commande :
Dans l'interface de ligne de commande, vous pouvez ajouter ou modifier la commande de profil de pare-feu d'application pour configurer les paramètres **XXE** . Vous pouvez activer les actions de blocage, de journalisation et de statistiques.

À l'invite de commande, tapez :

```
set appfw profile <name> [-inferContentTypeXmlPayloadAction <inferContentTypeXmlPayloa
 <block | log | stats | none>]
```

> Remarque :
>
> Par défaut, l'action XXE est définie comme « aucun. «

Exemple :

```
set appfw profile profile1 -inferContentTypeXmlPayloadAction Block
```

Où, les types d'actions sont les suivants :

Bloquer : la demande est bloquée sans exception en ce qui concerne les URL qu'elle contient.

Journal : en cas de non-concordance entre le type de contenu d'un en-tête de requête HTTP et la charge utile, les informations relatives à la demande non conforme doivent figurer dans le message du journal.

Statistiques : si une incompatibilité entre les types de contenu est détectée, les statistiques correspondantes pour ce type de violation sont incrémentées.

Aucune : aucune action n'est entreprise si une incompatibilité entre les types de contenu est détectée. Aucune ne peut être combinée avec aucun autre type d'action. L'action par défaut est définie sur Aucune.

Configurer le contrôle d'injection XXE à l'aide de l'interface graphique NetScaler

Procédez comme suit pour configurer le contrôle d'injection XXE.

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page de **profil du Web App Firewall NetScaler**, accédez à la section **Paramètres avancés** et cliquez sur Contrôles **de sécurité**.



4. Dans la section **Contrôles de sécurité**, sélectionnez **Induire le type de contenu XML Payload** et cliquez sur Paramètres **d'action** .
5. Dans la page Infer Content Type XML Payload Settings, définissez les paramètres suivants :
   a) Des actions. Sélectionnez une ou plusieurs actions à effectuer pour le contrôle de sécurité de l'injection XXE.
6. Cliquez sur **OK**.



Affichage des statistiques relatives au trafic d'injection XXE et aux infractions

La page des statistiques du Web App Firewall NetScaler affiche les détails du trafic de sécurité et des violations de sécurité sous forme de tableau ou de graphique.

Pour afficher les statistiques de sécurité à l'aide de l'interface de commande.

À l'invite de commande, tapez :

```
stat appfw profile profile1
```


Affichage des statistiques d'injection XXE à l'aide de l'interface graphique NetScaler

Procédez comme suit pour afficher les statistiques d'injection XXE :

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet de détails, sélectionnez un profil de Web App Firewall et cliquez sur **Statistiques**.
3. La page des **statistiques du pare-feu NetScaler Web App** affiche le trafic d'injection de commandes XXE et les détails des violations.
4. Vous pouvez sélectionner **Vue tabulaire** ou passer en mode Affichage **graphique pour afficher** les données sous forme de tableau ou de graphique.



Contrôle du dépassement de la mémoire tampon

May 5, 2023

La vérification de débordement de la mémoire tampon détecte les tentatives de provoquer un débordement de la mémoire tampon sur le serveur Web. Si le Web App Firewall détecte que l'URL, les cookies ou l'en-tête sont plus longs que la longueur configurée, il bloque la demande car cela peut provoquer un dépassement de la mémoire tampon.

La vérification de débordement de la mémoire tampon empêche les attaques contre les logiciels non sécurisés du système d'exploitation ou du serveur Web qui peuvent se bloquer ou se comporter de manière imprévisible lorsqu'il reçoit une chaîne de données plus grande qu'elle ne peut gérer. Des techniques de programmation appropriées empêchent les débordements de mémoire tampon en vérifiant les données entrantes et en rejetant ou en tronquant les chaînes trop longues. Cependant, de nombreux programmes ne vérifient pas toutes les données entrantes et sont donc vulnérables aux débordements de mémoire tampon. Ce problème affecte particulièrement les anciennes versions des logiciels et des systèmes d'exploitation de serveurs Web, dont beaucoup sont encore en cours d'utilisation.

Le contrôle de sécurité Buffer Overflow vous permet de configurer les actions **Block**, **Log**et **Stats** . En outre, vous pouvez également configurer les paramètres suivants :

- **Longueur maximale de l'URL**. La longueur maximale autorisée par le Web App Firewall dans une URL demandée. Les demandes avec des URL plus longues sont bloquées. **Valeurs possibles** : 0—65535. **Par défaut** : 1024
- **Longueur maximale du cookie**. La longueur maximale autorisée par le Web App Firewall pour tous les cookies d'une requête. Les demandes avec des cookies plus longs déclenchent les violations. **Valeurs possibles** : 0—65535. **Par défaut** : 4096
- **Longueur maximale de l'en-tête**. Longueur maximale autorisée par le Web App Firewall pour les en-têtes HTTP. Les demandes avec des en-têtes plus longs sont bloquées. **Valeurs possibles** : 0—65535. **Par défaut** : 4096
- **Longueur de chaîne de requête**. Longueur maximale autorisée pour la chaîne de requête dans une demande entrante. Les requêtes avec des requêtes plus longues sont bloquées. Valeurs possibles : 0—65535. Par défaut : 1024
- **Durée totale de la demande**. Longueur maximale de demande autorisée pour une demande entrante. Les demandes plus longues sont bloquées. Valeurs possibles : 0—65535. Par défaut : 24820

Utilisation de la ligne de commande pour configurer le contrôle de sécurité de Buffer Overflow

Pour configurer les actions de contrôle de sécurité de Buffer Overflow et d'autres paramètres à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
add appfw profile <name> -bufferOverflowMaxURLLength <positive_integer> -
bufferOverflowMaxHeaderLength <positive_integer> - bufferOverflowMaxCookieLength
 <positive_integer> -bufferOverflowMaxQueryLength <positive_integer> -
bufferOverflowMaxTotalHeaderLength <positive_integer>
```

Exemple :


```
add appfw profile profile1 -bufferOverflowMaxURLLength 7000 -bufferOverflowMaxHeaderLe
 7250 - bufferOverflowMaxCookieLength 7100 -bufferOverflowMaxQueryLength
7300 -bufferOverflowMaxTotalHeaderLength 7300
```

Configurer le contrôle de sécurité contre le dépassement de la mémoire tampon à l'aide de l'interface graphique NetScaler

1. Accédez à **Sécurité** > **Pare-feu et**profils**des applications Web**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page de **profil du Web App Firewall NetScaler**, accédez à la section **Paramètres avancés** et cliquez sur Contrôles **de sécurité**.
4. Dans **la section Contrôles de sécurité**, sélectionnez **Buffer Overflow** et cliquez sur **Paramètres d'action.**
5. Sur la page **Paramètres du Buffer Overflow**, définissez les paramètres suivants.
   a. Des actions. Sélectionnez une ou plusieurs actions à effectuer pour le contrôle de sécurité par injection de commandes.
   b. Longueur maximale de l'URL. Longueur maximale, en caractères, des URL de vos sites Web protégés. Les demandes avec des URL plus longues sont bloquées.
   c. Longueur maximale du cookie. Longueur maximale, en caractères, des cookies envoyés à vos sites Web protégés. Les demandes contenant des cookies plus longs sont bloquées.
   d. Longueur maximale de l'en-tête. Longueur maximale, en caractères, des en-têtes HTTP dans les requêtes envoyées à vos sites Web protégés. Les demandes avec des en-têtes plus longs sont bloquées.
   e. Longueur maximale de la requête. Longueur maximale, en octets, de la chaîne de requête envoyée à vos sites Web protégés. Les demandes comportant des chaînes de requête plus longues sont bloquées.
   f. Longueur totale maximale de l'en-tête. Longueur maximale, en octets, de la longueur totale de l'en-tête HTTP des requêtes envoyées à vos sites Web protégés. La valeur minimale de ceci et de maxHeaderLen dans HttpProfile sera utilisée. Les demandes plus longues sont bloquées.
6. Cliquez sur **OK** et sur **Fermer**.



Utilisation de la fonction de journalisation avec le contrôle de sécurité du Buffer Overflow

****Lorsque l'action du journal est activée, les violations du contrôle de sécurité de Buffer Overflow sont enregistrées dans le journal d'audit sous la forme APPFW_BUFFEROVERFLOW_URL, APPFW_BUFFEROVERFLOW_COOKIE et **APPFW_BUFFEROVERFLOW_HDR**.** Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur Syslog distant.

Si vous utilisez l'interface graphique pour consulter les journaux, vous pouvez utiliser la fonctionnalité de déploiement en un clic pour appliquer les relaxations indiquées dans les journaux.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Passez au shell et suivez le fichier ns.logs dans le dossier **/var/log/** pour accéder aux messages du journal relatifs aux violations du Buffer Overflow :

```
1 > \*\*Shell\*\*
2 > \*\*tail -f /var/log/ns.log | grep APPFW_BUFFEROVERFLOW\*\*
3 <!--NeedCopy-->
```

Exemple de message de journal CEF indiquant une violation de BufferOverflowMaxCookieLength en mode non bloc


```
Oct 22 17:35:20 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_COOKIE\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=41198 method=GET request=http://aaron.
    stratum8.net/FFC/sc11.html \*\*msg=Cookie header length(43) is
    greater than maximum allowed(16).\*\* cn1=119 cn2=465 cs1=
    owa_profile cs2=PPE1 cs3=wvOOOb+cJ2ZRbstZpyeNXIqLj7Y0001 cs4=ALERT
    cs5=2015 \*\*act=not blocked\*\*
<!--NeedCopy-->
```

Exemple de message de journal CEF indiquant une violation de BufferOverflowMaxUrlLength en mode non bloc

```
Oct 22 18:39:56 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_URL\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=19171 method=GET request=http://aaron.
    stratum8.net/FFC/sc11.html \*\*msg=URL length(39) is greater than
    maximum allowed(20).\*\* cn1=707 cn2=402 cs1=owa_profile cs2=PPE0
    cs3=kW49GcKbnwKByByi3+jeNzfgWa80000 cs4=ALERT cs5=2015 \*\*act=not
    blocked\*\*
<!--NeedCopy-->
```

Exemple de message du journal au format natif indiquant une violation de BufferOverflowMaxHeaderLength en mode bloc

```
Oct 22 18:44:00 <local0.info> 10.217.31.98 10/22/2015:18:44:00 GMT ns
    0-PPE-2 : default APPFW \*\*APPFW_BUFFEROVERFLOW_HDR\*\* 155 0 :
    10.217.253.62 374-PPE2 khhBEeY4DB8V2D3H2sMLkXmfWnA0002 owa_profile
    \*\*Header(User-Agent) length(82) is greater than maximum allowed
    (10)\*\* : http://aaron.stratum8.net/ \*\*<blocked>\*\*
<!--NeedCopy-->
```

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique inclut un outil utile (**Syslog Viewer**) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **Pare-feu des applications** > **Profils**, sélectionnez le profil cible, puis cliquez sur **Contrôles de sécurité**. Sélectionnez la ligne **Buffer Overflow** et cliquez sur **Logs**. Lorsque vous accédez aux journaux directement à partir du contrôle de sécurité du profil Buffer Overflow, l'interface utilisateur filtre les messages du journal et affiche uniquement les journaux relatifs à ces violations de contrôle de sécurité.
- ****Vous pouvez également accéder à la visionneuse Syslog en accédant à **NetScaler** > Système > Audit.**** Dans la section Messages d'audit, cliquez sur le lien **des messages Syslog** pour afficher le visualiseur Syslog, qui affiche tous les messages du journal, y compris les

autres journaux de violations des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de contrôle de sécurité peuvent être déclenchées pendant le traitement des demandes.

- Accédez à **Pare-feu des applications** > **Stratégies** > **Audit**. Dans la section **Messages d'audit**, cliquez sur le lien **des messages Syslog** pour afficher le visualiseur Syslog, qui affiche tous les messages du journal, y compris les autres journaux de violations des contrôles de sécurité.

Le visualiseur Syslog basé sur XML fournit diverses options de filtrage pour sélectionner uniquement les messages du journal qui vous intéressent. **Pour sélectionner les messages du journal pour la vérification du**Buffer Overflow**, filtrez en sélectionnant**APPFW**dans les options de la liste déroulante du module. La liste des**types d'événements**propose trois options,**APPFW_BUFFEROVERFLOW_URL, APPFW_BUFFEROVERFLOW_COOKIE et A PPFW_BUFFEROVERFLOW_HDR **pour afficher tous les messages de journal relatifs au contrôle de sécurité du dépassement**de mémoire tampon.** Vous pouvez sélectionner une ou plusieurs options pour affiner votre sélection. Par exemple, si vous cochez la case **APPFW_BUFFEROVERFLOW_COOKIE** et que vous cliquez sur le bouton **Appliquer**, seuls les messages du journal relatifs aux violations du contrôle de **sécurité de Buffer Overflow** pour l'en-tête Cookie apparaissent dans le visualiseur Syslog. Si vous placez le curseur sur la ligne correspondant à un message de journal spécifique, plusieurs options, telles que le **module**, le **type d'événement**, l' **ID d'événement**et l' **adresse IP du client**, apparaissent sous le message du journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

Déploiement en un clic : l'interface graphique fournit une fonctionnalité de déploiement par clic, qui n'est actuellement prise en charge que pour les messages du journal de dépassement de la mémoire tampon relatifs aux violations de longueur d'URL. Vous pouvez utiliser le visualiseur Syslog non seulement pour visualiser les violations déclenchées, mais également pour prendre des décisions éclairées en fonction de la longueur observée des messages bloqués. Si la valeur actuelle est trop restrictive et déclenche des faux positifs, vous pouvez sélectionner un message et le déployer pour remplacer la valeur actuelle par la valeur de longueur d'URL affichée dans le message. Les messages de journal doivent être au format de journal CEF pour cette opération. Si la relaxation peut être déployée pour un message de journal, une case à cocher apparaît sur le bord droit de la zone du **visualiseur Syslog**, sur la ligne. Cochez la case, puis sélectionnez une option dans la liste des **actions** pour déployer la relaxation. Les options**Modifier et déployer**, **Déployer**et **Tout déployer** sont disponibles en tant qu'options **d'action** . Vous pouvez utiliser le filtre **APPFW_BUFFEROVERFLOW_URL** pour isoler tous les messages de journal relatifs aux violations de longueur d'URL configurées.

Si vous sélectionnez un message de journal individuel, les trois options d'action **Modifier et**déployer**, Déployer**et **Déployer tout** sont disponibles. Si vous sélectionnez **Modifier et déployer**, la boîte de dialogue des **paramètres de Buffer Overflow** s'affiche. La nouvelle longueur d'URL observée dans la demande est insérée dans le champ de **saisie Longueur d'URL maximale** . Si vous cliquez sur **Fermer** sans aucune modification, les valeurs actuellement configurées restent inchangées. Si vous cliquez

sur le bouton **OK**, la nouvelle valeur de la longueur maximale de l'URL remplace la valeur précédente.

> **Remarque**
>
> Les cases à cocher relatives au **blocage**, au **journal** et aux **statistiques** ne sont pas cochées dans la boîte de dialogue des **paramètres de Buffer Overflow** qui s'affiche et doivent être reconfigurées si vous sélectionnez l'option **Modifier et déployer** . Assurez-vous d'activer ces cases à cocher avant de cliquer sur **OK**, sinon la nouvelle longueur d'URL sera configurée mais les actions seront définies sur **aucune**.

Si vous cochez les cases correspondant à plusieurs messages de journal, vous pouvez utiliser l'option **Déployerou Tout déployer**. Si les messages du journal déployés ont des longueurs d'URL différentes, la valeur configurée est remplacée par la valeur de longueur d'URL la plus élevée observée dans les messages sélectionnés. Le déploiement de la règle entraîne uniquement la modification de la valeur**BufferOverflowMaxUrlLength** . Les actions configurées sont conservées et restent inchangées.

Pour utiliser la fonctionnalité Click-to-Deploy dans l'interface graphique

1. Dans la visionneuse Syslog, sélectionnez **APPFW** dans les options du **module** .
2. **Cochez la case**APPFW_BUFFEROVERFLOW_URL**comme type d'événement pour filtrer les messages de journal correspondants.**
3. Cochez la case pour sélectionner la règle.
4. Utilisez la liste déroulante des options **Action** pour déployer la relaxation.
5. Accédez à **Application Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Security Checks** pour accéder au volet des paramètres de **Buffer Overflow** afin de vérifier que la valeur de **longueur d'URL maximale** est mise à jour.

Statistiques relatives aux violations du Buffer Overflow

Lorsque l'action statistique est activée, le compteur du contrôle de sécurité du Buffer Overflow est incrémenté lorsque le Web App Firewall entreprend une action pour ce contrôle de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, une demande concernant une page contenant trois violations de Buffer Overflow incrémente le compteur de statistiques d'une unité, car la page est bloquée lorsque la première violation est détectée. Toutefois, si le blocage est désactivé, le traitement de la même demande augmente le compteur de statistiques des violations, car chaque violation génère un message de journal distinct.

Pour afficher les statistiques du Buffer Overflow Security Check à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
> sh appfw stats
```


Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> stat appfw profile <profile name>
```

Pour afficher les statistiques de Buffer Overflow à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Pare-feu d'application**.
2. Dans le volet droit, accédez au lien **Statistiques** .
3. Utilisez la barre de défilement pour consulter les statistiques relatives aux violations de Buffer Overflow et aux journaux. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Résumé

- Le contrôle de sécurité relatif au dépassement de la mémoire tampon vous permet de configurer des limites pour appliquer la longueur maximale des URL, des cookies et des en-têtes autorisés.
- Les actions de**blocage**, de **journalisation** et de **statistiques** vous permettent de surveiller le trafic et de configurer une protection optimale pour votre application.
- Le visualiseur Syslog vous permet de filtrer et d'afficher tous les messages du journal relatifs aux violations de dépassement de la mémoire tampon.
- **La fonctionnalité**Click-to-Deploy**est prise en charge pour les violations BufferOverflow-MaxURLLength.** Vous pouvez sélectionner et déployer une règle individuelle ou sélectionner plusieurs messages de journal pour modifier et assouplir la valeur actuellement configurée de la longueur maximale autorisée de l'URL. La valeur la plus élevée de l'URL du groupe sélectionné est définie comme nouvelle valeur, afin d'autoriser toutes les demandes actuellement signalées comme des violations.
- Le Web App Firewall évalue désormais les cookies individuels lors de l'inspection de la demande entrante. Si la longueur d'un cookie reçu dans l'en-tête Cookie dépasse le paramètre **BufferOverflowMaxCookieLength configuré, la violation Buffer Overflow est déclenchée**.

> **Important**
>
> Dans la version 10.5.e (dans quelques versions d'améliorations intermédiaires antérieures à la version 59.13xx.e) et dans la version 11.0 (dans les versions antérieures à 65.x), le traitement de l'en-tête Cookie par le Web App Firewall a été modifié. Dans ces versions, chaque cookie est évalué individuellement, et si la longueur d'un cookie reçu dans l'en-tête Cookie dépasse le paramètre BufferOverflowMaxCookieLength configuré, la violation Buffer Overflow est déclenchée. À la suite de cette modification, les requêtes bloquées dans les versions 10.5 et antérieures peuvent être autorisées, car la longueur de l'ensemble de l'en-tête du cookie n'est pas calculée pour déterminer la longueur du cookie. ** Dans certains cas, la taille totale

> des cookie transférés au serveur peut être supérieure à la valeur acceptée, et le serveur peut répondre par « 400 mauvaises demandes ».
>
> Cette modification a été annulée. Le comportement de la version 10.5.e ->59.13xx.e et des versions d'amélioration 10.5.e ultérieures, en plus de la version 11.0 65.x et des versions ultérieures, est désormais similaire à celui des versions non améliorées de la version 10.5. L'intégralité de l'en-tête Cookie brut est désormais prise en compte lors du calcul de la longueur du cookie. Les espaces environnants et les points-virgules (;) séparant les paires nom-valeur sont également inclus dans la détermination de la longueur du cookie.

Support du Web App Firewall pour la boîte à outils Web de Google

May 8, 2023

Remarque : Cette fonctionnalité est disponible dans NetScaler version 10.5.e.

Les serveurs Web utilisant les mécanismes RPC (Remote Procedure Call) de Google Web Toolkit (GWT) peuvent être sécurisés par le NetScaler Web App Firewall sans nécessiter de configuration spécifique pour activer le support GWT.

Qu'est-ce que GWT

Le GWT est utilisé pour créer et optimiser des applications Web complexes à hautes performances par des personnes qui n'ont pas d'expertise en XMLHttpRequest et en JavaScript. Cette boîte à outils de développement libre et open source est largement utilisée pour développer des applications à petite et grande échelle et est assez fréquemment utilisée pour afficher des données basées sur des navigateurs, telles que les résultats de recherche pour les vols, les hôtels, etc. Le GWT fournit un ensemble de base d'API et de widgets Java pour écrire des scripts JavaScript optimisés pouvant être exécutés sur la plupart des navigateurs et appareils mobiles. Le framework GWT RPC permet aux composants client et serveur de l'application Web d'échanger facilement des objets Java via HTTP. Les services GWT RPC ne sont pas les mêmes que les services Web basés sur SOAP ou REST. Il s'agit simplement d'une méthode légère pour transférer des données entre le serveur et l'application GWT sur le client. GWT gère la sérialisation des objets Java en échangeant les arguments dans les appels de méthode et la valeur de retour.

Pour les sites Web populaires qui utilisent GWT, voir

https://www.quora.com/What-web-applications-use-Google-Web-Toolkit-%28GWT%29

Comment fonctionne une demande GWT

La requête GWT RPC est délimitée par des canaux et possède un nombre variable d'arguments. Il est transporté en tant que charge utile de HTTP POST et possède les valeurs suivantes :

1. Type de contenu = text/x-gwt-rpc. Le jeu de caractères peut prendre n'importe quelle valeur.
2. Méthode = POST.

Les requêtes HTTP GET et POST sont considérées comme des requêtes GWT valides si le type de contenu est « text/x-gwt-rpc ». Les chaînes de requête sont désormais prises en charge dans le cadre des requêtes GWT. Configurez le paramètre « InspectQueryContentTypes » du profil App Firewall sur « OTHER » pour examiner la partie de requête pour le type de contenu « text/x-gwt-rpc ».

L'exemple suivant montre une charge utile valide pour une demande GWT :

```
5|0|8|http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com
   .test.client.TestService|testMethod|java.lang.String|java.lang.
   Integer| myInput1|java.lang.Integer/3438268394|1|2|3|4|2|5|6|7|8|1|
<!--NeedCopy-->
```

La demande peut être divisée en trois parties :

a) `Header: 5|0|8|`

Les 3 premiers chiffres `5|0|8|` de la requête ci-dessus représentent respectivement « la version, la subversion et la taille de la table ». Il doit s'agir de nombres entiers positifs.

b) Table à chaînes :

```
http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com.test.
client.TestService|testMethod|java.lang.String|java.lang.Integer|myInput1|
java.lang.Integer/3438268394|
```

Les membres de la table de chaînes délimitées par des tuyaux ci-dessus contiennent les entrées fournies par l'utilisateur. Ces entrées sont analysées pour les vérifications du Web App Firewall et sont identifiées comme suit :

- 1er : `http://localhost:8080/test/`

  Il s'agit de l'URL de la demande.

- 2e : `16878339F02B83818D264AE430C20468`

  Identifiant HEX unique. Une requête est considérée comme mal formée si cette chaîne contient des caractères non hexadécimaux.

- 3e : `com.test.client.TestService`

  Nom de la classe de service

- 4e : `testMethod`

  Nom de la méthode de service

- À partir de la 5e : `java.lang.String|java.lang.Integer|myInput1|java.lang.Integer/3438268394`

  Types de données et données. Les types de données non primitifs sont spécifiés comme

  `<container>.<sub-cntnr>.name/<integer><identifier>`

c) `Payload`: `1|2|3|4|2|5|6|7|8|1|`

La charge utile se compose de références aux éléments de la table de chaînes. Ces valeurs entières ne peuvent pas être supérieures au nombre d'éléments de la table de chaînes.

Protection par le Web App Firewall pour les applications GWT

Le Web App Firewall comprend et interprète les requêtes GWT RPC, inspecte la charge utile pour détecter les violations des contrôles de sécurité et prend des mesures spécifiques.

Les en-têtes du Web App Firewall et les contrôles des cookies pour les requêtes GWT sont similaires à ceux des autres formats de demande. Après un décodage d'URL et une conversion du jeu de caractères appropriés, tous les paramètres de la table de chaînes sont inspectés. Le corps de la requête GWT ne contient pas de noms de champs, mais uniquement les valeurs des champs. Les valeurs d'entrée peuvent être validées par rapport au format spécifié à l'aide de la vérification du format du champ du Web App Firewall, qui peut également être utilisée pour contrôler la longueur de la saisie. Les attaques **par**script intersite**et par injection SQL présentes** dans les entrées peuvent être facilement détectées et contrecarrées par le Web App Firewall.

Règles d'apprentissage et de relaxation : l'apprentissage et le déploiement des règles de relaxation sont pris en charge pour les requêtes GWT. Les règles du Web App Firewall se présentent sous la forme d'un <actionURL> <gieldName> mappage \ \. Le format de requête GWT ne contient pas les noms de champs et nécessite donc un traitement spécial. Le Web App Firewall insère des noms de champs fictifs dans les règles apprises qui peuvent être déployées sous forme de règles de relaxation. L'indicateur -IsRegex fonctionne de la même manière que pour les règles non GWT.

- URL de l'action :

  Plusieurs services répondant à un RPC peuvent être configurés sur le même serveur Web. La requête HTTP contient l'URL du serveur Web, et non celle du service qui gère le RPC. Par conséquent, la relaxation n'est pas appliquée sur la base de l'URL de la requête HTTP, car cela assouplirait tous les services de cette URL pour le champ cible. Pour les requêtes GWT, le Web App Firewall utilise l'URL du service réel trouvé dans la charge utile GWT, dans le quatrième champ de la table de chaînes.

- Nom du champ :

  Étant donné que le corps de la requête GWT ne contient que des valeurs de champ, le Web App Firewall insère des noms de champs fictifs tels que 1, 2, etc. lorsqu'il recommande des règles apprises.

  Exemple de règle apprise par GWT

```
POST /abcd/def/gh HTTP/1.1
Content-type: text/x-gwt-rpc
Host: 10.217.222.75
Content-length: 157

5|0|8|http://localhost:8080/acdtest/|16878339
   F02Baf83818D264AE430C20468|
com.test.client.TestService|testMethod|java.lang.String%3b|java.
   lang.Integer|onblur|

  The learn data will be as follows:
> sh learningdata pr1 crossSiteScripting
Profile: pr1    SecurityCheck: crossSiteScripting
1)  Url:    http://localhost:8080/acdtest/  >> From GWT Payload.
    Field:  10
    Hits:   1
 Done
<!--NeedCopy-->
```

  Exemple de règle de relaxation GWT

```
bind appfw profile pr1 -crossSiteScripting 1 abcd -isregex NOTREGEX
```

Messages du journal : le Web App Firewall génère des messages de journal pour les violations des contrôles de sécurité détectées dans les demandes GWT. Un message de journal généré par une demande GWT mal formée contient la chaîne « GWT » pour faciliter l'identification.

Exemple de message de journal pour une demande GWT mal formée :

```
Dec 5 21:48:02 <local0.notice> 10.217.31.247 12/05/2014:21:48:02 GMT ns
0-PPE-0 : APPFW Message 696 0 : "GWT RPC request with malformed payload. <
blocked>"
```

Différence entre le traitement des demandes GWT et celui des demandes non GWT :

La même charge utile peut déclencher différentes violations des contrôles de sécurité du Web App Firewall pour différents types de contenu. Prenons l'exemple suivant :

```
5|0|8|http://localhost:8080/acdtest/|16878339F02Baf83818D264AE430C20468|com
.test.client.TestService|testMethod|java.lang.String%3b|java.lang.Integer|
```



```
select|
```

Type de contenu : application/x-www-form-urlencoded :

Une demande envoyée avec ce type de contenu entraîne une violation SQL si le type d'injection SQL est configuré pour utiliser l'une des quatre options disponibles : SQLSplCharAndKeyword, SQLSplCharOrKeyword, SQLKeyword ou SQLSplChar. Le Web App Firewall considère « & » comme le séparateur de champs et « = » comme le séparateur nom-valeur lors du traitement de la charge utile ci-dessus. Comme aucun de ces caractères n'apparaît nulle part dans le corps du message, l'ensemble du contenu est traité comme un seul nom de champ. Le nom du champ de cette requête contient à la fois un caractère spécial SQL (;) et un mot clé SQL (select). Les violations sont donc détectées pour les quatre options de type d'injection SQL.

Type de contenu : text/x-gwt-rpc :

Une demande envoyée avec ce type de contenu déclenche une violation SQL uniquement si le type d'injection SQL est défini sur l'une des trois options suivantes : SQLSplCharOrKeyword, SQLKeyword ou SQLSplChar. Aucune violation n'est déclenchée si le type d'injection SQL est défini sur SQLSplCharAndKeyword, qui est l'option par défaut. Le Web App Firewall considère la barre | verticale comme le séparateur de champs pour la charge utile ci-dessus dans la requête GWT. Par conséquent, le corps du message est divisé en différentes valeurs de champs de formulaire et des noms de champs de formulaire sont ajoutés (conformément à la convention décrite précédemment). En raison de cette division, le caractère spécial SQL et le mot clé SQL font partie de champs de formulaire distincts.

Champ de formulaire 8 : `java.lang.String%3b -\> %3b is the (;)char`

Champ de formulaire 10 : `select`

Par conséquent, lorsque le type d'injection SQL est défini sur **SQLSplChar**, le champ 8 indique la violation SQL. Pour **SQLKeyword**, le champ 10 indique la violation. L'un ou l'autre de ces deux champs peut indiquer une violation si le type SQL Inject est configuré avec l'option **SQLSplCharorKeyword**, qui recherche la présence d'un mot clé ou d'un caractère spécial. ****Aucune violation n'est détectée pour l'option par défaut ****SQLSplCharAndKeyword**, car aucun champ ne possède une valeur contenant à la fois SQLSplChar et SQLKeyword.**

Astuces :

- Aucune configuration spéciale du Web App Firewall n'est requise pour activer le support GWT.
- Le type de contenu doit être text/x-gwt-rpc.
- L'apprentissage et le déploiement des règles de relaxation pour tous les contrôles de sécurité pertinents du Web App Firewall appliqués à la charge utile GWT fonctionnent de la même manière que pour les autres types de contenu pris en charge.
- Seules les requêtes POST sont considérées comme valides pour GWT. Toutes les autres méthodes de requête sont bloquées si le type de contenu est text/x-gwt-rpc.
- Les requêtes GWT sont soumises à la limite de corps POST configurée pour le profil.

- Le paramètre sans session pour les contrôles de sécurité n'est pas applicable et sera ignoré.
- Le format de journal CEF est pris en charge pour les messages du journal GWT.

Protection des cookies

May 5, 2023

Un cookie est un petit paquet de données envoyé par un serveur Web à un navigateur client. Les cookies transportent des données sensibles telles que des mots de passe, des informations d'authentification des utilisateurs et des informations d'identification via une connexion HTTP et sont stockées dans un navigateur Web. Il est donc très important de protéger les cookies contre les attaquants qui volent des informations.

Contrôle de cohérence des cookies : examine les cookies renvoyés avec les demandes des utilisateurs afin de vérifier qu'ils correspondent aux cookies que votre serveur Web a définis pour cet utilisateur. Si un cookie modifié est trouvé, il est retiré de la demande avant que la demande soit transférée au serveur Web. Pour plus d'informations, consultez la rubrique Vérification de la cohérence des cookies .

Protection contre le détournement de cookies : Le détournement désigne une situation où un attaquant obtient un accès non autorisé aux cookies. Pour protéger les cookie contre tout accès autorisé, le NetScaler Web App Firewall (WAF) conteste la connexion TLS depuis le client ainsi que la validation de la cohérence des cookie WAF. Pour chaque nouvelle demande client, l'appliance valide la connexion TLS et vérifie également la cohérence des cookies d'application et de session dans la requête. Pour plus d'informations, consultez la rubrique Protection contre le détournement des cookies .

Attribut de cookie Samesite : L' `SameSite` attribut de la réponse HTTP Set-Cookie vous permet de déclarer si votre cookie doit être limité à un contexte de première partie ou de même site. Le paramètre de cookie atténue les attaques et fournit une communication Web sécurisée. Pour plus d'informations, consultez la rubrique Attribut de cookie SameSite .

Contrôle de cohérence des cookies

January 25, 2023

Le contrôle de cohérence des cookies examine les cookies renvoyés par les utilisateurs afin de vérifier qu'ils correspondent aux cookies que votre site Web a définis pour cet utilisateur. Si un cookie modifié est détecté, il est supprimé de la demande avant que celle-ci ne soit transmise au serveur Web. Vous pouvez également configurer le contrôle de cohérence des cookies pour transformer tous les

cookies du serveur qu'il traite, en cryptant les cookies, en les transmettant par proxy ou en ajoutant des indicateurs aux cookies. Cette vérification s'applique aux demandes et aux réponses.

Un attaquant modifie normalement un cookie pour accéder à des informations privées sensibles en se faisant passer pour un utilisateur préalablement authentifié, ou pour provoquer un dépassement de tampon. La vérification du dépassement de la mémoire tampon protège contre les tentatives visant à provoquer un débordement de la mémoire tampon en utilisant un cookie long. Le contrôle de cohérence des cookies se concentre sur le premier scénario.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue
Modifier le contrôle de cohérence des cookies, dans l'onglet
Général, vous pouvez activer ou désactiver les actions suivantes :

- Bloquer
- Journal
- Apprendre
- Statistiques
- Transformez. Si elle est activée, l'action Transformer modifie tous les cookies comme indiqué dans les paramètres suivants :
  - **Chiffrez les cookies du serveur.** Chiffrez les cookies définis par votre serveur Web, à l'exception de ceux figurant dans la liste d'assouplissement du contrôle de cohérence des cookies, avant de transmettre la réponse au client. Les cookies cryptés sont déchiffrés lorsque le client envoie une demande ultérieure, et les cookies déchiffrés sont réinsérés dans la demande avant qu'elle ne soit transmise au serveur Web protégé. Spécifiez l'un des types de chiffrement suivants :
    * **None.** Ne cryptez ni ne déchiffrez les cookies. La valeur par défaut.
    * **Déchiffrer uniquement.** Déchiffrez uniquement les cookies cryptés. Ne cryptez pas les cookies.
    * **Chiffrez uniquement la session.** Chiffrez uniquement les cookies de session. Ne cryptez pas les cookies persistants. Déchiffrez tous les cookies cryptés.
    * **Chiffrez tout.** Chiffrez les cookies de session et les cookies persistants. Déchiffrez tous les cookies cryptés.

      Remarque : lors du chiffrement des cookies, le Web App Firewall ajoute l'indicateur **HttpOnly** au cookie. Cet indicateur empêche les scripts d'accéder au cookie et de l'analyser. L'indicateur empêche donc un virus ou un cheval de Troie basé sur un script d'accéder à un cookie déchiffré et d'utiliser ces informations pour enfreindre la sécurité. Cela se fait indépendamment des paramètres des indicateurs à ajouter dans les cookies, qui sont gérés indépendamment des paramètres des cookies du serveur Encrypt.
- **Cookies du serveur proxy.** Proxy tous les cookies non persistants (de session) définis par votre serveur Web, à l'exception de ceux figurant dans la liste d'assouplissement du contrôle de cohérence des cookies. Les cookies sont créés par proxy à l'aide du cookie de session Web App

Firewall existant. Le Web App Firewall supprime les cookies de session définis par le serveur Web protégé et les enregistre localement avant de transmettre la réponse au client. Lorsque le client envoie une demande ultérieure, le Web App Firewall réinsère les cookies de session dans la demande avant de la transmettre au serveur Web protégé. Spécifiez l'un des paramètres suivants :

- **None.** N'utilisez pas de cookies proxy. La valeur par défaut.
- **Session uniquement.** Cookies de session proxy uniquement. Ne pas utiliser de cookies persistants par proxy
  Remarque : si vous désactivez le proxy de cookie après l'avoir activé (définissez cette valeur sur Aucune après avoir été définie sur Session uniquement), le proxy de cookie est conservé pour les sessions qui ont été établies avant que vous ne le désactiviez. Vous pouvez donc désactiver cette fonctionnalité en toute sécurité pendant que le Web App Firewall traite les sessions utilisateur.

- **Drapeaux à ajouter dans les cookies**. Ajoutez des indicateurs aux cookies lors de la transformation. Spécifiez l'un des paramètres suivants :
  - **None.** N'ajoutez pas de drapeaux aux cookies. La valeur par défaut.
  - **HTTP uniquement.** Ajoutez l'indicateur HttpOnly à tous les cookies. Les navigateurs qui prennent en charge l'indicateur HttpOnly n'autorisent pas les scripts à accéder aux cookies pour lesquels cet indicateur est activé.
  - **Sécurisé**. Ajoutez l'indicateur Secure aux cookies qui doivent être envoyés uniquement via une connexion SSL. Les navigateurs qui prennent en charge l'indicateur sécurisé n'envoient pas les cookies marqués via une connexion non sécurisée.
  - **Tout.** Ajoutez l'indicateur HttpOnly à tous les cookies et l'indicateur Secure aux cookies qui doivent être envoyés uniquement via une connexion SSL.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer les commandes suivantes pour configurer le contrôle de cohérence des cookies :

- `set appfw profile <name> -cookieConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]`
- `set appfw profile <name> -cookieTransforms ([**ON**] | [**OFF**])`
- `set appfw profile <name> -cookieEncryption ([**none**] | [**decryptOnly**] | [**encryptSession**] | [**encryptAll**])`
- `set appfw profile <name> -cookieProxying ([**none**] | [**sessionOnly**])`
- `set appfw profile <name> -addCookieFlags ([**none**] | [**httpOnly**] | [**secure**] | [**all**])`

Pour définir des assouplissements pour le contrôle de cohérence des cookies, vous devez utiliser l'interface graphique. Dans l'onglet Contrôles de la boîte de dialogue Modifier le contrôle de cohérence des cookies, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter une relaxation du contrôle de cohérence des cookies, ou sélectionnez une relaxation existante et cliquez sur Ouvrir

pour ouvrir la boîte de dialogue Modifier la relaxation du contrôle de cohérence des cookies. L'une ou l'autre des boîtes de dialogue fournit les mêmes options pour configurer une relaxation.

Vous trouverez ci-dessous des exemples d'assouplissements relatifs à la vérification de la cohérence des cookies :

- **Champs de connexion.** L'expression suivante exempte tous les noms de cookie commençant par la chaîne logon_ suivie d'une chaîne de lettres ou de chiffres d'au moins deux caractères et d'au plus quinze caractères :

```
^logon_[0-9A-Za-z]{
2,15 }
$
<!--NeedCopy-->
```

- **Champs de connexion (caractères spéciaux).** L'expression suivante exempte tous les noms de cookie commençant par la chaîne türkçe-logon_ suivie d'une chaîne de lettres ou de chiffres d'au moins deux caractères et d'au plus quinze caractères :

```
^txC3xBCrkxC3xA7e-logon_[0-9A-Za-z]{
2,15 }
$
<!--NeedCopy-->
```

- **Chaînes arbitraires.** Autorisez les cookies contenant la chaîne sc-item_, suivie de l'identifiant d'un article que l'utilisateur a ajouté à son panier ([0-9a-Za-z] +), d'un second trait de soulignement (_) et enfin du nombre d'articles qu'il souhaite `([1-9][0-9]?)`, à être modifiables par l'utilisateur :

```
^sc-item_[0-9A-Za-z]+_[1-9][0-9]?$
<!--NeedCopy-->
```

Attention : Les expressions régulières sont puissantes. Surtout si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne voulez pas ou attendez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification de la cohérence des cookies aurait autrement bloqué.

Protection contre le détournement de cookies

May 5, 2023

La protection contre le piratage de cookies atténue les attaques de vol de cookies par des pirates informatiques. Lors d'une attaque de sécurité, un attaquant prend le contrôle d'une session utilisateur pour obtenir un accès non autorisé à une application Web. Lorsqu'un utilisateur navigue sur un site Web, par exemple une application bancaire, le site Web établit une session avec le navigateur. Au cours de la session, l'application enregistre les informations de l'utilisateur telles que les informations de connexion et les visites de pages dans un fichier cookie. Le fichier cookie est ensuite envoyé au navigateur du client dans la réponse. Le navigateur enregistre les cookies pour maintenir les sessions actives. L'attaquant peut voler ces cookies soit manuellement à partir de la banque de cookie du navigateur, soit via une extension de navigateur rouge. L'attaquant utilise ensuite ces cookies pour accéder aux sessions de l'application Web de l'utilisateur.

Pour atténuer les attaques par cookie, le NetScaler Web App Firewall (WAF) conteste la connexion TLS depuis le client ainsi que la validation de la cohérence des cookie WAF. Pour chaque nouvelle demande client, l'appliance valide la connexion TLS et vérifie également la cohérence des cookies d'application et de session dans la requête. Si un attaquant tente de mélanger et de faire correspondre les cookies d'application et les cookies de session volés à la victime, la validation de la cohérence des cookies échoue et l'action de détournement de cookie configurée est appliquée. Pour plus d'informations sur la cohérence des cookie, voir Vérification de la cohérence des cookies.

> **Remarque :**
>
> La fonctionnalité de piratage de cookies prend en charge la journalisation et les pièges SNMP. Pour plus d'informations sur la journalisation, consultez la rubrique ADM et pour plus d'informations sur la configuration SNMP, consultez la rubrique SNMP.

Limitations

- JavaScript doit être activé dans le navigateur client.
- La protection contre le détournement de cookies n'est pas prise en charge sur TLS version 1.3.
- Prise en charge limitée du navigateur Internet Explorer (IE) car le navigateur ne réutilise pas les connexions SSL. Il en résulte plusieurs redirections envoyées pour une demande, entraînant éventuellement une erreur « REDIRECTIONS MAXIMALES EXCÉDÉES » dans le navigateur IE.

Comment fonctionne la protection contre le détournement de cookies

Les scénarios suivants expliquent comment fonctionne la protection contre le piratage de cookie dans une appliance NetScaler.

Scénario 1 : utilisateur accédant à la première page Web sans cookie de session



1. L'utilisateur tente de s'authentifier dans une application Web et commence à accéder à la première page Web sans aucun cookie de session ADC dans la demande.
2. Lorsque la demande est reçue, l'appliance crée une session de pare-feu d'applications avec un identifiant de cookie de session.
3. Cela initie une connexion TLS pour la session. Comme le code JavaScript n'est pas envoyé et exécuté sur le navigateur client, l'appliance marque la connexion TLS comme validée et aucune vérification n'est requise.

   > **Remarque :**
   >
   > Même si un attaquant essaie d'envoyer tous les identifiants de cookies d'application d'une victime sans envoyer de cookie de session, l'appliance détecte le problème et supprime tous les cookies d'application de la demande avant de la transmettre au serveur principal. Le serveur principal considère cette demande sans aucun cookie d'application et prend les mesures nécessaires conformément à sa configuration.

4. Lorsque le serveur principal envoie une réponse, l'appliance reçoit la réponse et la transmet à l'aide d'un jeton de session JavaScript et d'un cookie de départ. L'appliance marque ensuite la connexion TLS comme étant vérifiée.
5. Lorsque le navigateur client reçoit la réponse, il exécute le code JavaScript et génère un identifiant de cookie transformé à l'aide du jeton de session et du cookie de départ.
6. Lorsqu'un utilisateur envoie une demande ultérieure via la connexion TLS, l'appliance contourne la validation du cookie transformé. Cela est dû au fait que la connexion TLS est déjà validée.

Scénario 2 : utilisateur accédant à des pages Web successives via une nouvelle connexion TLS avec un cookie de session



1. Lorsqu'un utilisateur envoie une demande HTTP pour des pages successives via une nouvelle connexion TLS, le navigateur envoie un identifiant de cookie de session et un identifiant de cookie transformé.
2. Comme il s'agit d'une nouvelle connexion TLS, l'appliance détecte la connexion TLS et demande au client de lui envoyer une réponse de redirection à l'aide d'un cookie de départ.
3. À la réception de la réponse de l'ADC, le client calcule le cookie transformé à l'aide du jeton de session et du nouveau cookie de départ.
4. Le client envoie ensuite ce cookie transformé nouvellement calculé avec un identifiant de session.
5. Si le cookie transformé calculé dans l'appliance ADC et celui envoyé via la demande correspondent, la connexion TLS est marquée comme vérifiée.
6. Si le cookie transformé calculé est différent de celui présent dans la demande du client, la validation échoue. Ensuite, l'appliance renvoie le défi au client, pour qu'il envoie un cookie correctement transformé.

Scénario 3 : Un attaquant se fait passer pour un utilisateur non authentifié



1. Lorsqu'un utilisateur s'authentifie dans l'application Web, l'attaquant utilise différentes techniques pour voler les cookies et les rejouer.
2. Comme il s'agit d'une nouvelle connexion TLS provenant de l'attaquant, l'ADC envoie un défi de redirection avec un nouveau cookie de départ.
3. Comme l'attaquant n'exécute pas JavaScript, la réponse de l'attaquant à la demande redirigée ne contient pas le cookie transformé.
4. Cela entraîne un échec de validation des cookie morphed du côté de l'appliance ADC. L'appliance envoie à nouveau un défi de redirection au client.
5. Si le nombre de tentatives de validation de cookie transformés dépasse le seuil, l'appliance signale le statut comme étant un piratage de cookie.
6. Si l'attaquant essaie de combiner des cookies d'application et des cookies de session volés à la victime, le contrôle de cohérence des cookie échoue et l'appliance applique l'action de piratage de cookie configurée.

Scénario 4 : Un attaquant se fait passer pour un utilisateur authentifié



1. Les attaquants peuvent également tenter de s'authentifier dans une application Web en tant qu'utilisateur authentique et de rejouer les cookies de la victime pour accéder à la session Web.
2. L'appliance ADC détecte également ces attaquants usurpés d'identité. Bien qu'une connexion TLS vérifiée soit utilisée par l'attaquant pour rejouer le cookie d'une victime, l'appliance ADC vérifie quand même si le cookie de session et le cookie d'application contenus dans la demande sont cohérents. L'appliance vérifie la cohérence d'un cookie d'application à l'aide du cookie de session contenu dans la demande. Étant donné que la demande contient un cookie de session de l'attaquant et un cookie d'application de la victime, la validation de cohérence des cookie échoue.
3. Par conséquent, l'appliance applique l'action de piratage de cookie configurée. Si l'action configurée est définie sur « bloquer », l'appliance supprime tous les cookies de l'application et envoie la demande au serveur principal.
4. Le serveur principal reçoit une demande sans cookie d'application et répond donc à une réponse d'erreur à l'attaquant, telle que « Utilisateur non connecté ».

Configurer le piratage des cookie à l'aide de la CLI

Vous pouvez sélectionner un profil de pare-feu d'application spécifique et définir une ou plusieurs actions pour empêcher le piratage de cookie.

À l'invite de commande, tapez :

```
set appfw profile <name> [-cookieHijackingAction <action-name> <block | log
 | stats | none>]
```

> **Remarque :**
>
> Par défaut, l'action est définie sur « aucune ».

Exemple :


```
set appfw profile profile1 - cookieHijackingAction Block
```

Où, les types d'actions sont les suivants :

Bloquer : bloquez les connexions qui enfreignent ce contrôle de sécurité.
Journal : consignez les violations de ce contrôle de sécurité.
Statistiques : générez des statistiques pour ce contrôle de sécurité.
Aucune : désactivez toutes les actions pour ce contrôle de sécurité.

Configurer le détournement de cookie à l'aide de l'interface graphique NetScaler

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page de **profil du Web App Firewall NetScaler**, accédez à la section **Paramètres avancés** et cliquez sur Contrôles **de sécurité**.



4. Dans la section **Contrôles de sécurité**, sélectionnez **Piratage de cookies**, puis cliquez sur les paramètres **Action**.

5. Sur la page **Paramètres de piratage des cookie**, sélectionnez une ou plusieurs actions pour empêcher le piratage de cookies.
6. Cliquez sur **OK**.



Ajouter une règle de relaxation pour la validation de la cohérence des cookie à l'aide de l'interface graphique NetScaler

Pour gérer les faux positifs lors de la validation de la cohérence des cookie, vous pouvez ajouter une règle d'assouplissement pour les cookies qui peuvent être exemptés de la validation des cookie.

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page de **profil du Web App Firewall NetScaler**, accédez à la section **Paramètres avancés** et cliquez sur Règles de **relaxation**.
4. Dans la section **Règles d'assouplissement**, sélectionnez **Cohérence des cookies** et cliquez sur **Action**.
5. Sur la page **Règle d'assouplissement de la cohérence des cookies**, définissez les paramètres suivants.
    a) Activé. Sélectionnez si vous souhaitez activer la règle de relaxation.
    b) Le nom du cookie est-il Regex. Sélectionnez si le nom du cookie est une expression régulière.
    c) Nom du cookie. Entrez le nom du cookie qui peut être exempté de la validation des cookie.
    d) Éditeur Regex. Cliquez sur cette option pour fournir les détails de l'expression régulière.
    e) Commentaires. Brève description du cookie.
6. Cliquez sur **Créer** et **Fermer**.

Afficher les statistiques de trafic et de violation des cookies à l'aide de l'interface de ligne de commande

Consultez les détails du trafic de sécurité et des violations de sécurité sous forme de tableau ou de graphique.

Pour consulter les statistiques de sécurité :

À l'invite de commande, tapez :

```
stat appfw profile profile1
```

Statistiques de trafic du profil Appfw	Taux (/s)	Total :
Demandes	0	0
Bytes de requête	0	0
Réponses	0	0
octets de réponse	0	0
Abandons	0	0
Redirections	0	0
Temps de réponse moyen à long terme (ms)	–	0
Temps de réponse de l'avenue récente (ms)	–	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
URL de démarrage	0	0
Refuser URL	0	0
En-tête de référence	0	0
débordement de tampon	0	0
Cohérence des cookies	0	0
Détournement de cookies	0	0
Balise de formulaire CSRF	0	0
Script intersite HTML	0	0
Injection HTML SQL	0	0
Format de champ	0	0
cohérence sur le terrain	0	0
Carte de crédit	0	0
Objet sûr	0	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
Violations de signature	0	0
Type de contenu	0	0
Déni de service JSON	0	0
Injection SQL JSON	0	0
Script intersite JSON	0	0
Types de téléchargement de fichiers	0	0
Déduire la charge utile XML du type de contenu	0	0
Injection de CMD HTML	0	0
Format XML	0	0
Déni de service XML (XDoS)	0	0
Validation des messages XML	0	0
Interopérabilité des services	0	0
Injection SQL XML	0	0
Script intersite XML	0	0
Pièce jointe XML	0	0
Violations d’erreur SOAP	0	0
Violations génériques XML	0	0
Nombre total de violations	0	0

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
Journaux d’URL de démarrage	0	0
Journaux d’URL refusées	0	0
Journaux d’en-tête Referer	0	0
Logs de débordement	0	0
Logs de débordement	0	0

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
Journaux de cohérence des cookies	0	0
Journaux de détournement de cookies	0	0
Journaux des balises de formulaire CSRF	0	0
Journaux de script intersite HTML	0	0
Journaux de transformation de script intersite HTML	0	0
Journaux d'injection HTML SQL	0	0
Journaux de transformation HTML SQL	0	0
Journaux de format de champ	0	0
Journaux de cohérence des champs	0	0
Cartes de crédit	0	0
Journaux de transformation des cartes de crédit	0	0
Journaux des objets sécurisés	0	0
Journaux de signature	0	0
Journaux du type de contenu	0	0
Journaux de déni de service JSON	0	0
Journaux d'injection JSON SQL	0	0
Journaux de script intersite JSON	0	0
Journaux des types de téléchargement de fichiers	0	0
Déduire la charge utile XML du type de contenu L	0	0

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
Journaux d'injection de commandes HTML	0	0
Journaux au format XML	0	0
Journaux de déni de service XML (XDoS)	0	0
Journaux de validation des messages XML	0	0
Journaux WSI	0	0
Journaux d'injection SQL XML	0	0
Journaux de script intersite XML	0	0
Journaux des pièces jointes XML	0	0
Journaux d'erreurs SOAP	0	0
Journaux génériques XML	0	0
Nombre total de messages journaux	0	0

Statistiques de réponse aux erreurs du serveur	Taux (/s)	Total :
Erreurs du client HTTP (4xx Resp)	0	0
Erreurs du serveur HTTP (5xx)	0	0

Afficher les statistiques sur le trafic et les violations des cookies à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un profil **Web App Firewall** et cliquez sur **Statistiques**.
3. La page des **statistiques du pare-feu NetScaler Web App** affiche les détails du trafic et des violations des cookie.

4. Vous pouvez sélectionner **Vue tabulaire** ou passer en mode Affichage **graphique pour afficher** les données sous forme de tableau ou de graphique.



Attribut cookie SameSite

May 5, 2023

Pour une communication Web sécurisée, Google a autorisé l'utilisation de l'attribut `SameSite` cookie. En se conformant à la nouvelle `SameSite` politique de Google Chrome, l'appliance NetScaler peut gérer les cookies tiers à l'aide de l' `SameSite` attribut défini dans l' `set-cookie` en-tête. Le paramètre de cookie atténue les attaques et fournit une communication Web sécurisée.

Jusqu'en février 2020, l' `SameSite` attribut n'était pas explicitement défini dans le cookie. Le navigateur a pris la valeur par défaut « Aucune ». Toutefois, certaines mises à niveau du navigateur, telles que Google Chrome 80, modifient le comportement interdomaine par défaut des cookies.

Définition de la valeur de l'attribut du cookie

L' `SameSite` attribut est défini sur l'une des valeurs suivantes et, pour le navigateur Google Chrome, la valeur par défaut est définie sur « Lax ».

Aucune. Indique que le navigateur doit utiliser le cookie pour les demandes dans le contexte intersite uniquement sur les connexions sécurisées.

Laxiste. Indique le navigateur qui doit utiliser le cookie pour les demandes dans le contexte du même site. Dans le contexte inter-site, seules les méthodes HTTP sûres comme la requête GET peuvent utiliser le cookie.

Stricte. Utilisez le cookie uniquement lorsque l'utilisateur demande explicitement le domaine.

> **Remarque :**
>
> Si les cookies définis (y compris les cookies de session du pare-feu) possèdent `SameSite` cet attribut et si l'indicateur d' `addcookiesamesite` attribut est activé dans le profil du pare-feu des applications Web, l' `SameSite` attribut est remplacé en fonction de la valeur configurée dans le profil.

Configurez l'attribut SameSite dans le profil Web App Firewall à l'aide de l'interface de ligne de commande

Pour configurer l' `SameSite` attribut, vous devez suivre les étapes suivantes :

1. Activez l'attribut `SameSite` cookie.
2. Définissez l'attribut cookie pour les cookies de session appfw.

Activer l'attribut de cookie « Samesite »

À l'invite de commande, tapez :

```
set appfw profile <profile-name> -insertCookieSameSiteAttribute ( ON | OFF)
```

Exemple :

```
set appfw profile p1 -insertCookieSameSiteAttribute ON
```

Définir la même valeur d'attribut de cookie de site pour les cookies de session du Web Application Firewall

À l'invite de commande, tapez :

```
set appfw profile <profile-name> - cookieSameSiteAttribute ( LAX | NONE |
STRICT )
```

Exemple :

```
set appfw profile p1 - cookieSameSiteAttribute LAX
```

Où se trouvent les types d'attributs,

Aucune. L'attribut de cookie SameSite est défini sur « aucun » et marqué comme sécurisé pour tous les cookies WAF et d'application.

Laxiste. L'attribut de cookie SameSite est défini sur « Lax » pour tous les cookies WAF et d'application.

Stricte. L'attribut de cookie SameSite est défini sur « Lax » pour tous les cookies WAF et d'application.

Configurez l'attribut de cookie SameSite dans le profil du Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page de **profil du NetScaler Web App Firewall**, cliquez sur Paramètres du **profil sous Paramètresavancés**.
4. Dans la section **Paramètres du profil**, définissez les paramètres suivants :

   a. Insérez l' `Samesite` attribut cookie. Cochez la case pour activer l' `Samesite` attribut cookie.
   b. Attribut du cookie Samesite. Sélectionnez une option dans la liste déroulante pour définir la valeur du `Samesite` cookie.
5. Cliquez sur **OK** et **Terminé**.



Vérification de la prévention des fuites de données

January 21, 2021

Les contrôles de prévention des fuites de données filtrent les réponses pour éviter les fuites d'informations sensibles, telles que les numéros de carte de crédit et les numéros de sécurité sociale, à des destinataires non autorisés.

Chèque de carte de crédit

May 5, 2023

Si votre application accepte les cartes de crédit ou si vos sites Web ont accès à des serveurs de base de données qui stockent les numéros de cartes de crédit, vous devez utiliser des mesures de prévention des fuites de données (DLP) et configurer la protection pour chaque type de carte de crédit que vous acceptez.

Le contrôle des cartes de crédit de NetScaler Web App Firewall empêche les attaquants d'exploiter les failles de prévention des fuites de données pour obtenir les numéros de carte de crédit de vos clients. En suivant des étapes de configuration simples, vous pouvez appliquer la protection d'une ou de plusieurs des cartes de crédit suivantes : 1) Visa, 2) Master Card, 3) Discover, 4) American Express (Amex), 5) JCB et 6) Diners Club.

Le contrôle de sécurité des cartes de crédit examine les réponses du serveur afin d'identifier les instances des numéros de carte de crédit cibles et applique une action spécifique lorsqu'un tel numéro est trouvé. L'action peut consister à transformer la réponse en supprimant tous les groupes de chiffres du numéro de carte de crédit sauf le dernier, ou à bloquer la réponse si elle contient plus qu'un nombre spécifié de numéros de carte de crédit. Si vous spécifiez les deux, l'action de blocage est prioritaire. Le paramètre Nombre maximum de cartes de crédit autorisées par page détermine à quel moment l'action de blocage est invoquée. Le paramètre par défaut, 0 (aucun numéro de carte de crédit n'est autorisé sur la page), est le plus sûr, mais vous pouvez en autoriser jusqu'à 255. Selon l'endroit où la violation est détectée dans la réponse et où l'action de blocage est déclenchée, vous pouvez obtenir un nombre de cartes de crédit inférieur au nombre maximum autorisé dans la réponse.

Pour éviter les faux positifs, vous pouvez appliquer des assouplissements pour exempter certains numéros de la vérification de la carte de crédit. Par exemple, un numéro de sécurité sociale, un numéro de bon de commande ou un numéro de compte Google peut être similaire à un numéro de carte de crédit. Vous pouvez spécifier des nombres individuels ou utiliser une expression régulière pour indiquer la chaîne de chiffres à contourner lors du traitement de l'URL de réponse pour l'inspection des cartes de crédit.

Si vous ne savez pas quels numéros de carte de crédit exempter, vous pouvez utiliser la fonction d'apprentissage pour générer des recommandations basées sur les données apprises. Pour obtenir des avantages optimaux sans compromettre les performances, vous pouvez activer cette option pendant une courte période afin d'obtenir un échantillon représentatif des règles, puis déployer les assouplissements et désactiver l'apprentissage.

Si vous activez la fonction de journalisation, la vérification de la carte de crédit génère des messages de journal indiquant les actions entreprises. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer que des tentatives d'accès ont été contrecarrées. Par défaut, le paramètre DoSecureCreditCardLogging est activé, de sorte que le numéro de carte de crédit n'est pas inclus dans le message de journal généré par la violation du protocole de sécurité du commerce (carte de crédit).

La fonction de statistiques rassemble des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée.

Pour configurer le contrôle de sécurité des cartes de crédit afin de protéger votre application, configurez le profil qui régit l'inspection du trafic à destination et en provenance de cette application.

> **Remarque** :
>
> Un site Web qui n'accède pas à une base de données SQL n'a généralement pas accès à des informations privées sensibles telles que les numéros de cartes de crédit.

Utilisation de la ligne de commande pour configurer le contrôle de carte de crédit

Dans l'interface de ligne de commande, vous pouvez utiliser la commande set appfw profile ou la commande add appfw profile pour activer la vérification des cartes de crédit et spécifier les actions à effectuer. Vous pouvez utiliser la commande unset appfw profile pour revenir aux paramètres par défaut. Pour spécifier des relaxations, utilisez la commande bind appfw pour lier les numéros de carte de crédit au profil.

Pour configurer une vérification de carte de crédit à l'aide de la ligne de commande

Utilisez la commande set appfw profile ou la commande add appfw profile, comme suit :

- `set appfw profile <name> -creditCardAction ( ([block][learn] [log][ stats])| [none])`
- `set appfw profile <name> -creditCard (VISA | MASTERCARD | DISCOVER | AMEX | JCB | DINERSCLUB)`
- `set appfw profile <name> -creditCardMaxAllowed <integer>`
- `set appfw profile <name> -creditCardXOut ([ON] | [OFF])<name> -doSecureCreditCard ([ON] | [OFF])`

- Pour configurer une règle d'assouplissement des règles relatives aux cartes de crédit à l'aide de la ligne de commande

  Utilisez la commande bind pour lier le numéro de carte de crédit au profil. Pour supprimer un numéro de carte de crédit d'un profil, utilisez la commande unbind, avec les mêmes arguments que ceux que vous avez utilisés pour la commande bind. Vous pouvez utiliser la commande show pour afficher les numéros de carte de crédit associés à un profil.

- Pour associer un numéro de carte de crédit à un profil

  ```
  bind appfw profile <profile-name> -creditCardNumber <any number/regex>
  "<url>"
  ```

  Exemple : bind appfw profile test_profile - Numéro de carte de crédit 378282246310005 `http:` `//www.example.com/credit\\_card\\_test.html`

  - Pour dissocier un numéro de carte de crédit d'un profil

    ```
    unbind appfw profile <profile-name> -creditCardNumber <credit card
    number / regex> <url>
    ```

  - Pour afficher la liste des numéros de cartes de crédit associés à un profil.

    ```
    show appfw profile <profile>
    ```

Utilisation de l'interface graphique pour configurer le contrôle de carte de crédit

Dans l'interface graphique, vous configurez le contrôle de sécurité de la carte de crédit dans le volet du profil associé à votre application.

Pour ajouter ou modifier le contrôle de sécurité de la carte de crédit à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils, sélectionnez** le profil cible et cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Contrôles de sécurité**.

   Le tableau de contrôle de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Deux options de configuration s'offrent à vous :

   a) Si vous souhaitez simplement activer ou désactiver les actions Block, Log, Stats et Learn pour les cartes de crédit, vous pouvez activer ou désactiver les cases à cocher dans le tableau, cliquer sur **OK**, puis sur **Enregistrer** et **fermer** pour fermer le volet de **contrôle de sécurité** .

   b) Si vous souhaitez configurer des options supplémentaires pour ce contrôle de sécurité, double-cliquez sur Carte de crédit ou sélectionnez la ligne et cliquez sur **Paramètres d'action** pour afficher les options supplémentaires suivantes :

      - Exclure : masquez tout numéro de carte de crédit détecté dans une réponse en remplaçant chaque chiffre, à l'exception des chiffres du dernier groupe, par la lettre « X ».

- Nombre maximum de cartes de crédit autorisées par page : spécifiez le nombre de cartes de crédit qui peuvent être transférées au client sans déclencher d'action de blocage.
- Cartes de crédit protégées. Cochez ou décochez une case pour activer ou désactiver la protection pour chaque type de carte de crédit.
- Vous pouvez également modifier les actions Block, Log, Stats et Learn dans le volet Paramètres de la carte de crédit.

  Après avoir apporté l'une des modifications ci-dessus, cliquez sur OK pour enregistrer les modifications et revenir au tableau des contrôles de sécurité. Vous pouvez procéder à la configuration d'autres contrôles de sécurité si nécessaire. Cliquez sur OK pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur Enregistrer et fermer pour fermer le volet Contrôle de sécurité.

3. Dans le volet **Paramètres avancés**, cliquez sur **Paramètres du profil**. Pour activer ou désactiver l'enregistrement sécurisé des numéros de cartes de crédit, cochez ou décochez la case **Enregistrement sécurisé des cartes de crédit** . (Par défaut, il est sélectionné).

   Cliquez sur **OK** pour enregistrer les modifications.

- Pour configurer une règle d'assouplissement des règles relatives aux cartes de crédit à l'aide de l'interface graphique

  1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
  2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**. Le tableau des règles de relaxation contient une entrée de carte de crédit. Vous pouvez double-cliquer ou sélectionner cette ligne et cliquer sur **Modifier** pour accéder à la boîte de dialogue relative aux règles d' **assouplissement des règles relatives aux cartes de crédit** . Vous pouvez effectuer des opérations Ajouter, Modifier, Supprimer, Activer ou Désactiver pour les règles de relaxation.

Utilisation de la fonction d'apprentissage avec la vérification de la carte de crédit

Lorsque l'action d'apprentissage est activée, le moteur d'apprentissage du Web App Firewall surveille le trafic et apprend les violations déclenchées. Vous pouvez inspecter périodiquement ces règles apprises. Après mûre réflexion, si vous souhaitez exempter une chaîne de chiffres spécifique du contrôle de sécurité des cartes de crédit, vous pouvez déployer la règle apprise en tant que règle d'assouplissement.

- Pour afficher ou utiliser les données apprises à l'aide de l'interface de ligne de commande

```
show appfw learningdata <profilename> creditCardNumber
```



```
rm appfw learningdata <profilename> -creditcardNumber <credit card
number> "<url>"

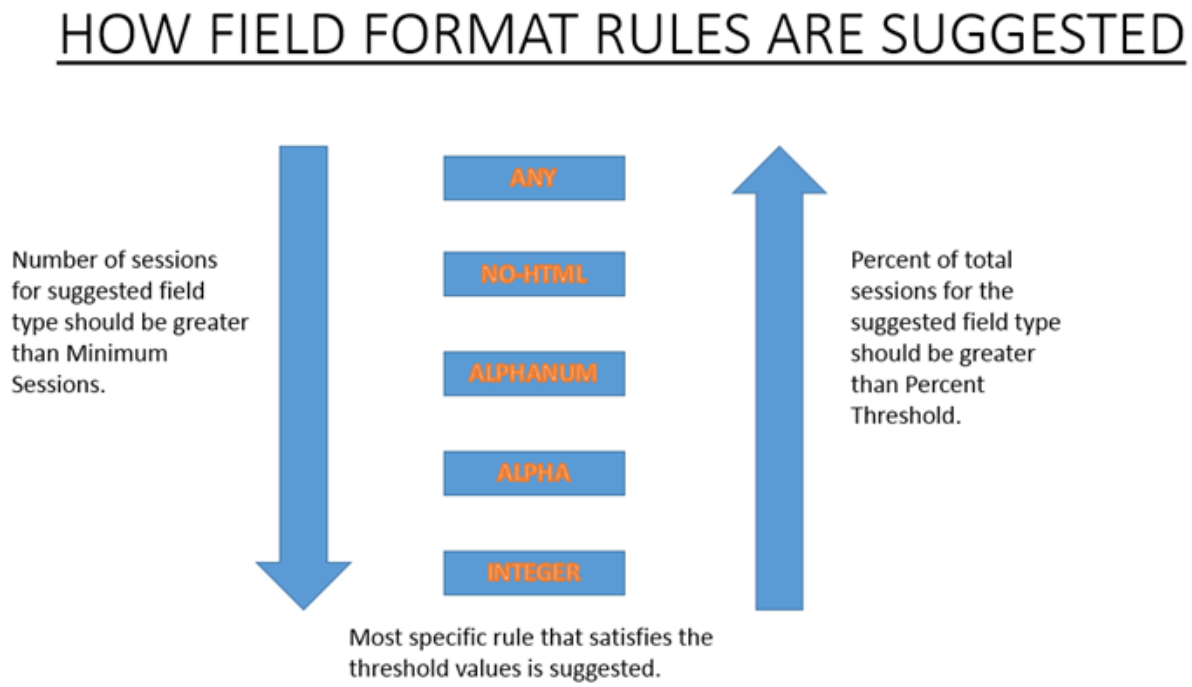
export appfw learningdata <profilename> creditCardNumber
```

- Pour afficher ou utiliser les données apprises à l'aide de l'interface graphique

  1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
  2. Dans le volet **Paramètres avancés**, cliquez sur **Règles apprises**. Vous pouvez sélectionner l'entrée relative à la carte de crédit dans le tableau des règles apprises et double-cliquer dessus pour accéder aux règles apprises. Vous pouvez déployer les règles apprises ou modifier une règle avant de la déployer en tant que règle de relaxation. Pour annuler une règle, vous pouvez la sélectionner et cliquer sur le bouton **Ignorer** . Vous ne pouvez modifier qu'une règle à la fois, mais vous pouvez sélectionner plusieurs règles à déployer ou à ignorer.

  Vous pouvez également afficher une vue résumée des relaxations apprises en sélectionnant l'entrée relative à la carte de crédit dans le tableau des règles apprises et en cliquant sur Visualiseur pour obtenir une vue consolidée de toutes les violations apprises. Le visualiseur permet de gérer très facilement les règles apprises. Il présente une vue complète des données sur un seul écran et facilite la prise de mesures sur un groupe de règles en un seul clic. Le principal avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de ces règles, en fonction du délimiteur et de l'URL d'action. Vous pouvez afficher 25, 50 ou 75 règles dans le visualiseur, en sélectionnant le nombre dans une liste déroulante. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer sous forme d'assouplissements. Vous pouvez également ignorer les règles pour les ignorer.

Utilisation de la fonction de journalisation avec la vérification de la carte de crédit

Lorsque l'action du journal est activée, les violations du contrôle de sécurité des cartes de crédit sont enregistrées dans le journal d'audit en tant que violations APPFW_SAFECOMMERCE ou APPFW_SAFECOMMERCE_XFORM. Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur Syslog distant.

Le paramètre par défaut pour DoSecureCreditCardLogging est ON. Si vous le définissez sur OFF, le numéro et le type de carte de crédit sont inclus dans le message du journal.

Selon les paramètres configurés pour les vérifications des cartes de crédit, les messages de journal générés par le pare-feu de l'application peuvent inclure les informations suivantes :

- La réponse a été bloquée ou n'a pas été bloquée.

- Les numéros de cartes de crédit ont été transformés (un X a été retiré). Un message de journal distinct est généré pour chaque numéro de carte de crédit transformé, de sorte que plusieurs messages de journal peuvent être générés lors du traitement d'une seule réponse.
- La réponse contenait le nombre maximum de numéros de cartes de crédit potentiels.
- Numéros de cartes de crédit et types correspondants.
- Pour accéder aux messages du journal à l'aide de la ligne de commande

  Passez au shell et suivez le fichier ns.logs dans le dossier /var/log/ pour accéder aux messages du journal relatifs aux violations des cartes de crédit :

  - Shell
  - tail -f /var/log/ns.log | grep SAFECOMMERCE
- Pour accéder aux messages du journal à l'aide de l'interface graphique

  1. L'interface graphique inclut un outil très utile (Syslog Viewer) pour analyser les messages du journal. Deux options s'offrent à vous pour accéder au visualiseur Syslog : Accédez au **profil cible** > Vérifications **de sécurité**. Surlignez la ligne Carte de crédit et cliquez sur Journaux. Lorsque vous accédez aux journaux directement à partir du contrôle de sécurité du profil par carte de crédit, il filtre les messages du journal et affiche uniquement les journaux relatifs à ces violations du contrôle de sécurité.
  2. ****Vous pouvez également accéder à la visionneuse Syslog en accédant à **NetScaler** > Système > Audit.**** Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation de vérification de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de contrôle de sécurité peuvent être déclenchées pendant le traitement des demandes.

     La visionneuse Syslog basée sur HTML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour accéder aux messages du journal des violations des contrôles de sécurité des cartes de crédit, filtrez en sélectionnant APPFW dans les options déroulantes du module. Le type d'événement affiche un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous cochez les cases APPFW_SAFECOMMERCE et APPFW_SAFECOMMERCE_XFORM et que vous cliquez sur le bouton Appliquer, seuls les messages du journal relatifs aux violations du contrôle de sécurité des cartes de crédit apparaissent dans le visualiseur Syslog.

     Si vous placez le curseur sur la ligne correspondant à un message de journal spécifique, plusieurs options, telles que Module et EventType, apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans les journaux.

Exemple de message de journal au format natif lorsque la réponse n'est pas bloquée


```
May 29 01:26:31 <local0.info> 10.217.31.98 05/29/2015:01:26:31 GMT ns
    0-PPE-0 :
default APPFW APPFW_SAFECOMMERCE 2181 0 :  10.217.253.62 1098-PPE0
4erNfkaHy0IeGP+nv2S9Rsdu77I0000 pr_ffc http://aaron.stratum8.net/FFC/
    CreditCardMind.html
Maximum number of potential credit card numbers seen <not blocked>
<!--NeedCopy-->
```

Exemple de message de journal au format CEF lorsque la réponse est transformée

```
May 28 23:42:48 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE_XFORM|6|src
    =10.217.253.62
spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
    CreditCardMind.html
msg=Transformed (xout) potential credit card numbers seen in server
    response
cn1=66 cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002
cs4=ALERT cs5=2015 act=transformed
<!--NeedCopy-->
```

Exemple de message de journal au format CEF lorsque la réponse est bloquée. Le numéro et le type de carte de crédit sont visibles dans le journal, car le paramètre DoSecureCreditCardLogging est désactivé.

```
May 28 23:42:48 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE|6|src
    =10.217.253.62
spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
    CreditCardMind.html
msg=Credit Card number 4505050504030302 of type Visa is seen in
    response cn1=68
cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002 cs4=
    ALERT cs5=2015
act=blocked
<!--NeedCopy-->
```

Statistiques relatives aux violations des cartes de crédit

Lorsque l'action statistique est activée, le compteur correspondant à la vérification de la carte de crédit est incrémenté lorsque le Web App Firewall prend une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. L'incrément du compteur de journaux peut varier en fonction des paramètres configurés.

Par exemple, si l'action de blocage est activée et que le paramètre Nombre maximum de cartes de crédit autorisées est 0, la demande d'une page contenant 20 numéros de carte de crédit incrémente le compteur de statistiques d'une unité lorsque la page est bloquée dès que le premier numéro de carte de crédit est détecté. Toutefois, si le blocage est désactivé et que la transformation est activée, le traitement de la même demande incrémente le compteur de statistiques des journaux de 20, car chaque transformation de carte de crédit génère un message de journal distinct.

- Pour afficher les statistiques des cartes de crédit à l'aide de la ligne de commande

  À l'invite de commande, tapez :

  ```
  sh appfw stats
  ```

  Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

  ```
  stat appfw profile <profile name>
  ```

  Pour afficher les statistiques des cartes de crédit à l'aide de l'interface graphique

  1. Accédez à **Système** > **Sécurité** > **Web App Firewall**.
  2. Dans le volet droit, accédez au lien **Statistiques** .
  3. Utilisez la barre de défilement pour consulter les statistiques sur les violations des cartes de crédit et les journaux. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Résumé

Prenez note des points suivants concernant le contrôle de sécurité de la carte de crédit :

- Le Web App Firewall vous permet de protéger les informations de carte de crédit et de détecter toute tentative d'accès à ces données sensibles.
- Pour utiliser le contrôle de protection des cartes de crédit, vous devez spécifier au moins un type de carte de crédit et une action. La vérification est ensuite appliquée aux profils HTML, XML et Web 2.0.
- Vous pouvez rediriger la sortie de la commande sh appfw profile et grep pour CreditCard pour voir toutes les configurations spécifiques à la carte de crédit. Par exemple, sh appfw profile my_profile | grep CreditCard affiche les paramètres configurés ainsi que les règles de relaxation relatives à la vérification des cartes de crédit pour le profil du Web App Firewall nommé my_profile.
- Vous pouvez exclure des numéros spécifiques de l'inspection des cartes de crédit sans contourner l'inspection de sécurité pour les autres numéros de carte de crédit.
- La fonctionnalité Relaxation est disponible pour tous les modèles de cartes de crédit protégés par le Web App Firewall. Dans l'interface graphique, vous pouvez utiliser le visualiseur pour spécifier les opérations d'ajout, de modification, de suppression, d'activation ou de désactivation sur les règles de relaxation.

- Le moteur d'apprentissage du Web App Firewall peut surveiller le trafic sortant afin de recommander des règles en fonction des violations observées. Le support du visualiseur est également disponible pour gérer les règles de carte de crédit apprises dans l'interface graphique. Vous pouvez modifier et déployer les règles apprises, ou les ignorer après une inspection minutieuse.
- Le paramètre du nombre de cartes de crédit autorisées s'applique à chaque réponse. Cela ne concerne pas le total cumulé des numéros de cartes de crédit observés pendant toute la session utilisateur.
- Le nombre de chiffres en X dépend de la longueur des numéros de carte de crédit. Pour les cartes de crédit comportant de 13 à 15 chiffres, les dix chiffres sont en croix. Douze chiffres sont supprimés en X pour les cartes de crédit à 16 chiffres. Si votre application ne nécessite pas l'envoi de l'intégralité du numéro de carte de crédit dans la réponse, Citrix vous recommande d'activer cette action pour masquer les chiffres des numéros de carte de crédit.
- L'opération X-out transforme toutes les cartes de crédit et fonctionne indépendamment des paramètres configurés pour le nombre maximum de cartes de crédit autorisées. Par exemple, si la réponse contient 4 cartes de crédit et que le paramètre CreditCardMaxAllowed est défini sur 10, les 4 cartes de crédit sont sorties en X, mais elles ne sont pas bloquées. Si les numéros de carte de crédit sont dispersés dans le document, une réponse partielle avec des numéros X'D-Out peut être envoyée au client avant que la réponse ne soit bloquée.
- Ne désactivez pas le paramètre DoSecureCreditCardLogging avant d'y avoir dûment réfléchi. Lorsque ce paramètre est désactivé, les numéros de carte de crédit s'affichent et sont accessibles dans les messages du journal. Ces chiffres ne sont pas masqués dans les journaux, même si l'action X-out est activée. Si vous envoyez des journaux à un serveur Syslog distant et que les journaux sont compromis, les numéros de carte de crédit peuvent être divulgués.
- Lorsque la page de réponse est bloquée en raison d'une violation de carte de crédit, le Web App Firewall ne redirige pas vers la page d'erreur.

Vérification des objets sécurisés

May 5, 2023

La vérification des objets sécurisés fournit une protection configurable par l'utilisateur pour les informations commerciales sensibles, telles que les numéros de clients, les numéros de commande et les numéros de téléphone ou codes postaux spécifiques à un pays ou à une région. Une expression régulière définie par l'utilisateur ou un plug-in personnalisé indique au Web App Firewall le format de ces informations et définit les règles à utiliser pour les protéger. Si une chaîne d'une demande utilisateur correspond à une définition d'objet sécurisé, le Web App Firewall bloque la réponse, masque les informations protégées ou supprime les informations protégées de la réponse avant de les envoyer à l'utilisateur, selon la façon dont vous avez configuré cette règle d'objet sécurisé particulière.

La vérification des objets sécurisés empêche les attaquants d'exploiter une faille de sécurité dans votre logiciel de serveur Web ou sur votre site Web pour obtenir des informations privées sensibles, telles que les numéros de carte de crédit de l'entreprise ou les numéros de sécurité sociale. Si vos sites Web n'ont pas accès à ce type d'informations, vous n'avez pas besoin de configurer cette vérification. Si vous disposez d'un panier d'achat ou d'une autre application qui peut accéder à ces informations, ou si vos sites Web ont accès à des serveurs de base de données contenant ces informations, vous devez configurer la protection pour chaque type d'informations privées sensibles que vous gérez et stockez.

> **Remarque :**
>
> Un site Web qui n'accède pas à une base de données SQL n'a généralement pas accès aux informations privées sensibles.

La vérification des objets sûrs ne ressemble à aucune autre vérification. Chaque expression d'objet sécurisé que vous créez est l'équivalent d'une vérification de sécurité distincte, similaire à la vérification de carte de crédit, pour ce type d'informations.

Configuration de la vérification des objets sécurisés à l'aide de l'interface

> **Remarque**
>
> Vous devez configurer la vérification des objets sûrs uniquement à l'aide de l'interface graphique. L'interface de ligne de commande n'est pas prise en charge.

Pour ajouter une vérification de sécurité des objets sécurisés à l'aide de l'interface graphique :

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Sélectionnez le profil souhaité et cliquez sur **Modifier**.
3. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
4. Sélectionnez **Safe Object** et cliquez sur **Edit**.
5. Cliquez sur **Ajouter** et configurez les éléments suivants :
    - **Nom de l'objet sécurisé.** Un nom pour votre nouvel objet sécurisé. Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement. Le nom peut être composé de 1 à 255 lettres, chiffres et du tiret (-), du point (.) livre (#), de l'espace (), du signe at (@), de l'égal (=), du deux-points (:) et du trait de soulignement (_).
    - **Des actions.** Activez ou désactivez les actions **Bloquer**, **Consigner**et **Statistiques**, ainsi que les actions suivantes :
        - **Sortie X.** Masquez toutes les informations qui correspondent à l'expression d'objet sécurisé par la lettre « X ».
        - **Remove.** Supprimez toutes les informations correspondant à l'expression d'objet sécurisé.

- **Expression régulière.** Entrez une expression régulière compatible PCRE qui définit l'objet sécurisé. Vous pouvez créer l'expression régulière de l'une des manières suivantes :
  - En saisissant l'expression régulière directement dans la zone de texte
  - En utilisant le menu **Regex Tokens** pour saisir des éléments d'expression régulière et des symboles directement dans la zone de texte
  - En ouvrant l'éditeur d'expressions régulières et en l'utilisant pour construire l'expression. L'expression régulière doit être composée uniquement de caractères ASCII. Ne coupez pas et ne collez pas de caractères qui ne font pas partie du jeu ASCII de base de 128 caractères. Si vous souhaitez inclure des caractères non ASCII, vous devez les saisir manuellement au format de codage hexadécimal PCRE.

  > **Remarque :**
  >
  > n'utilisez pas d'ancres de début (^) au début des expressions d'objet sécurisé, ni d'ancres de fin ($) à la fin des expressions d'objet sécurisé. Ces entités PCRE ne sont pas prises en charge dans les expressions d'objet sécurisé et, si elles sont utilisées, votre expression ne correspond pas à ce qu'elle était censée correspondre.

- **Durée maximale du match.** Entrez un entier positif qui représente la longueur maximale de la chaîne à laquelle vous souhaitez faire correspondre. Par exemple, si vous souhaitez faire correspondre les numéros de sécurité sociale américains, saisissez le chiffre 11 dans ce champ. Cela permet à votre expression régulière de faire correspondre une chaîne de neuf chiffres et deux tirets. Si vous souhaitez faire correspondre les numéros de permis de conduire californiens, saisissez le chiffre huit (8).

  > **Attention :**
  >
  > Si vous ne définissez pas la longueur maximale de correspondance, le Web App Firewall utilise la valeur par défaut de un (1) lors du filtrage des chaînes correspondant à vos expressions d'objet sûres. Par conséquent, la plupart des expressions d'objet sûres ne correspondent pas à leurs chaînes cibles.

Vous pouvez modifier un express existant en sélectionnant l'expression requise, en cliquant sur **Ouvrir**, puis en configurant l'expression dans la boîte de dialogue **Modifier l'objet sécurisé** .

Voici des exemples d'expressions régulières de vérification d'objets sûrs :

- Recherchez les chaînes qui semblent être des numéros de sécurité sociale (SSN) américains. Le SSN se compose des caractères suivants dans l'ordre indiqué :
  - Trois chiffres (dont le premier ne doit pas être zéro)
  - Un trait d'union
  - Encore deux chiffres
  - Un deuxième trait d'union
  - Une suite de quatre autres chiffres


```
[1-9][0-9]{
3,3 }
-[0-9]{
2,2 }
-[0-9]{
4,4 }

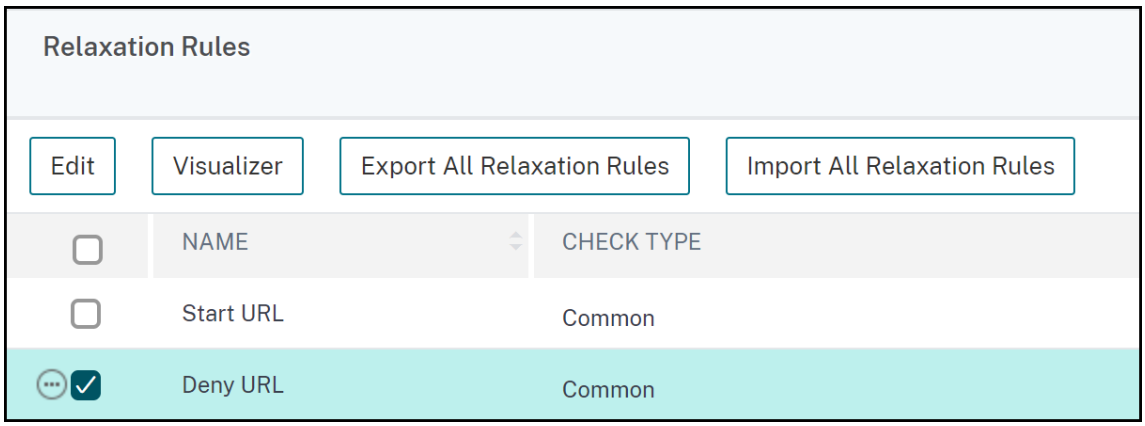
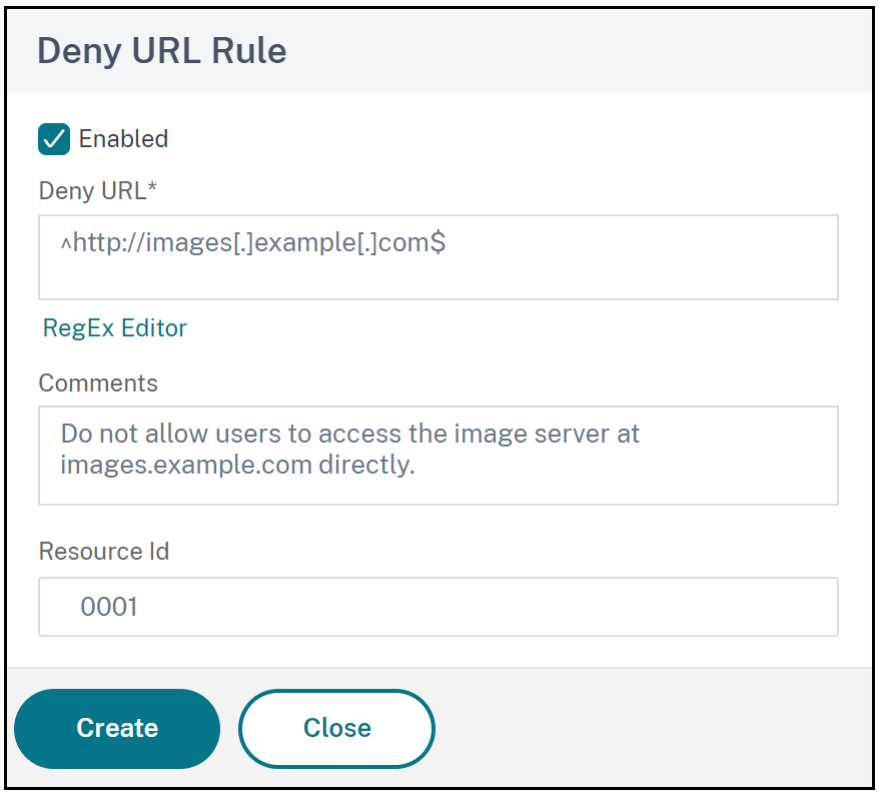
<!--NeedCopy-->
```

- Recherchez les chaînes qui semblent être des numéros de permis de conduire californiens, qui commencent par une lettre et sont suivies d'une chaîne de sept chiffres exactement :

```
[A-Za-z][0-9]{
7,7 }

<!--NeedCopy-->
```

- Recherchez les chaînes qui semblent être des identifiants de clients. Les identifiants clients se composent des éléments suivants dans l'ordre indiqué :
  - Une chaîne de cinq caractères hexadécimaux (tous les chiffres et les lettres de A à F)
  - Un trait d'union
  - Un code à trois lettres
  - Un deuxième trait d'union
  - Une chaîne de 10 chiffres

```
[0-9A-Fa-f]{
5,5 }
-[A-Za-z]{
3,3 }
-[0-9]{
10,10 }

<!--NeedCopy-->
```

> **Attention :**
>
> Les expressions régulières sont puissantes. Si vous êtes moins familiarisé avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous que l'expression régulière définit exactement le type de chaîne que vous souhaitez ajouter en tant que définition d'objet sécurisée. L'utilisation négligente de caractères génériques, et en particulier de la combinaison métacaractère/caractère générique point-astérisque (.*), peut avoir des résultats que vous ne vouliez pas ou que vous n'attendiez pas, tels que le blocage de l'accès

> à du contenu Web que vous n'aviez pas l'intention de bloquer.

Contrôles avancés de protection des formulaires

December 3, 2021

Les contrôles avancés de protection des formulaires examinent les données des formulaires Web pour empêcher les attaquants de compromettre votre système en modifiant les formulaires Web de vos sites Web ou en envoyant des types et des quantités inattendus de données à votre site Web sous forme.

> **Remarque :**
>
> Les contrôles de protection SQL, de script intersite, FFC et FieldFormat sont appliqués si l'option **Exclure les fichiers de chargement des contrôles de sécurité** n'est pas définie.

Un téléchargement de fichier est également un élément de formulaire qui a champ **nom** de contrôle qui est soumis dans le cadre de la soumission de formulaire.

Pour plus d'informations, reportez-vous à cette page : Formulaires

> **Remarque**
>
> Les protections de formulaires ferment les formulaires imbriqués lorsque des vérifications basées sur des formulaires sont activées. Cela permet de s'assurer que la norme HTML est respectée.

Vérification des formats de champs

May 5, 2023

Le contrôle Formats de champ vérifie les données que les utilisateurs envoient à vos sites Web dans les formulaires Web. Il examine à la fois la longueur et le type des données afin de s'assurer qu'elles sont adaptées au champ de formulaire dans lequel elles apparaissent. Si le Web App Firewall détecte des données de formulaire Web inappropriées dans une demande utilisateur, il bloque la demande.

En empêchant un attaquant d'envoyer des données de formulaire Web inappropriées à votre site Web, la vérification des formats de champs prévient certains types d'attaques sur votre site Web et vos serveurs de base de données. Par exemple, si un champ particulier demande à l'utilisateur de saisir un numéro de téléphone, la vérification des formats de champ examine la saisie soumise par l'utilisateur pour s'assurer que les données correspondent au format d'un numéro de téléphone. Si

un champ particulier attend un prénom, la vérification des formats de champ garantit que les données de ce champ sont d'un type et d'une longueur appropriés pour un prénom. Il fait la même chose pour chaque champ de formulaire que vous le configurez pour protéger.

Cette vérification s'applique uniquement aux requêtes HTML. Elle ne s'applique pas aux requêtes XML. Vous pouvez configurer la vérification du format des champs dans les profils HTML ou les profils Web 2.0 pour inspecter la charge utile HTML afin de protéger vos applications. Le Web App Firewall prend également en charge la protection Field Format Check pour les applications Google Web Toolkit (GWT).

Pour vérifier les formats de champs, vous devez activer une ou plusieurs actions. Le Web App Firewall examine les entrées soumises et applique les actions spécifiées.

> **Remarque**
>
> Les règles relatives au format des champs sont des règles plus strictes. Les ajouter à la liste de relaxation à partir des données apprises agit comme une règle de blocage.
>
> Pour assouplir les règles de format de champ, supprimez le « nom de champ » spécifique de la liste des assouplissements de format de champ.

Vous avez la possibilité de définir les formats de champ par défaut pour spécifier le type de champ et la longueur minimale et maximale des données attendues dans chaque champ de formulaire Web que vous souhaitez protéger. Vous pouvez déployer des règles de relaxation pour configurer un format de champ pour un champ individuel d'un formulaire spécifique. Plusieurs règles peuvent être ajoutées pour spécifier le nom du champ, l'URL de l'action et les formats de champ. Spécifiez des formats de champ pour accepter différents types d'entrées dans différents champs de formulaire. La fonction d'apprentissage peut fournir des recommandations concernant les règles de relaxation.

Actions de mise en forme des champs : vous pouvez activer les actions de blocage, de journalisation, de statistiques et d'apprentissage. Au moins l'une de ces actions doit être activée pour activer la protection Field Format Check.

- **Bloquer**. Si vous activez le blocage, l'action de blocage est déclenchée si l'entrée n'est pas conforme au format de champ spécifié. Si une règle a été configurée pour le champ cible, la saisie est vérifiée par rapport à la règle spécifiée. Dans le cas contraire, il est vérifié par rapport à la spécification du format de champ par défaut. Toute incompatibilité dans le type de champ ou la spécification de longueur min/max entraîne le blocage de la demande.
- **Journal**. Si vous activez la fonctionnalité de journalisation, la vérification du format des champs génère des messages de journal indiquant les actions entreprises. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives malveillantes de lancer une attaque.
- **Statistiques**. Si elle est activée, la fonction de statistiques recueille des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer

que votre application est attaquée ou que vous devrez peut-être revoir la configuration pour voir si le format de champ spécifié est trop restrictif.

- **Apprenez**. Si vous n'êtes pas sûr des types de champs ou des valeurs de longueur minimale et maximale les mieux adaptés à votre application, vous pouvez utiliser la fonction d'apprentissage pour générer des recommandations basées sur les données apprises. Le moteur d'apprentissage Web App Firewall surveille le trafic et fournit des recommandations de format de champ en fonction des valeurs observées. Pour obtenir des avantages optimaux sans compromettre les performances, vous pouvez activer l'option d'apprentissage pendant une courte période afin d'obtenir un exemple représentatif des règles, puis déployer les règles et désactiver l'apprentissage.
  Remarque : Le moteur d'apprentissage du Web App Firewall ne peut distinguer que les 128 premiers octets du nom. Si un formulaire comporte plusieurs champs dont les noms correspondent aux 128 premiers octets, le moteur d'apprentissage peut ne pas être en mesure de les distinguer. De même, la règle de relaxation déployée peut par inadvertance assouplir tous ces champs.

Format de champ par défaut—Outre la configuration des actions, vous pouvez configurer le format de champ par défaut pour spécifier le type de données attendu dans tous les champs de formulaire de votre application. Un type de champ peut être sélectionné comme type de format de champ. Les paramètres de longueur minimale et de longueur maximale peuvent être utilisés pour spécifier la longueur des entrées autorisées. Comme alternative aux types de champs, vous pouvez utiliser des cartes de caractères pour spécifier ce qui est autorisé dans un champ (sauf dans les déploiements de clusters).

- **Type de champ**—Les types de champs sont des expressions nommées auxquelles vous attribuez des valeurs de priorité. Les expressions de type de champ spécifient les entrées autorisées et sont comparées aux données soumises afin de déterminer si les valeurs reçues sont cohérentes avec les valeurs autorisées. Les types de champs sont vérifiés dans l'ordre de leurs numéros de priorité. Un chiffre inférieur indique une priorité plus élevée. Le Web App Firewall vous permet d'ajouter vos propres types de champs et de leur attribuer les priorités que vous souhaitez. La valeur de priorité peut être comprise entre 0 et 64 000. Les types de champs intégrés suivants sont fournis pour simplifier le processus de configuration :

```
1  > sh appfw fieldtype
2  1)      Name:  integer          Regex:  "^[+-]?[0-9]+$"
3                  Priority:  30           Comment:  Integer
4                  Builtin:  IMMUTABLE
5  2)      Name:  alpha            Regex:  "^[a-zA-Z]+$"
6                  Priority:  40           Comment:  "Alpha
                      characters"
7               Builtin:  IMMUTABLE
8  3)      Name:  alphanum         Regex:  "^[a-zA-Z0-9]+$"
```



```
                Priority:  50            Comment:  "Alpha-numeric
                    characters"
                Builtin:  IMMUTABLE
4)      Name:  nohtml            Regex:  "^[^&<>]\*$"
                Priority:  60            Comment:  "Not HTML"
                Builtin:  IMMUTABLE
5)      Name:  any               Regex:  "^.\*$"
             Priority:  70            Comment:  Anything
                Builtin:  IMMUTABLE
    Done
>
<!--NeedCopy-->
```

> **Remarque :** Les types de champs intégrés sont IMMUABLES. Ils ne peuvent être ni modifiés ni supprimés. Tous les types de champs que vous ajoutez sont MODIFIABLES. Vous pouvez les modifier ou les supprimer.

La configuration d'un type de champ en tant que format de champ par défaut peut s'avérer utile lorsque vous disposez d'une expression PCRE capable d'identifier les entrées valides dans tous ou dans la plupart des champs de formulaire de votre application et d'exclure les entrées non valides. Par exemple, si toutes les entrées de vos formulaires de demande ne doivent contenir que des chiffres et des lettres, vous pouvez utiliser le type de champ alphanum intégré comme type de champ par défaut. Tout caractère non alphanumérique tel qu'une barre oblique inverse () ou un point-virgule présent dans la saisie déclenchera une violation. Vous pouvez également ajouter vos propres Types de champs personnalisés et les utiliser pour configurer les Formats de champs par défaut. Par exemple, si vous souhaitez que les minuscules « x », « y » et « z » soient les seuls caractères alpha autorisés, vous pouvez configurer un type de champ personnalisé avec l'expression régulière « ^ [x-z] +$ ». Vous pouvez lui attribuer une priorité plus élevée (numéro de priorité inférieure) que les Types de champs intégrés et l'utiliser comme Type de champ par défaut.

- **Longueur minimale : longueur** de données minimale par défaut attribuée aux champs de formulaire dans les formulaires Web qui n'ont pas de paramètre explicite. Ce paramètre est défini sur 0 par défaut, ce qui permet à l'utilisateur de laisser le champ vide. Tout paramètre plus élevé oblige les utilisateurs à remplir le champ.

  Attention : Si la valeur de longueur minimale est 0 mais que le type de champ est entier, alpha ou alphanumérique, une demande est bloquée si un champ de saisie est laissé vide, malgré le paramètre de longueur minimale. Cela est dû au fait que le RegEx pour ces types de champs contient un caractère +, ce qui signifie un ou plusieurs caractères. Pour distinguer un entier d'un caractère alpha, il faut au moins un caractère.

- **Longueur maximale** : longueur de données maximale par défaut attribuée aux champs de for-

mulaire dans les formulaires Web qui n'ont pas de paramètre explicite. Ce paramètre est défini sur 65535 par défaut.

> **Remarque : Nombre** de caractères par rapport au nombre d'octets. Les longueurs minimale et maximale des formats de champ représentent le nombre d'octets et non le nombre de caractères. Les langues dont la représentation des caractères est supérieure à un octet peuvent entraîner le dépassement de la limite avec un nombre de caractères inférieur au nombre configuré pour la valeur maximale. Par exemple, dans le cas d'une représentation de caractères sur deux octets, la valeur maximale de 9 n'autorise pas plus de 4 caractères. **Conseil :** L'interface graphique vous permet de couper et coller des caractères UTF-8 directement dans l'interface graphique sans avoir à les convertir en hexadécimal.

- **Cartes de caractères** : en plus de recommander les types de champs, le moteur d'apprentissage du Web App Firewall vous propose une option supplémentaire, Utiliser les cartes de caractères, pour déployer les règles de vérification du format. Une table de caractères est un ensemble de caractères autorisés dans un champ de formulaire particulier. Vous pouvez affiner la spécification du format de champ pour autoriser ou interdire des caractères spécifiques à l'aide des cartes de caractères. Une table de caractères distincte est générée pour chaque champ de formulaire. Les caractères alpha et numériques sont traités différemment dans les cartes de caractères. Si un caractère alpha apparaît dans l'entrée, tous les caractères alpha [a-za-z] seront autorisés par l'expression PCRE recommandée dans la table des caractères. De même, si un chiffre est inclus, tous les chiffres [0-9] seront autorisés. Les caractères non imprimables sont spécifiés à l'aide de la construction x. Seuls les caractères codés sur un octet dont les valeurs sont comprises entre 0 et 255 sont pris en compte pour les recommandations de la table de caractères.

  Une table de caractères peut être plus précise que la recommandation de type de champ correspondante. Dans certains cas, les cartes de caractères peuvent être une meilleure option, car elles vous permettent de mieux contrôler l'ensemble de caractères autorisés comme entrées. Les cartes de caractères déployées sont affichées sous forme de chaînes commençant par le préfixe « CM » suivi de chiffres. La priorité pour les cartes de personnages commence à 10 000. Comme pour les types de champs ajoutés par l'utilisateur, vous pouvez ajouter, modifier ou supprimer une table de caractères. Les cartes de personnages actuellement utilisées dans les règles déployées ne peuvent pas être modifiées ni supprimées.

  Remarque : Les cartes de caractères ne sont pas prises en charge dans les déploiements de clusters.

> **Remarque**
>
> Lorsque vous ajoutez une règle de mise en forme de champ avec un type de champ intégré, que vous utilisez une table de caractères au lieu du type de champ et que vous l'enregistrez, les modifications ne sont pas enregistrées et la règle s'affiche toujours avec le type de champ.

> Lorsque la carte de caractères correspond à l'un des types intégrés, le type de champ est réutilisé au lieu de créer une nouvelle carte de caractères.

Utilisation de la ligne de commande pour configurer la vérification du format des champs

Dans l'interface de ligne de commande, vous pouvez utiliser la commande add appfw fieldtype pour ajouter un nouveau type de champ. Vous pouvez utiliser la commande set appfw profile ou la commande add appfw profile pour configurer la vérification du format de champ et spécifier les actions à effectuer. Vous pouvez utiliser la commande unset appfw profile pour rétablir les paramètres configurés à leurs valeurs par défaut. Pour spécifier une règle de format de champ, utilisez la commande bind appfw pour lier un type de champ à un champ de formulaire et à l'URL de l'action, ainsi que les spécifications de longueur minimale et maximale.

Pour ajouter, supprimer ou afficher un type de champ à l'aide de la ligne de commande :

Utilisez la commande Ajouter pour ajouter un type de champ. Vous devez spécifier le nom, l'expression régulière et la priorité lorsque vous ajoutez un nouveau type de champ. Vous avez également la possibilité d'ajouter un commentaire. Vous pouvez utiliser la commande show pour afficher les types de champs configurés. Vous pouvez également supprimer un type de champ à l'aide de la commande de suppression, qui nécessite uniquement le nom du type de champ.

```
add [appfw] fieldType <name> <regex> <priority> [-comment <string>]
```

où :

<regex> est une expression régulière

<priority> est un entier positif

Exemple :

```
1  add fieldtype "Cust_Zipcode" "^[0-9]{
2   5 }
3   [-][0-9]{
4   4 }
5   $" 4
6
7  -  show [appfw] fieldType [<name>]
8
9      Example: sh fieldtype
10
11     sh appfw fieldtype
12
13     sh appfw fieldtype cust_zipcode
14
```



```
- `rm [appfw] fieldType <name>`

    Example: rm fieldtype cusT_ziPcode

    `rm appfw fieldtype cusT_ziPcode`
<!--NeedCopy-->
```

> **Remarque :** Comme indiqué ci-dessus, l'utilisation de « appfw » dans la commande est facultative. Par exemple, « Ajouter un type de champ » ou « Ajouter un type de champ appfw » sont deux options valides. Les noms des types de champs ne distinguent pas les majuscules des minuscules en raison de la normalisation. Comme indiqué dans les exemples ci-dessus, Cust_Zipcode, cust_zipcode et Cust_Zipcode font référence au même type de champ.

Pour configurer une vérification du format de champ à l'aide de la ligne de commande

Utilisez la commande set appfw profile ou la commande add appfw profile, comme suit :

- `set appfw profile <name> -fieldFormatAction (([block] [learn] [log] [ stats])| [none])`
- `set appfw profile <name>-defaultFieldFormatType <string>`
- `set appfw profile <name> -defaultFieldFormatMinLength <integer>`
- `set appfw profile <name> -defaultFieldFormatMaxLength <integer>`

Pour configurer une règle de relaxation du format de champ à l'aide de la ligne de commande

```
bind appfw profile <name> (-fieldFormat <string> <formActionURL>  <
    fieldType>
[-fieldFormatMinLength <positive_integer>]  [-fieldFormatMaxLength <
    positive_integer>]
[-isRegex ( REGEX | NOTREGEX )])
<!--NeedCopy-->
```

Exemple :

```
bind appfw profile pr_ffc -fieldFormat "login_name" ".*/login.php"
    integer -fieldformatMinLength 3 -FieldformatMaxlength 6
<!--NeedCopy-->
```

Utilisation de l'interface graphique pour configurer le contrôle de sécurité des formats de champs

Dans l'interface graphique, vous pouvez gérer les types de champs. Vous pouvez également configurer le contrôle de sécurité des formats de champ dans le volet du profil associé à votre application.

Pour ajouter, modifier ou supprimer un type de champ à l'aide de l'interface graphique

1. Accédez au nœud Application Firewall. Dans les paramètres, cliquez sur **Gérer les types de champs** pour afficher la boîte de dialogue Configurer le type de champ du pare-feu d'applications.
2. Cliquez sur **Ajouter** pour ajouter un nouveau type de champ. Suivez les instructions de ce volet et cliquez sur Créer. Vous pouvez également modifier ou supprimer tout type de champ ajouté par l'utilisateur s'il n'est actuellement pas utilisé par une règle déployée.

Pour ajouter ou modifier le contrôle de sécurité des formats de champs à l'aide de l'interface graphique

1. Accédez à **Application Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Contrôles de sécurité**.

   Le tableau de contrôle de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Deux options de configuration s'offrent à vous :

   a) Si vous souhaitez simplement activer ou désactiver les actions **Block**, **Log**, **Stats**et **Learn** pour les formats de champs, vous pouvez activer ou désactiver les cases à cocher dans le tableau, cliquer sur **OK**, puis sur **Enregistrer et fermer** pour fermer le volet de contrôle de sécurité.
   b) Si vous souhaitez configurer des options supplémentaires pour ce contrôle de sécurité, double-cliquez sur Formats de champ ou sélectionnez la ligne et cliquez sur Paramètres d'action pour afficher les options suivantes pour le **format de champ par défaut** :
      - **Type de champ**—Sélectionnez le type de champ que vous souhaitez configurer comme type de champ par défaut. Vous pouvez sélectionner les types de champs intégrés et définis par l'utilisateur. Les cartes de personnages déployées sont également incluses dans la liste et peuvent être sélectionnées.
      - **Longueur minimale**—Spécifiez le nombre minimum de caractères que doit contenir chaque champ. Valeurs possibles : 0-65535.
      - **Longueur maximale**— Spécifiez le nombre maximum de caractères que doit contenir chaque champ. Valeurs possibles : 1-65535.
        Vous pouvez également modifier les actions **Block**, **Log**, **Stats** et **Learn** dans le volet Paramètres des formats de champs.

   Après avoir apporté l'une des modifications ci-dessus, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau des contrôles de sécurité. Vous pouvez procéder à la configuration d'autres contrôles de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur **Enregistrer et fermer** pour fermer le volet Contrôle de sécurité.

Pour configurer une règle de relaxation Field Formats à l'aide de l'interface graphique

1. Accédez à **Application Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Modifier**.

2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**. Le tableau des règles de relaxation contient une entrée Formats de champs. Vous pouvez double-cliquer ou sélectionner cette ligne et cliquer sur le bouton Modifier pour accéder à la boîte de dialogue Règles de relaxation des formats de champs. Vous pouvez effectuer des opérations d' **ajout**, de **modification**, de **suppression**, **d'activation**ou de **désactivation** pour les règles de relaxation.

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez surligner la ligne Formats de champ et cliquer sur Visualiseur. Le visualiseur pour les relaxations déployées vous offre la possibilité d' ajouter une nouvelle règle ou de modifier une règle existante. Vous pouvez également activer ou désactiver un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Utilisation de la fonction d'apprentissage avec la vérification des formats de champs

Lorsque l'action d'apprentissage est activée, le moteur d'apprentissage du Web App Firewall surveille le trafic et apprend les violations déclenchées. Vous pouvez inspecter périodiquement ces règles apprises. Après mûre réflexion, vous pouvez déployer la règle apprise en tant que règle de relaxation du format de champ.

Amélioration de**l'apprentissage des formats de champs : une amélioration**de l'apprentissage du Web App Firewall a été introduite dans la version 11.0. Dans les versions précédentes, une fois que la recommandation de format de champ appris est déployée, le moteur d'apprentissage Web App Firewall arrête de surveiller les demandes valides dans le but de recommander de nouvelles règles sur la base des nouveaux points de données. Cela limite la protection de sécurité configurée, car la base de données d'apprentissage n'inclut aucune représentation des nouvelles données présentes dans les demandes valides traitées par le contrôle de sécurité.

Les violations ne sont plus associées à l'apprentissage. Le moteur d'apprentissage apprend et émet des recommandations concernant les formats de champs, quelles que soient les violations. En plus de vérifier les demandes bloquées pour déterminer si le format de champ actuel est trop restrictif et doit être assoupli, le moteur d'apprentissage surveille également les demandes autorisées pour déterminer si le format de champ actuel est trop permissif et permet d'améliorer la sécurité en déployant une règle plus restrictive.

Vous trouverez ci-dessous un résumé du comportement d'apprentissage des formats de champs :

Aucun format de champ n'est lié : le comportement reste inchangé dans ce scénario. Toutes les données d'apprentissage sont envoyées au moteur aslearn. Le moteur d'apprentissage suggère une règle de format de champ basée sur l'ensemble de données.

Le format du champ est limité : dans les versions précédentes, les données observées étaient envoyées au moteur aslearn uniquement en cas de violation. Le moteur d'apprentissage suggère une règle de format de champ basée sur l'ensemble de données. Dans la version 11.0, toutes les données sont envoyées au moteur aslearn même si aucune violation n'est déclenchée. Le moteur

d'apprentissage suggère une règle de format de champ basée sur l'ensemble de données de toutes les entrées reçues.

Cas d'utilisation pour l'amélioration de l'apprentissage :

Si les règles apprises pour le format de champ initial sont basées sur un petit échantillon de données, quelques valeurs non typiques peuvent donner lieu à une recommandation trop indulgente pour le champ cible. L'apprentissage continu permet au Web App Firewall d'observer les points de données de chaque demande afin de collecter un échantillon représentatif pour les recommandations apprises. Cela permet de renforcer encore la sécurité afin de déployer le format d'entrée optimal avec une valeur de plage adéquate.



L'apprentissage au format de champ utilise la priorité des types de champs ainsi que les paramètres configurés des seuils d'apprentissage suivants :

- **FieldFormatMinThreshold** : nombre minimum de fois qu'un champ de formulaire spécifique doit être observé avant qu'une relaxation apprise ne soit générée. Par défaut : 1.
- **FieldFormatPercentThreshold** : pourcentage de fois qu'un champ de formulaire correspond à un type de champ particulier, avant qu'une relaxation apprise ne soit générée. Par défaut : 0.

Les recommandations relatives aux règles de format des champs sont basées sur les critères suivants :

- **Recommandations relatives aux types**de champs : les recommandations relatives aux types de champs sont déterminées par les priorités attribuées aux types de champs existants et par les seuils de format de champ spécifiés. Les priorités déterminent l'ordre dans lequel les types de champs sont mis en correspondance avec les entrées. Un nombre inférieur indique une priorité plus élevée. Par exemple, le type de champ entier a la priorité la plus élevée (30) et est

donc évalué avant le type de champ alphanum (50). Les seuils déterminent le nombre d'entrées évaluées pour collecter un échantillon représentatif pour le point de données. Il est essentiel d'attribuer la bonne priorité aux types de champs configurés et de configurer une valeur de **paramètre d'apprentissage** appropriée pour les paramètres **FieldFormatPercentThreshold et FieldFormatMinThresholdpour obtenir la bonne recommandation de format de champ** . Le type de champ ayant la priorité la plus élevée, en fonction des seuils configurés, est mis en correspondance en premier avec les entrées. En cas de correspondance, ce type de champ est suggéré sans tenir compte des autres types de champs. Par exemple, trois types de champs par défaut (entier, alphanumérique, etc.) correspondront si toutes les entrées ne contiennent que des nombres. Toutefois, un entier sera recommandé car il a la priorité la plus élevée.

- **Recommandations relatives aux longueurs minimale et maximale** : les calculs des longueurs minimale et maximale pour le format de champ sont effectués indépendamment de la détermination du type de champ. Les calculs de longueur du format de champ sont basés sur la longueur moyenne de toutes les entrées observées. La moitié de cette moyenne calculée est suggérée comme valeur minimale, et le double de la valeur de cette moyenne est suggérée comme valeur maximale. La plage de longueur minimale est comprise entre 0 et 65 535 et la plage de longueur maximale est comprise entre 1 et 65 535. La valeur configurée pour la longueur minimale ne peut pas dépasser la longueur maximale.
- **Gestion des espaces** : la vérification du format de champ compte chaque caractère d'espace lors de la vérification de la longueur des formats de champ. Les espaces de début ou de fin ne sont pas supprimés, et les multiples espaces consécutifs au milieu de la chaîne d'entrée ne sont plus consolidés en un seul espace pendant le traitement des entrées.

Exemple illustrant les recommandations relatives au format des champs :

```
Total requests: 100
Number of Req with Field Type:
Int : 22            (22 int values)  -  22%
Alpha : 44                  (44 alpha values)  -  44%
Alphanum: 14            (14 + 44 + 22 = 80 alphanum values) = 80%
noHTML: 10              (80 + 10 = 90 noHTML values) = 90%
any : 10                     (90 + 10 = 100 any values) = 100%

% threshold                              Suggested Field Type
0-22                int
23-44               alpha
45-80               alphanum
81-90               noHTML
91-100              any
<!--NeedCopy-->
```

Pour afficher ou utiliser les données apprises à l'aide de l'interface de ligne de commande


```
show appfw learningdata <profilename> FieldFormat
rm appfw learningdata <profilename> -fieldFormat <string>  <
   formActionURL>
export appfw learningdata <profilename> FieldFormat
<!--NeedCopy-->
```

Pour afficher ou utiliser les données apprises à l'aide de l'interface graphique

1. Accédez à **Application Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles apprises**. Vous pouvez sélectionner l'entrée Formats de champ dans le tableau des règles apprises et double-cliquer dessus pour accéder aux règles apprises. Vous pouvez déployer les règles apprises ou modifier une règle avant de la déployer en tant que règle de relaxation. Pour annuler une règle, vous pouvez la sélectionner et cliquer sur le bouton **Ignorer** . Vous ne pouvez modifier qu'une règle à la fois, mais vous pouvez sélectionner plusieurs règles à déployer ou à ignorer.

   Vous pouvez également afficher une vue résumée des relaxations apprises en sélectionnant l'entrée Formats de champ dans le tableau des règles apprises et en cliquant sur Visualiseur pour obtenir une vue consolidée de toutes les violations apprises. Le visualiseur permet de gérer très facilement les règles apprises. Il présente une vue complète des données sur un seul écran et facilite la prise de mesures sur un groupe de règles en un seul clic. Le principal avantage du visualiseur est qu'il recommande des expressions régulières pour consolider plusieurs règles. Vous pouvez sélectionner un sous-ensemble de ces règles, en fonction du délimiteur et de l'URL d'action. Vous pouvez afficher 25, 50 ou 75 règles dans le visualiseur, en sélectionnant le nombre dans une liste déroulante. Le visualiseur des règles apprises offre la possibilité de modifier les règles et de les déployer sous forme d'assouplissements. Vous pouvez également ignorer les règles pour les ignorer.

Utilisation de la fonction de journalisation avec la vérification des formats de champs

Lorsque l'action du journal est activée, les violations du contrôle de sécurité des formats de champ sont enregistrées dans le journal d'audit en tant que violations APPFW_FIELDFORMAT. Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur Syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Passez au shell et suivez le fichier ns.logs dans le dossier /var/log/ pour accéder aux messages du journal relatifs aux violations des formats de champs :

- `Shell`
- `tail -f /var/log/ns.log | grep APPFW_FIELDFORMAT`

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique inclut un outil très utile (Syslog Viewer) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **Pare-feu des applications** > **Profils**, sélectionnez le profil cible, puis cliquez sur **Contrôles de sécurité**. Mettez en surbrillance la ligne Formats de champ et cliquez sur **Journaux**. Lorsque vous accédez aux journaux directement à partir du contrôle de **sécurité des formats de champ** du profil, il filtre les messages du journal et affiche uniquement les journaux relatifs à ces violations de contrôle de sécurité.
- ****Vous pouvez également accéder à la visionneuse Syslog en accédant à **NetScaler** > Système > Audit.**** Dans la section **Messages d'audit**, cliquez sur le lien **des messages Syslog** pour afficher le **visualiseur Syslog**, qui affiche tous les messages du journal, y compris les autres journaux de violations des contrôles de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de contrôle de sécurité peuvent être déclenchées pendant le traitement des demandes.
- Accédez à **Pare-feu des applications** > **Stratégies** > **Audit**. Dans la section **Messages d'audit**, cliquez sur le lien des messages Syslog pour afficher le visualiseur Syslog, qui affiche tous les messages du journal, y compris les autres journaux de violations des contrôles de sécurité.

  La visionneuse Syslog basée sur HTML fournit diverses options de filtre pour sélectionner uniquement les messages de journal qui vous intéressent. Pour accéder aux messages du journal des violations des contrôles de sécurité des formats de champs, filtrez en sélectionnant APPFW dans les options déroulantes du module. Le type d'événement affiche un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous cochez la case **APPFW_FIELDFORMAT** et que vous cliquez sur le bouton **Appliquer**, seuls les messages de journal relatifs aux violations du contrôle de sécurité des formats de champs apparaissent dans le visualiseur Syslog.

Si vous placez le curseur sur la ligne correspondant à un message de journal spécifique, plusieurs options, telles que Module et EventType, apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans les journaux.

Exemple de message de journal au format natif lorsque la demande n'est pas bloquée

```
1 Jun 10 22:32:26 <local0.info> 10.217.31.98 06/10/2015:22:32:26 GMT ns
     0-PPE-0 :
2 default APPFW APPFW_FIELDFORMAT 97 0 :  10.217.253.62 562-PPE0
3 x1MV+YnNGzQFM3Bsy2wti4bhXio0001 pr_ffc http://aaron.stratum8.net/FFC/
     login_post.php
4 Field format check failed for field passwd="65568888sz-*_" <not blocked
     >
```



```
Example of a CEF format log message when the request is blocked
Jun 11 00:03:51 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_FIELDFORMAT|6|src
   =10.217.253.62 spt=27076
method=POST requet=http://aaron.stratum8.net/FFC/maxlen_post.php msg=
   Field format check
failed for field text_area="" cn1=108 cn2=644 cs1=pr_ffc cs2=PPE0
cs3=GaUROfl1Nx1jJTvja5twH5BBqI0000 cs4=ALERT cs5=2015 act=blocked
<!--NeedCopy-->
```

Statistiques relatives aux violations des formats de champs

Lorsque l'action statistique est activée, le compteur correspondant à la vérification des formats de champs est incrémenté lorsque le Web App Firewall prend une action pour cette vérification de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. L'incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, la demande d'une page contenant 3 violations de format de champ incrémente le compteur de statistiques d'une unité, car la page est bloquée dès que la première violation de format de champ est détectée. Toutefois, si le blocage est désactivé, le traitement de la même demande augmente de 3 le compteur de statistiques pour les violations et les journaux, car chaque violation des formats de champs génère un message de journal distinct.

Pour afficher les statistiques relatives aux formats de champs à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
sh appfw stats
```

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
stat appfw profile <profile name>
```

Pour afficher les statistiques sur les formats de champs à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Pare-feu d'application**.
2. Dans le volet droit, accédez au lien Statistiques .
3. Utilisez la barre de défilement pour consulter les statistiques relatives aux violations des formats de champs et aux journaux. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Conseil de déploiement

- Activez le format des champs (journal des actions, apprentissage et statistiques).
- Après avoir exécuté un échantillon représentatif du trafic vers votre application, passez en revue les recommandations apprises.

- Si un type de champ est recommandé par la plupart des règles apprises, configurez ce type de champ comme type de champ par défaut. Pour les longueurs minimale et maximale, utilisez la plage la plus large suggérée par ces règles.
- Déployez des règles pour d'autres champs pour lesquels différents types de champs ou différentes longueurs minimales/maximales sont mieux adaptés.
- Activez le blocage et désactivez l'apprentissage.
- Surveillez les statistiques et les journaux. Si un nombre important de violations continuent d'être déclenchées, vous pouvez consulter les messages du journal pour confirmer qu'il s'agit de demandes malveillantes qui ont dû être bloquées. Si des demandes valides sont signalées comme des violations, vous pouvez soit modifier la règle de format de champ configurée pour l'assouplir davantage, soit réactiver l'apprentissage pour obtenir des recommandations basées sur les nouveaux points de données.

> **Remarque :** Vous pouvez affiner votre configuration en obtenant de nouvelles recommandations d'apprentissage.

Résumé

Prenez note des points suivants concernant le contrôle de sécurité du format de champ :

- **Protection** : en configurant des règles de format de champ optimales, vous pouvez vous protéger contre de nombreuses attaques. Par exemple, si vous spécifiez qu'un champ ne peut contenir que des nombres entiers, les pirates informatiques ne pourront pas lancer d'attaques par injection SQL ou par script intersite à l'aide de ce champ, car les entrées requises pour lancer de telles attaques ne répondront pas aux exigences de format de champ configurées.
- **Performances** : vous pouvez limiter la longueur minimale et maximale autorisée pour les entrées dans les règles de format des champs. Cela peut empêcher un utilisateur malveillant de saisir des chaînes d'entrée trop volumineuses dans le but d'alourdir le traitement du serveur ou, pire encore, d'amener le serveur à vider le noyau en raison d'un débordement de pile. En limitant la taille des entrées, vous pouvez réduire le temps nécessaire au traitement des demandes légitimes.
- **Configuration des formats de champs** : vous devez activer l'une des actions (bloquer, enregistrer, statistiques, apprendre) pour activer la protection des formats de champ. Vous pouvez également spécifier les règles de format des champs pour identifier les entrées autorisées dans les champs de votre formulaire.
- **Sélection de cartes de personnages vs. Types de champs** : les cartes de caractères et les types de champs utilisent des expressions régulières. Cependant, une carte de caractères fournit une expression plus spécifique en limitant la liste des caractères autorisés. Par exemple, pour une entrée telle que janedoe@citrix.com, le moteur d'apprentissage peut recommander le type de champ nohtml mais la table de caractères [. @-za-Z] pourrait être plus précis, car cela réduit le nombre de caractères non alphabétiques autorisés. L'option Character Map permet,

en plus des caractères alpha, seulement deux caractères non alpha : point (.) et at (@).

- **Apprentissage continu** : le Web App Firewall surveille et prend en compte toutes les données entrantes (violations et entrées autorisées) afin de créer un tableau d'apprentissage permettant de recommander des règles. Les règles sont révisées et mises à jour à mesure que de nouvelles données entrantes arrivent. De nouvelles règles de format de champ sont suggérées pour un champ même s'il possède déjà une règle de format de champ liée. Si les formats de champ configurés sont trop restrictifs et bloquent les demandes valides, vous pouvez déployer un format de champ plus souple. De même, si les formats de champ actuels sont trop génériques, vous pouvez affiner et renforcer la sécurité en déployant un format de champ plus restrictif.
- **Remplacement des règles** : si une règle a déjà été déployée pour une combinaison champ/URL, l'interface utilisateur permet à l'utilisateur de mettre à jour le format du champ. Une boîte de dialogue vous demande de confirmer le remplacement de la règle existante. Si vous utilisez l'interface de ligne de commande, vous devez dissocier explicitement la liaison précédente, puis lier la nouvelle règle.
- **Correspondance multiple** : si plusieurs formats de champ correspondent à un nom de champ donné et à son URL d'action, le Web App Firewall sélectionne arbitrairement l'un d'entre eux à appliquer.
- **Limite de la zone tampon** : si la valeur d'un champ s'étend sur plusieurs zones tampons de diffusion et que le format de ces deux parties de la valeur du champ est différent, un format de champ correspondant à « n'importe quel » est envoyé à la base de données d'apprentissage.
- **Format de champ par rapport à Contrôle de cohérence des champs** : le contrôle du format des champs et le contrôle de cohérence des champs sont des contrôles de protection basés sur des formulaires. La vérification des formats de champs fournit un type de protection différent de celui du contrôle de cohérence des champs de formulaire. Le contrôle de cohérence des champs de formulaire vérifie que la structure des formulaires Web renvoyés par les utilisateurs est intacte, que les restrictions de format de données configurées dans le code HTML sont respectées et que les données des champs masqués n'ont pas été modifiées. Il peut le faire sans aucune connaissance spécifique de vos formulaires Web autre que ce qu'il déduit du formulaire Web lui-même. La vérification des formats de champs vérifie que les données de chaque champ de formulaire correspondent aux restrictions de mise en forme spécifiques que vous avez configurées manuellement ou que la fonctionnalité d'apprentissage a été générée et que vous avez approuvée. En d'autres termes, la vérification de cohérence des champs de formulaire applique la sécurité générale des formulaires Web, tandis que la vérification Formats de champ applique les règles spécifiques pour les entrées autorisées pour vos formulaires Web.

Contrôle de cohérence des champs de formulaire

August 20, 2021

La vérification de cohérence des champs de formulaire examine les formulaires Web renvoyés par les utilisateurs de votre site Web et vérifie que les formulaires Web n'ont pas été modifiés de façon inappropriée par le client. Cette vérification s'applique uniquement aux demandes HTML qui contiennent un formulaire Web, avec ou sans données. Il ne s'applique pas aux requêtes XML.

La vérification de cohérence des champs de formulaire empêche les clients d'apporter des modifications non autorisées à la structure des formulaires Web de votre site Web lorsqu'ils remplissent et soumettent un formulaire. Il garantit également que les données soumises par un utilisateur respectent les restrictions HTML pour la longueur et le type, et que les données des champs masqués ne sont pas modifiées. Cela empêche un attaquant de falsifier un formulaire Web et d'utiliser le formulaire modifié pour obtenir un accès non autorisé au site Web, rediriger la sortie d'un formulaire de contact qui utilise un script non sécurisé et envoyant ainsi des courriels non sollicités en masse, ou d'exploiter une vulnérabilité dans votre logiciel de serveur Web pour prendre le contrôle du Web ou le système d'exploitation sous-jacent. Les formulaires Web constituent un maillon faible sur de nombreux sites Web et attirent un large éventail d'attaques.

La vérification de cohérence des champs de formulaire vérifie tous les éléments suivants :

- Si un champ est envoyé à l'utilisateur, la vérification garantit qu'il est renvoyé par l'utilisateur.
- La vérification applique les longueurs et les types de champs HTML.

  > **Remarque :**
  >
  > – La vérification de cohérence des champs de formulaire applique des restrictions HTML sur le type et la longueur des données, mais ne valide pas autrement les données dans les formulaires Web. Vous pouvez utiliser la vérification Formats de champ pour configurer des règles qui valident les données renvoyées dans des champs de formulaire spécifiques de vos formulaires Web.
  >
  > – La protection de cohérence des champs de formulaire insère un champ masqué « as_fid » dans les formulaires de réponse envoyés au client. Le même champ masqué sera effacé par ADC lorsque le client soumet le formulaire. S'il y a un javascript côté client effectuant un calcul de somme de contrôle sur les champs du formulaire et la vérification de la même somme de contrôle sur le backend peut provoquer une rupture de l'application. Dans ce scénario, Il est recommandé de détendre le champ caché de la cohérence du champ de pare-feu d'application champ caché « as_fid » à partir du calcul de somme de contrôle javascript côté client.

- Si votre serveur Web n'envoie pas de champ à l'utilisateur, la vérification ne permet pas à l'utilisateur d'ajouter ce champ et d'y retourner des données.
- Si un champ est en lecture seule ou masqué, la vérification vérifie que les données n'ont pas changé.
- Si un champ est une zone de liste ou un champ de bouton radio, la vérification vérifie que les

données de la réponse correspondent à l'une des valeurs de ce champ.

Si un formulaire Web renvoyé par un utilisateur viole un ou plusieurs contrôles de cohérence du champ de formulaire et que vous n'avez pas configuré le pare-feu de l'application Web pour autoriser ce formulaire Web à enfreindre les contrôles de cohérence du champ de formulaire, la demande est bloquée.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier le contrôle de cohérence des champs de formulaire, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journaliser, Apprendre et Statistiques.

Vous configurez également la cohérence des champs sans session dans l'onglet Général. Si Cohérence des champs sans session est activée, le Web App Firewall vérifie uniquement la structure du formulaire Web, en supprimant les parties de la vérification de cohérence des champs de formulaire qui dépendent de la tenue à jour des informations de session. Cela peut accélérer la vérification de la cohérence des champs de formulaire avec peu de pénalité de sécurité pour les sites Web qui utilisent de nombreux formulaires. Pour utiliser la cohérence des champs sans session sur tous les formulaires Web, sélectionnez Activer. Pour l'utiliser uniquement pour les formulaires soumis avec la méthode HTTP POST, sélectionnez PostOnly

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer le contrôle de cohérence des champs de formulaire :

- `set appfw profile <name> -fieldConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]`

Pour spécifier des relaxations pour la vérification de cohérence des champs de formulaire, vous devez utiliser l'interface graphique. Sous l'onglet Vérifications de la boîte de dialogue Modifier le contrôle de cohérence des champs de formulaire, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter une relaxation du contrôle de cohérence des champs de formulaire ou sélectionnez une relaxation existante et cliquez sur Ouvrir pour ouvrir la boîte de dialogue Modifier la relaxation du contrôle de cohérence des champs de formulaire. L'une ou l'autre des boîtes de dialogue offre les mêmes options de configuration d'une relaxation, comme décrit dans Configuration manuelle à l'aide de l'interface graphique.

Voici des exemples d'assouplissements de vérification de cohérence des champs de formulaire :

Noms des champs de formulaire :

- Choisissez les champs de formulaire avec le nom UserType :

```
1 ^UserType$
2 <!--NeedCopy-->
```

- Choisissez des champs de formulaire dont les noms commencent par UserType_ et sont suivis d'une chaîne qui commence par une lettre ou un chiffre et se compose de une à vingt et un

lettres, des chiffres ou de l'apostrophe ou du trait d'union :

```
^UserType_[0-9A-Za-z][0-9A-Za-z'-]{
0,20 }
$
<!--NeedCopy-->
```

- Choisissez des champs de formulaire avec des noms commençant par Turkish-userType_ et qui sont autrement les mêmes que l'expression précédente, sauf qu'ils peuvent contenir des caractères spéciaux turcs dans l'ensemble :

```
^T\xC3\xBCrk\xC3\xA7e-UserType_([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa
   -f])+$
<!--NeedCopy-->
```

> **Remarque :**
>
> Voir Format de codage de caractères PCRE pour une description complète des caractères spéciaux pris en charge et comment les encoder correctement.

- Choisissez des noms de champs de formulaire qui commencent par une lettre ou un chiffre, qui sont constitués d'une combinaison de lettres et/ou de chiffres uniquement et qui contiennent la chaîne Num n'importe où dans la chaîne :

```
^[0-9A-Za-z]\*Num[0-9A-Za-z]\*$
<!--NeedCopy-->
```

URL d'action du champ de formulaire :

- Choisissez les URL commençant par`http://www.example.com/search.pl?` et contenant une chaîne après la requête, à l'exception d'une nouvelle requête :

```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Choisissez les URL commençant par `http://www.example-español.com` et dont les chemins d'accès et les noms de fichiers sont constitués de majuscules et minuscules, de chiffres, de caractères spéciaux non ASCII et de symboles sélectionnés dans le chemin d'accès. Le caractère ñ et tous les autres caractères spéciaux sont représentés sous la forme de chaînes UTF-8 codées contenant le code hexadécimal attribué à chaque caractère spécial dans le jeu de caractères UTF-8 :

```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-
   Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9
   A-Fa-f][0-9A-Fa-f])
```



```
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)
   $
<!--NeedCopy-->
```

- Choisissez toutes les URL qui contiennent la chaîne /search.cgi?:

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

> **Attention :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'elles définissent exactement l'URL que vous voulez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne voulez pas ou attendez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification de la cohérence des cookies aurait autrement bloqué.

Vérification du balisage des formulaires CSRF

May 5, 2023

La vérification de balisage de formulaire CSRF (Falsification de requête inter-site) balise chaque formulaire Web envoyé par un site Web protégé aux utilisateurs avec un FormID unique et imprévisible, puis examine les formulaires Web renvoyés par les utilisateurs pour s'assurer que le formulaire fourni est correct. Cette vérification protège contre les attaques par falsification de requêtes intersites. Cette vérification s'applique uniquement aux requêtes HTML qui contiennent un formulaire Web, avec ou sans données. Elle ne s'applique pas aux requêtes XML.

Le contrôle du balisage des formulaires CSRF empêche les attaquants d'utiliser leurs propres formulaires Web pour envoyer un volume élevé de réponses contenant des données à vos sites Web protégés. Cette vérification nécessite relativement peu de capacité de traitement du processeur par rapport à certains autres contrôles de sécurité qui analysent en profondeur les formulaires Web. Il est donc capable de gérer des attaques de volume élevé sans sérieusement dégrader les performances du site Web protégé ou du Web App Firewall lui-même.

Avant d'activer la vérification du balisage des formulaires CSRF, vous devez prendre en compte les points suivants :

- Vous devez activer le balisage des formulaires. La vérification CSRF dépend du balisage des formulaires et ne fonctionne pas sans celui-ci.
- Vous devez désactiver la fonctionnalité de mise en cache intégrée de NetScaler pour toutes les pages Web contenant des formulaires protégés par ce profil. La fonctionnalité de mise en cache intégrée et le balisage des formulaires CSRF ne sont pas compatibles.
- Vous devez envisager d'activer la vérification des référents. La vérification des référents fait partie de la vérification de l'URL de démarrage, mais elle empêche la falsification des requêtes intersites, et non les violations de l'URL de démarrage. La vérification des référents sollicite également moins le processeur que la vérification du balisage des formulaires CSRF. Si une demande enfreint la vérification des référents, elle est immédiatement bloquée, de sorte que le contrôle du balisage des formulaires CSRF n'est pas invoqué.
- La vérification du balisage des formulaires CSRF ne fonctionne pas avec les formulaires Web qui utilisent des domaines différents dans l'URL d'origine du formulaire et l'URL d'action du formulaire. Par exemple, le balisage de formulaire CSRF ne peut pas protéger un formulaire Web dont l'URL d'origine du formulaire `http://www.example.com` et l'URL d'action du formulaire est `http://www.example.org/form`.pl, car exemple.com et example.org sont des domaines différents.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification du balisage des formulaires CSRF, sous l'onglet Général, vous pouvez activer ou désactiver les actions Block, Log, Learn et Statistics.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer le CSRF Form Tagging Check :

- `set appfw profile <name> -CSRFtagAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Pour spécifier des relaxations pour la vérification du balisage des formulaires CSRF, vous devez utiliser l'interface graphique. Dans l'onglet Contrôles de la boîte de dialogue Modifier la vérification du balisage des formulaires CSRF, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter une relaxation du balisage des formulaires CSRF, ou sélectionnez une relaxation existante et cliquez sur Ouvrir pour ouvrir la boîte de dialogue Modifier la relaxation des contrôles de balisage des formulaires CSRF. L'une ou l'autre des boîtes de dialogue fournit les mêmes options pour configurer une relaxation.

Une alerte est générée lorsque vous définissez la limite de session de NetScaler Web App Firewall sur une valeur inférieure ou égale à 0, car ce paramètre affecte la fonctionnalité de contrôle de protection avancée qui nécessite le bon fonctionnement de la session Web App Firewall.

Vous trouverez ci-dessous des exemples d'assouplissements liés au contrôle du balisage des formulaires CSRF :

Remarque : Les expressions suivantes sont des expressions URL qui peuvent être utilisées à la fois dans les rôles URL d'origine du formulaire et URL d'action du formulaire.

- Choisissez les URL commençant par `http://www.example.com/search.pl?` et contenant n'importe quelle chaîne après la requête, à l'exception d'une nouvelle requête :

```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Choisissez des URL commençant par et dont les chemins `http://www.example-español.com` et les noms de fichiers sont composés de lettres majuscules et minuscules, de chiffres, de caractères spéciaux non ASCII et de symboles sélectionnés dans le chemin. Le caractère ñ et tous les autres caractères spéciaux sont représentés sous forme de chaînes UTF-8 codées contenant le code hexadécimal attribué à chaque caractère spécial du jeu de caractères UTF-8 :

```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Choisissez toutes les URL contenant la chaîne /search.cgi ? :

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

Important

Les expressions régulières sont puissantes. Si vous n'êtes pas parfaitement familiarisé avec les expressions régulières au format PCRE, revérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne voulez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification aurait autrement bloquée.

Conseil

Lorsque l'en-tête de référence enableValidate est activé sous l'action d'URL de démarrage, assurez-vous que l'URL d'en-tête de référence est également ajoutée à StartURL.

Remarque

Lorsque NetScaler atteint le seuil appfw_session_limit et que les contrôles CSRF sont activés, l'application Web se bloque.

Pour empêcher le blocage des applications Web, réduisez le délai d'expiration de la session et

> augmentez la limite de session à l'aide des commandes suivantes :
>
> Depuis l'interface de ligne de commande : > définir les paramètres appfw —sessiontimeout 300 Depuis le shell : root @ns # nsapimgr_wr.sh -s appfw_session_limit=200000
>
> La journalisation et la génération d'alarmes SNMP lorsque appfw_session_limit est atteinte vous aident à résoudre les problèmes et à déboguer.

Gestion des assouplissements liés au balisage des formulaires CSRF

May 5, 2023

Vous configurez une exception (ou une relaxation) à la vérification de sécurité du balisage des formulaires CSRF dans la boîte de dialogue Ajouter un balisage des demandes intersites pour falsification ou dans la boîte de dialogue Modifier les demandes intersites pour falsifier le balisage des faux sites ou dans la boîte de dialogue Modifier la relaxation des demandes intersites.

Pour configurer le balisage d'un formulaire CSRF, vérifiez la relaxation à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet **Profils**, sélectionnez le profil que vous souhaitez configurer, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le profil du Web App Firewall**, cliquez sur l'onglet **Vérifications de sécurité** . L'onglet **Contrôles de sécurité** contient la liste des contrôles de sécurité du Web App Firewall.
4. Pour ajouter ou modifier une relaxation CSRF, effectuez l'une des opérations suivantes :
   - Pour ajouter une nouvelle relaxation, cliquez sur Ajouter.
   - Pour modifier une relaxation existante, sélectionnez la relaxation que vous souhaitez modifier, puis cliquez sur **Ouvrir**.

   La boîte de **dialogue Ajouter un balisage multisite Request Forgery Check Relaxation** ou **Modifier une demande intersite Forgery Tagging Check** Relaxation s'affiche. À l'exception du titre, ces boîtes de dialogue sont identiques.
5. Remplissez la boîte de dialogue comme décrit ci-dessous.
   - Case à**cocher activée : cochez**cette case pour activer cette relaxation ou cette règle ; désactivez-la pour la désactiver.
   - **URL d'origine du formulaire** : dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL qui héberge le formulaire.

- **URL de l'action du formulaire** : dans la zone de texte, entrez une expression régulière au format PCRE qui définit l'URL vers laquelle les données saisies dans le formulaire sont envoyées.
- **Commentaires**—Dans la zone de texte, tapez un commentaire. Facultatif.

> **Remarque :**
>
> Pour tout élément nécessitant une expression régulière, vous pouvez saisir l'expression régulière, utiliser le menu **Regex Tokens** pour insérer des éléments d'expression régulière et des symboles directement dans la zone de texte, ou cliquer sur **Regex Editor** pour ouvrir la boîte de dialogue **Ajouter une expression régulière** et l'utiliser pour créer l'expression.

6. Cliquez sur **OK**. La boîte de dialogue **Ajouter le balisage des demandes intersites, vérifier la relaxation** ou **modifier le balisage des demandes intersites, vérifier la relaxation se ferme et vous revenez à la boîte de dialogue Modifier la vérification du balisagedes demandes intersites** .
7. Pour supprimer une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Supprimer**.
8. Pour activer une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Activer**.
9. Pour désactiver une relaxation ou une règle, sélectionnez-la, puis cliquez sur **Désactiver**.
10. Pour configurer les paramètres et les relations de toutes les relaxations existantes dans un affichage graphique interactif intégré, cliquez sur **Visualizer**et utilisez les outils d'affichage.
11. Pour vérifier et configurer les règles apprises pour la vérification CSRF, cliquez sur **Apprentissage** et effectuez les étapes de la section Pour configurer et utiliser la fonctionnalité d'apprentissage.
12. Cliquez sur **OK**.

Vérifications de la protection des URL

January 21, 2021

Les contrôles de protection des URL examinent les URL de requête pour empêcher les pirates de tenter agressivement d'accéder à plusieurs URL (navigation forcée) ou d'utiliser une URL pour déclencher une vulnérabilité de sécurité connue dans les logiciels de serveur Web ou les scripts de site Web.

Démarrer la vérification de l'URL

August 20, 2021

La vérification de l'URL de démarrage examine les URL dans les demandes entrantes et bloque la tentative de connexion si l'URL ne répond pas aux critères spécifiés. Pour répondre aux critères, l'URL doit correspondre à une entrée de la liste URL de démarrage, sauf si le paramètre Imposer la fermeture de l'URL est activé. Si vous activez ce paramètre, un utilisateur qui clique sur un lien sur votre site Web est connecté à la cible de ce lien.

Le but principal de la vérification de l'URL de démarrage est d'empêcher les tentatives répétées d'accès aux URL aléatoires sur un site Web (navigation forcée) par le biais de signets, de liens externes, ou de sauter vers des pages en saisissant manuellement les URL pour ignorer les pages requises pour accéder à cette partie du site Web. Une navigation forcée peut être utilisée pour déclencher un dépassement de tampon, trouver du contenu auquel les utilisateurs n'étaient pas censés accéder directement, ou trouver une porte dérobée dans les zones sécurisées de votre serveur Web. Le Web App Firewall applique la traversée ou le chemin logique donné d'un site Web en autorisant uniquement l'accès aux URL configurées en tant qu'URL de démarrage.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification de l'URL de démarrage, sous l'onglet Général, vous pouvez activer ou désactiver Bloquer, Journal, Statistiques, Actions d'apprentissage et les paramètres suivants :

- **Imposer la fermeture de l'URL.** Permettez aux utilisateurs d'accéder à n'importe quelle page web de votre site Web en cliquant sur un lien hypertexte sur n'importe quelle autre page de votre site Web. Les utilisateurs peuvent accéder à n'importe quelle page de votre site Web accessible à partir de la page d'accueil ou de toute page de démarrage désignée en cliquant sur des hyperliens.
  Remarque : La fonction de fermeture d'URL permet à toute chaîne de requête d'être ajoutée et envoyée avec l'URL d'action d'un formulaire Web soumis à l'aide de la méthode HTTP GET. Si vos sites Web protégés utilisent des formulaires pour accéder à une base de données SQL, assurez-vous que la vérification d'injection SQL est activée et correctement configurée.
- **Fermeture d'URL sans session.** Du point de vue du client, ce type de fermeture d'URL fonctionne exactement de la même manière que la fermeture d'URL standard, sensible à la session, mais utilise un jeton intégré dans l'URL au lieu d'un cookie pour suivre l'activité de l'utilisateur, ce qui consomme beaucoup moins de ressources. Lorsque la fermeture d'URL sans session est activée, le Web App Firewall ajoute une balise « as_url_id » à toutes les URL qui sont en fermeture d'URL.
  Remarque : Lorsque vous activez la fermeture d'URL sans session (Fermeture d'URL sans session), vous devez également activer la fermeture d'URL régulière (
  Forcer la fermeture d'URL) ou la fermeture d'URL sans session ne fonctionne pas.
- **Valider l'en-tête du référent.** Vérifiez que l'en-tête Referer dans une demande contenant des données de formulaire Web provenant de votre site Web protégé au lieu d'un autre site Web. Cette action vérifie que votre site Web, et non un attaquant extérieur, est la source du formulaire Web. Cela protège contre les falsifications de requêtes inter-sites (CSRF) sans nécessiter le balisage de formulaire, ce qui nécessite plus de CPU que les vérifications d'en-tête. Le Web App

Firewall peut gérer l'en-tête HTTP Referer de l'une des quatre manières suivantes, selon l'option sélectionnée dans la liste déroulante :

- **Off**—Ne pas valider l'en-tête Referer.
- **If-Present**—Valide l'en-tête Referer si un en-tête Referer existe. Si un en-tête Referer non valide est trouvé, la demande génère une violation d'en-tête référent-référent. Si aucun en-tête Referer n'existe, la demande ne génère pas de violation d'en-tête référent-référent. Cette option permet au Web App Firewall d'effectuer la validation de l'en-tête Referer sur les demandes qui contiennent un en-tête Referer, mais ne bloque pas les demandes des utilisateurs dont le navigateur ne définit pas l'en-tête Referer ou qui utilisent des proxy Web ou des filtres qui suppriment cet en-tête.
- **URL Always Except Start** : validez toujours l'en-tête Referer. S'il n'y a pas d'en-tête Referer et que l'URL demandée n'est pas exemptée par la règle de relaxation StarTURL, la demande génère une violation d'en-tête référent-référent. Si l'en-tête Referer est présent mais qu'il n'est pas valide, la requête génère une violation d'en-tête référent-référent.
- **Always Except First Request**—Validez toujours l'en-tête du référent. S'il n'y a pas d'en-tête référent, seule l'URL qui est accédé en premier est autorisée. Toutes les autres URL sont bloquées sans en-tête référent valide. Si l'en-tête Referer est présent mais qu'il n'est pas valide, la requête génère une violation d'en-tête référent-référent.

Un paramètre d'URL de démarrage, **Exempter les URL de fermeture des vérifications de sécurité**, n'est pas configuré dans la boîte de dialogue Modifier la vérification d'URL de démarrage, mais est configuré dans l'onglet Paramètres du profil. Si cette option est activée, ce paramètre indique au Web App Firewall de ne pas exécuter d'autres vérifications basées sur le formulaire (telles que le script inter-site et l'inspection SQL Injection) sur les URL qui répondent aux critères de fermeture d'URL.

> **Remarque**
>
> Bien que la vérification de l'en-tête du référent et la vérification de sécurité de l'URL de démarrage partagent les mêmes paramètres d'action, il est possible de violer la vérification de l'en-tête du référent sans violer la vérification de l'URL de démarrage. La différence est visible dans les journaux, qui les violations de vérification de l'en-tête du référent de journal séparément des violations de vérification de l'URL de démarrage.

Les paramètres d'en-tête Referer (OFF, IF-Present, AlwaysExceptStartURLs et AlwaysExceptFirstRequest) sont organisés dans l'ordre le moins restrictif à le plus restrictif et fonctionnent comme suit :

OFF :

- En-tête du référent non coché.

If-Present :

- La requête n'a pas d'en-tête référent -> La requête est autorisée.
- La requête a l'en-tête du référent et l'URL du référent est dans la fermeture de l'URL -> La requête est autorisée.

- La requête a l'en-tête du référent et l'URL du référent **n'est pas** dans la fermeture de l'URL -> La requête est bloquée.

AlwaysExceptStartURLs :

- La requête n'a pas d'en-tête référent et l'URL de la requête est une URL de démarrage -> La requête est autorisée.
- La demande n'a pas d'en-tête référent et l'URL de la demande n'est pas une URL de démarrage ->La demande est bloquée.
- La requête a l'en-tête du référent et l'URL du référent est dans la fermeture de l'URL -> La requête est autorisée.
- La requête a l'en-tête du référent et l'URL du référent **n'est pas** dans la fermeture de l'URL -> La requête est bloquée.

AlwaysExceptFirstRequest :

- Request n'a pas d'en-tête référent et est la première URL de requête de la session -> Request is allowed.
- La requête n'a pas d'en-tête référent et **n'est pas** la première URL de requête de la session -> La requête est bloquée.
- Request a l'en-tête référent et est soit la première URL de requête de la session, soit est en fermeture d'URL -> Request is allowed.
- La requête a l'en-tête référent et n'est ni la première URL de requête de la session ni est en fermeture d'URL -> La requête est bloquée.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer les commandes suivantes pour configurer la vérification de l'URL de démarrage :

- `set appfw profile <name> -startURLAction [block] [learn] [log] [stats] [none]`
- `set appfw profile <name> -startURLClosure ([ON] | [OFF])`
- `set appfw profile <name> -sessionlessURLClosure ([ON] | [OFF])`
- `set appfw profile <name> -exemptClosureURLsFromSecurityChecks ([ON] | [OFF)`
- `set appfw profile <name> -RefererHeaderCheck ([OFF] | [if-present] | [AlwaysExceptStartURLs] | [AlwaysExceptFirstRequest])`

Pour spécifier des relaxations pour la vérification de l'URL de démarrage, vous devez utiliser l'interface graphique. Sous l'onglet Vérifications de la boîte de dialogue Modifier la vérification de l'URL de début, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter la relaxation de la vérification de l'URL de début ou sélectionnez une relaxation existante et cliquez sur Ouvrir pour ouvrir la boîte de dialogue Modifier la relaxation de la vérification de l'URL de début. L'une ou l'autre des boîtes de dialogue fournit les mêmes options pour configurer une relaxation.

Voici des exemples de relaxations de vérification de l'URL de démarrage :

- Autoriser les utilisateurs à accéder à la page d'accueil à l'adresse www.example.com :

```
^http://www[.]example[.]com$
<!--NeedCopy-->
```

- Autoriser les utilisateurs à accéder à toutes les pages Web au format HTML statique (.htm et .html), HTML analysé par serveur (.htp et .shtml), PHP (.php) et Microsoft ASP (.asp) à l'adresse www.example.com :

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Autoriser les utilisateurs à accéder aux pages Web avec des noms de chemin d'accès ou des noms de fichiers contenant des caractères non ASCII sur www.example-español.com :

```
^http://www[.]example-espaxC3xB1ol[.]com/(([0-9A-Za-z]|x[0-9A-Fa-
   f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*
([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f
   ][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

Remarque : Dans l'expression ci-dessus, chaque classe de caractères a été regroupée avec la chaîne
x[0-9a-fa-F][0-9A-Fa-f], qui correspond à toutes les chaînes de codage de caractères correctement construites, mais n'autorise pas les barres obliques inverse errantes qui ne sont pas associées à une chaîne de codage de caractères UTF-8. La double barre oblique inverse () est une barre oblique inverse échappée, qui indique au Web App Firewall de l'interpréter comme une barre oblique inverse littérale. Si vous n'incluez qu'une barre oblique inverse, le Web App Firewall interpréterait à la place le crochet gauche suivant ([) comme un caractère littéral au lieu de l'ouverture d'une classe de caractères, ce qui romprait l'expression.

- Autoriser les utilisateurs à accéder à tous les graphiques au format GIF (.png), JPEG (.jpg et .jpeg) et PNG (.png) à l'adresse www.example.com :

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](gif|jpe?g|png)$
<!--NeedCopy-->
```

- Autoriser les utilisateurs à accéder aux scripts CGI (.cgi) et PERL (.pl), mais uniquement dans le répertoire CGI-BIN :

```
^http://www[.]example[.]com/CGI-BIN/[0-9A-Za-z][0-9A-Za-z_
   .-]*[.](cgi|pl)$
```



```
<!--NeedCopy-->
```

- Autoriser les utilisateurs à accéder à Microsoft Office et à d'autres fichiers de documents dans le répertoire docsarchive :

```
^http://www[.]example[.]com/docsarchive/[0-9A-Za-z][0-9A-Za-z_
   -.]*[.](doc|xls|pdf|ppt)$
<!--NeedCopy-->
```

> **Remarque**
>
> Par défaut, toutes les URL du Web App Firewall sont considérées comme des expressions régulières.

Attention : Les expressions régulières sont puissantes. Surtout si vous n'êtes pas familier avec les expressions régulières au format PCRE, vérifiez les expressions régulières que vous écrivez. Assurez-vous qu'elles définissent exactement l'URL que vous voulez ajouter en tant qu'exception, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (
.*), peut avoir des résultats que vous ne voulez pas, comme bloquer l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou autoriser une attaque que la vérification de l'URL de démarrage aurait autrement bloquée.

> **Conseil**
>
> Vous pouvez ajouter le *-and-* à la liste autorisée de mots-clés SQL pour le schéma d'attribution de noms d'URL. Par exemple, https://FQDN/bread-and-butter.

Refuser la vérification de l'URL

May 5, 2023

La vérification Refuser l'URL examine et bloque les connexions aux URL fréquemment consultées par les pirates informatiques et les codes malveillants. Cette vérification contient une liste d'URL qui sont des cibles courantes de pirates informatiques ou de code malveillant et qui apparaissent rarement, voire jamais, dans les requêtes légitimes. Vous pouvez également ajouter des URL ou des modèles d'URL à la liste. Le contrôle Refuser l'URL empêche les attaques visant diverses failles de sécurité connues dans les logiciels de serveur Web ou sur de nombreux sites Web.

La vérification Refuser l'URL a la priorité sur la vérification de l'URL de départ et refuse ainsi les tentatives de connexion malveillantes, même lorsqu'un assouplissement de l'URL de départ autoriserait normalement le traitement d'une demande.

Dans la boîte de dialogue Modifier la vérification de l'URL refusée, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Consigner et Statistiques.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification Refuser l'URL :

```
set appfw profile <name> -denyURLAction [\*\*block\*\*] [\*\*log\*\*]
    [\*\*stats\*\*] [\*\*none\*\*]
<!--NeedCopy-->
```

Vous pouvez créer et configurer vos propres URL de refus uniquement dans l'interface graphique de NetScaler.

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Sélectionnez un profil pour lequel vous souhaitez ajouter une URL de refus et cliquez sur **Modifier**.
3. Sur la page de **profil du Web App Firewall NetScaler**, sélectionnez **Règles de relaxation** dans la section **Paramètres avancés.**
4. Sélectionnez **Refuser l'URL** et cliquez sur **Modifier**.



5. Sur la page **Règles de refus d'URL**, cliquez sur **Ajouter**.
6. Spécifiez les informations suivantes et cliquez sur **Créer**.
   - **Refuser l'URL** : expression régulière permettant de définir une URL de refus.
   - **Commentaires** : description de l'expression.
   - **ID de ressource** : identifiant unique permettant d'identifier la règle de refus d'URL.



7. Cliquez sur **Fermer**.
8. **Sur la page de**profil du pare-feu NetScaler Web App**, cliquez sur OK.**

Vous trouverez ci-dessous des exemples d'expressions d'URL de refus :

- N'autorisez pas les utilisateurs à accéder directement au serveur d'images sur images.example.com :

```
^http://images[.]example[.]com$
<!--NeedCopy-->
```

- N'autorisez pas les utilisateurs à accéder directement aux scripts CGI (.cgi) ou PERL (.pl) :

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](cgi|pl)$
<!--NeedCopy-->
```

- Voici la même URL de refus, modifiée pour prendre en charge les caractères non ASCII :

```
^http://www[.]example[.]com/(([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f
   ])
([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|x[0-9A-
   Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])*[.](cgi|pl)$
<!--NeedCopy-->
```


> **Attention :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL ou le modèle que vous souhaitez bloquer, et rien d'autre. L'utilisation négligente des caractères génériques, et en particulier de la combinaison de métacaractères/caractères génériques (.*), peut avoir des résultats que vous ne voulez pas, tels que le blocage de l'accès au contenu Web que vous n'aviez pas l'intention de bloquer.

Vérifications de protection XML

January 21, 2021

Les contrôles XML Protection examinent les demandes d'attaques basées sur XML de tous types.

> **Attention :**
>
> Les vérifications de sécurité XML s'appliquent uniquement au contenu envoyé avec un en-tête de type de contenu HTTP text/xml. Si l'en-tête de type de contenu est manquant ou est défini sur une valeur différente, toutes les vérifications de sécurité XML sont contournées. Si vous envisagez de protéger les applications Web XML ou Web 2.0, les webmasters de chaque serveur Web hébergeant ces applications doivent s'assurer que l'en-tête de type de contenu HTTP approprié est envoyé.

Vérification du format XML

January 21, 2021

La vérification Format XML examine le format XML des demandes entrantes et bloque les demandes qui ne sont pas bien formées ou qui ne répondent pas aux critères de la spécification XML pour les documents XML correctement formés. Certains de ces critères sont les suivants :

- Un document XML doit contenir uniquement des caractères Unicode codés correctement qui correspondent à la spécification Unicode.
- Aucun caractère de syntaxe XML spécial, tel que <, > et &, ne peut être inclus dans le document, sauf lorsqu'il est utilisé dans le balisage XML.
- Toutes les balises de début, de fin et d'élément vide doivent être imbriquées correctement, sans qu'il soit manquant ou superposé.
- Les balises d'éléments XML sont sensibles à la casse. Toutes les balises de début et de fin doivent correspondre exactement.

- Un seul élément racine doit contenir tous les autres éléments du document XML.

Un document qui ne répond pas aux critères d'un XML bien formé ne répond pas à la définition d'un document XML. Strictement parlant, ce n'est pas XML. Cependant, toutes les applications XML et les services Web n'appliquent pas la norme XML bien formée, et tous ne gèrent pas correctement les XML mal formés ou non valides. Une manipulation inappropriée d'un document XML mal formé peut entraîner des failles de sécurité. Le but de la vérification du format XML est d'empêcher un utilisateur malveillant d'utiliser une requête XML mal formée pour enfreindre la sécurité de votre application XML ou service Web.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification du format XML, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journal et Statistiques.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification du format XML :

- `set appfw profile <name> -xmlFormatAction [**block**] [**log**] [**stats**] [**none**]`

Vous ne pouvez pas configurer les exceptions à la vérification Format XML. Vous ne pouvez l'activer ou le désactiver que.

Vérification par déni de service XML

August 20, 2021

La vérification du déni de service XML (XML DoS ou XDoS) examine les demandes XML entrantes pour déterminer si elles correspondent aux caractéristiques d'une attaque par déni de service (DoS). S'il y a une correspondance, bloque ces requêtes. Le but de la vérification XML DoS est d'empêcher un attaquant d'utiliser des requêtes XML pour lancer une attaque par déni de service sur votre serveur Web ou site Web.

Si vous utilisez l'Assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification du déni de service XML, sous l'onglet **Général**, vous pouvez activer ou désactiver les actions Bloquer, Journal, Statistiques et Learn :

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification de déni de service XML :

- `set appfw profile <name> -xmlDoSAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Pour configurer des règles de déni de service XML individuelles, vous devez utiliser l'interface graphique. Sous l'onglet **Vérifications** de la boîte de dialogue **Modifier la vérification du déni de**

service XML, sélectionnez une règle et cliquez sur **Ouvrir** pour ouvrir la boîte de dialogue **Modifier le déni de service XML** pour cette règle. Les boîtes de dialogue individuelles diffèrent selon les règles mais sont simples. Certains vous permettent uniquement d'activer ou de désactiver la règle ; d'autres vous permettent de modifier un nombre en tapant une nouvelle valeur dans une zone de texte.

> **Remarque :**
>
> Le comportement attendu du moteur d'apprentissage pour les attaques par déni de service est basé sur l'action configurée. Si l'action est définie comme « Bloquer », le moteur apprend la valeur de liaison configurée +1 et l'analyse XML s'arrête en cas de violation. Si l'action configurée n'est pas définie comme « Bloquer », le moteur apprend la valeur réelle de longueur de violation entrante.

Les règles de déni de service XML individuelles sont les suivantes :

- Profondeur maximale de l'élément. Limitez le nombre maximal de niveaux imbriqués dans chaque élément individuel à 256. Si cette règle est activée et que le Web App Firewall détecte une demande XML avec un élément dont le nombre maximal de niveaux autorisés est supérieur au nombre maximal, il bloque la demande. Vous pouvez modifier le nombre maximal de niveaux à n'importe quelle valeur de un (1) à 65 535.
- Longueur maximale du nom de l'élément. Limitez la longueur maximale de chaque nom d'élément à 128 caractères. Cela inclut le nom dans l'espace de noms développé, qui inclut le chemin d'accès XML et le nom de l'élément dans le format suivant :

```
{
http://prefix.example.com/path/ }
target_page.xml
<!--NeedCopy-->
```

L'utilisateur peut modifier la longueur maximale du nom à n'importe quelle valeur comprise entre un (1) caractère et 65 535.

- Nombre maximum d'éléments. Limitez le nombre maximal d'un type d'élément par document XML à 65 535. Vous pouvez modifier le nombre maximal d'éléments à n'importe quelle valeur comprise entre un (1) et 65 535.
- Nombre maximum d'enfants d'élément. Limitez le nombre maximal d'enfants (y compris les autres éléments, les informations de caractère et les commentaires) que chaque élément individuel est autorisé à avoir à 65 535. Vous pouvez modifier le nombre maximal d'enfants d'élément à n'importe quelle valeur comprise entre un (1) et 65 535.
- Nombre maximum d'attributs. Restreindre le nombre maximal d'attributs que chaque élément individuel est autorisé à avoir à 256. Vous pouvez modifier le nombre maximal d'attributs à n'importe quelle valeur comprise entre un (1) et 256.

- Longueur maximale du nom d'attribut. Limitez la longueur maximale de chaque nom d'attribut à 128 caractères. Vous pouvez modifier la longueur maximale du nom d'attribut à n'importe quelle valeur comprise entre un (1) et 2,048.
- Longueur maximale de la valeur d'attribut. Limitez la longueur maximale de chaque valeur d'attribut à 2048 caractères. Vous pouvez modifier la longueur maximale du nom d'attribut à n'importe quelle valeur comprise entre un (1) et 2,048.
- Longueur maximale des données de caractère. Limitez la longueur maximale des données de caractères pour chaque élément à 65 535. Vous pouvez modifier la longueur à n'importe quelle valeur comprise entre un (1) et 65 535.
- Taille maximale du fichier. Limitez la taille de chaque fichier à 20 Mo. Vous pouvez modifier la taille maximale du fichier à n'importe quelle valeur.
- Taille minimale du fichier. Exiger que chaque fichier ait une longueur minimale de 9 octets. Vous pouvez modifier la taille minimale du fichier à n'importe quel entier positif représentant différents octets.
- Nombre maximal d'extensions d'entités. Limitez le nombre d'extensions d'entités autorisées au nombre spécifié. Par défaut : 1024.
- Profondeur maximale d'extension de l'entité. Limitez le nombre maximal d'expansions d'entités imbriquées au nombre spécifié. Par défaut : 32.
- Nombre maximum d'espaces de noms. Limitez le nombre de déclarations d'espace de noms dans un document XML au maximum au nombre spécifié. Par défaut : 16.
- Longueur maximale de l'URI d'espace de noms. Limitez la longueur d'URL de chaque déclaration d'espace de noms au maximum le nombre de caractères spécifié. Par défaut : 256.
- Instructions de traitement des blocs. Bloquer toutes les instructions spéciales de traitement incluses dans la demande. Cette règle ne comporte aucune valeur modifiable par l'utilisateur.
- Bloquer la DTD. Bloquer toutes les définitions de type de document (DTD) incluses dans la demande. Cette règle ne comporte aucune valeur modifiable par l'utilisateur.
- Bloquer les entités externes. Bloquer toutes les références aux entités externes dans la demande. Cette règle ne comporte aucune valeur modifiable par l'utilisateur.
- Vérification de la baie SOAP. Activez ou désactivez les vérifications de tableau SOAP suivantes :
  - **Taille maximale du tableau SOAP.** Taille totale maximale de toutes les baies SOAP dans une requête XML avant que la connexion ne soit bloquée. Vous pouvez modifier cette valeur. Par défaut : 20000000.
  - **Rang maximum du tableau SOAP.** Rang ou dimensions maximum d'un tableau SOAP unique dans une requête XML avant que la connexion ne soit bloquée. Vous pouvez modifier cette valeur. Par défaut : 16.

Vérification des scripts XML intersites

May 5, 2023

Le contrôle XML Cross-Site Scripting examine les demandes des utilisateurs pour détecter d'éventuelles attaques par script intersite dans la charge utile XML. S'il détecte une éventuelle attaque par script intersite, il bloque la requête.

Pour empêcher toute utilisation abusive des scripts de vos services Web protégés dans le but d'enfreindre la sécurité de vos services Web, le contrôle XML Cross-Site Scripting bloque les scripts qui enfreignent la même règle d'origine, selon laquelle les scripts ne doivent pas accéder au contenu ni le modifier sur un serveur autre que celui sur lequel ils se trouvent. Tout script qui enfreint la même règle d'origine est appelé script intersite, et la pratique consistant à utiliser des scripts pour accéder ou modifier du contenu sur un autre serveur est appelée script intersite. La raison pour laquelle les scripts intersites constituent un problème de sécurité est qu'un serveur Web qui autorise le script intersite peut être attaqué à l'aide d'un script qui ne se trouve pas sur ce serveur Web, mais sur un autre serveur Web, tel qu'un serveur détenu et contrôlé par l'attaquant.

Le Web App Firewall propose diverses options d'action pour mettre en œuvre la protection par script intersite XML. Vous avez la possibilité de configurer les actions de **blocage**, de **journalisation**et de **statistiques** .

Le contrôle des scripts intersites XML du Web App Firewall est effectué sur la charge utile des demandes entrantes et les chaînes d'attaque sont identifiées même si elles sont réparties sur plusieurs lignes. La vérification recherche les chaînes d'attaque par script intersites dans les valeurs de l' **élément** et des **attributs** . Vous pouvez appliquer des assouplissements pour contourner les contrôles de sécurité dans des conditions spécifiques. Les journaux et les statistiques peuvent vous aider à identifier les relaxations nécessaires.

La section CDATA de la charge utile XML peut être un domaine d'intérêt intéressant pour les pirates car les scripts ne sont pas exécutables en dehors de la section CDATA. Une section CDATA est utilisée pour le contenu qui doit être traité entièrement comme des données de caractères. Les délimiteurs de balises HTML **<**, **>** **et**/** n'obligeront pas l'analyseur à interpréter le code comme des éléments HTML. L'exemple suivant montre une section CDATA avec une chaîne d'attaque par script intersite :

```
1     <![CDATA[rn
2     <script language="Javascript" type="text/javascript">alert ("Got
         you")</script>rn
3     ]]>
4 <!--NeedCopy-->
```


Options d'action

Une action est appliquée lorsque la vérification du script intersite XML détecte une attaque de script intersite dans la demande. Les options suivantes sont disponibles pour optimiser la protection des scripts intersites XML pour votre application :

- **Bloquer** : l'action de blocage est déclenchée si les balises de script intersites sont détectées dans la demande.
- **Journal** : génère des messages de journal indiquant les actions entreprises par le contrôle XML Cross-Site Scripting. Si le blocage est désactivé, un message de journal distinct est généré pour chaque emplacement (ELEMENT, ATTRIBUTE) dans lequel la violation de script intersite est détectée. Toutefois, un seul message est généré lorsque la demande est bloquée. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.
- **Statistiques** : collectez des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si des demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer de nouvelles règles de relaxation ou modifier celles existantes.

Règles de relaxation

Si votre application exige que vous contourniez la vérification du cross-site scripting pour un ÉLÉMENT ou UN ATTRIBUT spécifique dans la charge utile XML, vous pouvez configurer une règle de relaxation. Les règles de relaxation du contrôle des scripts intersites XML comportent les paramètres suivants :

- **Nom**—Vous pouvez utiliser des chaînes littérales ou des expressions régulières pour configurer le nom de l'ÉLÉMENT ou de l'attribut. L'expression suivante exempte tous les ÉLÉMENTS commençant par la chaîne name_ suivie d'une chaîne de lettres majuscules ou minuscules, ou de chiffres, d'au moins deux et pas plus de quinze caractères :

```
^name_[0-9A-Za-z]{ 2,15 } $
```

> **Remarque**
>
> Les noms sont sensibles à la casse. Les doublons ne sont pas autorisés, mais vous pouvez utiliser la majuscule des noms et les différences d'emplacement pour créer des entrées similaires. Par exemple, chacune des règles de relaxation suivantes est unique :
>
> 1. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`
> 2. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`

3. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`
4. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`

- **Emplacement**—Vous pouvez spécifier l'emplacement de l'exception Cross-site Scripting Check dans votre charge utile XML. L'option ELEMENT est sélectionnée par défaut. Vous pouvez le remplacer par ATTRIBUTE.
- **Commentaire** : il s'agit d'un champ facultatif. Vous pouvez utiliser une chaîne de 255 caractères maximum pour décrire l'objectif de cette règle de relaxation.

> **Avertissement**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement le nom que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation imprudente d'expressions régulières peut avoir des conséquences indésirables, par exemple en bloquant l'accès à du contenu Web que vous n'aviez pas l'intention de bloquer ou en autorisant une attaque que le contrôle des scripts intersites XML aurait autrement bloquée.

Utilisation de la ligne de commande pour configurer la vérification des scripts intersites XML

Pour configurer les scripts intersites XML, vérifiez les actions et d'autres paramètres à l'aide de la ligne de commande

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer les commandes suivantes pour configurer le XML Cross-Site Scripting Check :

```
> set appfw profile <name> -XMLcross-site scriptingAction (([block] [log] [
stats])| [none])
```

Pour configurer un script intersite XML, vérifiez la règle de relaxation à l'aide de la ligne de commande

Vous pouvez ajouter des règles de relaxation pour contourner l'inspection des attaques par script intersites à un emplacement spécifique. Utilisez la commande bind ou unbind pour ajouter ou supprimer la liaison à la règle de relaxation, comme suit :

```
> bind appfw profile <name> -XMLcross-site scripting <string> [isRegex (
REGEX | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )] -comment <string> [-
state ( ENABLED | DISABLED )]
```

```
> unbind appfw profile <name> -XMLcross-site scripting <String>
```

Exemple :


```
> bind appfw profile test_pr -XMLcross-site scripting ABC
```

Après avoir exécuté la commande ci-dessus, la règle de relaxation suivante est configurée. La règle est activée, le nom est traité comme un nom littéral (NOTREGEX) et ELEMENT est sélectionné comme emplacement par défaut :

```
1)      XMLcross-site scripting:  ABC             IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

`> unbind appfw profile test_pr -XMLcross-site scripting abc`

ERROR: No such XMLcross-site scripting check

`> unbind appfw profile test_pr -XMLcross-site scripting ABC`

 Done
<!--NeedCopy-->
```

Utilisation de l'interface graphique pour configurer la vérification des scripts intersites XML

Dans l'interface graphique, vous pouvez configurer la vérification des scripts intersites XML dans le volet correspondant au profil associé à votre application.

Pour configurer ou modifier le script intersite XML, procédez à une vérification à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet Paramètres avancés, cliquez sur **Contrôles de sécurité**.

Le tableau de contrôle de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Deux options de configuration s'offrent à vous :

a) Si vous souhaitez simplement activer ou désactiver les actions de **blocage**, de **journalisation**et de **statistiques** pour la **vérification des scripts intersites XML**, vous pouvez activer ou désactiver les cases à cocher dans le tableau, cliquer sur **OK**, puis sur Enregistrer et fermer pour fermer le volet de contrôle de sécurité.

b) Vous pouvez double-cliquer sur **XML Cross-Site Scripting**ou sélectionner la ligne et cliquer sur **Paramètres d'action**pour afficher les options d'action. Après avoir modifié l'un des paramètres d'action, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau des contrôles de sécurité.

Vous pouvez procéder à la configuration d'autres contrôles de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur **Enregistrer et fermer** pour fermer le volet Contrôle de sécurité.

Pour configurer une règle de relaxation relative aux scripts intersites XML à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
3. **Dans le tableau Règles de relaxation, double-cliquez sur l'entrée**XML Cross-Site Scripting**ou sélectionnez-la et cliquez sur Modifier.**
4. **Dans la boîte de dialogue**Règles de relaxation des scripts intersites XML**, effectuez des opérations d'**ajout**, de**modification**, de**suppression**, d'**activation ou de désactivation**pour les règles de relaxation.**

Pour gérer les règles de relaxation relatives aux scripts intersites XML à l'aide du visualiseur

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez surligner la ligneXML Cross-Site Scripting**dans le tableau des règles de relaxation, puis cliquer sur Visualiseur.** Le visualiseur pour les relaxations déployées vous offre la possibilité d' **ajouter** une nouvelle règle ou de **modifier** une règle existante. Vous pouvez également **activer** ou **désactiver** un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Pour afficher ou personnaliser les modèles de script intersite à l'aide de l'interface graphique

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser la liste par défaut des attributs autorisés ou des balises autorisées pour les scripts intersites. Vous pouvez également afficher ou personnaliser la liste par défaut des modèles refusés par script intersite.

Les listes par défaut sont spécifiées dans **Web App Firewall** > **Signatures > Signaturespar défaut**. Si vous ne liez aucun objet de signature à votre profil, la liste par défaut des scripts intersites autorisés et refusés spécifiée dans l'objet Signatures par défaut sera utilisée par le profil pour le traitement du contrôle de sécurité des scripts intersites. Les balises, les attributs et les modèles, spécifiés dans l'objet signatures par défaut, sont en lecture seule. Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez les modifier ou les modifier, faites une copie de l'objet Signatures par défaut pour créer un objet signature défini par l'utilisateur. Modifiez les listes autorisées ou refusées du nouvel objet de signature défini par l'utilisateur et utilisez cet objet de signature dans le profil qui traite le trafic pour lequel vous souhaitez utiliser ces listes personnalisées d'autorisations et de refus.

Pour plus d'informations sur les signatures, consultez http://support.citrix.com/proddocs/topic/ns-security-10-map/appfw-signatures-con.html.

Pour afficher les modèles de script intersite par défaut :

1. Accédez à **Web App Firewall** > **Signatures**, sélectionnez ***Signatures par défaut**, puis cliquez sur **Modifier**. Cliquez ensuite sur **Gérer les modèles de script SQL/intersite**.

Le tableau **Manage SQL/Cross-Site Scripting Paths contient** les trois lignes suivantes relatives aux scripts intersites :

```
1             xss/allowed/attribute
2
3             xss/allowed/tag
4
5             xss/denied/pattern
6 <!--NeedCopy-->
```

Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les éléments de script intersite correspondants (balise, attribut, modèle) utilisés par la vérification du script **intersite** du Web App Firewall.

Pour personnaliser les éléments de script intersites : vous pouvez modifier l'objet de signature défini par l'utilisateur pour personnaliser la balise autorisée, les attributs autorisés et les modèles refusés. Vous pouvez ajouter de nouvelles entrées ou supprimer celles qui existent déjà.

1. **Accédez à Web App Firewall** > **Signatures**, sélectionnez la signature cible définie par l'utilisateur, puis cliquez sur **Modifier**. Cliquez sur **Gérer les modèles de script SQL/intersite** pour afficher le tableau **Gérer les chemins de script SQL/intersite** .
2. Sélectionnez la ligne de script intersite cible.

a) Cliquez sur **Gérer les éléments**pour **ajouter**, **modifier** ou **supprimer** l'élément de script intersite correspondant.

b) Cliquez sur **Supprimer** pour supprimer la ligne sélectionnée.

> **Avertissement**
>
> Soyez très prudent lorsque vous supprimez ou modifiez un élément de script intersite par défaut, ou supprimez le chemin de script intersite pour supprimer la ligne entière. Les signatures, le contrôle de sécurité des scripts intersites HTML et le contrôle de sécurité des scripts intersites XML s'appuient sur ces éléments pour détecter les attaques afin de protéger vos applications. Personnalisation des scripts intersites Les éléments peuvent rendre votre application vulnérable aux attaques de script intersite si le modèle requis est supprimé pendant la modification.

Utilisation de la fonction de journalisation avec la vérification des scripts intersites XML

Lorsque l'action de journalisation est activée, les violations du contrôle de sécurité des scripts intersites XML sont enregistrées dans le journal d'audit en tant que violations de script **AppFW_XML_Cross-**

site . Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur Syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Passez au shell et suivez le fichier ns.logs dans le dossier /var/log/ pour accéder aux messages de journal relatifs aux violations des scripts intersites XML :

```
> \*\*Shell\*\*

> \*\*tail -f /var/log/ns.log | grep APPFW_XML_cross-site scripting\*\*
<!--NeedCopy-->
```

Exemple de message de journal des violations du contrôle de sécurité XML Cross-Site Scripting au format de journal natif indiquant une action <blocked>

```
Oct  7 01:44:34 <local0.warn> 10.217.31.98 10/07/2015:01:44:34 GMT ns
    0-PPE-1 : default APPFW APPFW_XML_cross-site scripting 1154 0 :
    10.217.253.69 3466-PPE1 - owa_profile http://10.217.31.101/FFC/login
    .html Cross-site script check failed for field script="Bad tag:
    script" <\*\*blocked\*\*>
<!--NeedCopy-->
```

Exemple de message de journal des violations du contrôle de sécurité XML Cross-Site Scripting au format journal CEF indiquant une action <not blocked>

```
Oct  7 01:46:52 <local0.warn> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|APPFW_XML_cross-site scripting|4|src=10.217.30.17
    geolocation=Unknown spt=33141 method=GET request=http://
    10.217.31.101/FFC/login.html msg=Cross-site script check failed for
    field script="Bad tag: script" cn1=1607 cn2=3538 cs1=owa_profile cs2
    =PPE0 cs4=ERROR cs5=2015 act=\*\*not blocked\*\*
<!--NeedCopy-->
```

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique inclut un outil utile (**Syslog Viewer**) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez au **Web App Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Security Checks**. **Sélectionnez la ligne**XML Cross-Site Scripting**et cliquez sur Journaux.** Lorsque vous accédez aux journaux directement à partir de la vérification du profil par script intersite XML, l'interface utilisateur filtre les messages du journal et affiche uniquement les journaux relatifs à ces violations de contrôle de sécurité.
- ****Vous pouvez également accéder à la visionneuse Syslog en accédant à **NetScaler** > Système > Audit.** Dans la section Messages d'audit, cliquez sur le lien Messages Syslog pour af-

ficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation de vérification de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de contrôle de sécurité peuvent être déclenchées pendant le traitement des demandes.

- Accédez à **Web App Firewall** > **stratégies** > **Audit**. Dans la section **Messages d'audit**, cliquez sur le lien **des messages Syslog** pour afficher le visualiseur Syslog, qui affiche tous les messages du journal, y compris les autres journaux de violations des contrôles de sécurité.

Le visualiseur Syslog basé sur XML fournit diverses options de filtrage pour sélectionner uniquement les messages du journal qui vous intéressent. **Pour sélectionner les messages du journal pour la vérification du**script intersite XML**, filtrez en sélectionnant**APPFW**dans les options déroulantes du module.** La liste **Type d'événement** offre un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous cochez la case **AppFW_XML_Cross-Site Scripting** et que vous cliquez sur le bouton **Appliquer**, seuls les messages de journal relatifs aux violations du contrôle de sécurité du script intersite XML apparaissent dans le visualiseur Syslog.

Si vous placez le curseur sur la ligne d'un message de journal spécifique, plusieurs options, telles que **Module**, **Type d'événement, ID**d'événement,**IP du client**, etc. apparaissent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

Statistiques relatives aux violations des scripts intersites XML

Lorsque l'action statistique est activée, le compteur du contrôle des scripts intersites XML est incrémenté lorsque le Web App Firewall prend une action pour ce contrôle de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, une demande concernant une page contenant trois violations de script intersite XML incrémente le compteur de statistiques d'une unité, car la page est bloquée dès que la première violation est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente le compteur de statistiques pour les violations et les journaux de trois, car chaque violation génère un message de journal distinct.

Pour afficher les statistiques du cross-site Scripting XML, vérifiez les statistiques à l'aide de la ligne de commande.

À l'invite de commande, tapez :

```
> **sh appfw stats**
```

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> **stat appfw profile** <profile name>
```

Pour afficher les statistiques du cross-site Scripting XML à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Web App Firewall**.
2. Dans le volet droit, accédez au lien **Statistiques** .
3. Utilisez la barre de défilement pour consulter les statistiques relatives aux violations et aux journaux relatifs aux scripts intersites XML. Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Vérification de l'injection XML SQL

May 5, 2023

Le contrôle d'injection XML SQL examine les demandes des utilisateurs pour détecter d'éventuelles attaques par injection SQL XML. S'il trouve du code SQL injecté dans des charges utiles XML, il bloque les requêtes.

Une attaque SQL XML peut injecter du code source dans une application Web afin qu'il puisse être interprété et exécuté comme une requête SQL valide pour effectuer une opération de base de données avec une intention malveillante. Par exemple, des attaques XML SQL peuvent être lancées pour obtenir un accès non autorisé au contenu d'une base de données ou pour manipuler les données stockées. Les attaques par injection SQL XML sont non seulement courantes, mais elles peuvent également être très dangereuses et coûteuses.

La compartimentation des privilèges des utilisateurs de la base de données peut contribuer à protéger la base de données dans une certaine mesure. Tous les utilisateurs de base de données doivent disposer uniquement des privilèges nécessaires pour effectuer les tâches prévues, afin qu'ils ne puissent pas exécuter de requêtes SQL pour effectuer d'autres tâches. Par exemple, un utilisateur en lecture seule ne doit pas être autorisé à écrire ou à manipuler des tables de données. Le contrôle d'injection SQL XML du Web App Firewall inspecte toutes les requêtes XML afin de fournir des défenses spéciales contre l'injection de code SQL non autorisé susceptible de porter atteinte à la sécurité. Si le Web App Firewall détecte du code SQL non autorisé dans une requête XML d'un utilisateur, il peut bloquer la demande.

Le NetScaler Web App Firewall inspecte la présence de mots clés SQL et de caractères spéciaux afin d'identifier l'attaque par injection SQL XML. Un ensemble de mots-clés et de caractères spéciaux par défaut fournit des mots-clés connus et des caractères spéciaux couramment utilisés pour lancer des attaques XML SQL. Le Web App Firewall considère trois caractères, le guillemet droit simple (‘), la barre oblique inverse () et le point-virgule (;) comme des caractères spéciaux pour le traitement des contrôles de sécurité SQL. Vous pouvez ajouter de nouveaux modèles et modifier le paramètre par défaut pour personnaliser l'inspection de vérification XML SQL.

Le Web App Firewall propose diverses options d'action pour mettre en œuvre la protection contre les injections SQL XML. Vous pouvez **bloquer** la demande, **enregistrer** un message dans le fichier

ns.log avec des détails concernant les violations observées et collecter des **statistiques** pour suivre le nombre d'attaques observées.

Outre les actions, plusieurs paramètres peuvent être configurés pour le traitement par injection XML SQL. Vous pouvez vérifier la présence de **caractères génériques SQL**. Vous pouvez modifier le type d'injection SQL XML et sélectionner l'une des 4 options (**SQLKeyword, SQLSplChar, SQLSplCharAndKeyword, SQLSplCharOrKeyword) pour indiquer comment évaluer les mots-clésSQL et les caractères spéciaux SQL lors du traitement**de la charge utile XML. Le paramètre **Gestion des commentaires XML SQL** vous permet de spécifier le type de commentaires qui doivent être inspectés ou exemptés lors de la détection d'une injection XML SQL.

Vous pouvez déployer des relaxations pour éviter les faux positifs. La vérification SQL XML du Web App Firewall est effectuée sur la charge utile des demandes entrantes, et les chaînes d'attaque sont identifiées même si elles sont réparties sur plusieurs lignes. La vérification recherche les chaînes d'injection SQL dans l' **élément** et les valeurs **d'attribut** . Vous pouvez appliquer des assouplissements pour contourner les contrôles de sécurité dans des conditions spécifiques. Les journaux et les statistiques peuvent vous aider à identifier les relaxations nécessaires.

Options d'action

Une action est appliquée lorsque le contrôle de l'injection SQL XML détecte une chaîne d'attaque par injection SQL dans la demande. Les actions suivantes sont disponibles pour configurer une protection optimisée contre les injections SQL XML pour votre application :

Bloquer—Si vous activez le blocage, l'action de blocage est déclenchée uniquement si l'entrée correspond à la spécification du type d'injection XML SQL. Par exemple, si **SQLSplCharAndKeyword** est configuré comme type d'injection SQL XML, une requête n'est pas bloquée si elle ne contient aucun mot clé, même si des caractères spéciaux SQL sont détectés dans la charge utile. **Une telle demande est bloquée si le type d'injection SQL XML est défini sur**SQLSplChar ou SQLSplCharOrKeyword**.**

Journal : si vous activez la fonctionnalité de journalisation, le contrôle d'injection SQL XML génère des messages de journal indiquant les actions entreprises. Si le blocage est désactivé, un message de journal distinct est généré pour chaque emplacement (**ELEMENT**, **ATTRIBUTE**) dans lequel la violation du code SQL XML a été détectée. Toutefois, un seul message est généré lorsque la demande est bloquée. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.

Stats : si elle est activée, la fonctionnalité de statistiques collecte des statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si des demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer de nouvelles règles de relaxation ou modifier celles existantes.

Paramètres SQL XML

Outre les actions de blocage, de journalisation et de statistiques, vous pouvez configurer les paramètres suivants pour la vérification de l'injection XML SQL :

Vérifiez la présence de caractères génériques XML SQL : les caractèresgénériques peuvent être utilisés pour élargir les sélections d'une instruction en langage de requête structuré (SQL-SELECT). Ces opérateurs génériques peuvent être utilisés conjointement avec les opérateurs **LIKE** et **NOT LIKE** pour comparer une valeur à des valeurs similaires. Le pourcentage (%) et le trait de soulignement (_) sont fréquemment utilisés comme caractères génériques. Le signe pour cent est analogue au caractère générique astérisque (*) utilisé avec MS-DOS et pour faire correspondre zéro, un ou plusieurs caractères dans un champ. Le trait de soulignement est similaire au point d'interrogation MS-DOS (?) caractère générique. Il correspond à un seul nombre ou caractère dans une expression.

Par exemple, vous pouvez utiliser la requête suivante pour effectuer une recherche de chaîne afin de rechercher tous les clients dont le nom contient le caractère D.

```
SELECT * from customer WHERE name like "%D%"
```

L'exemple suivant combine les opérateurs pour rechercher toutes les valeurs salariales dont le deuxième et le troisième caractère sont 0.

```
SELECT * from customer WHERE salary like '_00%
```

Différents fournisseurs de SGBD ont étendu les caractères génériques en ajoutant des opérateurs supplémentaires. Le pare-feu NetScaler Web App peut protéger contre les attaques lancées en injectant ces caractères génériques. Les 5 caractères génériques par défaut sont le pourcentage (%), le trait de soulignement (_), le caret (^), le crochet ouvrant ([) et le crochet fermant (]). Cette protection s'applique aux profils HTML et XML.

Les caractères génériques par défaut sont une liste de littéraux spécifiés dans ***Signatures par défaut** :

```
1 -  <wildchar type=" LITERAL" >%</wildchar>
2 -  <wildchar type=" LITERAL" >_</wildchar>
3 -  <wildchar type=" LITERAL" >^</wildchar>
4 -  <wildchar type=" LITERAL" >[</wildchar>
5 -  <wildchar type=" LITERAL" >]</wildchar>
6 <!--NeedCopy-->
```

Les caractères génériques d'une attaque peuvent être PCRE, comme [^A-F]. Le Web App Firewall prend également en charge les caractères génériques PCRE, mais les caractères génériques littéraux ci-dessus sont suffisants pour bloquer la plupart des attaques.

> **Remarque**
>
> La vérification des **caractères génériques** XML SQL est différente de la vérification des **caractères spéciaux** XML SQL. Cette option doit être utilisée avec précaution afin d'éviter les faux positifs.

Demande de vérification contenant le type d'injection SQL : le Web App Firewall propose 4 options pour mettre en œuvre le niveau de rigueur souhaité pour l'inspection par injection SQL, en fonction des besoins individuels de l'application. La demande est vérifiée par rapport à la spécification du type d'injection pour détecter les violations SQL. Les 4 options de type d'injection SQL sont les suivantes :

- **Caractère spécial et mot clé**SQL : un mot clé SQL et un caractère spécial SQL doivent tous deux être présents à l'emplacement inspecté pour déclencher une violation SQL. Ce paramètre le moins restrictif est également le paramètre par défaut.
- **Caractère spécial SQL** : au moins l'un des caractères spéciaux doit être présent dans la chaîne de charge utile traitée pour déclencher une violation SQL.
- **Mot-clé SQL**—Au moins l'un des mots-clés SQL spécifiés doit être présent dans la chaîne de charge utile traitée pour déclencher une violation SQL. Ne sélectionnez pas cette option sans avoir dûment pris en considération. Pour éviter les faux positifs, assurez-vous qu'aucun des mots-clés n'est attendu dans les entrées.
- **Caractère spécial ou mot clé SQL** : le mot clé ou la chaîne de caractères spéciaux doit être présent dans la charge utile pour déclencher la violation du contrôle de sécurité.

> **Conseil**
>
> Si vous sélectionnez l'option Caractère spécial SQL, le Web App Firewall ignore les chaînes qui ne contiennent aucun caractère spécial. Étant donné que la plupart des serveurs SQL ne traitent pas les commandes SQL qui ne sont pas précédées d'un caractère spécial, l'activation de cette option peut réduire considérablement la charge sur le Web App Firewall et accélérer le traitement sans mettre en danger vos sites Web protégés.

Gestion des commentaires SQL : par défaut, le Web App Firewall analyse et vérifie tous les commentaires contenus dans les données XML pour détecter les commandes SQL injectées. De nombreux serveurs SQL ignorent tout contenu dans un commentaire, même s'il est précédé d'un caractère spécial SQL. Pour accélérer le traitement, si votre serveur SQL XML ignore les commentaires, vous pouvez configurer le Web App Firewall pour ignorer les commentaires lors de l'examen des demandes de SQL injecté. Les options de gestion des commentaires XML SQL sont les suivantes :

- **ANSI**—Ignorez les commentaires SQL au format ANSI, qui sont normalement utilisés par les bases de données SQL basées sur UNIX.
- **Imbriqué**—Ignorer les commentaires SQL imbriqués, qui sont normalement utilisés par Microsoft SQL Server.
- **ANSI/imbriqué**—Ignorer les commentaires qui respectent les normes ANSI et SQL de commentaires imbriqués. Les commentaires qui correspondent uniquement à la norme ANSI, ou unique-

ment à la norme imbriquée, sont toujours vérifiés pour détecter le code SQL injecté.

- **Vérifiez tous les commentaires** : vérifiez l'intégralité de la demande de SQL injecté, sans rien ignorer. C'est le réglage par défaut.

> **Conseil**
>
> Dans la plupart des cas, vous ne devez pas choisir l'option Nested ou ANSI/Nested sauf si votre base de données principale s'exécute sur Microsoft SQL Server. La plupart des autres types de logiciels SQL Server ne reconnaissent pas les commentaires imbriqués. Si des commentaires imbriqués apparaissent dans une demande dirigée vers un autre type de serveur SQL, ils peuvent indiquer une tentative de violation de la sécurité sur ce serveur.

Règles de relaxation

Si votre application exige que vous contourniez l'inspection par injection SQL XML pour un ÉLÉMENT ou UN ATTRIBUT spécifique dans la charge utile XML, vous pouvez configurer une règle de relaxation. Les règles de relaxation relatives à l'inspection par injection SQL XML comportent les paramètres suivants :

- **Nom :** Vous pouvez utiliser des chaînes littérales ou des expressions régulières pour configurer le nom de l' **ÉLÉMENT** ou de l' **ATTRIBUT**. L'expression suivante exempte tous les **ÉLÉMENTS** commençant par la chaîne **PurchaseOrder_** suivie d'une chaîne de chiffres d'au moins deux et d'au plus dix caractères :

  Commentaire : « Vérification SQL XML exemptée pour les éléments du bon de commande »

```
    XMLSQLInjection:  "PurchaseOrder_[0-9A-Za-z]{
 2,10 }
 "

    IsRegex:  REGEX          Location:  ELEMENT

    State:  ENABLED
<!--NeedCopy-->
```

Remarque : Les noms font la distinction entre majuscules et minuscules. Les doublons ne sont pas autorisés, mais vous pouvez utiliser la majuscule des noms et les différences d'emplacement pour créer des entrées similaires. Par exemple, chacune des règles de relaxation suivantes est unique :

```
1)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX

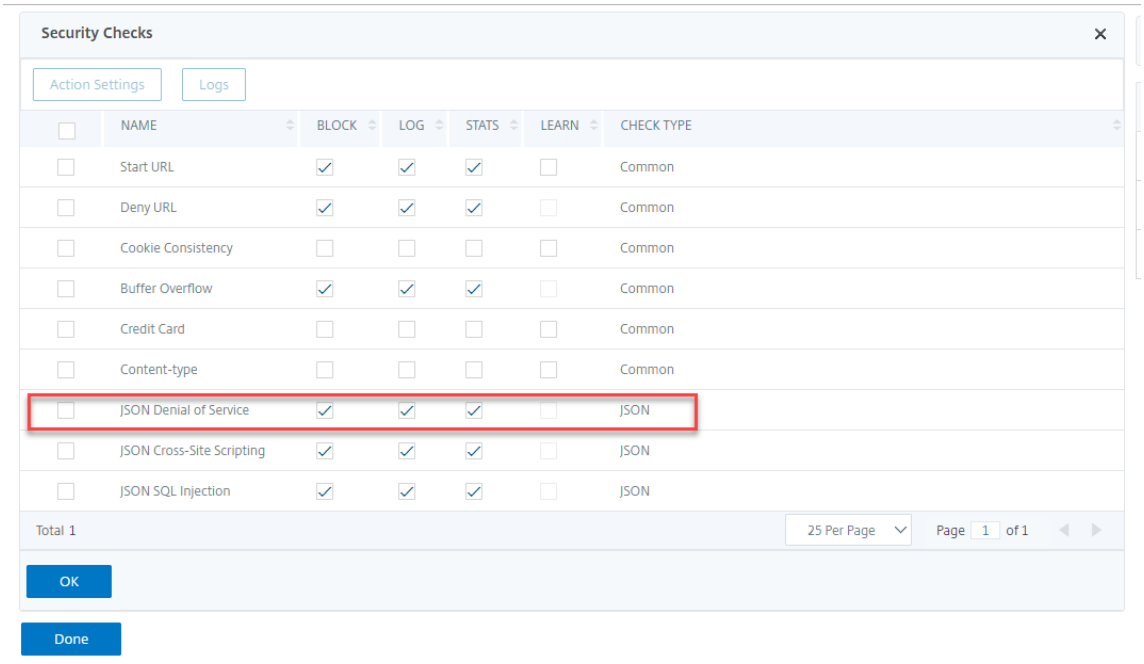
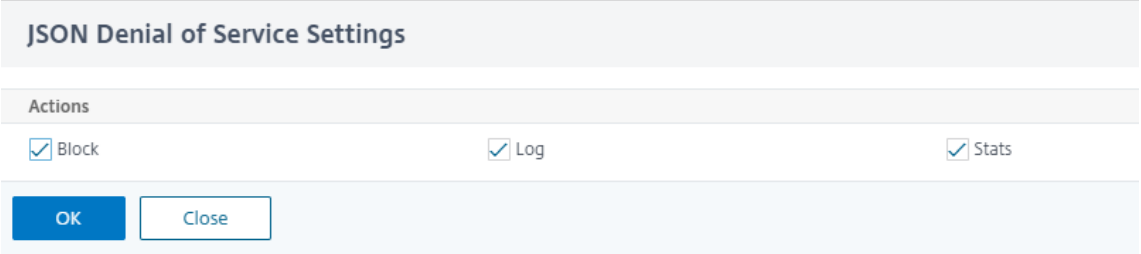
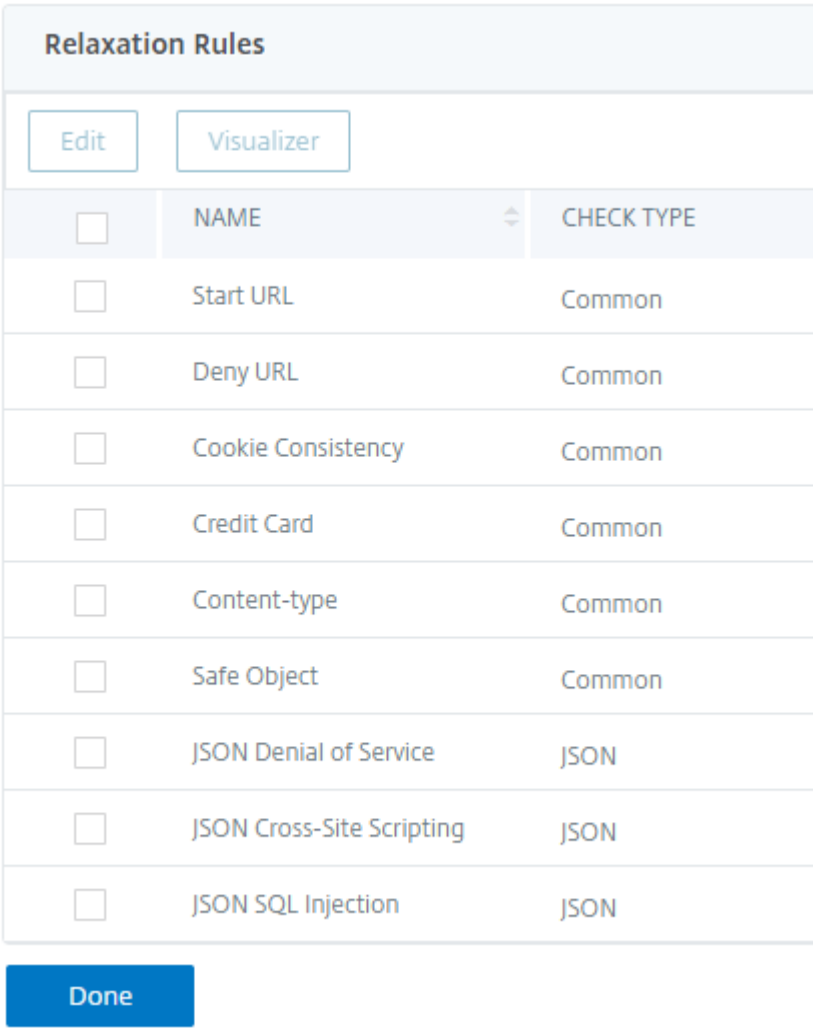
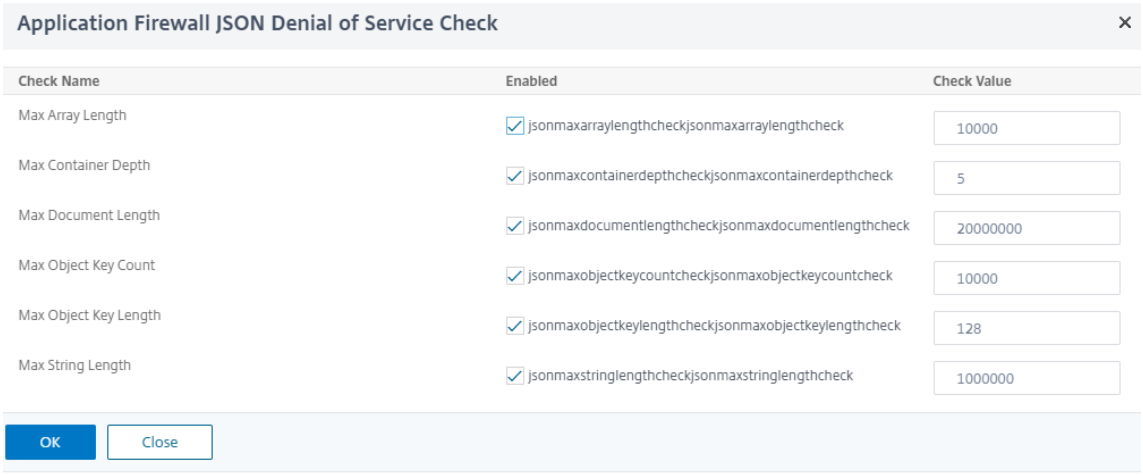
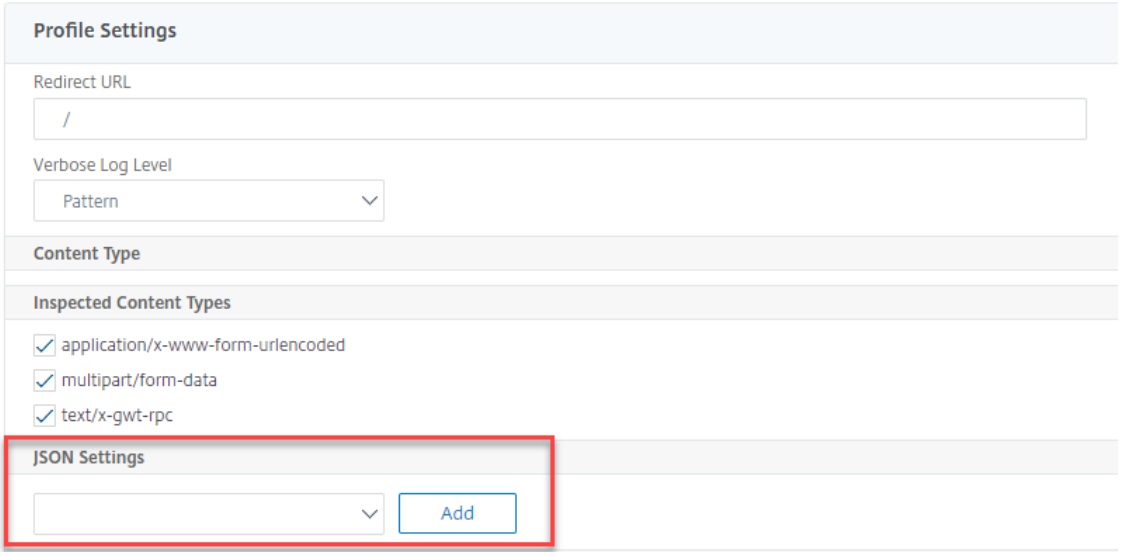
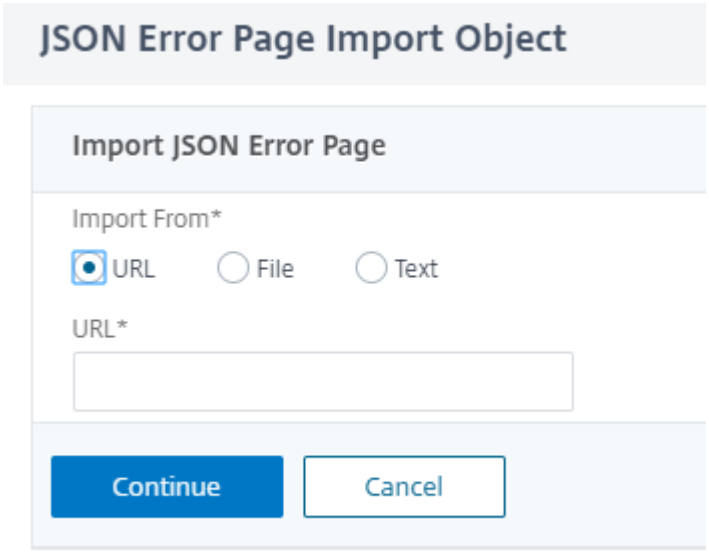
        Location:  ELEMENT       State:  ENABLED

2)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX

```



```
7          Location:  ELEMENT       State:  ENABLED
8
9  3)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX
10
11         Location:  ATTRIBUTE     State:  ENABLED
12
13 4)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX
14
15         Location:  ATTRIBUTE     State:  ENABLED
16 <!--NeedCopy-->
```

- **Emplacement** : vous pouvez spécifier l'emplacement de l'exception XML SQL Inspection dans votre charge utile XML. L'option **ELEMENT** est sélectionnée par défaut. Vous pouvez le remplacer par **ATTRIBUTE**.
- **Commentaire** : Ce champ est facultatif. Vous pouvez utiliser une chaîne de 255 caractères maximum pour décrire l'objectif de cette règle de relaxation.

> **Avertissement**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement le nom que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation imprudente d'expressions régulières peut avoir des conséquences indésirables, par exemple en bloquant l'accès à du contenu Web que vous n'aviez pas l'intention de bloquer ou en autorisant une attaque que l'inspection par injection SQL XML aurait autrement bloquée.

Utilisation de la ligne de commande pour configurer le contrôle d'injection XML SQL

Pour configurer les actions d'injection SQL XML et d'autres paramètres à l'aide de la ligne de commande :

Dans l'interface de ligne de commande, vous pouvez utiliser la commande **set appfw profile** ou la commande **add appfw profile** pour configurer les protections d'injection SQL XML. Vous pouvez activer les actions de blocage, de journalisation et de statistiques. Sélectionnez le type de modèle d'attaque SQL (mots clés, caractères génériques, chaînes spéciales) que vous souhaitez détecter dans les charges utiles. Utilisez la commande **unset appfw profile** pour rétablir les paramètres configurés à leurs valeurs par défaut. Chacune des commandes suivantes ne définit qu'un seul paramètre, mais vous pouvez inclure plusieurs paramètres dans une seule commande :

- `set appfw profile <name> **-XMLSQLInjectionAction** (([block] [log] [stats])| [none])`
- `set appfw profile <name> -XMLSQLInjectionCheckSQLWildChars (ON |OFF)`

- `set appfw profile <name> -XMLSQLInjectionType ([SQLKeyword] | [SQLSplChar] | [SQLSplCharANDKeyword] | [SQLSplCharORKeyword])`
- `set appfw profile <name> -XMLSQLInjectionParseComments ([checkall] | [ansi|nested] | [ansinested])`

Pour configurer une règle de relaxation d'injection SQL à l'aide de la ligne de commande

Utilisez la commande bind or unbind pour ajouter ou supprimer des règles de relaxation, comme suit :

```
1 -  bind appfw profile <name> -XMLSQLInjection <string> [isRegex (REGEX
     | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )]  - comment <string>
     [-state ( ENABLED | DISABLED )]
2 -  unbind appfw profile <name> -XMLSQLInjection <String>
3 <!--NeedCopy-->
```

Exemple :

```
1 > bind appfw profile test_profile -XMLSQLInjection "PurchaseOrder_[0-9A
     -Za-z]{
2  2,15 }
3  " -isregex REGEX -location ATTRIBUTE
4
5 > unbind appfw profile test_profile  - XMLSQLInjection "PurchaseOrder_
     [0-9A-Za-z]{
6  2,15 }
7  " -location ATTRIBUTE
8 <!--NeedCopy-->
```

Utilisation de l'interface graphique pour configurer le contrôle de sécurité de l'injection XML/SQL

Dans l'interface graphique, vous pouvez configurer le contrôle de sécurité de l'injection SQL XML dans le volet du profil associé à votre application.

Pour configurer ou modifier l'injection XML SQL, vérifiez à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet Paramètres avancés, cliquez sur **Contrôles de sécurité**.

Le tableau de contrôle de sécurité affiche les paramètres d'action actuellement configurés pour tous les contrôles de sécurité. Deux options de configuration s'offrent à vous :

a. Si vous souhaitez simplement activer ou désactiver les actions de blocage, de journalisation et de statistiques pour l'injection SQL XML, vous pouvez activer ou désactiver les cases à cocher dans le tableau, cliquer sur OK, puis sur Enregistrer et fermer pour fermer le volet de contrôle de sécurité.

b. Si vous souhaitez configurer des options supplémentaires pour ce contrôle de sécurité, double-cliquez sur Injection SQL XML ou sélectionnez la ligne et cliquez sur **Paramètres d'action**pour afficher les options suivantes :

Rechercher les caractères génériques SQL : considérez les caractères génériques SQL dans la charge utile comme des modèles d'attaque.

Check Request Containing : type d'injection SQL (SQLKeyword, SQLSplChar, SQLSplCharAndKeyword ou SQLSplCharOrKeyword) à vérifier.

Gestion des commentaires SQL : type de commentaires (cocher tous les commentaires, ANSI, imbriqué ou ANSI/imbriqué) à vérifier.

Après avoir modifié l'un des paramètres ci-dessus, cliquez sur **OK** pour enregistrer les modifications et revenir au tableau Contrôles de sécurité. Vous pouvez procéder à la configuration d'autres contrôles de sécurité si nécessaire. Cliquez sur **OK** pour enregistrer toutes les modifications que vous avez apportées dans la section Contrôles de sécurité, puis cliquez sur **Enregistrer** et **fermer** pour fermer le volet Contrôle de sécurité.

Pour configurer une règle de relaxation d'injection SQL XML à l'aide de l'interface graphique

1. Accédez à **Web App Firewall** > **Profils**, mettez en surbrillance le profil cible, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
3. Dans le tableau des règles de relaxation, double-cliquez sur l'entrée **XML SQL Injection** ou sélectionnez-la et cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Règles de relaxation XML SQL Injection**, effectuez des opérations d' **ajout**, de **modification**, de **suppression**, **d'activation**ou de **désactivation** pour les règles de relaxation.

Pour gérer les règles de relaxation de l'injection SQL XML à l'aide du visualiseur

Pour obtenir une vue consolidée de toutes les règles de relaxation, vous pouvez surligner la ligne **d'injection SQL XML** dans le tableau des règles de relaxation, puis cliquer sur **Visualiseur.** Le visualiseur pour les relaxations déployées vous offre la possibilité d' **ajouter** une nouvelle règle ou de **modifier** une règle existante. Vous pouvez également **activer** ou **désactiver** un groupe de règles en sélectionnant un nœud et en cliquant sur les boutons correspondants dans le visualiseur de relaxation.

Pour afficher ou personnaliser les modèles d'injection SQL à l'aide de l'interface graphique :

Vous pouvez utiliser l'interface graphique pour afficher ou personnaliser les modèles SQL.

Les modèles SQL par défaut sont spécifiés dans **Web App Firewall** > **Signatures** > ***Signatures**par défaut. Si vous ne liez aucun objet de signature à votre profil, les modèles SQL par défaut spécifiés dans l'objet Signatures par défaut seront utilisés par le profil pour le traitement des contrôles de sécurité par injection SQL XML. Les règles et modèles de l'objet Signatures par défaut sont en lecture seule.

Vous ne pouvez pas les modifier ou les modifier. Si vous souhaitez modifier ou changer ces modèles, créez un objet de signature défini par l'utilisateur en copiant l'objet Signatures par défaut et en modifiant les modèles SQL. Utilisez l'objet signature défini par l'utilisateur dans le profil qui traite le trafic pour lequel vous souhaitez utiliser ces modèles SQL personnalisés.

Pour plus d'informations, voir Signatures.

Pour afficher les modèles SQL par défaut :

a. Accédez à **Web App Firewall** > **Signatures**, sélectionnez ***Signatures par défaut**, puis cliquez sur **Modifier**. Cliquez ensuite sur **Gérer les modèles de script SQL/intersite**.

Le tableau Manage SQL/Cross-Site Scripting Paths contient les quatre lignes suivantes relatives à l'injection SQL :

```
Injection (not_alphanum, SQL)/ Keyword

Injection (not_alphanum, SQL)/ specialstring

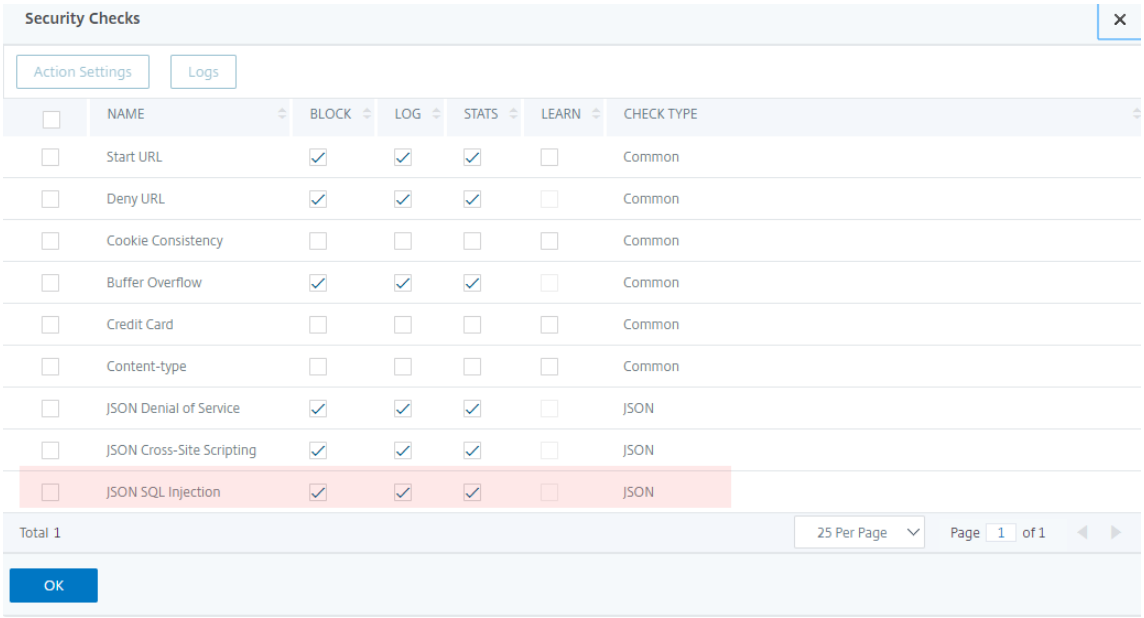
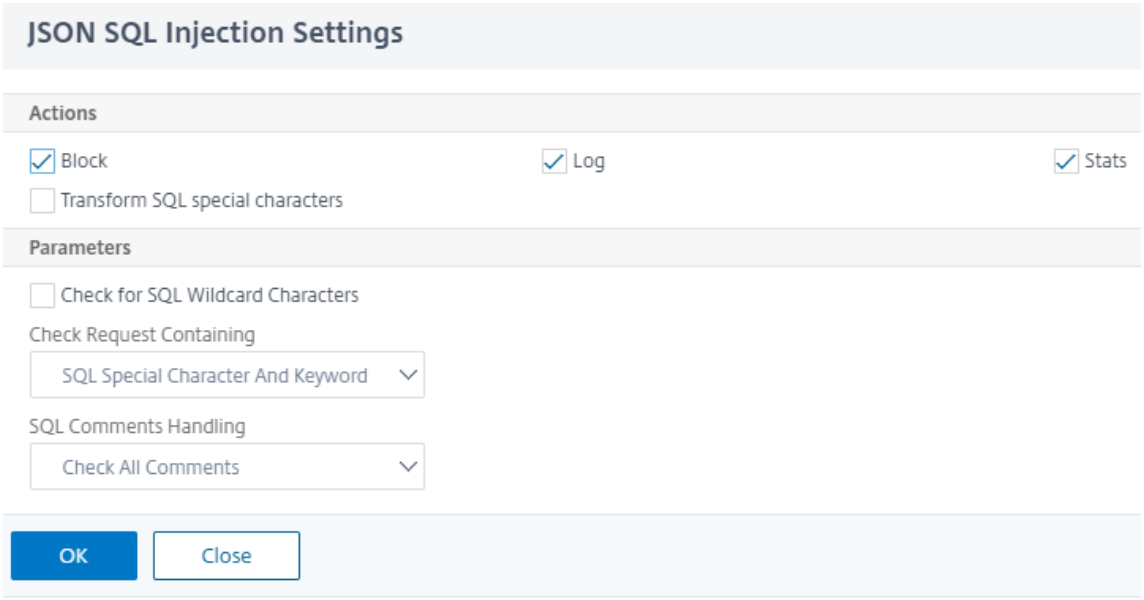
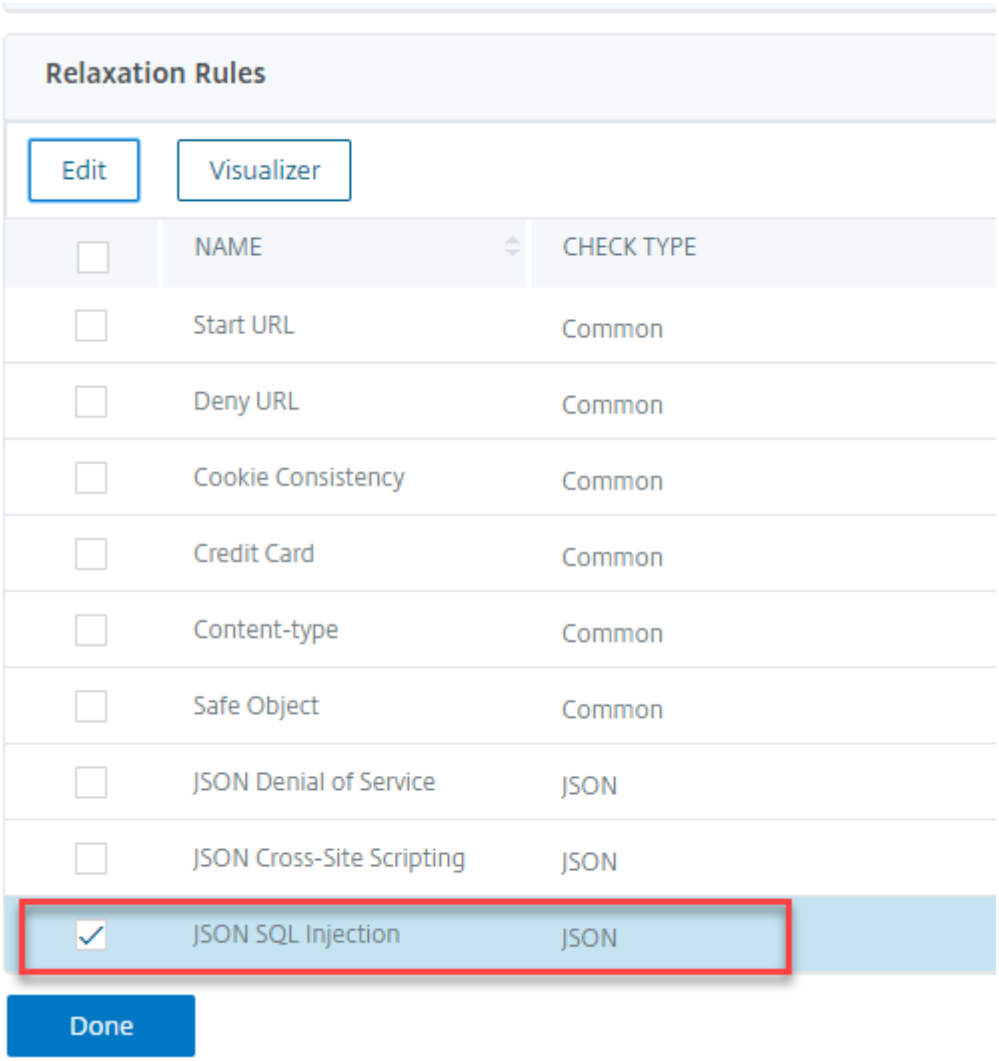
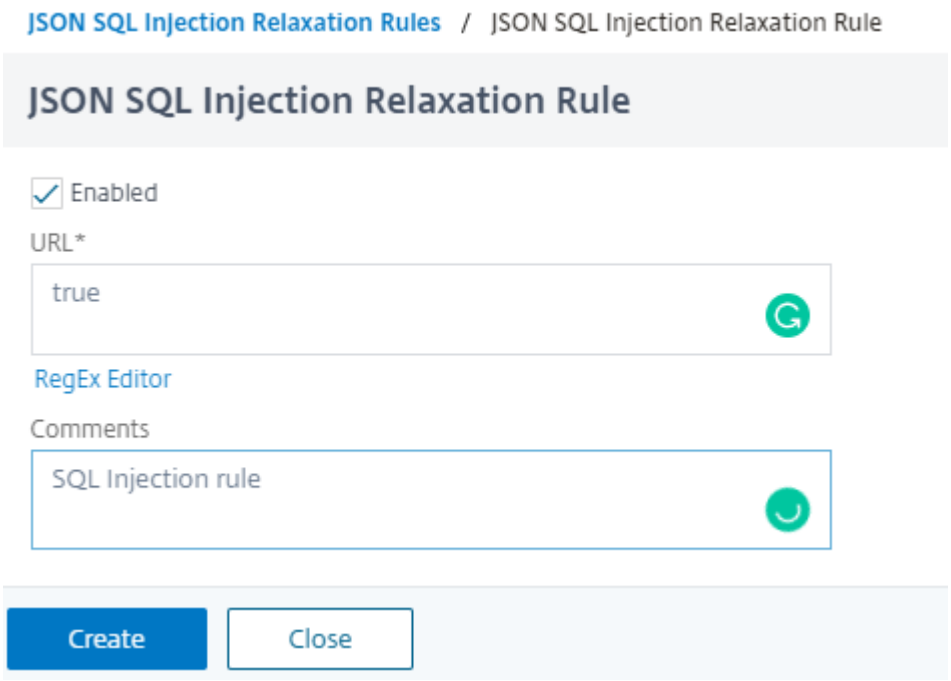
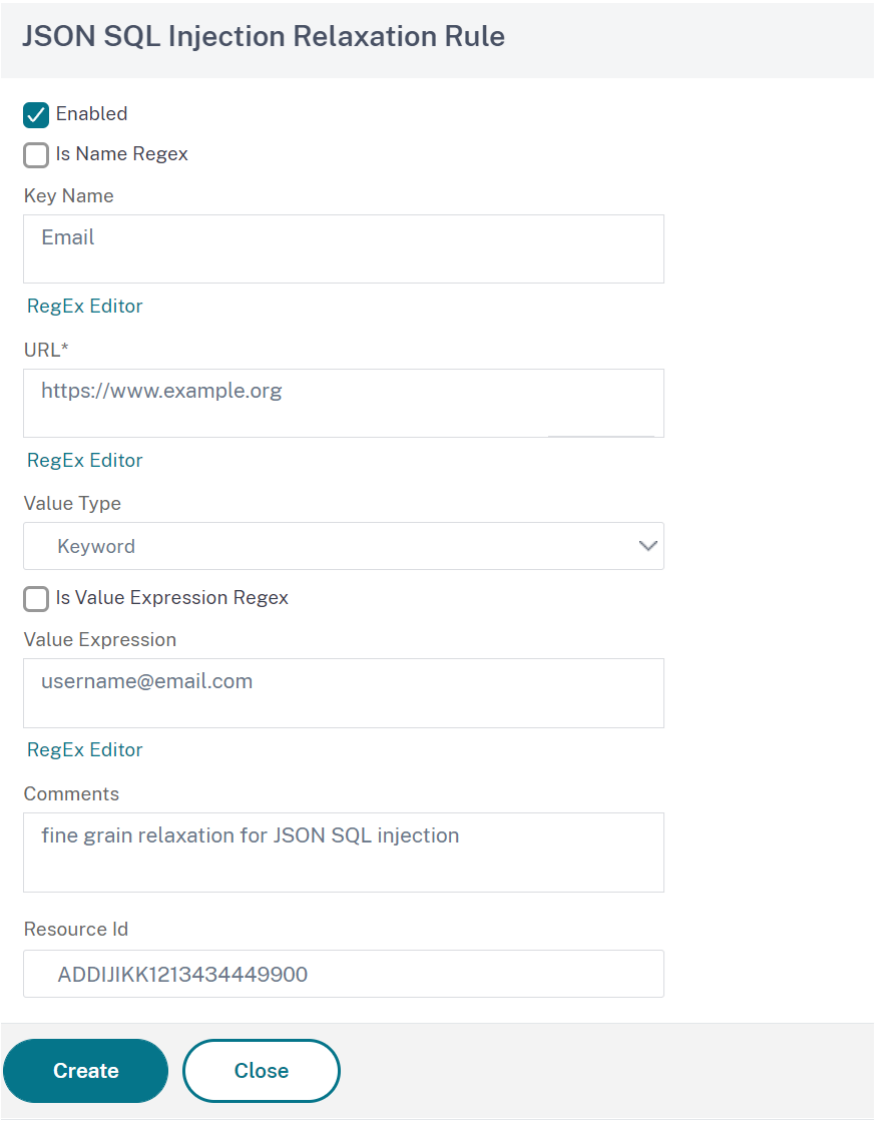
Injection (not_alphanum, SQL)/ transformrules/transform

Injection (not_alphanum, SQL)/ wildchar
<!--NeedCopy-->
```

b. Sélectionnez une ligne et cliquez sur **Gérer les éléments** pour afficher les modèles SQL correspondants (mots-clés, chaînes spéciales, règles de transformation ou caractères génériques) utilisés par le contrôle d'injection SQL du Web App Firewall.

Pour personnaliser les modèles SQL : vous pouvez modifier un objet de signature défini par l'utilisateur pour personnaliser les mots clés SQL, les chaînes spéciales et les caractères génériques. Vous pouvez ajouter de nouvelles entrées ou supprimer celles qui existent déjà. Vous pouvez modifier les règles de transformation pour les chaînes spéciales SQL.

a. Accédez à **Web App Firewall** > **Signatures**, mettez en surbrillance la signature définie par l'utilisateur cible, puis cliquez sur **Modifier**. Cliquez sur **Gérer les modèles de script SQL/intersite** pour afficher le tableau **Gérer les chemins de script SQL/intersite** .

b. Sélectionnez la ligne SQL cible.

i. Cliquez sur **Gérer les éléments**pour **ajouter**, **modifier** ou **supprimer** l'élément SQL correspondant.

ii. Cliquez sur **Supprimer** pour supprimer la ligne sélectionnée.

> **Avertissement**
>
> Vous devez être très prudent lorsque vous supprimez ou modifiez un élément SQL par défaut, ou lorsque vous supprimez le chemin SQL pour supprimer la ligne entière. Les règles de signature ainsi que le contrôle de sécurité de l'injection SQL XML s'appuient sur ces éléments pour détecter

> les attaques par injection SQL afin de protéger vos applications. La personnalisation des modèles SQL peut rendre votre application vulnérable aux attaques SQL XML si le modèle requis est supprimé lors de la modification.

Utilisation de la fonction de journalisation avec le contrôle d'injection XML SQL

Lorsque l'action de journalisation est activée, les violations du contrôle de sécurité de l' **injection SQL XML** sont enregistrées dans le journal d'audit en tant que violations **APPFW_XML_SQL** . Le Web App Firewall prend en charge les formats de journaux natifs et CEF. Vous pouvez également envoyer les journaux à un serveur Syslog distant.

Pour accéder aux messages du journal à l'aide de la ligne de commande :

Passez au shell et suivez le fichier ns.logs dans le dossier /var/log/ pour accéder aux messages de journal relatifs aux violations des scripts intersites XML :

```
1 > Shell
2
3 > tail -f /var/log/ns.log | grep APPFW_XML_SQL
4 <!--NeedCopy-->
```

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique inclut un outil utile (Syslog Viewer) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Accédez à **Web App Firewall** > **Profils**, sélectionnez le profil cible et cliquez sur **Security Checks**. Sélectionnez la ligne **d'injection SQL XML** et cliquez sur **Journaux**. Lorsque vous accédez aux journaux directement à partir de la vérification du profil par injection SQL XML, l'interface utilisateur filtre les messages du journal et affiche uniquement les journaux relatifs à ces violations de contrôle de sécurité.
- **Vous pouvez également accéder au visualiseur Syslog en accédant à**Système**> Audit.** Dans la section Messages d'audit, cliquez sur le lien **Messages Syslog** pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris les autres journaux de violation de vérification de sécurité. Ceci est utile pour le débogage lorsque plusieurs violations de contrôle de sécurité peuvent être déclenchées pendant le traitement des demandes.
- Accédez à **Web App Firewall** > **Politiques** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien **des messages Syslog** pour afficher le **visualiseur Syslog**, qui affiche tous les messages du journal, y compris les autres journaux de violations des contrôles de sécurité.

Le visualiseur Syslog basé sur XML fournit diverses options de filtrage pour sélectionner uniquement les messages du journal qui vous intéressent. **Pour sélectionner les messages du journal pour la vérification de l'**injection SQL XML**, filtrez en sélectionnant**APPFW**dans les options déroulantes**

du module. La liste **Type d'événement** offre un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous cochez la case **APPFW_XML_SQL** et cliquez sur le bouton **Appliquer**, seuls les messages de journal relatifs aux violations du contrôle de sécurité de l' **injection SQL XML** apparaissent dans le visualiseur Syslog.

Si vous placez le curseur sur la ligne correspondant à un message de journal spécifique, plusieurs options, telles que le **module**, le **type d'événement**, l' **ID d'événement**et l' **adresse IP du client**, apparaissent sous le message du journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans le message de journal.

Statistiques relatives aux violations d'injection XML SQL

Lorsque l'action statistique est activée, le compteur du contrôle **d'injection SQL XML** est incrémenté lorsque le Web App Firewall entreprend une action pour ce contrôle de sécurité. Les statistiques sont collectées pour le taux et le nombre total pour le trafic, les violations et les journaux. La taille d'un incrément du compteur de journaux peut varier en fonction des paramètres configurés. Par exemple, si l'action de blocage est activée, une demande concernant une page contenant trois violations **d'injection SQL XML** augmente le compteur de statistiques d'une unité, car la page est bloquée dès que la première violation est détectée. Toutefois, si le bloc est désactivé, le traitement de la même demande incrémente le compteur de statistiques pour les violations et les journaux de trois, car chaque violation génère un message de journal distinct.

Pour afficher les statistiques d'injection XML SQL à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
> sh appfw stats
```

Pour afficher les statistiques d'un profil spécifique, utilisez la commande suivante :

```
> stat appfw profile <profile name>
```

Pour afficher les statistiques d'injection XML SQL à l'aide de l'interface graphique

1. Accédez à **Système** > **Sécurité** > **Web App Firewall**.
2. Dans le volet droit, accédez au lien **Statistiques** .
3. Utilisez la barre de défilement pour afficher les statistiques relatives aux violations et aux journaux **relatifs aux injections SQL XML** . Le tableau des statistiques fournit des données en temps réel et est mis à jour toutes les 7 secondes.

Vérification des pièces jointes XML

January 21, 2021

La vérification des pièces jointes XML examine les demandes entrantes de pièces jointes malveillantes et bloque celles qui contiennent des pièces jointes susceptibles d'enfreindre la sécurité des applications. Le but de la vérification des pièces jointes XML est d'empêcher un attaquant d'utiliser une pièce jointe XML pour enfreindre la sécurité de votre serveur.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification des pièces jointes XML, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Apprendre, Journaliser, Statistiques et Apprendre :

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification des pièces jointes XML :

- `set appfw profile <name> -xmlAttachmentAction [block] [learn] [log] [stats] [none]`

Vous devez configurer les autres paramètres de vérification des pièces jointes XML dans l'interface graphique. Dans la boîte de dialogue `Modify XML Attachment` Vérifier, sous l'onglet Vérifications, vous pouvez configurer les paramètres suivants :

- **Taille maximale de la pièce jointe.** Autorisez les pièces jointes qui ne sont pas supérieures à la taille maximale que vous spécifiez. Pour activer cette option, activez d'abord la case à cocher Activé, puis tapez la taille maximale de la pièce jointe en octets dans la zone de texte `Size`.
- **Type de contenu de pièce jointe.** Autoriser les pièces jointes du type de contenu spécifié. Pour activer cette option, activez d'abord la case à cocher Activé, puis entrez une expression régulière qui correspond à l'attribut Content-Type des pièces jointes que vous souhaitez autoriser.
  - Vous pouvez taper l'expression URL directement dans la fenêtre de texte. Si vous le faites, vous pouvez utiliser le menu `Regex Tokens` pour entrer un certain nombre d'expressions régulières utiles au niveau du curseur au lieu de les taper manuellement.
  - Vous pouvez cliquer sur Regex Editor pour ouvrir la`Add Regular Expression` boîte de dialogue et l'utiliser pour construire l'expression URL.

Contrôle de l'interopérabilité des services Web

January 21, 2021

La vérification de l'interopérabilité des services Web (WS-I) examine à la fois les demandes et les réponses pour vérifier la conformité à la norme WS-I et bloque les demandes et réponses qui ne respectent pas cette norme. Le but de la vérification WS-I est de bloquer les requêtes qui pourraient ne pas interagir avec d'autres XML de manière appropriée. Un attaquant peut utiliser des incohérences dans l'interopérabilité pour lancer une attaque sur votre application XML.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier le contrôle de

l'interopérabilité des services Web, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journal, Statistiques et Apprendre.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification d'interopérabilité des services Web :

- `set appfw profile <name> -xmlWSIAction [block] ][log] [learn] [stats] [ none]`

Pour configurer des règles d'interopérabilité des services Web individuelles, vous devez utiliser l'interface graphique. Sous l'onglet Vérifications de la boîte de dialogue Modifier le contrôle de l'interopérabilité des services Web, sélectionnez une règle et cliquez sur Activer ou Désactiver pour activer ou désactiver la règle. Vous pouvez également cliquer sur Ouvrir pour ouvrir la boîte de message Détail de l'interopérabilité des services Web pour cette règle. La boîte de message affiche des informations en lecture seule sur la règle. Vous ne pouvez pas modifier ou apporter d'autres modifications de configuration à l'une de ces règles.

La vérification WS-I utilise les règles répertoriées dans WS-I Basic Profile 1.0. WS-I propose les meilleures pratiques pour le développement de solutions de services Web interopérables. Les vérifications WS-I sont effectuées uniquement sur les messages SOAP.

La description de chaque règle standard WSI est fournie ci-dessous :

Règle	Description
BP1201	Le corps du message doit être un soap:envelope avec espace de noms.
R1000	Lorsqu'une ENVELOPE est une erreur, l'élément SOAP:Fault NE DOIT PAS avoir des enfants d'élément autres que faultcode, faultstring, faultactor et detail.
R1001	Lorsqu'une ENVELOPE est une erreur, les enfants de l'élément SOAP:Fault DOIVENT être non qualifiés.
R1003	UN RÉCEPTEUR DOIT accepter les messages d'erreur qui comportent un certain nombre d'attributs qualifiés ou non qualifiés, y compris zéro, apparaissant sur l'élément de détail. L'espace de noms des attributs qualifiés peut être autre que l'espace de noms de l'élément de document qualifié Envelope.

Règle	Description
R1004	Lorsqu'une ENVELOPE contient un élément de code faultcode, le contenu de cet élément doit être soit l'un des codes d'erreur définis dans SOAP 1.1 (fournissant des informations supplémentaires si nécessaire dans l'élément detail), soit un Qname dont l'espace de noms est contrôlé par l'autorité de spécification de la faute (dans cet ordre de préférence).
R1005	Une ENVELOPE NE DOIT PAS contenir l'attribut SOAP:encodingStyle sur l'un des éléments dont l'espace de noms est le même que l'espace de noms de l'élément de document qualifié Envelope.
R1006	Une ENVELOPE NE DOIT PAS contenir les attributs SOAP:EncodingStyle sur un élément qui est un enfant de SOAP:Body.
R1007	Une ENVELOPE décrite dans une liaison littérale rpc-NE DOIT PAS contenir l'attribut SOAP:encodingStyle sur un élément qui est un petit-fils de Soap:body.
R1011	Une ENVELOPE NE DOIT PAS avoir d'enfant élément de SOAP:Envelope suivant l'élément SOAP:Body.
R1012	Un MESSAGE DOIT être sérialisé en UTF-8 ou UTF-16.
R1013	Une ENVELOPE contenant un attribut SOAP:MustUnderderderit DOIT utiliser uniquement les formes lexicales 0 et 1.
R1014	Les enfants de l'élément SOAP:body dans une ENVELOPE DOIVENT être qualifiés d'espace de noms.
R1015	Un RECEPTEUR DOIT générer une erreur s'il rencontre une enveloppe dont l'élément de document n'est pas SOAP:Envelope.

Règle	Description
R1031	Lorsqu'une ENVELOPE contient un élément de code faultcode, le contenu de cet élément ne doit PAS utiliser la notation des points SOAP 1.1 pour affiner la signification de la faute.
R1032	Les éléments SOAP:envelope, SOAP:header et SOAP:body d'une ENVELOPE NE DOIVENT PAS avoir des attributs dans le même espace de noms que celui de l'élément de document qualifié Envelope
R1033	Une ENVELOPE NE DEVRAIT PAS contenir la déclaration d'espace de noms :`xmlns:xml=http://www.w3.org/XML/1998/namespace.`
R1109	La valeur du champ d'en-tête HTTP SoapAction dans une requête HTTP MESSAGE DOIT être une chaîne entre guillemets.
R1111	Une INSTANCE DEVRAIT utiliser un code d'état HTTP 200 OK sur un message de réponse contenant une enveloppe qui n'est pas une erreur.
R1126	Une INSTANCE DOIT renvoyer un code d'état HTTP d'erreur serveur interne 500 si l'enveloppe de réponse est une erreur.
R1132	Une requête HTTP MESSAGE DOIT utiliser la méthode HTTP POST.
R1140	UN MESSAGE DEVRAIT être envoyé en utilisant HTTP/1.1.
R1141	Un MESSAGE DOIT être envoyé en utilisant HTTP/1.1 ou HTTP/1.0.
R2113	Une ENVELOPE NE DOIT PAS inclure l'attribut SOAPENC:ArrayType.
R2211	Une ENVELOPE décrite avec une liaison littérale rpc-NE DOIT PAS avoir l'attribut xsi:nil avec une valeur de 1 ou true sur les accesseurs de pièce.

Règle	Description
R2714	Pour les opérations à sens unique, une INSTANCE NE DOIT PAS renvoyer une réponse HTTP contenant une enveloppe. Plus précisément, l'entité de réponse HTTP doit être vide.
R2729	Une ENVELOPE décrite avec une liaison littérale rpc-qui est une réponse DOIT avoir un élément wrapper dont le nom est le nom wsdl:operation correspondant suffixé avec StringResponse.
R2735	Une ENVELOPE décrite avec une liaison littérale rpc-DOIT placer les éléments d'accesseur de pièce pour les paramètres et renvoyer la valeur dans aucun espace de noms.
R2738	Une ENVELOPE DOIT inclure tous les soapbind:headers spécifiés sur un wsdl:input ou wsdl:output d'un wsdl:operation d'un wsdl:binding qui le décrit.
R2740	Un wsdl:binding dans une DESCRIPTION DEVRAIT contenir un soapbind:fault décrivant chaque défaut connu.
R2744	Une requête HTTP MESSAGE DOIT contenir un champ d'en-tête HTTP SoapAction avec une valeur entre guillemets égale à la valeur de l'attribut SoapAction de soapbind:operation, s'il est présent dans la description WSDL correspondante.

Vérification de validation des messages XML

August 20, 2021

La vérification de validation des messages XML examine les demandes contenant des messages XML pour s'assurer qu'elles sont valides. Si une demande contient un message XML non valide, le Web App Firewall bloque la demande. Le but de la vérification de validation XML est d'empêcher un attaquant

d'utiliser des messages XML invalides spécialement conçus pour enfreindre la sécurité de votre application.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier la vérification de validation des messages XML, sous l'onglet Général, vous pouvez activer ou désactiver les actions Bloquer, Journal et Statistiques.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification de validation des messages XML :

- `set appfw profile <name> -xmlValidationAction [**block**] [**log**] [**stats**] [**none**]`

Vous devez utiliser l'interface graphique pour configurer les autres paramètres de vérification de validation XML. Dans la boîte de dialogue
Modifier la vérification de validation des messages XML, sous l'onglet
Vérifications, vous pouvez configurer les paramètres suivants :

- **Validation des messages XML.** Utilisez l'une des options suivantes pour valider le message XML :
  - **Enveloppe SOAP.** Valider uniquement l'enveloppe SOAP des messages XML.
  - **WSDL.** Valider les messages XML à l'aide d'un XML SOAP WSDL. Si vous choisissez la validation WSDL, dans la liste déroulante Objet WSDL, vous devez choisir un WSDL. Si vous souhaitez valider un fichier WSDL qui n'a pas encore été importé dans le Web App Firewall, vous pouvez cliquer sur le bouton Importer pour ouvrir la boîte de dialogue Gérer les importations WSDL et importer votre fichier WSDL. Voir WSDL pour plus d'informations.
    * Si vous souhaitez valider l'URL entière, laissez le bouton radio Absolute dans le tableau de boutons Vérification du point de terminaison sélectionné. Si vous souhaitez valider uniquement la partie de l'URL après l'hôte, sélectionnez le bouton radio Relative.
    * Si vous souhaitez que le Web App Firewall applique strictement le WSDL et qu'il n'autorise pas d'en-têtes XML supplémentaires non définis dans le WSDL, vous devez désactiver la case à cocher Autoriser les en-têtes supplémentaires non définis dans le WSDL.

      Attention : Si vous décochez la case
      Autoriser les en-têtes supplémentaires non définis dans le WSDL et que votre WSDL ne définit pas tous les en-têtes XML que votre application XML protégée ou Web 2.0 attend ou qu'un client envoie, vous pouvez bloquer l'accès légitime à votre service protégé.
  - **Schéma XML.** Valider les messages XML à l'aide d'un schéma XML. Si vous choisissez la validation de schéma XML, dans la liste déroulante Objet de schéma XML, vous devez choisir un schéma XML. Si vous souhaitez valider un schéma XML qui n'a pas encore été importé dans le Web App Firewall, vous pouvez cliquer sur le bouton Importer pour ouvrir la boîte

de dialogue Gérer les importations de schéma XML et importer votre WSDL. Voir WSDL pour plus d'informations.

- **Validation des réponses.** Par défaut, le Web App Firewall ne tente pas de valider les réponses. Si vous souhaitez valider les réponses de votre application protégée ou de votre site Web 2.0, activez la case à cocher Valider la réponse. Lorsque vous le faites, la case à cocher Réutiliser le schéma XML spécifié dans la validation de la demande et la liste déroulante Objet de schéma XML sont activées.
  - Cochez la case Réutiliser le schéma XML pour utiliser le schéma que vous avez spécifié pour la validation de la demande pour effectuer également la validation de la réponse. Remarque : Si vous cochez cette case, la liste déroulante Objet de schéma XML est grisée.
  - Si vous souhaitez utiliser un schéma XML différent pour la validation de réponse, utilisez la liste déroulante Objet de schéma XML pour sélectionner ou télécharger ce schéma XML.

Vérification du filtrage des erreurs XML SOAP

January 21, 2021

La vérification de filtrage des erreurs XML SOAP examine les réponses de vos services Web protégés et filtre les erreurs XML SOAP. Cela empêche les fuites d'informations sensibles aux attaquants.

Si vous utilisez l'assistant ou l'interface graphique, dans la boîte de dialogue Modifier le contrôle du filtrage des erreurs SOAP XML, sous l'onglet **Général**, vous pouvez activer ou désactiver les actions Bloquer, Journal et Statistiques et Supprimer, qui supprime les erreurs SOAP avant de transférer la réponse à l'utilisateur.

Si vous utilisez l'interface de ligne de commande, vous pouvez entrer la commande suivante pour configurer la vérification du filtrage des erreurs XML SOAP :

```
set appfw profile <name> -XMLSOAPFaultAction [block] [log] [stats] [none]
```

Vous ne pouvez pas configurer des exceptions à la vérification XML SOAP Fault Filtering. Vous ne pouvez l'activer ou le désactiver que.

Vérifications de protection JSON

May 5, 2023

NetScaler Web App Firewall protège vos applications JSON contre les attaques DoS, SQL ou par script intersite au niveau du contenu. Lorsqu'une requête JSON fait l'objet d'une attaque DoS, SQL ou par

script intersite, vous devez protéger votre application en définissant des limites pour les structures JSON telles que les tableaux et les chaînes.

> **Remarque :**
>
> Les contrôles de sécurité JSON s'appliquent uniquement au contenu envoyé avec un en-tête de type de contenu JSON. Si l'en-tête du type de contenu est absent ou s'il est défini sur une valeur différente, tous les contrôles de sécurité JSON sont contournés. Si vous souhaitez protéger vos applications JSON, les webmasters de chaque serveur Web qui héberge ces applications doivent s'assurer qu'un en-tête de type de contenu JSON approprié est envoyé.
>
> La fonctionnalité d'apprentissage n'est pas compatible avec les types de contenu JSON SQL, les scripts intersites et les types de contenu DOS.

Vérification de la protection par déni de service JSON

May 5, 2023

La vérification par déni de service (DoS) JSON examine une demande JSON entrante et valide si des données correspondent aux caractéristiques d'une attaque DoS. Si la demande comportait des violations JSON, l'appliance bloque la demande, consigne les données, envoie une alerte SNMP et affiche également une page d'erreur JSON. Le but de la vérification de déni de service JSON est d'empêcher un attaquant d'envoyer une demande JSON pour lancer des attaques de déni de service sur vos applications JSON ou votre site Web.

Lorsqu'un client envoie une demande à une appliance NetScaler, l'analyseur JSON analyse la charge utile de la demande et si une violation est observée, l'appliance applique des contraintes sur la structure JSON. La contrainte impose une limite de taille à la demande JSON. Par conséquent, si une violation JSON a été observée, l'appliance applique une action et répond par la page d'erreur JSON.

Règles JSON DoS

Lorsque l'appliance reçoit une demande JSON, la protection DOS JSON impose une limite de taille sur les paramètres DoS suivants dans la charge utile de la demande.

1. profondeur maximale : imbrication maximale (profondeur) du document JSON. Cette vérification protège contre les documents dont la hiérarchie est trop approfondie.
2. longueur maximale du document : longueur maximale du document JSON.
3. longueur maximale du tableau : longueur maximale du tableau dans l'un des objets JSON. Cette vérification protège contre les réseaux ayant de grandes longueurs.
4. longueur maximale de la chaîne : longueur maximale de la chaîne dans le JSON. Ce chèque protège contre les cordes de grande longueur.

5. nombre maximum de clés d'objet : nombre maximum de clés dans l'un des objets JSON. Cette vérification protège contre les objets comportant un grand nombre de clés.
6. longueur maximale de la clé de l'objet : longueur maximale de la clé dans l'un des objets JSON. Cette vérification protège contre les objets dotés de grandes clés.

Voici une liste des règles de déni de service JSON validées lors de l'analyse JSON.

1. JSONMaxContainerDepth. Cette vérification peut être activée en configurant la vérification JSONMaxContainerDepth et, par défaut, l'option est DÉSACTIVÉE.
2. JSONMaxContainerDepth. Cette vérification peut être activée/désactivée par l'option configurable JSONMaxContainerDepthCheck et la valeur par défaut peut être modifiée par l'option JSONMaxContainerDepth. Toutefois, vous pouvez modifier les niveaux maximum jusqu'à une valeur comprise entre 1 et 127. Valeur par défaut : 5, Valeur minimale : 1, Valeur maximale : 127
3. JSONMaxDocumentLength. Cette vérification peut être activée en configurant la vérification JSONMaxDocumentLength et l'option par défaut est OFF.
4. JSONMaxDocumentLength. Cette vérification peut être activée en configurant la vérification JSONMaxDocumentLength et la longueur par défaut est définie sur 20000000 octets. Valeur minimale : 1, valeur maximale : 2147483647
5. JSONMaxObjectKeyCount. La règle valide si la vérification du nombre maximum de clés d'objet JSON est activée ou désactivée. Valeurs possibles : ON, OFF, Valeur par défaut : OFF
6. JSONMaxObjectKeyCount. Cette vérification peut être activée en configurant la vérification JSONMaxObjectKeyCount. La vérification protège contre les objets qui ont un grand nombre de clés et la valeur par défaut est définie sur 1000 octets. Valeur minimale : 0, valeur maximale : 2147483647
7. JSONMaxObjectKeyLength. Cette vérification peut être activée en configurant la vérification JSONMaxObjectKeyLength. La règle valide si la vérification de la longueur maximale de la clé d'objet JSON est activée ou désactivée. Par défaut, il est désactivé.
8. JSONMaxObjectKeyLength. La vérification protège contre les objets ayant une grande longueur de clé. Valeur par défaut : 128. Valeur minimale : 1, valeur maximale : 2147483647
9. JSONMaxArrayLength. La règle valide si la vérification de la longueur maximale du tableau JSON est activée ou désactivée. Par défaut, il est désactivé.
10. JSONMaxArrayLength. La vérification protège contre les baies de grandes longueurs. Par défaut, la valeur est définie sur 10000. Valeur minimale : 1, valeur maximale : 2147483647
11. JSONMaxStringLength. Cette vérification peut être activée en configurant la vérification JSONMaxStringLength. La vérification valide si la longueur maximale de la chaîne JSON est ON ou OFF. Par défaut, il est désactivé.

12. JSONMaxStringLength. Le carreau protège contre les cordes de grande longueur. Par défaut, il est défini sur 1000000. Valeur minimale : 1, valeur maximale : 2147483647

Configurer le contrôle de protection JSON DoS

Pour configurer la protection DoS JSON, vous devez effectuer les étapes suivantes :

1. Ajoutez un profil de pare-feu d'application pour JSON.
2. Définissez le profil de pare-feu d'application pour les paramètres DoS JSON.
3. Configurez les variables DoS JSON en liant le profil de pare-feu d'application.

Ajouter un profil de pare-feu d'application pour la protection JSON DoS

Vous devez d'abord créer un profil qui spécifie comment le pare-feu d'application doit protéger votre contenu Web JSON contre les attaques DoS JSON.
À l'invite de commande, tapez :

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> *Remarque* :
>
> Lorsque vous définissez le type de profil sur JSON, les autres vérifications telles que HTML ou XML ne s'appliquent pas.

Exemple

```
add appfw profile profile1 -type JSON
```

Définition du profil de pare-feu d'application pour la protection JSON DoS

Vous devez configurer le profil pour une ou plusieurs actions de déni de service JSON et objet d'erreur de déni de service JSON à définir sur le profil de pare-feu d'application.
À l'invite de commande, tapez :

```
set appfw profile <name> -JSONDoSAction [block] | [log] | [stats] | [none]
```

Bloquer : bloquez les connexions qui ne respectent pas ce contrôle de sécurité.
Journal - Consigner les violations de cette vérification de sécurité.
Stats - Générez des statistiques pour cette vérification de sécurité.
Aucun : désactivez toutes les actions pour ce contrôle de sécurité.

> *Remarque* :

> Pour activer une ou plusieurs actions, tapez « set appfw profile -JsondosAction » suivi des actions à activer.

Exemple

```
set appfw profile profile1 -JSONDoSAction block log stat
```

Configurer les variables DoS en liant le profil de pare-feu d'application

Pour fournir une protection DoS JSON, vous devez lier le profil de pare-feu d'application aux paramètres de déni de service JSON.
À l'invite de commande, tapez :

```
bind appfw profile <name> -JSONDoSURL <expression> [-JSONMaxContainerDepthCheck
 ( ON | OFF )[-JSONMaxContainerDepth <positive_integer>]] [-JSONMaxDocumentLengthCheck
 ( ON | OFF )[-JSONMaxDocumentLength <positive_integer>]] [-JSONMaxObjectKeyCountCheck
 ( ON | OFF )[-SONMaxObjectKeyCount <positive_integer>]] [-JSONMaxObjectKeyLengthCheck
 ( ON | OFF )[-JSONMaxObjectKeyLength <positive_integer>]] [-JSONMaxArrayLengthCheck
 ( ON | OFF )[-JSONMaxArrayLength <positive_integer>]] [-JSONMaxStringLengthCheck
 ( ON | OFF )[-JSONMaxStringLength <positive_integer>]]
```

Exemple

```
bind appfw profile profile1 -JSONDoSURL  ".*"  -JSONMaxContainerDepthCheck ON
```

> *Remarque* :
>
> Les vérifications de déni de service JSON ne seront applicables que si le type de profil est sélectionné en tant que JSON. En outre, le SQL, les scripts intersites, le format de champ et les signatures de champ de formulaire sont appliqués aux paramètres de requête dans les cas de profil JSON.

Page d'erreur Importation JSON

Si une demande entrante a subi une attaque DoS et que vous bloquez la demande, l'appliance affiche un message d'erreur. Pour ce faire, vous devez importer la page d'erreur JSON.
À l'invite de commande, tapez :

```
import appfw jsonerrorpage <src> <name> [-comment <string>] [-overwrite]
```

Où,

src. URL (protocole, hôte, chemin et nom) de l'emplacement où stocker l'objet d'erreur JSON importé.

> *Remarque* :
>
> L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite une authentification par certificat client pour y accéder. Il s'agit d'un argument obligatoire. Longueur maximale : 2047.

Nom. Nom à attribuer à l'objet d'erreur JSON sur NetScaler. Il s'agit d'un argument obligatoire. Longueur maximale : 31
commentaires. Tout commentaire destiné à conserver les informations relatives à l'objet d'erreur JSON. Longueur maximale : 255
écrasements. Remplacez tout objet d'erreur JSON existant du même nom.

Exemple de configuration

```
Add appfw prof profjson - type JSON
Bind appfw prof profjson - JSONDoSURL ".*" -
    JSONMaxDocumentLengthCheck ON -JSONMaxDocumentLength 30 -
    JSONMaxContainerDepthCheck ON -JSONMaxContainerDepth 3
    JSONMaxObjectKeyCountCheck ON -JSONMaxObjectKeyCount 4 -
    JSONMaxObjectKeyLengthCheck ON -JSONMaxObjectKeyLength 10 -
    JSONMaxArrayLengthCheck ON -JSONMaxArrayLength 5 -
    JSONMaxStringLengthCheck ON -JSONMaxStringLength 30
<!--NeedCopy-->
```

Exemples de charges utiles, de messages de journal et de compteurs :

JSONMaxDocumentLength Violation

JSONMaxDocumentLength: 30
Payload: {"a":"A","b":"B","c":"C","d":"D","e":"E"}

Message du journal :

```
Document Length exceeds 20000000 May 29 20:23:32 <local0.info>
    10.217.31.243 05/29/2019:20:23:32 GMT 0-PPE-0 : default APPFW
    APPFW_JSON_DOS_MAX_DOCUMENT_LENGTH 136 0 : 10.217.32.134 114-PPE0 -
    profjson http://10.217.30.120/forms/login.html Document exceeds
    maximum document length (30). cn1=30467 cn2=115 cs1=profjson cs2=
    PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Compteurs :

```
1 0 6 as_viol_json_dos
2 0 3 as_viol_json_dos_max_document_length
```



```
3 0 6 as_log_json_dos
4 0 3 as_log_json_dos_max_document_length
5 0 6 as_viol_json_dos_profile appfw__(profile1)
6 0 3 as_viol_json_dos_max_document_length_profile appfw__(profile1)
7 0 6 as_log_json_dos_profile appfw__(profile1)
8 0 3 as_log_json_dos_max_document_length_profile appfw__(profile1)
9 <!--NeedCopy-->
```

JSONMaxContainerDepth Violation

JSONMaxContainerDepth: 3
Payload: {“a”: {”b”: {“c”: {“d”: { ”e” : “f” }}}}}

Message du journal :

```
1 May 29 19:33:59 <local0.info> 10.217.31.243 05/29/2019:19:33:59 GMT 0-
    PPE-1 : default APPFW APPFW_JSON_DOS_MAX_CONTAINER_DEPTH 4626 0 :
    10.217.31.247 22-PPE1 - profjson http://10.217.30.120/forms/login.
    html Document at offset (15) exceeds maximum container depth (3).
    cn1=30466 cn2=113 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=
    blocked
2 <!--NeedCopy-->
```

Compteurs :

```
1 36 20999 7 1 0 as_viol_json_dos
2 37 0 6 1 0 as_viol_json_dos_max_container_depth
3 38 0 7 1 0 as_log_json_dos
4 39 0 6 1 0 as_log_json_dos_max_container_depth
5 40 0 7 1 0 as_viol_json_dos_profile appfw__(profile1)
6 41 0 6 1 0 as_viol_json_dos_max_container_depth_profile appfw__(
    profile1)
7 42 0 7 1 0 as_log_json_dos_profile appfw__(profile1)
8 43 0 6 1 0 as_log_json_dos_max_container_depth_profile appfw__(profile1
    )
9 <!--NeedCopy-->
```

JSONMaxObjectKeyCount Violation

JSONMaxObjectKeyCount: 4

Payload: {“a”: ”A”, “b”: “B”, “c”:“C”, “d” :“D”, ”e” : “E” }

Message du journal :


```
May 30 19:42:41 <local0.info> 10.217.31.243 05/30/2019:19:42:41 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_COUNT 457 0 : 10.217.32.134 219-PPE1 - profjson http://10.217.30.120/forms/login.html Object at offset (41) that exceeds maximum key count (4). cn1=30468 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Compteurs :

```
94 119105 15 1 0 as_viol_json_dos
95 0 4 1 0 as_viol_json_dos_max_object_key_count
96 0 15 1 0 as_log_json_dos
97 0 4 1 0 as_log_json_dos_max_object_key_count
98 0 15 1 0 as_viol_json_dos_profile appfw__(profile1)
99 0 4 1 0 as_viol_json_dos_max_object_key_count_profile appfw__(profile1)
100 0 15 1 0 as_log_json_dos_profile appfw__(profile1)
101 0 4 1 0 as_log_json_dos_max_object_key_count_profile appfw__(profile1)
<!--NeedCopy-->
```

JSONMaxObjectKeyLength Violation

JSONMaxObjectKeyLength: 10
Payload: {“a”: ”A”, “b1234567890”: “B”, “c”:“C”, “d” :“D”, ”e” : “E” }

Message du journal :

```
May 31 20:26:10 <local0.info> 10.217.31.243 05/31/2019:20:26:10 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_LENGTH 102 0 : 10.217.32.134 89-PPE1 - profjson http://10.217.30.120/forms/login.html Object key(b1234567890) at offset (12) exceeds maximum key length (10). cn1=30469 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Compteurs :

```
242172 6 1 0 as_viol_json_dos
0 1 1 0 as_viol_json_dos_max_object_key_length
10 0 5 1 0 as_log_json_dos
11 0 1 1 0 as_log_json_dos_max_object_key_length
12 0 6 1 0 as_viol_json_dos_profile appfw__(profile1)
```



```
13 0 1 1 0 as_viol_json_dos_max_object_key_length_profile appfw__(
   profile1)
14 0 5 1 0 as_log_json_dos_profile appfw__(profile1)
15 0 1 1 0 as_log_json_dos_max_object_key_length_profile appfw__(
   profile1)
<!--NeedCopy-->
```

Violation JSONMaxArrayLength

JSONMaxArrayLength: 5

Payload: {“a”: ”A”, “c”:[”d”,”e”,”f”,”g”,”h”,”i”],”e”:[“E”,”e”]}

Message du journal :

```
May 29 20:58:39 <local0.info> 10.217.31.243 05/29/2019:20:58:39 GMT 0-
   PPE-1 : default APPFW APPFW_JSON_DOS_MAX_ARRAY_LENGTH 4650 0 :
   10.217.32.134 153-PPE1 -profjson http://10.217.30.120/forms/login.
   html Array at offset (37) that exceeds maximum array length (5). cn1
   =30469 cn2=120 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Compteurs :

```
36 182293 10 1 0 as_viol_json_dos
37 0 1 1 0 as_viol_json_dos_max_array_length
38 0 10 1 0 as_log_json_dos 39 0 1 1 0 as_log_json_dos_max_array_length
40 0 10 1 0 as_viol_json_dos_profile appfw__(profile1)
41 0 1 1 0 as_viol_json_dos_max_array_length_profile appfw__(profile1)
42 0 10 1 0 as_log_json_dos_profile appfw__(profile1)
43 0 1 1 0 as_log_json_dos_max_array_length_profile appfw__(profile1))
<!--NeedCopy-->
```

JSONMaxStringLength Violation

JSONMaxStringLength: 10

Payload: {“a”: ”A”, “c”:”CcCcCcCcCcCcCcCcCc”,”e”:[“E”,”e”]}

Message du journal :

```
May 29 20:05:02 <local0.info> 10.217.31.243 05/29/2019:20:05:02 GMT 0-
   PPE-0 : default APPFW APPFW_JSON_DOS_MAX_STRING_LENGTH 134 0 :
   10.217.32.134 80-PPE0 - profjson http://10.217.30.120/forms/login.
   html String(CcCcCcCcCcCcCc) at offset (27) that exceeds maximum
   string length (10). n1=30470 cn2=122 cs1=profjson cs2=PPE0 cs4=ALERT
    cs5=2019 act=blocked
```



```
<!--NeedCopy-->
```

Compteurs :

```
44 91079 3 1 0 as_viol_json_dos
45 0 1 1 0 as_viol_json_dos_max_string_length
46 0 3 1 0 as_log_json_dos
47 0 1 1 0 as_log_json_dos_max_string_length
48 0 3 1 0 as_viol_json_dos_profile appfw__(profile1)
49 0 1 1 0 as_viol_json_dos_max_string_length_profile appfw__(profile1)
50 0 3 1 0 as_log_json_dos_profile appfw__(profile1)
51 0 1 1 0 as_log_json_dos_max_string_length_profile appfw__(profile1
<!--NeedCopy-->
```

Configuration de la protection DoS JSON à l'aide de l'interface graphique

Suivez la procédure ci-dessous pour définir les paramètres de protection JSON DoS.

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.
2. Sur la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Contrôles de sécurité sous Paramètres avancés**.
4. Dans la section **Vérifications de sécurité**, accédez aux paramètres **de déni de service JSON** .
5. Cliquez sur l'icône exécutable à côté de la case à cocher.



6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres de déni de service JSON** .
7. Sélectionnez l'action DoS JSON.
8. Cliquez sur **OK**.



9. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Règles de relaxation** sous Paramètres **avancés**.
10. Dans la section **Règles de relaxation**, sélectionnez Paramètres **de déni de service JSON** et cliquez sur **Modifier**.



11. Dans la **vérification du déni de service JSON du pare-feu d'application**, définissez les valeurs de validation de déni de service JSON.
12. Cliquez sur **OK**.



13. Sur la page de **profil du NetScaler Web App Firewall**, cliquez sur Paramètres du **profil sous Paramètresavancés**.
14. Dans la section **Paramètres du profil**, accédez à la sous-section **Paramètres d'erreur JSON** pour définir la page **d'erreur de déni de service JSON** .



15. Dans la **page d'erreur JSON Importer un objet**, définissez les paramètres suivants :

    a) Importer depuis. Importez la page d'erreur sous forme de texte, de fichier ou d'URL.
    b) URL. URL pour rediriger l'utilisateur vers la page d'erreur.
    1 fichier. Sélectionnez un fichier à importer en tant que fichier d'erreur JSON DoS.
    c) Texte. Entrez le contenu du fichier JSON.
    d) Cliquez sur Continuer.
    e) Dossier. Entrez le nom du fichier.
    f) Contenu du fichier. Ajoutez le contenu du fichier d'erreur.
    g) Cliquez sur **OK**.



16. Cliquez sur **OK**.
17. Cliquez sur **Terminé**.

Vérification de la protection par injection SQL JSON

May 5, 2023

Une requête JSON entrante peut recevoir une injection SQL sous la forme de chaînes de requête SQL partielles ou de commandes non autorisées dans le code. Cela entraîne le vol de données de la base de données JSON de vos serveurs Web. À la réception d'une telle demande, l'appliance bloque cette demande afin de protéger vos données.

Imaginons un scénario dans lequel un client envoie une requête SQL JSON à une appliance NetScaler, l'analyseur JSON analyse la charge utile de la demande et, si une injection SQL est observée, l'appliance applique des contraintes sur le contenu JSON SQL. La contrainte impose une limite de taille à la requête SQL JSON. Par conséquent, si une injection SQL JSON est observée, l'appliance applique une action et répond par la page d'erreur SQL JSON.

Configurer la protection par injection SQL JSON

Pour configurer la protection SQL JSON, vous devez effectuer les étapes suivantes :

1. Ajoutez un profil de pare-feu d'application au format JSON.
2. Définition du profil de pare-feu d'application pour les paramètres d'injection SQL JSON
3. Configurez l'action SQL JSON en liant le profil de pare-feu d'application.

Ajouter un profil de pare-feu d'application de type JSON

Vous devez d'abord créer un profil qui spécifie comment le pare-feu d'application doit protéger votre contenu Web JSON contre les attaques par injection SQL JSON.
À l'invite de commande, tapez :

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> *Remarque* :
>
> Lorsque vous définissez le type de profil sur JSON, les autres vérifications telles que HTML ou XML ne s'appliquent pas.

Exemple

```
add appfw profile profile1 -type JSON
```

Configurer l'action d'injection SQL JSON

Vous devez configurer une ou plusieurs actions d'injection SQL JSON pour protéger votre application contre les attaques par injection JSON SQL.
À l'invite de commande, tapez :

```
set appfw profile <name> - JSONSQLInjectionAction [block] [log] [stats] [
none]
```

Les actions d'injection SQL sont les suivantes :
Bloquer - Bloquer les connexions qui violent ce contrôle de sécurité.
Journal - Consigner les violations de cette vérification de sécurité.
Stats - Générez des statistiques pour cette vérification de sécurité.
Aucun : désactivez toutes les actions pour ce contrôle de sécurité.

Configurer le type d'injection SQL JSON

Pour configurer le type d'injection SQL JSON sur un profil de pare-feu d'application, à l'invite de commandes, tapez :

```
set appfw profile <name> - JSONSQLInjectionType <JSONSQLInjectionType>
```

Exemple

```
set appfw profile profile1 -JSONSQLInjectionType SQLKeyword
```

Où sont les types d'injection SQL
disponibles : Types d'injection SQL disponibles.

SQLSplChar. Vérifie les caractères spéciaux SQL,
SQLKeyword. Vérifie les mots-clés SQL.
SQLSplCharANDKeyword. Vérifie à la fois les blocs et s'ils sont trouvés.
SQLSplCharORKeyword. . Bloque si un caractère spécial SQL ou un mot-clé spl est trouvé.
Valeurs possibles : SqlSplChar, SQLKeyword, SqlSplCharOrKeyword, SqlSplCharAndKeyword.

> *Remarque* :
> Pour activer une ou plusieurs actions, tapez « set appfw profile - JSONSQLinjectionAction » suivi des actions à activer.

Exemple

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

L'exemple suivant montre un exemple de charge utile, le message de journal correspondant et les compteurs de statistiques :

```
Payload:
=======
{

  "test": "data",
  "username": "waf",
  "password": "select * from t1;",
  "details": {

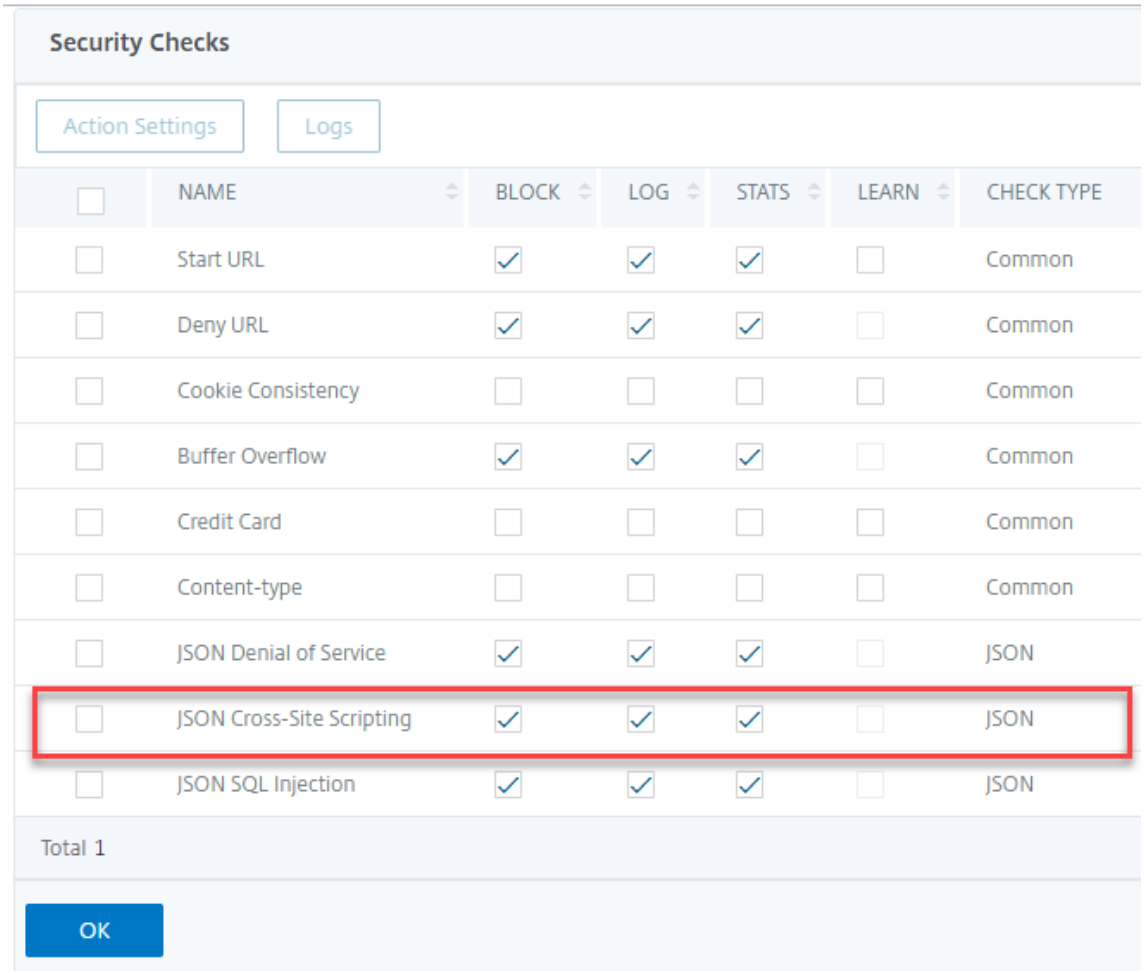
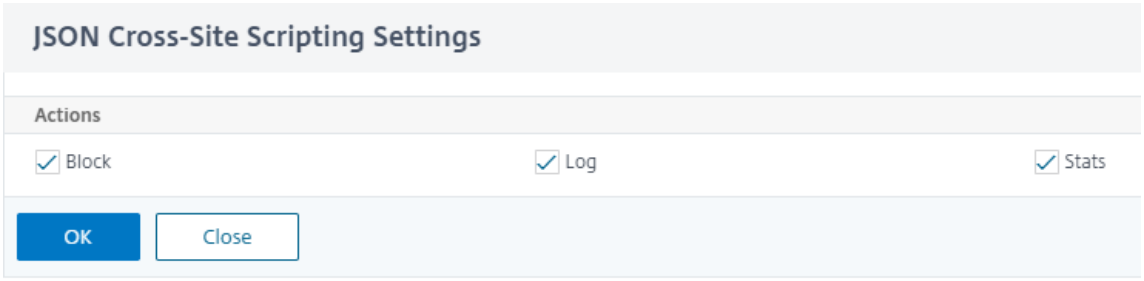
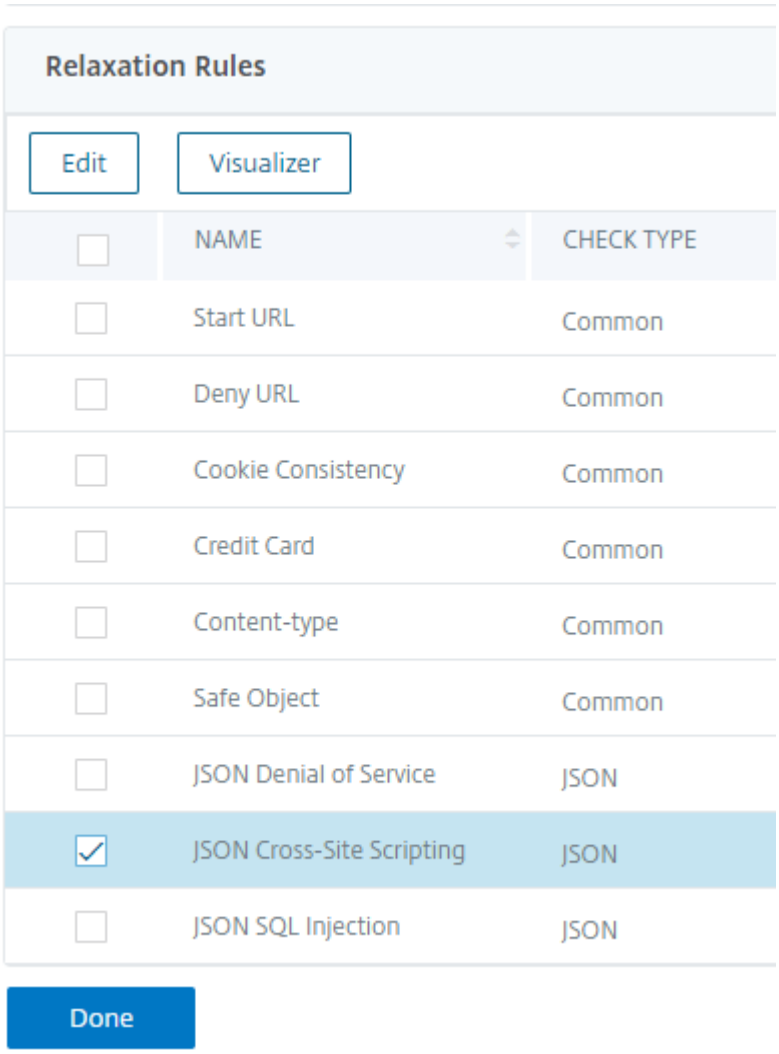
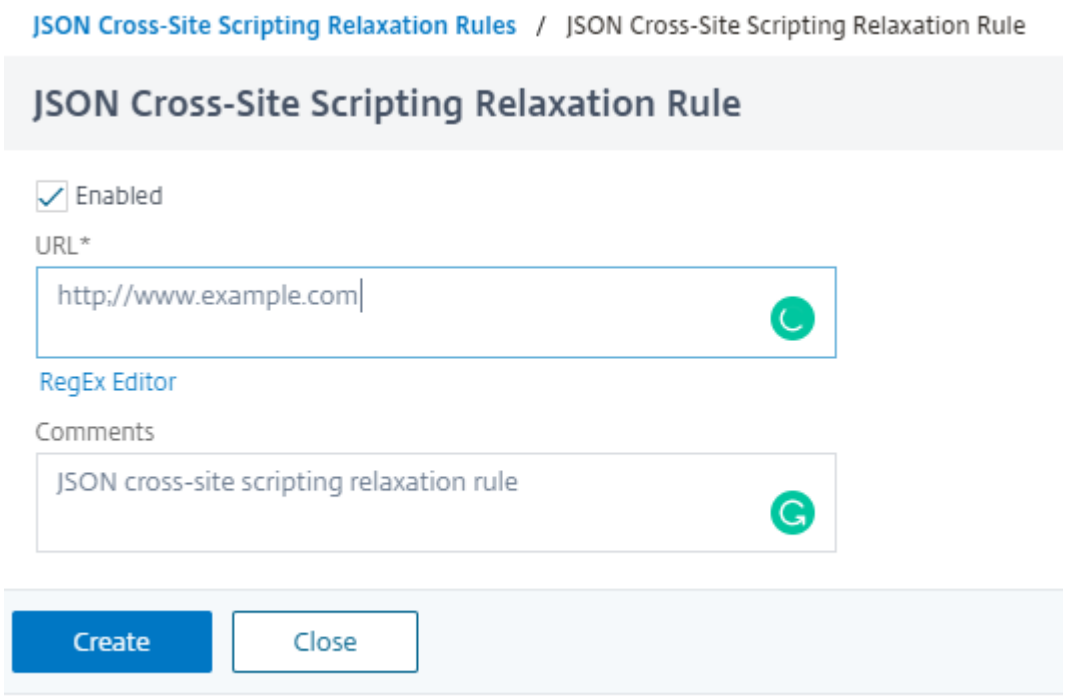
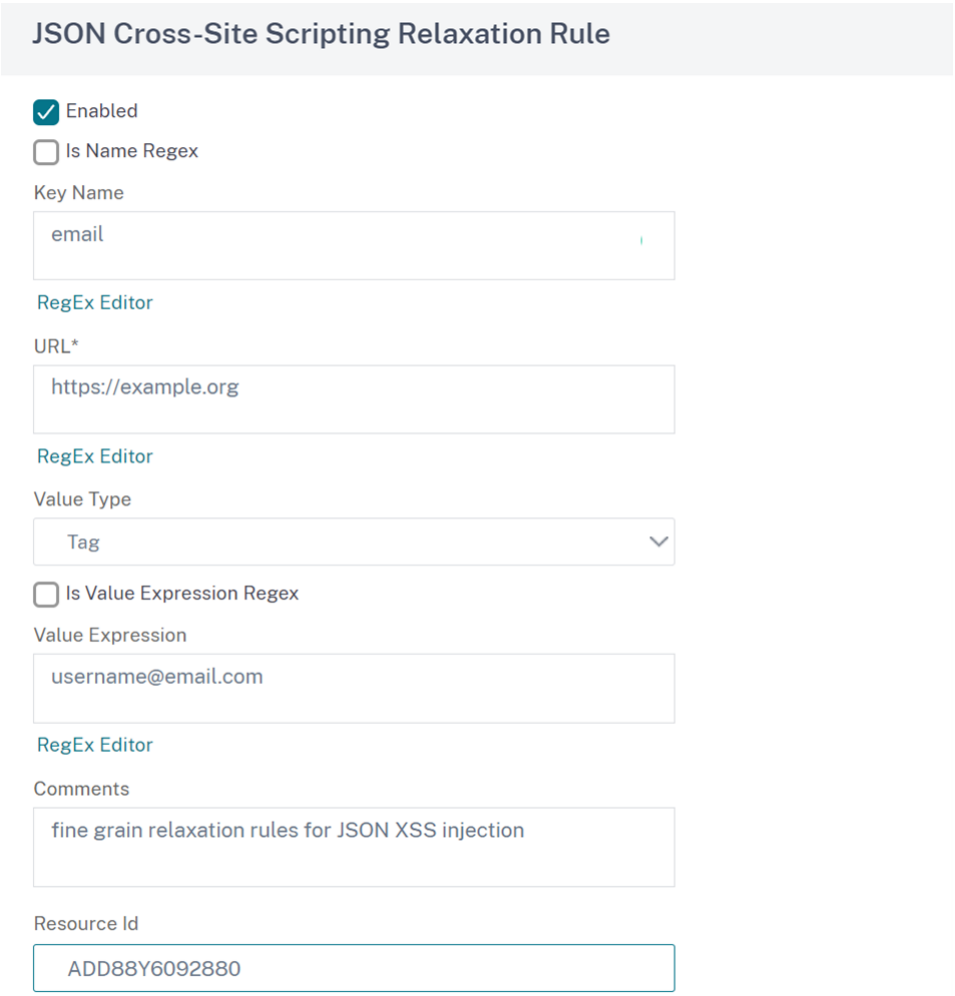
    "surname": "test",
    "age": "23"
   }

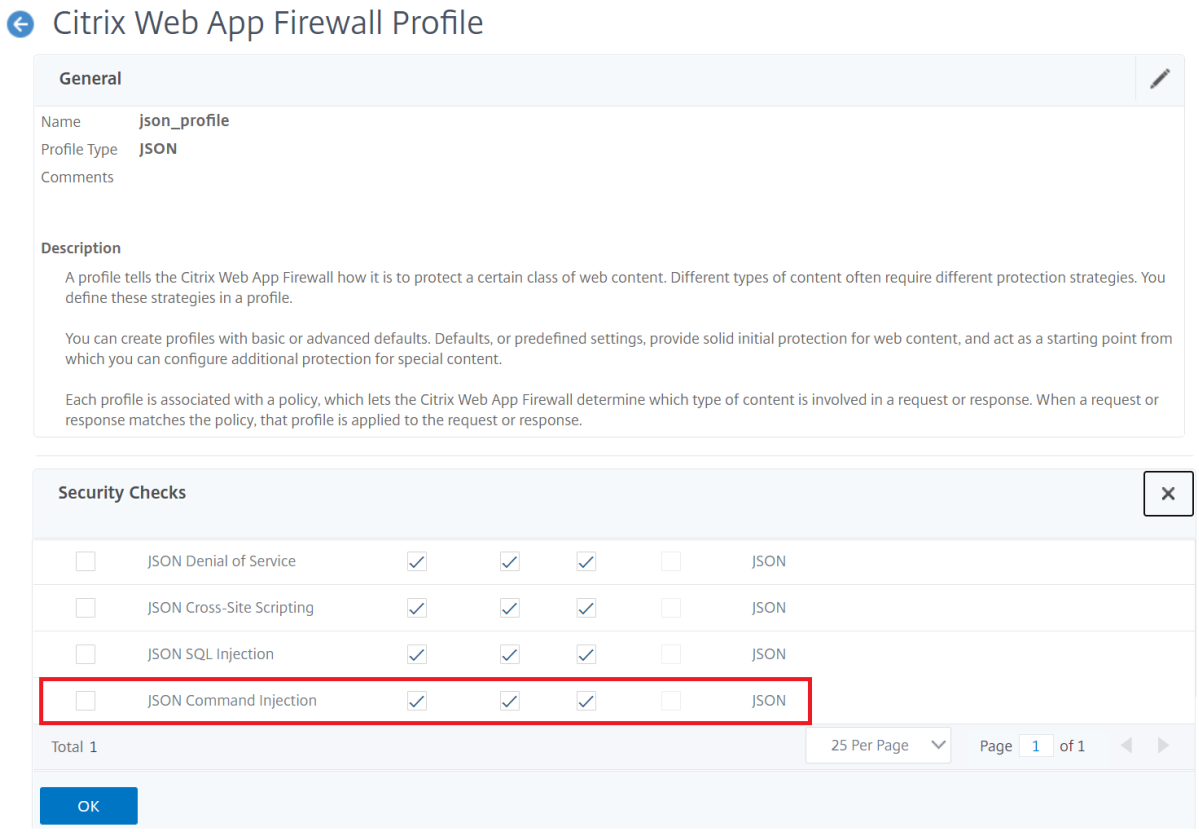
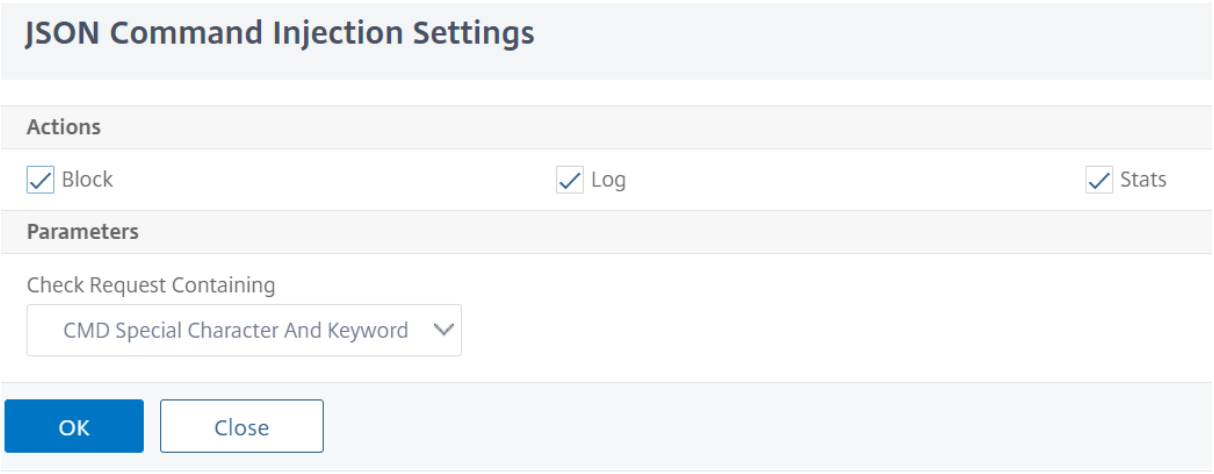
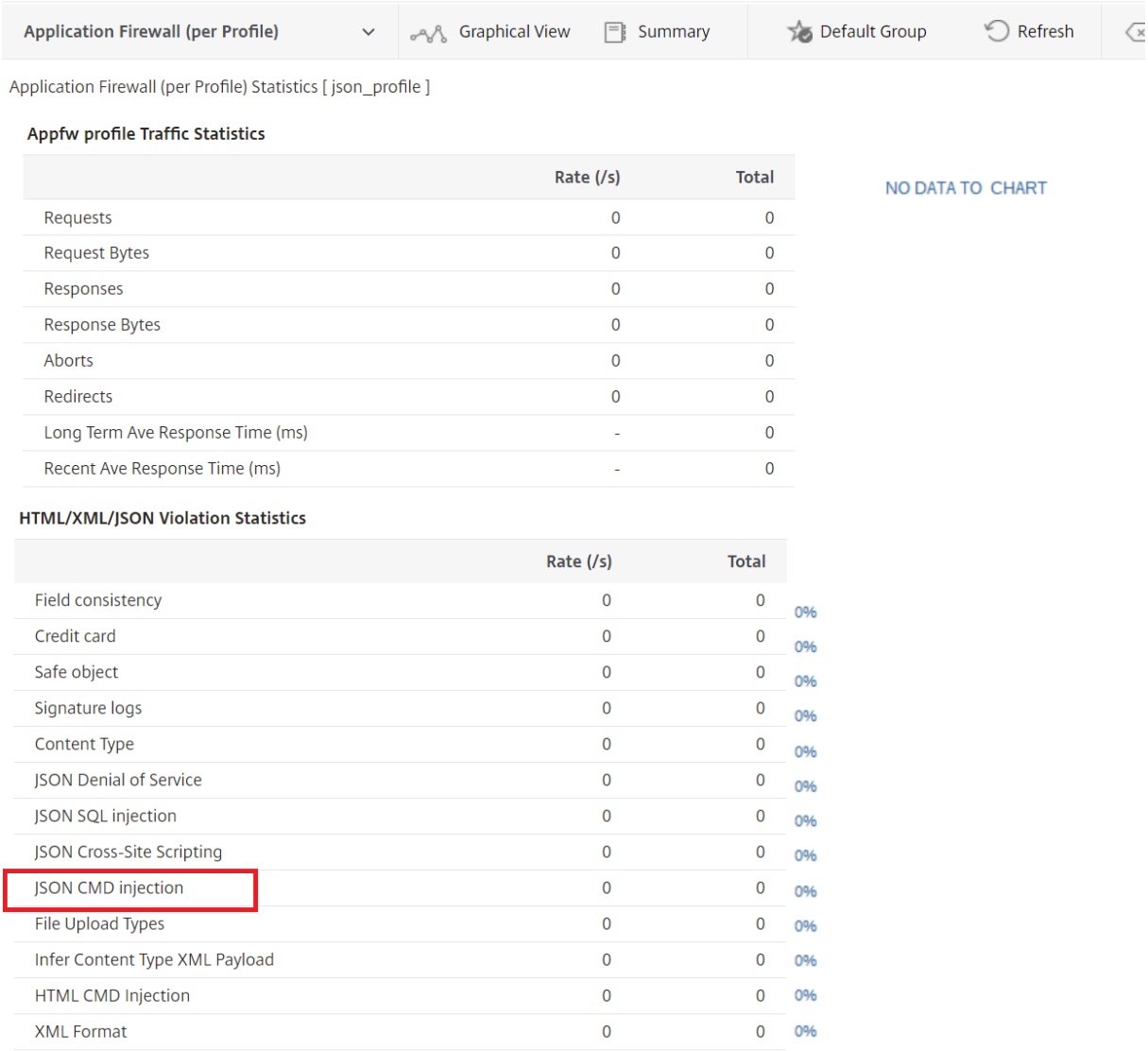
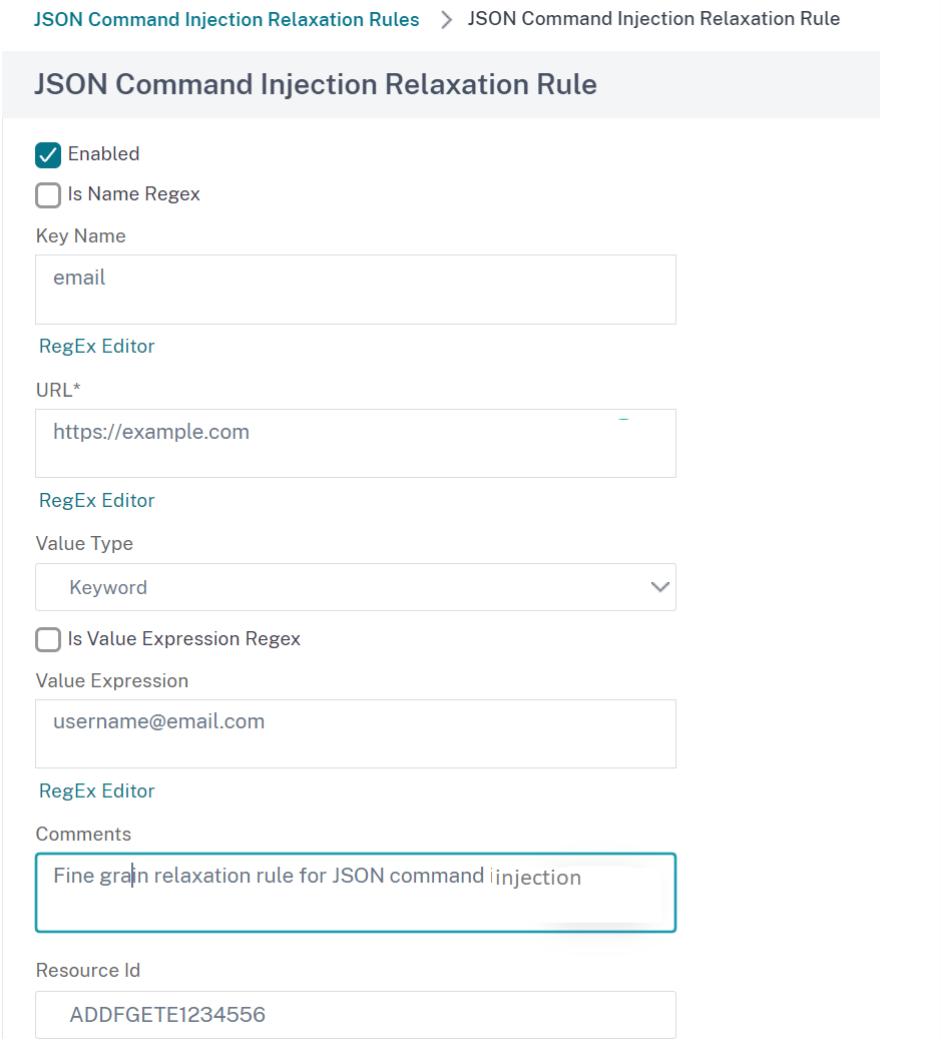
 }

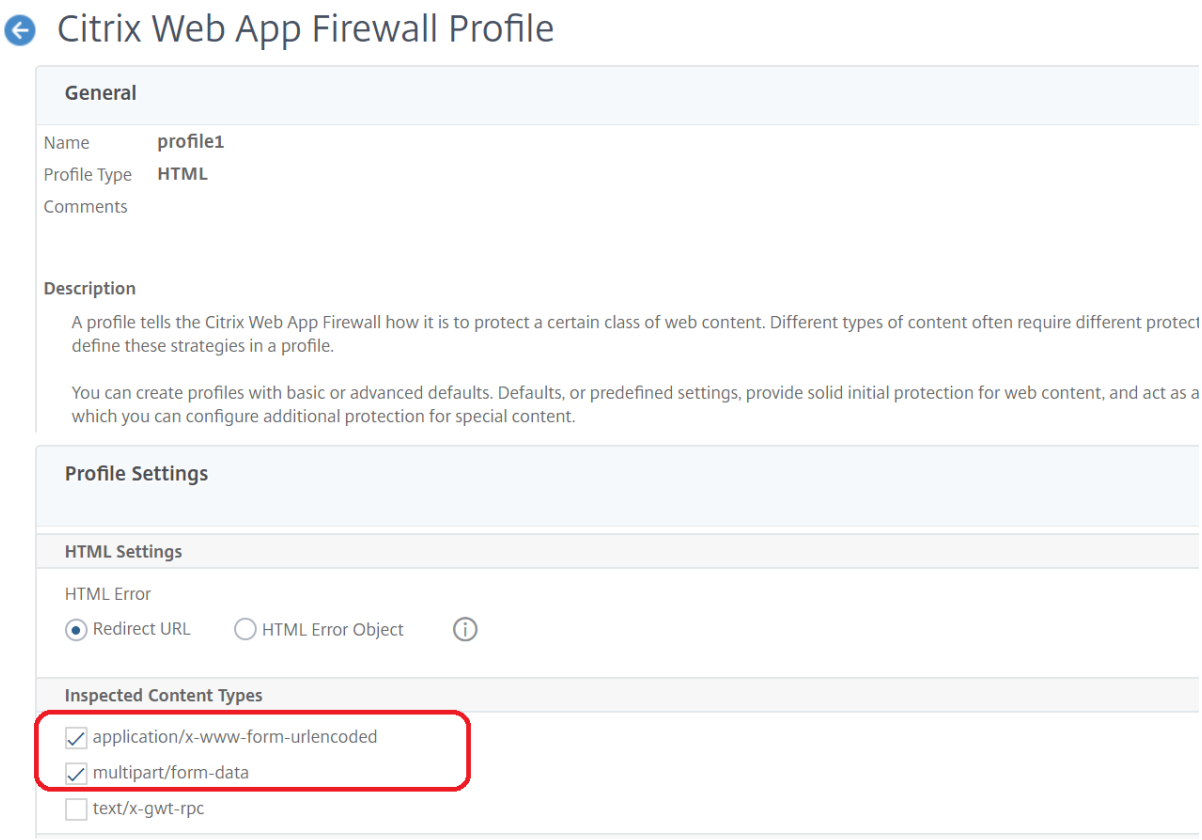
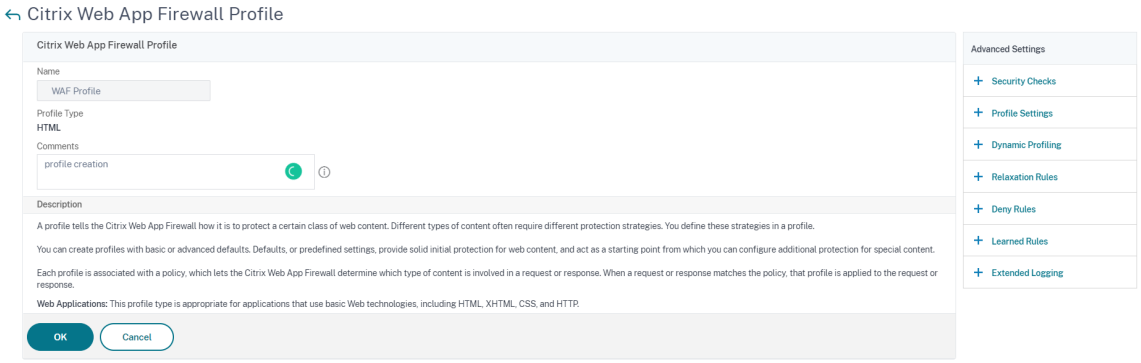
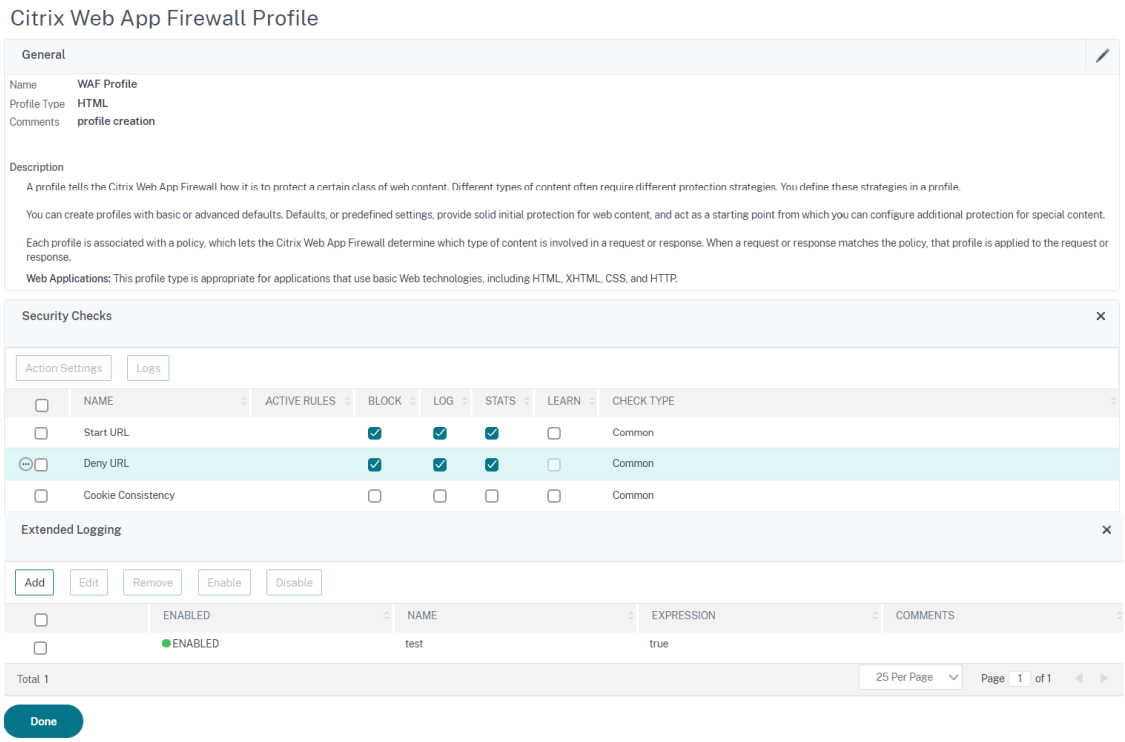
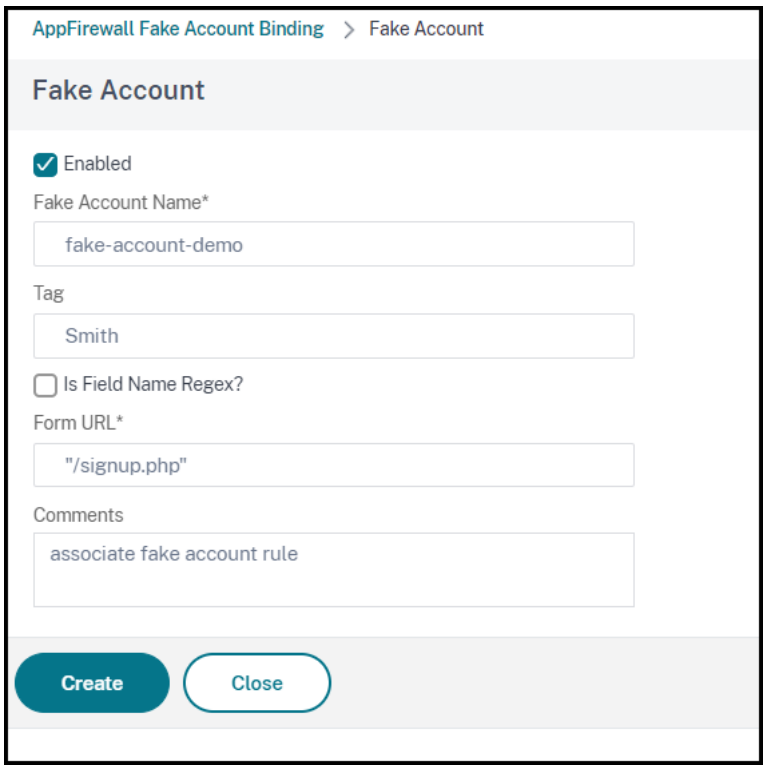
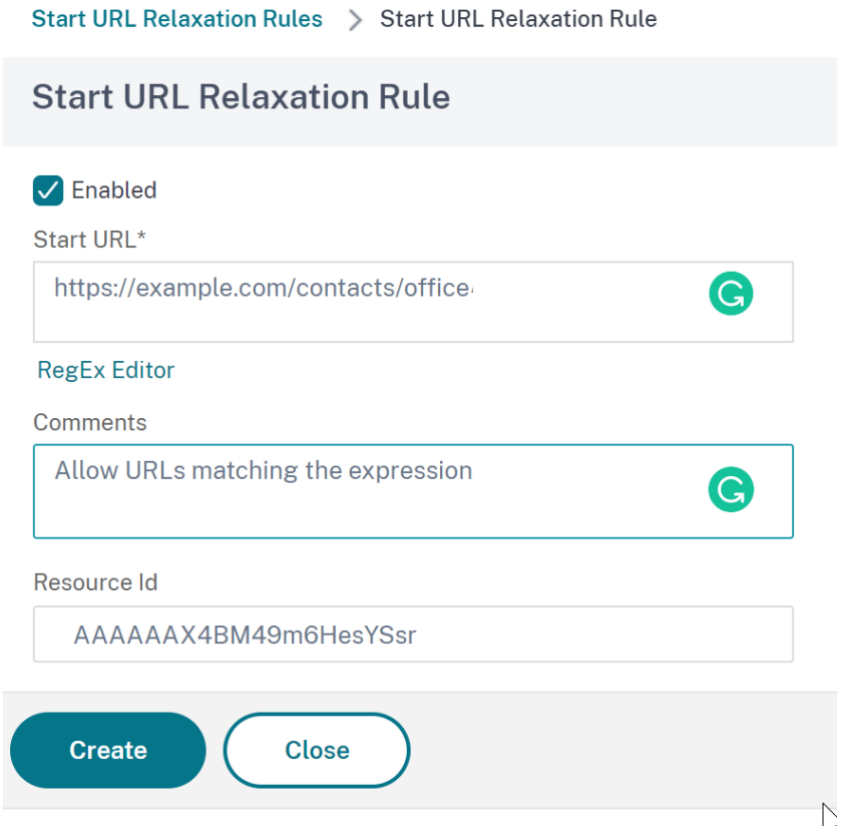
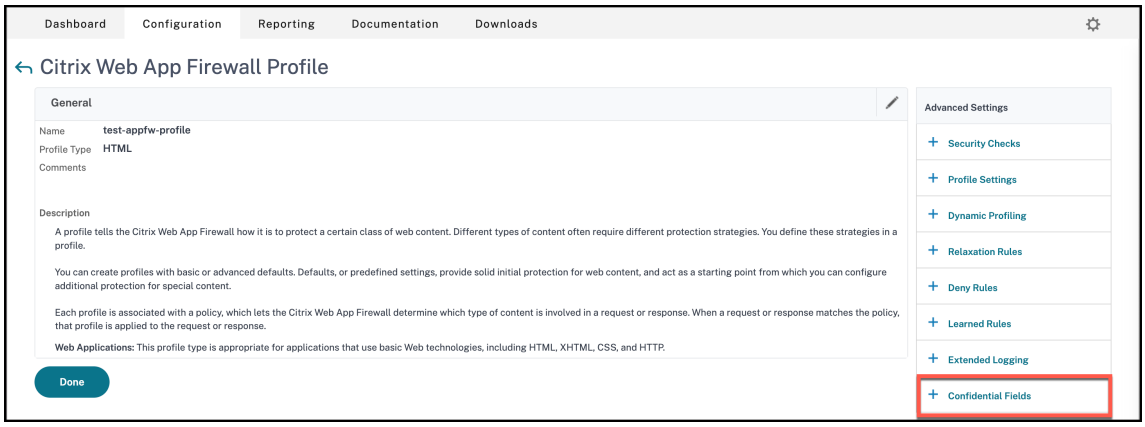
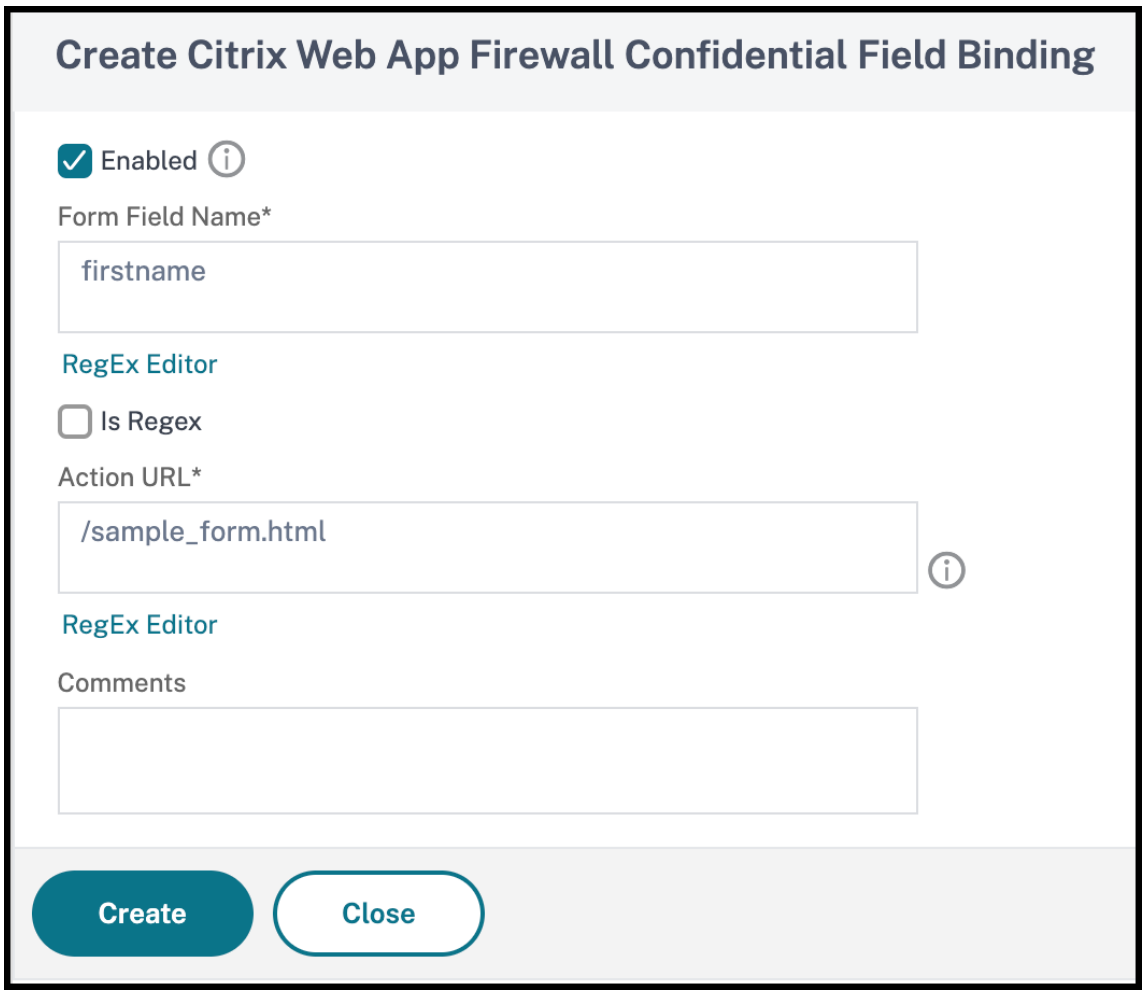
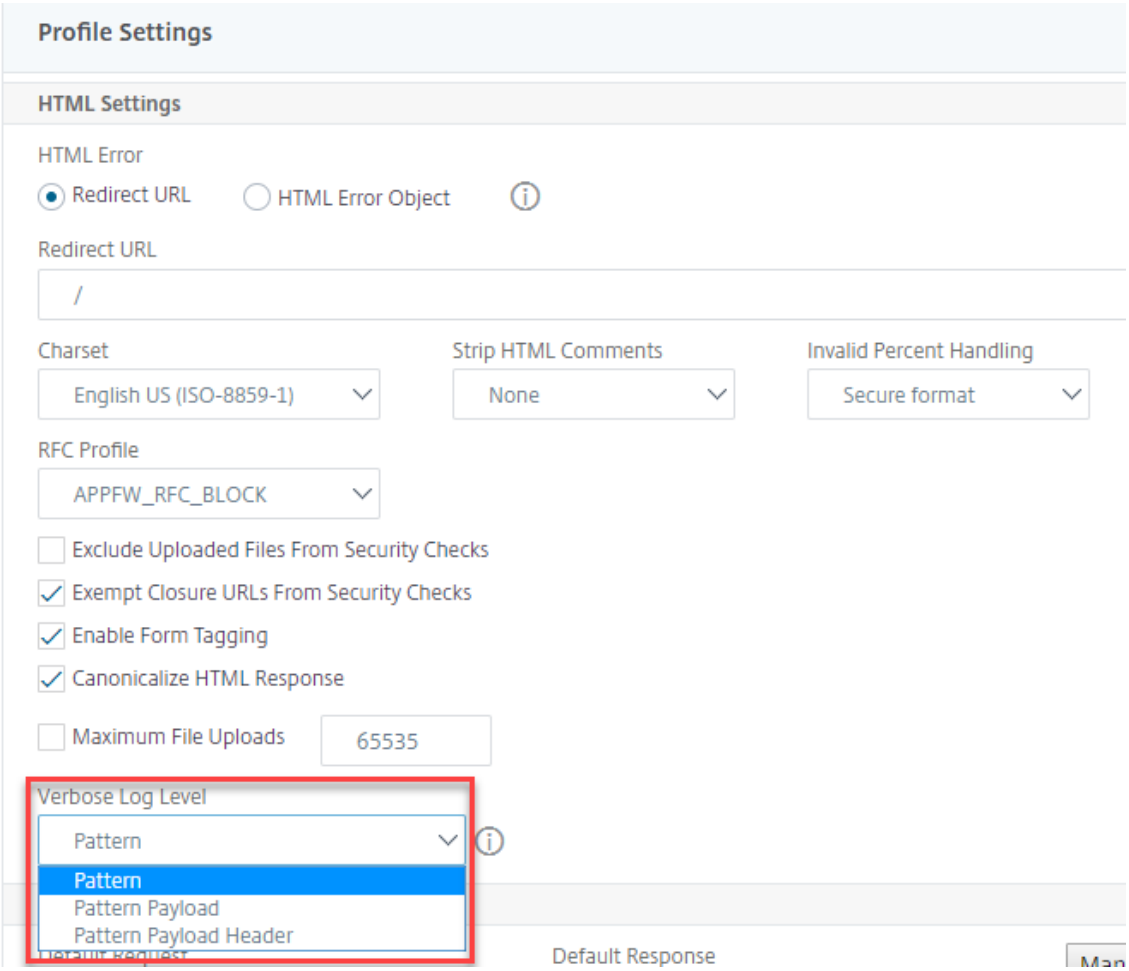
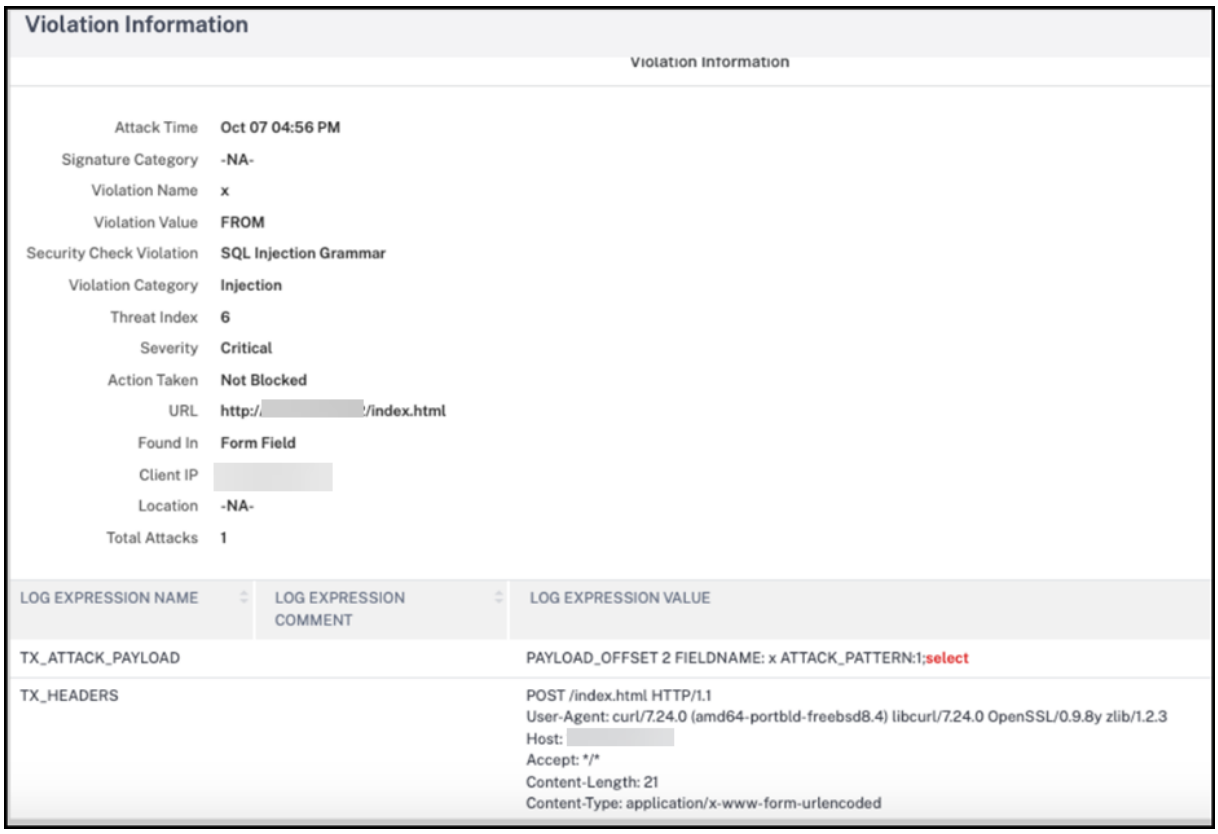
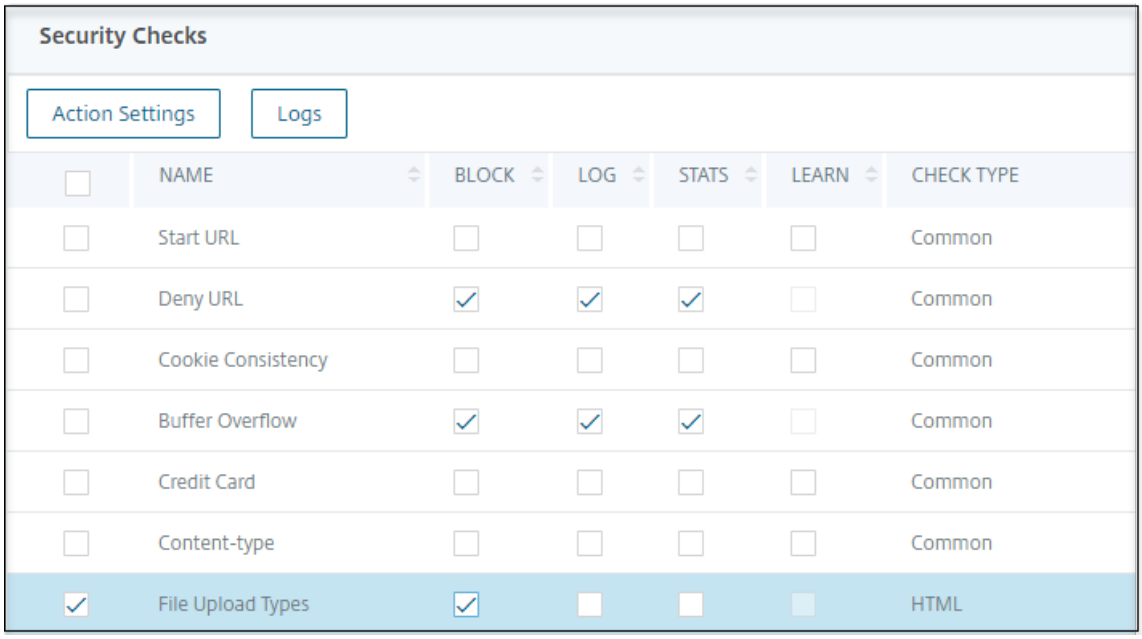
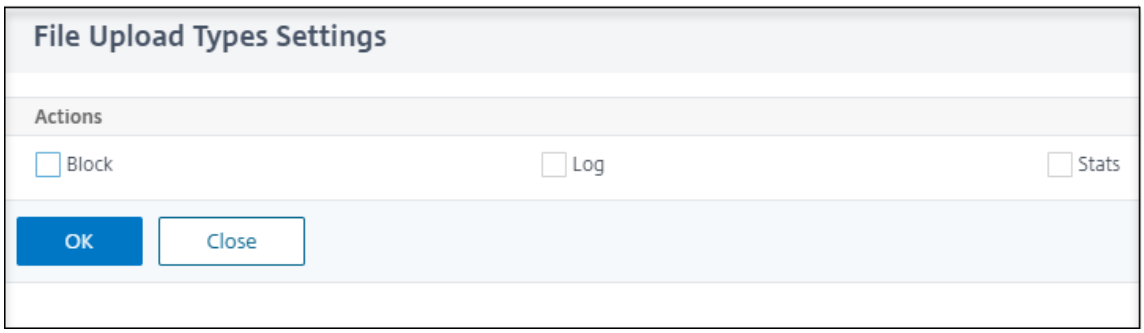
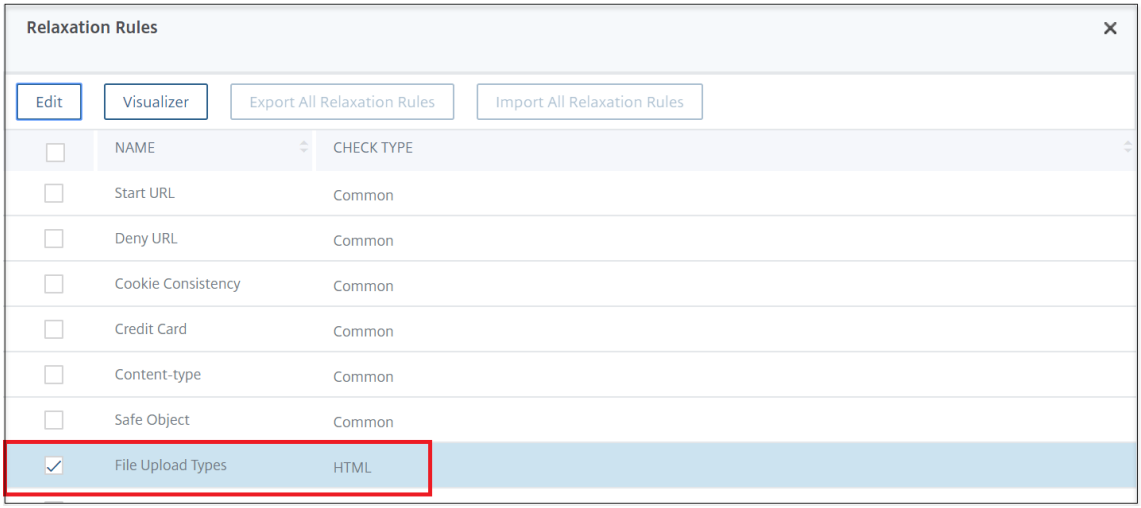
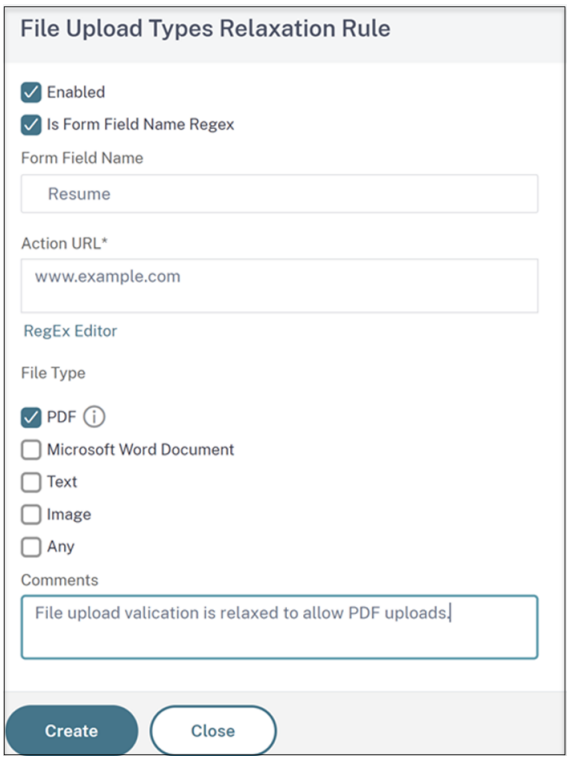
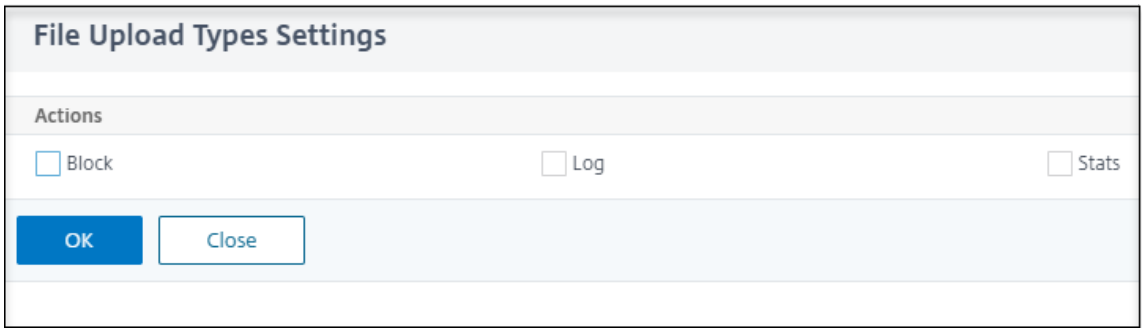
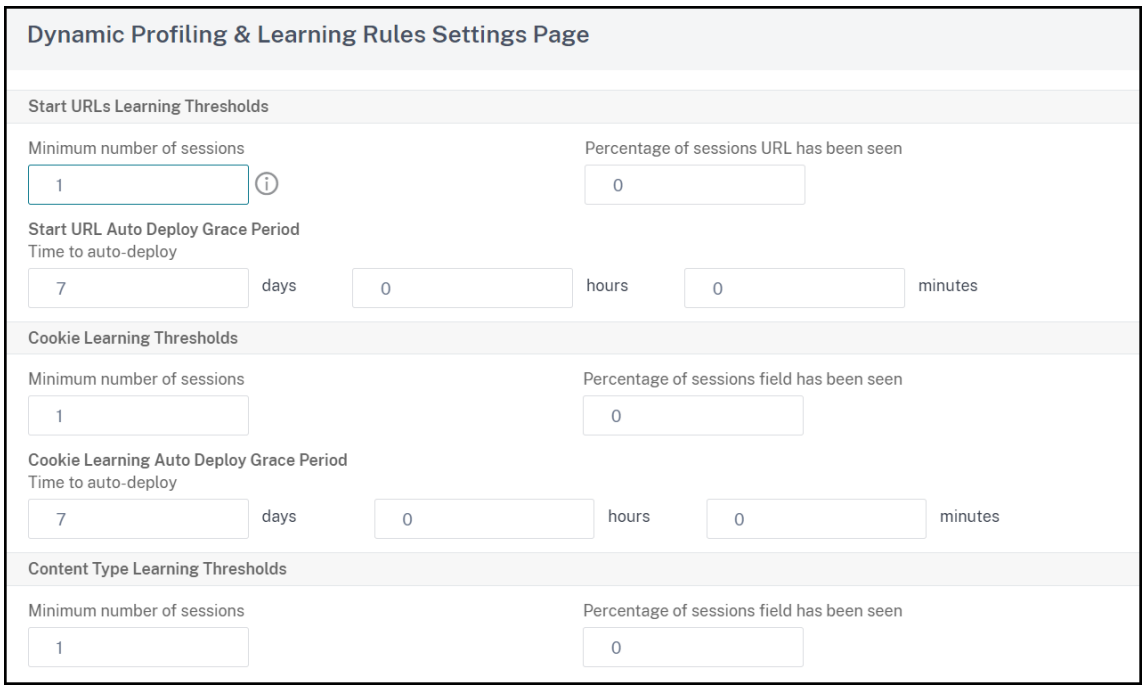
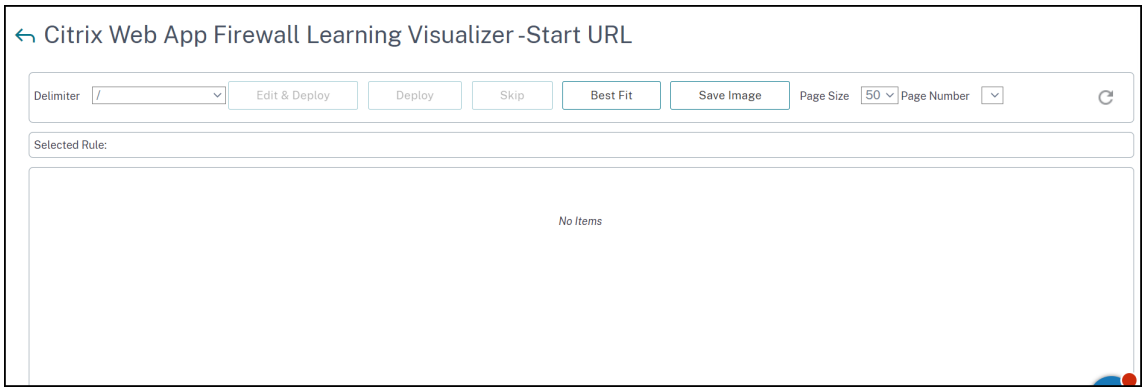

Log Message:
============
08/19/2019:08:49:46 GMT pegasus121 Informational 0-PPE-0 : default
   APPFW APPFW_JSON_SQL 6656 0 :  10.217.32.165 18402-PPE0 - profjson
   http://10.217.32.147/test.html SQL Keyword check failed for object
   value(with violation="select(;)") starting at offset(52) <blocked>
Counters:
========
   1  441083             1 as_viol_json_sql
   3       0             1 as_log_json_sql
   5       0             1 as_viol_json_sql_profile appfw__(profjson)
   7       0             1 as_log_json_sql_profile appfw__(profjson)
```



```
<!--NeedCopy-->
```

Configuration de la protection contre les injections SQL JSON à l'aide de l'interface graphique

Suivez la procédure ci-dessous pour définir les paramètres de protection par injection SQL JSON.

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.
2. Sur la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Contrôles de sécurité** sous Paramètres **avancés**.
4. Dans la section **Vérifications de sécurité**, accédez aux paramètres **d'injection SQL JSON** .
5. Cliquez sur l'icône exécutable située près de la case à cocher.



6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres d'injection JSON SQL**.
7. Sélectionnez les actions **d'injection SQL JSON** .
8. Cliquez sur **OK**.



9. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Règles de relaxation** sous Paramètres **avancés**.
10. Dans la section **Règles de relaxation**, sélectionnez Paramètres **d'injection SQL JSON** et cliquez sur **Modifier**.



11. Sur la page Règle de relaxation par injection SQL JSON, saisissez l'URL à laquelle la demande doit être envoyée. Toutes les demandes envoyées à cette URL ne seront pas bloquées.
12. Cliquez sur **Create**.



Configuration de la relaxation des grains fins pour la protection par injection JSON SQL

Le Web App Firewall vous permet d'assouplir une clé ou une valeur JSON spécifique à partir de la vérification d'inspection par injection SQL basée sur JSON. Vous pouvez configurer plusieurs options pour détendre les charges utiles JSON à l'aide de règles de relaxation de grain fin.

Auparavant, la seule façon de configurer des relaxations pour les contrôles de protection JSON était de spécifier l'URL complète, ce qui contournait la vérification de l'URL complète.

La protection de sécurité SQL basée sur JSON fournit une relaxation pour les éléments suivants :

- Noms des clés
- Valeurs des clés

La vérification de la protection SQL basée sur JSON vous permet de configurer des relaxations qui autorisent des modèles spécifiques et bloquent le reste. Par exemple, le Web App Firewall possède actuellement un ensemble par défaut de plus de 100 mots-clés SQL. Étant donné que les pirates informatiques peuvent utiliser ces mots clés dans des attaques par injection SQL, le Web App Firewall les identifie tous comme des menaces potentielles. Si vous souhaitez assouplir un ou plusieurs mots clés considérés comme sûrs pour un emplacement spécifique, vous pouvez configurer une règle d'assouplissement qui peut contourner le contrôle de sécurité et bloquer le reste. Les commandes utilisées dans les relaxations ont des paramètres facultatifs pour le type de valeur et l'expression de valeur. Vous pouvez spécifier si l'expression de valeur est une expression régulière ou une chaîne littérale. Le type de valeur peut être laissé vide, ou vous pouvez sélectionner Mot-clé ou Chaîne spéciale.

> **Remarque :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation imprudente de caractères génériques, et en particulier du métacaractère ou de la combinaison de caractères génériques points-astérisques (.*), peut avoir des résultats que vous ne souhaitez pas, tels que le blocage de l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou l'autorisation d'une attaque que la vérification d'injection SQL JSON aurait autrement bloquée.

Points à prendre en compte

- L'expression de valeur est un argument facultatif. Le nom d'un champ peut ne pas comporter d'expression de valeur.
- Un nom de clé peut être lié à plusieurs expressions de valeur.
- Les expressions de valeur doivent se voir attribuer un type de valeur. Le type de valeur peut être : 1) Mot-clé, 2) SpecialString.
- Vous pouvez définir plusieurs règles de relaxation par nom de clé ou combinaison d'URL.

Configuration de la relaxation du grain fin JSON pour les attaques par injection de commandes à l'aide de

Pour configurer la règle de relaxation du grain du fichier JSON, vous devez lier les entités de relaxation de grain fin au profil Web App Firewall.

À l'invite de commande, tapez :

```
bind appfw profile <profile name> -jsoncmdURL <URL> -key <key name> -
    isregex <REGEX/NOTREGEX> -valueType <keyword/SpecialString> <value
    Expression> -isvalueRegex <REGEX/NOTREGEX>
<!--NeedCopy-->
```

Exemple :

```
bind appfw profile appprofile1 -jsonsqlurl www.example.com -key
    stn_name  -isRegex NOTREGEX -valueType Keyword  “union”  -
    isvalueRegex NOTREGEX
<!--NeedCopy-->
```

Pour configurer la règle de relaxation fine pour les attaques par injection de commandes basées sur JSON à l'aide de l'interface graphique

1. Accédez à **Pare-feu d'application > Profils**, sélectionnez un profil, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
3. Dans la section **Règles de relaxation**, sélectionnez un enregistrement d' **injection JSON SQL** et cliquez sur **Modifier**.
4. Dans le curseur **Règle de relaxation par injection SQL JSON**, cliquez sur **Ajouter**.
5. Dans la page **Règle de relaxation par injection SQL JSON**, définissez les paramètres suivants.
    a) Activé
    b) Is Name Regex
    c) Nom de la clé
    d) URL
    e) Type de valeur
    f) Commentaires
    g) ID de ressource
6. Cliquez sur **Create**.



Vérification de la protection par script intersite JSON

May 5, 2023

Si une charge utile JSON entrante contient des données de script intersite malveillantes, WAF bloque la demande. Les procédures suivantes expliquent comment configurer cela via les interfaces CLI et GUI.

Configurer la protection par script intersite JSON

Pour configurer la protection par script intersite JSON, vous devez effectuer les étapes suivantes :

1. Ajoutez un profil de pare-feu d'application au format JSON.
2. Configurer l'action de script intersite JSON pour bloquer la charge utile malveillante de script intersite

Ajouter un profil de pare-feu d'application de type JSON

Vous devez d'abord créer un profil qui spécifie comment le pare-feu d'application doit protéger votre contenu Web JSON contre les attaques de script intersite JSON.

À l'invite de commande, tapez :

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> **Remarque** :
>
> Lorsque vous définissez le type de profil sur JSON, les autres vérifications telles que HTML ou XML ne s'appliquent pas.

Exemple

```
add appfw profile profile1 -type JSON
```

Exemple de sortie pour violation de script intersite JSON

```
JSONcross-site scriptingAction: block log stats
Payload: {
 "username":"<a href="jAvAsCrIpT:alert(1)">X</a>","password":"xyz" }


Log message: Aug 19 06:57:33 <local0.info> 10.106.102.21
    08/19/2019:06:57:33 GMT  0-PPE-0 : default APPFW APPFW_JSON_cross-
    site scripting 58 0 :  10.102.1.98 12-PPE0 - profjson http://
    10.106.102.24/ Cross-site script check failed for object value(with
    violation="Bad URL: jAvAsCrIpT:alert(1)") starting at offset(12). <
    blocked>

Counters
    1  357000                  1 as_viol_json_xss
    3  0                       1 as_log_json_xss
    5  0                       1 as_viol_json_xss_profile appfw__(
       profjson)
    7  0                       1 as_log_json_xss_profile appfw__(
       profjson)

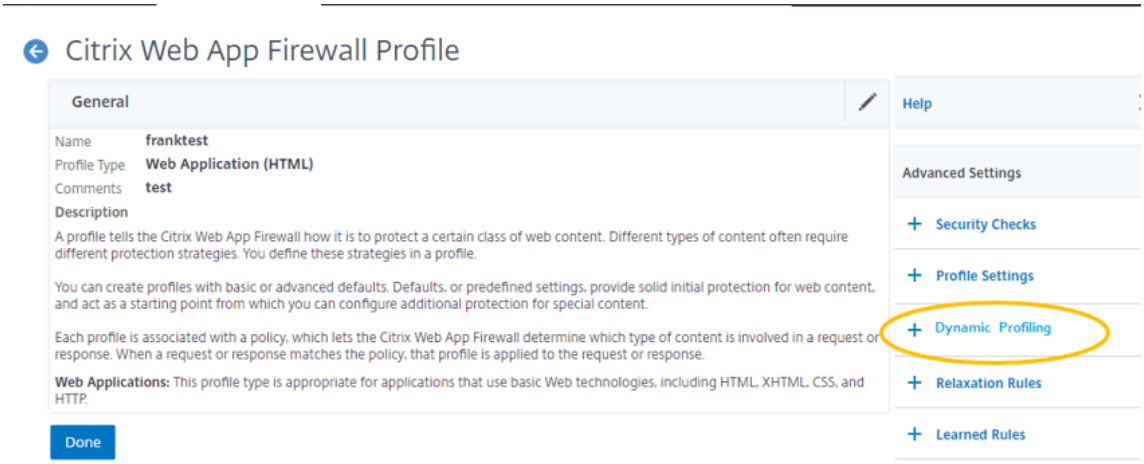
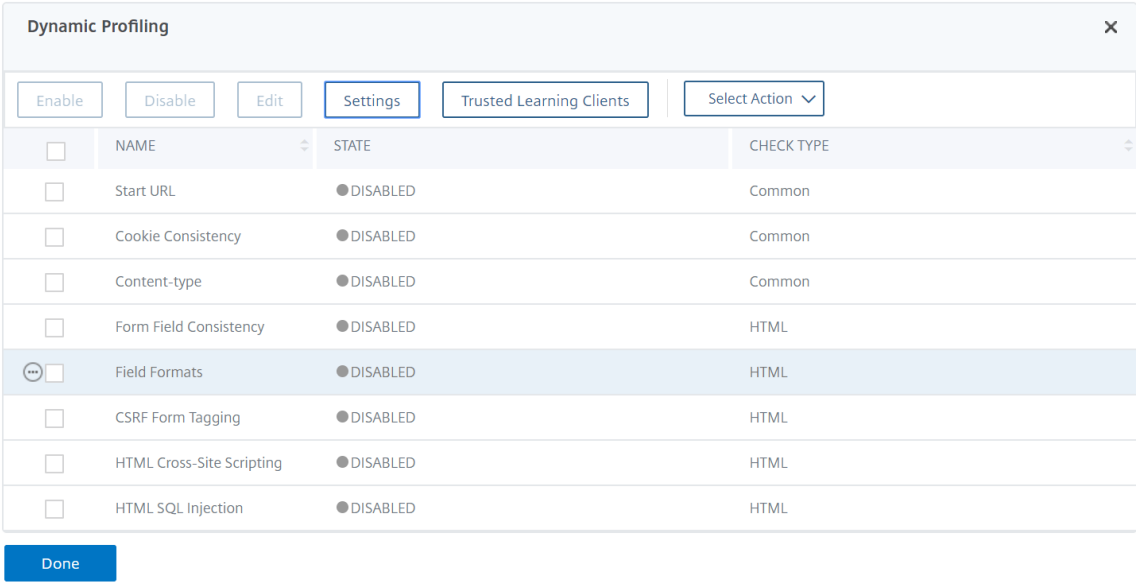
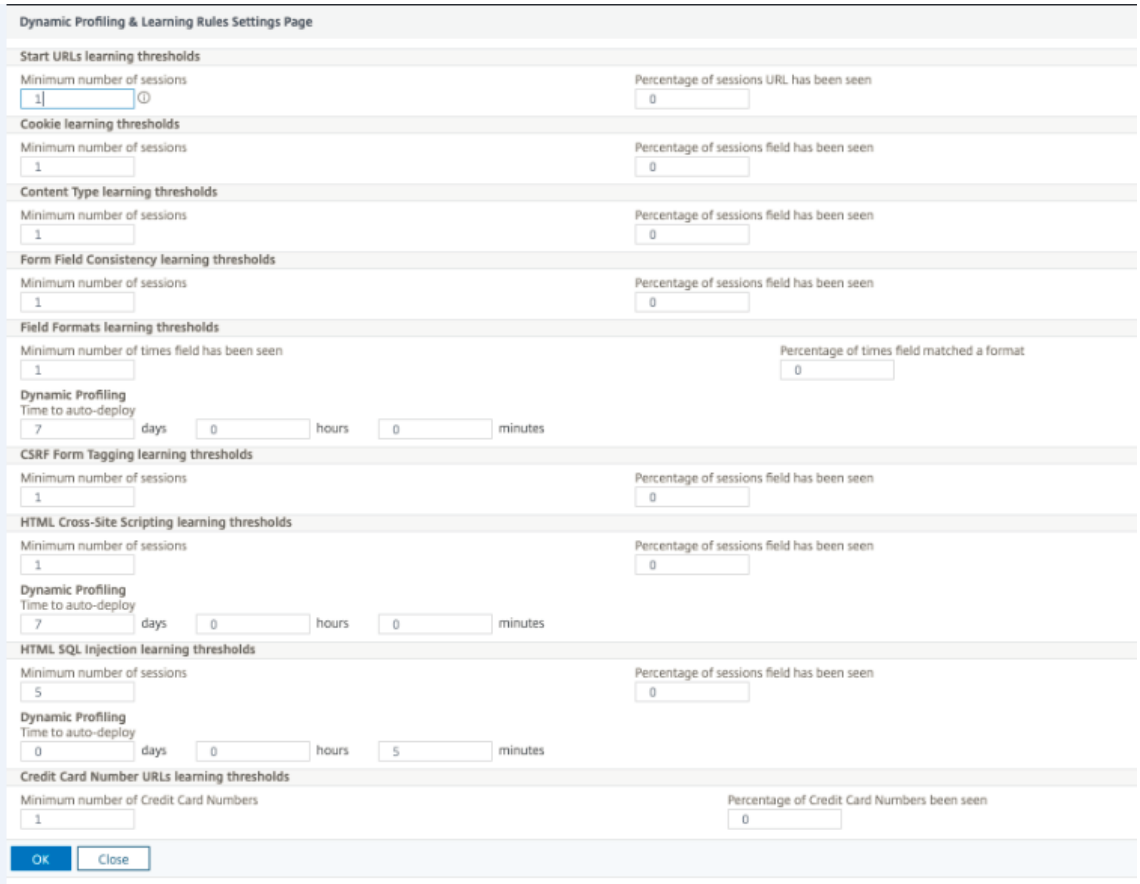
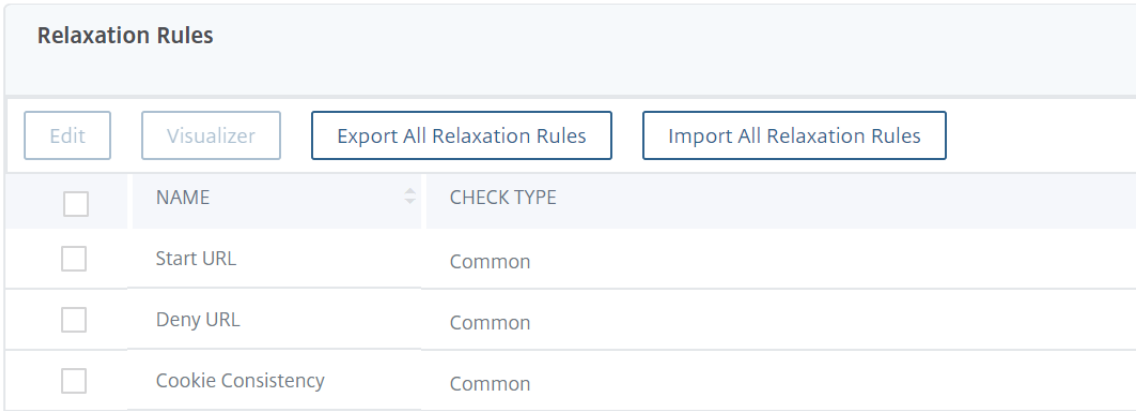
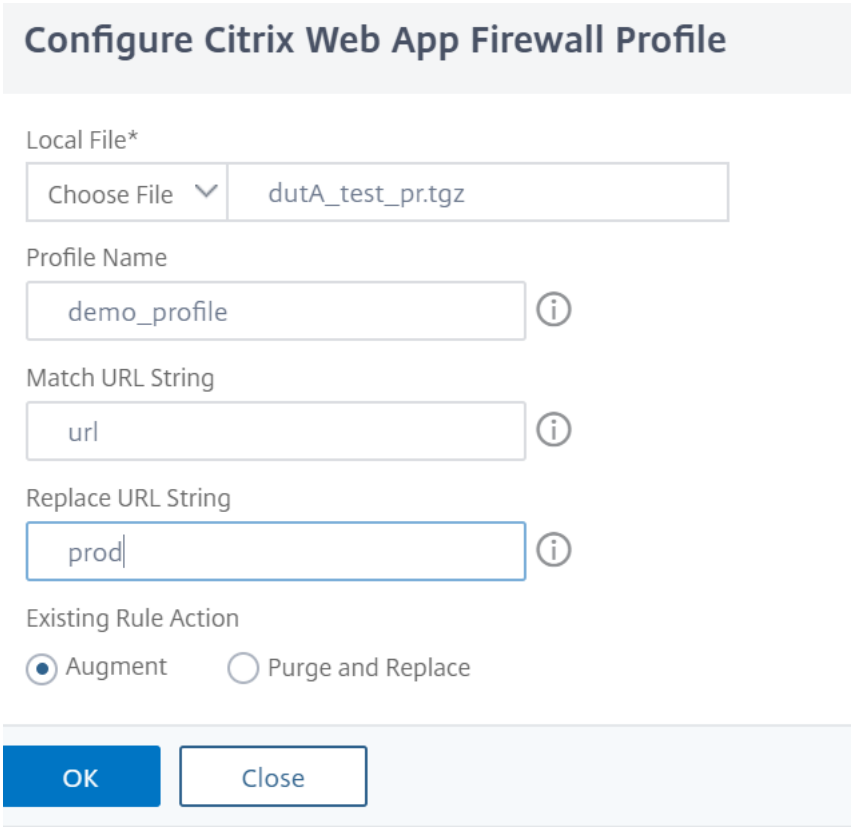
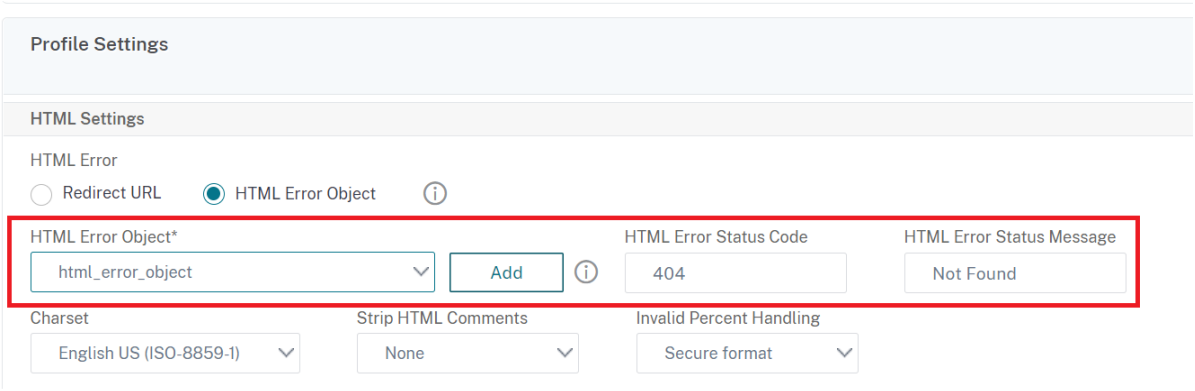
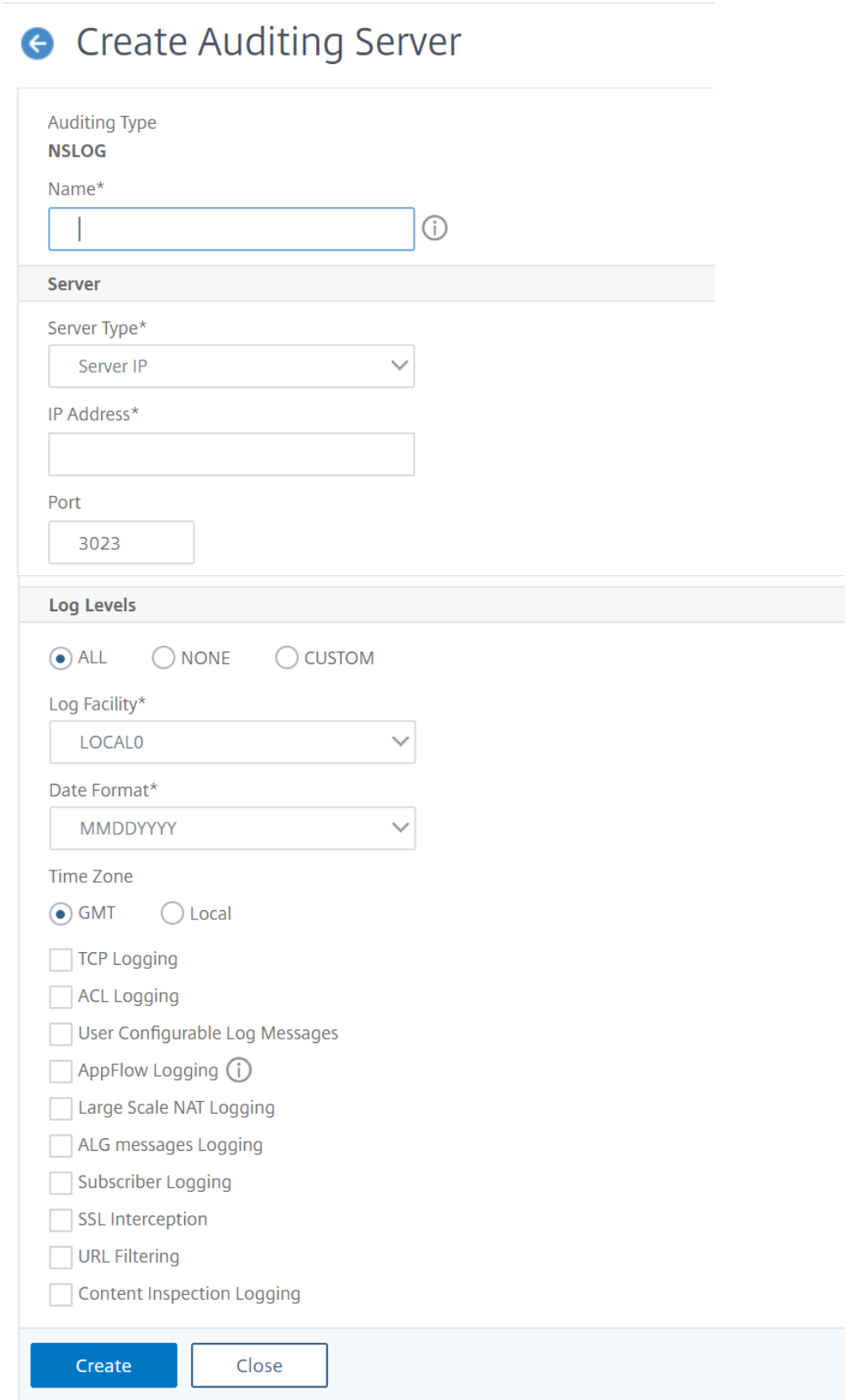
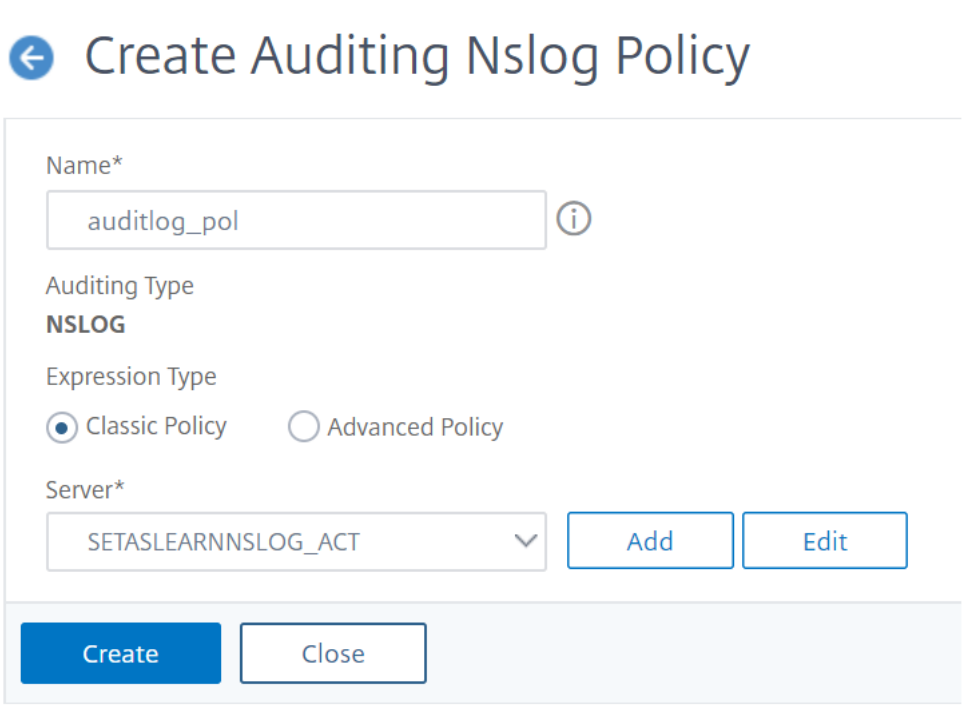
<!--NeedCopy-->
```


Action Configurer les scripts intersites JSON

Vous devez configurer une ou plusieurs actions de script intersite JSON pour protéger votre application contre les attaques de script intersite JSON.
À l'invite de commande, tapez :

```
set appfw profile <name> - JSONcross-site scriptingAction [block] [log] [
stats] [none]
```

Exemple

```
set appfw profile profile1 -JSONcross-site scriptingAction block
```

Les actions de script intersite disponibles sont les suivantes :
Bloquer - Bloquer les connexions qui ne respectent pas ce contrôle de sécurité.
Journal - Consigner les violations de cette vérification de sécurité.
Stats - Générez des statistiques pour cette vérification de sécurité.
Aucun : désactivez toutes les actions pour ce contrôle de sécurité.

> **Remarque** :
> Pour activer une ou plusieurs actions, tapez « set appfw profile - JSONCross-site ScriptingAction » suivi des actions à activer.

Exemple

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

Configurer la protection JSON Cross Site Scripting (cross-site scripting) à l'aide de l'interface graphique

Suivez la procédure ci-dessous pour définir les paramètres de protection par script intersite (script intersite).

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.
2. Sur la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Contrôles de sécurité** sous Paramètres **avancés**.
4. Dans la section **Vérifications de sécurité**, accédez aux paramètres de **script intersite JSON (script intersite)** .
5. Cliquez sur l'icône exécutable à côté de la case à cocher.



6. Cliquez sur **Paramètres d'action** pour accéder à la page **Paramètres de script intersite JSON** .
7. Sélectionnez les actions de script intersite JSON.
8. Cliquez sur **OK**.



9. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Règles de relaxation** sous Paramètres **avancés**.
10. Dans la section **Règles de relaxation**, sélectionnez Paramètres de script intersite JSON et

cliquez sur **Modifier**.



11. Dans la page **Règle de relaxation de script intersite JSON**, cliquez sur **Ajouter** pour ajouter une règle de relaxation de script intersite JSON.
12. Entrez l'URL à laquelle la demande doit être envoyée. Toutes les demandes envoyées à cette URL ne seront pas bloquées.
13. Cliquez sur **Create**.



Configurer la relaxation fine pour les scripts intersites basés sur JSON

Le Web App Firewall vous permet d'assouplir une clé ou une valeur JSON spécifique de la vérification d'inspection par script intersite (XSS) basé sur JSON. Vous pouvez configurer plusieurs options pour détendre les charges utiles JSON à l'aide de règles de relaxation de grain fin.
Auparavant, la seule façon de configurer des relaxations pour les contrôles de protection JSON était de spécifier l'URL complète, ce qui contournait la vérification de l'URL complète.
La protection de sécurité SQL basée sur JSON fournit une relaxation pour les éléments suivants :

- Noms des clés
- Valeurs des clés

La protection par script intersite (XSS) basée sur JSON vous permet de configurer des relaxations qui autorisent des modèles spécifiques et bloquent le reste. Par exemple, le Web App Firewall possède actuellement un ensemble par défaut de plus de 100 mots-clés SQL. Étant donné que les pirates informatiques peuvent utiliser ces mots clés dans des attaques par injection SQL, le Web App Firewall les identifie tous comme des menaces potentielles. Si vous souhaitez assouplir un ou plusieurs mots clés considérés comme sûrs pour un emplacement spécifique, vous pouvez configurer une règle d'assouplissement qui peut contourner le contrôle de sécurité et bloquer le reste. Les commandes utilisées dans les relaxations ont des paramètres facultatifs pour le type de valeur et l'expression de valeur. Vous pouvez spécifier si l'expression de valeur est une expression régulière ou une chaîne littérale. Le type de valeur peut être laissé vide, ou vous pouvez sélectionner Mot-clé ou Chaîne spéciale.

> **Remarque :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation imprudente de caractères génériques, et en particulier du métacaractère ou de la combinaison de caractères génériques points-astérisques (.*), peut avoir des résultats que vous ne souhaitez pas, tels que le blocage de l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou l'autorisation d'une attaque que la vérification d'injection SQL JSON aurait autrement bloquée.

Points à prendre en compte

- L'expression de valeur est un argument facultatif. Le nom d'un champ peut ne pas comporter d'expression de valeur.
- Un nom de clé peut être lié à plusieurs expressions de valeur.
- Les expressions de valeur doivent se voir attribuer un type de valeur. Les types de valeur sont balise, attribut et modèle.
- Vous pouvez définir plusieurs règles de relaxation par combinaison de nom de clé/URL.

Configurer la relaxation du grain fin JSON pour les attaques par injection de script intersite (XSS) à l'aide de l'interface de commande

Pour configurer la règle de relaxation du grain du fichier JSON, vous devez lier les entités de relaxation de grain fin au profil Web App Firewall.

À l'invite de commande, tapez :

```
bind appfw profile <profile name> -jsonxssURL <URL> -key <key name> -
    isregex <REGEX/NOTREGEX> -valueType <keyword/SpecialString> <value
    Expression> -isvalueRegex <REGEX/NOTREGEX>
<!--NeedCopy-->
```

Exemple :

```
bind appfw profile appprofile1 -jsonxssurl www.example.com -key name  -
    isRegex NOTREGEX -valueType Tag  “sname”  -isvalueRegex NOTREGEX
<!--NeedCopy-->
```

Pour configurer une règle de relaxation du grain fin par injection de script intersite (XSS) basée sur JSON à l'aide de l'interface graphique

1. Accédez à **Pare-feu d'application > Profils**, sélectionnez un profil, puis cliquez sur **Modifier**.

2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
3. Dans la section **Règles de relaxation**, sélectionnez un enregistrement d'injection SQL JSON et cliquez sur **Modifier**.
4. Dans le curseur **Règles de relaxation des scripts intersites JSON**, cliquez sur **Ajouter**.
5. Dans la page **Règle de relaxation des scripts intersites JSON**, définissez les paramètres suivants.
    a) Activé
    b) Is Name Regex
    c) Nom de la clé
    d) URL
    e) Type de valeur
    f) Commentaires
    g) ID de ressource
6. Cliquez sur **Create**.



Contrôle de protection contre l'injection de commande JSON

May 5, 2023

La vérification d'injection de commande JSON examine le trafic JSON entrant à la recherche de commandes non autorisées qui violent la sécurité du système ou modifient le système. Lors de l'examen du trafic, si des commandes malveillantes sont détectées, l'appliance bloque la demande ou exécute l'action configurée.

Lors d'une attaque par injection de commandes, l'attaquant vise à exécuter des commandes non autorisées sur le système d'exploitation NetScaler ou le serveur principal. Pour ce faire, l'attaquant injecte des commandes du système d'exploitation à l'aide d'une application vulnérable. L'application dorsale est vulnérable aux attaques par injection si l'appliance transmet simplement une demande sans aucun contrôle de sécurité. Par conséquent, il est très important de configurer un contrôle de sécurité afin que l'appliance NetScaler puisse protéger votre application Web en bloquant les données non sécurisées.

Comment fonctionne la protection par injection de commande

1. Pour une demande JSON entrante, WAF examine le trafic à la recherche de mots-clés ou de caractères spéciaux. Si la demande JSON ne comporte aucun modèle correspondant à l'un des mots-clés ou caractères spéciaux refusés, la demande est autorisée. Sinon, la demande est bloquée, abandonnée ou redirigée en fonction de l'action configurée.
2. Si vous préférez exclure un mot-clé ou un caractère spécial de la liste, vous pouvez créer une règle d'assouplissement pour contourner le contrôle de sécurité dans des conditions spécifiques.
3. Vous pouvez activer la journalisation pour générer des messages de journal. Vous pouvez surveiller les journaux pour déterminer si les réponses aux demandes légitimes sont bloquées. Une forte augmentation du nombre de messages de journal peut indiquer des tentatives de lancement d'une attaque.
4. Vous pouvez également activer la fonctionnalité de statistiques pour collecter des données statistiques sur les violations et les journaux. Une augmentation inattendue du compteur de statistiques peut indiquer que votre application est attaquée. Si des demandes légitimes sont bloquées, vous devrez peut-être revoir la configuration pour voir si vous devez configurer la nouvelle règle de relaxation ou modifier celle existante.

Mots clés et caractères spéciaux refusés pour la vérification de l'injection de commande

Pour détecter et bloquer les attaques par injection de commandes JSON, l'appliance dispose d'un ensemble de modèles (mots-clés et caractères spéciaux) définis dans le fichier de signature par défaut.

Voici une liste de mots-clés bloqués lors de la détection d'injection de commande.

```
<commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
…
</commandinjection>

<!--NeedCopy-->
```

Les caractères spéciaux définis dans le fichier de signature sont les suivants :
| ; & $ > < '\ ! >> ##

Configuration de la vérification d'injection de commande JSON à l'aide de l'interface

Dans l'interface de ligne de commande, vous pouvez utiliser la commande set appfw profile ou ajouter une commande de profil appfw pour configurer les paramètres d'injection de commande JSON. Vous pouvez activer les actions de blocage, de journalisation et de statistiques. Vous devez également définir le type d'injection de commande, tel que les mots-clés et les caractères de chaîne que vous souhaitez détecter dans les charges utiles.

À l'invite de commande, tapez :

```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Remarque :**
>
> Par défaut, l'action d'injection de commande est définie sur « statistiques du journal de blocage ». En outre, le type d'injection de commande par défaut est défini comme CmdSplCharANDKeyWord. Après une mise à niveau, les profils Web App Firewall existants ont l'action définie sur « Aucun ».

Exemple :

```
set appfw profile profile1 -JSONCMDInjectionAction block -JSONCMDInjectionType
 CmdSplChar
```

Les actions d'injection de commande JSON disponibles sont les suivantes :

Aucun : désactive la protection par injection de commandes.
Log - Consigne les violations d'injection de commande pour le contrôle de sécurité.
Bloquer : bloque le trafic qui enfreint le contrôle de sécurité de l'injection de commande.
Stats - Génère des statistiques sur les violations de sécurité liées à l'injection

Les types d'injection de commande JSON disponibles sont les suivants :

`Cmd SplChar` - Vérifie les caractères spéciaux
`CmdKeyWord` - Vérifie l'injection de commande Mots-clés
`CmdSplCharANDKeyWord` - Il s'agit de l'action par défaut. L'action vérifie les caractères spéciaux et l'injection de commandes. Mots clés et blocs uniquement si les deux sont présents.
`CmdSplCharORKeyWord` - Vérifie les caractères spéciaux et les mots-clés d'injection de commande et les blocs si l'un d'entre eux est trouvé.

Configuration des règles de relaxation pour la vérification de la protection contre l'injection de commandes

Si votre application nécessite que vous contourniez l'inspection d'injection de commande JSON pour un élément ou un ATTRIBUTE spécifique dans la charge utile, vous pouvez configurer une règle de relaxation.

Les règles de relaxation de l'inspection par injection de commande JSON ont la syntaxe suivante.

```
bind appfw profile <profile name> -JSONCMDURL <expression> -comment <string
> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED )-state ( ENABLED |
DISABLED )
```

Exemple de règle de relaxation pour Regex dans l'en-tête

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/hello.html
```

Attendu que ce qui suit assouplit les requêtes de toutes les URL hébergées sur 1.1.1.1 :

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/*"
```

Pour supprimer la relaxation, utilisez « délier ».

```
unbind appfw profile abc_json -jsoncmDURL  " http://1.1.1.1/*"
```

Configurer la vérification d'injection de commande JSON à l'aide de l'interface graphique

Procédez comme suit pour configurer la vérification d'injection de commande JSON.

1. Accédez à **Sécurité > NetScaler Web App Firewall and Profiles**.
2. Sur la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page de **profil du Web App Firewall NetScaler**, accédez à la section **Paramètres avancés** et cliquez sur Contrôles **de sécurité**.



1. Dans **la section Contrôles de sécurité**, sélectionnez **Injection de commande JSON** et cliquez sur Paramètres **d'action** .
2. Dans la page **Paramètres d'injection de commandes JSON**, définissez les paramètres suivants
   a) Des actions. Sélectionnez une ou plusieurs actions à effectuer pour le contrôle de sécurité de l'injection de commandes JSON.
   b) Demande de contrôle contenant. Sélectionnez un modèle d'injection de commande pour vérifier si la demande entrante possède le modèle.
3. Cliquez sur **OK**.



Affichage des statistiques sur le trafic d'injection de commandes et les violations

La page des **statistiques du Web App Firewall NetScaler** affiche les détails du trafic de sécurité et des violations de sécurité sous forme de tableau ou de graphique.

Pour afficher les statistiques de sécurité à l'aide de l'interface de commande.

À l'invite de commande, tapez :

```
stat appfw profile profile1
```

Statistiques de trafic du profil Appfw	Taux (/s)	Total :
Demandes	0	0
Bytes de requête	0	0
Réponses	0	0
octets de réponse	0	0
Abandons	0	0
Redirections	0	0
Temps de réponse moyen à long terme (ms)	–	0
Temps de réponse de l'avenue récente (ms)	–	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
URL de démarrage	0	0
Refuser URL	0	0
En-tête de référence	0	0
débordement de tampon	0	0
Cohérence des cookies	0	0
Détournement de cookies	0	0
Balise de formulaire CSRF	0	0
Script intersite HTML	0	0
Injection HTML SQL	0	0
Format de champ	0	0
cohérence sur le terrain	0	0
Carte de crédit	0	0
Objet sûr	0	0
Violations de signature	0	0
Type de contenu	0	0
Déni de service JSON	0	0
Injection SQL JSON	0	0
Script intersite JSON	0	0
Types de téléchargement de fichiers	0	0
Déduire la charge utile XML du type de contenu	0	0
Injection de CMD HTML	0	0
Format XML	0	0
Déni de service XML (XDoS)	0	0
Validation des messages XML	0	0
Interopérabilité des services	0	0
Injection SQL XML	0	0
Script intersite XML	0	0

Statistiques sur les violations HTML/XML/JSON	Taux (/s)	Total :
Pièce jointe XML	0	0
Violations d'erreur SOAP	0	0
Violations génériques XML	0	0
Nombre total de violations	0	0

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
Journaux d'URL de démarrage	0	0
Journaux d'URL refusées	0	0
Journaux d'en-tête Referer	0	0
Logs de débordement	0	0
Journaux de cohérence des cookies	0	0
Journaux de détournement de cookies	0	0
CSRF à partir des journaux de balises	0	0
Journaux de script intersite HTML	0	0
Journaux de transformation de script intersite HTML	0	0
Journaux d'injection HTML SQL	0	0
Journaux de transformation HTML SQL	0	0
Journaux de format de champ	0	0
Journaux de cohérence des champs	0	0
Cartes de crédit	0	0

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
Journaux de transformation des cartes de crédit	0	0
Journaux des objets sécurisés	0	0
Journaux de signature	0	0
Journaux du type de contenu	0	0
Journaux de déni de service JSON	0	0
Journaux d’injection JSON SQL	0	0
Journaux de script intersite JSON	0	0
Journaux des types de téléchargement de fichiers	0	0
Déduire la charge utile XML du type de contenu L	0	0
Injection de CMD JSON	0	0
Journaux d’injection de commandes HTML	0	0
Journaux au format XML	0	0
Journaux de déni de service XML (XDoS)	0	0
Journaux de validation des messages XML	0	0
Journaux WSI	0	0
Journaux d’injection SQL XML	0	0
Journaux de script intersite XML	0	0
Journaux des pièces jointes XML	0	0
Journaux d’erreurs SOAP	0	0
Journaux génériques XML	0	0

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
Nombre total de messages journaux	0	0

Taux de statistiques de réponse aux erreurs du serveur (/s) | Total : |
|—|–|–|
Erreurs client HTTP (4xx Resp) | 0 | 0| Erreurs serveur
HTTP (5xx Resp) | 0 | 0 |

Statistiques des journaux HTML/XML/JSON	Taux (/s)	Total :
Journaux d’injection de commandes JSON	0	0
Journaux au format XML	0	0

Affichage des statistiques d’injection de commandes JSON à l’aide de l’interface graphique NetScaler

Procédez comme suit pour afficher les statistiques d’injection de commandes :

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet de détails, sélectionnez un profil de Web App Firewall et cliquez sur **Statistiques**.
3. La page des **statistiques du pare-feu NetScaler Web App** affiche le trafic d’injection de commandes JSON et les détails des violations.
4. Vous pouvez sélectionner **Vue tabulaire** ou passer en mode Affichage **graphique pour afficher** les données sous forme de tableau ou de graphique.

Statistiques de trafic d’injection de commandes JSON

HTML/XML/JSON Log Statistics

	Rate (/s)	Total
Start URL logs	0	0
Deny URL logs	0	0
Field consistency logs	0	0
Credit cards	0	0
Credit card transform logs	0	0
Safe object logs	0	0
Signature logs	0	0
Content Type logs	0	0
JSON Denial of Service logs	0	0
JSON SQL injection logs	0	0
JSON Cross-Site Scripting logs	0	0
JSON CMD injection logs	0	0
File upload types logs	0	0
Infer Content Type XML Payload Logs	0	0

JSON CMD injection logs: X
Number of JSON Command Injection security check log messages generated by the Application Firewall.

Statistiques sur les violations d’injection de commande JSON



Configurer la relaxation des grains fins pour l'injection de commandes JSON

Le Web App Firewall vous permet d'assouplir une clé ou une valeur JSON spécifique à partir de la vérification par injection de commande basée sur JSON. Vous pouvez contourner complètement l'inspection pour un ou plusieurs champs en configurant les règles de relaxation des grains fins.

Auparavant, la seule façon de configurer des relaxations pour les contrôles de protection JSON était de spécifier l'URL complète, ce qui contournait la vérification de l'URL complète.

La protection de sécurité par injection de commandes basée sur JSON fournit une relaxation pour les éléments suivants :

- Noms des clés
- Valeurs des clés

La protection par injection de commandes basée sur JSON vous permet de configurer des relaxations qui autorisent des modèles spécifiques et bloquent le reste. Par exemple, le Web App Firewall possède actuellement un ensemble par défaut de plus de 100 mots-clés SQL. Étant donné que les pirates informatiques peuvent utiliser ces mots clés dans des attaques par injection de commandes, le Web App Firewall les identifie tous comme des menaces potentielles. Si vous souhaitez assouplir un ou plusieurs mots clés considérés comme sûrs pour un emplacement spécifique, vous pouvez configurer une règle d'assouplissement qui peut contourner le contrôle de sécurité et bloquer le reste. Les commandes utilisées dans les relaxations ont des paramètres facultatifs pour le type de valeur et l'expression de valeur. Vous pouvez spécifier si l'expression de valeur est une expression régulière ou une chaîne littérale. Le type de valeur peut être laissé vide, ou vous pouvez sélectionner Mot-clé ou Chaîne spéciale.

> **Remarque :**
>
> Les expressions régulières sont puissantes. Surtout si vous n'êtes pas très familier avec les expressions régulières au format PCRE, vérifiez toutes les expressions régulières que vous écrivez. Assurez-vous qu'ils définissent exactement l'URL que vous souhaitez ajouter en tant qu'exception, et rien d'autre. L'utilisation imprudente de caractères génériques, et en particulier du métacaractère ou de la combinaison de caractères génériques points-astérisques (.*), peut avoir des résultats que vous ne souhaitez pas, tels que le blocage de l'accès au contenu Web que vous n'aviez pas l'intention de bloquer ou l'autorisation d'une attaque que la vérification d'injection SQL JSON aurait autrement bloquée.

Points à prendre en compte

- L'expression de valeur est un argument facultatif. Le nom d'un champ peut ne pas comporter d'expression de valeur.
- Un nom de clé peut être lié à plusieurs expressions de valeur.
- Les expressions de valeur doivent se voir attribuer un type de valeur. Le type de valeur peut être : 1) Mot-clé, 2) SpecialString.
- Vous pouvez définir plusieurs règles de relaxation par combinaison de nom de clé/URL.

Configuration de la relaxation du grain fin JSON pour les attaques par injection de commandes à l'aide de

Pour configurer la règle de relaxation du grain du fichier JSON, vous devez lier les entités de relaxation de grain fin au profil Web App Firewall.

À l'invite de commande, tapez :

```
bind appfw profile <profile name> -jsoncmdURL <URL> -key <key name> -
    valueType <keyword/SpecialString> <value Expression>
```



```
<!--NeedCopy-->
```

Exemple :

```
bind appfw profile appprofile1 -jsoncmdurl www.example.com -key blg_cnt -isRegex NOTREGEX -valueType Keyword “cat” -isvalueRegex NOTREGEX
```

Pour configurer la règle de relaxation fine pour les attaques par injection de commandes basées sur JSON à l’aide de l’interface graphique

1. Accédez à **Pare-feu d’application > Profils**, sélectionnez un profil, puis cliquez sur **Modifier**.
2. Dans le volet **Paramètres avancés**, cliquez sur **Règles de relaxation**.
3. Dans la section **Règles de relaxation**, sélectionnez un enregistrement d’ **injection de commande JSON** et cliquez sur **Modifier**.
4. Dans le curseur **Règle de relaxation d’injection de commande JSON**, cliquez sur **Ajouter**.
5. Dans la page **Règle de relaxation pour l’injection de commandes JSON**, définissez les paramètres suivants.
    a) Activé
    b) Is Name Regex
    c) Nom de la clé
    d) URL
    e) Type de valeur
    f) Commentaires
    g) ID de ressource
6. Cliquez sur **Create**.



Gestion des types de contenu

July 7, 2023

Les serveurs Web ajoutent un en-tête Content-Type avec une définition MIME/Type pour chaque type de contenu. Les serveurs Web diffusent de nombreux types de contenu différents. Par exemple, le code HTML standard se voit attribuer le type MIME « text/html ». Les images JPG se voient attribuer le type de contenu « image/jpeg » ou « image/jpg ». Un serveur Web normal peut diffuser différents types de contenu, tous définis dans l'en-tête du type de contenu par le type MIME attribué.

De nombreuses règles de filtrage du Web App Firewall sont conçues pour filtrer un type de contenu spécifique. Les règles de filtrage s'appliquent à un type de contenu tel que le HTML et sont souvent inappropriées lors du filtrage d'un autre type de contenu (comme les images). Par conséquent, le

Web App Firewall tente de déterminer le type de contenu des demandes et des réponses avant de les filtrer. Si un serveur Web ou un navigateur n'ajoute pas d'en-tête Content-Type à une demande ou à une réponse, le Web App Firewall applique un type de contenu par défaut et filtre le contenu en conséquence.

Le type de contenu par défaut est généralement « application/octet-stream » avec la définition de type MIME la plus générique. Le type MIME convient à tout type de contenu qu'un serveur Web est susceptible de diffuser. Mais ne fournit pas beaucoup d'informations au Web App Firewall pour lui permettre de choisir le filtrage approprié. Si un serveur Web protégé est configuré pour ajouter des en-têtes de type de contenu précis, vous pouvez alors créer un profil pour le serveur Web et lui attribuer un type de contenu par défaut. Ceci est fait pour améliorer à la fois la vitesse et la précision du filtrage.

Vous pouvez également configurer une liste des types de contenu de demande autorisés pour un profil spécifique. Lorsque cette fonctionnalité est configurée, si le Web App Firewall filtre une demande qui ne correspond pas à l'un des types de contenu autorisés, il bloque la demande.

Les demandes doivent toujours être du type « application/x-www-form-urlencoded », « multipart/form-data » ou « text/x-gwt-rpc ». Le Web App Firewall bloque toute demande associée à un autre type de contenu.

> **Remarque**
>
> Vous ne pouvez pas inclure les types de contenu « application/x-www-form-urlencoded » ou « multipart/form-data » dans la liste des types de contenu de réponse autorisés.

Pour définir le type de contenu de demande par défaut à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> -requestContentType <type>`
- `save ns config`

Exemple

L'exemple suivant définit le type de contenu « text/html » comme type de contenu par défaut pour le profil spécifié :

```
1 set appfw profile profile1 -requestContentType "text/html"
2 save ns config
3 <!--NeedCopy-->
```


Pour supprimer le type de contenu de demande par défaut défini par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `unset appfw profile <name> -requestContentType <type>`
- `save ns config`

Exemple

L'exemple suivant supprime le type de contenu par défaut « text/html » pour le profil spécifié, ce qui permet au type de revenir à « application/octet-stream » :

```
1 unset appfw profile profile1 -requestContentType "text/html"
2 save ns config
3 <!--NeedCopy-->
```

> **Remarque**
>
> Utilisez toujours le dernier en-tête de type de contenu pour le traitement et supprimez les en-têtes de type de contenu restants, le cas échéant, afin de garantir que le serveur principal reçoive une demande avec un seul type de contenu.
>
> Pour bloquer les requêtes qui peuvent être ignorées, ajoutez une stratégie de Web App Firewall avec la règle HTTP.REQ.HEADER ("content-type").COUNT.GT(1)' et le profil *appfw_block.*
>
> Si une demande est reçue sans en-tête Content-Type ou si la demande comporte un en-tête Content-Type sans aucune valeur, Web App Firewall applique la valeur **RequestContentType configurée et traite la demande** en conséquence.

Pour définir le type de contenu de réponse par défaut à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> -responseContentType <type>`
- `save ns config`

Exemple

L'exemple suivant définit le type de contenu « text/html » comme type de contenu par défaut pour le profil spécifié :

```
1 set appfw profile profile1 -responseContentType "text/html"
2 save ns config
```



```
<!--NeedCopy-->
```

Pour supprimer le type de contenu de réponse par défaut défini par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `unset appfw profile <name> -responseContentType <type>`
- `save ns config`

Exemple

L'exemple suivant supprime le type de contenu par défaut « text/html » pour le profil spécifié, ce qui permet au type de revenir à « application/octet-stream » :

```
unset appfw profile profile1 -responseContentType "text/html"
save ns config
<!--NeedCopy-->
```

Pour ajouter un type de contenu à la liste des types de contenu autorisés à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `bind appfw profile <name> -ContentType <contentTypeName>`
- `save ns config`

Exemple

L'exemple suivant ajoute le type de contenu « text/shtml » à la liste des types de contenu autorisés pour le profil spécifié :

```
bind appfw profile profile1 -contentType "text/shtml"
save ns config
<!--NeedCopy-->
```

Pour supprimer un type de contenu de la liste des types de contenu autorisés à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `unbind appfw profile <name> -ContentType <contentTypeName>`

- `save ns config`

Exemple

L'exemple suivant supprime le type de contenu « text/shtml » de la liste des types de contenu autorisés pour le profil spécifié :

```
1 unbind appfw profile profile1 -contentType "text/shtml"
2 save ns config
3 <!--NeedCopy-->
```

Gérez les types de contenu codés en URL et multipartites

Le NetScaler Web App Firewall vous permet désormais de configurer les types de contenu à code URL et à formulaires multiples pour les formulaires. La configuration du type de contenu est similaire à celle des listes XML et JSON. En fonction de la configuration, le Web App Firewall classe les demandes et inspecte le type de contenu codé en URL ou en plusieurs parties.

Pour configurer le profil Web App Firewall avec des types de contenu Urlencoded et Multipart-Form À l'invite de commande, tapez :

```
bind appfw profile p2 -contentType <string>
```

Exemple :

```
bind appfw profile p2 -contentType UrlencodedFormContentType

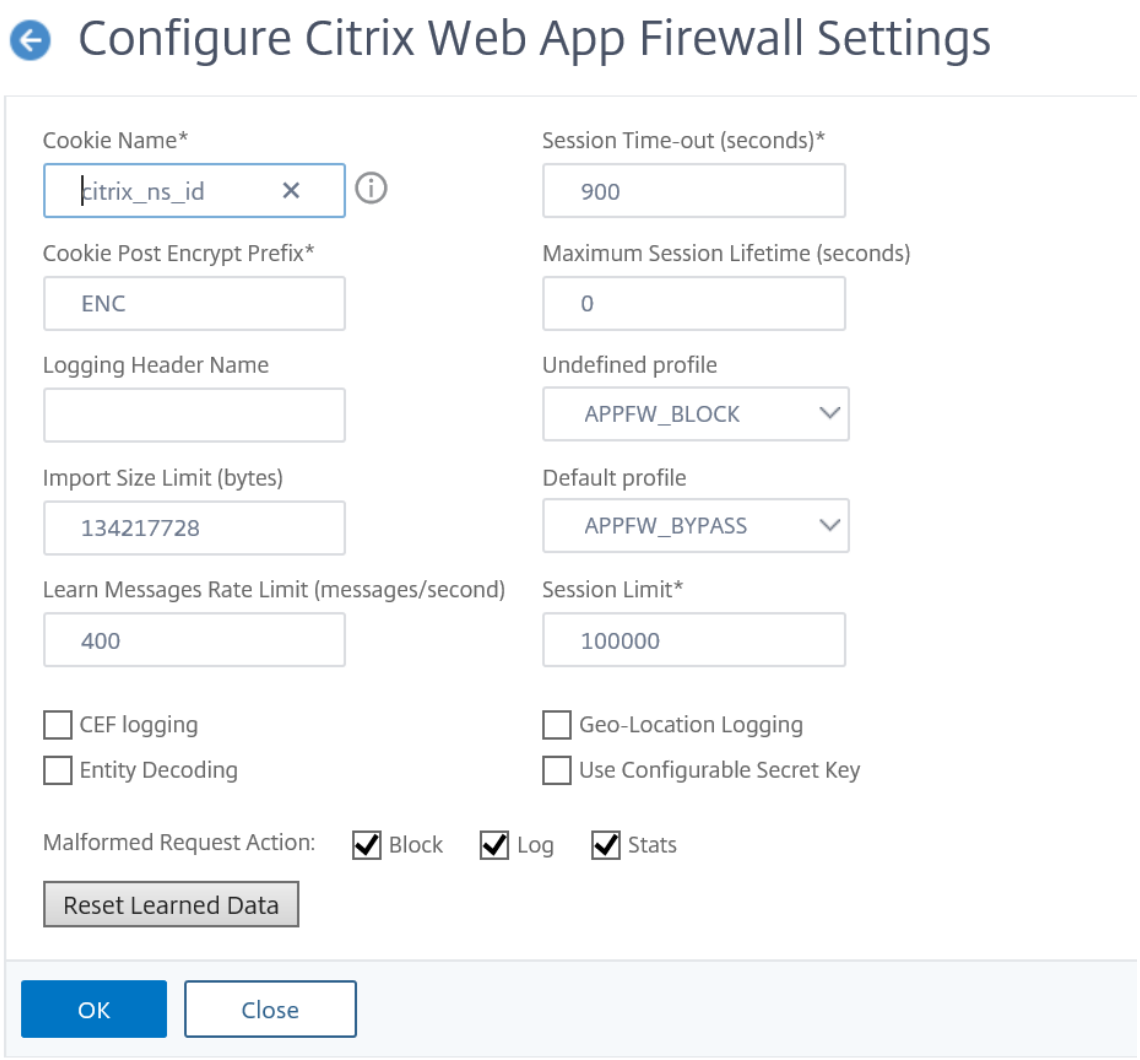
bind appfw profile p2 -ContentType appfwmultipartform
```

Pour gérer les types de contenu par défaut et autorisés à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet d'informations, sélectionnez le profil que vous souhaitez configurer, puis cliquez sur **Modifier**. La boîte de dialogue **Configurer le profil du Web App Firewall** s'affiche.
3. Dans la boîte de dialogue **Configurer le profil du Web App Firewall**, cliquez sur l'onglet **Paramètres** .
4. Dans l'onglet **Paramètres**, faites défiler l'écran vers le bas jusqu'à la zone Type de contenu.
5. Dans la zone Type de contenu, configurez le type de contenu de demande ou de réponse par défaut :
   - Pour configurer le type de contenu de demande par défaut, tapez la définition MIME/Type du type de contenu que vous souhaitez utiliser dans la zone de texte Demande par défaut.

- Pour configurer le type de contenu de réponse par défaut, tapez la définition MIME/Type du type de contenu que vous souhaitez utiliser dans la zone de texte Réponse par défaut.
- Pour créer un nouveau type de contenu autorisé, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un type de contenu autorisé** s'affiche.
- Pour modifier un type de contenu autorisé existant, sélectionnez ce type de contenu, puis cliquez sur **Ouvrir**. La boîte de dialogue **Modifier le type de contenu autorisé** s'affiche.

6. Pour gérer les types de contenu autorisés, cliquez sur Gérer les types de contenu autorisés.
7. Pour ajouter un nouveau type de contenu ou modifier un type de contenu existant, cliquez sur Ajouter ou sur Ouvrir, puis dans la boîte de dialogue **Ajouter un type** de **contenu autorisé ou Modifier le type** de contenu autorisé, procédez comme suit.
   a) Cochez/décochez la case Activé pour inclure le type de contenu dans la liste des types de contenu autorisés ou l'exclure de celle-ci.
   b) Dans la zone de texte Type de contenu, tapez une expression régulière qui décrit le type de contenu que vous souhaitez ajouter, ou modifiez l'expression régulière de type de contenu existante.
   Les types de contenu sont formatés exactement comme le sont les descriptions des types MIME.
   > **Remarque :**
   > Vous pouvez inclure n'importe quel type MIME valide dans la liste des types de contenus autorisés. Étant donné que de nombreux types de documents peuvent contenir du contenu actif et donc potentiellement du contenu malveillant, vous devez faire preuve de prudence lorsque vous ajoutez des types MIME à cette liste.
   c) Fournissez une brève description expliquant la raison pour laquelle ce type MIME particulier a été ajouté à la liste des types de contenus autorisés.
   d) Cliquez sur **Créer** ou **sur OK** pour enregistrer vos modifications.
8. Cliquez sur **Fermer** pour fermer la boîte de dialogue Gérer les types de contenu autorisés et revenir à l'onglet **Paramètres** .
9. Cliquez sur **OK** pour enregistrer vos modifications.

Pour gérer les types de contenu codés en URL et sous forme de formulaires en plusieurs parties à l'aide de l'interface graphique de NetScaler

1. Accédez à **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet d'informations, sélectionnez le profil que vous souhaitez configurer, puis cliquez sur **Modifier**.
3. Sur la page **Configurer le profil du Web App Firewall**, sélectionnez les **paramètres du profil** dans la section **Paramètres avancés** .
4. Dans la section **Type de contenu inspecté**, définissez les paramètres suivants :

a) application/x-www-form-urlencoded. Cochez la case pour inspecter le type de contenu codé en URL.
b) données multiparties/de formulaire. Cochez la case pour inspecter le type de contenu du formulaire multipartie.

5. Cliquez sur **OK**.



Profils

August 20, 2021

Un profil est un ensemble de paramètres de sécurité qui sont utilisés pour protéger des types spécifiques de contenu Web ou des parties spécifiques de votre site Web. Dans un profil, vous déterminez comment le Web App Firewall applique chacun de ses filtres (ou vérifications) aux demandes adressées à vos sites Web, ainsi que les réponses de ceux-ci. Le Web App Firewall prend en charge deux types de profils : quatre profils intégrés (par défaut) qui ne nécessitent pas de configuration supplémentaire, et les profils définis par l'utilisateur qui nécessitent une configuration supplémentaire.

Profilés intégrés

Les quatre profils intégrés du Web App Firewall offrent une protection simple pour les applications et sites Web qui ne nécessitent pas de protection ou qui ne doivent pas être directement accessibles par les utilisateurs. Ces types de profils sont les suivants :

- **APPFW_BYPASS.** Ignore tout le filtrage du Web App Firewall et envoie le trafic non modifié à l'application ou au site Web protégé, ou au client.
- **APPFW_RESET.** Réinitialise la connexion, exigeant que le client rétablisse sa session en visitant une page de démarrage désignée.
- **APPFW_DROP.** Supprime tout trafic vers ou depuis l'application ou le site Web protégé, et n'envoie aucune réponse d'aucune sorte au client.
- **APPFW_BLOCK.** Bloque le trafic vers ou en provenance de l'application ou du site Web protégé.

Vous utilisez les profils intégrés exactement comme vous le faites, en configurant une stratégie qui sélectionne le trafic auquel vous souhaitez appliquer le profil, puis en associant le profil à votre stratégie. Comme vous n'avez pas besoin de configurer une stratégie intégrée, elle fournit un moyen rapide d'autoriser ou de bloquer certains types de trafic ou de trafic qui sont envoyés à des applications ou à des sites Web spécifiques.

Profils définis par l'utilisateur

Les profils définis par l'utilisateur sont des profils créés et configurés par les utilisateurs. Contrairement aux profils par défaut, vous devez configurer un profil défini par l'utilisateur avant qu'il ne puisse être utilisé pour filtrer le trafic à destination et en provenance de vos applications protégées.

Il existe trois types de profils définis par l'utilisateur :

- **HTML.** Protège les pages Web HTML.
- **XML.** Protège les services Web basés sur XML et les sites Web.
- **Web 2.0.** Protège le contenu Web 2.0 qui combine des contenus HTML et XML, tels que les flux ATOM, les blogs et les flux RSS.

Le Web App Firewall comporte un certain nombre de contrôles de sécurité, qui peuvent tous être activés ou désactivés, et configurés de différentes manières dans chaque profil. Chaque profil possède également un certain nombre de paramètres qui contrôlent la façon dont il gère différents types de contenu. Enfin, plutôt que de configurer manuellement tous les contrôles de sécurité, vous pouvez activer et configurer la fonctionnalité d'apprentissage. Cette fonctionnalité observe le trafic normal vers vos sites Web protégés pendant un certain temps et utilise ces observations pour vous fournir une liste personnalisée des exceptions recommandées (*assouplissements*) à certains contrôles de sécurité, ainsi que des règles supplémentaires pour d'autres contrôles de sécurité.

Lors de la configuration initiale, que ce soit à l'aide de l'Assistant Web App Firewall ou manuellement, vous créez normalement un profil à usage général pour protéger tout le contenu de vos sites Web

qui n'est pas couvert par un profil plus spécifique. Après cela, vous pouvez créer autant de profils spécifiques que vous le souhaitez pour protéger un contenu plus spécialisé.

Le volet Profils est constitué d'un tableau qui contient les éléments suivants :

Nom. Affiche tous les profils de Web App Firewall configurés dans l'appliance.

Signature liée. Affiche l'objet signatures lié au profil dans la colonne précédente, le cas échéant.

Stratégies. Affiche la stratégie de Web App Firewall qui appelle le profil dans la colonne la plus à gauche de cette ligne, le cas échéant.

Commentaires. Affiche le commentaire associé au profil dans la colonne la plus à gauche de cette ligne, le cas échéant.

Type de profil. Affiche le type de profil. Les types sont intégrés, HTML, XML et Web 2.0.

Au-dessus du tableau se trouve une rangée de boutons et une liste déroulante qui vous permettent de créer, configurer, supprimer et afficher des informations sur vos profils :

- **Add.** Ajoutez un nouveau profil à la liste.
- **Modifier.** Modifiez le profil sélectionné.
- **Supprimer.** Supprimez le profil sélectionné de la liste.
- **Statistiques.** Affichez les statistiques du profil sélectionné.
- **Action.** Liste déroulante contenant des commandes supplémentaires. Vous permet actuellement d'importer un profil qui a été exporté à partir d'une autre configuration de Web App Firewall.

Création de profils de Web App Firewall

May 5, 2023

Vous pouvez créer un profil de Web App Firewall de deux manières : à l'aide de la ligne de commande et à l'aide de l'interface graphique. Pour créer un profil à l'aide de la ligne de commande, vous devez spécifier des options sur la ligne de commande. Le processus est similaire à celui de la configuration d'un profil et, à quelques exceptions près, les deux commandes prennent les mêmes paramètres.

> **Remarque**
>
> :**Profil principal** : ce profil est disponible dans la version 33.x et les versions ultérieures. Il contient des contrôles de sécurité limités mais fondamentaux activés par défaut, tandis que les profils de base et avancés ont de nombreux autres contrôles de sécurité activés par défaut. Le profil principal contient les contrôles de sécurité suivants :
>
> - Injection SQL basée sur la grammaire

> - Injection CMD basée sur la grammaire
> - Scriptage intersite
> - débordement de tampon
> -
>
> **Profil CVE**des mots clés de blocage : ce profil est disponible dans la version 42.x et les versions ultérieures. Utilisez ce profil uniquement pour ajouter et lier une signature. Il désactive toutes les vérifications effectuées par le NetScaler Web App Firewall, à l'exception de la vérification CVE.

Lorsque vous créez un profil, spécifiez l'une des options suivantes : basique, avancée, principale ou CVE. La configuration par défaut pour les différents contrôles et paramètres de sécurité qui font partie de ce profil est appliquée. Vous pouvez également ajouter un commentaire. Après avoir créé le profil, vous devez le configurer en le sélectionnant dans le volet de données, puis en cliquant sur **Modifier**.

Si vous envisagez d'utiliser la fonctionnalité d'apprentissage ou d'activer et de configurer de nombreuses protections avancées, vous devez choisir les paramètres par défaut avancés. En particulier, si vous envisagez de configurer l'une ou l'autre des vérifications d'injection SQL, soit les vérifications de script intersite, toute vérification offrant une protection contre les attaques de formulaires Web ou la vérification de cohérence des cookie, vous devez prévoir d'utiliser la fonctionnalité d'apprentissage. À moins que vous n'incluiez les exceptions appropriées pour vos sites Web protégés lors de la configuration de ces vérifications, ils peuvent bloquer le trafic légitime. Il est difficile d'anticiper toutes les exceptions sans en créer de trop générales. La fonction d'apprentissage facilite grandement cette tâche. Sinon, les valeurs par défaut de base sont rapides et doivent fournir la protection dont vos applications Web ont besoin.

Il existe trois types de profils :

- **HTML.** Protège les sites Web HTML standard.
- **XML.** Protège les services Web et les sites Web XML.
- **Web 2.0 (HTML XML).** Protège les sites Web qui contiennent des éléments HTML et XML, tels que des flux ATOM, des blogs et des flux RSS.

Il existe également quelques restrictions sur le nom que vous pouvez attribuer à un profil. Un nom de profil ne peut pas être identique au nom attribué à un autre profil ou action dans une fonctionnalité du dispositif NetScaler. Certains noms d'actions ou de profils sont attribués à des actions ou profils intégrés et ne peuvent jamais être utilisés pour des profils utilisateur. Vous trouverez une liste complète des noms non autorisés dans les informations supplémentairesdu profil du pare-feu Web App Firewall. Si vous tentez de créer un profil avec un nom qui a déjà été utilisé pour une action ou un profil, un message d'erreur s'affiche et le profil n'est pas créé.

Pour créer un profil de Web App Firewall à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw profile <name> [-defaults ( basic | advanced | core | cve)]`
- `set appfw profile <name> -type ( HTML | XML | HTML XML )`
- `set appfw profile <name> -comment "<comment>"`
- `save ns config`

Exemple

L'exemple suivant ajoute un profil nommé `pr-basic`, avec des valeurs par défaut de base, et attribue un type de profil HTML. Il s'agit de la configuration initiale appropriée pour un profil afin de protéger un site Web HTML.

```
1 add appfw profile pr-basic -defaults basic -comment "Simple profile for
      websites."
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```

Pour créer un profil de Web App Firewall à l'aide de l'interface graphique

Suivez la procédure suivante pour créer un profil de Web App Firewall :

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la page **Créer un profil de Web App Firewall**, définissez les paramètres de base suivants :
    a) Nom
    b) Type de profil
    c) Commentaires
    d) Valeurs par défaut
    e) Description
4. Cliquez sur **OK**.
5. Sélectionnez le profil que vous avez créé et cliquez sur **Modifier**.
6. Dans la section **Paramètres avancés**, effectuez les configurations suivantes :
    a) Contrôles de sécurité
    b) Paramètres du profil
    c) Profilage dynamique
    d) Règles de relaxation
    e) Règles de refus
    f) Règle apprise

g) Journalisation étendue



7. Dans la section **Contrôles de sécurité**, sélectionnez une protection de sécurité et cliquez sur **Paramètres d'action**.
8. Dans la page de vérification de sécurité, définissez les paramètres.

   > **Remarque :**
   >
   > Le paramètre **Règle active** est disponible uniquement pour la vérification **d'injection SQL HTML** afin d'activer la règle de relaxation ou la règle de refus pour la vérification d'injection SQL. Pour plus d'informations, consultez la rubrique Règles de relaxation et de refus .

9. Cliquez sur **OK** et sur **Fermer**.
10. Dans la section **Paramètres du profil**, définissez les paramètres du profil. Pour plus d'informations, consultez la rubrique Configurer les paramètres du profil de Web App Firewall .
11. Dans la section **Profilage dynamique**, sélectionnez une vérification de sécurité pour ajouter des paramètres de profil dynamique. Pour plus d'informations, consultez la rubrique Profil dynamique .
12. Dans la section **Règles de relaxation**, cliquez sur **Modifier** pour ajouter une règle de relaxation pour un contrôle de sécurité. Pour plus d'informations, consultez la section Règle de relaxation pour plus de détails.
13. Dans la section **Règles de refus**, ajoutez une règle de refus pour la vérification HTML SQL Injection. Pour plus d'informations, consultez la rubrique Règles de refus HTML .
14. Dans la section **Règle apprise**, définissez les paramètres d'apprentissage. Pour plus d'informations, consultez la rubrique d' apprentissage sur le Web App Firewall .
15. Dans la section **Journalisation étendue**, cliquez sur **Ajouter** pour masquer les données sensibles. Pour plus d'informations, consultez la rubrique de journalisation étendue .
16. Cliquez sur **Terminé**, puis cliquez sur **Fermer**.



Configurer les règles de détection des faux comptes

La création de faux comptes est un processus automatisé de création de nombreux comptes d'utilisateurs qui ne sont pas associés à une personne réelle ou de création de comptes utilisateur avec les informations de la personne réelle sans son consentement. Les faux comptes créés par des utilisateurs non légitimes utilisent des informations d'enregistrement qui ne correspondent pas à la véritable identité d'une personne. Ces comptes sont créés pour abuser des services offerts par une application Web à des fins non légitimes telles que des attaques de phishing, la diffusion de fausses nouvelles, le scalping, etc. Le plus souvent, ces comptes sont créés par des robots gérés par des utilisateurs malveillants.

L'appliance NetScaler est améliorée pour détecter les faux comptes en liant les règles de détection des faux comptes à un profil Web App Firewall. La règle se compose d'URL de formulaire et de paramètres de formulaire pour chaque URL. Si une demande entrante correspond à une expression ou à une URL de formulaire (pages d'inscription) configurée pour une règle de détection de faux compte, l'évaluation est vraie pour une tentative d'inscription suspecte et les données de demande sont envoyées au serveur ADM pour une inspection plus approfondie.

Procédez comme suit pour configurer la détection de faux comptes à l'aide de l'interface de commande :

1. Activer la fonction de détection des faux comptes
2. Lier les règles de faux comptes

Activer la fonction de détection des faux comptes

À l'invite de commande, tapez :

```
add/set appfw profile <name> -FakeAccountDetection ( ON | OFF )
```

Exemple :

```
add appfw profile profile1 -FakeAccountDetection ON
```

Lier les règles de faux comptes

À l'invite de commande, tapez :

```
bind appfw profile <name> -FakeAccount (string|expression)isFieldNameRegex
 (ON|OFF)-tag <TagExpression> ([-formUrl <FormURL>]| [-formExpression <
FormExpression>)])-state (ENABLED|DISABLED)
```

Où,

- `formUrl`: URL d'action de formulaire HTTP.
  FormExpression : expression de formulaire à évaluer.
- `fakeaccount`: nom du faux compte.
  tag : expression de balise.
- `isFieldNameRegex`: indique si le FieldName est une expression régulière. Valeur par défaut OFF.

Exemple :

```
bind appfw profile profile1 -FakeAccount john -formURL  "/signup.php"-tag "
smith"
bind appfw profile profile2 -FakeAccount Will -formExpression "HTTP.REQ.
HEADER(\"Authorization\").CONTAINS(\"/test_accounts\").NOT && HTTP.REQ.URL.
CONTAINS(\"/login.php\")"-fieldName -tag "smith"
```

Exemple d'entrée pour une demande de publication HTTP pour la page `example.com` d'inscription.

S.non	Entrée	Exemple
1	URL du point de terminaison de la demande HTTP POST	`https://webapi.example.com/account/api/v1.0/contacts/`
2	Nom du champ e-mail dans la demande de publication HTTP	Adresse e-mail

S.non	Entrée	Exemple
3	Prénom Nom du champ dans la demande de publication HTTP	Prénom
4	Nom de famille Nom du champ dans la demande de publication HTTP	Nom de famille

Configurer la règle de détection des faux comptes du Web App Firewall à l'aide de l'interface

Suivez les étapes ci-dessous pour configurer la règle de détection des faux comptes à l'aide de l'interface graphique.

1. **Accédez à**Configuration**>**Sécurité**>**NetScaler Web App Firewall > Profil**.**
2. Sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Contrôles de sécurité** dans Paramètres **avancés**.
4. Dans la section **Vérifications intégrées à Citrix Cloud**, sélectionnez une fausse règle de compte et cliquez sur **Modifier**.
5. Dans le curseur **Liaison de faux compte AppFirewall**, sélectionnez une règle à modifier ou cliquez sur **Ajouter**.
6. Dans la page **Règle de faux compte**, définissez les paramètres suivants :
   a) **Activé**. Sélectionnez cette option pour activer la règle de faux compte.
   b) **Faux nom de compte**. Nom de la règle de faux compte.
   c) **Balise**. Prénom dans le faux formulaire d'enregistrement de compte.
   d) **Est-ce que Field Name Regex ?** Indiquez si le champ de formulaire est une expression régulière.
   e) **Expression de forme**. Expression régulière qui définit le faux compte.
   f) **URL du formulaire**. Entrez la fausse URL de détection de compte.
   g) **Commentaires**. Brève description de la règle de détection des faux comptes.
7. Cliquez sur **Create**.



Appliquer la conformité HTTP RFC

May 5, 2023

NetScaler Web App Firewall inspecte le trafic entrant pour vérifier sa conformité aux RFC HTTP et supprime par défaut toute demande présentant des violations des RFC. Toutefois, dans certains scénarios, l'appliance peut devoir contourner ou bloquer une demande de conformité non RFC. Dans ce cas, vous pouvez configurer l'appliance pour contourner ou bloquer ces demandes au niveau global ou au niveau du profil.

Bloquer ou contourner les demandes non conformes à la RFC au niveau mondial

Le module HTTP identifie une demande comme non valide si elle est incomplète et que de telles demandes ne peuvent pas être traitées par WAF. Par exemple, une requête HTTP entrante dont l'en-tête d'hôte est manquant. Pour bloquer ou contourner ces demandes non valides, vous devez configurer l'option `malformedReqAction` dans les paramètres globaux du pare-feu de l'application.

Le paramètre « MalformedReqAction » valide la requête entrante pour une longueur de contenu non valide, une requête fragmentée non valide, une absence de version HTTP et un en-tête incomplet.

> **Remarque :**
>
> Si vous désactivez l'option de blocage dans le paramètre `malformedReqAction`, l'appliance contourne l'ensemble du traitement du pare-feu de l'application pour toutes les demandes de conformité non RFC et transmet les demandes au module suivant.

Pour bloquer ou contourner les demandes HTTP non valides non conformes à la RFC à l'aide de l'interface de ligne de commande

Pour bloquer ou contourner les demandes non valides, saisissez la commande suivante :

```
set appfw settings -malformedreqaction <action>
```

Exemple :

```
set appfw settings -malformedReqAction block
```

Pour afficher des paramètres d'action de demande incorrects

Pour afficher les paramètres d'action de demande incorrects, saisissez la commande suivante :

```
show appfw settings
```

Sortie :

```
1 DefaultProfile: APPFW_BYPASS UndefAction: APPFW_BLOCK SessionTimeout:
      900 LearnRateLimit: 400 SessionLifetime: 0
    SessionCookieName: citrix_ns_id ImportSizeLimit: 134217728
    SignatureAutoUpdate: OFF SignatureUrl:"https://s3.amazonaws.com/
    NSAppFwSignatures/SignaturesMapping.xml" CookiePostEncryptPrefix:
    ENC GeoLocationLogging: OFF CEFLogging: OFF EntityDecoding:
     OFF UseConfigurableSecretKey: OFF SessionLimit: 100000
    MalformedReqAction: block log stats
2  Done
3 <!--NeedCopy-->
```

Pour bloquer ou contourner les requêtes HTTP non conformes à la norme RFC non valides à l'aide de l'interface graphique NetScaler

1. Accédez à **Sécurité** > **NetScaler Web App Firewall**.
2. **Sur la page**NetScaler Web App Firewall**, cliquez sur**Modifier les paramètres du moteur sous Paramètres**.**
3. Sur la page **Configurer les paramètres du pare-feu NetScaler Web App**, sélectionnez l'option Enregistrer les **demandes malformées** sous la forme Block, Log ou Stats.
4. Cliquez sur **OK** et sur **Fermer**.

> **Remarque :**
>
> Si vous désélectionnez l'action de blocage ou si vous ne sélectionnez aucune action de demande mal formée, l'appliance contourne la demande sans en insinuer l'utilisateur.

Bloquer ou contourner les demandes non conformes RFC au niveau du profil

D'autres demandes non conformes RFC peuvent être configurées pour bloquer ou contourner au niveau du profil. Vous devez configurer le profil RFC en mode Block ou Bypass. En effectuant cette configuration, tout trafic non valide correspondant au profil Web App Firewall est contourné ou bloqué en conséquence. Le profil RFC valide les contrôles de sécurité suivants :

- Demandes GWT-RPC non valides
- En-têtes de type de contenu
- Demandes en plusieurs parties non valides
- Demandes JSON non valides
- Vérifications de paires de noms de cookie en double

> **Remarque :**
>
> Lorsque vous définissez le profil `RFC` en mode « Contournement », vous devez vous assurer de désactiver l'option de transformation dans les sections **Paramètres de script intersiteHTML et Paramètres d'injection SQL HTML** . Si vous activez et définissez le `RFC` profil en mode Contournement, l'appliance affiche un message d'avertissement, « Transformer les scripts inter-sites » et « Transformer les caractères spéciaux SQL » sont tous deux activés. Il est recommandé de l'éteindre lorsqu'il est utilisé avec `APPFW_RFC_BYPASS`.
>
> **Important :**
>
> De plus, l'appliance affiche une note d'avertissement : « Les contrôles de sécurité Appfw activés peuvent ne pas être applicables aux demandes qui enfreignent les vérifications RFC lorsque ce profil est défini. L'activation d'un paramètre de transformation n'est pas recommandée car les demandes peuvent être partiellement transformées qui contiennent des violations RFC. »

Pour configurer un profil RFC dans le profil Web App Firewall à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
set appfw profile <profile_name> -rfcprofile <rfcprofile_name
```

Exemple

```
set appfw profile P1 -rfcprofile APPFW_RFC_BLOCK
```


> **Remarque :**
>
> Par défaut, le profil RFC est lié au profil Web App Firewall en mode Bloquer.

Pour configurer un profil RFC dans le profil Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans la page **Profils**, sélectionnez un profil et cliquez sur **Modifier**.
3. Dans la page **Profil du Web App Firewall**, cliquez sur **Paramètres de profil dans** la section **Paramètres avancés** .
4. Dans la section **Paramètres HTML**, définissez le profil RFC sur le mode APPFW_RFC_BYPASS. Le système affiche un message d'avertissement : « Les vérifications de sécurité Appfw activées peuvent ne pas s'appliquer aux demandes qui violent les vérifications RFC lorsque ce profil est défini. L'activation d'un paramètre de transformation n'est pas recommandée car les requêtes peuvent être partiellement transformées qui contiennent des violations RFC ».

Configuration des profils Web App Firewall

May 5, 2023

Pour configurer un profil Web App Firewall défini par l'utilisateur, configurez d'abord les contrôles de sécurité, appelés *protections profondes* ou *protections avancées* dans l'Assistant Web App Firewall. Certaines vérifications nécessitent une configuration si vous voulez les utiliser. D'autres ont des configurations par défaut qui sont sûres mais dont la portée est limitée ; vos sites Web peuvent avoir besoin ou bénéficier d'une configuration différente qui tire parti des fonctionnalités supplémentaires de certains contrôles de sécurité.

Après avoir configuré les contrôles de sécurité, vous pouvez également configurer d'autres paramètres qui contrôlent le comportement, non pas d'un seul contrôle de sécurité, mais de la fonctionnalité Web App Firewall. La configuration par défaut est suffisante pour protéger la plupart des sites Web, mais vous devez les consulter pour vous assurer qu'ils conviennent à vos sites Web protégés.

> **Remarque :**
>
> La longueur du nom du profil et toute la longueur du nom d'objet d'importation peuvent être définies à 127 caractères.

Pour plus d'informations sur les contrôles de sécurité Web App Firewall, voir Protections avancées.

Pour configurer un profil Web App Firewall à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> <arg1> [<arg2> ...]`

  où :

  - `<arg1>` = un paramètre et toutes les options associées.
  - `<arg2>` = un second paramètre et toutes les options associées.
  - … = paramètres et options supplémentaires.

  Pour obtenir une description des paramètres à utiliser lors de la configuration de contrôles de sécurité spécifiques, voir Protections avancées.

- `save ns config`

Exemple

L'exemple suivant montre comment activer le blocage pour les vérifications HTML SQL Injection et HTML Cross-Site Scripting dans un profil nommé `pr-basic`. Cette commande permet de bloquer ces actions tout en n'apportant aucune autre modification au profil.

```
1 set appfw profile pr-basic -crossSiteScriptingAction block -
     SQLInjectionAction block
2 <!--NeedCopy-->
```

Règle de relaxation de liaison à un profil Web App Firewall

Lorsqu'un Web App Firewall détecte une violation, l'utilisateur a la possibilité de contourner l'action appliquée par le biais de règles d'assouplissement. La règle d'assouplissement est une exception appliquée à la violation de sécurité détectée. Par exemple, les règles de relaxation de l'URL de démarrage protègent contre la navigation forcée. Les vulnérabilités connues des serveurs Web exploitées par des pirates peuvent être détectées et bloquées en activant un ensemble de règles de refus d'URL par défaut. Les attaques lancées couramment, telles que Buffer Overflow, SQL ou cross-site scripting peuvent également être facilement détectées.

Pour lier des règles d'exemption ou d'assouplissement de sécurité à l'aide de

À l'invite de commande, tapez :

```
1 bind appfw profile <name> ((-startURL <expression> [-resourceId  <
     string>]) | -denyURL <expression> | (-fieldConsistency <string>   <
     formActionURL> [-isRegex ( REGEX | NOTREGEX )]) | (-
     cookieConsistency <string> [-isRegex ( REGEX | NOTREGEX )]) | (-
```



```
      SQLInjection <string> <formActionURL> [-isRegex ( REGEX | NOTREGEX )
      ] [-location <location>] [-valueType <valueType> <valueExpression
      >....
<!--NeedCopy-->
```

Pour lier les règles d'exemption ou de relaxation de sécurité à l'aide de l'interface

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Règles de relaxation** dans la section **Paramètres avancés** .
4. Dans la section **Règles de relaxation**, cliquez sur **StartURL**, puis sur **Modifier**.
5. Dans la page **Règles de relaxation de l'URL de démarrage**, cliquez sur **Ajouter**.
6. Dans la page **Règle de relaxation d'URL de démarrage**, définissez les paramètres suivants :
   a) Activé. Activez la case à cocher pour activer la règle de relaxation.
   b) URL de démarrage. Entrez la valeur d'expression régulière
   c) Commentaires. Fournissez une brève description de la règle de relaxation.
7. Cliquez sur **Créer** et **Fermer**.



Pour configurer un profil Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet d'informations, sélectionnez le profil que vous souhaitez configurer, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Configurer le profil de Web App Firewall**, sous l'onglet **Vérifications de sécurité**, configurez les contrôles de sécurité.
   - Pour activer ou désactiver une action pour une vérification, dans la liste, activez ou désactivez la case à cocher correspondant à l'action.
   - Pour configurer les paramètres des contrôles de sécurité de la liste, cochez la case et cliquez sur **Paramètres actifs**.
   - Pour vérifier les entrées du journal pour la vérification de sécurité sélectionnée, cochez la case et cliquez sur **Journaux**. Vous pouvez utiliser ces informations pour déterminer les contrôles de sécurité qui correspondent aux attaques, afin de pouvoir bloquer le trafic pour les contrôles de sécurité. Vous pouvez également utiliser ces informations pour déterminer les vérifications qui correspondent au trafic légitime, afin de pouvoir configurer une exemption appropriée pour autoriser ces connexions légitimes. Pour plus d'informations sur les journaux, consultez Journaux, statistiques et rapports.
   - Pour désactiver complètement une coche, dans la liste, désactivez toutes les cases à droite de cette coche.
4. Dans l'onglet **Paramètres**, configurez les paramètres du profil.
   - Pour associer le profil à l'ensemble de signatures que vous avez précédemment créé et configuré, sous Paramètres communs, choisissez cet ensemble de signatures dans la liste déroulante **Signatures** .

     > **Remarque :**
     >
     > Vous devez utiliser la barre de défilement à droite de la boîte de dialogue pour faire défiler vers le bas afin d'afficher la section Paramètres communs.

   - Pour configurer un objet d'erreur HTML ou XML, sélectionnez-le dans la liste déroulante appropriée.

     > **Remarque :**
     >
     > Vous devez d'abord charger l'objet d'erreur que vous souhaitez utiliser dans le volet Importations. Pour plus d'informations sur l'importation d'objets d'erreur, voir Importations.

   - Pour configurer le type de contenu XML par défaut, tapez la chaîne de type de contenu directement dans les zones de texte Demande par défaut et réponse par défaut, ou cliquez

sur Gérer les types de contenu autorisés pour gérer la liste des types de contenu autorisés. »Plus….

5. Si vous souhaitez utiliser la fonctionnalité d'apprentissage, cliquez sur Apprentissage et configurez les paramètres d'apprentissage du profil, comme décrit dans Configuration et utilisation de la fonctionnalité d'apprentissage.
6. Cliquez sur **OK** pour enregistrer vos modifications et revenir au volet **Profils** .

Champs confidentiels du profil WAF

> **Remarque**
>
> Cette fonctionnalité est disponible dans la version 13.1 build 27.x et versions ultérieures.

Vous pouvez désormais ajouter des champs confidentiels dans un profil WAF. Ces champs sont masqués et ne sont pas capturés dans les journaux ADC lorsqu'une violation se produit. Auparavant, vous pouviez ajouter ces champs uniquement à l'aide de paramètres. Pour plus d'informations sur l'ajout de champs confidentiels à l'aide des paramètres, voir Champs confidentiels

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Sélectionnez un profil et cliquez sur **Modifier**.
3. Dans les **paramètres avancés**, cliquez sur **Champs confidentiels**.



4. Cliquez sur **Ajouter**.
5. Entrez des valeurs pour les paramètres suivants :
   - Nom du champ de formulaire*
   - URL de l'action*
   - Commentaires



A ⋆ indique un champ obligatoire

6. Cliquez sur **Create**.
7. Cliquez sur **Terminé**.

Paramètres du profil du pare-feu d'application Web

May 5, 2023

Voici les paramètres de profil que vous devez configurer sur la solution matérielle-logicielle.

À l'invite de commande, tapez :

```
add appfw profile <name> [-invalidPercentHandling <invalidPercentHandling
>] [-checkRequestHeaders ( ON | OFF )] [-URLDecodeRequestCookies ( ON |
 OFF )] [-optimizePartialReqs ( ON | OFF )] [-errorURL <expression>] [-
logEveryPolicyHit ( ON | OFF )] [-stripHtmlComments <stripHtmlComments>] [-
```



```
stripXmlComments ( none | all )] [-postBodyLimitSignature <positive_integer
>][-fileUploadMaxNum <positive_integer>][-canonicalizeHTMLResponse ( ON
| OFF )][-percentDecodeRecursively ( ON | OFF )] [-multipleHeaderAction
<multipleHeaderAction> ...][-inspectContentTypes <inspectContentTypes>
...][-semicolonFieldSeparator ( ON | OFF )]
```

Exemple :

```
add appfw profile profile1 [-invalidPercentHandling secure_mode] [-checkRequestHeaders
 ON] [-URLDecodeRequestCookies OFF] [-optimizePartialReqs OFF]
```

Où,

InvalidPercentHandling : configurez la méthode de gestion des noms et des valeurs codés en pourcentage.

Les paramètres disponibles fonctionnent comme suit :

asp_mode - Enlève et analyse le pourcentage non valide pour l'analyse.

Exemple : `curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz)` est enlevé, le reste du contenu est inspecté et une action est entreprise pour la vérification SQLInjection.

secure_mode - Nous détectons la valeur codée en pourcentage non valide et l'ignorons.

Exemple : `curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz)` est détecté, les compteurs sont incrémentés et le contenu est transmis tel qu'il est au serveur.

apache_mode - Ce mode fonctionne de la même manière que le mode sécurisé.

> **Remarque :**
>
> À partir de la version 13.1 build 45.x, la `apache_mode` fonction est obsolète.

Valeurs possibles : apache_mode, asp_mode, secure_mode

Valeur par défaut : secure_mode

OptimizePartialReqs : lorsqu'elle est désactivée/activée (sans objet sécurisé), une appliance NetScaler envoie la demande partielle au serveur principal. Cette réponse partielle a été renvoyée au client. OptimizePartialReqs est logique lorsque l'objet Safe est configuré. La solution matérielle-logicielle envoie des demandes de réponse complète du serveur lorsqu'elle est désactivée, et ne demande qu'une réponse partielle lorsqu'elle est activée.

Les paramètres disponibles sont les suivants :

ON - Les demandes partielles du client entraînent des demandes partielles adressées au serveur principal.

OFF : les demandes partielles du client sont remplacées par des demandes complètes adressées au serveur principal.

Valeurs possibles : ON, OFF Valeur
par défaut : ON

Cookies de demande de décodage d'URL. URL Decode demande des cookies avant de les soumettre à des vérifications SQL et de script intersite.

Valeurs possibles : ON, OFF Valeur
par défaut : OFF

Limite du corps de la publication de signature (octets). Limite la charge utile de la requête (en octets) inspectée à la recherche de signatures avec l'emplacement spécifié comme « HTTP_POST_BODY ».

Valeur par défaut : 8096 Valeur
minimale : 0 Valeur
maximale : 4294967295

Limite de corps de publication (octets). Limite la charge utile de la demande (en octets) inspectée par le pare-feu d'application Web.

Valeur par défaut : 20000000 Valeur
minimale : 0 Valeur
maximale : 10 Go

Pour plus d'informations sur le paramètre de sécurité et sa procédure GUI, consultez la rubrique Configurer le profil du Web App Firewall .

PostBodyLimitAction. PostBodyLimit respecte les paramètres d'erreur lorsque vous spécifiez la taille maximale du corps HTTP à autoriser. Pour respecter les paramètres d'erreur, vous devez configurer une ou plusieurs actions Limite du corps de publication. La configuration s'applique également aux demandes pour lesquelles l'en-tête de codage de transfert est segmenté.

```
set appfw profile <profile_name> -PostBodyLimitAction block log stats
```

Où,
Bloquer - Cette action bloque la connexion qui viole le contrôle de sécurité et elle est basée sur la taille maximale du corps HTTP configuré (limite de corps post-). Vous devez toujours activer cette option.

Journal - Consigner les violations de cette vérification de sécurité.

Stats - Générez des statistiques pour cette vérification de sécurité.

> **Remarque :**
>
> Le format du journal pour l'action de limitation du corps de publication est désormais modifié pour suivre le format de journalisation d'audit

> standard, par exemple :
> ns.log.4.gz:Jun 25 1.1.1.1. <local0.info> 10.101.10.100 06/25/2020:10:10:28 GMT 0-PPE-0 : **default** APPFW APPFW_POSTBODYLIMIT 1506 0 : <Netscaler IP> 4234-PPE0 - testprof ><URL> Request post body length(<Post Body Length >)exceeds post body limit.

InspectQueryContentTypes Inspectez les requêtes de demande et les formulaires Web pour les scripts SQL injectés et intersite pour les types de contenu suivants.

```
set appfw profile p1 -inspectQueryContentTypes HTML XML JSON OTHER
```

Valeurs possibles : HTML, XML, JSON, OTHER

Par défaut, ce paramètre est défini sur « InspectQueryContentTypes : HTML JSON OTHER » pour les profils appfw de base et avancés.

Exemple pour inspecter le type de contenu de la requête en tant que XML :

```
1 > set appfw profile p1 -type XML
2 Warning: HTML, JSON checks except "InspectQueryContentTypes" & "
    Infer Content-Type XML Payload Action" will not be applicable when
    profile type is not HTML or JSON respectively.
3 <!--NeedCopy-->
```

Exemple pour inspecter le type de contenu de la requête en HTML :

```
1 > set appfw profile p1 -type HTML
2 Warning: XML, JSON checks except "InspectQueryContentTypes" & "Infer
     Content-Type XML Payload Action" will not be applicable when
    profile type is not XML or JSON respectively
3 Done
4 <!--NeedCopy-->
```

Exemple pour inspecter le type de contenu de requête au format JSON :

```
1 > set appfw profile p1 -type JSON
2 Warning: HTML, XML checks except "InspectQueryContentTypes" & "Infer
     Content-Type XML Payload Action will not be applicable when profile
     type is not HTML or XML respectively
3 Done
4 <!--NeedCopy-->
```

Expression ErrorUrl. URL que le NetScaler Web App Firewall utilise comme URL d'erreur. Longueur maximale : 2047.

> **Remarque :**
>
> Pour bloquer les violations dans une URL demandée, si l'URL d'erreur est similaire à l'URL de signature, la solution matérielle-logicielle réinitialise la connexion.

LogeVeryPolicyHit - Consignez chaque correspondance de profil, quels que soient les résultats des contrôles de sécurité.
Valeurs possibles : ON, OFF.
Valeur par défaut : OFF.

StripXMLComments - Supprimez les commentaires XML avant de transférer une page Web envoyée par un site Web protégé en réponse à une demande d'un utilisateur.
Valeurs possibles : none, all, exclude_script_tag.
Valeur par défaut : aucune

PostBodyLimitSignature - Taille maximale autorisée du corps de publication HTTP pour l'inspection des signatures pour l'emplacement HTTP_POST_BODY dans les signatures, en octets.
Les changements de valeur peuvent avoir un impact sur le processeur et le profil de latence.
Valeur par défaut : 2048.
Valeur minimale : 0 Valeur
maximale : 4294967295

FileUploadMaxNum : nombre maximal autorisé de téléchargements de fichiers par demande de soumission de formulaire. Le paramètre maximum (65535) permet un nombre illimité de téléchargements.
Valeur par défaut : 65535 Valeur
minimale : 0 Valeur
maximale : 65535

CanonicAlizeHTMLResponse - Effectuez le codage des entités HTML pour tous les caractères spéciaux des réponses envoyées par vos sites Web protégés.
Valeurs possibles : ON, OFF Valeur
par défaut : ON

PercentDecodeRecursivement - Configurez si le pare-feu d'application doit utiliser le décodage récursif en pourcentage.
Valeurs possibles : ON, OFF Valeur
par défaut : ON

MultipleHeaderAction - Une ou plusieurs actions d'en-tête multiples. Les paramètres disponibles fonctionnent comme suit :

- Bloquer. Bloquez les connexions comportant plusieurs en-têtes.
- Bûche. Consignez les connexions qui ont plusieurs en-têtes.
- KeepLast. Ne conservez que le dernier en-tête lorsque plusieurs en-têtes sont présents.

InspectContentTypes : une ou plusieurs listes InspectContentType.

- application/x-www-form-urlencoded
- données multipart/formulaire
- texte/x-gwt-rpc

Valeurs possibles : aucun, application/x-www-form-urlencoded, multipart/form-data, text/x-gwt-rpc

SemiColonFieldSeparator - Autorise « ; » comme séparateur de champ de formulaire dans les requêtes URL et les corps de formulaire POST.
Valeurs possibles : ON, OFF Valeur
par défaut : OFF

Modification du type de profil d'un Web App Firewall

May 5, 2023

Si vous avez choisi le mauvais type de profil pour un profil Web App Firewall ou si le type de contenu du site Web protégé a changé, vous pouvez modifier le type de profil.

> **Remarque** Lorsque vous modifiez le type de profil, vous perdez tous les paramètres de configuration et les assouplissements ou règles apprises pour les fonctionnalités que le nouveau type de profil ne prend pas en charge. Par exemple, si vous remplacez le type de profil Web 2.0 par XML, vous perdez toutes les options de configuration pour l'URL de démarrage, le contrôle de cohérence des champs de formulaire et les autres contrôles de sécurité spécifiques au HTML. La configuration de toutes les options prises en charge à la fois par l'ancien et le nouveau type de profil reste inchangée.

Pour modifier le type de profil d'un Web App Firewall à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set appfw profile <name> -type ( **HTML** | **XML** | **HTML XML** )`
- `save ns config`

Exemple

L'exemple suivant modifie le type d'un profil nommé pr-basic, de HTML à HTML XML, ce qui est équivalent au type Web 2.0 dans l'interface graphique.

```
1 set appfw profile pr-basic -type HTML XML
```



```
save ns config
<!--NeedCopy-->
```

Pour modifier le type de profil d'un Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Politiques**.
2. Dans le volet d'informations, cliquez sur **Action**, puis sur **Modifier le type de profil**.
3. Dans la boîte de dialogue **Modifier le type de profil du Web App Firewall**, dans la liste déroulante **Type de profil**, sélectionnez un nouveau type de profil.
4. Cliquez sur **OK** pour enregistrer vos modifications et revenir au volet **Profils** .

Exportation et importation d'un profil de Web App Firewall

January 21, 2021

Vous pouvez répliquer toute la configuration d'un profil de Web App Firewall (y compris tous les objets liés, tels que l'objet d'erreur HTML, l'objet d'erreur XML, le schéma WSDL ou XML, les signatures, etc.) sur plusieurs appliances. Vous pouvez sélectionner un profil cible et exporter la configuration pour l'enregistrer dans le système de fichiers local de votre ordinateur, ou transférer la configuration archivée pour la stocker sur un serveur. De même, vous pouvez parcourir le système de fichiers local de votre ordinateur ou importer l'archive depuis le serveur pour sélectionner un profil précédemment exporté et l'importer dans votre appliance NetScaler.

L'option permettant d'exporter l'intégralité de la configuration du profil, puis de l'importer dans une autre appliance, peut s'avérer utile dans différents cas d'utilisation. Par exemple, vous pouvez configurer un profil de Web App Firewall dans une configuration de banc d'essai pour tester et valider qu'il fonctionne comme prévu. Une fois que vous êtes satisfait, vous pouvez exporter le profil et importer la configuration du profil vers vos appliances NetScaler de production. Cette fonctionnalité est également utile pour sauvegarder votre configuration. Vous pouvez exporter le profil avant d'apporter des modifications, de sorte que vous pouvez facilement restaurer la configuration à un état connu si nécessaire.

> **Remarque**
>
> Les profils de Web App Firewall exportés et archivés à partir d'une version ne peuvent pas être restaurés sur un système exécutant une version différente, car les modifications introduites dans les versions les plus récentes peuvent entraîner des problèmes de compatibilité. Si vous tentez de restaurer un profil archivé dans une version différente de celle à partir de laquelle il a été exporté, un message d'erreur est enregistré dans ns.log.

La fonctionnalité de profil d'exportation et d'importation est disponible dans l'interface graphique (GUI) et l'interface de ligne de commande (CLI). L'interface graphique est recommandée, car elle offre des options **d'action** faciles à utiliser. En cliquant sur un bouton, vous pouvez **exporter** ou **importer** toute la configuration d'un profil.

Exportation de profils de Web App Firewall avec l'interface de ligne de commande

Si vous utilisez l'interface de ligne de commande pour **exporter** un profil, vous devez **archiver** la configuration, puis **l'exporter**. Pour **importer** un profil, vous devez **importer** l'archive dans l'appliance NetScaler, puis exécuter la commande **restore** pour extraire la configuration. L'ensemble de commandes CLI suivant peut être utilisé pour exporter, importer et gérer les configurations de profils.

Commandes CLI pour exporter les archives :

- `archive appfw profile <name> <archivename> [-comment <string>]`
- `export appfw archive <name> <target>`

Commandes CLI pour importer des archives :

- **`import`** `appfw archive <src> <name> [-comment <string>]`
- `restore appfw profile <archivename>`

Commandes CLI pour gérer les archives :

- `show appfw archive`
- `rm appfw archive <name>`

L'exportation d'un profil à partir d'une appliance et l'importation vers une autre nécessite cinq étapes dans l'interface de ligne de commande. Les 3 premières étapes sont exécutées sur l'appliance source sur laquelle la configuration de profil est initialement créée, et les 2 étapes suivantes sont exécutées sur l'appliance cible sur laquelle la configuration de profil doit être répliquée.

Exporter le profil à partir de l'appliance NetScaler source :

Étape 1 : Créer une archive du profil configuré.

Étape 2 : Exportez l'archive vers le système de fichiers NetScaler.

Étape 3 : Utilisez un utilitaire de transfert de fichiers tel que scp pour transférer le fichier d'archive exporté à partir de l'appliance NetScaler A vers l'appliance NetScaler cible.

Importer le profil vers l'appliance NetScaler cible :

Étape 4 : Exécutez la commande import pour importer le fichier archivé. Vous pouvez importer l'archive à partir du système de fichiers local de NetScaler ou utiliser le protocole HTTP ou HTTPS pour importer l'archive à partir d'un serveur à l'aide de l'URL.

Étape 5 : Exécutez la commande restore pour restaurer la configuration du profil à partir de l'archive importée

Pour exporter un profil de Web App Firewall à l'aide de l'interface de ligne de commande :

Tout d'abord, **archivez** la configuration du profil, puis **exportez** l'archive vers un emplacement cible. À l'invite de commandes, tapez les commandes suivantes :

```
archive appfw profile <profileName> <archiveName>
```

où :

- <profileName> est le nom du profil à archiver.
- <archiveName> est le nom du fichier d'archive à créer.

L'exécution de la commande ci-dessus crée 2 instances du fichier d'archive. Un dans le dossier /var/tmp et un autre dans le dossier /var/archive/appfw.

```
export appfw archive <archiveName> <target>
```

où :

- <archiveName> est le nom de l'archive à exporter. (Le même nom que dans la commande précédente.
- <target> est un chemin de fichier commençant par local : comme préfixe, suivi de <archiveName>.

L'exécution de la commande export enregistre le fichier d'archive exporté sur le système de fichiers de votre appliance NetScaler dans le dossier /var/tmp.

Exemples :

```
> archive appfw profile test_pr archived_test_pr
```

```
> export appfw archive archived_test_pr local:dutA_test_pr
```

Après l'exécution des deux commandes ci-dessus, le dossier /var/tmp contient le fichier archived_test_pr et la copie exportée, duta_test_pr, dont la taille est identique. À partir de l'interface de ligne de commande, vous pouvez passer dans le shell pour accéder au dossier afin de vérifier que ces fichiers sont présents.

Après avoir exporté le fichier d'archive, vous pouvez utiliser **scp** ou un autre utilitaire de transfert de fichiers de ce type pour transférer une copie du fichier d'archive de l'appliance NetScaler sur laquelle ils ont été créés vers votre appliance NetScaler cible.

Importation de profils de Web App Firewall à l'aide de l'interface de ligne de commande

Après avoir correctement scp le fichier archivé de l'appliance source vers l'appliance cible, vous êtes prêt à **importer** l'archive du profil, puis à exécuter la commande **restore** pour répliquer la configuration du profil sur l'appliance cible.

Connectez-vous à l'appliance cible. Passez dans le shell et le cd dans le dossier /var/tmp pour vérifier que la taille du fichier scp 'd de cette appliance correspond à la taille du fichier archivé d'origine sur l'appliance source. Quittez le shell pour revenir à la ligne de commande.

Pour importer un profil à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez les commandes suivantes :

```
import appfw archive <src> <name> [-comment <string>]
```

où

- <src> est l'emplacement du fichier d'archive après qu'il a été transféré à partir de l'appliance source sur laquelle il a été créé. Vous pouvez utiliser un système de fichiers local et un nom de fichier. Si vous avez placé l'archive sur un serveur, vous pouvez utiliser une URL pour importer le fichier archivé. Si le chemin d'accès ou le nom du fichier contient des espaces, placez l'URL entre guillemets droits.
- <name> est le nom du fichier d'archive à importer.
- <string> est une description facultative du but de l'archive.

```
restore appfw profile <archiveName>
```

Exemples :

A. Importer à partir d'un fichier local suivi de la restauration :

```
> import appfw archive local:dutA_test_pr dut2_test_pr
```

```
> restore appfw profile dut2_test_pr
```

B. Importer à partir de l'URL suivie de la restauration :

```
import appfw archive http://10.217.30.16/FFC/Profile_ImportExport/
dutA_test_pr.tgz my_archive
restore appfw profile my_archive
```

Cet exemple restaure le profil test_pr ainsi que tous les objets liés (tels que les signatures, la page d'erreur html, les règles de relaxation, etc.) sur l'appliance NetScaler cible.

Vous pouvez utiliser les commandes CLI suivantes pour accéder aux pages de manuel pour plus de détails.

- man archive appfw profil
- man export archive appfw
- man import archive appfw
- homme restaurer profil appfw
- man show archive appfw
- archive man rm appfw

Exportation et importation de profils de Web App Firewall à l'aide de l'interface graphique

L'interface graphique est plus facile à utiliser que l'interface de ligne de commande. L'utilitaire effectue à la fois les opérations d'archivage et d'exportation lorsque vous cliquez sur **Exporter**. De même, il exécute à la fois l'importation et la restauration lorsque vous cliquez sur **Importer**. L'interface graphique peut accéder au système de fichiers local de l'ordinateur à partir duquel vous accédez à l'utilitaire. Vous pouvez exporter une copie de l'archive et l'enregistrer sur votre ordinateur local. Vous pouvez ensuite importer cette copie directement dans l'appliance cible sans avoir à transférer manuellement le fichier d'archive d'une appliance à l'autre (s).

Pour exporter un profil de Web App Firewall à l'aide de l'interface graphique :

1. Accédez à **Configuration** > **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet d'informations, sélectionnez un profil à exporter. Cliquez sur **Actions** et sélectionnez **Exporter** pour télécharger et enregistrer une copie dans le système de fichiers local de votre ordinateur.

Pour importer un profil de Web App Firewall à l'aide de l'interface graphique :

1. Accédez à **Configuration** > **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet d'informations, cliquez sur **Actions** et sélectionnez **Importer**. Dans le volet Importer le profil du Web App Firewall, la zone de sélection Importer de* vous offre 2 options :

URL : vous pouvez choisir d'importer une archive en spécifiant une **URL**. Lorsque cette option est sélectionnée, vous devez indiquer un chemin absolu pour le fichier archivé dans la zone de saisie **URL**.

Fichier : Vous pouvez choisir d'importer une archive à partir du **fichier** local. Lorsque cette option est sélectionnée, un champ de sélection **Fichier local** s'affiche. Vous pouvez parcourir les fichiers locaux de votre ordinateur pour sélectionner le fichier d'archive cible.

Cliquez sur **Créer** pour importer l'archive spécifiée. L'exécution réussie de l'opération d'importation crée la configuration de profil sur l'appliance cible.

Résumé

- Vous pouvez répliquer l'intégralité de la configuration (y compris tous les objets d'importation ainsi que les règles de relaxation configurées pour le profil) sur plusieurs appliances, sans devoir répéter les étapes de configuration, à l'aide des fonctionnalités d'exportation et d'importation des profils.
- Les objets importés, tels que les signatures, WSDL, Schéma, page d'erreur, etc., sont inclus dans le fichier tar archivé et répliqués sur l'appliance cible.
- Les types de champs personnalisés sont inclus dans le fichier tar archivé et répliqués sur l'appliance cible.

- Les liaisons de stratégie du profil archivé ne sont pas répliquées lorsque la configuration est restaurée. Vous devez configurer la stratégie et la lier au profil après avoir importé le profil dans l'appliance.
- Le nom du fichier d'archive peut avoir jusqu'à 31 caractères. Comme pour les noms de profils, un nom d'archive doit commencer par un caractère alphanumérique ou un trait de soulignement et contenir uniquement des caractères alphanumériques et des traits de soulignement (_), nombre (#), point (.), espace (), deux-points (:), arobase (@), égal à (=) ou tiret (-).
- Les commentaires associés à l'archive doivent être suffisamment descriptifs pour indiquer le but de la configuration archivée. La longueur maximale autorisée pour un commentaire est de 255 caractères.
- La `clear config -force basic` commande ne supprime pas les profils archivés.
- La fonctionnalité de profil d'importation et d'exportation est prise en charge dans les déploiements haute disponibilité (HA).

Conseils de débogage

- Surveillez le fichier /var/log/ns.log pendant l'exécution des commandes pour voir s'il y a des messages d'ERREUR.
- Des journaux supplémentaires (_restore.log, remove.log, import.log) sont générés dans le dossier /var/tmp/. Ils peuvent aider à déboguer les problèmes pendant les opérations correspondantes. Lorsque ces journaux atteignent un Mo de taille, les messages de journal sont purgés pour réduire le fichier journal à un quart de la taille d'origine.
- Si la commande d'importation échoue lorsque vous utilisez l'option URL au lieu du système de fichiers local, vérifiez que les paramètres du serveur de noms DNS et du routage sont correctement configurés.
- Si vous utilisez le protocole HTTPS pour importer l'archive, la commande peut échouer si le serveur HTTPS nécessite une authentification de certificat client.

Facilité de dépannage grâce aux journaux du Web Application Firewall

May 5, 2023

En cas d'attaque de sécurité, il est important de capturer la journalisation WAF détaillée sur l'appliance. Pour cela, vous pouvez configurer le paramètre « VerboseLogLevel » sur un profil de pare-feu d'application.

Prenons l'exemple d'une attaque de sécurité pour le trafic Web. Lorsque l'appliance reçoit le trafic, les détails de violation tels que les détails de l'en-tête HTTP, le modèle de journal et les informations de charge utile du modèle sont consignés et envoyés au serveur ADM. Le serveur ADM surveille les journaux détaillés et les affiche sur la page Security Insight à des fins de surveillance et de suivi.

Configuration du niveau de journalisation détaillé à l'aide de l'interface de commande

Pour capturer des journaux WAF détaillés, configurez la commande suivante.
Dans l'interface de commande, tapez :

```
set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload|
patternPayloadHeader)
```

Exemple

```
set appfw profile profile1 -VerboseLogLevel patternPayloadHeader
```

Les niveaux de journalisation disponibles sont les suivants :

1. Motif. Consigne uniquement le modèle de violation.
2. Charge utile du motif. Consigne le modèle de violation et 150 octets de charge utile d'élément de champ supplémentaire.
3. En-tête de charge utile du motif Patter de violation des journaux, 150 octets de charge utile d'élément de champ supplémentaire et informations d'en-tête HTTP.

Configuration du niveau de journalisation détaillé à l'aide de l'interface graphique NetScaler

Suivez la procédure ci-dessous pour configurer le niveau de journalisation détaillé dans le profil WAF.

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.
2. Sur la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page de **profil du NetScaler Web App Firewall**, cliquez sur Paramètres du **profil sous Paramètresavancés**.
4. Dans la section **Paramètres du profil**, sélectionnez le niveau de journal WAF détaillé dans le champ Niveau de journal détaillé.
5. Cliquez sur **OK** et **Terminé**.



Journalisation détaillée pour les contrôles de sécurité JSON (SQL, CMD et script intersite)

Lorsqu'un type de demande entrante est JSON, vous pouvez configurer le paramètre de niveau de journal détaillé pour capturer des journaux de violation détaillés tels que le modèle, la charge utile du modèle et les informations d'en-tête HTTP. Les détails du journal sont ensuite envoyés au serveur NetScaler ADM pour surveiller et résoudre les violations JSON. Le message de consignation verbeux n'est pas stocké dans le fichier ns.log.
La journalisation détaillée pour la protection de la sécurité des types de contenu JSON peut être configurée pour les types de violation suivants :

- Injection SQL
- Scriptage intersite
- Injection de commande

Configurer la journalisation détaillée pour la protection de sécurité JSON à l'aide de l'interface de ligne

Pour capturer des informations d'en-tête HTTP détaillées sous forme de journaux, vous pouvez configurer le paramètre de journalisation détaillé dans le profil Web App Firewall. À l'invite de commande, tapez :

```
set appfw profile <profile_name> -VerboseLogLevel ( pattern |
   patternPayload | patternPayloadHeader )
<!--NeedCopy-->
```

Exemple :

```
set appfw profile profile1 -VerboseLogLevel patternPayloadHeader
```

Les niveaux de journalisation disponibles sont les suivants :

Motif. Consigne uniquement le modèle de violation.

Charge utile du motif. Modèle de violation des journaux et 150 octets de charge utile JSON supplémentaire.

En-tête de charge utile du motif Patter de violation des journaux, 150 octets de charge utile JSON supplémentaire et informations d'en-tête HTTP.

Configuration du niveau de journalisation détaillé à l'aide de l'interface graphique NetScaler

Suivez la procédure ci-dessous pour configurer le niveau de journalisation détaillé pour la protection de sécurité JSON.

1. Dans le volet de navigation, accédez à **Sécurité > Profils**.
2. Sur la page **Profils**, cliquez sur **Ajouter**.
3. Sur la page de **profil du pare-feu NetScaler Web App**, cliquez sur **Contrôles de sécurité** sous Paramètres **avancés**.
4. Dans la section **Contrôles de sécurité**, sélectionnez **JSON** et cliquez sur **Paramètres d'action**.
5. Sur la page **Paramètres de sécurité JSON**, définissez le paramètre de **niveau de journalisation détaillé** .
6. Cliquez sur **OK** et **Terminé**.

Sur la base des détails capturés par la journalisation détaillée JSON de NetScaler WAF, les détails des violations suivants peuvent être inspectés sur le serveur NetScaler ADM.



Protection contre le chargement de fichiers

July 31, 2023

De nombreux attaquants tentent de télécharger du code malveillant, des virus ou des logiciels malveillants sous forme de pièces jointes lors de la soumission de formulaires multiples. Il est important de protéger notre réseau et de surmonter ces menaces. Pour empêcher de tels téléchargements de fichiers malveillants, un administrateur NetScaler configure un ensemble de formats de téléchargement de fichiers autorisés dans le profil WAF. Ce faisant, vous limitez les téléchargements de fichiers à des formats spécifiques et protégez l'appliance contre les téléchargements de fichiers malveillants. La protection ne fonctionne que lorsque vous désactivez l'option `ExcludeFileUploadFormChecks` dans le profil WAF.

Fonctionnement du téléchargement de fichiers

Lorsque vous configurez des formats de téléchargement de fichiers autorisés, l'interaction entre les composants est la suivante :

- La demande du client comporte une soumission de formulaire avec un type de téléchargement de fichier, par exemple PDF.
- Dans le cadre du contrôle de sécurité, WAF inspecte la charge utile de la demande et valide le type de fichier (sur la base de numéros de signature magiques).
- Si le type de fichier n'est pas dans un format pris en charge, l'action correspondante basée sur la liaison de type de fichier est appliquée.
- Pour valider le type de fichier, l'appliance inspecte la charge utile et vérifie les nombres magiques connus aux décalages connus. Chaque type de fichier possède une séquence de nombres magiques qui valide le type de fichier.

Configurer le chargement du type de fichier à l'aide de NetScaler CLI

Pour configurer les formats de fichiers autorisés, l'appliance utilise un profil WAF lié aux paramètres de chargement de fichiers.

1. Configurer le profil du pare-feu d'application Web

À l'invite de commande, tapez :

```
set appfw profile <profile_name> [-fileUploadTypesAction <fileUploadTypesAction
>]<fileUploadTypesAction> = ( none | block | log | stats )
```

Exemple

```
set appfw profile profile1 -fileUploadTypesAction block
```

1. Liez le profil de pare-feu d'application Web avec les paramètres de téléchargement de fichiers. La commande lie l'exemption (relaxation) ou la règle spécifiée au profil de pare-feu d'application spécifié.

À l'invite de commande, tapez :

```
bind appfw profile <profile_name> - fileUploadType <form_field > <form_action_url
> [-isNameRegex ( REGEX | NOTREGEX )] -fileType <fileType> ( pdf | msdoc |
text | image | any)
```

> **Remarque :**
>
> Le nom du champ de formulaire est un type d'expression régulière. La valeur par défaut est NOTREGEX.

Exemple

```
> bind appfw profile test -fileuploadType thefile "http://10.10.10.10/
fileupload_sample/upload.php"-isNameRegex NOTREGEX -filetype image
```


–>

Configuration de la protection de sécurité du téléchargement de fichiers à l'aide de l'interface graphique NetScaler

1. Dans le volet de navigation, accédez à **Sécurité** > **Profils**.
2. Sur la page Profils, cliquez sur **Ajouter**.
3. Sur la page Profil de **NetScaler Web App Firewall**, cliquez sur **Contrôles de sécurité** sous **Paramètres avancés**.
4. Dans la section **Contrôles de sécurité**, sélectionnez **Types de téléchargement de fichiers** et cliquez sur **Paramètres d'action**.



5. Dans la page **Paramètres des types de téléchargement de fichiers**, définissez l'action de chargement de fichiers.
6. Cliquez sur **OK**.



7. Sur la page de profil de **NetScaler Web App Firewall**, cliquez sur **OK** et cliquez sur **Terminé**.

Configurer la règle de relaxation pour le téléchargement de fichiers à l'aide de l'interface graphique NetScaler

Vous pouvez assouplir la protection de sécurité du chargement de fichiers pour éviter les faux positifs. Par exemple, l'appliance peut bloquer les chargements de fichiers, mais vous pouvez ajouter une règle de relaxation pour autoriser le téléchargement de fichiers à partir de sites Web spécifiques. Ce faisant, l'appliance contourne l'inspection de sécurité pour le champ de formulaire spécifié et autorise les utilisateurs à télécharger des fichiers à partir du site Web mentionné dans l'URL de l'action.

> **Remarque :**
>
> La validation du chargement de fichiers échoue si la **règle de correction des types de chargement de fichiers** n'est pas activée.

Procédez comme suit pour créer une règle de relaxation.

1. Dans le volet de navigation, accédez à **Sécurité** > **NetScaler Web App Firewall** > **Profils**.
2. Sur la page Profils, cliquez sur **Ajouter**.
3. Sur la page de profil de **NetScaler Web App Firewall**, cliquez sur **Règles de relaxation** sous **Paramètres avancés**.
4. Dans la section **Règles de relaxation**, sélectionnez **Types de téléchargement de fichiers** et cliquez sur **Modifier**.



5. Dans la page **Règles de réévaluation des types de chargement de fichiers**, cliquez sur **Ajouter**.
6. Dans la page **Règle de relaxation des types de chargement de fichiers**, définissez les paramètres suivants :
   a) Activé : sélectionnez cette option pour activer la règle de relaxation.
   b) Est-ce que le nom du champ de formulaire est Regex - Sélectionnez cette option pour mettre à jour un modèle de regex pour le nom du champ de formulaire.

c) Nom du champ du formulaire : entrez le nom du fichier qui ne nécessite pas de contrôle de sécurité.
d) URL de l'action : URL de soumission du formulaire qui doit être exemptée des contrôles de sécurité.
e) Type de fichier : format de fichier pris en charge qui peut être chargé.
f) Commentaires : brève description du chargement du fichier.

7. Cliquez sur **Create**.



8. Sur la page de profil de **NetScaler Web App Firewall**, cliquez sur **OK** et cliquez sur **Terminé**.



Configuration et utilisation de la fonction d'apprentissage

May 5, 2023

La fonction d'apprentissage est un filtre de modèle répétitif qui observe l'activité sur un site Web ou une application protégé par le Web App Firewall, afin de déterminer ce qui constitue une activité normale sur ce site Web ou cette application. Il génère ensuite une liste d'un maximum de 2 000 règles ou exceptions (assouplissements) suggérées pour chaque contrôle de sécurité qui inclut la prise en charge de la fonction d'apprentissage. Les utilisateurs trouvent normalement plus facile de configurer les relaxations en utilisant la fonction d'apprentissage qu'en saisissant manuellement les relaxations nécessaires.

Les contrôles de sécurité qui prennent en charge la fonctionnalité d'apprentissage sont les suivants :

- Vérification d'URL de démarrage
- Contrôle de cohérence des cookies
- Vérification de cohérence des champs de formulaire
- Vérification des formats de champ
- Vérification du balisage des formulaires CSRF
- Vérification d'injection HTML SQL
- Vérification des scripts intersites HTML
- Vérification du déni de service XML
- Vérification des pièces jointes XML
- Vérification d'interopérabilité des services Web

Vous réalisez deux types d'activités différents lorsque vous utilisez la fonction d'apprentissage. Tout d'abord, vous activez et configurez la fonctionnalité pour l'utiliser. Vous pouvez connaître tout le trafic vers vos applications Web protégées ou configurer une liste d'adresses IP (appelée liste *Ajouter des clients d'apprentissage fiables*) à partir de laquelle la fonctionnalité d'apprentissage peut générer des recommandations. Ensuite, une fois que la fonctionnalité a été activée et a traité une certaine quantité de trafic vers vos sites Web protégés, vous passez en revue la liste des règles et assouplissements suggérés (règles apprises) et marquez chacun d'entre eux avec l'une des désignations suivantes :

- **Éditer et déployer.** La règle est extraite dans la boîte de dialogue Modifier afin que vous puissiez la modifier, et le formulaire modifié est déployé.
- **Déployer.** La règle apprise non modifiée est placée dans la liste des règles ou des assouplissements pour ce contrôle de sécurité.
- **Skip.** La règle apprise est placée sur une liste de règles ou d'assouplissements qui ne sont pas déployés. La règle apprise est supprimée lorsqu'elle est ignorée. Cependant, comme ils ne sont pas ajoutés aux relaxations, ils peuvent être réappris.

L'apprentissage n'est pas effectué uniquement lorsque des relaxations sont en place, à l'exception des règles de format de champ. Lorsque les règles sont ignorées, elles sont uniquement supprimées de la base de données apprise. Comme les relaxations ne sont pas ajoutées, elles peuvent être réapprises. Lorsque les règles sont déployées, elles sont supprimées de la base de données apprise et des assouplissements sont également ajoutés pour les règles. Au fur et à mesure que des relaxations sont ajoutées, elles ne seront plus réapprises. Pour la protection du format de terrain, l'apprentissage est

effectué indépendamment des relaxations.

Bien que vous puissiez utiliser l'interface de ligne de commande pour la configuration de base de la fonctionnalité d'apprentissage, la fonctionnalité est principalement conçue pour la configuration via l'assistant Web App Firewall ou l'interface graphique. Vous ne pouvez effectuer qu'une configuration limitée de la fonction d'apprentissage à l'aide de la ligne de commande.

L'assistant intègre la configuration des fonctionnalités d'apprentissage à la configuration du Web App Firewall dans son ensemble. Il s'agit donc de la méthode la plus simple pour configurer cette fonctionnalité sur une nouvelle appliance NetScaler ou lors de la gestion d'une configuration simple du Web App Firewall. Le visualiseur graphique et l'interface manuelle fournissent tous deux un accès direct à toutes les règles apprises pour tous les contrôles de sécurité et sont donc souvent préférables lorsque vous devez revoir les règles apprises pour de nombreux contrôles de sécurité.

La taille de la base de données d'apprentissage est limitée à 20 Mo, ce qui est atteint après la génération d'environ 2 000 règles ou relaxations apprises par contrôle de sécurité pour lequel l'apprentissage est activé. Si vous ne révisez pas régulièrement et que vous n'approuvez pas ou ignorez les règles apprises et que cette limite est atteinte, une erreur est consignée dans le journal NetScaler et aucune autre règle apprise n'est générée tant que vous n'avez pas examiné les règles apprises et les assouplissements existants.

Si l'apprentissage s'arrête parce que la base de données a atteint sa taille limite, vous pouvez recommencer l'apprentissage soit en révisant les règles apprises et les relaxations existantes, soit en réinitialisant les données d'apprentissage. Une fois que les règles ou les assouplissements apprises sont approuvés ou ignorés, ils sont supprimés de la base de données. Après avoir réinitialisé les données d'apprentissage, toutes les données d'apprentissage existantes sont supprimées de la base de données et sont réinitialisées à leur taille minimale. Lorsque la taille de la base de données est inférieure à 20 Mo, l'apprentissage redémarre automatiquement.

Pour configurer les paramètres d'apprentissage à l'aide de l'interface de ligne de commande

Spécifiez le profil Web App Firewall à configurer et, pour chaque contrôle de sécurité que vous souhaitez inclure dans ce profil, spécifiez le seuil minimum ou le seuil de pourcentage. Le seuil minimum est un entier représentant le nombre minimum de sessions utilisateur que le Web App Firewall doit traiter avant d'apprendre une règle ou un assouplissement (valeur par défaut : 1). Le seuil de pourcentage est un entier représentant le pourcentage de sessions utilisateur dans lesquelles le Web App Firewall doit observer un modèle particulier (URL, cookie, champ, pièce jointe ou violation de règle) avant d'apprendre une règle ou un assouplissement (valeur par défaut : 0). Utilisez les commandes suivantes :

- `set appfw learningsettings <profileName> [-startURLMinThreshold <positive_integer>] [-startURLPercentThreshold <positive_integer>] [-`


```
cookieConsistencyMinThreshold <positive_integer>] [-cookieConsistencyPercentThres
 <positive_integer>] [-CSRFtagMinThreshold <positive_integer>] [-
CSRFtagPercentThreshold <positive_integer>] [-fieldConsistencyMinThreshold
 <positive_integer>] [-fieldConsistencyPercentThreshold <positive_integer
>] [-crossSiteScriptingMinThreshold <positive_integer>] [-crossSiteScriptingPerce
 <positive_integer>] [-SQLInjectionMinThreshold <positive_integer>] [-
SQLInjectionPercentThreshold <positive_integer>] [-fieldFormatMinThreshold
 <positive_integer>] [-fieldFormatPercentThreshold <positive_integer>]
 [-XMLWSIMinThreshold <positive_integer>] [-XMLWSIPercentThreshold <
positive_integer>] [-XMLAttachmentMinThreshold <positive_integer>] [-
XMLAttachmentPercentThreshold <positive_integer>]
```

- `save ns config`

Exemple

L'exemple suivant active et configure les paramètres d'apprentissage dans le profil pour le contrôle de sécurité Injection HTML SQL. Il s'agit d'une configuration initiale appropriée d'apprentissage du banc d'essai, dans laquelle vous avez un contrôle total sur le trafic envoyé au Web App Firewall.

```
1 set appfw learningsettings pr-basic -SQLInjectionMinThreshold 10
2 set appfw learningsettings pr-basic -SQLInjectionPercentThreshold 70
3 save ns config
4 <!--NeedCopy-->
```

Pour réinitialiser les paramètres d'apprentissage par défaut à l'aide de l'interface de ligne de commande

Pour supprimer toute configuration personnalisée des paramètres d'apprentissage pour le profil et le contrôle de sécurité spécifiés, et rétablir les paramètres d'apprentissage par défaut, à l'invite de commandes, tapez les commandes suivantes :

```
- unset appfw learningsettings <profileName> [-startURLMinThreshold
   ] [-startURLPercentThreshold] [-cookieConsistencyMinThreshold] [-
  cookieConsistencyPercentThreshold] [-CSRFtagMinThreshold ] [-CSRFtagPercentThresh
   ] [-fieldConsistencyMinThreshold ] [-fieldConsistencyPercentThreshold
  ] [-crossSiteScriptingMinThreshold ] [-crossSiteScriptingPercentThreshold
   ] [-SQLInjectionMinThreshold ] [-SQLInjectionPercentThreshold ] [-
  fieldFormatMinThreshold] [-fieldFormatPercentThreshold ] [-XMLWSIMinThreshold
   ] [-XMLWSIPercentThreshold ] [-XMLAttachmentMinThreshold ] [-XMLAttachmentPercen
  ]
- save ns config
```


Pour afficher les paramètres d'apprentissage d'un profil à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
show appfw learningsettings <profileName>
```

Pour afficher les règles apprises ou les assouplissements non revus pour un profil à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
show appfw learningdata <profileName> <securityCheck>
```

Pour supprimer des règles apprises ou des relaxations spécifiques non révisées de la base de données d'apprentissage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
rm appfw learningdata <profileName> (-startURL <expression> | -cookieConsistency
 <string> | (-fieldConsistency <string> <formActionURL>)| (-crossSiteScripting
 <string> <formActionURL>)| (-SQLInjection <string> <formActionURL>)| (-
fieldFormat <string><formActionURL>)| (-CSRFTag <expression> <CSRFFormOriginURL
>)| -XMLDoSCheck <expression> | -XMLWSICheck <expression> | -XMLAttachmentCheck
 <expression>)[-TotalXMLRequests]
```

Exemple

L'exemple suivant supprime tous les relaxations apprises non révisées pour le profil, vérification de sécurité HTML SQL Injection, qui s'appliquent au champ de **formulaire LastName** .

```
1 rm appfw learningdata pr-basic -SQLInjection LastName
2 <!--NeedCopy-->
```

Pour supprimer toutes les données apprises non examinées à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
reset appfw learningdata
```


Pour exporter les données d'apprentissage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
export appfw learningdata <profileName> <securitycheck>[-target <string>]
```

Exemple

L'exemple suivant exporte les relaxations apprises pour le profil et le contrôle de sécurité HTML SQL Injection vers un fichier au format de valeurs séparées par des virgules (CSV) dans le répertoire /var/learnt_data/ sous le nom de fichier spécifié dans le paramètre -target.

```
1 export appfw learningdata pr-basic SQLInjection -target sqli_ld
2 <!--NeedCopy-->
```

Pour configurer la fonction d'apprentissage à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet **Profils**, sélectionnez le profil, puis cliquez sur **Modifier**.
3. Cliquez sur **Règles apprises** dans la section **Paramètres avancés** .
4. Dans la section **Règles apprises**, sélectionnez un contrôle de sécurité et cliquez sur **Paramètres**.
5. Dans la page **Paramètres du contrôle de sécurité**, définissez les paramètres suivants :
   a) **Seuil de nombre minimum.** Selon les paramètres d'apprentissage du contrôle de sécurité que vous configurez, le seuil de nombre minimum peut faire référence au nombre minimum de sessions utilisateur totales qui doivent être observées, au nombre minimum de demandes qui doivent être observées ou au nombre minimum de fois qu'un champ de formulaire spécifique doit être observé, avant qu'une relaxation apprise ne soit générée. Par défaut : 1
   b) **Pourcentage de fois le seuil.** Selon les paramètres d'apprentissage du contrôle de sécurité que vous configurez, le seuil de pourcentage de fois peut faire référence au pourcentage du nombre total de sessions utilisateur observées qui ont enfreint le contrôle de sécurité, au pourcentage de demandes ou au pourcentage de fois qu'un champ de formulaire correspondait à un type de champ particulier, avant un une relaxation apprise est générée. Par défaut : 0
6. Cliquez sur **OK** et sur **Fermer**.



7. Cliquez sur **Supprimer toutes les données apprises** pour supprimer toutes les données apprises et réinitialiser la fonction d'apprentissage, afin qu'elle doive recommencer ses observations depuis le début.

   > **Remarque :**
   >
   > Ce bouton supprime uniquement les recommandations apprises qui n'ont pas été examinées, approuvées ou ignorées. Il ne supprime pas les relaxations apprises qui ont été acceptées et déployées.

8. Pour limiter le moteur d'apprentissage au trafic provenant d'un ensemble spécifique d'adresses IP, cliquez sur **Trusted Learning Clients**, puis ajoutez les adresses IP que vous souhaitez utiliser à la liste.

   a) Pour ajouter une adresse IP ou une plage d'adresses IP à la liste Trusted Learning Clients, cliquez sur **Ajouter**.
   b) Dans la boîte de dialogue **Ajouter des clients de formation fiables**, zone de liste IP des clients de confiance, tapez l'adresse IP ou une plage d'adresses IP au format CIDR.
   c) Dans la zone de texte Commentaires, saisissez un commentaire décrivant cette adresse IP ou cette plage.
   d) Cliquez sur **Créer** pour ajouter votre nouvelle adresse IP ou plage à la liste.
   e) Pour modifier une adresse IP ou une plage existante, cliquez sur l'adresse IP ou la plage, puis sur **Ouvrir**. À l'exception du nom, la boîte de dialogue qui s'affiche est identique à la boîte de dialogue **Ajouter des clients de formation approuvés** .
   f) Pour désactiver ou activer une adresse IP ou une plage, mais la laisser dans la liste, cliquez sur l'adresse IP ou la plage, puis cliquez sur **Désactiver ou Activer**, le cas échéant.

g) Pour supprimer complètement une adresse IP ou une plage, cliquez sur l'adresse IP ou la plage, puis sur **Supprimer**.

9. Cliquez sur **Fermer** pour revenir à la page Configurer le profil du Web App Firewall.
10. Cliquez sur **Terminé**.

Pour consulter les règles ou les relaxations apprises à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Profils**.
2. Dans le volet **Profils**, sélectionnez le profil, puis cliquez sur **Modifier**.
3. Cliquez sur **Règles apprises** dans la section **Paramètres avancés** .
4. Dans la section **Règles apprises**, sélectionnez un contrôle de sécurité et cliquez sur **Paramètres**.
5. Pour examiner les données apprises de manière hiérarchique sous forme d'arbre de ramification, vous permettant de choisir des modèles généraux qui correspondent à de nombreux modèles appris, cliquez sur **Visualiseur**.
6. Si vous avez choisi de passer en revue les modèles appris réels, effectuez les étapes suivantes.
7. Sélectionnez la première relaxation apprise et choisissez comment la gérer.
   a) Pour modifier puis accepter la relaxation, cliquez sur **Modifier et déployer**, modifiez l'expression régulière de relaxation, puis cliquez sur **OK**.
   b) Pour accepter la relaxation sans modification, cliquez sur **Déployer**.
   c) Pour supprimer la relaxation de la liste sans la déployer, cliquez sur **Ignorer**.
   d) Répétez l'étape précédente pour passer en revue chaque relaxation apprise supplémentaire.
8. Cliquez sur **Fermer** pour revenir à la boîte de dialogue **Gérer les règles apprises** .
9. Cliquez sur **Terminé**.



Profilage dynamique

May 5, 2023

La fonction d'apprentissage est un filtre de modèles qui observe et apprend les activités sur le serveur principal. Sur la base de l'observation, le moteur d'apprentissage génère jusqu'à 2000 règles ou exceptions (assouplissements) pour chaque contrôle de sécurité. Pour automatiser le processus et déployer automatiquement les règles de relaxation, l'appliance NetScaler utilise le profilage dynamique.

Avec le profilage dynamique, l'appliance enregistre les données apprises pour un seuil prédéfini et envoie une alerte SNMP à l'utilisateur. Si l'utilisateur ne saute pas les données pendant un délai de grâce, l'appliance les déploie automatiquement en tant que règle de relaxation. Auparavant, l'utilisateur devait déployer manuellement les règles de relaxation. Actuellement, le profilage dynamique n'est disponible que pour les contrôles de sécurité suivants :

1. Injection HTML SQL
2. Script HTML Cross Site
3. Format de champ
4. URL de démarrage
5. Type de contenu
6. Formats de champs
7. Balisage de formulaire CSRF
8. Cohérence des cookies
9. Refuser URL
10. Dépassement de tampon
11. Carte de crédit
12. Protection du type de contenu
13. Protection contre les injections JSON Cmd

Par exemple, considérez la vérification de sécurité HTML SQL Injection activée avec le profilage dynamique. Vous pouvez utiliser la formation pour une liste d'adresses IP (appelée liste des clients de formation approuvés) à partir desquelles la fonctionnalité de formation doit générer des recommandations. Pour configurer une liste de clients approuvés, consultez la rubrique Apprentissage des clients de confiance. Si le trafic entrant comporte des violations, il est enregistré en tant que données apprises. Si les données apprises sont enregistrées dans le moteur d'apprentissage, la solution matérielle-logicielle envoie une alerte SNMP à l'utilisateur. Si l'utilisateur ne reconnaît pas un faux positif et n'ignore pas les données apprises dans un délai de grâce, l'appliance les déploie automatiquement en tant que règle de relaxation.

> **Remarque :**
> Après avoir configuré le profil dynamique, vous devez régulièrement revoir la configuration

> de l'appliance pour le déploiement automatique des règles de relaxation et l'enregistrer sur l'appliance.

Configurer le profilage dynamique à l'aide de l'interface de commande NetScaler

Le profilage dynamique est disponible pour les vérifications de sécurité de l'URL de démarrage, du script intersite HTML, du format des champs ou de l'injection SQL HTML. Pour configurer le profilage dynamique, vous devez suivre les étapes suivantes.

1. Configuration de l'apprentissage dynamique
2. Configuration de la période de grâce du déploiement automatique

Configuration de l'apprentissage dynamique

Dans un premier temps, vous devez configurer l'apprentissage dynamique sur votre solution matérielle-logicielle. À l'invite de commande, tapez :

```
set appfw profile <profile_name> dynamicLearning <security_checks>
```

Exemple

```
set appfw profile test1 dynamicLearning SQLInjection CrossSiteScripting
fieldFormat startURL
```

Configuration de la période de grâce du déploiement automatique

Une fois que vous avez activé la fonctionnalité sur des vérifications de sécurité spécifiques, vous devez configurer la période de grâce pour le déploiement automatique.

```
set appfw learningsettings <profile name> -crossSiteScriptingAutoDeployGracePeriod
 <seconds>

set appfw learningsettings <profile name> fieldFormatAutoDeploymentGracePeriod
 <seconds>

set appfw learningsettings <profile name> SQLInjectionAutoDeploymentGracePeriod
 <seconds>

set appfw learningsettings <profile name> -startURLAutoDeployGracePeriod <
seconds>
```


Exemple

```
set appfw learningsettings test1 -crossSiteScriptingAutoDeployGracePeriod 30
set appfw learningsettings test1 -startURLAutoDeployGracePeriod 7
set appfw learningsettings test1 -fieldFormatAutoDeploymentGracePeriod 10
set appfw learning settings test1 -SQLInjectionAutoDeploymentGracePeriod 12
```

> **Remarque :**
>
> Ici, la période de grâce du déploiement automatique est de quelques minutes.

Configuration du profilage dynamique à l'aide de l'interface graphique NetScaler

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profil**.
2. Dans le volet d'informations, sélectionnez un profil et cliquez sur **Modifier**.
3. Dans la page **Profil de Citrix Web App**, cliquez sur **Profilage dynamique** sous **Paramètres avancés**.



4. Dans la section **Profilage dynamique**, sélectionnez une vérification de sécurité et cliquez sur **Modifier**.



5. Dans la page **Paramètres de profilage et d'apprentissage dynamiques**, définissez la période de grâce du contrôle de sécurité.



6. Cliquez sur **OK** et **Terminé**.

Exportation et importation de règles de relaxation

Lorsque vous activez le profilage dynamique, les données apprises sont automatiquement déployées en tant que règles de relaxation. Parallèlement, l'appliance vous permet également d'exporter les règles de relaxation basées sur le profilage dynamique et les règles de relaxation régulières. Vous pouvez exporter les règles depuis l'environnement de transit et les importer dans l'environnement de production.

> **Remarque :**
>
> Lorsque vous importez des règles dans l'environnement de production, vous devez vous assurer que le processus est additif et qu'il ne remplace pas la configuration existante.

Comment exporter et importer des règles de relaxation

Pour exporter et importer les règles de relaxation, vous devez effectuer les étapes suivantes :

1. Vous devez d'abord exporter les données de profilage dynamique. Pour cela, l'option d'exportation est disponible pour les règles de relaxation du profil WAF. Lorsque vous sélectionnez cette option, vous exportez les règles de relaxation de profilage dynamique et les règles de relaxation standard. Vous pouvez utiliser l'option d'exportation pour télécharger la configuration sous forme de bundle compressé sur la solution matérielle-logicielle.
2. Une fois que vous avez exporté les données depuis l'environnement intermédiaire, vous devez les importer vers une autre appliance NetScaler. Pour cela, vous devez utiliser l'option d'importation disponible dans les règles de relaxation du profil WAF. Lorsque vous sélectionnez cette option, la solution matérielle-logicielle importe les règles de relaxation spécifiées groupées et les restaure dans le profil WAF de la solution matérielle-logicielle sélectionnée.

> **Remarque :**
>
> Si vous souhaitez importer des règles de relaxation dans un profil WAF, il existe deux types d'action :
> Augmenter — Cette action garantit que l'importation est additive et ne remplace donc aucune configuration existante.
> Remplacer — Cette action remplace la configuration existante par la configuration présente dans le bundle d'exportation compressé. »

Importer le fichier de règles de relaxation archivées à l'aide de l'interface

Pour importer les règles de relaxation, vous devez importer l'archive dans l'appliance NetScaler, puis exécuter la commande de restauration pour extraire la configuration. L'ensemble de commandes CLI suivant peut être utilisé pour exporter, importer et gérer les configurations.

Pour importer le fichier archivé à partir de l'emplacement spécifique et restaurer, à l'invite de commandes, tapez :

```
import appfw archive <src> <name> [-comment <string>]
```

Où,
« src » : Indique la source du fichier d'archive tar sous la forme, `<protocol>://<host>[:<port>][/<path>]`
« name » : Indique le nom de l'archive.
« commentaire » : Commentaires associés à cette archive.

```
restore appfw profile <archivename> [-relaxationRules] [-importProfileName <string>] [-matchUrlString <string>] [-replaceUrlString <string>] [-overwrite] [-augment]
```

Où,
`archivename` : indique la source de l'archive tar. Il s'agit d'un argument obligatoire.
« RelaxationRules » : Possibilité d'importer toutes les règles de relaxation appfw.

`importProfileName`: indique le nom de profil créé ou mis à jour pour associer les règles de relaxation pendant l'opération de restauration.
« MatChurlString » : indique la chaîne URL d'action à correspondre dans les règles de relaxation archivées.

`replaceUrlString`: indique une chaîne à remplacer l'URL en action lors de la restauration des règles de relaxation.

`overwrite`: action de règles existantes pour purger les règles de relaxation existantes et les remplacer pendant l'importation.

`augment`: action de règles existantes pour augmenter les règles de relaxation lors de l'importation.

Exemple :

```
import appfw archive local: dutA_test_pr.tgz demo
restore appfw profile dutA_test_pr
```

Exportez le fichier archivé vers l'appliance sélectionnée à l'aide de l'interface de ligne de commande

Si vous utilisez l'interface de ligne de commande pour exporter les règles de relaxation appfw, vous devez archiver la configuration, puis l'exporter.
Pour archiver et exporter le fichier archivé, à l'invite de commandes, tapez :

```
archive appfw profile <name> <archivename> [-comment <string>]
```

Où,
`archive name` : indique la source de l'archive tar. Il s'agit d'un argument obligatoire.

`name`: indique le nom du profil appfw contenant les règles de relaxation à exporter

```
export appfw archive <name> <target>
```

Où,
nom. Nom de l'archive tar. Il s'agit d'un argument obligatoire. Longueur maximale : 31
cibles. Chemin d'accès au fichier à exporter. Il s'agit d'un argument obligatoire. Longueur maximale : 2047

Exemple :

```
> archive appfw profile test_pr archived_test_pr
> export appfw archive archived_test_pr local:dutA_test_pr
```

Pour exporter des règles de relaxation à l'aide de l'interface graphique NetScaler

Suivez les étapes ci-dessous pour exporter les règles de relaxation :

1. Accédez à **Sécurité** > **NetScaler Web App Firewall**.
2. Dans la page de détails, cliquez sur le lien **NetScaler Web App Firewall Profiles** dans la section **Résumé de la configuration** .
3. Sur la page de **profil du Web App Firewall NetScaler**, cliquez sur le lien **Règles de relaxation** dans la section **Paramètres avancés.**
4. Dans la section **Règles de relaxation**, cliquez sur **Exporter toutes les règles de relaxation**. L'action s'applique à tous les contrôles de sécurité et à ceux pour lesquels l'apprentissage dynamique est activé sur ce profil.



Pour importer des règles de relaxation à l'aide de l'interface graphique NetScaler

Suivez les étapes pour importer des règles de relaxation :

1. Accédez à **Sécurité** > **NetScaler Web App Firewall**.

2. Sur la page de détails, cliquez sur le lien **NetScaler Web App Firewall Profiles** dans la section **Résumé de la configuration** .
3. Sur la page de **profil du Web App Firewall NetScaler**, cliquez sur le lien **Règles de relaxation** dans la section **Paramètres avancés.**
4. Dans la section **Règles de relaxation**, cliquez sur **Importer toutes les règles de relaxation**.
5. Sur la page **Configurer le profil de NetScaler Web App Firewall**, définissez les paramètres suivants :
   a) Fichier local. Nom du fichier archivé compressé contenant les règles de relaxation.
   b) Nom du profil. Nom du profil auquel les règles de relaxation sont liées.
   c) Chaîne d'URL correspondante. Partie de l'URL qui correspond.
   d) Remplacez la chaîne d'URL. Partie de l'URL qui remplace la chaîne d'URL.
   e) Action de règle existante. Sélectionnez si la règle doit remplacer les règles existantes ou augmenter les règles existantes.
6. Cliquez sur **OK**.



Informations supplémentaires sur les profils

May 5, 2023

Vous trouverez ci-dessous des informations supplémentaires sur des aspects particuliers des profils Web App Firewall. Ces informations expliquent comment inclure des caractères spéciaux dans une règle de vérification de sécurité ou une relaxation, et comment utiliser des variables lors de la configuration des profils.

Support des variables de configuration

Au lieu d'utiliser des valeurs statiques, vous pouvez désormais utiliser des variables nommées NetScaler standard pour configurer les contrôles et les paramètres de sécurité du Web App Firewall. En créant des variables, vous pouvez plus facilement exporter puis importer des configurations vers de nouvelles appliances NetScaler, ou mettre à jour des appliances NetScaler existantes à partir d'un seul ensemble de fichiers de configuration. Cela simplifie les mises à jour lorsque vous utilisez une configuration de banc d'essai pour développer une configuration complexe de Web App Firewall adaptée à votre réseau et à vos serveurs locaux, puis que vous transférez cette configuration vers vos appliances NetScaler de production.

Vous créez des variables de configuration du Web App Firewall de la même manière que n'importe quelle autre variable nommée NetScaler, conformément aux conventions NetScaler standard. Vous pouvez créer une variable d'expression nommée à l'aide de la ligne de commande ou de l'interface graphique NetScaler.

Les URL et expressions suivantes peuvent être configurées avec des variables au lieu de valeurs statiques :

- **Start URL** (-starturl)
- **Deny URL** (-denyurl)
- **Form Action URL** for *Form Field Consistency Check* (-fieldconsistency)
- **Action URL** for *XML SQL Injection Check* (-xmlSQLInjection)
- **Action URL** for X*ML Cross-Site Scripting Check* (-xmlcross-site scripting)
- **Form Action URL** for *HTML SQL Injection Check* (-sqlInjection)
- **Form Action URL** for *Field Format Check* (-fieldFormat)
- **Form Origin URL** and **Form Action URL** for *Cross-Site Request Forgery (CSRF) Check* (-csrfTag)
- **Form Action URL** for *HTML Cross-Site Scripting Check* (-crossSiteScripting)
- **Safe Object** (-safeObject)
- **Action URL** for *XML Denial-of-Service (XDoS) check* (-XMLDoS)
- **URL** for *Web Services Interoperability check* (-XMLWSIURL)
- <**URL** for *XML Validation check* (-XMLValidationURL)

- **URL** for *XML Attachment check* (-XMLAttachmentURL)

Pour plus d'informations, voir Stratégies et expressions.

Pour utiliser une variable dans la configuration, vous placez le nom de la variable entre deux symboles à (@), puis l'utilisez exactement comme vous le feriez pour la valeur statique qu'elle remplace. Par exemple, si vous configurez la vérification Refuser l'URL à l'aide de l'interface graphique et que vous souhaitez ajouter la variable d'expression nommée myDenyURL à la configuration, vous devez taper @myDenyURL @ dans la boîte de dialogue Ajouter une URL de refus, zone de texte Refuser l'URL. Pour effectuer la même tâche à l'aide de la ligne de commande NetScaler, tapez add appfw profile <name> -DenyURLAction @myDenyURL @.

Format de codage de caractères PCRE

Le système d'exploitation NetScaler prend uniquement en charge la saisie directe de caractères dans le jeu de caractères ASCII imprimable, à savoir les caractères comportant des codes hexadécimaux compris entre HEX 20 (ASCII 32) et HEX 7E (ASCII 127). Pour inclure un caractère dont le code se trouve en dehors de cette plage dans votre configuration Web App Firewall, vous devez entrer son code hexadécimal UTF-8 en tant qu'expression régulière PCRE.

Un certain nombre de types de caractères nécessitent un codage à l'aide d'une expression régulière PCRE si vous les incluez dans votre configuration Web App Firewall en tant qu'URL, nom de champ de formulaire ou expression d'objet sécurisé. Ils incluent :

- **Caractères ASCII supérieurs.** Caractères dont le codage va de HEX 7F (ASCII 128) à HEX FF (ASCII 255). Selon la table de caractères utilisée, ces codages peuvent faire référence à des codes de contrôle, des caractères ASCII accentués ou d'autres modifications, des caractères alphabétiques non latins et des symboles non inclus dans le jeu ASCII de base. Ces caractères peuvent apparaître dans les URL, les noms de champs de formulaire et les expressions d'objets sécurisés.
- **Caractères sur deux octets.** Caractères dont l'encodage utilise deux mots de 8 octets. Les caractères codés sur deux octets sont principalement utilisés pour représenter du texte chinois, japonais et coréen au format électronique. Ces caractères peuvent apparaître dans les URL, les noms de champs de formulaire et les expressions d'objets sécurisés.
- **Caractères de contrôle ASCII.** Caractères non imprimables utilisés pour envoyer des commandes à une imprimante. Tous les caractères ASCII dont le code hexadécimal est inférieur à HEX 20 (ASCII 32) entrent dans cette catégorie. Toutefois, ces caractères ne doivent jamais apparaître dans une URL ou un nom de champ de formulaire et apparaîtront rarement, voire jamais, dans une expression d'objet sécurisé.

L'appliance NetScaler ne prend pas en charge l'intégralité du jeu de caractères UTF-8, mais uniquement les caractères contenus dans les huit jeux de caractères suivants :

- **Anglais américain (ISO-8859-1).** Bien que l'étiquette indique « Anglais américain », le Web App Firewall prend en charge tous les caractères du jeu de caractères ISO-8859-1, également appelé jeu de caractères latin-1. Ce jeu de caractères représente entièrement la plupart des langues modernes d'Europe occidentale et représente tous les caractères rares sauf quelques uns dans le reste.
- **Chinois traditionnel (Big5).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères BIG5, qui inclut tous les caractères chinois traditionnels (idéogrammes) couramment utilisés en chinois moderne tels qu'ils sont parlés et écrits à Hong Kong, à Macao, à Taïwan et par de nombreuses personnes d'origine ethnique chinoise qui vivent en dehors de la Chine continentale.
- **Chinois simplifié (GB2312).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères GB2312, qui inclut tous les caractères chinois simplifiés (idéogrammes) couramment utilisés en chinois moderne tels qu'ils sont parlés et écrits en Chine continentale.
- **japonais (SJIS).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères Shift-JIS (SJIS), qui inclut la plupart des caractères (idéogrammes) couramment utilisés en japonais moderne.
- **japonais (EUC-JP).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères EUC-JP, qui inclut tous les caractères (idéogrammes) couramment utilisés en japonais moderne.
- **Coréen (EUC-KR).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères EUC-KR, qui inclut tous les caractères (idéogrammes) couramment utilisés en coréen moderne.
- **Turc (ISO-8859-9).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères ISO-8859-9, qui inclut toutes les lettres utilisées en turc moderne.
- **Unicode (UTF-8).** Le Web App Firewall prend en charge certains caractères supplémentaires dans le jeu de caractères UTF-8, y compris ceux utilisés en russe moderne.

Lors de la configuration du Web App Firewall, vous entrez tous les caractères non ASCII en tant qu'expressions régulières au format PCRE à l'aide du code hexadécimal attribué à ce caractère dans la spécification UTF-8. Les symboles et les caractères du jeu de caractères ASCII normal, auxquels sont affectés des codes simples à deux chiffres dans ce jeu de caractères, se voient attribuer les mêmes codes dans le jeu de caractères UTF-8. Par exemple, le point d'exclamation (!) , auquel est affecté le code hexadécimal 21 dans le jeu de caractères ASCII, est également hexadécimal 21 dans le jeu de caractères UTF-8. Les symboles et les caractères d'un autre jeu de caractères pris en charge sont associés à un jeu de codes hexadécimaux appariés dans le jeu de caractères UTF-8. Par exemple, la lettre a avec un accent aigu (á) se voit attribuer le code UTF-8 C3 A1.

La syntaxe que vous utilisez pour représenter ces codes UTF-8 dans la configuration du Web App Firewall est « xNN » pour les caractères ASCII ; « \xNN\xNN » pour les caractères non ASCII utilisés

en anglais, russe et turc ; et « \xNN\xNN\xNN » pour les caractères utilisés en chinois, japonais et coréen. Par exemple, si vous souhaitez représenter un ! dans une expression régulière du Web App Firewall sous la forme d'un caractère UTF-8, tapez \x21. Si vous souhaitez inclure un á, vous devez taper \xC3\xA1.

> **Remarque :**
>
> Normalement, vous n'avez pas besoin de représenter les caractères ASCII au format UTF-8, mais lorsque ces caractères peuvent confondre un navigateur Web ou un système d'exploitation sous-jacent, vous pouvez utiliser la représentation UTF-8 du personnage pour éviter cette confusion. Par exemple, si une URL contient un espace, vous pouvez coder l'espace en x20 pour éviter de confondre certains navigateurs et logiciels de serveur Web.

Vous trouverez ci-dessous des exemples d'URL, de noms de champs de formulaire et d'expressions d'objets sécurisés contenant des caractères non ASCII qui doivent être entrés en tant qu'expressions régulières au format PCRE pour être inclus dans la configuration du Web App Firewall. Chaque exemple montre d'abord l'URL, le nom de champ ou la chaîne d'expression, suivi d'une expression régulière au format PCRE correspondant.

- URL contenant des caractères ASCII étendus.

  URL réelle : `http://www.josénuñez.com`

  URL codée : `^http://www\[.\]jos\xC3\xA9nu\xC3\xB1ez\[.\]com$`

- Une autre URL contenant des caractères ASCII étendus.

  URL réelle : `http://www.example.de/trömso.html`

  URL codée : `^http://www[.]example\[.]de/tr\xC3\xB6mso[.]html$`

- Un nom de champ de formulaire contenant des caractères ASCII étendus.

  `Actual Name: nome_do_usuário`

  Nom codé : `^nome_do_usu\xC3\xA1rio$`

- Expression d'objet sécurisée contenant des caractères ASCII étendus.

  Expression non codée [A-Z]{3,6}¥[1-9][0-9]{6,6}

  Expression codée : [A-Z]{3,6}\xC2\xA5[1-9][0-9]{6,6}

Vous pouvez trouver un certain nombre de tables qui incluent l'ensemble du jeu de caractères Unicode et les encodages UTF-8 correspondants sur Internet. Un site Web utile contenant ces informations se trouve à l'adresse suivante :

`http://www.utf8-chartable.de/unicode-utf8-table.pl`

Pour que les caractères du tableau de ce site Web s'affichent correctement, une police Unicode appropriée doit être installée sur votre ordinateur. Si ce n'est pas le cas, l'affichage visuel du personnage

peut être erroné. Même si vous n'avez pas installé de police appropriée pour afficher un caractère, la description et les codes UTF-8 et UTF-16 de cet ensemble de pages Web seront corrects.

Expressions PCRE inversées

Outre le contenu correspondant qui contient un modèle, vous pouvez faire correspondre un contenu qui ne contient pas de modèle à l'aide d'une expression PCRE inversée. Pour inverser une expression, il suffit d'inclure un point d'exclamation (!) suivi d'un espace en tant que premier caractère de l'expression.

> **Remarque :** Si une expression se compose uniquement d'un point d'exclamation sans rien suivre, le point d'exclamation est traité comme un caractère littéral, et non comme une syntaxe indiquant une expression inversée.

Les commandes du Web App Firewall suivantes prennent en charge les expressions PCRE inversées :

- URL de démarrage (URL)
- Refuser l'URL (URL)
- Cohérence des champs de formulaire (URL d'action de formulaire)
- Cohérence des cookies (URL d'action de formulaire)
- Falsification de demande intersite (CSRF) (URL de l'action du formulaire)
- Script intersite HTML (URL d'action de formulaire)
- Format du champ (URL de l'action du formulaire)
- Type de champ (type)
- Champ confidentiel (URL)

Remarque : Si le contrôle de sécurité contient un indicateur ou une case à cocher IsRegex, il doit être défini sur OUI ou coché pour activer les expressions régulières dans le champ. Sinon, le contenu de ce champ est traité comme littéral et aucune expression régulière (inversée ou non) n'est analysée.

Noms non autorisés pour les profils de Web App Firewall

Les noms suivants sont attribués à des actions et à des profils intégrés sur l'appliance NetScaler et ne peuvent pas être utilisés comme noms pour un profil Web App Firewall créé par l'utilisateur.

- AGRESSIVE
- ALLOW
- BASIC
- CLIENTAUTH
- COMPRESS
- CSSMINIFY
- DEFLATE
- DENY

- DNS-NOP
- ABANDONNER
- GZIP
- HTMLMINIFY
- IMGOPTIMIZE
- JSMINIFY
- MODERATE
- NOCLIENTAUTH
- NOCOMPRESS
- NONE
- NOOP
- NOREWRITE
- RÉINITIALISER
- SETASLEARNNSLOG_ACT
- SETNSLOGPARAMS_ACT
- SETSYSLOGPARAMS_ACT
- SETTMSESSPARAMS_ACT
- SETVPNPARAMS_ACT
- SET_PREAUTHPARAMS_ACT
- default_DNS64_action
- dns_default_act_Cachebypass
- dns_default_act_Drop
- nshttp_default_profile
- nshttp_default_strict_validation
- NSTCP_Default_Mobile_Profile
- NSTCP_Default_XA_XD_Profile
- nstcp_default_profile
- nstcp_default_tcp_interactive_stream
- nstcp_default_tcp_lan
- nstcp_default_tcp_lan_thin_stream
- nstcp_default_tcp_lfp
- nstcp_default_tcp_lfp_thin_stream
- nstcp_default_tcp_lnp
- nstcp_default_tcp_lnp_thin_stream
- nstcp_internal_apps

Statut et message d'erreur personnalisés pour l'objet d'erreur HTML, XML et JSON

May 5, 2023

Lorsque le NetScaler Web App Firewall détecte une violation, l'appliance gère le scénario d'erreur à l'aide d'une URL de redirection ou de l'objet d'erreur (importé dans le profil et activé). Si le scénario est géré à l'aide d'une configuration d'objet d'erreur, le profil WAF fournit un code et un message d'état de réponse personnalisés. Vous pouvez personnaliser les détails de l'erreur de réponse pour un objet d'erreur HTML, XML ou JSON dans le profil WAF.

> **Remarque :**
>
> Par défaut, le code d'erreur et le message d'erreur sont définis comme « 200 » et « OK » si les paramètres des objets d'erreur sont configurés.

Lors de la gestion des scénarios d'erreur, il est important que l'appliance réponde avec un code et un message d'état de réponse HTTP appropriés pour résoudre les problèmes. En fournissant un message d'état d'erreur personnalisé et un code d'état d'erreur personnalisé, l'appliance peut fournir une meilleure intervention de l'utilisateur pour résoudre un problème en cas de violation. Par exemple, si vous définissez le code d'erreur de réponse sur « 404 » et que le message d'état sur « Non trouvé », l'utilisateur peut inspecter le code d'état de la réponse et le message pour vérifier si une violation s'est produite. Cela peut aider l'utilisateur à filtrer les réponses contenant l'objet error.

Configurer un code d'état et un message personnalisés pour l'objet d'erreur HTML dans un profil WAF à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set appfw profile <profile-name> -HTMLErrorStatusCode <value> -
    HTMLErrorStatusMessage <value> -useHTMLErrorObject ON
<!--NeedCopy-->
```

Exemple :

```
set appfw profile profile_1 -HTMLErrorStatusCode 404 -HTMLErrorStatusMessage
  “Not Found”  -useHTMLErrorObject ON
```

Configurer un code d'état personnalisé et un message pour un objet d'erreur XML dans un profil WAF à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
set appfw profile <profile-name> -XMLErrorStatusCode <value> -
    XMLErrorStatusMessage <value>
<!--NeedCopy-->
```

Exemple :

```
set appfw profile profile_1 -XMLErrorStatusCode 406 - XMLErrorStatusMessage
  “Not Acceptable”
```

Configurer un code d’état et un message personnalisés pour l’objet d’erreur JSON dans un profil WAF à l’aide de l’interface de ligne de commande

À l’invite de commande, tapez :

```
set appfw profile <profile-name> -JSONErrorStatusCode <value> -
    JSONErrorStatusMessage <value>
<!--NeedCopy-->
```

Exemple :

```
set appfw profile profile_1 -JSONErrorStatusCode 500 - JSONErrorStatusMessage
  “Internal Server Error”
```

Configurer un code d’état et un message personnalisés pour un objet d’erreur HTML, JSON ou XML dans un profil WAF à l’aide de l’interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet d’informations, cliquez sur **Modifier**.
3. Dans la page **Créer un profil de Web App Firewall**, cliquez sur **Paramètres de profil dans** la section **Paramètres avancés** .
4. Dans la section **Paramètres du profil**, définissez les paramètres suivants.

   a. Objet d’erreur HTML. Sélectionnez l’option permettant de gérer des scénarios d’erreur à l’aide d’un objet d’erreur HTML. Importez l’objet erreur à partir d’une URL, d’un fichier ou d’un texte.
   b. Code d’état d’erreur HTML. Fournissez un code d’état d’erreur personnalisé.
   c. Message d’état d’erreur HTML. Fournissez un message d’erreur client.
5. Cliquez sur **OK** et **Terminé**.

> **Remarque :**
>
> La même procédure s’applique aux paramètres d’objets d’erreur personnalisés JSON et XML.



Étiquettes de stratégie

May 5, 2023

Une étiquette de stratégie se compose d'un ensemble de stratégies, d'autres étiquettes de stratégie et de banques de stratégies spécifiques au serveur virtuel. Le Web App Firewall évalue chaque stratégie liée à l'étiquette de stratégie par ordre de priorité. Si la stratégie correspond, elle filtre la connexion telle qu'elle est spécifiée dans le profil associé. Ensuite, il fait tout ce que spécifie le paramètre Goto, qui peut être de mettre fin à l'évaluation de la stratégie, d'accéder à la stratégie suivante ou d'accéder à la stratégie avec la priorité spécifiée. Si le paramètre Invoke est défini, il met fin au traitement de l'étiquette de stratégie actuelle et commence à traiter l'étiquette de stratégie ou le serveur virtuel spécifié.

Pour créer une étiquette de stratégie de Web App Firewall à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw policylabel <labelName> http_req`
- `save ns config`

Exemple

L'exemple suivant crée une étiquette de stratégie nommée policylbl1.

```
1 add appfw policylabel policylbl1 http_req
2 save ns config
3 <!--NeedCopy-->
```


Pour lier une stratégie à une étiquette de stratégie à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `bind appfw policylabel <labelName> <policyName> <priority> [<gotoPriorityExpressi >] [-invoke (<labelType> <labelName>)]`
- `save ns config`

Exemple

L'exemple suivant lie la stratégie 1 à l'étiquette de stratégie policylbl1 avec une priorité de 1.

```
1 bind appfw policylabel policylbl1 policy1 1
2 save ns config
3 <!--NeedCopy-->
```

Pour configurer une étiquette de stratégie de Web App Firewall à l'aide de l'interface graphique

1. Accédez à **Sécurité > NetScaler Web App Firewall > Libellés de politique**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour ajouter une nouvelle étiquette de stratégie, cliquez sur **Ajouter**.
   - Pour configurer une étiquette de stratégie existante, sélectionnez-la, puis cliquez sur **Ouvrir**.

   La boîte de dialogue **Créer une étiquette de stratégie de Web App FirewallWeb App ou Configurer l'étiquette de stratégie de pare-feu** Web App s'ouvre. Les boîtes de dialogue sont presque identiques.
3. Si vous créez une nouvelle étiquette de stratégie, dans la boîte de dialogue Créer une étiquette de stratégie de Web App Firewall, tapez un nom pour votre nouvelle étiquette de stratégie.

   Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement, et peut comprendre de 1 à 127 lettres, chiffres et les symboles tiret (-), point (.) livre (#), espace (), at (@), égal (=), deux-points (:) et trait de soulignement (_).
4. Sélectionnez **Insérer une stratégie** pour insérer une nouvelle ligne et afficher une liste déroulante avec toutes les stratégies de Web App Firewall existantes.
5. Sélectionnez la stratégie que vous souhaitez lier à l'étiquette de stratégie ou sélectionnez Nouvelle stratégie pour créer une nouvelle stratégie et suivez les instructions de la section Pour créer et configurer une stratégie à l'aide de l'interface graphique. La stratégie que vous avez sélectionnée ou créée est insérée dans la liste des stratégies de Web App Firewall globalement liées.

6. Effectuez des ajustements supplémentaires.
    - Pour modifier la priorité de la stratégie, cliquez sur le champ pour l'activer, puis tapez une nouvelle priorité. Vous pouvez également sélectionner Régénérer les priorités pour renuméroter les priorités uniformément.
    - Pour modifier l'expression de stratégie, double-cliquez sur ce champ pour ouvrir la boîte de dialogue Configurer la stratégie de Web App Firewall, dans laquelle vous pouvez modifier l'expression de stratégie.
    - Pour définir l'expression Goto, double-cliquez sur le champ dans l'en-tête de colonne Goto Expression pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression.
    - Pour définir l'option Invoke, double-cliquez sur le champ dans l'en-tête de colonne Invoke pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression
7. Répétez les étapes 5 à 7 pour lier les stratégies de Web App Firewall supplémentaires souhaitées à l'étiquette de stratégie.
8. Cliquez sur **Créer** ou **sur OK**, puis sur **Fermer**. Un message apparaît dans la barre d'état indiquant que vous avez correctement créé ou modifié l'étiquette de stratégie.

Stratégies

May 5, 2023

Le Web App Firewall utilise deux types de politiques : les stratégies de pare-feu et les stratégies d'audit. Les politiques de pare-feu contrôlent le trafic envoyé au Web App Firewall. Les politiques d'audit contrôlent le serveur de journaux auquel les journaux du Web App Firewall sont envoyés.

Les politiques de pare-feu peuvent être complexes car la règle de politique peut se composer de plusieurs expressions dans le langage d'expressions NetScaler, qui est un langage de programmation orienté objet à part entière capable de définir avec une extrême précision les connexions à filtrer. Étant donné que les politiques de pare-feu fonctionnent dans le contexte du Web App Firewall, elles doivent répondre à certains critères liés au fonctionnement du Web App Firewall et au trafic qui est filtré de manière appropriée par celui-ci. Tant que vous gardez ces critères à l'esprit, les politiques de pare-feu sont similaires à celles des autres fonctionnalités de NetScaler. Les instructions présentées ici ne visent pas à couvrir tous les aspects de la rédaction des politiques de pare-feu, mais fournissent uniquement une introduction aux politiques et abordent les critères propres au Web App Firewall.

Les politiques d'audit sont simples car la règle de stratégie est toujours ns_true. Vous devez uniquement spécifier le serveur de journaux auquel vous souhaitez envoyer les journaux, les niveaux de journalisation que vous souhaitez utiliser et quelques autres critères expliqués en détail.

Stratégies de Web App Firewall

May 5, 2023

Une stratégie de pare-feu est une règle associée à un profil. La règle est une expression ou un groupe d'expressions qui définissent les types de paires requête/réponse que le Web App Firewall doit filtrer en appliquant le profil. Les expressions de politique de pare-feu sont écrites dans le langage d'expressions NetScaler, un langage de programmation orienté objet doté de fonctionnalités spéciales destinées à prendre en charge des fonctions NetScaler spécifiques. Le profil est l'ensemble des actions que le Web App Firewall doit utiliser pour filtrer les paires requête/réponse qui correspondent à la règle.

Les stratégies de pare-feu vous permettent d'attribuer différentes règles de filtrage à différents types de contenu Web. Tous les contenus Web ne se ressemblent pas. Un site Web simple qui n'utilise aucun script complexe et qui accède et ne traite aucune donnée privée peut nécessiter uniquement le niveau de protection fourni par un profil créé avec des valeurs par défaut de base. Le contenu Web qui contient des formulaires Web améliorés par JavaScript ou qui accède à une base de données SQL nécessite probablement une protection plus personnalisée. Vous pouvez créer un profil différent pour filtrer ce contenu et créer une stratégie de pare-feu distincte qui peut déterminer les demandes qui tentent d'accéder à ce contenu. Vous associez ensuite l'expression de stratégie à un profil que vous avez créé et vous liez globalement la stratégie pour la mettre en œuvre.

Le Web App Firewall traite uniquement les connexions HTTP et utilise donc un sous-ensemble du langage d'expressions NetScaler global. Les informations ici sont limitées aux rubriques et exemples susceptibles d'être utiles lors de la configuration du Web App Firewall. Vous trouverez ci-dessous des liens vers des informations supplémentaires et des procédures relatives aux stratégies de pare-feu :

- Pour connaître les procédures expliquant comment créer et configurer une stratégie, reportez-vous à la section Création et configuration de stratégies de Web App Firewall.
- Pour obtenir une procédure expliquant en détail comment créer une règle de stratégie (expression), reportez-vous à la section Pour créer ou configurer une règle de Web App Firewall (expression).
- Pour obtenir une procédure expliquant comment utiliser la boîte de dialogue Ajouter une expression pour créer une règle de stratégie, reportez-vous à la section Pour ajouter une règle de pare-feu (expression) à l'aide de la boîte de dialogue Ajouter une expression.
- Pour obtenir une procédure expliquant comment afficher les liaisons actuelles d'une stratégie, reportez-vous à la section Affichage des liaisons d'une stratégie de pare-feu.
- Pour connaître les procédures expliquant comment lier une stratégie de Web App Firewall, reportez-vous à la section Liaison des stratégies de Web App Firewall.
- Pour des informations détaillées sur le langage d'expressions NetScaler, consultez Politiques etexpressions.

Remarque

Web App Firewall évalue les stratégies en fonction de la priorité configurée et des expressions goto. À la fin de l'évaluation de la stratégie, la dernière stratégie évaluée à true est utilisée et la configuration de sécurité du profil correspondant est appelée pour traiter la demande.

Par exemple, imaginez un scénario dans lequel il existe deux stratégies.

- Policy_1 est une stratégie générique avec expression=NS_true et possède un profile_1 correspondant qui est un profil de base. La priorité est fixée à 100.
- Policy_2 est plus spécifique avec expression=HTTP.REQ.URL.contains (« XYZ ») et a un profile_2 correspondant qui est un profil avancé. L'expression GoTo est définie sur NEXT et la priorité est définie sur 95, ce qui est une priorité supérieure à celle de Policy_1.

Dans ce scénario, si la chaîne cible « XYZ » est détectée dans l'URL de la demande traitée, la correspondance Policy_2 est déclenchée car elle a une priorité plus élevée, même si Policy_1 est également une correspondance. Toutefois, conformément à la configuration de l'expression GoTo de Policy_2, l'évaluation de la stratégie se poursuit et la prochaine policy_1 est également traitée. À la fin de l'évaluation de la stratégie, Policy_1 évalue la valeur true et les vérifications de sécurité de base configurées dans Profile_1 sont appelées.

Si la stratégie Policy_2 est modifiée et que l'expression GoTo passe de **NEXT** à **END**, la demande traitée qui contient la chaîne cible « XYZ » déclenche la correspondance Policy_2 en raison de la priorité et, conformément à la configuration de l'expression GoTo, l'évaluation de la stratégie se termine à ce point. Policy_2 est évalué comme vrai et les vérifications de sécurité avancées configurées dans Profile_2 sont appelées.

FIN SUIVANTE

L'évaluation des politiques se fait en un seul passage. Une fois que l'évaluation de la stratégie est terminée pour la demande et que les actions de profil correspondantes sont invoquées, la demande ne passe pas par une autre ronde d'évaluation de la stratégie.

Création et configuration de politiques de Web App Firewall

May 5, 2023

Une politique de pare-feu se compose de deux éléments : une *règle*et un *profil*associé. La règle sélectionne le trafic HTTP qui correspond aux critères que vous avez définis et envoie ce trafic au Web App Firewall pour le filtrage. Le profil contient les critères de filtrage utilisés par le Web App Firewall.

La règle de politique consiste en une ou plusieurs expressions dans le langage d'expressions NetScaler. La syntaxe des expressions NetScaler est un puissant langage de programmation ori-

enté objet qui vous permet de désigner précisément le trafic que vous souhaitez traiter avec un profil spécifique. **Pour les utilisateurs qui ne sont pas familiarisés avec la syntaxe du langage d'expressions NetScaler ou qui préfèrent configurer leur appliance NetScaler à l'aide d'une interface Web, l'interface graphique fournit deux outils : le menu**Préfixe et la boîte**de dialogue Ajouter une expression.** Les deux vous aident à écrire des expressions qui sélectionnent exactement le trafic que vous souhaitez traiter. Les utilisateurs expérimentés qui connaissent parfaitement la syntaxe peuvent préférer utiliser la ligne de commande NetScaler pour configurer leurs appliances NetScaler.

> **Remarque :**
>
> Outre la syntaxe des expressions par défaut, pour des raisons de rétrocompatibilité, le système d'exploitation NetScaler prend en charge la syntaxe des expressions classiques NetScaler sur les appliances NetScaler Classic et nCore et les appliances virtuelles. Les expressions classiques ne sont pas prises en charge sur les appliances NetScaler Cluster et les appliances virtuelles. Les utilisateurs actuels de NetScaler qui souhaitent migrer des configurations existantes vers le NetScaler Cluster doivent migrer toutes les politiques contenant des expressions classiques vers la syntaxe des expressions par défaut.

Pour des informations détaillées sur les langages d'expressions NetScaler, consultez Politiques etexpressions.

Vous pouvez créer une politique de pare-feu à l'aide de l'interface graphique ou de la ligne de commande NetScaler.

Pour créer et configurer une politique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw policy <name><rule> <profileName>`
- `save ns config`

Exemple

L'exemple suivant ajoute une politique nommée pl-blog, avec une règle qui intercepte tout le trafic à destination ou en provenance de l'hôte blog.example.com, et associe cette politique au profil pr-blog. Il s'agit d'une politique appropriée pour protéger un blog hébergé sous un nom d'hôte spécifique.

```
1 add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com
     ")" pr-blog
2 <!--NeedCopy-->
```


Pour créer et configurer une politique à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall** > **Politiques**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une politique de pare-feu, cliquez sur **Ajouter**. La **politique de création de Web App Firewall** s'affiche.
   - Pour modifier une politique de pare-feu existante, sélectionnez la politique, puis cliquez sur **Modifier**.

   La fenêtre **Créer une politique de Web App Firewall** ou **Configurer une politique de pare-feu pour applications Web** s'affiche.
3. Si vous créez une politique de pare-feu, dans la boîte de dialogue **Créer une politique de Web App Firewall**, zone de texte Nom de la stratégie, tapez le nom de votre nouvelle politique.

   Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement et peut comprendre de 1 à 128 lettres, chiffres et le tiret (-), le point (.), la livre (#), l'espace (), l'arobase (@), l'égal (=), les deux points (:) et le trait de soulignement (_).

   Si vous configurez une politique de pare-feu existante, ce champ est en lecture seule. Vous ne pouvez pas le modifier.
4. Sélectionnez le profil que vous souhaitez associer à cette politique dans la liste déroulante Profil. Vous pouvez créer un profil à associer à votre politique en cliquant sur Nouveau, et vous pouvez modifier un profil existant en cliquant sur Modifier.
5. Dans la zone de texte Expression, créez une règle pour votre politique.
   - Vous pouvez saisir une règle directement dans la zone de texte.
   - Vous pouvez cliquer sur Préfixe pour sélectionner le premier terme de votre règle et suivre les instructions.
   - Vous pouvez cliquer sur Ajouter pour ouvrir la boîte de dialogue Ajouter une expression et l'utiliser pour créer la règle.
6. Cliquez sur **Créer** ou **sur OK**, puis sur **Fermer**.

Pour créer ou configurer une règle de Web App Firewall (expression)

La règle de politique, également appelée *expression*, définit le trafic Web que le Web App Firewall filtre à l'aide du profil associé à la politique. Comme les autres règles (ou *expressions*) de politique NetScaler, les règles du Web App Firewall utilisent la syntaxe des expressions NetScaler. Cette syntaxe est puissante, flexible et extensible. C'est trop complexe pour être décrit complètement dans cet ensemble d'instructions. Vous pouvez utiliser la procédure suivante pour créer une règle de politique de pare-feu simple, ou vous pouvez la lire comme une vue d'ensemble du processus de création de la politique.

1. Si ce n'est pas déjà fait, accédez à l'emplacement approprié dans l'assistant **Web App Firewall** ou dans l'interface graphique de NetScaler pour créer votre règle de politique :

   - Si vous configurez une stratégie dans l'assistant **Web App Firewall**, dans le volet de navigation, cliquez sur **Web App Firewall**, puis dans le volet d'informations, cliquez sur **Assistant Web App Firewall**, puis accédez à l'écran **Spécifier une règle** .
   - Si vous configurez une politique manuellement, dans le volet de navigation, développez **Web App Firewall**, puis **Politiques**, puis **Firewall**. Dans le volet d'informations, pour créer une politique, cliquez sur **Ajouter**. Pour modifier une politique existante, sélectionnez-la, puis cliquez sur **Ouvrir**.

2. Dans l'écran **Spécifier une règle**, dans la boîte de dialogue **Créer un profil de Web App Firewall** d' **applications Web ou dans la boîte de dialogue de configuration du profil de parefeu** d'applications Web, cliquez sur **Préfixe**, puis choisissez le préfixe de votre expression dans la liste déroulante. Vos choix sont les suivants :

   - **HTTP.** Choisissez un protocole HTTP si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole.
   - **SYS.** Choisissez des sites Web protégés si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
   - **CLIENT.** Choisissez le client qui a envoyé la demande. Choisissez cette option si vous souhaitez examiner certains aspects de l'expéditeur de la demande.
   - **SERVEUR.** Choisissez le client auquel la demande a été envoyée et si vous souhaitez examiner certains aspects du destinataire de la demande.

   Une fois que vous avez choisi un préfixe, le Web App Firewall affiche une fenêtre d'invite en deux parties qui affiche les choix suivants possibles en haut et une brève explication de la signification du choix sélectionné en bas.

3. Choisissez votre prochain mandat.

   Si vous avez choisi le protocole HTTP comme préfixe, votre seul choix est REQ, qui spécifie la paire Requête/Réponse. (Le Web App Firewall fonctionne sur la demande et la réponse comme une unité plutôt que séparément.) Si vous choisissez un autre préfixe, vos choix sont plus variés. Pour obtenir de l'aide sur un choix spécifique, cliquez une fois sur ce choix pour afficher les informations le concernant dans la fenêtre contextuelle inférieure.

   Lorsque vous avez choisi le terme que vous souhaitez utiliser, double-cliquez dessus pour l'insérer dans la fenêtre **Expression** .

4. Tapez un point après le terme que vous venez de choisir. Vous êtes ensuite invité à choisir votre prochain terme, comme décrit à l'étape précédente. Lorsqu'un terme nécessite que vous saisissiez une valeur, renseignez la valeur appropriée. Par exemple, si vous choisissez HTTP.REQ.HEADER (« »), saisissez le nom de l'en-tête entre guillemets.

5. Continuez à choisir des termes à partir des instructions et à saisir les valeurs nécessaires jusqu'à ce que votre expression soit terminée.

   Vous trouverez ci-dessous quelques exemples d'expressions destinées à des fins spécifiques.

   - **Hébergeur Web spécifique.** Pour faire correspondre le trafic provenant d'un hébergeur en particulier :

     ```
     1 HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
     2 <!--NeedCopy-->
     ```

     Remplacez par le nom de l'hébergeur auquel vous souhaitez faire correspondre le nom. `shopping.example.com`

   - **Dossier ou répertoire Web spécifique.** Pour faire correspondre le trafic provenant d'un dossier ou d'un répertoire spécifique sur un hôte Web, procédez comme suit :

     ```
     1 HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
     2 <!--NeedCopy-->
     ```

     Pour www.example.com, remplacez le nom de l'hébergeur Web. Remplacez le dossier ou le chemin d'accès au contenu auquel vous souhaitez faire correspondre. Par exemple, si votre panier se trouve dans un dossier nommé /solutions/orders, vous remplacez cette chaîne par dossier.

   - **Type de contenu spécifique : images GIF.** Pour faire correspondre des images au format GIF :

     ```
     1 HTTP.REQ.URL.ENDSWITH(".png")
     2 <!--NeedCopy-->
     ```

     Pour faire correspondre des images d'un autre format, remplacez .png par une autre chaîne.

   - **Type de contenu spécifique : scripts.** Pour faire correspondre tous les scripts CGI situés dans le répertoire CGI-BIN :

     ```
     1 HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
     2 <!--NeedCopy-->
     ```

     Pour associer tous les fichiers JavaScript aux extensions .js :

     ```
     1 HTTP.REQ.URL.ENDSWITH(".js")
     2 <!--NeedCopy-->
     ```

     Pour plus d'informations sur la création d'expressions de stratégie, voir Stratégies et expressions.

> **Remarque :**
>
> Si vous utilisez la ligne de commande pour configurer une politique, pensez à éviter les guillemets doubles dans les expressions NetScaler. Par exemple, l'expression suivante est correcte si elle est saisie dans l'interface graphique :

```
1 HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
2 <!--NeedCopy-->
```

Toutefois, si vous la saisissez sur la ligne de commande, vous devez plutôt taper la commande suivante :

```
1 HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
2 <!--NeedCopy-->
```

Pour ajouter une règle de pare-feu (expression) à l'aide de la boîte de dialogue Ajouter une expression

La boîte de dialogue **Ajouter une expression** (également appelée éditeur d'expressions) aide les utilisateurs qui ne sont pas familiarisés avec le langage d'expressions NetScaler à élaborer une politique correspondant au trafic qu'ils souhaitent filtrer.

1. Si ce n'est pas déjà fait, accédez à l'emplacement approprié dans l'assistant **Web App Firewall** ou dans l'interface graphique de NetScaler :
   - Si vous configurez une stratégie dans l'assistant **Web App Firewall**, dans le volet de navigation, cliquez sur **Web App Firewall**, puis dans le volet d'informations, cliquez sur **Assistant Web App Firewall**, puis accédez à l'écran **Spécifier une règle** .
   - Si vous configurez une politique manuellement, dans le volet de navigation, développez **Web App Firewall**, puis **Politiques**, puis **Firewall**. Dans le volet d'informations, pour créer une politique, cliquez sur **Ajouter**. Pour modifier une politique existante, sélectionnez-la, puis cliquez sur **Ouvrir**.
2. Sur l'écran **Spécifier une règle**, dans la boîte de dialogue **Créer un profil de Web App Firewall** ou dans la boîte de dialogue de **configuration du profil de Web App Firewall**, cliquez sur **Ajouter**.
3. Dans la boîte de **dialogue Ajouter une expression**, dans la zone Construire une expression, dans la première zone de liste, choisissez l'un des préfixes suivants :
   - **HTTP.** Choisissez le protocole HTTP si vous souhaitez examiner certains aspects de la demande qui se rapportent au protocole HTTP. Le choix par défaut.
   - **SYS.** Choisissez des sites Web protégés si vous souhaitez examiner certains aspects de la demande qui concernent le destinataire de la demande.
   - **CLIENT.** Choisissez l'ordinateur qui a envoyé la demande si vous souhaitez examiner certains aspects de l'expéditeur de la demande.

- **SERVEUR.** Choisissez l'ordinateur auquel la demande a été envoyée et examinez certains aspects du destinataire de la demande.

4. Dans la deuxième zone de liste, choisissez votre prochain terme. Les termes disponibles varient en fonction du choix que vous avez fait à l'étape précédente, car la boîte de dialogue ajuste automatiquement la liste pour ne contenir que les termes qui sont valides pour le contexte. Par exemple, si vous avez sélectionné HTTP dans la zone de liste précédente, le seul choix est REQ, pour les requêtes. Étant donné que le Web App Firewall traite les demandes et les réponses associées comme une seule unité et filtre les deux, vous n'avez pas besoin de réponses spécifiques séparément. Une fois que vous avez choisi votre deuxième terme, une troisième zone de liste apparaît à droite du second. La fenêtre d'aide affiche la description du deuxième terme et la fenêtre **Aperçu de l'expression** affiche votre expression.
5. Dans la troisième zone de liste, choisissez le terme suivant. Une nouvelle zone de liste apparaît sur la droite et la fenêtre d'aide change pour afficher la description du nouveau terme. La fenêtre **Aperçu de l'expression** se met à jour pour afficher l'expression telle que vous l'avez spécifiée jusqu'à présent.
6. Continuez à choisir des termes et, lorsque vous y êtes invité, à saisir des arguments, jusqu'à ce que votre expression soit complète. Si vous faites une erreur ou souhaitez modifier votre expression alors que vous avez déjà sélectionné un terme, vous pouvez simplement en choisir un autre. L'expression est modifiée et tous les arguments ou autres termes que vous avez ajoutés après le terme que vous avez modifié sont effacés.
7. Lorsque vous avez fini de créer votre expression, cliquez sur **OK** pour fermer la boîte de dialogue **Ajouter une expression** . Votre expression est insérée dans la zone de texte **Expression** .

Politiques de Web App Firewall contraignantes

May 5, 2023

Après avoir configuré vos politiques de Web App Firewall, vous les liez à Global ou à un point de liaison pour les mettre en œuvre. Après la liaison, toute demande ou réponse correspondant à une politique de Web App Firewall est transformée par le profil associé à cette politique.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel nombre entier positif. Dans le système d'exploitation NetScaler, les priorités des politiques fonctionnent dans l'ordre inverse : plus le nombre est élevé, plus la priorité est faible.

Étant donné que la fonctionnalité Web App Firewall met en œuvre uniquement la première politique à laquelle une demande correspond, et non les politiques supplémentaires auxquelles elle pourrait également correspondre, la priorité des politiques est importante pour obtenir les résultats souhaités. Si vous attribuez à votre première politique une faible priorité (par exemple 1000), vous configurez le

Web App Firewall pour qu'il ne l'exécute que si d'autres politiques ayant une priorité plus élevée ne correspondent pas à une demande. Si vous accordez à votre première politique une priorité élevée (par exemple, 1), vous configurez le Web App Firewall pour qu'il l'exécute en premier, et vous ignorez toutes les autres politiques qui pourraient également correspondre. Vous pouvez vous laisser beaucoup de place pour ajouter d'autres stratégies dans n'importe quel ordre, sans avoir à réaffecter des priorités, en définissant des priorités avec des intervalles de 50 ou 100 entre chaque stratégie lorsque vous liez vos stratégies.

Pour plus d'informations sur les politiques de liaison sur l'appliance NetScaler, consultez « Politiques et expressions ». «

Pour lier une stratégie de Web App Firewall à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `bind appfw global <policyName>`
- `bind appfw profile <profile_name> -crossSiteScripting data`

Exemple

L'exemple suivant lie la politique nommée pl-blog et lui attribue une priorité de 10.

```
bind appfw global pl-blog 10
save ns config
<!--NeedCopy-->
```

Configuration des expressions de journal

La prise en charge des expressions de journal pour lier le Web App Firewall est ajoutée pour consigner les informations d'en-tête HTTP en cas de violation.

L'expression du journal est liée au profil de l'application, et la liaison contient l'expression qui doit être évaluée et envoyée aux frameworks de journalisation en cas de violation.

L'enregistrement du journal des violations du Web App Firewall avec les informations d'en-tête HTTP est enregistré. Vous pouvez spécifier une expression de journal personnalisée qui facilite l'analyse et le diagnostic lorsque des violations sont générées pour le flux actuel (demande/réponse).

Exemple de configuration

```
bind appfw profile <profile> -logexpression <string> <expression>
add policy expression headers "" HEADERS(100):"+HTTP.REQ.FULL_HEADER"
```



```
add policy expression body_100 ""BODY:"+HTTP.REQ.BODY(100)"
bind appfw profile test -logExpression log_body body_100
bind appfw profile test -logExpression log_headers  headers
bind appfw profile test -logExpression ""URL:"+HTTP.REQ.URL+" IP:"+
   CLIENT.IP.SRC"
<!--NeedCopy-->
```

Exemples de journaux

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
   .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
   POST request=http://10.217.222.44/test/credit.html msg= HEADERS(100)
   :POST /test/credit.html HTTP/1.1^M User-Agent: curl/7.24.0 (amd64-
   portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Host:
    10.217.222.44^M Accept: /^M Content-Length: 33^M Content-Type:
   application/x-www-form-urlencoded^M ^M  cn1=58 cn2=174 cs1=test cs2=
   PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
   .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
   POST request=http://10.217.222.44/test/credit.html msg=BODY:ata=
   asdadasdasdasddddddddddddddddd cn1=59 cn2=174 cs1=test cs2=PPE1 cs4=
   ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
   .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
   POST request=http://10.217.222.44/test/credit.html msg=URL:/test/
   credit.html IP:10.217.222.128 cn1=60 cn2=174 cs1=test cs2=PPE1 cs4=
   ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Other violation logs
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
   .1|APPFW|APPFW_STARTURL|6|src=10.217.222.128 spt=26409 method=POST
   request=http://10.217.222.44/test/credit.html msg=Disallow Illegal
   URL. cn1=61 cn2=174 cs1=test cs2=PPE1 cs4=ALERT cs5=2017 act=not
   blocked
<!--NeedCopy-->
```



```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_SAFECOMMERCE|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=Maximum
    number of potential credit card numbers seen cn1=62 cn2=174 cs1=test
     cs2=PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

Remarque

1. Seul le support Auditlog est disponible. La prise en charge du logstream et la visibilité dans Security Insight seront ajoutées dans les prochaines versions.
2. Si des journaux d'audit sont générés, seuls 1024 octets de données peuvent être générés par message de journal.
3. Si le streaming de journaux est utilisé, les limites sont basées sur la taille maximale prise en charge par les limites de taille du protocole Log Stream et IPFIX. La taille maximale de prise en charge pour le flux de journaux est supérieure à 1024 octets.

Pour lier une politique de Web App Firewall à l'aide de l'interface graphique

1. Procédez comme suit :
   - Accédez à **Sécurité** > **Web App Firewall**, puis dans le volet de détails, cliquez sur Gestionnaire de politiques du Web App Firewall.
   - Accédez à **Sécurité** > **Web App Firewall** > **Politiques > Politiquesde pare-feu**, puis dans le volet de détails, cliquez sur**Policy Manager**.
2. Dans la boîte de dialogue du **gestionnaire de politiques du Web App Firewall**, choisissez le point de liaison auquel vous souhaitez lier la politique dans la liste déroulante. Les choix sont les suivants :
   - **Remplacez Global.** Les politiques liées à ce point de liaison traitent l'ensemble du trafic provenant de toutes les interfaces de l'appliance NetScaler et sont appliquées avant toute autre politique.
   - **Serveur virtuel LB.** Les politiques liées à un serveur virtuel d'équilibrage de charge sont appliquées uniquement au trafic traité par ce serveur virtuel d'équilibrage de charge et sont appliquées avant toute politique globale par défaut. Après avoir sélectionné le serveur virtuel LB, vous devez également sélectionner le serveur virtuel d'équilibrage de charge spécifique auquel vous souhaitez lier cette politique.
   - **Serveur virtuel CS.** Les politiques liées à un serveur virtuel de commutation de contenu sont appliquées uniquement au trafic traité par ce serveur virtuel de commutation de contenu et sont appliquées avant toute politique globale par défaut. Après avoir sélectionné CS Virtual Server, vous devez également sélectionner le serveur virtuel de commutation de contenu spécifique auquel vous souhaitez lier cette politique.

- **Global par défaut.** Les politiques liées à ce point de liaison traitent l'ensemble du trafic provenant de toutes les interfaces de l'appliance NetScaler.
- **Libellé de politique.** Les politiques liées à une étiquette de stratégie traitent le trafic que l'étiquette de stratégie leur achemine. L'étiquette de politique contrôle l'ordre dans lequel les politiques sont appliquées à ce trafic.
- **None.** Ne liez la politique à aucun point de liaison.

3. Cliquez sur **Continuer**. La liste des politiques de Web App Firewall existantes s'affiche.
4. Sélectionnez la politique que vous souhaitez lier en cliquant dessus.
5. Apportez tous les ajustements supplémentaires à la reliure.
   - Pour modifier la priorité de la stratégie, cliquez sur le champ pour l'activer, puis tapez une nouvelle priorité. Vous pouvez également sélectionner Régénérer les priorités pour renuméroter les priorités uniformément.
   - Pour modifier l'expression de politique, double-cliquez sur ce champ pour ouvrir la boîte de dialogue **Configurer la politique de Web App Firewall**, dans laquelle vous pouvez modifier l'expression de stratégie.
   - Pour définir l'expression Goto, double-cliquez sur **le champ** dans l'en-tête de la colonne Goto Expression pour afficher la liste déroulante dans laquelle vous pouvez choisir une expression.
   - Pour définir l'option Invoke, double-cliquez sur le champ dans l'en-tête de colonne Invoke pour afficher la liste déroulante, dans laquelle vous pouvez choisir une expression
6. Répétez les étapes 3 à 6 pour ajouter les politiques de Web App Firewall supplémentaires que vous souhaitez lier globalement.
7. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la stratégie a été liée avec succès.

Afficher les liaisons d'une politique

May 5, 2023

Vous pouvez rapidement vérifier quelles sont les liaisons en place pour chaque politique de pare-feu en consultant les liaisons dans l'interface graphique.

Pour afficher les liaisons d'une politique de pare-feu pour applications Web

1. Accédez à **Sécurité > NetScaler Web App Firewall > Politiques > Politiques de pare-feu**
2. Dans le volet de détails, sélectionnez la politique que vous souhaitez vérifier, puis cliquez sur Afficher les liaisons. La boîte de message Détails de la liaison pour la politique : Politique s'affiche, avec la liste des liaisons pour la politique sélectionnée.
3. Cliquez sur **Fermer**.

Informations supplémentaires sur les politiques du Web App Firewall

May 5, 2023

Vous trouverez ci-dessous des informations supplémentaires sur des aspects particuliers des politiques du Web App Firewall que les administrateurs système qui gèrent le Web App Firewall peuvent avoir besoin de connaître.

Comportement correct mais inattendu

La sécurité des applications Web et les sites Web modernes sont complexes. Dans un certain nombre de scénarios, une politique NetScaler peut entraîner un comportement du Web App Firewall différent dans certaines situations de ce à quoi s'attendrait normalement un utilisateur familiarisé avec les politiques. Vous trouverez ci-dessous un certain nombre de cas dans lesquels le Web App Firewall peut se comporter de manière inattendue.

- **Requête avec un en-tête HTTP Host manquant et une URL absolue.** Lorsqu'un utilisateur envoie une demande, dans la majorité des cas, l'URL de la demande est relative. C'est-à-dire qu'il prend comme point de départ l'URL de référence, l'URL où se trouve le navigateur de l'utilisateur lorsqu'il envoie la demande. Si une demande est envoyée sans en-tête Host et avec une URL relative, elle est normalement bloquée à la fois parce qu'elle enfreint la spécification HTTP et parce qu'une demande qui ne spécifie pas l'hôte peut dans certaines circonstances constituer une attaque. Toutefois, si une demande est envoyée avec une URL absolue, même si l'en-tête Host est absent, la demande contourne le Web App Firewall et est transmise au serveur Web. Bien qu'une telle requête viole la spécification HTTP, elle ne constitue pas une menace possible car une URL absolue contient l'hôte.

Stratégies d'audit

May 5, 2023

Les politiques d'audit déterminent les messages générés et enregistrés au cours d'une session Web App Firewall. Les messages sont enregistrés au format SYSLOG sur le serveur NSLOG local ou sur un serveur de journalisation externe. Différents types de messages sont enregistrés en fonction du niveau de journalisation sélectionné.

Pour créer une politique d'audit, vous devez d'abord créer un serveur NSLOG ou un serveur SYSLOG. Ensuite, vous créez la politique et spécifiez le type de journal et le serveur auquel les journaux sont envoyés.

Pour créer un serveur d'audit à l'aide de l'interface de ligne de commande

Vous pouvez créer deux types de serveurs d'audit différents : un serveur NSLOG ou un serveur SYSLOG. Les noms des commandes sont différents, mais les paramètres des commandes sont les mêmes.

Pour créer un serveur d'audit, à l'invite de commandes, tapez les commandes suivantes :

- `add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]`
- `save ns config`

Exemple

L'exemple suivant crée un serveur syslog nommé syslog1 à l'adresse IP 10.124.67.91, avec des niveaux de journalisation d'urgence, de critique et d'avertissement. La fonction de journalisation est définie sur LOCAL1, qui enregistre toutes les connexions TCP :

```
1 add audit syslogAction syslog1 10.124.67.91 -logLevel emergency
     critical warning -logFacility
2 LOCAL1 -tcp ALL
3 save ns config
4 <!--NeedCopy-->
```

Pour modifier ou supprimer un serveur d'audit à l'aide de l'interface de ligne de commande

- Pour modifier un serveur d'audit, tapez la `<type>` commande set audit, le nom du serveur d'audit et les paramètres à modifier, avec leurs nouvelles valeurs.
- Pour supprimer un serveur d'audit, tapez la `<type>` commande rm audit et le nom du serveur d'audit.

Exemple

L'exemple suivant modifie le serveur syslog nommé syslog1 pour ajouter des erreurs et des alertes au niveau du journal :

```
1 set audit syslogAction syslog1 10.124.67.91 -logLevel emergency
     critical warning alert error
2 -logFacility LOCAL1 -tcp ALL
3 save ns config
```



```
<!--NeedCopy-->
```

Pour créer ou configurer un serveur d'audit à l'aide de l'interface graphique

1. **Accédez à**Sécurité**>**NetScaler Web App Firewall**>**Politiques**>**Audit**> Nslog.**
2. Sur la page Nslog Audit, cliquez sur l'onglet **Serveurs.**
3. Procédez comme suit :
   - Pour ajouter un nouveau serveur d'audit, cliquez sur **Ajouter**.
   - Pour modifier un serveur d'audit existant, sélectionnez le serveur, puis cliquez sur **Modifier**.
4. Sur la page **Créer un serveur d'audit**, définissez les paramètres suivants :
   - Nom
   - Type de serveur
   - Adresse IP
   - Port
   - Niveaux de journalisation
   - Facilité de journalisation
   - Format de date
   - Fuseau horaire
   - Journalisation TCP
   - Journalisation ACL
   - Messages de journal configurables par l'utilisateur
   - Journalisation AppFlow
   - Journalisation NAT à grande échelle
   - Enregistrement des messages ALG
   - Enregistrement des abonnés
   - Interception SSL
   - filtrage d'URL
   - Journalisation de l'inspection du contenu
5. Cliquez sur **Créer** et **Fermer**.



Pour créer une politique d'audit à l'aide de l'interface de ligne de commande

Vous pouvez créer une politique NSLOG ou une stratégie SYSLOG. Le type de politique doit correspondre au type de serveur. Les noms des commandes des deux types de politique sont différents, mais les paramètres des commandes sont les mêmes.

À l'invite de commandes, tapez les commandes suivantes :

- `add audit syslogPolicy <name> <-rule > <action>`
- `save ns config`

Exemple

L'exemple suivant crée une politique nommée SyslogP1 qui enregistre le trafic du Web App Firewall vers un serveur syslog nommé syslog1.

```
add audit syslogPolicy syslogP1 rule "ns_true"action syslog1
save ns config
```

Pour configurer une politique d'audit à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `set audit syslogPolicy <name> [-rule <expression>] [-action <string>]`
- `save ns config`

Exemple

L'exemple suivant modifie la politique nommée SyslogP1 pour enregistrer le trafic du Web App Firewall vers un serveur syslog nommé syslog2.

```
set audit syslogPolicy syslogP1 rule "ns_true"action syslog2
save ns config
```

Pour configurer une politique d'audit à l'aide de l'interface graphique

1. **Accédez à**Sécurité**>**NetScaler Web App Firewall > Politiques**.**
2. Dans le volet de détails, cliquez sur **Audit Nslog Policy.**
3. Sur la page Nslog Auditing, cliquez sur **l'onglet Politiques** et effectuez l'une des opérations suivantes :
   - Pour ajouter une nouvelle politique, cliquez sur **Ajouter**.
   - Pour modifier une stratégie existante, sélectionnez-la, puis cliquez sur **Modifier**.

4. Sur la page **Créer une politique d'audit Nslog**, définissez les paramètres suivants :
   - Nom
   - Type d'audit
   - Type d'expression
   - Serveur
5. Cliquez sur **Create**.



Importations

May 5, 2023

Plusieurs fonctionnalités du Web App Firewall utilisent des fichiers externes que vous chargez vers le Web App Firewall lors de sa configuration. À l'aide de l'interface graphique, vous gérez ces fichiers dans le volet Importations, qui comporte quatre onglets correspondant aux quatre types de fichiers que vous pouvez importer : objets d'erreur HTML, objets d'erreur XML, schémas XML et fichiers WSDL (Web Services Description Language). À l'aide de la ligne de commande NetScaler, vous pouvez importer ces types de fichiers, mais vous ne pouvez pas les exporter.

Objet d'erreur HTML

Lorsque la connexion d'un utilisateur à une page HTML ou Web 2.0 est bloquée, ou qu'un utilisateur demande une page HTML ou Web 2.0 inexistante, le Web App Firewall envoie une réponse d'erreur HTML au navigateur de l'utilisateur. Lorsque vous configurez la réponse d'erreur que le Web App Firewall doit utiliser, vous avez deux choix :

- Vous pouvez configurer une URL de redirection, qui peut être hébergée sur n'importe quel serveur Web auquel les utilisateurs ont également accès. Par exemple, si vous avez une page d'erreur personnalisée sur votre serveur Web, 404.html, vous pouvez configurer le Web App Firewall pour rediriger les utilisateurs vers cette page lorsqu'une connexion est bloquée.
- Vous pouvez configurer un objet d'erreur HTML, qui est une page Web HTML hébergée sur le Web App Firewall lui-même. Si vous choisissez cette option, vous devez charger l'objet d'erreur HTML vers le Web App Firewall. Vous pouvez le faire dans le volet Importations, dans l'onglet Objet d'erreur HTML.

L'objet d'erreur doit être un fichier HTML standard ne contenant aucune syntaxe autre que HTML, à l'exception des variables de personnalisation de l'objet d'erreur du Web App Firewall. Il ne peut pas contenir de scripts CGI, de code analysé par le serveur ou de code PHP. Les variables de personnalisation vous permettent d'intégrer des informations de dépannage dans l'objet d'erreur que l'utilisateur reçoit lorsqu'une demande est bloquée. Bien que la plupart des requêtes bloquées par le Web App Firewall soient illégitimes, même un Web App Firewall correctement configuré peut parfois bloquer des demandes légitimes, en particulier lorsque vous le déployez pour la première fois ou après avoir apporté des modifications importantes à vos sites Web protégés. En intégrant des informations dans la page d'erreur, vous fournissez à l'utilisateur les informations qu'il doit communiquer au support technique afin que les problèmes puissent être résolus.

Les variables de personnalisation de la page d'erreur du Web App Firewall sont les suivantes :

- $ {NS_TRANSACTION_ID}. L'ID de transaction que le Web App Firewall a attribué à cette transaction.
- $ {NS_APPFW_SESSION_ID}. L'ID de session du Web App Firewall.
- $ {NS_APPFW_VIOLATION_CATEGORY}. Le contrôle ou la règle de sécurité spécifique du Web App Firewall qui a été violée.
- $ {NS_APPFW_VIOLATION_LOG}. Le message d'erreur détaillé associé à la violation.
- $ {COOKIE Le contenu du cookie spécifié. Remplacez par le nom du cookie spécifique que vous souhaitez afficher sur la page d'erreur. `<CookieName>` Si vous souhaitez afficher le contenu de plusieurs cookies à des fins de résolution des problèmes, vous pouvez utiliser plusieurs instances de cette variable de personnalisation, chacune portant le nom de cookie approprié.
  Remarque : Si le blocage est activé pour le contrôle de cohérence des cookies, les cookies bloqués ne s'affichent pas sur la page d'erreur car le Web App Firewall les bloque.

Pour utiliser ces variables, vous les incorporez dans le code HTML ou XML de l'objet de la page d'erreur comme s'il s'agissait d'une chaîne de texte ordinaire. Lorsque l'objet d'erreur est affiché à l'utilisateur, pour chaque variable de personnalisation, le Web App Firewall remplace les informations auxquelles la variable fait référence. Un exemple de page d'erreur HTML qui utilise des variables personnalisées est illustré ci-dessous.

```
<!doctype html public "-//w3c//dtd html 4.0//en"> <html> <head> <
   title>Page Not Accessible</title> </head> <body> <h1>Page Not
   Accessible</h1> <p>The page that you accessed is not available. You
    can:</p> <ul> <li>return to the <b><a href="[homePage]">home page
   </a></b>, re-establish your session, and try again, or,</li> <li>
   report this incident to the help desk via <b><a href="mailto:[
   helpDeskEmailAddress]">email</a></b> or by calling [
   helpDeskPhoneNumber].</li> </ul> <p>If you contact the help desk,
   please provide the following information:</p> <table cellpadding=8
   width=80%> <tr><th align="right" width=30%>Transaction ID:</th><td
   align="left" valign="top" width=70%>${
 NS_TRANSACTION_ID }
 </td></tr> <tr><th align="right" width=30%>Session ID:</th><td align=
    "left" valign="top" width=70%>${
 NS_APPFW_SESSION_ID }
 </td></tr> <tr><th align="right" width=30%>Violation Category:</th><
    td align="left" valign="top" width=70%>${
 NS_APPFW_VIOLATION_CATEGORY }
 </td></tr> <tr><th align="right" width=30%>Violation Log:</th><td
    align="left" valign="top" width=70%>${
 NS_APPFW_VIOLATION_LOG }
 </td></tr> <tr><th align="right" width=30%>Cookie Name:</th><td align
    ="left" valign="top" width=70%>${
 COOKIE("[cookieName]") }
 </td></tr> </table> <body> <html>
<!--NeedCopy-->
```

Pour utiliser cette page d'erreur, copiez-la dans un éditeur de texte ou HTML. Remplacez les variables suivantes par les informations locales appropriées, qui sont placées entre crochets pour les distinguer des variables NetScaler. (Laissez-les inchangés.) :

- [homePage]. L'URL de la page d'accueil de votre site Web.
- [helpDeskEmailAddress]. Adresse e-mail que vous souhaitez que les utilisateurs utilisent pour signaler les incidents de blocage.
- [helpDeskPhoneNumber]. Le numéro de téléphone que vous souhaitez que les utilisateurs appellent pour signaler les incidents de blocage.
- [cookieName]. Le nom du cookie dont vous souhaitez afficher le contenu sur la page d'erreur.

Objet d'erreur XML

Lorsque la connexion d'un utilisateur à une page XML est bloquée ou qu'un utilisateur demande une application XML inexistante, le Web App Firewall envoie une réponse d'erreur basée sur XML au navigateur de l'utilisateur. Vous configurez la réponse à l'erreur en téléchargeant une page d'erreur XML vers le Web App Firewall dans le volet Imports, sous l'onglet Objet d'erreur XML. Toutes les réponses d'erreur XML sont hébergées sur le Web App Firewall. Vous ne pouvez pas configurer d'URL de redirection pour les applications XML.

> **Remarque** :
> Vous pouvez utiliser les mêmes variables de personnalisation dans un objet d'erreur XML que dans un objet d'erreur HTML.

Schéma XML

Lorsque le Web App Firewall effectue un contrôle de validation sur la demande d'un utilisateur pour une application XML ou Web 2.0, il peut valider la demande par rapport au schéma XML ou au document de type de conception (DTD) de cette application et rejeter toute demande qui ne suit pas le schéma ou la DTD. Un schéma XML et une DTD sont tous deux des fichiers de configuration XML standard qui décrivent la structure d'un type spécifique de document XML.

WSDL

Lorsque le Web App Firewall effectue un contrôle de validation sur la demande d'un utilisateur pour un service Web XML SOAP, il peut valider la demande par rapport au fichier de définition de type de services Web (WSDL) pour ce service Web. Un fichier WSDL est un fichier de configuration SOAP XML standard qui définit les éléments d'un service Web SOAP XML spécifique.

Importation et exportation de fichiers

May 5, 2023

Vous pouvez importer des objets d'erreur HTML ou XML, des schémas XML, des DTD et des WSDL dans le Web App Firewall à l'aide de l'interface graphique ou de la ligne de commande. Vous pouvez modifier n'importe lequel de ces fichiers dans une zone de texte Web après les avoir importés, pour apporter de petites modifications directement sur NetScaler au lieu d'avoir à les apporter sur votre ordinateur puis à les réimporter. Enfin, vous pouvez exporter n'importe lequel de ces fichiers vers votre ordinateur ou supprimer n'importe lequel de ces fichiers à l'aide de l'interface graphique.

> **Remarque :**
>
> Vous ne pouvez pas supprimer ou exporter un fichier importé à l'aide de la ligne de commande.

Pour importer un fichier à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `import appfw htmlerrorpage <src> <name>`
- `<save> ns config`

Exemple

L'exemple suivant importe un objet d'erreur HTML à partir d'un fichier nommé error.html et lui attribue le nom HTMLError.

```
1 import htmlerrorpage error.html HTMLError
2 save ns config
3 <!--NeedCopy-->
```

Pour importer un fichier à l'aide de l'interface graphique

Avant de tenter d'importer un schéma XML, un fichier DTD ou WSDL, ou un objet d'erreur HTML ou XML à partir d'un emplacement réseau, vérifiez que NetScaler peut se connecter à l'ordinateur Internet ou LAN sur lequel se trouve le fichier. Dans le cas contraire, vous ne pouvez pas importer le fichier ou l'objet.

1. Accédez à **Sécurité > NetScaler Web App Firewall**Importations.
2. Accédez à **Application Firewall** > **Importations**.
3. Dans le volet **Importations du pare-feu des applications**, sélectionnez l'onglet correspondant au type de fichier que vous souhaitez importer, puis cliquez sur **Ajouter**.

   Les onglets sont Page d'erreur HTML, Page d'erreur XML, Schéma XML ou WSDL. Le processus de téléchargement est identique sur les quatre onglets du point de vue de l'utilisateur.
4. Renseignez les champs de la boîte de dialogue.
   - **Nom** : nom de l'objet importé.
   - **Importer depuis** : choisissez l'emplacement du fichier HTML, du fichier XML, du schéma XML ou du fichier WSDL que vous souhaitez importer dans la liste déroulante :
     - **URL : URL** Web sur un site Web accessible à l'appliance.

- **Fichier :** fichier sur un disque dur local ou en réseau ou sur un autre périphérique de stockage.
- **Texte :** saisissez ou collez le texte de la réponse personnalisée directement dans un champ de texte de l'interface graphique.

La troisième zone de texte prend la valeur appropriée. Les trois valeurs possibles sont indiquées ci-dessous.

- **URL**—Tapez l'URL dans la zone de texte.
- **Fichier** : saisissez directement le chemin et le nom du fichier HTML, ou cliquez sur Parcourir pour accéder au fichier HTML.
- **Texte** : le troisième champ est supprimé, laissant un espace vide.

5. Cliquez sur **Continuer**. La boîte de dialogue Contenu du fichier s'affiche. Si vous avez choisi URL ou Fichier, la zone de texte Contenu du fichier contient le fichier HTML que vous avez spécifié. Si vous avez sélectionné Texte, la zone de texte Contenu du fichier est vide.
6. Si vous avez choisi Texte, tapez ou copiez-collez le code HTML de réponse personnalisé que vous souhaitez importer.
7. Cliquez sur **Terminé**.
8. Pour supprimer un objet, sélectionnez-le, puis cliquez sur **Supprimer**.

Pour exporter un fichier à l'aide de l'interface graphique

Avant de tenter d'exporter un schéma XML, un fichier DTD ou WSDL, ou un objet d'erreur HTML ou XML, vérifiez que l'appliance Web App Firewall peut accéder à l'ordinateur sur lequel le fichier doit être enregistré. Dans le cas contraire, vous ne pouvez pas exporter le fichier.

1. Accédez à **Sécurité** > **Web App Firewall** > **Importations**.
2. Dans le volet **Importations du Web App Firewall**, sélectionnez l'onglet correspondant au type de fichier que vous souhaitez exporter.

   Le processus d'exportation est identique sur les quatre onglets du point de vue de l'utilisateur.
3. Sélectionnez le fichier que vous souhaitez exporter.
4. Développez la liste déroulante Action, puis sélectionnez **Exporter**.
5. Dans la boîte de dialogue, choisissez **Enregistrer le fichier** et cliquez sur **OK**.
6. Dans la boîte de dialogue **Parcourir**, accédez au système de fichiers local et au répertoire dans lesquels vous souhaitez enregistrer le fichier exporté, puis cliquez sur **Enregistrer**.

Pour modifier un objet d'erreur HTML ou XML dans l'interface graphique

Vous modifiez le texte des objets d'erreur HTML et XML dans l'interface graphique sans les exporter puis les réimporter.

1. Accédez à **Sécurité > NetScaler Web App Firewall > Importations**, puis sélectionnez l'onglet correspondant au type de fichier que vous souhaitez modifier.
2. Accédez à **Application Firewall** > **Importations**, puis sélectionnez l'onglet correspondant au type de fichier que vous souhaitez modifier.
3. Sélectionnez le fichier que vous souhaitez modifier, puis cliquez sur **Modifier**.

   Le texte de l'objet d'erreur HTML ou XML s'affiche dans une zone de texte du navigateur. Vous pouvez modifier le texte à l'aide des outils et méthodes d'édition standard de votre navigateur.

   Remarque : La fenêtre d'édition est conçue pour vous permettre d'apporter des modifications mineures à votre objet d'erreur HTML ou XML. Pour apporter des modifications importantes, vous pouvez préférer exporter l'objet d'erreur vers votre ordinateur local et utiliser des outils d'édition de pages Web HTML ou XML standard.
4. Cliquez sur **OK**, puis sur **Fermer**.

Configuration globale

January 21, 2021

La configuration globale du Web App Firewall affecte tous les profils et stratégies. Les éléments de configuration globale sont les suivants :

- **Paramètres du moteur.** Ensemble de paramètres globaux (nom de cookie de session, délai d'expiration de session, durée de vie maximale de session, nom d'en-tête de journalisation, profil non défini, profil par défaut et limite de taille d'importation) qui concernent toutes les connexions que le Web App Firewall traite, plutôt qu'un sous-ensemble spécifique de connexions.
- **Champs confidentiels.** Jeu de champs de formulaire dans les formulaires Web qui contiennent des informations sensibles qui ne doivent pas être consignées dans les journaux du Web App Firewall. Les champs de formulaire tels que les champs de mot de passe sur une page d'ouverture de session ou les informations de carte de crédit sur un formulaire de commande de panier d'achat sont normalement désignés comme des champs confidentiels.
- **Types de champs.** Liste des types de champs de formulaire Web utilisés par la vérification de sécurité Formats de champ. Chacun de ces types de champ est défini par une expression régulière conforme à la norme PCRE qui définit le type de données et la longueur minimum/-maximale des données qui doivent être autorisées dans ce type de champ de formulaire.

- **Types de contenu XML.** Liste des types de contenu reconnus comme XML et soumis à des vérifications de sécurité spécifiques au XML. Chacun de ces types de contenu est défini par une expression régulière conforme à la norme PCRE qui définit le type MIME exact attribué à ce contenu.
- **Types de contenu JSON.** Liste des types de contenu reconnus comme JSON et soumis à des vérifications de sécurité spécifiques à JSON. Chacun de ces types de contenu est défini par une expression régulière conforme à la norme PCRE qui définit le type MIME exact attribué à ce contenu.

Réglages du moteur

May 5, 2023

Les paramètres du moteur affectent toutes les demandes et réponses traitées par NetScaler Web App Firewall. Les paramètres sont les suivants :

- **Nom du cookie** : nom du cookie qui stocke l'ID de session NetScaler.
- **Délai d'expiration de session** : période d'inactivité maximale autorisée. Si une session utilisateur ne montre aucune activité pendant cette durée, la session est interrompue et l'utilisateur doit la rétablir en accédant à une page de démarrage désignée.
- **Préfixe de post-chiffrement du cookie** : chaîne qui précède la partie cryptée de tout cookie crypté.
- Durée de**vie maximale de la session** : durée maximale, en secondes, pendant laquelle une session est autorisée à rester active. Une fois cette période atteinte, la session est terminée et l'utilisateur doit la rétablir en accédant à une page de démarrage désignée. Ce paramètre ne peut pas être inférieur au délai d'expiration de la session. Pour désactiver ce paramètre afin qu'il n'y ait pas de durée de vie maximale de session, définissez la valeur sur zéro (0).
- **Nom de l'en-tête de journalisation** : nom de l'en-tête HTTP qui contient l'adresse IP du client, pour la journalisation.
- Profil**non défini : profil**appliqué lorsque l'action de politique correspondante est considérée comme non définie.
- **Profil par défaut** : profil appliqué aux connexions qui ne correspondent pas à une politique.
- **Limite de taille d'importation** : nombre maximal d'octets pour tous les fichiers importés dans l'appliance, y compris les signatures, les WSDL, les schémas, les pages d'erreur HTML et XML. Lors d'une importation, si la taille de l'objet importé fait que le nombre cumulé de tous les fichiers importés dépasse la limite configurée, l'opération d'importation échoue. Et l'appliance affiche le message d'erreur suivant : « *ERREUR : échec de l'importation : dépassement de la limite de taille totale configurée pour les objets importés* ».
- **Limite de débit des messages Learn** : nombre maximum de demandes et de réponses par sec-

onde que le moteur d'apprentissage doit traiter. Les demandes ou réponses supplémentaires dépassant cette limite ne sont pas envoyées au moteur d'apprentissage.

- **Serveur proxy** : un serveur proxy est un serveur intermédiaire qui récupère des données sur Internet pour le compte de l'utilisateur. Il fournit un niveau de sécurité supplémentaire à votre appliance. L'appliance NetScaler sur laquelle l'authentification par proxy est activée s'authentifie auprès du serveur proxy avant de télécharger les mises à jour depuis Internet. De cette façon, il protège les appliances contre les téléchargements malveillants. Configurez les paramètres suivants :
  - **Serveur proxy** : adresse IP du serveur proxy à partir duquel les dernières signatures AWS sont téléchargées.
  - **Port proxy** : numéro de port du serveur proxy à partir duquel les dernières signatures AWS sont téléchargées.
  - **Nom d'utilisateur du proxy** : numéro de port du serveur proxy à partir duquel les dernières signatures AWS sont téléchargées.
  - **Mot de passe du proxy** : mot de passe permettant de s'authentifier auprès du serveur proxy pour télécharger les mises à jour des signatures.
- Décodage des**entités : permet de décoder**les entités HTML lors de l'exécution des vérifications du Web App Firewall.
- **Enregistrer les requêtes malformées : active**la journalisation des requêtes HTTP malformées.
- **Utiliser une clé secrète configurable** : utilisez une clé secrète configurable pour les opérations du Web App Firewall. Cette clé secrète est utilisée pour signer et vérifier les données. Lorsque « UseConfigurableSecretKey » est activé, vous devez utiliser la clé activée dans le paramètre « set ns EncryptionParams ».
- **Réinitialiser les données apprises** : supprimez toutes les données apprises du Web App Firewall. Redémarre le processus d'apprentissage en collectant de nouvelles données.

Deux paramètres, *Réinitialiser les données apprises* et *Mise à jour automatique des signatures*, se trouvent à différents endroits selon que vous utilisez l'interface de commande ou l'interface graphique de NetScaler pour configurer votre NetScaler Web App Firewall. Lorsque vous utilisez l'interface de commande, vous configurez Reset Learned Data à l'aide de la commande reset appfw learning data. Cela ne prend aucun paramètre et n'a aucune autre fonction. Vous pouvez configurer la mise à jour automatique des signatures dans la commande set appfw settings. Le paramètre -SignatureAutoUpdate active ou désactive la mise à jour automatique des signatures, et -SignatureURL configure l'URL qui héberge le fichier de signatures mis à jour.

Lorsque vous utilisez l'interface graphique de NetScaler, vous configurez la réinitialisation des données apprises dans **Sécurité > NetScaler Web App Firewall > Paramètres**du moteur. L'option **Réinitialiser les données apprises** se trouve au bas de la boîte de dialogue. Vous configurez la mise à jour automatique des signatures pour chaque ensemble de signatures dans **Sécurité** > **NetScaler Web App Firewall** > **Signatures, en sélectionnant le fichier de signatures**, en cliquant sur le bouton

droit de la souris et en sélectionnant Paramètres de mise à jour **automatique**.

Normalement, les valeurs par défaut des paramètres du **Web App Firewall** sont correctes. Si les paramètres par défaut provoquent un conflit avec d'autres serveurs ou entraînent la déconnexion prématurée de vos utilisateurs, vous devez toutefois les modifier.

La limite de session du **Web App Firewall** est configurable à l'aide de la commande suivante :

```
> set appfw settings -sessionLimit 500000

Done

Default value:100000   Max value:500000 per PE
<!--NeedCopy-->
```

Pour configurer les paramètres du moteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- set appfw settings [-sessionCookieName <name>] [-sessionTimeout <positiveInteger>] [-sessionLifetime <positiveInteger>][-clientIPLoggingHeader <headerName>] [-undefaction <profileName>] [-defaultProfile <profileName>] [-importSizeLimit <positiveInteger>] [-logMalformedReq (ON | OFF)] [-signatureAutoUpdate (ON | OFF)] [-signatureUrl <expression>] [-cookiePostEncryptPrefix <string>] [-entityDecoding (ON | OFF)] [-useConfigurableSecretKey (ON | OFF)][-learnRateLimit <positiveInteger>] [-proxyServer <proxy server ip>] [-proxyPort <proxy server port>] [-proxyUsername <username>] [-proxyPassword <password>]
- save ns config

Exemple

```
set appfw settings -sessionCookieName citrix-appfw-id -sessionTimeout
    3600
-sessionLifetime 14400 -clientIPLoggingHeader NS-AppFW-Client-IP -
    undefaction APPFW_RESET
-defaultProfile APPFW_RESET -importSizeLimit 4096 -proxyServer
    10.102.30.112 -proxyPort 3128 -proxyUsername defaultusername -
    proxyPassword defaultpassword
save ns config
<!--NeedCopy-->
```


Pour configurer les paramètres du moteur à l'aide de l'interface graphique NetScaler

1. Accédez à **Sécurité** > **NetScaler Web App Firewall**
2. Dans le volet de détails, cliquez sur **Modifier les paramètres du moteur** sous **Paramètres**.
3. Dans la boîte de dialogue **Paramètres du moteur Web App Firewall**, définissez les paramètres suivants :
    - Nom du cookie
    - Délai d'expiration de la session
    - Préfixe Cookie Post Encrypt
    - Durée de vie maximale des sessions
    - Nom de l'en-tête de journalisation
    - Profil non défini
    - Profil par défaut
    - Limite de taille d'importation
    - Limite de débit Learn Messages
    - Serveur proxy
    - Port du proxy
    - Nom d'utilisateur du proxy
    - Mot de passe du proxy
    - Décodage d'entités
    - Enregistrer une demande mal formée
    - Utiliser une clé secrète
    - Limite de débit de messages Learn
    - Mise à jour automatique des signatures
4. Cliquez sur **OK**.



Champs confidentiels

May 5, 2023

Vous pouvez définir les champs de formulaire Web comme confidentiels afin de protéger les informations que les utilisateurs y saisissent. Normalement, toutes les informations qu'un utilisateur saisit dans un formulaire Web sur l'un de vos serveurs Web protégés sont enregistrées dans les journaux NetScaler. Les informations saisies dans un champ de formulaire Web désigné comme confidentiel ne sont toutefois pas enregistrées. Ces informations ne sont enregistrées que lorsque le site Web est configuré pour enregistrer ces données, normalement dans une base de données sécurisée.

Les types courants d'informations que vous pouvez vouloir protéger avec une désignation de champ confidentiel sont les suivants :

- Mots de passe
- Numéros de carte de crédit, codes de validation et dates d'expiration
- Numéros de sécurité sociale
- Numéros d'identification fiscale
- Adresses domiciliaires
- Numéros de téléphone privés

En plus d'être une bonne pratique, l'utilisation appropriée de désignations de champs confidentielles peut être nécessaire pour la conformité PCI-DSS sur les serveurs de commerce électronique, la conformité HIPAA sur les serveurs qui gèrent les informations médicales aux États-Unis et la conformité à d'autres normes de protection des données.

> **Important** :
>
> Dans les deux cas suivants, la désignation de champ confidentiel ne fonctionne pas comme prévu :

- Si un formulaire Web comporte un champ confidentiel ou une URL d'action de plus de 256 caractères, le champ ou l'URL d'action est tronqué dans les journaux NetScaler.
- Avec certaines transactions SSL, les journaux sont tronqués si le champ confidentiel ou l'URL de l'action comporte plus de 127 caractères.

Dans l'un ou l'autre de ces cas, le Web App Firewall masque une chaîne de quinze caractères avec la lettre « x », au lieu de la chaîne normale de huit caractères. Pour garantir la suppression de toute information confidentielle, l'utilisateur doit utiliser le nom du champ de formulaire et les expressions d'URL d'action qui correspondent aux 256 premiers caractères ou (dans les cas où SSL est utilisé) aux 127 premiers caractères.

Pour configurer votre Web App Firewall afin qu'il traite un champ de formulaire Web d'un site Web protégé comme confidentiel, vous ajoutez ce champ à la liste Champs confidentiels. Vous pouvez entrer le nom du champ sous forme de chaîne ou saisir une expression régulière compatible PCRE spécifiant un ou plusieurs champs. Vous pouvez activer la désignation du champ confidentiel lorsque vous ajoutez le champ, ou vous pouvez modifier la désignation ultérieurement.

> **Remarque**
>
> À partir de la version 13.1 build 27.x, les champs confidentiels sont également pris en charge dans les profils WAF. Pour plus d'informations, consultez Champs confidentiels dans le profil WAF.

Pour ajouter un champ confidentiel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX )] [-comment "<string>"] [-state ( ENABLED | DISABLED )]`

- save ns config

Exemple

L'exemple suivant ajoute tous les champs de formulaire Web dont le nom commence par Password à la liste des champs confidentiels.

```
1 add appfw confidField Password "https?://www[.]example[.]com/[^<>]\*[^a
    -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)" -isRegex
    REGEX -state ENABLED
2 save ns config
3 <!--NeedCopy-->
```

Pour modifier un champ confidentiel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- set appfw confidField <fieldName> <url> [-isRegex (REGEX | NOTREGEX)][-comment "<string>"] [-state (ENABLED | DISABLED)]
- save ns config

Exemple

L'exemple suivant modifie la désignation du champ confidentiel pour y ajouter un commentaire.

```
1 set appfw confidField Password "https?://www[.]example[.]com/[^<>]\*[^a
    -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)" -comment "
    Protect password fields." -isRegex REGEX -state ENABLED
2 save ns config
3 <!--NeedCopy-->
```

Pour supprimer un champ confidentiel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- rm appfw confidField <fieldName> <url>
- save ns config

Pour configurer un champ confidentiel à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Pare-feu d'applications**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Gérer les champs confidentiels**.

3. Dans la boîte de dialogue Gérer les champs confidentiels, effectuez l'une des opérations suivantes :
   - Pour ajouter un nouveau champ de formulaire à la liste, cliquez sur Ajouter.
   - Pour modifier la désignation d'un champ confidentiel existant, sélectionnez-le, puis cliquez sur **Modifier**.

     La boîte de dialogue **Champs confidentiels du Web App Firewall** s'affiche.

     > **Remarque** :
     > Si vous sélectionnez une désignation de champ confidentiel existant, puis que vous cliquez sur **Ajouter**, la boîte de dialogue **Créer un champ de formulaire confidentiel** affiche les informations relatives à ce champ confidentiel. Vous pouvez modifier ces informations pour créer votre nouveau champ confidentiel.
4. Dans la boîte de dialogue, remplissez les éléments. Ils sont :
   - **Case à cocher Activée.** Sélectionnez ou désactivez cette option pour activer/désactiver cette désignation de champ confidentiel.
   - **Case à cocher Nom du champ de formulaire est-il une expression régulière ?** Sélectionnez ou désactivez cette option pour activer les expressions régulières au format PCRE dans le nom du champ de formulaire.
   - **Nom du champ.** Entrez une chaîne littérale ou une expression régulière au format PCRE qui représente un nom de champ spécifique ou qui met en correspondance plusieurs champs dont les noms suivent un modèle.
   - **URL de l'action.** Entrez une URL littérale ou une expression régulière qui définit une ou plusieurs URL de la ou des pages Web sur lesquelles se trouvent le (s) formulaire (s) Web contenant le champ confidentiel.
   - **Commentaires.** Saisissez un commentaire. Facultatif.
5. Cliquez sur **Créer** ou **sur OK**.
6. Pour supprimer une désignation de champ confidentiel de la liste des champs confidentiels, sélectionnez la liste des champs confidentiels que vous souhaitez supprimer, puis cliquez sur Supprimer pour la supprimer, puis cliquez sur **OK** pour confirmer votre choix.
7. Lorsque vous avez terminé d'ajouter, de modifier et de supprimer les désignations de champs confidentielles, cliquez sur **Fermer**.

Exemples

Voici quelques expressions régulières qui définissent des noms de champs de formulaire qui peuvent vous être utiles :

- `^passwd_ (Applies confidential-field status to all field names that begin with the “passwd_” string.)`
- `^((\[0-9a-zA-Z._-]*||\\x\[0-9A-Fa-f][0-9A-Fa-f])+-)?passwd_ (Applies confidential-field status to all field names that begin with the string`


```
passwd_, or that contain the string -passwd_ after another string that
might contain non-ASCII special characters.)
```

Voici quelques expressions régulières qui définissent des types d'URL spécifiques qui peuvent vous être utiles. Remplacez votre (vos) propre (s) hébergeur (s) Web et domaine (s) par ceux des exemples.

- Si le formulaire Web apparaît sur plusieurs pages Web de l'hôte Web www.exemple.com, mais que toutes ces pages Web sont nommées logon.pl ? , vous pouvez utiliser l'expression régulière suivante :

```
1 https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_.-]*/)*logon
     [.]pl?
2 <!--NeedCopy-->
```

- Si le formulaire Web apparaît sur plusieurs pages Web de l'hôte Web www.example-español.com, qui contient le caractère spécial n-tilde (ñ), vous pouvez utiliser l'expression régulière suivante, qui représente le caractère spécial n-tilde sous la forme d'une chaîne UTF-8 codée contenant C3 B1, le code hexadécimal assigné à caractère dans le jeu de caractères UTF-8 :

```
1 https?://www[.]example-espa\xC3\xB1ol[.]com/([0-9A-Za-z][0-9A-Za-
     z_.-]\*/)\* logon[.]pl?
2 <!--NeedCopy-->
```

- Si le formulaire Web contenant query.pl apparaît sur plusieurs pages Web sur différents hôtes du domaine exemple.com, vous pouvez utiliser l'expression régulière suivante :

```
1 https?://([0-9A-Za-z][0-9A-Za-z_-.]*[.])\*example[.]com/([0-9A-Za
     -z][0-9A-Za-z_-.]\*/)*logon[.]pl?
2 <!--NeedCopy-->
```

- Si le formulaire Web contenant query.pl apparaît sur plusieurs pages Web sur différents hôtes dans différents domaines, vous pouvez utiliser l'expression régulière suivante :

```
1 https?://([0-9A-Za-z][0-9A-Za-z_-.]\*[.])\*[0-9A-Za-z][0-9A-Za-z_
     -.]+[.][a-z]{
2 2,6 }
3 /([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon[.]pl?
4 <!--NeedCopy-->
```

- Si le formulaire Web apparaît sur plusieurs pages Web de l'hôte Web www.exemple.com, mais que toutes ces pages Web sont nommées logon.pl ? , vous pouvez utiliser l'expression régulière suivante :


```
https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon
   [.]pl?
<!--NeedCopy-->
```

Types de champs

August 20, 2021

Un type de champ est une expression régulière au format PCRE qui définit un format de données particulier et des longueurs minimum/maximales de données pour un champ de formulaire dans un formulaire Web. Les types de champs sont utilisés dans la vérification Formats des champs.

Le Web App Firewall est livré avec plusieurs types de champs par défaut, à savoir :

- entier. Chaîne de n'importe quelle longueur composée de nombres seulement, sans virgule décimale, et avec un signe moins (-) facultatif.
- Alpha. Chaîne de n'importe quelle longueur composée de lettres seulement.
- alphanum. Chaîne de n'importe quelle longueur composée de lettres et/ou de chiffres.
- nohtml. Chaîne de n'importe quelle longueur composée de caractères, y compris la ponctuation et les espaces, qui ne contient pas de symboles ou de requêtes HTML.
- tout. N'importe quoi du tout.

  > **Important :**
  >
  > L'affectation de n'importe quel type de champ comme type de champ par défaut, ou à un champ, permet d'envoyer des scripts actifs, des commandes SQL et d'autres contenus potentiellement dangereux à vos sites Web et applications protégés dans ce champ de formulaire. Vous devez utiliser le n'importe quel type avec parcimonie, si vous l'utilisez du tout.

Vous pouvez également ajouter vos propres types de champs à la liste Types de champs. Par exemple, vous pouvez ajouter un type de champ pour un numéro de sécurité sociale, un code postal ou un numéro de téléphone dans votre pays. Vous pouvez également ajouter un type de champ pour un numéro d'identification client ou un numéro de carte de crédit de magasin.

Pour ajouter un type de champ à la liste Types de champ, saisissez le nom du champ sous la forme d'une chaîne littérale ou d'une expression régulière au format PCRE.

Pour ajouter un type de champ à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- add appfw fieldType <name> <regex> <priority> [-comment "<string>"]
- save ns config

Exemple

L'exemple suivant montre comment ajouter un type de champ nommé SSN qui correspond aux numéros de sécurité sociale américains à la liste Types de champs et définir sa priorité sur 1.

```
add appfw fieldType SSN "^[1-9][0-9]{
 2,2 }
 -[0-9 }
 {
 2,2 }
 -[0-9]{
 4,4 }
 $" 1
save ns config
<!--NeedCopy-->
```

Pour modifier un type de champ à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- set appfw fieldType <name> <regex> <priority> [-comment "<string>"]
- save ns config

Exemple

L'exemple suivant montre comment modifier le type de champ pour ajouter un commentaire.

```
set appfw fieldType SSN "^[1-9][0-9]{
 2,2 }
 -[0-9 }
 {
 2,2 }
 -[0-9]{
 4,4 }
 $" 1 -comment "US Social Security Number"
save ns config
<!--NeedCopy-->
```


Pour supprimer un type de champ à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- >rm appfw fieldType <name>
- save ns config

Pour configurer un type de champ à l'aide de l'interface graphique

1. Accédez à Sécurité > Pare-feu d'application.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Gérer les types de champs**.
3. Dans la boîte de dialogue **Gérer les types de champs**, effectuez l'une des opérations suivantes :
   - Pour ajouter un nouveau type de champ à la liste, cliquez sur **Ajouter**.
   - Pour modifier un type de champ existant, sélectionnez-le, puis cliquez sur **Modifier**. La boîte de dialogue **Configurer le type de champ** s'affiche.

   > **Remarque :**
   >
   > Si vous sélectionnez une désignation de type de champ existante, puis cliquez sur **Ajouter**, la boîte de dialogue affiche les informations relatives à ce type de champ. Vous pouvez modifier ces informations pour créer votre nouveau type de champ.
4. Dans la boîte de dialogue, remplissez les éléments. Ils sont :
   - Nom
   - Expression régulière
   - Priority
   - Commentaire
5. Cliquez sur Créer ou sur OK.
6. Pour supprimer un type de champ de la liste Types de champ, sélectionnez le type de champ à supprimer, puis cliquez sur **Supprimer** pour le supprimer, puis cliquez sur **OK** pour confirmer votre choix.
7. Lorsque vous avez terminé d'ajouter, de modifier et de supprimer des types de champ, cliquez sur **Fermer**.

Exemples

Voici quelques expressions régulières pour les types de champs que vous pourriez trouver utiles :

Numéros de sécurité sociale aux^[1-9][0-9]{ 2,2 } -[0-9 } { 2,2 } -[0-9]{ 4,4 } $ États-Unis

Numéro du permis de conduire en^\[A-C\]\[0-9\]{ 7,7 } $ Californie

Numéros de téléphone`^+[0-9]{ 1,3 } [0-9()-]{ 1,40 } $` internationaux avec codes de pays

Numéros de code postal`^[0-9]{ 5,5 } -[0-9]{ 4,4 } $` américain

`^[0-9A-Za-z][0-9A-Za-z.+_-]{ 0,25 } @([0-9A-Za-z][0-9A-Za-z_-]*[.]){ 1,4 } [A-Za-z]{ 2,6 } $` Adresses e-mail

Types de contenu XML

January 21, 2021

Par défaut, le Web App Firewall traite les fichiers qui suivent certaines conventions de dénomination comme XML. Vous pouvez configurer le Web App Firewall pour examiner le contenu Web à la recherche de chaînes ou de modèles supplémentaires indiquant que ces fichiers sont des fichiers XML. Cela peut garantir que le Web App Firewall reconnaît tout le contenu XML de votre site, même si certains contenus XML ne respectent pas les conventions normales d'attribution de noms XML, ce qui garantit que le contenu XML est soumis à des vérifications de sécurité XML.

Pour configurer les types de contenu XML, ajoutez les modèles appropriés à la liste Types de contenu XML. Vous pouvez entrer un type de contenu sous forme de chaîne, ou vous pouvez entrer une expression régulière compatible PCRE spécifiant une ou plusieurs chaînes. Vous pouvez également modifier les modèles de types de contenu XML existants.

Pour ajouter un modèle de type de contenu XML à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw XMLContentType <XMLContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Exemple

L'exemple suivant montre comment ajouter le motif. */xml à la liste des types de contenu XML et la désigne comme une expression régulière.

```
1 add appfw XMLContentType ".*/xml" -isRegex REGEX
2 <!--NeedCopy-->
```


Pour supprimer un modèle de type de contenu XML à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `rm appfw XMLContentType <XMLContenttypevalue>`
- `save ns config`

Pour configurer la liste des types de contenu XML à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Web App Firewall**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Gérer les types de contenu XML**.
3. Dans la boîte de dialogue **Gérer les types de contenu XML**, effectuez l'une des opérations suivantes :
   - Pour ajouter un nouveau type de contenu XML, cliquez sur Ajouter.
   - Pour modifier un type de contenu XML existant, sélectionnez-le, puis cliquez sur Modifier. La boîte de dialogue Configurer le type de contenu XML du Web App Firewall apparaît. Remarque : Si vous sélectionnez un modèle de type de contenu XML existant, puis cliquez sur Ajouter, la boîte de dialogue affiche les informations relatives à ce modèle de type de contenu XML. Vous pouvez modifier ces informations pour créer votre nouveau modèle de type de contenu XML.
4. Dans la boîte de dialogue, remplissez les éléments. Ils sont :
   - **IsRegex.** Sélectionnez ou désactivez pour activer les expressions régulières au format PCRE dans le nom du champ de formulaire.
   - **Type de contenu XML** Entrez une chaîne littérale ou une expression régulière au format PCRE correspondant au modèle de type de contenu XML que vous souhaitez ajouter.
5. Cliquez sur **Créer**.
6. Pour supprimer un modèle de type de contenu XML de la liste, sélectionnez-le, puis cliquez sur **Supprimer** pour le supprimer, puis cliquez sur **OK** pour confirmer votre choix.
7. Lorsque vous avez terminé d'ajouter et de supprimer des modèles de type de contenu XML, cliquez sur **Fermer**.

Types de contenu JSON

January 21, 2021

Par défaut, le Web App Firewall traite les fichiers avec le type de contenu "application/json" comme des fichiers JSON. Le paramètre par défaut permet au pare-feu d'application Web de reconnaître le contenu JSON dans les requêtes et les réponses, et de gérer ce contenu de manière appropriée.

Vous pouvez configurer le Web App Firewall pour examiner le contenu Web à la recherche de chaînes ou de modèles supplémentaires indiquant que ces fichiers sont des fichiers JSON. Cela peut garantir que le Web App Firewall reconnaît tout le contenu JSON de votre site, même si certains contenus JSON ne suivent pas les conventions d'attribution de noms JSON normales, garantissant que le contenu JSON est soumis à des vérifications de sécurité JSON.

Pour configurer les types de contenu JSON, ajoutez les modèles appropriés à la liste Types de contenu JSON. Vous pouvez entrer un type de contenu sous forme de chaîne, ou vous pouvez entrer une expression régulière compatible PCRE spécifiant une ou plusieurs chaînes. Vous pouvez également modifier les modèles de types de contenu JSON existants.

Pour ajouter un modèle de type de contenu JSON à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add appfw JSONContentType <JSONContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Exemple

L'exemple suivant montre comment ajouter le motif. */json à la liste des types de contenu JSON et la désigne comme une expression régulière.

```
1 add appfw JSONContentType ".*/json" -isRegex REGEX
2 <!--NeedCopy-->
```

Pour configurer la liste des types de contenu JSON à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Pare-feu d'application**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Gérer les types de contenu JSON**.
3. Dans la boîte de dialogue Gérer les types de contenu JSON, effectuez l'une des opérations suivantes :
   - Pour ajouter un nouveau type de contenu JSON, cliquez sur Ajouter.
   - Pour modifier un type de contenu JSON existant, sélectionnez-le, puis cliquez sur Modifier. La boîte de dialogue Configurer le type de contenu JSON du Web App Firewall s'affiche. Remarque : Si vous sélectionnez un modèle de type de contenu JSON existant, puis cliquez sur Ajouter, la boîte de dialogue affiche les informations relatives à ce modèle de type de contenu JSON. Vous pouvez modifier ces informations pour créer votre nouveau modèle de type de contenu JSON.

4. Dans la boîte de dialogue, remplissez les éléments. Ils sont :
   - **IsRegex.** Sélectionnez ou désactivez pour activer les expressions régulières au format PCRE dans le nom du champ de formulaire.
   - **Type de contenu JSON** Entrez une chaîne littérale ou une expression régulière au format PCRE qui correspond au modèle de type de contenu JSON que vous souhaitez ajouter.
5. Cliquez sur **Créer** ou **sur OK**.
6. Pour supprimer un modèle de type de contenu JSON de la liste, sélectionnez-le, puis cliquez sur **Supprimer** pour le supprimer, puis cliquez sur **OK** pour confirmer votre choix.
7. Lorsque vous avez terminé d'ajouter et de supprimer des modèles de type de contenu XML, cliquez sur **Fermer**.

Statistiques et rapports

May 5, 2023

Les informations conservées dans les journaux et les statistiques, et affichées dans les rapports, fournissent des conseils importants pour la configuration et la maintenance du Web App Firewall.

Statistiques du Web App Firewall

Lorsque vous activez l'action de statistiques pour les signatures ou les contrôles de sécurité du Web App Firewall, le Web App Firewall conserve des informations sur les connexions qui correspondent à cette signature ou à cette vérification de sécurité. Vous pouvez afficher les informations statistiques accumulées dans l'onglet
Surveillance en sélectionnant l'un des choix suivants dans la zone de liste Sélectionner un groupe :

- **Web App Firewall.** Récapitulatif de toutes les informations statistiques collectées par votre appliance Web App Firewall pour tous les profils.
- **Web App Firewall (par profil).** Les mêmes informations, mais affichées par profil plutôt que résumées.

Vous pouvez utiliser ces informations pour surveiller le fonctionnement de votre Web App Firewall et déterminer s'il existe une activité anormale ou un nombre anormal d'accès à une signature ou à un contrôle de sécurité. Si vous constatez un tel schéma d'activité anormale, vous pouvez consulter les journaux pour détecter cette signature ou cette vérification de sécurité afin de diagnostiquer et de prendre des mesures correctives.

Compteur statistique Relaxation

En fonction de l'assouplissement appliqué au trafic violé, vous pouvez également afficher des informations statistiques telles que le nombre de fois qu'une violation se produit sur l'appliance, le nombre de règles de relaxation appliquées au moment de la violation et son dernier horodatage appliqué. En effectuant cette opération, le moteur d'apprentissage centralisé peut supprimer automatiquement les liaisons de relaxation inutilisées ou redondantes. Pour plus d'informations, consultez la rubrique Moteur d'apprentissage WAF .

Le compteur statistique des coups de relaxation est disponible uniquement pour les contrôles de sécurité suivants.

- Scriptage intersite
- Injection SQL
- Cohérence des cookies
- JSON SQL
- Script intersite JSON
- DDoS JSON
- Injection de CMD JSON
- Falsification de demande intersite
- Format de champ
- URL de démarrage
- Denyurl
- Protection du type de contenu

Pour afficher les statistiques des compteurs d'accès aux règles de relaxation à l'aide de la CLI

À l'invite de commande, tapez :

```
stat appfw profile p1
```

Exemple :

```
stat appfw profile p1 -fullvalues
```

Statistiques des règles Starturl

Rule	hits	Taux	heure du dernier accès
87a4…51177	0	0	Jeu… 1970
5b83…dc12a	0	0	Jeu… 1970
12345	0	0	Jeu… 1970

Pour afficher les statistiques des compteurs d'accès aux règles de relaxation à l'aide de l'interface graphique

Procédez comme suit pour afficher les statistiques du compteur d'accès aux règles de relaxation :

1. Accédez à **Sécurité > NetScaler Web App Firewall > Profils**.
2. Dans le volet de détails, sélectionnez un **profil de Web App Firewall** et cliquez sur **Statistiques**.
3. La page des **statistiques de NetScaler Web App Firewall** affiche les détails des statistiques.
4. Vous pouvez sélectionner Vue tabulaire ou passer en mode Affichage graphique pour afficher les données sous forme de tableau ou de graphique.

Rapports sur le Web App Firewall

Les rapports Web App Firewall fournissent des informations sur la configuration de votre Web App Firewall et sur la façon dont il gère le trafic pour vos sites Web protégés.

Le rapport PCI DSS

La norme de sécurité des données de l'industrie des cartes de paiement (PCI), version 1.2, comprend 12 critères de sécurité que la plupart des sociétés de cartes de crédit exigent des entreprises qui acceptent les paiements en ligne par carte de crédit et de débit. Les critères sont conçus pour empêcher le vol d'identité, le piratage et d'autres types de fraude. Si un fournisseur de services Internet ne répond pas aux critères PCI DSS, il peut perdre l'autorisation d'accepter les paiements par carte de crédit via le site Web.

Les FAI et les marchands en ligne prouvent qu'ils sont conformes à la norme PCI DSS en faisant effectuer un audit par une société d'évaluation de la sécurité qualifiée (QSA) PCI DSS. Le rapport PCI DSS est conçu pour les aider à la fois avant et pendant l'audit. Avant l'audit, il indique quels paramètres de Web App Firewall sont pertinents pour PCI DSS, comment ils doivent être configurés et (surtout) si votre configuration actuelle de Web App Firewall est conforme à la norme. Au cours de l'audit, le rapport peut être utilisé pour démontrer la conformité à un critère PCI DSS pertinent.

Le rapport PCI DSS se compose d'une liste de ces critères qui sont pertinents pour la configuration de votre Web App Firewall. Sous chaque critère, il répertorie vos options de configuration actuelles, indique si votre configuration actuelle est conforme au critère PCI DSS et explique comment configurer le Web App Firewall afin que vos sites Web protégés soient conformes au critère.

Le rapport PCI DSS se trouve sous **Système > Rapports**. Pour générer le rapport sous forme de fichier Adobe PDF, cliquez sur **Générer un rapport PCI DSS**. Selon les paramètres de votre navigateur, le rapport s'affiche dans la fenêtre contextuelle ou vous êtes invité à l'enregistrer sur votre disque dur.

> **Remarque :**
>
> Pour afficher ce rapport et d'autres, le programme Adobe Reader doit être installé sur votre ordinateur.

Le rapport PCI DSS comprend les sections suivantes :

- **Descriptif.** Description du rapport Récapitulatif de conformité PCI DSS.
- **Statut de la licence et des fonctionnalités du pare-feu.** Vous indique si le Web App Firewall est sous licence et activé sur votre appliance NetScaler.
- **Résumé exécutif.** Tableau qui répertorie les critères PCI DSS et indique lesquels de ces critères sont pertinents pour le Web App Firewall.
- **Informations détaillées sur les critères PCI DSS.** Pour chaque critère PCI DSS pertinent à la configuration de votre Web App Firewall, le rapport PCI DSS fournit une section qui contient des informations indiquant si votre configuration est conforme et, si ce n'est pas le cas, comment la mettre en conformité.
- **Configuration.** Les données des profils individuels, auxquels vous accédez soit en cliquant sur Configuration du Web App Firewall en haut du rapport, soit directement à partir du volet Rapports. Le rapport de configuration du Web App Firewall est le même que le rapport PCI DSS, avec le résumé spécifique à PCI DSS omis.

Le rapport de configuration du Web App Firewall

Le rapport de configuration du Web App Firewall se trouve sous **Système > Rapports**. Pour l'afficher, cliquez sur **Générer le rapport de configuration du Web App Firewall**. Selon les paramètres de votre navigateur, le rapport s'affiche dans la fenêtre contextuelle ou vous êtes invité à l'enregistrer sur votre disque dur.

Le rapport de configuration du Web App Firewall commence par une page Récapitulatif, qui comprend les sections suivantes :

- **Stratégies de Web App Firewall.** Tableau qui répertorie vos stratégies de Web App Firewall actuelles, indiquant le nom de la stratégie, le contenu de la stratégie, l'action (ou le profil) à laquelle elle est associée et des informations de liaison globale.
- **Profils de Web App Firewall.** Tableau qui répertorie vos profils de Web App Firewall actuels et indique à quelle stratégie chaque profil est associé. Si aucun profil n'est associé à une stratégie, le tableau affiche INACTIF à cet emplacement.

Pour télécharger toutes les pages de rapport pour toutes les stratégies, en haut de la page Récapitulatif des profils, cliquez sur **Télécharger tous les profils**. Vous affichez la page de rapport de chaque profil individuel en sélectionnant ce profil dans le tableau en bas de l'écran. La page Profil d'un profil

individuel indique si chaque action de vérification est activée ou désactivée pour chaque vérification, ainsi que les autres paramètres de configuration de la vérification.

Pour télécharger un fichier PDF contenant la page de rapport PCI DSS pour le profil actuel, cliquez sur **Télécharger le profil actuel** en haut de la page. Pour revenir à la page Récapitulatif des profils, cliquez sur **Profils du Web App Firewall**. Pour revenir à la page principale, cliquez sur **Accueil**. Vous pouvez actualiser le rapport PCI DSS à tout moment en cliquant sur **Actualiser** dans le coin supérieur droit du navigateur.

Journaux du Web App Firewall

May 5, 2023

Le Web App Firewall génère des messages de journal pour le suivi de la configuration, l'appel de stratégie et les détails de violation de contrôle de sécurité.

Lorsque vous activez l'action de journalisation pour les contrôles de sécurité ou les signatures, les messages de journal qui en résultent fournissent des informations sur les demandes et les réponses que le Web App Firewall a observées lors de la protection de vos sites Web et applications. Les informations les plus importantes sont l'action entreprise par le Web App Firewall lorsqu'une signature ou une violation du contrôle de sécurité a été observée. Pour certains contrôles de sécurité, le message de journal peut fournir des informations utiles, telles que l'emplacement de l'utilisateur ou le schéma détecté ayant déclenché une violation. Une augmentation excessive du nombre de messages de violation dans les journaux peut indiquer une augmentation du nombre de requêtes malveillantes. Le message vous avertit que votre application est peut-être attaquée pour exploiter une vulnérabilité spécifique détectée et contrecarrée par les protections du Web App Firewall.

> **Remarque :**
>
> Si vous souhaitez séparer les journaux de NetScaler Web App Firewall des journaux système, vous devez utiliser un serveur SYSLOG externe.

Journaux au format NetScaler (natif)

Le Web App Firewall utilise les journaux au format NetScaler (également appelés journaux au format natif) par défaut. Ces journaux ont le même format que ceux générés par les autres fonctionnalités de NetScaler. Chaque journal contient les champs suivants :

- Horodatage. Date et heure de la connexion.
- Gravité. Niveau de gravité du journal.
- module. Module NetScaler qui a généré l'entrée du journal.

- Type d'événement. Type d'événement, tel qu'une violation de signature ou une violation du contrôle de sécurité.
- ID de l'événement. ID attribué à l'événement.
- Adresse IP du client. Adresse IP de l'utilisateur dont la connexion a été enregistrée.
- ID de transaction. ID attribué à la transaction à l'origine du journal.
- ID de session. ID attribué à la session utilisateur à l'origine du journal.
- Message. Le message du journal. Contient des informations identifiant la signature ou le contrôle de sécurité qui a déclenché l'entrée du journal.

Vous pouvez rechercher n'importe lequel de ces champs ou n'importe quelle combinaison d'informations provenant de différents champs. Votre sélection est limitée uniquement par les fonctionnalités des outils que vous utilisez pour afficher les journaux. Vous pouvez consulter les messages du journal du Web App Firewall dans l'interface graphique en accédant à la visionneuse Syslog NetScaler, ou vous pouvez vous connecter manuellement à l'appliance NetScaler et accéder aux journaux depuis l'interface de ligne de commande, ou vous pouvez accéder au shell et suivre les journaux directement depuis le. `/var/log/folder`

Exemple de message de journal au format natif

```
1 Jun 22 19:14:37 <local0.info> 10.217.31.98 06/22/2015:19:14:37 GMT ns
     0-PPE-1 :
2 default APPFW APPFW_cross-site scripting 60 0 :  10.217.253.62 616-PPE1
     y/3upt2K8ySWWId3Kavbxyni7Rw0000
3 pr_ffc http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
4 12345&drinking_pref=on&text_area=%3Cscript%3E%0D%0A&loginButton=
     ClickToLogin&as_sfid=
5 AAAAAAWEXcNQLlSokNmqaYF6dvfqlChNzSMsdyO9JXOJomm2v
6 BwAMOqZIChv21EcgBc3rexIUcfm0vckKlsgoOeC_BArx1Ic4NLxxkWMtrJe4H7SOfkiv9NL7AG4juPIan

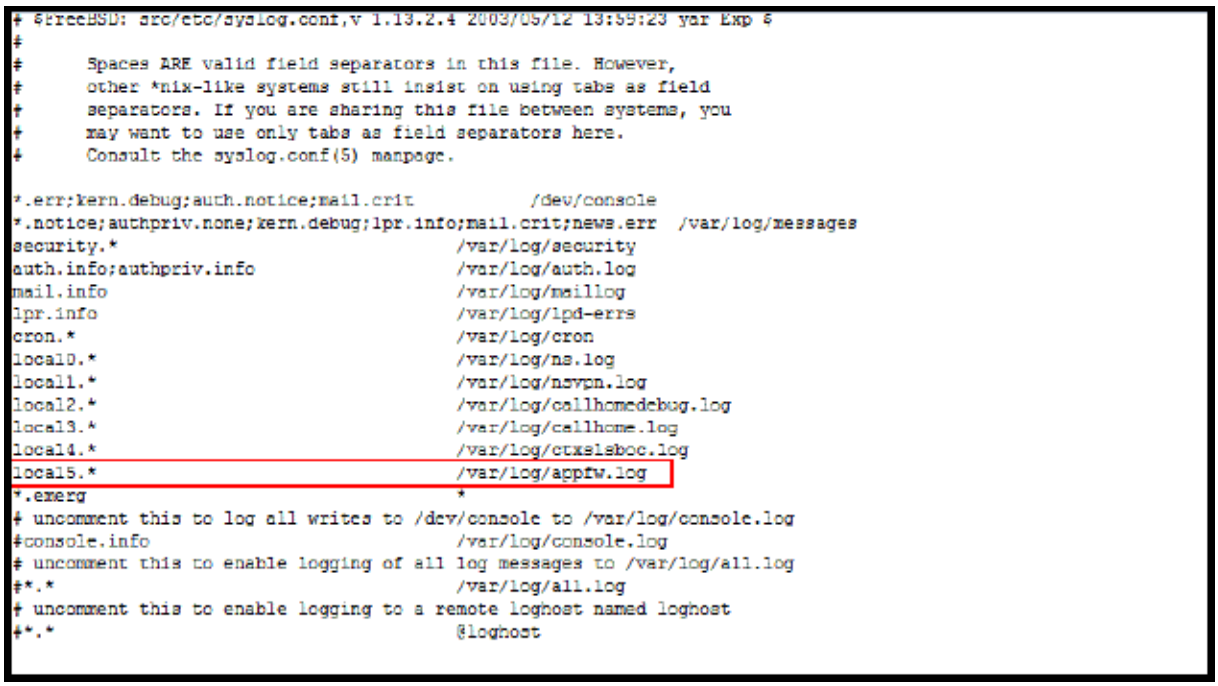
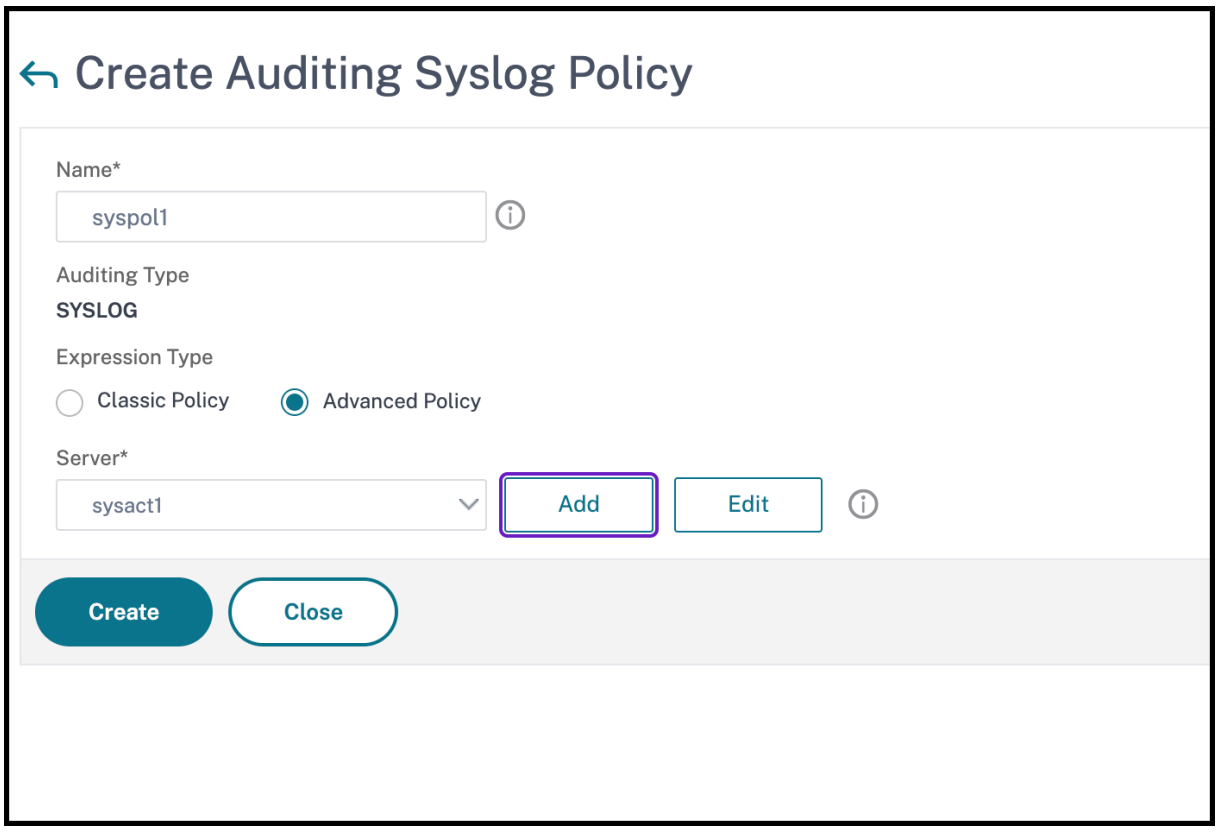
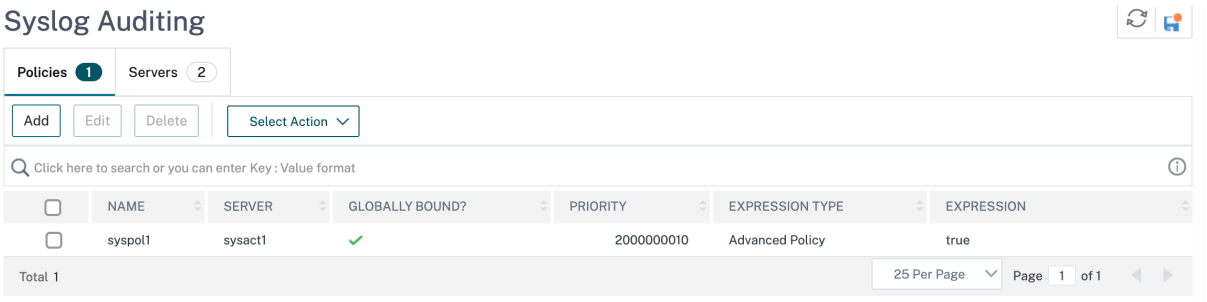
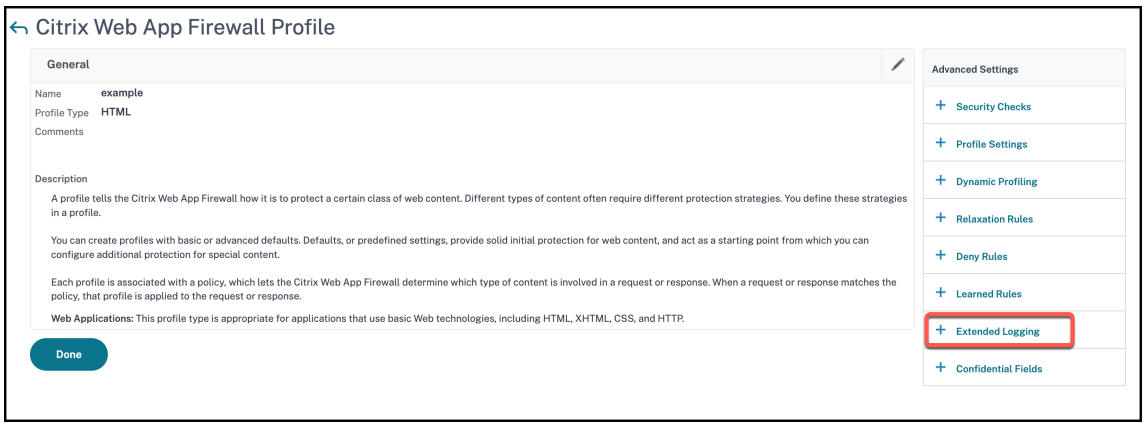
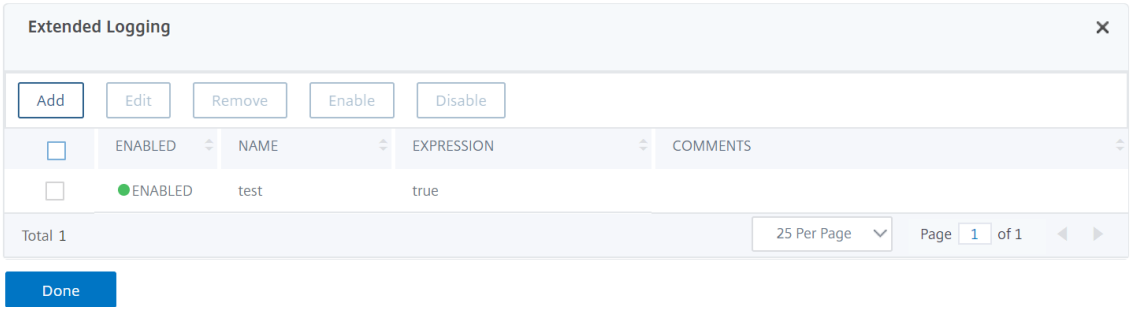
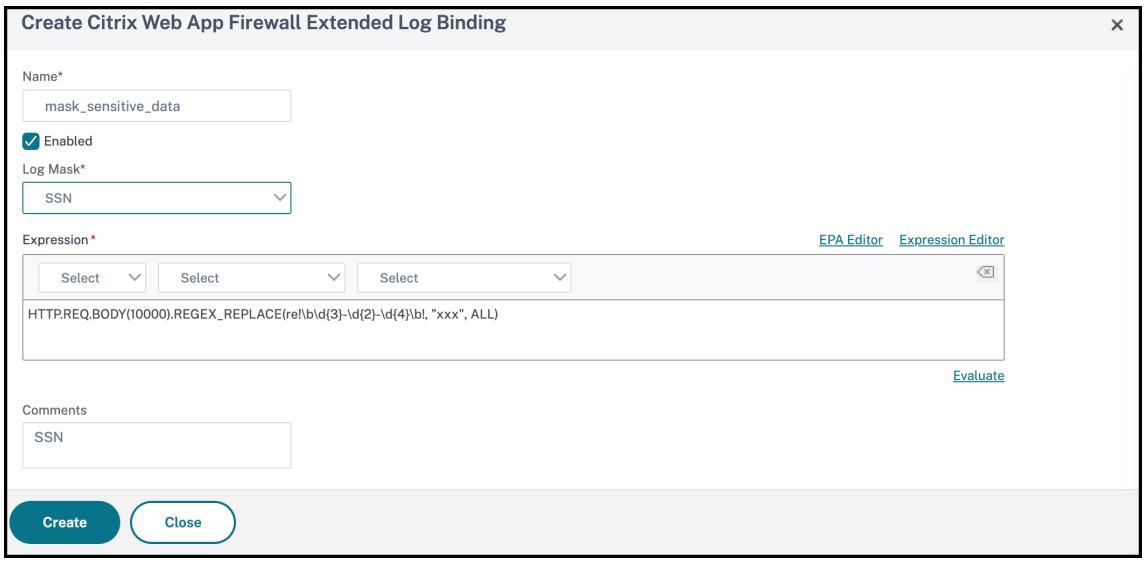
7 %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c Cross-site script
     check failed for
8 field text_area="Bad tag: script" <blocked>
9 <!--NeedCopy-->
```

Journaux du format d'événement commun (CEF)

Le Web App Firewall prend également en charge les journaux CEF. CEF est une norme de gestion des journaux ouverts qui améliore l'interopérabilité des informations liées à la sécurité provenant de différents périphériques et applications de sécurité et de réseau. Le CEF permet aux clients d'utiliser un format de journal des événements commun afin que les données puissent être facilement collectées et agrégées pour analyse par un système de gestion d'entreprise. Le message de journal est divisé en différents champs afin que vous puissiez facilement analyser le message et écrire des scripts pour identifier les informations importantes.

Analyse du message de journal CEF

Outre la date, l'horodatage, l'adresse IP du client, le format du journal, l'appliance, la société, la version de build, le module et les informations de vérification de sécurité, les messages de journal CEF de Web App Firewall incluent les informations suivantes :

- src — adresse IP source
- spt — numéro de port source
- request — URL de la demande
- act — action (par exemple bloqué, transformé)
- msg — message (message concernant la violation du contrôle de sécurité observée)
- Offset : représente les octets depuis le début du fichier.
- cn1 — ID d'événement
- cn2 — ID de transaction HTTP
- cs1 — nom du profil
- cs2 — ID PPE (par exemple PPE1)
- cs3 - ID de session
- cs4 — Gravité (par exemple INFO, ALERT)
- CS5 — année de l'événement
- cs6 - Catégorie de violation de signature
- method — Méthode (par exemple GET/POST)

Par exemple, considérez le message de journal au format CEF suivant, qui a été généré lorsqu'une violation d'URL de démarrage a été déclenchée :

```
1 Jun 12 23:37:17 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
     .0
2 |APPFW|APPFW_STARTURL|6|src=10.217.253.62 spt=47606 method=GET
3 request=http://aaron.stratum8.net/FFC/login.html msg=Disallow Illegal
     URL. cn1=1340
4 cn2=653 cs1=pr_ffc cs2=PPE1 cs3=EsdGd3VD0OaaURLcZnj05Y6DOmE0002 cs4=
     ALERT cs5=2015
5 act=blocked
6 <!--NeedCopy-->
```

Le message ci-dessus peut être divisé en différents composants. Reportez-vous au tableau des composants du journal CEP .

Exemple de violation de vérification de demande au format journal CEF : la demande n'est pas bloquée

```
1 Jun 13 00:21:28 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
     .0|APPFW|
2 APPFW_FIELDCONSISTENCY|6|src=10.217.253.62 spt=761 method=GET request=
3 http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
```



```
123456789234&drinking_pref=on&text_area=&loginButton=ClickToLogin&
    as_sfid
=
    AAAAAAWIahZuYoIFbjBhYMP05mJLTwEfIY0a7AKGMg3jIBaKmwtK4t7M7lNxOgj7Gmd3SZc8KUj6CF

7W5kIWDRHN8PtK1Zc-txHkHNx1WknuG9DzTuM7t1THhluevXu9I4kp8%3D&as_fid=
    feeec8758b4174
0eedeeb6b35b85dfd3d5def30c msg=Field consistency check failed for field
     passwd cn1=1401
cn2=707 cs1=pr_ffc cs2=PPE1 cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=
    ALERT cs5=2015 act=
not blocked
<!--NeedCopy-->
```

Exemple d'une violation de vérification de réponse au format CEF : la réponse est transformée

```
Jun 13 00:25:31 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_SAFECOMMERCE|6|src=10.217.253.62 spt=34041 method=GET request=
http://aaron.stratum8.net/FFC/CreditCardMind.html msg=Maximum number of
     potential credit
card numbers seen cn1=1470 cn2=708 cs1=pr_ffc cs2=PPE1
cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=ALERT cs5=2015 act=transformed
<!--NeedCopy-->
```

Exemple de violation de signature côté requête au format CEF : la demande est bloquée

```
Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method=GET request=
http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=Signature
    violation rule ID 807:
web-cgi /wwwboard/passwd.txt access  cn1=140 cn2=841 cs1=pr_ffc cs2=
    PPE0
cs3=OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=
    blocked
<!--NeedCopy-->
```

Exemple de violation du contrôle des réponses au format CEF pour un Offset :

```
Jan 24 10:00:00 <local0.warn> 10.175.4.47 CEF:0|Citrix|NetScaler|NS13
    .0|APPFW|APPFW_XML_ERR_NOT_WELLFORMED|4|src=5.31.100.129 spt=20644
    method=GET request=https://wifiuae.duwifi.ae/publishApplications/en
    /5dafe3e74fa8015599009bc1/images/fallback_photo.svg msg=XML Format
    check failed: Message is not a well-formed XML.Error string is '
```



```
      unclosed token'. Offset:-517597 cn1=547290214 cn2=974226675 cs1=
      WIFI_UAE_AppFw cs2=PPE0 cs4=ERROR cs5=2023 act=blocked
<!--NeedCopy-->
```

Dans cet exemple, la violation XML_ERR_NOT_WELLFORMED s'est produite en raison de `unclosed token`. Cette violation se trouve à l'emplacement 517597 depuis le début du fichier.

Consigner la géolocalisation dans les messages de violation du Web App Firewall

Les détails du journal identifient l'emplacement d'où proviennent les demandes et vous aident à configurer le Web App Firewall pour un niveau de sécurité optimal. Pour contourner les implémentations de sécurité telles que la limitation de débit, qui reposent sur les adresses IP des clients, les logiciels malveillants ou les ordinateurs malveillants peuvent continuer à modifier l'adresse IP source dans les demandes. L'identification de la région spécifique d'où proviennent les demandes peut aider à déterminer si les demandes proviennent d'un utilisateur valide ou d'un appareil tentant de lancer des cyberattaques. Par exemple, si un nombre excessif de demandes sont reçues d'une zone spécifique, il est facile de déterminer si elles sont envoyées par des utilisateurs ou par une machine non fiable. L'analyse de géolocalisation du trafic reçu peut être utile pour dévier des attaques telles que les attaques par déni de service (DoS).

Le Web App Firewall vous permet d'utiliser facilement la base de données NetScaler intégrée pour identifier les emplacements correspondant aux adresses IP d'où proviennent les demandes malveillantes. Vous pouvez ensuite appliquer un niveau de sécurité plus élevé pour les demandes provenant de ces emplacements. Les expressions de syntaxe par défaut (PI) de NetScaler vous permettent de configurer des politiques basées sur la localisation qui peuvent être utilisées avec la base de données de localisation intégrée pour personnaliser la protection par pare-feu, renforçant ainsi votre défense contre les attaques coordonnées lancées par des clients malhonnêtes dans une région spécifique.

Vous pouvez utiliser la base de données intégrée de NetScaler ou n'importe quelle autre base de données. Si la base de données ne contient aucune information d'emplacement pour l'adresse IP du client en particulier, le journal CEF affiche la géolocalisation en tant que géolocalisation inconnue.

> **Remarque :**
>
> La journalisation de la géolocalisation utilise le format d'événement commun (CEF). Par défaut, `CEF logging` et `GeoLocationLogging` sont désactivés. Vous devez explicitement activer les deux paramètres.

Exemple de message de journal CEF affichant des informations de géolocalisation

```
June 8 00:21:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_STARTURL|6|src=10.217.253.62 geolocation=NorthAmerica.US.Arizona.
    Tucson.\*.\*
```



```
spt=18655 method=GET request=http://aaron.stratum8.net/FFC/login.html
msg=Disallow Illegal URL. cn1=77 cn2=1547 cs1=test_pr_adv cs2=PPE1
cs3=KDynjg1pbFtfhC/nt0rBU1o/Tyg0001 cs4=ALERT cs5=2015 act=not blocked
<!--NeedCopy-->
```

Exemple de message de journal indiquant geolocation= Unknown

```
June 9 23:50:53 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|
APPFW|APPFW_STARTURL|6|src=10.217.30.251 geolocation=Unknown spt=5086
method=GET request=http://aaron.stratum8.net/FFC/login.html msg=
    Disallow Illegal URL.
cn1=74 cn2=1576 cs1=test_pr_adv cs2=PPE2 cs3=
    PyR0eOEM4gf6GJiTyauiHByL88E0002
cs4=ALERT cs5=2015 act=not blocked
<!--NeedCopy-->
```

Configurer l'action du journal et d'autres paramètres de journalisation à l'aide de

Pour configurer l'action de journalisation pour une vérification de sécurité d'un profil à l'aide de la ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `set appfw profile <name> SecurityCheckAction ([log] | [none])`
- `unset appfw profile <name> SecurityCheckAction`

Exemples

```
set appfw profile pr_ffc StartURLAction log
```

```
unset appfw profile pr_ffc StartURLAction
```

Pour configurer la journalisation CEF à l'aide de la ligne de commande

La journalisation CEF est désactivée par défaut. À l'invite de commandes, tapez l'une des commandes suivantes pour modifier ou afficher le paramètre actuel :

- `set appfw settings CEFLogging on`
- `unset appfw settings CEFLogging`
- `sh appfw settings | grep CEFLogging`

Pour configurer la consignation des numéros de carte de crédit à l'aide de la ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `set appfw profile <name> -doSecureCreditCardLogging ([ON] | [OFF])`
- `unset appfw profile <name> -doSecureCreditCardLogging`

Pour configurer la journalisation de la géolocalisation à l'aide de la ligne de commande

1. Utilisez la commande set pour activer GeolocationLogging. Vous pouvez activer la journalisation CEF en même temps. Utilisez la commande unset pour désactiver la journalisation de géolocalisation. La commande show affiche les paramètres actuels de tous les paramètres de Web App Firewall, sauf si vous incluez la commande grep pour afficher le paramètre d'un paramètre spécifique.

   - `set appfw settings GeoLocationLogging ON [CEFLogging ON]`
   - `unset appfw settings GeoLocationLogging`
   - `sh appfw settings | grep GeoLocationLogging`

2. Spécifiez la base de données

   ```
   add locationfile /var/netscaler/inbuilt_db/Citrix_netscaler_InBuilt_GeoIP_DB
   .csv
   ```

   ou

   ```
   add locationfile <path to database file>
   ```

Personnaliser les journaux du Web App Firewall

Les expressions de format par défaut (PI) vous permettent de personnaliser les informations incluses dans les journaux. Vous avez la possibilité d'inclure les données spécifiques que vous souhaitez capturer dans les messages de journal générés par le Web App Firewall. Par exemple, si vous utilisez l'authentification AAA-TM en même temps que les vérifications de sécurité du Web App Firewall et que vous souhaitez connaître l'URL consultée qui a déclenché la violation du contrôle de sécurité, le nom de l'utilisateur qui a demandé l'URL, l'adresse IP source et le port source à partir duquel l'utilisateur a envoyé la demande, vous peut utiliser les commandes suivantes pour spécifier des messages de journal personnalisés qui incluent toutes les données :

```
1 > sh version
2 NetScaler NS12.1: Build 50.0013.nc, Date: Aug 28 2018, 10:51:08   (64-
     bit)
3  Done
4 <!--NeedCopy-->
```

```
1 > add audit messageaction custom1 ALERT 'HTTP.REQ.URL + " " + HTTP.REQ.
     USER.NAME + " " + CLIENT.IP.SRC + ":" + CLIENT.TCP.SRCPORT'
2 Warning: HTTP.REQ.USER has been deprecated. Use AAA.USER instead.
3  Done
4 <!--NeedCopy-->
```

```
1 > add appfw profile test_profile
```



```
 Done
<!--NeedCopy-->
```

```
> add appfw policy appfw_pol true test_profile -logAction custom1
 Done
<!--NeedCopy-->
```

Configurer la stratégie Syslog pour séparer les journaux du Web App Firewall

Le pare-feu Web App vous offre la possibilité d'isoler et de rediriger les messages du journal de sécurité du Web App Firewall vers un autre fichier journal. Cela peut être souhaitable si le Web App Firewall génère de nombreux journaux, ce qui rend difficile l'affichage des autres messages du journal NetScaler. Vous pouvez également utiliser cette option lorsque vous souhaitez uniquement afficher les messages du journal du Web App Firewall et que vous ne souhaitez pas voir les autres messages de journal.

Pour rediriger les journaux du Web App Firewall vers un autre fichier journal, configurez une action Syslog pour envoyer les journaux du Web App Firewall à une autre fonction de journalisation. Vous pouvez utiliser cette action lors de la configuration de la stratégie Syslog et la lier globalement pour une utilisation par Web App Firewall.

> **Remarque :**
>
> Pour lier globalement les stratégies de Web App Firewall, vous pouvez configurer le paramètre de liaison global, « APPFW_GLOBAL » dans les commandes « audit de liaison SyslogGlobal » et « bind audit NSLogGlobal ». Les stratégies de journal d'audit liées globales peuvent évaluer les messages de journal dans le contexte de journalisation du Web App Firewall.

Exemple :

1. Passez au shell et utilisez un éditeur tel que vi pour éditer le fichier /etc/syslog.conf. Ajoutez une nouvelle entrée pour utiliser local2.* pour envoyer les journaux vers un fichier distinct, comme illustré dans l'exemple suivant :

   ```
   local2.\* /var/log/ns.log.appfw
   ```

2. Redémarrez le processus Syslog. Vous pouvez utiliser la commande grep pour identifier l'ID de processus Syslog (PID), comme illustré dans l'exemple suivant :

   ```
   root@ns\## **ps -A | grep syslog**
   ```

   ```
   1063 ?? Ss 0:03.00 /usr/sbin/syslogd -b 127.0.0.1 -n -v -v -8 -C
   ```

   ```
   root@ns## **kill -HUP** 1063
   ```


3. À partir de l'interface de ligne de commande, configurez la stratégie SYSLOG avancée ou classique avec une action et liez-la en tant que stratégie globale de Web App Firewall. Citrix vous recommande de configurer la stratégie SYSLOG avancée.

   Configuration avancée de la stratégie SYSLOG

   ```
   add audit syslogAction sysact1 1.1.1.1 -logLevel ALL -logFacility
   LOCAL2

   add audit syslogPolicy syspol1 true sysact1

   bind audit syslogGlobal -policyName syspol1 -priority 100 -globalBindType
    APPFW_GLOBAL
   ```

   Configuration de la stratégie classique SYSLOG

   ```
   add audit syslogAction sysact1 1.1.1.1 -logLevel ALL -logFacility
   LOCAL2

   add audit syslogPolicy syspol1 ns_true sysact1

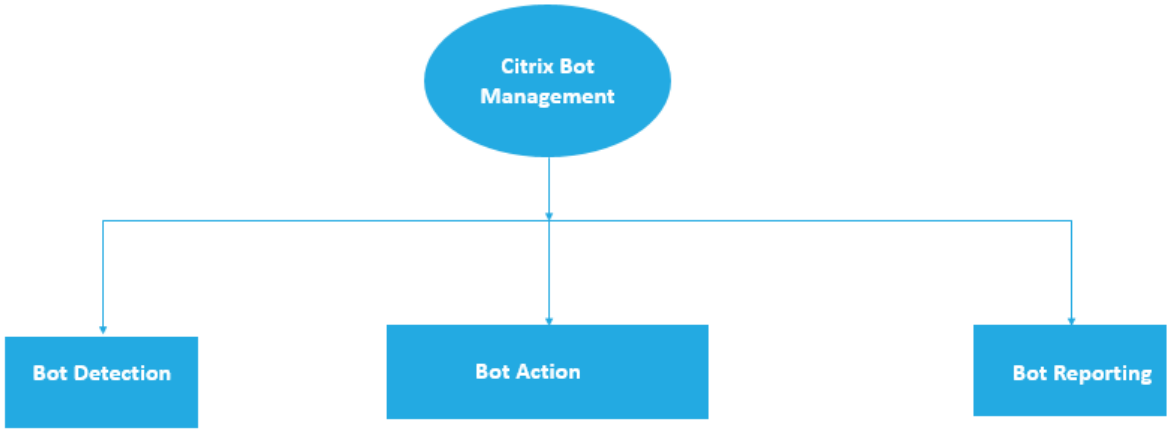
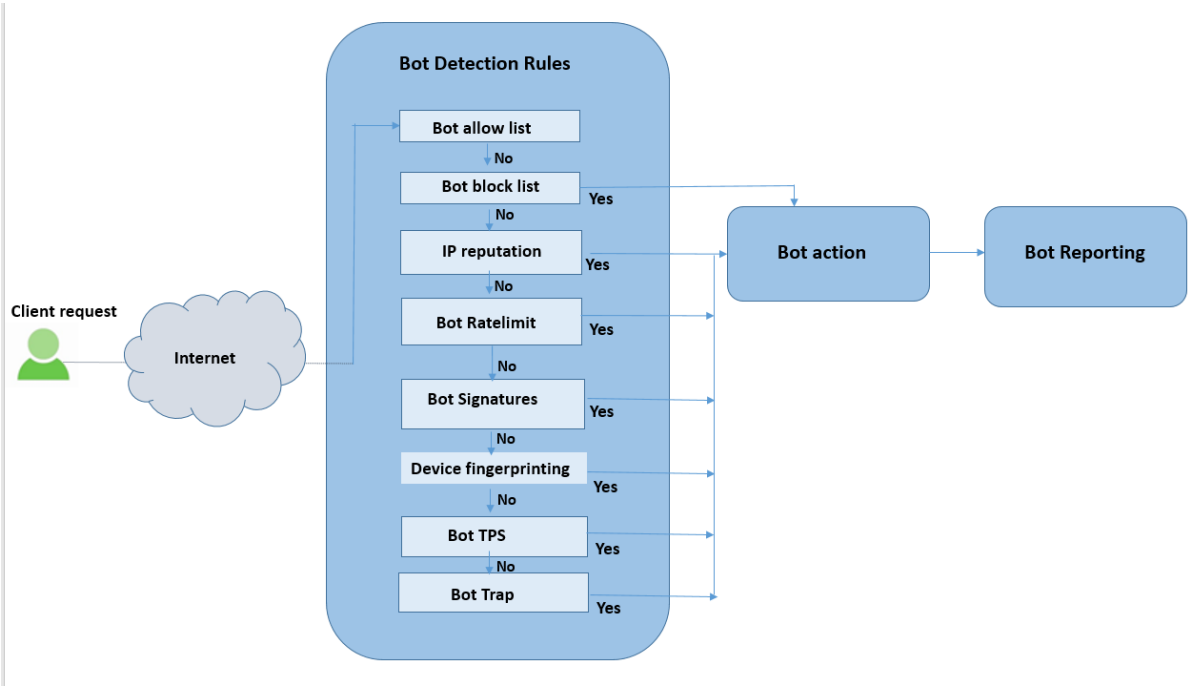
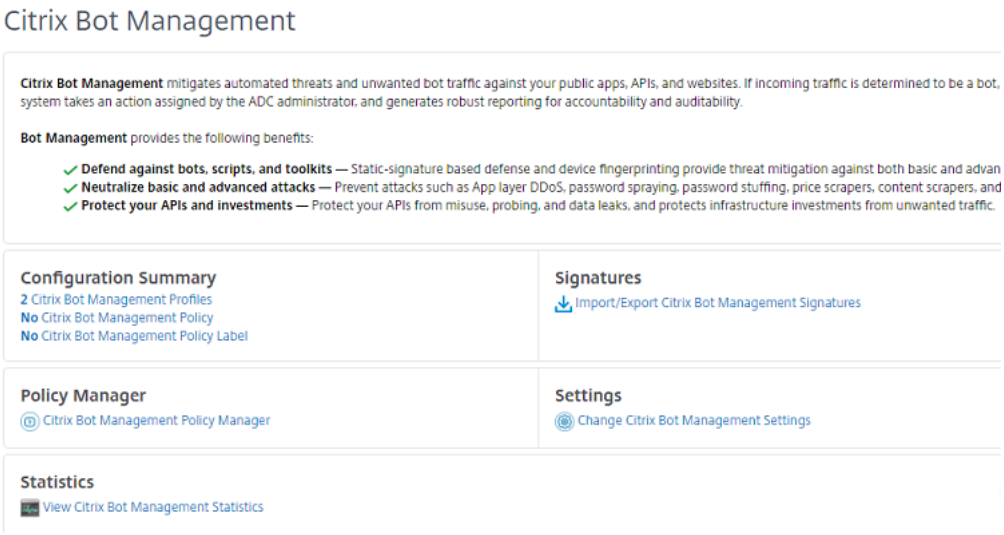
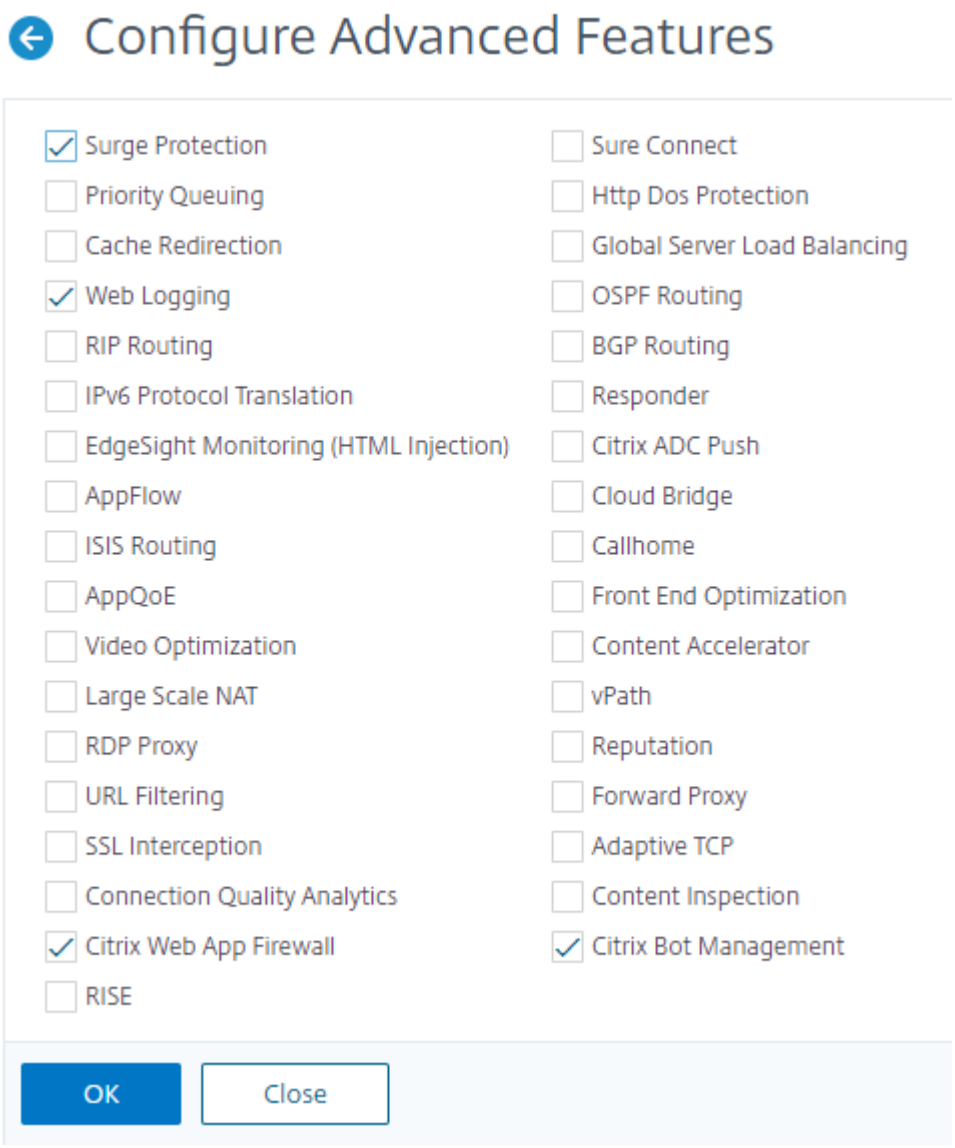
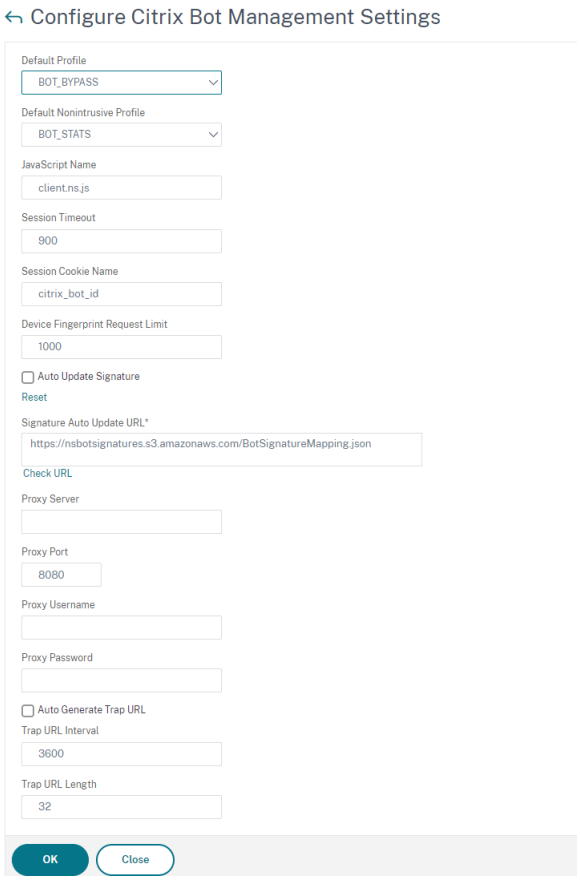
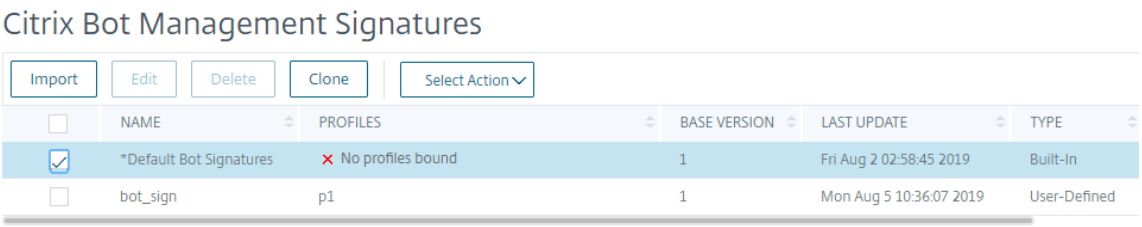
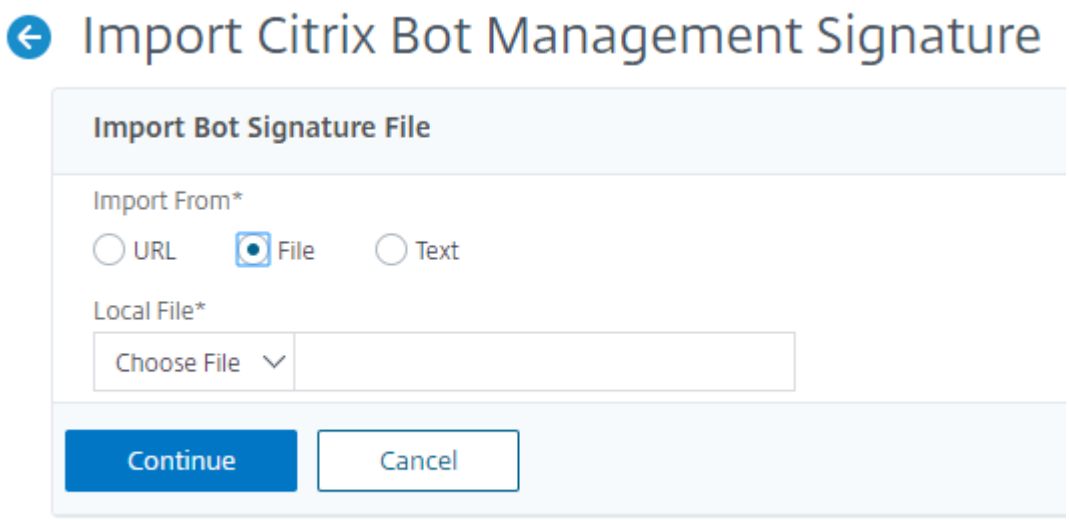
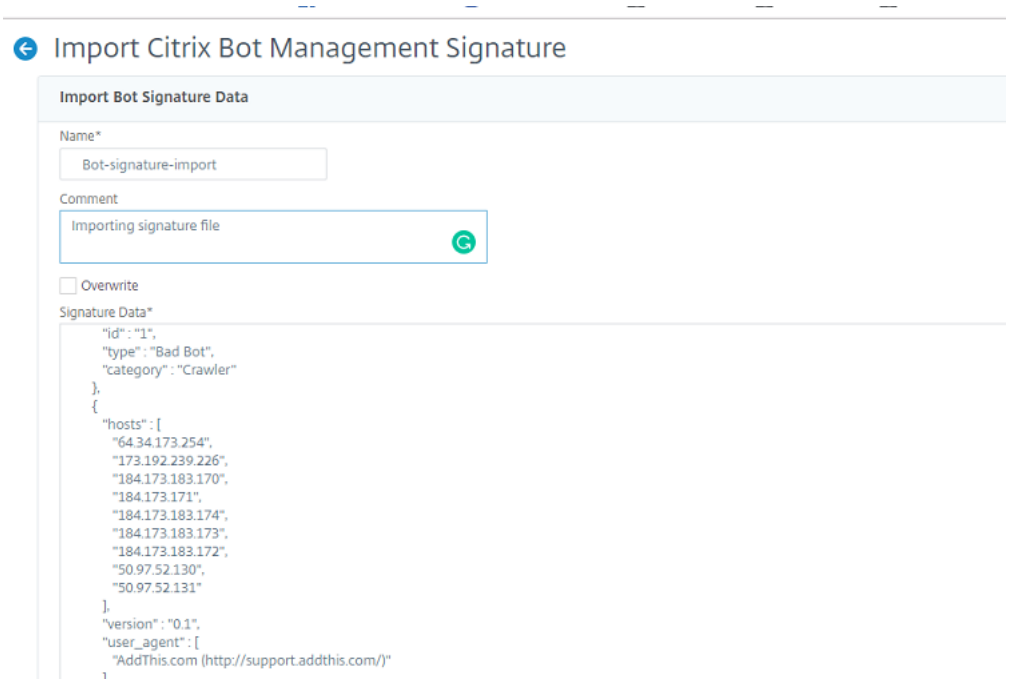
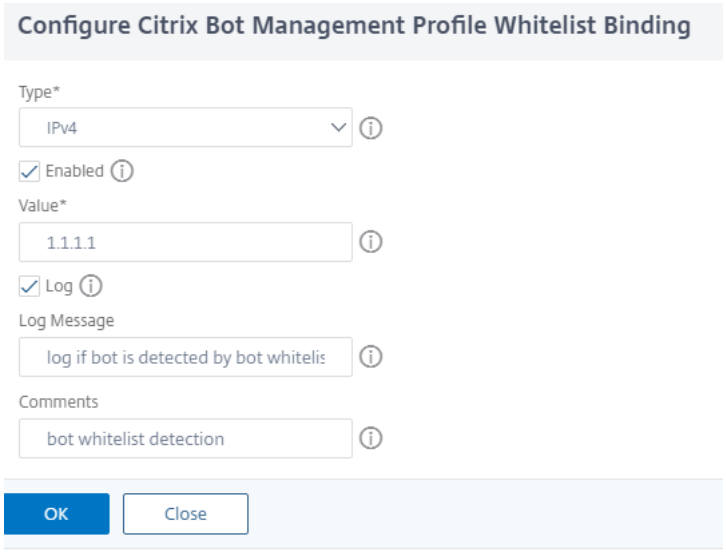
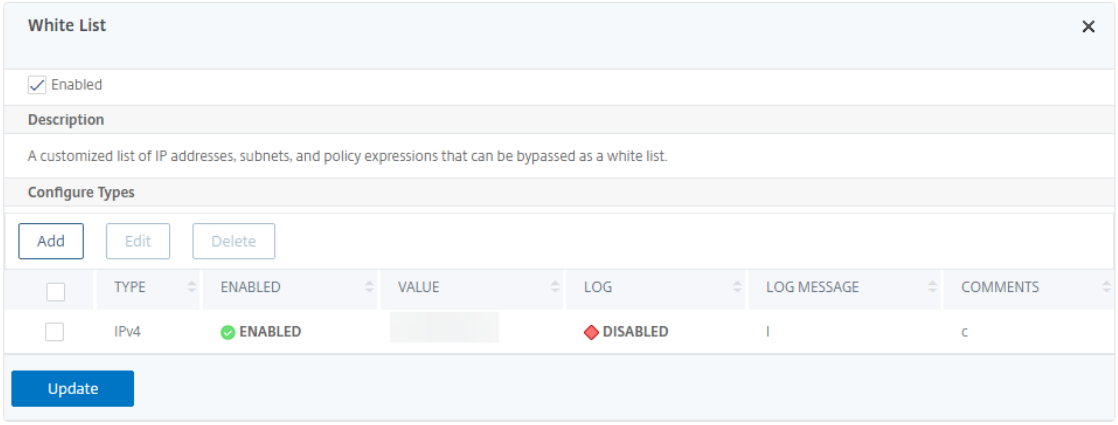
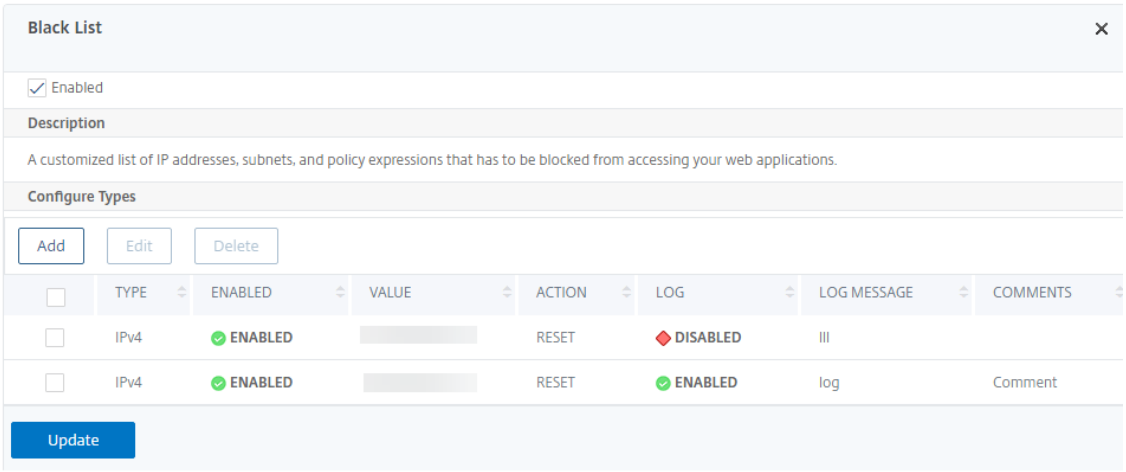
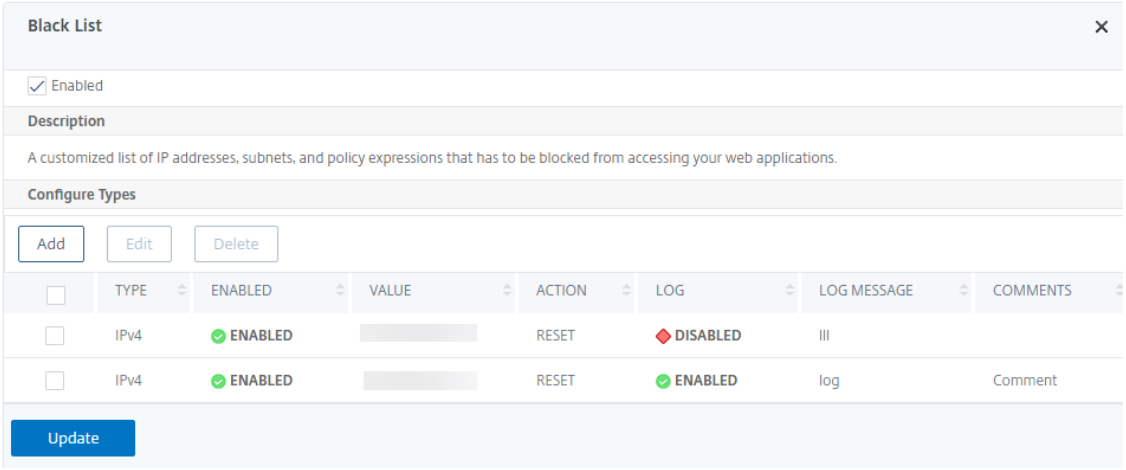
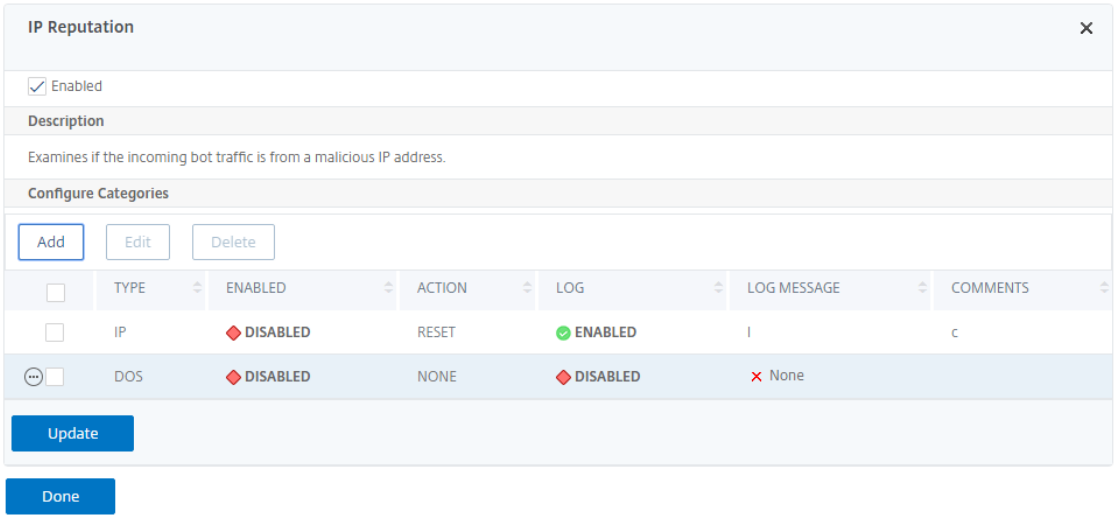
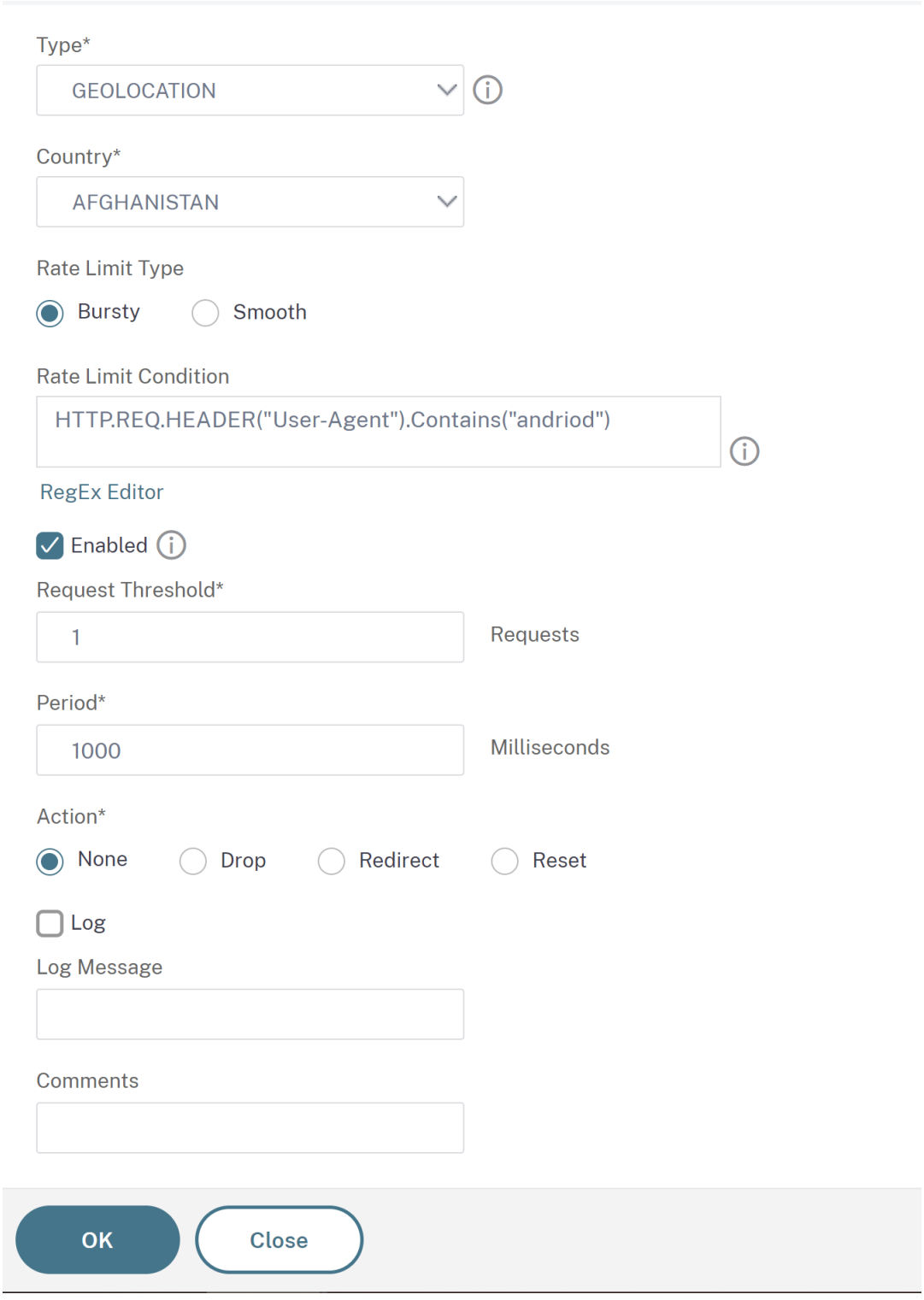
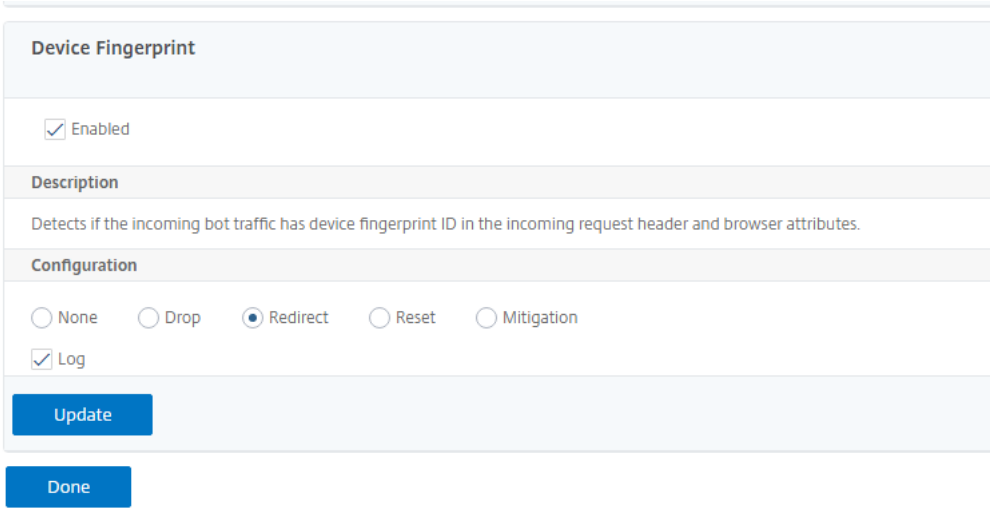
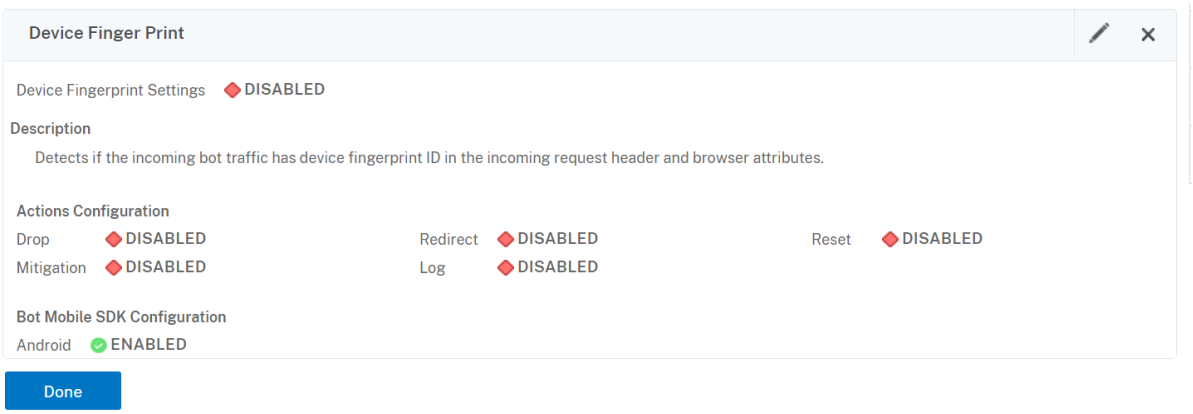
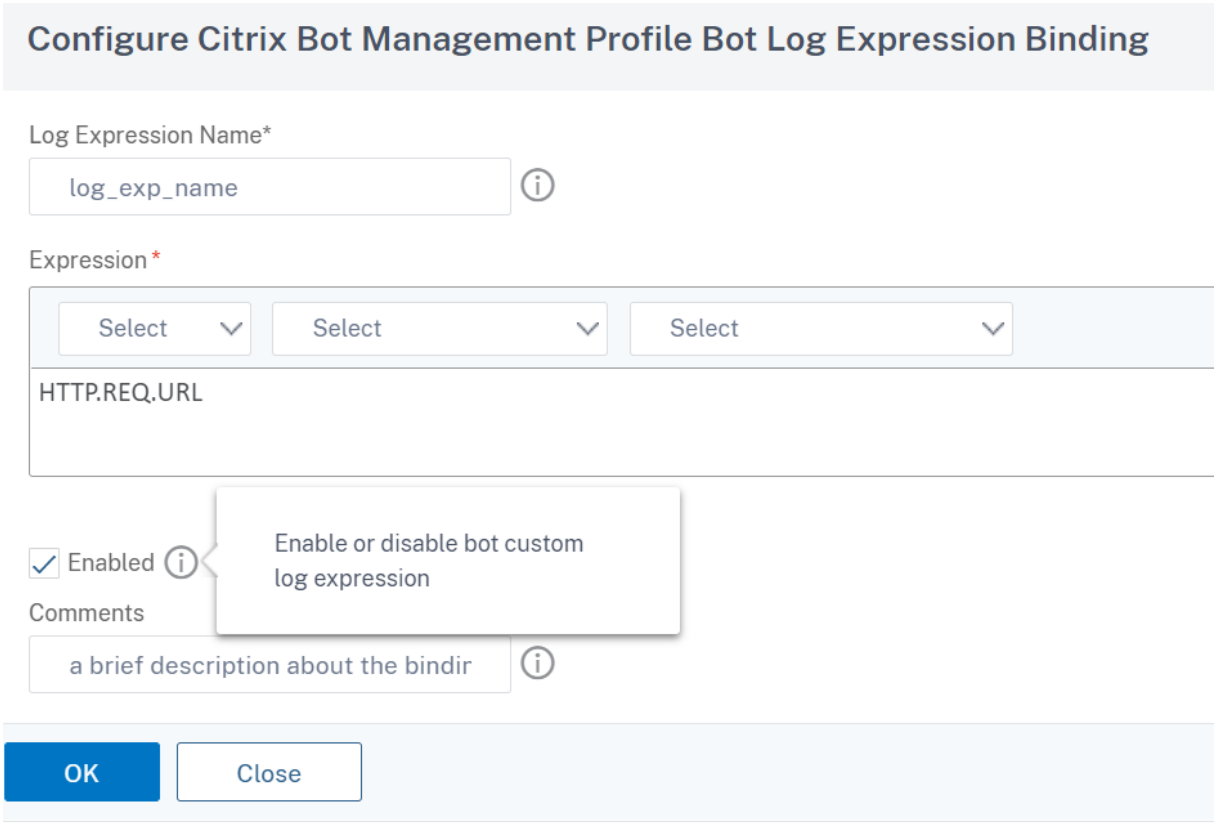
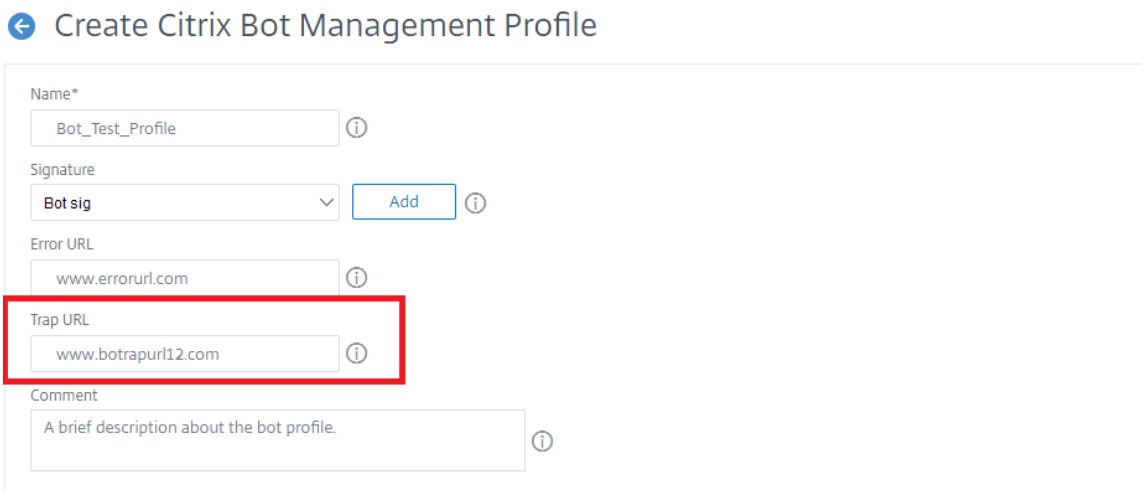
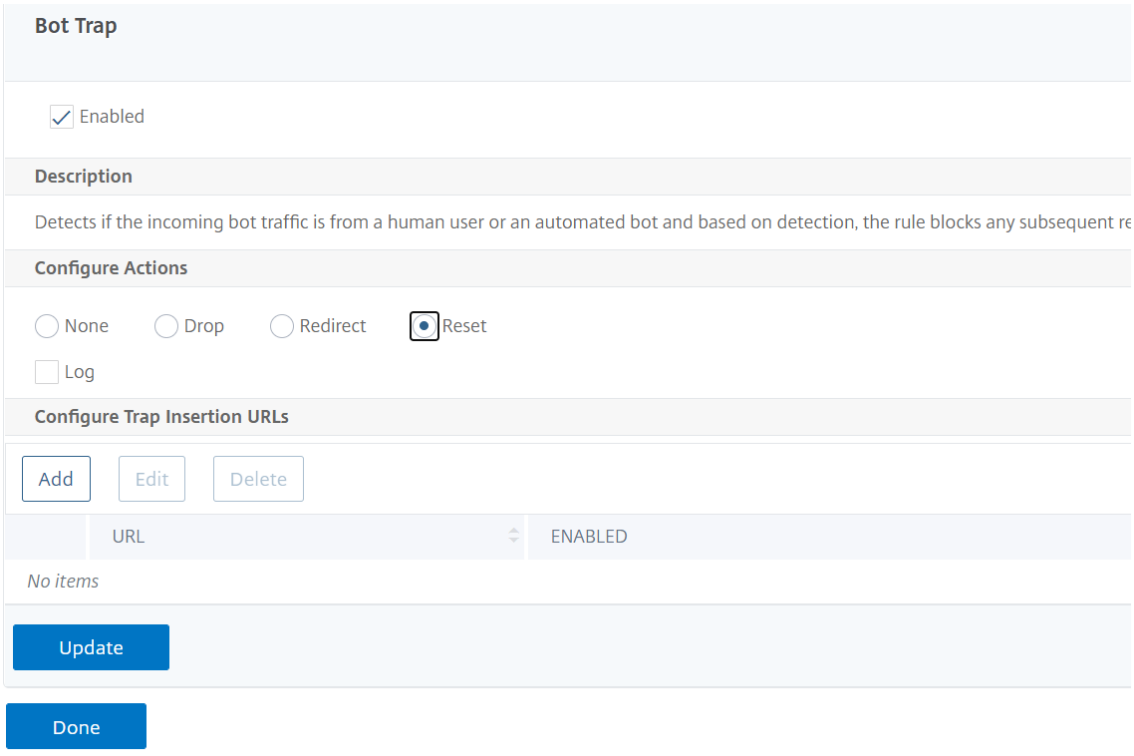
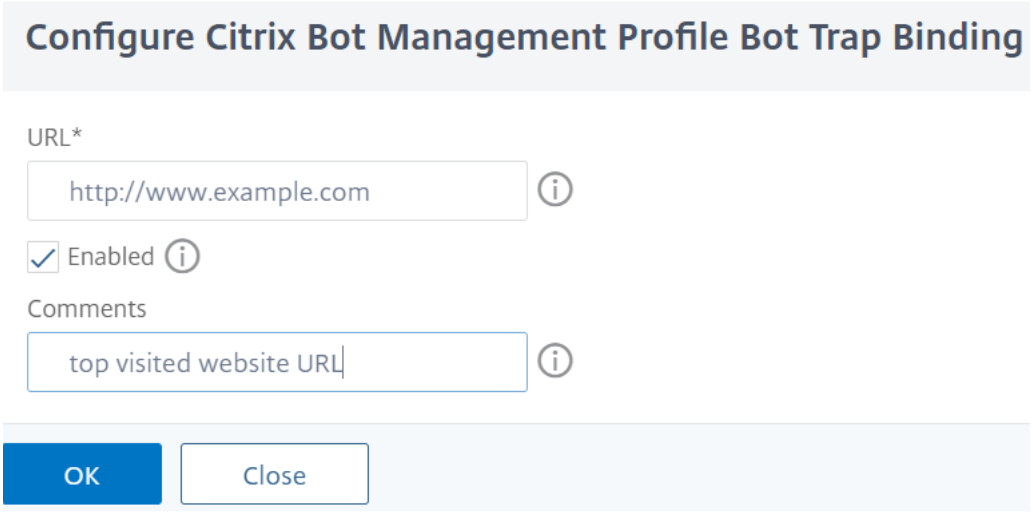
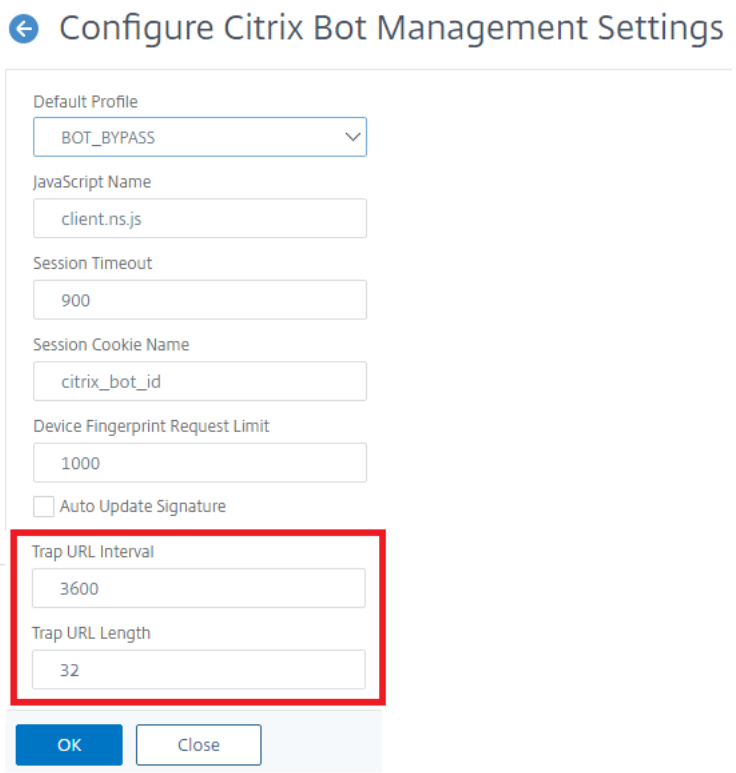
   bind appfw global syspol1 100
   ```

4. Toutes les violations du contrôle de sécurité du Web App Firewall seront désormais redirigées vers le fichier `/var/log/ns.log.appfw`. Vous pouvez suivre ce fichier pour afficher les violations du Web App Firewall qui sont déclenchées pendant le traitement du trafic en cours.

   ```
   root@ns## tail -f ns.log.appfw
   ```

Avertissement : Si vous avez configuré la stratégie Syslog pour rediriger les journaux vers une autre installation de journalisation, les messages de journal du Web App Firewall n'apparaissent plus dans le fichier `/var/log/ns.log`.

> **Remarque :**
>
> Si vous souhaitez envoyer des journaux vers un autre fichier journal sur l'appliance NetScaler locale, vous pouvez créer un serveur syslog sur cette appliance NetScaler locale. Ajoutez `syslogaction` à sa propre adresse IP et configurez l'ADC comme vous le feriez pour un serveur externe. L'ADC agit en tant que serveur pour stocker vos journaux. Deux actions ne peuvent pas être ajoutées avec la même adresse IP et le même port. Dans `syslogaction`, par défaut, la valeur IP est définie sur `127.0.0.1` et la valeur de port est définie sur `514`.

Envoyer les messages du pare-feu d'application à un serveur SYSLOG distinct

Pour envoyer les messages du pare-feu d'application à un serveur SYSLOG distinct, vous devez effectuer les étapes suivantes :

- Un utilitaire de transfert de fichiers sécurisé tel que WinSCP

- Un utilitaire permettant d'ouvrir une console SSH sur l'appliance, tel que PuTTY

Les étapes suivantes sont impliquées pour envoyer les messages du pare-feu d'application à un serveur SYSLOG distinct :

1. Connectez-vous à l'appliance NetScaler via WinSCP.
2. Mettez à jour le fichier /etc/syslog.conf et ajoutez la ligne suivante dans le fichier :
   `local5.* /var/log/appfw.log`



1. Exécutez la commande suivante à partir de l'interface de ligne de commande pour redémarrer le PID Syslog :
   `kill -HUP <PID>`
2. Exécutez la commande suivante à partir de l'interface de ligne de commande pour ajouter une action Syslog telle que sysact1 :
   `add audit syslogAction sysact1 127.0.0.1 -logLevel ALL -logFacility LOCAL5`
3. Exécutez la commande suivante pour ajouter la stratégie syspol1, qui utilise le serveur sysact1 :
   `add audit syslogPolicy syspol1 ns_true sysact1`
   Ou ajoutez une stratégie Syslog avancée :
   `add audit syslogPolicy syspol1 true sysact1`



1. Exécutez la commande suivante pour lier la stratégie de pare-feu d'applications et assurez-vous qu'elle est enregistrée dans le fichier ns.conf :
   `bind appfw global syspol1 100`
   Vous pouvez également exécuter la commande suivante pour lier la stratégie Syslog avancée :

```
bind audit syslogGlobal -policyName syspol1 -priority 100 -globalBindType
APPFW_GLOBAL
```



Toutes les violations du contrôle de sécurité du pare-feu d'application sont redirigées vers le `/var/log/appfw.log` et n'apparaîtront plus dans le `ns.log`. Vous pouvez maintenant exécuter la commande tail et afficher les dernières entrées dans le `/var/log/appfw.log`.

Afficher les journaux du Web App Firewall

Vous pouvez consulter les journaux à l'aide de la visionneuse Syslog ou en vous connectant à l'appliance NetScaler, en ouvrant un shell UNIX et en utilisant l'éditeur de texte UNIX de votre choix.

Pour accéder aux messages du journal à l'aide de la ligne de commande

Passez à l'interpréteur de commandes et suivez les ns.logs dans le dossier **/var/log/** pour accéder aux messages de journal relatifs aux violations de vérification de **sécurité du Web App Firewall** :

- `Shell`
- `tail -f /var/log/ns.log`

Vous pouvez utiliser l'éditeur vi, ou n'importe quel éditeur de texte Unix ou outil de recherche de texte, pour afficher et filtrer les journaux pour des entrées spécifiques. Par exemple, vous pouvez utiliser la commande `grep` pour accéder aux messages de journal relatifs aux violations de carte de crédit :

- `tail -f /var/log/ns.log | grep SAFECOMMERCE`

Pour accéder aux messages du journal à l'aide de l'interface graphique

L'interface graphique inclut un outil utile (Syslog Viewer) pour analyser les messages du journal. Vous disposez de plusieurs options pour accéder à la visionneuse Syslog :

- Pour afficher les messages de journal d'une vérification de sécurité spécifique d'un profil, accédez à **Web App Firewall** > **Profils**, sélectionnez le profil cible, puis cliquez sur Vérifications de sécurité. Mettez en surbrillance la ligne correspondant au contrôle de sécurité cible, puis cliquez sur Journaux. Lorsque vous accédez aux journaux directement à partir de la vérification de sécurité sélectionnée du profil, il filtre les messages de journal et affiche uniquement les journaux relatifs aux violations du contrôle de sécurité sélectionné. La visionneuse Syslog peut afficher les journaux du Web App Firewall au format natif et au format CEF. Cependant, pour que la visionneuse Syslog filtre les messages de journal spécifiques au profil cible, les journaux doivent être au format de journal CEF lorsqu'ils sont accessibles à partir du profil.
- ****Vous pouvez également accéder à la visionneuse Syslog en accédant à **NetScaler** > Système > Audit.** Dans la section Messages d'audit, cliquez sur le lien Messages Syslog pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris tous les journaux de violation de contrôle de sécurité du Web App Firewall pour tous les profils. Les messages de journal sont utiles pour le débogage lorsque plusieurs violations de contrôle de sécurité peuvent être déclenchées pendant le traitement de la demande.
- Accédez à **Web App Firewall** > **stratégies** > **Audit**. Dans la section Messages d'audit, cliquez sur le lien Messages Syslog pour afficher la visionneuse Syslog, qui affiche tous les messages de journal, y compris tous les journaux de violation de contrôle de sécurité pour tous les profils.

La visionneuse Syslog basée sur HTML fournit les options de filtre suivantes pour sélectionner uniquement les messages de journal qui vous intéressent :

- **Fichier**—Le fichier `/var/log/ns.log` actuel est sélectionné par défaut et les messages correspondants apparaissent dans la visionneuse Syslog. Liste des autres fichiers journaux du répertoire /var/log disponibles au format .gz compressé. Pour télécharger et décompresser un fichier journal archivé, sélectionnez le fichier journal dans l'option de liste déroulante. Les messages de journal relatifs au fichier sélectionné sont ensuite affichés dans la visionneuse Syslog. Pour actualiser l'affichage, cliquez sur l'icône Actualiser (un cercle de deux flèches).
- **Zone de liste des modules** : vous pouvez sélectionner le module NetScaler dont vous souhaitez consulter les journaux. Vous pouvez le définir sur APPFW pour les journaux de Web App Firewall.
- **Zone de liste Type d'événement** : cette zone contient un ensemble de cases à cocher permettant de sélectionner le type d'événement qui vous intéresse. Par exemple, pour afficher les messages de journal relatifs aux violations de signature, vous pouvez activer la case à cocher **APPFW_SIGNATURE_MATCH** . De même, vous pouvez cocher une case pour activer le contrôle de sécurité spécifique qui vous intéresse. Vous pouvez sélectionner plusieurs options.
- **Gravité** : vous pouvez sélectionner un niveau de gravité spécifique pour afficher uniquement les journaux correspondant à ce niveau de gravité. Laissez toutes les cases à cocher vides si vous souhaitez voir tous les journaux.

  Pour accéder aux messages du journal des violations de contrôle de sécurité du Web App Firewall pour un contrôle de sécurité spécifique, filtrez en sélectionnant **APPFW** dans les options de la liste déroulante pour Module. Le type d'événement affiche un ensemble complet d'options pour affiner votre sélection. Par exemple, si vous activez la case à cocher **APPFW_FIELDFORMAT** et que vous cliquez sur le bouton Appliquer, seuls les messages de journalisation relatifs aux violations des contrôles de sécurité des formats de champ apparaissent dans la visionneuse Syslog. De même, si vous activez les cases à cocher **APPFW_SQL** et **APPFW_STARTURL** et que vous cliquez sur le bouton **Appliquer**, seuls les messages de journal relatifs à ces deux violations de contrôle de sécurité apparaissent dans la visionneuse Syslog.

Si vous placez le curseur sur la ligne d'un message de journal spécifique, plusieurs options, telles que **Module**, **Type d'événement**, **ID d'événement**ou **Message**, s'affichent sous le message de journal. Vous pouvez sélectionner l'une de ces options pour mettre en surbrillance les informations correspondantes dans les journaux.

Résumé

- **Prise en charge du format de journal CEF** : l'option de format de journal CEF fournit une option pratique pour surveiller, analyser et analyser les messages de journal du Web App Firewall afin d'identifier les attaques, d'affiner les paramètres configurés afin de réduire les faux positifs et de recueillir des statistiques.
- **Option de personnalisation des messages de journal** : vous pouvez utiliser des expressions PI avancées pour personnaliser les messages de journal et inclure les données que vous souhaitez

voir dans les journaux.

- **Séparer les journaux spécifiques au Web App Firewall** : vous avez la possibilité de filtrer et de rediriger les journaux spécifiques au pare-feu d'application vers un fichier journal distinct.
- **Journalisation à distance** : vous pouvez rediriger les messages de journal vers un serveur Syslog distant.
- **Journalisation de la géolocalisation** : vous pouvez configurer le Web App Firewall pour inclure la géolocalisation de la zone à partir de laquelle la demande est reçue. Une base de données de géolocalisation intégrée est disponible, mais vous avez la possibilité d'utiliser une base de données de géolocalisation externe. L'appliance NetScaler prend en charge les bases de données de géolocalisation statiques IPv4 et IPv6.
- **Message de journal riche en informations** : voici quelques exemples du type d'informations pouvant être incluses dans les journaux, en fonction de la configuration :
  - Une stratégie Web App Firewall a été déclenchée.
  - Une violation du contrôle de sécurité a été déclenchée.
  - Une demande a été considérée comme mal formée.
  - Une demande ou une réponse a été bloquée ou non bloquée.
  - Les données de demande (telles que les caractères spéciaux de script SQL ou intersite) ou les données de réponse (telles que les numéros de carte de crédit ou les chaînes d'objets sûrs) ont été transformées.
  - Le nombre de cartes de crédit dans la réponse a dépassé la limite configurée.
  - Le numéro et le type de la carte de crédit.
  - Les chaînes de journaux configurées dans les règles de signature et l'ID de signature.
  - Informations de géolocalisation sur la source de la demande.
  - Saisie utilisateur masquée (sortie X) pour les champs confidentiels protégés.

Masquer les données sensibles à l'aide d'un modèle regex

La fonction de stratégie avancée `REGEX_REPLACE` (PI) d'une expression de journal (liée à un profil de pare-feu d'application Web (WAF)) vous permet de masquer les données sensibles dans les journaux WAF. Vous pouvez utiliser cette option pour masquer les données à l'aide d'un modèle d'expression régulière et fournir un modèle de caractère ou de chaîne pour masquer les données. Vous pouvez également configurer la fonction PI pour remplacer la première occurrence ou toutes les occurrences du modèle d'expression régulière.

Par défaut, l'interface graphique fournit le masque suivant :

- SSN
- Carte de crédit
- Mot de passe
- Nom d'utilisateur

Masquer les données sensibles dans les journaux du pare-feu d'application Web

Vous pouvez masquer les données sensibles dans les journaux WAF en configurant l'expression de stratégie avancée `REGEX_REPLACE` dans l'expression de journal liée à un profil WAF.
Pour masquer les données sensibles, vous devez effectuer les étapes suivantes :

1. Ajouter un profil de pare-feu d'application Web
2. Liaison d'une expression de journal au profil WAF

Ajouter un profil de pare-feu d'application Web

À l'invite de commande, tapez :

```
add appfw profile <name>
```

Exemple :

```
Add appfw profile testprofile1
```

Liaison d'une expression de journal avec le profil de pare-feu d'application Web

À l'invite de commande, tapez :

```
bind appfw profile <name> -logExpression <string> <expression> -comment <
string>
```

Exemple :

```
bind appfw profile testProfile -logExpression "MaskSSN""HTTP.REQ.BODY
(10000).REGEX_REPLACE(re!\b\d{ 3 } -\d{ 2 } -\d{ 4 } \b!, “xxx” , ALL)"-
comment "SSN Masked"
```

Masquer les données sensibles dans les journaux du Web Application Firewall à l'aide de l'interface graphique NetScaler

1. **Dans le volet de navigation, ouvrez**Sécurité**>**NetScaler Web App Firewall > Profils**.**
2. Sur la page **Profils**, cliquez sur **Modifier**.
3. Sur la page de **profil du Web App Firewall NetScaler**, accédez à la section **Paramètres avancés** et cliquez sur **Extended**Logging.



4. Dans la section **Enregistrement étendu**, cliquez sur **Ajouter**.



5. Sur la page **Create NetScaler Web App Firewall Extended Log Binding**, définissez les paramètres suivants :

   a) Nom. Nom de l'expression du journal.
   b) Activé. Sélectionnez cette option pour masquer les données sensibles.
   c) Masque de journal. Sélectionnez les données à masquer.
   d) Expression : Entrez l'expression de stratégie avancée qui vous permet de masquer les données sensibles dans les journaux WAF
   e) Commentaires. Brève description du masquage des données sensibles.

6. Cliquez sur **Créer** et **Fermer**.



Annexes

January 21, 2021

Le matériel supplémentaire suivant fournit des détails supplémentaires sur les tâches de Web App Firewall complexes ou périphériques.

Format de codage de caractères PCRE

May 5, 2023

Le **système d'exploitation NetScaler prend uniquement en charge la saisie directe** de caractères dans le jeu de caractères ASCII imprimable, à savoir les caractères comportant des codes hexadécimaux compris entre HEX 20 (ASCII 32) et HEX 7E (ASCII 127). Pour inclure un caractère dont le code se trouve en dehors de cette plage dans votre configuration Web App Firewall, vous devez entrer son code hexadécimal UTF-8 en tant qu'expression régulière PCRE.

De nombreux types de caractères nécessitent un codage à l'aide d'une expression régulière PCRE si vous les incluez dans la configuration de votre Web App Firewall sous forme d'URL, de nom de champ de formulaire ou d'expression d'objet sécurisé. Ils incluent :

- **Caractères ASCII supérieurs.** Caractères dont le codage va de HEX 7F (ASCII 128) à HEX FF (ASCII 255). Selon la table de caractères utilisée, ces codages peuvent faire référence à des codes de contrôle, des caractères ASCII accentués ou d'autres modifications, des caractères alphabétiques non latins et des symboles non inclus dans le jeu ASCII de base. Ces caractères peuvent

apparaître dans les URL, les noms de champs de formulaire et les expressions d'objets sécurisés.

- **Caractères sur deux octets.** Caractères dont l'encodage utilise deux mots de 8 octets. Les caractères codés sur deux octets sont principalement utilisés pour représenter du texte chinois, japonais et coréen au format électronique. Ces caractères peuvent apparaître dans les URL, les noms de champs de formulaire et les expressions d'objets sécurisés.

  Caractères de contrôle ASCII. Caractères non imprimables utilisés pour envoyer des commandes à une imprimante. Tous les caractères ASCII dont le code hexadécimal est inférieur à HEX 20 (ASCII 32) entrent dans cette catégorie. Toutefois, ces caractères ne doivent jamais apparaître dans une URL ou un nom de champ de formulaire et apparaîtront rarement, voire jamais, dans une expression d'objet sécurisé.

L'appliance NetScaler ne prend pas en charge l'intégralité du jeu de caractères UTF-8, mais uniquement les caractères contenus dans les huit jeux de caractères suivants :

- **Anglais américain (ISO-8859-1).** Bien que l'étiquette indique « English US », le Web App Firewall prend en charge tous les caractères du jeu de caractères ISO-8859-1, également appelé jeu de caractères Latin-1. Ce jeu de caractères représente entièrement la plupart des langues modernes d'Europe occidentale et représente tous les caractères rares sauf quelques uns dans le reste.
- **Chinois traditionnel (Big5).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères BIG5, qui inclut tous les caractères chinois traditionnels (idéogrammes) couramment utilisés en chinois moderne tels qu'ils sont parlés et écrits à Hong Kong, à Macao, à Taïwan et par de nombreuses personnes d'origine ethnique chinoise qui vivent en dehors de la Chine continentale.
- **Chinois simplifié (GB2312).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères GB2312, qui inclut tous les caractères chinois simplifiés (idéogrammes) couramment utilisés en chinois moderne tels qu'ils sont parlés et écrits en Chine continentale.
- **japonais (SJIS).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères Shift-JIS (SJIS), qui inclut la plupart des caractères (idéogrammes) couramment utilisés en japonais moderne.
- **japonais (EUC-JP).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères EUC-JP, qui inclut tous les caractères (idéogrammes) couramment utilisés en japonais moderne.
- **Coréen (EUC-KR).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères EUC-KR, qui inclut tous les caractères (idéogrammes) couramment utilisés en coréen moderne.
- **Turc (ISO-8859-9).** Le Web App Firewall prend en charge tous les caractères du jeu de caractères ISO-8859-9, qui inclut toutes les lettres utilisées en turc moderne.

- **Unicode (UTF-8).** Le Web App Firewall prend en charge certains caractères supplémentaires du jeu de caractères UTF-8, y compris ceux utilisés en russe moderne.

Lors de la configuration du Web App Firewall, vous entrez tous les caractères non ASCII en tant qu'expressions régulières au format PCRE à l'aide du code hexadécimal attribué à ce caractère dans la spécification UTF-8. Les symboles et les caractères du jeu de caractères ASCII normal, auxquels sont affectés des codes simples à deux chiffres dans ce jeu de caractères, reçoivent les mêmes codes dans le jeu de caractères UTF-8. Par exemple, le point d'exclamation (!) , auquel est affecté le code hexadécimal 21 dans le jeu de caractères ASCII, est également hexadécimal 21 dans le jeu de caractères UTF-8. Les symboles et les caractères d'un autre jeu de caractères pris en charge sont associés à un jeu de codes hexadécimaux appariés dans le jeu de caractères UTF-8. Par exemple, la lettre a avec un accent aigu (á) se voit attribuer le code UTF-8 C3 A1.

La syntaxe que vous utilisez pour représenter ces codes UTF-8 dans la configuration du Web App Firewall est « \ xNN » pour les caractères ASCII ; « \ xNN \ xNN » pour les caractères non ASCII utilisés en anglais, en russe et en turc ; et « \ xNN \ xNN \ xNN » pour les caractères utilisés en chinois, japonais et coréen. Par exemple, si vous souhaitez représenter un ! dans une expression régulière du Web App Firewall sous forme de caractère UTF-8, vous devez taper \ x21. Si vous souhaitez inclure un á, vous devez taper \xC3\xA1.

> **Remarque :**
>
> Normalement, vous n'avez pas besoin de représenter les caractères ASCII au format UTF-8, mais lorsque ces caractères peuvent confondre un navigateur Web ou un système d'exploitation sous-jacent, vous pouvez utiliser la représentation UTF-8 du personnage pour éviter cette confusion. Par exemple, si une URL contient un espace, vous pouvez encoder cet espace sous la forme \ x20 pour éviter de confondre certains navigateurs et certains logiciels de serveur Web.

Vous trouverez ci-dessous des exemples d'URL, de noms de champs de formulaire et d'expressions d'objets sécurisés contenant des caractères non ASCII qui doivent être entrés en tant qu'expressions régulières au format PCRE pour être inclus dans la configuration du Web App Firewall. Chaque exemple montre d'abord l'URL, le nom de champ ou la chaîne d'expression, suivi d'une expression régulière au format PCRE correspondant.

- URL contenant des caractères ASCII étendus.

  URL réelle : URL `http://www.josénuñez.com`
  codée : `^http://www\[.\]jos\\xC3\\xA9nu\\xC3\\xB1ez\[.\]com$`

- Une autre URL contenant des caractères ASCII étendus.

  URL réelle : URL `http://www.example.de/trömso.html`
  codée : `^http://www[.]example[.\]de/tr\xC3\xB6mso[.]html$`

  Un nom de champ de formulaire contenant des caractères ASCII étendus.

Nom réel : nome_do_usuário Nom
encodé : ^nome_do_usu \ xC3 \ xA1RIo$

- Expression d'objet sécurisée contenant des caractères ASCII étendus.

  Expression non codée [A-Z] {3,6} ¥[1-9 \][0-9]{6,6} Expression
  codée : [A-Z] {3,6} \ xC2 \ xA5 [1-9] [0-9] {6,6}

Vous pouvez trouver plusieurs tables qui incluent l'ensemble du jeu de caractères Unicode et les encodages UTF-8 correspondants sur Internet. Un site Web utile contenant ces informations est disponible dans le tableau suivant.

http://www.utf8-chartable.de/unicode-utf8-table.pl

Pour que les caractères du tableau de ce site Web s'affichent correctement, une police Unicode appropriée doit être installée sur votre ordinateur. Si ce n'est pas le cas, l'affichage visuel du personnage peut être erroné. Même si vous n'avez pas de police appropriée installée pour afficher un caractère, la description et les codes UTF-8 et UTF-16 de cet ensemble de pages Web sont corrects.

Types de signatures Whitehat WASC pour utilisation avec WAF

May 5, 2023

Le pare-feu NetScaler Web App accepte et génère des règles de blocage pour tous les types de vulnérabilités générés par les scanners Whitehat. Toutefois, certaines vulnérabilités concernent surtout un pare-feu d'applications Web. Vous trouverez ci-dessous des listes de ces vulnérabilités, classées selon qu'elles sont traitées par les types de signature WASC 1.0, WASC 2.0 ou selon les meilleures pratiques.

Types de signature WASC 1.0

- Contrebande de requêtes HTTP
- Fractionnement des réponses HTTP
- Contrebande de réponses HTTP
- Injection d'octets nuls
- Inclusion de fichiers à distance
- Abus de redirection d'URL

Types de signature WASC 2.0

- Abus de fonctionnalité
- Force brute

- Usurpation de contenu
- Déni de service
- Indexation d'annuaires
- Fuite d'informations
- Anti-automatisation insuffisant
- Authentification insuffisante
- Autorisation insuffisante
- Expiration de session insuffisante
- Injection LDAP
- Fixation des sessions

Recommandations

- Attribut de saisie semi-automatique
- Contrôle d'accès aux cookies insuffisant
- Sécurité du mot de passe insuffisante
- Utilisation de la méthode HTTP non valide
- Cookie de session non HTTP uniquement
- Cookie de session persistant
- Informations personnelles identifiables
- Messages HTTP sécurisés pouvant être mis en cache
- Cookie de session non sécurisé

Support du streaming pour le traitement des demandes

May 5, 2023

NetScaler Web App Firewall prend en charge le streaming côté demande afin d'améliorer considérablement les performances. Au lieu de mettre en mémoire tampon une demande, l'appliance examine le trafic entrant pour détecter toute violation de sécurité telle que SQL, script intersite, cohérence des champs, formats de champ. Lorsque l'appliance termine le traitement des données pour un champ, la demande est transmise au serveur principal tandis que l'appliance continue d'évaluer d'autres champs. Ce traitement des données améliore considérablement le temps de traitement dans le traitement des formulaires comportant de nombreux champs.

Citrix vous recommande d'activer le streaming pour le contenu de charge utile supérieur à 20 Mo. En outre, le serveur principal doit accepter les demandes segmentées si la diffusion en continu est activée.

> **Remarque :**
>
> L'action Post Body Limit est toujours définie sur Bloquer et s'applique aux modes streaming et non-streaming. Si le trafic entrant est supérieur à 20 Mo, Citrix vous recommande de `PostBodyLimit` configurer le sur la valeur attendue.

Bien que le processus de diffusion en continu soit transparent pour les utilisateurs, des ajustements mineurs de configuration sont nécessaires en raison des modifications suivantes :

Correspondance de motif RegEx : la correspondance de motif RegEx est désormais limitée à 4K pour une correspondance de chaîne de caractères contiguë.

Correspondance de nom de champ : Le moteur d'apprentissage du Web App Firewall ne peut distinguer que les 128 premiers octets du nom. Si un formulaire comporte plusieurs champs dont les noms ont une correspondance de chaîne identique pour les 128 premiers octets, le moteur d'apprentissage ne les distingue pas. De même, la règle de relaxation déployée peut par inadvertance assouplir tous ces champs.

La suppression des espaces blancs, le décodage en pourcentage, le décodage Unicode et la conversion des jeux de caractères sont effectués pendant la canonisation afin de fournir une inspection de contrôle de sécurité. La limite de 128 octets s'applique à la représentation canonique du nom de champ au format de caractères UTF-8. Les caractères ASCII ont une longueur d'un octet, mais la représentation UTF-8 des caractères dans certaines langues internationales peut aller de 1 octet à 4 octets. Si chaque caractère d'un nom prend 4 octets pour être converti au format UTF-8, seuls les 32 premiers caractères du nom peuvent être distingués par la règle apprise.

Vérification de la cohérence des champs : Lorsque vous activez la cohérence des champs, tous les formulaires de la session sont stockés en fonction de la balise « as_fid » insérée par le Web App Firewall sans tenir compte de l'option « action_url ».

- **Balisage de formulaire obligatoire pour la cohérence des champs de formulaire :** lorsque le contrôle de cohérence des champs est activé, la balise de formulaire doit également l'être. La protection de cohérence des champs peut ne pas fonctionner si le balisage de formulaire est désactivé.
- **Cohérence des champs de formulaire sans session :** le Web App Firewall n'effectue plus la conversion « GET » en « POST » des formulaires lorsque le paramètre de cohérence des champs sans session est activé. La balise de formulaire est également requise pour la cohérence des champs sans session.
- **Falsification de as_fid :** si un formulaire est soumis après avoir falsifié as_fid, il déclenche une violation de cohérence de champ même si aucun champ n'a été falsifié. Dans les demandes non diffusées, cela était autorisé car les formulaires peuvent être validés à l'aide de « action_url » stocké dans la session.

Signatures : Les signatures présentent désormais les spécifications suivantes :

- **Emplacement :** Il est désormais obligatoire de spécifier un emplacement pour chaque modèle. Tous les modèles de la règle **DOIVENT** avoir une <Location> étiquette.
- **Correspondance rapide :** Toutes les règles de signature doivent avoir un modèle de correspondance rapide. S'il n'y a pas de modèle de correspondance rapide, une tentative est faite pour en sélectionner un si possible. La correspondance rapide est une chaîne littérale mais PCRE peut être utilisée pour une correspondance rapide si elle contient une chaîne littérale utilisable.
- Emplacements**déconseillés : Les emplacements** suivants ne sont plus pris en charge dans les règles de signature.
  - HTTP_ANY
  - HTTP_RAW_COOKIE
  - HTTP_RAW_HEADER
  - HTTP_RAW_RESP_HEADER
  - HTTP_RAW_SET_COOKIE

script intersite/Transformation SQL : les données brutes sont utilisées pour la transformation car les caractères spéciaux SQL tels que le guillemet simple (‘), la barre oblique inverse () et le point-virgule (;)) et les balises de script intersite sont identiques et ne nécessitent pas la canonisation des données. La représentation des caractères spéciaux tels que le codage d'entité HTML, le codage en pourcentage ou l'ASCII est évaluée pour l'opération de transformation.

Le Web App Firewall n'inspecte plus à la fois le nom et la valeur de l'attribut pour l'opération de transformation de script intersite. Désormais, seuls les noms d'attributs de script intersite sont transformés lorsque le streaming est activé.

Traitement des balises de script intersite : dans le cadre des modifications de diffusion en continu dans NetScaler 10.5.e et versions ultérieures, le traitement des balises de script intersite a changé. Dans les versions précédentes, la présence d'un crochet ouvert (<), or close bracket (>) ou des deux crochets ouverts et fermants (<>) était signalée comme Violation de script intersite. Le comportement a changé à partir de la version 10.5.e. La présence du seul caractère de crochet ouvert (<), ou uniquement du caractère de crochet fermé (>) n'est plus considérée comme une attaque. C'est lorsqu'un caractère de crochet ouvert (<) est suivi par un caractère de crochet fermé (>), l'attaque par script intersite est signalée. Les deux caractères doivent être présents dans le bon ordre (< suivi de >) pour déclencher la violation de script intersite.

> **Remarque :**
>
> **Modification du journal des violations SQL Message : dans** le cadre des modifications de streaming apportées à la version 10.5.e de NetScaler et aux versions ultérieures, nous traitons désormais les données d'entrée par blocs. La correspondance de motifs RegEx est désormais limitée à 4K pour la correspondance de chaînes de caractères contiguës. Avec cette modification, les messages du journal des violations SQL peuvent inclure des informations différentes

> par rapport aux versions précédentes. Le mot-clé et le caractère spécial de l'entrée sont séparés par de nombreux octets. L'appliance dispose d'un suivi des mots-clés SQL et des chaînes spéciales lors du traitement des données, au lieu de mettre en mémoire tampon la valeur d'entrée entière. Outre le nom du champ, le message de journal inclut le mot-clé SQL, le caractère spécial SQL ou à la fois le mot-clé SQL et le caractère spécial SQL. Le reste de l'entrée n'est plus inclus dans le message de journal, comme illustré dans l'exemple suivant :
>
> **Exemple :**
>
> Dans la version 10.5, lorsque le Web App Firewall détecte la violation SQL, la chaîne d'entrée complète peut être incluse dans le message de journal suivant :
>
> La vérification du mot-clé SQL a échoué pour le champ **text=”select a name from testbed1\;\(\;\)”:*<blocked>**
>
> Dans la version 11.0, nous enregistrons uniquement le nom du champ, le mot-clé et le caractère spécial (le cas échéant) dans le message de journal suivant.
>
> La vérification du mot-clé SQL a échoué pour le champ `text="select(;)"<blocked>`
>
> ****Cette modification s'applique aux demandes contenant des **types de contenu application/x-www-form-urlencoded, multipart/form-data ou text/x-gwt-rpc.** Les messages de journal générés lors du traitement des charges utiles **JSON** ou **XML** ne sont pas affectés par cette modification.

Corps RAW POST : Les contrôles de sécurité sont toujours effectués sur le corps RAW POST.

ID du formulaire : Le Web App Firewall a inséré la balise « as_fid », qui est un hachage calculé du formulaire est plus unique pour la session utilisateur. Il s'agit d'une valeur identique pour un formulaire spécifique quel que soit l'utilisateur ou la session.

Jeu de caractères : si une demande ne possède pas de jeu de caractères, le jeu de caractères par défaut spécifié dans le profil d'application est utilisé lors du traitement de la demande.

Compteurs :

Des compteurs avec les préfixes « se » et « appfwreq » sont ajoutés pour suivre les compteurs de requêtes du moteur de streaming et du moteur de streaming.

```
nsconsmg -d statswt0 -g se_err_

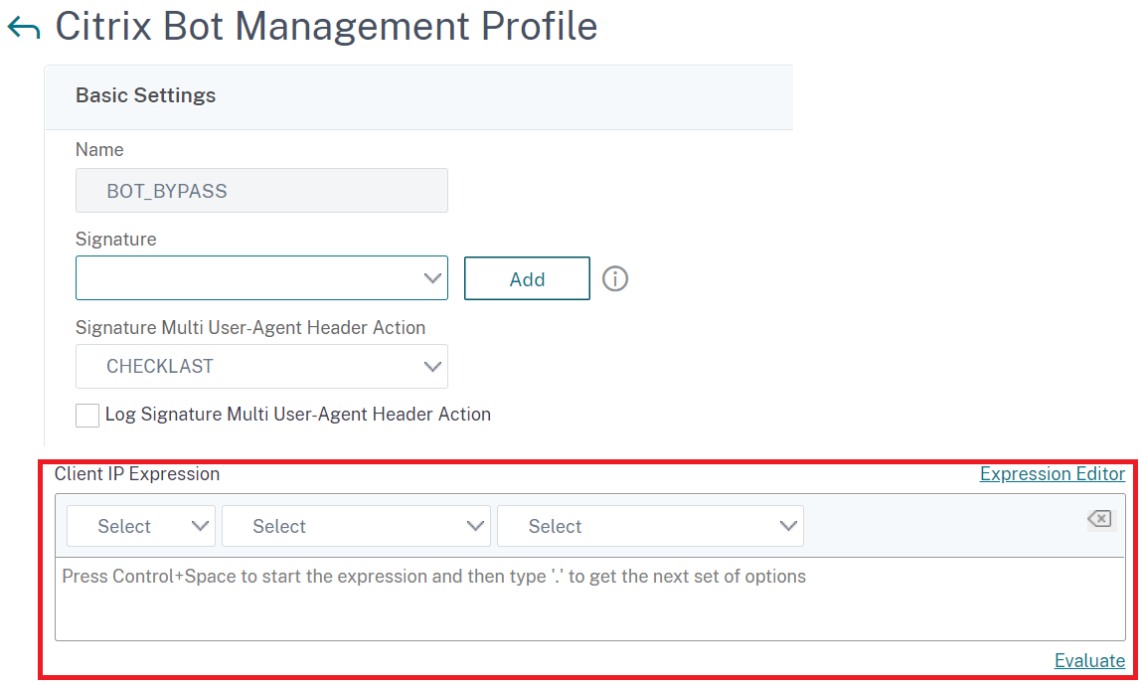
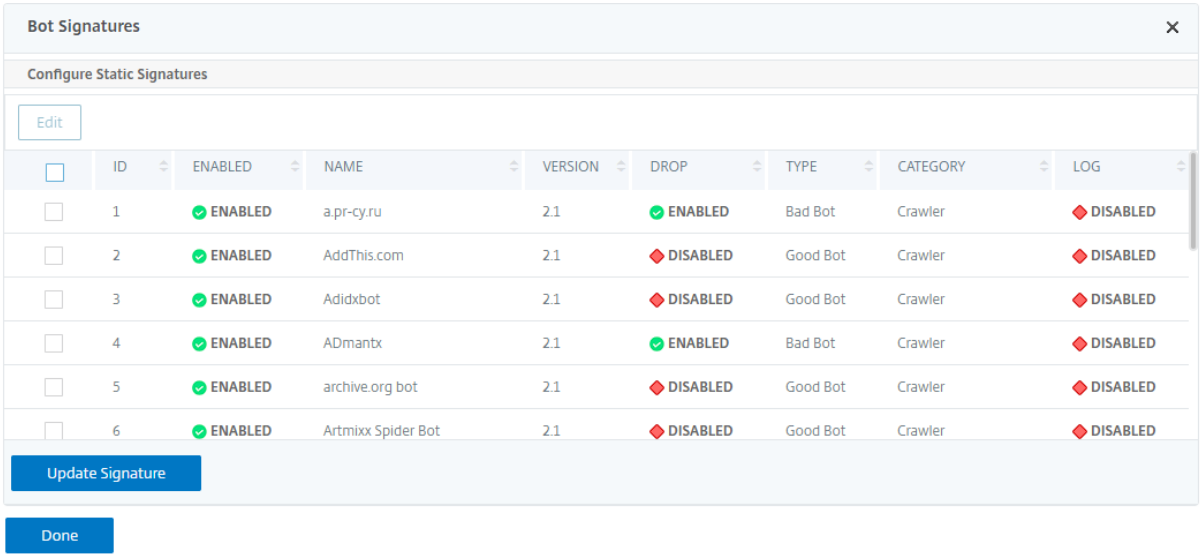
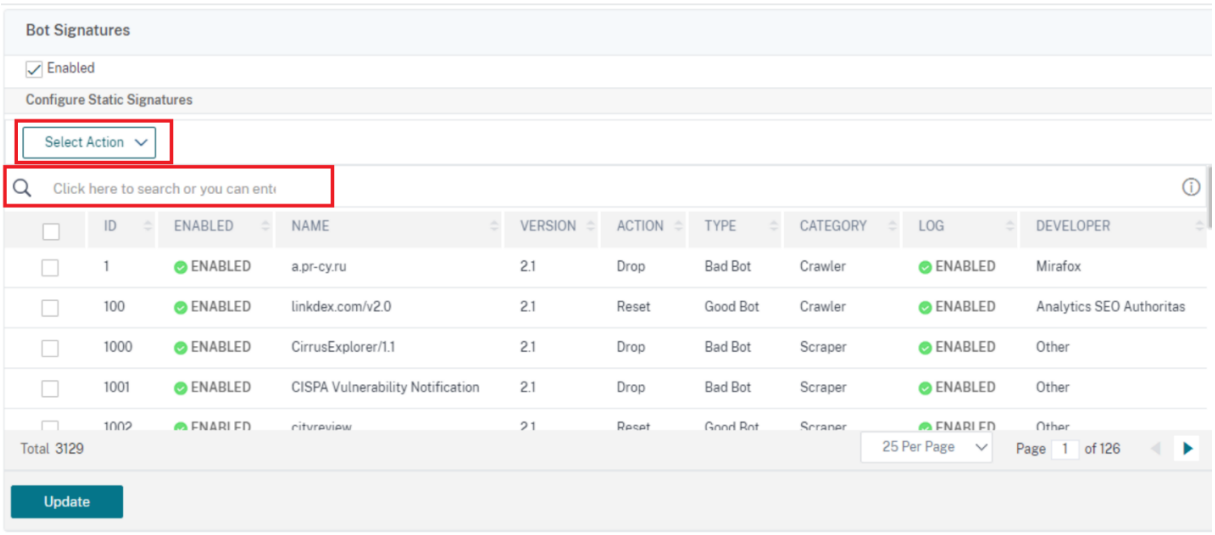
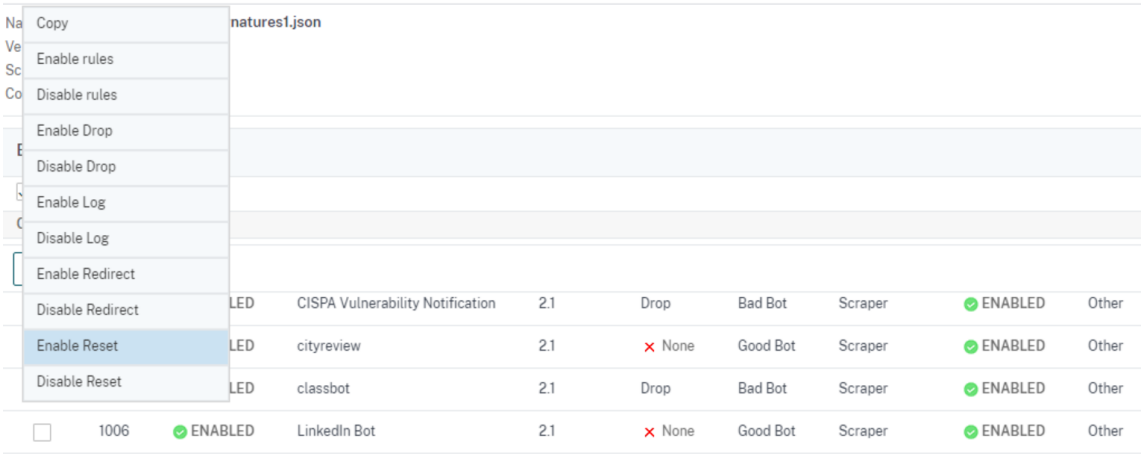
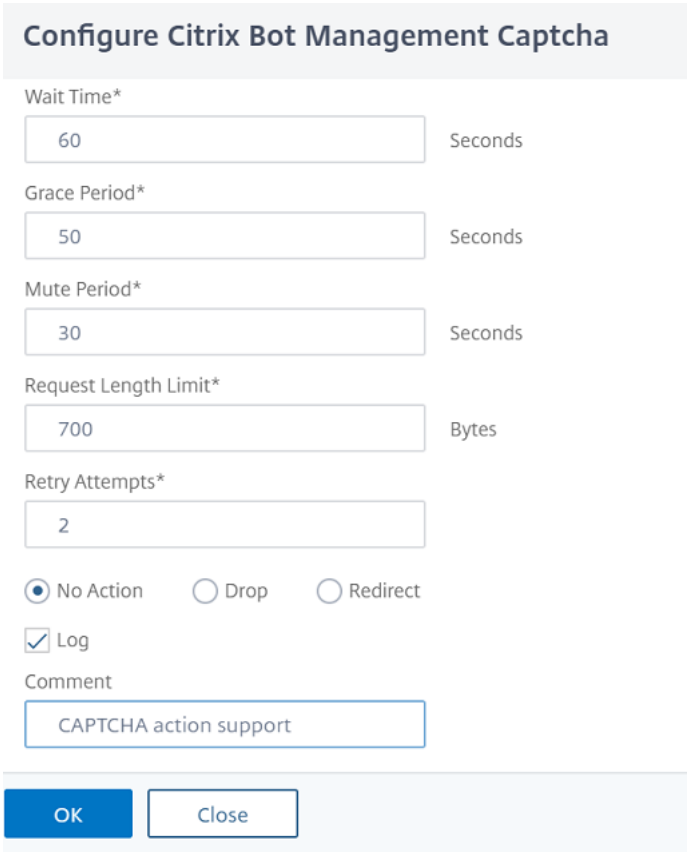
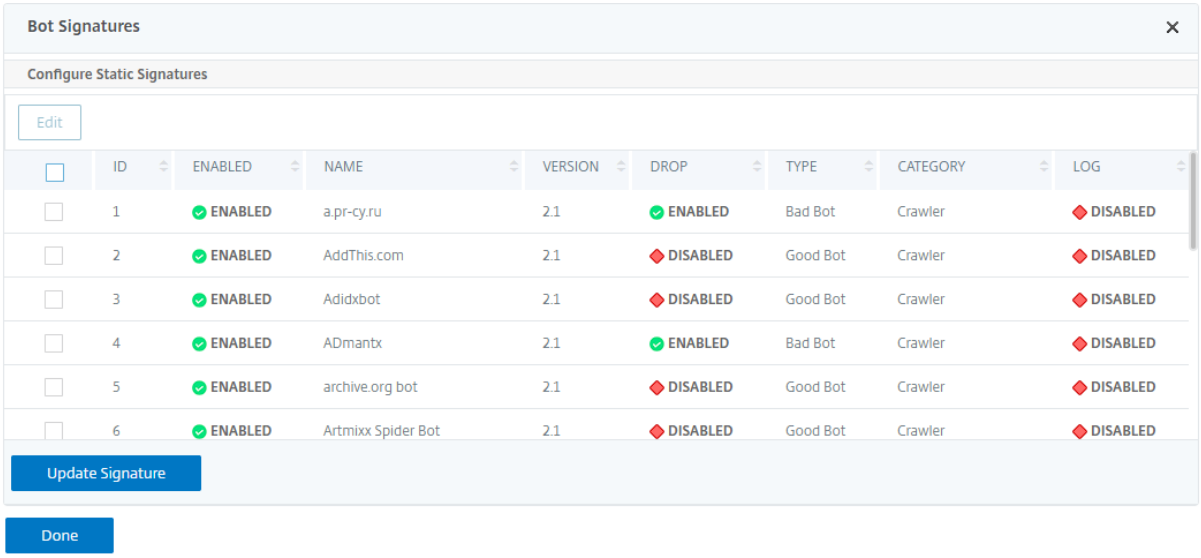
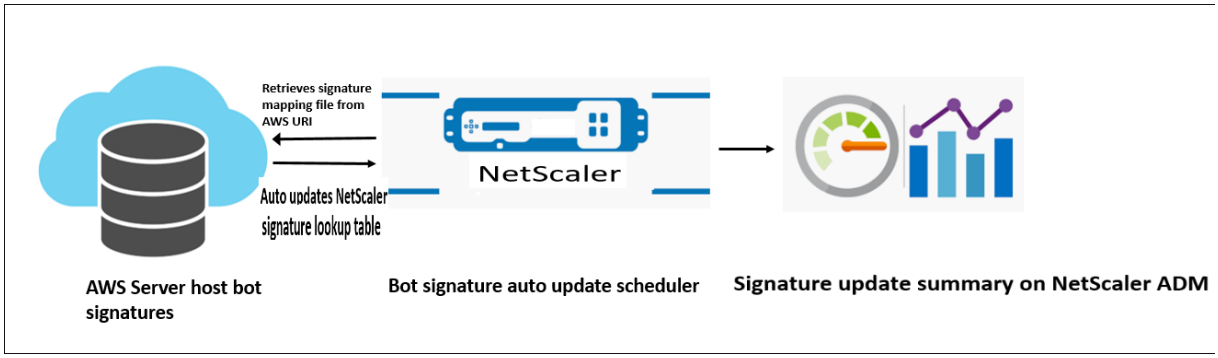
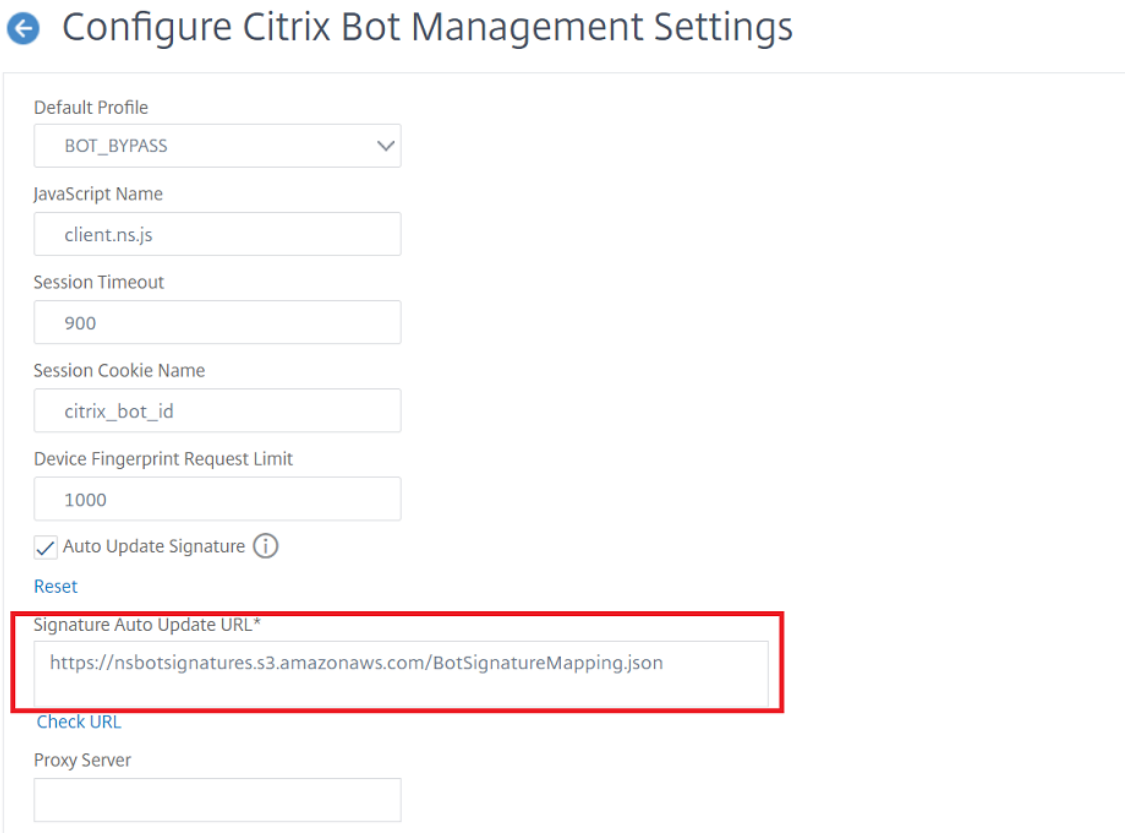
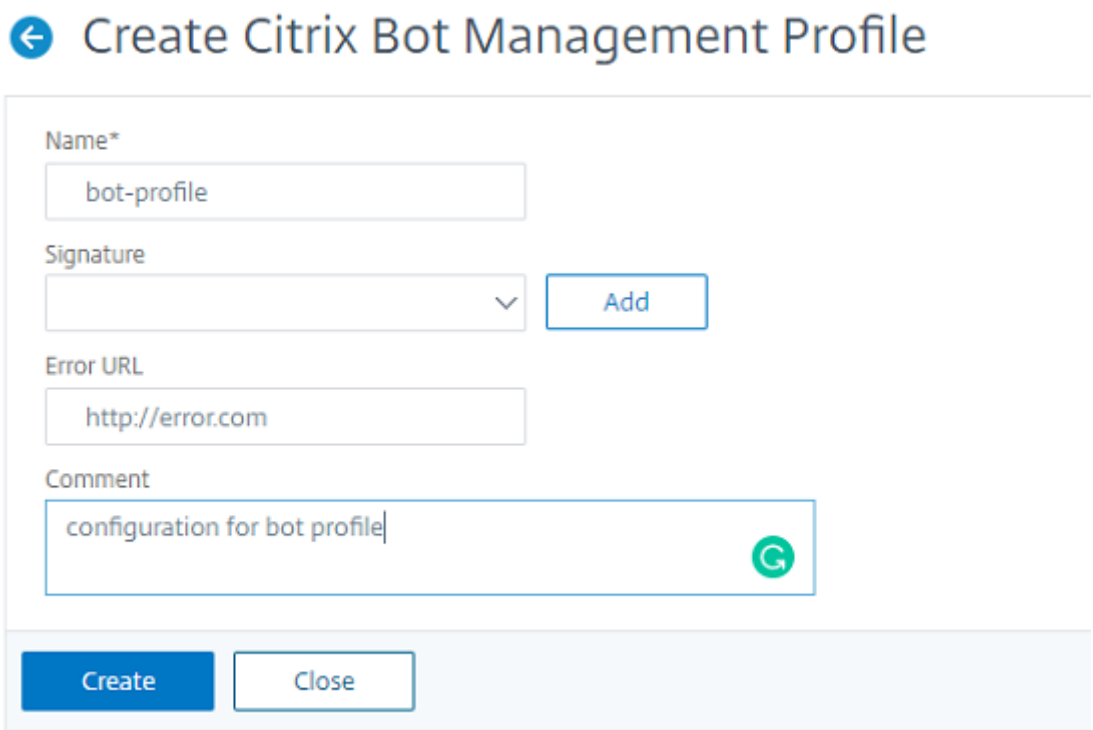
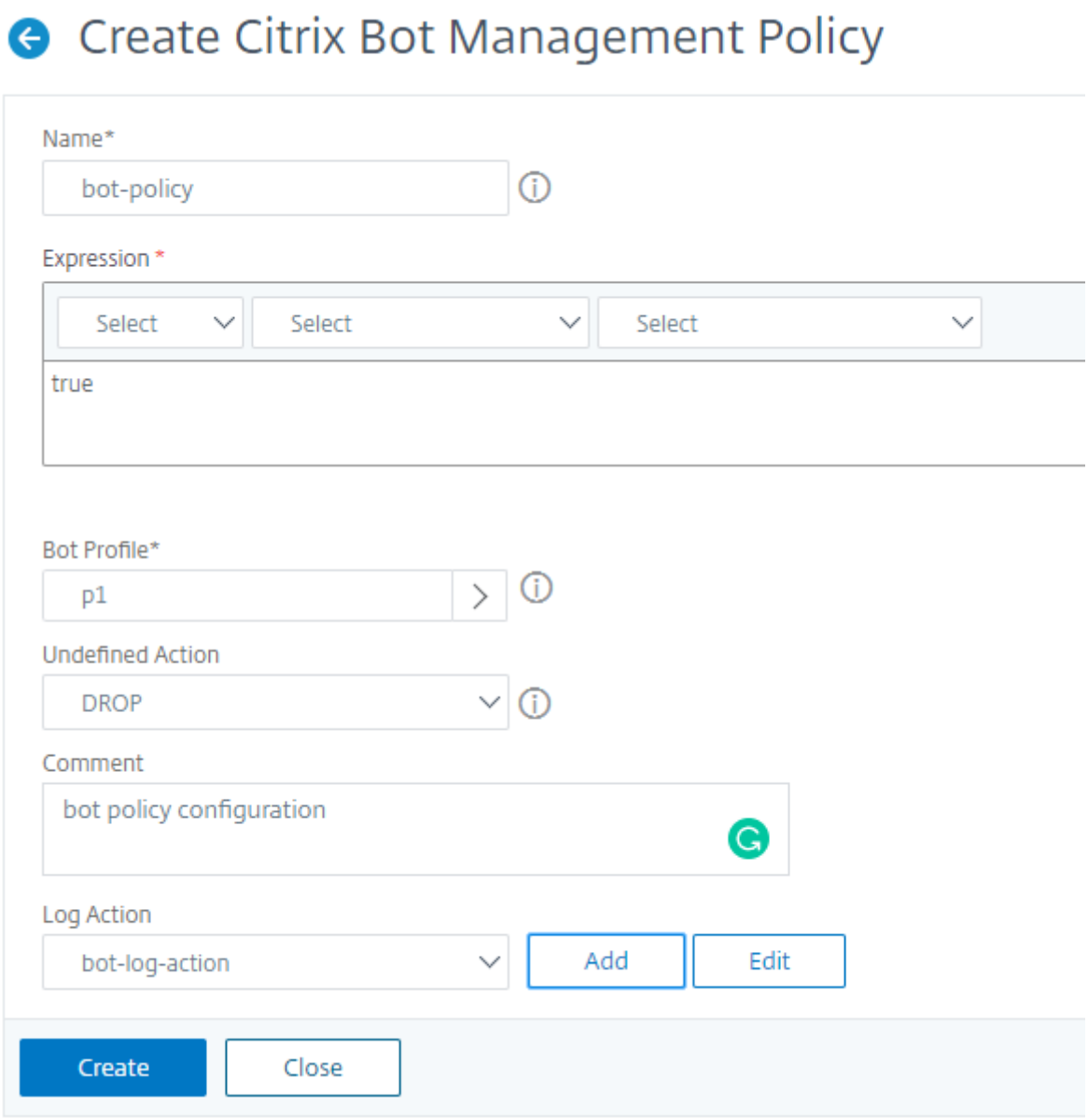
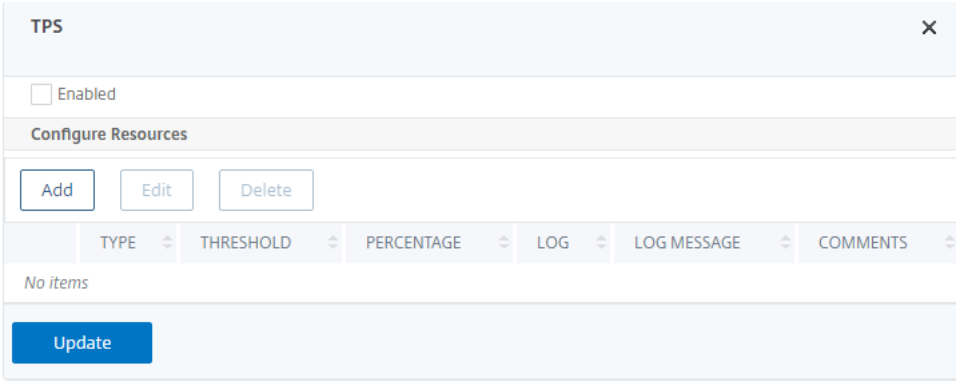
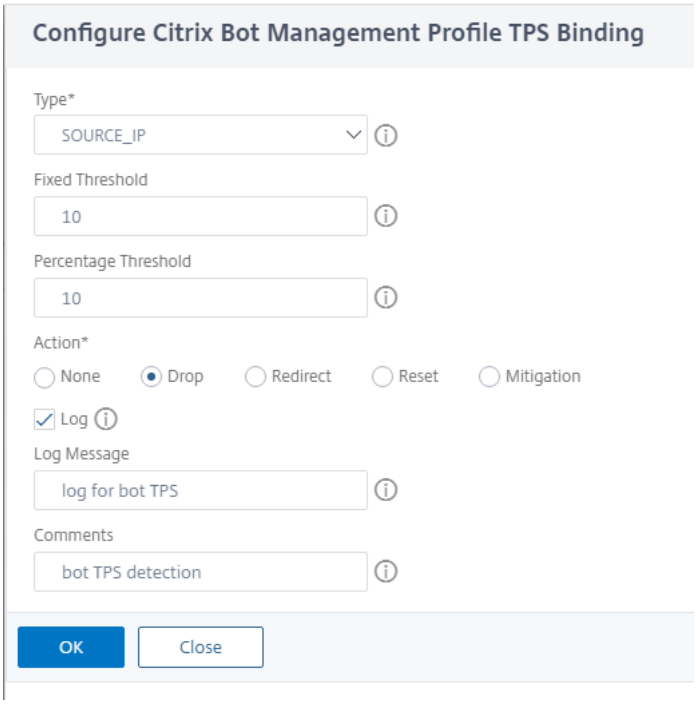
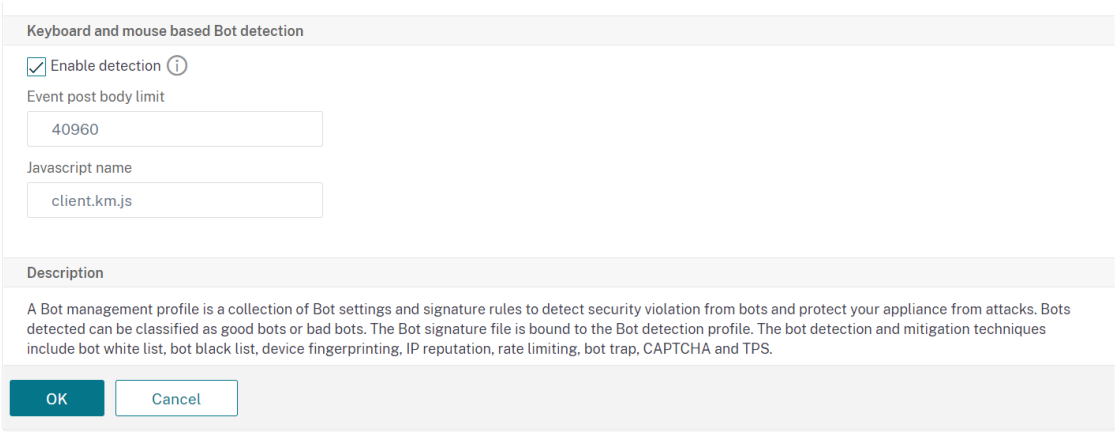
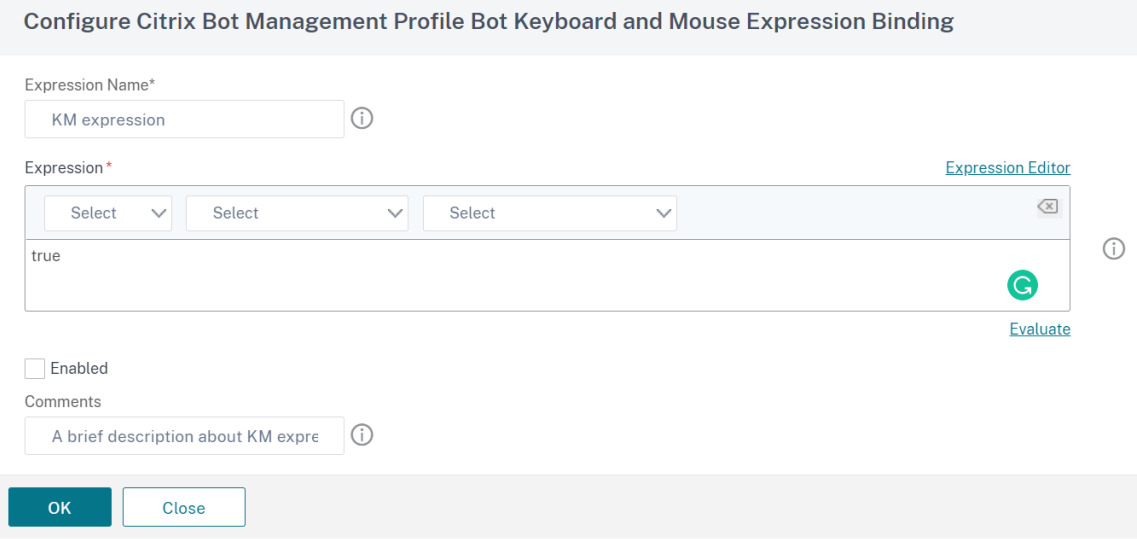
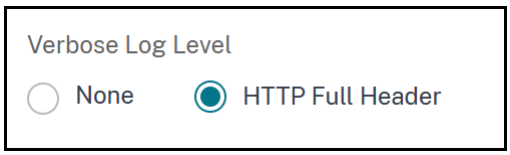
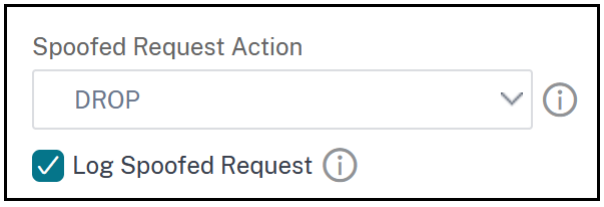
nsconsmg -d statswt0 -g se_tot_

nsconsmg -d statswt0 -g se_cur_

nsconsmg -d statswt0 -g appfwreq_err_

nsconsmg -d statswt0 -g appfwreq_tot_

nsconsmg -d statswt0 -g appfwreq_cur_
```


`_err counters`: indique l'événement rare qui a dû réussir mais qui a échoué en raison d'un problème d'allocation de mémoire ou d'un autre problème de ressources.

`_tot counters`: des compteurs toujours plus nombreux.

`_cur counters`: compteurs indiquant les valeurs actuelles qui ne cessent de changer en fonction de l'utilisation des transactions en cours.

Conseils :

- Les contrôles de sécurité du Web App Firewall doivent fonctionner de la même manière qu'auparavant.
- Il n'y a pas d'ordre défini pour le traitement des contrôles de sécurité.
- Le traitement côté réponse n'est pas affecté et reste inchangé.
- Le streaming n'est pas activé si un VPN sans client est utilisé.

> **Important :**
>
> **Calcul de la longueur du cookie :** dans la version 10.5.e, en plus de la version 11.0 de NetScaler (dans les versions antérieures à 65.x), la méthode de traitement de l'en-tête du cookie par Web App Firewall a été modifiée. L'appliance a évalué le cookie individuellement, et si la longueur d'un cookie dans l'en-tête du cookie dépassait la longueur configurée, la violation de débordement de tampon était déclenchée. Par conséquent, les demandes bloquées dans la version NetScaler 10.5 ou les versions antérieures peuvent être autorisées. La longueur de l'en-tête du cookie n'est pas calculée pour déterminer la longueur du cookie. Dans certains cas, la taille totale du cookie peut être supérieure à la valeur acceptée et le serveur peut répondre par « 400 demandes erronées ».
>
> **Remarque :**
> La modification a été annulée. Le comportement dans NetScaler versions 10.5.e à 59.13xx.e et ses versions ultérieures est similaire à celui des versions sans amélioration de la version 10.5. L'intégralité de l'en-tête Cookie brut est désormais prise en compte lors du calcul de la longueur du cookie. Les espaces environnants et les points-virgules (;) séparant les paires nom-valeur sont également inclus dans la détermination de la longueur du cookie.

Suivez les requêtes HTML à l'aide de journaux de sécurité

May 5, 2023

> **Remarque :**
>
> Cette fonctionnalité est disponible dans NetScaler version 10.5.e.

Le dépannage nécessite l'analyse des données reçues dans la demande du client et peut s'avérer difficile. Surtout s'il y a beaucoup de trafic dans l'appliance. Le diagnostic des problèmes peut affecter les fonctionnalités ou la sécurité de l'application peut nécessiter une réponse rapide.

NetScaler isole le trafic pour un profil de Web App Firewall et le collecte `nstrace` pour les requêtes HTML. Les `nstrace` informations collectées en mode appfw incluent les détails de la demande avec les messages du journal. Vous pouvez utiliser « Suivre le flux TCP » dans le traçage pour afficher les détails de chaque transaction, y compris les en-têtes, la charge utile et le message de journal correspondant sur le même écran.

Cela vous donne un aperçu complet de votre trafic. Il peut être utile de disposer d'une vue détaillée de la demande, de la charge utile et des enregistrements de journal associés pour analyser les violations des contrôles de sécurité. Vous pouvez facilement identifier le schéma à l'origine de la violation. Si le modèle doit être autorisé, vous pouvez décider de modifier la configuration ou d'ajouter une règle de relaxation.

Avantages

1. **Isoler le trafic pour un profil spécifique** : cette amélioration est utile lorsque vous isolez le trafic pour un seul profil ou pour des transactions spécifiques d'un profil à des fins de résolution de problèmes. Vous n'avez plus à parcourir l'intégralité des données collectées dans le traçage ni à avoir besoin de filtres spéciaux pour isoler les demandes qui vous intéressent, ce qui peut s'avérer fastidieux en cas de trafic important. Vous pouvez consulter les données que vous préférez.
2. **Collecter des données pour des demandes spécifiques** : La trace peut être collectée pendant une durée spécifiée. Vous ne pouvez collecter des traces que pour quelques requêtes afin d'isoler, d'analyser et de déboguer des transactions spécifiques si nécessaire.
3. **Identifiez les réinitialisations ou les abandons** : la fermeture inattendue des connexions n'est pas facilement visible. La trace collectée en mode —appfw capture une réinitialisation ou un abandon, déclenché par le Web App Firewall. Cela permet d'isoler plus rapidement un problème lorsque vous ne voyez pas de message de violation du contrôle de sécurité. Les demandes mal formées ou autres demandes non conformes aux RFC annulées par le Web App Firewall seront désormais plus faciles à identifier.
4. **Afficher le trafic SSL décrypté** : le trafic HTTPS est capturé en texte brut pour faciliter le dépannage.
5. **Fournit une vue complète** : vous permet d'examiner l'intégralité de la demande au niveau du paquet, de vérifier la charge utile, de consulter les journaux pour vérifier quelle violation du contrôle de sécurité est déclenchée et d'identifier le modèle de correspondance dans la charge utile. Si la charge utile est constituée de données inattendues, de chaînes indésirables ou de caractères non imprimables (caractère nul, \ r ou \ n, etc.), il est facile de les découvrir dans le traçage.

6. **Modifier la configuration** : Le débogage peut fournir des informations utiles pour décider si le comportement observé est le bon comportement ou si la configuration doit être modifiée.
7. **Temps de réponse**plus rapide : un débogage plus rapide sur le trafic cible peut améliorer le temps de réponse pour fournir des explications ou analyser les causes profondes par l'équipe d'ingénierie et de support de NetScaler.

Pour plus d'informations, voir Configuration manuelle à l'aide de la rubrique Interface de ligne de commande .

Pour configurer le suivi de débogage d'un profil à l'aide de l'interface de ligne de commande

Étape 1. Activez ns trace.

Vous pouvez utiliser la commande show pour vérifier le paramètre configuré.

- `set appfw profile <profile> -trace ON`

Étape 2. Recueillez des traces. Vous pouvez continuer à utiliser toutes les options applicables à la `nstrace` commande.

- `start nstrace -mode APPFW`

Étape 3. Arrêtez le traçage.

- `stop nstrace`

Emplacement de la trace : elle`nstrace` est stockée dans un dossier horodaté créé dans le répertoire /var/nstrace et pouvant être consulté à l'aide de. `wireshark` Vous pouvez suivre le lien `/var/log/ns.log` pour voir les messages du journal fournissant des détails concernant l'emplacement de la nouvelle trace.

Conseils :

- Lorsque l'option du mode appfw est utilisée, les données ne `nstrace` seront collectées que pour un ou plusieurs profils pour lesquels le « nstrace » a été activé.
- L'activation de la trace sur le profil ne lancera pas automatiquement la collecte des traces tant que vous n'aurez pas exécuté explicitement la commande « start ns trace » pour collecter la trace.
- Bien que l'activation du traçage sur un profil n'ait aucun effet négatif sur les performances du Web App Firewall, vous souhaiterez peut-être activer cette fonctionnalité uniquement pendant la durée pendant laquelle vous souhaitez collecter les données. Il est recommandé de désactiver l'indicateur —trace après avoir collecté la trace. Cette option évite le risque d'obtenir par inadvertance des données à partir de profils pour lesquels vous avez activé cet indicateur par le passé.
- L'action de blocage ou de journalisation doit être activée pour que le contrôle de sécurité de l'enregistrement des transactions soit inclus dans le `nstrace`.

- Les réinitialisations et les abandons sont enregistrés indépendamment des actions des contrôles de sécurité lorsque le traçage est « activé » pour les profils.
- Cette fonctionnalité ne s'applique qu'à la résolution des problèmes liés aux demandes reçues du client. Les traces en mode —appfw n'incluent pas les réponses reçues du serveur.
- Vous pouvez continuer à utiliser toutes les options applicables à la `nstrace` commande. Par exemple,

  ```
  start nstrace -tcpdump enabled -size 0 -mode appFW
  ```

- Si une demande déclenche plusieurs violations, l'enregistrement `nstrace` correspondant inclut tous les messages de journal correspondants.
- Le format des messages de journal CEF est pris en charge pour cette fonctionnalité.
- Les violations de signature déclenchant une action de blocage ou de journalisation pour les vérifications latérales des demandes seront également incluses dans le traçage.
- Seules les requêtes HTML (non-XML) sont collectées dans la trace.

Support du Web App Firewall pour les configurations de clusters

May 5, 2023

> **Remarque :**
>
> Le pare-feu NetScaler Web App pour les configurations réparties par bandes et partiellement réparties par bandes a été introduit dans la version 11.0 de NetScaler.

Un cluster est un groupe d'appliances NetScaler configurées et gérées comme un seul système. Chaque appliance du cluster est appelée nœud. Selon le nombre de nœuds sur lesquels les configurations sont actives, les configurations de cluster sont appelées configurations réparties par bandes, partiellement réparties par bandes ou par points. Le Web App Firewall est entièrement pris en charge dans toutes les configurations.

Les deux principaux avantages de la prise en charge des serveurs virtuels répartis par bandes et partiellement répartis par bandes dans les configurations en cluster sont les suivants :

1. Prise en charge du basculement de session : les configurations de serveurs virtuels répartis par bandes et partiellement réparties par bandes prennent en charge le basculement de session. Les fonctionnalités de sécurité avancées du Web App Firewall, telles que la fermeture de l'URL de démarrage et la cohérence des champs de formulaire, vérifient, gèrent et utilisent des sessions pendant le traitement des transactions. Dans une configuration haute disponibilité ou dans une configuration de cluster repéré, lorsque le nœud qui traite le trafic du Web App Firewall tombe en panne, toutes les informations de session sont perdues et l'utilisateur doit

rétablir la session. Dans les configurations de serveurs virtuels répartis par bandes, les sessions utilisateur sont répliquées sur plusieurs nœuds. Si un nœud tombe en panne, le nœud exécutant la réplique en devient le propriétaire. Les informations de session sont conservées sans aucun impact visible pour l'utilisateur.

2. Évolutivité : n'importe quel nœud du cluster peut traiter le trafic. Plusieurs nœuds du cluster peuvent traiter les demandes entrantes traitées par le serveur virtuel réparti par bandes. Cela améliore la capacité du Web App Firewall à gérer plusieurs demandes simultanées, améliorant ainsi les performances globales.

Les contrôles de sécurité et les protections des signatures peuvent être déployés sans nécessiter de configuration supplémentaire du Web App Firewall spécifique au cluster. Vous pouvez effectuer la configuration habituelle du Web App Firewall sur le nœud Coordinateur de configuration (CCO) pour la propagation vers tous les nœuds.

> **Remarque :**
>
> Les informations de session sont répliquées sur plusieurs nœuds, mais pas sur tous les nœuds de la configuration par bandes. Par conséquent, la prise en charge du basculement prend en charge un nombre limité de défaillances simultanées. Si plusieurs nœuds tombent en panne simultanément, le Web App Firewall risque de perdre les informations de session si une défaillance survient avant que la session ne soit répliquée sur un autre nœud.

Résumé

- Le Web App Firewall offre une évolutivité, un haut débit et une prise en charge du basculement de session dans les déploiements de clusters.
- Toutes les vérifications de sécurité et les protections des signatures du Web App Firewall sont prises en charge dans toutes les configurations de cluster.
- Les cartes de caractères ne sont pas encore prises en charge pour un cluster. Le moteur d'apprentissage recommande les types de champs dans les règles apprises pour le contrôle de sécurité du format de champ.
- Les statistiques et les règles apprises sont agrégées à partir de tous les nœuds d'un cluster.
- La table de hachage distribuée (DHT) assure la mise en cache de la session et permet de répliquer les informations de session sur plusieurs nœuds. Lorsqu'une demande parvient au serveur virtuel, l'appliance NetScaler crée des sessions Web App Firewall dans le DHT et peut également récupérer les informations de session à partir du DHT.
- Le clustering est sous licence avec les licences Advanced et Premium. Cette fonctionnalité n'est pas disponible avec la licence Standard.

Débogage et dépannage

August 20, 2021

Reportez-vous aux informations de dépannage et de débogage suivantes liées à chacune des fonctionnalités de Web App Firewall :

- Pare-feu d'application - CPU élevé
- Mémoire
- Échec du chargement de fichiers volumineux
- Apprentissage
- Signatures
- Journal de suivi
- Divers

Processeur élevé

May 5, 2023

Vous trouverez ci-dessous certains des problèmes de débogage liés aux fonctionnalités et à l'utilisation intensive du processeur rencontrés, ainsi que les meilleures pratiques à suivre lors de l'utilisation du Web App Firewall :

Vérifiez les accès aux politiques, les liaisons, la configuration du réseau, la configuration du Web App Firewall :

- Identifiez les erreurs de configuration
- Identifiez le *serveur virtuel* qui dessert le trafic concerné

Consultez les journaux des fichiers journaux suivants pour détecter les violations de sécurité et les modifications de configuration récentes :

- `/var/log/ns.log`
- `/var/nslog/import.log`
- `/var/nslog/aslearn.log`
- `tail -f /var/log/ns.log | grep APPFW_SIGNATURE_MATCH`

Exemple :

```
Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW| APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method
    =GET request= http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=
    Signature violation rule ID 807: web-cgi /wwwboard/passwd.txt access
```



```
        cn1=140 cn2=841 cs1=pr_ffc cs2=PPE0 cs3=
       OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=
       not blocked
<!--NeedCopy-->
```

Isolez le trafic concerné :

- Isolez le profil
- Isolez le contrôle de sécurité
- Isolez l'URL, le serveur virtuel et les paramètres de trafic

Le suivi conditionnel au niveau du profil permet d'identifier les enregistrements de trafic et d'infractions :

- `set appfw profile <profile> -trace ON`
- `start nstrace -mode APPFW -size 0`
- `stop nstrace`

Remarque : Assurez-vous que la trace est collectée avec l'option -size 0.

Vérifiez les compteurs d'activité appfw, dht et de réputation IP :

- `nsconmsg -g as_ -g appfwreq_ -g iprep -d current`

Surveillez la taille de la fenêtre pour les réinitialisations lors de la connexion :

Appfw définit la taille de la fenêtre sur 9845 lorsque NetScaler réinitialise la connexion en raison d'un message http non valide.

Exemples :

- Requête mal formée reçue - réinitialisation de la connexion
- Problèmes liés à un processeur élevé
- Consultez les fiches techniques pour connaître les limites du système
- Vérifiez l'utilisation du processeur, l'appfw, le DHT et les activités liées à la mémoire. Surveillez les sessions d'appfw
- nsconmsg -g cc_cpu_use -g appfwreq -g as -g dht -g MEM_AS_obj -g MEM_AS_component -d current

Surveillez la mémoire allouée et libérée par les composants et les objets du Web App Firewall pendant la période cible. Cela permet d'isoler la protection qui entraîne une utilisation élevée du processeur.

- Sortie du profileur
- Observez les journaux

Isolez la vérification appfw qui entraîne une augmentation du processeur :

- Fermeture de l'URL de démarrage

- Cohérence des fichiers de formulaire
- CSRF
- Protections relatives aux cookies
- Vérification de l'en-tête du référent

Vérifiez que la mise à jour automatique des signatures n'entraîne pas une surcharge du processeur (Désactivez pour confirmer).

Mémoire

August 20, 2021

Voici quelques-unes des meilleures pratiques à suivre en cas de problèmes liés à la mémoire d'utilisation du Web App Firewall :

nsconmsg, commande utilisation :

- Recherchez des statistiques de mémoire globales pour vérifier qu'il y a suffisamment de mémoire dans le système et qu'il n'y a pas d'échecs d'allocation de mémoire en exécutant la commande suivante :

  ```
  * *- nsconmsg -d memstats
  ```

- Observez les limites de mémoire allouées et maximales actuelles pour appsecure, la réputation IP, le cache et la compression en exécutant la commande suivante :

  ```
  nsconmsg -d memstats | egrep -i APPSECURE|IPREP|CACHE|CMP
  ```

- Vérifiez les compteurs d'activité appfw, DHT, IP réputation en exécutant la commande suivante :

  ```
  nsconmsg -g as -g appfwreq_ -g iprep -d current
  ```

- Vérifiez tous les compteurs d'erreur du Web App Firewall en exécutant la commande suivante :

  ```
  nsconmsg -g as_ -g appfwreq_ -g iprep_ -d stats | grep err
  ```

- Vérifiez tous les compteurs d'erreurs système en exécutant la commande suivante :

  ```
  nsconmsg -g err -d current
  ```

- Inspectez les compteurs CPU, APPFWREQ, AS et DHT en exécutant la commande suivante :

  ```
  nsconmsg -g cc_cpu_use -g appfwreq -g as -g dht -d current
  ```

- Vérifiez la mémoire cache configurée en exécutant la commande suivante :
- `show cacheparameter`
- Vérifiez la mémoire configurée en exécutant la commande suivante :

  ```
  nsconmsg -d memstats | egrep -i CACHE
  ```


- Identifier la distribution de la mémoire dans les composants et objets du Web App Firewall :

Afficher la mémoire AS_OBJ_ :

```
nsconmsg -K newnslog -d stats | grep AS_OBJ | egrep -v AppFW_cpu0|total |
sort -k3
```

Afficher la mémoire AS_COMPONENT_ :

```
nsconmsg -K newnslog -d stats | grep AS_COMPONENT | egrep -v AppFW_cpu0|
total | sort -k3
```

Vérifiez le nombre de sessions actives en exécutant la commande suivante :

Nombre de**sessions actives de moniteur/tracé** :

```
nsconmsg -g as_alive_sessions -d current
```

Moniteur/tracé total alloué, gratuit, sessions mises à jour :

- `nsconmsg -g as_tot_alloc_sessions -g as_tot_free_sessions -d current`
- `nsconmsg -g as_tot_update_sessions -d current`

Si nécessaire, réduisez le délai d'expiration de session pour vous assurer que les limites de session ne sont pas utilisées en exécutant la commande suivante :

```
set appfwsettings -sessionTimeout <300>
```

Si nécessaire, définissez la durée de vie maximale de la session en exécutant la commande suivante :

```
set appfwsettings -sessionLifetime <7200>
```

Vérification de la mémoire allouée et utilisée

Pour vérifier la mémoire totale allouée et la mémoire utilisée :

- Utilisez la commande **nsconmsg —d memstats**. Observez le champ **MEM_APPSECURE**.
- Utilisez la commande **stat appfw** pour obtenir des informations sur la consommation de mémoire.

Le Web App Firewall ne supprime pas automatiquement les journaux après une certaine période de temps ou de taille.

- `All AppFw logs are archived in the */var/log/ns.log*` fichier. Le fichier *ns.log* effectue la tâche de survol.

Pour plus d'informations, consultez le lien suivant :<http://support.citrix.com/article/CTX121898>

Augmentation de la mémoire de Web App Firewall :

- Il n'y a pas d'option CLI pour augmenter la mémoire du Web App Firewall. La mémoire de Web App Firewall est spécifique à la plate-forme.
- Vous pouvez utiliser l'option *nsapimgr* pour augmenter la mémoire, mais ce n'est pas recommandé.

La mémoire maximale autorisée pour le Web App Firewall est déterminée par la plate-forme et la désactivation de l'IC n'affecte pas l'allocation de mémoire.

Échec du téléchargement de fichiers volumineux

January 21, 2021

Lorsque vous rencontrez des échecs de téléchargement de fichiers volumineux, vérifiez les éléments suivants :

— Limite postbody du pare-feu d'application mal configurée
— Activation de l'analyse de téléchargement de fichiers entraînant une augmentation du temps de traitement.
— Atteler les limites du système ;

Pour les charges utiles supérieures à 20 Mo, Citrix vous recommande d'activer la diffusion en continu sur le profil de pare-feu de l'application. En outre, vous devez vous assurer que le serveur principal prend en charge les requêtes tronquées avant d'activer la diffusion en continu.

Depuis la version 11.0, l'indicateur de diffusion peut être activé par profil pour éviter la mise en mémoire tampon en exécutant la commande suivante :

```
set appfw profile <profile name> -streaming on
```

Apprentissage

August 20, 2021

Voici quelques-unes des meilleures pratiques recommandées en cas de problèmes de fonctionnalité d'apprentissage :

Processus d'apprentissage :

- Vérifiez que le processus *aslearn est en* cours d'exécution.
- Vérifier la sortie de la commande supérieure
- Vérifiez la sortie de la commande ps en exécutant la commande suivante :


```
ps -ax | grep aslearn | grep -v "grep"
```

Exemple :

```
root@ns# ps -ax | grep aslearn | grep -v "grep"
1439  ??  Ss     0:03.86 /netscaler/aslearn -start -f /netscaler/
   aslearn.conf
<!--NeedCopy-->
```

- Identifiez les commandes de configuration récentes exécutées avant le problème observé en vérifiant le fichier *ns.log* :

  ```
  /var/log/ns.log
  ```

- Inspectez les journaux d'apprentissage pour rechercher les messages d'apprentissage :

  ```
  /var/log/aslearn.log
  ```

- Isoler le profil et le contrôle de sécurité effectué
- Identifiez l'interface graphique et la commande CLI qui échoue en exécutant la commande suivante :

  ```
  show appfw learningdata <profileName> <securityCheck>
  ```

  Exemples :

  - `show learningdata test_profile starturl`
  - `show learningdata test_profile crosssiteScripting`
  - `show learningdata test_profile sqLInjection`
  - `show learningdata test_profile csRFtag`
  - `show learningdata test_profile fieldformat`
  - `show learningdata test_profile fieldconsistency`

- Effectuer la vérification de l'intégrité de sqlite à partir de l'invite de shell bsd :

  ```
  nsshell ## sqlite3 /var/nslog/asl/<profile_name_in_lowercase>.db '
  pragma integrity_check;
  ```

  Exemples :

  ```
  root@ns# sqlite3 /var/nslog/asl/tsk0247284.db 'pragma
     integrity_check;'
  ok
  <!--NeedCopy-->
  ```

- Déployez ou supprimez des règles pour recommencer à apprendre :
  - Si 2000 éléments d'apprentissage (par protection) sont atteints, vous ne pouvez plus commencer à apprendre pour cette protection.

  - Si une taille de 20 Mo est atteinte pour la base de données, arrêtez l'apprentissage pour toutes les protections
  - Redémarrer comme processus d'apprentissage

```
*/netscaler/aslearn -start -f/netscaler/aslearn.conf*
```

- Vérifiez l'espace dans le dossier /var en exécutant ce qui suit :

```
du -h /var
```

- Vérifiez les limites de seuil d'apprentissage en exécutant la commande suivante :

```
show appfwlearningsettings <profile_name> <securityCheck>
```

- Collectez les données apprises en exécutant la commande suivante :

```
export appfwlearningdata <profile_name> <securityCheck>
```

- vérifier que les données apprises sont téléchargées dans le collecteur.

Signatures

January 21, 2021

Prise en main des signatures

Pour ajouter une signature :

1. Sélectionnez la signature **par défaut**et cliquez sur **ajouter**pour en faire une copie.
2. Donnez un nom significatif. Le nouvel objet sig est ajouté en tant qu'objet défini par l'utilisateur.
3. Activez les règles cibles qui correspondent à vos besoins spécifiques.
   - Les règles sont désactivées par défaut.
   - plus de règles nécessitent plus de traitement
4. Configurez les actions :

   Les actions Bloquer et Log sont activées par défaut. Stats est une autre option
5. Définissez la signature à utiliser par votre profil.

Conseils pour l'utilisation des signatures

- Optimisez les frais de traitement en activant uniquement les signatures applicables à la protection de votre application.

- Chaque motif de la règle doit correspondre pour déclencher une correspondance de signature.
- Vous pouvez ajouter vos propres règles personnalisées pour inspecter les requêtes entrantes afin de détecter différents types d'attaques, telles que les attaques par injection SQL ou par script intersite.
- Vous pouvez également ajouter des règles pour inspecter les réponses afin de détecter et de bloquer les fuites d'informations sensibles telles que les numéros de carte de crédit.
- Ajoutez plusieurs conditions de vérification de sécurité pour créer votre propre vérification personnalisée.

Meilleures pratiques d'utilisation des signatures

Voici quelques-unes des meilleures pratiques que vous pouvez suivre lorsque vous rencontrez des problèmes liés à Signatures :

- Vérifiez que la commande import a réussi sur primaire et secondaire.
- Vérifiez que les sorties CLI et GUI sont cohérentes.
- Vérifiez ns.log pour identifier les erreurs lors de l'importation de signature et de la mise à jour automatique.
- Vérifiez si le serveur de noms DNS est configuré correctement.
- Vérifiez l'incompatibilité de la version du schéma.
- Vérifiez si le périphérique n'est pas en mesure d'accéder à l'URL Signature Update hébergée sur AWS pour la mise à jour automatique.
- Vérifiez l'incompatibilité de version entre les signatures par défaut et celles ajoutées par l'utilisateur.
- Vérifiez l'incompatibilité de version entre les objets de signature sur les nœuds principal et secondaire.
- Surveiller l'utilisation élevée du processeur (désactivez la mise à jour automatique pour exclure le problème avec la mise à jour de signature).

Journal de suivi

January 21, 2021

Pour enregistrer les journaux de suivi :

1. Activez le suivi du profil. Vous pouvez utiliser la commande show pour vérifier le paramètre configuré.

```
set appfw profile <profile> -trace ON
```

1. Commencez à collecter la trace. Vous pouvez continuer à utiliser toutes les options applicables à la commande nstrace.

```
start nstrace -mode APPFW
```

1. Arrêter la collecte de la trace

```
stop nstrace
```

Emplacement de la trace : Le nstrace est stocké dans un dossier horodaté qui est créé dans le répertoire */var/nstrace* et peut être consulté à l'aide de wireshark. Vous pouvez suivre le fichier */var/log/ns.log* pour voir les messages de journal fournissant des détails sur l'emplacement de la nouvelle trace.

Avantages des journaux de suivi :

- Isoler le trafic pour un profil spécifique
- Collecter des données pour des demandes spécifiques
- Identifier les réinitialisations ou les abandons
- Afficher le trafic SSL déchiffré : le trafic HTTPS est capturé en texte brut pour faciliter le dépannage.
- Offre une vue complète : permet d'examiner la demande entière au niveau des paquets, de vérifier la charge utile, d'afficher les journaux pour vérifier quelle violation de vérification de sécurité est déclenchée et d'identifier le modèle de correspondance dans la charge utile. Si la charge utile est constituée de données inattendues, de chaînes de courrier indésirable ou de caractères non imprimables (caractère nul, \r ou \n etc), ils sont faciles à découvrir dans la trace.
- Accélérer le temps de réponse : débogage plus rapide sur le trafic cible pour effectuer une analyse des causes premières.

Divers

August 20, 2021

Voici les résolutions de certains des problèmes que vous pouvez rencontrer lors de l'utilisation du Web App Firewall.

- Le Web App Firewall définit la taille de la fenêtre sur 9845 lors de la réinitialisation de la connexion pour les messages http non valides.

— Demande mal formée reçue - réinitialisation de la connexion [Client/Serveur envoyant un en-tête de longueur de contenu non valide]
— Type de contenu inconnu dans les en-têtes de demande

- Limite système : l'application semble gelée

  — Se produit lorsque la limite maximale de session est atteinte. (100 Ko)
  — Moins de mémoire système pour le fonctionnement.

  - La fonctionnalité de réputation IP ne fonctionne pas
    : le processus iprep prend environ cinq minutes après l'activation de la fonction de réputation. La fonctionnalité de réputation IP peut ne pas fonctionner pendant cette durée.

- Violations inattendues Web App Firewall en cours de déclenchement

  — Le délai d'expiration de la session a une valeur par défaut de 900 secondes. Si le délai d'expiration de session est défini sur une valeur faible, le navigateur peut déclencher des faux positifs pour les vérifications qui reposent sur la sessionisation (par exemple CSRF, FFC). Vérifiez le délai d'expiration de session et regardez l'ID de session (cs3 dans les journaux CEF). Si l'ID de session est différent, le délai d'expiration de session peut en être la raison.
  — Si le formulaire est généré dynamiquement par javascript, il peut déclencher de fausses violations FFC.

- Nom de champ vide dans les journaux des violations FFC (avant la version 11.0)

  Cela peut être vu dans des scénarios où nous rencontrons un champ de formulaire qui n'est pas dans les formulaires de notre session.

  Scénarios où cela peut se produire :

  — La session a expiré à partir du moment où le formulaire a été envoyé au client et de sa réception.
  — Le formulaire a été généré côté client à l'aide d'un script java.

Références

May 5, 2023

Reportez-vous aux ressources supplémentaires suivantes pour plus d'informations sur les fonctionnalités du Web App Firewall.

- Comment NetScaler Web App Firewall modifie le trafic de données des applications.
- Suivez les requêtes HTML à l'aide des journaux de violations de sécurité du Web App Firewall sur l'appliance NetScaler
- Protection de haut niveau

- Relaxations de sécurité
- Informations sur la configuration et le déploiement d'une application :
  - Application
  - Pare-feu
  - Journaux
- Articles de mise à jour
- Gestion des bots

Articles relatifs aux alertes de signature

May 5, 2023

NetScaler Web App Firewall (WAF) annonce les mises à jour des signatures que vous pouvez télécharger et appliquer sur votre appliance. Lorsque vous détectez une attaque de sécurité, vous recevez une notification par e-mail concernant la nouvelle mise à jour de la signature. Vous pouvez télécharger la signature et l'appliquer sur votre appliance.

Comment recevoir une notification d'alerte de signature

Cet article explique comment s'abonner à des flux RSS pour recevoir des notifications concernant les nouvelles mises à jour de signatures. Une fois inscrit, vous recevez des flux RSS réguliers chaque fois que de nouvelles signatures sont disponibles au téléchargement.

> **Remarque :**
>
> - Pour obtenir des mises à jour sur les signatures du Web App Firewall, vous devez configurer la fonctionnalité de mise à jour automatique des signatures. Pour plus d'informations, consultez la rubrique Mise à jour automatique des signatures .
> - Pour obtenir des mises à jour sur les nouvelles signatures de bot, vous devez configurer la fonctionnalité de mise à jour automatique des signatures de bot. Pour plus d'informations, consultez la rubrique Mise à jour automatique des signatures de bot .

Pour vous abonner aux flux RSS afin de recevoir les nouvelles mises à jour des signatures, suivez les étapes ci-dessous :

1. Ouvrez la rubrique Historique du document de l'article Signature Alert dans un navigateur Web.
2. En haut à droite de la page, cliquez sur le bouton RSS et copiez l' URL du flux RSS.
3. Ajoutez l' URL du flux RSS copié au lecteur de flux RSS de votre choix.

Mise à jour des signatures pour novembre 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2015-11-2022. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version 97 de signature applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998841	CVE-2022-40043	WEB-MISC Centreon avant la version 22.04.1 - Vulnérabilité d'injection SQL via esc_name (CVE-2022-40043)
998842	CVE-2022-35153	WEB-MISC FusionPBX 5.0.1 et versions antérieures - Vulnérabilité d'injection de commandes du système d'exploitation (CVE-2022-35153)
998843	CVE-2022-3387	WEB-MISC Advantech R-SeeNet avant la version 2.4.21 - Vulnérabilité liée à la traversée de chemins (CVE-2022-3387)

Règle de signature	ID CVE	Description
998844	CVE-2022-3385	WEB-MISC Advantech R-SeeNet avant la version 2.4.21 - Vulnérabilité liée au débordement de la mémoire tampon liée au nom du fichier (CVE-2022-3385)
998845	CVE-2022-31680	WEB-MISC VMware vCenter Server antérieur à 6.5 U3u - Vulnérabilité de désérialisation non sécurisée via PSC (CVE-2022-31680)
998846	CVE-2022-28732	WEB-MISC Apache JSPWiki avant la version 2.11.3 - Vulnérabilité XSS de WeblogPlugin via Weblog.StartDate (CVE-2022-28732)
998847	CVE-2022-28732	WEB-MISC Apache JSPWiki avant la version 2.11.3 - Vulnérabilité XSS dans WeblogPlugin via StartDate (CVE-2022-28732)
998848	CVE-2022-28730	WEB-MISC Apache JSPWiki avant la version 2.11.3 - Vulnérabilité dans AjaxPreview XSS via le plugin Deonce (CVE-2022-28730)
998849	CVE-2022-23463	WEB-MISC Nepxion Discovery - Vulnérabilité liée à l'injection de SPel (CVE-2022-23463)

Mise à jour des signatures pour octobre 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-10-23. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version 96 de signature applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998850	CVE-2022-42889	WEB-MISC Apache Commons Text - Vulnérabilité d'exécution de code à distance via une URL (CVE-2022-42889)
998851	CVE-2022-42889	WEB-MISC Apache Commons Text - Vulnérabilité d'exécution de code à distance via HEADER (CVE-2022-42889)
998852	CVE-2022-42889	WEB-MISC Apache Commons Text - Vulnérabilité d'exécution de code à distance via BODY (CVE-2022-42889)
998853	CVE-2022-42889	WEB-MISC Apache Commons Text - Vulnérabilité d'exécution de code à distance via FORM (CVE-2022-42889)

Règle de signature	ID CVE	Description
998854	CVE-2022-38358	WEB-MISC Eyes of Network - Vulnérabilité XSS via admin_user (CVE-2022-38358)
998855	CVE-2022-38358	WEB-MISC Eyes of Network - Vulnérabilité XSS via admin_notifier (CVE-2022-38358)
998856	CVE-2022-38358	WEB-MISC Eyes of Network - Vulnérabilité XSS via report_event (CVE-2022-38358)
998857	CVE-2022-38257	WEB-MISC Eyes of Network - Vulnérabilité liée à l'injection d'iFrame (CVE-2022-38257)
998858	CVE-2022-36981	WEB-MISC Ivanti Avalanche avant la version 6.3.4 : une vulnérabilité de traversée de chemins permet l'exécution de code à distance (CVE-2022-36981)
998859	CVE-2022-36961	WEB-MISC SolarWinds Orion avant 2022.3 - Vulnérabilité d'injection SQL (CVE-2022-36961)
998860	CVE-2022-36804	WEB-MISC Atlassian Bitbucket Server and Data Center - Vulnérabilité d'exécution de code à distance via Body (CVE-2022-36804)
998861	CVE-2022-36804	WEB-MISC Atlassian Bitbucket Server and Data Center - Vulnérabilité d'exécution de code à distance via une URL (CVE-2022-36804)

Règle de signature	ID CVE	Description
998862	CVE-2022-3323	WEB-MISC Advantech iView 5.7.04.6469 - Vulnérabilité d'injection SQL via l'URI CommandServlet et column_value (CVE-2022-3323)
998863	CVE-2022-3323	WEB-MISC Advantech iView 5.7.04.6469 - Vulnérabilité d'injection SQL via l'URI CommandServlet et le nom de colonne (CVE-2022-3323)
998864	CVE-2022-3323	WEB-MISC Advantech iView 5.7.04.6469 - Vulnérabilité d'injection SQL via l'URI et column_value de ConfigurationServlet (CVE-2022-3323)
998865	CVE-2022-3323	WEB-MISC Advantech iView 5.7.04.6469 - Vulnérabilité d'injection SQL via l'URI et le nom de colonne de colonne de ConfigurationServlet (CVE-2022-3323)
998866	CVE-2022-29548	WEB-MISC WSO2 Multiple products - Vulnérabilité XSS due à un faux état de connexion (CVE-2022-29548)
998867	CVE-2022-29548	WEB-MISC WSO2 Multiple Products - Vulnérabilité XSS due à un échec de connexion (CVE-2022-29548)

Règle de signature	ID CVE	Description
998868	CVE-2022-2142	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité d'injection SQL de second ordre via CommandServlet (CVE-2022-2142)
998869	CVE-2022-2142	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité d'injection SQL de second ordre via NetworkServlet (CVE-2022-2142)
998870	CVE-2022-0666	Microweber WEB-MISC antérieur à 1.2.11 - Vulnérabilité d'injection CRLF (CVE-2022-0666)

Mise à jour des signatures pour octobre 2022

May 5, 2023

Des règles de signatures modifiées sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-10-07. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version 95 de signature applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
811	CVE-2000-0066	Accès par chemin d'accès au site WEB-CGI
1029	NESSUS-11032	Accès à la navigation par scripts WEB-IIS
1047	CVE-2001-0251	WEB-MISC Netscape Enterprise DOS
1048	CVE-2001-0250	Tentative d'inscription à l'annuaire WEB-MISC Netscape
1663	NESSUS-11007	Accès WEB-MISC *%20.pl
1725	CVE-2000-0630, CVE-2001-0004	Tentative de fragment de code WEB-IIS+.ht
16521	CVE-2009-0478	CLIENT WEB : tentative de dépassement du numéro de version http de Squid Proxy

Mise à jour des signatures pour octobre 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-10-06. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 94 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le

> processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998871	CVE-2022-41082, CVE-2022-41040	WEB-MISC Microsoft Exchange Server - Vulnérabilité RCE (CVE-2022-41082, CVE-2022-41040)

Mise à jour des signatures pour octobre 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-10-02. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version 93 de signature applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998871	CVE-2022-41082, CVE-2022-41040	WEB-MISC Microsoft Exchange Server - Vulnérabilité RCE (CVE-2022-41082, CVE-2022-41040)
998872	CVE-2022-37299	WEB-MISC Shirne CMS 1.2.0 - Vulnérabilité de traversée de chemin via /static/ueditor/php/controller.php (CVE-2022-37299)
998873	CVE-2022-36923	WEB-MISC Zoho ManageEngine Multiple Products Multiple Versions — Vulnérabilité de contournement de l'authentification (CVE-2022-36923)
998874	CVE-2022-33891	WEB-MISC Interface utilisateur Apache Spark, versions multiples - Vulnérabilité d'exécution de code à distance via un paramètre DoAS (CVE-2022-33891)
998875	CVE-2022-3184, CVE-2022-3183	WEB-MISC DataProbe iBoot-PDU antérieur au 1.42.06162022 - Vulnérabilité d'exécution de code à distance (CVE-2022-3184, CVE-2022-3183)
998876	CVE-2022-31814	WEB-MISC pfSense pfBlockerNG antérieur à 2.1.4_26 - Vulnérabilité d'exécution de code à distance (CVE-2022-31814)

Règle de signature	ID CVE	Description
998877	CVE-2022-31097	WEB-MISC Apache Grafana - Vulnérabilité XSS stockée liée aux alertes unifiées (CVE-2022-31097)
998878	CVE-2022-2903	Plugin WEB-WORDPRESS NinjaForms antérieur à 3.6.13 - Vulnérabilité d'injection d'objets PHP (CVE-2022-2903)
998879	CVE-2022-2552	Plug-in WEB-WORDPRESS Duplicator antérieur à 1.4.7.1 - Vulnérabilité de divulgation d'informations non authentifiées (CVE-2022-2552)
998880	CVE-2022-23854	WEB-MISC AVEVA InTouch Access Anywhere Secure Gateway - Vulnérabilité de traversée de chemin via une URI SG (CVE-2022-23854)
998881	CVE-2022-23854	WEB-MISC AVEVA InTouch Access Anywhere Secure Gateway - Vulnérabilité de traversée de chemin via Blaze URI (CVE-2022-23854)
998882	CVE-2022-23854	WEB-MISC AVEVA InTouch Access Anywhere Secure Gateway - Vulnérabilité de traversée de chemin via l'URI AccessAnywhere (CVE-2022-23854)

Règle de signature	ID CVE	Description
998883	CVE-2017-9841	WEB-MISC PHPUnit avant 4.8.28 et 5.x avant 5.6.3 - Vulnérabilité d'exécution de code à distance via eval-stdin.php (CVE-2017-9841)

Règles de signature consolidées et mises à jour

Quelques règles de signature redondantes sont supprimées et les identifiants CVE de ces règles sont consolidés dans les règles mises à jour. Assurez-vous d'activer les règles de signature correspondantes pour chaque règle supprimée.

Le tableau suivant répertorie les ID de règles de signature consolidés et mis à jour :

Règles de signature supprimées	Règles de signature mises à jour	ID CVE
1242	1243	CVE-2000-0071
1245	1244	CVE-2000-0071
1589	1221	CVE-2001-0224, NESSUS-10609
1648	832	CVE-1999-0509, NESSUS-10173, www.cert.org/advisories/CA-1996-11.html
1700	821	CVE-1999-0951, NESSUS-10122
2598	2597	CVE-2004-0600
999779	999721	CVE-2019-14994
999861	999859	CVE-2019-12099

Règles de signature supprimées	Règles de signature mises à jour	ID CVE
999862	999857	https://www.wordfence.com/blog/2019/05s-command-injection-vulnerability-patched-in-wp-database-backup-plugin/
999863	999858	https://www.wordfence.com/blog/2019/05/privilege-escalation-flaw-present-in-slick-popup-plugin/

Mise à jour des signatures pour septembre 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-09-22. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version 92 de signature applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998884	CVE-2022-38130	WEB-MISC Keysight SMS antérieur à la version 2.4.1 : une vulnérabilité liée au téléchargement arbitraire de fichiers permet l'injection de code SQL (CVE-2022-38130)
998885	CVE-2022-35741	WEB-MISC Apache Cloudstack antérieur à la version 4.16.1.1 - Vulnérabilité liée à l'injection d'entités externes XML via SamlResponse (CVE-2022-35741)
998886	CVE-2022-35650	Versions multiples de WEB-MISC Moodle - Vulnérabilité liée à la traversée de chemins via Blackboard Questions (CVE-2022-35650)
998887	CVE-2022-32551	WEB-MISC Zoho ManageEngine ServiceDesk MSP antérieur à 10604 - Divulgation d'informations non authentifiées via /WEB-INF (CVE-2022-32551)
998888	CVE-2022-31675	WEB-MISC VMware vRealize Operations Manager - Vulnérabilité de contournement de l'authentification (CVE-2022-31675)
998889	CVE-2022-31674	WEB-MISC VMware vRealize Operations Manager - Vulnérabilité liée à la divulgation d'informations (CVE-2022-31674)

Règle de signature	ID CVE	Description
998890	CVE-2022-31656	WEB-MISC VMware Workspace ONE Access - Vulnérabilité de contournement de l'authentification (CVE-2022-31656)
998891	CVE-2022-31474	Plugin WEBWORDPRESS BackupBuddy antérieur à la version 8.7.5 - Divulgation d'informations via backup-buddy_local_download (CVE-2022-31474)
998892	CVE-2022-31137, CVE-2022-31126	WEB-MISC Roxy-WI avant la version 6.1.1.0 - Vulnérabilités d'injection de commandes multiples (CVE-2022-31137, CVE-2022-31126)
998893	CVE-2022-28731	WEB-MISC Apache JSPWiki antérieur à la version 2.11.3 - Vulnérabilité de falsification de requêtes côté serveur (CVE-2022-28731)
998894	CVE-2022-2551	Plug-in WEB-WORDPRESS Duplicator antérieur à 1.4.7.1 - Vulnérabilité de téléchargement de sauvegarde non authentifiée (CVE-2022-2551)
998895	CVE-2022-2546	Plugin de migration WP tout-en-un WEB-WORDPRESS antérieur à la version 7.63 - Vulnérabilité XSS reflétée via ai1wm_export (CVE-2022-2546)

Règle de signature	ID CVE	Description
998896	CVE-2022-2546	Plugin de migration WP tout-en-un WEB-WORDPRESS antérieur à la version 7.63 - Vulnérabilité XSS reflétée via ai1wm_import (CVE-2022-2546)
998897	CVE-2022-24948	WEB-MISC Apache JSPWiki antérieur à 2.11.2 - Vulnérabilité XSS (CVE-2022-24948)
998898	CVE-2022-2139	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité de traversée de chemins via l'URI et la page MenuServlet (CVE-2022-2139)
998899	CVE-2022-2139	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité de traversée de chemins via l'URI et la page CommandServlet (CVE-2022-2139)
998900	CVE-2022-2139	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité de traversée de chemin via l'URI et le nom de fichier CommandServlet (CVE-2022-2139)
998901	CVE-2022-2139	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité de traversée de chemin via l'URI et le nom de fichier NetworkServlet (CVE-2022-2139)

Règle de signature	ID CVE	Description
998902	CVE-2022-0817	Plugin WEB-WORDPRESS BadgeOS antérieur à la version 3.7.1 - Vulnérabilité SQLi via des résultats obtenus et des exclusions (CVE-2022-0817)
998903	CVE-2022-0817	Plugin WEB-WORDPRESS BadgeOS antérieur à 3.7.1 - Vulnérabilité SQLi due à l'obtention de résultats obtenus et à l'inclusion (CVE-2022-0817)
998904	CVE-2022-0817	Plugin WEB-WORDPRESS BadgeOS antérieur à la version 3.7.1 - Vulnérabilité SQLi liée aux résultats obtenus et à la commande (CVE-2022-0817)
998905	CVE-2022-0817	Plugin WEB-WORDPRESS BadgeOS antérieur à 3.7.1 - Vulnérabilité SQLi via get-earned-achievements et orderby (CVE-2022-0817)
998906	CVE-2022-0817	Plugin WEB-WORDPRESS BadgeOS antérieur à la version 3.7.1 - Vulnérabilité SQLi via les résultats obtenus et l'offset (CVE-2022-0817)
998907	CVE-2022-0817	Plugin WEB-WORDPRESS BadgeOS antérieur à la version 3.7.1 - Vulnérabilité SQLi via les résultats obtenus et la limite (CVE-2022-0817)

Règle de signature	ID CVE	Description
998908	CVE-2018-20062, CVE-2019-9082	WEB-MISC ThinkPHP 5.x antérieur à 5.1.32 - Vulnérabilité d'exécution de code à distance non authentifiée (CVE-2018-20062, CVE-2019-9082)

Mise à jour des signatures pour août 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-08-23. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 91 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998909	CVE-2022-38129	WEB-MISC Keysight SMS antérieur à 2.4.1 - Une vulnérabilité de traversée de chemin autorise le RCE (CVE-2022-38129)

Règle de signature	ID CVE	Description
998910	CVE-2022-37042, CVE-2022-27925	WEB-MISC Zimbra Collaboration Suite - Multiples vulnérabilités dans MailboxImportServlet (CVE-2022-37042, CVE-2022-27925)
998911	CVE-2022-36446	WEB-MISC Webmin Multiple Versions - Vulnérabilités d'injection HTML et d'exécution de code à distance (CVE-2022-36446)
998912	CVE-2022-35405	WEB-MISC Zoho ManageEngine Password Manager Pro antérieur à 12101 - Vulnérabilité de désérialisation dans Java (CVE-2022-35405)
998913	CVE-2022-34872	WEB-MISC Centreon antérieur à 21.10.7 - Vulnérabilité d'injection SQL via vhidden (CVE-2022-34872)
998914	CVE-2022-34872	WEB-MISC Centreon antérieur à 21.10.7 - Vulnérabilité d'injection SQL via rpn_function (CVE-2022-34872)
998915	CVE-2022-34872	WEB-MISC Centreon antérieur à 21.10.7 - Vulnérabilité d'injection SQL via unit_name (CVE-2022-34872)
998916	CVE-2022-34872	WEB-MISC Centreon antérieur à 21.10.7 - Vulnérabilité d'injection SQL via warn (CVE-2022-34872)

Règle de signature	ID CVE	Description
998917	CVE-2022-34872	WEB-MISC Centreon antérieur à 21.10.7 - Vulnérabilité d'injection SQL via crit (CVE-2022-34872)
998918	CVE-2022-34872	WEB-MISC Centreon antérieur à 21.10.7 - Vulnérabilité d'injection SQL via def_type (CVE-2022-34872)
998919	CVE-2022-31813	WEB-MISC Apache HTTP Server jusqu'à 2.4.53 - Vulnérabilité de suppression des en-têtes X-Forwarded-* dans mod_proxy (CVE-2022-31813)
998920	CVE-2022-31125	WEB-MISC Roxy-WI antérieur à 6.1.1.0 - Vulnérabilité de contournement de l'authentification via alert_consumer (CVE-2022-31125)
998921	CVE-2022-31101	WEB-MISC Prestashop Blockwishlist antérieure à 2.1.1 — Vulnérabilité d'injection SQL (CVE-2022-31101)
998922	CVE-2022-26137	WEB-MISC Plusieurs versions des produits Atlassian - Vulnérabilité de contournement du partage de ressources entre origines multiples (CVE-2022-26137)

Règle de signature	ID CVE	Description
998923	CVE-2022-24299	WEB-MISC pfSense CE antérieur à 2.6.0 - Vulnérabilité d'exécution de code à distance via vpn_openvpn_client.php (CVE-2022-24299)
998924	CVE-2022-24299	WEB-MISC pfSense CE antérieur à 2.6.0 - Vulnérabilité d'exécution de code à distance via vpn_openvpn_server.php (CVE-2022-24299)
998925	CVE-2022-0817	Plugin WEB-WORDPRESS BadgeOS antérieur à la version 3.7.1 — Vulnérabilité d'injection SQL via get-achievements et user_id (CVE-2022-0817)
998926	CVE-2021-36749	WEB-MISC Apache Druid — Vulnérabilité de divulgation de fichiers locaux arbitraires (CVE-2021-36749)
998927	CVE-2021-26919	WEB-MISC Apache Druid antérieur à 0.20.2 - Vulnérabilité de désérialisation non fiable via AutoDeserialize=true (CVE-2021-26919)
998928	CVE-2021-26919	WEB-MISC Apache Druid antérieur à la version 0.20.2 : vulnérabilité de désérialisation non fiable via DetectCustomCollations=true (CVE-2021-26919)

Mise à jour de la signature pour juillet 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-07-30. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version 90 de signature applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998929	CVE-2022-34871	WEB-MISC Centreon antérieur à 21.10.6 - Vulnérabilité d'injection SQL (CVE-2022-34871)
998930	CVE-2022-29846	WEB-MISC En cours Ipswitch WhatsUp Gold — Vulnérabilité de divulgation d'informations (CVE-2022-29846)
998931	CVE-2022-29845	WEB-MISC En cours Ipswitch WhatsUp Gold - Vulnérabilité de traversée de chemins (CVE-2022-29845)
998932	CVE-2022-28055	WEB-MISC FusionPBX antérieur à 5.0.1 - Vulnérabilité d'exécution de code à distance (CVE-2022-28055)

Règle de signature	ID CVE	Description
998933	CVE-2022-26138	WEB-MISC Questions Atlassian pour l'application Confluence - Vulnérabilité des informations d'identification codées en dur via l'API REST (CVE-2022-26138)
998934	CVE-2022-26138	WEB-MISC Questions Atlassian pour l'application Confluence - Vulnérabilité des informations d'identification codées en dur via le formulaire de connexion (CVE-2022-26138)
998935	CVE-2022-26135	WEB-MISC Jira Server and Data Center - Vulnérabilité de falsification de requête côté serveur de plug-in mobile (CVE-2022-26135)
998936	CVE-2022-21445	WEB-MISC Oracle OBIEE ADF Faces - Vulnérabilité de désérialisation de données non fiables (CVE-2022-21445)
998937	CVE-2022-2143	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité RCE via l'URI NetworkServlet et le nom de fichier fwfilename (CVE-2022-2143)
998938	CVE-2022-2143	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité RCE via l'URI CommandServlet et le nom de fichier fwfilename (CVE-2022-2143)

Règle de signature	ID CVE	Description
998939	CVE-2022-2143	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité RCE via l'URI NetworkServlet et backup_filename (CVE-2022-2143)
998940	CVE-2022-2143	WEB-MISC Advantech iView antérieur à 5.7.04.6469 - Vulnérabilité RCE via l'URI CommandServlet et backup_filename (CVE-2022-2143)
998941	CVE-2022-2099	Plugin WooCommerce WEB-WORDPRESS antérieur à 6.6.0 - Vulnérabilité d'injection HTML dans la passerelle de paiement (CVE-2022-2099)

Mise à jour de la signature pour juillet 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-07-08. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 89 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998942	CVE-2022-32532	WEB-MISC Apache Shiro antérieur à 1.9.1 - Vulnérabilité de contournement de RegexRequestMatcher via un saut de ligne (CVE-2022-32532)
998943	CVE-2022-32532	WEB-MISC Apache Shiro antérieur à 1.9.1 - Vulnérabilité de contournement de RegexRequestMatcher via le retour chariot (CVE-2022-32532)
998944	CVE-2022-30157	WEB-MISC Microsoft SharePoint - Vulnérabilité RCE via la désérialisation de données non fiables (CVE-2022-30157)
998945	CVE-2022-29847	WEB-MISC En cours Ipswitch WhatsUp Gold - Vulnérabilité de falsification de requêtes côté serveur non authentifiées (CVE-2022-29847)
998946	CVE-2022-29535	WEB-MISC Zoho ManageEngine OpManager Multiple Versions - Vulnérabilité d'injection SQL via bview (CVE-2022-29535)

Règle de signature	ID CVE	Description
998947	CVE-2022-29535	WEB-MISC Zoho ManageEngine OpManager Multiple Versions - Vulnérabilité d'injection SQL par catégorie (CVE-2022-29535)
998948	CVE-2022-28219	WEB-MISC Zoho ManageEngine AdAudit Plus antérieur à 7060 - Vulnérabilité d'exécution de code à distance (CVE-2022-28219)
998949	CVE-2022-28219	WEB-MISC Zoho ManageEngine AdAudit Plus antérieur à 7060 - Vulnérabilité d'injection XXE via un nouveau contenu de tâche (CVE-2022-28219)
998950	CVE-2022-28219	WEB-MISC Zoho ManageEngine AdAudit Plus antérieur à 7060 - Vulnérabilité d'injection XXE via le contenu des tâches (CVE-2022-28219)
998951	CVE-2022-23642	WEB-MISC Sourcegraph antérieur à 3.37 - Vulnérabilité d'exécution de code à distance dans le service gitserver (CVE-2022-23642)
998952	CVE-2022-23206	WEB-MISC Apache Traffic Control Traffic Control Traffic Ops antérieures aux versions 5.1.6 et 6.1.0 : vulnérabilité SSRF (CVE-2022-23206)

Règle de signature	ID CVE	Description
998953	CVE-2022-1609	Plugin WEB-WORDPRESS Weblizar School Management Pro antérieur à la version 9.9.7 - Vulnérabilité d'exécution de code à distance (CVE-2022-1609)
998954	CVE-2022-1209	Plugin WordPress WEB-WORDPRESS Ultimate Member avant 2.3.2 — Vulnérabilité de redirection ouverte (CVE-2022-1209)
998955	CVE-2021-46360	WEB-MISC Composr-CMS - Vulnérabilité d'exécution de code à distance (CVE-2021-46360)
998956	CVE-2021-43350	WEB-MISC Apache Traffic Control Traffic Control Traffic Ops antérieures à 5.1.4 et 6.0.1 : vulnérabilité d'injection LDAP (CVE-2021-43350)
998957	CVE-2017-9248	Interface utilisateur WEB-MISC Telerik pour ASP.NET AJAX avant R2 2017 SP1 - Vulnérabilité de divulgation de clé de chiffrement (CVE-2017-9248)

Mise à jour de la signature pour juin 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-06-16. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 88 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998958	CVE-2022-28810	WEB-MISC Zoho ManageEngine AdSelfService antérieur à 6122 - Vulnérabilité d'injection de commandes du système d'exploitation via le script UNLOCK (CVE-2022-28810)
998959	CVE-2022-28810	WEB-MISC Zoho ManageEngine AdSelfService antérieur à 6122 - Vulnérabilité d'injection de commandes du système d'exploitation via le script RESET (CVE-2022-28810)
998960	CVE-2022-25237	WEB-MISC Bonita Web antérieur à 7.14.0 - Vulnérabilité de contournement d'autorisation via i18ntranslation/../(CVE-2022-25237)

Règle de signature	ID CVE	Description
998961	CVE-2022-25237	WEB-MISC Bonita Web antérieur à 7.14.0 - Vulnérabilité de contournement d'autorisation via ; i18ntranslation (CVE-2022-25237)
998962	CVE-2022-0540	WEB-MISC Atlassian Jira Server and Data Center - Vulnérabilité de contournement de l'authentification dans Jira Seraph (CVE-2022-0540)
998963	CVE-2021-44548	WEB-MISC Apache Solr antérieur à 8.11.1 - Vulnérabilité des attaques SMB DataImportHandler (CVE-2021-44548)

Mise à jour de la signature pour juin 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 07/06/2022. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 87 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998964	CVE-2022-30525	WEB-MISC Zyxel Firewalls Multiple Versions - Vulnérabilité d'injection de commande de système d'exploitation non authentifiée dans SetWanPortst (CVE-2022-30525)
998965	CVE-2022-29108	WEB-MISC Microsoft SharePoint - Vulnérabilité liée à la désérialisation de données non fiables (CVE-2022-29108)
998966	CVE-2022-26134	WEB-MISC Atlassian Confluence Multiple Versions - Vulnérabilité d'injection OGNL non authentifiée (CVE-2022-26134)
998967	CVE-2022-26019	WEB-MISC pfSense CE < 2.6.0 - Vulnérabilité d'exécution de code à distance via services_ntpd_gps.php et gpsport (CVE-2022-26019)
998968	CVE-2022-26019	WEB-MISC pfSense CE < 2.6.0 - Vulnérabilité d'exécution de code à distance via services_ntpd.php et gpsport (CVE-2022-26019)
998969	CVE-2022-24288	WEB-MISC Apache Airflow jusqu'à 2.2.3 - Exemple de vulnérabilité d'exécution de code à distance DAG via my_param (CVE-2022-24288)

Règle de signature	ID CVE	Description
998970	CVE-2022-24288	WEB-MISC Apache Airflow jusqu'à 2.2.3 - Exemple de vulnérabilité d'exécution de code à distance DAG via foo ou miff (CVE-2022-24288)
998971	CVE-2022-22978	WEB-MISC Spring Security jusqu'à 5.5.6 et 5.6.3 - Vulnérabilité de contournement de RegexRequestMatcher via un saut de ligne (CVE-2022-22978)
998972	CVE-2022-22978	WEB-MISC Spring Security jusqu'à 5.5.6 et 5.6.3 - Vulnérabilité de contournement de RegexRequestMatcher via Carriage Return (CVE-2022-22978)
998973	CVE-2022-22957	WEB-MISC Produits multiples VMware - Vulnérabilité d'exécution de code à distance (CVE-2022-22957)
998974	CVE-2021-45232	WEB-MISC Tableau de bord Apache APISIX antérieur à la version 2.10.1 - Vulnérabilité de contournement de l'authentification via l'exportation (CVE-2021-45232)

Règle de signature	ID CVE	Description
998975	CVE-2021-45232	WEB-MISC Tableau de bord Apache APISIX antérieur à la version 2.10.1 - Vulnérabilité de contournement de l'authentification via l'importation (CVE-2021-45232)
998976	CVE-2021-41739	WEB-MISC Artica Proxy - Vulnérabilité d'injection de commande de système d'exploitation via cyrus.events.php (CVE-2021-41739)
998977	CVE-2021-37927	WEB-MISC ManageEngine AdManager Plus antérieur à 7111 - Vulnérabilité de contournement de l'authentification (CVE-2021-37927)
998978	CVE-2021-36356	WEB-MISC Kramer VIA VSM Server - Vulnérabilité d'exécution de code à distance non authentifiée dans WriteBrowseFilePathAjax (CVE-2021-36356)
998979	CVE-2021-25094	Plugin WEB-WORDPRESS Tatsu Builder avant la version 3.3.12 - Vulnérabilité d'exécution de code à distance (CVE-2021-25094)

Mise à jour des signatures pour mai 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 20/05/2022. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 86 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998980	CVE-2022-30525	WEB-MISC Zyxel Firewalls Multiple Versions - Vulnérabilité d'injection de commande de système d'exploitation non authentifiée dans SetWanPortst (CVE-2022-30525)
998981	CVE-2021-25094	Plugin WEB-WORDPRESS Tatsu Builder avant la version 3.3.12 - Vulnérabilité d'exécution de code à distance (CVE-2021-25094)

Mise à jour des signatures pour mai 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-05-13. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 85 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998982	CVE-2022-26352	WEB-MISC DotCMS - Vulnérabilité de téléchargement arbitraire de fichiers via PUT (CVE-2022-26352)
998983	CVE-2022-26352	WEB-MISC DotCMS - Vulnérabilité de téléchargement arbitraire de fichiers via POST (CVE-2022-26352)
998984	CVE-2022-1388	WEB-MISC F5 BIG-IP - Vulnérabilité de contournement de l'authentification REST iControl (CVE-2022-1388)

Règle de signature	ID CVE	Description
998985	CVE-2022-1162	WEB-MISC Gitlab CE/EE Multiple Versions - Vulnérabilité d'identification codée en dur (CVE-2022-1162)
998986	CVE-2022-0888	WEB-WORDPRESS Plugin Ninja Forms Chargements de fichiers antérieurs à la version 3.3.1 - Vulnérabilité de téléchargement arbitraire de fichiers (CVE-2022-0888)
998987	CVE-2021-35244	WEB-MISC SolarWinds Orion avant 2020.2.6 HF3 - Vulnérabilité de chargement arbitraire de fichiers via l'action WriteToFile (CVE-2021-35244)

Mise à jour des signatures pour mai 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-05-08. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 84 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998988	CVE-2022-26986	WEB-MISC ImpressCMS avant la version 1.4.3 - Vulnérabilité d'injection SQL via mimetypeid (CVE-2022-26986)
998989	CVE-2022-24112	WEB-MISC Module externe de requêtes par lots pour Apache APISIX - Vulnérabilité de contournement de restriction IP (CVE-2022-24112)
998990	CVE-2021-37558	WEB-MISC Centreon avant les 20.04.14, 20.10.8 et 21.04.2 - Vulnérabilité d'injection SQL via service_description (CVE-2021-37558)
998991	CVE-2021-37558	WEB-MISC Centreon avant les 20.04.14, 20.10.8 et 21.04.2 - Vulnérabilité d'injection SQL via host_name (CVE-2021-37558)
998992	CVE-2021-22056	WEB-MISC Vulnérabilité liée à la falsification de requête côté serveur dans VMware Workspace ONE Access and Identity Manager (CVE-2021-22056)

Mise à jour des signatures pour mai 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la se-

maine 04/05/2022. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 83 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998993	CVE-2022-29464	WEB-MISC WSO2 Multiple Products - Vulnérabilité de chargement de fichiers sans restriction (CVE-2022-29464)
998994	CVE-2022-22954	WEB-MISC VMware Workspace ONE Access and Identity Manager - Vulnérabilité d'exécution de code à distance via DeviceType (CVE-2022-22954)
998995	CVE-2022-22954	WEB-MISC VMware Workspace ONE Access and Identity Manager - Vulnérabilité d'exécution de code à distance via DeviceUDID (CVE-2022-22954)

Règle de signature	ID CVE	Description
998996	CVE-2022-1329	WEB-WORDPRESS WordPress Elementor Website Builder avant la version 3.6.3 - Vulnérabilité liée à une action AJAX non autorisée (CVE-2022-1329)

Mise à jour des signatures pour avril 2022

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-04-23. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 82 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
998997	CVE-2022-27924	WEB-MISC Zimbra Collaboration Joule - Vulnérabilité d'empoisonnement du cache (CVE-2022-27924)

Règle de signature	ID CVE	Description
998998	CVE-2022-21907	WEB-MISC Microsoft HTTP Protocol Stack - Vulnérabilité d'exécution de code à distance (CVE-2022-21907)
998999	CVE-2021-37930	WEB-MISC ManageEngine AdManager Plus avant 7111 - Vulnérabilité de téléchargement arbitraire de fichiers via SM_domainName (CVE-2021-37930)
999000	CVE-2021-37930	WEB-MISC ManageEngine AdManager Plus avant 7111 - Vulnérabilité de chargement arbitraire de fichiers via SM_OperationId (CVE-2021-37930)

Mise à jour des signatures pour avril 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-04-08. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 81 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999001	CVE-2022-0479	Plugin de création de fenêtres contextuelles WEB-WORDPRESS antérieur à 4.1.1 - Vulnérabilité d'injection SQL (CVE-2022-0479)
999002	CVE-2021-36393	WEB-MISC Moodle antérieur à 3.11.1 - Vulnérabilité liée à l'injection SQL (CVE-2021-36393)
999003	CVE-2021-26599	WEB-MISC ImpressCMS avant 1.4.3 - Vulnérabilité liée à l'injection SQL (CVE-2021-26599)

Mise à jour des signatures pour avril 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 04/04/2022. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version 80 de signature applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999004	CVE-2022-22965	WEB-MISC Spring4Shell Spring Core Framework - Vulnérabilité RCE (CVE-2022-22965)

Mise à jour de signatures pour mars 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-03-29. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques vulnérables à la sécurité.

Version de signature

Version de signature 79 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
18959 (règle mise à jour)	CVE-2022-22965	WEB-MISC VMware Spring4Shell, SpringSource Spring Framework class.classloader tentative RCE

Règle de signature	ID CVE	Description
999005	CVE-2022-22963	Fonction Spring Cloud WEB-MISC - Vulnérabilité d'injection de code (CVE-2022-22963)

Mise à jour de signatures pour mars 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-03-29. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques vulnérables à la sécurité.

Version de signature

Signature version 78 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999006		WEB-MISC Zabbix Plusieurs versions - Vulnérabilité d'exécution de code à distance via items.php
999007	CVE-2022-24266	WEB-MISC Cuppa CMS v1.0 - Vulnérabilité d'injection SQL via order_orientation (CVE-2022-24266)

Règle de signature	ID CVE	Description
999008	CVE-2022-24266	WEB-MISC Cuppa CMS v1.0 - Vulnérabilité d'injection SQL via order_by (CVE-2022-24266)
999009	CVE-2022-22005	WEB-MISC Microsoft SharePoint - RCE via la désérialisation d'une vulnérabilité de données non fiables (CVE-2022-22005)
999010	CVE-2022-21705	WEB-MISC OctoberCMS avant les versions 474 et 1.1.10 - Vulnérabilité d'exécution de code à distance (CVE-2022-21705)
999011	CVE-2022-0557	WEB-MISC Microweber avant 1.2.11 - Vulnérabilité d'exécution de code à distance (CVE-2022-0557)
999012	CVE-2022-0513	Plugin de statistiques WEB-WORDPRESS WP antérieur à la version 13.1.5 - Vulnérabilité d'injection SQL aveugle (CVE-2022-0513)
999013	CVE-2022-0332	WEB-MISC Moodle 3.11.0 à 3.11.4 - Vulnérabilité d'injection SQL liée à l'activité H5P (CVE-2022-0332)
999014	CVE-2021-46088	WEB-MISC Plusieurs versions de Zabbix - Vulnérabilité d'exécution de code à distance (CVE-2021-46088)
999015	CVE-2021-43789	WEB-MISC PrestaShop avant 1.7.8.2 - Vulnérabilité d'injection SQL via SortOrder (CVE-2021-43789)

Règle de signature	ID CVE	Description
999016	CVE-2021-43789	WEB-MISC PrestaShop antérieur à 1.7.8.2 - Vulnérabilité d'injection SQL via OrderBy (CVE-2021-43789)
999017	CVE-2021-43408	Plugin de publication en double WEB-WORDPRESS antérieur à 1.1.9 - Vulnérabilité d'injection SQL (CVE-2021-43408)
999018	CVE-2021-43319	WEB-MISC Zoho ManageEngine NCM antérieur à 125488 - Vulnérabilité d'injection de commande du système d'exploitation (CVE-2021-43319)
999019	CVE-2021-41282	WEB-MISC pfSense 2.5.2 - Vulnérabilité d'exécution de code à distance (CVE-2021-41282)
999020	CVE-2021-39115, CVE-2021-43947	WEB-MISC Serveur et centre de données Atlassian Jira - Vulnérabilité d'injection de modèles côté serveur (CVE-2021-39115, CVE-2021-43947)
999021	CVE-2021-38452	WEB-MISC Gestion du réseau Moxa MxView avant 3.2.2 - Vulnérabilité de traversée de chemin (CVE-2021-38452)
999022	CVE-2021-37918	WEB-MISC Zoho ManageEngine AdManager Plus avant 7111 - Vulnérabilité de traversée de chemin via DomainName (CVE-2021-37918)

Règle de signature	ID CVE	Description
999023	CVE-2021-37918	WEB-MISC Zoho ManageEngine AdManager Plus avant 7111 - Vulnérabilité de traversée de chemin via BM_OperationId (CVE-2021-37918)
999024	CVE-2021-37918	WEB-MISC Zoho ManageEngine AdManager Plus antérieur à 7111 - Vulnérabilité liée au téléchargement de fichiers arbitraires dans RCE (CVE-2021-37918)
999025	CVE-2021-32649	WEB-MISC OctoberCMS avant les versions 473 et 1.1.6 - Vulnérabilité d'exécution de code à distance via Twig (CVE-2021-32649)
999026	CVE-2021-32648	WEB-MISC OctoberCMS avant la version 472 et v1.1.5 - Vulnérabilité de réinitialisation de mot de passe (CVE-2021-32648)
999027	CVE-2021-32099, CVE-2020-26518	WEB-MISC Artica Pandora avant 743 - Vulnérabilité d'injection SQL via chart_generator (CVE-2021-32099, CVE-2020-26518)
999028	CVE-2021-32098	WEB-MISC Artica Pandora avant 743 - Vulnérabilité de désérialisation Phar via Progressbubble (CVE-2021-32098)

Règle de signature	ID CVE	Description
999029	CVE-2021-32098	WEB-MISC Artica Pandora avant 743 - Vulnérabilité de désérialisation Phar via la barre de progression (CVE-2021-32098)
999030	CVE-2021-30149	WEB-MISC Composr 10.0.36 - Vulnérabilité d'exécution de code à distance (CVE-2021-30149)
999031	CVE-2021-25114	Plugin Pro pour les adhésions payantes WEB-WORDPRESS avant 2.6.7 - Vulnérabilité SQLi via rest_route et discount_code (CVE-2021-25114)
999032	CVE-2021-25114	Plugin Pro pour les adhésions payantes WEB-WORDPRESS avant 2.6.7 - Vulnérabilité SQLi via wp-json et discount_code (CVE-2021-25114)
999033	CVE-2021-21984	WEB-MISC VMware vRealize Business for Cloud 7.x antérieur à 7.6.0 - Vulnérabilité d'exécution de code à distance (CVE-2021-21984)

Mise à jour des signatures pour février 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-02-25. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Signature version 77 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1, NetScaler 13.0, NetScaler 13.1.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999034		WEB-WORDPRESS WordPress 5.9 - Vulnérabilité XSS stockée via un extrait de page dans un objet Json
999035		WEB-WORDPRESS WordPress 5.9 - Vulnérabilité XSS stockée via un extrait de page dans le formulaire
999036		WEB-WORDPRESS WordPress 5.9 - Vulnérabilité XSS stockée via post.php
999037		WEB-WORDPRESS WordPress 5.9 - Vulnérabilité XSS stockée via un extrait de post dans un objet Json
999038		WEB-WORDPRESS WordPress 5.9 - Vulnérabilité XSS stockée via un extrait de post dans le formulaire
999039		Vulnérabilité de traversée de chemin WEB-MISC via les valeurs des champs de formulaire

Règle de signature	ID CVE	Description
999040		Vulnérabilité liée à la traversée de chemin WEB-MISC via URI
999041	CVE-2022-23221	Console WEB-MISC H2 avant 2.1.210 - Vulnérabilité d'exécution de code à distance via test.do (CVE-2022-23221)
999042	CVE-2022-23221	Console WEB-MISC H2 avant 2.1.210 - Vulnérabilité d'exécution de code à distance via login.do (CVE-2022-23221)
999043	CVE-2022-21662	WEB-WORDPRESS WordPress avant 5.8.3 - Vulnérabilité de script intersite stocké (CVE-2022-21662)
999044	CVE-2022-0320	WEB-WORDPRESS Les addons essentiels pour le plugin Elementor avant 5.0.5 - LFI Via eael_product_gallery (CVE-2022-0320)
999045	CVE-2022-0320	WEB-WORDPRESS Les addons essentiels pour le plugin Elementor avant 5.0.5 - LFI Via woo_product_pagination_product (CVE-2022-0320)
999046	CVE-2022-0320	WEB-WORDPRESS Les addons essentiels pour le plugin Elementor avant 5.0.5 - LFI via load_more (CVE-2022-0320)

Mise à jour des signatures pour février 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2022-02-20. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version de signature 76 applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1 et NetScaler 13.0.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999047	CVE-2022-23863	WEB-MISC FusionPBX avant 4.5.30 - Injection de commande du système d'exploitation via fax_page_size (CVE-2021-43406)
999048	CVE-2021-44515	WEB-MISC JetBrains TeamCity - Vulnérabilité d'exécution de code à distance via l'agent Push (CVE-2021-43193)
999049	CVE-2021-43406	WEB-MISC GoAhead avant 5.1.5 - Vulnérabilité d'injection de variables dans l'environnement CGI (CVE-2021-42342)

Règle de signature	ID CVE	Description
999050	CVE-2021-43193	WEB-MISC SonicWall Secure Mobile Access - Vulnérabilité d'exécution de code à distance (CVE-2021-20045)
999051	CVE-2021-42342	WEB-MISC GoAhead avant 5.1.5 - Vulnérabilité d'injection de variables dans l'environnement CGI (CVE-2021-42342)
999052	CVE-2021-20045	WEB-MISC SonicWall Secure Mobile Access - Vulnérabilité d'exécution de code à distance (CVE-2021-20045)
999053	CVE-2021-20044	WEB-MISC SonicWall Secure Mobile Access - Vulnérabilité d'injection de commande (CVE-2021-20044)
999054		Plugin ADSanity WEB-WORDPRESS - Vulnérabilité d'exécution de code à distance via le chargement de fichiers HTML5

Mise à jour des signatures pour janvier 2022

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine du 20/01/2022. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Version 75 de signature applicable aux plateformes NetScaler VPX 11.1, NetScaler 12.0, NetScaler 12.1 et NetScaler 13.0.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999055	CVE-2021-44224	Serveur HTTP Apache WEB-MISC - Vulnérabilité UDS malformée via un proxy direct et inverse (CVE-2021-44224)
999056	CVE-2021-43815	WEB-MISC Apache Grafana - Vulnérabilité de traversée du chemin d'une source de données TestData DB (CVE-2021-43815)
999057	CVE-2021-43813	WEB-MISC Apache Grafana - Vulnérabilité liée à la traversée de chemins via Markdown (CVE-2021-43813)
999058	CVE-2021-43405	WEB-MISC FusionPBX avant la version 4.5.30 - Injection de commandes du système d'exploitation via fax_extension (CVE-2021-43405)
999059	CVE-2021-42392	Console WEB-MISC H2 antérieure à la version 2.0.206 - Vulnérabilité d'exécution de code à distance (CVE-2021-42392)

Règle de signature	ID CVE	Description
999060	CVE-2021-42362	Plugin de publication populaire WEB-WORDPRESS antérieur à 5.3.3 - Vulnérabilité liée au téléchargement de fichiers arbitraires (CVE-2021-42362)
999061	CVE-2021-42129	WEB-MISC Ivanti Avalanche avant la version 6.3.3 - Vulnérabilité d'injection de commandes du système d'exploitation via TxtuPass (CVE-2021-42129)
999062	CVE-2021-42129	WEB-MISC Ivanti Avalanche avant la version 6.3.3 - Vulnérabilité d'injection de commandes du système d'exploitation via TxtuName (CVE-2021-42129)
999063	CVE-2021-42129	WEB-MISC Ivanti Avalanche avant la version 6.3.3 - Vulnérabilité d'injection de commandes du système d'exploitation via TxTuncPath (CVE-2021-42129)
999064	CVE-2021-40345	WEB-MISC Nagios XI avant la version 5.8.6 - Vulnérabilité d'injection de commandes du système d'exploitation via un fichier ZIP conçu de manière malveillante (CVE-2021-40345)

Règle de signature	ID CVE	Description
999065	CVE-2021-37928	WEB-MISC Zoho ManageEngine ADManager Plus avant 7110 - Vulnérabilité liée au téléchargement illimité de fichiers (CVE-2021-37928)
999066	CVE-2021-25037	Plugin de référencement tout-en-un WEB-WORDPRESS antérieur à la version 4.1.5.3 - Vulnérabilité d'injection SQL via des objets, API REST et rest_route
999067	CVE-2021-25037	Plugin de référencement tout-en-un WEB-WORDPRESS antérieur à la version 4.1.5.3 - Vulnérabilité d'injection SQL via l'API REST d'objets
999068	CVE-2021-25036	Plugin de référencement tout-en-un WEB-WORDPRESS antérieur à la version 4.1.5.3 - Vulnérabilité d'escalade de privilèges via l'API REST et rest_route
999069	CVE-2021-25036	Plugin de référencement tout-en-un WEB-WORDPRESS antérieur à la version 4.1.5.3 - Vulnérabilité d'escalade de privilèges via l'API REST
999070	CVE-2021-21917	WEB-MISC Advantech R-SeeNet avant la version 2.4.17 - Vulnérabilité d'injection SQL via Word (CVE-2021-21917)

Règle de signature	ID CVE	Description
999071	CVE-2021-20040	Accès mobile sécurisé WEB-MISC SonicWall - Vulnérabilité d'écriture de fichier arbitraire (CVE-2021-20040)
999072	CVE-2021-20039	Accès mobile sécurisé WEB-MISC SonicWall - Vulnérabilité liée à l'injection de commandes (CVE-2021-20039)

Mise à jour des signatures pour décembre 2021

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-12-21. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page Cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999073	CVE-2021-44077	WEB-MISC Zoho ManageEngine ServiceDesk Plus avant 11306 - Vulnérabilité RCE avant Auth via ImportTechnicians (CVE-2021-44077)
999074	CVE-2021-43798	WEB-MISC Apache Grafana 8.0.0 jusqu'à la version 8.3.0 - Vulnérabilité de traversée de chemin (CVE-2021-43798)
999075	CVE-2021-35216	WEB-MISC SolarWinds Orion avant 2020.2.6 - Vulnérabilité de désérialisation via EditTopXX.aspx (CVE-2021-35216)
999076	CVE-2021-34993	WEB-MISC Commvault CommCell - Vulnérabilité de contournement d'authentification CVSearchService (CVE-2021-34993)

Mise à jour des signatures pour décembre 2021

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-12-13. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du

cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous la liste des règles de signature, des ID CVE et leur description qui sont mises à jour.

> **Remarque :**
>
> Les règles de signature ci-dessous (999077, 999078, 999079, 999080) concernent les deux CVE (CVE-2021-44228 et CVE-2021-45046).

Règle de signature	ID CVE	Description
999077	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j - Vulnérabilité d'exécution de code à distance via FORM (CVE-2021-44228, CVE-2021-45046)
999078	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j - Vulnérabilité d'exécution de code à distance via BODY (CVE-2021-44228, CVE-2021-45046)
999079	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j - Vulnérabilité d'exécution de code à distance via HEADER (CVE-2021-44228, CVE-2021-45046)
999080	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j - Vulnérabilité d'exécution de code à distance via une URL (CVE-2021-44228, CVE-2021-45046)

Mise à jour des signatures pour décembre 2021

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-12-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999077	CVE-2021-44228	WEB-MISC Apache Log4j - Vulnérabilité d'exécution de code à distance via FORM (CVE-2021-44228)
999078	CVE-2021-44228	WEB-MISC Apache Log4j - Vulnérabilité d'exécution de code à distance via BODY (CVE-2021-44228)
999079	CVE-2021-44228	WEB-MISC Apache Log4j - Vulnérabilité d'exécution de code à distance via HEADER (CVE-2021-44228)

Règle de signature	ID CVE	Description
999080	CVE-2021-44228	WEB-MISC Apache Log4j - Vulnérabilité d'exécution de code à distance via une URL (CVE-2021-44228)
999081	CVE-2021-42847	WEB-MISC Zoho ManageEngine AdAudit Plus avant 7006 - Vulnérabilité d'écriture de fichiers arbitraires non authentifiés (CVE-2021-42847)
999082	CVE-2021-42321	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance (CVE-2021-42321)
999083	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2021 - Vulnérabilité d'injection SQL non authentifiée via txTid (CVE-2021-42258)
999084	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2020 - Vulnérabilité d'injection SQL non authentifiée via txTid (CVE-2021-42258)
999085	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2019 - Vulnérabilité d'injection SQL non authentifiée via txTid (CVE-2021-42258)
999086	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2018 - Vulnérabilité d'injection SQL non authentifiée via txTid (CVE-2021-42258)

Règle de signature	ID CVE	Description
999087	CVE-2021-42237	WEB-MISC Sitecore de 7.5.0 à 8.2.7 - Vulnérabilité d'exécution de code à distance (CVE-2021-42237)
999088	CVE-2021-41950	WEB-MISC ResourceSpace 9.6 avant la rév. 18277 - Vulnérabilité de traversée de chemin non authentifiée via variant (CVE-2021-41950)
999089	CVE-2021-41950	WEB-MISC ResourceSpace 9.6 avant la rév. 18277 - Vulnérabilité de traversée de chemin non authentifiée via un fournisseur (CVE-2021-41950)
999090	CVE-2021-41349	WEB-MISC Microsoft Exchange Server - Vulnérabilité de script intersite (CVE-2021-41349)
999091	CVE-2021-35217	WEB-MISC SolarWinds Orion avant 2020.2.6 HF1 - Vulnérabilité de désérialisation via WSAsyncExecuteTasks.aspx (CVE-2021-35217)
999092	CVE-2021-34416	Connecteur WEB-MISC Zoom Meeting 4.6.360.20210325 - Vulnérabilité d'exécution de code à distance (CVE-2021-34416)
999093	CVE-2021-22941	WEB-MISC Citrix ShareFile Storage avant 5.11.20 - Vulnérabilité de contrôle d'accès incorrect (CVE-2021-22941)

Règle de signature	ID CVE	Description
999094	CVE-2020-35136	WEB-MISC Dolibarr avant 12.0.4 - Vulnérabilité d'exécution de code à distance via zipfilename_template et bz (CVE-2020-35136)
999095	CVE-2020-35136	WEB-MISC Dolibarr avant 12.0.4 - Vulnérabilité d'exécution de code à distance via zipfilename_template et gz (CVE-2020-35136)
999096	CVE-2020-2950, CVE-2021-2456	WEB-MISC - Vulnérabilité liée au chargement de fichiers arbitraires dans Oracle BI Publisher (CVE-2020-2950, CVE-2021-2456)
999097	CVE-2020-2950, CVE-2021-2456	WEB-MISC Oracle BI Publisher - Vulnérabilité d'exécution de code à distance (CVE-2020-2950, CVE-2021-2456)

Mise à jour des signatures pour novembre 2021

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-11-18. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999098	CVE-2021-41765	WEB-MISC ResourceSpace 9.5 et 9.6 avant la révision 18274 - Vulnérabilité d'injection SQL (CVE-2021-41765)
999099	CVE-2021-41288	WEB-MISC Zoho ManageEngine OpManager avant la génération 125467 - Vulnérabilité d'injection SQL via l'API GetReportData (CVE-2021-41288)
999100	CVE-2021-40493	WEB-MISC Zoho ManageEngine OpManager avant la génération 125437 - Vulnérabilité d'injection SQL via DeviceName (CVE-2021-40493)
999101	CVE-2021-40493	WEB-MISC Zoho ManageEngine OpManager avant la génération 125437 - Vulnérabilité d'injection SQL via PollingObject (CVE-2021-40493)
999102	CVE-2021-40438	Serveur HTTP Apache WEB-MISC — Vulnérabilité de transfert de requête mod_proxy (CVE-2021-40438)

Règle de signature	ID CVE	Description
999103	CVE-2021-39341	Plugin WEB-WORDPRESS OptinMonster jusqu'à 2.6.4 - Vulnérabilité de contournement d'autorisation REST_ROUTE (CVE-2021-39341)
999104	CVE-2021-39341	Plugin WEB-WORDPRESS OptinMonster jusqu'à 2.6.4 - Vulnérabilité de contournement des autorisations d'API REST (CVE-2021-39341)
999105	CVE-2021-37344	Assistant de commutation WEB-MISC Nagios XI avant 2.5.7 - Vulnérabilité d'exécution de code à distance via le paramètre ip_address (CVE-2021-37344)
999106	CVE-2021-35218	WEB-MISC SolarWinds Orion avant 2020.2.6 - Vulnérabilité de désérialisation via Chart.ashx (CVE-2021-35218)
999107	CVE-2021-35215	WEB-MISC SolarWinds Orion Platform avant 2020.2.6 - Vulnérabilité d'exécution de code à distance via la création de rapports (CVE-2021-35215)
999108	CVE-2021-35215	WEB-MISC SolarWinds Orion Platform avant 2020.2.6 - Vulnérabilité d'exécution de code à distance via des alertes (CVE-2021-35215)
999109	CVE-2021-24889	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.6.4 - Vulnérabilité d'injection SQL (CVE-2021-24889)

Règle de signature	ID CVE	Description
999110	CVE-2021-24381	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.5.8.2 - Vulnérabilité de script intersite stockée par nom de classe personnalisé (CVE-2021-24381)
999111	CVE-2021-2401	WEB-MISC Oracle BI Publisher - Vulnérabilité dans DomParser XXE via le service X ReportTemplateService mobile (CVE-2021-2401)
999112	CVE-2021-2401	WEB-MISC Oracle BI Publisher - Vulnérabilité dans DomParser XXE via ReportTemplateService mobile (CVE-2021-2401)
999113	CVE-2021-2401	WEB-MISC Oracle BI Publisher - Vulnérabilité dans DomParser XXE via xmlpservice X ReportTemplateService (CVE-2021-2401)
999114	CVE-2021-2401	WEB-MISC Oracle BI Publisher - Vulnérabilité dans DomParser XXE via xmlpservice ReportTemplateService (CVE-2021-2401)
999115	CVE-2021-2392	WEB-MISC Oracle BI Publisher — Vulnérabilité liée au téléchargement de fichiers arbitraires (CVE-2021-2392)

Règle de signature	ID CVE	Description
999116	CVE-2021-2244	WEB-MISC Oracle Hyperion-Essbase Analytic Provider Services - Vulnérabilité d'exécution de code à distance via Essbase (CVE-2021-2244)
999117	CVE-2021-2244	WEB-MISC Oracle Hyperion-Essbase Analytic Provider Services - Vulnérabilité d'exécution de code à distance via un administrateur (CVE-2021-2244)
999118	CVE-2021-2244	WEB-MISC Oracle Hyperion-Essbase Analytic Provider Services - Vulnérabilité d'exécution de code à distance via JAPI (CVE-2021-2244)
999119	CVE-2021-22205	WEB-MISC GitLab CE/EE - Vulnérabilité d'exécution de code à distance via des fichiers JPEG/TIFF conçus de manière malveillante (CVE-2021-22205)
999120	CVE-2021-22017	WEB-MISC VMware vCenter - Vulnérabilité de traversée de chemin via rhhtproxy (CVE-2021-22017)
999121	CVE-2021-20837	Type mobile WEB-MISC antérieur à r.5003 - Exécution de code à distance via mt.handler_to_coderef (CVE-2021-20837)

Règle de signature	ID CVE	Description
999122	CVE-2021-20131	WEB-MISC Zoho ManageEngine AdManager avant la version 7115 - Vulnérabilité d'exécution de code à distance via le téléchargement de fichiers (CVE-2021-20131)
999123	CVE-2021-20130	WEB-MISC Zoho ManageEngine AdManager avant la version 7115 - Vulnérabilité d'exécution de code à distance via le téléchargement de fichiers (CVE-2021-20130)
999124	CVE-2021-20034	WEB-MISC SonicWall Secure Mobile Access - Vulnérabilité de traversée de chemin (CVE-2021-20034)
999125		Plugin WEB-WORDPRESS BuddyPress avant 9.1.1 - Vulnérabilité de divulgation d'informations via l'API REST d'inscription et rest_route
999126		Plugin WEB-WORDPRESS BuddyPress avant 9.1.1 - Vulnérabilité de divulgation d'informations via l'API REST d'inscription

Mise à jour des signatures pour octobre 2021

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-10-26. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre

appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999127	CVE-2021-42013	Serveur HTTP Apache WEB-MISC 2.4.49 et 2.4.50 - Vulnérabilité de traversée de chemin via %%32 (CVE-2021-42013)
999128	CVE-2021-42013	Serveur HTTP Apache WEB-MISC 2.4.49 et 2.4.50 - Vulnérabilité de traversée de chemin via % 2% (CVE-2021-42013)
999129	CVE-2021-41773	Serveur HTTP Apache WEB-MISC 2.4.49 - Vulnérabilité de traversée de chemin via %2e%2e (CVE-2021-41773)
999130	CVE-2021-41773	Serveur HTTP Apache WEB-MISC 2.4.49 - Vulnérabilité de traversée de chemin via.% 2e (CVE-2021-41773)

Règle de signature	ID CVE	Description
999131	CVE-2021-40539	WEB-MISC Zoho ManageEngine AdSelfService Plus 6.1 avant la version 6114 - Vulnérabilité de contournement de l'authentification (CVE-2021-40539)
999132	CVE-2021-34648	Plugin Web-WordPress Ninja Forms jusqu'à 3.5.7 - Vulnérabilité REST_ROUTE via les soumissions par e-mail (CVE-2021-34648)
999133	CVE-2021-34648	Plugin WEB-WORDPRESS Ninja Forms Jusqu'à 3.5.7 - Vulnérabilité de l'API REST via les soumissions par e-mail (CVE-2021-34648)
999134	CVE-2021-34647	Plugin Web-WordPress Ninja Forms jusqu'à 3.5.7 - Vulnérabilité REST_ROUTE via l'exportation de soumissions (CVE-2021-34647)
999135	CVE-2021-34647	Plugin Web-WordPress Ninja Forms jusqu'à 3.5.7 - Vulnérabilité de l'API REST via l'exportation de soumissions (CVE-2021-34647)
999136	CVE-2021-34623	Plugin WEB-WORDPRESS ProfilePress antérieur à 3.1.4 - Vulnérabilité de téléchargement de fichier arbitraire via eup_cover_image (CVE-2021-34623)

Règle de signature	ID CVE	Description
999137	CVE-2021-34623	Plugin WEB-WORDPRESS ProfilePress antérieur à 3.1.4 - Vulnérabilité de téléchargement de fichier arbitraire via eup_avatar (CVE-2021-34623)
999138	CVE-2021-2400	WEB-MISC Oracle BI Publisher - Vulnérabilité dans SaxParser XXE via le service X ReportTemplateService mobile (CVE-2021-2400)
999139	CVE-2021-2400	WEB-MISC Oracle BI Publisher - Vulnérabilité dans SaxParser XXE via ReportTemplateService mobile (CVE-2021-2400)
999140	CVE-2021-2400	WEB-MISC Oracle BI Publisher - Vulnérabilité dans SaxParser XXE via xmlpservice X ReportTemplateService (CVE-2021-2400)
999141	CVE-2021-2400	WEB-MISC Oracle BI Publisher - Vulnérabilité dans SaxParser XXE via xmlpservice ReportTemplateService (CVE-2021-2400)
999142	CVE-2021-21985	WEB-MISC VMware vCenter - Vulnérabilité d’exécution de code à distance du plug-in de vérification de l’état de santé Virtual SAN (CVE-2021-21985)

Règle de signature	ID CVE	Description
999143	CVE-2021-20078	WEB-MISC Zoho ManageEngine OpManager 12.5 avant la génération 125362 - Vulnérabilité de traversée de chemin (CVE-2021-20078)
999144	CVE-2020-29448	Serveur et centre de données WEB-MISC Atlassian Confluence - Vulnérabilité de divulgation d'informations via WEB-INF (CVE-2020-29448)
999145	CVE-2020-29448	Serveur et centre de données WEB-MISC Atlassian Confluence - Vulnérabilité de divulgation d'informations via META-INF (CVE-2020-29448)
999146	CVE-2020-12442	WEB-MISC Ivanti Avalanche 6.3 - Vulnérabilité d'injection SQL non authentifiée via un point de terminaison osupdate (CVE-2020-12442)
999147	CVE-2020-12442	WEB-MISC Ivanti Avalanche 6.3 - Vulnérabilité d'injection SQL non authentifiée via un point de terminaison wapl (CVE-2020-12442)
999148		Plugin WEB-WORDPRESS BuddyPress avant 9.1.1 - Vulnérabilité d'injection SQL via la fonctionnalité bp-members-invitations

Mise à jour des signatures pour octobre 2021

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-10-09. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999149	CVE-2021-38312	Bibliothèque de modèles WEB-WORDPRESS Gutenberg et plug-in Redux Framework avant 4.2.12 - Vulnérabilité REST_ROUTE (CVE-2021-38312)
999150	CVE-2021-38312	Bibliothèque de modèles WEB-WORDPRESS Gutenberg et plug-in Redux Framework avant 4.2.12 - Vulnérabilité de l'API REST (CVE-2021-38312)

Règle de signature	ID CVE	Description
999151	CVE-2021-34639	Plugin de gestionnaire de téléchargement WEB-WORDPRESS antérieur à 3.1.25 - Vulnérabilité de téléchargement de double extension (CVE-2021-34639)
999152	CVE-2021-34621	Plugin WEB-WORDPRESS ProfilePress avant 3.1.3 - Vulnérabilité d'élévation de privilèges via wp_capabilities (CVE-2021-34621)
999153	CVE-2021-32682	WEB-MISC ElFinder avant 2.1.59 - Vulnérabilité de traversée de chemin via la commande Renommer (CVE-2021-32682)
999154	CVE-2021-32682	WEB-MISC ElFinder avant 2.1.59 - Vulnérabilité de traversée de chemin via la commande Abort (CVE-2021-32682)
999155	CVE-2021-26086	WEB-MISC Atlassian Jira Server and Data Center - Vulnérabilité de divulgation d'informations via WEB-INF (CVE-2021-26086)
999156	CVE-2021-26086	WEB-MISC Atlassian Jira Server and Data Center - Vulnérabilité de divulgation d'informations via META-INF (CVE-2021-26086)
999157	CVE-2021-22005	WEB-MISC VMware vCenter - Vulnérabilité liée au chargement de fichiers via une application de données (CVE-2021-22005)

Règle de signature	ID CVE	Description
999158	CVE-2021-22005	WEB-MISC VMware vCenter - Vulnérabilité liée au chargement de fichiers via le journal des étapes de télémétrie (CVE-2021-22005)
999159	CVE-2021-22005	WEB-MISC VMware vCenter - Vulnérabilité liée au chargement de fichiers via le journal de production de télémétrie (CVE-2021-22005)
999160	CVE-2021-20081	WEB-MISC Zoho ManageEngine Service Desk antérieur à 11.2.0.5 - Vulnérabilité d'exécution de code à distance (CVE-2021-20081)
999161	CVE-2020-29453	Serveur et centre de données Atlassian Jira WEB-MISC - Vulnérabilité de divulgation d'informations via WEB-INF (CVE-2020-29453)
999162	CVE-2020-29453	Serveur et centre de données Atlassian Jira WEB-MISC - Vulnérabilité de divulgation d'informations via META-INF (CVE-2020-29453)

Mise à jour des signatures pour septembre 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-09-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999163	CVE-2021-37556	WEB-MISC Centreon Multiple Versions - Vulnérabilité d'injection SQL via un paramètre de fin (CVE-2021-37556)
999164	CVE-2021-37556	WEB-MISC Centreon Multiple Versions - Vulnérabilité d'injection SQL via le paramètre de démarrage (CVE-2021-37556)
999165	CVE-2021-37353	Assistant Docker WEB-MISC Nagios XI antérieur à 1.1.3 - Vulnérabilité SSRF via un paramètre hôte sans schéma d'URI (CVE-2021-37353)
999166	CVE-2021-37353	Assistant Docker WEB-MISC Nagios XI antérieur à 1.1.3 - Vulnérabilité SSRF via un paramètre hôte avec schéma d'URI (CVE-2021-37353)

Règle de signature	ID CVE	Description
999167	CVE-2021-34638	Plugin de gestionnaire de téléchargement WEB-WORDPRESS antérieur à 3.1.25 - Vulnérabilité de traversée de répertoires (CVE-2021-34638)
999168	CVE-2021-33766	WEB-MISC Microsoft Exchange Server - Vulnérabilité de divulgation d'informations (CVE-2021-33766)
999169	CVE-2021-32682	WEB-MISC ElFinder antérieur à 2.1.59 - Vulnérabilité d'injection de commande via l'archivage (CVE-2021-32682)
999170	CVE-2021-26084	WEB-MISC Confluence Server and Data Center - Vulnérabilité d'injection OGNL via doenterpagevariables (CVE-2021-26084)
999171	CVE-2021-26084	WEB-MISC Confluence Server and Data Center - Vulnérabilité d'injection OGNL via createpage-entervariables (CVE-2021-26084)
999172	CVE-2021-23394	WEB-MISC ElFinder antérieur à 2.1.59 - Vulnérabilité d'exécution de code à distance via Phar Makefile (CVE-2021-23394)
999173	CVE-2021-23394	WEB-MISC ElFinder antérieur à 2.1.59 - Vulnérabilité d'exécution de code à distance via Phar Rename (CVE-2021-23394)

Règle de signature	ID CVE	Description
999174	CVE-2021-23394	WEB-MISC ElFinder antérieur à 2.1.59 - Vulnérabilité d'exécution de code à distance via Phar Upload (CVE-2021-23394)
999175	CVE-2020-36289	WEB-MISC Atlassian Jira Server - Vulnérabilité de divulgation d'informations via QueryComponentRenderer-erValue (CVE-2020-36289)
999176	CVE-2020-16245	WEB-MISC Advantech IView antérieur à 5.7.03.6112 - Vulnérabilité de traversée de chemin via FindSumma-ryCfgDeviceListExport (CVE-2020-16245)
999177	CVE-2020-16245	WEB-MISC Advantech IView antérieur à 5.7.03.6112 - Vulnérabilité de traversée de chemin via FindUpdateDeviceListExport (CVE-2020-16245)
999178	CVE-2020-13774	WEB-MISC Ivanti Endpoint Manager Versions multiples - Vulnérabilité RCE via EditLaunchPadDialog.aspx (CVE-2020-13774)
999179	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance via une page personnalisée (CVE-2020-1147)

Règle de signature	ID CVE	Description
999180	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance via quicklinksdialogform.aspx (CVE-2020-1147)
999181	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance via quicklinks.aspx (CVE-2020-1147)
999182	CVE-2020-11110	WEB-MISC Apache Grafana jusqu'à la version 6.7.1 - Vulnérabilité XSS (CVE-2020-11110)
999522	CVE-2020-13379	WEB-MISC Grafana 3.0.1 à 7.0.1 - Contournement de CSRF menant à une vulnérabilité DOS (CVE-2020-13379)

Mise à jour des signatures pour août 2021

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-08-29. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du

cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999183	CVE-2021-37557	WEB-MISC Centreon Multiple versions - Vulnérabilité d'injection SQL (CVE-2021-37557)
999184	CVE-2021-35501	WEB-MISC Artica Pandora FMS jusqu'à 7.54 - Vulnérabilité XSS stockée dans Visual Console (CVE-2021-35501)
999185	CVE-2021-35464	WEB-MISC ForgeRock Access Management et OpenAM - Vulnérabilité d'exécution de code à distance (CVE-2021-35464)
999186	CVE-2021-34523	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'élévation de privilèges (CVE-2021-34523)
999187	CVE-2021-34473	WEB-MISC Microsoft Exchange Server - Vulnérabilité de contournement de l'authentification par contrefaçon de requête côté serveur par requête (CVE-2021-34473)

Règle de signature	ID CVE	Description
999188	CVE-2021-34473	WEB-MISC Microsoft Exchange Server - Vulnérabilité de contournement de l'authentification par falsification de requête côté serveur via un cookie (CVE-2021-34473)
999189	CVE-2021-33203	WEB-MISC Django - Vulnérabilité de divulgation de l'existence d'un fichier TemplateDetailView via un chemin absolu (CVE-2021-33203)
999190	CVE-2021-33203	WEB-MISC Django - Vulnérabilité de divulgation de l'existence d'un fichier TemplateDetailView via la traversée de chemin (CVE-2021-33203)
999191	CVE-2021-33203	WEB-MISC Django — Vulnérabilité de divulgation de l'existence d'un fichier TemplateDetailView par barre oblique inverse (CVE-2021-33203)
999192	CVE-2021-33203	WEB-MISC Django - Vulnérabilité de divulgation de l'existence d'un fichier TemplateDetailView par barre oblique (CVE-2021-33203)
999193	CVE-2021-3287, CVE-2020-28653	WEB-MISC Zoho ManageEngine OpManager avant 12.5.329 - Vulnérabilité RCE non authentifiée (CVE-2021-3287, CVE-2020-28653)

Règle de signature	ID CVE	Description
999194	CVE-2021-32789	Plugin WooCommerce WEB-WORDPRESS jusqu'à 5.5.0 - Vulnérabilité d'injection SQL via la taxonomie et rest_route (CVE-2021-32789)
999195	CVE-2021-32789	Plugin WooCommerce WEB-WORDPRESS jusqu'à 5.5.0 - Vulnérabilité d'injection SQL via la taxonomie (CVE-2021-32789)
999196	CVE-2021-32604	WEB-MISC SolarWinds Serv-U avant 15.2.3 - Vulnérabilité de script intersite via le paramètre SenderEmail (CVE-2021-32604)
999197	CVE-2021-32093	WEB-MISC Emissary 5.9.0 de l'Agence nationale de sécurité nationale - Vulnérabilité en lecture de fichiers arbitraires (CVE-2021-32093)
999198	CVE-2021-31760	WEB-MISC Webmin antérieur à 1.974 - Une vulnérabilité CSRF entraînait un ECR via run.cgi (CVE-2021-31760)
999199	CVE-2021-31207	WEB-MISC Microsoft Exchange Server - Vulnérabilité liée au contournement des fonctionnalités de sécurité (CVE-2021-31207)
999200	CVE-2021-31195	WEB-DIVERS Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance (CVE-2021-31195)

Règle de signature	ID CVE	Description
999201	CVE-2021-28474	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance (CVE-2021-28474)
999202	CVE-2021-24385	Plugin WEB-WORDPRESS FileBird 4.7.3 - Vulnérabilité d'injection SQL via le paramètre SelectedFolder et rest_route (CVE-2021-24385)
999203	CVE-2021-24385	Plugin WEB-WORDPRESS FileBird 4.7.3 - Vulnérabilité d'injection SQL via le paramètre SelectedFolder (CVE-2021-24385)
999204	CVE-2021-24385	Plugin WEB-WORDPRESS FileBird 4.7.3 - Vulnérabilité d'injection SQL via un corps codé en JSON (CVE-2021-24385)
999205	CVE-2021-24356	WEB-WORDPRESS Simple 301 redirige le plugin avant 2.0.4 - Vulnérabilité d'activation arbitraire de plug-in (CVE-2021-24356)
999206	CVE-2021-23024	Versions multiples WEB-MISC F5 BIG-IQ - Vulnérabilité d'exécution de code à distance (CVE-2021-23024)
999207	CVE-2021-22911	WEB-MISC Rocket.Chat Server 3.11, 3.12 et 3.13 - Vulnérabilité d'injection NOSQL aveugle (CVE-2021-22911)

Règle de signature	ID CVE	Description
999208	CVE-2021-22900	WEB-MISC Pulse Connect Secure avant 9.1R11.4 - Vulnérabilité d'exécution de code à distance via smimeCert.cgi (CVE-2021-22900)
999209	CVE-2021-22900	WEB-MISC Pulse Connect Secure avant la version 9.1R11.4 - Vulnérabilité d'exécution de code à distance via admincert.cgi (CVE-2021-22900)
999210	CVE-2021-22900	WEB-MISC Pulse Connect Secure avant la version 9.1R11.4 - Vulnérabilité d'exécution de code à distance via clientauthcert.cgi (CVE-2021-22900)
999211	CVE-2021-22160	WEB-MISC Apache Pulsar - Vulnérabilité de contournement de l'authentification par jetons Web JSON (CVE-2021-22160)
999212	CVE-2021-21809	WEB-MISC Moodle - Vulnérabilité d'exécution de code à distance via le plug-in Correcteur orthographique et la méthode GetSuggestions (CVE-2021-21809)
999213	CVE-2021-21809	WEB-MISC Moodle - Vulnérabilité d'exécution de code à distance via le plug-in Correcteur orthographique et la méthode CheckWords (CVE-2021-21809)

Règle de signature	ID CVE	Description
999214	CVE-2021-21809	WEB-MISC Moodle - Vulnérabilité d'exécution de code à distance via s__aspellpath (CVE-2021-21809)
999215	CVE-2021-21805	WEB-MISC Advantech R-SeeNet - Vulnérabilité d'exécution de code à distance non authentifié (CVE-2021-21805)
999216	CVE-2021-21804	WEB-MISC Advantech R-SeeNet - Vulnérabilité d'inclusion de fichiers locaux via sub_opt (CVE-2021-21804)
999217	CVE-2021-21587	WEB-MISC Dell Wyse Management Suite avant 3.3 - Vulnérabilité de traversée de chemin via /image/os/listfiles (CVE-2021-21587)
999218	CVE-2021-21587	WEB-MISC Dell Wyse Management Suite avant 3.3 - Vulnérabilité de traversée de chemin via /image/app/rsp/listfiles (CVE-2021-21587)
999219	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite avant 3.3 - Vulnérabilité de traversée de chemin via /image/app et FileName (CVE-2021-21586)
999220	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite avant 3.3 - Vulnérabilité de traversée de chemin via /image/os et FileName (CVE-2021-21586)

Règle de signature	ID CVE	Description
999221	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite avant 3.3 - Vulnérabilité de traversée de chemin via /image/os et FilePath (CVE-2021-21586)
999222	CVE-2020-25223	WEB-MISC Sophos SG UTM - Exécution de code à distance via SID et /var (CVE-2020-25223)
999223	CVE-2020-25223	WEB-MISC Sophos SG UTM - Exécution de code à distance via SID et /webadmin.plx (CVE-2020-25223)
999224	CVE-2020-21056	WEB-MISC FusionPBX 4.5.7 - Vulnérabilité de traversée de chemin via un nouveau dossier (CVE-2020-21056)
999225	CVE-2020-21055	WEB-MISC FusionPBX 4.5.7 - Vulnérabilité de traversée de chemin via la fonction de renommage de fichiers (CVE-2020-21055)
999226	CVE-2020-16245	WEB-MISC Advantech iView avant 5.7.03.6112 - Vulnérabilité de traversée de chemin dans FindSummaryUpdateDeviceListExpo (CVE-2020-16245)
999227	CVE-2020-16245	WEB-MISC Advantech iView avant 5.7.03.6112 - Vulnérabilité de traversée de chemin via FindCfgDeviceListExport (CVE-2020-16245)

Règle de signature	ID CVE	Description
999228	CVE-2020-14181	WEB-MISC Atlassian Jira Server - Vulnérabilité de divulgation d'informations via ViewUserHover.jspa (CVE-2020-14181)
999229	CVE-2020-14005	WEB-MISC SolarWinds Orion avant 2020.2.1 HF 2 - Exécution de code à distance via le type d'action ExecuteVBScript (CVE-2020-14005)
999230	CVE-2020-14005	WEB-MISC SolarWinds Orion avant 2020.2.1 HF 2 - Exécution de code à distance via le type d'action ExecuteExternalProgram (CVE-2020-14005)

Mise à jour de la signature pour juillet 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-07-08. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le

> processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999231	CVE-2021-34074	WEB-MISC Artica Pandora FMS jusqu'à 7.54 - Vulnérabilité de chargement arbitraire de fichiers via un chemin relatif (CVE-2021-34074)
999232	CVE-2021-32633	WEB-MISC Plone CMS - Vulnérabilité d'exécution de code à distance des modèles de pages Zope via le téléchargement (CVE-2021-32633)
999233	CVE-2021-32633	WEB-MISC Plone CMS - Vulnérabilité d'exécution de code à distance des modèles de pages Zope via un nouveau (CVE-2021-32633)
999234	CVE-2021-31181	WEB-MISC Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance (CVE-2021-31181)
999235	CVE-2021-24370	Web-WORDPRESS Fancy Product Designer Plugin avant 5.6.9 - Vulnérabilité RCE via fpd_custom_uplod_file (CVE-2021-24370)

Règle de signature	ID CVE	Description
999236	CVE-2021-24370	Web-WORDPRESS Fancy Product Designer Plugin avant 5.6.9 - Vulnérabilité RCE via custom-image-handler.php (CVE-2021-24370)
999237	CVE-2021-24354	WEB-WORDPRESS Simple 301 Redirige le plugin avant 2.0.4 - Vulnérabilité d'installation arbitraire du plugin (CVE-2021-24354)
999238	CVE-2021-24352	Plugin de redirection WEB-WORDPRESS Simple 301 avant 2.0.4 - Vulnérabilité d'exportation de redirection (CVE-2021-24352)
999239	CVE-2021-1497, CVE-2021-1498	WEB-MISC Cisco HyperFlex HX antérieur à 4.0 (2e) - Vulnérabilité d'exécution de code à distance (CVE-2021-1497, CVE-2021-1498)
999240	CVE-2020-21057	WEB-MISC FusionPBX 4.5.7 - Vulnérabilité de traversée de chemin via la fonction de suppression de dossier (CVE-2020-21057)
999241	CVE-2020-16245	WEB-MISC Advantech iView antérieur à la version 5.7.03.6112 - Vulnérabilité de traversée de chemin via BackupDatabase (CVE-2020-16245)

Règle de signature	ID CVE	Description
999242	CVE-2020-10148	WEB-MISC SolarWinds Orion Multiple Versions - Vulnérabilité de contournement de l'authentification (CVE-2020-10148)

Mise à jour de la signature pour juin 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-06-02. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999243	CVE-2021-31761	WEB-MISC Webmin antérieur à 1.974 - Vulnérabilité XSS via /servers/link.cgi/ (CVE-2021-31761)

Règle de signature	ID CVE	Description
999244	CVE-2021-31761	WEB-MISC Webmin avant 1.974 - Vulnérabilité XSS via /tunnel/link.cgi/ (CVE-2021-31761)
999245	CVE-2021-31166	Pile de protocole HTTP Microsoft WEB-IIS - Vulnérabilité d'exécution de code à distance (CVE-2021-31166)
999246	CVE-2021-29447	WEB-WORDPRESS WordPress antérieur à 5.7.1 - Vulnérabilité XXE des médiathèques (CVE-2021-29447)
999247	CVE-2021-28157	Serveur WEB-MISC Devolutions avant 2021.1 et 2020.3.18 - Vulnérabilité d'injection SQL via la suppression de l'utilisateur (CVE-2021-28157)
999248	CVE-2021-27905	WEB-MISC Apache Solr antérieur à 8.2.2 - Vulnérabilité SSRF ReplicationHandler via LeaderURL (CVE-2021-27905)
999249	CVE-2021-27905	WEB-MISC Apache Solr antérieur à 8.2.2 - Vulnérabilité SSRF ReplicationHandler via MasterURL (CVE-2021-27905)
999250	CVE-2021-27890	WEB-MISC MyBB antérieur à 1.8.26 - Vulnérabilité par injection SQL Propriétés du thème (CVE-2021-27890)

Règle de signature	ID CVE	Description
999251	CVE-2021-27850, CVE-2019-0195	WEB-MISC Apache Tapestry - Vulnérabilité de divulgation d'informations non authentifiées (CVE-2021-27850 et CVE-2019-0195)
999252	CVE-2021-27183	WEB-MISC MDaemon antérieur à 20.0.4 - Vulnérabilité d'écriture arbitraire de fichiers (CVE-2021-27183)
999253	CVE-2021-27181	WEB-MISC MDaemon antérieur à la version 20.0.4 - Vulnérabilité de fixation de jetons anti-CSRF (CVE-2021-27181)
999254	CVE-2021-27180	WEB-MISC MDaemon avant 20.0.4 - Vulnérabilité XSS réfléchie (CVE-2021-27180)
999255	CVE-2021-24340	Statistiques WP WEB-WORDPRESS antérieures à 13.0.8 - Vulnérabilité d'injection SQL non authentifiée (CVE-2021-24340)
999256	CVE-2021-24171	Web-WORDPRESS WooCommerce Upload Files Plugin avant 59.4 - Vulnérabilité de traversée de chemin (CVE-2021-24171)
999257	CVE-2021-24171	Web-WORDPRESS WooCommerce Upload Files Plugin avant 59.4 - Vulnérabilité de téléchargement arbitraire de fichiers (CVE-2021-24171)

Règle de signature	ID CVE	Description
999258	CVE-2021-22658	WEB-MISC Advantech iView Antérieur à 5.7.03.6112 - Vulnérabilité SQLi via Uservlet et user_password (CVE-2021-22658)
999259	CVE-2021-22658	WEB-MISC Advantech iView Antérieur à 5.7.03.6112 - Vulnérabilité SQLi via Uservlet et nom_utilisateur (CVE-2021-22658)
999260	CVE-2021-22658	WEB-MISC Advantech iView Antérieur à 5.7.03.6112 - Vulnérabilité SQLi via CommandServlet et user_password (CVE-2021-22658)
999261	CVE-2021-22658	WEB-MISC Advantech iView Antérieur à 5.7.03.6112 - Vulnérabilité SQLi via CommandServlet et nom_utilisateur (CVE-2021-22658)
999262	CVE-2021-21983	WEB-MISC VMware vRealize Operations Manager antérieur à la version 8.4 - Vulnérabilité d’écriture de fichiers arbitraire (CVE-2021-21983)
999263	CVE-2020-6754	DotCMS WEB-MISC antérieur à la version 5.2.4 - Vulnérabilité de traversée d’annuaire via les ressources (CVE-2020-6754)

Règle de signature	ID CVE	Description
999264	CVE-2020-27128	WEB-MISC Cisco SD-WAN vManage antérieur à la version 20.3.1 - Vulnérabilité d'écriture de fichiers arbitraire via le traitement à distance (CVE-2020-27128)
999265	CVE-2020-27128	WEB-MISC Cisco SD-WAN vManage antérieur à 20.3.1 - Vulnérabilité d'écriture de fichiers arbitraire via dr (CVE-2020-27128)
999266	CVE-2020-15714	WEB-MISC RConfig 3.9.5 et antérieur - Vulnérabilité par injection SQL (CVE-2020-15714)
999267	CVE-2020-15713	WEB-MISC RConfig antérieur à 3.9.6 - Vulnérabilité par injection SQL (CVE-2020-15713)
999268	CVE-2020-14295	Cactus WEB-MISC antérieurs à 1.2.13 - Vulnérabilité par injection SQL (CVE-2020-14295)
999269	CVE-2020-13778	WEB-MISC RConfig antérieur à 3.9.5 - Vulnérabilité d'exécution de code à distance via ajaxEditTemplate.php (CVE-2020-13778)
999270	CVE-2020-13778	WEB-MISC RConfig antérieur à 3.9.5 - Vulnérabilité d'exécution de code à distance via ajaxAddTemplate.php (CVE-2020-13778)

Règle de signature	ID CVE	Description
999271	CVE-2020-13592	Application de gestion de projets WEB-MISC Rukovoditel - Vulnérabilité par injection SQL via selected_fields (CVE-2020-13592)
999272	CVE-2020-13592	Application de gestion de projets WEB-MISC Rukovoditel - Vulnérabilité par injection SQL via lists_id (CVE-2020-13592)
999273	CVE-2020-13591	Application de gestion de projets WEB-MISC Rukovoditel - Vulnérabilité par injection SQL (CVE-2020-13591)
999274	CVE-2020-13550	WEB-MISC Advantech WebAccess/SCADA - Vulnérabilité de traversée de chemin via FileName (CVE-2020-13550)

Mise à jour des signatures pour avril 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-04-22. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du

cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999275	CVE-2021-3378	WEB-MISC FortiLogger 4.4.2.2 - Vulnérabilité de téléchargement de fichiers arbitraires non authentifiés (CVE-2021-3378)
999276	CVE-2021-28925	Analyseur de réseau WEB-MISC Nagios antérieur à 2.4.3 - Vulnérabilité par injection SQL (CVE-2021-28925)
999277	CVE-2021-28924	Analyseur de réseau WEB-MISC Nagios antérieur à 2.4.3 - Vulnérabilité XSS (CVE-2021-28924)
999278	CVE-2021-27927	WEB-MISC Zabbix - Vulnérabilité CSRF via action=authentication.update (CVE-2021-27927)
999279	CVE-2021-26295	WEB-MISC Apache of Biz 17.12.06 - Vulnérabilité de désérialisation arbitraire non authentifiée (CVE-2021-26295)

Règle de signature	ID CVE	Description
999280	CVE-2021-25770	WEB-MISC JetBrains YouTrack avant 2020.5.3123 - Vulnérabilité d'injection de modèles côté serveur (CVE-2021-25770)
999281	CVE-2021-25283	WEB-MISC SaltStack antérieur à 3002.5 - Vulnérabilité d'exécution de code à distance (CVE-2021-25283)
999282	CVE-2021-25283	WEB-MISC SaltStack antérieur à 3002.5 - Vulnérabilité d'exécution de code à distance via un objet JSON (CVE-2021-25283)
999283	CVE-2021-24218	Plugin WEB-WORDPRESS Facebook pour WordPress antérieur à la version 3.0.4 - Vulnérabilité de script intersite stockée (CVE-2021-24218)
999284	CVE-2021-24217	Plugin WEB-WORDPRESS Facebook pour WordPress antérieur à la version 3.0.2 - Vulnérabilité d'injection d'objets PHP (CVE-2021-24217)
999285	CVE-2021-24209	Plugin Web-WORDPRESS WP Super Cache antérieur à 1.7.2 - Vulnérabilité d'exécution de code à distance dans wp-cache-config.php (CVE-2021-24209)

Règle de signature	ID CVE	Description
999286	CVE-2021-24209	Plugin Web-WORDPRESS WP Super Cache antérieur à 1.7.2 - Vulnérabilité d'injection de code arbitraire (CVE-2021-24209)
999287	CVE-2021-24165	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.4.34 - Vulnérabilité de redirection ouverte (CVE-2021-24165)
999288	CVE-2021-21975	WEB-MISC vRealize Operations Manager - Vulnérabilité de falsification de requête côté serveur non authentifiée (CVE-2021-21975)
999289	CVE-2020-35578	WEB-MISC Nagios XI antérieur à 5.8.0 - Vulnérabilité d'exécution de code à distance (CVE-2020-35578)
999290	CVE-2020-2766	WEB-MISC Oracle WebLogic Server - Vulnérabilité SSRF non authentifiée (CVE-2020-2766)
999291	CVE-2020-17523	WEB-MISC Apache Shiro antérieur à la version 1.7.1 - Vulnérabilité de contournement d'authentification via l'espace (CVE-2020-17523)
999292	CVE-2020-17523	WEB-MISC Apache Shiro antérieur à la version 1.7.1 - Vulnérabilité de contournement d'authentification via Dot (CVE-2020-17523)

Règle de signature	ID CVE	Description
999293	CVE-2020-15160	WEB-MISC PrestaShop antérieur à 1.7.6.8 - Vulnérabilité par injection SQL (CVE-2020-15160)

Mise à jour des signatures pour avril 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-04-08. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999294	CVE-2021-3273	WEB-MISC NagioSXi antérieur à la version 5.7 - Vulnérabilité par injection de code (CVE-2021-3273)

Règle de signature	ID CVE	Description
999295	CVE-2021-3197	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité d'exécution de code à distance via ssh_priv (CVE-2021-3197)
999296	CVE-2021-3197	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité d'exécution de code à distance via ssh_port (CVE-2021-3197)
999297	CVE-2021-3197	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité d'exécution de code à distance via ssh_options (CVE-2021-3197)
999298	CVE-2021-3197	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité d'exécution de code à distance via ProxyCommand dans un objet JSON (CVE-2021-3197)
999299	CVE-2021-25282	WEB-MISC SaltStack antérieur à 3002.3 - Vulnérabilité de traversée de chemin via pillar_roots.write (CVE-2021-25282)
999300	CVE-2021-24166	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.4.34 - Vulnérabilité CSRF (CVE-2021-24166)
999301	CVE-2021-24085	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'usurpation (CVE-2021-24085)

Règle de signature	ID CVE	Description
999302	CVE-2021-22986	API REST WEB-MISC F5 iControl - Vulnérabilité d'exécution de code à distance (CVE-2021-22986)
999303	CVE-2021-21978	WEB-MISC VMware View Planner Harness 4.x antérieur à 4.6 Security Patch 1 - Vulnérabilité d'exécution de code à distance (CVE-2021-21978)
999304	CVE-2020-23132	WEB-MISC Joomla! Avant 3.9.25 - Vulnérabilité du chemin de téléchargement com_media non sécurisé via file_path (CVE-2020-23132)
999305	CVE-2020-23132	WEB-MISC Joomla! Avant 3.9.25 - Vulnérabilité du chemin de téléchargement com_media non sécurisé via image_path (CVE-2020-23132)
999306	CVE-2020-22425	WEB-MISC Centreon antérieur à 20.10.4 - Vulnérabilité par injection SQL (CVE-2020-22425)

Mise à jour de signatures pour mars 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-03-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999307	CVE-2021-27065	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance (CVE-2021-27065)

Mise à jour de signatures pour mars 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-03-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999308	CVE-2021-21302	WEB-MISC PrestaShop antérieur à 1.7.7.2 - Vulnérabilité d'injection CSV (CVE-2021-21302)
999309	CVE-2020-35749	Web-WORDPRESS Simple Job Board avant 2.9.4 - Vulnérabilité de divulgation arbitraire de fichiers (CVE-2020-35749)
999310	CVE-2019-16012	WEB-MISC Cisco SD-WAN vManage antérieur à la version 19.2.2 - Vulnérabilité par injection SQL (CVE-2019-16012)

Mise à jour de signatures pour mars 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-03-09. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999311	CVE-2021-26855	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance via X-AnonResource-Backend (CVE-2021-26855)
999312	CVE-2021-26855	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance via X-BEResource (CVE-2021-26855)

Mise à jour de signatures pour mars 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-03-08. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du

cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999313	CVE-2021-25299	WEB-MISC NagioSXi Jusqu'à 5.7.5 - Vulnérabilité XSS via URL (CVE-2021-25299)
999314	CVE-2021-25298	WEB-MISC NagioSXi Jusqu'à 5.7.5 - Vulnérabilité d'exécution de code à distance via l'assistant DigitalOcean (CVE-2021-25298)
999315	CVE-2021-25297	WEB-MISC NagioSXi Jusqu'à 5.7.5 - Vulnérabilité d'exécution de code à distance via l'assistant Switch (CVE-2021-25297)
999316	CVE-2021-25296	WEB-MISC NagioSXi Jusqu'à 5.7.5 - Vulnérabilité d'exécution de code à distance via l'assistant WindowsWMI (CVE-2021-25296)
999317	CVE-2021-24164	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.4.34.1 - Vulnérabilité de divulgation d'informations (CVE-2021-24164)

Règle de signature	ID CVE	Description
999318	CVE-2021-24163	Plugin WEB-WORDPRESS Ninja Forms antérieur à 3.4.34 - Vulnérabilité de contournement d'autorisation (CVE-2021-24163)
999319	CVE-2021-21972	Plugin WEB-MISC VMware vCenter Server - Vulnérabilité d'exécution de code à distance (CVE-2021-21972)
999320	CVE-2020-35129	WEB-MISC Mautic avant 3.2.4 - Vulnérabilité XSS via un nouveau formulaire de surveillance sociale (CVE-2020-35129)
999321	CVE-2020-35129	WEB-MISC Mautic avant 3.2.4 - Vulnérabilité XSS via Edit Social Monitoring Form (CVE-2020-35129)
999322	CVE-2020-35128	WEB-MISC Mautic avant 3.2.4 - Formulaire Vulnérabilité XSS via les nouvelles entreprises (CVE-2020-35128)
999323	CVE-2020-35128	WEB-MISC Mautic avant 3.2.4 - Vulnérabilité XSS via le formulaire Edit Companies (CVE-2020-35128)
999324	CVE-2020-35125	WEB-MISC Mautic antérieur à 3.2.4 - Vulnérabilité XSS via l'en-tête de référence (CVE-2020-35125)
999325	CVE-2020-35125	WEB-MISC Mautic avant 3.2.4 - Vulnérabilité XSS via mauticform [return] (CVE-2020-35125)

Règle de signature	ID CVE	Description
999326	CVE-2020-13933	WEB-MISC Apache Shiro antérieur à la version 1.6.0 - Vulnérabilité de contournement d'authentification via un point-virgule (CVE-2020-13933)
999327	CVE-2020-13921, CVE-2020-9483	WEB-MISC Apache SkyWalking antérieur à la version 8.4.0 - Vulnérabilité par injection SQL via la fonctionnalité QueryLogs (CVE-2020-13921, CVE-2020-9483)

Mise à jour des signatures pour février 2021

May 5, 2023

De nouvelles règles de signatures sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-02-17. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999328	CVE-2021-3317	WEB-MISC KLog Server 2.4.1 et antérieur - Vulnérabilité d'injection de commandes OS (CVE-2021-3317)
999329	CVE-2021-3110	WEB-MISC PrestaShop antérieur à 1.7.7.1 - Vulnérabilité par injection SQL via id_products (CVE-2021-3110)
999330	CVE-2021-3110	WEB-MISC PrestaShop antérieur à 1.7.7.1 - Vulnérabilité par injection SQL via /module/Product-Comments/CommentGrade (CVE-2021-3110)
999331	CVE-2021-25646	WEB-MISC Apache Druid antérieur à 0.20.1 - Vulnérabilité d'exécution de code à distance (CVE-2021-25646)
999332	CVE-2020-36171	Plugin WEB-WORDPRESS Elementor Page Builder antérieur à 3.0.14 - Vulnérabilité XSS (CVE-2020-36171)
999333	CVE-2020-35765	WEB-MISC Zoho ManageEngine Applications Manager avant la version 15000 - Vulnérabilité par injection SQL (CVE-2020-35765)

Règle de signature	ID CVE	Description
999334	CVE-2020-35589	Tentatives de connexion de limite WEB-WORDPRESS rechargées avant 2.15.2 - Vulnérabilité de script intersite reflétée (CVE-2020-35589)
999335	CVE-2020-26282	Proxy BrowserUp WEB-MISC antérieur à 2.1.2 - Injection de modèle entraînant une vulnérabilité RCE via MostRecentEntry (CVE-2020-26282)
999336	CVE-2020-26282	Proxy BrowserUp WEB-MISC antérieur à 2.1.2 - Injection de modèle entraînant une vulnérabilité RCE via des entrées (CVE-2020-26282)
999337	CVE-2020-14815	WEB-MISC Oracle Business Intelligence Enterprise Edition - Vulnérabilité de script intersite reflétée (CVE-2020-14815)
999338		Addon de base de données WEB-WORDPRESS Contact Form 7 avant 1.2.5.4 - Vulnérabilité SQLi via l'action Supprimer en masse

Mise à jour des signatures pour février 2021

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2021-02-03. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999339		Connecteur WEB-MISC Zoom Meeting 4.6.348.20201217 - Vulnérabilité d'exécution de code à distance via ProxyPasswd
999340		Connecteur WEB-MISC Zoom Meeting 4.6.348.20201217 - Vulnérabilité d'exécution de code à distance via ProxyName
999341	CVE-2021-3129	WEB-MISC Ignition avant 2.5.2 - Vulnérabilité d'exécution de code à distance non authentifié (CVE-2021-3129)
999342	CVE-2021-3025	WEB-MISC Invision Community IPS Community Suite antérieure à 4.5.4.2 - Vulnérabilité d'injection SQL via SortDir (CVE-2021-3025)

Règle de signature	ID CVE	Description
999343	CVE-2021-2109	WEB-MISC Oracle WebLogic Server - Vulnérabilité d'exécution de code à distance par injection JNDI (CVE-2021-2109)
999344	CVE-2020-7200	WEB-MISC HPE Systems Insight Manager 7.6.x - Vulnérabilité liée à la désérialisation non sécurisée AMF (CVE-2020-7200)
999345	CVE-2020-7199	WEB-MISC HPE EIM avant 1.21 - Vulnérabilité d'authentification incorrecte dans /Private/EIMApplianceIP (CVE-2020-7199)
999346	CVE-2020-7199	WEB-MISC HPE EIM avant 1.21 - Vulnérabilité d'authentification incorrecte dans /Private/AdminPassReset (CVE-2020-7199)
999347	CVE-2020-7199	WEB-MISC HPE EIM avant 1.21 - Vulnérabilité d'authentification incorrecte dans /Private/ResetAppliance (CVE-2020-7199)
999348	CVE-2020-6136	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité de SQLi via DownloadWindow.php (CVE-2020-6136)

Règle de signature	ID CVE	Description
999349	CVE-2020-35729	WEB-MISC KLog Server 2.4.1 et versions antérieures - Vulnérabilité d'injection de commande du système d'exploitation (CVE-2020-35729)
999350	CVE-2020-35701	WEB-MISC Cacti 1.2.16 et versions antérieures - Vulnérabilité d'injection SQL via site_id (CVE-2020-35701)
999351	CVE-2020-35489	Formulaire de contact WEB-WORDPRESS 7 antérieur à 5.3.2 - Vulnérabilité liée au téléchargement de fichiers non restreint (CVE-2020-35489)
999352	CVE-2020-27615	Plug-in de connexion WEB-WORDPRESS avant 1.6.4 - Vulnérabilité d'injection SQL (CVE-2020-27615)
999353	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et versions antérieures - Vulnérabilité XSS via /fuel/sitevariables/create (CVE-2020-26046)
999354	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et versions antérieures - Vulnérabilité XSS via /fuel/sitevariables/edit (CVE-2020-26046)
999355	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et versions antérieures - Vulnérabilité XSS via /fuel/navigation/create (CVE-2020-26046)

Règle de signature	ID CVE	Description
999356	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et versions antérieures - Vulnérabilité XSS via /fuel/navigation/edit (CVE-2020-26046)
999357	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et versions antérieures - Vulnérabilité XSS via /fuel/blocks/create (CVE-2020-26046)
999358	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 et versions antérieures - Vulnérabilité XSS via /fuel/blocks/edit (CVE-2020-26046)
999359	CVE-2020-26045	WEB-MISC Fuel CMS 1.4.11 - Vulnérabilité dans SQLi via /fuel/permissions/create (CVE-2020-26045)
999360	CVE-2020-17519	WEB-MISC Apache Flink avant 1.11.3 - Vulnérabilité de divulgation de fichiers arbitraires (CVE-2020-17519)
999361	CVE-2020-17518	WEB-MISC Apache Flink 1.5.1 à 1.11.2 - Vulnérabilité liée au chargement de fichiers d’emplacement arbitraire (CVE-2020-17518)
999362	CVE-2019-16010	WEB-MISC Cisco SD-WAN vManage avant 19.2.2 - Vulnérabilité XSS stockée (CVE-2019-16010)

Règle de signature	ID CVE	Description
999363	CVE-2019-15000	WEB-MISC Serveur et centre de données VMware Bitbucket - Vulnérabilité d'injection de commande Git via at (CVE-2019-15000)
999364	CVE-2019-15000	WEB-MISC Serveur et centre de données VMware Bitbucket - Vulnérabilité d'injection de commande Git via Until/UntiliD (CVE-2019-15000)
999365	CVE-2019-15000	WEB-MISC Serveur et centre de données VMware Bitbucket - Vulnérabilité d'injection de commande Git via SinceID (CVE-2019-15000)

Mise à jour des signatures pour janvier 2021

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine du 18/01/2021. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999366	CVE-2020-8466	WEB-MISC Trend Micro IWSSVA 6.5 SP2 avant la build 1919 - Vulnérabilité d'injection de commande de système d'exploitation non authentifiée (CVE-2020-8466)
999367	CVE-2020-6135	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité de SQLi via Validator.php (CVE-2020-6135)
999368	CVE-2020-4001	WEB-DIVERS VMware SD-WAN Orchestrator - Vulnérabilité de transmission du hachage (CVE-2020-4001)
999369	CVE-2020-4000	WEB-MISC VMware SD-WAN Orchestrator - Vulnérabilité de traversée de chemin (CVE-2020-4000)
999370	CVE-2020-3984	WEB-MISC VMware SD-WAN Orchestrator - Vulnérabilité d'injection SQL via module (CVE-2020-3984)
999371	CVE-2020-35606	WEB-MISC Webmin jusqu'à 1.962 - Vulnérabilité d'exécution de code à distance (CVE-2020-35606)
999372	CVE-2020-17143	WEB-MISC Microsoft Exchange Server - Vulnérabilité de divulgation d'informations (CVE-2020-17143)

Règle de signature	ID CVE	Description
999373	CVE-2020-17141	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance via RouteComplaint (CVE-2020-17141)
999374	CVE-2020-10816	WEB-MISC Zoho ManageEngine Applications Manager 14 avant la build 14790 - Vulnérabilité d'authentification incorrecte (CVE-2020-10816)
999375	CVE-2019-5533	WEB-MISC VMware SD-WAN Orchestrator - Vulnérabilité de divulgation d'informations (CVE-2019-5533)
999376	CVE-2018-15961	WEB-MISC Adobe ColdFusion 12 avant la mise à jour 6 ou 14 - Vulnérabilité de téléchargement de fichier arbitraire (CVE-2018-15961)

Mise à jour des signatures pour décembre 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-12-17. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999377		Plugin WEB-WORDPRESS TI WooCommerce Wishlist avant 1.21.11 - Vulnérabilité de divulgation d'informations via tinvwl_export_settings
999378		WEB-WORDPRESS TI WooCommerce Wishlist Plugin avant 1.21.11 - Vulnérabilité de modification des options WP via tinvwl_import_settings
999379	CVE-2020-6134	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité de SQLi via MassDropModal.php (CVE-2020-6134)
999380	CVE-2020-6133	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité dans SQLi via CourseMoreInfo.php (CVE-2020-6133)
999381	CVE-2020-6132	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité dans SQLi via ChooseCP.php (CVE-2020-6132)
999382	CVE-2020-6131	WEB-MISC OS4Ed OpenSIS antérieur à 7.5 - Vulnérabilité dans SQLi via MassScheduleSessionSet.php (CVE-2020-6131)

Règle de signature	ID CVE	Description
999383	CVE-2020-6130	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité dans SQLi via MassDropSessionSet.php (CVE-2020-6130)
999384	CVE-2020-6129	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité de SQLi via CpSessionSet.php (CVE-2020-6129)
999385	CVE-2020-35234	Plugin SMTP WEB-WORDPRES Easy WP antérieur à 1.4.4 - Vulnérabilité de divulgation d'informations (CVE-2020-35234)
999386	CVE-2020-25042	WEB-MISC Mara CMS 7.5 - Vulnérabilité liée au chargement arbitraire de fichiers (CVE-2020-25042)
999387	CVE-2020-13526	WEB-MISC ProcessMaker - Vulnérabilité d'injection SQL via ClientSetupAjax (CVE-2020-13526)
999388	CVE-2020-13525	WEB-MISC ProcessMaker - Vulnérabilité d'injection SQL via ReportTables_Ajax (CVE-2020-13525)
999389	CVE-2020-12147	WEB-MISC Silver Peak Unity Orchestrator - Vulnérabilité liée aux requêtes MySQL arbitraires via l'API REST SQLExecution (CVE-2020-12147)

Règle de signature	ID CVE	Description
999390	CVE-2020-12146	WEB-MISC Silver Peak Unity Orchestrator - Vulnérabilité de traversée de chemin via l'API REST DebugFiles (CVE-2020-12146)
999391	CVE-2020-12145	WEB-MISC Silver Peak Unity Orchestrator - Vulnérabilité de contournement d'authentification (CVE-2020-12145)
999392	CVE-2019-8394	WEB-MISC Zoho ManageEngine ServiceDesk Plus avant 10.0 Build 10012 - Vulnérabilité liée au chargement arbitraire de fichiers (CVE-2019-8394)
999393	CVE-2019-11447	WEB-MISC CutePHP CuteNews 2.1.2 - Vulnérabilité d'exécution de code à distance (CVE-2019-11447)

Mise à jour des signatures pour décembre 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-12-02. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler. Dans le cadre de la mise à jour de signature version 54, la chaîne de journal pour la signature 999720 est modifiée afin de garantir qu'elle inclut uniquement des caractères ASCI.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999394	CVE-2020-8255	WEB-MISC Pulse Connect Secure avant 9.1R9 - Vulnérabilité de divulgation d'informations (CVE-2020-8255)
999395	CVE-2020-6128	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité de SQLi via CoursePeriodModal.php (CVE-2020-6128)
999396	CVE-2020-6126, CVE-2020-6127	WEB-MISC OS4Ed OpenSIS antérieur à 7.5 - Vulnérabilité de SQLi via CoursePeriodModal.php (CVE-2020-6126, CVE-2020-6127)
999397	CVE-2020-28328	WEB-MISC SuiteCRM avant 7.11.16 - Vulnérabilité d'exécution de code à distance (CVE-2020-28328)
999398	CVE-2020-27995	WEB-MISC Zoho ManageEngine Applications Manager 14 avant la build 14560 - Vulnérabilité d'injection SQL (CVE-2020-27995)

Règle de signature	ID CVE	Description
999399	CVE-2020-26879	WEB-MISC Ruckus vRioT Server avant 1.6.0 - Vulnérabilité de contournement d'autorisation via /service/ (CVE-2020-26879)
999400	CVE-2020-26879	WEB-MISC Ruckus vRioT Server avant la version 1.6.0 - Vulnérabilité de contournement d'autorisation via /reboot (CVE-2020-26879)
999401	CVE-2020-26879	WEB-MISC Ruckus vRioT Server avant la version 1.6.0 - Vulnérabilité de contournement d'autorisation via /patch/ (CVE-2020-26879)
999402	CVE-2020-26879	WEB-MISC Ruckus vRioT Server avant 1.6.0 - Vulnérabilité de contournement d'autorisation via /upgrade/ (CVE-2020-26879)
999403	CVE-2020-26879	WEB-MISC Ruckus vRioT Server avant 1.6.0 - Vulnérabilité de contournement d'autorisation via /module/ (CVE-2020-26879)
999404	CVE-2020-26878	WEB-MISC Ruckus vRioT Server avant la version 1.6.0 - Vulnérabilité d'injection de commande arbitraire dans le système d'exploitation (CVE-2020-26878)

Règle de signature	ID CVE	Description
999405	CVE-2020-25790	WEB-MISC Typesetter CMS 5.x à 5.1 - Vulnérabilité liée au téléchargement non sécurisé de fichiers (CVE-2020-25790)
999406	CVE-2020-25540	WEB-MISC ThinkAdmin v6 - Vulnérabilité de traversée de répertoires (CVE-2020-25540)
999407	CVE-2020-14883	WEB-MISC Oracle WebLogic Server - Vulnérabilité d'exécution de code à distance authentifiée (CVE-2020-14883)
999408	CVE-2020-14882, CVE-2020-14750	WEB-MISC Vulnérabilité liée au contournement de l'authentification dans Oracle WebLogic Server (CVE-2020-14882, CVE-2020-14750)
999409	CVE-2020-11975, CVE-2020-13942	WEB-MISC Apache Unomi avant la version 1.5.2 - Vulnérabilité d'exécution de code à distance (CVE-2020-11975, CVE-2020-13942)
999410	CVE-2020-11803	WEB-MISC Titan SpamTitan avant la version 7.08 - Vulnérabilité d'exécution de code à distance (CVE-2020-11803)

Mise à jour des signatures pour novembre 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la se-

maine 2020-11-10. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999411		Plug-in WordPress WEB-WORDPRESS WPDiscuz 7.0.0 Jusqu'à 7.0.4 - Vulnérabilité de téléchargement de fichiers arbitraires non authentifiés
999412		WEB-WORDPRESS Quiz & Survey Master - Vulnérabilité de script intersite dans la fonction Questions
999413		Gestionnaire de fichiers du plug-in WordPress WEB-WORDPRESS avant 6.9 - Vulnérabilité d'exécution de commandes ElFinder non authentifiées

Règle de signature	ID CVE	Description
999414	CVE-2020-11700	WEB-MISC Titan SpamTitan avant la version 7.08 - Vulnérabilité de divulgation d'informations (CVE-2020-11700)
999415	CVE-2020-9446	WEB-MISC Apache OFBiz 17.12.03 - Vulnérabilité de désérialisation non sécurisée dans XML-RPC (CVE-2020-9446)
999416	CVE-2020-9446	WEB-MISC Apache OFBiz 17.12.03 - Vulnérabilité de script intersite dans XML-RPC (CVE-2020-9446)
999417	CVE-2020-9047	Service Web WEB-MISC ExacQVision jusqu'au 20.06.3.0 - Vulnérabilité d'injection de commande du système d'exploitation (CVE-2020-9047)
999418	CVE-2020-8866	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Vulnérabilité liée au téléchargement illimité de fichiers via edit.php (CVE-2020-8866)
999419	CVE-2020-8866	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Vulnérabilité liée au téléchargement illimité de fichiers via add.php (CVE-2020-8866)

Règle de signature	ID CVE	Description
999420	CVE-2020-8865	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Vulnérabilité d'inclusion arbitraire de fichiers via edit.php (CVE-2020-8865)
999421	CVE-2020-8816	WEB-MISC Pi-hole avant 4.3.2 - Vulnérabilité d'exécution de code à distance via removeStatic (CVE-2020-8816)
999422	CVE-2020-8816	WEB-MISC Pi-hole avant 4.3.2 - Vulnérabilité d'exécution de code à distance via AddMac (CVE-2020-8816)
999423	CVE-2020-8243	WEB-MISC Pulse Connect Secure avant 9.1R8.2 - Vulnérabilité d'exécution de code à distance (CVE-2020-8243)
999424	CVE-2020-8218	WEB-MISC Pulse Connect Secure avant 9.1R8 - Vulnérabilité d'exécution de code à distance (CVE-2020-8218)
999425	CVE-2020-6143, CVE-2020-6144	WEB-MISC OS4Ed OpenSIS - Vulnérabilité d'injection de code via /install/Ins1.php (CVE-2020-6143, CVE-2020-6144)
999426	CVE-2020-6142	WEB-MISC OS4Ed OpenSIS - Vulnérabilité de traversée de chemin via modname (CVE-2020-6142)

Règle de signature	ID CVE	Description
999427	CVE-2020-6141	WEB-MISC OS4Ed OpenSIS antérieur à 7.4 - Vulnérabilité liée à SQL Li non authentifié via un nom d'utilisateur (CVE-2020-6141)
999428	CVE-2020-6140	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité liée à SQL Li non authentifié via username_stn_id (CVE-2020-6140)
999429	CVE-2020-6139	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité liée à SQL Li non authentifié via username_stf_email (CVE-2020-6139)
999430	CVE-2020-6138	WEB-MISC OS4Ed OpenSIS antérieur à 7.5 - Vulnérabilité liée à SQL Li non authentifié via uname (CVE-2020-6138)
999431	CVE-2020-6137	WEB-MISC OS4ed OpenSIS avant 7.5 - Vulnérabilité liée à SQL Li non authentifié via password_stf_email (CVE-2020-6137)
999432	CVE-2020-6125	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité dans SQLi via les paramètres GetSchool.php et u (CVE-2020-6125)
999433	CVE-2020-6124	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité dans SQLi via EmailCheckOthers.php (CVE-2020-6124)

Règle de signature	ID CVE	Description
999434	CVE-2020-6123	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité dans SQLi via EmailCheck.php et le paramètre p_id (CVE-2020-6123)
999435	CVE-2020-6123	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité SQLi via EmailCheck.php et un paramètre de messagerie (CVE-2020-6123)
999436	CVE-2020-6122	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité SQLi via CheckDuplicateStudent.php et le paramètre mn (CVE-2020-6122)
999437	CVE-2020-6121	WEB-MISC OS4ed OpenSIS avant 7.5 - Vulnérabilité SQL via CheckDuplicateStudent.php et le paramètre ln (CVE-2020-6121)
999438	CVE-2020-6120	WEB-MISC OS4Ed OpenSIS avant 7.5 - Vulnérabilité SQLi via CheckDuplicateStudent.php et le paramètre fn (CVE-2020-6120)
999439	CVE-2020-6119	WEB-MISC OS4ed OpenSIS avant 7.5 - Vulnérabilité SQLi via CheckDuplicateStudent.php et le paramètre byear (CVE-2020-6119)

Règle de signature	ID CVE	Description
999440	CVE-2020-6118	WEB-MISC OS4ed OpenSIS antérieur à 7.5 - Vulnérabilité dans SQLi via CheckDuplicateStudent.php et le paramètre bmonth (CVE-2020-6118)
999441	CVE-2020-6117	WEB-MISC OS4ed OpenSIS avant 7.5 - Vulnérabilité SQLi via CheckDuplicateStudent.php et le paramètre bday (CVE-2020-6117)
999442	CVE-2020-5780	Abonnés aux e-mails et newsletters du plug-in WordPress WEB-WORDPRESS avant 4.5.6 - Vulnérabilité de falsification de courrier électronique (CVE-2020-5780)
999443	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation non sécurisée de Java via JSON-RPC (CVE-2020-4280)
999444	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation non sécurisée de Java via RemoteMethod (CVE-2020-4280)
999445	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation non sécurisée de Java via RemoteJavaScript (CVE-2020-4280)

Règle de signature	ID CVE	Description
999446	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation non sécurisée de Java via JSON-RPC (CVE-2020-4280)
999447	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation non sécurisée de Java via RemoteMethod (CVE-2020-4280)
999448	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 et 7.4 - Vulnérabilité de désérialisation non sécurisée de Java via RemoteJavaScript (CVE-2020-4280)
999449	CVE-2020-24786	WEB-MISC Zoho ManageEngine AdManager Plus 7.0 avant la version 55 - Vulnérabilité d'authentification incorrecte (CVE-2020-24786)
999450	CVE-2020-24389	Plug-in WEB-WORDPRESS glisser-déposer de plusieurs fichiers avant 1.3.5.5 - Vulnérabilité de contournement de sécurité (CVE-2020-24389)
999451	CVE-2020-24046	WEB-MISC TitanHQ SpamTitan Gateway 7.08 - Vulnérabilité d'escalade de privilèges (CVE-2020-24046)
999452	CVE-2020-17506	WEB-MISC Artica Web Proxy 4.30.000000 - Vulnérabilité d'injection SQL dans PreAuth via un paramètre Apikey (CVE-2020-17506)

Règle de signature	ID CVE	Description
999453	CVE-2020-17505	WEB-MISC Artica Web Proxy 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via le paramètre Service-CMDS-PeForm (CVE-2020-17505)
999454	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/users/items (CVE-2020-17463)
999455	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/sitevariables/items (CVE-2020-17463)
999456	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/permissions/items (CVE-2020-17463)
999457	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/pages/items (CVE-2020-17463)
999458	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/navigation/items (CVE-2020-17463)
999459	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/logs/items (CVE-2020-17463)
999460	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - Vulnérabilité dans SQLi via /fuel/blocs/items (CVE-2020-17463)

Règle de signature	ID CVE	Description
999461	CVE-2020-16875	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance dans la stratégie DLP (CVE-2020-16875)
999462	CVE-2020-16171	WEB-MISC Acronis Cyber Backup avant 12.5 Build 16342 - Vulnérabilité liée à un en-tête de fragment dans SSRF (CVE-2020-16171)
999463	CVE-2020-14947	Inventaire OCS WEB-MISC antérieur à 2.8 - Vulnérabilité d'injection de commande du système d'exploitation via SNMP_MIB_DIRECTORY (CVE-2020-14947)
999464	CVE-2020-14947	Inventaire OCS WEB-MISC antérieur à 2.8 - Vulnérabilité d'injection de commande du système d'exploitation via mib_file (CVE-2020-14947)
999465	CVE-2020-14008	WEB-MISC Zoho ManageEngine Applications Manager jusqu'à 14710 - Vulnérabilité d'exécution de code à distance (CVE-2020-14008)
999466	CVE-2020-13925	WEB-MISC Apache Kylin avant 3.1.0 - Vulnérabilité d'exécution de code à distance via une tâche (CVE-2020-13925)

Règle de signature	ID CVE	Description
999467	CVE-2020-13925	WEB-MISC Apache Kylin avant 3.1.0 - Vulnérabilité d'exécution de code à distance via un projet (CVE-2020-13925)
999468	CVE-2020-13854	WEB-MISC Artica Pandora FMS - Vulnérabilité d'escalade de privilèges (CVE-2020-13854)
999469	CVE-2020-13405	WEB-MISC Microweber avant 1.1.20 - Vulnérabilité de divulgation d'informations non authentifiées (CVE-2020-13405)
999470	CVE-2020-13376	WEB-MISC SecurEnvoy SecurMail 9.3.503 - Vulnérabilité de traversée de chemin de cookie SecurEnvoyReply (CVE-2020-13376)
999471	CVE-2020-13159	WEB-MISC Artica Web Proxy avant 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via un domaine (CVE-2020-13159)
999472	CVE-2020-13159	WEB-MISC Artica Web Proxy avant 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via netbiosname (CVE-2020-13159)

Règle de signature	ID CVE	Description
999473	CVE-2020-13159	WEB-MISC Artica Web Proxy antérieur à 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via un alias (CVE-2020-13159)
999474	CVE-2020-13159	WEB-MISC Artica Web Proxy avant 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via un nom d'hôte (CVE-2020-13159)
999475	CVE-2020-13159	WEB-MISC Artica Web Proxy avant 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via dhclient_server (CVE-2020-13159)
999476	CVE-2020-13159	WEB-MISC Artica Web Proxy avant 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via dhclient_interface (CVE-2020-13159)
999477	CVE-2020-13159	WEB-MISC Artica Web Proxy avant 4.30.000000 - Vulnérabilité d'injection de commande du système d'exploitation via dhclient_mac (CVE-2020-13159)

Règle de signature	ID CVE	Description
999478	CVE-2020-13158	WEB-MISC Artica Web Proxy avant 4.30.000000 - Vulnérabilité de traversée de chemin via une fenêtre contextuelle (CVE-2020-13158)
999479	CVE-2020-12851	WEB-MISC Pydio Cellules antérieures à la version 2.0.7 - Vulnérabilité en écriture de fichiers arbitraires (CVE-2020-12851)
999480	CVE-2020-12848	WEB-MISC Pydio Cellules antérieures à la version 2.0.7 - Vulnérabilité liée à la connexion en tant qu'utilisateur partagé temporaire (CVE-2020-12848)
999481	CVE-2020-11699	WEB-MISC Titan SpamTitan avant la version 7.08 - Vulnérabilité d'exécution de code à distance (CVE-2020-11699)
999482	CVE-2020-11579	WEB-MISC PHPKBV9 - Vulnérabilité d'exfiltration de fichiers (CVE-2020-11579)
999483	CVE-2020-10818	WEB-MISC Artica Web Proxy 4.26 - Vulnérabilité d'injection de commande du système d'exploitation via fw.system.info.php (CVE-2020-10818)

Règle de signature	ID CVE	Description
999484	CVE-2020-10228	WEB-MISC Vtenext CE antérieur à la version 20 - Téléchargement illimité de fichiers présentant une vulnérabilité de type dangereux (CVE-2020-10228)
999485	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager avant 3.21.2 - Vulnérabilité RCE via des rôles COREUI_user (CVE-2020-10204)
999486	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager avant 3.21.2 - Vulnérabilité RCE via les privilèges COREUI_Role (CVE-2020-10204)
999487	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager avant 3.21.2 - Vulnérabilité RCE via des rôles COREUI_Role (CVE-2020-10204)
999488	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager avant 3.21.2 - Vulnérabilité RCE via le point de terminaison REST /bower/group (CVE-2020-10199)
999489	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager avant 3.21.2 - Vulnérabilité RCE via le point de terminaison REST /go/group (CVE-2020-10199)

Règle de signature	ID CVE	Description
999490	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager avant 3.21.2 - Vulnérabilité RCE via le point de terminaison REST /docker/group (CVE-2020-10199)
999491	CVE-2019-19699	WEB-MISC Centreon jusqu'à 19.10 - Vulnérabilité d'exécution de code à distance (CVE-2019-19699)
999492	CVE-2019-19499	WEB-MISC Apache Grafana jusqu'à 6.4.3 - Vulnérabilité en lecture de fichiers arbitraires (CVE-2019-19499)
999493	CVE-2019-18394	WEB-MISC Ignite Realtime Openfire jusqu'à 4.4.2 - Vulnérabilité de falsification de requête côté serveur FaviConservlet (CVE-2019-18394)
999494	CVE-2019-18393	WEB-MISC Ignite Realtime Openfire jusqu'à 4.4.2 - Vulnérabilité de traversée de répertoire de type « plug-in-servlet » (CVE-2019-18393)
999495	CVE-2019-16759	WEB-MISC vBulletin antérieur à 5.6.2 - Vulnérabilité d'exécution de code à distance via un modèle imbriqué (CVE-2019-16759)
999496	CVE-2019-15715	WEB-MISC MantisBT avant 1.3.20 et 2.22.1 - Vulnérabilité d'exécution de code à distance via neato_tool (CVE-2019-15715)

Règle de signature	ID CVE	Description
999497	CVE-2019-15715	WEB-MISC MantisBT avant 1.3.20 et 2.22.1 - Vulnérabilité d'exécution de code à distance via dot_tool (CVE-2019-15715)
999498	CVE-2019-11043	WEB-MISC PHP-FPM Versions multiples - Une vulnérabilité d'écriture hors limites permet l'exécution de code arbitraire (CVE-2019-11043)
999499		WEB-WORDPRESS plug-in WordPress Autoptimize jusqu'à 2.7.6 - Vulnérabilité de téléchargement de fichier arbitraire authentifié

Mise à jour des signatures pour octobre 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-10-29. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler. En outre, les versions vulnérables sont mentionnées dans certaines chaînes de journal des règles de signature. Vous devez l'activer en conséquence.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999500	CVE-2018-14667	WEB-MISC RichFaces Framework 3.X à 3.3.4 - Injection EL via une ressource utilisateur (CVE-2018-14667)
999501	CVE-2018-12533	WEB-MISC RichFaces Framework 3.1.0 à 3.3.4 - Injection EL via Paint2D Resource (CVE-2018-12533)
999502	CVE-2015-0279, CVE-2018-12532	WEB-MISC RichFaces Framework 4.X à 4.5.17 - Injection EL via MediaOutputResource (CVE-2015-0279, CVE-2018-12532)
999503	CVE-2013-2165	WEB-MISC RichFaces v4 avant la version 4.3.3 - Vulnérabilité liée à la désérialisation d'objets Java (CVE-2013-2165)
999504	CVE-2013-2165	WEB-MISC RichFaces v3 antérieure à 3.3.4 - Vulnérabilité de désérialisation d'objet Java (CVE-2013-2165)

Mise à jour des signatures pour octobre 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-10-13. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999505		Plug-in WordPress WEB-WORDPRESS WPDiscuz 7.0.0 Jusqu'à 7.0.4 - Vulnérabilité de téléchargement de fichiers arbitraires non authentifiés
999506		WEB-WORDPRESS Quiz & Survey Master - Vulnérabilité de script intersite dans la fonction Questions
999507	CVE-2020-8604	AV WEB-MISC Trend Micro IWS avant 6.5 SP2 Patch 4 - Vuln de traversée de chemin via /log_search et cf Param (CVE-2020-8604)
999508	CVE-2020-8604	AV WEB-MISC Trend Micro IWS avant 6.5 SP2 Patch 4 - Vuln de traversée de chemin via /collection et cf Param (CVE-2020-8604)

Règle de signature	ID CVE	Description
999509	CVE-2020-8604	AV WEB-MISC Trend Micro IWS avant 6.5 SP2 Patch 4 - Vuln de traversée de chemin via /log_search et paramètre de fichier (CVE-2020-8604)
999510	CVE-2020-8604	AV WEB-MISC Trend Micro IWS avant 6.5 SP2 Patch 4 - Vuln de traversée de chemin via /collection et paramètre de fichier (CVE-2020-8604)
999511	CVE-2020-7361	WEB-MISC ZenTao Enterprise 8.8.3 et versions antérieures - Vulnérabilité d'exécution de code à distance via Repo-Edit (CVE-2020-7361)
999512	CVE-2020-7361	WEB-MISC ZenTao Pro 8.8.3 et versions antérieures - Vulnérabilité d'exécution de code à distance via Repo-Edit (CVE-2020-7361)
999513	CVE-2020-7361	WEB-MISC ZenTao Enterprise 8.8.3 et versions antérieures - Vulnérabilité d'exécution de code à distance via Repo-Create (CVE-2020-7361)
999514	CVE-2020-7361	WEB-MISC ZenTao Pro 8.8.3 et versions antérieures - Vulnérabilité d'exécution de code à distance via Repo-Create (CVE-2020-7361)
999515	CVE-2020-5768	Plug-in pour les abonnés aux e-mails et aux newsletters WEB-WORDPRESS Icegram avant 4.5.1 - Vulnérabilité d'injection SQL (CVE-2020-5768)

Règle de signature	ID CVE	Description
999516	CVE-2020-5767	Plug-in pour les abonnés aux e-mails et aux newsletters WEB-WORDPRESS Icegram avant 4.5.1 - Vulnérabilité CSRF (CVE-2020-5767)
999517	CVE-2020-15299	Plug-in WEB-WORDPRESS KingComposer avant 2.9.5 - Vulnérabilité de script intersite (CVE-2020-15299)
999518	CVE-2020-13854	WEB-MISC Artica Pandora FMS - Vulnérabilité d'escalade de privilèges (CVE-2020-13854)
999519	CVE-2020-13852	WEB-MISC Artica Pandora FMS - Vulnérabilité liée au chargement arbitraire de fichiers via le gestionnaire de fichiers (CVE-2020-13852)
999520	CVE-2020-13700	Plug-in WEB-WORDPRESS WordPress acf-to-rest-api avant 3.3.0 - Vulnérabilité de divulgation d'informations via URI (CVE-2020-13700)
999521	CVE-2020-13700	Plug-in WEB-WORDPRESS WordPress acf-to-rest-api avant 3.3.0 - Vulnérabilité de divulgation d'informations via l'URL (CVE-2020-13700)
999522	CVE-2020-13379	WEB-MISC Grafana 3.0.1 à 7.0.1 - Contournement de CSRF menant à une vulnérabilité DOS (CVE-2020-13379)

Règle de signature	ID CVE	Description
999523	CVE-2020-12851	WEB-MISC Pydio Cellules antérieures à la version 2.0.7 - Vulnérabilité en écriture de fichiers arbitraires (CVE-2020-12851)
999524	CVE-2020-12848	WEB-MISC Pydio Cellules antérieures à la version 2.0.7 - Vulnérabilité liée à la connexion en tant qu'utilisateur partagé temporaire (CVE-2020-12848)
999525	CVE-2020-11749	WEB-MISC Artica Pandora FMS avant 7.47 - Vulnérabilité de script intersite via le navigateur SNMP (CVE-2020-11749)
999526	CVE-2020-11579	WEB-MISC PHPKBV9 - Vulnérabilité d'exfiltration de fichiers (CVE-2020-11579)
999527	CVE-2020-10546	WEB-MISC rConfig avant 3.9.5 - Vulnérabilité SQL non authentifiée dans les stratégies de conformité via SearchColumn (CVE-2020-10546)
999528	CVE-2020-10546	WEB-MISC rConfig avant 3.9.5 - Vulnérabilité SQL non authentifiée dans les stratégies de conformité via SearchField (CVE-2020-10546)
999529	CVE-2019-16876	Portainer WEB-MISC avant 1.22.1 - Vulnérabilité liée à la traversée de répertoires (CVE-2019-16876)

Règle de signature	ID CVE	Description
999530		WEB-WORDPRESS - Plug-in AdNing avant 1.5.6 - Vulnérabilité liée à la suppression de fichiers arbitraires
999531		WEB-WORDPRESS - Plug-in AdNing antérieur à 1.5.6 - Vulnérabilité de téléchargement de fichier arbitraire non authentifié

Mise à jour des signatures pour septembre 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 26/09/2020. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999532	CVE-2020-1956	WEB-MISC Apache Kylin - Exécution de code à distance de Cube Migrate via dest-config (CVE-2020-1956)
999533	CVE-2020-1956	WEB-MISC Apache Kylin - Exécution de code à distance de migration de cube via src-config (CVE-2020-1956)
999534	CVE-2020-1956	WEB-MISC Apache Kylin - Exécution de code à distance Cube Migrate via ProjectName (CVE-2020-1956)
999535	CVE-2020-3247	WEB-MISC Cisco UCS Director - Vulnérabilité liée à la création de liens symboliques arbitraires dans CopyFileRunnable (CVE-2020-3247)
999536	CVE-2019-16872	Portainer WEB-MISC avant 1.22.1 - Vulnérabilité de contrôle d'accès incorrect via des piles de mise à jour (CVE-2019-16872)
999537	CVE-2019-16872	Portainer WEB-MISC avant 1.22.1 - Vulnérabilité de contrôle d'accès incorrect via Create Stacks (CVE-2019-16872)
999538	CVE-2020-13855	WEB-MISC Artica Pandora FMS 7.44 - Vulnérabilité liée au chargement arbitraire de fichiers via le gestionnaire de référentiel de fichiers (CVE-2020-13855)

Règle de signature	ID CVE	Description
999539	CVE-2020-5902	WEB-MISC F5 BIG-IP - Vulnérabilité RCE de l'interface utilisateur de gestion du trafic via /hsqldb (CVE-2020-5902)
999540	CVE-2020-5902	WEB-MISC F5 BIG-IP - Vulnérabilité RCE de l'interface utilisateur de gestion du trafic via /tmui (CVE-2020-5902)
999541		WEB-MISC WebRP 4.15.1 et versions antérieures - Vulnérabilité de divulgation d'informations non authentifiées
999542	CVE-2020-7209	WEB-MISC HP LinuxKI avant 6.0-2 - Vulnérabilité RCE non authentifiée via timeline.php et paramètre d'horodatage (CVE-2020-7209)
999543	CVE-2020-7209	WEB-MISC HP LinuxKI avant 6.0-2 - Vulnérabilité de type RCE non authentifiée via kivis.php et ts Param (CVE-2020-7209)
999544	CVE-2020-7209	WEB-MISC HP LinuxKI avant 6.0-2 - Vulnérabilité RCE non authentifiée via kivis.php et end Param (CVE-2020-7209)
999545	CVE-2020-7209	WEB-MISC HP LinuxKI avant 6.0-2 - Vulnérabilité RCE non authentifiée via kivis.php et start Param (CVE-2020-7209)

Règle de signature	ID CVE	Description
999546	CVE-2020-7209	WEB-MISC HP LinuxKI avant 6.0-2 - Vulnérabilité RCE non authentifiée via kivis.php et pid Param (CVE-2020-7209)
999547	CVE-2020-7209	WEB-MISC HP LinuxKI avant 6.0-2 - Vulnérabilité RCE non authentifiée via kidsk_trace_view.php et end Param (CVE-2020-7209)
999548	CVE-2020-7209	WEB-MISC HP LinuxKI avant 6.0-2 - Vulnérabilité RCE non authentifiée via kidsk_trace_view.php et start Param (CVE-2020-7209)
999549		WEB-MISC PHP-Fusion avant 9.03.70 - Vulnérabilité d’injection d’objets PHP
999550	CVE-2020-1181	WEB-MISC Microsoft SharePoint Server - Exécution de code à distance via des composants WebPart (CVE-2020-1181)
999551	CVE-2020-10547	WEB-MISC rConfig avant 3.9.5 - Vulnérabilité SQL non authentifiée dans les éléments de stratégie via SearchColumn (CVE-2020-10547)
999552	CVE-2020-10547	WEB-MISC rConfig avant 3.9.5 - Vulnérabilité SQL non authentifiée dans les éléments de stratégie via SearchField (CVE-2020-10547)

Règle de signature	ID CVE	Description
999553	CVE-2020-8605	Appliance virtuelle WEB-MISC Trend Micro InterScan Web Security antérieure à la version 6.5 SP2 Patch 4 - Vulnérabilité RCE (CVE-2020-8605)
999554	CVE-2019-10068	Versions multiples WEB-MISC Kentico CMS - Vulnérabilité d'exécution de code à distance non authentifié (CVE-2019-10068)
999555	CVE-2020-11108	WEB-MISC PI-hole jusqu'à 4.4 - Vulnérabilité RCE authentifiée (CVE-2020-11108)

Mise à jour des signatures pour août 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 26/08/2020. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999556	CVE-2020-13241	WEB-MISC Microweber 1.1.18 - Chargement illimité de fichiers présentant une vulnérabilité de type dangereux (CVE-2020-13241)
999557	CVE-2020-3250	WEB-MISC Cisco UCS Director - Vulnérabilité de traversée de chemin de l'API REST via UserApiDownloadFile (CVE-2020-3250)
999558		Plug-in WEB-WORDPRESS PageBuilder KingComposer avant 2.9.4 - Suppression arbitraire de répertoires via action=bulk-delete
999559		Plugin WEB-WORDPRESS PageBuilder KingComposer avant 2.9.4 - Vulnérabilité d'exécution de code à distance via action=upload
999560	CVE-2018-1999024	WEB-MISC Moodle - Vulnérabilité de script intersite Unicode MathJax (CVE-2018-1999024)
999561	CVE-2020-13693	Plug-in WEB-WORDPRESS bbPress antérieur à 2.6.5 - Vulnérabilité d'escalade de privilèges non authentifiés (CVE-2020-13693)

Règle de signature	ID CVE	Description
999562	CVE-2020-12847	Cellules Pydio WEB-MISC antérieures à 2.0.7 - Vulnérabilité d'exécution de code à distance (CVE-2020-12847)

Mise à jour de la signature pour juillet 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 01/07/2020. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999563		Plug-in PageLayer du générateur de pages WEB-WORDPRESS avant 1.1.2 - Vulnérabilité de script intersite Via pagelayer_cf_to_email
999564		Plug-in WEB-WORDPRESS Page Builder PageLayer avant 1.1.2 - Vulnérabilité de script intersite via pagelayer-phone
999565		Plug-in PageLayer du générateur de pages WEB-WORDPRESS avant 1.1.2 - Vulnérabilité de script intersite via l'adresse pagelayer-address
999566	CVE-2020-1961	WEB-MISC Apache Syncope - Vulnérabilité d'injection de modèles côté serveur (CVE-2020-1961)
999567	CVE-2019-18935	WEB-MISC Progress Telerik UI pour ASP.NET AJAX - Vulnérabilité de désérialisation dans RadAsyncUpload .NET (CVE-2019-18935)
999568	CVE-2020-9463	WEB-MISC Centreon 19.10 - Vulnérabilité d'injection de commande du système d'exploitation (CVE-2020-9463)
999569		Plug-in de révision du support WEB-WORDPRESS avant 3.7.6 - Vulnérabilité de script intersite stocké non authentifié

Règle de signature	ID CVE	Description
999570		Plug-in WEB-WORDPRESS Page Builder PageLayer avant 1.1.2 - Vuln de contrôle d'accès incorrect via pagelayer_save_template
999571		Plug-in WEB-WORDPRESS Page Builder PageLayer avant 1.1.2 - Vuln de contrôle d'accès incorrect Via pagelayer_update_site_title
999572		Plug-in WEB-WORDPRESS Page Builder PageLayer avant 1.1.2 - Vuln de contrôle d'accès incorrect via pagelayer_save_content
999573		WEB-WORDPRESS Drag And Drop Upload pour le formulaire de contact 7 avant 1.3.3.3 - Vulnérabilité de téléchargement d'extensions
999574	CVE-2020-9314	WEB-MISC Oracle iPlanet Web Server 7.0.x - Vulnérabilité d'injection d'image (CVE-2020-9314)
999575	CVE-2020-9484	WEB-MISC Plusieurs versions d'Apache Tomcat - Désérialisation de données non fiables (CVE-2020-9484)
999576	CVE-2020-13252	WEB-MISC Centreon avant 19.04.15 - Vulnérabilité d'exécution de code à distance (CVE-2020-13252)
999577	CVE-2020-11453	WEB-MISC Microstrategy Web - Vulnérabilité CSRF via SOAP (CVE-2020-11453)

Règle de signature	ID CVE	Description
999578	CVE-2020-11453	WEB-MISC Microstrategy Web - Vulnérabilité CSRF (CVE-2020-11453)
999579	CVE-2020-7237	Cactus WEB-MISC antérieurs à 1.2.8 - Vulnérabilité d'exécution de code à distance (CVE-2020-7237)

Mise à jour de la signature pour juin 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2020-06-12. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999580	CVE-2020-6010	Plug-in LearnPress LMS WEB-WORDPRESS avant 3.2.6.9 - Vulnérabilité d'injection SQL (CVE-2020-6010)
999581		WEB-MISC Nagios XI jusqu'à 5.6.13 - Vulnérabilité d'exécution de commande arbitraire dans Service Command_Test
999582	CVE-2020-0932	Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance avec le balisage source WebPart via SOAP 1.2 (CVE-2020-0932)
999583	CVE-2020-0932	Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance avec le balisage source WebPart via SOAP 1.1 (CVE-2020-0932)
999584	CVE-2020-12642	Plug-in WEB-WORDPRESS Ninja Forms avant 3.4.24.2 - Vulnérabilité de contrefaçon de requête intersite via des champs d'importation (CVE-2020-12642)
999585	CVE-2020-12642	Plug-in WEB-WORDPRESS Ninja Forms avant 3.4.24.2 - Vulnérabilité de contrefaçon de requête intersite via un formulaire d'importation (CVE-2020-12642)
999586	CVE-2020-11450	WEB-MISC Microstrategy Web 10.4 - Vulnérabilité de divulgation d'informations (CVE-2020-11450)

Règle de signature	ID CVE	Description
999587	CVE-2020-7935	WEB-MISC Artica Pandora FMS 7.0 - Le téléchargement illimité de fichiers présentant une vulnérabilité de type dangereux autorise le RCE (CVE-2020-7935)
999588	CVE-2020-12116	WEB-MISC Zoho ManageEngine OpManager avant la build 125125 - Vulnérabilité de divulgation d'informations (CVE-2020-12116)
999589		Générateur de pages WEB-WORDPRESS Elementor avant 2.9.6 - Vulnérabilité d'escalade de privilèges
999590	CVE-2020-11738	WEB-WORDPRESS - Plug-in de duplication de Snap Creek avant 1.3.28 - Vulnérabilité de traversée de chemin (CVE-2020-11738)
999591	CVE-2020-10389	WEB-MISC Chadha PHPKB Standard multilingue 9 - Vulnérabilité d'exécution de code à distance (CVE-2020-10389)
999592	CVE-2020-11516	Plug-in WEB-WORDPRESS Contact Form 7 Datepicker jusqu'à 2.6.0 - Vulnérabilité de script intersite stocké (CVE-2020-11516)
999593		WEB-MISC Nagios XI Jusqu'à 5.6.13 - Vulnérabilité d'exécution de commande arbitraire dans Export-RRD via Step

Règle de signature	ID CVE	Description
999594		WEB-MISC Nagios XI Jusqu'à 5.6.13 - Vulnérabilité d'exécution de commande arbitraire dans Export-RRD via la fin
999595		WEB-MISC Nagios XI Jusqu'à 5.6.13 - Vulnérabilité d'exécution de commande arbitraire dans Export-RRD via Start
999596	CVE-2019-19799	Zoho ManageEngine Applications Manager antérieur à 14600 - Vulnérabilité de divulgation d'informations (CVE-2019-19799)
999597	CVE-2020-10458	WEB-MISC Chadha PHPKB Standard multilingue 9 - Vulnérabilité liée à la suppression de dossiers arbitraires (CVE-2020-10458)
999598	CVE-2017-9822	WEB-MISC DNN avant 9.1.1 - Vulnérabilité d'exécution de code à distance via le cookie DNNPersonalization (CVE-2017-9822)
999599	CVE-2020-7953	WEB-MISC OpServices OpMon 9.3.2 - Vulnérabilité de divulgation d'informations non authentifiées via le paramètre nmap_options (CVE-2020-7953)

Règle de signature	ID CVE	Description
999600	CVE-2020-7953	WEB-MISC OpServices OpMon 9.3.2 - Vulnérabilité de divulgation d'informations non authentifiées via un paramètre hôte (CVE-2020-7953)
999601		WEB-MISC Bolt CMS 3.7.0 - Renommer un fichier en une vulnérabilité de type dangereux via le paramètre newname
999602		WEB-MISC Bolt CMS 3.7.0 - Vulnérabilité de traversée de chemin via le paramètre newname
999603		WEB-MISC Bolt CMS 3.7.0 - Vulnérabilité de traversée de chemin via le paramètre oldname
999604		WEB-MISC Bolt CMS 3.7.0 - Vulnérabilité de traversée de chemin via le paramètre parent
999605		WEB-MISC Bolt CMS 3.7.0 - Vulnérabilité de validation de champ incorrecte dans le paramètre displayname
999606	CVE-2020-9004	WEB-MISC - Moteur de diffusion Wowza 4.7.8 - Vulnérabilité d'autorisation incorrecte dans les journaux View (CVE-2020-9004)

Règle de signature	ID CVE	Description
999607	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8 - Vulnérabilité d'autorisation incorrecte dans les paramètres du cache multimédia (CVE-2020-9004)
999608	CVE-2020-9004	WEB-MISC - Moteur de diffusion Wowza 4.7.8 - Vulnérabilité d'autorisation incorrecte dans les paramètres des applications (CVE-2020-9004)
999609	CVE-2020-9004	WEB-MISC - Wowza Streaming Engine 4.7.8 - Vulnérabilité d'autorisation incorrecte dans les paramètres du serveur (CVE-2020-9004)
999610		WEB-MISC PrestaShop 1.7.6.5 - Vulnérabilité CSRF via le gestionnaire de fichiers
999611	CVE-2020-10238	WEB-MISC Joomla! Précédent À 3.9.16 - Vulnérabilité de contournement de sécurité via com_templates (CVE-2020-10238)
999612	CVE-2020-11510	Plug-in LearnPress LMS WEB-WORDPRESS avant 3.2.6.9 - Escalade de privilèges via learnpress_create_page (CVE-2020-11510)
999613	CVE-2020-11510	Plug-in LearnPress LMS WEB-WORDPRESS avant 3.2.6.9 - Escalade de privilèges via learn-press_update_order_status (CVE-2020-11510)

Règle de signature	ID CVE	Description
999614	CVE-2020-8636	WEB-MISC OpServices OpMon 9.3.2 - Vulnérabilité d'exécution de code à distance non authentifiée via le paramètre nmap_options (CVE-2020-8636)
999615	CVE-2020-8636	WEB-MISC OpServices OpMon 9.3.2 - Vulnérabilité d'exécution de code à distance non authentifiée via un paramètre hôte (CVE-2020-8636)
999616	CVE-2020-11511	Plug-in LearnPress LMS WEB-WORDPRESS avant 3.2.6.9 - Augmentation de privilèges via l'acceptation d'être enseignant (CVE-2020-11511)
999617	CVE-2020-11451	WEB-MISC Microstrategy Web - Vulnérabilité de téléchargement de type de fichier non sécurisé via JSP (CVE-2020-11451)
999618	CVE-2020-11451	WEB-MISC Microstrategy Web - Vulnérabilité de téléchargement de type de fichier non sécurisé via ASP (CVE-2020-11451)
999619	CVE-2020-11515	Classement mathématique du plug-in WEB-WORDPRESS WP SEO avant 1.0.41 - Vulnérabilité de redirection via l'API REST via l'URL (CVE-2020-11515)

Règle de signature	ID CVE	Description
999620	CVE-2020-11515	WEB-WORDPRESS WP SEO Plug-in Rank Math avant 1.0.41 - Vulnérabilité de redirection via le paramètre rest_route de l'API REST (CVE-2020-11515)
999621	CVE-2020-10457	WEB-MISC Chadha PHPKB Standard multilingue 9 - Vulnérabilité liée au changement de nom de fichier arbitraire via ImgName (CVE-2020-10457)
999622	CVE-2020-10457	WEB-MISC Chadha PHPKB Standard multilingue 9 - Vulnérabilité liée au changement de nom de fichier arbitraire via ImGurl (CVE-2020-10457)
999623	CVE-2019-1821	WEB-MISC Infrastructure Cisco Prime - Vulnérabilité d'exécution de code à distance (CVE-2019-1821)
999624		Plug-in WEB-WORDPRESS Page Builder avant 2.10.16 - Vulnérabilité CSRF via Ajax action_builder_content
999625		Plug-in WEB-WORDPRESS Page Builder avant 2.10.16 - Vulnérabilité CSRF via Live Editor
999626	CVE-2020-11514	Plug-in WEB-WORDPRESS WP SEO Rank Math avant 1.0.41 - Escalade de privilèges via l'API REST via l'URL (CVE-2020-11514)

Règle de signature	ID CVE	Description
999627	CVE-2020-11514	Plug-in SEO WEB-WORDPRESS WP Classement mathématique avant 1.0.41 - Escalade de privilèges via le paramètre rest_route de l'API REST (CVE-2020-11514)
999628	CVE-2019-6713	WEB-MISC ThinkCMF avant 5.0.190312 - Vulnérabilité d'injection de code via /route/editpost.html (CVE-2019-6713)
999629	CVE-2019-6713	WEB-MISC ThinkCMF avant 5.0.190312 - Vulnérabilité d'injection de code via /route/addpost.html (CVE-2019-6713)
999630		Plug-in WEB-WORDPRESS Google Site Kit avant 1.8.0 - Vulnérabilité de vérification non protégée
999631	CVE-2020-9315	WEB-MISC Oracle iPlanet Web Server 7.0.x - Vulnérabilité de contrôle d'accès incorrect (CVE-2020-9315)
999632	CVE-2020-1947	WEB-MISC Apache ShardingSphere 4.0.0-RC3 et 4.0.0 - Vulnérabilité d'exécution de code à distance dans SnakeYaml (CVE-2020-1947)
999633	CVE-2020-7961	Liferay Portal avant 7.2.1 CE GA2 - Vulnérabilité RCE liée à la désérialisation JSON-WS via JSON-RPC (CVE-2020-7961)

Règle de signature	ID CVE	Description
999634	CVE-2020-7961	Liferay Portal avant 7.2.1 CE GA2 - Vulnérabilité RCE liée à la désérialisation JSONWS via un chemin d'URL (CVE-2020-7961)
999635	CVE-2020-7961	Liferay Portal avant 7.2.1 CE GA2 - Vulnérabilité RCE liée à la désérialisation JSONWS via une requête de formulaire et d'URI (CVE-2020-7961)
999636	CVE-2020-8518	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Vulnérabilité d'exécution de code à distance (CVE-2020-8518)
999637	CVE-2020-7351	WEB-MISC Fonality Trixbox CE 2.8.0.4 et versions antérieures - Vulnérabilité d'exécution de code à distance (CVE-2020-7351)
999638	CVE-2020-12720	WEB-MISC vBulletin antérieur au correctif de niveau 1 5.6.1 - Vulnérabilité d'injection SQL non authentifiée (CVE-2020-12720)
999639	CVE-2019-19800	Vulnérabilité liée à la traversée de chemin dans Zoho ManageEngine Applications Manager antérieure à 14520 (CVE-2019-19800)
999640	CVE-2020-10386	WEB-MISC Chadha PHPKB Standard multilingue 9 - Exécution de code à distance (CVE-2020-10386)

Règle de signature	ID CVE	Description
999641	CVE-2020-8497	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité de divulgation d'informations non authentifiées (CVE-2020-8497)
999642	CVE-2020-6009	WEB-WORDPRESS LearnDash LMS Plug-in antérieur à 3.1.6 - Vulnérabilité d'injection SQL non authentifiée (CVE-2020-6009)

Mise à jour de la signature pour juin 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 03/06/2020. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999643		WEB-WORDPRESS 10Web Map Builder pour le plug-in Google Maps avant 10.0.64 - Vulnérabilité de script intersite non authentifié via la page gmwd_setup
999644		WEB-WORDPRESS 10Web Map Builder pour le plug-in Google Maps 10.0.64 et versions antérieures - Vulnérabilité de script intersite via la page options_gmwd
999645	CVE-2020-5187	WEB-MISC DNN jusqu'à 9.4.4 - Vulnérabilité de traversée de chemin via URL (CVE-2020-5187)
999646	CVE-2020-5187	WEB-MISC DNN jusqu'à 9.4.4 - Vulnérabilité de traversée de chemin via local (CVE-2020-5187)
999647	CVE-2020-9335	Plug-in de galerie de photos WEB-WORDPRESS avant 1.5.46 - Vulnérabilité de script intersite via le champ image_alt_text_ (CVE-2020-9335)
999648	CVE-2020-9335	Plug-in WEB-WORDPRESS Photo Gallery antérieur à 1.5.46 - Vulnérabilité de script intersite via un champ de nom (CVE-2020-9335)

Règle de signature	ID CVE	Description
999649	CVE-2020-9335	Plug-in WEB-WORDPRESS Photo Gallery antérieur à 1.5.46 - Vulnérabilité de script intersite via des champs de description (CVE-2020-9335)
999650	CVE-2020-10189	WEB-MISC Zoho ManageEngine Desktop Central avant 10.0.479 - Vuln d'exécution de code à distance non authentifié (CVE-2020-10189)
999651	CVE-2020-10189	WEB-MISC Zoho ManageEngine Desktop Central avant 10.0.479 - Vuln de téléchargement de fichiers arbitraires non authentifiés (CVE-2020-10189)
999652		Champs de paiement flexibles WEB-WORDPRESS pour le plug-in WooCommerce avant 2.3.2 - Vuln de modification des paramètres non authentifiés
999653	CVE-2020-0688	WEB-MISC Microsoft Exchange Server - Vulnérabilité d'exécution de code à distance avec clé de validation (CVE-2020-0688)
999654	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité d'exécution de code à distance via le paramètre ip_src (CVE-2020-8947, CVE-2019-20224)

Règle de signature	ID CVE	Description
999655	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité d'exécution de code à distance via le paramètre dst_port (CVE-2020-8947, CVE-2019-20224)
999656	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité d'exécution de code à distance via le paramètre src_port (CVE-2020-8947, CVE-2019-20224)
999657	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Vulnérabilité d'exécution de code à distance via le paramètre ip_dst (CVE-2020-8947, CVE-2019-20224)
999658	CVE-2020-5186	WEB-MISC DNN jusqu'à 9.5.0 - Vulnérabilité de script intersite via le téléchargement XML de journal (CVE-2020-5186)
999659		Plug-in de page de site WEB-WORDPRESS WP 1.6.2 et versions antérieures - Vulnérabilité de script intersite via wsp_exclude_pages
999660	CVE-2020-5188	WEB-MISC DNN jusqu'à 9.5.0 - Vulnérabilité liée aux autorisations non sécurisées via UploadFromURL (CVE-2020-5188)

Règle de signature	ID CVE	Description
999661	CVE-2020-5188	WEB-MISC DNN jusqu'à 9.5.0 - Vulnérabilité liée aux autorisations non sécurisées via UploadFromLocal (CVE-2020-5188)
999662	CVE-2020-7799	WEB-MISC FusionAuth avant 1.11.0 - Vulnérabilité d'exécution de code à distance via un thème d'API (CVE-2020-7799)
999663	CVE-2020-7799	WEB-MISC FusionAuth avant 1.11.0 - Vulnérabilité d'exécution de code à distance via un modèle d'e-mail d'API (CVE-2020-7799)
999664	CVE-2020-7799	WEB-MISC FusionAuth avant 1.11.0 - Vulnérabilité d'exécution de code à distance via un thème graphique (CVE-2020-7799)
999665	CVE-2020-7799	WEB-MISC FusionAuth avant 1.11.0 - Vulnérabilité d'exécution de code à distance via un modèle d'e-mail graphique (CVE-2020-7799)

Mise à jour des signatures pour mai 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 26/05/2020. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler. Selon la dernière version de Snort, les règles de signature portant l'ID 1258, 1306, 2520, 2661, 5695, 10996, 11817, 12056, 15471, 17049 et 21634 ont été supprimées.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999666		Plug-in WEB-WORDPRESS Duplicator avant 1.3.28 - Vulnérabilité de téléchargement de fichiers arbitraires non authentifiés
999667	CVE-2020-10220	WEB-MISC rConfig jusqu'à 3.94 - Vulnérabilité d'injection SQL (CVE-2020-10220)
999668	CVE-2020-5844	WEB-MISC Artica Pandora FMS 7.0 - Exécution de fichiers arbitraires de type dangereux via /attachment/files_repo/ (CVE-2020-5844)
999669	CVE-2020-8813	Cactus WEB-MISC avant 1.2.10 - Vulnérabilité d'exécution de code à distance via graph_realtime.php (CVE-2020-8813)

Règle de signature	ID CVE	Description
999670	CVE-2020-8654	WEB-MISC EyesOfNetwork 5.3 - Vulnérabilité d'exécution de code à distance (CVE-2020-8654)
999671	CVE-2020-10196	Plug-in WEB-WORDPRESS Sygnoos Popup Builder avant 3.64.1 - Vulnérabilité de script intersite non authentifié (CVE-2020-10196)
999672	CVE-2019-15949	WEB-MISC Nagios XI avant 5.6.6 - Vulnérabilité liée à l'exécution de code à distance en tant que superutilisateur (CVE-2019-15949)
999673	CVE-2020-10879	WEB-MISC RConfig 3.9.5 et versions antérieures - Vulnérabilité d'exécution de code à distance via search.crud.php (CVE-2020-10879)
999674	CVE-2020-8656	WEB-MISC EyesOfNetwork 5.3 - Vulnérabilité d'injection SQL 2.4.2 dans l'API EyesOfNetwork (CVE-2020-8656)
999675	CVE-2020-10195	Plug-in WEB-WORDPRESS Sygnoos Popup Builder avant 3.64.1 - Divulgation d'informations système authentifiées (CVE-2020-10195)
999676	CVE-2020-10195	Plug-in WEB-WORDPRESS Sygnoos Popup Builder avant 3.64.1 - Divulgation d'informations d'abonné authentifié (CVE-2020-10195)

Règle de signature	ID CVE	Description
999677	CVE-2020-10195	Plug-in WEB-WORDPRESS Sygnoos Popup Builder avant 3.64.1 - Modification des paramètres authentifiés (CVE-2020-10195)
999678	CVE-2020-0646	Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance dans le workflow .NET Framework via SOAP 1.2 (CVE-2020-0646)
999679	CVE-2020-0646	Microsoft SharePoint Server - Vulnérabilité d'exécution de code à distance dans le workflow .NET Framework via SOAP 1.1 (CVE-2020-0646)
999680	CVE-2020-10221	WEB-MISC rConfig jusqu'à 3.94 - Vulnérabilité d'exécution de code à distance (CVE-2020-10221)
999681	CVE-2019-19134	WEB-WORDPRESS Hero Maps Premium avant 2.2.3 - Vulnérabilité de script intersite réfléchi non authentifié (CVE-2019-19134)
999682	CVE-2020-10385	Plug-in WEB-WORDPRESS WPForms antérieur à 1.5.9 - Vulnérabilité de script intersite stocké (CVE-2020-10385)

Mise à jour des signatures pour avril 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la se-

maine 2020-04-27. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999683	CVE-2020-9043	Plug-in WEB-WORDPRESS WPCentral avant 1.5.1 - Vulnérabilité de divulgation de clé de connexion (CVE-2020-9043)
999684		Plug-in WEB-WORDPRESS Duplicate-Post version 3.2.3 et antérieures - Script intersite persistant
999685		Plug-in WEB-WORDPRESS Duplicate-Post version 3.2.3 et antérieures - Script intersite persistant
999686	CVE-2020-0618	WEB-MISC Microsoft SQL Server Reporting Services - Vulnérabilité d'exécution de code à distance (CVE-2020-0618)

Règle de signature	ID CVE	Description
999687	CVE-2019-16278	WEB-MISC Nostromo Nhttpd avant 1.3.7 - La fonction Strcutl permet l'exécution de code à distance non authentifié (CVE-2019-16278)
999688	CVE-2019-1937	WEB-MISC Cisco UCS Director 6.6.0.0 à 6.6.1.0 et 6.7.0.0 à 6.7.1.0 - Vulnérabilité de contournement d'authentification (CVE-2019-1937)
999689		Plug-in WEB-WORDPRESS Duplicate-Post version 3.2.3 et antérieures - Script intersite persistant
999690	CVE-2020-9006	Plug-in WEB-WORDPRESS Popup Builder avant 3.0 - Vulnérabilité liée à l'injection SQL via la désérialisation de PHP (CVE-2020-9006)
999691		Plug-in WEB-WORDPRESS Duplicate-Post version 3.2.3 et antérieures - Script intersite persistant
999692		WEB-MISC empêche la contrebande de demandes via la longueur du contenu et l'en-tête de codage de transfert
999693		Plug-in WEB-WORDPRESS ThemeGrill Demo Importer avant 1.6.3 - Vulnérabilité de contournement de l'authentification

Règle de signature	ID CVE	Description
999694	CVE-2019-17237	WEB-WORDPRESS IgniteUp bientôt disponible et plug-in du mode de maintenance avant 3.4.1 - Vulnérabilité CSRF par message (CVE-2019-17237)
999695	CVE-2019-17237	WEB-WORDPRESS IgniteUp Bientôt disponible et plug-in Mode de maintenance avant 3.4.1 - Vulnérabilité CSRF via Subject (CVE-2019-17237)

Mise à jour des signatures pour février 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine du 27/02/2020. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999696	CVE-2019-15983	WEB-MISC Cisco Data Center Network Manager avant 11.3 (1) - Vulnérabilité d'entité externe XML (CVE-2019-15983) via CablePlans
999697	CVE-2019-20197	WEB-MISC Nagios XI 5.6.9 - Vulnérabilité d'exécution de commandes arbitraires authentifiées (CVE-2019-20197)
999698	CVE-2020-8417	Plug-in d'extraits de code WEB-WORDPRESS avant 2.14.0 - Vulnérabilité CSRF (CVE-2020-8417)
999699		Plug-in WEB-WORDPRESS WPCentral avant la version 1.4.8 - Vulnérabilité d'escalade de privilèges
999700	CVE-2020-8596	Plug-in de base de données des participants WEB-WORDPRESS avant 1.9.5.6 - Vulnérabilité d'injection SQL authentifiée (CVE-2020-8596)
999701	CVE-2020-8426	Plug-in WEB-WORDPRESS Elementor Page Builder avant 2.8.5 - Vulnérabilité de script intersite réfléchi authentifié (CVE-2020-8426)
999702	CVE-2019-19509	WEB-MISC RConfig 3.9.3 - Vulnérabilité d'exécution de code à distance via ajaxArchiveFiles.php (CVE-2019-19509)

Règle de signature	ID CVE	Description
999703	CVE-2019-8449	WEB-MISC Atlassian Jira Server avant la version 8.4.0 - Vulnérabilité de divulgation d'informations (CVE-2019-8449)
999704	CVE-2019-9194	WEB-MISC ElFinder avant 2.1.48 - Vulnérabilité d'injection de commande dans le connecteur PHP (CVE-2019-9194)
999705	CVE-2019-15985	WEB-MISC Cisco Data Center Network Manager avant 11.3 (1) - Vulnérabilité d'injection SQL (CVE-2019-15985) via GetVMHostData
999706	CVE-2020-8549	WEB-WORDPRESS Strong Témoignages Plug-in antérieur à 2.40.1 - Vulnérabilité de script intersite stockée (CVE-2020-8549)

Mise à jour des signatures pour février 2020

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine du 11/02/2020. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du

cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999707		Plug-in WEB-WORDPRESS WPCentral avant la version 1.4.8 - Vulnérabilité d'escalade de privilèges
999708	CVE-2019-15979	WEB-MISC Cisco Data Center Network Manager avant 11.3 (1) - Vulnérabilité d'injection de commande (CVE-2019-15979)
999709	CVE-2019-15978	WEB-MISC Cisco Data Center Network Manager avant 11.3 (1) - Vulnérabilité d'injection de commande (CVE-2019-15978)
999710	CVE-2019-15975	WEB-MISC Cisco Data Center Network Manager avant 11.3 (1) - Vulnérabilité de contournement d'authentification (CVE-2019-15975)
999711	CVE-2019-15976	WEB-MISC Cisco Data Center Network Manager avant 11.3 (1) - Vulnérabilité de contournement d'authentification (CVE-2019-15976)

Règle de signature	ID CVE	Description
999712	CVE-2019-16405	WEB-MISC Centreon avant la version 19.10.2 - Vulnérabilité d'exécution de code à distance (CVE-2019-16405)
999713	CVE-2020-7048	Plug-in de réinitialisation de la base de données WEB-WORDPRESS WP jusqu'à 3.1 - Vulnérabilité liée à la réinitialisation non authentifiée de table de base (CVE-2020-7048)
999714	CVE-2020-7108	Plug-in WEB-WORDPRESS LearnDash antérieur à la version 3.1.2 - Vulnérabilité de script intersite reflétée (CVE-2020-7108)
999715	CVE-2019-15977	WEB-MISC Cisco Data Center Network Manager avant 11.3 (1) - Vulnérabilité de contournement d'authentification (CVE-2019-15977)
999716	CVE-2020-2096	WEB-MISC Jenkins Gitlab Hook version 1.4.2 et antérieures - Vulnérabilité de script intersite (CVE-2020-2096)

Mise à jour de signature version 41

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 04/02/2020. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques. La mise à jour de la signature inclut l'ID de signature, la version de la

signature et la liste des CVE adressés.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> La version 41 de mise à jour de signature inclut un correctif pour la règle de signature incorrecte 1861.
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999717		WEB-WORDPRESS WordPress Version 5.3.x et antérieures - Vulnérabilité de déni de service via la méthode pingback.ping xmlrpc.php
999718		Sauvegarde et mise en scène WEB-WORDPRESS par plug-in WP Time Capsule avant 1.21.16 - Vulnérabilité de contournement d'authentification
999719	CVE-2019-19731	WEB-MISC Roxy Fileman pour .NET 1.4.5 - Vulnérabilité de traversée de chemin via RENAMEFILE (CVE-2019-19731)

Règle de signature	ID CVE	Description
999720	CVE-2019-19915	Redirections WEB-WORDPRESS 301 — Plug-in Easy Redirect Manager jusqu'à 2.4.0 - Vulnérabilités multiples (CVE-2019-19915)
999721	CVE-2019-17662	Logiciel WEB-MISC Cybele ThinVNC antérieur à la version 1.0b1 - Vulnérabilité liée à la traversée de répertoires (CVE-2019-17662)
999722	CVE-2020-6168	WEB-WORDPRESS Minimal bientôt disponible et plug-in du mode de maintenance avant 2.17 - Vulnérabilité du paramètre de maintenance (CVE-2020-6168)
999723	CVE-2020-6166	WEB-WORDPRESS Minimal bientôt disponible et plug-in du mode de maintenance avant 2.17 - Vulnérabilité liée au changement de thème (CVE-2020-6166)
999724	CVE-2020-6166	WEB-WORDPRESS Minimal bientôt disponible et plug-in du mode de maintenance avant 2.17 - Vulnérabilité des paramètres d'exportation (CVE-2020-6166)
999725		Plug-in du client INfiniteWP WEB-WORDPRESS avant 1.9.4.5 - Vulnérabilité de contournement

Règle de signature	ID CVE	Description
999726	CVE-2019-16773	Versions de WordPress WEB-WORDPRESS antérieures à 5.3.1 - Vulnérabilité de script intersite via l'API REST avec un objet JSON (CVE-2019-16773)
999727	CVE-2019-16773	Versions de WordPress WEB-WORDPRESS antérieures à 5.3.1 - Vulnérabilité de script intersite via l'API REST avec FORM FIELD (CVE-2019-16773)
999728	CVE-2019-16773	Versions de WordPress WEB-WORDPRESS antérieures à 5.3.1 - Vulnérabilité de script intersite via user-edit.php (CVE-2019-16773)
999729	CVE-2019-16773	Versions de WordPress WEB-WORDPRESS antérieures à 5.3.1 - Vulnérabilité de script intersite via profile.php (CVE-2019-16773)
999730	CVE-2019-16113	WEB-MISC Bludit 3.9.2 - Vulnérabilité d'exécution de code à distance lors du chargement d'images via un uuid (CVE-2019-16113)
999731	CVE-2019-16113	WEB-MISC Bludit 3.9.2 - Vulnérabilité d'exécution de code à distance lors du chargement d'images via un nom de fichier (CVE-2019-16113)

Mise à jour de signature version 40

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 14/01/2020. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques. La mise à jour de la signature inclut l'ID de signature, la version de la signature et la liste des CVE adressés.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> La version 40 de mise à jour de signature inclut un correctif pour la règle de signature incorrecte 1861.
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999732	CVE-2019-1620	WEB-MISC Cisco Data Center Network Manager avant 11.2 (1) - Vulnérabilité liée au téléchargement arbitraire de fichiers (CVE-2019-1620)
999733	CVE-2019-16702	WEB-MISC Integard Pro 2.2.0.9026 - Vulnérabilité liée au débordement de la mémoire tampon dans NoJS (CVE-2019-16702)

Règle de signature	ID CVE	Description
999734	CVE-2019-1621	WEB-MISC Cisco Data Center Network Manager avant 11.2 (1) - Vulnérabilité liée au téléchargement arbitraire de fichiers (CVE-2019-1621)
999735	CVE-2019-8451	WEB-MISC Atlassian Jira Server avant la version 8.4.0 - Vulnérabilité de contrefaçon de requête côté serveur (CVE-2019-8451)
999736		Plug-in de conformité des cookies RGPD WEB-WORDPRESS avant 4.0.3 - Vulnérabilité de suppression de paramètres arbitraires
999737	CVE-2019-11287	WEB-MISC Pivotal RabbitMQ 3.7.x avant 3.7.21 et 3.8.x avant 3.8.1 - Vulnérabilité de déni de service (CVE-2019-11287)
999738		Addons ultimes WEB-WORDPRESS pour Elementor avant 1.20.1 - Contournement d'authentification via une vulnérabilité de connexion Facebook
999739		Addons ultimes WEB-WORDPRESS pour Elementor avant 1.20.1 - Contournement d'authentification via une vulnérabilité de connexion Google

Règle de signature	ID CVE	Description
999740	CVE-2019-19366	WEB-MISC FusionPBX avant 4.4.10 - Vulnérabilité de script intersite dans xml_cdr_search.php via un paramètre de redirection (CVE-2019-19366)
999741	CVE-2019-16931	Plug-in du visualiseur WEB-WORDPRESS antérieur à la version 3.3.1 - Vulnérabilité de script intersite non authentifié (CVE-2019-16931)
999742	CVE-2019-16932	Plug-in du visualiseur WEB-WORDPRESS avant la version 3.3.1 - SSRF non authentifié (CVE-2019-16932)
999743	CVE-2019-1619	WEB-MISC Cisco Data Center Network Manager avant 11.1 (1) - Vulnérabilité de contournement d'authentification (CVE-2019-1619)
999744	CVE-2019-12562	WEB-MISC DotNetNuke avant la version 9.4.0 - Vulnérabilité de script intersite stocké (CVE-2019-12562)
999745	CVE-2019-8371	WEB-MISC OpenEMR avant 5.0.2 - Vulnérabilité d'exécution de code à distance via le champ Form_Filedata (CVE-2019-8371)
999746	CVE-2019-8371	WEB-MISC OpenEMR avant 5.0.2 - Vulnérabilité d'exécution de code à distance via le champ Form_Image (CVE-2019-8371)

Règle de signature	ID CVE	Description
999747		WEB-WORDPRESS Beaver Builder Ultimate Addons avant 1.24.1 - Contournement d'authentification via une vulnérabilité de connexion Facebook
999748		WEB-WORDPRESS Beaver Builder Ultimate Addons avant 1.24.1 - Contournement d'authentification via une vulnérabilité de connexion Google
999749	CVE-2019-19650	WEB-MISC Zoho ManageEngine AM avant la build 13640 - SQLi via servlet d'agent (CVE-2019-19650)
999750		WEB-MISC Zoho ManageEngine AM avant la build 13620 - Divulgation de la clé API via le servlet OPMRequestHandlerServlet
999751	CVE-2019-1622	WEB-MISC Cisco Data Center Network Manager 11.0 (1) - Vulnérabilité de divulgation d'informations (CVE-2019-1622)
999752	CVE-2019-16759	WEB-MISC vBulletin antérieur au correctif de niveau 1 5.5.4 - Vulnérabilité d'exécution de code à distance (CVE-2019-16759)

Règle de signature	ID CVE	Description
999753		Image présentée par WEB-WORDPRESS à partir du plug-in URL avant 2.7.8 - Contrôles d'accès manquants sur la vulnérabilité de l'API REST
999754	CVE-2019-10098	Serveur HTTP Apache WEB-MISC jusqu'à 2.4.39 - Vulnérabilité de redirection autoréférentielle mod_rewrite (CVE-2019-10098)
999755	CVE-2019-1936	WEB-MISC Cisco UCS Director 6.0 à 6.6.1.0 et 6.7.0.0 à 6.7.1.0 - Vulnérabilité d'injection de commande (CVE-2019-1936)
999756	CVE-2019-19649	WEB-MISC Zoho ManageEngine AM avant la build 13620 - SQLi non authentifié via le paramètre EventID (CVE-2019-19649)
999757	CVE-2019-19649	WEB-MISC Zoho ManageEngine AM avant la build 13620 - SQLi non authentifié via un paramètre d'entité (CVE-2019-19649)
999758	CVE-2019-15036	WEB-MISC JetBrains TeamCity avant 2019.1 - Vulnérabilité d'injection de commande du système d'exploitation (CVE-2019-15036)

Règle de signature	ID CVE	Description
999759	CVE-2019-17239	WEB-WORDPRESS Télécharger des plug-ins et des thèmes à partir du plug-in Dashboard Jusqu'à 1.5 - Vulnérabilité de script intersite stocké (CVE-2019-17239)

Mise à jour des signatures pour décembre 2019

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées au cours de la semaine 2019-12-19. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999760		Versions WEB-MISC FusionPBX antérieures aux versions 4.4.7 et 4.5.5 - Vulnérabilité d'exécution de code à distance via /app/exec/exec.php
999761	CVE-2019-12747	WEB-MISC Typo3 avant 8.7.27 et 9.5.8 - Désérialisation de données non fiables (CVE-2019-12747)
999762	CVE-2019-13608	WEB-MISC Citrix StoreFront Server - Vulnérabilité d'injection d'entité externe XML (CVE-2019-13608)
999763		WEB-WORDPRESS WordPress avant 5.2.4 - Vulnérabilité de vue non authentifiée des articles/pages privés ou brouillons via FORM
999764		WEB-WORDPRESS WordPress avant 5.2.4 - Vulnérabilité de vue non authentifiée des articles/pages privés ou brouillons via URL
999765	CVE-2019-15954	WEB-MISC Total.js CMS 12.0.0 - Vulnérabilité d'injection de code JavaScript dans un widget via JSON (CVE-2019-15954)
999766	CVE-2019-15954	WEB-MISC Total.js CMS 12.0.0 - Vulnérabilité d'injection de code JavaScript dans un widget via FORM (CVE-2019-15954)

Règle de signature	ID CVE	Description
999767		Plug-in évolué WEB-WORDPRESS SyntaxHighlighter avant 5.3.1 - Vulnérabilité de script intersite stocké via un commentaire
999768		Plug-in évolué WEB-WORDPRESS SyntaxHighlighter avant 5.3.1 - Vulnérabilité de script intersite stocké via POST
999769		Plug-in évolué WEB-WORDPRESS SyntaxHighlighter avant 5.3.1 - Vulnérabilité de script intersite stocké via JSON
999770	CVE-2019-16120	Plug-in de tickets d'événement WEB-WORDPRESS avant 4.10.7.2 - Vulnérabilité d'injection CSV (CVE-2019-16120)
999771	CVE-2019-15029	WEB-MISC FusionPBX avant la version 4.4.8 - Vulnérabilité d'exécution de code à distance (CVE-2019-15029)
999772		Plug-in de partage social WEB-WORDPRESS Sassy avant 3.3.4 - Vulnérabilité de script intersite non authentifié

Règle de signature	ID CVE	Description
999773		Plug-in pour les abonnés aux e-mails et newsletters WEB-WORDPRESS version 4.3.1 et antérieures - Vulnérabilité liée à un SQL aveugle
999774	CVE-2019-3398	WEB-MISC Atlassian Confluence ou centre de données - Vulnérabilité de traversée de chemin de téléchargement de toutes les pièces jointes (CVE-2019-3398)
999775	CVE-2019-15952	WEB-MISC Total.js CMS 12.0.0 - Vulnérabilité de traversée de chemin d'accès au modèle de page (CVE-2019-15952)
999776	CVE-2019-17236	WEB-WORDPRESS IgniteUp bientôt disponible et plug-in du mode de maintenance jusqu'à 3.4.0 - Script intersite stocké (CVE-2019-17236)
999777	CVE-2019-10475	Plug-in 1.3 de WEB-MISC Jenkins Build-Metrics - Vulnérabilité de script intersite reflétée (CVE-2019-10475)
999778	CVE-2019-17132	WEB-MISC vBulletin antérieur au correctif 5.5.4 de niveau 2 - Vulnérabilité d'exécution de code à distance dans les points de terminaison de l'API UpdateAvatar (CVE-2019-17132)

Règle de signature	ID CVE	Description
999779	CVE-2019-14994	WEB-MISC Atlassian Jira Service Desk - Vulnérabilité de traversée de chemin (CVE-2019-14994)
999780	CVE-2019-19367	WEB-MISC FusionPBX 4.4.1 et versions antérieures - Vulnérabilité de script intersite (CVE-2019-19367)
999781	CVE-2019-18668	Plug-in WEB-WORDPRESS Currency Switcher avant 2.11.2 - Vulnérabilité de contournement du paramètre de devise via POST (CVE-2019-18668)
999782	CVE-2019-18668	Plug-in WEB-WORDPRESS Currency Switcher avant 2.11.2 - Vulnérabilité de contournement du paramètre monétaire via GET (CVE-2019-18668)
999783	CVE-2019-16663	WEB-MISC RConfig 3.9.2 et versions antérieures - Vulnérabilité d'exécution de code à distance via Search.crud.php (CVE-2019-16663)
999784		WEB-MISC Apache Solr jusqu'à 8.3.0 - Exécution de code à distance non authentifié via un modèle personnalisé VelocityResponseWriter

Règle de signature	ID CVE	Description
999785	CVE-2019-17235	WEB-WORDPRESS IgniteUp bientôt disponible et plug-in du mode de maintenance jusqu'à 3.4.0 - Divulgation d'informations via Csv (CVE-2019-17235)
999786	CVE-2019-17235	WEB-WORDPRESS IgniteUp bientôt disponible et plug-in du mode de maintenance jusqu'à 3.4.0 - Divulgation d'informations via Cci (CVE-2019-17235)
999787	CVE-2019-12276	WEB-MISC GrandNode 4.40 - Vulnérabilité de traversée de chemin dans LetsEncryptController (CVE-2019-12276)
999788		Plug-in Abonnés aux e-mails et newsletters WEB-WORDPRESS avant la version 4.2.3 - Divulgation d'informations non authentifiées
999789	CVE-2019-4013	WEB-MISC IBM BigFix Platform 9.5 - Chargement de fichiers arbitraires authentifiés avec privilèges racine (CVE-2019-4013)
999790	CVE-2019-11409	WEB-MISC FusionPBX versions 4.4.3 et antérieures - Exécution de code à distance via /app/basic_operator_panel/exec.php (CVE-2019-11409)

Règle de signature	ID CVE	Description
999791	CVE-2019-11409	WEB-MISC FusionPBX versions 4.4.3 et antérieures - Exécution de code à distance via /app/operator_panel/exec.php (CVE-2019-11409)
999792	CVE-2019-16662	WEB-MISC RConfig 3.9.2 et versions antérieures - Exécution de code à distance non authentifié via AjaxServerSettingsChk.php (CVE-2019-16662)
999793	CVE-2019-7609	WEB-MISC Elastic Kibana avant 5.6.15 et 6.6.1 - Une vulnérabilité liée à la pollution par un prototype permet un RCE non authentifié (CVE-2019-7609)
999794	CVE-2019-10092	Serveur HTTP Apache WEB-MISC jusqu'à 2.4.39 - script intersite limité mod_proxy (CVE-2019-10092)
999795	CVE-2019-16520	Plug-in WEB-WORDPRESS All In One SEO Pack avant 3.2.7 - Vulnérabilité de script intersite stocké (CVE-2019-16520)
999796	CVE-2019-17234	WEB-WORDPRESS IgniteUp bientôt disponible et plug-in du mode de maintenance jusqu'à 3.4.0 - Suppression arbitraire de fichiers (CVE-2019-17234)

Règle de signature	ID CVE	Description
999797	CVE-2019-16525	Plug-in WEB-WORDPRESS Checklist antérieur à la version 1.1.9 - Vulnérabilité de script intersite (CVE-2019-16525)
999798		Plug-in SVG sécurisé WEB-WORDPRESS avant 1.9.6 - Vulnérabilité de script intersite
999799		Plug-in Abonnés aux e-mails et newsletters WEB-WORDPRESS avant la version 4.2.3 - Création d'options arbitraires non authentifiées

Mise à jour de signature version 38

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 38. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999800	CVE-2019-12517	Plug-in WEB-WORDPRESS SlickQuiz version 1.3.7.1 et antérieures - Vulnérabilité de script intersite (CVE-2019-12517)
999801	CVE-2019-10392	Plug-in 2.8.4 et versions antérieures du client Git Jenkins WEB-MISC - Vulnérabilité d'injection de commande dans le système d'exploitation (CVE-2019-10392)
999802	CVE-2019-8371	WEB-MISC OpenEMR avant 5.0.2 - Vulnérabilité d'exécution de code à distance via le champ Form_Filedata (CVE-2019-8371)
999803	CVE-2019-8371	WEB-MISC OpenEMR avant 5.0.2 - Vulnérabilité d'exécution de code à distance via le champ Form_Image (CVE-2019-8371)
999804	CVE-2019-12516	Plug-in WEB-WORDPRESS SlickQuiz version 1.3.7.1 et antérieures - Vulnérabilité d'injection SQL (CVE-2019-12516)
999805	CVE-2019-1262	WEB-MISC Microsoft SharePoint Server - Vulnérabilité de script intersite (CVE-2019-1262)

Mise à jour de signature version 37

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 37. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999806	CVE-2019-3394	WEB-MISC Atlassian Confluence ou centre de données - Vulnérabilité de divulgation de fichiers locaux (CVE-2019-3394)
999807	CVE-2019-13569	Plug-in Abonnés aux e-mails et newsletters WEB-WORDPRESS Icegram avant 4.1.8 - SQLi Via ESFPX_Lists Param (CVE-2019-13569)

Règle de signature	ID CVE	Description
999808	CVE-2019-13569	Plug-in d'abonnés aux e-mails et newsletters WEB-WORDPRESS Icegram avant 4.1.8 - SQLi Via Order Param (CVE-2019-13569)
999809	CVE-2019-2768	WEB-MISC Oracle BI Publisher - Vulnérabilité de jeton de session prévisible (CVE-2019-2768)
999810	CVE-2019-1003001	Plug-in Groovy du pipeline Jenkins WEB-MISC Jusqu'à 2,61 - Vulnérabilité de contournement du bac à sable via une mise à jour de travail (CVE-2019-1003001)
999811	CVE-2019-13575	Plug-in WEB-WORDPRESS WPEverest Everest Forms avant 1.5.0 - Injection SQL (CVE-2019-13575)
999812	CVE-2019-15896	Plug-in WEB-WORDPRESS LifterLMS jusqu'à 3.34.5 - Vulnérabilité de contournement de sécurité (CVE-2019-15896)
999813	CVE-2019-3396	WEB-MISC Atlassian Confluence ou centre de données - Vulnérabilité d'exécution de code à distance (CVE-2019-3396)
999814	CVE-2019-5475	WEB-MISC Sonatype Nexus Repository Manager avant 2.14.14 - Exécution de code à distance via le chemin Createrepo (CVE-2019-5475)

Règle de signature	ID CVE	Description
999815	CVE-2019-5475	WEB-MISC Sonatype Nexus Repository Manager avant 2.14.14 - Exécution de code à distance via le chemin du dépôt de fusion (CVE-2019-5475)
999816	CVE-2019-15104	WEB-MISC Zoho ManageEngine OpManager version antérieure à 12.4 - Vulnérabilité d'injection SQL (CVE-2019-15104)

Mise à jour de signature version 36

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 36. Vous pouvez télécharger et configurer les règles de signature pour protéger votre appliance contre les attaques vulnérables à la sécurité.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999817		Plug-in d'insertion publicitaire WordPress WEB-WORDPRESS avant la version 2.4.22 - Exécution de code à distance
999818	CVE-2019-7839	WEB-MISC Versions multiples d'Adobe ColdFusion - Vulnérabilité d'exécution de code à distance via HTTP/SOAP DotNet-to-Java (CVE-2019-7839)
999819	CVE-2019-7839	WEB-MISC Versions multiples d'Adobe ColdFusion - Vulnérabilité d'exécution de code à distance via HTTP/SOAP Java-to-DotNet (CVE-2019-7839)
999820	CVE-2019-11469	WEB-MISC Zoho ManageEngine Applications Manager antérieur à 14 Build 14150 autorise SQLi via le paramètre resourceid (CVE-2019-11469)
999821	CVE-2019-11448	WEB-MISC Zoho ManageEngine Application Manager 11.0 à 14.0 - Injection SQL non authentifiée (CVE-2019-11448)
999822	CVE-2019-1003000	Plug-in de sécurité des scripts Jenkins WEB-MISC jusqu'à 1,49 - Vulnérabilité de contournement du bac à sable (CVE-2019-1003000)

Règle de signature	ID CVE	Description
999823		Plug-in WEB-WORDPRESS WordPress Cforms2 Jusqu'à 15.0.1 - Vulnérabilité d'injection HTML non authentifiée
999824	CVE-2019-0193	WEB-MISC Apache Solr avant la version 8.2 - Vulnérabilité d'exécution de code à distance dans DIH via le paramètre DataConfig (CVE-2019-0193)
999825	CVE-2019-11580	Plug-in de développement WEB-MISC Atlassian Crowd PDKinstall activé - RCE non authentifié (CVE-2019-11580)
999826	CVE-2019-0192	WEB-MISC Apache Solr jusqu'à 5.5.5/6.6.5 - Vulnérabilité d'exécution de code à distance dans l'API de configuration (CVE-2019-0192)
999827		Plug-in WEB-WORDPRESS WooCommerce Variation Swatches jusqu'à 1.0.61 - Vulnérabilité de script intersite reflétée
999828	CVE-2019-1003001	Plug-in Groovy du pipeline Jenkins WEB-MISC Jusqu'à 2,61 - Vulnérabilité de contournement du bac à sable via la création de tâches (CVE-2019-1003001)

Règle de signature	ID CVE	Description
999829	CVE-2019-1003001	Plug-in Groovy du pipeline Jenkins WEB-MISC jusqu'à 2,61 - Vulnérabilité de contournement du bac à sable (CVE-2019-1003001)
999830		Plug-in WordPress WordPress Bold Page Builder avant 2.3.2 - Vulnérabilité de contournement de sécurité
999831	CVE-2019-15107	WEB-MISC Webmin avant 1.930 - Vulnérabilité d'exécution de code à distance non authentifié (CVE-2019-15107)
999832	CVE-2019-2767	WEB-MISC Oracle BI Publisher 11.1.1.9.0 et 12.2.1.4 - Vulnérabilité XXE (CVE-2019-2767)
999833	CVE-2019-15106	WEB-MISC Zoho ManageEngine OpManager jusqu'à 12.4x - Vulnérabilité de contournement d'authentification (CVE-2019-15106)
999948	CVE-2014-0114	Apache Struts 1 à 1.3.10 permet la manipulation de ClassLoader permettant l'exécution de code arbitraire via HTTP_FORM_FIELD
999949	CVE-2013-4316	Apache Struts 2 avant la version 2.3.15.2 autorise l'appel de méthode dynamique en affectant la confidentialité, l'intégrité ou la disponibilité

Règle de signature	ID CVE	Description
999950	CVE-2013-4316	Apache Struts 2 avant la version 2.3.15.2 autorise l'appel de méthode dynamique en affectant la confidentialité, l'intégrité ou la disponibilité

> **Remarque :**
>
> La règle de signature 999947 est supprimée en raison d'un problème de performances.

Mise à jour de signature version 35

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 35. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999834	CVE-2019-13024	WEB-MISC Centreon versions 19.04 et antérieures - Vulnérabilité d'injection de commande
999835	CVE-2019-5420	Mode de développement de WEB-MISC Rails - Vulnérabilité de divulgation
999836	CVE-2019-5418	Vue d'action de WEB-MISC Rails - Vulnérabilité de divulgation
999837	CVE-2018-12426, CVE-2019-11185	Plug-in WEB-WORDPRESS WP Live Chat Support Pro avant 8.0.26 - Téléchargement arbitraire de fichiers
999838	CVE-2019-10270	Plug-in WordPress WEB-WORDPRESS Membre ultime avant la version 2.0.40 - Réinitialisation arbitraire du mot de passe
999839	CVE-2019-12826	Logique du widget WEB-WORDPRESS Plug-in WordPress avant 5.10.2 - Vulnérabilité CSRF
999840		Calendrier des événements tout-en-un du plug-in WordPress WEB-WORDPRESS avant 2.5.39 - Vulnérabilité de script intersite
999841	CVE-2019-11565	Plug-in WordPress WEB-WORDPRESS Imprimer mon blog avant 1.6.7 - Vulnérabilité SSRF non authentifiée

Règle de signature	ID CVE	Description
999842		Plug-in WordPress WEB-WORDPRESS Membre ultime avant la version 2.0.46 - Plusieurs `cross-site scripting</LogString`

Mise à jour de signature version 34

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 34. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999843		Plug-in WordPress WEB-WORDPRESS Ultimate Member avant la version 2.0.46 - Définition d'un fichier arbitraire pour la lecture

Règle de signature	ID CVE	Description
999844		Plug-in WordPress WEB-WORDPRESS Ultimate Member avant la version 2.0.46 - Lecture arbitraire de fichiers
999845		Plug-in WordPress WEB-WORDPRESS Ultimate Member avant la version 2.0.46 - Suppression de fichiers via le remplacement de fichiers
999846		Plug-in WordPress WEB-WORDPRESS Ultimate Member avant la version 2.0.46 - Suppression de fichiers
999847		Liens courts du plug-in WordPress WEB-WORDPRESS avant 2.1.10 - Vulnérabilité d'injection CSV
999848		Liens courts du plug-in WordPress WEB-WORDPRESS avant 2.1.10 - Vulnérabilité de script intersite stocké non authentifié
999849		Plug-in WEB-WORDPRESS WordPress FV Flowplayer Video Player avant 7.3.13.727 - Vulnérabilité de script intersite stocké non authentifié

Règle de signature	ID CVE	Description
999850		Plug-in WEB-WORDPRESS WordPress Easy Digital Downloads avant 2.9.16 - Vulnérabilité de script intersite stocké non authentifié
999851		Plug-in WordPress WEB-WORDPRESS Crelly Slider avant la version 1.3.5 - Vulnérabilité de téléchargement arbitraire
999853	CVE-2019-2615	Vulnérabilité liée à la divulgation d'informations dans Oracle WebLogic Server
999854	CVE-2019-11872	Hustle du plug-in WordPress avant 6.0.8.1 - Vulnérabilité d'injection CSV
999855	CVE-2019-11231	WEB-MISC GetSimple CMS versions 3.3.15 et antérieures - Vulnérabilité liée au téléchargement arbitraire de fichiers
999856	CVE-2019-11231	WEB-MISC GetSimple CMS versions 3.3.15 et antérieures - Divulgation des informations clés de l'API
999857		WEB-WORDPRESS Plug-in WordPress Sauvegarde de base de données WP avant 5.2 - Vulnérabilité
999858		Plug-in WordPress WEB-WORDPRESS Slick Popup Jusqu'à 1.7.1 - Vulnérabilité d'escalade de privilèges

Règle de signature	ID CVE	Description
999859	CVE-2019-12099	Vulnérabilité d'exécution de code à distance WEB-MISC PHP Fusion CMS dans les versions 9.03.00 et antérieures

Mise à jour de signature version 33

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 33. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions .

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Rule	CVE	Description	Référence de vulnérabilité
999860		Plug-in WordPress Yuzo Articles connexes Vulnérabilité de script intersite	https://www.wordfence.com/blog/2019/04/yuzo-related-posts-zero-day-vulnerability-exploited-in-the-wild
999861	CVE-2019-12099		cve,2019-12099
999862		Plug-in WordPress Sauvegarde de base de données <= 5.2 - Exécution de code	https://www.wordfence.com/blog/2019/05/os-command-injection-vulnerability-patched-in-wp-database-backup-plug-in
999863		Plug-in WordPress Slick Popup - Escalade de privilèges	https://www.wordfence.com/blog/2019/05/privilege-escalation-flaw-present-in-slick-popup-plug-in
999864	CVE-2019-10866	Plug-in WordPress Form Maker 1.13.3 - Injection SQL	cve,2019-10866
999865		Plug-in WordPress Give — Script intersite stocké pour les donateurs	https://blog.sucuri.net/2019/05/wordpress-plug-in-give-stored-xss-for-donors.html

Rule	CVE	Description	Référence de vulnérabilité
999866		Plug-in WordPress My Calendar <= 3.1.9 - Vulnérabilité de script intersite non authentifié	https://wpvulndb.com/vulnerabilities/9267
999867		Plug-in WordPress Slimstat <= 4.8 - Script intersite stocké non authentifié	https://blog.sucuri.net/2019/05/slimstat-stored-xss-from-visitors.html
999868	CVE-2019-2618	Vulnérabilité liée au téléchargement arbitraire	cve,2019-2618
999869	CVE-2019-11871	Suite de champs personnalisés du plug-in WordPress WEB-WORDPRESS avant 2.5.15 - Vulnérabilité de script intersite	cve,2019-11871
999870		WEB-WORDPRESS WordPress Prise en charge du chat en direct Plug-in Script intersite persistant Vulnérabilité antérieure à 8.0.27 via le paramètre wplc_custom_js	https://blog.sucuri.net/2019/05/persistent-cross-site-scripting-in-wp-live-chat-support-plug-in.html

Rule	CVE	Description	Référence de vulnérabilité
999871		Plug-in WEB-WORDPRESS WordPress W3 Total Cache avant 0.9.7.4 - Vulnérabilité d'exécution de code à distance PHAR	https://wpvulndb.com/vulnerabilities/9270
999872		Plug-in WEB-WORDPRESS WordPress W3 Total Cache avant 0.9.7.4 - Vulnérabilité d'exécution de code à distance PHAR	https://wpvulndb.com/vulnerabilities/9269
999873	CVE-2019-0604	WEB-DIVERS Microsoft Windows Sharepoint Server - Vulnérabilité d'exécution de code à distance	cve,2019-0604
999874		WEB-WORDPRESS Yuzo Related Posts Vulnérabilité de script intersite stocké non authentifié dans 5.12.91	https://www.wordfence.com/blog/2019/04/yuzo-related-posts-zero-day-vulnerability-exploited-in-the-wild

Mise à jour de signature version 32

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 32. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre

les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999875	CVE-2016-4438, CVE-2016-3087	WEB-STRUTS Vulnérabilité d'exécution à distance via URL dans Apache Struts 2.3.20 à 2.3.28.1
999876	CVE-2019-10867	WEB-MISC Pimcore avant 5.7.1 - Vulnérabilité liée à la désérialisation (CVE-2019-10867)

Mise à jour de signature version 30

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 30. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

> **Remarque :**
>
> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999879	<>	Plug-in WordPress WEB-MISC WooCommerce Checkout Manager - Vulnérabilité de téléchargement
999880	<>	Plug-in WEB-MISC WordPress Advance Contact Form 7 DB avant 1.6.1 - Vulnérabilité d'injection SQL
999881	<>	Plug-in WordPress WEB-MISC Contact Form Builder avant 1.0.67 - Vulnérabilité d'inclusion de fichiers locaux
999882	<>	Tentative d'injection aveugle d'URI HTTP
999883	<>	Plugin WordPress WEB-MISC Loco Translate 2.1.1 et versions antérieures - Vulnérabilité d'inclusion de fichiers locaux
999884	<>	Page dupliquée du plug-in WordPress WEB-MISC avant 3.4 - Vulnérabilité d'injection SQL

Règle de signature	ID CVE	Description
999885	CVE-2019-0232	WEB-MISC Apache Tomcat RCE via des scripts CGI .CMD lorsque EnableCmdLineArguments=True dans MS Windows
999886	CVE-2019-0232	WEB-MISC Apache Tomcat RCE via des scripts CGI .BAT lorsque EnableCmdLineArguments=True dans MS Windows
999887	CVE-2019-10692	Plug-in WWEB-MISC WordPress wp-google-maps avant 7.11.18 - Vulnérabilité d'injection SQL.
999888	CVE-2019-10946	WEB-MISC Joomla! Avant 3.9.5 - Vulnérabilité de contournement de sécurité
999889	CVE-2019-10945	WEB-MISC Joomla! Avant 3.9.5 - Vulnérabilité liée à la traversée de répertoires
999890	CVE-2019-9912	Plug-in WordPress WEB-MISC WPGoogleMaps avant 7.10.41 Vulnérabilité de script intersite reflétée
999890	CVE-2019-9912	Plug-in WordPress WEB-MISC WPGoogleMaps avant 7.10.41 Vulnérabilité de script intersite reflétée
999891	CVE-2019-9911	Affiche automatique des réseaux sociaux du plug-in WordPress WEB-MISC avant 4.2.8 - Vulnérabilité de script intersite reflétée
999892	CVE-2019-9908	Plug-in WordPress WEB-MISC Font_Organizer 2.1.1 - Script intersite reflété

Règle de signature	ID CVE	Description
999893	CVE-2019-9787	WEB-MISC WordPress avant 4.9.7 - Vulnérabilité d'exécution de code à distance
999894	CVE-2019-9568	Formulaire de contact WEB-MISC Forminator, Plug-in WordPress Poll & Quiz Builder avant 1.6 Vulnérabilité Blind SQLi
999895	CVE-2019-9567	Formulaire de contact WEB-MISC Forminator, plug-in WP Poll & Quiz Builder avant 1.6 Vulnérabilité persistante de script intersite
999877	CVE-2018-20062	WEB-MISC NoneCMS V1.3 - Vulnérabilité d'exécution de code PHP arbitraire dans le filtre ThinkPHP
999878	CVE-2019-9082	Vulnérabilité d'exécution de code à distance WEB-MISC dans ThinkPHP 5.x avant 5.1.32

Mise à jour de signature version 29

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 29. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

Remarque :

> L'activation des règles de signature du corps du message et du corps de réponse peut affecter le processeur NetScaler.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999896	CVE-2019-2725	Weblogic 10.3.6 Exécution de code à distance
999897	CVE-2019-2725	Weblogic 10.3.6 Exécution de code à distance

Mise à jour de signature version 28

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 28. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques. La mise à jour de la signature inclut l'ID de signature, la version de la signature et la liste des CVE adressés.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999898	CVE-2018-12895	WEB-MISC WordPress avant 4.9.7 Vulnérabilité de traversée de répertoires.
999899	CVE-2019-9618	Web-misc-Gracemedia Media Player Plug-in WordPress 1.0 Vulnérabilité d'inclusion arbitraire de fichiers locaux
999900	CVE-2018-20714	Plugin WordPress WEB-MISC WooCommerce avant 3.4.6 - Vulnérabilité de suppression de fichiers.
999901	CVE-2018-11868	WEB-MISC FlowPaper FlexPaper avant la version 2.3.7 peut permettre l'exécution de code à distance-réinitialisation des fichiers de configuration.
999902	CVE-2018-11868	WEB-MISC FlowPaper FlexPaper avant 2.3.7 peut permettre l'exécution de code à distance.
999903	CVE-2019-9184	Joomla ! Plug-in J2Store 3.x avant 3.3.7 Autorise l'injection SQL.
999904	CVE-2019-9168	Plug-in WordPress WEB-MISC WooCommerce avant le script intersite 3.5.5 via la légende Photoswipe.
999905		Plug-in WordPress WEB-MISC Panier abandonné avant 5.1.3 pour le script intersite stocké dans WooCommerce.
999906	CVE-2019-8942	WEB-MISC WordPress avant 4.9.9 et 5.x avant 5.0.1 exécution de code à distance.

Règle de signature	ID CVE	Description
999907	CVE-2019-8942	WEB-MISC WordPress avant 4.9.9 et 5.x avant 5.0.1 exécution de code à distance.
999908	CVE-2019-8942	WEB-MISC WordPress avant 4.9.9 et 5.x avant 5.0.1 exécution de code à distance
999909	CVE-2017-16562	Thème Web-misc-Deluxe Vulnérabilité de contournement de sécurité du plug-in WordPress UserPro via up_auto_log=true Paramètre
999910	CVE-2018-20782	Plug-in WordPress WEB-MISC GloBee avant 1.1.2 pour l'usurpation de messages WooCommerce-IPN
999911	CVE-2019-6340	Exécution de code à distance Drupal arbitraire dans Drupal Core 8 RESTful WebServices

Mise à jour de signature version 27

May 5, 2023

De nouvelles règles de signature sont générées pour les vulnérabilités identifiées dans la version 27. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques. La mise à jour de la signature inclut l'ID de signature, la version de la signature et la liste des CVE adressés.

Version de signature

Les signatures sont compatibles avec les versions logicielles suivantes de Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 et 13.1.

La version 12.0 de NetScaler est en fin de vie (EOL). Pour plus d'informations, consultez la page du cycle de vie des versions.

Aperçu de Common Vulnerability Entry (CVE)

Vous trouverez ci-dessous une liste des règles de signature, des identifiants CVE et de leur description.

Règle de signature	ID CVE	Description
999921	cve-2018-1002000	Vulnérabilité de répondeur automatique Web-miscWordPress Arigato et d'injection SQL Newsletter.
999920		Plug-in Web-miscWordPress Corner Ad 1.0.7 - Script intersite stocké
999919	cve-2018-1002009	Vulnérabilité de script intersite Web-miscWordPress Arigato Autoresponder et Newsletter bft_unsubscribe.
999918	cve-2018-1002002	Vulnérabilité de script intersite multiple Web-miscWordPress Arigato Autoresponder et Newsletter.
999918	cve-2018-1002003	Vulnérabilité de script intersite multiple Web-miscWordPress Arigato Autoresponder et Newsletter.
999918	cve-2018-1002004	Vulnérabilité de script intersite multiple Web-miscWordPress Arigato Autoresponder et Newsletter.
999918	cve-2018-1002005	Vulnérabilité de script intersite multiple Web-miscWordPress Arigato Autoresponder et Newsletter.
999918	cve-2018-1002006	Vulnérabilité de script intersite multiple Web-miscWordPress Arigato Autoresponder et Newsletter.

Règle de signature	ID CVE	Description
999918	cve-2018-1002007	Vulnérabilité de script intersite multiple Web-miscWordPress Arigato Autoresponder et Newsletter.
999917	cve-2018-1002001	Vulnérabilité de script intersite multiple Web-miscWordPress Arigato Autoresponder et Newsletter.
999917	cve-2018-1002008	Vulnérabilité de script intersite multiple Web-miscWordPress Arigato Autoresponder et Newsletter.
999916	cve-2018-8719	Journal d'audit de sécurité WP plug-in Web-miscWordPress - wp-content/uploads/wp-security-audit-log/* accès illimité
999915	cve-2019-7743	WEB-MISC- Joomla phar:// vulnérabilité d'injection d'objet d'enveloppe de flux exécution de fichiers non phar téléchargés
999914		Plug-in Web-miscWordPress Abonnés aux e-mails et newsletters 3.4.7 vulnérabilité de divulgation d'informations
999913		Plug-in Web-miscWordPress AD Manager WD v1.0.11 - wd_ads_admin_class.php Téléchargement de fichier arbitraire
999912		WEB-IISMicrosoft IIS - Divulgation du nom de fichier/dossier court

Gestion des bots

May 5, 2023

Parfois, le trafic Web entrant est composé de bots et la plupart des organisations souffrent d'attaques de bot. Les applications Web et mobiles sont des moteurs de revenus importants pour les entreprises et la plupart des entreprises sont menacées par des cyberattaques avancées, telles que les robots.
Un bot est un logiciel qui effectue automatiquement certaines actions à plusieurs reprises à un rythme beaucoup plus rapide qu'un humain. Les robots peuvent interagir avec des pages Web, envoyer des formulaires, exécuter des actions, numériser des textes ou télécharger du contenu. Ils peuvent accéder à des vidéos, publier des commentaires et tweeter sur les plateformes de réseaux sociaux. Certains robots, appelés chatbots, peuvent tenir des conversations de base avec des utilisateurs humains.
Un bot qui fournit un service utile, tel que le service client, le chat automatisé et les robots d'exploration des moteurs de recherche, est un bon robot. Dans le même temps, un bot qui peut capturer ou télécharger du contenu à partir d'un site Web, voler des informations d'identification d'utilisateur, du contenu de spam et effectuer d'autres types de cyberattaques est un bot malveillant. Compte tenu du grand nombre de robots malveillants exécutant des tâches malveillantes, il est essentiel de gérer le trafic des robots et de protéger vos applications Web contre les attaques de robots. En utilisant la gestion des bots NetScaler, vous pouvez détecter le trafic de bots entrant et atténuer les attaques de bots afin de protéger vos applications Web.
La gestion des robots NetScaler permet d'identifier les robots malveillants et de protéger votre appliance contre les attaques de sécurité avancées. Il détecte les bots bons et les bots malveillants et identifie si le trafic entrant est une attaque de bot. En utilisant la gestion des bots, vous pouvez atténuer les attaques et protéger vos applications Web.

La gestion des robots NetScaler offre les avantages suivants :

- **Défendez-vous contre les robots, les scripts et les boîtes à outils**. Fournit une atténuation des menaces en temps réel grâce à une défense basée sur les signatures statiques et à l'empreinte digitale des appareils.
- **Neutralisez les attaques automatisées de base et avancées**. Empêche les attaques, telles que les DDoS de couche d'application, la pulvérisation de mot de passe, le remplissage de mot de passe, les racleurs de prix et les racleurs de contenu.
- **Protégez vos API et vos investissements**. Protège vos API contre les utilisations abusives et protège les investissements d'infrastructure contre le trafic automatisé.

Voici quelques cas d'utilisation dans lesquels vous pouvez tirer parti du système de gestion des bots NetScaler :

- Connexion par force brute. Un portail Web gouvernemental est constamment attaqué par des robots qui tentent de forcer brutalement les connexions des utilisateurs. L'organisation a décou-

vert l'attaque en consultant des journaux Web et en constatant que des utilisateurs spécifiques étaient sélectionnés à maintes reprises, lors de tentatives de connexion rapides et en incrémentant les mots de passe à l'aide d'une approche d'attaque par dictionnaire. En vertu de la loi, ils doivent se protéger eux-mêmes et protéger leurs utilisateurs. En déployant la solution de gestion des robots NetScaler, ils peuvent arrêter la connexion par force brute à l'aide de techniques d'identification des appareils et de limitation du débit.

- Bloquez les robots malveillants et les robots inconnus par empreinte digitale d'appareil Une entité Web reçoit 100 000 visiteurs par jour. Ils doivent améliorer leur empreinte sous-jacente et ils dépensent une fortune. Lors d'un récent audit, l'équipe a découvert que 40 % du trafic provenait de robots, du scraping de contenu, de la sélection d'actualités, de la vérification des profils des utilisateurs, etc. Ils souhaitent bloquer ce trafic pour protéger leurs utilisateurs et réduire leurs coûts d'hébergement. Grâce à la gestion des bots, ils peuvent bloquer les robots malveillants connus et identifier les robots inconnus qui s'attaquent à leur site. En bloquant ces bots, ils peuvent réduire le trafic de bots de 90 %.

À quoi sert la gestion des robots NetScaler ?

La gestion des bots de NetScaler aide les entreprises à protéger leurs applications Web et leurs actifs publics contre les attaques de sécurité avancées. Lorsqu'un trafic entrant est un bot, le système de gestion du bot détecte le type de bot, attribue une action et génère des informations sur les robots, comme indiqué dans le diagramme suivant.



Comment fonctionne la gestion des robots NetScaler

Le schéma suivant montre le fonctionnement de la gestion des bots NetScaler. Le processus implique huit techniques de détection qui permettent de détecter le trafic entrant comme un bon ou un mauvais robot. Par défaut, les bons robots détectés par les signatures sont autorisés et les robots défectueux détectés par les signatures sont supprimés.



1. Le processus commence par l'activation de la fonctionnalité de gestion des robots sur l'appliance.
2. Lorsqu'un client envoie une demande, l'appliance évalue le trafic à l'aide des règles de politique relatives aux robots. Si la demande entrante est identifiée comme étant un robot, l'appliance applique un profil de détection de robots.
3. Vous devez lier le fichier de signature de robot par défaut ou personnalisé au profil de détection des robots. Le fichier de signature de bot contient une liste de règles de signature de bot permettant d'identifier le type de bot entrant.
4. Les règles de détection des robots sont disponibles dans huit catégories de détection dans le fichier de signature. Les catégories sont la liste d'autorisation, la liste de blocage, la signature statique, la réputation IP, l'empreinte digitale de l'appareil et la limitation de débit. Sur la base du trafic des robots, le système applique une règle de détection au trafic.
5. Si le trafic bot entrant correspond à une entrée de la liste des robots autorisés, le système contourne les autres techniques de détection et l'action associée consigne les données.
6. Pour les techniques de détection autres que la liste d'autorisation des robots, si une demande entrante correspond à une règle configurée, l'action correspondante est appliquée. Les actions possibles sont le dépôt, la redirection, la réinitialisation, l'atténuation et le journal. CAPTCHA est une action d'atténuation prise en charge pour la réputation IP, les empreintes digitales des appareils et les techniques de détection TPS.

Détection de bot

July 31, 2023

Le système de gestion des bots NetScaler utilise différentes techniques pour détecter le trafic de bots entrant. Les techniques sont utilisées comme règles de détection pour détecter le type de bot. Les techniques sont les suivantes :

> **Remarque :**
>
> La gestion des bots prend en charge un maximum de 32 entités de configuration pour les techniques de liste de blocage, de liste d'autorisation et de limitation de débit.

Liste de**robots autorisés : liste** personnalisée d'adresses IP (IPv4 et IPv6), de sous-réseaux (IPv4 et IPv6) et d'expressions de politique qui peuvent être ignorées en tant que liste autorisée.

Liste de robots bloqués : liste personnalisée d'adresses IP (IPv4 et IPv6), de sous-réseaux (IPv4 et IPv6) et d'expressions de politique dont l'accès à vos applications Web doit être bloqué.

Réputation IP : cette règle détecte si le trafic entrant du bot provient d'une adresse IP malveillante.

Empreinte de l'appareil : cette règle détecte si le trafic bot entrant contient l'identifiant de l'empreinte digitale de l'appareil dans l'en-tête de la demande entrante et les attributs de navigateur d'un trafic bot client entrant.

> **Limitation :**
>
> 1. JavaScript doit être activé dans le navigateur client.
> 2. Ne fonctionne pas pour les réponses XML.

Expression du journal des robots : la technique de détection vous permet de capturer des informations supplémentaires sous forme de messages de journal. Les données peuvent être le nom de l'utilisateur qui a demandé l'URL, l'adresse IP source et le port source à partir duquel l'utilisateur a envoyé la demande ou les données générées à partir d'une expression.

Limite de débit - Cette règle limite le taux de plusieurs demandes provenant du même client.

Trap de robots : détecte et bloque les robots automatisés en publiant une URL de piège dans la réponse du client. L'URL apparaît invisible et n'est pas accessible si le client est un utilisateur humain. La technique de détection est efficace pour bloquer les attaques de robots automatisés.

TPS - Détecte le trafic entrant sous forme de robots si le nombre maximum de demandes et le pourcentage d'augmentation des demandes dépassent l'intervalle de temps configuré.

CAPTCHA - Cette règle utilise un CAPTCHA pour atténuer les attaques de robots. Un CAPTCHA est une validation de question-réponse pour déterminer si le trafic entrant provient d'un utilisateur humain ou d'un robot automatisé. La validation permet de bloquer les bots automatisés qui causent des vio-

lations de sécurité aux applications Web. Vous pouvez configurer CAPTCHA en tant qu'action de bot dans les techniques de réputation IP et de détection des empreintes digitales de l'appareil.

Voyons maintenant comment configurer chaque technique pour détecter et gérer le trafic de votre bot.

Comment mettre à niveau votre appliance vers une configuration de gestion des bots basée sur NetScaler CLI

Si vous mettez à niveau votre appliance à partir d'une version plus ancienne (NetScaler version 13.0 build 58.32 ou antérieure), vous devez d'abord convertir manuellement la configuration de gestion des bots existante en configuration de gestion des bots basée sur NetScaler CLI une seule fois. Suivez les étapes suivantes pour convertir manuellement votre configuration de gestion des bots.

1. Après la mise à niveau vers la dernière version, connectez-vous à l'outil de mise à niveau "upgrade_bot_config.py" à l'aide de la commande suivante

   À l'invite de commande, tapez :

   ```
   shell "/var/python/bin/python /netscaler/upgrade_bot_config.py > /var/bot_upgrade_commands.txt"
   ```

2. Exécutez la configuration à l'aide de la commande suivante.

   À l'invite de commande, tapez :

   ```
   batch -f /var/bot_upgrade_commands.txt
   ```

3. Enregistrez la configuration mise à niveau.

```
save ns config
```

Configurer la gestion des bots basée sur NetScaler CLI

La configuration de la gestion des bots vous permet de lier une ou plusieurs techniques de détection de bots à un profil de bot spécifique.
Vous devez suivre les étapes suivantes pour configurer la gestion des bots basée sur NetScaler :

1. Enable bot management
2. Import bot signature
3. Add bot profile
4. Bind bot profile
5. Add bot policy
6. Bind bot policy
7. Configure bot settings

> **Remarque :**
>
> Si vous mettez à niveau votre appliance à partir d'une version antérieure, vous devez d'abord convertir manuellement la configuration existante de gestion des robots. Pour plus d'informations, consultez la section Comment effectuer une mise à niveau vers la configuration de la gestion des bots basée sur NetScaler CLI .

Enable bot management

Avant de commencer, assurez-vous que la fonctionnalité de gestion des bots est activée sur l'appliance. Si vous possédez un nouveau NetScaler ou VPX, vous devez activer la fonctionnalité avant de la configurer. Si vous mettez à niveau un dispositif NetScaler d'une version antérieure vers la version actuelle, vous devez activer la fonctionnalité avant de la configurer. À l'invite de commande, tapez :

```
enable ns feature Bot
```

Import bot signature

Vous pouvez importer le fichier bot de signature par défaut et le lier au profil de robot. À l'invite de commande, tapez :

```
import bot signature [<src>] <name> [-comment <string>] [-overwrite]
```

Où :

`src` - Nom du chemin local ou URL (protocole, hôte, chemin et nom de fichier). Longueur maximale : 2047.
> **Remarque :**
>
> L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS qui nécessite l'authentification par certificat client pour y accéder.

`name` - Nom de l'objet du fichier de signature du bot. Il s'agit d'un argument obligatoire. Longueur maximale : 31.

`comment` - Description de l'objet du fichier de signature. Longueur maximale : 255.

`overwrite` - Action qui remplace le fichier existant.
> **Remarque :**
>
> Utilisez l' `overwrite` option pour mettre à jour le contenu du fichier de signature. Vous pouvez également utiliser la `update bot signature <name>` commande pour mettre à jour le fichier de signature sur l'appliance NetScaler.

Exemple

```
import bot signature http://www.example.com/signature.json signaturefile -
comment commentsforbot -overwrite
```

> **Remarque :**
>
> Vous pouvez utiliser l'option de remplacement pour mettre à jour le contenu du fichier de signature. Vous pouvez également utiliser la `update bot signature <name>` commande pour mettre à jour le fichier de signature dans l'appliance NetScaler.

Add bot profile

Un profil de bot est un ensemble de paramètres de profil permettant de configurer la gestion des bots sur l'appliance. Vous pouvez configurer les paramètres pour effectuer la détection des bots.

À l'invite de commande, tapez :

```
add bot profile <name> [-signature <string>] [-errorURL <string>] [-trapURL
 <string>] [-whiteList ( ON | OFF )] [-blackList ( ON | OFF )] [-rateLimit
( ON | OFF )] [-deviceFingerprint ( ON | OFF )] [-deviceFingerprintAction (
 none | log | drop | redirect | reset | mitigation )] [-ipReputation ( ON |
 OFF )] [-trap ( ON | OFF )]
```

Exemple :

```
add bot profile profile1 -signature signature -errorURL http://www.example
.com/error.html -trapURL /trap.html -whitelist ON -blacklist ON -ratelimit
 ON -deviceFingerprint ON -deviceFingerprintAction drop -ipReputation ON -
trap ON
```

Bind bot profile

Après avoir créé un profil de bot, vous devez lier le mécanisme de détection des bots au profil.

À l'invite de commande, tapez :

```
bind bot profile <name> | (-ipReputation [-category <ipReputationCategory>]
 [-enabled ( ON | OFF )] [-action ( none | log | drop | redirect | reset |
mitigation )] [-logMessage <string>]
```

Exemple :

L'exemple suivant concerne la liaison de la technique de détection de réputation IP à un profil de bot spécifique.

```
bind bot profile profile5 -ipReputation -category BOTNET -enabled ON -
action drop -logMessage message
```


Add bot policy

Vous devez ajouter la stratégie de bot pour évaluer le trafic des robots.

À l'invite de commande, tapez :

```
add bot policy <name> -rule <expression> -profileName <string> [-undefAction
 <string>] [-comment <string>] [-logAction <string>]
```

Où,

`Name`- Nom de la politique relative aux robots. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Peut être modifié après l'ajout de la stratégie de bot.

`Rule`- Une expression que la politique utilise pour déterminer s'il convient d'appliquer le profil de bot à la demande spécifiée. Il s'agit d'un argument obligatoire. Longueur maximale : 1499

`profileName`- Nom du profil de bot à appliquer si la demande correspond à cette politique de bot. Il s'agit d'un argument obligatoire. Longueur maximale : 127

`undefAction`- Action à effectuer si le résultat de l'évaluation de la politique n'est pas défini (UNDEF). Un événement UNDEF indique une condition d'erreur interne. Longueur maximale : 127

`Comment`- Description de cette politique en matière de bots. Longueur maximale : 255

`logAction` - Nom de l'action de journalisation à utiliser pour les demandes qui correspondent à cette politique. Longueur maximale : 127

Exemple :

```
add bot policy pol1 -rule "HTTP.REQ.HEADER(\"header\").CONTAINS(\"custom
\")"- profileName profile1 -undefAction drop -comment commentforbotpolicy -
logAction log1
```

Bind bot policy global

À l'invite de commande, tapez :

```
bind bot global -policyName <string> -priority <positive_integer> [-gotoPriorityExpres
 <expression>][-type ( REQ_OVERRIDE | REQ_DEFAULT )] [-invoke (-labelType (
 vserver | policylabel )-labelName <string>)]
```

Exemple :

```
bind bot global -policyName pol1 -priority 100 -gotoPriorityExpression NEXT
-type REQ_OVERRIDE
```


Bind bot policy to a virtual server

À l'invite de commande, tapez :

```
bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )| <
serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>]
[-gotoPriorityExpression <expression>]
```

Exemple :

```
bind lb vserver lb-server1 -policyName pol1 -priority 100 -gotoPriorityExpression
 NEXT -type REQ_OVERRIDE
```

Configure bot settings

Vous pouvez personnaliser les paramètres par défaut si nécessaire.
À l'invite de commande, tapez :

```
1 set bot settings [-defaultProfile <string>] [-javaScriptName <string>]
      [-sessionTimeout <positive_integer>] [-sessionCookieName <string>]
      [-dfpRequestLimit <positive_integer>] [-signatureAutoUpdate ( ON |
      OFF )] [-signatureUrl <URL>] [-proxyServer <ip_addr|ipv6_addr|\*>]
      [-proxyPort <port|\*>]
2 <!--NeedCopy-->
```

Où,

`defaultProfile` - Profil à utiliser lorsqu'une connexion ne correspond à aucune politique. Le paramètre par défaut est « », qui renvoie les connexions non correspondantes au NetScaler sans essayer de les filtrer davantage. Longueur maximale : 31

`javaScriptName` - Nom du code JavaScript que la fonctionnalité BotNet utilise en réponse. Doit commencer par une lettre ou un chiffre et peut être composé de 1 à 31 lettres, chiffres et symboles de trait d'union (-) et de trait de soulignement (_). L'exigence suivante s'applique uniquement à la CLI NetScaler : si le nom inclut un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « mon nom de cookie » ou « mon nom de cookie »). Longueur maximale : 31

`sessionTimeout` - Expiration de la session, en secondes, après quoi la session utilisateur est interrompue.

`Minimum value` - 1, valeur maximale : 65535

`sessionCookieName` - Nom du SessionCookie que la fonctionnalité BotNet utilise pour le suivi. Doit commencer par une lettre ou un chiffre et peut être composé de 1 à 31 lettres, chiffres et symboles de trait d'union (-) et de trait de soulignement (_). L'exigence suivante s'applique uniquement à la CLI NetScaler : si le nom inclut un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « mon nom de cookie » ou « mon nom de cookie »). Longueur maximale : 31

`dfpRequestLimit` - Nombre de demandes à autoriser sans cookie de session de bot si l'empreinte digitale de l'appareil est activée. Valeur minimale : 1, Valeur maximale : 4294967295

`signatureAutoUpdate` - Indicateur utilisé pour activer/désactiver les signatures de mise à jour automatique des robots. Valeurs possibles : ON, OFF.
Valeur par défaut : OFF

`signatureUrl` - URL pour télécharger le fichier de mappage des signatures du bot depuis le serveur. Valeur par défaut : `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`. Longueur maximale : 2047

`proxyServer` - IP du serveur proxy pour obtenir des signatures mises à jour depuis AWS.

`proxyPort` - Port du serveur proxy pour obtenir des signatures mises à jour depuis AWS. Valeur par défaut : 8080

`proxyUsername` - Nom d'utilisateur permettant de s'authentifier auprès du serveur proxy pour télécharger les mises à jour des signatures.

`proxyPassword` — Mot de passe pour s'authentifier auprès du serveur proxy afin de télécharger les mises à jour des signatures.

Exemple :

```
set bot settings -defaultProfile profile1 -javaScriptName json.js -sessionTimeout
 1000 -sessionCookieName session -proxyServer 10.102.30.112 -proxyPort 3128
-proxyUsername defaultuser -proxyPassword defaultPassword
```

Configuration de la gestion des bots à l'aide de l'interface graphique NetScaler

Vous pouvez configurer la gestion des robots NetScaler en activant d'abord la fonctionnalité sur l'appliance. Une fois que vous l'avez activée, vous pouvez créer une stratégie de bot pour évaluer le trafic entrant en tant que bot et envoyer le trafic vers le profil de bot. Ensuite, vous créez un profil de bot, puis vous liez le profil à une signature de bot. Vous pouvez également cloner le fichier de signature du bot par défaut et utiliser le fichier de signature pour configurer les techniques de détection. Après avoir créé le fichier de signature, vous pouvez l'importer dans le profil du bot.



1. Activer la fonctionnalité de gestion des robots
2. Configuration des paramètres de gestion des bots
3. Cloner la signature par défaut du bot NetScaler
4. Importer la signature du bot NetScaler
5. Configuration des paramètres de signature du bot
6. Créer un profil de bot
7. Créer une stratégie de bot

Activer la fonctionnalité de gestion des robots

Pour activer la gestion des bots, procédez comme suit :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Sur la page **Configurer les fonctionnalités avancées**, cochez la case **Gestion des robots** .
3. Cliquez sur **OK**, puis sur **Fermer**.



Configuration des paramètres de gestion des bots pour la technique d'empreinte digitale

Pour configurer la technique d'empreinte digitale de l'appareil, procédez comme suit :

1. Accédez à **Sécurité > Gestion** des **robots NetScaler.**
2. Dans le volet de détails, sous **Paramètres, cliquez sur Modifier les paramètresde gestion des bots NetScaler**.
3. Dans la section **Configurer les paramètres de gestion des bots NetScaler, définissez les paramètres**suivants.
   a) Profil par défaut. Sélectionnez un profil de bot.

b) Nom JavaScript. Nom du fichier JavaScript utilisé par la gestion des robots dans sa réponse au client.

c) Délai d'expiration de session. Délai d'expiration en secondes après lequel la session utilisateur est interrompue.

d) Cookie de session. Nom du cookie de session utilisé par le système de gestion des robots pour le suivi.

e) Limite de demande d'empreinte digitale du périphérique Nombre de demandes à autoriser sans cookie de session du bot, si l'empreinte digitale de l'appareil est activée.

f) Serveur proxy : adresse IP du serveur proxy à partir de laquelle les dernières signatures sont téléchargées.

g) Port proxy : numéro de port de la machine à partir de laquelle les dernières signatures sont téléchargées.

h) Nom d'utilisateur du proxy : nom d'utilisateur pour l'authentification du serveur proxy

i) Mot de passe proxy : mot de passe pour l'authentification du serveur proxy.

> **Remarque :**
>
> Les champs Nom d'utilisateur proxy et Mot de passe proxy sont activés si les champs Serveur proxy et Port proxy sont configurés.



4. Cliquez sur **OK**.

Fichier de signature de robot clone

Pour cloner le fichier de signature du bot, procédez comme suit :

1. Accédez à **Sécurité** > **Gestion des robots NetScaler** et **signatures**.
2. Sur la page **NetScaler Bot Management Signatures**, sélectionnez l'enregistrement de signatures de bot par défaut et cliquez sur **Cloner**.
3. Dans la page **Signature du robot clone**, saisissez un nom et modifiez les données de signature.
4. Cliquez sur **Create**.



Importer le fichier de signature de bot

Si vous possédez votre propre fichier de signature, vous pouvez l'importer sous forme de fichier, de texte ou d'URL. Effectuez les étapes suivantes pour importer le fichier de signature du bot :

1. Accédez à **Sécurité** > **Gestion des robots NetScaler** et **signatures**.
2. Sur la page **NetScaler Bot Management Signatures**, importez le fichier sous forme d'URL, de fichier ou de texte.
3. Cliquez sur **Continuer**.



4. Sur la page Importer la signature de gestion des robots NetScaler, définissez les paramètres suivants.
   a) Nom : nom du fichier de signature du bot.
   b) Commentaire : brève description du fichier importé.
   c) Remplacer : cochez la case pour autoriser le remplacement des données lors de la mise à jour du fichier.
   d) Données de signature - Modifier les paramètres de signature
5. Cliquez sur **Terminé**.



Configurer la liste d'autorisation des robots à l'aide de l'interface graphique NetScaler

Cette technique de détection vous permet de contourner les URL que vous configurez une URL répertoriée autorisée. Pour configurer une URL de liste d'autorisation, procédez comme suit :

1. **Accédez à**Sécurité**>**NetScaler Bot**Management and Profiles.**
2. Sur la page **NetScaler Bot Management Profiles**, sélectionnez un fichier et cliquez sur **Modifier**.
3. Sur la page du **profil de gestion des robots NetScaler**, accédez à la section **Paramètres de signature** et cliquez sur Liste **blanche**.
4. Dans la section **Liste blanche**, définissez les paramètres suivants :
   a) Activé. Cochez la case pour valider les URL de la liste d'autorisation dans le cadre du processus de détection.
   b) Configurez les types. Configurez une URL de liste d'autorisation. L'URL est ignorée lors de la détection du bot. Cliquez sur Ajouter pour ajouter une URL à la liste des robots autorisés.
   c) Sur la page **Configurer la liaison à la liste blanche du profil de gestion des robots NetScaler**, définissez les paramètres suivants :
      i. Type. Le type d'URL peut être une adresse IPv4, une adresse IP de sous-réseau ou une adresse IP correspondant à une expression de stratégie.
      ii. Activé. Cochez la case pour valider l'URL.
      iii. Valeur. adresse URL.
      iv. Journal. Cochez la case pour enregistrer les entrées du journal.

v. Message du journal. Brève description du journal.
vi. Commentaires. Brève description de l'URL de la liste d'autorisation.
vii. Cliquez sur **OK**.



5. Cliquez sur **Update**.
6. Cliquez sur **Terminé**.



Configuration de la liste de robots bloqués à l'aide de l'interface graphique NetScaler

Cette technique de détection vous permet de supprimer les URL que vous configurez comme URL répertoriées dans la liste des blocs. Pour configurer une URL de liste de blocage, procédez comme suit.

1. **Accédez à**Sécurité**>**NetScaler Bot**Management and Profiles.**
2. Sur la page **NetScaler Bot Management Profiles**, sélectionnez un fichier de signature et cliquez sur **Modifier**.

3. Sur la page du **profil de gestion des robots NetScaler**, accédez à la section **Paramètres de signature** et cliquez sur **Liste noire**.
4. Dans la section **Liste noire**, définissez les paramètres suivants :
   a) Activé. Cochez la case pour valider les URL des listes de blocage dans le cadre du processus de détection.
   b) Configurez les types. Configurez une URL pour qu'elle fasse partie du processus de détection de la liste des bots bloqués. Ces URL sont supprimées lors de la détection du bot. Cliquez sur Ajouter pour ajouter une URL à la liste des bots bloqués
   c) Sur la page **Configurer la liaison à la liste noire du profil de gestion des robots NetScaler**, définissez les paramètres suivants.
      i. Type. Le type d'URL peut être une adresse IPv4, une adresse IP de sous-réseau ou une adresse IP.
      ii. Activé. Cochez la case pour valider l'URL.
      iii. Valeur. adresse URL.
      iv. Journal. Cochez la case pour enregistrer les entrées du journal.
      v. Message du journal. Brève description de la connexion.
      vi. Commentaires. Brève description de l'URL de la liste de blocage.
      vii. Cliquez sur **OK**.



5. Cliquez sur **Update**.
6. Cliquez sur **Terminé**.



Configuration de la réputation IP à l'aide de l'interface graphique NetScaler

La technique du bot de réputation IP utilise la base de données de réputation IP et la base de données des fournisseurs de services cloud de Webroot pour vérifier si une demande client est une adresse IP malveillante ou une adresse IP de cloud public. Dans le cadre des catégories de robots est configurée, puis une action de bot y est associée. Suivez les étapes ci-dessous pour configurer la réputation IP Webroot et les catégories de bases de données des fournisseurs de services cloud.

1. Accédez à **Sécurité** > **NetScaler bot Management** et **Profiles**.
2. Sur la page **Profils de gestion des bots NetScaler**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page du **profil de gestion des robots NetScaler**, accédez à la section **Paramètres du profil** et cliquez sur Réputation **IP**.
4. Dans la section **Réputation IP**, définissez les paramètres suivants :
   a) Activé. Cochez la case pour valider le trafic entrant des robots dans le cadre du processus de détection.
   b) Configurer les catégories. Vous pouvez utiliser la technique de réputation IP pour le trafic entrant des robots dans différentes catégories. En fonction de la catégorie configurée, vous pouvez supprimer ou rediriger le trafic du bot. Cliquez sur **Ajouter** pour configurer une catégorie de robots malveillants.
   c) Sur la page **Configurer la liaison de réputation IP du profil de gestion des robots NetScaler**, définissez les paramètres suivants :
      i. Catégorie. Sélectionnez une catégorie de bot de réputation IP Webroot pour valider une demande client en tant qu'adresse IP malveillante.

A. IP_BASED - Cette catégorie vérifie si l'adresse IP du client (IPv4 et IPv6) est malveillante ou non.
B. BOTNET - Cette catégorie comprend les canaux C&C de botnet et les machines zombies infectées contrôlées par Bot Master.
C. SPAM_SOURCES - Cette catégorie comprend le tunneling des messages de spam via un proxy, les activités SMTP anormales et les activités de spam sur les forums.
D. SCANNERS - Cette catégorie comprend toutes les reconnaissances telles que les sondes, l'analyse de l'hôte, l'analyse de domaine et l'attaque par force brute par mot de passe
E. DOS - Cette catégorie comprend DOS, DDOS, inondation de synchronisation anormale et détection de trafic anormal.
F. RÉPUTATION - Cette catégorie interdit l'accès à partir d'adresses IP (IPv4 et IPv6) actuellement connues pour être infectées par des logiciels malveillants. Cette catégorie comprend également les adresses IP dont le score d'indice de réputation Webroot est faible en moyenne. L'activation de cette catégorie empêche l'accès des sources identifiées pour contacter les points de distribution de logiciels malveillants.
G. HAMEÇONNAGE - Cette catégorie comprend les adresses IP (IPv4 et IPv6) hébergeant des sites d'hameçonnage et d'autres types d'activités frauduleuses telles que la fraude au clic publicitaire ou la fraude au jeu.
H. PROXY - Cette catégorie comprend les adresses IP (IPv4 et IPv6) fournissant des services proxy.
I. RÉSEAU - IP fournissant des services de proxy et d'anonymisation, y compris The Onion Router aka TOR ou dark net.
J. MOBILE_THREATS - Cette catégorie vérifie l'adresse IP du client (IPv4 et IPv6) avec la liste des adresses dangereuses pour les appareils mobiles.

ii. Catégorie. Sélectionnez une catégorie de fournisseur de services de cloud public Webroot pour valider qu'une demande client est une adresse IP de cloud public.

A. AWS - Cette catégorie vérifie l'adresse IP du client avec la liste des adresses de cloud public d'AWS.
B. GCP - Cette catégorie vérifie l'adresse IP du client avec la liste des adresses cloud publiques de Google Cloud Platform.
C. AZURE - Cette catégorie vérifie l'adresse du client avec la liste des adresses de cloud public d'Azure.
D. ORACLE - Cette catégorie vérifie l'adresse IP du client avec la liste des adresses de cloud public d'Oracle
E. IBM - Cette catégorie vérifie l'adresse IP du client avec la liste des adresses de cloud public d'IBM.
F. SALESFORCE - Cette catégorie vérifie l'adresse IP du client avec la liste des

adresses de cloud public de Salesforce.

Valeurs possibles pour la catégorie de robots Webroot IP Reputation : IP, BOTNETS, SPAM_SOURCES, SCANNERS, DOS, REPUTATION, PHISHING, PROXY, NETWORK, MOBILE_THREATS.

Valeurs possibles pour la catégorie de fournisseur de services de cloud public Webroot : AWS, GCP, AZURE, ORACLE, IBM, SALESFORCE.

iii. Activé. Cochez la case pour valider la détection des signatures de réputation IP.

iv. Action du bot. En fonction de la catégorie configurée, vous ne pouvez affecter aucune action, aucune baisse, redirection ou action d'atténuation.

v. Journal. Cochez la case pour enregistrer les entrées du journal.

vi. Message du journal. Brève description du journal.

vii. Commentaires. Brève description de la catégorie de robots.

5. Cliquez sur **OK**.
6. Cliquez sur **Update**.
7. Cliquez sur **Terminé**.



> **Remarque**
>
> Si vous désactivez **la réputation IP**, veillez à arrêter ses téléchargements. Procédez comme suit pour arrêter les téléchargements liés à la réputation IP :
>
> 1. Accédez à **Sécurité > Gestion des robots NetScaler > Modifier les paramètres de gestion des robots NetScaler**
> 2. Modifiez le **profil non intrusif par défaut** en **BOT_BYPASS**.

Configurer la technique de limite de débit des robots

La technique de limitation du débit des robots vous permet de limiter le trafic des robots dans un certain laps de temps en fonction de la géolocalisation de l'utilisateur, de l'adresse IP du client, de la session, du cookie ou de la ressource configurée (URL).
En configurant la technique de limite de débit des robots, vous pouvez vous assurer que :

- Bloquez les activités des bots malveillants.
- Réduisez la charge de trafic vers les serveurs Web.

Configurer la limite de débit des robots à l'aide de l'interface de ligne de commande NetScaler

À l'invite de commande, tapez :

```
bind bot profile <name>... -ratelimit  -type <type> Geolocation -
    countryCode <countryName> -rate  <positive_integer> -timeSlice <
    positive_integer> [-action <action> ...] [-limitType ( BURSTY |
    SMOOTH )] [-condition <expression>] [-enabled ( ON | OFF )]
<!--NeedCopy-->
```

Où,

*SOURCE_IP - Limitation de débit en fonction de l'adresse IP du client.

*SESSION - Limitation du débit en fonction du nom du cookie configuré.

*URL - Limitation de débit en fonction de l'URL configurée.

*GEOLOCATION - Limitation du débit en fonction du nom de pays configuré.

Possible values - SESSION, SOURCE_IP, URL, GÉOLOCALISATION

Exemple :

```
 bind bot profile geo_prof -ratelimit -type Geolocation -countryCode IN
     -rate 100 -timeSlice 1000 -limitType SMOOTH -condition HTTP.REQ.
    HEADER("User-Agent").contains("anroid") -action log,drop -enabled
    on
<!--NeedCopy-->
```

Configurer la limite de débit de bots à l'aide de l'interface graphique NetScaler

Effectuez les étapes suivantes pour configurer la technique de détection de la limite de débit des robots :

1. **Accédez à**Sécurité > NetScaler Bot**Management and Profiles.**
2. Sur la page **NetScaler Bot Management Profiles**, sélectionnez un profil et cliquez sur **Modifier**.

3. Sur la page du **profil de gestion des robots NetScaler**, accédez à la section **Paramètres du profil** et cliquez sur Limite **de débit**.
4. Dans la section **Limite de débit**, définissez les paramètres suivants :
   a) Activé. Cochez la case pour valider le trafic entrant du bot dans le cadre du processus de détection.
   b) Cliquez sur **Ajouter** pour configurer les liaisons de limites de débit.
5. Sur la page **Configurer la limite de débit de gestion des robots NetScaler**, définissez les paramètres suivants.
   a) Type : limite de débit le trafic des robots en fonction des paramètres suivants :
      i. Géolocalisation - Limite de débit basée sur la situation géographique de l'utilisateur.
      ii. Source_IP - Limite le débit du trafic en fonction de l'adresse IP du client.
      iii. Session : limite le débit du trafic des robots en fonction de la session ou du nom du cookie.
      iv. URL : limite le débit du trafic des robots en fonction de l'URL configurée.
   b) Pays - Sélectionnez une géolocalisation en tant que pays ou région.
   c) Type de limite de débit : limite le type de trafic en fonction des types suivants.
      - Bursty — Transfère toutes les demandes qui ne dépassent pas le seuil défini et la période spécifiée.
      - Fluide : transférez les demandes de manière uniforme sur la période spécifiée.
   d) Connexion à limite de débit : vous permet de créer plusieurs règles pour une condition.
   e) Activé : cochez la case pour valider le trafic entrant du bot.
   f) Seuil de demande : nombre maximum de demandes autorisées dans un certain délai.
   g) Période : durée en millisecondes.
   h) Action : choisissez une action de robot pour la catégorie sélectionnée.
   i) Journal : cochez la case pour enregistrer les entrées du journal.
   j) Message du journal : brève description du journal.
   k) Commentaires - Brève description de la catégorie de robots.
6. Cliquez sur **OK**.
7. Cliquez sur **Update**.
8. Cliquez sur **Terminé**.



Configurer la technique d'empreinte digitale de l'appareil à l'aide de l'interface graphique NetScaler

Cette technique de détection envoie un défi de script Java au client et extrait les informations du périphérique. En fonction des informations de l'appareil, la technique supprime ou contourne le trafic du bot. Suivez les étapes pour configurer la technique de détection.

1. **Accédez à**Sécurité**>**NetScaler Bot**Management and Profiles.**
2. Sur la page **NetScaler Bot Management Profiles**, sélectionnez un fichier de signature et cliquez sur **Modifier**.
3. Sur la page du **profil de gestion des robots NetScaler**, accédez à la section **Paramètres de signature** et cliquez sur Empreinte digitale de **l'appareil**.
   Dans la section **Empreinte digitale de l'appareil**, définissez les paramètres suivants :
   a) Enabled - Select to enable the rule.
   b) Configuration - Select one of the following options:
      i. None - Allows the traffic.
      ii. Drop - Drops the traffic.
      iii. Redirect - Redirects the traffic to error URL.
      iv. Mitigation, or CAPTCHA - Validates and allows the traffic.

      > **Note:**
      > During session replay attacks using the device fingerprint cookies, requests are dropped even if the device fingerprint configuration is set to **Mitigation**.
4. Cliquez sur **Update**.
5. Cliquez sur **Terminé**.



Configuration de la technique d'empreinte digitale de l'appareil pour les applications mobiles (Android)

La technique d'empreinte digitale du périphérique détecte un trafic entrant en tant que bot en insérant un script JavaScript dans la réponse HTML au client. Le script JavaScript, lorsqu'il est appelé par le navigateur, collecte les attributs du navigateur et du client et envoie une demande à l'appliance. Les attributs sont examinés pour déterminer si le trafic est un bot ou un humain.

La technique de détection est encore étendue pour détecter les bots sur une plateforme mobile (Android). Contrairement aux applications Web, dans le trafic mobile (Android), la détection des bots basée sur un script JavaScript ne s'applique pas. Pour détecter les bots dans un réseau mobile, la technique utilise un SDK mobile de bot intégré aux applications mobiles côté client. Le SDK intercepte le trafic mobile, collecte les détails de l'appareil et envoie les données à l'appliance. Du côté de l'appliance, la technique de détection examine les données et détermine si la connexion provient d'un bot ou d'un humain.

Comment fonctionne la technique d'empreinte digitale de l'appareil pour l'application mobile

Les étapes suivantes expliquent le flux de travail de détection des bots permettant de détecter si une demande émanant d'un appareil mobile provient d'un humain ou d'un robot.

1. Lorsqu'un utilisateur interagit avec une application mobile, le SDK mobile du bot enregistre le comportement de l'appareil.
2. Le client envoie une demande à l'appliance NetScaler.
3. Lors de l'envoi de la réponse, l'appliance insère un cookie de session de bot avec les détails de la session et les paramètres pour collecter les paramètres du client.
4. Lorsque l'application mobile reçoit la réponse, le SDK NetScaler bot intégré à l'application mobile valide la réponse, extrait les paramètres d'empreinte digitale enregistrés de l'appareil et les envoie à l'appliance.
5. La technique de détection des empreintes digitales de l'appareil côté appliance valide les détails de l'appareil et met à jour le cookie de session de bot s'il s'agit d'un robot suspecté ou non.
6. Lorsque le cookie a expiré ou que la protection par empreinte digitale de l'appareil préfère valider et collecter périodiquement les paramètres de l'appareil, toute la procédure ou le défi est répété.

Prérequis

Pour commencer à utiliser la technique de détection des empreintes digitales des appareils NetScaler pour les applications mobiles, vous devez télécharger et installer le SDK mobile pour robots dans votre application mobile.

Configuration de la technique de détection des empreintes digitales pour les applications mobiles (Android) à l'aide de la CLI

À l'invite de commande, tapez :

```
set bot profile <profile name> -deviceFingerprintMobile ( NONE | Android )
```

Exemple :

```
set bot profile profile 1 -deviceFingerprintMobile Android
```

Configurer la technique de détection des empreintes digitales de l'appareil pour les applications mobiles (Android) à l'aide de l'interface graphique

1. **Accédez à**Sécurité**>**NetScaler Bot**Management and Profiles.**
2. Sur la page **NetScaler Bot Management Profiles**, sélectionnez un fichier et cliquez sur **Modifier**.
3. Sur la page du **profil de gestion des robots NetScaler**, cliquez sur **Empreinte digitale de l'appareil sous Paramètres** du **profil**.
4. Dans la section **Configure Bot Mobile SDK**, sélectionnez le type de client mobile.
5. Cliquez sur **Mettre à jour** et **terminé**.



Configurer l'expression du journal des robots

Si le client est identifié comme un bot, la gestion des robots NetScaler vous permet de capturer des informations supplémentaires sous forme de messages de journal. Les données peuvent être le nom de l'utilisateur qui a demandé l'URL, l'adresse IP source et le port source à partir duquel l'utilisateur a envoyé la demande ou les données générées à partir d'une expression. Pour effectuer une journalisation personnalisée, vous devez configurer une expression de journal dans le profil de gestion des robots.

Liez l'expression de journal dans le profil de robot à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind bot profile <name> (-logExpression -name <string> -expression <
    expression> [-enabled ( ON | OFF )]) -comment <string>
<!--NeedCopy-->
```

Exemple :

```
bind bot profile profile1 -logExpression exp1 -expression HTTP.REQ.URL -
enabled ON -comment "testing log expression"
```

Lier l'expression de journal au profil de bot à l'aide de l'interface graphique

1. Accédez à **Sécurité > Gestion des robots NetScaler > Profils**.
2. Sur la page **NetScaler Bot Management Profiles**, sélectionnez **Bot Log Expressions** dans la section **Paramètres du profil.**
3. Dans la section Paramètres d'expression du journal de **bots*, cliquez sur **Ajouter**.
4. Sur la page **Configurer la liaison entre les expressions du journal du bot du profil de gestion des robots NetScaler**, définissez les paramètres suivants.
   a) Nom de l'expression du journal. Nom de l'expression du journal.
   b) Expression : Saisissez l'expression de journal.
   c) Activé. Activez ou désactivez la liaison de l'expression de journal.
   d) Commentaires. Une brève description de la liaison d'expression du journal de bot.
5. Cliquez sur**OK** et sur **Terminé**.



Configurer la technique de piège bot

La technique NetScaler Bot Trap insère de manière aléatoire ou périodique une URL d'interception dans la réponse du serveur. Vous pouvez également créer une liste d'URL de déroutement et ajouter des URL pour cela. L'URL apparaît invisible et inaccessible si le client est un utilisateur humain. Toutefois, si le client est un robot automatisé, l'URL est accessible et lorsqu'on y accède, l'attaquant est classé comme robot et toute demande ultérieure du bot est bloquée. La technique du piège est efficace pour bloquer les attaques des robots.

L'URL de déroutement est une URL alphanumérique de longueur configurable et elle est générée automatiquement à un intervalle configurable. La technique vous permet également de configurer une URL d'insertion d'interruption pour les sites Web les plus visités ou les sites Web fréquemment visités. Ce faisant, vous pouvez définir le but de l'insertion de l'URL d'interruption du bot pour les demandes correspondant à l'URL d'insertion d'interruption.

> **Remarque :**
>
> Bien que l'URL d'interception des robots soit générée automatiquement, la gestion des robots

> NetScaler vous permet toujours de configurer une URL d'interception personnalisée dans le profil du bot. Ceci est fait pour renforcer
> la technique de détection des bots et rendre plus difficile l'accès des attaquants à l'URL de trap.

Pour terminer la configuration du bot trap, vous devez suivre les étapes suivantes.

1. Activer l'URL de bot-trap
2. Configurer l'URL d'interruption de bot dans le profil de bot
3. Lier l'URL d'insertion d'un piège à robots au profil
4. Configurer la longueur et l'intervalle de l'URL d'interruption de bots dans les paramètres

Activer la protection des URL de bot-trap

Avant de commencer, vous devez vous assurer que la protection de l'URL de déroutement de bots est activée sur l'appliance. À l'invite de commande, tapez :

```
enable ns feature Bot
```

Configurer l'URL d'interruption de bot dans le profil de bot

Vous pouvez configurer l'URL de l'interruption de bot et spécifier une action d'interruption dans le profil du bot.
À l'invite de commande, tapez :

```
add bot profile <name> -trapURL <string> -trap ( ON | OFF )-trapAction <
trapAction>
```

Où,

- `trapURL` est l'URL que Bot Protection utilise comme URL du piège. Longueur maximale : 127
- `trap` consiste à activer la détection des pièges à robots. Valeurs possibles : ON, OFF. Valeur par défaut : OFF
- `trapAction` est une action à effectuer sur la base de la détection de robots. Valeurs possibles : NONE, LOG, DROP, REDIRECT, RESET, MITIGATION. Valeur par défaut : AUCUN

Exemple :

```
add bot profile profile1 -trapURL www.bottrap1.com trap ON -trapAction
RESET
```

Lier l'URL d'insertion d'un piège à robots au profil

Vous pouvez configurer l'URL d'insertion de l'interruption de bot et la lier au profil du bot.
À l'invite de commande, tapez :


```
bind bot profile <profile_name> trapInsertionURL -url <url> -enabled ON|OFF
-comment <comment>
```

Où,

URL - Le modèle regex de l'URL de demande pour lequel l'URL du bot trap est insérée. Longueur maximale : 127

Exemple :

```
bind bot profile profile1 trapInsertionURL -url www.example.com -enabled ON
-comment insert a trap URL randomly
```

Configurer la longueur et l'intervalle de l'URL d'interruption de bots dans les paramètres

Vous pouvez configurer la longueur de l'URL de l'interruption de bot et également définir l'intervalle de génération automatique de l'URL d'interruption de bot.
À l'invite de commande, tapez :

```
set bot settings -trapURLAutoGenerate ( ON | OFF )-trapURLInterval <positive_integer
> -trapURLLength <positive_integer>
```

Où,

- trapURLInterval est le délai, en secondes, au bout duquel l'URL du bot trap est mise à jour. Valeur par défaut : 3600, Valeur minimale : 300, Valeur maximale : 86400
- trapURLLength. Longueur de l'URL d'interruption de bots générée automatiquement. Valeur par défaut : 32, Valeur minimale : 10, Valeur maximale : 255

Exemple :

```
set bot settings -trapURLAutoGenerate ON -trapURLInterval 300 -trapURLLength
 60
```

Configurer l'URL de bot-trap à l'aide de l'interface graphique

1. Accédez à **Sécurité > Gestion des robots NetScaler > Profils**.
2. Sur la page **NetScaler Bot Management Profiles**, cliquez sur **Modifier** pour configurer la technique d'URL d'interception des robots.
3. Sur la page **Créer un profil de gestion des robots NetScaler**, entrez l'URL du piège à robots dans la section générale.



4. Sur la page **Créer un profil de gestion des robots NetScaler**, cliquez sur **Bot Trap dans les paramètres** du **profil**.
5. Dans la section **Bot Trap**, définissez les paramètres suivants.

   a. Activé. Cochez la case pour activer la détection des robots
   piégés b. Description. Brève description de l'URL.
   c. Configurez les actions. Action à entreprendre pour le bot détecté par l'accès au bot-trap.



6. Dans la section **Configurer les URL d'insertion de déroutement**, cliquez sur **Ajouter**.
7. Sur la page **Configurer le profil de gestion des robots NetScaler Bot Trap Binding**, définissez

les paramètres suivants.

a) URL de déroutement. Tapez l'URL que vous souhaitez confirmer comme URL d'insertion d'interruption de bot.
b) Activé. Activez ou désactivez l'URL d'insertion d'interruption de bot.
c) Commentaire. Brève description de l'URL d'insertion d'interruption.



8. Dans la section **Paramètres de signature**, cliquez sur **Bot Trap**.
9. Dans la section **Bot Trap**, définissez les paramètres suivants :
   a) Activé. Cochez la case pour activer la détection des robots piégés.
   b) Dans la section Configurer, définissez les paramètres suivants.
      i. Action. Action à entreprendre pour le bot détecté par l'accès au bot-trap.
      ii. Journal. Activez ou désactivez la journalisation pour la liaison de bots trap.
10. Cliquez sur **Mettre à jour** et **terminé**.

Configurer les paramètres de l'URL de l'interruption

Effectuez les étapes suivantes pour configurer les paramètres de l'URL d'interruption de bot :

1. Accédez à **Sécurité > Gestion des robots NetScaler.**
2. Dans le volet de détails, sous **Paramètres, cliquez sur Modifier les paramètresde gestion des robots NetScaler**.
3. Dans la section **Configurer les paramètres de gestion des robots NetScaler, définissez les paramètres**suivants.
   a) Intervalle d'URL d'interruption. Durée en secondes après laquelle l'URL de l'interruption de bot est mise à jour.

b) Longueur de l'URL de déroutement. Longueur de l'URL d'interruption de bots générée automatiquement.

4. Cliquez sur **OK** et **Terminé**.



Expression de stratégie IP client pour la détection de robots

La gestion des robots NetScaler vous permet désormais de configurer une expression de stratégie avancée pour extraire l'adresse IP du client à partir d'un en-tête de requête HTTP, d'un corps de requête HTTP, d'une URL de requête HTTP ou à l'aide d'une expression de stratégie avancée. Les valeurs extraites sont utilisées par un mécanisme de détection de robots (tel que le TPS, le bot trap ou la limite de débit) pour détecter si la demande entrante est un robot.

> **Remarque :**
>
> Si vous n'avez pas configuré d'expression IP client, l'adresse IP du client source par défaut ou existante est utilisée pour la détection des robots. Si une expression est configurée, le résultat de l'évaluation fournit l'adresse IP du client pouvant être utilisée pour la détection des robots.

Vous pouvez configurer et utiliser l'expression IP du client pour extraire l'adresse IP du client réelle si la demande entrante passe par un serveur proxy et si l'adresse IP du client est présente dans l'en-tête. En ajoutant cette configuration, l'appliance peut utiliser le mécanisme de détection des robots pour assurer une sécurité accrue aux clients et serveurs logiciels.

Configurer l'expression de stratégie IP du client dans le profil de robot à l'aide de l'interface de ligne

À l'invite de commande, tapez :

```
add bot profile <name> [-clientIPExpression <expression>]
<!--NeedCopy-->
```

Exemple :

```
add bot profile profile1 -clientIPExpression 'HTTP.REQ.HEADER("X-Forwarded-For")ALT CLIENT.IP.SRC.TYPECAST_TEXT_T'

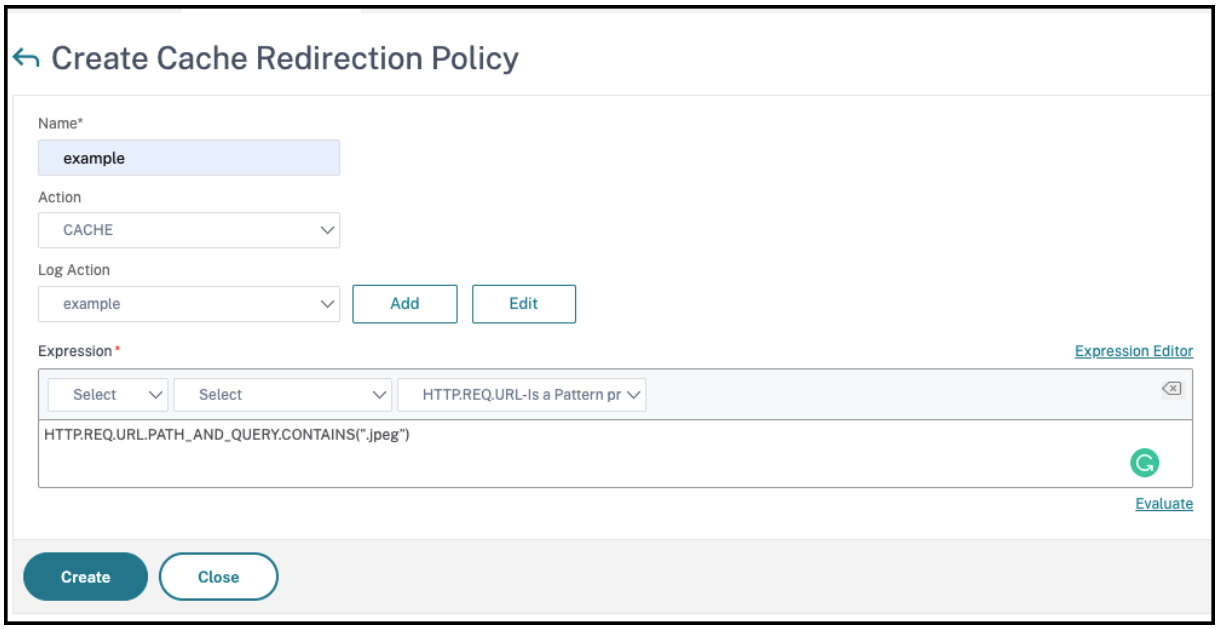
add bot profile profile1 -clientIPExpression 'HTTP.REQ.HEADER("X-Forwarded-For")ALT CLIENT.IPv6.SRC.TYPECAST_TEXT_T'
```

Configurer l'expression de stratégie IP du client dans le profil de robot à l'aide de l'interface graphique

1. Accédez à **Sécurité > Gestion des robots NetScaler > Profils**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer un profil de gestion de robots NetScaler**, définissez l'expression IP du client.
4. Cliquez sur **Créer** et **Fermer**.



Configurer CAPTCHA pour la réputation IP et la détection des empreintes digitales des périphériques

CAPTCHA est un acronyme qui signifie « Completely Automated Public Turing test to tell Computers and Humans Apart ». CAPTCHA est conçu pour tester si un trafic entrant provient d'un utilisateur humain ou d'un robot automatisé. CAPTCHA permet de bloquer les bots automatisés qui causent des violations de sécurité aux applications Web. Dans NetScaler, le CAPTCHA utilise le module Challenge-Response pour déterminer si le trafic entrant provient d'un utilisateur humain et non d'un robot automatique.

Configurer les signatures statiques des robots

Cette technique de détection vous permet d'identifier les informations de l'agent utilisateur à partir des détails du navigateur. Sur la base des informations de l'agent utilisateur, le bot est identifié comme un bot mauvais ou bon, puis vous lui attribuez une action de bot.

Procédez comme suit pour configurer la technique de signature statique :

1. Dans le volet de navigation, ouvrez **Security > NetScaler Bot Management > Signatures**.
2. Sur la page **NetScaler Bot Management Signatures**, sélectionnez un fichier de signature et cliquez sur **Modifier**.
3. Sur la page **NetScaler Bot Management Signature**, accédez à la section **Paramètres de signature** et cliquez sur **Signatures de bot**.
4. Dans la section **Bot Signatures**, définissez les paramètres suivants :
    a) Configurez les signatures statiques. Cette section contient une liste d'enregistrements de signatures statiques de robots. Vous pouvez sélectionner un enregistrement et cliquer sur **Modifier** pour lui attribuer une action de robot.
    b) Cliquez sur **OK**.
5. Cliquez sur **Mettre à jour la signature**.
6. Cliquez sur **Terminé**.



Délimitation des signatures statiques

La gestion des robots NetScaler protège votre application Web contre les robots. Les signatures statiques des bots aident à identifier les robots bons et défectueux en fonction de paramètres de requête tels que l'agent utilisateur dans la demande entrante.
La liste des signatures dans le fichier est énorme et de nouvelles règles sont ajoutées et les règles périmées sont supprimées périodiquement. En tant qu'administrateur, il se peut que vous souhaitiez rechercher une signature spécifique ou une liste de signatures sous une catégorie. Pour filtrer facilement les signatures, la page de signature du bot offre une fonctionnalité de recherche améliorée. La fonction de recherche vous permet de trouver des règles de signature et de configurer sa propriété en fonction d'un ou de plusieurs paramètres de signature tels que l'action, l'ID de signature, le développeur et le nom de la signature.

Action : sélectionnez une action de robot que vous préférez configurer pour une catégorie spécifique de règles de signature. Les types d'action disponibles sont les suivants :

- Activer la sélection : active toutes les règles de signature sélectionnées.
- Désactiver la sélection : désactive toutes les règles de signatures sélectionnées.
- Supprimer la sélection : sélectionnez l'action « Supprimer » dans toutes les règles de signature sélectionnées.
- Redirection sélectionnée : appliquez l'action « Rediriger » à toutes les règles de signature sélectionnées.
- Réinitialiser la sélection - Appliquez l'action « Réinitialiser » à toutes les règles de signature sélectionnées.
- Journal sélectionné : appliquez l'action « Enregistrer » à toutes les règles de signature sélectionnées.
- Supprimer la suppression sélectionnée : désactivez l'action de dépôt sur toutes les règles de

signature sélectionnées.
- Supprimer la redirection sélectionnée : désactivez l'action de redirection vers toutes les règles de signature sélectionnées.
- Supprimer la réinitialisation sélectionnée : désactivez l'action de réinitialisation de toutes les règles de signature sélectionnées.
- Supprimer le journal sélectionné : désactivez l'action de journalisation sur toutes les règles de signature sélectionnées.

Catégorie : sélectionnez une catégorie pour filtrer les règles de signature en conséquence. Vous trouverez ci-dessous la liste des catégories disponibles pour le tri des règles de signature.

- Action : triez en fonction de l'action du robot.
- Catégorie : triez en fonction de la catégorie du robot.
- Développeur : triez en fonction de l'éditeur de la société hôte.
- Activé : triez en fonction des règles de signature activées.
- Id : permet de trier en fonction de l'ID de la règle de signature.
- Journal : triez en fonction des règles de signature pour lesquelles la journalisation est activée.
- Nom : permet de trier en fonction du nom de la règle de signature.
- Type : permet de trier en fonction du type de signature.
- Version : triez en fonction de la version de la règle de signature.

Recherchez les règles de signature statique des robots en fonction des types d'actions et de catégories à l'aide de l'interface graphique NetScaler

1. Accédez à **Sécurité > Gestion des robots NetScaler > Signature**.
2. Dans la page de détails, cliquez sur **Ajouter**.
3. Sur la page **NetScaler Bot Management Signatures**, cliquez sur Modifier dans la section **Signature statique** .
4. Dans la section **Configurer la signature statique**, sélectionnez une action de signature dans la liste déroulante.
5. Utilisez la fonction de recherche pour sélectionner une catégorie et filtrer les règles en conséquence.
6. Cliquez sur **Update**.



Modifiez la propriété de la règle de signature statique du bot à l'aide de l'interface graphique NetScaler

1. Accédez à **Sécurité > Gestion des robots NetScaler > Signature**.
2. Dans la page de détails, cliquez sur **Ajouter**.
3. Sur la page **NetScaler Bot Management Signatures**, cliquez sur Modifier dans la section **Signature statique** .
4. Dans la section **Configurer la signature statique**, sélectionnez une action dans la liste déroulante.
5. Utilisez la fonction de recherche pour sélectionner une catégorie et filtrer les règles en conséquence.
6. Dans la liste de signatures statiques, sélectionnez une signature pour modifier sa propriété.



7. Cliquez sur **OK** pour confirmer.

Comment fonctionne le CAPTCHA dans la gestion des robots NetScaler

Dans la gestion des robots NetScaler, la validation CAPTCHA est configurée comme une action de stratégie à exécuter après l'évaluation de la stratégie des robots. L'action CAPTCHA n'est disponible que pour les techniques de réputation IP et de détection des empreintes digitales de l'appareil. Voici les étapes à suivre pour comprendre le fonctionnement du CAPTCHA :

1. Si une violation de sécurité est observée pendant la détection de la réputation IP ou de l'empreinte digitale de l'appareil, l'appliance ADC envoie un défi CAPTCHA.
2. Le client envoie la réponse CAPTCHA.
3. L'appliance valide la réponse CAPTCHA et, si le CAPTCHA est valide, la demande est autorisée et transmise au serveur principal.
4. Si la réponse CATCHA n'est pas valide, l'appliance envoie un nouveau défi CAPTCHA jusqu'à ce que le nombre maximal de tentatives soit atteint.
5. Si la réponse CAPTCHA n'est pas valide, même après le nombre maximal de tentatives, l'appliance abandonne ou redirige la demande vers l'URL d'erreur configurée.
6. Si vous avez configuré l'action de journalisation, l'appliance stocke les détails de la demande dans le fichier ns.log.

Configurer les paramètres CAPTCHA à l'aide de l'interface graphique NetScaler

L'action CAPTCHA de gestion des bots n'est prise en charge que pour les techniques de réputation IP et de détection des empreintes digitales de l'appareil. Suivez les étapes suivantes pour configurer les paramètres **CAPTCHA** .

1. Accédez à **Sécurité > Gestion et profils des robots NetScaler**.
2. Sur la page **NetScaler Bot Management Profiles**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page **NetScaler Bot Management Profile**, accédez à la section **Signature Settings** et cliquez sur **CAPTCHA**.
4. Dans la section **Paramètres CAPTCHA**, cliquez sur **Ajouter pour configurer les paramètres CAPTCHA** sur le profil :
5. Sur la page **Configurer le CAPTCHA de NetScaler Bot Management**, définissez les paramètres suivants.
    a) URL. URL de bot pour laquelle l'action CAPTCHA est appliquée pendant les techniques de réputation IP et de détection des empreintes digitales de l'appareil.
    b) Activé. Définissez cette option pour activer la prise en charge du CAPTCHA.
    c) L'heure de la grâce. Durée jusqu'à ce qu'aucun nouveau défi CAPTCHA n'est envoyé après la réception de la réponse CAPTCHA valide actuelle.

d) Le temps d'attente. Durée d'attente de l'appliance ADC jusqu'à ce que le client envoie la réponse CAPTCHA.

e) Période de mise en sourdine. Durée pendant laquelle le client qui a envoyé une réponse CAPTCHA incorrecte doit attendre jusqu'à ce qu'il soit autorisé à essayer ensuite. Pendant cette période de mise en sourdine, l'appliance ADC n'autorise aucune demande. Portée : 60 à 900 secondes, Recommandé : 300 secondes

f) Limite de durée de la demande. Longueur de la demande pour laquelle le challenge CAPTCHA est envoyé au client. Si la longueur est supérieure à la valeur de seuil, la demande est abandonnée. La valeur par défaut est de 10 à 3 000 octets.

g) Tentatives de nouvelle tentative. Nombre de tentatives que le client est autorisé à réessayer de résoudre le défi CAPTCHA. Plage : 1-10, Recommandé : 5.

h) Aucune action d'action/supérieur/redirection à effectuer si le client échoue à la validation CAPTCHA.

i) Journal. Définissez cette option pour stocker les informations de demande du client en cas d'échec du CAPTCHA de réponse. Les données sont stockées dans un fichier `ns.log`.

j) Commentaire. Une brève description de la configuration CAPTCHA.

6. Cliquez sur **OK** et **Terminé**.



7. Accédez à **Sécurité > Gestion des robots NetScaler > Signatures**.
8. Sur la page **NetScaler Bot Management Signatures**, sélectionnez un fichier de signature et cliquez sur **Modifier**.
9. Sur la page **NetScaler Bot Management Signature**, accédez à la section **Paramètres de signature** et cliquez sur **Signatures de bot**.
10. Dans la section **Bot Signatures**, définissez les paramètres suivants :
11. Configurez les **signatures statiques**. Sélectionnez un enregistrement de signature statique de robot et cliquez sur Modifier pour lui attribuer une action de robot.
12. Cliquez sur **OK**.
13. Cliquez sur **Mettre à jour la signature**.
14. Cliquez sur **Terminé**.



Mise à jour automatique des signatures de bots

La technique de signature statique des bots utilise une table de recherche de signature avec une liste de bons bots et de mauvais robots. Les robots sont classés en fonction de la chaîne de l'agent utilisateur et des noms de domaine. Si la chaîne de l'agent utilisateur et le nom de domaine dans le trafic de bot entrant correspondent à une valeur de la table de recherche, une action de bot configurée est appliquée.

Les mises à jour des signatures de bots sont hébergées sur le cloud AWS et la table de recherche de signature communique avec la base de données AWS pour les mises à jour des signatures. Le planificateur de mise à jour automatique des signatures s'exécute toutes les heures pour vérifier la **base de données AWS** et mettre à jour la table des signatures dans l'appliance NetScaler.

L'URL de mise à jour automatique de signature à configurer est la suivante : `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`

> **Remarque :**
>
> Vous pouvez également configurer un serveur proxy et mettre à jour périodiquement les signatures depuis le cloud AWS vers l'appliance via le proxy. Pour la configuration du proxy, vous devez définir l'adresse IP et l'adresse du port du proxy dans les paramètres du bot.

Fonctionnement de la mise à jour automatique de signature

Le schéma suivant montre comment les signatures des robots sont récupérées depuis le cloud AWS, mises à jour sur NetScaler et affichées sur NetScaler ADM pour un résumé de la mise à jour des signatures.



Le planificateur de mise à jour automatique des signatures de bot effectue les opérations suivantes :

1. Récupère le fichier de mappage à partir de l'URI AWS.
2. Vérifie les dernières signatures du fichier de mappage avec les signatures existantes dans l'appliance ADC.
3. Télécharge les nouvelles signatures depuis AWS et vérifie l'intégrité de la signature.
4. Met à jour les signatures de bots existantes avec les nouvelles signatures dans le fichier de signature du bot.
5. Génère une alerte SNMP et envoie le résumé de la mise à jour des signatures à NetScaler ADM.

Configurer la mise à jour automatique de

Pour configurer la mise à jour automatique de la signature du bot, procédez comme suit :

Activer la mise à jour automatique de signature

Vous devez activer l'option de mise à jour automatique dans les paramètres du bot sur l'appliance ADC.
À l'invite de commande, tapez :


```
set bot settings -signatureAutoUpdate ON
```

Configurer les paramètres du serveur proxy (facultatif)

Si vous accédez à la base de données de signatures AWS via un serveur proxy, vous devez configurer le serveur proxy et le port.

```
set bot settings -proxyserver -proxyport
```

Exemple :

```
set bot settings -proxy server 1.1.1.1 -proxyport 1356
```

Configurer la mise à jour automatique de la signature du bot à l'aide de l'interface graphique NetScaler

Suivez les étapes suivantes pour configurer la mise à jour automatique de la signature du bot :

1. Accédez à **Sécurité > Gestion des robots NetScaler.**
2. Dans le volet de détails, sous **Paramètres, cliquez sur Modifier les paramètresde gestion des robots NetScaler**.
3. Dans la section **Configurer les paramètres de gestion des robots NetScaler**, cochez la case Mise à jour **automatique de la signature** .



4. Cliquez sur **OK** et sur **Fermer**.

Créer un profil de gestion des bots

Un profil de bot est un ensemble de paramètres de gestion des bots utilisés pour détecter le type de bot. Dans un profil, vous déterminez comment le Web App Firewall applique chacun de ses filtres (ou vérifications) au trafic des robots vers vos sites Web, ainsi que les réponses de ceux-ci.

Pour configurer le profil de bot, procédez comme suit :

1. **Accédez à**Sécurité**>**NetScaler Bot**Management > Profils.**
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer un profil de gestion de robots NetScaler**, définissez les paramètres suivants.
   a) Nom. Nom du profil du bot.
   b) Signature. Nom du fichier de signature du bot.
   c) URL d'erreur. URL pour les redirections.
   d) Commentaire. Brève description du profil.
4. Cliquez sur **Créer** et **Fermer**.



Créer une stratégie de bot

La stratégie de bot contrôle le trafic acheminé vers le système de gestion des bots et contrôle également les journaux de bots envoyés au serveur de journaux d'audit. Suivez la procédure pour configurer la stratégie de bot.

1. Accédez à **Sécurité** > **Gestion des robots NetScaler** > Stratégies relatives aux **robots**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Créer une stratégie de gestion des robots NetScaler**, définissez les paramètres suivants.
   a) Nom. Nom de la stratégie Bot.
   b) Expression : Tapez l'expression ou la règle de stratégie directement dans la zone de texte.
   c) Profil de bot. Profil de bot pour appliquer la stratégie de bot.
   d) Action non définie. Sélectionnez une action que vous préférez attribuer.
   e) Commentaire. Brève description de la stratégie.
   f) Action de journalisation. Action de message du journal d'audit pour la journalisation du trafic des robots. Pour plus d'informations sur l'action du journal d'audit, consultez la rubrique Journalisation d'audit.
4. Cliquez sur **Créer** et **Fermer**.



Transactions de bots par seconde (TPS)

La technique de robot Transactions Per Second (TPS) détecte le trafic entrant en tant que bot si le nombre de requêtes par seconde (RPS) et le pourcentage d'augmentation du RPS dépassent la valeur de seuil configurée. La technique de détection protège vos applications Web contre les bots automatisés qui peuvent provoquer des activités de grattage Web, une connexion par forçage brute et d'autres attaques malveillantes.

> **Remarque :**
>
> La technique de bot détecte un trafic entrant en tant que bot uniquement si les deux paramètres

> sont configurés et si les deux valeurs dépassent la limite de seuil.
> Imaginons un scénario dans lequel l'appliance reçoit de nombreuses demandes provenant d'une URL spécifique et où vous souhaitez que la gestion des bots de NetScaler détecte s'il s'agit d'une attaque de bot. La technique de détection TPS examine le nombre de demandes (valeur configurée) provenant de l'URL en moins d'une seconde et l'augmentation en pourcentage (valeur configurée) du nombre de demandes reçues en 30 minutes. Si les valeurs dépassent la limite de seuil, le trafic est considéré comme un robot et l'appliance exécute l'action configurée.

Configurer la technique des transactions de bot par seconde (TPS)

Pour configurer TPS, vous devez effectuer les étapes suivantes :

1. Activer le bot TPS
2. Liaison des paramètres TPS au profil de gestion des bots

Liaison des paramètres TPS au profil de gestion des bots

Une fois que vous avez activé la fonctionnalité TPS de robot, vous devez lier les paramètres TPS au profil de gestion des robots.

À l'invite de commande, tapez :

```
bind bot profile <name>… (-tps [-type ( SourceIP | GeoLocation | RequestURL
 | Host )] [-threshold <positive_integer>] [-percentage <positive_integer
>] [-action ( none | log | drop | redirect | reset | mitigation )] [-
logMessage <string>])
```

Exemple :

```
bind bot profile profile1 -tps -type RequestURL -threshold 1 -percentage
100000 -action drop -logMessage log
```

Activer la transaction de robot par seconde (TPS)

Avant de commencer, vous devez vous assurer que la fonctionnalité Bot TPS est activée sur l'appliance. À l'invite de commande, tapez :

```
set bot profile profile1 -enableTPS ON
```

Configurer les transactions des robots par seconde (TPS) à l'aide de l'interface graphique NetScaler

Suivez les étapes suivantes pour configurer les transactions de bot par seconde :

1. Accédez à **Sécurité > Gestion des robots NetScaler > Profils**.

2. Sur la page **NetScaler Bot Management Profiles**, sélectionnez un profil et cliquez sur **Modifier**.
3. Sur la page **Créer un profil de gestion des robots NetScaler**, cliquez sur **TPS dans la section Paramètres** de **signature** .
4. Dans la section **TPS**, activez la fonctionnalité et cliquez sur **Ajouter**.



5. Dans la page **Configurer le profil de gestion des robots NetScaler (TPS Binding**), définissez les paramètres suivants.
   a) Type : types d'entrée autorisés par la technique de détection. Valeurs possibles : IP SOURCE, GÉOLOCALISATION, HÔTE, URL.

      SOURCE_IP — TPS basé sur l'adresse IP du client.

      GÉOLOCALISATION — TPS en fonction de l'emplacement géographique du client.

      HOST - TPS basé sur les demandes des clients transférées vers une adresse IP de serveur principal spécifique.

      URL : TPS basé sur les demandes des clients provenant d'une URL spécifique.

   b) Seuil fixe : nombre maximal de demandes autorisées à partir d'un type d'entrée TPS dans un intervalle de temps d'une seconde.

   c) Seuil de pourcentage : augmentation maximale en pourcentage des demandes provenant d'un type d'entrée TPS dans un intervalle de temps de 30 minutes.

   d) Action : action à effectuer pour un bot détecté par une liaison TPS.

   e) Journal : active ou désactive la journalisation pour la liaison TPS.

   f) Message du journal. Message à consigner pour le bot détecté par la liaison TPS. Longueur maximale : 255.

   g) Commentaires : brève description de la configuration du TPS. Longueur maximale : 255
6. Cliquez sur **OK**, puis sur **Fermer**.



Détection de robots basée sur la dynamique de la souris et du clavier

Pour détecter les robots et atténuer les anomalies liées au scraping Web, la gestion des robots NetScaler utilise une technique de détection des robots améliorée basée sur le comportement de la souris et du clavier. Contrairement aux techniques de robots classiques qui nécessitent une interaction humaine directe (par exemple, la validation CAPTCHA), la technique améliorée surveille passivement la dynamique de la souris et du clavier. L'appliance NetScaler collecte ensuite les données utilisateur en temps réel et analyse le comportement entre un humain et un bot.

La détection passive des robots utilisant la dynamique de la souris et du clavier présente les avantages suivants par rapport aux mécanismes de détection de robots existants :

- Assure une surveillance continue tout au long de la session utilisateur et élimine un point de contrôle unique.
- Ne nécessite aucune interaction humaine et est transparent pour les utilisateurs.

Fonctionnement de la détection des robots à l'aide de la dynamique de la souris

La technique de détection des robots utilisant la dynamique du clavier et de la souris se compose de deux composants, un enregistreur de pages Web et un détecteur de robots. L'enregistreur de pages Web est un code JavaScript qui enregistre les mouvements du clavier et de la souris lorsqu'un utilisateur effectue une tâche sur la page Web (par exemple, en remplissant un formulaire d'inscription). L'enregistreur envoie ensuite les données par lots à l'appliance NetScaler. L'appliance stocke ensuite

les données sous forme d'enregistrement KM et les envoie au détecteur de robots sur le serveur NetScaler ADM, qui analyse si l'utilisateur est un humain ou un robot.

Les étapes suivantes expliquent comment les composants interagissent entre eux :

1. L'administrateur NetScaler configure l'expression des stratégies via ADM StyleBook, CLI, NITRO ou toute autre méthode.
2. L'URL est définie dans le profil du bot lorsque l'administrateur active la fonctionnalité sur l'appliance.
3. Lorsqu'un client envoie une demande, l'appliance NetScaler suit la session et toutes les demandes qu'elle contient.
4. L'appliance insère un code JavaScript (enregistreur de page Web) dans la réponse si la demande correspond à l'expression configurée sur le profil du bot.
5. Le JavaScript collecte ensuite toute l'activité du clavier et de la souris et envoie les données KM dans une URL POST (transitoire).
6. L'appliance NetScaler stocke les données et les envoie au serveur NetScaler ADM à la fin de la session. Une fois que l'appliance reçoit les données complètes d'une demande POST, les données sont envoyées au serveur ADM.
7. Le service NetScaler ADM analyse les données et, sur la base de cette analyse, le résultat est disponible sur l'interface graphique du service NetScaler ADM.

L'enregistreur JavaScript enregistre les mouvements suivants de la souris et du clavier :

- Événements clavier — tous les événements
- Événements de souris - déplacement de la souris, souris vers le haut, souris vers le bas
- Événements Presse-papiers - coller
- Événements personnalisés : saisie automatique, saisie automatique et annulation
- horodatage de chaque événement

Configurer la détection de bots à l'aide de la dynamique de

La configuration de gestion des bots de NetScaler inclut l'activation ou la désactivation de la fonctionnalité de détection basée sur le clavier et la souris, et configure l'URL JavaScript dans le profil du bot. Procédez comme suit pour configurer la détection des robots à l'aide de la dynamique de la souris et du clavier :

1. Activer la détection basée sur le clavier et la souris
2. Configurer l'expression pour décider quand le JavaScript peut être injecté dans la réponse HTTP

Activer la détection des robots basée sur la souris clavier

Avant de commencer la configuration, assurez-vous d'avoir activé la fonctionnalité de détection de robots basée sur le clavier et la souris sur l'appliance.

À l'invite de commande, tapez :

```
1 add bot profile <name> -KMDetection ( ON | OFF )
2 <!--NeedCopy-->
```

Exemple :

```
add bot profile profile1 -KMDetection ON
```

Configurer l'expression de bot pour l'insertion JavaScript

Configurez l'expression du bot pour évaluer le trafic et insérer JavaScript. Le JavaScript est inséré uniquement si l'expression est évaluée comme true.

À l'invite de commande, tapez :

```
1 bind bot profile <name> -KMDetectionExpr -name <string> -expression <
     expression> -enabled ( ON | OFF ) - comment <string>
2 <!--NeedCopy-->
```

Exemple :

```
bind bot profile profile1 -KMDetectionExpr -name test -expression http.req.
url.startswith("/testsite")-enabled ON
```

Configurer le nom de fichier JavaScript inséré dans la réponse HTTP pour la détection de bots basée sur le clavier et la souris

Pour collecter les détails de l'action de l'utilisateur, l'appliance envoie un nom de fichier JavaScript dans la réponse HTTP. Le fichier JavaScript collecte toutes les données d'un enregistrement KM et les envoie à l'appliance.

À l'invite de commande, tapez :

```
1 set bot profile profile1 - KMJavaScriptName <string>
2 <!--NeedCopy-->
```

Exemple :

```
set bot profile profile1 -KMJavaScriptName script1
```

Configurer la taille de la biométrie comportementale

Vous pouvez configurer la taille maximale des données de comportement de la souris et du clavier qui peuvent être envoyées en tant qu'enregistrement KM à l'appliance et traitées par le serveur ADM.

À l'invite de commande, tapez :


```
set bot profile profile1 -KMEventsPostBodyLimit <positive_integer>
<!--NeedCopy-->
```

Exemple :

```
set bot profile profile1 - KMEventsPostBodyLimit 25
```

Une fois que vous avez configuré l'appliance NetScaler pour configurer le JavaScript et collecter les données biométriques du comportement du clavier et de la souris, l'appliance envoie les données au serveur NetScaler ADM. Pour plus d'informations sur la façon dont le serveur NetScaler ADM détecte les robots à partir de la biométrie comportementale, consultez la rubrique Violations liées aux robots.

Configurer les paramètres d'expression des robots clavier et souris à l'aide de l'interface graphique

1. Accédez à **Sécurité > Gestion et profils des robots NetScaler**.
2. Sur la page **NetScaler Bot Management Profiles**, sélectionnez un profil et cliquez sur **Modifier**.
3. Dans la section **Détection de robots basée sur le clavier et la souris**, définissez les paramètres suivants :
   a) Activez la détection. Cochez la case pour détecter le comportement dynamique du clavier et de la souris basé sur un robot.
   b) Limite de corps post-événement. Taille des données dynamiques du clavier et de la souris envoyées par le navigateur pour être traitées par l'appliance NetScaler.
4. Cliquez sur **OK**.



5. Sur la page du **profil de gestion des robots NetScaler**, accédez à la section **Paramètres du profil et cliquez sur Paramètres** d' **expression de bot basés sur le clavier et la souris**.
6. Dans la section **Paramètres d'expression de bots basés sur le clavier et la souris**, cliquez sur **Ajouter**.

7. Sur la page **Configurer la liaison des expressions clavier et souris du profil de gestion des robots NetScaler**, définissez les paramètres suivants :

   a) Nom de l'expression. Nom de l'expression de stratégie de robot pour la dynamique de détection du clavier et de la souris.
   b) Expression : Expression de stratégie de bot.
   c) Activé. Cochez la case pour activer la liaison d'expressions clavier et robot entre le clavier et la souris.
   d) Commentaires. Une brève description de l'expression de stratégie du bot et de sa liaison au profil du bot.
   e) Cliquez sur **OK** et sur **Fermer**.

8. Dans la section **Paramètres d'expression de bots basés sur le clavier et la souris**, cliquez sur **Mettre à jour**.



Journalisation verbale pour le trafic des robots

Lorsqu'une demande entrante est identifiée comme étant un bot, l'appliance NetScaler enregistre davantage de détails sur l'en-tête HTTP à des fins de surveillance et de résolution des problèmes. La fonctionnalité de journalisation verbeuse des robots est similaire à la journalisation verbeuse du module Web App Firewall.

Considérez un trafic entrant provenant d'un client. Si le client est identifié comme un bot, l'appliance NetScaler utilise la fonctionnalité de journalisation détaillée pour enregistrer les informations complètes de l'en-tête HTTP, telles que l'adresse du domaine, l'URL, l'en-tête de l'agent utilisateur, l'en-tête du cookie. Les détails du journal sont ensuite envoyés au serveur ADM à des fins de surveillance et de dépannage. Le message de consignation verbeux n'est pas stocké dans le fichier "ns.log".

Configurer la journalisation verbale des robots à l'aide de l'interface de ligne de commande

Pour capturer des informations d'en-tête HTTP détaillées sous forme de journaux, vous pouvez configurer le paramètre de journalisation détaillée dans le profil de bot. À l'invite de commande, tapez :

```
set bot profile <name> [-verboseLogLevel ( NONE | HTTP_FULL_HEADER ) ]
<!--NeedCopy-->
```

Exemple :

```
set bot profile p1 -verboseLogLevel HTTP_FULL_HEADER
```

Configurer la journalisation détaillée des robots à l'aide de l'interface graphique NetScaler

Suivez la procédure pour configurer le niveau de journalisation détaillé dans le profil du bot.

1. Dans le volet de navigation, accédez à **Sécurité > NetScaler Bot Management.**
2. Dans la page **NetScaler Bot Management Profiles**, cliquez sur **Ajouter**.
3. Dans la page **Create NetScaler Bot Management Profile**, sélectionnez le niveau de journalisation verbeux en tant qu' **en-tête complet HTTP**.
4. Cliquez sur **OK** et **Terminé**.



Configurer une action pour les demandes de robots usurpées

Un attaquant peut tenter de se faire passer pour un robot compétent et d'envoyer des requêtes à votre serveur d'applications. Ces robots sont identifiés comme des robots usurpés à l'aide de la signature du bot. Configurez les actions suivantes contre les robots usurpés afin de protéger votre serveur d'applications :

- ABANDONNER
- NONE
- REDIRIGER
- RESET

Configurer une action pour les demandes de robots usurpées à l'aide de l'interface de ligne de commande

Exécutez la commande suivante pour configurer une action pour les demandes de robots usurpées :


```
set bot profile <bot-profile-name> -spoofedReqAction <action> LOG
<!--NeedCopy-->
```

Exemple :

```
set bot profile bot_profile -spoofedReqAction DROP LOG
<!--NeedCopy-->
```

Dans cet exemple, les requêtes provenant de robots usurpés sont supprimées et enregistrées dans une appliance NetScaler.

> **Conseil**
>
> Pour enregistrer les événements provenant des robots usurpés, spécifiez `LOG` dans la commande.

Configurer une action pour les demandes de robots usurpées à l'aide de l'interface graphique

Suivez les étapes pour configurer une action pour les demandes usurpées du bot :

1. Accédez à **Sécurité > Gestion des robots NetScaler.**
2. Dans la page **NetScaler Bot Management Profiles**, cliquez sur **Ajouter**.
3. Sélectionnez une action dans la liste des **actions de demande usurpée** .
4. Sélectionnez **Enregistrer les demandes usurpées**.

   Cette action enregistre les événements provenant de robots usurpés.

   

5. Cliquez sur **Create**.

En-têtes de requête supprimés par NetScaler Bot Management

La plupart des en-têtes de demande liés à la mise en cache sont supprimés pour afficher chaque demande dans le contexte d'une session. De même, si la demande inclut un en-tête de codage permettant au serveur Web d'envoyer des réponses compressées, la direction du bot supprime cet en-tête afin que le contenu de la réponse du serveur non compressée soit inspecté par la direction du bot pour insérer le code JavaScript.

La gestion des robots supprime les en-têtes de demande suivants :

Plage : utilisée pour effectuer une restauration après un transfert de fichier partiel ou ayant échoué.

If-Range - Permet à un client de récupérer un objet partiel lorsqu'il contient déjà une partie de cet objet dans son cache (GET conditionnel).

If-Modified-Since - Si l'objet demandé n'est pas modifié depuis l'heure spécifiée dans ce champ, aucune entité n'est renvoyée par le serveur. Vous obtenez une erreur HTTP 304 non modifiée.

If-None-Match : permet des mises à jour efficaces des informations mises en cache avec un minimum de surcharge.

Accept-Encoding - Quelles méthodes de codage sont autorisées pour un objet particulier, tel que gzip.

Gestion des bots

May 5, 2023

Vous trouverez ci-dessous certains des scénarios de résolution des problèmes abordés dans la gestion des robots NetScaler.

1. Comment gérer les cas de faux positifs ?

   Vous pouvez utiliser la fonctionnalité de liste d'autorisation du bot pour gérer les cas de faux positifs et ces transactions peuvent être contournées.

2. Comment obtenir plus de détails sur le mauvais trafic de bots ?

   Vous pouvez utiliser la fonctionnalité de journalisation des audits pour obtenir des détails sur le trafic classé comme mauvais robots.

3. Pourquoi devriez-vous modifier le nom de signature par défaut ?

   Vous pouvez modifier le nom de signature par défaut si des conflits sont détectés au niveau des ressources du point de terminaison desservies par l'appliance NetScaler.

Gestion des bots

May 5, 2023

1. Qu'est-ce que la gestion des robots NetScaler ?

   La gestion des bots de NetScaler détecte et distingue le trafic des bons bots, des mauvais bots et des clients humains. La fonctionnalité de gestion des bots protège vos applications Web contre les mauvais robots en appliquant une action configurée sur les demandes entrantes.

2. Pourquoi NetScaler doit gérer les robots pour votre application Web ?

   Les robots malveillants représentent 30% de votre trafic Internet. Les bots malveillants ont un impact sur les applications Web de diverses manières, telles que le lancement d'une attaque DoS, le spam d'adresses e-mail, le ralentissement de l'application à l'aide de programmes de téléchargement, le téléchargement de contenu à partir de sites Web, etc. En outre, les robots peuvent facilement contourner certains des mécanismes de détection bien connus entraînant une perte de données, de revenus et de réputation pour votre organisation.

3. Quelles sont les techniques utilisées pour détecter un bot entrant ?

   L'appliance utilise des techniques de détection telles que la réputation IP, la limitation du débit, l'empreinte digitale de l'appareil, le TPS et les techniques de détection des bots. En outre, vous pouvez configurer une liste de blocage personnalisée sur l'interface graphique de NetScaler pour classer les robots malveillants spécifiques à l'organisation.

4. Qu'est-ce qu'un fichier de signature de bot et son objectif ?

   Le fichier de signature du bot contient l'empreinte des bons et des mauvais robots connus. Le fichier de signatures est mis à jour périodiquement pour inclure les dernières signatures de bots pour une meilleure protection contre les bots.

5. Quel type de licence NetScaler dois-je acheter ?

   La gestion des robots est disponible avec la licence ADC Premium.

6. Où puis-je trouver des journaux de bot pour le dépannage ?

   Les journaux d'audit NetScaler fournissent des informations détaillées sur les bots détectés. Pour plus d'informations, consultez la rubrique Audit Logging .

7. Existe-t-il une fonctionnalité de mise à jour automatique pour les fichiers de signature de bot ?

   Oui, la gestion des robots NetScaler prend en charge la fonctionnalité de mise à jour automatique.

8. Existe-t-il une condition préalable à l'utilisation de la technique de réputation IP des robots ?

   Activez la fonctionnalité de réputation IP avant d'activer et de configurer la réputation IP dans le profil de bot.

Mise à jour automatique des signatures de

May 5, 2023

La fonctionnalité de mise à jour automatique de la signature du bot vous permet d'obtenir les dernières signatures qui offrent une meilleure protection et une meilleure gestion du trafic contre les bons et les mauvais robots.

Les signatures sont automatiquement mises à jour toutes les heures, ce qui élimine le besoin de vérifier constamment la disponibilité de la mise à jour la plus récente. Si vous avez activé la fonctionnalité de mise à jour automatique des signatures, l'appliance NetScaler se connecte au serveur hébergeant les signatures pour vérifier si une version plus récente est disponible.

Les dernières signatures de bot hébergées sur le cloud Amazon sont configurées comme URL de signature par défaut pour vérifier la dernière mise à jour. Pour que la fonctionnalité de mise à jour automatique fonctionne, vous devez également configurer le serveur DNS pour accéder au site externe.

Signatures de

Tous les objets de signature définis par l'utilisateur qui sont créés à l'aide de l'objet de signature par défaut du bot ont une version supérieure à zéro. Si vous activez la mise à jour automatique des signatures, toutes les signatures sont mises à jour automatiquement. Vous pouvez mettre à jour l'action par défaut pour les signatures de robots en sélectionnant une signature ou un groupe de signatures à l'aide de la fonctionnalité de recherche de l'interface graphique de gestion des robots NetScaler.

URL de mise à jour de la signature de bot : `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`

Configurer la mise à jour automatique des signatures

Pour activer la fonctionnalité de mise à jour automatique des signatures, vous devez exécuter la commande suivante :

À l'invite de commande, tapez :

```
set bot settings SignatureAutoUpdate ON
<!--NeedCopy-->
```

Articles d'alerte de signature de bot

May 5, 2023

La gestion des robots NetScaler annonce les mises à jour des signatures que vous pouvez télécharger et appliquer sur votre appliance. Lorsque vous détectez une attaque de bot, vous recevez une notification par e-mail concernant la mise à jour de la nouvelle signature. Vous pouvez télécharger la signature et l'appliquer sur votre appliance.

Pour obtenir des mises à jour sur les nouvelles signatures de bot, vous devez configurer la fonctionnalité de mise à jour automatique des signatures. Pour plus d'informations, consultez la rubrique Mise à jour automatique des signatures de bot .

Mise à jour de la signature du bot pour novembre 2020

May 5, 2023

De nouvelles règles de signatures sont générées pour les bots identifiés dans la semaine 2020-11-11. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

Signature version 5 applicable à la plate-forme NetScaler 13.0.

Signatures de nouveaux robots

Vous trouverez ci-dessous une liste des règles de signature de bot, de la catégorie et de son type.

Catégorie	Type de robot	Nombre de signatures
Scraper	Bot correct	3
Marketing	Bot correct	23
Feed Fetcher	Bot correct	2
Outil	Bot incorrect	3
Moteur de recherche	Bot correct	34
Crawler	Bot correct	6
Sans catégorie	Bot incorrect	6
Analyseur de virus	Bot correct	1
Créateur de capture d’écran	Bot correct	7
Scraper	Bot incorrect	1
Outil	Bot correct	7

Mise à jour de la signature du bot pour janvier 2021

May 5, 2023

Certaines signatures de bots existantes sont mises à jour. Vous pouvez télécharger et configurer ces

règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

La version 6 de Signature est applicable aux plateformes NetScaler dotées de versions 13.0 61.x ou ultérieures.

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
143	Crawler	Bot correct
561	Scraper	Bot correct
857	Moniteur de site	Bot correct
892	Moniteur de site	Bot incorrect
894	Moniteur de site	Bot incorrect
980	Scraper	Bot incorrect
1025	Moniteur de site	Bot incorrect
1029	Feed Fetcher	Bot incorrect
1030	Créateur de capture d’écran	Bot incorrect
1034	Outil	Bot incorrect
1039	Marketing	Bot incorrect
1042	Moniteur de site	Bot incorrect
1047	Moniteur de site	Bot incorrect
1053	Moniteur de site	Bot incorrect
1072	Moteur de recherche	Bot incorrect
1073	Feed Fetcher	Bot incorrect
1074	Sans catégorie	Bot incorrect
1078	Créateur de capture d’écran	Bot incorrect
1109	Marketing	Bot incorrect
1132	Feed Fetcher	Bot incorrect
1138	Marketing	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
1150	Moteur de recherche	Bot incorrect
1164	Moteur de recherche	Bot incorrect
1167	Marketing	Bot incorrect
1173	Outil	Bot incorrect
1174	Marketing	Bot incorrect
1176	Moteur de recherche	Bot incorrect
1178	Tester de vitesse	Bot incorrect
1185	Créateur de capture d'écran	Bot incorrect
1209	Sans catégorie	Bot incorrect
1244	Moniteur de site	Bot incorrect
1251	Moteur de recherche	Bot incorrect
1254	Moniteur de site	Bot incorrect
1256	Sans catégorie	Bot incorrect
1259	Outil	Bot incorrect
1287	Moteur de recherche	Bot incorrect
1296	Moteur de recherche	Bot incorrect
1312	Sans catégorie	Bot incorrect
1316	Marketing	Bot incorrect
1322	Moniteur de site	Bot incorrect
1325	Créateur de capture d'écran	Bot incorrect
1328	Moteur de recherche	Bot incorrect
1330	Marketing	Bot incorrect
1337	Outil	Bot incorrect
1360	Moteur de recherche	Bot incorrect
1367	Moteur de recherche	Bot incorrect
1374	Outil	Bot incorrect
1380	Sans catégorie	Bot incorrect
1388	Moteur de recherche	Bot incorrect
1400	Feed Fetcher	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
1413	Sans catégorie	Bot incorrect
1420	Feed Fetcher	Bot incorrect
1422	Moniteur de site	Bot incorrect
1442	Sans catégorie	Bot incorrect
1447	Moteur de recherche	Bot incorrect
1460	Marketing	Bot incorrect
1467	Outil	Bot incorrect
1469	Outil	Bot incorrect
1471	Moteur de recherche	Bot incorrect
1484	Sans catégorie	Bot incorrect
1493	Marketing	Bot incorrect
1502	Moniteur de site	Bot incorrect
1504	Sans catégorie	Bot incorrect
1506	Sans catégorie	Bot incorrect
1518	Sans catégorie	Bot incorrect
1520	Moteur de recherche	Bot incorrect
1531	Feed Fetcher	Bot incorrect
1533	Sans catégorie	Bot incorrect
1540	Moteur de recherche	Bot incorrect
1556	Marketing	Bot incorrect
1560	Sans catégorie	Bot incorrect
1564	Outil	Bot incorrect
1570	Moniteur de site	Bot incorrect
1575	Moteur de recherche	Bot incorrect
1586	Analyseur de virus	Bot incorrect
1588	Sans catégorie	Bot incorrect
1594	Outil	Bot incorrect
1619	Marketing	Bot incorrect
1623	Outil	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
1626	Moteur de recherche	Bot incorrect
1632	Feed Fetcher	Bot incorrect
1648	Moteur de recherche	Bot incorrect
1652	Marketing	Bot incorrect
1660	Marketing	Bot incorrect
1713	Outil	Bot incorrect
1719	Moteur de recherche	Bot incorrect
1722	Sans catégorie	Bot incorrect
1744	Sans catégorie	Bot incorrect
1754	Sans catégorie	Bot incorrect
1757	Sans catégorie	Bot incorrect
1762	Sans catégorie	Bot incorrect
1769	Sans catégorie	Bot incorrect
1771	Marketing	Bot incorrect
1779	Outil	Bot incorrect
1782	Outil	Bot incorrect
1785	Tester de vitesse	Bot incorrect
1786	Outil	Bot incorrect
1792	Moniteur de site	Bot incorrect
1869	Outil	Bot incorrect
1928	Marketing	Bot incorrect
1942	Moniteur de site	Bot incorrect
1949	Marketing	Bot incorrect
1954	Marketing	Bot incorrect
1964	Sans catégorie	Bot incorrect
1969	Moteur de recherche	Bot incorrect
2294	Moteur de recherche	Bot incorrect
2303	Sans catégorie	Bot incorrect
2308	Scraper	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
2335	Marketing	Bot incorrect
2374	Sans catégorie	Bot incorrect
2377	Sans catégorie	Bot incorrect
2385	Outil	Bot incorrect
2389	Sans catégorie	Bot incorrect
2414	Sans catégorie	Bot incorrect
2421	Sans catégorie	Bot incorrect
2424	Sans catégorie	Bot incorrect
2427	Sans catégorie	Bot incorrect
2429	Moteur de recherche	Bot incorrect
2437	Sans catégorie	Bot incorrect
2440	Moteur de recherche	Bot incorrect
2443	Sans catégorie	Bot incorrect
2453	Marketing	Bot incorrect
2472	Marketing	Bot incorrect
2474	Feed Fetcher	Bot incorrect
2482	Sans catégorie	Bot incorrect
2500	Créateur de capture d’écran	Bot incorrect
2503	Sans catégorie	Bot incorrect
2507	Sans catégorie	Bot incorrect
2516	Outil	Bot incorrect
2536	Marketing	Bot incorrect
2543	Outil	Bot incorrect
2548	Outil	Bot incorrect
2557	Marketing	Bot incorrect
2561	Sans catégorie	Bot incorrect
2572	Sans catégorie	Bot incorrect
2578	Sans catégorie	Bot incorrect
2584	Sans catégorie	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
2588	Sans catégorie	Bot incorrect
2592	Moteur de recherche	Bot incorrect
2600	Outil	Bot incorrect
2606	Sans catégorie	Bot incorrect
2611	Sans catégorie	Bot incorrect
2622	Outil	Bot incorrect
2625	Outil	Bot incorrect
2631	Outil	Bot incorrect
2635	Outil	Bot incorrect
2637	Créateur de capture d’écran	Bot incorrect
2641	Moteur de recherche	Bot incorrect
2655	Sans catégorie	Bot incorrect
2657	Marketing	Bot incorrect
2663	Sans catégorie	Bot incorrect
2666	Outil	Bot incorrect
2672	Feed Fetcher	Bot incorrect
2674	Outil	Bot incorrect
2681	Moteur de recherche	Bot incorrect
2684	Marketing	Bot incorrect
2690	Sans catégorie	Bot incorrect
2704	Sans catégorie	Bot incorrect
2707	Sans catégorie	Bot incorrect
2714	Feed Fetcher	Bot incorrect
2722	Sans catégorie	Bot incorrect
2726	Feed Fetcher	Bot incorrect
2730	Créateur de capture d’écran	Bot incorrect
2736	Sans catégorie	Bot incorrect
2749	Sans catégorie	Bot incorrect
2753	Outil	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
2756	Outil	Bot incorrect
2760	Tester de vitesse	Bot incorrect
2780	Outil	Bot incorrect
2785	Moniteur de site	Bot incorrect
2789	Sans catégorie	Bot incorrect
2797	Outil	Bot incorrect
2801	Outil	Bot incorrect
2808	Outil	Bot incorrect
2810	Sans catégorie	Bot incorrect
2813	Sans catégorie	Bot incorrect
2816	Sans catégorie	Bot incorrect
2820	Vérificateur de liens	Bot incorrect
2824	Vérificateur de liens	Bot incorrect
2831	Créateur de capture d’écran	Bot incorrect
2843	Outil	Bot incorrect
2846	Outil	Bot incorrect
2849	Marketing	Bot incorrect
2851	Sans catégorie	Bot incorrect
2855	Sans catégorie	Bot incorrect
2859	Outil	Bot incorrect
2873	Sans catégorie	Bot incorrect
2875	Créateur de capture d’écran	Bot incorrect
2879	Sans catégorie	Bot incorrect
2881	Sans catégorie	Bot incorrect
2886	Moniteur de site	Bot incorrect
2899	Sans catégorie	Bot incorrect
2916	Sans catégorie	Bot incorrect
2924	Outil	Bot incorrect
2932	Marketing	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
2935	Vérificateur de liens	Bot incorrect
2939	Marketing	Bot incorrect
2942	Sans catégorie	Bot incorrect
2955	Moteur de recherche	Bot incorrect
2960	Outil	Bot incorrect
2964	Sans catégorie	Bot incorrect
2972	Marketing	Bot incorrect
2978	Analyseur de vulnérabilité	Bot incorrect
2980	Outil	Bot incorrect
2985	Marketing	Bot incorrect
2993	Sans catégorie	Bot incorrect
2999	Créateur de capture d’écran	Bot incorrect
3003	Feed Fetcher	Bot incorrect
3005	Sans catégorie	Bot incorrect
3013	Sans catégorie	Bot incorrect
3016	Sans catégorie	Bot incorrect
3021	Moteur de recherche	Bot incorrect
3026	Sans catégorie	Bot incorrect
3030	Marketing	Bot incorrect
3065	Marketing	Bot incorrect
3068	Sans catégorie	Bot incorrect
3072	Marketing	Bot incorrect
3077	Marketing	Bot incorrect
3080	Sans catégorie	Bot incorrect
3086	Scraper	Bot incorrect
3092	Moteur de recherche	Bot incorrect
3100	Sans catégorie	Bot incorrect
3104	Outil	Bot incorrect
3111	Sans catégorie	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
3116	Moniteur de site	Bot incorrect
3118	Outil	Bot incorrect
3120	Marketing	Bot incorrect
3122	Moteur de recherche	Bot incorrect
3126	Marketing	Bot incorrect
3141	Outil	Bot incorrect
3143	Sans catégorie	Bot incorrect
3145	Scraper	Bot incorrect
3150	Sans catégorie	Bot incorrect
3173	Vérificateur de liens	Bot incorrect
3176	Sans catégorie	Bot incorrect
3186	Tester de vitesse	Bot incorrect
3190	Scraper	Bot incorrect
3203	Moteur de recherche	Bot incorrect
3216	Sans catégorie	Bot incorrect
3220	Outil	Bot incorrect
3223	Vérificateur de liens	Bot incorrect
3241	Sans catégorie	Bot incorrect
3245	Moniteur de site	Bot incorrect
3285	Sans catégorie	Bot incorrect
3304	Marketing	Bot incorrect
3307	Vérificateur de liens	Bot incorrect
3316	Outil	Bot incorrect
3326	Marketing	Bot incorrect
3333	Moteur de recherche	Bot incorrect
3340	Moteur de recherche	Bot incorrect
3344	Marketing	Bot incorrect
3350	Sans catégorie	Bot incorrect
3355	Marketing	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
3365	Sans catégorie	Bot incorrect
3378	Sans catégorie	Bot incorrect
3388	Outil	Bot incorrect
3396	Sans catégorie	Bot incorrect
3400	Sans catégorie	Bot incorrect
3421	Sans catégorie	Bot incorrect
3439	Sans catégorie	Bot incorrect
3447	Feed Fetcher	Bot incorrect
3451	Outil	Bot incorrect
3459	Créateur de capture d’écran	Bot incorrect
3469	Analyseur de vulnérabilité	Bot incorrect
3475	Sans catégorie	Bot incorrect
3485	Moteur de recherche	Bot incorrect
3493	Outil	Bot incorrect
3502	Marketing	Bot incorrect
3507	Moteur de recherche	Bot incorrect
3523	Sans catégorie	Bot incorrect
3535	Tester de vitesse	Bot incorrect
3549	Sans catégorie	Bot incorrect
3556	Sans catégorie	Bot incorrect
3561	Sans catégorie	Bot incorrect
3565	Sans catégorie	Bot incorrect
3572	Moteur de recherche	Bot incorrect
3578	Sans catégorie	Bot incorrect
3610	Moteur de recherche	Bot incorrect
3617	Sans catégorie	Bot incorrect
3621	Marketing	Bot incorrect
3632	Outil	Bot incorrect
3635	Marketing	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
3653	Sans catégorie	Bot incorrect
3661	Moteur de recherche	Bot incorrect
3704	Sans catégorie	Bot incorrect
3707	Sans catégorie	Bot incorrect
3711	Sans catégorie	Bot incorrect
3730	Moteur de recherche	Bot incorrect
3740	Moniteur de site	Bot incorrect
3759	Moteur de recherche	Bot incorrect
3764	Sans catégorie	Bot incorrect
3770	Sans catégorie	Bot incorrect

Mise à jour de la signature du bot pour mars 2021

May 5, 2023

Certaines signatures de bots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

La version 7 de Signature est applicable aux plateformes NetScaler dotées de versions 13.0 61.x ou ultérieures.

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
278	Scraper	Bot correct
378	Scraper	Bot correct
379	Scraper	Bot correct
380	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
381	Scraper	Bot correct
382	Scraper	Bot correct
383	Scraper	Bot correct
384	Scraper	Bot correct
385	Scraper	Bot correct
386	Scraper	Bot correct
387	Scraper	Bot correct
389	Scraper	Bot correct
390	Scraper	Bot correct
391	Scraper	Bot correct
494	Scraper	Bot correct
627	Moteur de recherche	Bot correct
660	Moteur de recherche	Bot correct
3840	Crawler	Bot correct

Mise à jour de la signature du bot pour août 2021

May 5, 2023

De nouvelles signatures sont ajoutées et certaines signatures de bots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

La version 8 de Signature est applicable aux plateformes NetScaler dotées de versions 13.0 61.x ou ultérieures.

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
236	Scraper	Bot correct
378	Scraper	Bot correct
381	Scraper	Bot correct
382	Scraper	Bot correct
390	Scraper	Bot correct
544	Scraper	Bot correct
702	Moteur de recherche	Bot correct
979	Scraper	Bot incorrect
3791	Tester de vitesse	Bot correct
3797	Marketing	Bot correct
3800	Marketing	Bot correct
3824	Crawler	Bot incorrect
3833	Moteur de recherche	Bot correct
3849	Crawler	Bot correct
3871	Marketing	Bot correct
3963	Marketing	Bot correct
4027	Moteur de recherche	Bot correct

Nouvelle signature de bot

ID de signature du bot	Catégorie de bot	Type de robot
4028	Marketing	Bot correct
4029	Outil	Bot correct
4030	Scraper	Bot correct
4031	Scraper	Bot correct
4032	Sans catégorie	Bot incorrect
4033	Crawler	Bot correct
4034	Crawler	Bot correct
4035	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4036	Analyseur de vulnérabilité	Bot correct
4037	Analyseur de vulnérabilité	Bot correct
4038	Sans catégorie	Bot incorrect
4039	Outil	Bot correct
4040	Crawler	Bot correct
4041	Outil	Bot correct
4042	Crawler	Bot correct
4043	Créateur de capture d’écran	Bot correct
4044	Scraper	Bot incorrect
4045	Scraper	Bot incorrect
4046	Scraper	Bot incorrect
4047	Sans catégorie	Bot incorrect
4048	Feed Fetcher	Bot correct
4049	Sans catégorie	Bot incorrect
4050	Crawler	Bot correct
4051	Crawler	Bot correct
4052	Outil	Bot correct
4053	Outil	Bot correct
4054	Scraper	Bot incorrect
4055	Sans catégorie	Bot correct
4056	Marketing	Bot correct
4057	Créateur de capture d’écran	Bot correct
4058	Crawler	Bot correct
4059	Sans catégorie	Bot incorrect
4060	Moteur de recherche	Bot correct
4061	Moteur de recherche	Bot correct
4062	Moteur de recherche	Bot correct
4063	Moteur de recherche	Bot correct
4064	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4065	Scraper	Bot correct
4066	Marketing	Bot correct
4067	Marketing	Bot correct
4068	Sans catégorie	Bot incorrect
4069	Sans catégorie	Bot incorrect
4070	Sans catégorie	Bot incorrect
4071	Outil	Bot correct
4072	Outil	Bot incorrect
4073	Sans catégorie	Bot incorrect
4074	Sans catégorie	Bot incorrect
4075	Outil	Bot incorrect
4076	Marketing	Bot correct
4077	Scraper	Bot correct
4078	Crawler	Bot correct
4079	Crawler	Bot correct
4080	Outil	Bot incorrect
4081	Moteur de recherche	Bot correct
4082	Outil	Bot correct
4083	Sans catégorie	Bot incorrect
4084	Sans catégorie	Bot incorrect
4085	Outil	Bot correct
4086	Outil	Bot correct
4087	Outil	Bot incorrect
4088	Moteur de recherche	Bot correct
4089	Marketing	Bot correct
4090	Outil	Bot correct
4091	Outil	Bot correct
4092	Outil	Bot correct
4093	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4094	Sans catégorie	Bot correct
4095	Moniteur de site	Bot correct
4096	Moniteur de site	Bot correct
4097	Moniteur de site	Bot correct
4098	Crawler	Bot correct
4099	Moteur de recherche	Bot correct
4100	Moteur de recherche	Bot correct
4101	Moteur de recherche	Bot correct
4102	Moteur de recherche	Bot correct
4103	Marketing	Bot correct
4104	Marketing	Bot correct
4105	Marketing	Bot correct
4106	Marketing	Bot correct
4107	Marketing	Bot correct
4108	Marketing	Bot correct
4109	Moteur de recherche	Bot correct
4110	Crawler	Bot correct
4111	Crawler	Bot correct
4112	Crawler	Bot correct
4113	Analyseur de vulnérabilité	Bot correct
4114	Crawler	Bot correct
4115	Outil	Bot correct
4116	Sans catégorie	Bot incorrect
4117	Sans catégorie	Bot incorrect
4118	Sans catégorie	Bot incorrect
4119	Sans catégorie	Bot incorrect
4120	Marketing	Bot correct
4121	Marketing	Bot correct
4122	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4123	Marketing	Bot correct
4124	Marketing	Bot correct
4125	Marketing	Bot correct
4126	Marketing	Bot correct
4127	Marketing	Bot correct
4128	Marketing	Bot correct
4129	Marketing	Bot correct
4130	Marketing	Bot correct
4131	Outil	Bot correct
4132	Marketing	Bot correct
4133	Marketing	Bot correct
4134	Outil	Bot correct
4135	Marketing	Bot correct
4136	Marketing	Bot correct
4137	Marketing	Bot correct
4138	Marketing	Bot correct
4139	Marketing	Bot correct
4140	Marketing	Bot correct
4141	Marketing	Bot correct
4142	Marketing	Bot correct
4143	Marketing	Bot correct
4144	Marketing	Bot correct
4145	Moteur de recherche	Bot correct
4146	Moteur de recherche	Bot correct
4147	Moteur de recherche	Bot correct
4148	Moteur de recherche	Bot correct
4149	Moteur de recherche	Bot correct
4150	Moteur de recherche	Bot correct
4151	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4152	Moteur de recherche	Bot correct
4153	Moteur de recherche	Bot correct
4154	Moteur de recherche	Bot correct
4155	Moteur de recherche	Bot correct
4156	Créateur de capture d’écran	Bot correct
4157	Moteur de recherche	Bot correct
4158	Moteur de recherche	Bot correct
4159	Moteur de recherche	Bot correct
4160	Créateur de capture d’écran	Bot correct
4161	Moteur de recherche	Bot correct
4162	Moteur de recherche	Bot correct
4163	Outil	Bot correct
4164	Moteur de recherche	Bot correct
4165	Marketing	Bot correct
4166	Sans catégorie	Bot incorrect
4167	Outil	Bot incorrect
4168	Tester de vitesse	Bot correct
4169	Scraper	Bot incorrect
4170	Outil	Bot correct
4171	Scraper	Bot incorrect
4172	Web Crawler	Bot correct
4173	Outil	Bot correct
4174	Crawler	Bot correct
4175	Crawler	Bot correct
4176	Outil	Bot correct
4177	Moteur de recherche	Bot correct
4178	Outil	Bot correct
4179	Web Crawler	Bot correct
4180	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4181	Moniteur de site	Bot correct
4182	Moniteur de site	Bot correct
4183	Moniteur de site	Bot correct
4184	Moniteur de site	Bot correct
4185	Moteur de recherche	Bot correct
4186	Outil	Bot correct
4187	Outil	Bot correct
4188	Créateur de capture d'écran	Bot correct
4189	Marketing	Bot correct
4190	Moteur de recherche	Bot correct
4191	Moteur de recherche	Bot correct
4192	Moteur de recherche	Bot correct
4193	Moteur de recherche	Bot correct
4194	Outil	Bot correct
4195	Moteur de recherche	Bot incorrect
4196	Outil	Bot correct
4197	Outil	Bot correct
4198	Marketing	Bot correct
4199	Marketing	Bot correct
4200	Analyseur de vulnérabilité	Bot correct
4201	Outil	Bot correct
4202	Outil	Bot correct
4203	Sans catégorie	Bot incorrect
4204	Sans catégorie	Bot incorrect
4205	Moteur de recherche	Bot correct
4206	Marketing	Bot correct
4207	Marketing	Bot correct
4208	Moteur de recherche	Bot correct
4209	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4210	Tester de vitesse	Bot correct
4211	Outil	Bot correct
4212	Feed Fetcher	Bot correct
4213	Feed Fetcher	Bot correct
4214	Scraper	Bot incorrect
4215	Outil	Bot correct
4216	Outil	Bot correct
4217	Outil	Bot incorrect
4218	Scraper	Bot incorrect
4219	Marketing	Bot correct
4220	Outil	Bot correct
4221	Outil	Bot incorrect
4222	Moniteur de site	Bot correct
4223	Marketing	Bot correct
4224	Moteur de recherche	Bot correct
4225	Moteur de recherche	Bot correct
4226	Moteur de recherche	Bot correct
4227	Marketing	Bot correct
4228	Marketing	Bot correct
4229	Outil	Bot correct
4230	Sans catégorie	Bot incorrect
4231	Créateur de capture d’écran	Bot correct
4232	Outil	Bot correct
4233	Moniteur de site	Bot correct
4234	Moniteur de site	Bot correct
4235	Moniteur de site	Bot correct
4236	Moniteur de site	Bot correct
4237	Moniteur de site	Bot correct
4238	Moniteur de site	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4239	Sans catégorie	Bot incorrect
4240	Marketing	Bot correct
4241	Marketing	Bot correct
4242	Marketing	Bot correct
4243	Marketing	Bot correct
4244	Marketing	Bot correct
4245	Marketing	Bot correct
4246	Marketing	Bot correct
4247	Moteur de recherche	Bot correct
4248	Moteur de recherche	Bot correct
4249	Créateur de capture d’écran	Bot correct
4250	Moteur de recherche	Bot correct
4251	Moteur de recherche	Bot correct
4252	Crawler	Bot correct
4253	Crawler	Bot correct
4254	Crawler	Bot correct
4255	Outil	Bot correct
4256	Sans catégorie	Bot correct
4257	Outil	Bot correct
4258	Crawler	Bot correct
4259	Crawler	Bot correct
4260	Outil	Bot correct
4261	Outil	Bot correct
4262	Outil	Bot correct
4263	Marketing	Bot correct
4264	Crawler	Bot incorrect
4265	Moteur de recherche	Bot correct
4266	Sans catégorie	Bot correct
4267	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4268	Outil	Bot correct
4269	Moteur de recherche	Bot correct
4270	Moteur de recherche	Bot correct
4271	Moteur de recherche	Bot correct
4272	Moteur de recherche	Bot correct
4273	Moteur de recherche	Bot correct
4274	Moteur de recherche	Bot correct
4275	Moteur de recherche	Bot correct
4276	Sans catégorie	Bot incorrect
4277	Sans catégorie	Bot incorrect
4278	Sans catégorie	Bot incorrect
4279	Marketing	Bot correct
4280	Crawler	Bot correct
4281	Sans catégorie	Bot incorrect
4282	Marketing	Bot correct
4283	Marketing	Bot correct
4284	Marketing	Bot correct
4285	Marketing	Bot correct
4286	Marketing	Bot correct
4287	Marketing	Bot correct
4288	Marketing	Bot correct
4289	Marketing	Bot correct
4290	Marketing	Bot correct
4291	Marketing	Bot correct
4292	Marketing	Bot correct
4293	Marketing	Bot correct
4294	Marketing	Bot correct
4295	Moteur de recherche	Bot correct
4296	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4297	Moteur de recherche	Bot correct
4298	Moteur de recherche	Bot correct
4299	Moteur de recherche	Bot correct
4300	Moteur de recherche	Bot correct
4301	Moteur de recherche	Bot correct
4302	Moteur de recherche	Bot correct
4303	Moteur de recherche	Bot correct
4304	Moteur de recherche	Bot correct
4305	Moteur de recherche	Bot correct
4306	Créateur de capture d’écran	Bot correct
4307	Moteur de recherche	Bot correct
4308	Moteur de recherche	Bot correct
4309	Moteur de recherche	Bot correct
4310	Moteur de recherche	Bot correct
4311	Créateur de capture d’écran	Bot correct
4312	Moteur de recherche	Bot correct
4313	Moteur de recherche	Bot correct
4314	Moteur de recherche	Bot correct
4315	Moteur de recherche	Bot correct
4316	Moteur de recherche	Bot correct
4317	Moteur de recherche	Bot correct
4318	Créateur de capture d’écran	Bot correct
4319	Créateur de capture d’écran	Bot correct
4320	Sans catégorie	Bot incorrect
4321	Sans catégorie	Bot correct
4322	Crawler	Bot correct
4323	Outil	Bot correct
4324	Outil	Bot correct
4325	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4326	Scraper	Bot incorrect
4327	Moteur de recherche	Bot correct
4328	Marketing	Bot correct
4329	Sans catégorie	Bot incorrect
4330	Moniteur de site	Bot correct
4331	Moteur de recherche	Bot correct
4332	Moteur de recherche	Bot correct
4333	Sans catégorie	Bot incorrect
4334	Scraper	Bot correct
4335	Marketing	Bot correct
4336	Marketing	Bot correct
4337	Outil	Bot correct
4338	Outil	Bot correct
4339	Outil	Bot correct
4340	Crawler	Bot correct
4341	Crawler	Bot correct
4342	Analyseur de vulnérabilité	Bot correct
4343	Analyseur de vulnérabilité	Bot correct
4344	Scraper	Bot correct
4345	Marketing	Bot correct
4346	Marketing	Bot correct
4347	Marketing	Bot correct
4348	Marketing	Bot correct
4349	Marketing	Bot correct
4350	Marketing	Bot correct
4351	Marketing	Bot correct
4352	Marketing	Bot correct
4353	Marketing	Bot correct
4354	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4355	Moteur de recherche	Bot correct
4356	Moteur de recherche	Bot correct
4357	Moteur de recherche	Bot correct
4358	Moteur de recherche	Bot correct
4359	Moteur de recherche	Bot correct
4360	Moteur de recherche	Bot correct
4361	Moteur de recherche	Bot correct
4362	Moteur de recherche	Bot correct
4363	Moteur de recherche	Bot correct
4364	Moteur de recherche	Bot correct
4365	Créateur de capture d’écran	Bot correct
4366	Moteur de recherche	Bot correct
4367	Moteur de recherche	Bot correct
4368	Moteur de recherche	Bot correct
4369	Moteur de recherche	Bot correct
4370	Créateur de capture d’écran	Bot correct
4371	Moteur de recherche	Bot correct
4372	Moteur de recherche	Bot correct
4373	Moteur de recherche	Bot correct
4374	Moteur de recherche	Bot correct
4375	Moteur de recherche	Bot correct
4376	Créateur de capture d’écran	Bot correct
4377	Crawler	Bot correct
4378	Crawler	Bot correct
4379	Moteur de recherche	Bot correct
4380	Moteur de recherche	Bot correct
4381	Moteur de recherche	Bot correct
4382	Moteur de recherche	Bot correct
4383	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4384	Moteur de recherche	Bot correct
4385	Outil	Bot correct
4386	Sans catégorie	Bot correct
4387	Crawler	Bot correct
4388	Crawler	Bot correct
4389	Outil	Bot correct
4390	Outil	Bot correct
4391	Outil	Bot correct
4392	Outil	Bot correct
4393	Outil	Bot correct
4394	Sans catégorie	Bot correct
4395	Outil	Bot correct
4396	Moniteur de site	Bot correct
4397	Moniteur de site	Bot correct
4398	Outil	Bot incorrect
4399	Outil	Bot incorrect
4400	Outil	Bot incorrect
4401	Outil	Bot incorrect
4402	Outil	Bot incorrect
4403	Outil	Bot incorrect
4404	Moteur de recherche	Bot correct
4405	Moteur de recherche	Bot correct
4406	Moteur de recherche	Bot correct
4407	Sans catégorie	Bot correct

Mise à jour de la signature des robots pour septembre 2021

May 5, 2023

De nouvelles signatures ont été ajoutées et certaines signatures de robots existantes sont mises à jour.

Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

Signature version 9 applicable aux plateformes NetScaler dotées de versions 13.0 61.48 ou ultérieures.

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
2	Crawler	Bot correct
5	Crawler	Bot correct
9	Crawler	Bot correct
45	Crawler	Bot correct
46	Crawler	Bot correct
48	Crawler	Bot correct
52	Crawler	Bot correct
60	Crawler	Bot correct
61	Crawler	Bot correct
63	Crawler	Bot correct
67	Crawler	Bot correct
71	Crawler	Bot correct
74	Crawler	Bot correct
75	Crawler	Bot correct
76	Crawler	Bot correct
78	Crawler	Bot correct
79	Crawler	Bot correct
80	Crawler	Bot correct
81	Crawler	Bot correct
82	Crawler	Bot correct
83	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
84	Crawler	Bot correct
87	Crawler	Bot correct
90	Crawler	Bot correct
95	Crawler	Bot correct
96	Crawler	Bot correct
97	Crawler	Bot correct
100	Crawler	Bot correct
101	Crawler	Bot correct
102	Crawler	Bot correct
103	Crawler	Bot correct
104	Crawler	Bot correct
107	Crawler	Bot correct
108	Crawler	Bot correct
110	Crawler	Bot correct
111	Crawler	Bot correct
114	Crawler	Bot correct
115	Crawler	Bot correct
123	Crawler	Bot correct
135	Crawler	Bot correct
136	Crawler	Bot correct
137	Crawler	Bot correct
140	Crawler	Bot correct
141	Crawler	Bot correct
143	Crawler	Bot correct
144	Crawler	Bot correct
145	Crawler	Bot correct
146	Crawler	Bot correct
147	Crawler	Bot correct
149	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
152	Crawler	Bot correct
155	Crawler	Bot correct
156	Crawler	Bot correct
157	Crawler	Bot correct
158	Crawler	Bot correct
159	Crawler	Bot correct
160	Crawler	Bot correct
161	Crawler	Bot correct
162	Crawler	Bot correct
163	Crawler	Bot correct
164	Crawler	Bot correct
165	Crawler	Bot correct
166	Crawler	Bot correct
167	Crawler	Bot correct
172	Crawler	Bot correct
173	Crawler	Bot correct
174	Crawler	Bot correct
176	Crawler	Bot correct
177	Crawler	Bot correct
180	Crawler	Bot correct
187	Crawler	Bot correct
197	Crawler	Bot correct
201	Crawler	Bot correct
202	Crawler	Bot correct
203	Crawler	Bot correct
206	Crawler	Bot correct
211	Feed Fetcher	Bot incorrect
217	Feed Fetcher	Bot correct
219	Feed Fetcher	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
229	Scraper	Bot correct
235	Scraper	Bot correct
236	Scraper	Bot correct
237	Scraper	Bot correct
248	Scraper	Bot correct
250	Scraper	Bot correct
260	Scraper	Bot correct
263	Scraper	Bot correct
265	Scraper	Bot correct
267	Scraper	Bot correct
268	Scraper	Bot correct
271	Scraper	Bot correct
272	Scraper	Bot correct
276	Scraper	Bot correct
277	Scraper	Bot correct
278	Scraper	Bot correct
279	Scraper	Bot correct
280	Scraper	Bot correct
281	Scraper	Bot correct
283	Scraper	Bot correct
285	Scraper	Bot correct
286	Scraper	Bot correct
287	Scraper	Bot correct
290	Scraper	Bot correct
292	Scraper	Bot correct
293	Scraper	Bot correct
342	Scraper	Bot correct
343	Scraper	Bot correct
344	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
355	Scraper	Bot correct
357	Scraper	Bot correct
360	Scraper	Bot correct
362	Scraper	Bot correct
366	Scraper	Bot correct
370	Scraper	Bot correct
371	Scraper	Bot correct
372	Scraper	Bot correct
373	Scraper	Bot correct
374	Scraper	Bot correct
376	Scraper	Bot correct
377	Scraper	Bot correct
380	Scraper	Bot correct
392	Scraper	Bot correct
393	Scraper	Bot correct
394	Scraper	Bot correct
396	Scraper	Bot correct
397	Scraper	Bot correct
414	Scraper	Bot correct
418	Scraper	Bot correct
419	Scraper	Bot correct
421	Scraper	Bot correct
422	Scraper	Bot correct
423	Scraper	Bot correct
424	Scraper	Bot correct
425	Scraper	Bot correct
426	Scraper	Bot correct
427	Scraper	Bot correct
428	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
430	Scraper	Bot correct
432	Scraper	Bot correct
433	Scraper	Bot correct
434	Scraper	Bot correct
435	Scraper	Bot correct
441	Scraper	Bot correct
445	Scraper	Bot correct
446	Scraper	Bot correct
451	Scraper	Bot correct
452	Scraper	Bot correct
454	Scraper	Bot correct
455	Scraper	Bot correct
456	Scraper	Bot correct
457	Scraper	Bot correct
458	Scraper	Bot correct
461	Scraper	Bot correct
465	Scraper	Bot correct
466	Scraper	Bot correct
469	Scraper	Bot correct
473	Scraper	Bot correct
474	Scraper	Bot correct
476	Scraper	Bot correct
477	Scraper	Bot correct
484	Scraper	Bot correct
485	Scraper	Bot correct
487	Scraper	Bot correct
488	Scraper	Bot correct
489	Scraper	Bot correct
490	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
493	Scraper	Bot correct
494	Scraper	Bot correct
495	Scraper	Bot correct
497	Scraper	Bot correct
498	Scraper	Bot correct
499	Scraper	Bot correct
500	Scraper	Bot correct
505	Scraper	Bot correct
506	Scraper	Bot correct
507	Scraper	Bot correct
512	Scraper	Bot correct
513	Scraper	Bot correct
514	Scraper	Bot correct
527	Scraper	Bot correct
533	Scraper	Bot correct
539	Scraper	Bot correct
540	Scraper	Bot correct
542	Scraper	Bot correct
544	Scraper	Bot correct
545	Scraper	Bot correct
546	Scraper	Bot correct
547	Scraper	Bot correct
548	Scraper	Bot correct
551	Scraper	Bot correct
552	Scraper	Bot correct
554	Scraper	Bot correct
556	Scraper	Bot correct
558	Scraper	Bot correct
560	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
561	Scraper	Bot correct
566	Scraper	Bot correct
575	Scraper	Bot correct
578	Scraper	Bot correct
581	Scraper	Bot correct
591	Scraper	Bot correct
593	Scraper	Bot correct
595	Scraper	Bot correct
600	Scraper	Bot correct
601	Scraper	Bot correct
602	Scraper	Bot correct
604	Scraper	Bot correct
605	Scraper	Bot correct
609	Scraper	Bot correct
610	Scraper	Bot correct
611	Scraper	Bot correct
612	Scraper	Bot correct
613	Scraper	Bot correct
615	Scraper	Bot correct
620	Moteur de recherche	Bot correct
622	Moteur de recherche	Bot correct
623	Moteur de recherche	Bot correct
624	Moteur de recherche	Bot correct
626	Moteur de recherche	Bot correct
627	Moteur de recherche	Bot correct
628	Moteur de recherche	Bot correct
629	Moteur de recherche	Bot correct
633	Moteur de recherche	Bot correct
634	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
636	Moteur de recherche	Bot correct
637	Moteur de recherche	Bot correct
639	Moteur de recherche	Bot correct
640	Moteur de recherche	Bot correct
641	Moteur de recherche	Bot correct
642	Moteur de recherche	Bot correct
643	Moteur de recherche	Bot correct
647	Moteur de recherche	Bot correct
649	Moteur de recherche	Bot correct
650	Moteur de recherche	Bot correct
651	Moteur de recherche	Bot correct
654	Moteur de recherche	Bot correct
656	Moteur de recherche	Bot correct
657	Moteur de recherche	Bot correct
658	Moteur de recherche	Bot correct
659	Moteur de recherche	Bot correct
660	Moteur de recherche	Bot correct
663	Moteur de recherche	Bot correct
664	Moteur de recherche	Bot correct
665	Moteur de recherche	Bot correct
666	Moteur de recherche	Bot correct
667	Moteur de recherche	Bot correct
669	Moteur de recherche	Bot correct
670	Moteur de recherche	Bot correct
671	Moteur de recherche	Bot correct
672	Moteur de recherche	Bot correct
673	Moteur de recherche	Bot correct
674	Moteur de recherche	Bot correct
675	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
676	Moteur de recherche	Bot correct
677	Moteur de recherche	Bot correct
679	Moteur de recherche	Bot correct
680	Moteur de recherche	Bot correct
690	Moteur de recherche	Bot correct
693	Moteur de recherche	Bot correct
694	Moteur de recherche	Bot correct
697	Moteur de recherche	Bot correct
698	Moteur de recherche	Bot correct
703	Moteur de recherche	Bot correct
706	Moteur de recherche	Bot correct
712	Moteur de recherche	Bot correct
714	Moteur de recherche	Bot correct
715	Moteur de recherche	Bot correct
716	Moteur de recherche	Bot correct
721	Moteur de recherche	Bot correct
723	Moteur de recherche	Bot correct
725	Moteur de recherche	Bot correct
727	Moteur de recherche	Bot correct
728	Moteur de recherche	Bot correct
729	Moteur de recherche	Bot correct
730	Moteur de recherche	Bot correct
731	Moteur de recherche	Bot correct
732	Moteur de recherche	Bot correct
735	Moteur de recherche	Bot correct
736	Moteur de recherche	Bot correct
740	Moteur de recherche	Bot correct
748	Moteur de recherche	Bot correct
749	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
750	Moteur de recherche	Bot correct
751	Moteur de recherche	Bot correct
756	Moteur de recherche	Bot correct
757	Moteur de recherche	Bot correct
758	Moteur de recherche	Bot correct
759	Moteur de recherche	Bot correct
760	Moteur de recherche	Bot correct
761	Moteur de recherche	Bot correct
762	Moteur de recherche	Bot correct
763	Moteur de recherche	Bot correct
764	Moteur de recherche	Bot correct
765	Moteur de recherche	Bot correct
766	Moteur de recherche	Bot correct
767	Moteur de recherche	Bot correct
768	Moteur de recherche	Bot correct
769	Moteur de recherche	Bot correct
770	Moteur de recherche	Bot correct
771	Moteur de recherche	Bot correct
772	Moteur de recherche	Bot correct
773	Moteur de recherche	Bot correct
776	Moteur de recherche	Bot correct
777	Moteur de recherche	Bot correct
780	Moteur de recherche	Bot correct
781	Moteur de recherche	Bot correct
784	Moteur de recherche	Bot correct
786	Moteur de recherche	Bot correct
787	Moteur de recherche	Bot correct
788	Moteur de recherche	Bot correct
789	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
790	Moteur de recherche	Bot correct
791	Moteur de recherche	Bot correct
792	Moteur de recherche	Bot correct
795	Moteur de recherche	Bot correct
796	Moteur de recherche	Bot correct
798	Moteur de recherche	Bot correct
800	Moteur de recherche	Bot correct
801	Moteur de recherche	Bot correct
802	Moteur de recherche	Bot correct
803	Moteur de recherche	Bot correct
805	Moteur de recherche	Bot correct
806	Moteur de recherche	Bot correct
807	Moteur de recherche	Bot correct
809	Moteur de recherche	Bot correct
810	Moteur de recherche	Bot correct
811	Moteur de recherche	Bot correct
812	Moteur de recherche	Bot correct
814	Moteur de recherche	Bot correct
815	Moteur de recherche	Bot correct
816	Moteur de recherche	Bot correct
817	Moteur de recherche	Bot correct
818	Moteur de recherche	Bot correct
819	Moteur de recherche	Bot correct
820	Moteur de recherche	Bot correct
821	Moteur de recherche	Bot correct
822	Moteur de recherche	Bot correct
823	Moteur de recherche	Bot correct
825	Moteur de recherche	Bot correct
827	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
830	Moteur de recherche	Bot correct
831	Moteur de recherche	Bot correct
834	Moteur de recherche	Bot correct
837	Moteur de recherche	Bot correct
838	Moteur de recherche	Bot correct
849	Moniteur de site	Bot correct
850	Moniteur de site	Bot correct
851	Moniteur de site	Bot correct
853	Moniteur de site	Bot correct
857	Moniteur de site	Bot correct
858	Moniteur de site	Bot correct
859	Moniteur de site	Bot correct
860	Moniteur de site	Bot correct
861	Moniteur de site	Bot correct
862	Moniteur de site	Bot correct
863	Moniteur de site	Bot correct
864	Moniteur de site	Bot correct
865	Moniteur de site	Bot correct
866	Moniteur de site	Bot correct
867	Moniteur de site	Bot correct
868	Moniteur de site	Bot correct
869	Moniteur de site	Bot correct
870	Moniteur de site	Bot correct
871	Moniteur de site	Bot correct
872	Moniteur de site	Bot correct
873	Moniteur de site	Bot correct
874	Moniteur de site	Bot correct
875	Moniteur de site	Bot correct
876	Moniteur de site	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
877	Moniteur de site	Bot correct
880	Moniteur de site	Bot correct
883	Moniteur de site	Bot correct
885	Moniteur de site	Bot correct
886	Moniteur de site	Bot correct
888	Moniteur de site	Bot correct
889	Moniteur de site	Bot correct
895	Moniteur de site	Bot correct
896	Moniteur de site	Bot correct
897	Moniteur de site	Bot correct
898	Moniteur de site	Bot correct
900	Moniteur de site	Bot correct
901	Moniteur de site	Bot correct
904	Moniteur de site	Bot correct
906	Moniteur de site	Bot correct
908	Moniteur de site	Bot correct
909	Moniteur de site	Bot correct
910	Moniteur de site	Bot correct
911	Moniteur de site	Bot correct
912	Moniteur de site	Bot correct
913	Moniteur de site	Bot correct
917	Moniteur de site	Bot correct
918	Moniteur de site	Bot correct
919	Moniteur de site	Bot correct
920	Moniteur de site	Bot correct
921	Moniteur de site	Bot correct
924	Moniteur de site	Bot correct
926	Moniteur de site	Bot correct
927	Moniteur de site	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
928	Moniteur de site	Bot correct
929	Moniteur de site	Bot correct
930	Moniteur de site	Bot correct
931	Moniteur de site	Bot correct
938	Moniteur de site	Bot correct
939	Moniteur de site	Bot correct
943	Moniteur de site	Bot incorrect
958	Moniteur de site	Bot correct
959	Moniteur de site	Bot correct
960	Moniteur de site	Bot correct
963	Moniteur de site	Bot correct
984	Scraper	Bot correct
996	Scraper	Bot correct
997	Scraper	Bot correct
998	Scraper	Bot correct
1002	Scraper	Bot correct
1006	Scraper	Bot correct
1588	Sans catégorie	Bot incorrect
2561	Scraper	Bot incorrect
2810	Crawler	Bot correct
3782	Marketing	Bot correct
3783	Moteur de recherche	Bot correct
3788	Outil	Bot correct
3789	Outil	Bot correct
3790	Crawler	Bot correct
3792	Outil	Bot correct
3793	Outil	Bot correct
3794	Crawler	Bot correct
3796	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3798	Marketing	Bot correct
3799	Marketing	Bot correct
3801	Marketing	Bot correct
3802	Créateur de capture d’écran	Bot correct
3803	Moteur de recherche	Bot correct
3804	Créateur de capture d’écran	Bot correct
3805	Moteur de recherche	Bot correct
3806	Outil	Bot correct
3807	Crawler	Bot correct
3808	Crawler	Bot correct
3809	Outil	Bot correct
3810	Scraper	Bot correct
3811	Outil	Bot correct
3813	Outil	Bot correct
3814	Crawler	Bot correct
3815	Sans catégorie	Bot correct
3817	Outil	Bot correct
3818	Outil	Bot correct
3819	Outil	Bot correct
3820	Crawler	Bot correct
3821	Moteur de recherche	Bot correct
3822	Marketing	Bot correct
3823	Sans catégorie	Bot correct
3831	Scraper	Bot correct
3834	Moteur de recherche	Bot correct
3835	Moteur de recherche	Bot correct
3836	Sans catégorie	Bot correct
3837	Sans catégorie	Bot correct
3838	Sans catégorie	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3839	Marketing	Bot correct
3840	Crawler	Bot correct
3842	Crawler	Bot correct
3843	Crawler	Bot correct
3844	Marketing	Bot correct
3845	Marketing	Bot correct
3846	Marketing	Bot correct
3847	Marketing	Bot correct
3848	Sans catégorie	Bot correct
3850	Outil	Bot correct
3851	Sans catégorie	Bot correct
3852	Outil	Bot correct
3853	Analyseur de vulnérabilité	Bot correct
3854	Crawler	Bot correct
3855	Crawler	Bot correct
3856	Outil	Bot correct
3861	Marketing	Bot correct
3862	Marketing	Bot correct
3863	Marketing	Bot correct
3864	Marketing	Bot correct
3865	Marketing	Bot correct
3866	Marketing	Bot correct
3867	Marketing	Bot correct
3868	Marketing	Bot correct
3869	Outil	Bot correct
3870	Marketing	Bot correct
3872	Marketing	Bot correct
3873	Moteur de recherche	Bot correct
3874	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3875	Moteur de recherche	Bot correct
3876	Moteur de recherche	Bot correct
3877	Créateur de capture d'écran	Bot correct
3878	Moteur de recherche	Bot correct
3879	Moteur de recherche	Bot correct
3880	Créateur de capture d'écran	Bot correct
3881	Créateur de capture d'écran	Bot correct
3882	Moteur de recherche	Bot correct
3883	Moteur de recherche	Bot correct
3884	Moteur de recherche	Bot correct
3885	Moteur de recherche	Bot correct
3886	Outil	Bot correct
3887	Crawler	Bot correct
3888	Crawler	Bot correct
3889	Sans catégorie	Bot correct
3890	Marketing	Bot correct
3893	Crawler	Bot correct
3894	Outil	Bot correct
3895	Outil	Bot correct
3896	Moteur de recherche	Bot correct
3897	Outil	Bot correct
3898	Outil	Bot correct
3899	Sans catégorie	Bot correct
3901	Crawler	Bot correct
3903	Outil	Bot correct
3904	Moteur de recherche	Bot correct
3905	Moteur de recherche	Bot correct
3906	Moteur de recherche	Bot correct
3912	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3918	Crawler	Bot correct
3919	Sans catégorie	Bot correct
3920	Sans catégorie	Bot correct
3921	Sans catégorie	Bot correct
3922	Sans catégorie	Bot correct
3923	Sans catégorie	Bot correct
3924	Sans catégorie	Bot correct
3925	Sans catégorie	Bot correct
3926	Marketing	Bot correct
3927	Marketing	Bot correct
3928	Marketing	Bot correct
3929	Outil	Bot correct
3930	Marketing	Bot correct
3931	Sans catégorie	Bot correct
3932	Crawler	Bot correct
3933	Marketing	Bot correct
3934	Marketing	Bot correct
3935	Scraper	Bot correct
3936	Marketing	Bot correct
3937	Scraper	Bot correct
3938	Feed Fetcher	Bot correct
3940	Moteur de recherche	Bot correct
3941	Crawler	Bot correct
3942	Scraper	Bot correct
3946	Feed Fetcher	Bot correct
3947	Crawler	Bot correct
3950	Analyseur de virus	Bot correct
3951	Marketing	Bot correct
3952	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3953	Marketing	Bot correct
3954	Marketing	Bot correct
3955	Marketing	Bot correct
3956	Marketing	Bot correct
3957	Marketing	Bot correct
3958	Marketing	Bot correct
3959	Marketing	Bot correct
3960	Marketing	Bot correct
3961	Marketing	Bot correct
3962	Marketing	Bot correct
3964	Marketing	Bot correct
3965	Marketing	Bot correct
3966	Marketing	Bot correct
3967	Marketing	Bot correct
3968	Marketing	Bot correct
3969	Marketing	Bot correct
3970	Moteur de recherche	Bot correct
3971	Créateur de capture d’écran	Bot correct
3972	Créateur de capture d’écran	Bot correct
3973	Moteur de recherche	Bot correct
3974	Moteur de recherche	Bot correct
3975	Moteur de recherche	Bot correct
3976	Moteur de recherche	Bot correct
3977	Moteur de recherche	Bot correct
3978	Créateur de capture d’écran	Bot correct
3979	Moteur de recherche	Bot correct
3980	Créateur de capture d’écran	Bot correct
3981	Moteur de recherche	Bot correct
3982	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3983	Moteur de recherche	Bot correct
3984	Moteur de recherche	Bot correct
3985	Moteur de recherche	Bot correct
3986	Moteur de recherche	Bot correct
3987	Créateur de capture d'écran	Bot correct
3988	Moteur de recherche	Bot correct
3989	Moteur de recherche	Bot correct
3990	Moteur de recherche	Bot correct
3991	Moteur de recherche	Bot correct
3992	Moteur de recherche	Bot correct
3993	Moteur de recherche	Bot correct
3994	Moteur de recherche	Bot correct
3995	Moteur de recherche	Bot correct
3996	Moteur de recherche	Bot correct
3997	Moteur de recherche	Bot correct
3998	Moteur de recherche	Bot correct
3999	Moteur de recherche	Bot correct
4000	Créateur de capture d'écran	Bot correct
4001	Moteur de recherche	Bot correct
4002	Moteur de recherche	Bot correct
4003	Moteur de recherche	Bot correct
4004	Moteur de recherche	Bot correct
4005	Créateur de capture d'écran	Bot correct
4006	Crawler	Bot correct
4007	Marketing	Bot correct
4008	Marketing	Bot correct
4011	Outil	Bot correct
4012	Crawler	Bot correct
4013	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4014	Outil	Bot correct
4015	Crawler	Bot correct
4016	Crawler	Bot correct
4017	Outil	Bot correct
4018	Outil	Bot correct
4019	Outil	Bot correct
4020	Outil	Bot correct
4021	Marketing	Bot correct
4024	Outil	Bot correct
4025	Moteur de recherche	Bot correct
4026	Moteur de recherche	Bot correct
4028	Marketing	Bot correct
4029	Outil	Bot correct
4030	Scraper	Bot correct
4031	Scraper	Bot correct
4035	Marketing	Bot correct
4037	Analyseur de vulnérabilité	Bot correct
4042	Crawler	Bot correct
4043	Créateur de capture d’écran	Bot correct
4048	Feed Fetcher	Bot correct
4052	Outil	Bot correct
4055	Sans catégorie	Bot correct
4056	Marketing	Bot correct
4057	Créateur de capture d’écran	Bot correct
4058	Crawler	Bot correct
4060	Moteur de recherche	Bot correct
4061	Moteur de recherche	Bot correct
4062	Moteur de recherche	Bot correct
4063	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4065	Scraper	Bot correct
4066	Marketing	Bot correct
4067	Marketing	Bot correct
4071	Outil	Bot correct
4076	Marketing	Bot correct
4078	Crawler	Bot correct
4079	Crawler	Bot correct
4081	Moteur de recherche	Bot correct
4082	Outil	Bot correct
4085	Outil	Bot correct
4086	Outil	Bot correct
4090	Outil	Bot correct
4091	Outil	Bot correct
4092	Outil	Bot correct
4093	Outil	Bot correct
4094	Sans catégorie	Bot correct
4095	Moniteur de site	Bot correct
4096	Moniteur de site	Bot correct
4097	Moniteur de site	Bot correct
4098	Crawler	Bot correct
4099	Moteur de recherche	Bot correct
4100	Moteur de recherche	Bot correct
4101	Moteur de recherche	Bot correct
4102	Moteur de recherche	Bot correct
4103	Marketing	Bot correct
4104	Marketing	Bot correct
4105	Marketing	Bot correct
4106	Marketing	Bot correct
4107	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4108	Marketing	Bot correct
4109	Moteur de recherche	Bot correct
4110	Crawler	Bot correct
4111	Crawler	Bot correct
4112	Crawler	Bot correct
4113	Analyseur de vulnérabilité	Bot correct
4114	Crawler	Bot correct
4115	Outil	Bot correct
4120	Marketing	Bot correct
4121	Marketing	Bot correct
4122	Marketing	Bot correct
4123	Marketing	Bot correct
4124	Marketing	Bot correct
4125	Marketing	Bot correct
4126	Marketing	Bot correct
4127	Marketing	Bot correct
4128	Marketing	Bot correct
4129	Marketing	Bot correct
4130	Marketing	Bot correct
4131	Outil	Bot correct
4132	Marketing	Bot correct
4133	Marketing	Bot correct
4134	Outil	Bot correct
4135	Marketing	Bot correct
4136	Marketing	Bot correct
4137	Marketing	Bot correct
4138	Marketing	Bot correct
4139	Marketing	Bot correct
4140	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4141	Marketing	Bot correct
4142	Marketing	Bot correct
4143	Marketing	Bot correct
4144	Marketing	Bot correct
4147	Moteur de recherche	Bot correct
4148	Moteur de recherche	Bot correct
4149	Moteur de recherche	Bot correct
4150	Moteur de recherche	Bot correct
4151	Moteur de recherche	Bot correct
4152	Moteur de recherche	Bot correct
4153	Moteur de recherche	Bot correct
4154	Moteur de recherche	Bot correct
4155	Moteur de recherche	Bot correct
4156	Créateur de capture d’écran	Bot correct
4157	Moteur de recherche	Bot correct
4158	Moteur de recherche	Bot correct
4159	Moteur de recherche	Bot correct
4160	Créateur de capture d’écran	Bot correct
4161	Moteur de recherche	Bot correct
4162	Moteur de recherche	Bot correct
4163	Outil	Bot correct
4164	Moteur de recherche	Bot correct
4168	Tester de vitesse	Bot correct
4170	Outil	Bot correct
4172	Crawler	Bot correct
4173	Outil	Bot correct
4174	Crawler	Bot correct
4175	Crawler	Bot correct
4176	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4177	Moteur de recherche	Bot correct
4178	Outil	Bot correct
4179	Crawler	Bot correct
4180	Outil	Bot correct
4181	Moniteur de site	Bot correct
4182	Moniteur de site	Bot correct
4183	Moniteur de site	Bot correct
4184	Moniteur de site	Bot correct
4185	Moteur de recherche	Bot correct
4186	Outil	Bot correct
4187	Outil	Bot correct
4190	Moteur de recherche	Bot correct
4191	Moteur de recherche	Bot correct
4192	Moteur de recherche	Bot correct
4193	Moteur de recherche	Bot correct
4194	Outil	Bot correct
4196	Outil	Bot correct
4197	Outil	Bot correct
4198	Marketing	Bot correct
4199	Marketing	Bot correct
4200	Analyseur de vulnérabilité	Bot correct
4201	Outil	Bot correct
4202	Outil	Bot correct
4205	Moteur de recherche	Bot correct
4206	Marketing	Bot correct
4207	Marketing	Bot correct
4208	Moteur de recherche	Bot correct
4209	Moteur de recherche	Bot correct
4210	Tester de vitesse	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4211	Outil	Bot correct
4212	Feed Fetcher	Bot correct
4213	Feed Fetcher	Bot correct
4215	Outil	Bot correct
4216	Outil	Bot correct
4219	Marketing	Bot correct
4220	Outil	Bot correct
4222	Moniteur de site	Bot correct
4223	Marketing	Bot correct
4224	Moteur de recherche	Bot correct
4225	Moteur de recherche	Bot correct
4226	Moteur de recherche	Bot correct
4227	Marketing	Bot correct
4228	Marketing	Bot correct
4229	Outil	Bot correct
4231	Créateur de capture d’écran	Bot correct
4232	Outil	Bot correct
4233	Moniteur de site	Bot correct
4234	Moniteur de site	Bot correct
4235	Moniteur de site	Bot correct
4236	Moniteur de site	Bot correct
4237	Moniteur de site	Bot correct
4238	Moniteur de site	Bot correct
4240	Marketing	Bot correct
4241	Marketing	Bot correct
4242	Marketing	Bot correct
4243	Marketing	Bot correct
4244	Marketing	Bot correct
4245	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4246	Marketing	Bot correct
4247	Moteur de recherche	Bot correct
4248	Moteur de recherche	Bot correct
4249	Créateur de capture d'écran	Bot correct
4250	Moteur de recherche	Bot correct
4251	Moteur de recherche	Bot correct
4252	Crawler	Bot correct
4253	Crawler	Bot correct
4254	Crawler	Bot correct
4255	Outil	Bot correct
4256	Sans catégorie	Bot correct
4257	Outil	Bot correct
4258	Crawler	Bot correct
4259	Crawler	Bot correct
4260	Outil	Bot correct
4261	Outil	Bot correct
4262	Outil	Bot correct
4265	Moteur de recherche	Bot correct
4266	Sans catégorie	Bot correct
4267	Outil	Bot correct
4268	Outil	Bot correct
4269	Moteur de recherche	Bot correct
4270	Moteur de recherche	Bot correct
4271	Moteur de recherche	Bot correct
4272	Moteur de recherche	Bot correct
4273	Moteur de recherche	Bot correct
4274	Moteur de recherche	Bot correct
4275	Moteur de recherche	Bot correct
4279	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4280	Crawler	Bot correct
4282	Marketing	Bot correct
4283	Marketing	Bot correct
4284	Marketing	Bot correct
4285	Marketing	Bot correct
4286	Marketing	Bot correct
4287	Marketing	Bot correct
4288	Marketing	Bot correct
4289	Marketing	Bot correct
4290	Marketing	Bot correct
4291	Marketing	Bot correct
4292	Marketing	Bot correct
4293	Marketing	Bot correct
4294	Marketing	Bot correct
4295	Moteur de recherche	Bot correct
4296	Moteur de recherche	Bot correct
4297	Moteur de recherche	Bot correct
4298	Moteur de recherche	Bot correct
4299	Moteur de recherche	Bot correct
4300	Moteur de recherche	Bot correct
4301	Moteur de recherche	Bot correct
4302	Moteur de recherche	Bot correct
4303	Moteur de recherche	Bot correct
4304	Moteur de recherche	Bot correct
4305	Moteur de recherche	Bot correct
4306	Créateur de capture d’écran	Bot correct
4307	Moteur de recherche	Bot correct
4308	Moteur de recherche	Bot correct
4309	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4310	Moteur de recherche	Bot correct
4311	Créateur de capture d'écran	Bot correct
4312	Moteur de recherche	Bot correct
4313	Moteur de recherche	Bot correct
4314	Moteur de recherche	Bot correct
4315	Moteur de recherche	Bot correct
4316	Moteur de recherche	Bot correct
4317	Moteur de recherche	Bot correct
4318	Créateur de capture d'écran	Bot correct
4319	Créateur de capture d'écran	Bot correct
4321	Sans catégorie	Bot correct
4322	Crawler	Bot correct
4323	Outil	Bot correct
4324	Outil	Bot correct
4325	Outil	Bot correct
4328	Marketing	Bot correct
4330	Moniteur de site	Bot correct
4331	Moteur de recherche	Bot correct
4332	Moteur de recherche	Bot correct
4335	Marketing	Bot correct
4336	Marketing	Bot correct
4337	Outil	Bot correct
4338	Outil	Bot correct
4339	Outil	Bot correct
4340	Crawler	Bot correct
4341	Crawler	Bot correct
4342	Analyseur de vulnérabilité	Bot correct
4343	Analyseur de vulnérabilité	Bot correct
4344	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4345	Marketing	Bot correct
4346	Marketing	Bot correct
4347	Marketing	Bot correct
4348	Marketing	Bot correct
4349	Marketing	Bot correct
4350	Marketing	Bot correct
4351	Marketing	Bot correct
4352	Marketing	Bot correct
4353	Marketing	Bot correct
4354	Marketing	Bot correct
4355	Moteur de recherche	Bot correct
4356	Moteur de recherche	Bot correct
4357	Moteur de recherche	Bot correct
4358	Moteur de recherche	Bot correct
4359	Moteur de recherche	Bot correct
4360	Moteur de recherche	Bot correct
4361	Moteur de recherche	Bot correct
4362	Moteur de recherche	Bot correct
4363	Moteur de recherche	Bot correct
4364	Moteur de recherche	Bot correct
4365	Créateur de capture d’écran	Bot correct
4366	Moteur de recherche	Bot correct
4367	Moteur de recherche	Bot correct
4368	Moteur de recherche	Bot correct
4369	Moteur de recherche	Bot correct
4370	Créateur de capture d’écran	Bot correct
4371	Moteur de recherche	Bot correct
4372	Moteur de recherche	Bot correct
4373	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4374	Moteur de recherche	Bot correct
4375	Moteur de recherche	Bot correct
4376	Créateur de capture d'écran	Bot correct
4377	Crawler	Bot correct
4378	Crawler	Bot correct
4379	Moteur de recherche	Bot correct
4380	Moteur de recherche	Bot correct
4381	Moteur de recherche	Bot correct
4382	Moteur de recherche	Bot correct
4383	Crawler	Bot correct
4384	Moteur de recherche	Bot correct
4385	Outil	Bot correct
4386	Sans catégorie	Bot correct
4387	Crawler	Bot correct
4388	Crawler	Bot correct
4389	Outil	Bot correct
4390	Outil	Bot correct
4391	Outil	Bot correct
4392	Outil	Bot correct
4393	Outil	Bot correct
4394	Sans catégorie	Bot correct
4395	Outil	Bot correct
4396	Moniteur de site	Bot correct
4397	Moniteur de site	Bot correct
4404	Moteur de recherche	Bot correct
4405	Moteur de recherche	Bot correct
4406	Moteur de recherche	Bot correct
4407	Sans catégorie	Bot correct

Mise à jour de la signature des robots pour octobre 2021

May 5, 2023

De nouvelles signatures ont été ajoutées et certaines signatures de robots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

Signature version 10 applicable aux plateformes NetScaler NetScaler dotées de versions 13.0 76.31 ou ultérieures.

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
71	Crawler	Bot correct
74	Crawler	Bot correct
75	Crawler	Bot correct
372	Scraper	Bot correct
373	Scraper	Bot correct
374	Scraper	Bot correct
375	Scraper	Bot correct
376	Scraper	Bot correct
377	Scraper	Bot correct
378	Scraper	Bot correct
379	Scraper	Bot correct
380	Scraper	Bot correct
381	Scraper	Bot correct
382	Scraper	Bot correct
383	Scraper	Bot correct
384	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
385	Scraper	Bot correct
386	Scraper	Bot correct
387	Scraper	Bot correct
389	Scraper	Bot correct
390	Scraper	Bot correct
391	Scraper	Bot correct
639	Moteur de recherche	Bot correct
702	Moteur de recherche	Bot correct
703	Moteur de recherche	Bot correct
1173	Outil	Bot correct
1174	Marketing	Bot correct
1176	Moteur de recherche	Bot correct
1178	Tester de vitesse	Bot correct
1185	Créateur de capture d’écran	Bot correct
1209	Sans catégorie	Bot correct
1531	Feed Fetcher	Bot correct
2586	Sans catégorie	Bot correct
2674	Outil	Bot correct
2756	Outil	Bot correct
2758	Sans catégorie	Bot correct
2759	Outil	Bot correct
2784	Outil	Bot correct
2952	Outil	Bot correct
3163	Outil	Bot correct
3554	Outil	Bot correct
3782	Marketing	Bot correct
3788	Outil	Bot correct
3789	Outil	Bot correct
3797	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3798	Marketing	Bot correct
3799	Marketing	Bot correct
3800	Marketing	Bot correct
3801	Marketing	Bot correct
3802	Créateur de capture d'écran	Bot correct
3803	Moteur de recherche	Bot correct
3804	Créateur de capture d'écran	Bot correct
3805	Moteur de recherche	Bot correct
3861	Marketing	Bot correct
3862	Marketing	Bot correct
3863	Marketing	Bot correct
3864	Marketing	Bot correct
3865	Marketing	Bot correct
3866	Marketing	Bot correct
3867	Marketing	Bot correct
3868	Marketing	Bot correct
3869	Outil	Bot correct
3871	Marketing	Bot correct
3872	Marketing	Bot correct
3873	Moteur de recherche	Bot correct
3874	Moteur de recherche	Bot correct
3875	Moteur de recherche	Bot correct
3876	Moteur de recherche	Bot correct
3877	Créateur de capture d'écran	Bot correct
3878	Moteur de recherche	Bot correct
3879	Moteur de recherche	Bot correct
3880	Créateur de capture d'écran	Bot correct
3881	Créateur de capture d'écran	Bot correct
3882	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3883	Moteur de recherche	Bot correct
3884	Moteur de recherche	Bot correct
3885	Moteur de recherche	Bot correct
3963	Marketing	Bot correct
4040	Crawler	Bot correct
4041	Outil	Bot correct
4120	Marketing	Bot correct
4122	Marketing	Bot correct
4123	Marketing	Bot correct
4124	Marketing	Bot correct
4125	Marketing	Bot correct
4133	Marketing	Bot correct
4134	Outil	Bot correct
4135	Marketing	Bot correct
4136	Marketing	Bot correct
4137	Marketing	Bot correct
4138	Marketing	Bot correct
4139	Marketing	Bot correct
4140	Marketing	Bot correct
4141	Marketing	Bot correct
4142	Marketing	Bot correct
4143	Marketing	Bot correct
4144	Marketing	Bot correct
4145	Moteur de recherche	Bot correct
4146	Moteur de recherche	Bot correct
4147	Moteur de recherche	Bot correct
4148	Moteur de recherche	Bot correct
4149	Moteur de recherche	Bot correct
4150	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4151	Moteur de recherche	Bot correct
4152	Moteur de recherche	Bot correct
4153	Moteur de recherche	Bot correct
4154	Moteur de recherche	Bot correct
4155	Moteur de recherche	Bot correct
4156	Créateur de capture d'écran	Bot correct
4157	Moteur de recherche	Bot correct
4158	Moteur de recherche	Bot correct
4159	Moteur de recherche	Bot correct
4160	Créateur de capture d'écran	Bot correct
4161	Moteur de recherche	Bot correct
4162	Moteur de recherche	Bot correct
4163	Outil	Bot correct
4164	Moteur de recherche	Bot correct
4209	Moteur de recherche	Bot correct
4240	Marketing	Bot correct
4241	Marketing	Bot correct
4248	Moteur de recherche	Bot correct
4249	Créateur de capture d'écran	Bot correct
4250	Moteur de recherche	Bot correct
4251	Moteur de recherche	Bot correct
4282	Marketing	Bot correct
4283	Marketing	Bot correct
4284	Marketing	Bot correct
4285	Marketing	Bot correct
4286	Marketing	Bot correct
4287	Marketing	Bot correct
4288	Marketing	Bot correct
4289	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4290	Marketing	Bot correct
4291	Marketing	Bot correct
4292	Marketing	Bot correct
4293	Marketing	Bot correct
4294	Marketing	Bot correct
4295	Moteur de recherche	Bot correct
4296	Moteur de recherche	Bot correct
4297	Moteur de recherche	Bot correct
4298	Moteur de recherche	Bot correct
4299	Moteur de recherche	Bot correct
4300	Moteur de recherche	Bot correct
4301	Moteur de recherche	Bot correct
4302	Moteur de recherche	Bot correct
4303	Moteur de recherche	Bot correct
4304	Moteur de recherche	Bot correct
4305	Moteur de recherche	Bot correct
4306	Créateur de capture d’écran	Bot correct
4307	Moteur de recherche	Bot correct
4308	Moteur de recherche	Bot correct
4309	Moteur de recherche	Bot correct
4310	Moteur de recherche	Bot correct
4311	Créateur de capture d’écran	Bot correct
4312	Moteur de recherche	Bot correct
4313	Moteur de recherche	Bot correct
4314	Moteur de recherche	Bot correct
4315	Moteur de recherche	Bot correct
4316	Moteur de recherche	Bot correct
4317	Moteur de recherche	Bot correct
4318	Créateur de capture d’écran	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4319	Créateur de capture d’écran	Bot correct
4337	Outil	Bot correct
4338	Outil	Bot correct
4345	Marketing	Bot correct
4346	Marketing	Bot correct
4347	Marketing	Bot correct
4348	Marketing	Bot correct
4349	Marketing	Bot correct
4350	Marketing	Bot correct
4351	Marketing	Bot correct
4352	Marketing	Bot correct
4353	Marketing	Bot correct
4354	Marketing	Bot correct
4355	Moteur de recherche	Bot correct
4356	Moteur de recherche	Bot correct
4357	Moteur de recherche	Bot correct
4358	Moteur de recherche	Bot correct
4359	Moteur de recherche	Bot correct
4360	Moteur de recherche	Bot correct
4361	Moteur de recherche	Bot correct
4362	Moteur de recherche	Bot correct
4363	Moteur de recherche	Bot correct
4364	Moteur de recherche	Bot correct
4365	Créateur de capture d’écran	Bot correct
4366	Moteur de recherche	Bot correct
4367	Moteur de recherche	Bot correct
4368	Moteur de recherche	Bot correct
4369	Moteur de recherche	Bot correct
4370	Créateur de capture d’écran	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4371	Moteur de recherche	Bot correct
4372	Moteur de recherche	Bot correct
4373	Moteur de recherche	Bot correct
4374	Moteur de recherche	Bot correct
4375	Moteur de recherche	Bot correct
4376	Créateur de capture d'écran	Bot correct

Mise à jour de la signature du bot pour novembre 2021

May 5, 2023

De nouvelles signatures ont été ajoutées et certaines signatures de robots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

Signature version 11 applicable aux plateformes NetScaler NetScaler dotées de versions 13.0 76.31 ou ultérieures.

Nouvelles signatures de robots

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
4408	Scraper	Bot correct
4409	Crawler	Bot incorrect
4411	Marketing	Bot correct
4412	Marketing	Bot correct
4413	Marketing	Bot correct
4421	Créateur de capture d'écran	Bot correct
4422	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4423	Outil	Bot incorrect
4424	Moniteur de site	Bot correct
4425	Marketing	Bot correct
4426	Crawler	Bot incorrect
4427	Scraper	Bot correct
4428	Scraper	Bot correct
4429	Créateur de capture d’écran	Bot correct
4430	Analyseur de virus	Bot correct
4431	Moniteur de site	Bot correct
4432	Outil	Bot correct
4433	Moteur de recherche	Bot correct
4434	Moteur de recherche	Bot correct
4435	Moteur de recherche	Bot correct
4436	Marketing	Bot correct
4437	Marketing	Bot correct
4438	Scraper	Bot correct
4439	Scraper	Bot correct
4440	Scraper	Bot correct
4441	Feed Fetcher	Bot correct
4442	Marketing	Bot correct
4443	Scraper	Bot correct
4445	Sans catégorie	Bot incorrect
4446	Scraper	Bot correct
4450	Créateur de capture d’écran	Bot correct
4451	Tester de vitesse	Bot correct
4452	Moteur de recherche	Bot correct
4466	Sans catégorie	Bot correct
4467	Créateur de capture d’écran	Bot correct
4468	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4469	Sans catégorie	Bot correct
4470	Outil	Bot correct
4472	Scraper	Bot correct
4473	Sans catégorie	Bot correct
4474	Marketing	Bot correct
4476	Crawler	Bot correct
4477	Crawler	Bot correct
4478	Crawler	Bot correct
4479	Crawler	Bot correct
4480	Crawler	Bot correct
4481	Crawler	Bot correct
4482	Crawler	Bot correct
4483	Crawler	Bot correct
4484	Crawler	Bot correct
4485	Crawler	Bot correct
4486	Scraper	Bot correct
4487	Scraper	Bot correct
4488	Scraper	Bot correct
4489	Moteur de recherche	Bot correct
4491	Outil	Bot correct
4492	Sans catégorie	Bot incorrect
4493	Crawler	Bot correct
4494	Outil	Bot correct
4496	Outil	Bot correct
4497	Crawler	Bot correct
4498	Sans catégorie	Bot incorrect
4499	Sans catégorie	Bot incorrect
4501	Marketing	Bot correct
4502	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4503	Marketing	Bot correct
4508	Sans catégorie	Bot correct
4509	Sans catégorie	Bot correct
4510	Sans catégorie	Bot correct
4511	Sans catégorie	Bot correct
4512	Outil	Bot correct
4513	Outil	Bot correct
4514	Outil	Bot correct
4515	Outil	Bot correct
4516	Sans catégorie	Bot correct
4518	Scraper	Bot incorrect
4519	Créateur de capture d’écran	Bot correct
4520	Marketing	Bot correct
4521	Sans catégorie	Bot correct
4522	Outil	Bot correct
4523	Sans catégorie	Bot incorrect
4524	Sans catégorie	Bot incorrect
4525	Crawler	Bot correct
4526	Crawler	Bot correct
4527	Crawler	Bot correct
4528	Crawler	Bot correct
4529	Crawler	Bot correct
4530	Sans catégorie	Bot incorrect
4531	Marketing	Bot correct
4532	Marketing	Bot correct
4533	Marketing	Bot correct
4534	Marketing	Bot correct
4535	Marketing	Bot correct
4541	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4552	Sans catégorie	Bot correct
4553	Outil	Bot incorrect
4554	Outil	Bot incorrect
4555	Outil	Bot correct
4556	Outil	Bot correct
4558	Scraper	Bot correct
4559	Crawler	Bot correct
4560	Crawler	Bot correct
4561	Moniteur de site	Bot correct
4562	Moteur de recherche	Bot correct
4563	Moteur de recherche	Bot correct
1000000	Navigateur	Bot correct
1000001	Scraper	Bot incorrect
1000002	Application	Bot incorrect
1000003	Navigateur	Bot correct
1000004	Scraper	Bot correct
1000005	Scraper	Bot correct
1000006	Crawler	Bot incorrect
1000007	Navigateur	Bot incorrect
1000008	Sans catégorie	Bot incorrect
1000009	Navigateur	Bot correct
1000010	Scraper	Bot incorrect
1000011	Navigateur	Bot incorrect
1000012	Navigateur	Bot correct
1000013	Navigateur	Bot incorrect
1000014	Scraper	Bot correct
1000015	Scraper	Bot incorrect
1000016	Scraper	Bot incorrect
1000017	Navigateur	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
1000018	Navigateur	Bot incorrect
1000019	Sans catégorie	Bot incorrect
1000020	Scraper	Bot correct
1000021	Navigateur	Bot incorrect
1000022	Scraper	Bot correct
1000023	Scraper	Bot correct
1000024	Crawler	Bot correct
1000025	Navigateur	Bot incorrect
1000026	Analyseur	Bot correct
1000027	Analyseur	Bot correct
1000028	Analyseur	Bot correct
1000029	Analyseur	Bot correct
1000030	Analyseur	Bot correct
1000031	Navigateur	Bot correct
1000032	Analyseur	Bot correct
1000033	Analyseur	Bot correct
1000034	Navigateur	Bot incorrect
1000035	Scraper	Bot correct
1000036	Scraper	Bot correct
1000037	Analyseur	Bot correct
1000038	Analyseur	Bot correct
1000039	Analyseur	Bot correct
1000040	Analyseur	Bot correct
1000041	Scraper	Bot correct
1000042	Analyseur	Bot correct
1000043	Analyseur	Bot correct
1000044	Crawler	Bot correct
1000045	Navigateur	Bot incorrect
1000046	Navigateur	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
1000047	Scraper	Bot correct
1000048	Navigateur	Bot incorrect
1000049	Analyseur	Bot correct
1000050	Navigateur	Bot incorrect
1000051	Navigateur	Bot correct
1000052	Navigateur	Bot incorrect
1000053	Scraper	Bot correct
1000054	Navigateur	Bot correct
1000055	Navigateur	Bot correct
1000056	Scraper	Bot incorrect
1000057	Crawler	Bot incorrect
1000058	Scraper	Bot incorrect
1000059	Analyseur	Bot correct
1000060	Navigateur	Bot incorrect
1000061	Navigateur	Bot incorrect
1000062	Navigateur	Bot incorrect
1000063	Scraper	Bot incorrect
1000064	Scraper	Bot incorrect
1000065	Scraper	Bot incorrect
1000066	Application	Bot incorrect
1000067	Scraper	Bot incorrect
1000068	Navigateur	Bot incorrect
1000069	Scraper	Bot incorrect
1000070	Scraper	Bot correct
1000071	Navigateur	Bot correct
1000072	Navigateur	Bot correct
1000073	Navigateur	Bot incorrect
1000074	Navigateur	Bot incorrect
1000075	Application	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
1000076	Scraper	Bot incorrect

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
2	Crawler	Bot correct
5	Crawler	Bot correct
9	Crawler	Bot correct
30	Crawler	Bot incorrect
45	Crawler	Bot correct
46	Crawler	Bot correct
48	Crawler	Bot correct
52	Crawler	Bot correct
60	Crawler	Bot correct
61	Crawler	Bot correct
63	Crawler	Bot correct
67	Crawler	Bot correct
76	Crawler	Bot correct
78	Crawler	Bot correct
79	Crawler	Bot correct
80	Crawler	Bot correct
81	Crawler	Bot correct
82	Crawler	Bot correct
83	Crawler	Bot correct
84	Crawler	Bot correct
87	Crawler	Bot correct
90	Crawler	Bot correct
95	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
96	Crawler	Bot correct
97	Crawler	Bot correct
100	Crawler	Bot correct
101	Crawler	Bot correct
102	Crawler	Bot correct
103	Crawler	Bot correct
104	Crawler	Bot correct
107	Crawler	Bot correct
108	Crawler	Bot correct
110	Crawler	Bot correct
111	Crawler	Bot correct
114	Crawler	Bot correct
115	Crawler	Bot correct
123	Crawler	Bot correct
135	Crawler	Bot correct
136	Crawler	Bot correct
137	Crawler	Bot correct
140	Crawler	Bot correct
141	Crawler	Bot correct
143	Crawler	Bot correct
144	Crawler	Bot correct
145	Crawler	Bot correct
146	Crawler	Bot correct
147	Crawler	Bot correct
149	Crawler	Bot correct
152	Crawler	Bot correct
155	Crawler	Bot correct
156	Crawler	Bot correct
157	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
158	Crawler	Bot correct
159	Crawler	Bot correct
160	Crawler	Bot correct
161	Crawler	Bot correct
162	Crawler	Bot correct
163	Crawler	Bot correct
164	Crawler	Bot correct
165	Crawler	Bot correct
166	Crawler	Bot correct
167	Crawler	Bot correct
172	Crawler	Bot correct
173	Crawler	Bot correct
174	Crawler	Bot correct
176	Crawler	Bot correct
177	Crawler	Bot correct
180	Crawler	Bot correct
182	Crawler	Bot correct
187	Crawler	Bot correct
197	Crawler	Bot correct
201	Crawler	Bot correct
202	Crawler	Bot correct
203	Crawler	Bot correct
206	Crawler	Bot correct
217	Feed Fetcher	Bot correct
219	Feed Fetcher	Bot correct
229	Scraper	Bot correct
235	Scraper	Bot correct
236	Scraper	Bot correct
237	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
248	Scraper	Bot correct
250	Scraper	Bot correct
252	Scraper	Bot correct
260	Scraper	Bot correct
263	Scraper	Bot correct
265	Scraper	Bot correct
267	Scraper	Bot correct
268	Scraper	Bot correct
271	Scraper	Bot correct
272	Scraper	Bot correct
276	Scraper	Bot correct
277	Scraper	Bot correct
278	Scraper	Bot correct
279	Scraper	Bot correct
280	Scraper	Bot correct
281	Scraper	Bot correct
283	Scraper	Bot correct
285	Scraper	Bot correct
286	Scraper	Bot correct
287	Scraper	Bot correct
290	Scraper	Bot correct
292	Scraper	Bot correct
293	Scraper	Bot correct
338	Scraper	Bot correct
342	Scraper	Bot correct
343	Scraper	Bot correct
344	Scraper	Bot correct
351	Scraper	Bot correct
352	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
353	Scraper	Bot correct
355	Scraper	Bot correct
357	Scraper	Bot correct
360	Scraper	Bot correct
362	Scraper	Bot correct
366	Scraper	Bot correct
370	Scraper	Bot correct
371	Scraper	Bot correct
392	Scraper	Bot correct
393	Scraper	Bot correct
394	Scraper	Bot correct
396	Scraper	Bot correct
397	Scraper	Bot correct
414	Scraper	Bot correct
418	Scraper	Bot correct
419	Scraper	Bot correct
421	Scraper	Bot correct
422	Scraper	Bot correct
423	Scraper	Bot correct
424	Scraper	Bot correct
425	Scraper	Bot correct
426	Scraper	Bot correct
427	Scraper	Bot correct
428	Scraper	Bot correct
430	Scraper	Bot correct
432	Scraper	Bot correct
433	Scraper	Bot correct
434	Scraper	Bot correct
435	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
441	Scraper	Bot correct
445	Scraper	Bot correct
446	Scraper	Bot correct
451	Scraper	Bot correct
452	Scraper	Bot correct
454	Scraper	Bot correct
455	Scraper	Bot correct
456	Scraper	Bot correct
457	Scraper	Bot correct
458	Scraper	Bot correct
461	Scraper	Bot correct
465	Scraper	Bot correct
466	Scraper	Bot correct
469	Scraper	Bot correct
473	Scraper	Bot correct
474	Scraper	Bot correct
476	Scraper	Bot correct
477	Scraper	Bot correct
484	Scraper	Bot correct
485	Scraper	Bot correct
487	Scraper	Bot correct
488	Scraper	Bot correct
489	Scraper	Bot correct
490	Scraper	Bot correct
493	Scraper	Bot correct
494	Scraper	Bot correct
495	Scraper	Bot correct
497	Scraper	Bot correct
498	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
499	Scraper	Bot correct
500	Scraper	Bot correct
505	Scraper	Bot correct
506	Scraper	Bot correct
507	Scraper	Bot correct
512	Scraper	Bot correct
513	Scraper	Bot correct
514	Scraper	Bot correct
527	Scraper	Bot correct
533	Scraper	Bot correct
539	Scraper	Bot correct
540	Scraper	Bot correct
542	Scraper	Bot correct
544	Scraper	Bot correct
545	Scraper	Bot correct
546	Scraper	Bot correct
547	Scraper	Bot correct
548	Scraper	Bot correct
551	Scraper	Bot correct
552	Scraper	Bot correct
554	Scraper	Bot correct
556	Scraper	Bot correct
558	Scraper	Bot correct
560	Scraper	Bot correct
561	Scraper	Bot correct
566	Scraper	Bot correct
575	Scraper	Bot correct
578	Scraper	Bot correct
581	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
582	Scraper	Bot correct
591	Scraper	Bot correct
593	Scraper	Bot correct
595	Scraper	Bot correct
600	Scraper	Bot correct
601	Scraper	Bot correct
602	Scraper	Bot correct
604	Scraper	Bot correct
605	Scraper	Bot correct
609	Scraper	Bot correct
610	Scraper	Bot correct
611	Scraper	Bot correct
612	Scraper	Bot correct
613	Scraper	Bot correct
615	Scraper	Bot correct
620	Moteur de recherche	Bot correct
622	Moteur de recherche	Bot correct
623	Moteur de recherche	Bot correct
624	Moteur de recherche	Bot correct
626	Moteur de recherche	Bot correct
627	Moteur de recherche	Bot correct
628	Moteur de recherche	Bot correct
629	Moteur de recherche	Bot correct
633	Moteur de recherche	Bot correct
634	Moteur de recherche	Bot correct
636	Moteur de recherche	Bot correct
637	Moteur de recherche	Bot correct
640	Moteur de recherche	Bot correct
641	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
642	Moteur de recherche	Bot correct
643	Moteur de recherche	Bot correct
647	Moteur de recherche	Bot correct
649	Moteur de recherche	Bot correct
650	Moteur de recherche	Bot correct
651	Moteur de recherche	Bot correct
654	Moteur de recherche	Bot correct
656	Moteur de recherche	Bot correct
657	Moteur de recherche	Bot correct
658	Moteur de recherche	Bot correct
659	Moteur de recherche	Bot correct
660	Moteur de recherche	Bot correct
663	Moteur de recherche	Bot correct
664	Moteur de recherche	Bot correct
665	Moteur de recherche	Bot correct
666	Moteur de recherche	Bot correct
667	Moteur de recherche	Bot correct
669	Moteur de recherche	Bot correct
670	Moteur de recherche	Bot correct
671	Moteur de recherche	Bot correct
672	Moteur de recherche	Bot correct
673	Moteur de recherche	Bot correct
674	Moteur de recherche	Bot correct
675	Moteur de recherche	Bot correct
676	Moteur de recherche	Bot correct
677	Moteur de recherche	Bot correct
679	Moteur de recherche	Bot correct
680	Moteur de recherche	Bot correct
690	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
693	Moteur de recherche	Bot correct
694	Moteur de recherche	Bot correct
697	Moteur de recherche	Bot correct
698	Moteur de recherche	Bot correct
702	Moteur de recherche	Bot correct
706	Moteur de recherche	Bot correct
712	Moteur de recherche	Bot correct
713	Moteur de recherche	Bot correct
714	Moteur de recherche	Bot correct
715	Moteur de recherche	Bot correct
716	Moteur de recherche	Bot correct
721	Moteur de recherche	Bot correct
723	Moteur de recherche	Bot correct
725	Moteur de recherche	Bot correct
727	Moteur de recherche	Bot correct
728	Moteur de recherche	Bot correct
729	Moteur de recherche	Bot correct
730	Moteur de recherche	Bot correct
731	Moteur de recherche	Bot correct
732	Moteur de recherche	Bot correct
735	Moteur de recherche	Bot correct
736	Moteur de recherche	Bot correct
740	Moteur de recherche	Bot correct
748	Moteur de recherche	Bot correct
749	Moteur de recherche	Bot correct
750	Moteur de recherche	Bot correct
751	Moteur de recherche	Bot correct
756	Moteur de recherche	Bot correct
757	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
758	Moteur de recherche	Bot correct
759	Moteur de recherche	Bot correct
760	Moteur de recherche	Bot correct
761	Moteur de recherche	Bot correct
762	Moteur de recherche	Bot correct
763	Moteur de recherche	Bot correct
764	Moteur de recherche	Bot correct
765	Moteur de recherche	Bot correct
766	Moteur de recherche	Bot correct
767	Moteur de recherche	Bot correct
768	Moteur de recherche	Bot correct
769	Moteur de recherche	Bot correct
770	Moteur de recherche	Bot correct
771	Moteur de recherche	Bot correct
772	Moteur de recherche	Bot correct
773	Moteur de recherche	Bot correct
776	Moteur de recherche	Bot correct
777	Moteur de recherche	Bot correct
780	Moteur de recherche	Bot correct
781	Moteur de recherche	Bot correct
784	Moteur de recherche	Bot correct
786	Moteur de recherche	Bot correct
787	Moteur de recherche	Bot correct
788	Moteur de recherche	Bot correct
789	Moteur de recherche	Bot correct
790	Moteur de recherche	Bot correct
791	Moteur de recherche	Bot correct
792	Moteur de recherche	Bot correct
795	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
796	Moteur de recherche	Bot correct
798	Moteur de recherche	Bot correct
800	Moteur de recherche	Bot correct
801	Moteur de recherche	Bot correct
802	Moteur de recherche	Bot correct
803	Moteur de recherche	Bot correct
805	Moteur de recherche	Bot correct
806	Moteur de recherche	Bot correct
807	Moteur de recherche	Bot correct
809	Moteur de recherche	Bot correct
810	Moteur de recherche	Bot correct
811	Moteur de recherche	Bot correct
812	Moteur de recherche	Bot correct
814	Moteur de recherche	Bot correct
815	Moteur de recherche	Bot correct
816	Moteur de recherche	Bot correct
817	Moteur de recherche	Bot correct
818	Moteur de recherche	Bot correct
819	Moteur de recherche	Bot correct
820	Moteur de recherche	Bot correct
821	Moteur de recherche	Bot correct
822	Moteur de recherche	Bot correct
823	Moteur de recherche	Bot correct
825	Moteur de recherche	Bot correct
827	Moteur de recherche	Bot correct
830	Moteur de recherche	Bot correct
831	Moteur de recherche	Bot correct
834	Moteur de recherche	Bot correct
837	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
838	Moteur de recherche	Bot correct
849	Moniteur de site	Bot correct
850	Moniteur de site	Bot correct
851	Moniteur de site	Bot correct
853	Moniteur de site	Bot correct
857	Moniteur de site	Bot correct
858	Moniteur de site	Bot correct
859	Moniteur de site	Bot correct
860	Moniteur de site	Bot correct
861	Moniteur de site	Bot correct
862	Moniteur de site	Bot correct
863	Moniteur de site	Bot correct
864	Moniteur de site	Bot correct
865	Moniteur de site	Bot correct
866	Moniteur de site	Bot correct
867	Moniteur de site	Bot correct
868	Moniteur de site	Bot correct
869	Moniteur de site	Bot correct
870	Moniteur de site	Bot correct
871	Moniteur de site	Bot correct
872	Moniteur de site	Bot correct
873	Moniteur de site	Bot correct
874	Moniteur de site	Bot correct
875	Moniteur de site	Bot correct
876	Moniteur de site	Bot correct
877	Moniteur de site	Bot correct
880	Moniteur de site	Bot correct
881	Moniteur de site	Bot correct
883	Moniteur de site	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
885	Moniteur de site	Bot correct
886	Moniteur de site	Bot correct
888	Moniteur de site	Bot correct
889	Moniteur de site	Bot correct
895	Moniteur de site	Bot correct
896	Moniteur de site	Bot correct
897	Moniteur de site	Bot correct
898	Moniteur de site	Bot correct
900	Moniteur de site	Bot correct
901	Moniteur de site	Bot correct
904	Moniteur de site	Bot correct
906	Moniteur de site	Bot correct
908	Moniteur de site	Bot correct
909	Moniteur de site	Bot correct
910	Moniteur de site	Bot correct
911	Moniteur de site	Bot correct
912	Moniteur de site	Bot correct
913	Moniteur de site	Bot correct
917	Moniteur de site	Bot correct
918	Moniteur de site	Bot correct
919	Moniteur de site	Bot correct
920	Moniteur de site	Bot correct
921	Moniteur de site	Bot correct
924	Moniteur de site	Bot correct
926	Moniteur de site	Bot correct
927	Moniteur de site	Bot correct
928	Moniteur de site	Bot correct
929	Moniteur de site	Bot correct
930	Moniteur de site	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
931	Moniteur de site	Bot correct
934	Moniteur de site	Bot correct
938	Moniteur de site	Bot correct
939	Moniteur de site	Bot correct
958	Moniteur de site	Bot correct
959	Moniteur de site	Bot correct
960	Moniteur de site	Bot correct
963	Moniteur de site	Bot correct
984	Scraper	Bot correct
991	Scraper	Bot incorrect
996	Scraper	Bot correct
997	Scraper	Bot correct
998	Scraper	Bot correct
1002	Scraper	Bot correct
1006	Scraper	Bot correct
1622	Créateur de capture d’écran	Bot correct
2810	Crawler	Bot correct
3432	Sans catégorie	Bot incorrect
3783	Moteur de recherche	Bot correct
3784	Scraper	Bot incorrect
3788	Outil	Bot correct
3790	Crawler	Bot correct
3791	Tester de vitesse	Bot correct
3792	Outil	Bot correct
3793	Outil	Bot correct
3794	Crawler	Bot correct
3796	Scraper	Bot correct
3797	Marketing	Bot correct
3799	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3800	Marketing	Bot correct
3806	Outil	Bot correct
3807	Crawler	Bot correct
3808	Crawler	Bot correct
3809	Outil	Bot correct
3810	Scraper	Bot correct
3811	Outil	Bot correct
3812	Crawler	Bot correct
3813	Outil	Bot correct
3814	Crawler	Bot correct
3815	Sans catégorie	Bot correct
3817	Outil	Bot correct
3818	Outil	Bot correct
3819	Outil	Bot correct
3820	Crawler	Bot correct
3821	Moteur de recherche	Bot correct
3822	Marketing	Bot correct
3823	Sans catégorie	Bot correct
3831	Scraper	Bot correct
3833	Moteur de recherche	Bot correct
3834	Moteur de recherche	Bot correct
3835	Moteur de recherche	Bot correct
3836	Sans catégorie	Bot correct
3838	Sans catégorie	Bot correct
3839	Marketing	Bot correct
3840	Crawler	Bot correct
3842	Crawler	Bot correct
3843	Crawler	Bot correct
3844	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3845	Marketing	Bot correct
3846	Marketing	Bot correct
3847	Marketing	Bot correct
3848	Sans catégorie	Bot correct
3849	Crawler	Bot correct
3850	Outil	Bot correct
3851	Sans catégorie	Bot correct
3852	Outil	Bot correct
3853	Analyseur de vulnérabilité	Bot correct
3854	Crawler	Bot correct
3855	Crawler	Bot correct
3856	Outil	Bot correct
3871	Marketing	Bot correct
3886	Outil	Bot correct
3887	Crawler	Bot correct
3888	Crawler	Bot correct
3889	Sans catégorie	Bot correct
3890	Marketing	Bot correct
3893	Crawler	Bot correct
3894	Outil	Bot correct
3895	Outil	Bot correct
3896	Moteur de recherche	Bot correct
3897	Outil	Bot correct
3898	Outil	Bot correct
3899	Sans catégorie	Bot correct
3901	Crawler	Bot correct
3902	Outil	Bot correct
3903	Outil	Bot correct
3904	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3905	Moteur de recherche	Bot correct
3906	Moteur de recherche	Bot correct
3907	Moteur de recherche	Bot correct
3912	Crawler	Bot correct
3917	Sans catégorie	Bot correct
3918	Crawler	Bot correct
3919	Sans catégorie	Bot correct
3920	Sans catégorie	Bot correct
3921	Sans catégorie	Bot correct
3922	Sans catégorie	Bot correct
3923	Sans catégorie	Bot correct
3924	Sans catégorie	Bot correct
3925	Sans catégorie	Bot correct
3926	Marketing	Bot correct
3927	Marketing	Bot correct
3928	Marketing	Bot correct
3929	Outil	Bot correct
3930	Marketing	Bot correct
3931	Sans catégorie	Bot correct
3932	Crawler	Bot correct
3933	Marketing	Bot correct
3934	Marketing	Bot correct
3935	Scraper	Bot correct
3936	Marketing	Bot correct
3937	Scraper	Bot correct
3938	Feed Fetcher	Bot correct
3940	Moteur de recherche	Bot correct
3941	Crawler	Bot correct
3942	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3946	Feed Fetcher	Bot correct
3947	Crawler	Bot correct
3950	Analyseur de virus	Bot correct
3951	Marketing	Bot correct
3952	Marketing	Bot correct
3953	Marketing	Bot correct
3954	Marketing	Bot correct
3955	Marketing	Bot correct
3956	Marketing	Bot correct
3957	Marketing	Bot correct
3958	Marketing	Bot correct
3959	Marketing	Bot correct
3960	Marketing	Bot correct
3961	Marketing	Bot correct
3962	Marketing	Bot correct
3963	Marketing	Bot correct
3964	Marketing	Bot correct
3965	Marketing	Bot correct
3966	Marketing	Bot correct
3967	Marketing	Bot correct
3968	Marketing	Bot correct
3969	Marketing	Bot correct
3970	Moteur de recherche	Bot correct
3971	Créateur de capture d’écran	Bot correct
3972	Créateur de capture d’écran	Bot correct
3973	Moteur de recherche	Bot correct
3974	Moteur de recherche	Bot correct
3975	Moteur de recherche	Bot correct
3976	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
3977	Moteur de recherche	Bot correct
3978	Créateur de capture d'écran	Bot correct
3979	Moteur de recherche	Bot correct
3980	Créateur de capture d'écran	Bot correct
3981	Moteur de recherche	Bot correct
3982	Moteur de recherche	Bot correct
3983	Moteur de recherche	Bot correct
3984	Moteur de recherche	Bot correct
3985	Moteur de recherche	Bot correct
3986	Moteur de recherche	Bot correct
3987	Créateur de capture d'écran	Bot correct
3988	Moteur de recherche	Bot correct
3989	Moteur de recherche	Bot correct
3990	Moteur de recherche	Bot correct
3991	Moteur de recherche	Bot correct
3992	Moteur de recherche	Bot correct
3993	Moteur de recherche	Bot correct
3994	Moteur de recherche	Bot correct
3995	Moteur de recherche	Bot correct
3996	Moteur de recherche	Bot correct
3997	Moteur de recherche	Bot correct
3998	Moteur de recherche	Bot correct
3999	Moteur de recherche	Bot correct
4000	Créateur de capture d'écran	Bot correct
4001	Moteur de recherche	Bot correct
4002	Moteur de recherche	Bot correct
4003	Moteur de recherche	Bot correct
4004	Moteur de recherche	Bot correct
4005	Créateur de capture d'écran	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4006	Crawler	Bot correct
4007	Marketing	Bot correct
4008	Marketing	Bot correct
4011	Outil	Bot correct
4012	Crawler	Bot correct
4013	Moteur de recherche	Bot correct
4014	Outil	Bot correct
4015	Crawler	Bot correct
4016	Crawler	Bot correct
4017	Outil	Bot correct
4018	Outil	Bot correct
4019	Outil	Bot correct
4020	Outil	Bot correct
4021	Marketing	Bot correct
4024	Outil	Bot correct
4025	Moteur de recherche	Bot correct
4026	Moteur de recherche	Bot correct
4027	Moteur de recherche	Bot correct
4028	Marketing	Bot correct
4029	Outil	Bot correct
4030	Scraper	Bot correct
4031	Scraper	Bot correct
4033	Crawler	Bot correct
4034	Crawler	Bot correct
4035	Marketing	Bot correct
4036	Analyseur de vulnérabilité	Bot correct
4037	Analyseur de vulnérabilité	Bot correct
4038	Sans catégorie	Bot incorrect
4039	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4042	Crawler	Bot correct
4043	Créateur de capture d'écran	Bot correct
4048	Feed Fetcher	Bot correct
4050	Crawler	Bot correct
4051	Crawler	Bot correct
4052	Outil	Bot correct
4053	Outil	Bot correct
4055	Sans catégorie	Bot correct
4056	Marketing	Bot correct
4057	Créateur de capture d'écran	Bot correct
4058	Crawler	Bot correct
4060	Moteur de recherche	Bot correct
4061	Moteur de recherche	Bot correct
4062	Moteur de recherche	Bot correct
4063	Moteur de recherche	Bot correct
4064	Outil	Bot correct
4065	Scraper	Bot correct
4066	Marketing	Bot correct
4067	Marketing	Bot correct
4071	Outil	Bot correct
4076	Marketing	Bot correct
4077	Scraper	Bot correct
4078	Crawler	Bot correct
4079	Crawler	Bot correct
4081	Moteur de recherche	Bot correct
4082	Outil	Bot correct
4085	Outil	Bot correct
4086	Outil	Bot correct
4087	Outil	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
4088	Moteur de recherche	Bot correct
4089	Marketing	Bot correct
4090	Outil	Bot correct
4091	Outil	Bot correct
4092	Outil	Bot correct
4093	Outil	Bot correct
4094	Sans catégorie	Bot correct
4095	Moniteur de site	Bot correct
4096	Moniteur de site	Bot correct
4097	Moniteur de site	Bot correct
4098	Crawler	Bot correct
4099	Moteur de recherche	Bot correct
4100	Moteur de recherche	Bot correct
4101	Moteur de recherche	Bot correct
4102	Moteur de recherche	Bot correct
4103	Marketing	Bot correct
4104	Marketing	Bot correct
4105	Marketing	Bot correct
4106	Marketing	Bot correct
4109	Moteur de recherche	Bot correct
4110	Crawler	Bot correct
4111	Crawler	Bot correct
4112	Crawler	Bot correct
4113	Analyseur de vulnérabilité	Bot correct
4114	Crawler	Bot correct
4115	Outil	Bot correct
4121	Marketing	Bot correct
4126	Marketing	Bot correct
4127	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4128	Marketing	Bot correct
4129	Marketing	Bot correct
4130	Marketing	Bot correct
4131	Outil	Bot correct
4132	Marketing	Bot correct
4165	Marketing	Bot correct
4168	Tester de vitesse	Bot correct
4170	Outil	Bot correct
4172	Crawler	Bot correct
4173	Outil	Bot correct
4174	Crawler	Bot correct
4175	Crawler	Bot correct
4176	Outil	Bot correct
4177	Moteur de recherche	Bot correct
4178	Outil	Bot correct
4179	Crawler	Bot correct
4180	Outil	Bot correct
4181	Moniteur de site	Bot correct
4182	Moniteur de site	Bot correct
4183	Moniteur de site	Bot correct
4184	Moniteur de site	Bot correct
4185	Moteur de recherche	Bot correct
4186	Outil	Bot correct
4187	Outil	Bot correct
4188	Créateur de capture d’écran	Bot correct
4189	Marketing	Bot correct
4190	Moteur de recherche	Bot correct
4191	Moteur de recherche	Bot correct
4192	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4193	Moteur de recherche	Bot correct
4194	Outil	Bot correct
4196	Outil	Bot correct
4197	Outil	Bot correct
4198	Marketing	Bot correct
4199	Marketing	Bot correct
4200	Analyseur de vulnérabilité	Bot correct
4201	Outil	Bot correct
4202	Outil	Bot correct
4205	Moteur de recherche	Bot correct
4209	Moteur de recherche	Bot correct
4210	Tester de vitesse	Bot correct
4211	Outil	Bot correct
4212	Feed Fetcher	Bot correct
4213	Feed Fetcher	Bot correct
4215	Outil	Bot correct
4216	Outil	Bot correct
4219	Marketing	Bot correct
4220	Outil	Bot correct
4222	Moniteur de site	Bot correct
4223	Marketing	Bot correct
4224	Moteur de recherche	Bot correct
4225	Moteur de recherche	Bot correct
4226	Moteur de recherche	Bot correct
4227	Marketing	Bot correct
4228	Marketing	Bot correct
4229	Outil	Bot correct
4231	Créateur de capture d’écran	Bot correct
4232	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4233	Moniteur de site	Bot correct
4236	Moniteur de site	Bot correct
4242	Marketing	Bot correct
4243	Marketing	Bot correct
4244	Marketing	Bot correct
4245	Marketing	Bot correct
4246	Marketing	Bot correct
4247	Moteur de recherche	Bot correct
4252	Crawler	Bot correct
4253	Crawler	Bot correct
4254	Crawler	Bot correct
4255	Outil	Bot correct
4256	Sans catégorie	Bot correct
4257	Outil	Bot correct
4258	Crawler	Bot correct
4259	Crawler	Bot correct
4260	Outil	Bot correct
4261	Outil	Bot correct
4262	Outil	Bot correct
4263	Marketing	Bot correct
4265	Moteur de recherche	Bot correct
4266	Sans catégorie	Bot correct
4267	Outil	Bot correct
4268	Outil	Bot correct
4269	Moteur de recherche	Bot correct
4270	Moteur de recherche	Bot correct
4271	Moteur de recherche	Bot correct
4272	Moteur de recherche	Bot correct
4273	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4274	Moteur de recherche	Bot correct
4275	Moteur de recherche	Bot correct
4279	Marketing	Bot correct
4280	Crawler	Bot correct
4321	Sans catégorie	Bot correct
4322	Crawler	Bot correct
4323	Outil	Bot correct
4324	Outil	Bot correct
4325	Outil	Bot correct
4327	Moteur de recherche	Bot correct
4328	Marketing	Bot correct
4330	Moniteur de site	Bot correct
4331	Moteur de recherche	Bot correct
4334	Scraper	Bot correct
4335	Marketing	Bot correct
4336	Marketing	Bot correct
4339	Outil	Bot correct
4340	Crawler	Bot correct
4341	Crawler	Bot correct
4342	Analyseur de vulnérabilité	Bot correct
4343	Analyseur de vulnérabilité	Bot correct
4344	Scraper	Bot correct
4377	Crawler	Bot correct
4378	Crawler	Bot correct
4379	Moteur de recherche	Bot correct
4380	Moteur de recherche	Bot correct
4381	Moteur de recherche	Bot correct
4382	Moteur de recherche	Bot correct
4383	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4384	Moteur de recherche	Bot correct
4385	Outil	Bot correct
4386	Sans catégorie	Bot correct
4387	Crawler	Bot correct
4388	Crawler	Bot correct
4389	Outil	Bot correct
4390	Outil	Bot correct
4391	Outil	Bot correct
4392	Outil	Bot correct
4393	Outil	Bot correct
4394	Sans catégorie	Bot correct
4395	Outil	Bot correct
4396	Moniteur de site	Bot correct
4397	Moniteur de site	Bot correct
4404	Moteur de recherche	Bot correct
4405	Moteur de recherche	Bot correct
4406	Moteur de recherche	Bot correct
4407	Sans catégorie	Bot correct

Mise à jour de la signature du bot pour mars 2022

May 5, 2023

De nouvelles signatures ont été ajoutées et certaines signatures de robots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

Signature version 12 applicable aux plateformes NetScaler dotées de versions 13.0 76.31 ou ultérieures.

Nouvelles signatures de robots

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
4564	Marketing	Bot correct
4565	Marketing	Bot correct
4566	Marketing	Bot correct
4567	Marketing	Bot correct
4568	Marketing	Bot correct
4569	Sans catégorie	Bot incorrect
4570	Sans catégorie	Bot incorrect
4571	Crawler	Bot correct
4572	Crawler	Bot correct
4573	Sans catégorie	Bot incorrect
4574	Sans catégorie	Bot incorrect
4575	Marketing	Bot correct
4576	Marketing	Bot correct
4577	Marketing	Bot correct
4578	Marketing	Bot correct
4579	Marketing	Bot correct
4580	Marketing	Bot correct
4581	Marketing	Bot correct
4582	Marketing	Bot correct
4583	Créateur de capture d’écran	Bot correct
4584	Moteur de recherche	Bot correct
4585	Moteur de recherche	Bot correct
4586	Créateur de capture d’écran	Bot correct
4587	Sans catégorie	Bot correct
4588	Tester de vitesse	Bot correct
4589	Crawler	Bot correct
4590	Outil	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4591	Outil	Bot correct
4592	Crawler	Bot incorrect
4593	Moteur de recherche	Bot correct
4594	Moteur de recherche	Bot correct
4595	Moteur de recherche	Bot correct
4596	Marketing	Bot correct
4597	Outil	Bot correct
4598	Moteur de recherche	Bot correct
4599	Marketing	Bot correct
4600	Marketing	Bot correct
4601	Marketing	Bot correct
4602	Moteur de recherche	Bot correct
4603	Sans catégorie	Bot correct
4604	Marketing	Bot correct
4605	Marketing	Bot correct
4606	Sans catégorie	Bot incorrect
4607	Sans catégorie	Bot incorrect
4608	Outil	Bot correct
4609	Sans catégorie	Bot incorrect
4610	Outil	Bot correct
4611	Outil	Bot correct
4612	Scraper	Bot correct
4613	Sans catégorie	Bot correct
4614	Sans catégorie	Bot correct
4615	Moniteur de site	Bot correct
4616	Crawler	Bot correct
4617	Moniteur de site	Bot correct
4618	Moteur de recherche	Bot correct
4619	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4620	Marketing	Bot correct
4621	Moteur de recherche	Bot correct
4622	Crawler	Bot correct
4623	Crawler	Bot correct
4624	Crawler	Bot correct
4625	Scraper	Bot correct
4626	Crawler	Bot correct
4627	Analyseur de vulnérabilité	Bot correct
4628	Outil	Bot correct
4629	Sans catégorie	Bot incorrect
4630	Sans catégorie	Bot incorrect
4631	Outil	Bot correct
4632	Feed Fetcher	Bot correct
4633	Crawler	Bot incorrect
4634	Sans catégorie	Bot correct
4635	Feed Fetcher	Bot correct
4636	Sans catégorie	Bot correct
4637	Outil	Bot correct
4638	Outil	Bot correct
4639	Scraper	Bot incorrect
4640	Sans catégorie	Bot incorrect
4641	Outil	Bot correct
4642	Crawler	Bot incorrect
4643	Moniteur de site	Bot correct
4644	Moniteur de site	Bot correct
4645	Moteur de recherche	Bot correct
4646	Moteur de recherche	Bot correct
4647	Moteur de recherche	Bot correct
4648	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4649	Moteur de recherche	Bot incorrect
4650	Sans catégorie	Bot correct

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
2554	Sans catégorie	Bot incorrect
3835	Moteur de recherche	Bot correct
4027	Moteur de recherche	Bot correct
4038	Sans catégorie	Bot incorrect
4085	Outil	Bot correct
4098	Crawler	Bot correct
4100	Moteur de recherche	Bot correct
4220	Outil	Bot correct
4224	Moteur de recherche	Bot correct
4281	Sans catégorie	Bot incorrect
4412	Marketing	Bot correct
4425	Marketing	Bot correct
4429	Créateur de capture d’écran	Bot correct
4430	Analyseur de virus	Bot correct
4483	Crawler	Bot correct
4552	Sans catégorie	Bot correct
4562	Moteur de recherche	Bot correct
1000000	Navigateur	Bot correct
1000003	Navigateur	Bot correct
1000004	Scraper	Bot correct
1000005	Google_Crawler	Bot incorrect
1000006	Navigateur	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
1000007	Bot	Bot incorrect
1000008	Navigateur	Bot incorrect
1000009	Navigateur	Bot correct
1000010	Bot	Bot incorrect
1000011	Navigateur	Bot incorrect
1000012	Scraper	Bot correct
1000013	Scraper	Bot incorrect
1000014	Scraper	Bot incorrect
1000015	Navigateur	Bot correct
1000016	Bot	Bot incorrect
1000017	Navigateur	Bot incorrect
1000018	Navigateur	Bot correct
1000019	Scraper	Bot correct
1000020	Scraper	Bot correct
1000021	Scraper	Bot correct
1000022	Google_Crawler	Bot correct
1000023	Navigateur	Bot incorrect
1000024	Analyseur	Bot correct
1000025	Analyseur	Bot correct
1000026	Analyseur	Bot correct
1000027	Analyseur	Bot correct
1000028	Analyseur	Bot correct
1000029	Navigateur	Bot correct
1000030	Analyseur	Bot correct
1000031	Analyseur	Bot correct
1000032	Navigateur	Bot incorrect
1000033	Analyseur	Bot correct
1000034	Navigateur	Bot incorrect
1000035	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
1000036	Scraper	Bot correct
1000037	Navigateur	Bot correct
1000038	Analyseur	Bot correct
1000039	Analyseur	Bot correct
1000040	Analyseur	Bot correct
1000041	Analyseur	Bot correct
1000042	Analyseur	Bot correct
1000043	Analyseur	Bot correct
1000044	Analyseur	Bot correct
1000045	Logiciel Google_App_Engine	Bot correct
1000046	Google_Crawler	Bot correct
1000047	Navigateur	Bot incorrect
1000048	Navigateur	Bot incorrect
1000049	Analyseur	Bot correct
1000050	Navigateur	Bot incorrect
1000051	Navigateur	Bot correct
1000052	Navigateur	Bot incorrect
1000053	Scraper	Bot correct
1000054	Google_Crawler	Bot incorrect
1000055	Scraper	Bot incorrect
1000056	Analyseur	Bot correct
1000057	Navigateur	Bot incorrect
1000058	Navigateur	Bot incorrect
1000059	Navigateur	Bot incorrect
1000060	Scraper	Bot incorrect
1000061	Application	Bot incorrect
1000062	Scraper	Bot incorrect
1000063	Scraper	Bot incorrect
1000064	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
1000065	Scraper	Bot incorrect
1000066	Scraper	Bot incorrect
1000067	Navigateur	Bot incorrect
1000068	Scraper	Bot incorrect
1000069	Navigateur	Bot incorrect
1000070	Scraper	Bot incorrect
1000071	Application	Bot incorrect

Mise à jour de la signature du bot pour août 2022

May 5, 2023

De nouvelles signatures ont été ajoutées et certaines signatures de robots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

Version 13 de signature applicable aux plateformes NetScaler dotées de versions 13.0 76.31 ou ultérieures.

Nouvelles signatures de robots

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
4651	Marketing	Bot correct
4652	Sans catégorie	Bot incorrect
4653	Moteur de recherche	Bot correct
4654	Outil	Bot correct
4655	Crawler	Bot correct
4656	Marketing	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4657	Scraper	Bot correct
4658	Feed Fetcher	Bot correct
4659	Sans catégorie	Bot incorrect
4660	Outil	Bot correct
4661	Outil	Bot correct
4662	Sans catégorie	Bot incorrect
4663	Sans catégorie	Bot incorrect
4664	Marketing	Bot correct
4665	Sans catégorie	Bot correct
4666	Sans catégorie	Bot correct
4667	Feed Fetcher	Bot correct
4668	Sans catégorie	Bot correct
4669	Outil	Bot correct
4670	Outil	Bot correct
4671	Moteur de recherche	Bot correct
4672	Outil	Bot correct
4673	Sans catégorie	Bot correct
4674	Sans catégorie	Bot correct
4675	Sans catégorie	Bot correct
4676	Marketing	Bot correct
4677	Scraper	Bot correct
4678	Marketing	Bot correct
4679	Crawler	Bot incorrect
4680	Sans catégorie	Bot correct
4681	Sans catégorie	Bot correct
4682	Moniteur de site	Bot correct
4683	Moniteur de site	Bot correct
4684	Moteur de recherche	Bot correct
4685	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4686	Moteur de recherche	Bot correct
4687	Moteur de recherche	Bot correct
4688	Moteur de recherche	Bot correct
4689	Moteur de recherche	Bot correct
4690	Moteur de recherche	Bot correct
4691	Moteur de recherche	Bot correct
4692	Moteur de recherche	Bot correct
4693	Sans catégorie	Bot correct
4694	Sans catégorie	Bot incorrect
4695	Crawler	Bot correct
4696	Crawler	Bot correct
4697	Crawler	Bot correct
4698	Moteur de recherche	Bot correct
4699	Moteur de recherche	Bot correct
4700	Moteur de recherche	Bot correct
4701	Outil	Bot incorrect
4702	Sans catégorie	Bot correct
4703	Outil	Bot correct
4704	Outil	Bot correct
4705	Crawler	Bot correct
4706	Moniteur de site	Bot correct
4707	Moteur de recherche	Bot correct
4708	Outil	Bot correct
4709	Analyseur de vulnérabilité	Bot correct
4710	Analyseur de vulnérabilité	Bot correct
4711	Crawler	Bot correct
4712	Crawler	Bot correct
4713	Crawler	Bot correct
4714	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4715	Outil	Bot correct
4716	Outil	Bot correct
4717	Moteur de recherche	Bot incorrect
4718	Sans catégorie	Bot correct
4719	Outil	Bot correct
4720	Marketing	Bot correct
4721	Marketing	Bot correct
4722	Moteur de recherche	Bot correct
4723	Sans catégorie	Bot incorrect
4724	Outil	Bot correct
4725	Moteur de recherche	Bot correct
4726	Moteur de recherche	Bot correct
4727	Outil	Bot correct
4728	Sans catégorie	Bot incorrect
4729	Moniteur de site	Bot correct
4730	Moteur de recherche	Bot correct
4731	Moteur de recherche	Bot correct
4732	Moteur de recherche	Bot correct
4733	Moteur de recherche	Bot correct
4734	Outil	Bot incorrect
4735	Outil	Bot incorrect
4736	Outil	Bot correct
4737	Marketing	Bot correct
4738	Outil	Bot correct
4739	Feed Fetcher	Bot correct
4740	Moteur de recherche	Bot correct
4741	Sans catégorie	Bot incorrect
4742	Moteur de recherche	Bot correct
4743	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4744	Outil	Bot correct
4745	Outil	Bot correct
4746	Marketing	Bot correct
4747	Sans catégorie	Bot incorrect
4748	Moteur de recherche	Bot correct
4749	Moteur de recherche	Bot correct
4750	Moteur de recherche	Bot correct
4751	Moteur de recherche	Bot correct
4752	Moteur de recherche	Bot correct

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
3796	Scraper	Bot correct
3835	Moteur de recherche	Bot correct
3935	Scraper	Bot correct
4027	Moteur de recherche	Bot correct
4061	Moteur de recherche	Bot correct
4100	Moteur de recherche	Bot correct
4451	Tester de vitesse	Bot correct
4562	Moteur de recherche	Bot correct
4575	Marketing	Bot correct
4577	Marketing	Bot correct
4578	Marketing	Bot correct
4579	Marketing	Bot correct
4580	Marketing	Bot correct
4583	Créateur de capture d’écran	Bot correct
4584	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4585	Moteur de recherche	Bot correct
4597	Outil	Bot correct
4599	Marketing	Bot correct
4601	Marketing	Bot correct
4623	Crawler	Bot correct
4630	Sans catégorie	Bot incorrect
4647	Moteur de recherche	Bot correct
1000000	Navigateur	Bot correct
1000001	Application	Bot incorrect
1000002	Navigateur	Bot correct
1000003	Scraper	Bot correct
1000004	Navigateur	Bot correct
1000005	Navigateur	Bot incorrect
1000006	Google Crawler	Bot incorrect
1000007	Scraper	Bot incorrect
1000008	Scraper	Bot correct
1000009	Navigateur	Bot incorrect
1000010	Bot	Bot incorrect
1000011	Bot	Bot incorrect
1000012	Scraper	Bot incorrect
1000013	Scraper	Bot incorrect
1000014	Navigateur	Bot incorrect
1000015	Navigateur	Bot correct
1000016	Navigateur	Bot incorrect
1000017	Scraper	Bot correct
1000018	Scraper	Bot incorrect
1000019	Scraper	Bot incorrect
1000020	Scraper	Bot incorrect
1000021	Navigateur	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
1000022	Scraper	Bot correct
1000023	Navigateur	Bot incorrect
1000024	Bot	Bot incorrect
1000025	Analyseur	Bot correct
1000026	Scraper	Bot correct
1000027	Navigateur	Bot incorrect
1000028	Navigateur	Bot incorrect
1000029	Scraper	Bot correct
1000030	Google Crawler	Bot correct
1000031	Navigateur	Bot incorrect
1000032	Analyseur	Bot correct
1000033	Bot	Bot incorrect
1000034	Analyseur	Bot correct
1000035	Analyseur	Bot correct
1000036	Analyseur	Bot correct
1000037	Analyseur	Bot correct
1000038	Scraper	Bot correct
1000039	Analyseur	Bot correct
1000040	Navigateur	Bot incorrect
1000041	Navigateur	Bot incorrect
1000042	Scraper	Bot correct
1000043	Navigateur	Bot correct
1000044	Analyseur	Bot correct
1000045	Analyseur	Bot correct
1000046	Analyseur	Bot correct
1000047	Analyseur	Bot correct
1000048	Analyseur	Bot correct
1000049	Navigateur	Bot incorrect
1000050	Google Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
1000051	Navigateur	Bot incorrect
1000052	Navigateur	Bot incorrect
1000053	Analyseur	Bot correct
1000054	Navigateur	Bot correct
1000055	Scraper	Bot correct
1000056	Navigateur	Bot correct
1000057	Analyseur	Bot correct
1000058	Google Crawler	Bot incorrect
1000059	Scraper	Bot incorrect
1000060	Navigateur	Bot incorrect
1000061	Navigateur	Bot correct
1000062	Navigateur	Bot incorrect
1000063	Navigateur	Bot incorrect
1000064	Navigateur	Bot incorrect
1000065	Scraper	Bot incorrect
1000066	Application	Bot incorrect
1000067	Scraper	Bot incorrect
1000068	Scraper	Bot incorrect
1000069	Navigateur	Bot correct
1000070	Application	Bot incorrect

Mise à jour de la signature du bot pour avril 2023

May 5, 2023

De nouvelles signatures ont été ajoutées et certaines signatures de robots existantes sont mises à jour. Vous pouvez télécharger et configurer ces règles de signature pour protéger votre appliance contre les attaques de bots.

Version de signature du bot

Signature version 14 applicable aux plateformes NetScaler dotées de versions 13.0 76.31 ou ultérieures.

Nouvelles signatures de robots

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
4753	Outil	Bot incorrect
4754	Sans catégorie	Bot incorrect
4755	Scraper	Bot correct
4756	Marketing	Bot correct
4757	Marketing	Bot correct
4758	Marketing	Bot correct
4759	Marketing	Bot correct
4760	Marketing	Bot correct
4761	Marketing	Bot correct
4762	Marketing	Bot correct
4763	Marketing	Bot correct
4764	Marketing	Bot correct
4765	Scraper	Bot incorrect
4766	Scraper	Bot incorrect
4767	Outil	Bot correct
4768	Scraper	Bot incorrect
4769	Outil	Bot correct
4770	Scraper	Bot incorrect
4771	Scraper	Bot incorrect
4772	Scraper	Bot incorrect
4773	Scraper	Bot incorrect
4774	Scraper	Bot incorrect
4775	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4776	Marketing	Bot correct
4777	Outil	Bot correct
4778	Outil	Bot correct
4779	Crawler	Bot correct
4780	Moniteur de site	Bot correct
4781	Moniteur de site	Bot correct
4782	Moniteur de site	Bot correct
4783	Sans catégorie	Bot correct
4784	Outil	Bot correct
4785	Outil	Bot correct
4786	Analyseur de vulnérabilité	Bot correct
4787	Outil	Bot correct
4788	Marketing	Bot correct
4789	Marketing	Bot correct
4790	Marketing	Bot correct
4791	Sans catégorie	Bot correct
4792	Sans catégorie	Bot correct
4793	Sans catégorie	Bot incorrect
4794	Sans catégorie	Bot incorrect
4795	Outil	Bot correct
4796	Moniteur de site	Bot correct
4797	Moniteur de site	Bot correct
4798	Sans catégorie	Bot correct
4799	Moteur de recherche	Bot correct
4800	Moteur de recherche	Bot correct
4801	Moteur de recherche	Bot correct
4802	Sans catégorie	Bot correct
4803	Outil	Bot incorrect
4804	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4805	Marketing	Bot correct
4806	Crawler	Bot correct
4807	Crawler	Bot correct
4808	Analyseur de vulnérabilité	Bot incorrect
4809	Analyseur de vulnérabilité	Bot correct
4810	Outil	Bot correct
4811	Outil	Bot correct
4812	Sans catégorie	Bot correct
4813	Sans catégorie	Bot correct
4814	Moniteur de site	Bot correct
4815	Scraper	Bot incorrect
4816	Moteur de recherche	Bot correct
4817	Sans catégorie	Bot correct
4818	Moniteur de site	Bot correct
4819	Moteur de recherche	Bot correct
4820	Moteur de recherche	Bot correct
4821	Moteur de recherche	Bot correct
4822	Moteur de recherche	Bot correct
4823	Moteur de recherche	Bot correct
4824	Sans catégorie	Bot correct
4825	Marketing	Bot correct
4826	Scraper	Bot correct
4827	Créateur de capture d’écran	Bot correct
4828	Sans catégorie	Bot incorrect
4829	Sans catégorie	Bot incorrect
4830	Sans catégorie	Bot incorrect
4831	Sans catégorie	Bot correct
4832	Sans catégorie	Bot incorrect
4833	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4834	Moteur de recherche	Bot correct
4835	Sans catégorie	Bot correct
4836	Moteur de recherche	Bot correct
4837	Outil	Bot correct
4838	Marketing	Bot correct
4839	Outil	Bot correct
4840	Scraper	Bot correct
4841	Moteur de recherche	Bot correct
4842	Moniteur de site	Bot correct
4843	Sans catégorie	Bot incorrect
4844	Moteur de recherche	Bot correct
4845	Moteur de recherche	Bot correct
4846	Crawler	Bot correct
4847	Marketing	Bot correct
4848	Outil	Bot correct
4849	Crawler	Bot correct
4850	Crawler	Bot correct
4851	Sans catégorie	Bot incorrect
4852	Moteur de recherche	Bot correct
4853	Sans catégorie	Bot correct
4854	Sans catégorie	Bot correct
4855	Moniteur de site	Bot correct
4856	Outil	Bot correct
4857	Outil	Bot correct
4858	Scraper	Bot incorrect
4859	Créateur de capture d’écran	Bot correct
4860	Moniteur de site	Bot correct
4861	Moniteur de site	Bot correct
4862	Crawler	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4863	Moteur de recherche	Bot correct
4864	Moteur de recherche	Bot correct
4865	Moteur de recherche	Bot correct
4866	Moteur de recherche	Bot correct
4867	Moteur de recherche	Bot correct
4868	Marketing	Bot correct
4869	Marketing	Bot correct
4870	Moteur de recherche	Bot correct
4871	Sans catégorie	Bot incorrect
4872	Sans catégorie	Bot incorrect
4873	Sans catégorie	Bot incorrect
4874	Sans catégorie	Bot incorrect
4875	Sans catégorie	Bot incorrect
4876	Sans catégorie	Bot incorrect
4877	Sans catégorie	Bot incorrect
4878	Sans catégorie	Bot incorrect
4879	Sans catégorie	Bot incorrect
4880	Sans catégorie	Bot correct
4881	Moteur de recherche	Bot correct
4882	Sans catégorie	Bot correct
4883	Outil	Bot correct
4884	Outil	Bot correct
4885	Outil	Bot correct
4886	Moniteur de site	Bot correct
4887	Moniteur de site	Bot correct
4888	Scraper	Bot incorrect
4889	Marketing	Bot correct
4890	Sans catégorie	Bot incorrect
4891	Moteur de recherche	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
4892	Moteur de recherche	Bot correct
4893	Marketing	Bot correct
4894	Sans catégorie	Bot incorrect
4895	Sans catégorie	Bot incorrect
4896	Analyseur de vulnérabilité	Bot correct
4897	Sans catégorie	Bot incorrect
4898	Sans catégorie	Bot incorrect
4899	Sans catégorie	Bot incorrect
4900	Crawler	Bot correct
4901	Crawler	Bot correct
4902	Analyseur de vulnérabilité	Bot correct
4903	Outil	Bot correct
4904	Feed Fetcher	Bot correct
4905	Outil	Bot correct
4906	Crawler	Bot correct
4907	Sans catégorie	Bot correct
4908	Sans catégorie	Bot incorrect
4909	Sans catégorie	Bot correct
4910	Moteur de recherche	Bot correct
4911	Moteur de recherche	Bot correct
4912	Sans catégorie	Bot correct
4913	Moteur de recherche	Bot correct
4914	Crawler	Bot correct

Signatures de bots mises à jour

Vous trouverez ci-dessous une liste des ID de règle de signature de bot, de la catégorie et de son type.

ID de signature du bot	Catégorie de bot	Type de robot
3935	Scraper	Bot correct
4012	Crawler	Bot correct
4013	Moteur de recherche	Bot correct
4027	Moteur de recherche	Bot correct
4038	Sans catégorie	Bot incorrect
4071	Outil	Bot correct
4100	Moteur de recherche	Bot correct
4220	Outil	Bot correct
4425	Marketing	Bot correct
4441	Feed Fetcher	Bot correct
4451	Tester de vitesse	Bot correct
4563	Moteur de recherche	Bot correct
4575	Marketing	Bot correct
4577	Marketing	Bot correct
4578	Marketing	Bot correct
4579	Marketing	Bot correct
4580	Marketing	Bot correct
4583	Créateur de capture d’écran	Bot correct
4584	Moteur de recherche	Bot correct
4585	Moteur de recherche	Bot correct
4586	Créateur de capture d’écran	Bot correct
4593	Moteur de recherche	Bot correct
4597	Outil	Bot correct
4599	Marketing	Bot correct
4600	Marketing	Bot correct
4601	Marketing	Bot correct
4618	Moteur de recherche	Bot correct
4633	Crawler	Bot incorrect
4639	Scraper	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
4647	Moteur de recherche	Bot correct
4651	Marketing	Bot correct
4660	Outil	Bot correct
4687	Moteur de recherche	Bot correct
4717	Moteur de recherche	Bot incorrect
4730	Moteur de recherche	Bot correct
1000000	Navigateur	Bot correct
1000001	Application	Bot incorrect
1000002	Navigateur	Bot correct
1000003	Scraper	Bot correct
1000004	Navigateur	Bot correct
1000005	Navigateur	Bot incorrect
1000006	Google_Crawler	Bot incorrect
1000007	Scraper	Bot incorrect
1000008	Scraper	Bot correct
1000009	Navigateur	Bot incorrect
1000010	Bot	Bot incorrect
1000011	Bot	Bot incorrect
1000012	Scraper	Bot incorrect
1000013	Scraper	Bot incorrect
1000014	Navigateur	Bot incorrect
1000015	Navigateur	Bot correct
1000016	Navigateur	Bot incorrect
1000017	Scraper	Bot correct
1000018	Scraper	Bot incorrect
1000019	Scraper	Bot incorrect
1000020	Scraper	Bot incorrect
1000021	Navigateur	Bot correct
1000022	Scraper	Bot correct

ID de signature du bot	Catégorie de bot	Type de robot
1000023	Navigateur	Bot incorrect
1000024	Bot	Bot incorrect
1000025	Analyseur	Bot correct
1000026	Scraper	Bot correct
1000027	Navigateur	Bot incorrect
1000028	Navigateur	Bot incorrect
1000029	Scraper	Bot correct
1000030	Google_Crawler	Bot correct
1000031	Navigateur	Bot incorrect
1000032	Analyseur	Bot correct
1000033	Bot	Bot incorrect
1000034	Analyseur	Bot correct
1000035	Analyseur	Bot correct
1000036	Analyseur	Bot correct
1000037	Analyseur	Bot correct
1000038	Scraper	Bot correct
1000039	Analyseur	Bot correct
1000040	Navigateur	Bot incorrect
1000041	Navigateur	Bot incorrect
1000042	Scraper	Bot correct
1000043	Navigateur	Bot correct
1000044	Analyseur	Bot correct
1000045	Analyseur	Bot correct
1000046	Analyseur	Bot correct
1000047	Analyseur	Bot correct
1000048	Analyseur	Bot correct
1000049	Navigateur	Bot incorrect
1000050	Google_Crawler	Bot correct
1000051	Navigateur	Bot incorrect

ID de signature du bot	Catégorie de bot	Type de robot
1000052	Navigateur	Bot incorrect
1000053	Analyseur	Bot correct
1000054	Navigateur	Bot correct
1000055	Scraper	Bot correct
1000056	Navigateur	Bot correct
1000057	Analyseur	Bot correct
1000058	Google_Crawler	Bot incorrect
1000059	Scraper	Bot incorrect
1000060	Navigateur	Bot incorrect
1000061	Navigateur	Bot correct
1000062	Navigateur	Bot incorrect
1000063	Navigateur	Bot incorrect
1000064	Navigateur	Bot incorrect
1000065	Scraper	Bot incorrect
1000066	Application	Bot incorrect
1000067	Scraper	Bot incorrect
1000068	Scraper	Bot incorrect
1000069	Navigateur	Bot correct
1000070	Application	Bot incorrect

Redirection de cache

May 5, 2023

Dans un déploiement classique, différents clients demandent à plusieurs reprises aux serveurs Web le même contenu. Pour soulager le serveur Web d'origine du traitement de chaque demande, une appliance NetScaler avec la redirection du cache activée peut diffuser ce contenu à partir d'un serveur de cache plutôt que depuis le serveur d'origine.

L'appliance NetScaler analyse les demandes entrantes, envoie des demandes de données pouvant être mises en cache aux serveurs de cache et envoie des demandes non mises en cache et des requêtes

HTTP dynamiques aux serveurs d'origine.

La redirection du cache est une fonctionnalité basée sur des règles. Par défaut, les demandes qui correspondent à une politique sont envoyées au serveur d'origine et toutes les autres demandes sont envoyées à un serveur de cache. Pour les tests ou la maintenance, vous pouvez ignorer l'évaluation des politiques et diriger toutes les demandes vers le cache ou vers le serveur d'origine.

Vous pouvez combiner la commutation de contenu avec la redirection de cache pour mettre en cache du contenu sélectif et diffuser du contenu à partir de serveurs de cache spécifiques pour des types spécifiques de contenu demandé.

Une appliance NetScaler configurée pour la redirection du cache peut être déployée à la périphérie d'un réseau, devant le serveur d'origine ou n'importe où sur le backbone du réseau. Dans un déploiement périphérique, couramment utilisé par les fournisseurs de services Internet (ISP), les câblodistributeurs, les réseaux de distribution de contenu et les réseaux d'entreprise, l'appliance NetScaler réside directement devant les clients. Dans un déploiement côté serveur, l'appliance NetScaler est plus proche des serveurs d'origine.

La redirection du cache est utilisée le plus souvent avec le type de service HTTP, mais elle prend également en charge le protocole sécurisé HTTPS.

Stratégies de redirection du cache

May 5, 2023

Un serveur virtuel de redirection de cache applique des politiques de redirection de cache à chaque demande entrante. Par défaut, si une demande correspond à l'une des politiques configurées, elle est considérée comme ne pouvant pas être mise en cache et l'appliance NetScaler l'envoie au serveur d'origine. Les autres demandes sont envoyées à un serveur de cache. Ce comportement peut être inversé, de sorte que les demandes correspondant aux politiques de redirection de cache configurées soient envoyées aux serveurs de cache.

L'appliance fournit un ensemble de politiques pour la redirection du cache. Si ces politiques intégrées ne sont pas adaptées à votre déploiement, vous pouvez configurer des politiques de redirection du cache définies par l'utilisateur.

Remarque : Une fois que vous avez déterminé les politiques de redirection de cache intégrées à utiliser ou que vous avez créé des politiques définies par l'utilisateur, procédez à la configuration de la redirection du cache. Pour utiliser cette fonctionnalité, vous devez configurer au moins un serveur virtuel de redirection de cache et, pour un fonctionnement normal, vous devez lier au moins une politique de redirection de cache à ce serveur virtuel.

Stratégies de redirection de cache intégrées

May 5, 2023

L'appliance NetScaler fournit des politiques de redirection de cache intégrées qui gèrent les demandes de cache classiques. Ces stratégies sont basées sur les méthodes HTTP, les jetons URL ou URL de la demande entrante, la version HTTP ou les en-têtes HTTP et leurs valeurs dans la demande.

Les stratégies de redirection de cache intégrées peuvent être directement liées à un serveur virtuel et ne nécessitent aucune configuration supplémentaire.

Les stratégies de redirection du cache utilisent deux types de langages d'expressions d'appliance, la stratégie classique et la stratégie avancée. Pour plus d'informations sur ces langues, voir Stratégies et expressions.

Stratégies de redirection de cache classiques intégrées

Les stratégies de redirection de cache intégrées basées sur des expressions classiques sont appelées *stratégies de redirection de cache classiques*. Pour obtenir une description complète des expressions classiques et la façon de les configurer, voir Stratégies et expressions.

Les stratégies de redirection de cache classiques évaluent les caractéristiques de base du trafic et d'autres données. Par exemple, les stratégies de redirection de cache classiques peuvent déterminer si une requête ou une réponse HTTP contient un type particulier d'en-tête ou d'URL.

L'appliance NetScaler fournit les politiques de redirection de cache classiques intégrées suivantes :

Nom de la stratégie intégrée	Description
bypass-non-get	Isolez le cache si la demande utilise une méthode HTTP autre que GET.
bypass-cache-control	Ignorez le cache si l'en-tête de la demande contient un en-tête Cache-Control : no-cache ou Cache-Control : no-store, ou si la requête HTTP contient un en-tête Pragma.
bypass-dynamic-url	Contournez le cache si l'URL suggère que le contenu est dynamique, comme l'indique la présence de l'une des extensions suivantes : cgi, asp, exe, cfm, ex, shtml ou htx. Contournez également le cache si l'URL commence par l'un des éléments suivants : /cgi-bin/, /bin/ ou /exec/.

Nom de la stratégie intégrée	Description
jetons d'URL de contournement	Contournez le cache car la demande est dynamique, comme indiqué par l'un des jetons suivants dans l'URL : ? , ! , ou =.
cookie de contournement	Contournez le cache pour toute URL contenant un en-tête de cookie et une extension autre que .png ou .jpg.

Stratégies de redirection de cache de stratégie avancées intégrées

Les stratégies de redirection de cache intégrées basées sur des expressions de stratégie avancées sont appelées *stratégies de redirection de cache de stratégie avancée*. Pour obtenir une description complète des expressions de stratégie avancées et savoir comment les configurer, consultez Stratégies et expressions.

Outre les mêmes types d'évaluations effectuées par les stratégies de redirection de cache classiques, les stratégies de redirection de cache de stratégie avancée vous permettent d'analyser davantage de données (par exemple, le corps d'une requête HTTP) et de configurer davantage d'opérations dans la règle de stratégie (par exemple, diriger la demande vers le cache ou serveur d'origine).

Les appliances NetScaler fournissent les deux actions intégrées suivantes pour les politiques avancées de redirection du cache des politiques :

- CACHE
- ORIGIN

Comme leur nom l'indique, ils dirigent la demande vers le serveur de cache ou le serveur d'origine, respectivement.

Remarque : Si vous utilisez la stratégie de redirection du cache de stratégie avancée intégrée, vous ne pouvez pas modifier l'action.

L'appliance NetScaler fournit les politiques avancées intégrées de redirection du cache suivantes :

Nom de la stratégie intégrée	Description
bypass-non-get_adv	Isolez le cache si la demande utilise une méthode HTTP autre que GET.
bypass-cache-control_adv	Ignorez le cache si l'en-tête de la demande contient un en-tête Cache-Control : no-cache ou Cache-Control : no-store, ou si la requête HTTP contient un en-tête Pragma.

Nom de la stratégie intégrée	Description
bypass-dynamic-url_adv	Contournez le cache si l'URL suggère que le contenu est dynamique, comme l'indique la présence de l'une des extensions suivantes : cgi, asp, exe, cfm, ex, shtml ou htx. Contournez également le cache si l'URL commence par l'un des éléments suivants : /cgi-bin/, /bin/ ou /exec/.
bypass-urltokens_adv	Contournez le cache car la demande est dynamique, comme indiqué par l'un des jetons suivants dans l'URL : ? , ! , ou =.
bypass-cookie_adv	Contournez le cache pour toute URL contenant un en-tête de cookie et une extension autre que .png ou .jpg.

Afficher les stratégies de redirection de cache intégrées

Vous pouvez afficher les stratégies de redirection de cache disponibles à l'aide de l'interface de ligne de commande ou de l'utilitaire de configuration.

Afficher les stratégies de redirection de cache intégrées à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show cr policy [<policyName>]
```

Exemple :

```
1 > show cr policy
2 1)       Cache-By-Pass RULE: NS_NON_GET          Policy:bypass-non-get
3 2)       Cache-By-Pass RULE: (NS_CACHECONTROL_NOSTORE ||
     NS_CACHECONTROL_NOCACHE || NS_HEADER_PRAGMA)    Policy:bypass-cache-
     control
4 3)       Cache-By-Pass RULE: (NS_EXT_CGI || NS_EXT_ASP || NS_EXT_EXE ||
      NS_EXT_CFM || NS_EXT_EX || NS_EXT_SHTML || NS_EXT_HTX) || (
     NS_URL_PATH_CGIBIN || NS_URL_PATH_EXEC || NS_URL_PATH_BIN)
     Policy:bypass-dynamic-url
5 4)       Cache-By-Pass RULE: NS_URL_TOKENS       Policy:bypass-
     urltokens
```



```
5)       Cache-By-Pass RULE: (NS_HEADER_COOKIE && NS_EXT_NOT_GIF &&
   NS_EXT_NOT_JPEG)     Policy:bypass-cookie
 Done
<!--NeedCopy-->
```

Afficher les stratégies de redirection de cache intégrées à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Stratégies. Les stratégies de redirection de cache configurées apparaissent dans le volet de détails.
2. Sélectionnez l'une des stratégies configurées pour afficher les détails.

Configurer une stratégie de redirection du cache

May 5, 2023

Une stratégie de redirection de cache inclut une expression (également appelée *règle*). L'expression représente une condition qui est évaluée lorsque la demande du client est comparée à la stratégie.

Vous ne configurez pas explicitement les actions des stratégies de redirection du cache.

Une stratégie de redirection de cache porte un nom et inclut une expression de stratégie avancée ou un ensemble de clauses d'expression de stratégie avancées combinées à l'aide d'opérateurs logiques, et les actions intégrées suivantes :

- CACHE
- ORIGIN

Pour plus d'informations sur les expressions de stratégie avancées, consultez la section Stratégies et expressions.

Ajouter une stratégie de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une stratégie de redirection du cache et vérifier la configuration :

```
-  add cr policy <policyName> \*\*-rule\*\* <expression> -action<string
   > [-logAction<string>]

-  show cr policy [<policyName>]

<!--NeedCopy-->
```


Exemples :

Stratégie avec une expression simple :

```
> add cr policy crpol1 -rule !(HTTP.REQ.URL.ENDSWITH(".jpeg")) -action origin
 Done
> show cr policy crpoll
    Policy: crpol1 Rule: !(HTTP.REQ.URL.ENDSWITH(".jpeg")) Action: ORIGIN
    Hits: 0
 Done

<!--NeedCopy-->
```

Stratégie avec une expression composée :

```
> add cr policy crpol11 -rule 'http.req.method.eq(post) && (HTTP.REQ.URL.ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))'  -action cache
 Done
> show cr policy crpol11
    Policy: crpol11    Rule: http.req.method.eq(post) && (HTTP.REQ.URL.ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))  Action: CACHE
    Hits: 0
 Done

<!--NeedCopy-->
```

Stratégie qui évalue un en-tête :

```
> add cr policy crpol12 -rule http.req.header("If-Modified-Since").exists -action origin
 Done
> show cr policy crpol12
    Policy: crpol12    Rule: http.req.header("If-Modified-Since").exists   Action: ORIGIN
    Hits: 0
 Done

<!--NeedCopy-->
```


Modifier ou supprimer une stratégie de redirection de cache à l'aide de l'interface de ligne de commande

- Pour modifier une stratégie de redirection de cache, utilisez la commande set cr policy, qui est tout comme la commande add cr policy, sauf que vous entrez le nom d'une stratégie existante et que vous n'avez qu'à fournir les paramètres que vous souhaitez modifier.
- Pour supprimer une stratégie, utilisez la commande `rm cr policy`, qui accepte uniquement l'argument <name>. Si la stratégie est liée à un serveur virtuel, vous devez la dissocier avant de pouvoir la supprimer.

Pour plus d'informations sur la suppression de la liaison d'une stratégie de redirection de cache, voir Délier une stratégie d'un serveur virtuel de redirection de cache.

Configurer une stratégie de redirection de cache avec une expression simple à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Stratégies**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une stratégie de redirection de cache**, dans la zone de texte **Nom**, tapez le nom de la stratégie.
4. Sélectionnez l'action **CACHE** ou **ORIGIN** appropriée dans la liste déroulante **Action** .
5. Dans la zone **Action du journal**, cliquez sur **Ajouter**. Saisissez un nom dans la boîte de dialogue **Créer une action de message d'audit** .
    - Configurez **le niveau de journal** en choisissant la valeur appropriée dans la liste déroulante :
        - **URGENCE**
        - **ALERTE**
        - **CRITIQUE**
        - **ERROR**
        - **AVERTISSEMENT**
        - **REMARQUER**
        - **INFORMATIONNEL**
        - **DEBUG**
    - Entrez l'expression dans la zone **Expression** .
        - Type d'expression - Général
        - Type de flux -REQ
        - Protocole -HTTP
        - Qualificatif -URL

- Opérateur - ! =
- Valeur - /.jpeg

- Cliquez sur **Create**.

6. Pour configurer une expression simple, saisissez-la. Voici un exemple d'expression qui vérifie la présence d'une `.jpeg` extension dans une URL :

   - Type d'expression - Général
   - Type de flux -REQ
   - Protocole -HTTP
   - Qualificatif -URL
   - Opérateur - ! =
   - Valeur - /.jpeg

   L'expression simple de l'exemple suivant vérifie la présence d'un en-tête If-Modified-Since dans une demande :

   - Type d'expression - Général
   - Type de flux -REQ
   - Protocole -HTTP
   - Qualificatif -HEADER
   - Opérateur -EXISTS
   - Nom de l'en-tête -If-Modified-Since

7. Lorsque vous avez fini de saisir l'expression, cliquez sur **Créer**.



Configurer une stratégie de redirection de cache avec une expression composée à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Stratégies**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la zone **de texte Nom**, saisissez un nom pour la stratégie.

   Le nom peut commencer par une lettre, un chiffre ou le symbole de soulignement, et peut comprendre de 1 à 127 lettres, chiffres et les symboles tiret (-), point (.), livre (#), espace (), at (@), égal (=) et trait de soulignement (_). Vous devez choisir un nom qui permet aux autres utilisateurs de savoir facilement quel type de contenu cette stratégie a été créée pour détecter.
4. Sélectionnez l'action **CACHE** ou **ORIGIN** appropriée dans la liste déroulante **Action** .
5. Dans la zone **Action du journal**, cliquez sur **Ajouter**. Saisissez un nom dans la boîte de dialogue **Créer une action de message d'audit** .
   - Configurez **le niveau de journal** en choisissant la valeur appropriée dans la liste déroulante :
     - **URGENCE**
     - **ALERTE**
     - **CRITIQUE**
     - **ERROR**
     - **AVERTISSEMENT**
     - **REMARQUER**
     - **INFORMATIONNEL**
     - **DEBUG**
   - Entrez l'expression dans la zone **Expression** .
     - Type d'expression - Général
     - Type de flux -REQ
     - Protocole -HTTP
     - Qualificatif -URL
     - Opérateur - ! =
     - Valeur - /.jpeg
   - Cliquez sur **Create**.
6. Choisissez le type d'expression composée que vous souhaitez créer. Vos choix sont les suivants :
   - **Correspond à toutes les expressions**. La stratégie correspond au trafic si une ou plusieurs expressions individuelles correspondent au trafic.

- **Correspond à toutes les expressions**. La stratégie ne correspond au trafic que si chaque expression individuelle correspond au trafic.
- **Expressions tabulaires**. Permet de basculer la liste Expressions au format tabulaire avec trois colonnes. Dans la colonne la plus à droite, vous placez l'un des opérateurs suivants :
  - L'opérateur AND [&&], pour exiger que, pour correspondre à la politique, une demande corresponde à la fois à l'expression actuelle et à l'expression suivante.
  - L'opérateur OR [||], pour exiger que, pour correspondre à la politique, une demande corresponde soit à l'expression actuelle, soit à l'expression suivante, soit aux deux. Ce n'est que si la demande ne correspond pas à l'une ou l'autre des expressions qu'elle ne correspond pas à la stratégie.

  Vous pouvez également regrouper des expressions dans des sous-groupes imbriqués en sélectionnant une expression existante et en cliquant sur l'un des opérateurs suivants :

  - L'opérateur BEGIN SUBGROUP [+ (], qui indique à l'appliance NetScaler de commencer un sous-groupe imbriqué avec l'expression sélectionnée. (Pour supprimer cet opérateur de l'expression, cliquez sur - (.)
  - L'opérateur END SUBGROUP [+)], qui indique à l'appliance NetScaler de terminer le sous-groupe imbriqué actuel avec l'expression sélectionnée. (Pour supprimer cet opérateur de l'expression, cliquez sur -).)
- **Forme libre avancée**. Désactive complètement l'éditeur d'expressions et transforme la liste Expressions en une zone de texte dans laquelle vous pouvez taper une expression composée. Il s'agit à la fois de la méthode la plus puissante et la plus difficile pour créer une expression de politique. Elle est recommandée uniquement aux personnes parfaitement familiarisées avec le langage d'expressions classiques de NetScaler.

  Pour plus d'informations sur la création d'expressions classiques dans la zone de texte de forme libre avancée, reportez-vous à la section Configuration des politiques et expressions classiques.

  Attention : Si vous passez en mode avancé d'édition d'expression de forme libre, vous ne pouvez pas revenir à aucun des autres modes. Ne choisissez pas ce mode d'édition d'expression, sauf si vous êtes sûr de vouloir l'utiliser.

7. Si vous avez choisi Correspondance à n'importe quelle expression, Correspondance à toutes les expressions ou Expressions tabulaires, cliquez sur **Ajouter** pour afficher la boîte de dialogue Ajouter une expression.

   Vous devez laisser le type d'expression défini sur Général pour les stratégies de redirection du cache.

8. Dans la liste déroulante Type de flux, choisissez un type de flux pour votre expression.

Le type de flux détermine si la stratégie examine les connexions entrantes ou sortantes. Deux choix s'offrent à vous :

- **REQ**. Configure l'appliance NetScaler pour examiner les connexions entrantes ou les demandes.
- **RES**. Configure l'appliance pour qu'elle examine les connexions sortantes ou les réponses.

9. Dans la liste déroulante Protocole, choisissez un protocole pour votre expression.

   Le protocole détermine le type d'informations que la stratégie examine dans la demande ou la réponse. Selon que vous avez choisi REQ ou RES dans la liste déroulante précédente, les quatre ou seulement trois des options suivantes sont disponibles :

   - **HTTP**. Configure l'appliance pour qu'elle examine l'en-tête HTTP.
   - **SSL**. Configure le dispositif pour qu'il examine le certificat client SSL. Disponible uniquement si vous avez choisi REQ (requêtes) dans la liste déroulante précédente.
   - **TCP**. Configure l'appliance pour qu'elle examine l'en-tête TCP.
   - **IP**. Configure l'appliance pour qu'elle examine l'adresse IP source ou de destination.

10. Sélectionnez un qualificatif pour votre expression dans la liste déroulante Qualificatif.

    Le contenu de la liste déroulante Qualificatif dépend du protocole que vous avez choisi. Le tableau suivant décrit les choix disponibles pour chaque protocole.

    Tableau 1. Qualificateurs de stratégie de redirection de cache disponibles pour chaque protocole

Protocole	Qualificatif	Définition
HTTP	METHOD	Méthode HTTP utilisée dans la demande.
-	URL	Contenu de l'en-tête de l'URL.
-	URLTOKENS	Jetons d'URL dans l'en-tête HTTP.
-	VERSION	Version HTTP de la connexion.
-	HEADER	Partie d'en-tête de la requête HTTP.
-	URLLEN	Longueur du contenu de l'en-tête de l'URL.
-	URLQUERY	Partie de requête du contenu de l'en-tête de l'URL.
-	URLQUERYLEN	Longueur de la partie de requête de l'en-tête de l'URL.

Protocole	Qualificatif	Définition
SSL	CLIENT.CERT	Certificat client SSL dans son ensemble.
-	CLIENT.CERT.SUBJECT	Contenu du champ Objet du certificat client.
-	CLIENT.CERT.ISSUER	Émetteur de certificat client.
-	CLIENT.CERT.SIGALGO	Algorithme de signature utilisé dans le certificat client.
-	CLIENT.CERT.VERSION	Version du certificat client.
-	CLIENT.CERT.VALIDFROM	Date à partir de laquelle le certificat client est valide. (La date de début.)
-	CLIENT.CERT.VALIDE POUR	Date après laquelle le certificat client n'est plus valide. (La date de fin.)
-	NUMÉRO DE SÉRIE CLIENT.CERT.SERIALNUMBER	Numéro de série du certificat client.
-	CLIENT.CIPHER.TYPE	Méthode de chiffrement utilisée dans le certificat client.
-	CLIENT.CIPHER.BITS	Nombre de bits significatifs dans la clé de chiffrement.
-	CLIENT.SSL.VERSION	Version SSL du certificat client.
TCP	SOURCEPORT	Port source de la connexion TCP.
-	DESTPORT	Port de destination de la connexion TCP.
-	MSS	Taille de segment maximale (MSS) de la connexion TCP.
IP	SOURCEIP	Adresse IP source de la connexion.
-	DESTIP	Adresse IP de destination de la connexion.

11. Sélectionnez l'opérateur de votre expression dans la liste déroulante Opérateur.

    Vos choix dépendent du qualificatif choisi à l'étape précédente. La liste complète des opérateurs pouvant apparaître dans cette liste déroulante est la suivante :

    - == . Correspond exactement à la chaîne de texte suivante.
    - != . Ne correspond pas à la chaîne de texte suivante.
      - . Est supérieur au nombre entier suivant.
    - CONTAINS . Contient la chaîne de texte suivante.
    - CONTENTS . Le contenu de l'en-tête, de l'URL ou de la requête URL désignés.
    - EXISTS . L'en-tête ou la requête spécifiés existe.
    - NOTCONTAINS . Ne contient pas la chaîne de texte suivante.
    - NOTEXISTS . L'en-tête ou la requête spécifiés n'existe pas.

    Si vous souhaitez que cette stratégie s'applique aux demandes envoyées à un hôte spécifique, vous pouvez laisser le signe par défaut, le signe égal (==).

12. Si la zone de texte Valeur est visible, tapez la chaîne ou le nombre approprié dans la zone de texte.

    Par exemple, si vous souhaitez que cette stratégie sélectionne les demandes envoyées à l'hôte shopping.example.com, vous devez taper cette chaîne dans la zone de texte Valeur.

13. Si vous avez choisi HEADER comme qualificatif, tapez l'en-tête souhaité dans la zone de texte Header Name (Nom de l'en-tête).

14. Cliquez sur **OK** pour ajouter votre expression à la liste Expression.

15. Répétez les étapes 4 à 11 pour créer d'autres expressions.

16. Cliquez sur **Fermer** pour fermer la boîte de dialogue Ajouter une expression et revenir à la boîte de dialogue **Créer une stratégie de redirection de cache** .

17. Lorsque vous avez fini de saisir l'expression, cliquez sur **Créer**.

Configurations de redirection du cache

May 5, 2023

En fonction de votre déploiement et de la topologie de votre réseau, vous pouvez configurer l'un des types de redirection de cache suivants :

- **Transparent**. Un cache transparent peut résider sur différents points le long d'une dorsale réseau afin de réduire le trafic le long de l'itinéraire de livraison. En mode transparent, le serveur virtuel de redirection du cache intercepte tout le trafic acheminé vers l'appliance NetScaler et applique des politiques de redirection du cache pour déterminer si le contenu doit être diffusé depuis le cache ou depuis le serveur d'origine.
- **Proxy de transfert**. Un serveur de cache proxy direct se trouve à la périphérie d'un réseau local d'entreprise et fait face au WAN. En mode proxy de transfert, le serveur virtuel de redirection du cache résout le nom d'hôte de la demande entrante à l'aide d'un serveur DNS et transmet les demandes de contenu ne pouvant pas être mis en cache aux serveurs d'origine résolus. Les demandes pouvant être mises en cache sont envoyées aux serveurs de cache configurés.
- **Proxy inversé**. Les caches de proxy inversé sont configurés pour des serveurs d'origine spécifiques. Le trafic entrant dirigé vers le proxy inverse peut être diffusé depuis un serveur de cache ou envoyé au serveur d'origine avec ou sans modification de l'URL.

Configurer la redirection transparente

May 5, 2023

Lorsque vous configurez la redirection transparente du cache, l'appliance NetScaler évalue tout le trafic qu'elle reçoit afin de déterminer s'il peut être mis en cache. Ce mode réduit le trafic le long de l'itinéraire de livraison et est souvent utilisé lorsque le serveur de cache se trouve sur le backbone d'un fournisseur de services Internet ou d'un opérateur.

Par défaut, les demandes pouvant être mises en cache sont envoyées à un serveur de cache et les demandes ne pouvant pas être mises en cache sont envoyées au serveur d'origine. Par exemple, lorsque l'appliance NetScaler reçoit une demande dirigée vers un serveur Web, elle compare les en-têtes HTTP de la demande à un ensemble d'expressions de politique. Si la demande ne correspond pas à la politique, l'appliance transmet la demande à un serveur de cache. Si la demande correspond à une stratégie, l'appliance transmet la demande, inchangée, au serveur Web.

Pour plus d'informations sur la façon de modifier ce comportement par défaut, voir Accès direct à la stratégie vers le cache plutôt que vers l'origine.

Pour configurer la redirection transparente, activez d'abord la redirection du cache et l'équilibrage de charge, puis configurez le mode Edge. Créez ensuite un serveur virtuel de redirection du cache avec une adresse IP générique (*), afin que ce serveur virtuel puisse recevoir le trafic en provenance de l'appliance sur n'importe quelle adresse IP que l'appliance possède. Liez à ce serveur virtuel les politiques de redirection du cache qui décrivent les types de demandes qui ne doivent pas être mises en cache. Créez ensuite un serveur virtuel d'équilibrage de charge qui recevra le trafic du serveur virtuel de redirection du cache pour les demandes pouvant être mises en cache. Enfin, créez un service qui représente un serveur de cache physique et liez-le au serveur virtuel d'équilibrage de charge.

Activer la redirection du cache et l'équilibrage de charge

October 5, 2021

Les fonctionnalités de redirection du cache et d'équilibrage de charge de l'appliance ne sont pas activées par défaut. Ils doivent être activés avant que toute configuration de redirection de cache puisse prendre effet.

Activer la redirection du cache et l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer la redirection du cache et l'équilibrage de charge, puis vérifiez les paramètres :

```
1 -  enable ns feature cr lb
2 -  show ns feature
3 <!--NeedCopy-->
```


Exemple :

```
> enable ns feature cr lb
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 4)     Content Switching               CS                  ON
 5)     Cache Redirection               CR                  ON
            ...
            ...
            ...

 23)    appliance Push                  push                OFF
 Done
<!--NeedCopy-->
```

Activer la redirection du cache et l'équilibrage de charge à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Pour activer la redirection du cache, dans le volet d'informations, sous **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.
   a) Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, cochez la case en regard de la **redirection du cache**, puis cliquez sur **OK**.
   b) Dans Activer/Désactiver les fonctionnalités ? , cliquez sur Oui.
3. Pour activer l'équilibrage de charge, dans le volet d'informations, sous **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités de base**.
   a) Dans la boîte de dialogue **Configurer les fonctionnalités de base**, cochez la case en regard de l'équilibrage de charge, puis cliquez sur **OK**.
   b) Dans Activer/Désactiver les fonctionnalités ? , cliquez sur Oui.

Configurer le mode Edge

May 5, 2023

Lorsqu'elle est déployée à la périphérie d'un réseau, l'appliance NetScaler apprend dynamiquement à connaître les serveurs de ce réseau. Le mode Edge permet à l'appliance de connaître dynamiquement jusqu'à 40 000 serveurs HTTP et les connexions TCP proxy pour ces serveurs.

Ce mode active la collecte de statistiques pour les services appris dynamiquement et est généralement utilisé dans les déploiements transparents pour la redirection du cache.

Activer le mode Edge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer le mode Edge et vérifier le paramètre :

```
-  enable ns mode Edge
-  show ns mode
<!--NeedCopy-->
```

Exemple :

```
> enable ns mode edge
 Done

> show ns mode

        Mode                          Acronym             Status
        -------                       -------             ------
          ...
          ...
          ...
 6)     MAC-based forwarding          MBF                 ON
 7)     Edge configuration            Edge                ON
 8)     Use Subnet IP                 USNIP               OFF
          ...
          ...
          ...
 16)    Bridge BPDUs                  BridgeBPDUs         OFF
 Done
<!--NeedCopy-->
```

Activer le mode Edge à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, puis cliquez sur Paramètres.
2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur Configurer les modes.
3. Dans la boîte de dialogue Configurer les modes, cochez la case à côté de la configuration Edge, puis cliquez sur OK.

4. Dans Activer/Désactiver la ou les fonctions ?, cliquez sur Oui.

Configurer un serveur virtuel de redirection de cache

August 20, 2021

Par défaut, un serveur virtuel de redirection de cache transfère les demandes pouvant être mises en cache au serveur virtuel d'équilibrage de charge pour le cache, et transfère les demandes non mises en cache au serveur d'origine (sauf dans une configuration de proxy inverse, dans laquelle les demandes non mises en cache sont envoyées à un serveur virtuel d'équilibrage de charge). Il existe trois types de serveurs virtuels de redirection de cache : transparents, proxy de transfert et proxy inverse.

Un serveur virtuel de redirection de cache transparent utilise une adresse IP de * et un numéro de port, généralement 80, qui peuvent accepter le trafic HTTP envoyé à n'importe quelle adresse IP que représente l'appliance. Par conséquent, vous ne pouvez configurer qu'un seul serveur virtuel de redirection de cache transparent. Tous les serveurs virtuels de redirection de cache supplémentaires que vous configurez doivent être des serveurs proxy de transfert ou de redirection de proxy inverse.

ajouter un serveur virtuel de redirection de cache en mode transparent à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un serveur virtuel de redirection de cache et vérifier la configuration :

```
1 - add cr vserver <name> <serviceType> [<IPAddress> <port> ] [-
    cacheType <cacheType>] [-redirect <redirect>]
2 - show cr vserver [<name>]
3 <!--NeedCopy-->
```

Exemple :

```
1 add cr vserver Vserver-CRD-1 HTTP * 80 -cacheType TRANSPARENT -redirect
    POLICY
2 > show cr vserver Vserver-CRD-1
3         Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
4         State: UP  ARP:DISABLED
5         Client Idle Timeout: 180 sec
6         Down state flush: ENABLED
7         Disable Primary Vserver On Down : DISABLED
8         Default:        Content Precedence: RULE        Cache:
              TRANSPARENT
9         On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
```



```
10          Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
11  Done
12 <!--NeedCopy-->
```

Modifier ou supprimer un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

- Pour modifier un serveur virtuel, utilisez la commande set cr vserver, qui ressemble à la commande add cr vserver, sauf que vous entrez le nom d'un serveur virtuel existant.
- Pour supprimer un serveur virtuel, utilisez la commande `rm cr vserver`, qui accepte uniquement l'argument <name>.

Ajouter un serveur virtuel de redirection de cache en mode transparent à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (redirection de cache), spécifiez les valeurs des paramètres suivants comme indiqué :

   - Nom* : nom
   - Port* : port

   *Paramètre obligatoire
4. Dans la liste déroulante Protocole, sélectionnez un protocole pris en charge (par exemple, **HTTP**). Si le serveur virtuel doit recevoir du trafic sur un port autre que le port standard pour le protocole sélectionné, entrez une nouvelle valeur dans le champ Port.
5. Cliquez sur l'onglet Avancé.
6. Vérifiez que Type de cache est défini sur TRANSPARENT et Redirection est défini sur POLICY.
7. Cliquez sur Créer, puis sur Fermer. Le volet Serveurs virtuels de redirection de cache affiche le nouveau serveur virtuel.
8. Sélectionnez le nouveau serveur virtuel de redirection de cache pour afficher les détails de sa configuration.

Lier les stratégies au serveur virtuel de redirection de cache

August 20, 2021

Les stratégies de redirection de cache ne sont pas automatiquement liées au serveur virtuel de redirection de cache. Un serveur virtuel de redirection de cache basé sur une stratégie ne peut pas fonctionner sauf si vous lui liez au moins une stratégie.

Liez des stratégies à un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
-  bind cr vserver <name> -policyName <string>
-  show cr vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
> bind cr vserver Vserver-CRD-1 -policyName bypass-cache-control
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-dynamic-url
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-urltokens
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-cookie
 Done

> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: bypass-dynamic-url
3)      Cache bypass  Policy: bypass-urltokens
4)      Cache bypass  Policy: bypass-cookie
 Done
<!--NeedCopy-->
```


Liez une stratégie définie par l'utilisateur à un serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Cliquez sur le serveur virtuel que vous souhaitez configurer, puis cliquez sur Ouvrir.
3. Sous l'onglet Stratégies, sélectionnez le type de la stratégie, puis cliquez sur Insérer une stratégie.
4. Sous colonne Nom de la stratégie, sélectionnez la stratégie que vous souhaitez lier.
5. Cliquez sur OK.

Délier une stratégie d'un serveur virtuel de redirection de cache

May 5, 2023

Lorsque vous dissociez une politique du serveur virtuel de redirection du cache, l'appliance NetScaler n'applique plus la politique lors de l'évaluation des demandes des clients.

Dissocier une politique d'un serveur virtuel de redirection de cache à l'aide de la commande CLI

À l'invite de commande, tapez :

```
-  unbind cr vserver <name> -policyName <string>
-  show cr vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
unbind cr vserver Vserver-CR-1 -policyName bypass-non-get
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
 Done
```



```
<!--NeedCopy-->
```

Dissocier une politique définie par l'utilisateur d'un serveur virtuel de redirection du cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Cliquez sur le serveur virtuel que vous souhaitez configurer, puis cliquez sur Ouvrir.
3. Dans l'onglet Politiques, sous Nom de la stratégie, sélectionnez la politique que vous souhaitez dissocier.
4. Cliquez sur Dissocier Policy, puis sur OK.

Créer un serveur virtuel d'équilibrage de charge

May 5, 2023

Le serveur virtuel de redirection du cache de l'appliance NetScaler peut envoyer des demandes soit à une batterie de serveurs de cache, si la demande peut être mise en cache, soit à la batterie de serveurs d'origine si la demande ne peut pas être mise en cache.

Chaque serveur de cache est représenté sur l'appliance par un service, qui est lié à un serveur virtuel d'équilibrage de charge qui reçoit les demandes du serveur virtuel de redirection de cache et transfère ces demandes aux serveurs.

Pour plus d'informations sur la configuration des serveurs virtuels d'équilibrage de charge et d'autres options de configuration, voir Équilibrage de charge.

Créer un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel d'équilibrage de charge et vérifier la configuration :

```
-  add lb vserver <name> <serviceType> [<IPAddress>] [<port>]
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
> add lb vserver Vserver-LB-CR HTTP 10.102.20.30 80
 Done
> show lb vserver Vserver-LB-CR
```



```
4          Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
5          State: DOWN
6          Last state change was at Fri Jul  2 08:47:52 2010
7          Time since last state change: 0 days, 00:00:08.470
8          Effective State: DOWN
9          Client Idle Timeout: 180 sec
10         Down state flush: ENABLED
11         Disable Primary Vserver On Down : DISABLED
12         Port Rewrite : DISABLED
13         No. of Bound Services :  0 (Total)       0 (Active)
14         Configured Method: LEASTCONNECTION
15         Mode: IP
16         Persistence: NONE
17         Vserver IP and Port insertion: OFF
18         Push: DISABLED  Push VServer:
19         Push Multi Clients: NO
20         Push Label Rule: none
21  Done
22 <!--NeedCopy-->
```

Création d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants, comme indiqué :

   - Nom*-Nom
   - Adresse IP* - Adresse IP
   - Port*-port

   *Paramètre obligatoire
4. Dans la liste des protocoles, sélectionnez un protocole pris en charge (par exemple, **HTTP**). Si le serveur virtuel doit recevoir du trafic sur un port autre que le port connu pour le protocole sélectionné, entrez une nouvelle valeur dans le champ Port.
5. Cliquez sur Créer, puis sur Fermer. Le volet Serveurs virtuels d'équilibrage de charge affiche le nouveau serveur virtuel.

Configuration d'un service HTTP

May 8, 2023

Sur l'appliance NetScaler, un service représente un serveur physique sur le réseau. Dans la configuration de redirection de cache transparente, le service représente le serveur de cache. Les demandes pouvant être mises en cache sont envoyées par le serveur virtuel de redirection du cache au serveur virtuel d'équilibrage de charge, qui à son tour transmet chaque demande au service approprié, qui la transmet au serveur de cache.

Configuration d'un service HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service HTTP et vérifier la configuration :

```
-  add service <name> <IP> <serviceType> <port> -cacheType <cacheType>
-  show service [<name>]
<!--NeedCopy-->
```

Exemple :

```
> add service Service-HTTP-1 10.102.29.40 HTTP 80 -cacheType
   TRANSPARENT
 Done
> show service Service-HTTP-1
        Service-HTTP-1 (10.102.29.40:80) - HTTP
        State: DOWN
        Last state change was at Fri Jul  2 09:14:17 2010
        Time since last state change: 0 days, 00:00:13.820
        Server Name: 10.102.29.40
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): YES
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
        Cache Type: TRANSPARENT Redirect Mode:
        Cacheable: NO
        SC: OFF
        SP: ON
```



```
22          Down state flush: ENABLED
23
24  1)      Monitor Name: tcp-default
25                  State: DOWN     Weight: 1
26                  Probes: 3       Failed [Total: 3 Current: 3]
27                  Last response: Failure - Time out during TCP connection
                        establishment stage
28                  Response Time: N/A
29   Done
30  <!--NeedCopy-->
```

Modifier ou supprimer un service à l'aide de la CLI

- Pour modifier un service, utilisez la commande set service, qui est similaire à la commande add service, sauf que vous entrez le nom d'un service existant.
- Pour supprimer un service, utilisez la `rm service` commande qui accepte uniquement l' <name> argument \.

Ajouter un service HTTP à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Services
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez des valeurs pour les paramètres suivants, comme indiqué :

   - Nom du service*—Nom
   - Serveur*—IP
   - Port*—port

   *Paramètre obligatoire
4. Dans la liste déroulante Protocole*, sélectionnez un protocole pris en charge (par exemple, **HTTP**).
5. Cliquez sur Créer, puis sur Fermer.

Lier/supprimer la liaison d'un service de/vers un serveur virtuel d'équilibrage de charge

August 20, 2021

Vous devez lier un service au serveur virtuel d'équilibrage de charge. Cela permet à l'équilibreur de charge de transférer la demande au serveur représenté par le service. Si votre configuration change, vous pouvez dissocier un service du serveur virtuel d'équilibrage de charge.

Liez un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
-  bind lb vserver <name> <serviceName>
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
> bind lb vserver vserver-LB-CR service-HTTP-1
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:42:25.610
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
 Done
<!--NeedCopy-->
```


Dissocier un service d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

Pour dissocier un service, utilisez la commande `unbind lb vserver` au lieu de `bind lb vserver`.

Lier/dissocier un service à partir d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels
2. Dans le volet d'informations, sélectionnez le serveur virtuel à partir duquel vous souhaitez lier/dissocier le service, puis cliquez sur Ouvrir.
3. Sous l'onglet Services, dans la colonne Actif, coche/désactivez la case à cocher en regard du nom du service.
4. Cliquez sur OK.

Désactivez le paramètre Utiliser le port proxy pour une mise en cache transparente

May 5, 2023

Si l'option Utiliser l'adresse IP source (USIP) est désactivée sur un service de cache configuré sur l'appliance NetScaler, l'appliance transmet les demandes des clients au service de cache en utilisant une adresse IP de sous-réseau appartenant à l'appliance (SNIP) ou une adresse IP mappée (MIP) comme adresse IP source et un port aléatoire comme port source. Le port sélectionné aléatoirement est appelé port proxy.

Toutefois, si vous souhaitez configurer un cache totalement transparent (une configuration de cache dans laquelle le service de cache reçoit l'adresse IP et le numéro de port du client), vous devez non seulement activer l'option USIP, soit globalement, soit sur le service de cache, mais également désactiver le paramètre Utiliser le port proxy, soit globalement, soit sur le service de cache. La désactivation du paramètre Utiliser le port proxy permet à l'appliance d'utiliser le port source du client comme port source lorsqu'elle se connecte au service de cache et garantit une configuration entièrement transparente du cache.

Pour plus d'informations sur la configuration de l'option Utiliser le port proxy globalement ou sur un service, consultez Configuration du port source pour les connexions côté serveur.

Attribuer une plage de ports à l'appliance NetScaler

May 5, 2023

Le partage de l'adresse IP du client peut créer un conflit empêchant les périphériques réseau, tels que les routeurs, les serveurs de cache, les serveurs d'origine et les autres appliances NetScaler, de déterminer l'appliance, et donc le client, auquel la réponse doit être envoyée.

Une méthode pour résoudre ce problème consiste à attribuer une plage de ports source à l'appliance NetScaler. Cette allocation permet aux périphériques réseau d'identifier sans ambiguïté l'appliance NetScaler qui a envoyé la demande.

Attribuez une plage de ports source à une appliance NetScaler à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ns param -crPortRange <startPortNumber-endPortNumber>
```

Attribuez une plage de ports source à une appliance NetScaler à l'aide de l'interface graphique de l'appliance

1. Dans le volet de navigation, cliquez sur Système, puis sur Paramètres.
2. Dans le groupe Paramètres, cliquez sur le lien Modifier les paramètres généraux du système.
3. Dans le groupe Plage de ports de redirection du cache, spécifiez la plage de ports de l'appliance en saisissant un numéro de port pour le port de départ et un numéro de port pour le port de fin.
4. Cliquez sur OK.

Activer les serveurs virtuels d'équilibrage de charge pour rediriger les demandes vers le cache

May 5, 2023

Si un serveur virtuel d'équilibrage de charge est configuré pour écouter sur une combinaison d'adresses IP et de ports particulière, il a la priorité sur le serveur virtuel de redirection du cache pour toutes les demandes destinées à cette combinaison adresse-port. Par conséquent, le serveur virtuel de redirection du cache ne traite pas ces demandes.

Si vous souhaitez remplacer cette fonctionnalité et laisser le serveur virtuel de redirection du cache décider si la demande doit être traitée à partir du cache ou non, configurez le serveur virtuel d'équilibrage de charge spécifique pour qu'il puisse être mis en cache.

Une telle configuration est généralement utilisée lorsqu'un fournisseur d'accès Internet utilise une appliance NetScaler à la périphérie de son réseau et que tout le trafic passe par l'appliance.

Activez les serveurs virtuels d'équilibrage de charge pour rediriger les demandes vers le cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
-  set lb vserver <name> [-cacheable ( YES | NO)]
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-CR  - cacheable YES
> show lb vserver vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 01:05:51.510
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Cacheable: YES  PQ: OFF SC: OFF
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
 Done
<!--NeedCopy-->
```

Pour une redirection transparente du cache, l'appliance intercepte tout le trafic et évalue chaque demande pour déterminer si elle peut être mise en cache. Les demandes ne pouvant pas être mises en cache sont envoyées telles quelles au serveur d'origine.

Lorsque vous utilisez la redirection transparente du cache, vous pouvez désactiver la redirection du

cache pour les serveurs virtuels d'équilibrage de charge qui dirigent toujours le trafic vers les serveurs d'origine.

Désactiver la mise en cache pour un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

Pour désactiver la mise en cache d'un système virtuel d'équilibrage de charge, utilisez la commande unset lb vserver au lieu de set lb vserver. Spécifiez la valeur NO pour le paramètre **pouvant être mis en cache** .

Activer ou désactiver les serveurs virtuels d'équilibrage de charge pour rediriger les demandes vers le cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet de détails, sélectionnez le serveur virtuel à partir duquel vous souhaitez activer/désactiver la mise en cache, puis cliquez sur Ouvrir.
3. Dans l'onglet Avancé, cochez/désactivez la case Redirection du cache.
4. Cliquez sur OK.

Configurer la redirection du proxy direct

May 5, 2023

Un proxy direct est un point de contact unique pour un client ou un groupe de clients. Dans cette configuration, l'appliance NetScaler redirige les demandes ne pouvant pas être mises en cache vers un serveur d'origine et redirige les demandes pouvant être mises en cache vers un cache proxy direct ou un cache transparent.

Lorsque l'appliance est configurée en tant que proxy de transfert, les utilisateurs doivent modifier leur navigateur afin que le navigateur envoie des demandes au proxy de transfert plutôt qu'aux serveurs de destination.

Un serveur virtuel de redirection du cache par proxy direct sur l'appliance compare la demande à une politique de mise en cache. Si la demande ne peut pas être mise en cache, l'appliance interroge un serveur virtuel d'équilibrage de charge DNS pour obtenir la résolution de la destination, puis envoie la demande au serveur d'origine. Si la demande peut être mise en cache, l'appliance transmet la demande à un serveur virtuel d'équilibrage de charge pour le cache.

L'appliance s'appuie sur un nom de domaine hôte ou une adresse IP figurant dans l'en-tête HOST de la demande pour déterminer la destination demandée. Si la demande ne contient aucun en-tête

HOST, l'appliance insère un en-tête HOST en fonction de l'adresse IP de destination figurant dans la demande.

Généralement, l'appliance NetScaler agit comme un proxy de transfert sur un réseau local d'entreprise. Dans une telle configuration, l'appliance se trouve à la périphérie d'un réseau local d'entreprise et intercepte les demandes des clients avant qu'elles ne soient transmises au réseau étendu. La configuration de l'appliance en mode proxy direct réduit le trafic sur le WAN.

Pour configurer la redirection du cache du proxy direct, activez d'abord l'équilibrage de charge et la redirection du cache sur l'appliance. Configurez ensuite un serveur virtuel d'équilibrage de charge DNS et les services associés. Configurez également un serveur virtuel d'équilibrage de charge et liez-y les services appropriés pour le cache. Configurez un serveur virtuel de redirection du cache par proxy direct et liez-y les serveurs virtuels DNS et d'équilibrage de charge. Vous devez également configurer les politiques de mise en cache et les lier au serveur virtuel de redirection du cache. Pour terminer la configuration, configurez les navigateurs clients pour qu'ils utilisent le proxy de transfert.

Pour plus d'informations sur la façon d'activer la redirection du cache et l'équilibrage de charge sur l'appliance, voir Activer la redirection du cache et l'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur virtuel d'équilibrage de charge, voir Créer un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la configuration des services représentant le serveur de cache, voir Configurer un service HTTP.

Pour plus d'informations sur la façon de lier le service à un serveur virtuel, voir Lier/dissocier un service vers/depuis un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur de redirection de cache proxy de transfert, consultez Configurer un serveur virtuel de redirection de cacheet créer un serveur virtuel de type TRANSPARENT ou FORWARD.

Pour plus d'informations sur la liaison des stratégies de redirection du cache au serveur virtuel de redirection du cache, voir Configurer une stratégie de redirection de cache.

Créer un service DNS

May 5, 2023

Un service DNS est une représentation, sur l'appliance NetScaler, d'un serveur DNS physique du réseau. Un serveur virtuel d'équilibrage de charge DNS envoie des requêtes DNS au serveur DNS du réseau via un tel service.

Création d'un service DNS à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour créer un service DNS et vérifier la configuration :

```
-  add service <name> <IP> <serviceType> <port>
-  show service [<name>]
<!--NeedCopy-->
```

Exemple :

```
add service Service-DNS-1 10.102.29.41 DNS 53
show service Service-DNS-1
        Service-DNS-1 (10.102.29.41:53) - DNS
        State: DOWN
        Last state change was at Fri Jul  2 10:14:32 2010
        Time since last state change: 0 days, 00:00:13.550
        Server Name: 10.102.29.41
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping-default
                State: DOWN     Weight: 1
                Probes: 3       Failed [Total: 3 Current: 3]
                Last response: Failure - Probe timed out.
                Response Time: 2000.0 millisec
 Done
<!--NeedCopy-->
```

Ajouter un service DNS à l'aide de l'interface graphique

1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans le volet de détails, cliquez sur Ajouter.

3. Dans la boîte de dialogue Créer un service, spécifiez des valeurs pour les paramètres suivants, comme indiqué :
    - Nom du service*—Nom
    - Serveur*—IP
    - Port*—port

*Paramètre obligatoire

1. Dans la liste déroulante Protocole*, sélectionnez un protocole pris en charge (par exemple, **DNS**).
2. Cliquez sur Créer, puis sur Fermer.

Créer un serveur virtuel d'équilibrage de charge DNS

August 20, 2021

Le serveur virtuel DNS permet au proxy de transfert d'effectuer la résolution DNS avant de transférer une demande client à un serveur d'origine. Le serveur virtuel d'équilibrage de charge DNS est associé au service DNS qui représente le serveur DNS physique sur le réseau.

Créer un serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour créer un serveur virtuel d'équilibrage de charge DNS et vérifier la configuration :

```
-  add lb vserver <name> <serviceType>
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
> add lb vserver Vserver-DNS-1 DNS
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:00:08.10
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
```



```
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
 Done
<!--NeedCopy-->
```

Créer un serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), dans la zone Nom, tapez un nom pour le serveur virtuel.
4. Dans la liste déroulante Protocol*, sélectionnez un protocole pris en charge (par exemple, **DNS**).
5. Cliquez sur Créer, puis sur Fermer. Le volet Serveurs virtuels DNS affiche le nouveau serveur virtuel.

Lier le service DNS au serveur virtuel

August 20, 2021

Pour que le serveur DNS réponde aux demandes DNS, le service représentant le serveur DNS doit être lié au serveur virtuel DNS.

Liez le service DNS au serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier le service DNS au serveur virtuel d'équilibrage de charge et vérifiez la configuration :

```
-  bind lb vserver <name> <serviceName>
-  show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind lb vserver Vserver-DNS-1 Service-DNS-1
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
```



```
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:12:16.80
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE

1) Service-DNS-1 (10.102.29.41: 53) - DNS State: DOWN   Weight: 1
 Done
>
<!--NeedCopy-->
```

Dissocier un service DNS du serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

Utilisez la commande `unbind lb vserver` au lieu de `bind lb vserver`.

Lier/supprimer la liaison d'un service DNS de/vers un serveur virtuel d'équilibrage de charge à partir de l'interface

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels
2. Dans le volet d'informations, sélectionnez le serveur virtuel vers/à partir duquel vous souhaitez lier/dissocier le service DNS, puis cliquez sur Ouvrir.
3. Sous l'onglet Services, dans la colonne Actif, coche/désactivez la case à cocher en regard du nom du service.
4. Cliquez sur OK.

Configurer un navigateur Web client pour utiliser un proxy de transfert

May 5, 2023

Lorsque vous configurez l'appliance NetScaler en tant que serveur virtuel de redirection du cache du proxy direct sur le réseau, vous devez configurer le navigateur Web du client pour qu'il envoie des demandes au proxy de transfert. Généralement, lorsque vous utilisez un proxy de transfert, la seule route vers les serveurs du réseau passe par le proxy de transfert.

Reportez-vous à la documentation de votre navigateur pour configurer le navigateur afin qu'il utilise un proxy de transfert. Spécifiez l'adresse IP et le numéro de port du serveur virtuel de redirection du cache du proxy direct pour cette configuration.

Configurer la redirection de proxy inverse

February 27, 2023

Un proxy inverse se trouve devant un ou plusieurs serveurs Web et protège le serveur d'origine des demandes des clients. Souvent, un cache proxy inverse est une interface pour toutes les demandes des clients adressées à un serveur. Un administrateur affecte un cache proxy inverse à un serveur d'origine spécifique. Le cache proxy inverse est différent des caches proxy transparents et transparents, qui mettent en cache le contenu fréquemment demandé pour toutes les demandes adressées à n'importe quel serveur d'origine, et le choix d'un serveur est basé sur la demande.

Contrairement à un cache de proxy transparent, le cache de proxy inverse a sa propre adresse IP et peut remplacer les domaines et URL de destination dans une requête non mise en cache par de nouveaux domaines et URL de destination.

Vous pouvez déployer la redirection inverse du cache proxy côté serveur d'origine ou à la périphérie d'un réseau. Lorsqu'il est déployé sur le serveur d'origine, le serveur virtuel de redirection du cache proxy inverse est une interface pour toutes les demandes adressées au serveur d'origine.

En mode proxy inverse, lorsque l'appliance reçoit une demande, le serveur virtuel de redirection du cache évalue la demande et la transmet soit à un serveur virtuel d'équilibrage de charge pour le cache, soit à un serveur virtuel d'équilibrage de charge pour l'origine. La demande entrante peut être transformée en modifiant l'en-tête ou l'URL de l'hôte avant d'être envoyée au serveur principal.

Pour configurer la redirection du cache proxy inverse, activez d'abord la redirection du cache et l'équilibrage de charge. Configurez ensuite un serveur virtuel et des services d'équilibrage de charge pour envoyer des demandes pouvant être mises en cache aux serveurs de cache. Configurez également un serveur virtuel d'équilibrage de charge et les services associés pour les serveurs d'origine. Configurez ensuite un serveur virtuel de redirection de cache par proxy inverse et associez-y les politiques de redirection de cache pertinentes. Enfin, configurez les politiques de mappage et liez-les au serveur virtuel de redirection du cache proxy inverse.

Les politiques de mappage sont associées à une action qui permet au serveur virtuel de redirection du cache de transmettre toute demande ne pouvant pas être mise en cache au serveur virtuel d'équilibrage de charge pour l'origine.

Assurez-vous de créer la destination du serveur de cache par défaut.

Pour plus d'informations sur la façon d'activer la redirection du cache et l'équilibrage de charge sur l'appliance, voir Activer la redirection du cache et l'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur virtuel d'équilibrage de charge, voir Créer un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la configuration des services représentant le serveur de cache, voir Configurer un service HTTP.

Pour plus d'informations sur la façon de lier le service à un serveur virtuel, voir Lier/dissocier un service vers/depuis un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur de redirection de cache proxy inverse, voir Configurer un serveur virtuel de redirection de cacheet créer un serveur virtuel de type REVERSE.

Pour plus d'informations sur la liaison des stratégies de redirection de cache intégrées au serveur virtuel de redirection du cache, voir Lier les stratégies au serveur virtuel de redirection du cache.

Configurer les stratégies de mappage

Si une demande entrante ne peut pas être mise en cache, le serveur virtuel de redirection de cache par proxy inverse remplace le domaine et l'URL de la demande par le domaine et l'URL d'un serveur d'origine cible et transmet la demande au serveur virtuel d'équilibrage de charge de l'origine.

Une politique de mappage permet au serveur virtuel de redirection du cache proxy inverse de remplacer le domaine et l'URL de destination et de transmettre la demande au serveur virtuel d'équilibrage de charge pour l'origine.

Une politique de mappage doit d'abord traduire le domaine et l'URL, puis transmettre la demande au serveur virtuel d'équilibrage de charge d'origine.

Une politique de mappage peut mapper un domaine, un préfixe d'URL et un suffixe d'URL, comme suit :

- Mappage de domaines : vous pouvez mapper un domaine sans préfixe ni suffixe. Le mappage de domaine est le mappage par défaut pour le serveur virtuel (par exemple, le mappage de www.mycompany.com à www.myrealcompany.com).
- Mappage de préfixes : vous pouvez remplacer un modèle spécifié préfixé dans le cadre de l'URL (par exemple, en mappant www.mycompany.com/sports/index.html à www.mycompany.com/news/index.h
- Mappage des suffixes : vous pouvez remplacer le suffixe du fichier dans l'URL (par exemple, en mappant www.mycompany.com/sports/index.html à www.mycompany.com/sports/index.asp).

Les chaînes source et destination mappées doivent être similaires. Si vous spécifiez un domaine source, vous devez spécifier un domaine de destination, et si vous spécifiez un suffixe source, vous devez spécifier un suffixe de destination. De même, si vous spécifiez une URL exacte à partir de la source, l'URL cible doit également être une URL exacte.

Une fois que vous avez configuré les politiques de mappage pour le mode proxy inverse, vous devez les lier au serveur virtuel de redirection du cache.

Vous pouvez utiliser des combinaisons d'URL source, d'URL cible et de domaines source et cible pour configurer les trois types de mappage de domaines.

Configurer une politique de mappage pour le mode proxy inverse à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour ajouter une carte des politiques et vérifier la configuration :

```
1 -  add policy map <mapPolicyName> -sd <string> [-su <string>] [-td <
     string>] [-tu <string>]
2 -  show policy map [<mapPolicyName>]
3 <!--NeedCopy-->
```

Exemple :

La commande suivante mappe un domaine figurant dans une demande client à un domaine cible :

```
1 > add policy map myMappingPolicy -sd www.mycompany.com -td www.
     myrealcompany.com
2  Done
3 > show policy map myMappingPolicy
4 1)      Name: myMappingPolicy
5         Source Domain: www.mycompany.com        Source Url:
6         Target Domain: www.myrealcompany.com    Target Url:
7  Done
8 <!--NeedCopy-->
```

Voici un exemple de mappage d'un suffixe d'URL à un suffixe d'URL différent :

```
1 > add policy map myOtherMappingPolicy -sd www.mycompany.com -td www.
     myrealcompany.com -su /news.html -tu /realnews.html
2  Done
3 > show policy map myOtherMappingPolicy
4 1)      Name: myOtherMappingPolicy
5         Source Domain: www.mycompany.com        Source Url: /news.html
6         Target Domain: www.myrealcompany.com    Target Url: /realnews.
             html
7  Done
8 <!--NeedCopy-->
```


Configurer une politique de mappage pour le mode proxy inverse à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Stratégies de carte**.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer une politique cartographique, spécifiez les valeurs des paramètres suivants, comme indiqué :
   - Nom*- MapPolicyName
   - Domaine source*-SD
   - Domaine cible*-td
   - URL de la source : SU
   - URL cible

   *Paramètre obligatoire
4. Cliquez sur Créer, puis sur Fermer. La fenêtre Carte affiche la nouvelle politique de mappage.

Liez la politique de mappage au serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier la politique de mappage au serveur virtuel de redirection du cache et vérifier la configuration :

```
-  bind cr vserver <name> -policyName <string> [<targetVserver>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> bind cr vserver Vserver-CRD-3 -policyName myMappingPolicy Vserver-LB-
    CR
 Done
> show cr vserver Vserver-CRD-3
        Vserver-CRD-3 (10.102.29.50:88) - HTTP  Type: CONTENT
        State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default: Vserver-LB-CR  Content Precedence: RULE        Cache:
           REVERSE
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

```



```
1)      Policy:         Target: Vserver-LB-CR   Priority: 0     Hits: 0
1)      Map: myMappingPolicy Target: Vserver-LB-CR
 Done
<!--NeedCopy-->
```

Liez la politique de mappage au serveur virtuel de redirection du cache à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel à partir duquel vous souhaitez lier la stratégie de mappage, puis cliquez sur **Ouvrir**.
3. Dans **Configurer le serveur virtuel**(redirection du cache), sous **l'onglet Stratégies**, sélectionnez **Carte**, puis cliquez sur **Insérer une stratégie**.
4. Dans la colonne **Nom de la stratégie**, sélectionnez la stratégie dans la liste déroulante.
5. Dans la colonne **Target**, cliquez sur la flèche vers le bas, puis sélectionnez le serveur virtuel dans la liste déroulante.
6. Cliquez sur **OK**.

Redirection sélective du cache

May 5, 2023

La redirection sélective du cache envoie des demandes pour des types de contenu particuliers, par exemple des images, à un serveur de cache ou à un groupe de serveurs de cache et envoie d'autres types de contenu à un autre serveur de cache ou groupe de serveurs de cache. Vous pouvez configurer la redirection avancée du cache en mode transparent, proxy inverse ou proxy direct.

Dans le cadre de la redirection sélective du cache, l'appliance NetScaler intercepte une demande client et transmet les demandes ne pouvant pas être mises en cache vers la destination d'origine de la demande client. Pour les demandes pouvant être mises en cache, l'appliance envoie les demandes au serveur de cache de destination qui peut servir du contenu d'un type de contenu spécifique.

La redirection sélective du cache implique la configuration de politiques de commutation de contenu en plus des politiques de redirection du cache. L'appliance évalue d'abord les politiques de redirection du cache liées au serveur virtuel de redirection du cache. Si une demande correspond à une politique de redirection du cache, le serveur virtuel de redirection du cache envoie la demande au serveur d'origine ou à un serveur virtuel d'équilibrage de charge pour l'origine. Si aucune politique de redirection du cache ne correspond à la demande, l'appliance évalue les politiques de commutation de contenu liées au serveur virtuel de redirection du cache. Si une politique de commutation de

contenu correspond à la demande, le serveur virtuel de redirection du cache redirige la demande vers un serveur virtuel d'équilibrage de charge pour le cache.

Pour configurer la redirection sélective du cache, activez d'abord la redirection du cache, l'équilibrage de charge et la commutation de contenu sur l'appliance NetScaler. Configurez ensuite un serveur virtuel d'équilibrage de charge pour le cache et un service HTTP associé. Ensuite, configurez un serveur virtuel de redirection de cache et liez-y à la fois les politiques de redirection de cache et de commutation de contenu. Une fois que vous avez défini les politiques, vous pouvez configurer le serveur virtuel pour donner la priorité aux politiques de commutation de contenu basées sur des règles ou basées sur des URL.

Lorsqu'elle est configurée pour la redirection du cache en mode transparent dans une topologie de déploiement Edge, l'appliance envoie tout le trafic HTTP pouvant être mis en cache vers une ferme de cache transparente. Les clients accèdent à Internet via l'appliance, qui est configurée comme un commutateur de couche 4 recevant le trafic sur le port 80.

L'appliance peut diriger les demandes d'images (par exemple, les fichiers .png et .jpg) vers un serveur de la batterie de cache transparente, et toutes les autres demandes de contenu statique vers les autres serveurs de la batterie de serveurs. Pour cette configuration, vous configurez des politiques de changement de contenu pour envoyer des images vers le cache d'images et envoyer tous les autres contenus pouvant être mis en cache vers un cache par défaut.

Remarque : La configuration décrite ici concerne la redirection sélective transparente du cache. Par conséquent, il ne nécessite pas de serveur virtuel d'équilibrage de charge pour l'origine, contrairement à une configuration de proxy inverse.

Pour configurer ce type de redirection sélective du cache, activez d'abord la redirection du cache, l'équilibrage de charge et la commutation de contenu. Configurez ensuite un serveur virtuel d'équilibrage de charge pour le cache et configurez un service HTTP associé. Ensuite, configurez un serveur virtuel de redirection de cache et créez et liez les stratégies de redirection de cache et de commutation de contenu à ce serveur virtuel.

Pour plus d'informations sur la façon d'activer la redirection du cache et l'équilibrage de charge sur l'appliance, voir Activer la redirection du cache et l'équilibrage de charge.

Activer la commutation de contenu

October 5, 2021

Pour configurer la redirection sélective du cache, après avoir activé les fonctionnalités d'équilibrage de charge et de redirection du cache sur l'appliance, vous devez activer la commutation de contenu.

Activer la commutation de contenu à l'aide de la CLI

À l'invite de commandes, tapez :

```
- enable ns feature CS

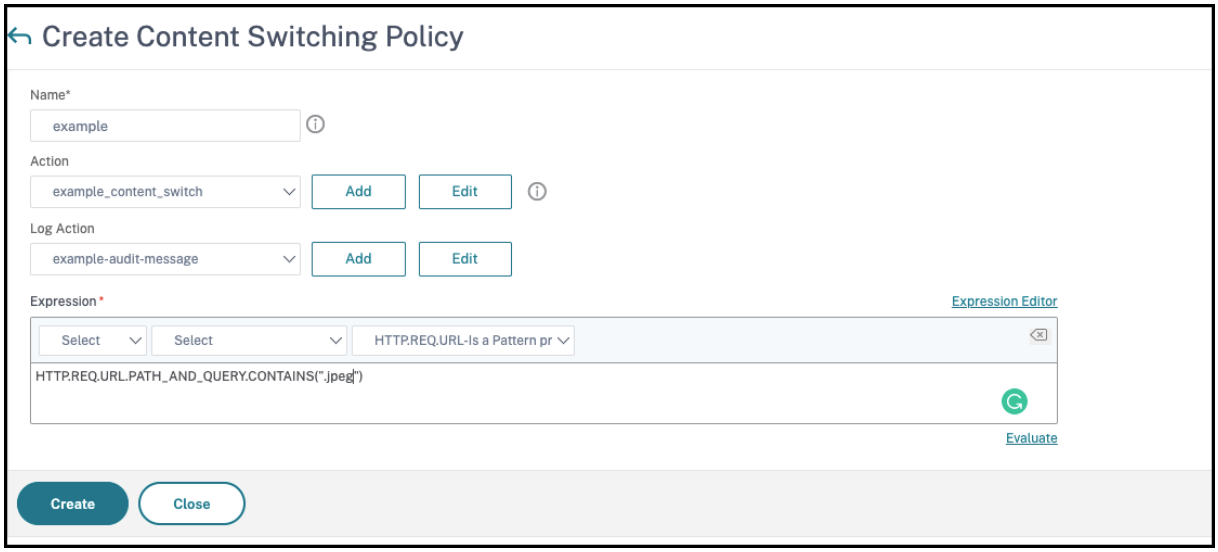
- show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature cs
 Done
> show ns feature

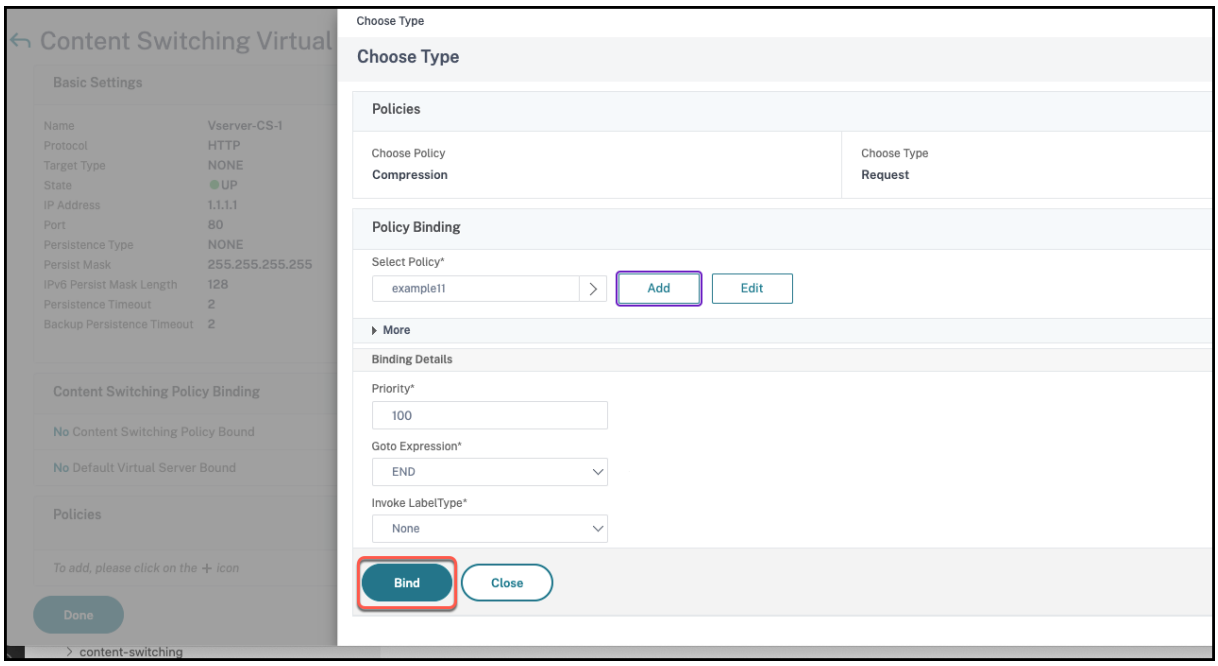
        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 4)     Content Switching               CS                  ON
 5)     Cache Redirection               CR                  ON
          ...
          ...
          ...
 23)    appliance Push                  push                OFF
 Done
<!--NeedCopy-->
```

Activer la redirection du cache et l'équilibrage de charge à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Dans le volet d'informations, sous Modes et fonctionnalités, cliquez sur **Configurer les fonctionnalités de base**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités de base**, cochez la case en regard du **changement de contenu**, puis cliquez sur **OK**.
4. Dans Activer/Désactiver les fonctionnalités ? , cliquez sur Oui.

Configurer un serveur virtuel d'équilibrage de charge pour le cache

May 5, 2023

Créez un serveur virtuel d'équilibrage de charge et un service HTTP pour chaque type de serveur de cache qui sera utilisé. Par exemple, si vous souhaitez diffuser des fichiers JPEG à partir d'un serveur de cache et des fichiers GIF à partir d'un autre serveur de cache, et utiliser un troisième serveur de cache pour le reste du contenu, créez un service HTTP et un serveur virtuel pour chacun des trois types de serveurs de cache. Ensuite, liez chaque service à son serveur virtuel respectif.

Pour plus d'informations sur la création d'un serveur virtuel d'équilibrage de charge, voir Créer un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la configuration des services représentant le serveur de cache, voir Configurer un service HTTP.

Pour plus d'informations sur la façon de lier le service à un serveur virtuel, voir Lier/dissocier un service vers/depuis un serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la création d'un serveur de redirection de cache proxy transparent, voir Configurer un serveur virtuel de redirection de cacheet créer un serveur virtuel de type TRANSPARENT.

Pour plus d'informations sur la liaison des stratégies de redirection de cache intégrées au serveur virtuel de redirection du cache, voir Lier les stratégies au serveur virtuel de redirection du cache.

Configurer une stratégie de redirection de cache pour un type de contenu spécifique

Pour identifier les demandes contenant une extension .png ou .jpeg comme pouvant être mises en cache, vous configurez une politique de redirection du cache et vous la liez au serveur virtuel de redirection du cache.

Remarque : Si une demande correspond à une politique, l'appliance NetScaler la transmet au serveur d'origine. Par conséquent, dans la procédure suivante, vous configurez les stratégies pour qu'elles correspondent aux demandes qui n'ont
pas d'extensions « .png » ou « .jpeg ».

Pour configurer la redirection du cache pour un type de contenu spécifique, configurez une stratégie qui utilise une expression simple, comme décrit dans Configurer une stratégie de redirection de cache.

Configurer les stratégies de commutation de contenu

December 3, 2021

Vous devez créer une stratégie de commutation de contenu pour identifier les types spécifiques de contenu à diriger vers un serveur ou une batterie de serveurs et identifier d'autres types de contenu à diffuser à partir d'un autre serveur de cache ou d'une autre batterie de serveurs. Par exemple, vous

pouvez configurer une stratégie pour déterminer l'emplacement des fichiers image portant les extensions .png et .jpeg.

Avant de créer la stratégie de commutation de contenu, vous devez définir une action de commutation de contenu pour décrire le serveur virtuel d'équilibrage de charge à sélectionner. Cette action est utilisée dans la stratégie de changement de contenu.

Après avoir défini la stratégie de commutation de contenu, vous la liez à un serveur virtuel de commutation de contenu et spécifiez un serveur virtuel d'équilibrage de charge. Les demandes qui correspondent à la stratégie sont transférées vers le serveur virtuel d'équilibrage de charge nommé. Les demandes qui ne correspondent pas à la stratégie de commutation de contenu sont transférées au serveur virtuel d'équilibrage de charge par défaut pour le cache.

Pour plus d'informations sur la fonction de commutation de contenu et la configuration des stratégies de commutation de contenu, voir Commutation de contenu.

Vous devez d'abord créer la stratégie de commutation de contenu, puis la lier au serveur virtuel de commutation de contenu.

Créer une stratégie de commutation de contenu à l'aide de la commande CLI

Sur la ligne de commande, tapez :

```
1 -  add cs action <name> [-targetLBVserver <string> | -targetVserver <
     string> | -targetVserverExpr <expression>]
2 -  add cs policy <policyName> -rule <expression> [-action <string>]
3 -  show cs policy [<policyName>]
4
5 <!--NeedCopy-->
```

Exemples :

```
1  > add cs action action-CS-JPEG -targetLBVserver lbcachejpeg
2  Done
3  > show cs action action-CS-JPEG
4      Name: action-CS-JPEG
5      Target LB Vserver: lbcachejpeg
6      Hits: 0
7      Undef Hits: 0
8      Action Reference Count: 0
9  Done
10
11 > add cs policy policy-CS-JPEG -rule 'HTTP.REQ.URL.SUFFIX == "jpeg"' -
       action action-CS-JPEG
12 Done
```



```
> show cs policy policy-CS-JPEG
    Policy: policy-CS-JPEG Rule: HTTP.REQ.URL.SUFFIX == "jpeg"
    Action: action-CS-JPEG

    HITS: 0
Done
>

> add cs action action-CS-GIF -targetLBVserver lbcachegif
Done
> show cs action action-CS-GIF
    Name: action-CS-GIF
    Target LB Vserver: lbcachegif
    Hits: 0
    Undef Hits: 0
    Action Reference Count: 0

Done
>
> add cs policy policy-CS-GIF -rule 'HTTP.REQ.URL.SUFFIX == "gif"' -
   action action-CS-GIF
Done
> show cs policy policy-CS-GIF
    Policy: policy-CS-GIF Rule: HTTP.REQ.URL.SUFFIX == "gif"
    Action: action-CS-GIF

    Hits: 0
Done
<!--NeedCopy-->
```

Créer une stratégie de changement de contenu basée sur des règles à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Changement de contenu > Stratégies**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une stratégie de commutation de contenu**, dans la zone de texte **Nom**, tapez un nom pour la stratégie.
4. Cliquez sur **Ajouter** dans l'onglet **Action** pour créer une action de changement de contenu. Ou sélectionnez l'action disponible dans la liste déroulante.
    - Saisissez un nom pour le contenu avec action dans l'onglet **Nom** .
    - Choisissez le serveur virtuel ou l'expression dans la liste déroulante :

- **Serveur virtuel d'équilibrage de charge**
- **Serveur virtuel d'équilibrage de charge global du serveur**
- **Serveur virtuel d'authentification**
- **Serveur virtuel NetScalar Gateway**
- **Expression**

• Cliquez sur **Ajouter** ou **modifier** pour configurer le **serveur virtuel d'équilibrage de charge cible**.

5. Cliquez sur **Ajouter** dans l'onglet **Action de journal** pour créer une action de message d'audit. Vous pouvez également sélectionner l'action de message d'audit disponible dans la liste déroulante.
6. Dans la zone **Expression**, sélectionnez le type d'expression requis.
7. Dans la boîte de dialogue **Éditeur d'expression**, choisissez la syntaxe d'expression que vous souhaitez utiliser.

   Dans la zone **Expression**, cliquez sur **Evaluer** pour évaluer un évaluateur d'expression. L'évaluateur évalue l'expression que vous avez saisie pour vérifier sa validité et affiche une analyse de l'effet de l'expression dans la zone de **résultat** .
8. Entrez vos expressions de stratégie.

   Pour plus d'informations sur l'utilisation de la syntaxe avancée, voir Configurer l'expression de stratégie avancée : Commencer.
9. Cliquez sur **Créer**. La stratégie que vous avez créée apparaît dans le volet **Stratégies de changement de contenu** .



Liez la stratégie de commutation de contenu à un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier la stratégie de commutation de contenu à un serveur virtuel de redirection de cache et vérifiez la configuration :

```
-  bind cs vserver <name> (-lbvserver <string> | -vServer <string> (-
    policyName <string> [-targetLBVserver <string>] [-priority<
    positive_integer>] [-gotoPriorityExpression <expression>] [-type <
    type>] [-invoke (<labelType> <labelName>) ] )

-  show cs vserver [<name>]
<!--NeedCopy-->
```

Exemple :

```
> bind cs vserver Vserver-CR-1 -policyName Policy-CS-JPEG -priority 100
 Done
> bind cs vserver Vserver-CR-1 -policyName Policy-CS-GIF -priority 200
 Done
> show cs vserver Vserver-CR-1
        Vserver-CR-1 (10.102.29.60:80) - HTTP   Type: CONTENT
        State: UP
        Last state change was at Fri Jul  2 12:53:45 2010
        Time since last state change: 0 days, 00:00:58.920
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow loggig: ENABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Cacheable: YES
        Vserver IP and Port insertion: OFF
        L2Conn: OFF    Case Sensitivity: ON
        Authentication: OFF
        401 Based Authentication: OFF
        Push: DISABLED  Push VServer:
        Push Label Rule: none
        HTTP Redirect Port: 0    Dtls:  OFF
        Persistence: NONE
        Listen Policy: NONE
        IcmpResponse: PASSIVE
        RHIstate: PASSIVE
        Traffic Domain:  0
```



```
30
31 1)      Content-Switching Policy: Policy-CS-JPEG Priority: 100     Hits
       : 0
32 2)      Content-Switching Policy: Policy-CS-GIF Priority: 200     Hits:
        0
33  Done
34 >
35 <!--NeedCopy-->
```

Liez la stratégie de commutation de contenu à un serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez lier la stratégie (par exemple, **vServer-CS-1**), puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Serveur virtuel de commutation de contenu**, sous **l'onglet Stratégiessous Paramètres avancés**, cliquez sur l'icône**Ajouter**, puis choisissez stratégie et type dans la liste déroulante**Choisir une stratégie**et**choisir un type** .
4. Cliquez sur **Continuer**.
5. Dans l'onglet **Liaison de stratégie**, sélectionnez la stratégie disponible dans la liste, puis cliquez sur **Sélectionner** ou sur **Ajouter** pour créer une nouvelle stratégie, puis cliquez sur **Créer**.
6. Cliquez sur **Lier** pour lier la stratégie de commutation de contenu au serveur virtuel.
7. Cliquez sur **Terminé**



Configurer la priorité pour l'évaluation des stratégies

August 20, 2021

Vous pouvez configurer une stratégie de commutation de contenu en fonction soit d'une règle, qui est une configuration générique pour prendre en charge différents types de contenu, soit d'une URL, plus spécifique et définissant exactement le type de contenu à envoyer à un serveur de cache particulier. Essentiellement, le même contenu peut être défini par une stratégie basée sur des règles ou une stratégie basée sur des URL.

Une fois que vous avez lié des stratégies de commutation de contenu de l'un ou l'autre type à un serveur virtuel de redirection de cache, vous pouvez configurer le serveur virtuel pour donner la priorité aux stratégies basées sur une règle ou une URL. Cela déterminera à son tour les serveurs vers lesquels les requêtes particulières sont dirigées.

Pour configurer la priorité pour l'évaluation de stratégie, utilisez le paramètre de priorité, qui spécifie le type de stratégie (URL ou RULE) qui a priorité sur le serveur virtuel de redirection de contenu.

Valeurs possibles : RULE, URL

Valeur par défaut : RULE

Configurer la priorité pour l'évaluation des stratégies à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la priorité pour l'évaluation des stratégies et vérifier la configuration :

```
-  set cr vserver <name> [-precedence (RULE | URL)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -precedence URL
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
<!--NeedCopy-->
```

Configurer la priorité pour l'évaluation des stratégies à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Changement de contenu > Serveurs virtuels.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la priorité (par exemple, **vServer-CS-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (Commutation de contenu), sous l'onglet Avancé, en regard de Priorité, cliquez sur Règle ou URL, puis cliquez sur OK.

Administrer un serveur virtuel de redirection de cache

January 21, 2021

Pour administrer un serveur virtuel de redirection de cache, vous devez afficher les statistiques de redirection de cache. Vous devrez peut-être activer ou désactiver les serveurs de redirection de cache ou diriger les appels de stratégie vers le cache au lieu de l'origine. Les tâches administratives incluent également la sauvegarde d'un serveur virtuel de redirection de cache et la gestion des connexions client.

Afficher les statistiques de redirection du cache du serveur virtuel

August 20, 2021

Vous pouvez afficher les propriétés d'un serveur virtuel de redirection de cache et les statistiques sur le trafic passé par un serveur virtuel de redirection de cache. Vous pouvez également afficher les serveurs virtuels de redirection de cache et les stratégies que vous avez liés à l'équilibrage de charge des serveurs virtuels.

Pour afficher les statistiques d'un serveur virtuel de redirection de cache spécifique, utilisez le paramètre name pour spécifier le nom du serveur virtuel pour lequel les statistiques seront affichées. Sinon, les statistiques de tous les serveurs virtuels de redirection de cache sont affichées. Longueur maximale : 127

Afficher les statistiques d'un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat cr vserver [<name>]
```

Exemple :

```
1  > stat cr vserver Vserver-CRD-1
2
3  Vserver Summary
4                            IP  port     Protocol        State
5  Vser...CRD-1         0.0.0.0    80         HTTP           UP
6
7  VServer Stats:
8                                          Rate (/s)
                                              Total
9  Requests                                       0
                         0
10 Responses                                      0
                         0
```



```
11 Request bytes                                        0
                          0
12 Response bytes                                       0
                          0
13
14  Done
15 >
16 <!--NeedCopy-->
```

Afficher les statistiques d'un serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez afficher les statistiques (par exemple, **vServer-CRD-1**), puis cliquez sur Statistiques.

omettez le nom du serveur pour afficher les statistiques de base pour tous les serveurs virtuels de redirection de cache. Inclure le nom du serveur pour afficher des statistiques détaillées pour ce serveur virtuel, y compris le nombre et la taille des demandes et des réponses qui passent par le serveur virtuel

Afficher les statistiques d'un serveur virtuel de redirection de cache à l'aide des utilitaires de surveillance et de tableau de bord

1. Pour afficher les statistiques à l'aide des utilitaires de surveillance, cliquez sur l'onglet Surveillance.
2. Dans le menu déroulant Sélectionner un groupe, choisissez Serveurs virtuels CR. Une liste des serveurs virtuels de redirection de cache apparaît.
3. Pour afficher les statistiques à l'aide des utilitaires de tableau de bord, cliquez sur l'onglet Tableau de bord.
4. Cliquez sur Client d'applet ou Client de démarrage Web en regard de l'utilitaire statistique.
5. Dans le menu déroulant Sélectionner un groupe, choisissez Serveurs virtuels CR. Le tableau de bord affiche des statistiques récapitulatives pour les serveurs virtuels de redirection de cache.
6. Pour afficher un graphique de l'activité du serveur virtuel, cliquez sur Graphique. Une représentation graphique des statistiques du serveur virtuel apparaît.

Activer ou désactiver un serveur virtuel de redirection de cache

May 5, 2023

Lorsque vous créez un serveur virtuel de redirection de cache, il est activé par défaut. Si vous désactivez un serveur virtuel de redirection de cache, son état passe à HORS SERVICE et il arrête de rediriger les demandes clients pouvant être mises en cache. Toutefois, l'appliance NetScaler continue de répondre aux demandes ARP et ping pour l'adresse IP de ce serveur virtuel.

Activer ou désactiver un serveur virtuel de redirection de cache à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez l'une des commandes suivantes :

```
-  enable cr vserver <name>
-  show cr vserver <name>
-  disable cr vserver <name>
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemples :

```
> enable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>

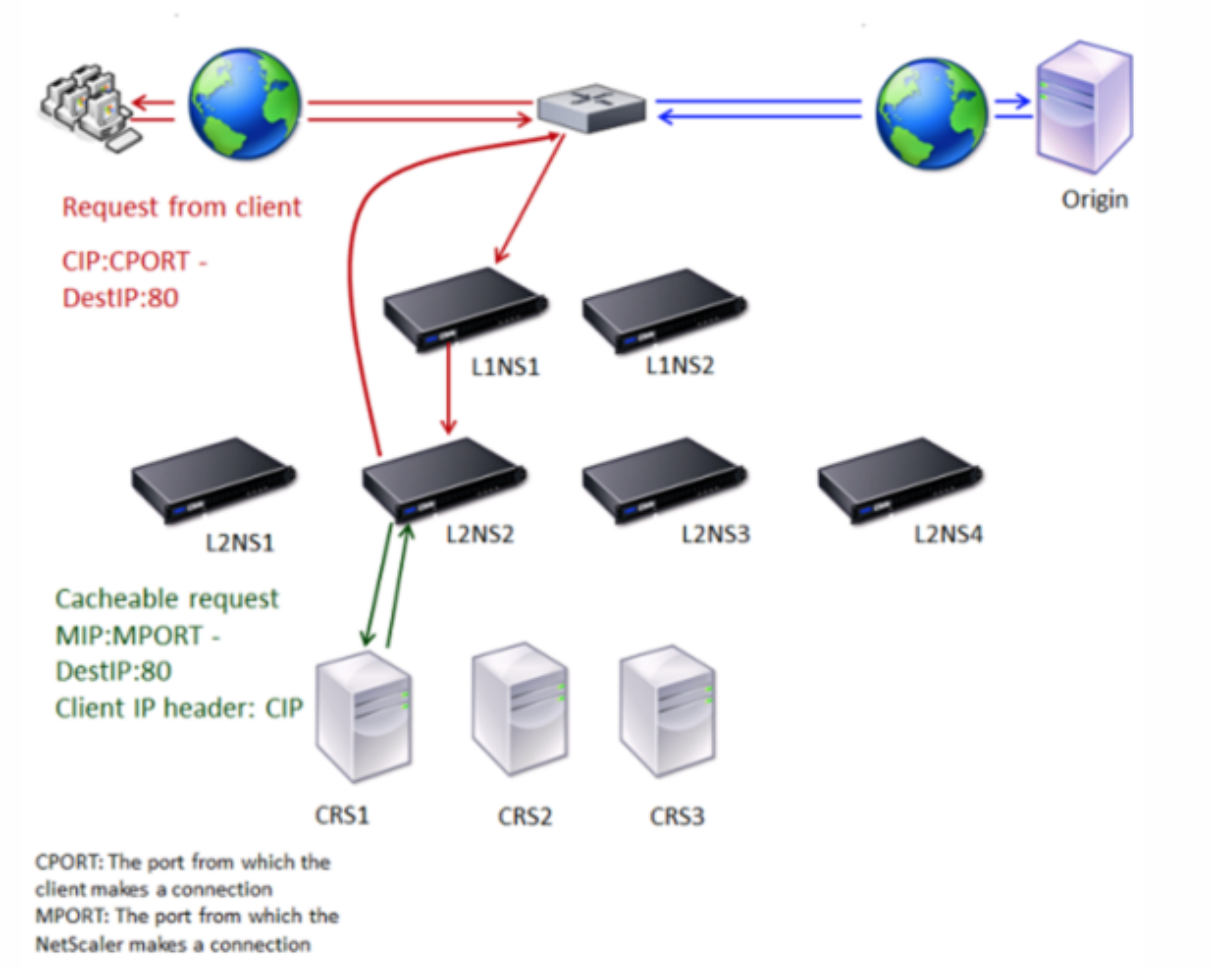
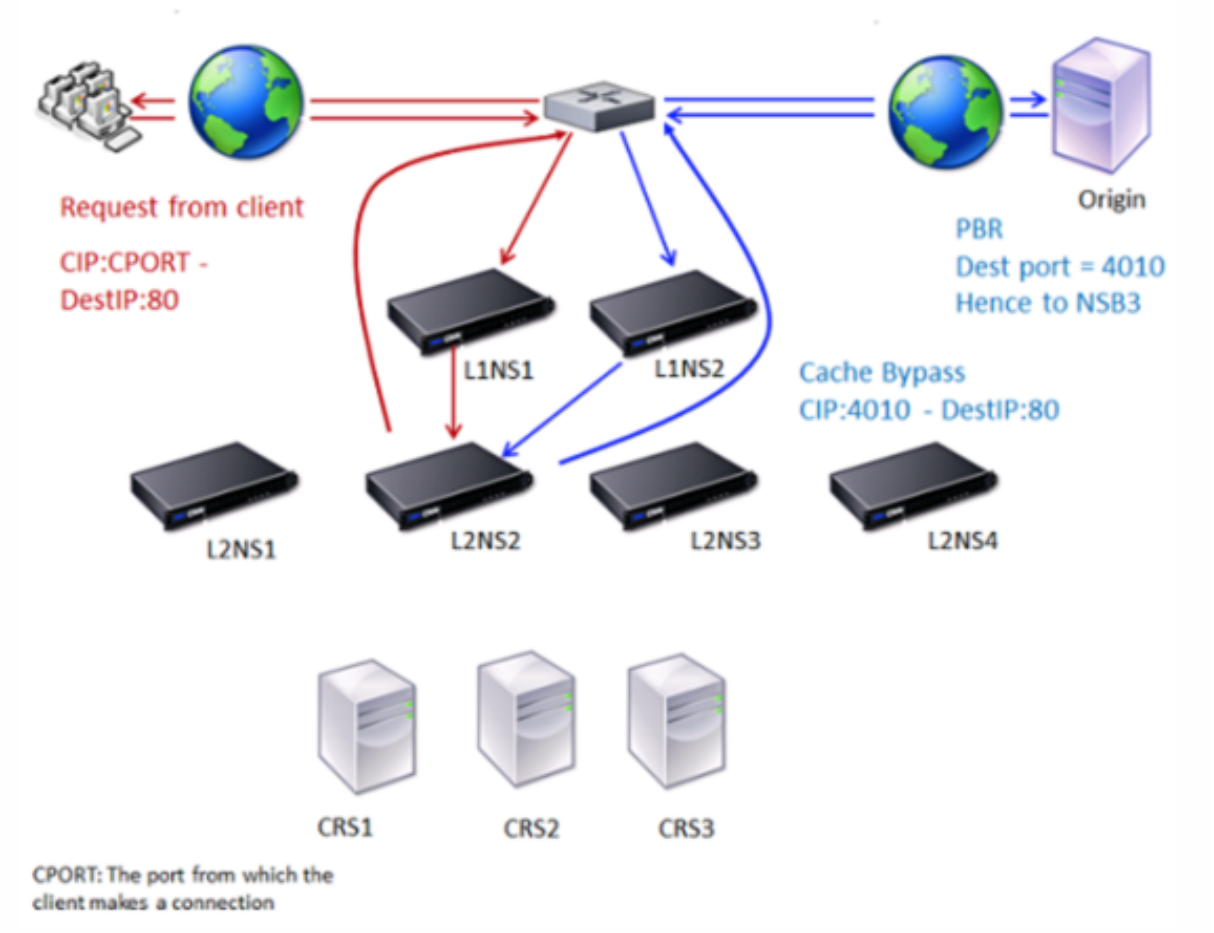
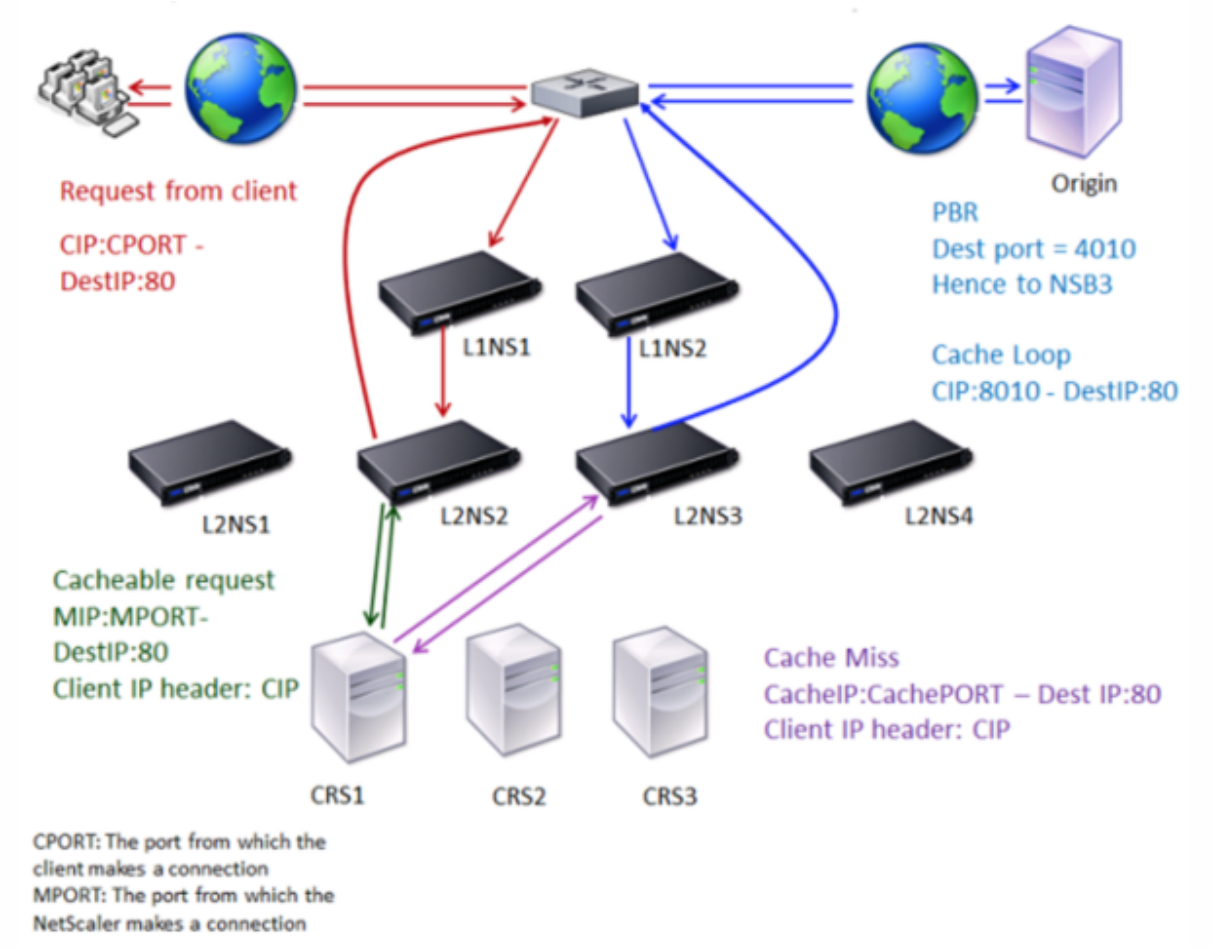
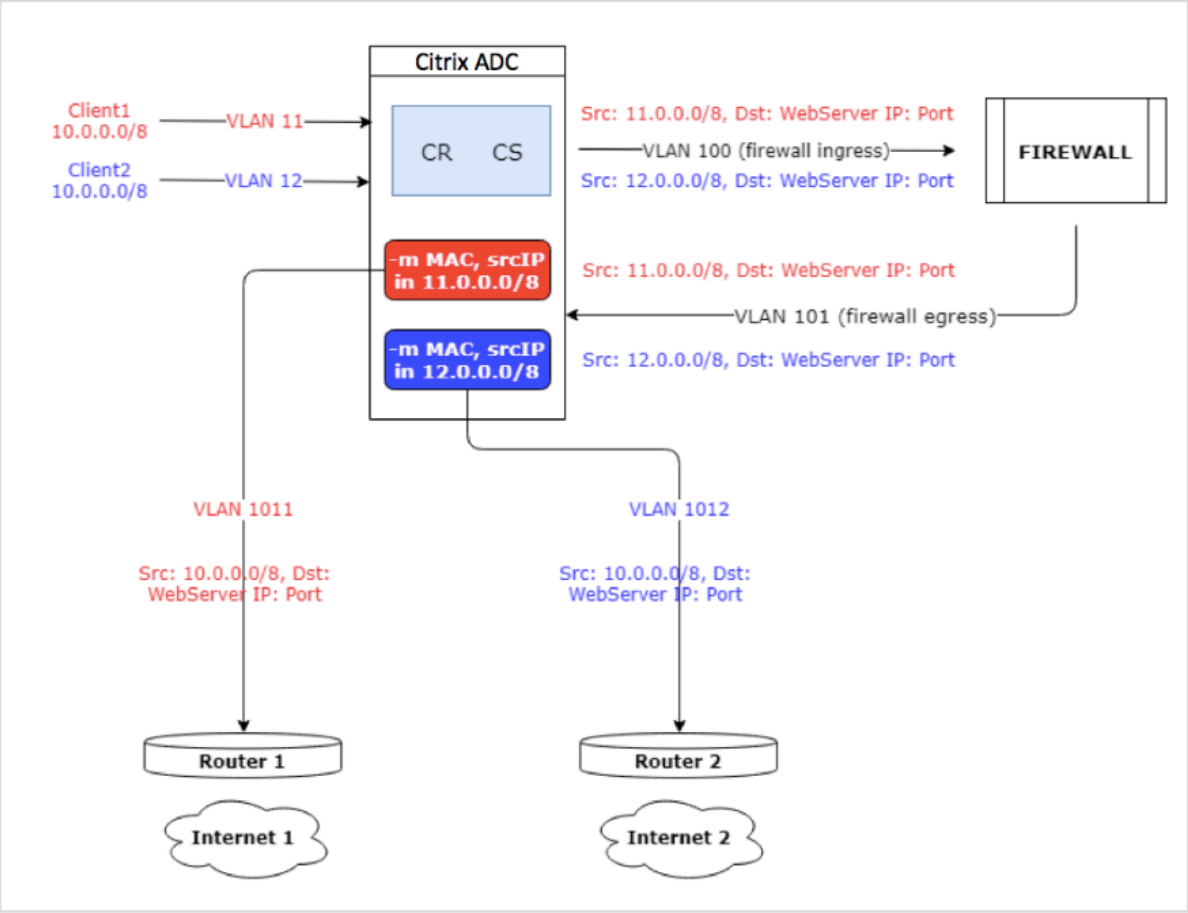
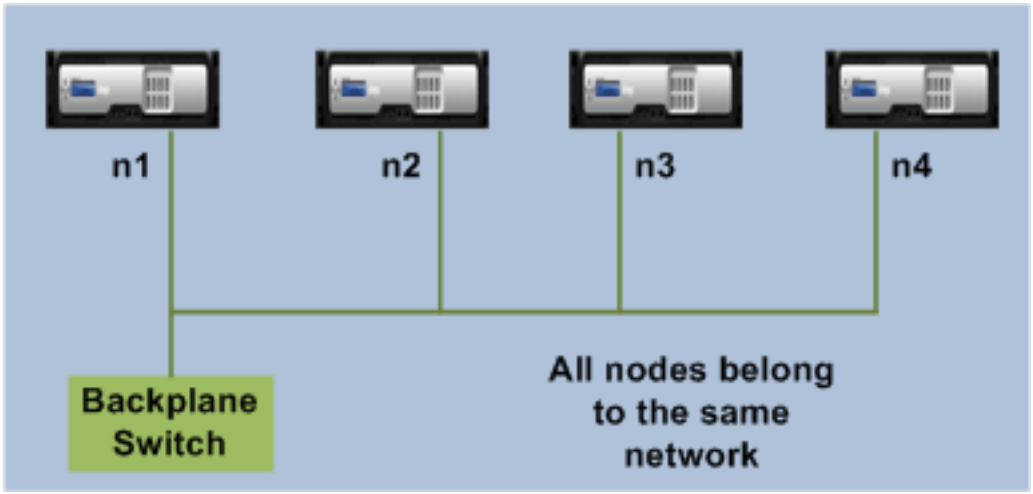
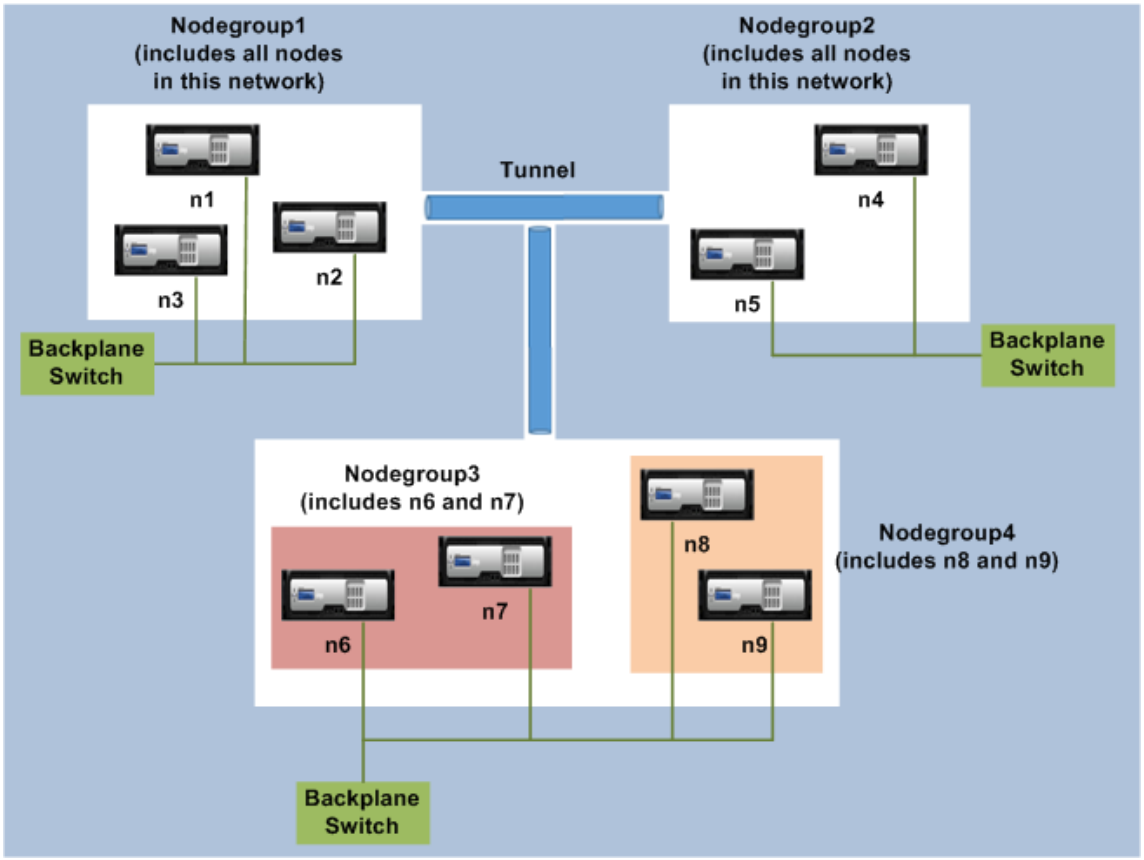
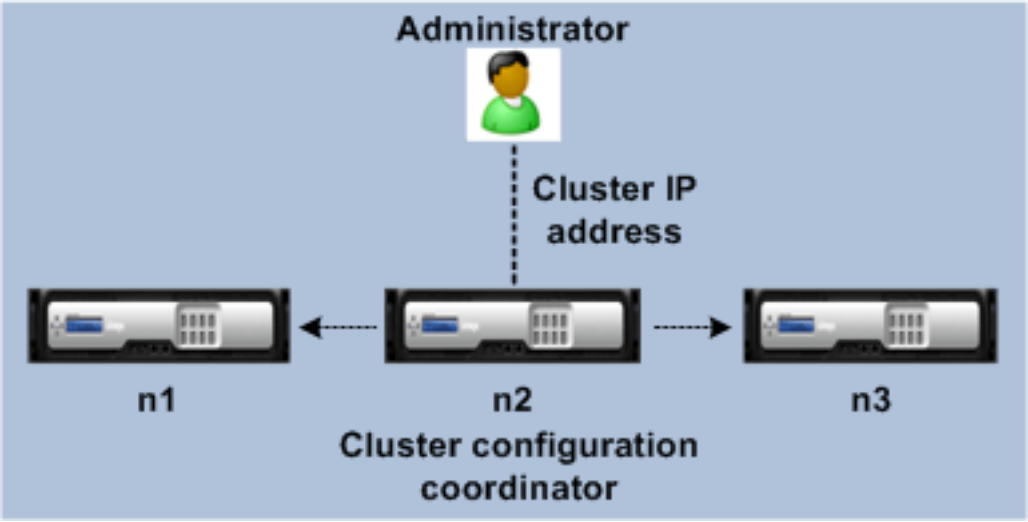
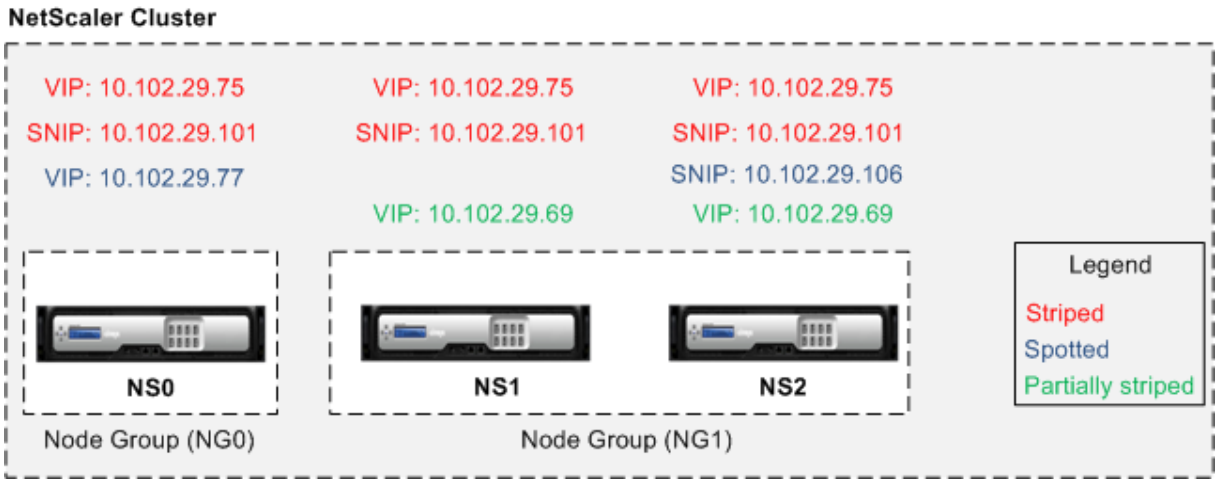
> disable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: OUT OF SERVICE  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
```



```
27          On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
28          Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
29
30  1)      Cache bypass  Policy: bypass-cache-control
31  2)      Cache bypass  Policy: Policy-CRD
32   Done
33  >
34  <!--NeedCopy-->
```

Activer ou désactiver un serveur virtuel de redirection de cache à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet de navigation, développez Redirection du cache, puis cliquez sur Serveurs virtuels.
3. Dans le volet de détails, sélectionnez le serveur virtuel que vous souhaitez activer ou désactiver (par exemple, **vServer-CRD-1**), puis cliquez sur Statistiques.
4. Dans la boîte de dialogue Continuer, cliquez sur Oui.

Demandes de stratégie directes de mise en cache au lieu du serveur Web d'origine

May 5, 2023

Par défaut, lorsqu'une demande correspond à une politique, l'appliance NetScaler la transmet directement au serveur d'origine ou à un serveur virtuel d'équilibrage de charge pour le serveur d'origine, selon la manière dont vous avez configuré la redirection du cache.

Vous pouvez modifier le comportement par défaut de sorte que lorsqu'une demande correspond à une stratégie, la demande soit transférée vers un serveur virtuel d'équilibrage de charge pour le cache.

Pour modifier la destination d'une demande de stratégie par l'origine ou le cache, utilisez le `onPolicyMatch` paramètre, qui spécifie où envoyer les demandes correspondant à la stratégie de redirection du cache.

Les options valides sont les suivantes :

1. `CACHE` - Dirige toutes les requêtes correspondantes vers le cache.
2. `ORIGIN` - Dirige toutes les requêtes correspondantes vers le serveur d'origine.

> **Remarque :**
>
> Pour que cette option fonctionne, vous devez sélectionner le type de redirection du cache

> comme POLICY.

Valeurs possibles : CACHE, ORIGIN

Valeur par défaut : ORIGIN

Modifier la destination d'une demande de stratégie par l'origine ou le cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier la destination d'un appel de stratégie et vérifier la configuration :

```
set cr vserver <name> [-onPolicyMatch (ORIGIN | CACHE)]
<!--NeedCopy-->
```

```
show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -onPolicyMatch CACHE
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Modifiez la destination d'un accès de politique à l'origine ou au cache à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez modifier la destination d'une demande de stratégie (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.

3. Dans la boîte de dialogue **Configurer le serveur virtuel (redirection du cache)**, cliquez sur **Avancé**.
4. Sélectionnez **CACHE** ou **ORIGIN** dans la liste déroulante **Rediriger vers** .
5. Cliquez sur **OK**.

Sauvegarder un serveur virtuel de redirection de cache

August 20, 2021

La redirection du cache peut échouer si le serveur virtuel principal échoue ou s'il est incapable de gérer un trafic excessif. Vous pouvez spécifier un serveur virtuel de sauvegarde pour prendre en charge le traitement du trafic lorsque le serveur virtuel principal échoue.

Pour spécifier un serveur virtuel de redirection de cache de sauvegarde, utilisez le paramètre BackupvServer, qui spécifie Sauvegarde Virtual Server. Longueur maximale : 127

Spécifier un serveur virtuel de redirection de cache de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour spécifier un serveur virtuel de redirection de cache de sauvegarde et vérifier la configuration :

```
-  set cr vserver <name> [-backupVServer <string>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -backupVServer Vserver-CRD-2
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

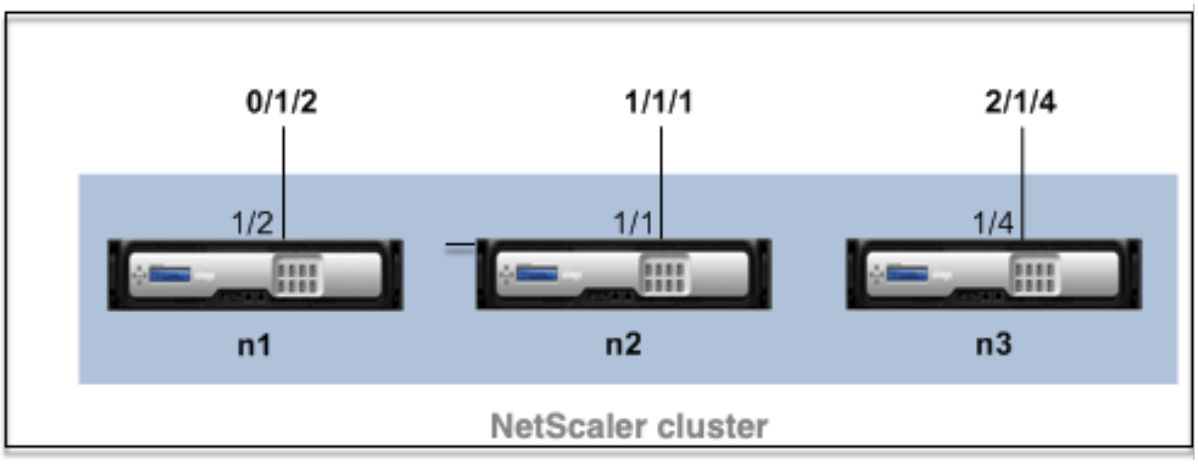
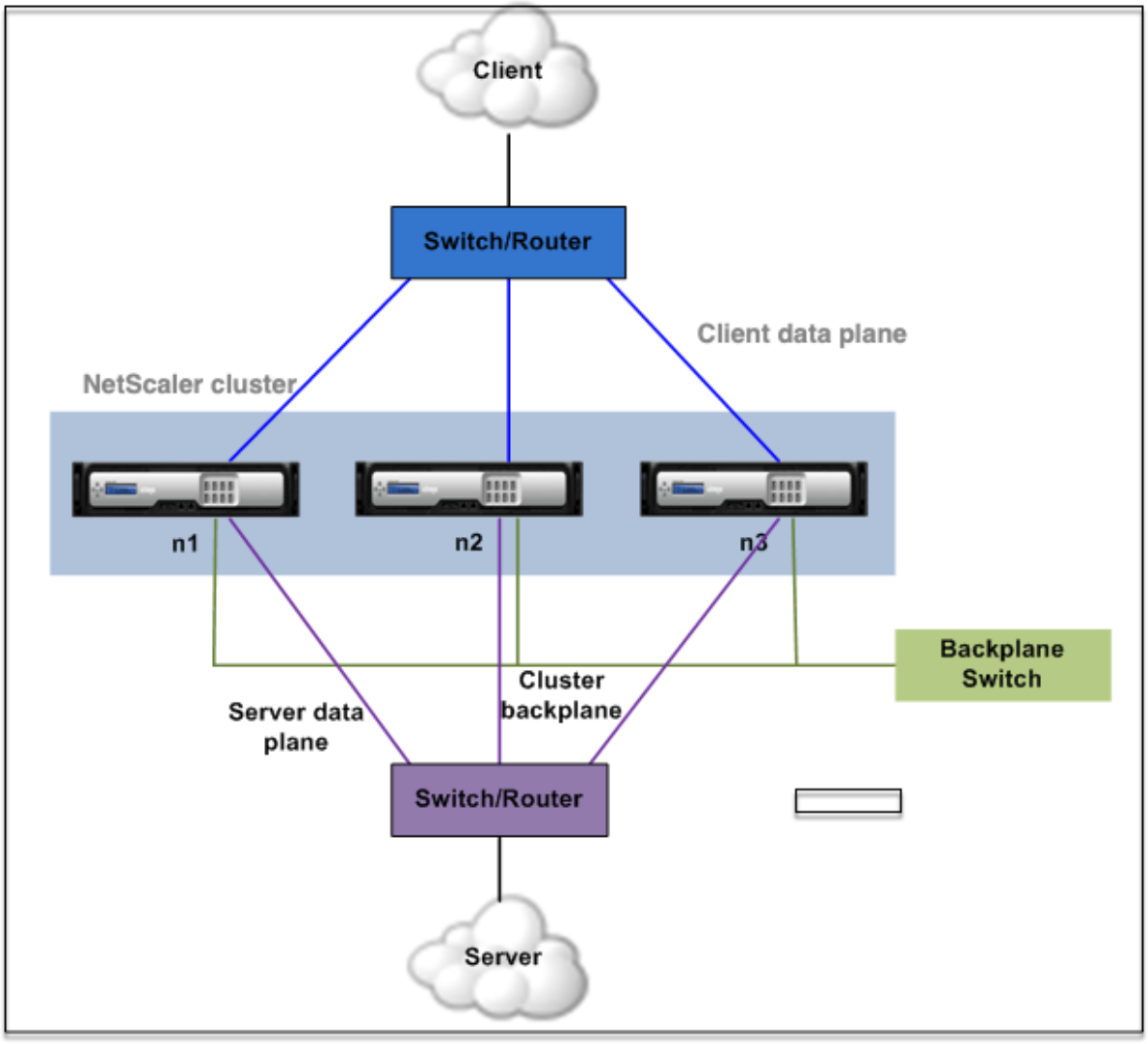
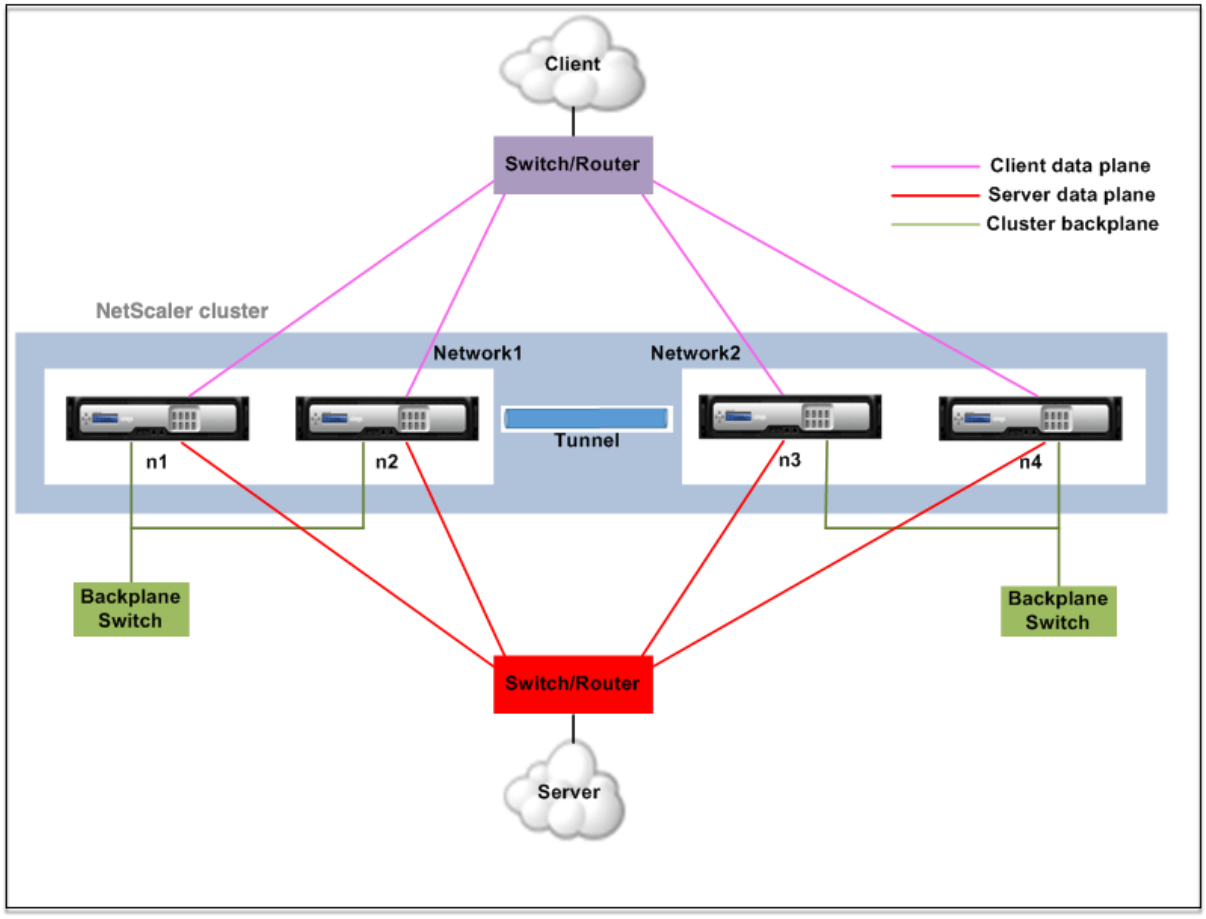
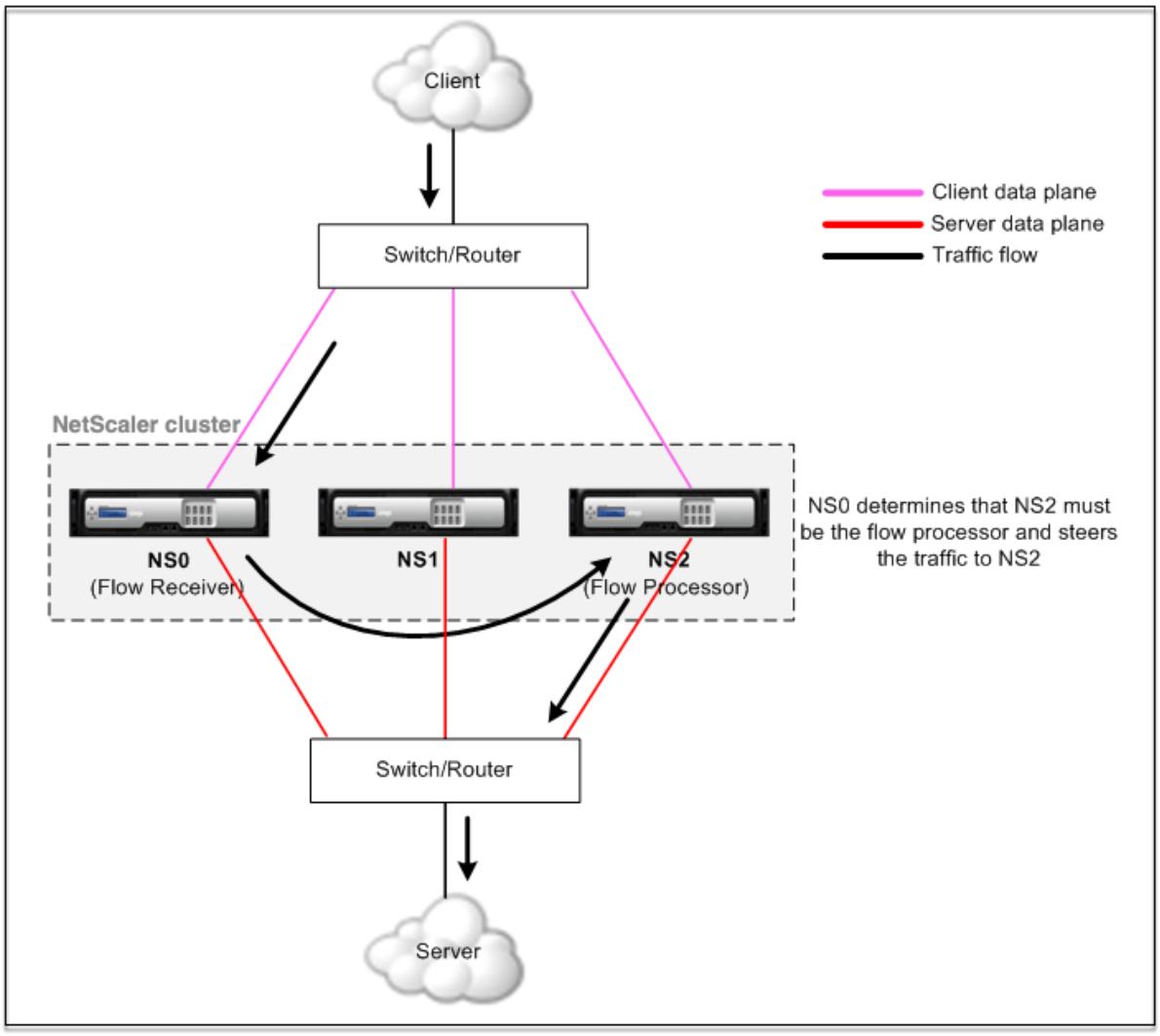
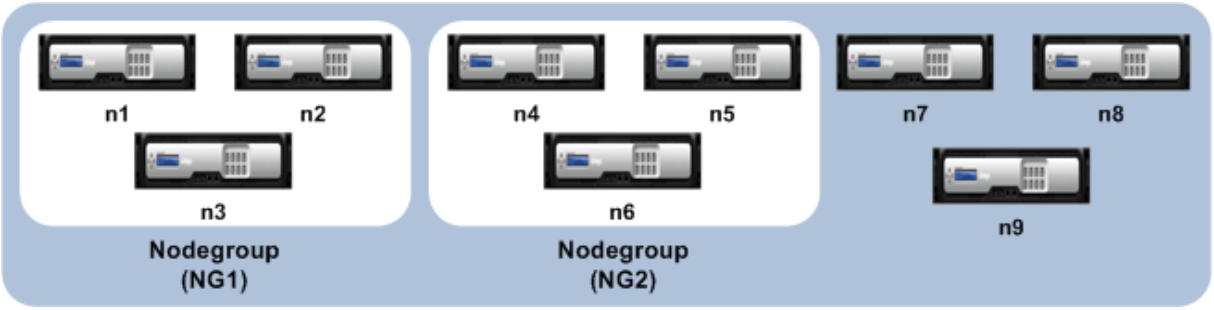
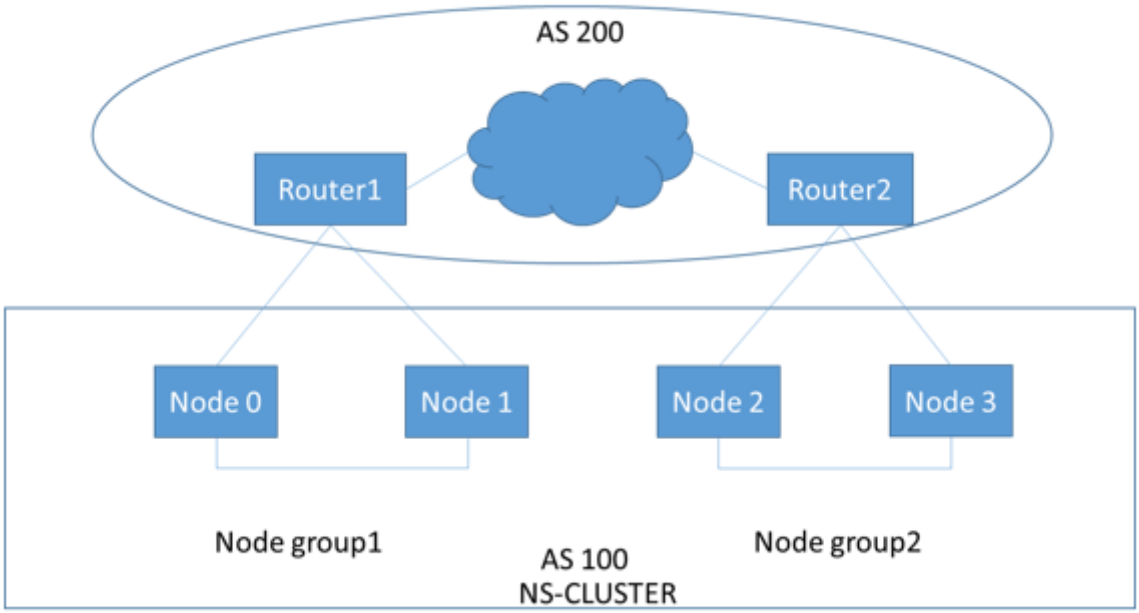
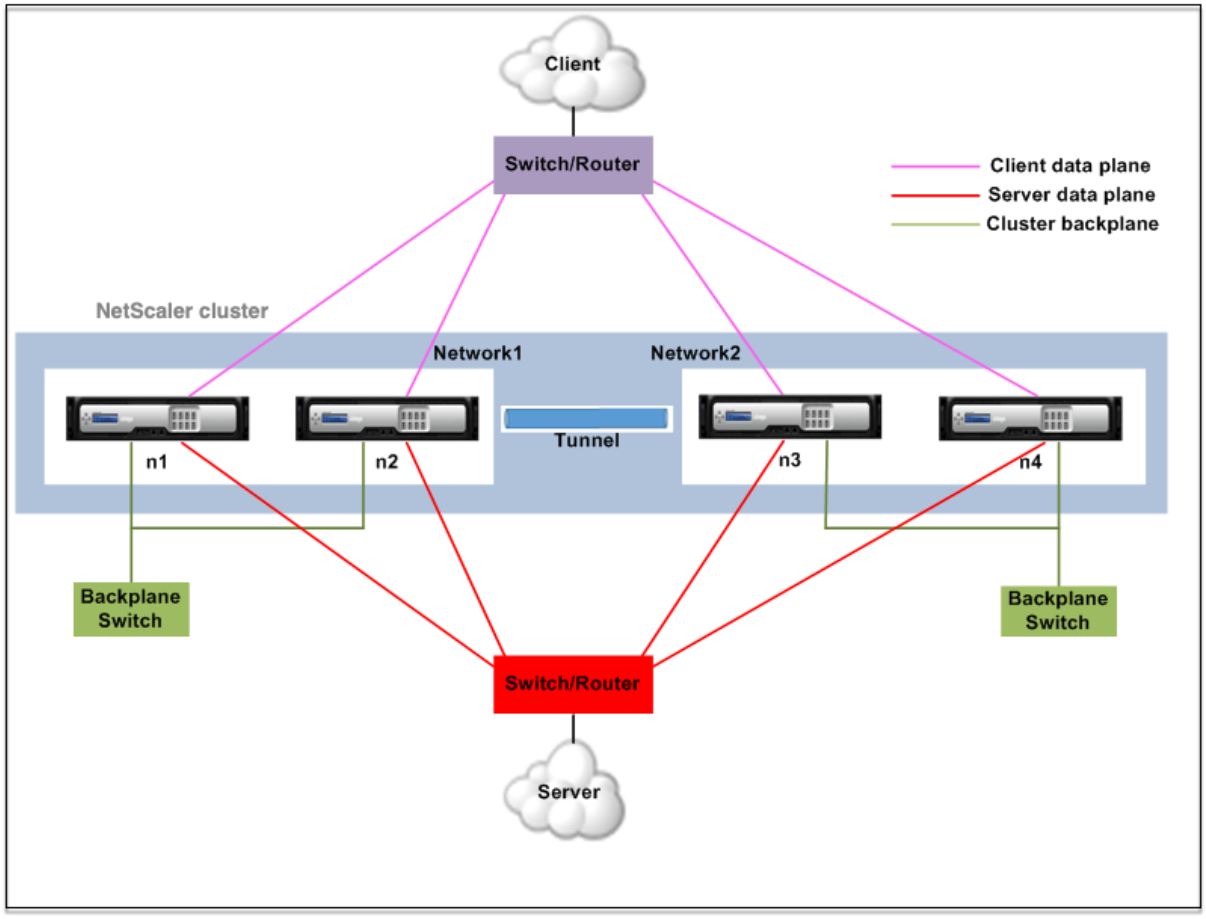
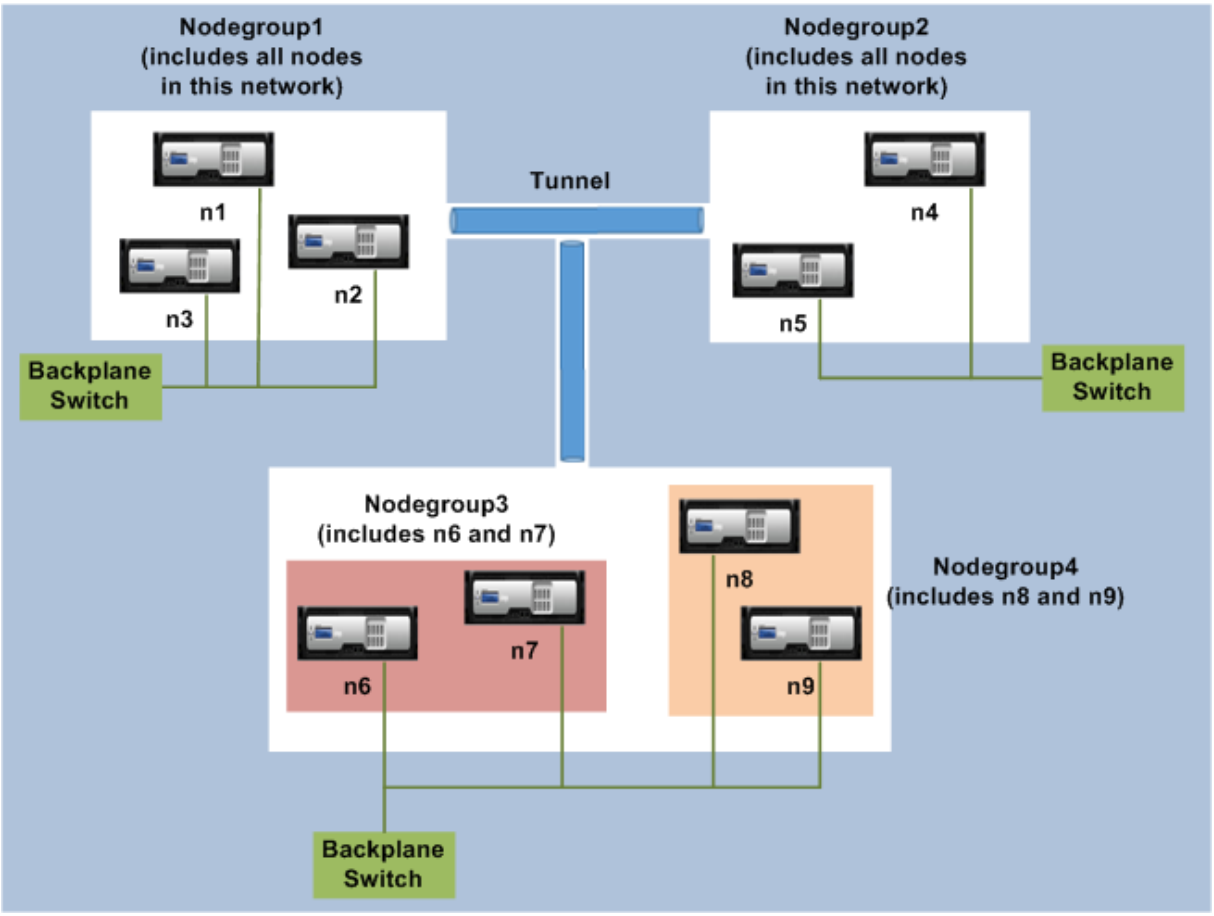
1)      Cache bypass  Policy: bypass-cache-control
```



```
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Spécifier un serveur virtuel de redirection de cache de sauvegarde à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel pour lequel vous souhaitez modifier la destination d'une demande de stratégie (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection du cache), sélectionnez l'onglet Avancé.
4. Dans la liste déroulante Sauvegarde Virtual Server, sélectionnez le serveur virtuel.
5. Cliquez sur OK.

Gestion des connexions client pour un serveur virtuel

May 5, 2023

Vous pouvez configurer les délais d'expiration sur un serveur virtuel de redirection de cache afin que les connexions client ne restent pas ouvertes indéfiniment. Vous pouvez également insérer des entêtes Via dans les requêtes. Pour éventuellement réduire la congestion du réseau, vous pouvez réutiliser les connexions TCP ouvertes. Vous pouvez activer ou désactiver le nettoyage différé des connexions au serveur virtuel de redirection du cache.

Vous pouvez configurer l'appliance pour qu'elle envoie des réponses ICMP aux demandes PING en fonction de vos paramètres. Sur l'adresse IP correspondant au serveur virtuel, définissez la réponse ICMP sur VSVR_CNTRLD, et sur le serveur virtuel, définissez la réponse ICMP VSERVER.

Les paramètres suivants peuvent être définis sur un serveur virtuel :

- Lorsque vous définissez ICMP VSERVER RESPONSE sur PASSIVE sur tous les serveurs virtuels, l'appliance répond toujours.
- Lorsque vous définissez ICMP VSERVER RESPONSE sur ACTIVE sur tous les serveurs virtuels, l'appliance répond même si l'un des serveurs virtuels est opérationnel.
- Lorsque vous définissez ICMP VSERVER RESPONSE sur ACTIVE sur certains et PASSIVE sur d'autres, l'appliance répond même si un serveur virtuel défini sur ACTIVE est en service.

Ce document contient les informations suivantes :

- Configurer le délai d'expiration du client

- Insérer des en-têtes Via dans les requêtes
- Réutilisez les connexions TCP
- Configurer le nettoyage différé des connexions

Configurer le délai d'expiration du client

Vous pouvez spécifier l'expiration des demandes du client en définissant une valeur de délai d'expiration pour le serveur virtuel de redirection du cache. La valeur du délai d'expiration est le nombre de secondes pendant lesquelles le serveur virtuel de redirection du cache attend de recevoir une réponse à la demande du client.

Pour configurer une valeur de délai d'expiration, utilisez le paramètre cltTimeout, qui spécifie le délai, en secondes, après lequel l'appliance NetScaler ferme toutes les connexions client inactives. La valeur par défaut est de 180 secondes pour les services basés sur HTTP/SSL et de 9 000 secondes pour les services basés sur TCP.

Configurer le délai d'expiration du client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le délai d'expiration du client et vérifier la configuration :

```
-  set cr vserver <name> [-cltTimeout <secs>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -cltTimeout 6000
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
```



```
<!--NeedCopy-->
```

Configurer le délai d'expiration du client à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet de détails, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le délai d'expiration du client (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection du cache), sélectionnez l'onglet Avancé.
4. Dans la zone de texte Délai d'expiration du client (secondes), entrez la valeur du délai d'expiration en secondes.
5. Cliquez sur OK.

Insérer des en-têtes Via dans les requêtes

Un en-tête Via répertorie les protocoles et les destinataires entre le point de départ et le point de fin d'une demande ou d'une réponse et informe le serveur des proxys via lesquels la demande a été envoyée. Vous pouvez configurer le serveur virtuel de redirection du cache pour insérer un en-tête Via dans chaque requête HTTP. Le paramètre via est activé par défaut lorsque vous créez un serveur virtuel de redirection de cache.

Pour activer ou désactiver l'insertion d'un en-tête VIA dans les requêtes client, utilisez le paramètre via, qui indique l'état du système lors de l'insertion d'un en-tête Via dans les requêtes HTTP.

Valeurs possibles : ON, OFF

Valeur par défaut : ON

Activer ou désactiver l'insertion d'en-têtes VIA dans les demandes du client à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
-  set cr vserver <name> [-via (ON|OFF)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -via ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
```



```
5           State: UP  ARP:DISABLED
6           Client Idle Timeout: 6000 sec
7           Down state flush: ENABLED
8           Disable Primary Vserver On Down : DISABLED
9           Default:        Content Precedence: URL Cache: TRANSPARENT
10          On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
11          Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
12          Backup: Vserver-CRD-2
13
14  1)      Cache bypass  Policy: bypass-cache-control
15  2)      Cache bypass  Policy: Policy-CRD
16   Done
17  >
18  <!--NeedCopy-->
```

Activer ou désactiver l'insertion d'en-têtes VIA dans les demandes du client à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet de détails, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le délai d'expiration du client (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection du cache), sélectionnez l'onglet Avancé.
4. Cochez la case Via.
5. Cliquez sur OK.

Réutilisez les connexions TCP

Vous pouvez configurer l'appliance NetScaler pour réutiliser les connexions TCP au cache et aux serveurs d'origine via les connexions client. Cela peut améliorer les performances en économisant le temps nécessaire à l'établissement d'une session entre le serveur et l'appliance. L'option de réutilisation est activée par défaut lorsque vous créez un serveur virtuel de redirection de cache.

Pour activer ou désactiver la réutilisation des connexions TCP, utilisez le paramètre reuse, qui spécifie l'état de réutilisation des connexions TCP au cache ou aux serveurs d'origine sur les connexions client.

Valeurs possibles : ON, OFF

Valeur par défaut : ON

Activer ou désactiver la réutilisation des connexions TCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
-  set cr vserver <name> [-reuse (ON|OFF)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> set cr vserver Vserver-CRD-1 -reuse ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Activer ou désactiver la réutilisation des connexions TCP à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet de détails, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le délai d'expiration du client (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection du cache), sélectionnez l'onglet Avancé.
4. Cochez la case Réutiliser.
5. Cliquez sur OK.

Configurer le nettoyage différé des connexions

L'option down state flush effectue un nettoyage différé des connexions sur un serveur virtuel de redirection de cache. L'option down state flush est activée par défaut lorsque vous créez un serveur virtuel

de redirection de cache.

Pour activer ou désactiver l'option down state flush, définissez le paramètre DownStateFlush.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

Activation ou désactivation de l'option Down State Flush à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le nettoyage différé des connexions et vérifier la configuration :

```
1 -  set cr vserver <name> [-downStateFlush (ENABLED | DISABLED)]
2 -  show cr vserver <name>
3 <!--NeedCopy-->
```

Exemple :

```
1  > set cr vserver Vserver-CRD-1 -downStateFlush ENABLED
2   Done
3  > show cr vserver Vserver-CRD-1
4          Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
5          State: UP  ARP:DISABLED
6          Client Idle Timeout: 6000 sec
7          Down state flush: ENABLED
8          Disable Primary Vserver On Down : DISABLED
9          Default:        Content Precedence: URL Cache: TRANSPARENT
10         On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
11         Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
12         Backup: Vserver-CRD-2
13
14 1)      Cache bypass  Policy: bypass-cache-control
15 2)      Cache bypass  Policy: Policy-CRD
16  Done
17 <!--NeedCopy-->
```

Activer ou désactiver la réutilisation des connexions TCP à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Redirection du cache > Serveurs virtuels.
2. Dans le volet de détails, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le délai d'expiration du client (par exemple, **vServer-CRD-1**), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (redirection du cache), cliquez sur l'onglet Avancé.

4. Cochez la case Down state flush.
5. Cliquez sur OK.

Activer la vérification de l'état TCP externe pour les serveurs virtuels UDP

May 5, 2023

Dans les clouds publics, vous pouvez utiliser l'appliance NetScaler comme équilibreur de charge de second niveau lorsque l'équilibreur de charge natif est utilisé comme premier niveau. L'équilibreur de charge natif peut être un équilibreur de charge d'application (ALB) ou un équilibreur de charge réseau (NLB). La plupart des clouds publics ne prennent pas en charge les sondes de santé UDP dans leurs équilibreurs de charge natifs. Pour surveiller l'état de l'application UDP, les clouds publics recommandent d'ajouter un point de terminaison TCP à votre service. Le point de terminaison reflète l'intégrité de l'application UDP.

L'appliance NetScaler prend en charge le contrôle de santé externe basé sur TCP pour un serveur virtuel UDP. Cette fonctionnalité introduit un écouteur TCP sur le VIP du serveur virtuel de redirection de cache et du port configuré. L'écouteur TCP reflète l'état du serveur virtuel.

Pour activer la vérification de l'état TCP externe pour les serveurs virtuels UDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer une vérification d'intégrité TCP externe avec l'option tcpProbePort :

```
add cr vserver <name> <serviceType> -tcpProbePort <tcpProbePort>

<!--NeedCopy-->
```

Exemple :

```
add cr vserver Vserver-CR-1 HTTP -tcpProbePort 80
<!--NeedCopy-->
```

Pour activer la vérification de l'état TCP externe pour les serveurs virtuels UDP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Redirection du cache > Serveurs virtuels**, puis créez un serveur virtuel.

2. Cliquez sur **Ajouter** pour créer un serveur virtuel.
3. Dans le volet **Paramètres de base**, ajoutez le numéro de port dans le champ **Port de la sonde TCP** .
4. Cliquez sur **OK**.

Redirection du cache N-Tier

May 5, 2023

Pour gérer efficacement de grandes quantités de données mises en cache, généralement plusieurs gigaoctets par seconde, un fournisseur de services Internet (ISP) déploie plusieurs serveurs de cache dédiés. La fonctionnalité de redirection du cache de l'appliance NetScaler peut aider à équilibrer la charge des serveurs de cache, mais une seule appliance ou plusieurs appliances peuvent ne pas gérer efficacement le volume important de trafic.

Vous pouvez résoudre le problème en déployant les appliances NetScaler sur deux niveaux (couches), les appliances du niveau supérieur équilibrant la charge du niveau inférieur et les appliances du niveau inférieur équilibrant la charge des serveurs de cache. Cet arrangement est appelé *redirection du cache à n niveaux*.

À des fins telles que l'audit et la sécurité, un FAI doit suivre les détails du client tels que l'adresse IP, les informations fournies et l'heure de l'interaction. Par conséquent, les connexions client via une appliance NetScaler doivent être totalement transparentes. Toutefois, si vous configurez la redirection transparente du cache, avec les appliances NetScaler déployées en parallèle, l'adresse IP du client doit être partagée entre toutes les appliances. Le partage de l'adresse IP du client crée un conflit qui empêche les périphériques réseau, tels que les routeurs, les serveurs de cache, les serveurs d'origine et les autres appliances NetScaler, de déterminer l'appliance, et donc le client, auquel la réponse doit être envoyée.

Comment la redirection du cache de niveau N est implémentée

Pour résoudre le problème, la redirection du cache de niveau n de l'appliance divise la plage de ports source entre les appliances du niveau inférieur et inclut l'adresse IP du client dans la demande envoyée aux serveurs de cache. Les appliances NetScaler de niveau supérieur sont configurées pour effectuer un équilibrage de charge sans session afin d'éviter toute charge inutile sur les appliances.

Lorsque l'appliance NetScaler de niveau inférieur communique avec un serveur de cache, elle utilise une adresse IP mappée (MIP) pour représenter l'adresse IP source. Par conséquent, le serveur de cache peut identifier l'appliance à partir de laquelle il a reçu la demande et envoyer la réponse à la même appliance.

L'appliance NetScaler de niveau inférieur insère l'adresse IP du client dans l'en-tête de la demande envoyée au serveur de cache. L'adresse IP du client figurant dans l'en-tête aide l'appliance à déterminer le client auquel le paquet doit être transféré lorsqu'elle reçoit la réponse d'un serveur de cache, ou le serveur d'origine en cas d'échec du cache. Le serveur d'origine détermine la réponse à envoyer en fonction de l'adresse IP du client insérée dans l'en-tête de la demande.

Le serveur d'origine envoie la réponse à un dispositif de niveau supérieur, y compris le numéro de port source à partir duquel le serveur d'origine a reçu la demande. L'ensemble de la plage de ports source, de 1024 à 65535, est répartie entre les appliances NetScaler de niveau inférieur. Chaque appliance de niveau inférieur se voit attribuer exclusivement un groupe d'adresses au sein de la plage. Cette allocation permet à l'appliance de niveau supérieur d'identifier sans ambiguïté l'appliance NetScaler de niveau inférieur qui a envoyé la demande au serveur d'origine. L'appliance de niveau supérieur peut donc transmettre la réponse à l'appliance de niveau inférieur appropriée.

Les appliances NetScaler de niveau supérieur sont configurées pour effectuer un routage basé sur des politiques, et les politiques de routage sont définies pour déterminer l'adresse IP de l'appliance de destination à partir de la plage de ports source.

Configuration nécessaire pour configurer N-Tier CRD

La configuration suivante est nécessaire au fonctionnement de la redirection du cache à n niveaux :

Pour chaque appliance NetScaler de niveau supérieur :

- Activez le mode couche 3.
- Définissez des politiques pour les itinéraires basés sur des politiques (PBR) afin que le trafic soit transféré en fonction de la portée du port de destination.
- Configurez un serveur virtuel d'équilibrage de charge.
- Configurez le serveur virtuel pour qu'il écoute tout le trafic provenant du client. Définissez le type/protocole de service sur ANY et l'adresse IP sous forme d'astérisque (*).
- Activez l'équilibrage de charge sans session avec le mode de redirection basé sur Mac pour éviter toute charge inutile sur les appliances NetScaler de niveau supérieur.
- Assurez-vous que l'option Utiliser le port proxy est activée.
- Créez un service pour chaque appliance de niveau inférieur et liez tous les services au serveur virtuel.

Pour chaque appliance NetScaler de niveau inférieur,

- Configurez la plage de ports de redirection du cache sur l'appliance. Attribuez une plage exclusive à chaque appliance de niveau inférieur.
- Configurez un serveur virtuel d'équilibrage de charge et activez la redirection basée sur Mac.
- Créez un service pour chaque serveur de cache dont la charge doit être équilibrée par cette appliance. Lors de la création du service, activez l'insertion de l'adresse IP du client dans l'en-tête. Liez ensuite tous les services au serveur virtuel d'équilibrage de charge.

- Configurez un serveur virtuel de redirection du cache en mode transparent avec les paramètres suivants :
  - Activez l'option Origin USIP.
  - Ajoutez une expression IP source pour inclure l'adresse IP du client dans l'en-tête.
  - Activez l'option Utiliser la plage de ports.

Comment fonctionne la redirection du cache de niveau N lors d'un accès au cache

La figure suivante montre comment fonctionne la redirection du cache lorsqu'une demande client peut être mise en cache et que la réponse est envoyée depuis un serveur de cache.

Figure 1. Redirection du cache en cas d'accès au cache



Deux appliances NetScaler, L1NS1 et L1NS2, sont déployées au niveau supérieur, et quatre appliances NetScaler, L2NS1, L2NS2, L2NS3 et L2NS4, sont déployées au niveau inférieur. Le client A envoie une demande qui est transmise par le routeur. Les serveurs de cache CRS1, CRS2 et CRS3 traitent les demandes de cache. Le système d'exploitation d'Origin Server traite les demandes non mises en cache.

Flux de trafic

1. Le client envoie une demande et le routeur la transmet à L1NS1.
2. L1NS1 équilibre la charge de la demande vers L2NS2.
3. L2NS2 équilibre la charge de la demande envoyée au serveur de cache CRS1, et la demande peut être mise en cache. L2NS2 inclut l'adresse IP du client dans l'en-tête de la requête.
4. CRS1 envoie la réponse à L2NS2 car L2NS2 a utilisé son MIP comme adresse IP source lors de la connexion à CRS1.
5. À l'aide de l'adresse IP du client dans l'en-tête de la demande, L2NS2 identifie le client d'où provient la demande. Le L2NS2 envoie directement la réponse au routeur, évitant ainsi une charge inutile sur l'appliance du niveau supérieur.
6. Le routeur transmet la réponse au client A.

Comment fonctionne la redirection du cache de niveau N lors d'un contournement du cache

La figure suivante montre comment fonctionne la redirection du cache lorsqu'une demande client est envoyée à un serveur d'origine pour obtenir une réponse.

Figure 2. Redirection du cache en cas de contournement du cache



Deux appliances NetScaler, L1NS1 et L1NS2, sont déployées au niveau supérieur, et quatre appliances NetScaler, L2NS1, L2NS2, L2NS3 et L2NS4, sont déployées au niveau inférieur. Le client A envoie une demande qui est transmise par le routeur. Les serveurs de cache CRS1, CRS2 et CRS3 traitent les demandes de cache. Le système d'exploitation d'Origin Server traite les demandes non mises en cache.

Flux de trafic

1. Le client envoie une demande et le routeur la transmet à L1NS1.
2. L1NS1 équilibre la charge de la demande vers L2NS2.
3. La requête ne peut pas être mise en cache (contournement du cache). Par conséquent, L2NS2 envoie la demande au serveur d'origine via le routeur.
4. Le serveur d'origine envoie la réponse à un dispositif de niveau supérieur, L1NS2.
5. Conformément aux politiques PBR, L1NS2 transfère le trafic vers l'appliance appropriée du niveau inférieur, L2NS2.
6. Le L2NS2 utilise l'adresse IP du client figurant dans l'en-tête de la demande pour identifier le client d'où provient la demande et envoie la réponse directement au routeur, évitant ainsi de surcharger inutilement l'appliance du niveau supérieur.

7. Le routeur transmet la réponse au client A.

Comment fonctionne la redirection du cache de niveau N en cas d'échec du cache

La figure suivante montre comment fonctionne la redirection du cache lorsqu'une demande client n'est pas mise en cache.

Figure 3. Redirection du cache en cas d'échec du cache



Deux appliances NetScaler, L1NS1 et L1NS2, sont déployées au niveau supérieur, et quatre appliances NetScaler, L2NS1, L2NS2, L2NS3 et L2NS4, sont déployées au niveau inférieur. Le client A envoie une demande qui est transmise par le routeur. Les serveurs de cache CRS1, CRS2 et CRS3 traitent les demandes de cache. Le système d'exploitation d'Origin Server traite les demandes non mises en cache.

Flux de trafic

1. Le client envoie une demande et le routeur la transmet à L1NS1.
2. L1NS1 équilibre la charge de la demande vers L2NS2.

3. L2NS2 équilibre la charge de la demande envoyée au serveur de cache CRS1 car la demande peut être mise en cache.
4. CRS1 n'a pas la réponse (échec du cache). CRS1 transmet la demande au serveur d'origine via l'appliance du niveau inférieur. Le L2NS3 intercepte le trafic.
5. L2NS3 prend l'adresse IP du client depuis l'en-tête et transmet la demande au serveur d'origine. Le port source inclus dans le paquet est le port L2NS3 à partir duquel la demande est envoyée au serveur d'origine.
6. Le serveur d'origine envoie la réponse à un dispositif de niveau supérieur, L1NS2.
7. Conformément aux politiques PBR, L1NS2 transfère le trafic vers l'appliance appropriée du niveau inférieur, L2NS3.
8. L2NS3 transmet la réponse au routeur.
9. Le routeur transmet la réponse au client A.

Configurer les appliances NetScaler de niveau supérieur

May 5, 2023

Configurez chacune des appliances NetScaler de niveau supérieur comme suit.

Configurer une appliance de niveau supérieur pour la redirection du cache à n niveaux à l'aide de la commande CLI

À l'invite de commandes, tapez les commandes suivantes :

- `add service \<name\>@ \<serviceIP\> \<serviceType\> \<port\>`

  Exécutez cette commande pour chaque service à ajouter.

- `add lb vserver \<name\>@ ANY \* \<port\> -persistenceType \<persistenceMethod \> -lbMethod \<lbMethod\> -m MAC -sessionless ENABLED -cltTimeout \< client\\_Timeout\\_Value\>`

- `bind lb vserver \<name\>@ \<serviceName\>`

  Exécutez cette commande pour chaque service à lier.

- `enable ns mode l3`

- `add ns pbr \<name\> \<action\> -srcPort \<sourcePortNumber\> -destPort \<startPortNumber-endPortNumber\> -nexthop \<serviceIpAddress\> -protocol TCP`

- `apply ns pbrs`

  Exécutez cette commande après avoir ajouté tous les PBR nécessaires.

Configurer une appliance de niveau supérieur pour la redirection du cache à n niveaux à l'aide de l'interface graphique

1. Activez le mode L3 :
   a) Dans le volet de navigation, cliquez sur Système, puis sur Paramètres.
   b) Dans le groupe Paramètres, cliquez sur le lien Configurer les modes.
   c) Cochez la case Mode couche 3 (transfert IP).
   d) Cliquez sur OK.
2. Configurer le routage basé sur des règles (PBR) :
   a) Accédez à Système > Réseau > PBR.
   b) Dans le volet Routage basé sur des politiques (PBR), cliquez sur Ajouter.
   c) Tapez un nom pour le PBR.
   d) Sélectionnez l'action Autoriser.
   e) Dans la zone Next Hop, tapez l'adresse IP du service, qui représente une appliance de niveau inférieur.
   f) Sélectionnez TCP dans la liste déroulante Protocol.
   g) Tapez le port source et la plage du port de destination correspondant à l'appliance de niveau inférieur ajoutée.
   h) Cliquez sur Create.
   i) Dans le volet de détails, sélectionnez le PBR et cliquez sur Appliquer.
   j) Répétez les étapes (i) à (vii) pour chaque appliance de niveau inférieur.
3. Créez un service pour chaque appliance de niveau inférieur :
   a) Accédez à Traffic Management > Load Balancing > Services.
   b) Dans le volet de détails, cliquez sur Ajouter.
   c) Spécifiez le nom, le protocole, l'adresse IP et le port. Le protocole doit être N'IMPORTE LEQUEL.
   d) Cliquez sur Create.
4. Configurez un serveur virtuel d'équilibrage de charge :
   a) Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
   b) Dans le volet de détails, cliquez sur Ajouter.
   c) Spécifiez le nom, le protocole, l'adresse IP et le port. Le protocole doit être N'IMPORTE LEQUEL et l'adresse IP doit être *.
   d) Dans l'onglet Services, sélectionnez les services qui représentent les appliances NetScaler de niveau inférieur.
   e) Dans l'onglet Avancé, sélectionnez le mode de redirection basé sur MAC et cochez la case Sans session.
   f) Cliquez sur Create.

Configurer les appliances NetScaler de niveau inférieur

May 5, 2023

Configurez chacune des appliances NetScaler de niveau inférieur comme suit.

Configurer une appliance de niveau inférieur pour la redirection du cache à n niveaux à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

- `add service <name>@ <cacheServiceIP> <serviceType> <port> -cip ENABLED "ClientIP"-cachetype transparent`

  Répétez l'opération pour chaque serveur de cache.

- `add lb vserver <name>@ <serviceType> -m MAC`
- `bind lb vserver <name>@ <cacheServiceName>`

  Répétez l'opération pour chaque serveur de cache.

- `add cr vserver <name> <serviceType> * <port> -srcIPExpr "HTTP.REQ.HEADER("ClientIP")"-originusip ON -usePortRange ON`
- `set ns param-crPortRange <startPortNumber-endPortNumber>`

Configurer une appliance de niveau inférieur pour la redirection du cache à n niveaux à l'aide de l'interface graphique

1. Créez un service pour chaque serveur de cache. Pour créer un service :
   a) Accédez à Traffic Management > Load Balancing > Services.
   b) Dans le volet de détails, cliquez sur Ajouter, puis spécifiez le nom et le protocole. Décochez la case Directement adressable.
   c) Dans l'onglet Avancé, cochez la case Override Global et la case Client IP, puis dans la zone En-tête, tapez ClientIP.
   d) Dans la zone Type de cache, sélectionnez Cache transparent.
   e) Cliquez sur Create.
2. Configurez un serveur virtuel d'équilibrage de charge :
   a) Accédez à Gestion du trafic > Équilibrage de charge > Services virtuels.
   b) Dans le volet de détails, cliquez sur Ajouter et spécifiez le nom, le protocole, l'adresse IP et le port. L'adresse IP doit être un astérisque (*).
   c) Dans l'onglet Services, sélectionnez les services qui représentent les serveurs de cache.
   d) Dans l'onglet Avancé, pour le mode de redirection, sélectionnez Basé sur MAC.

e) Cliquez sur Create.

3. Configurez un serveur virtuel de redirection de cache :
   a) Accédez à Gestion du trafic > Équilibrage de charge > Services virtuels.
   b) Dans le volet de détails, cliquez sur Ajouter et spécifiez le nom, le protocole, l'adresse IP et le port. L'adresse IP doit être *.
   c) Pour Type de cache, sélectionnez Transparent.
   d) Dans l'onglet Avancé, dans la zone Serveur de cache, sélectionnez le nouveau serveur virtuel d'équilibrage de charge et cochez les cases Origin USIP et Use Port Range. Dans la zone Expression IP source, tapez HTTP.REQ.HEADER (« ClientIP »).
   e) Cliquez sur Create.
4. Attribuez une plage de ports source à l'appliance :
   a) Dans le volet de navigation, cliquez sur Système, puis sur Paramètres.
   b) Dans le groupe Paramètres, cliquez sur le lien Modifier les paramètres généraux du système.
   c) Dans le groupe Plage de ports de redirection du cache, spécifiez la plage de ports de l'appliance en saisissant un numéro de port pour le port de départ et un numéro de port pour le port de fin.
   d) Cliquez sur OK.

Traduire l'adresse IP de destination d'une requête vers l'adresse IP d'origine

May 5, 2023

Vous pouvez configurer le serveur virtuel de redirection du cache proxy direct sur l'appliance NetScaler pour traduire l'adresse IP de destination de la demande arrivant sur le serveur virtuel de redirection du cache en adresse IP du serveur d'origine. Cette traduction s'effectue indépendamment du fait que la demande soit envoyée aux serveurs en cache ou au serveur d'origine.
Auparavant, le serveur virtuel de redirection du cache par proxy direct dans un environnement de fournisseur de services ne pouvait pas être utilisé efficacement pour envoyer du trafic via le pare-feu en raison des limites de la redirection du cache à l'aide de politiques de commutation de contenu. Le serveur virtuel de redirection du cache n'a pas traduit l'adresse IP d'origine en adresse IP de destination lorsque le paquet a été envoyé au cache. L'adresse IP de destination était celle du serveur d'origine uniquement lorsque les demandes étaient traitées à partir du serveur en cache.

Remarque : La traduction de l'adresse IP de destination d'une demande en adresse IP d'origine n'est pas prise en charge pour un serveur virtuel de redirection de cache transparent. Pour un serveur virtuel de redirection de cache transparent, cette option doit être définie sur OFF.

Cas d'utilisation

Dans un déploiement dans lequel l'appliance NetScaler est configurée pour la redirection du cache du proxy direct, le pare-feu et les adresses IP des clients réutilisées, le pare-feu ne peut pas distinguer/utiliser les adresses IP réutilisées. Par conséquent, ces adresses IP réutilisées doivent être traduites en différentes adresses IP. Pour traduire les adresses IP réutilisées, l'appliance NetScaler doit effectuer les opérations suivantes :

1. Interrogez un serveur virtuel d'équilibrage de charge DNS pour obtenir la résolution de la destination.
2. Mettez à jour l'adresse IP d'origine et le numéro de port de la destination.
3. Renvoie la demande au pare-feu.

Envisagez le déploiement suivant qui comporte une appliance NetScaler configurée pour la redirection directe du cache du proxy, un pare-feu et deux routeurs (routeur 1 et routeur 2). Le trafic réseau circule vers Internet 1 via le routeur 1 et vers Internet 2 via le routeur 2 respectivement.



Dans cet exemple, les demandes d'entrée des clients proviennent de deux VLAN différents, VLAN11 ou VLAN12. L'adresse IP du client (10.0.0.0) est réutilisée.
Selon les politiques de redirection du cache et de commutation de contenu, la demande peut être

transmise directement au serveur d'origine ou au pare-feu.

- Si la demande doit contourner le pare-feu et accéder à Internet, en fonction du VLAN de la demande d'entrée, le routeur 1 ou le routeur 2 est sélectionné et la demande est envoyée à Internet 1 ou Internet 2.
- Si la demande doit passer par le pare-feu, l'adresse IP source de la demande doit être traduite en une adresse IP spécifique. L'adresse IP traduite peut être utilisée pour identifier le VLAN par lequel la demande provient. Par exemple, si la demande d'entrée provient du VLAN11, l'adresse IP source est traduite en 11.x.x.x. Si la demande provient du VLAN12, l'adresse IP source est traduite en 12.x.x.x.

Une fois que le pare-feu a traité la demande, celle-ci est renvoyée à l'appliance. À l'aide de la combinaison de la politique d'écoute et des profils réseau, l'appliance traduit ensuite l'adresse IP source en adresse IP d'origine et envoie la demande au routeur 1 ou au routeur 2 en fonction de l'ID VLAN d'entrée.

Remarque : Le mode du serveur virtuel d'équilibrage de charge lié au cache doit toujours être réglé sur le mode MAC. Bien que le mode IP de cette fonctionnalité ne soit pas bloqué, le réglage en mode IP entraîne un comportement inattendu.

Pour traduire l'adresse IP de destination et le numéro de port de la demande en adresse IP d'origine à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
set cr vserver <vsname> -useoriginIpPortForCache <YES|NO>
<!--NeedCopy-->
```

Exemple :

```
set cr vserver cvsrv1 -useoriginIpPortForCache YES
<!--NeedCopy-->
```

Lorsque UseOriginIPPortForCache est défini sur Oui et si la demande doit être traitée à partir des serveurs mis en cache, l'adresse IP de destination de la demande est convertie en adresse IP du serveur d'origine.

Remarque : Si UseOriginIPPortForCache est activé, définissez toujours le serveur virtuel d'équilibrage de charge lié au cache en mode MAC.

Pour traduire l'adresse IP de destination et le port de la demande en adresse IP d'origine à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Redirection du cache** > **Serveurs virtuels** et cliquez sur **Ajouter**.

2. Spécifiez les détails du serveur virtuel de redirection du cache.
3. Sélectionnez **Utiliser le port IP d'origine** pour le cache afin d'activer la traduction de l'adresse IP de destination de la demande en adresse IP d'origine.
4. Cliquez sur **OK**.

Clustering

May 5, 2023

> **Remarque**
>
> Cette fonctionnalité est disponible avec une licence NetScaler Advanced ou Premium.

Un cluster NetScaler est un groupe d'appliances nCore travaillant ensemble sous la forme d'une image système unique. Chaque appliance du cluster est appelée nœud. Le cluster peut comporter une appliance ou jusqu'à 32 appliances matérielles ou virtuelles NetScaler nCore en tant que nœuds.

Le trafic client est réparti entre les nœuds pour fournir une haute disponibilité, un haut débit et une évolutivité.

Pour créer un cluster, vous devez suivre les étapes suivantes :

- Ajoutez les appliances en tant que nœuds de cluster.
- Configurez la communication entre les nœuds.
- Configurez des liens vers les réseaux du client et du serveur.
- Configurez les appliances et configurez la distribution du trafic client et serveur.

Matrice de prise en charge pour le cluster NetScaler

May 5, 2023

Le clustering dans l'appliance NetScaler prend en charge un large éventail de fonctionnalités dans les configurations NetScaler.

Le tableau suivant répertorie les fonctionnalités de NetScaler et indique l'état de prise en charge des différentes versions de NetScaler de configurations de clusters. L'état de prise en charge de certaines fonctionnalités NetScaler dans un cluster NetScaler BLX est différent de celui d'un cluster NetScaler non-BLX (MPX, ou VPX, SDX ADC).

> **Important**
>
> L'entrée « Niveau de nœud » dans le tableau indique que la fonctionnalité est prise en charge uniquement sur les nœuds de cluster individuels.

Fonctionnalités de NetScaler	12.1	13	Cluster NetScaler BLX 13.0	NetScaler 13.1	Cluster NetScaler BLX 13.1
FIPS SSL	Non	Non	Non	Non	Non
Offre groupée de certificats SSL	Non	Non	Non	Non	Non
Interception SSL	Non	Non	Non	Non	Non
Actions de changement de contenu	Oui	Oui	Oui	Oui	Oui
Journalisation basée sur des règles pour les stratégies de changement de contenu	Oui	Oui	Oui	Oui	Oui
Limitation de débit	Oui	Oui	Oui	Oui	Oui
Analyse des actions	Oui	Oui	Non	Oui	Non
GSLB	Oui	Oui	Oui	Oui	Oui
RTSP	Oui	Oui	Oui	Oui	Oui
DNSSEC	Non	Non	Non	Non	Non
DNS64	Non	Non	Non	Non	Non
FTP	Oui	Oui	Non	Oui	Non
TFTP	Oui	Oui	Oui	Oui	Oui

Fonctionnalités de NetScaler	12.1	13	Cluster NetScaler BLX 13.0	NetScaler 13.1	Cluster NetScaler BLX 13.1
Mise en miroir des connexions	Non	Non	Non	Non	Non
Mise en cache intégrée	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds	Non
Cache partagé volumineux	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds	Non
Optimisation frontale	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds	Non
Pare-feu d'application	Oui	Oui	Non	Oui	Non
Protection par déni de service HTTP (HDOSP)	Obsolète	Obsolète	Obsolète	Supprimé	Obsolète
Queuing prioritaire (PQ)	Niveau de noeuds	Niveau de noeuds	Obsolète	Supprimé	Obsolète
Connexion sûre (SC)	Niveau de noeuds	Niveau de noeuds	Obsolète	Supprimé	Obsolète
AppQoE	Oui	Oui	Non	Oui	Non
Protection contre les surtensions	Niveau de noeuds	Niveau de noeuds	Oui	Niveau de noeuds	Oui
MPTCP	Oui	Oui	Non	Oui	Non

Fonctionnalités de NetScaler	12.1	13	Cluster NetScaler BLX 13.0	NetScaler 13.1	Cluster NetScaler BLX 13.1
SNIP striped	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.
MSR	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.
IS-IS (IPv4 et IPv6)	Oui	Oui	Non	Oui	Non
Trames Jumbo	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Non	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Non
Tunnelage IP-IP	Oui	Oui	Non	Oui	Non

Fonctionnalités de NetScaler	12.1	13	Cluster NetScaler BLX 13.0	NetScaler 13.1	Cluster NetScaler BLX 13.1
Équilibrage de charge de liaison	Oui	Oui	Oui	Oui	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.
FIS (ensemble d'interfaces de basculement)	Oui	Oui	Non	Oui	Non
Redondance des liens (LR)	Oui	Oui	Non	Oui	Non
NAT46	Non	Oui	Oui	Oui	Oui
NAT64	Non	Oui	Oui	Oui	Oui
RNAT6	Oui	Oui	Oui	Oui	Oui
LSN/CGNAT	Oui	Oui	Non	Oui	Non
ReadyLogo IPv6	Oui	Oui	Non	Oui	Non
Domaines de trafic	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Non	Oui ; Remarque : pris en charge dans les clusters L2. Non pris en charge dans les clusters L3.	Non
Moniteur de routage	Oui	Oui	Oui	Oui	Oui

Fonctionnalités de NetScaler	12.1	13	Cluster NetScaler BLX 13.0	NetScaler 13.1	Cluster NetScaler BLX 13.1
Tunnelage GRE (CB)	Non	Non	Non	Non	Non
Mode couche 2	Oui	Oui	Non	Oui	Non
Profils de réseau	Oui	Oui	Non	Oui	Non
Légende HTTPS	Oui	Oui	Oui	Oui	Oui
AAA-TM	Oui	Oui	Non	Oui	Non
AppFlow	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds	Non
Web Insight	Oui	Oui	Non	Oui	Non
HDX Insight	Oui	Oui	Non	Oui	Non
VMAC/VRRP	Oui	Oui	Non	Oui	Non
NetScaler Push	Non	Non	Non	Non	Non
Basculement de connexion avec état	Non	Non	Non	Non	Non
Arrêt gracieux	Oui	Oui	Oui	Oui	Oui
Mise à l'Autoscale DBS	Non	Oui	Oui	Oui	Oui
DSR utilisant TOS	Non	Non	Oui	Oui	Oui
Finer Startup-RR Control	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds	Non
XML XSM	Non	Non	Non	Non	Non
DHCP RA	Non	Non	Non	Oui	Non
Groupe de ponts	Oui	Oui	Non	Oui	Non

Fonctionnalités de NetScaler	12.1	13	Cluster NetScaler BLX 13.0	NetScaler 13.1	Cluster NetScaler BLX 13.1
Pont réseau	Non	Non	Non	Non	Non
Interface Web sur NetScaler (WIonNS)	Oui	Oui	Non	Oui	Non
Surveillance EdgeSight	Obsolète	Obsolète	Non	Obsolète	Non
Tables de mesures - Local	Non	Non	Non	Non	Non
Mise en cache DNS	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds	Niveau de noeuds
Call Home	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds	Non
{{page.gateway-onprem}} Mode proxy ICA	Oui	Oui	Non	Oui	Non
{{page.gateway-onprem}} (VPN SSL/VPN complet et VPN sans client)	Niveau de noeuds	Niveau de noeuds	Non	Niveau de noeuds	Non
Connecteur Citrix CloudBridge	Oui	Oui	Non	Oui	Non
Routage basé sur des stratégies (PBR/PBR6)	Oui	Oui	Non	Oui	Non

Fonctionnalités de NetScaler	12.1	13	Cluster NetScaler BLX 13.0	NetScaler 13.1	Cluster NetScaler BLX 13.1
Routage basé sur une stratégie IPv4 (PBR) avec serveur virtuel LLB comme prochain saut	Non	Oui	Non	Oui	Non
Routage basé sur une stratégie IPv6 (PBR6) avec serveur virtuel LLB comme saut suivant	Non	Non	Non	Non	Non
Sensibilisation des abonnés	Non	Non	Non	Non	Non
Routage dynamique	Oui, avec prise en charge des protocoles v6 (ospfv3, RipNG, ISIS6, BGP6)	Oui, avec prise en charge des protocoles v6 (ospfv3, RipNG, ISIS6, BGP6)	Oui	Oui, avec prise en charge des protocoles v6 (ospfv3, RipNG, ISIS6, BGP6)	Oui
SYSLOG-TCP, équilibrage de charge des serveurs syslog, prise en charge SNIP et prise en charge de FQDN pour syslog	Oui	Oui	Oui	Oui	Oui

Fonctionnalités de NetScaler	12.1	13	Cluster NetScaler BLX 13.0	NetScaler 13.1	Cluster NetScaler BLX 13.1
Gestion des robots	Non	Oui	Non	Oui	Non
VXLAN	Non	Non	Non	Non	Non
NSVLAN	Oui	Oui	Non	Oui	Oui

Les configurations NetScaler suivantes sont également prises en charge :

Équilibrage de charge, persistance de l'équilibrage de charge, équilibrage de charge DNS, SIP, MaxClient, Spillover (connexion et dynamique). Spillover basé sur la bande passante, DataStream, le contrôle de la compression, le filtrage du contenu, la mise en mémoire tampon TCP, la redirection du cache, le déni de service distribué (DDoS). Keep-alive du client, mise en réseau de base (IPv4 et IPv6), OSPF (IPv4 et IPv6), RIP (IPv4 et IPv6), RIP (IPv4 et IPv6). VLAN, ICMP, fragmentation, MBF, ACL, ACL simple, MSR, découverte MTU de chemin, IP IP, SNMP, stratégies (classiques et avancées). Réécriture, répondeur, légende HTTP, journalisation du serveur Web, journalisation d'audit (NSLOG et Syslog). USIP, commandes de localisation, API NITRO, AppExpert, KRPC.

Les configurations NetScaler suivantes sont également prises en charge :

Équilibrage de charge, persistance de l'équilibrage de charge, équilibrage de charge DNS, SIP, MaxClient, Spillover (connexion et dynamique). Spillover basé sur la bande passante, DataStream, le contrôle de la compression, le filtrage du contenu, la mise en mémoire tampon TCP, la redirection du cache, le déni de service distribué (DDoS). Keep-alive du client, mise en réseau de base (IPv4 et IPv6), OSPF (IPv4 et IPv6), RIP (IPv4 et IPv6), RIP (IPv4 et IPv6). VLAN, ICMP, fragmentation, MBF, ACL, ACL simple, MSR, découverte MTU de chemin, IP IP, SNMP, stratégies (classiques et avancées). Réécriture, répondeur, légende HTTP, journalisation du serveur Web, journalisation d'audit (NSLOG et Syslog). USIP, commandes de localisation, API NITRO, AppExpert, KRPC.

Composants requis

July 31, 2023

Les appliances NetScaler (MPX, VPX, SDX ADC, BLX) qui doivent être ajoutées à un cluster doivent répondre aux prérequis suivants :

- Toutes les appliances doivent avoir la même version et la même version logicielles.

- Toutes les appliances doivent être du même type de plate-forme. Cela signifie qu'un cluster doit disposer de toutes les appliances matérielles (NetScaler MPX) ou de toutes les appliances NetScaler VPX, de toutes les appliances NetScaler BLX ou de toutes les instances NetScaler SDX ADC.

  Remarque :

  - Pour un cluster d'appliances matérielles (MPX), les appliances doivent être du même type de modèle.
  - Pour la formation du cluster hétérogène, toutes les appliances doivent être de type plate-forme MPX.
  - Pour un cluster de appliances virtuelles (VPX), les appliances doivent être déployées sur les hyperviseurs suivants : XenServer, Hyper-V, VMware ESX et KVM.
  - Pour configurer un cluster d'instances SDX NetScaler, consultez Configurer un cluster d'instances NetScaler.
  - Les trames Jumbo sont prises en charge sur un cluster NetScaler composé d'instances NetScaler SDX.
  - Vous pouvez créer des clusters L3 d'instances SDX.
  - Pour plus d'informations sur la configuration d'un cluster NetScaler BLX, consultez la section Cluster NetScalerBLX.
- Les appareils peuvent appartenir à différents réseaux.
- Être initialement configuré et connecté à un réseau côté client et côté serveur commun.
- Pour un cluster d'appliances virtuelles (instance NetScaler VPX, NetScaler BLX ou NetScaler SDX ADC) comportant de grandes configurations, il est recommandé d'utiliser 6 Go de RAM pour chaque nœud du cluster.

Aperçu des clusters

May 5, 2023

Un cluster NetScaler est formé en regroupant les appliances NetScaler. En fonction de l'emplacement réseau des appliances NetScaler auxquelles vous souhaitez ajouter le cluster, vous devez connaître les configurations de cluster suivantes :

> **Remarque**
>
> Sauf indication contraire, les fonctionnalités et les configurations des clusters sont les mêmes pour les clusters L2 et L3.

- **Cluster L2 :** dans ce déploiement de cluster, tous les nœuds du cluster appartiennent au même réseau.



- **Cluster L3 (également appelé « cluster en mode INC ») :** dans ce déploiement de cluster, les nœuds du cluster peuvent appartenir à différents réseaux. Les nœuds de cluster d'un réseau spécifique doivent être regroupés en groupes de nœuds qui incluent uniquement les nœuds de ce réseau. Sur la figure suivante, nous voyons que les nœuds n1, n2, n3 font partie du même réseau et sont regroupés dans Nodegroup1.

  De même, c'est le cas pour les nœuds n4 et n5, qui sont regroupés dans Nodegroup2. Dans le troisième réseau, il existe deux groupes de nœuds. Nodegroup3 inclut n6 et n7 et Nodegroup4 inclut n8 et n9.

  > **Remarque**
  >
  > Pris en charge à partir de NetScaler 11.0.



- **État de synchronisation :** la commande **show cluster** affiche l'état du nœud du cluster. Les états de synchronisation de la commande **show cluster node** sont les suivants :
  - **Activer :**cet état indique que le nœud a la capacité d'effectuer une synchronisation de configuration à partir d'autres nœuds.
  - **En cours :** il s'agit d'un état temporaire qui s'affiche lorsque le nœud synchronise les configurations d'autres nœuds.
  - **Succès :** cet état représente l'état de la dernière synchronisation qui a eu lieu sur ce nœud.

Synchronisation entre les nœuds de cluster

May 5, 2023

Toutes les configurations d'un cluster NetScaler sont effectuées sur l'adresse IP du cluster, qui est l'adresse de gestion du cluster. Le nœud du cluster possède l'adresse IP du cluster appelée coordinateur de configuration du cluster (CCO), comme illustré dans la figure suivante :



Les configurations disponibles sur le CCO sont automatiquement propagées aux autres nœuds du cluster et, par conséquent, tous les nœuds du cluster ont les mêmes configurations.

- NetScaler n'autorise que quelques configurations à effectuer sur des nœuds de cluster individuels via leur adresse NSIP. Dans ces cas, vous devez garantir manuellement la cohérence de la configuration sur tous les nœuds du cluster. Ces configurations ne sont pas propagées sur les autres nœuds de cluster. Pour plus d'informations sur les opérations prises en charge sur chaque nœud de cluster, voir Opérations prises en charge sur des nœuds de cluster individuels.
- Les commandes suivantes lorsqu'elles sont exécutées sur l'adresse IP du cluster ne sont pas propagées vers d'autres nœuds de cluster :
  - **arrêt.** Ferme uniquement le coordinateur de configuration.
  - **redémarrer.** Redémarre uniquement le coordinateur de configuration.
  - **instance de cluster rm.** Supprime l'instance de cluster du nœud sur lequel vous exécutez la commande.
- Pour qu'une commande soit propagée vers d'autres nœuds du cluster :
  - Le quorum doit être configuré sur l'instance du cluster.
  - La majeure partie du quorum du cluster avec (n/2 + 1) des nœuds du cluster doit être active pour que le cluster soit opérationnel.
  - Un cluster peut fonctionner avec un nombre minimum de nœuds lorsque la règle de la majorité (n/2 + 1) est assouplie.

Lorsqu'un nœud est ajouté à un cluster, les configurations et les fichiers (certificats SSL, licences, DNS, etc.) disponibles sur le CCO sont synchronisés avec le nœud de cluster nouvellement ajouté. Lorsqu'un nœud de cluster existant, qui a été désactivé intentionnellement ou qui a échoué, est à nouveau ajouté, le cluster compare les configurations disponibles sur le nœud avec les configurations disponibles sur le CCO. En cas de non-concordance entre les configurations, le nœud est synchronisé à l'aide de l'une des méthodes suivantes :

- **Full synchronization.** Si la différence entre les configurations dépasse 255 commandes, toutes

les configurations du CCO sont appliquées au nœud qui rejoint le cluster. Le nœud reste indisponible sur le plan opérationnel pendant la synchronisation.

- **Synchronisation incrémentielle.** Si la différence entre les configurations est inférieure ou égale à 255 commandes, seules les configurations qui ne sont pas disponibles sont appliquées au nœud qui rejoint le cluster. L'état de fonctionnement du nœud n'est pas affecté.

> **Remarque**
>
> Vous pouvez également synchroniser manuellement les configurations et les fichiers. Pour plus d'informations, consultezSynchronisation des configurations de cluster et Synchronisation des fichiers de cluster.

Configurations striped, striped partielles et spotted

August 20, 2021

En vertu de la propagation des commandes, tous les nœuds d'un cluster ont les mêmes configurations. Toutefois, vous pouvez souhaiter que certaines configurations soient disponibles uniquement sur certains nœuds de cluster. Bien que vous ne puissiez pas restreindre les nœuds sur lesquels les configurations sont disponibles, vous pouvez spécifier les nœuds sur lesquels les configurations sont actives.

Par exemple, vous pouvez :

- définir une adresse SNIP pour être active sur un seul noeud, ou
- définir une adresse SNIP pour être active sur tous les nœuds, ou
- définir une adresse VIP pour être active sur un seul noeud, ou
- définir une adresse VIP pour être active sur tous les nœuds, ou
- définir une adresse VIP pour être active uniquement sur deux nœuds d'un cluster à 3 nœuds

Selon le nombre de nœuds sur lesquels les configurations sont actives, les configurations de cluster sont appelées configurations striped, striped partielles et spotted.

Figure 1. Cluster à trois nœuds avec configurations striped, striped partielles et spotted



Le tableau suivant fournit plus de détails sur les types de configurations :

Type de configuration	Actif sur	Applicable à	Configurations
Configuration par bandes	Tous les nœuds de cluster	Toutes les entrées	Aucune configuration spécifique n'est requise pour créer une entité striped. Par défaut, toutes les entités définies sur une adresse IP de cluster sont agrégées sur tous les nœuds de cluster.
Configuration striped partielle	Sous-ensemble de nœuds de cluster	Reportez-vous à Groupes de nœuds de cluster.	Liez les entités que vous souhaitez partiellement striped à un groupe de nœuds. La configuration est active uniquement sur les nœuds de cluster appartenant au groupe de nœuds.

Type de configuration	Actif sur	Applicable à	Configurations
Configuration spotted	Nœud de cluster unique	Adresse SNIP, ID de moteur SNMP, nom d'hôte des nœuds de cluster, entités pouvant être liées à un groupe de nœuds	Une configuration spotted peut être définie à l'aide de l'une des deux approches. **Adresse SNIP** Lors de la création de l'adresse SNIP, spécifiez le nœud sur lequel vous souhaitez que l'adresse SNIP soit active, en tant que nœud propriétaire. **Exemple**, `add ns ip 10.102.29.106 255.255.255.0 -type SNIP -ownerNode 2` (en supposant que l'ID NS2 du nœud est 2). **Remarque** : vous ne pouvez pas modifier la propriété d'une adresse SNIP spotted au moment de l'exécution. Pour modifier la propriété, vous devez d'abord supprimer l'adresse SNIP et l'ajouter à nouveau en spécifiant le nouveau propriétaire. **Entités pouvant être liées à un groupe de nœuds.** En liant l'entité à un groupe de nœuds à un seul membre.

Type de configuration	Actif sur	Applicable à	Configurations

> **Remarque**
>
> - Lorsque vous désactivez USIP, Citrix vous recommande d'utiliser des adresses SNIP repérées. Vous pouvez utiliser des adresses SNIP striped uniquement en cas de pénurie d'adresses IP. L'utilisation d'adresses IP striped peut entraîner des problèmes de flux ARP si aucune adresse IP spotted n'est présente dans le même sous-réseau pour la résolution ARP.
> - Lorsque vous activez USIP, Citrix vous recommande d'utiliser des adresses SNIP striped en tant que Gateway pour le trafic initié par le serveur.

Prise en charge des propriétaires ARP pour IP par bandes

Dans une configuration de cluster, vous pouvez configurer un nœud spécifique pour répondre à la demande ARP pour une adresse IP répartie. Le nœud configuré répond au trafic ARP.

Un nouveau paramètre « ARPowner » est introduit dans les commandes « add, set et unset IP ».

Pour activer le propriétaire ARP sur un nœud à l'aide de l'interface de ligne de commande.

À l'invite de commandes, tapez :

```
add ns ip <ip_address> -arpOwner <node_id>
```

> **Remarque**
>
> Le paramètre propriétaire ARP est pris en charge uniquement dans le cluster L2.

Prise en charge du propriétaire de découverte de voisins pour l'adresse IPv6 par répartition

Dans une configuration de cluster, vous pouvez configurer un nœud spécifique en tant que propriétaire de découverte de voisin (ND) pour l'adresse IPv6 par répartition afin de déterminer l'adresse de la couche de liaison. Un client envoie un message de sollicitation de voisin (NS) à tous les nœuds de la configuration du cluster. Le propriétaire ND répond à l'aide d'un message Neighbor Advertisement (NA) avec l'adresse de couche de liaison pour l'adresse IPv6 par répartition et sert le trafic.

Pour activer le propriétaire ND sur un nœud à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
add ns ip6 <IPv6Address> -ndOwner <node id>

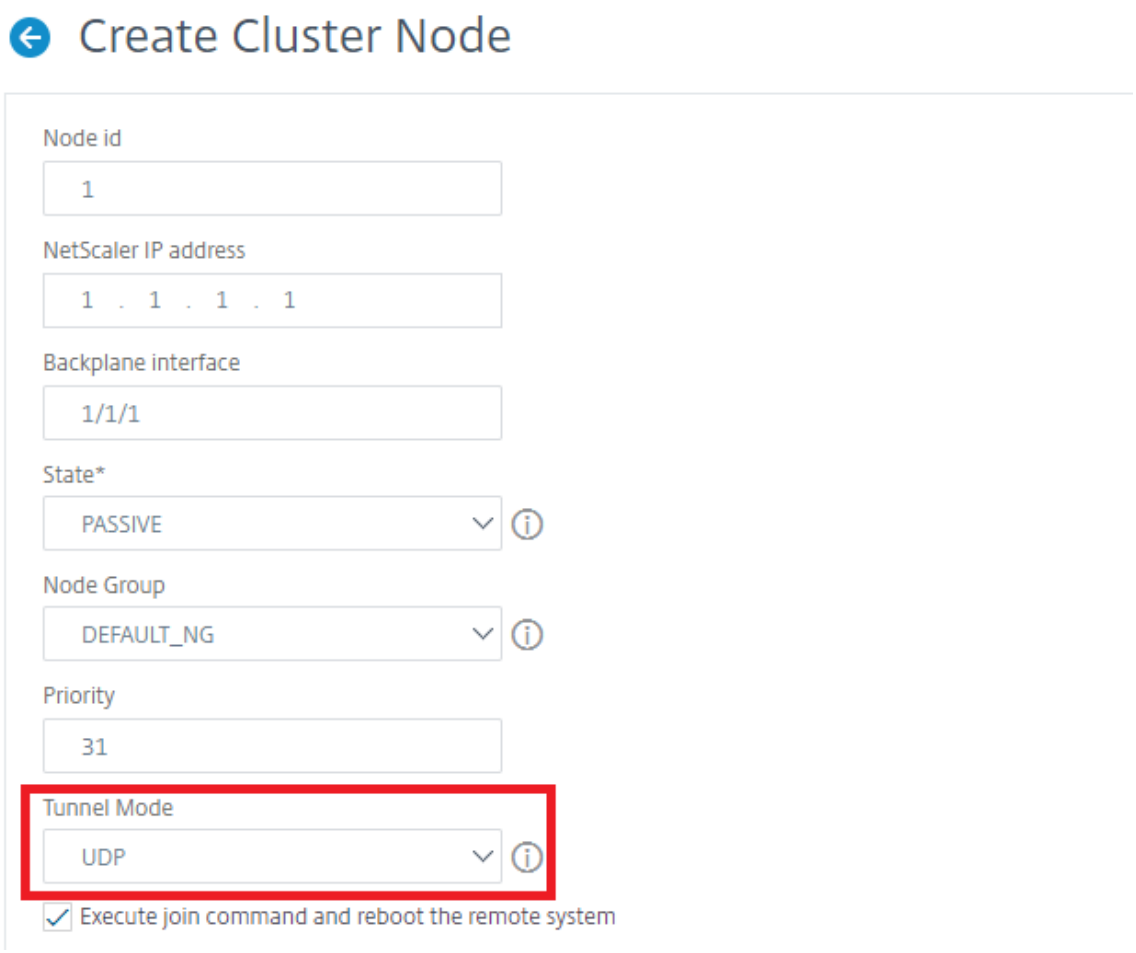
set  ns ip6 <IPv6Address> -ndOwner <node id>
<!--NeedCopy-->
```

Exemple :

```
add ns ip6 2001::21/64 -ndOwner 1

set ns ip6 2001::21/64 -ndOwner 1
<!--NeedCopy-->
```

Pour activer le propriétaire ND sur un nœud à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > IP**.
2. Dans la page **IPs**, accédez à l'onglet **IPv6s** et cliquez sur **Ajouter**.
3. Dans la page **Créer IPv6**, sélectionnez l'un des ID de noeud répertoriés dans **NDOwner dans le menu déroulant Cluster**.

> **Remarque**
>
> Le paramètre de propriétaire ND est pris en charge uniquement dans le cluster L2.

Communication dans une configuration de cluster

May 5, 2023

Les interfaces des appliances NetScaler ajoutées à un cluster sont préfixées par un ID de nœud. Cela permet d'identifier le nœud du cluster auquel appartient l'interface. Par conséquent, l'identifiant d'interface c/u, où c est le numéro du contrôleur et u le numéro d'unité, devient désormais n/c/u, où n est l'ID du nœud. Par exemple, dans la figure suivante, l'interface 1/2 du nœud n1 est représentée par 0/1/2, l'interface 1/1 du nœud n2 est représentée par 1/1/1 et l'interface 1/4 du nœud n3 est représentée par 2/1/4.

Figure 1. Convention de dénomination des interfaces dans un cluster



- **Communication avec le serveur** :
  le cluster communique avec le serveur via les connexions physiques entre le nœud du cluster et le périphérique de connexion côté serveur. Le groupement logique de ces connexions physiques est appelé plan de données du serveur.
- **Communication avec le client** : le cluster communique avec le client via les connexions physiques entre le nœud du cluster et le périphérique de connexion côté client. Le regroupement logique de ces connexions physiques est appelé plan de données client.
- **Communication entre les nœuds** : les nœuds du cluster peuvent également communiquer entre eux. La manière dont ils communiquent varie selon que le nœud existe sur le même réseau ou sur plusieurs réseaux.
  - Les nœuds de cluster d'un même réseau communiquent entre eux à l'aide du backplane du cluster. Le backplane est un ensemble d'interfaces dans lequel une interface de chaque nœud est connectée à un commutateur commun, appelé commutateur de fond de cluster. Les différents types de trafic qui transitent par le panneau arrière utilisé pour la communication entre nœuds sont les suivants :
    * Messagerie nœud à nœud (NNM)
    * Trafic dirigé
    * Propagation et synchronisation de la configuration
  - Chaque nœud du cluster utilise une adresse de commutateur de fond de cluster MAC spéciale pour communiquer avec les autres nœuds via le backplane. Le MAC spécial du cluster se présente sous la forme suivante : `0x02 0x00 0x6F <cluster_id> <node_id> <reserved>`), où se `cluster_id` trouve l'ID de l'instance du cluster, `node_id` est le numéro de nœud de l'appliance NetScaler ajoutée à un cluster.

Les figures suivantes montrent les interfaces de communication dans les clusters L2 et L3.

Figure 2. Interfaces de communication de cluster - cluster L2



Figure 3. Interfaces de communication de cluster - cluster L3



Distribution du trafic dans une configuration de cluster

May 5, 2023

Dans une configuration en cluster, les réseaux externes considèrent l'ensemble des appliances NetScaler comme une entité unique. Ainsi, le cluster doit sélectionner un nœud unique qui doit recevoir le trafic. Le cluster effectue cette sélection en utilisant le mécanisme ECMP (Equal Cost Multiple Path) ou le mécanisme de distribution du trafic par agrégation de liens de cluster. Le nœud sélectionné est appelé récepteur de flux.

> **Remarque**
>
> Pour un cluster L3 (nœuds répartis sur différents réseaux), seule la distribution du trafic ECMP peut être utilisée.

Le récepteur de flux reçoit le trafic puis, à l'aide de la logique de cluster interne, détermine le nœud qui doit traiter le trafic. Ce nœud est appelé processeur de flux. Le récepteur de flux oriente le trafic vers le processeur de flux via le fond de panier si le récepteur de flux et le processeur de flux se trouvent

sur le même réseau. Le trafic est dirigé à travers le tunnel si le récepteur de débit et le processeur de débit se trouvent sur des réseaux différents.

> **Remarque**
>
> - Le récepteur de flux et le processeur de flux doivent être des nœuds capables de traiter le trafic.
> - À partir de NetScaler 11, vous pouvez désactiver la direction sur le backplane du cluster. Pour plus d'informations, voir Désactivation du pilotage sur le fond de panier de cluster.

Figure 1. Distribution du trafic dans un cluster



La figure précédente montre une demande client qui traverse le cluster. Le client envoie une demande à une adresse IP virtuelle (VIP). Un mécanisme de distribution du trafic configuré sur le plan de données client sélectionne l'un des nœuds du cluster comme récepteur de flux. Le récepteur de flux reçoit le trafic, détermine le nœud qui doit traiter le trafic et dirige la demande vers ce nœud (à moins que le récepteur de flux ne se sélectionne lui-même comme processeur de flux).

Le processeur de flux établit une connexion avec le serveur. Le serveur traite la demande et envoie la réponse à l'adresse IP du sous-réseau (SNIP) qui a envoyé la demande au serveur.

- Si l'adresse SNIP est une adresse IP entrelacée ou partiellement entrelacée, le mécanisme de distribution du trafic configuré sur le plan de données du serveur sélectionne l'un des nœuds du cluster comme récepteur de flux. Le récepteur de flux reçoit le trafic, détermine le processeur de flux et dirige la demande vers le processeur de flux via le panneau principal du cluster.
- Si l'adresse SNIP est une adresse IP spotted, le nœud qui possède l'adresse SNIP reçoit la réponse du serveur.

Dans une topologie de cluster asymétrique (tous les nœuds de cluster ne sont pas connectés au commutateur externe), vous devez utiliser des jeux de liens exclusivement ou combinés avec ECMP ou agrégation de liens de cluster. Pour plus d'informations, voir Utilisation de jeux de liens.

Groupes de nœuds de cluster

May 5, 2023

> **Remarque**
>
> Les groupes de nœuds sont pris en charge à partir de NetScaler 10.1.

Comme son nom l'indique, un groupe de nœuds de cluster est un groupe de nœuds de cluster.

Figure 1. Cluster NetScaler avec groupes de nœuds



La figure précédente montre un cluster dont les groupes de nœuds NG1 et NG2 incluent chacun 3 nœuds de cluster. Le cluster possède également 3 nœuds qui ne font partie d'aucun groupe de nœuds.

Un groupe de nœuds peut être configuré pour les opérations suivantes :

- Pour définir des configurations spotted et striped partielles. Pour plus d'informations, voir Groupes de nœuds pour configurations ponctuées et partiellement réparties.
- Pour configurer la redondance des groupes de nœuds. Pour plus d'informations, voir Configuration de la redondance pour les groupes de nœuds.
  Remarque : pris en charge à partir de NetScaler 10.5 Build 52.1115.e.

- Pour définir un cluster L3 (également appelé cluster en mode INC). Dans un cluster L3, les nœuds du cluster peuvent provenir de différents réseaux. Vous devez regrouper les nœuds qui appartiennent à un réseau dans un seul groupe de nœuds. Par exemple, si n1, n2, n3 sont dans network1 et n4, n5, n6 sont dans network2, alors NG1 doit inclure des nœuds de network1 et NG2 doit inclure des nœuds de network2. Pour configurer un cluster L3, consultez la section Création d'un cluster NetScaler.

> **Remarque**
>
> - Pris en charge à partir de NetScaler 11.
> - Les fonctions précédentes d'un groupe de nœuds s'excluent mutuellement. Cela signifie qu'un groupe de nœuds ne peut fournir qu'une seule des fonctionnalités mentionnées ci-dessus.

État du cluster et du nœud

January 21, 2021

Pour qu'un cluster soit fonctionnel, la plupart des nœuds (n/2 + 1) doivent être opérationnels (l'état opérationnel est ACTIF).

> **Important**
>
> À partir de NetScaler version 10.5, vous pouvez configurer le cluster pour qu'il soit fonctionnel même lorsque le critère majoritaire n'est pas satisfait. Cette configuration doit être effectuée lors de la création d'un cluster.

Pour plus d'informations sur les états d'un nœud de cluster, reportez-vous à la section États d'un nœud de cluster.

Routage dans un cluster

May 5, 2023

Le routage dans un cluster fonctionne à peu près de la même manière que le routage dans un système autonome. Quelques points à noter :

- Toutes les configurations de routage doivent être effectuées à partir de l'adresse IP du cluster et les configurations sont propagées aux autres nœuds du cluster.
- Les routes sont limitées au nombre maximum de routes ECMP prises en charge par le routeur en amont.

- Les configurations de routage spécifiques au nœud doivent être effectuées à l'aide de l'argument owner-node comme suit :

```
  router ospf
    owner-node 0
      ospf router-id 97.131.0.1
    exit-owner-node
  !
<!--NeedCopy-->
```

La commande suivante affiche la configuration de cluster consolidée pour tous les nœuds de VTYSH.

```
show cluster-config
```

La commande suivante affiche l'état du cluster sur chaque nœud.

```
show cluser node
```

Routage IPv4 dans un cluster L2

La section suivante contient des exemples de configurations qui vous aident à configurer le routage IPv4 OSPF et BGP dans le cluster L2.

Ajouter une adresse SNIP repérée et activer le routage dynamique

Dans la configuration suivante, le routage OSPF et BGP est activé. Des adresses SNIP repérées sont également ajoutées et le routage dynamique est activé sur ces adresses SNIP.

```
en ns fea ospf bgp
add vlan 10
add ns ip 10.10.10.1 255.255.255.0 -dynamicrouting enabled -ownernode 1
add ns ip 10.10.10.2 255.255.255.0 -dynamicrouting enabled -ownernode 2
add ns ip 10.10.10.3 255.255.255.0 -dynamicrouting enabled -ownernode 3
bind vlan 10 -ipaddress 10.10.10.1 255.255.255.0
<!--NeedCopy-->
```

Configuration OSPF VTYSH IPv4

Pour configurer l'OSPF IPv4 dans le cluster L2, vous devez :

- Définissez la priorité sur zéro.
- Configurez l'ID du routeur en tant que configuration repérée.

> **Remarque**
>
> Les directives de configuration OSPF pour le cluster L2 s'appliquent également à OSPFv3.

Dans l'exemple de configuration suivant, l'OSPF IPv4 est configuré.

```
       interface vlan10
        IP OSPF PRIORITY 0
        !
       router ospf
           owner-node 1
             ospf router-id 97.131.0.1
           exit-owner-node
           owner-node 2
             ospf router-id 97.131.0.2
           exit-owner-node
           owner-node 3
             ospf router-id 97.131.0.3
           exit-owner-node
       network 10.10.10.0/24 area 0
       redistribute kernel
        !
<!--NeedCopy-->
```

Configuration BGP VTSH IPv4

Dans l'exemple de configuration VTYSH suivant, le protocole BGP IPv4 est configuré.

```
     router bgp 100
       neighbor 10.10.10.10 remote-as 200
      owner-node 1
       neighbor 10.10.10.10 update-source 10.10.10.1
      exit-owner-node
      owner-node 2
       neighbor 10.10.10.10 update-source 10.10.10.2
      exit-owner-node
      owner-node 3
       neighbor 10.10.10.10 update-source 10.10.10.3
      exit-owner-node
     redistribute kernel
     !
<!--NeedCopy-->
```


> **Remarque**
>
> La commande update-source est utilisée pour chaque voisin avec l'argument owner-node dans la configuration suivante afin de se connecter à l'adresse IP source appropriée.

Routage IPv6 dans un cluster L2

La section suivante contient des exemples de configurations qui vous aident à configurer le routage IPv6 OSPF et BGP dans le cluster L2.

Activer le routage IPv6

Avant de configurer le routage IPv6 dans un cluster L2, vous devez activer la fonctionnalité IPv6.

Pour activer le routage IPv6 à l'aide de l'interface de ligne de commande,

À l'invite de commande, tapez :

- `enable ns fea ipv6pt`

Ajouter une adresse SNIP6 repérée et activer le routage dynamique

Dans la configuration suivante, le routage OSPF et BGP est activé. Des adresses SNIP6 repérées sont également ajoutées et le routage dynamique est activé sur ces adresses SNIP6.

```
add ns ip6 3ffa::1/64 -dynamicrouting enabled -ownernode 1
add ns ip6 3ffa::2/64 -dynamicrouting enabled -ownernode 2
add ns ip6 3ffa::3/64 -dynamicrouting enabled -ownernode 3
add vlan 10
bind vlan 10 -ipaddress 3ffa::1/64
<!--NeedCopy-->
```

Configuration BGP IPv6 VTYSH

Dans l'exemple de configuration VTYSH suivant, le protocole BGP IPv6 est configuré.

```
  router bgp 100
   neighbor 3ffa::10 remote-as 200
     owner-node 1
      neighbor 3ffa::10 update-source 3ffa::1
     exit-owner-node
     owner-node-2
      neighbor 3ffa::10 update-source 3ffa::2
     exit-owner-node
```



```
    owner-node-3
     neighbor 3ffa::10 update-source 3ffa::3
    exit-owner-node
   no neighbor 3ffa::10 activate
   address-family ipv6
    redistribute kernel
    neighbor 3ffa::10 activate
   exit-address-family
  !
<!--NeedCopy-->
```

Installer les routes apprises en IPv6

Le cluster NetScaler peut utiliser des routes apprises par différents protocoles de routage après avoir installé les routes dans la table de routage du cluster NetScaler.

Pour installer les itinéraires IPv6 appris vers la table de routage interne à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `ns route-install ipv6 bgp`
- `ns route-install ipv6 ospf`
- `ns route-install default`

> **Remarque**
>
> - Si vous devez échanger des routes IPv4 sur un voisin IPv6, vous devez supprimer la commande `no neighbor 3ffa::10 active` VTYSH de la configuration précédente.
> - La commande `update-source` VTYSH doit être utilisée pour chaque nœud propriétaire afin de spécifier la bonne adresse IP source IPv6 lors de la connexion à l'homologue BGP, comme indiqué dans la configuration IPv4 BGP.

Routage dans un cluster L3

Le routage dans un cluster L3 ne fonctionne que lorsque les configurations suivantes sont effectuées sur l'appliance NetScaler.

- Activez le routage dynamique pour un VLAN.

```
set vlan <id> -dynamicrouting enabled
<!--NeedCopy-->
```


- Pour atteindre tous les nœuds du cluster, les adresses IP VIP, CLIP et NetScaler (NSIP) doivent être annoncées par les protocoles de routage en même temps que la commande. `set vlan`

Scénario de déploiement pour BGP dans un cluster L3

Prenons un exemple où tous les nœuds du cluster sont regroupés dans le réseau AS 100 et les routeurs en amont se trouvent dans un autre AS 200.

La figure suivante décrit le déploiement de l'AS 100 et de l'AS 200 dans une configuration de cluster.



Dans ce déploiement, CLIP annonce le CCO auprès des routeurs en amont. Certains nœuds du cluster interrompent le trafic annoncé lorsqu'une boucle AS est détectée.

Pour résoudre ce problème, configurez la commande suivante en mode routeur VTYSH BGP pour chaque voisin.

À l'invite de commande VTYSH, tapez :

```
neighbor <peer_ip> allowas-in 1
```

Comme meilleure pratique, Citrix vous recommande de configurer l'une des options suivantes :

- Configurez les cartes de routage pour connaître uniquement les réseaux souhaités, tels que l'itinéraire par défaut, NetScaler IP (NSIP) et les sous-réseaux NSIP sur les nœuds du cluster.
- Configurez les routes en amont pour annoncer uniquement les réseaux souhaités tels que CLIP et NetScaler IP (NSIP) en cluster.

Adressage IP pour un cluster

May 5, 2023

Outre les types standard d'adresses IP appartenant à NetScaler (NetScaler NSIP, Virtual IP (VIP) et Subnet IP (SNIP), une appliance NetScaler en cluster peut disposer d'une adresse IP de gestion de cluster (CLIP). Il peut également comporter des adresses IP réparties par bandes et repérées.

- **Adresse CLIP.** Adresse IP appartenant au nœud coordinateur du cluster (CCO). L'adresse CLIP peut flotter entre différents nœuds dans une configuration de cluster. Si le CLIP est déplacé vers un autre nœud du cluster, ce nœud devient le CCO. Le CCO est l'appliance NetScaler qui est responsable des tâches de gestion dans le cluster. Un administrateur réseau utilise l'adresse CLIP pour se connecter au cluster afin d'effectuer des tâches de configuration et de gestion, telles que l'accès à l'interface graphique unifiée, la création de rapports, le suivi du flux de paquets et la collecte de journaux. Vous pouvez ajouter plusieurs adresses CLIP dans un cluster sur le même réseau ou sur des réseaux différents. Seules les configurations effectuées sur le CCO via l'adresse IP du cluster sont propagées vers les autres nœuds du cluster.
- **Adresse IP par bandes**. Adresse IP logique disponible sur tous les nœuds du cluster. Il peut s'agir d'une adresse VIP ou SNIP.
- **Adresse IP repérée**. Une adresse IP logique (de préférence une adresse SNIP) n'est disponible que sur un nœud. Une adresse IP repérée n'est visible que sur ce nœud. Pour minimiser les frais de gestion du trafic, Citrix vous recommande d'utiliser une adresse SNIP repérée pour les communications dorsales avec le serveur.

Le tableau suivant fournit les détails des configurations.

Adresse IP	NSIP	VIP	SNIP
Repéré	Oui	Oui	Oui
Rayé	Non	Oui	Oui

Par exemple, dans un groupe de clusters à quatre nœuds, vous devez configurer chaque nœud avec une adresse SNIP spotted. Pour plus d'informations sur la configuration d'une configuration IP ponctuée, consultez Configurations rayées, partiellement rayées et ponctuées.

Vous pouvez définir une adresse SNIP pour être active sur un seul nœud, ou active sur tous les nœuds. Si l'adresse IP virtuelle et l'adresse IP du sous-réseau ne sont disponibles que sur un nœud spécifique, il s'agit d'une configuration repérée. La configuration est définie comme agrégée par bandes si l'adresse IP du sous-réseau et l'adresse IP du serveur virtuel sont disponibles sur tous les nœuds. Les adresses SNIP repérées contribuent à réduire le trafic sur le volant et dans le panneau arrière.

Meilleures pratiques pour les liaisons VLAN et la configuration des itinéraires lors de la connexion d'un nœud au cluster

Liaisons IP VLAN

Lorsque vous liez un VLAN à l'adresse IP repérée, le cluster NetScaler doit être configuré avec les adresses IP repérées dans le même sous-réseau sur tous les nœuds. Par exemple, dans un cluster à deux nœuds avec le nœud 0 et le nœud 1, vous pouvez avoir la configuration suivante :

```
1 add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 1
2 add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 0
3 add vlan 100
4 bind vlan 100 -IPAddress 192.254.101.101 255.255.255.0
5 <!--NeedCopy-->
```

Configuration du routage

Lorsque la configuration du routage est requise avec l'adresse IP repérée comme passerelle par défaut, le cluster ADC doit être configuré avec les adresses IP repérées dans le même sous-réseau sur tous les nœuds. Par exemple, dans un cluster à deux nœuds avec le nœud 0 et le nœud 1, vous pouvez avoir la configuration suivante :

```
1 add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 1
2 add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 0
3
4 add route 192.254.102.0 255.255.255.0 192.254.101.103
5 <!--NeedCopy-->
```

> **Remarque**
>
> Dans une configuration de cluster L3, seule la configuration SNIP repérée est prise en charge.

Configuration du clustering de couche 3

May 5, 2023

Comprendre le cluster L3

La demande visant à étendre le déploiement de la haute disponibilité et à accroître l'évolutivité du trafic client sur différents réseaux a guidé la mise en place du cluster L3. Le cluster L3 vous permet de regrouper les appliances NetScaler sur des sous-réseaux individuels (cluster L2).

Le cluster L3 est également appelé « cluster en mode de configuration réseau indépendante (INC) ». Dans le déploiement d'un cluster L3, les nœuds du cluster d'un même réseau sont regroupés pour former un groupe de nœuds. Le cluster L3 utilise le tunneling GRE pour diriger les paquets sur les réseaux. Les messages de pulsation à travers les clusters L3 sont routés.

Ce document comprend les détails suivants :

- Architecture
- Exemple

Architecture

L'architecture du cluster L3 comprend les composants suivants :

- **Groupe de nœuds**. Les nœuds de cluster de chaque réseau (n1, n2) et (n3, n4), comme indiqué dans la figure suivante, sont regroupés pour former un groupe de nœuds. Ces groupes de nœuds sont reliés au commutateur de couche 3 de chaque côté du réseau.
  - Le cluster communique avec le client via les connexions physiques entre le nœud de cluster et le périphérique de connexion côté client. Le regroupement logique de ces connexions physiques est appelé plan de données client.
  - Le cluster communique avec le serveur via les connexions physiques entre le nœud du cluster et le périphérique de connexion côté serveur. Le groupement logique de ces connexions physiques est appelé plan de données du serveur.
- **Interrupteur de fond de panier.** Les nœuds de cluster d'un même réseau communiquent entre eux à l'aide du backplane du cluster. Le backplane est un ensemble d'interfaces dans lequel une interface de chaque nœud est connectée à un commutateur commun, appelé commutateur de fond de cluster.
- **Tunnel GRE.** Les paquets entre les nœuds d'un cluster L3 sont échangés via un tunnel GRE non crypté qui utilise les adresses NSIP des nœuds source et destination pour le routage. Le mécanisme de pilotage change pour les nœuds appartenant aux différents réseaux. Les paquets sont dirigés via un tunnel GRE vers le nœud de l'autre sous-réseau, au lieu de réécrire le MAC.



Exemple

Prenons un exemple de déploiement de cluster L3 comprenant les éléments suivants :

- Trois nœuds des appliances NetScaler (n1, n2 et n3) sont regroupés dans Nodegroup1.
- De même, les nœuds n4 et n5 sont regroupés dans Nodegroup2. Dans le troisième réseau, il existe deux groupes de nœuds. Nodegroup3 inclut n6 et n7 et Nodegroup4 inclut n8 et n9.
- Les appliances NetScaler qui appartiennent au même réseau sont combinées pour former un groupe de nœuds.



Points à prendre en compte avant de configurer le cluster L3

Tenez compte des points suivants avant de configurer le cluster L3 sur une appliance NetScaler :

- Le backplane n'est pas obligatoire lors de la configuration des sous-réseaux L3. Si le fond de panier n'est pas spécifié, le nœud ne passe pas à l'état d'échec du fond de panier.

  > **Remarque**
  >
  > Si vous avez plusieurs nœuds dans le même réseau L2, il est obligatoire de définir l'interface du fond de panier. Si l'interface du fond de panier n'est pas mentionnée, les nœuds passent à l'état d'échec du fond de panier.

- Les fonctionnalités L2 et les SNIP entrelacés ne sont pas pris en charge dans le cluster L3.
- La distribution du trafic externe dans le cluster L3 prend uniquement en charge le protocole ECMP (Equal Cost Multiple Path).
- Les erreurs et la fragmentation ICMP ne sont pas traitées lorsque le pilotage est désactivé dans un déploiement de cluster L3 :

- Les entités réseau (`route`, `route6`, `pbr`, et `pbr6`) doivent être liées au groupe de nœuds de configuration.
- Le VLAN, le RNAT et le tunnel IP ne peuvent pas être liés à un groupe de nœuds de configuration.
- Le groupe de nœuds de configuration doit toujours avoir la propriété STRICT « YES ».
- Les nœuds de cluster ne doivent pas être ajoutés à un groupe de nœuds de configuration via la commande « ajouter un nœud de cluster ».
- La commande `add cluster instance -INC enabled` efface les entités réseau (route, route6, PBR, pb6, RNAT, tunnel IP, ip6tunnel).
- La commande `clear config extended`+ ne prend pas en charge les entités (route, route6, PBR, pb6, RNAT, tunnel IP, ip6tunnel) dans un cluster L3.

Configuration du cluster L3

Dans une configuration de cluster L3, la commande cluster a différents attributs à configurer qui sont basés sur les nœuds et les groupes de nœuds. La configuration du cluster L3 inclut également un profil IPv6 en dehors des profils IPv4.

La configuration d'un cluster L3 sur une appliance NetScaler comprend les tâches suivantes :

- Créer une instance de cluster
- Création d'un groupe de nœuds dans un cluster L3
- Ajouter une appliance NetScaler au cluster et au groupe avec le groupe de nœuds
- Ajouter l'adresse IP du cluster au nœud
- Activer l'instance de cluster
- Enregistrez la configuration
- Ajouter un nœud à un groupe de nœuds existant
- Création d'un groupe de nœuds dans un cluster L3
- Regroupez les nouveaux nœuds dans le groupe de nœuds nouvellement créé
- Joindre le nœud au cluster

Configuration des éléments suivants à l'aide de l'interface de ligne de commande

- **Pour créer une instance de cluster**

  ```
  add cluster instance <clid> -inc (<ENABLED|DISABLED>)[-processLocal <
  ENABLED | DISABLED]
  ```

- **Pour créer un groupe de nœuds dans un cluster L3**

  ```
  add cluster nodegroup <name>
  ```


- **Pour ajouter une appliance NetScaler au cluster et l'associer à nodegroup**

  ```
  add cluster node <nodeid> <nodeip> -backplane <interface_name> node group <ng>
  ```

- **Pour ajouter l'adresse IP du cluster sur ce nœud**

  ```
  add ns ip <IPAddress> <netmask> -type clip
  ```

- **Activer l'instance de cluster**

  ```
  enable cluster instance <clId>
  ```

- **Enregistrez la configuration**

  ```
  save ns config
  ```

- **Redémarrage à chaud de l'appliance**

  ```
  reboot -warm
  ```

- **Pour ajouter un nouveau nœud à un groupe de nœuds existant**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **Pour créer un nouveau groupe de nœuds dans un cluster L3**

  ```
  add cluster nodegroup <ng>
  ```

- **Pour regrouper de nouveaux nœuds dans le groupe de nœuds nouvellement créé**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **Pour joindre le nœud au cluster**

```
1     join cluster  - clip <ip_addr> -password <password>
2
3     add cluster instance 1  - inc ENABLED  - processLocal  ENABLED
4
5        Done
6 <!--NeedCopy-->
```

> **Remarque**
>
> Le paramètre « inc » doit être ACTIVÉ pour un cluster L3.

```
1     add cluster nodegroup ng1
2
3        Done
4
5     > add cluster node 0 1.1.1.1  - state ACTIVE -backplane 0/1/1  -
          nodegroup ng1
6
```



```
7          Done
8
9       > add ns ip 1.1.1.100 255.255.255.255  - type clip
10
11         Done
12
13      > enable cluster instance 1
14
15         Done
16
17      > save ns config
18
19         Done
20
21      > add cluster node 1 1.1.1.2  - state ACTIVE  - nodegroup ng1
22
23         Done
24
25      > add cluster nodegroup ng2
26
27         Done
28
29      > add cluster node 4 2.2.2.1  - state ACTIVE  - nodegroup ng2
30
31         Done
32
33      > add cluster node 5 2.2.2.2  - state ACTIVE  - nodegroup ng2
34
35         Done
36
37      > join cluster -clip 1.1.1.100 -password nsroot
38 <!--NeedCopy-->
```

Adresse IP du cluster de publicité d'un cluster L3

Configurez l'adresse IP du cluster à annoncer au routeur en amont afin de rendre la configuration du cluster accessible depuis n'importe quel sous-réseau. L'adresse IP du cluster est annoncée en tant que route du noyau par les protocoles de routage dynamique configurés sur un nœud.

La publicité de l'adresse IP du cluster comprend les tâches suivantes :

- **Activez l'option de route hôte de l'adresse IP du cluster**. L'option de route hôte transmet l'adresse IP du cluster à une table de routage ZebOS pour la redistribution des routes du noyau via des protocoles de routage dynamiques.

- **Configuration d'un protocole de routage dynamique sur un nœud**.Un protocole de routage dynamique annonce l'adresse IP du cluster au routeur amont. Pour plus d'informations sur la configuration d'un protocole de routage dynamique, voirConfiguration des routes dynamiques.

Pour activer l'option de routage hôte de l'adresse IP du cluster à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 -  add nsip <IPAddress> <netmask> -hostRoute ENABLED
2
3 -  show nsip \<IPAddress\>
4
5     > add ns ip 10.102.29.60 255.255.255.255 -hostRoute ENABLED
6
7        Done
8 <!--NeedCopy-->
```

Configurations repérées et partiellement réparties sur un cluster L3

Les configurations à points et partiellement entrelacés du cluster L3 diffèrent légèrement de celles du cluster L2. La configuration peut différer d'un nœud à l'autre, car les nœuds résident sur des sous-réseaux différents. Les configurations réseau peuvent être spécifiques aux nœuds du cluster L3. Vous devez donc configurer les configurations repérées ou partiellement réparties en fonction des paramètres mentionnés ci-dessous.

Pour configurer des configurations repérées partiellement réparties par bandes sur une appliance NetScaler via le cluster L3, effectuez les tâches suivantes :

- Ajouter un groupe propriétaire de cluster à une table de routage statique IPv4
- Ajouter un groupe propriétaire de cluster à une table de routage statique IPv6
- Ajouter un groupe propriétaire de cluster à un routage IPv4 basé sur des stratégies (PBR)
- Ajouter un groupe propriétaire de cluster à un PBR IPv6
- Ajouter un VLAN
- Lier un VLAN à un groupe de propriétaires ou à un groupe de nœuds de cluster spécifique

Configuration des éléments suivants à l'aide de l'interface de ligne de commande

- **Pour ajouter un groupe propriétaire de cluster à une table de routage statique IPv4 de l'appliance NetScaler**

  ```
  add route <network> <netmask> <gateway> -owner group <ng>
  ```


- **Pour ajouter un groupe propriétaire de cluster à une table de routage statique IPv6 de l'appliance NetScaler**

  ```
  add route6 <network> -owner group <ng>
  ```

- **Pour ajouter un groupe-propriétaire de cluster à un PBR IPv4**

  ```
  add pbr <name> <action> -owner group <ng>
  ```

- **Pour ajouter un groupe-propriétaire de cluster à un PBR IPv6**

  ```
  add pbr6 <name> <action> -owner group <ng>
  ```

- **Pour ajouter un VLAN**

  ```
  add vlan <id>
  ```

- **Pour lier un VLAN à un propriétaire/groupe de nœuds de cluster spécifique**

  ```
  bind vlan <id> -ifnum - [IPAddress <ip_addr | ipv6_addr> [-owner group
  <ng>]
  ```

  Les commandes suivantes sont des exemples de configurations ponctuelles et partiellement entrelacées qui peuvent être configurées à l'aide de l'interface de ligne de commande.

```
1     > add route 10.102.29.0 255.255.255.0 10.102.29.2  - ownergroup ng2
2
3         Done
4
5     > add route6 fe80::9404:60ff:fedd:a464/64  - ownergroup ng1
6
7         Done
8
9     > add pbr pbr1 allow  - ownergroup ng1
10
11        Done
12
13    > add pbr6 pbr2 allow  - ownergroup ng2
14
15        Done
16
17    > add vlan 2
18
19        Done
20
21    > bind vlan 2  - ifnum 1/2  - [IPAddress 10.102.29.80 | fe80::9404:60
         ff:fedd:a464/64-ownergroup ng1
22
23        Done
```



```
<!--NeedCopy-->
```

Configurer le groupe de nœuds

Dans un cluster L3, pour répliquer le même ensemble de configurations sur plusieurs groupes de nœuds, les commandes suivantes sont utilisées :

Configuration des éléments suivants à l'aide du CLU

- **Pour ajouter une route statique IPv4 à la table de routage de l'appliance NetScaler**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Exemple de configuration :

```
add route 0 0 10.102.53.1 -ownerGroup ng1

add route 0 0 10.102.53.1 -ownerGroup ng2
<!--NeedCopy-->
```

Vous définissez un nouveau groupe de nœuds « tous » pour prendre en charge la configuration précédente, et vous devez configurer les commandes suivantes :

Configuration des éléments suivants à l'aide de l'interface de ligne de commande

- **Pour ajouter un nouveau groupe de nœuds au cluster avec un paramètre strict**

  ```
  add cluster node group <name> -strict <YES | NO>
  ```

- **Pour lier un nœud de cluster ou une entité au groupe de nœuds donné**

  ```
  bind cluster nodegroup <name> -node <nodeid>
  ```

- **Pour ajouter une route statique IPv4 à tous les groupes de propriétaires**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Exemple de configuration :

```
add cluster nodegroup all -strict YES

bind cluster nodegroup all -node 1

bind cluster nodegroup all -node 2

add route 0 0 10.102.53.1 -ownerGroup all
<!--NeedCopy-->
```


Distribution du trafic dans un cluster L3

Dans une configuration en cluster, les réseaux externes considèrent l'ensemble des appliances NetScaler comme une entité unique. Ainsi, le cluster doit sélectionner un nœud unique qui doit recevoir le trafic. Dans le cluster L3, cette sélection est effectuée à l'aide de l'ECMP. Le nœud sélectionné est appelé récepteur de flux.

> **Remarque**
>
> Pour un cluster L3 (nœuds répartis sur différents réseaux), seule la distribution du trafic ECMP peut être utilisée.

Le récepteur de flux reçoit le trafic puis, à l'aide de la logique de cluster interne, détermine le nœud qui doit traiter le trafic. Ce nœud est appelé processeur de flux. Le récepteur de flux oriente le trafic vers le processeur de flux via le fond de panier si le récepteur de flux et le processeur de flux se trouvent sur le même réseau. Le trafic est dirigé à travers le tunnel si le récepteur de débit et le processeur de débit se trouvent sur des réseaux différents.

> **Remarque**
>
> - Le récepteur de flux et le processeur de flux doivent être des nœuds capables de traiter le trafic.
> - À partir de NetScaler 11, vous pouvez désactiver la direction sur le backplane du cluster. Pour plus d'informations, voir Désactivation du pilotage sur le fond de panier du cluster.

La figure précédente montre une demande client qui traverse le cluster. Le client envoie une demande à une adresse IP virtuelle (VIP). Un mécanisme de distribution du trafic configuré sur le plan de données client sélectionne l'un des nœuds du cluster comme récepteur de flux. Le récepteur de flux reçoit le trafic, détermine le nœud qui doit traiter le trafic et dirige la demande vers ce nœud (à moins que le récepteur de flux ne se sélectionne lui-même comme processeur de flux). Si le processeur de flux et le récepteur de flux se trouvent dans le même groupe de nœuds, le paquet est dirigé sur le fond de panier. Et si le processeur de flux et le récepteur de flux se trouvent dans des groupes de nœuds différents, le paquet est dirigé à travers le tunnel sur le chemin routé.

Le processeur de flux établit une connexion avec le serveur. Le serveur traite la demande et envoie la réponse à l'adresse IP du sous-réseau (SNIP) qui a envoyé la demande au serveur. Étant donné que dans le cluster L3, le SNIP est toujours un SNIP repéré, le nœud propriétaire de l'adresse SNIP reçoit la réponse du serveur.

Configuration d'un cluster NetScaler

May 5, 2023

Les appliances NetScaler que vous souhaitez ajouter au cluster doivent satisfaire aux critères spécifiés dans Prérequispour les nœuds de cluster. Avant de configurer un cluster, vous devez connaître les bases du cluster. Pour plus d'informations, voir Présentation du cluster.

Pour former un cluster, vous devez configurer la communication entre les nœuds, créer le cluster (en ajoutant la première appliance NetScaler), puis ajouter les autres nœuds du cluster. Chacune de ces étapes est expliquée avec des détails pertinents dans les rubriques suivantes.

> **Remarque**
>
> Bien qu'il existe certaines différences entre la configuration d'un cluster L2 et L3, il existe également de nombreuses similitudes. Les rubriques suivantes expliquent la configuration des deux types de clusters tout en mettant en évidence les configurations spécifiques aux clusters L3.

Configuration de la communication entre nœuds

May 5, 2023

Les nœuds d'une configuration de cluster communiquent entre eux à l'aide des mécanismes de communication inter-nœuds suivants :

- Les nœuds qui se trouvent au sein du réseau (même sous-réseau) communiquent entre eux via le panneau arrière du cluster. Le fond de panier doit être configuré de manière explicite. Les étapes détaillées sont les suivantes.
- Sur les réseaux, le pilotage des paquets s'effectue via un tunnel GRE et les autres communications de nœud à nœud sont acheminées entre les nœuds selon les besoins.

> **Important**
>
> - À partir de la version 11.0, toutes les versions d'un cluster peuvent inclure des nœuds provenant de différents réseaux.
> - À partir de la version 13.0 build 58.3, le pilotage GRE est pris en charge sur les cartes réseau Fortville dans un cluster L3.

Pour configurer le backplane du cluster, procédez comme suit pour chaque nœud

1. Identifiez l'interface réseau que vous souhaitez utiliser pour le fond de panier.
2. Connectez un câble Ethernet ou optique entre l'interface réseau sélectionnée et le commutateur du panneau arrière du cluster.

Par exemple, pour utiliser l'interface 1/2 comme interface de fond de panier pour le nœud 4, connectez un câble entre l'interface 1/2 du nœud 4 et le commutateur de fond de panier.

Points importants à prendre en compte lors de la configuration du backplane du cluster

- N'utilisez pas l'interface de gestion (0/x) de l'appliance comme interface de fond de panier. Dans un cluster, l'interface 0/1/x se lit comme suit :

  0 -> ID de nœud 0
  1/x -> interface NetScaler

- N'utilisez pas les interfaces de fond de panier pour les plans de données client ou serveur.
- Citrix recommande d'utiliser le canal Link Aggregate (LA) pour le fond de panier du cluster.
- Dans un cluster à deux nœuds, où le fond de panier est connecté dos à dos, le cluster est opérationnel hors service dans l'une des conditions suivantes :
  - L'un des nœuds est redémarré.
  - L'interface de fond de panier de l'un des nœuds est désactivée.

  Citrix vous recommande donc de dédier un commutateur distinct au backplane, afin que l'autre nœud du cluster et le trafic ne soient pas affectés. Vous ne pouvez pas étendre le cluster à l'aide d'un lien dos à dos. Vous pouvez rencontrer une interruption de l'environnement de production lorsque vous augmentez la taille des nœuds du cluster.
- Les interfaces du backplane de tous les nœuds d'un cluster doivent être connectées au même commutateur et liées au même VLAN L2.
- Si vous avez plusieurs clusters avec le même ID d'instance de cluster, assurez-vous que les interfaces du backplane de chaque cluster sont liées à un VLAN différent.
- L'interface du backplane est toujours surveillée, quels que soient les paramètres de surveillance HA de cette interface.
- L'état de l'usurpation d'adresse MAC sur les différentes plateformes de virtualisation peut affecter le mécanisme de pilotage du panneau arrière du cluster. Assurez-vous donc que l'état approprié est configuré :
  - XenServer - Désactiver l'usurpation d'adresse MAC
  - Hyper-V - Activer l'usurpation d'adresse MAC
  - VMware ESX : activez l'usurpation d'adresse MAC (assurez-vous également que les « transmissions falsifiées » sont activées)
- Le MTU du fond de panier du cluster est automatiquement mis à jour. Toutefois, si des trames jumbo sont configurées sur le cluster, la MTU du backplane du cluster doit être configurée de manière explicite. La valeur doit être définie sur 78 + X, où X est la MTU maximale des plans de données client et serveur. Par exemple, si le MTU d'un plan de données serveur est 7500 et celui du plan de données client est 8922. Le MTU du fond de panier d'un cluster doit être réglé sur 78 + 8922 = 9 000. Pour définir ce MTU, utilisez la commande suivante :

```
> set interface <backplane_interface> -mtu <value>
```


- La MTU pour les interfaces du commutateur de fond de panier doit être supérieure ou égale à 1 578 octets. Cela s'applique si le cluster possède des fonctionnalités telles que le MBF, les politiques L2, les ACL, le routage dans les déploiements CLAG et VPath.

Support de tunnel basé sur UDP pour les clusters L2 et L3

À partir de NetScaler version 13.0 build 36.x, les clusters NetScaler L2 et L3 peuvent diriger le trafic à l'aide d'un tunneling basé sur UDP. Il est défini pour les communications entre deux nœuds d'un cluster. En utilisant le paramètre « mode tunnel », vous pouvez définir le mode tunnel GRE ou UDP à partir de la commande add and set cluster node.

Dans un déploiement de cluster L3, les paquets entre les nœuds NetScaler sont échangés via un tunnel GRE non crypté qui utilise les adresses NSIP des nœuds source et destination pour le routage. Lorsque cet échange a lieu sur Internet, en l'absence d'un tunnel IPsec, le NSIP est exposé sur Internet et peut entraîner des problèmes de sécurité.

> **Important**
>
> Citrix recommande à ses clients d'établir leur propre solution IPsec lorsqu'ils utilisent un cluster L3.

Le tableau suivant vous aide à classer la prise en charge des tunnels en fonction des différents déploiements.

Types de direction	AWS	Microsoft Azure	Sur site
MAC	Non pris en charge	Non pris en charge	Prise en charge
Tunnel GRE	Prise en charge	Non pris en charge	Prise en charge
Tunnel UDP	Prise en charge	Prise en charge	Prise en charge

> **Important**
>
> Dans un cluster L3, le mode tunnel est défini sur GRE par défaut.

Configuration d'un tunnel basé sur UDP

Vous pouvez ajouter un nœud de cluster en définissant les paramètres de l'ID du nœud et en mentionnant l'état. Configurez le fond de panier en fournissant le nom de l'interface et sélectionnez le mode tunnel de votre choix (GRE ou UDP).

Procédures CLI

Pour activer le mode tunnel UDP à l'aide de l'interface de ligne de commande.

À l'invite de commande, tapez :

- `add cluster node <nodeId>@ [-state <state>] [-backplane <interface_name>] [-tunnelmode <tunnelmode>]`
- `set cluster node <nodeId>@ [-state <state>] [-tunnelmode <tunnelmode>]`

> **Remarque**
>
> Les valeurs possibles pour le mode tunnel sont NONE, GRE, UDP.

Exemple

- `add cluster node 1 -state ACTIVE -backplane 1/1/1 -tunnelmode UDP`
- `set cluster node 1 -state ACTIVE -tunnelmode UDP`

Procédures GUI

Pour activer le mode tunnel UDP à l'aide de l'interface graphique.

1. Accédez à **Système > Cluster > Nœuds**.
2. Sur la page **Nœuds de cluster**, cliquez sur **Ajouter**.
3. Dans le **nœud Create Cluster**, définissez le paramètre **Mode tunnel** sur UDP et cliquez sur **Créer**.



4. Cliquez sur **Fermer**.

Création d'un cluster NetScaler

May 5, 2023

Pour créer un cluster, commencez par utiliser l'une des appliances NetScaler que vous souhaitez ajouter au cluster. Sur ce nœud, vous devez créer l'instance de cluster et définir l'adresse IP du cluster. Ce nœud est le premier nœud de cluster et s'appelle le coordinateur de configuration de cluster (CCO). Toutes les configurations effectuées sur l'adresse IP du cluster sont stockées sur ce nœud, puis propagées aux autres nœuds de cluster.

La responsabilité du CCO dans un cluster n'est pas fixée à un nœud spécifique. Elle peut évoluer au fil du temps en fonction des facteurs suivants :

- La priorité du nœud. Le nœud ayant la priorité la plus élevée (numéro de priorité le plus bas) devient CCO. Par conséquent, si un nœud dont le numéro de priorité est inférieur au CCO existant

est ajouté, le nouveau nœud prend le relais en tant que CCO.

- Si le CCO actuel tombe en panne, le nœud ayant le numéro de priorité le plus bas prend le relais en tant que CCO. Si la priorité n'est pas définie ou s'il existe plusieurs nœuds avec le numéro de priorité le plus faible, le CCO est sélectionné parmi l'un des nœuds disponibles.

> **Remarque :**
>
> Les configurations de l'appliance (y compris les adresses SNIP et les VLAN) sont effacées en exécutant implicitement la commande `clear ns config extended`. Toutefois, le VLAN et le NSVLAN par défaut ne sont pas effacés du dispositif. Par conséquent, si vous souhaitez que le NSVLAN soit sur le cluster, assurez-vous qu'il est créé avant que le dispositif ne soit ajouté au cluster. Pour un cluster L3 (nœuds de cluster sur différents réseaux), les configurations réseau ne sont pas effacées de l'appliance.
>
> **Important :**
>
> Le moniteur HA (HAMON) sur une configuration de cluster est utilisé pour surveiller la santé d'une interface sur chaque nœud. Le paramètre HAMON doit être activé sur chaque nœud pour surveiller l'état de l'interface. Si l'état de fonctionnement de l'interface compatible HAMON tombe en panne pour une raison quelconque, le nœud de cluster respectif est marqué comme étant défectueux (NOT UP) et ce nœud ne peut pas desservir le trafic.

Création d'un cluster à l'aide de l'interface de ligne de commande

- Ouvrez une session sur une appliance NetScaler (par exemple, une appliance avec l'adresse NSIP 10.102.29.60) que vous souhaitez ajouter au cluster.
- Ajoutez une instance de cluster.

```
1  add cluster instance <clId> -quorumType <NONE | MAJORITY> -inc <
      ENABLED | DISABLED> -backplanebasedview <ENABLED | DISABLED>
2  <!--NeedCopy-->
```

- L'option `-dfdretainl2params` vous permet d'ajouter les en-têtes L2 étendus pour le trafic de fond de panier.

  À l'invite de commande, tapez :

  ```
  add cluster instance 1 -dfdretainl2params <ENABLED|DISABLED>
  ```

  La commande suivante affiche l'état du `-dfdretainl2params` :

  ```
  show cluster instance <clusterid>
  ```

  Utilisez la commande suivante pour activer ou désactiver `-dfdretainl2params` :

  ```
  set cluster instance 1 -dfdretainl2params <ENABLED|DISABLED>
  ```


- L'option `-proxyarpstatus` active ou désactive la fonctionnalité arp du proxy pour le cluster.

  À l'invite de commande, tapez :

  ```
  add cluster instance 1 -proxyarpstatus <ENABLED|DISABLED>
  ```

  La commande suivante affiche l'état du `proxyarpstatus` :

  ```
  show cluster instance <clusterid>
  ```

  Vous pouvez utiliser la commande suivante pour activer ou désactiver `proxyarpstatus` :

  ```
  set cluster instance 1 -proxyarpstatus <ENABLED|DISABLED>
  ```

> **Remarque :**
>
> - L'ID d'instance de cluster doit être unique au sein d'un réseau local.
> - Le paramètre `-quorumType` doit être défini sur MAJORITY et non NONE dans les scénarios suivants :
>   - Topologies which do not have redundant links between cluster nodes. These topologies might be prone to network partition due to a single point of failure.
>   - During any cluster operations such as node addition or removal.
> - Pour un cluster L3, assurez-vous que le paramètre `-inc` est défini sur ENABLED. Le paramètre `-inc` doit être désactivé pour un cluster L2.
> - Lorsque le paramètre `-backplanebasedview` est activé, la vue opérationnelle (ensemble de nœuds qui desservent le trafic) est décidée en fonction des pulsations cardiaques reçues uniquement sur l'interface du fond de panier. Par défaut, ce paramètre est désactivé. Lorsque ce paramètre est désactivé, un nœud ne dépend pas de la réception des pulsations de cœur uniquement sur le fond de panier.

1. [Uniquement pour un cluster L3] Créez un groupe de nœuds. À l'étape suivante, le nœud de cluster nouvellement ajouté doit être associé à ce groupe de nœuds.

   > **Remarque :**
   >
   > Ce groupe de nœuds inclut la totalité ou un sous-ensemble des appliances NetScaler qui appartiennent au même réseau.

   ```
   add cluster nodegroup <name>
   <!--NeedCopy-->
   ```

2. Ajoutez l'appliance NetScaler au cluster.

   ```
   add cluster node <nodeId> <IPAddress> -state <state> -backplane <
       interface_name> -nodegroup <name>
   <!--NeedCopy-->
   ```


> **Remarque :**
>
> Pour un cluster L3 :
>
> - Le paramètre de groupe de nœuds doit être défini sur le nom du groupe de nœuds créé.
> - Le paramètre de fond de panier est obligatoire pour les nœuds associés à un groupe de nœuds comportant plusieurs nœuds, afin que les nœuds du réseau puissent communiquer entre eux.

Exemple :

Ajout d'un nœud pour un cluster L2 (tous les nœuds de cluster se trouvent sur le même réseau).

```
1   add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1
2   <!--NeedCopy-->
```

Ajout d'un nœud pour un cluster L3 qui comprend un seul nœud de chaque réseau. Ici, vous n'avez pas besoin de régler le fond de panier.

```
1   add cluster node 0 10.102.29.60 -state PASSIVE -nodegroup ng1
2   <!--NeedCopy-->
```

Ajout d'un nœud pour un cluster L3 qui comprend plusieurs nœuds de chaque réseau. Ici, vous devez définir le fond de panier afin que les nœuds d'un réseau puissent communiquer entre eux.

```
1   add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1
       -nodegroup ng1
2   <!--NeedCopy-->
```

3. Ajoutez l'adresse IP du cluster (par exemple, 10.102.29.61) sur ce nœud.

```
1 add ns ip <IPAddress> <netmask> -type clip
2 <!--NeedCopy-->
```

Exemple

```
1 add ns ip 10.102.29.61 255.255.255.255 -type clip
2 <!--NeedCopy-->
```

4. Activez l'instance de cluster.

```
1 enable cluster instance <clId>
2 <!--NeedCopy-->
```


5. Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```

6. Redémarrez l'appliance à chaud.

```
reboot -warm
<!--NeedCopy-->
```

Vérifiez les configurations de cluster à l'aide de la commande show cluster instance. Vérifiez que la sortie de la commande affiche l'adresse NSIP de l'appliance en tant que nœud du cluster.

7. Une fois que le nœud est UP, connectez-vous au CLIP et modifiez les informations d'identification RPC pour l'adresse IP du cluster et l'adresse IP du nœud. Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.

Pour créer un cluster à l'aide de l'interface graphique

1. Ouvrez une session sur un dispositif (par exemple, un dispositif avec l'adresse NSIP 10.102.29.60) que vous avez l'intention d'ajouter au cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, cliquez sur le lien **Gérer le cluster** .
4. Dans la boîte de dialogue Configuration du cluster, définissez les paramètres requis pour créer un cluster. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur la zone de texte correspondante.
5. Cliquez sur **Create**.
6. Dans la boîte de dialogue Configurer l'instance de cluster, activez la case à cocher Activer l'instance de cluster.
7. Dans le volet Cluster Nodes, sélectionnez le nœud et cliquez sur **Ouvrir.**
8. Dans la boîte de dialogue Configurer le nœud de cluster, définissez l'état.
9. Cliquez sur **OK**, puis sur **Enregistrer.**
10. Redémarrez l'appliance à chaud.
11. Une fois que le nœud est UP, connectez-vous au CLIP et modifiez les informations d'identification RPC pour l'adresse IP du cluster et l'adresse IP du nœud. Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.

Prise en charge du mode strict pour l'état de synchronisation du cluster

Vous pouvez désormais configurer un nœud de cluster pour afficher les erreurs lors de l'application de la configuration. Un nouveau paramètre, « SyncStatusStrictMode » est introduit à la fois dans la commande add et set cluster instance pour suivre l'état de chaque nœud d'un cluster. Par défaut, le paramètre `syncStatusStrictMode` est désactivé.

Pour activer le mode strict à l'aide de la CLI

À l'invite de commande, tapez :

```
set cluster instance <clID> [-syncStatusStrictMode (ENABLED | DISABLED)
    ]
<!--NeedCopy-->
```

Exemple :

```
set cluster instance 1  - syncStatusStrictMode ENABLED
<!--NeedCopy-->
```

Pour afficher l'état du mode strict à l'aide de l'interface de ligne de commande

```
    >show cluster instance
    1) Cluster ID: 1
        Dead Interval: 3 secs
        Hello Interval: 200 msecs
        Preemption: DISABLED
        Propagation: ENABLED
        Quorum Type: MAJORITY
        INC State: DISABLED
        Process Local: DISABLED
        Retain Connections: NO
        Heterogeneous: NO
        Backplane based view: DISABLED
        Cluster sync strict mode: ENABLED
        Cluster Status: ENABLED(admin), ENABLED(operational), UP

      WARNING(s):
        (1) - There are no spotted SNIPs configured on the cluster.
           Spotted SNIPs can help improve cluster performance

        Member Nodes:
        Node ID     Node IP      Health     Admin State  Operational
           State
```



```
21          -------     -------      ------     -----------
                -----------------
22      1)      1           192.0.2.20      UP          ACTIVE       ACTIVE(
           Configuration Coordinator)
23      2)      2           192.0.2.21      UP          ACTIVE       ACTIVE
24      3)      3           192.0.2.19*     UP          ACTIVE       ACTIVE
25  <!--NeedCopy-->
```

Pour afficher la raison de l'échec de synchronisation d'un nœud de cluster à l'aide de l'interface graphique

1. Accédez à **Système > Cluster > Nœuds de cluster**.
2. Dans la page **Nœuds de cluster**, faites défiler vers l'extrême droite pour afficher les détails de la raison de l'échec de synchronisation des nœuds de cluster.

Ajout d'un nœud au cluster

May 5, 2023

Vous pouvez facilement augmenter la taille d'un cluster pour inclure un maximum de 32 nœuds. Lorsqu'une appliance NetScaler est ajoutée au cluster, les configurations de cette appliance sont effacées (en exécutant en interne la commande clear ns config -extended). Les adresses SNIP, les paramètres **MTU** de l'interface du backplane et toutes les configurations VLAN (à l'exception du VLAN et du NSVLAN par défaut) sont également supprimés de l'appliance.

Les configurations du cluster sont ensuite synchronisées sur ce nœud. Il peut y avoir une baisse intermittente du trafic pendant que la synchronisation est en cours.

> **Important**
>
> Avant d'ajouter une appliance NetScaler à un cluster :
>
> - Configurez l'interface de fond de panier pour le nœud. Consultez la rubrique précédente.
> - Vérifiez si les licences disponibles sur l'appliance correspondent à celles disponibles sur le coordinateur de configuration. L'appliance est ajoutée uniquement si les licences correspondent.
> - Si vous souhaitez que le NSVLAN soit intégré au cluster, assurez-vous que le NSVLAN est créé sur l'appliance avant de l'ajouter au cluster.
> - Citrix vous recommande d'ajouter le nœud en tant que nœud passif. Ensuite, après avoir joint le nœud au cluster, terminez la configuration spécifique au nœud à partir de l'adresse IP du cluster. Exécutez la commande force cluster sync si le cluster n'a détecté que des

adresses IP. Et qui possède une liaison VLAN L3 ou possède des routes statiques.
- Lorsqu'un dispositif doté d'un canal d'agrégation de liens (LA) préconfiguré est ajouté à un cluster, le canal LA continue d'exister dans l'environnement du cluster. Le canal LA est renommé de LA/x en NodeID/LA/x, où LA/x est l'identifiant du canal LA.

Pour ajouter un nœud au cluster à l'aide de l'interface de ligne de commande

Remarque

Lorsque vous ajoutez un nœud à une configuration de cluster, si le nœud possède une route statique par défaut, il est ajouté au nœud coordinateur de cluster (CCO). Si cette route statique par défaut pointe vers une passerelle incorrecte, cela peut entraîner une interruption des services. Vérifiez donc l'itinéraire statique par défaut du nouveau nœud avant de l'ajouter à la configuration du cluster.

1. Ouvrez une session sur l'adresse IP du cluster, à l'invite de commandes, procédez comme suit :
   - Ajoutez l'appliance (par exemple, 10.102.29.70) au cluster.

Remarque

Pour un cluster L3 :

- Le paramètre du groupe de nœuds doit être défini sur un groupe de nœuds qui possède des nœuds du même réseau.
- Si ce nœud appartient au même réseau que le premier nœud ajouté, configurez le groupe de nœuds utilisé pour ce nœud.
- Si ce nœud appartient à un autre réseau, créez un groupe de nœuds et liez ce nœud au groupe de nœuds.
- Le paramètre de fond de panier est obligatoire pour les nœuds associés à un groupe de nœuds comportant plusieurs nœuds, afin que les nœuds du réseau puissent communiquer entre eux.

```
add cluster node <nodeId> <IPAddress> -state <state> -backplane <
   interface_name> -nodegroup <name>

Example:

add cluster node 1 10.102.29.70 -state PASSIVE -backplane 1/1/1
<!--NeedCopy-->
```

   - Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```


2. Ouvrez une session sur le nœud récemment ajouté (par exemple, 10.102.29.70) et joignez le nœud au cluster.

```
join cluster -clip <ip_addr> -password <password>

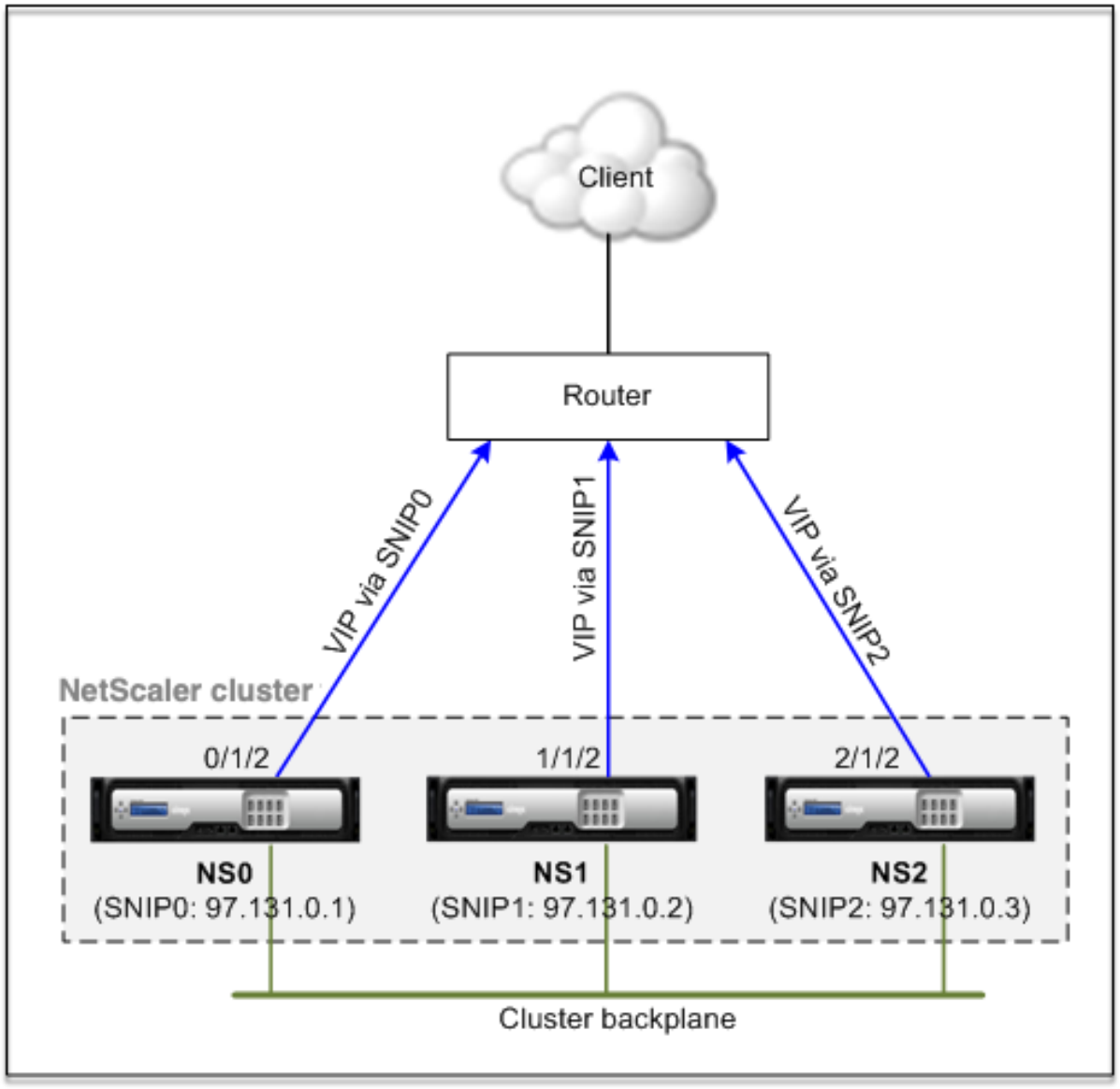
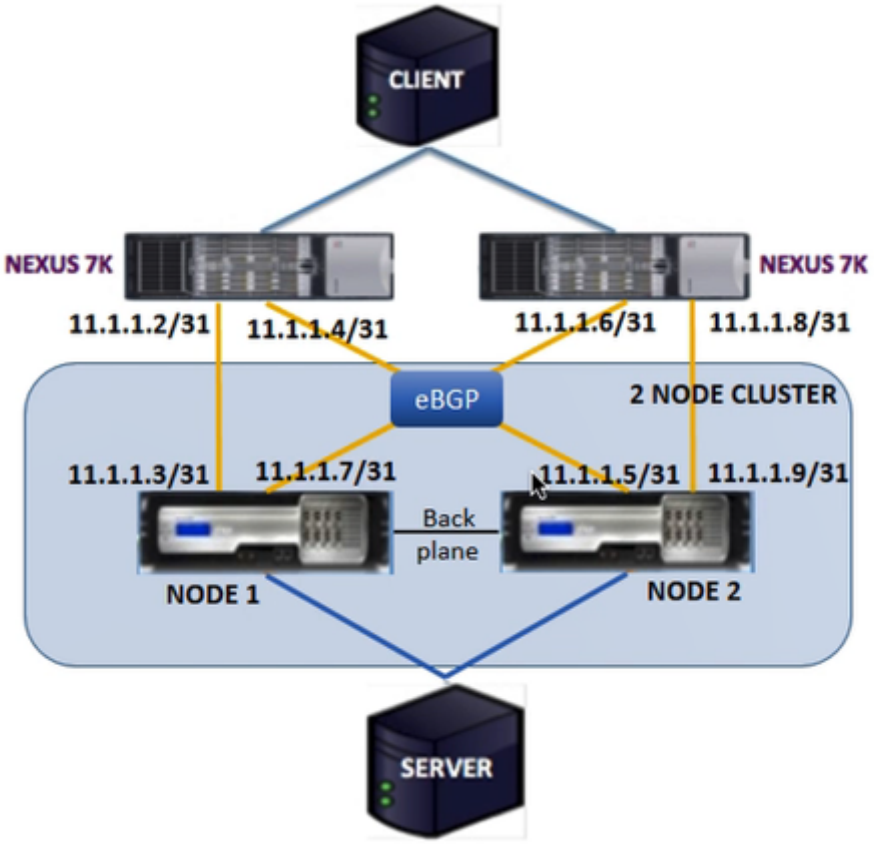
Example:

join cluster -clip 10.102.29.61 -password nsroot
<!--NeedCopy-->
```

3. Configurez les commandes suivantes sur le CLIP.

   - Lier un VLAN à une interface

```
bind vlan <id> -ifnum <interface_name>
<!--NeedCopy-->
```

     Exemple :

```
bind vlan 1 -ifnum 2/1/2
<!--NeedCopy-->
```

   - Ajouter une adresse IP repérée au nœud nouvellement ajouté

```
add ns ip <IpAddress> <netmask> -ownerNode <positive_interger
    >
<!--NeedCopy-->
```

     Exemple :

```
add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2
<!--NeedCopy-->
```

   - Vérifiez le VLAN sur NSIP

```
show vlan <id>
<!--NeedCopy-->
```

     Exemple :

```
show vlan 1
<!--NeedCopy-->
```

4. Effectuez les configurations suivantes :

   - Si le nœud est ajouté à un cluster qui ne possède que des adresses IP repérées, les configurations sont synchronisées avant que les adresses IP repérées ne soient attribuées à ce

nœud. Dans de tels cas, les liaisons VLAN L3 peuvent être perdues. Pour éviter cette perte, ajoutez une adresse IP par bandes ou ajoutez les liaisons VLAN L3.

- Définissez les configurations repérées requises.
- Définissez le MTU pour l'interface du fond de panier.

5. Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```

6. Redémarrez l'appliance à chaud.

```
reboot -warm
<!--NeedCopy-->
```

7. Une fois que le nœud est UP et que la synchronisation a réussi, modifiez les informations d'identification RPC pour le nœud à partir de l'adresse IP du cluster. Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.

```
set rpcNode <node-NSIP> -password <passwd>

Example:

set rpcNode 192.0.2.4 -password mypassword
<!--NeedCopy-->
```

8. Définissez le nœud du cluster sur Actif.

```
set cluster node <nodeID> -state active.

Example:

set cluster node 1 -state active
<!--NeedCopy-->
```

Pour ajouter un nœud au cluster à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Nœuds**.
3. Dans le volet de détails, cliquez sur **Ajouter** pour ajouter le nouveau nœud (par exemple, 10.102.29.70).
4. Dans la boîte de dialogue **Créer un nœud de cluster**, configurez le nouveau nœud. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur la zone de texte correspondante.

5. Cliquez sur **Create**. Lorsque vous êtes invité à effectuer un redémarrage à chaud, cliquez sur **Oui.**
6. Une fois que le nœud est UP et que la synchronisation a réussi, modifiez les informations d'identification RPC pour le nœud à partir de l'adresse IP du cluster. Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.
7. Accédez à **Système > Cluster > Noeuds > Modifier**.
8. Modifiez l'état sur **ACTIF** et confirmez.

Pour joindre un nœud précédemment ajouté au cluster à l'aide de l'interface graphique

Si vous avez utilisé l'interface de ligne de commande pour ajouter un nœud au cluster, mais que vous n'avez pas joint le nœud au cluster, vous pouvez utiliser la procédure suivante.

> **Remarque**
>
> Lorsqu'un nœud rejoint le cluster, il reprend sa part du trafic provenant du cluster et une connexion existante peut donc être interrompue.

1. Ouvrez une session sur le nœud que vous souhaitez rejoindre au cluster (par exemple, 10.102.29.70).
2. Accédez à **Système > Cluster.**
3. Dans le volet de détails, sous Commencer, cliquez sur le lien Rejoindre un cluster.
4. Dans la boîte de dialogue Joindre à un cluster existant, définissez l'adresse IP du cluster et le `nsroot` mot de passe du coordinateur de configuration. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur la zone de texte correspondante.
5. Cliquez sur **OK.**

Affichage des détails d'un cluster

January 21, 2021

Vous pouvez afficher les détails de l'instance de cluster et des nœuds de cluster en vous connectant à l'adresse IP du cluster.

Pour afficher les détails d'une instance de cluster à l'aide de l'interface de ligne de commande

Ouvrez une session sur l'adresse IP du cluster et, à l'invite de commandes, tapez :


```
show cluster instance <clId>
```

> **Remarque**
>
> Lorsque la commande précédente est exécutée à partir de l'adresse NSIP du nœud non-CCO, la commande affiche l'état du cluster sur ce nœud.

Pour afficher les détails d'un nœud de cluster à l'aide de l'interface de ligne de commande

Ouvrez une session sur l'adresse IP du cluster et, à l'invite de commandes, tapez :

```
show cluster node <nodeId>
```

Pour afficher les détails d'une instance de cluster à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, sous **Mise en route**, cliquez sur le lien **Gérer le cluster**pour afficher les détails du cluster.

Pour afficher les détails d'un nœud de cluster à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Nœuds.**
3. Dans le volet d'informations, cliquez sur le nœud pour lequel vous souhaitez afficher les détails.

Distribution du trafic sur les nœuds de cluster

May 5, 2023

Après avoir créé le cluster NetScaler et effectué les configurations requises, vous devez déployer Equal Cost Multiple Path (ECMP) ou Cluster Link Aggregation (LA) sur le plan de données client (pour le trafic client) ou le plan de données serveur (pour le trafic serveur). Ces mécanismes distribuent le trafic externe entre les nœuds du cluster.

Direction du panneau arrière basée sur des règles

Le backplane steering (PBS) basé sur des politiques est un mécanisme de déploiement de clusters qui oriente le trafic entre les nœuds du cluster en fonction de la méthode de hachage définie pour le flux.

Le flux est défini par une combinaison de paramètres L2 et L3 similaires à la liste de contrôle d'accès (ACL).

Le PBS prend en charge à la fois le trafic IPv4 et IPv6. Dans le cas de déploiements IPv6, le pilotage prend en charge une option `[dfdprefix <positive_integer>]`supplémentaire. Il offre la flexibilité de choisir le même processeur de flux pour le même préfixe IP. L'option de préfixe est prise en charge uniquement pour les méthodes de hachage de l'adresse IP source ou de l'adresse IP de destination.

> **Remarque**
>
> Si le mécanisme PBS n'est pas utilisé pour diriger le trafic, celui-ci est dirigé selon la méthode par défaut.

Pour configurer les nouveaux attributs ACL, tapez les commandes suivantes sur l'interface de ligne de commande :

Commandes CLI pour IPv4

- `add ns acl <aclname> <aclaction> [-type (classic | dfd)] [-dfdhash <dfdhash>]`
- `set ns acl <aclname> <aclaction> [-dfdhash <dfdhash>`
- `show ns acl [<aclname>][-type (classic | DFD)]`
- `apply ns acls [-type (classic | DFD)]`
- `clear ns acls [-type (classic | DFD)]`
- `renumber ns acls [-type (classic | DFD)]`

Commandes CLI pour IPv6

- `add ns acl6 <acl6name> <acl6action> [-type (classic | dfd)][-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`
- `set ns acl6 <acl6name> <acl6action> [-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`
- `show ns acl6 [<acl6name>][-type (classic | DFD)]`
- `apply ns acls6 [-type (classic | DFD)]`
- `clear ns acls6 [-type (classic | DFD)]`
- `renumber ns acls6 [-type (classic | DFD)]`

Les différents types de méthodes de hachage que vous pouvez spécifier pour diriger le paquet vers le processeur de flux sont les suivants :

- SIP-SPORT-DIP-SPORT
- SIP
- TREMPAGE

- TREMPETTE
- SPORT DE GLISSE

Limitations

1. La répartition du flux de trafic entre les nœuds du cluster n'est pas garantie, car le processeur de flux est déterminé par les règles configurées par l'administrateur.
2. Le mode L2 n'est pas pris en charge.
3. Les groupes de nœuds et les SNIP répartis par bandes ne sont pas pris en charge, car il n'existe aucun scénario de déploiement.
4. Le protocole MPTCP n'est pas pris en charge.
5. Support uniquement pour le trafic TCP, UDP et ICMP.
6. Le mode Cluster over L3 n'est pas pris en charge.
7. Le processus local au niveau du service n'est pas pris en charge.

Utilisation du chemin d'accès multiple à coût égal (ECMP)

August 20, 2021

En utilisant le mécanisme ECMP (Equal Cost Multiple Path) sur un déploiement de cluster, les nœuds de cluster actifs annoncent les adresses IP du serveur virtuel. Le nœud de cluster qui reçoit le trafic annoncé dirige le trafic vers le nœud qui doit traiter le trafic. Il peut y avoir une direction redondante dans les serveurs virtuels repérés et partiellement entrelacés. Par conséquent, à partir de NetScaler 11, les adresses IP de serveurs virtuels spotted et striped partiels annoncent les nœuds propriétaires, ce qui réduit la direction redondante.

Vous devez avoir une connaissance détaillée des protocoles de routage pour utiliser ECMP. Pour plus d'informations, reportez-vous à la section Configuration des routes dynamiques. Pour plus d'informations sur le routage dans un cluster, voir Routage dans un cluster.

Pour utiliser ECMP, vous devez d'abord effectuer les opérations suivantes :

- Activez le protocole de routage requis (OSPF, RIP, BGP ou ISIS) sur l'adresse IP du cluster.
- Liez les interfaces et l'adresse IP spotted (avec le routage dynamique activé) à un VLAN.
- Configurez le protocole de routage sélectionné et redistribuez les routes du noyau sur les ZEBO à l'aide du shell VTYSH.

Effectuez des configurations similaires sur l'adresse IP du cluster et sur le périphérique de connexion externe.

Remarque

- Assurez-vous que les licences du cluster prennent en charge le routage dynamique, sinon ECMP ne fonctionne pas.
- ECMP n'est pas pris en charge pour les serveurs virtuels génériques car RHI a besoin d'une adresse VIP pour faire de la publicité sur un routeur et des serveurs virtuels génériques. Comme ils n'ont pas d'adresses VIP associées.

Figure 1. Topologie ECMP



Lorsque vous utilisez le mécanisme ECMP pour la distribution du trafic sur un déploiement de cluster, les nœuds de cluster actifs annoncent les adresses IP du serveur virtuel sur le routeur amont. Le routeur ECMP peut atteindre l'adresse VIP via SNIP0, SNIP1 ou SNIP2. Le flux de trafic dans la figure 1

est décrit comme suit :

1. Le client envoie une requête au VIP hébergé sur le cluster.
2. Le routeur amont, basé sur les routes apprises du VIP, transmet le paquet à l'un des nœuds. Disons NS1. Le nœud NS1 est le récepteur de flux.
3. Le récepteur de flux (NS1) détermine le nœud qui doit traiter le trafic, appelé processeur de flux. Par exemple, Node NS2 est le processeur de flux.
4. Le récepteur de flux (NS1) avec SNIP1 (97.131.0.2) achemine la demande vers le processeur de flux (NS2) avec SNIP2 (97.131.0.3).
5. Le processeur de flux (NS2) établit une connexion avec le serveur.
6. Le serveur traite la demande et envoie la réponse à l'adresse SNIP qui a envoyé la demande au serveur.

Remarques :

- Seuls les nœuds ACTIVE annoncent les routes VIP.
- Les nœuds INACTIFS n'annoncent pas les routes VIP.
- Tous les nœuds ACTIVE annoncent les VIP rayés.
- Seuls les nœuds de propriétaire ACTIVE annoncent des VIP ponctués ou partiellement rayés.

Pour configurer ECMP sur le cluster à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.
2. Activez le protocole de routage.

```
enable ns feature <feature>
```

Exemple : pour activer le protocole de routage OSPF.

```
enable ns feature ospf
```

3. Ajoutez un VLAN.

```
add vlan <id>
```

Exemple

```
add vlan 97
```

4. Liez les interfaces des nœuds de cluster au VLAN.

```
bind vlan <id> -ifnum <interface_name>
```

Exemple


```
bind vlan 97 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Ajoutez une adresse SNIP spotted pour chaque nœud et activez le routage dynamique sur celui-ci.

```
add ns ip <SNIP> <netmask> -ownerNode <positive_integer> -
    dynamicRouting ENABLED
```

Exemple

```
add ns ip 97.131.0.1 255.0.0.0 -ownerNode 0 -dynamicRouting
    ENABLED -type SNIP
add ns ip 97.131.0.2 255.0.0.0 -ownerNode 1 -dynamicRouting
    ENABLED -type SNIP
add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2 -dynamicRouting
    ENABLED -type SNIP
```

6. Liez l'une des adresses SNIP spotted au VLAN. Lorsque vous liez une adresse SNIP spotted à un VLAN, toutes les autres adresses SNIP spotted définies sur le cluster dans ce sous-réseau sont automatiquement liées au VLAN.

```
bind vlan <id> -IPAddress <SNIP> <netmask>
```

Exemple

```
bind vlan 97 -ipAddress 97.131.0.1 255.0.0.0
```

> **Remarque**
>
> Vous pouvez utiliser les adresses NSIP des nœuds de cluster au lieu d'ajouter des adresses SNIP. Si c'est le cas, vous n'avez pas à effectuer les étapes 3 à 6.

7. Configurez le protocole de routage sur les ZEBOs à l'aide du shell VTYSH.

Exemple :

Pour configurer un protocole de routage OSPF sur les ID de nœud 0, 1 et 2.

```
vtysh
! interface vlan97 !
 router ospf   owner-node 0
ospf router-id 97.131.0.1   exit-owner-node
owner-node 1    ospf router-id 97.131.0.2
exit-owner-node
owner-node 2
```



```
8 ospf router-id 97.131.0.3   exit-owner-node   redistribute kernel
    network 97.0.0.0/8 area 0  !
```

> **Remarque**
>
> Pour que les adresses VIP soient annoncées, le paramètre RHI est fait en utilisant le paramètre vServerRhilevel comme suit :

```
1 add ns ip <IPAddress> <netmask> -type VIP -vserverRHILevel <
    vserverRHILevel>
```

Pour les paramètres RHI spécifiques à OSPF, il existe d'autres paramètres qui peuvent être effectués comme suit :

```
1 add ns ip <IPAddress> <netmask> -type VIP -ospfLSAType ( TYPE1 |
    TYPE5 ) -ospfArea <positive_integer>
```

Utilisez la commande add ns ip6 pour exécuter les commandes précédentes sur les adresses IPv6.

8. Configurez ECMP sur le commutateur externe. Les exemples de configuration suivants sont fournis pour le commutateur Cisco® Nexus 7000 C7010 version 5.2(1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
1 //For OSPF (IPv4 addresses) Global config: Configure terminal
    feature ospf    Interface config:  Configure terminal
    interface Vlan10      no shutdown      ip address 97.131.0.5/8
       Configure terminal  router ospf 1  network 97.0.0.0/8 area
    0.0.0.0  --------------------------------
2
3 //For OSPFv3 (IPv6 addresses) Global config:  Configure terminal
    feature ospfv3    Configure terminal  interface Vlan10      no
    shutdown      ipv6 address use-link-local-only      ipv6 router
     ospfv3 1 area 0.0.0.0    Configure terminal  router ospfv3 1
```

Noeuds de cluster de surveillance de routeur dans le déploiement ECMP

Dans une configuration de cluster, sur un nœud propriétaire qui possède une configuration d'adresse SNIP spotted, vous pouvez maintenant désactiver l'option OwnerDownResponse. Par défaut, l'option est activée, permettant au nœud de répondre à une requête ICMP/ARP/ICMP6/ND6 provenant du routeur en amont. Vous pouvez maintenant désactiver cette option pour permettre au routeur de surveiller si un nœud de cluster est actif ou inactif. Lorsque le routeur envoie une demande, si l'option est désactivée, il identifie le nœud propriétaire comme étant inactif et indisponible pour la distribution du trafic.

Pour configurer ECMP pour la distribution du trafic des routes statiques à l'aide de l'interface de ligne de commande

```
add ns ip <ipddress> <netmask> -ownernode <node-id>  - ownerDownResponse
    disable
```

Cas d'utilisation : ECMP avec routage BGP

January 21, 2021

Pour configurer ECMP avec le protocole de routage BGP, effectuez les opérations suivantes :

1. Connectez-vous à l'adresse IP du cluster.
2. Activer le protocole de routage BGP.

```
> enable ns feature bgp
```

3. Ajoutez un VLAN et liez les interfaces requises.

```
> add vlan 985
> bind vlan 985 -ifnum 0/0/1 1/0/1
```

4. Ajoutez les adresses IP spotted et liez-les au VLAN.

```
> add ns ip 10.100.26.14 255.255.255.0 -ownerNode 1 -
    dynamicRouting ENABLED
> add ns ip 10.100.26.15 255.255.255.0 -ownerNode 2 -
    dynamicRouting ENABLED
> bind vlan 985 -ipAddress 10.100.26.10 255.255.255.0
```

5. Configurez le protocole de routage BGP sur les ZEBOs à l'aide du shell VTYSH.

```
> vtysh conf t router bgp 65535 neighbor 10.100.26.1 remote-as
    65535
```

6. Configurez BGP sur le commutateur externe. Les exemples de configuration suivants sont fournis pour le commutateur Cisco® Nexus 7000 C7010 version 5.2(1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
> router bgp 65535 no synchronization
  bgp log-neighbor-changes neighbor 10.100.26.14 remote-as 65535
     neighbor 10.100.26.15 remote-as 65535 no auto-summary
  dont-capability-negotiate
```



```
4   dont-capability-negotiate
5   no dynamic-capability
```

Configuration du cluster ECMP à l'aide du commutateur Cisco Nexus 7000 avec protocole de routage

May 5, 2023

Avec la configuration ECMP sur un cluster, une appliance NetScaler est capable de gérer le trafic via un protocole de routage. Le mécanisme ECMP permet de publier les adresses IP du serveur virtuel via tous les nœuds de cluster actifs.

Pour utiliser ECMP, vous devez d'abord activer le protocole BGP sur l'adresse IP du cluster. Liez les interfaces et l'adresse IP repérée (avec le routage dynamique activé) à un VLAN. Configurez le protocole de routage sélectionné et redistribuez les routes du noyau sur le ZEBOS à l'aide du shell VTYSH.

Cas d'utilisation : Cluster ECMP à l'aide du commutateur Cisco Nexus 7000 avec protocole de routage

Prenons l'exemple d'un déploiement de cluster avec un commutateur Cisco Nexus 7000 :

- Deux appliances NetScaler (nœud 1 et nœud 2), connectées au commutateur Nexus (en amont).
- Deux commutateurs Cisco Nexus 7000.
- Client et serveur (attirant le trafic HTTP via le commutateur Nexus). Avec le protocole HSRP (Hot Standby Router Protocol) activé côté client.



Composants requis

Tenez compte des points suivants avant de configurer des nœuds de cluster sur une appliance NetScaler.

1. Toutes les appliances doivent être du même type de plate-forme.
2. Le protocole BGP (Border Gateway Protocol) doit être activé sur les nœuds du cluster.

Configuration à l'aide de l'interface de ligne de commande sur une appliance NetScaler

1. Connectez-vous à une appliance (par exemple, une appliance avec l'adresse NSIP 1.1.1.1)
2. Pour ajouter un nœud de cluster.

```
add cluster node 0 1.1.1.2 -state ACTIVE -backplane 0/10/8
```

3. Pour ajouter l'adresse IP du cluster

```
add ns ip 1.1.1.10 255.255.255.254 -type clip
```


4. Enregistrez la configuration

```
save ns config
```

5. Redémarrage à chaud de l'appliance

```
reboot -warm
```

6. Pour ajouter le nœud 1 à l'aide de CLIP

```
add cluster node 1 2.2.2.2 -state ACTIVE -backplane 1/10/8
```

7. Pour joindre un nœud au cluster

```
join cluster -clip 1.1.1.10 -password nsroot
```

8. Effectuez la configuration suivante sur CLIP

   - `enable ns feature bgp ospf DYNAMICROUTING`
   - `add ns ip 11.1.1.3 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0`
   - `add ns ip 11.1.1.7 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0`
   - `add ns ip 11.1.1.5 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1`
   - `add ns ip 11.1.1.9 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1`

Sur le routeur Cisco Nexus (11.1.1.2/31 et 11.1.1.4/31), vous devez effectuer les configurations suivantes à l'aide de la ligne de commande :

- `feature ospf`
- `feature bgp`
- `feature interface-vlan`
- `feature hsrp`

```
> interface vlan100
   no shutdown
   ip address 50.1.1.1/8
    hsrp 50
     ip 50.50.50.50

```



```
> interface Ethernet 4/15
  ip address 11.1.1.2/31
  no shutdown

> interface Ethernet 4/19
  ip address 11.1.1.4/31
  no shutdown

> interface Ethernet 4/22
  switchport
   switchport access vlan 100
```

Sur le routeur Cisco Nexus (11.1.1.6/31 et 11.1.1.8/31), vous devez effectuer les configurations suivantes à l'aide de la ligne de commande :

- `feature ospf`
- `feature bgp`
- `feature interface-vlan`
- `feature hsrp`

```
> interface vlan100
  no shutdown
  no ip redirects
  ip address 50.1.1.2/8
   hsrp 50
   ip 50.50.50.50

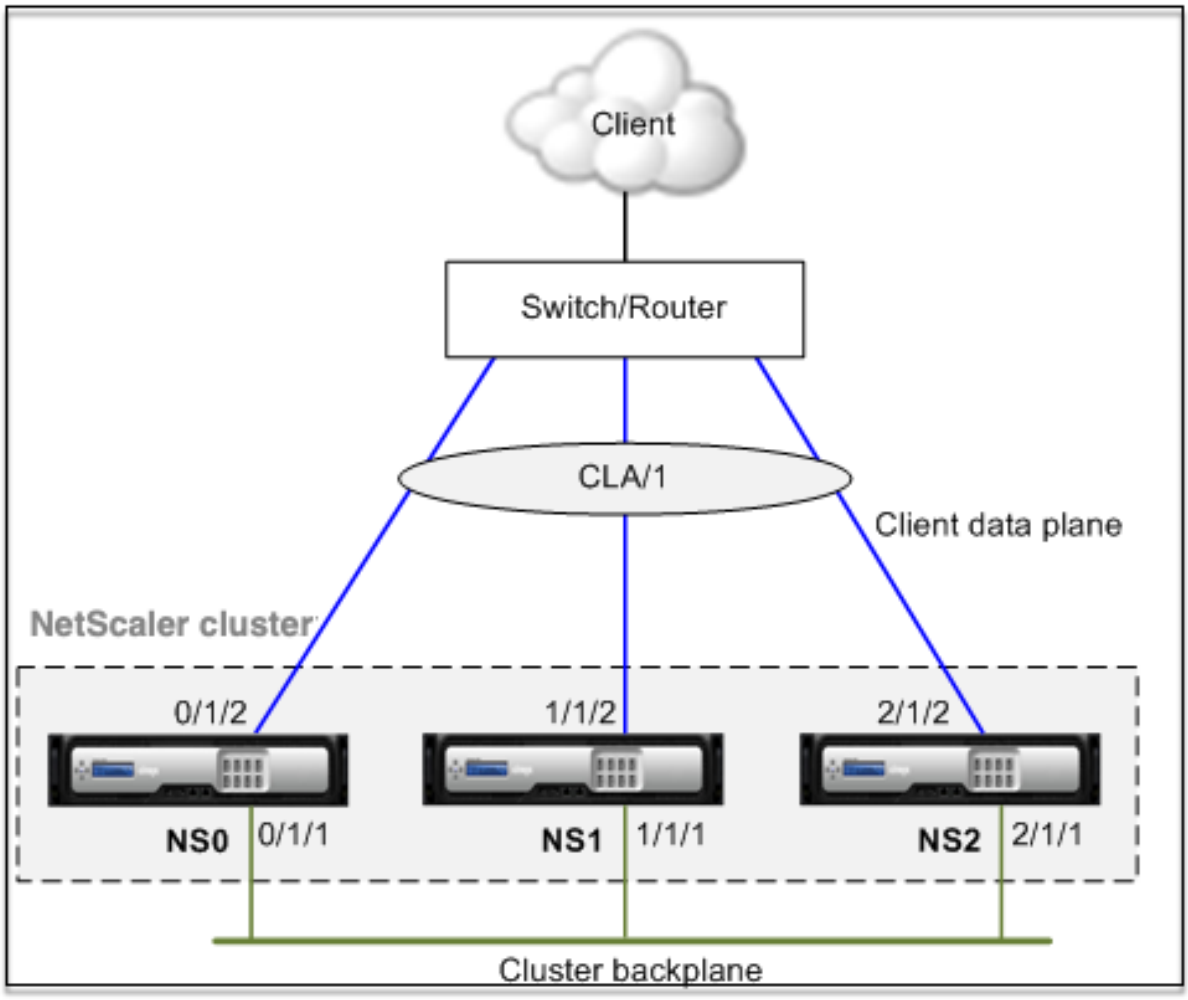
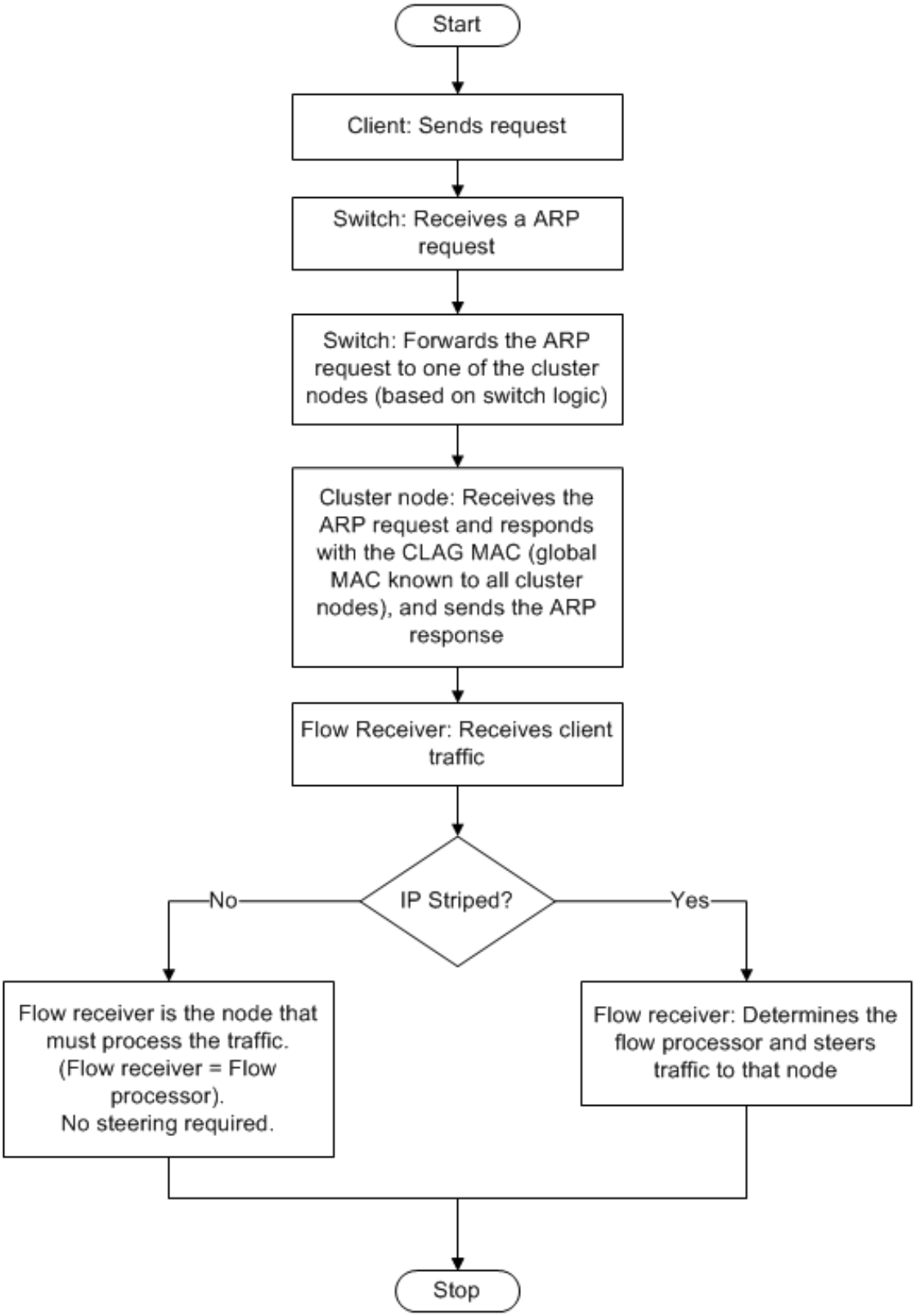
> interface Ethernet 4/13
  ip address 11.1.1.6/31
  no shutdown

> interface Ethernet 4/15
  ip address 11.1.1.8/31
  no shutdown

> interface Ethernet 4/22
  switchport
  switchport access vlan 100
```

Pour le protocole BGP, vous devez effectuer les configurations suivantes sur CLIP de l'appliance NetScaler :

```
> vtysh
ns# router bgp 1
```



```
 redistribute kernel
 owner-node 0
 neighbor 11.1.1.2 remote-as 2
 neighbor 11.1.1.2 as-origination-interval 1
 neighbor 11.1.1.2 advertisement-interval 0
 neighbor 11.1.1.6 remote-as 2
 neighbor 11.1.1.6 as-origination-interval 1
 neighbor 11.1.1.6 advertisement-interval 0
owner-node 1
 neighbor 11.1.1.4 remote-as 2
 neighbor 11.1.1.4 as-origination-interval 1
 neighbor 11.1.1.4 advertisement-interval 0
 neighbor 11.1.1.8 remote-as 2
 neighbor 11.1.1.8 as-origination-interval 1
 neighbor 11.1.1.8 advertisement-interval 0
exit-owner-node
```

Effectuez les configurations suivantes sur le routeur Cisco Nexus (11.1.1.3 et 11.1.1.5)

```
> ip access-list acl1
  10 permit ip 50.0.0.0/8 any
  route-map test permit
  match ip address acl1
 router bgp 2
  address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
 neighbor 11.1.1.3 remote-as 1
  address-family ipv4 unicast
  neighbor 11.1.1.5 remote-as 1
 address-family ipv4 unicast
```

Effectuez les configurations suivantes sur le routeur Cisco Nexus (11.1.1.7 et 11.1.1.9)

```
> ip access-list acl1
   10 permit ip 50.0.0.0/8 any
  route-map test permit 1
   match ip address acl1
  router bgp 2
   address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
  neighbor 11.1.1.7 remote-as 1
   address-family ipv4 unicast
  neighbor 11.1.1.9 remote-as 1
```



```
12    address-family ipv4 unicast
```

Pour le protocole OSPF, vous devez effectuer les configurations suivantes sur le CLIP de l'appliance NetScaler :

```
1  > vtysh
2  ns# router osfp 1
3  redistribute kernel
4  owner-node 0
5   network 15.1.1.2/31 area 0
6   network 15.1.1.6/31 area 0
7  exit-owner-node
8
9  owner-node 1
10  network 15.1.1.4/31 area 0
11  network 15.1.1.8/31 area 0
12 exit-owner-node
13
14 route-map map2 permit 1
15 set metric 10
```

Sur le routeur Cisco Nexus (11.1.1.2/31 et 11.1.1.4/31), vous devez effectuer les configurations suivantes à l'aide de la ligne de commande :

```
1  > route-map- map2 permit 1
2     set metric 10
3
4     interface Ethernet4/15
5       ip address 15.1.1.2/31
6       ip router ospf 1 area 0.0.0.0
7       no shutdown
8
9     interface Ethernet4/19
10      ip address 15.1.1.4/31
11      ip router ospf 1 area 0.0.0.0
12      no shutdown
13
14    router ospf 1
15     router-id 1.1.1.1
16     redistribute direct route-map map2
```

Sur le routeur Cisco Nexus (11.1.1.7/31 et 11.1.1.9/31), vous devez effectuer les configurations suivantes à l'aide de la ligne de commande :

```
1  > route-map- map2 permit 1
```



```
    set metric 10

  interface Ethernet4/13
    ip address 15.1.1.6/31
    ip router ospf 1 area 0.0.0.0
    no shutdown

   interface Ethernet4/15
    ip address 15.1.1.8/31
    ip router ospf 1 area 0.0.0.0
    no shutdown

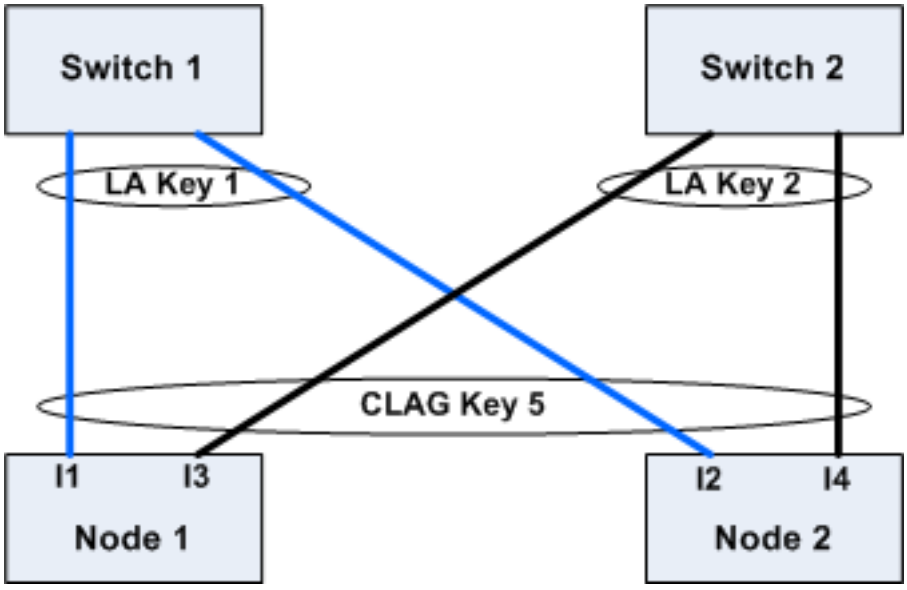
   router ospf 1
     router-id 1.1.1.2
     redistribute direct route-map map2
```

Utilisation de l'agrégation de liens de cluster

May 5, 2023

L'agrégation de liens de cluster est un groupe d'interfaces de nœuds de cluster. Il s'agit d'une extension de l'agrégation de liens NetScaler. La seule différence est que, alors que l'agrégation de liens nécessite que les interfaces proviennent du même périphérique, dans l'agrégation de liens de cluster, les interfaces proviennent de différents nœuds du cluster. Pour plus d'informations sur l'agrégation de liens, voir Configuration de l'agrégation de liens.

> **Important**
>
> - L'agrégation de liens de cluster est prise en charge pour un cluster d'appliances matérielles (MPX).
> - L'agrégation de liens de cluster est prise en charge pour un cluster d'appliances virtuelles (VPX) déployées sur des hyperviseurs ESX et KVM, avec les restrictions suivantes :
> - Des interfaces dédiées doivent être utilisées. Cela signifie que les interfaces ne doivent pas être partagées avec d'autres machines virtuelles.
> - Lorsqu'un nœud devient INACTIF, l'interface LA du cluster correspondante est marquée comme étant hors tension, de sorte que le trafic de données n'est pas envoyé vers un nœud INACTIF.
> - Lorsqu'un nœud devient ACTIF, l'interface LA du cluster correspondante est marquée comme étant sous tension.

- Si les interfaces des membres de l'agrégation de liens de cluster sont désactivées manuellement ou si l'agrégation de liens de cluster elle-même est désactivée manuellement, la capacité de mise hors tension de l'interface n'est atteinte que par le mécanisme de temporisation LACP.
- La MTU Jumbo n'est pas prise en charge sur l'agrégation de liens de clusters LACP.

Remarque : L'agrégation de liens de cluster n'est pas prise en charge sur les appliances VPX déployées sur XenServer, AWS et Hyper-V.

- À partir de la version 12.0, l'agrégation de liens de cluster est prise en charge sur les appliances NetScaler SDX.
- Le nombre d'interfaces pouvant être liées au cluster LA est de 16 (à partir de chaque nœud). Le nombre maximum d'interfaces dans le cluster LA peut être de (16 * n), où n est le nombre de nœuds dans un cluster. Le nombre total d'interfaces dans le cluster LA dépend du nombre d'interfaces pour chaque canal de port sur le commutateur en amont.
- Si une appliance NetScaler utilise des interfaces Intel Fortville, le passage d'un nœud de cluster en mode passif peut provoquer une panne de quelques secondes avec CLAG. Le problème se produit car le LACP est activé pour que CLAG fonctionne correctement et que la durée de la panne dépend des temporisateurs LACP de la carte réseau.

Prenons l'exemple d'un cluster à trois nœuds dans lequel les trois nœuds sont connectés au commutateur en amont. Un canal LA en cluster (CLA/1) est formé par des interfaces de liaison 0/1/2, 1/1/2 et 2/1/2.

Figure 1. Topologie d'agrégation de liens de cluster



Un canal LA de cluster possède les attributs suivants :

- Chaque canal possède un MAC unique convenu par les nœuds du cluster.
- Le canal peut lier les interfaces des nœuds locaux et distants.
- Un maximum de quatre canaux LA de cluster sont pris en charge dans un cluster.
- Les interfaces de fond de panier ne peuvent pas faire partie d'un canal LA de cluster.
- Lorsqu'une interface est liée à un canal LA du cluster, les paramètres du canal ont la priorité sur les paramètres de l'interface réseau. Une interface réseau ne peut être liée qu'à un seul canal.
- L'accès de gestion à un nœud de cluster ne doit pas être configuré sur un canal LA du cluster (par exemple, CLA/1) ou sur ses interfaces membres. Cela est dû au fait que lorsque le nœud est INACTIF, l'interface LA du cluster correspondante est marquée comme étant hors tension et perd donc l'accès à la gestion.

Figure 2. Flux de distribution du trafic à l'aide du cluster LA



Support de sauvegarde et de restauration du cluster LA sur NetScaler MPX

Vous pouvez sauvegarder et restaurer la configuration du cluster de LA sur NetScaler MPX. L'adresse MAC LA du cluster est indépendante de l'adresse MAC de l'interface physique des nœuds du cluster et peut changer après le processus de sauvegarde et de restauration. La CLUSTER LA peut servir le trafic une fois le processus de restauration de cluster terminé. Pour plus d'informations sur la sauvegarde et la restauration, reportez-vous à la section Sauvegarde et restauration de la configuration du cluster

Agrégation de liens de cluster statique

August 20, 2021

Vous devez configurer un canal LA de cluster statique sur l'adresse IP du cluster et sur le périphérique de connexion externe. Si possible, configurez le commutateur amont pour distribuer le trafic en fonction de l'adresse IP ou du port au lieu de l'adresse MAC.

Pour configurer un canal LA de cluster statique à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.

   > **Remarque**
   >
   > Assurez-vous de configurer le canal LA du cluster sur l'adresse IP du cluster avant de configurer l'agrégation des liens sur le commutateur externe. Sinon, le commutateur transfère le trafic au cluster même si le canal LA du cluster n'est pas configuré. Cela peut entraîner une perte de trafic.

2. Créez un canal LA de cluster.

   ```
   add channel <id> -speed <speed>
   ```

   Exemple

   ```
   add channel CLA/1 -speed 1000
   ```

   > **Remarque**
   >
   > Vous ne devez pas spécifier la vitesse comme AUTO. Vous devez plutôt spécifier explicitement la vitesse comme 10, 100, 1000 ou 10000. Seules les interfaces dont la vitesse correspond à l' <speed> attribut dans le canal LA du cluster sont ajoutées à la liste de distribution active.

3. Liez les interfaces requises au canal LA du cluster. Assurez-vous que les interfaces ne sont pas utilisées pour le backplane du cluster.

```
bind channel <id> <ifnum>
```

Exemple

```
bind channel CLA/1 0/1/2 1/1/2 2/1/2
```

4. Vérifiez les configurations.

```
show channel <id>
```

Exemple

```
show channel CLA/1
```

> **Remarque**
>
> Vous pouvez lier le canal LA du cluster à un VLAN à l'aide de la `bind vlan` commande. Les interfaces du canal sont automatiquement liées au VLAN.

5. Configurez LA statique sur le commutateur externe. Les exemples de configuration suivants sont fournis pour le Cisco® Nexus 7000 C7010 version 5.2 (1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
Global config:
Configure terminal

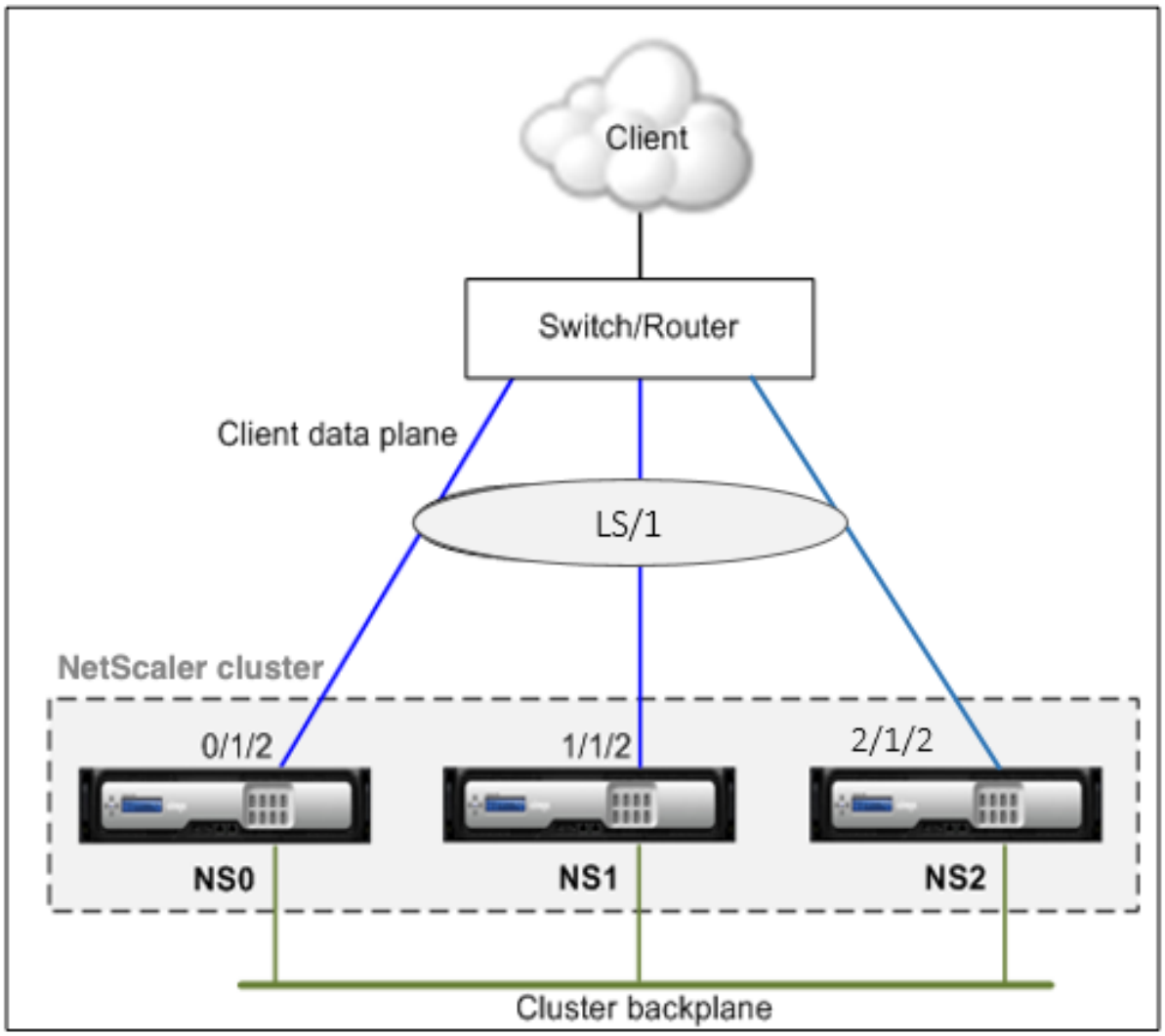
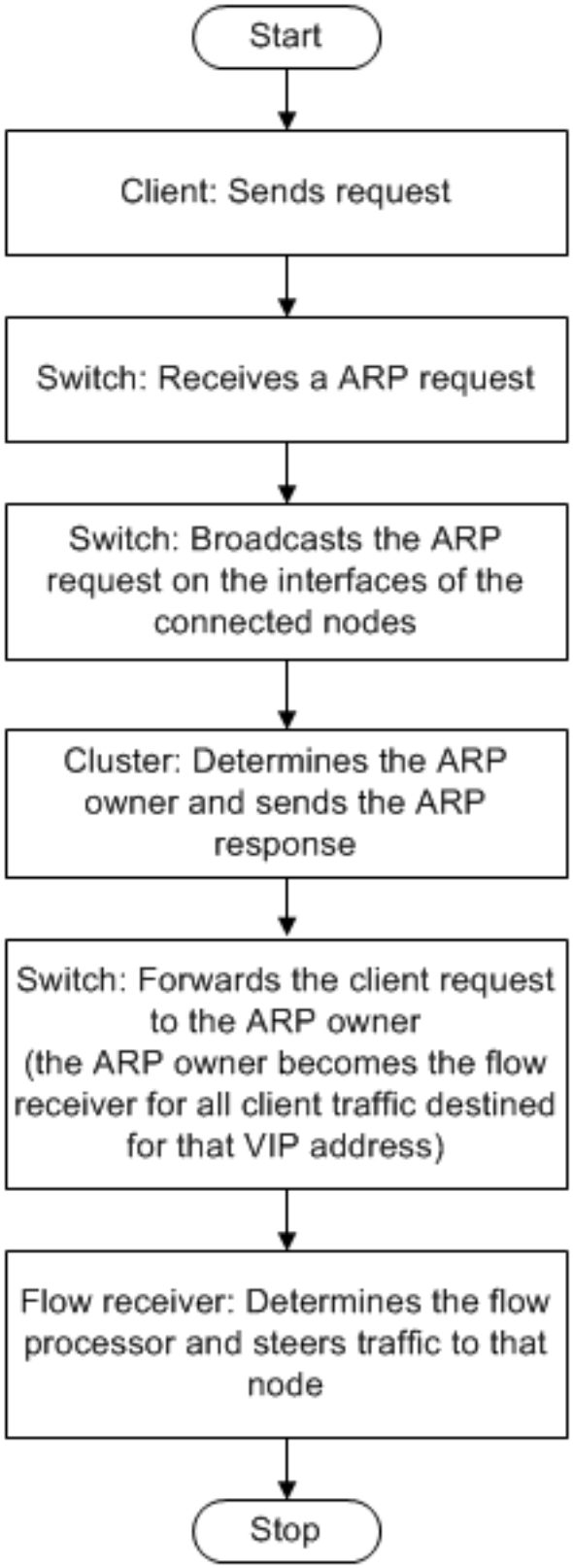
Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode on
no shutdown

interface Ethernet2/48
switchport
switchport access vlan 10
channel-group 7 mode on
no shutdown
```


Agrégation de liens de cluster dynamique

May 5, 2023

Le canal LA du cluster dynamique utilise le protocole LACP (Link Aggregation Control Protocol).

Vous devez effectuer des configurations similaires sur l'adresse IP du cluster et sur le périphérique de connexion externe. Si possible, configurez le commutateur en amont pour distribuer le trafic en fonction de l'adresse IP ou du port au lieu de l'adresse MAC.

> **Points à retenir**
>
> - Activez LACP (en spécifiant le mode LACP comme ACTIVE ou PASSIVE).

```
>**Note**
>
> Make sure the LACP mode is not set as PASSIVE on both the NetScaler
    cluster and the external connecting device.
```

> - Spécifiez la même clé LACP sur chaque interface que vous souhaitez faire partie du canal. Pour créer un canal LA de cluster, la clé LACP peut avoir une valeur comprise entre 5 et 8. Par exemple, si vous définissez la touche LACP sur les interfaces 0/1/2, 1/1/2 et 2/1/2 sur 5, CLA/1 est créé. Les interfaces 0/1/2, 1/1/2 et 2/1/2 sont automatiquement liées à CLA/1. De même, si vous définissez la touche LACP sur 6, le canal CLA/2 est créé.
> - Spécifiez le type de LAG comme Cluster.

Pour configurer un canal LA dynamique d'un cluster à l'aide de l'interface de ligne de commande

Sur l'adresse IP du cluster, pour chaque interface que vous souhaitez ajouter au canal LA du cluster, tapez :

```
set interface <id> -lacpMode <lacpMode> -lacpKey <positive_integer> -
lagType CLUSTER<!--NeedCopy-->
```

Exemple :

Pour configurer un cluster CLA/1 canal LA sur 3 interfaces.

```
> set interface 0/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
```


> **Remarque**
>
> Vous pouvez également activer la redondance des liens dans un cluster avec LACP.

De même, configurez LA dynamique sur le commutateur externe. Les exemples de configuration suivants sont fournis pour le Cisco® Nexus 7000 C7010 version 5.2 (1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
Global config:
Configure terminal
feature lacp
Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown

interface Ethernet2/48
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown
```

Redondance des liens dans un cluster avec LACP

May 5, 2023

Un cluster NetScaler assure la redondance des liens pour le LACP afin de garantir que tous les nœuds disposent de la même clé partenaire.

Pour comprendre le besoin de redondance des liens, prenons l'exemple de la configuration de cluster suivante ainsi que les cas qui l'accompagnent (en prêtant attention au cas 3) :



Dans cette configuration, les interfaces I1, I2, I3 et I4 sont liées au canal LACP avec KEY 5. Du côté du partenaire, I1 et I2 sont connectés au commutateur 1 pour former un seul canal LA avec KEY 1. De même, I3 et I4 sont connectés au commutateur 2 pour former un seul canal LA avec KEY 2.

Examinons maintenant les cas suivants pour comprendre le besoin de redondance des liens :

- **Cas 1 : le commutateur 1 est activé et le commutateur 2 est éteint**

  Dans ce cas, le cluster LA sur les deux nœuds cesserait de recevoir des LacPDU depuis Key2 et commencerait à recevoir des LacPDU depuis Key1. Sur les deux nœuds, le cluster LA est connecté à KEY 1 et I1 et I2 sont actifs et le canal des deux nœuds serait ouvert.

- **Cas 2 : le commutateur 1 s'arrête et le commutateur 2 passe à la vitesse supérieure**

  Dans ce cas, le cluster LA sur les deux nœuds cesserait de recevoir des LacPDU depuis Key1 et commencerait à recevoir des LacPDU depuis Key2. Sur les deux nœuds, le cluster LA est connecté à Key2 et I3 et I4 sont actifs et le canal sur les deux nœuds serait actif.

- **Cas 3 : Le Switch1 et le Switch2 sont actifs**

  Dans ce cas, il est possible que le cluster LA sur le nœud 1 choisisse Key1 comme partenaire et que le cluster LA sur le nœud 2 choisisse Key2 comme partenaire. Cela signifie que I1 sur le nœud 1 et I4 sur le nœud 2 reçoivent du trafic indésirable. Cela peut se produire parce que la machine d'état LACP se situe au niveau des nœuds et choisit ses partenaires selon le principe du premier arrivé, premier servi.

  Pour résoudre ces problèmes, la redondance des liens du cluster dynamique LA est prise en charge. Pour configurer la redondance des liens sur un canal ou une interface, vous devez l'activer et éventuellement spécifier le seuil de débit comme suit :

  ```
  set channel CLA/1 -linkRedundancy ON -lrMinThroughput <positive_integer
  >
  ```


Le débit des canaux partenaires est vérifié par rapport au seuil de débit configuré. Le canal partenaire qui satisfait le seuil de débit est sélectionné selon le principe du premier entré, premier sorti (FIFO). Si aucun canal partenaire n'atteint le seuil, ou si le débit seuil n'est pas configuré, le canal partenaire avec le nombre maximum de liens est sélectionné.

> **Remarque**
>
> Le seuil de débit peut être configuré à partir de NetScaler 11.

Utilisation du mode USIP dans le cluster

May 5, 2023

En mode Use Source IP (USIP), le cluster ou l'appliance NetScaler transmet chaque paquet au serveur principal approprié avec l'adresse IP du client.

Distribution du trafic en mode USIP

Le comportement du mode USIP diffère de la distribution du trafic entre le plan de données client et le plan de données du serveur dans le déploiement ECMP et CLAG. La section suivante fournit plus d'informations sur le comportement du mode USIP. Pour plus d'informations sur CLAG en mode USIP, voir Utilisation de l'agrégation de liens de cluster.

Mode USIP

Le cluster utilise l'adresse IP du client pour ouvrir la connexion côté serveur. Le port source peut ou non être préservé en fonction du `useproxyport` paramètre.

`useproxyport` Scénarios USIP

L'USIP `useproxyport` est activé pour le flux de trafic, le port source est sélectionné de manière à ce que le trafic inverse se hache vers le processeur de flux. Il assure une direction unique côté serveur.

L'USIP `useproxyport` est désactivé pour le flux de trafic, le port source est préservé et il y a donc une double direction côté serveur.

> **Important**
>
> - Lorsque USIP est allumé, l'adresse IP du client est utilisée dans la connexion au serveur principal, et la distribution du trafic pour la réponse est nécessaire entre les nœuds de cluster. Vous pouvez utiliser le déploiement ECMP ou CLAG pour la distribution du trafic côté serveur. En l'absence de distribution du trafic côté serveur, l'ensemble du trafic de retour

> peut atterrir sur un nœud de cluster unique, ce qui entraîne une congestion.
> - La `set rsskeytype -rsskey symmetric` commande est utilisée pour réduire la double direction à la direction unique du trafic dans les déploiements `useproxyport` hors tension. Où le 4 tuple de la connexion reste le même pour le serveur et le client. Par exemple, serveur virtuel en mode MAC générique.

Limitations

L'USIP ne fonctionne pas lorsque le processus local est désactivé.

Déploiement en mode USIP

La figure suivante illustre un déploiement en mode USIP dans une configuration de cluster.

Configurer les éléments suivants à l'aide de l'interface

1. Activez le protocole de routage.

```
enable ns feature <feature>
```

Exemple :

```
enable ns feature ospf
```

2. Ajoutez une adresse SNIP spotted pour chaque nœud et activez le routage dynamique sur celui-ci.

```
add ns ip <SNIP> <netmask> -dynamicRouting ( ENABLED | DISABLED )
    - ownerNode <positive_interger>  - ownerdownResponse ( YES | NO
   )
```

Exemple

```
- add ns ip 192.0.2.1 255.255.255.0 -dynamicRouting ENABLED -
  ownerNode 0 - ownerDownResponse NO
- add ns ip 192.0.2.2 255.255.255.0 -dynamicRouting ENABLED -
  ownerNode 1 - ownerDownResponse NO
- add ns ip 192.0.2.3 255.255.255.0 -dynamicRouting ENABLED -
  ownerNode 2 - ownerDownResponse NO
```

3. Ajoutez un VLAN.

```
add vlan <id>
```


Exemple

```
add vlan 300
```

4. Liez les interfaces des nœuds du cluster au VLAN.

```
bind vlan <id> -ifnum <interface_name>
```

Exemple

```
bind vlan 300 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Liez l'une des adresses SNIP spotted au VLAN. Lorsque vous liez une adresse SNIP repérée à un VLAN, toutes les autres adresses SNIP repérées définies sur le cluster de ce sous-réseau sont automatiquement liées au VLAN.

```
bind vlan <id> -IPAddress <ip_addr | ipv6_addr> -netmask
```

Exemple

```
bind vlan 300  - IPAddress 192.0.2.1 255.255.255.0
```

6. Configurez le protocole de routage sur les ZEBOs à l'aide du shell VTYSH. Configurez le protocole de routage OSPF sur les ID de nœud 0, 1 et 2.

```
vtysh
configure terminal
ns block-sec-rtadv
router ospf
owner -node 0
router-id 192.0.2.1
exit-owner-node
owner-node 1
router-id 192.0.2.2
exit-owner-node
owner-node 2
router-id 192.0.2.3
exit-owner-node
network 192.0.2.0/24 area 0

default-information originate always
```

7. Effectuez les configurations suivantes sur le routeur Cisco 3750 à l'aide de l'interface de ligne de commande.


```
Configure terminal
feature ospf
interface vlan300
no shutdown
ip address 192.0.2.100/24
Configure terminal
router ospf 1
router-id 192.0.2.100
network 192.0.2.0 0.0.0.255 area 0
```

Remarques

- La distribution du trafic sur le client et le serveur n'est pas nécessairement identique. Par exemple, vous pouvez configurer ECMP côté client et CLAG côté serveur ou opposé.
- Prévoyez une capacité supplémentaire du fond de panier car il y a plus de surcharge de direction dans le déploiement USIP.
- La configuration associée à CLAG et à Monitor Static Route (MSR) doit rester la même côté serveur.
- La direction du trafic est plus présente dans les déploiements en mode USIP.

Gestion du cluster NetScaler

May 5, 2023

Une fois que vous avez créé un cluster et configuré le mécanisme de distribution du trafic requis, le cluster est en mesure de gérer le trafic. Pendant la durée de vie du cluster, vous pouvez effectuer les tâches suivantes :

- Configuration des groupes de nœuds
- Désactivation des nœuds d'un cluster
- À la découverte des appliances NetScaler
- Affichage des statistiques
- Synchronisation des configurations de cluster et des fichiers de cluster
- Synchronisation de l'heure entre les nœuds
- Mise à niveau ou rétrogradation du logiciel des nœuds du cluster

Configuration des jeux de liens

January 21, 2021

Linkset est un groupe d'interfaces de nœuds de cluster qui appartiennent au même domaine de diffusion. Dans les ensembles de liens, chaque nœud possède les informations sur les interfaces des autres nœuds qui sont connectées au même domaine de diffusion.

> **Remarque**
>
> Les jeux de liens sont une configuration obligatoire dans les scénarios suivants :
>
> - Pour les déploiements nécessitant le transfert basé sur Mac (MBF).
> - Pour le mode « -m MAC » activé sur le serveur virtuel avec le mode MBF activé globalement.
> - Améliorer la gérabilité des stratégies ACL et L2 impliquant des interfaces. Vous définissez un jeu de liens des interfaces et ajoutez des stratégies ACL et L2 basées sur des ensembles de liens.

Dans une configuration de cluster, les fonctionnalités suivantes utilisent MBF en interne.

- Transmission de la session
- L2Conn
- Serveur virtuel en mode MAC
- Moniteur transparent
- LLB

Les jeux de liens doivent être configurés uniquement via l'adresse IP du cluster.

Prenons un exemple avec un cluster à trois nœuds. Dans la figure suivante, les interfaces 0/1/2, 1/1/2 et 2/1/2 sont dans le même domaine de diffusion et peuvent donc être configurées en tant que linkset (LS/1).

Figure 1. Topologie des jeux de liens



Figure 2. Flux de distribution du trafic à l'aide de jeux de liens



Pour configurer un jeu de liens à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.
2. Créez un jeu de liens.

   "'add linkset

   ```
   **Exemple**

   ```add linkset LS/1<!--NeedCopy-->
   ```

3. Liez les interfaces requises au jeu de liens. Assurez-vous que les interfaces ne sont pas utilisées pour le backplane du cluster.

   "'bind linkset -ifnum ...

   ```
   **Exemple**

   ```bind linkset LS/1 -ifnum 0/1/2 1/1/2 2/1/2<!--NeedCopy-->
   ```

4. Vérifiez les configurations du jeu de liens.

   "'show linkset

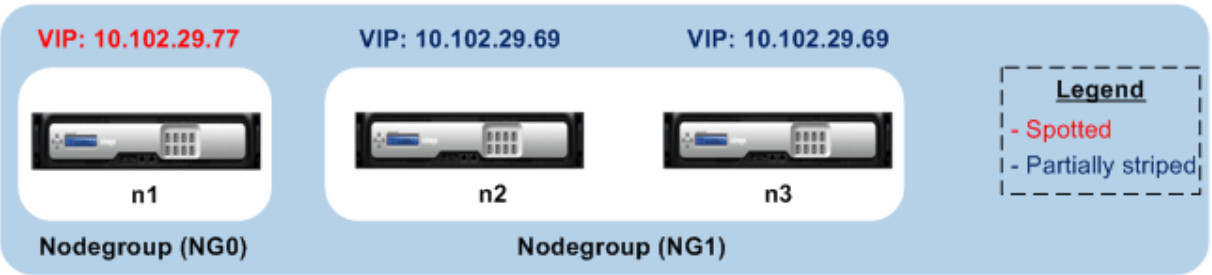
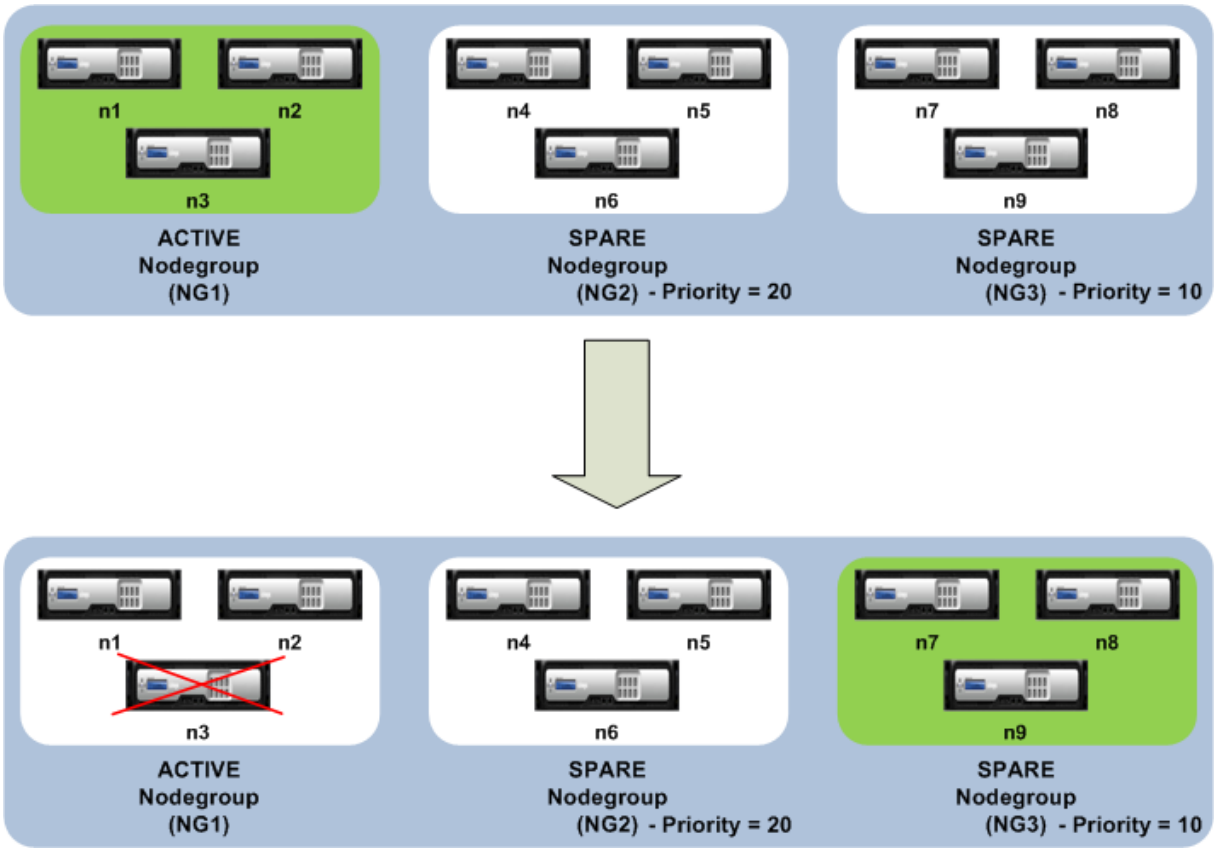
   ```
   **Exemple**

   ```show linkset LS/1<!--NeedCopy-->
   ```

> **Remarque**
>
> Vous pouvez lier le jeu de liens à un VLAN à l'aide de la `bind vlan` commande. Les interfaces du jeu de liens sont automatiquement liées au VLAN.

Pour configurer un jeu de liens à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Réseau > Linksets**.
3. Dans le volet d'informations, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Créer un jeu de liens** :
   - Spécifiez le nom du jeu de liens en définissant le paramètre Linkset.
   - Spécifiez les interfaces à ajouter au jeu de liens et cliquez sur Ajouter . Répétez cette étape pour chaque interface que vous souhaitez ajouter au jeu de liens.
5. Cliquez sur **Créer**, puis sur **Fermer**.


   ```

# Groupes de nœuds pour les configurations ponctuelles et partiellement réparties par bandes

May 5, 2023

En raison du comportement par défaut du cluster, toutes les configurations effectuées sur l'adresse IP du cluster sont disponibles sur tous les nœuds du cluster. Toutefois, dans certains cas, vous pouvez avoir besoin que certaines configurations soient disponibles uniquement sur des nœuds de cluster spécifiques.

Vous pouvez répondre à cette exigence en définissant un groupe de nœuds qui inclut les nœuds de cluster spécifiques, puis en liant la configuration à ce groupe de nœuds. Cela garantit que la configuration est active uniquement sur ces nœuds du cluster. Ces configurations sont appelées partiellement rayées ou ponctuées (si elles sont actives un seul nœud). Pour plus d'informations, voir Configurations rayées, partiellement rayées et ponctuées.

Par exemple, considérez un cluster avec trois nœuds. Vous créez un groupe de nœuds NG0 qui inclut le nœud n1 et un autre groupe de nœuds NG1 qui inclut n2 et n3. Liez les serveurs virtuels d'équilibrage de charge 0.77 à NG0 et le serveur virtuel d'équilibrage de charge 0.69 à NG1.

Cela signifie que le serveur virtuel 0.77 est actif uniquement sur n1 et que, par conséquent, seul n1 reçoit le trafic dirigé vers 0.77. De même, le serveur virtuel 0.69 est actif uniquement sur les nœuds n2 et n3 et, par conséquent, seuls n2 et n3 reçoivent le trafic dirigé vers 0.69.

Figure 1. Cluster NetScaler avec groupes de nœuds configurés pour des configurations ponctuelles et partielles




Les entités ou configurations que vous pouvez lier à un groupe de nœuds sont les suivantes :

- Équilibrage de charge, commutation de contenu, redirection du cache, authentification, autorisation et audit des serveurs virtuels

  > **Remarque**
  >
  > Les serveurs virtuels d'équilibrage de charge FTP ne peuvent pas être liés à des groupes de nœuds.

- Serveur virtuel VPN (pris en charge à partir de NetScaler 10.5 Build 50.10)

 

- Sites GSLB (Global Server Load Balancing) et autres entités GSLB (pris en charge à partir de NetScaler 10.5 Build 52.11)
- Identifiants de limite et identifiants de flux

## Comportement des groupes de nœuds

May 5, 2023

En raison de l'interopérabilité des groupes de nœuds avec différentes fonctionnalités et entités de NetScaler, certains aspects comportementaux doivent être pris en compte. Les nœuds d'un groupe de nœuds peuvent également être sauvegardés. Lisez la suite pour plus d'informations.

### Comportement général d'un groupe de nœuds de cluster

- Un groupe de nœuds auquel sont liées des entités ne peut pas être supprimé.
- Un nœud de cluster qui appartient à un groupe de nœuds auquel sont liées des entités ne peut pas être supprimé.
- Une instance de cluster qui comporte des groupes de nœuds auxquels sont liées des entités ne peut pas être supprimée.
- Vous ne pouvez pas ajouter une entité qui dépend d'une autre entité. Il ne doit pas faire partie du groupe de nœuds. Si vous devez le faire, supprimez d'abord la dépendance. Ajoutez ensuite les deux entités au groupe de nœuds et réassociez-les.

  **Exemples :**

  - Supposons que vous disposez d'un serveur virtuel, VS1, dont la sauvegarde est le serveur virtuel VS2. Pour ajouter VS1 à un groupe de nœuds, assurez-vous d'abord que VS2 est supprimé en tant que serveur de sauvegarde de VS1. Liez ensuite chaque serveur individuellement au groupe de nœuds, puis configurez VS2 comme sauvegarde pour VS1.
  - Supposons que vous disposiez d'un serveur virtuel de commutation de contenu, CSVS1, dont le serveur virtuel d'équilibrage de charge cible est LBVS1. Pour ajouter CSVS1 à un groupe de nœuds, supprimez d'abord LBVS1 comme cible. Liez ensuite chaque serveur individuellement au groupe de nœuds, puis configurez LBVS1 comme cible.
  - Supposons que vous disposiez d'un serveur virtuel d'équilibrage de charge, LBVS1, dont la politique appelle un autre serveur virtuel d'équilibrage de charge, LBVS2. Pour ajouter l'un des serveurs virtuels, supprimez d'abord l'association. Liez ensuite chaque serveur individuellement au groupe de nœuds, puis réassociez les serveurs virtuels.

 

- Vous ne pouvez pas lier une entité à un groupe de nœuds. Il n'a pas de nœuds et l'option stricte est activée. Par conséquent, vous ne pouvez pas dissocier le dernier nœud d'un groupe de nœuds auquel sont liées des entités et auquel l'option stricte est activée.
- L'option stricte ne peut pas être modifiée pour un groupe de nœuds qui ne comporte aucun nœud mais auquel sont liées des entités.

### Sauvegarde des nœuds d'un groupe de nœuds

Par défaut, un groupe de nœuds est conçu pour fournir des nœuds de sauvegarde aux membres d'un groupe de nœuds. Si un membre du groupe de nœuds tombe en panne, un nœud de cluster qui n'est pas membre du groupe de nœuds remplace dynamiquement le nœud défaillant. Ce nœud est appelé nœud de remplacement.

> **Remarque**
>
> Pour un groupe de nœuds à membre unique, un nœud de sauvegarde est automatiquement présélectionné lorsqu'une entité est liée au groupe de nœuds.

Lorsque le membre d'origine du groupe de nœuds apparaît, le nœud de remplacement est remplacé par défaut par le nœud membre d'origine.

À partir de NetScaler 10.5 Build 50.10, NetScaler vous permet toutefois de modifier ce comportement de remplacement. Lorsque vous activez l'option permanente, le nœud de remplacement est conservé même après l'apparition du nœud membre d'origine. Le nœud d'origine prend le relais uniquement lorsque le nœud de remplacement tombe en panne.

Vous pouvez également désactiver la fonctionnalité de sauvegarde. Pour ce faire, vous devez activer l'option stricte. Dans ce scénario, lorsqu'un membre du groupe de nœuds tombe en panne, aucun autre nœud du cluster n'est sélectionné comme nœud de secours. Le nœud d'origine continue de faire partie du groupe de nœuds lorsqu'il apparaît. Cette option garantit que les entités liées à un groupe de nœuds ne sont actives que sur les membres du groupe de nœuds.

> **Remarque**
>
> L'option stricte et rémanente ne peut être définie que lors de la création d'un groupe de nœuds.

## Configuration de groupes de nœuds pour des configurations ponctuelles et partiellement réparties par bandes

May 5, 2023

Pour configurer un groupe de nœuds pour des configurations ponctuelles et partiellement réparties par bandes, vous devez d'abord créer un groupe de nœuds, puis lier les nœuds requis au groupe de

 

nœuds. Vous associez ensuite les entités requises à ce groupe de nœuds. Les entités liées au groupe de nœuds sont les suivantes :

- **Repéré** : s'il est lié à un groupe de nœuds ne comportant qu'un seul nœud.
- **Partiellement rayé** : s'il est lié à un groupe de nœuds comportant plusieurs nœuds.

**Quelques points à retenir :**

- GSLB est pris en charge sur un cluster uniquement lorsque les sites GSLB sont liés à des groupes de nœuds qui ont un seul nœud de cluster. Pour plus d'informations, voir Configuration de GSLB dans un cluster.
- NetScaler Gateway est pris en charge sur un cluster uniquement lorsque les serveurs virtuels VPN sont liés à des groupes de nœuds dotés d'un seul nœud de cluster. L'option permanente doit être activée sur le groupe de nœuds.
- Pour les versions antérieures à NetScaler 11, le pare-feu applicatif n'est pris en charge que sur des nœuds de cluster individuels (configuration repérée). Les profils de pare-feu d'applications ne peuvent être associés qu'à des serveurs virtuels liés à des groupes de nœuds dotés d'un seul nœud de cluster. Cela signifie que vous n'êtes pas autorisé à effectuer les opérations suivantes dans cette application :
  - Liez les profils de pare-feu d'applications à des serveurs virtuels répartis par bandes ou partiellement répartis par bandes.
  - Liez la politique à un point de liaison global ou à des étiquettes de politique définies par l'utilisateur.
  - Dissociez d'un groupe de nœuds un serveur virtuel doté de profils de pare-feu d'applications.
- NetScaler 11 a introduit la prise en charge du pare-feu des applications pour les configurations par bandes et partiellement répartites. Pour plus d'informations, voir Prise en charge du pare-feu d'application pour les configurations de cluster.

Consultez les fonctionnalités de NetScaler prises en charge dans un cluster pour voir les versions de NetScaler à partir desquelles GSLB, NetScaler Gateway et le pare-feu d'applications sont pris en charge dans un cluster.

### Pour configurer un groupe de nœuds à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.
2. Créez un groupe de nœuds. Type :

   ```
   add cluster nodegroup <name> -strict (YES | NO)<!--NeedCopy-->
   ```

   Exemple

   ```
   1 add cluster nodegroup NG0 -strict YES
   ```


3. Liez les nœuds requis au groupe de nœuds. Tapez la commande suivante pour chaque membre du groupe de nœuds :

   ```
   bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
   ```

   Exemple

   Pour lier des nœuds avec les ID 1, 5 et 6.

   ```
   1 > bind cluster nodegroup NG0 -node 1
   2 > bind cluster nodegroup NG0 -node 5
   3 > bind cluster nodegroup NG0 -node 6
   ```

4. Liez l'entité au groupe de nœuds. Tapez la commande suivante une fois pour chaque entité que vous souhaitez lier :

   ```
   bind cluster nodegroup <name> (-vServer <string> | -identifierName <
   string> | -gslbSite <string> -service <string>)<!--NeedCopy-->
   ```

   > **Remarque**
   >
   > Les paramètres de GSLBsite et de service sont disponibles à partir de NetScaler 10.5.

   Exemple

   Pour lier des serveurs virtuels VS1 et VS2 et l'identificateur de limite de débit nommé identifier1.

   ```
   1 > bind cluster nodegroup NG0 -vServer VS1
   2 > bind cluster nodegroup NG0 -vServer VS2
   3 > bind cluster nodegroup NG0 -identifierName identifier1
   ```

5. Vérifiez les configurations en affichant les détails du groupe de nœuds. Type :

   ```
   show cluster nodegroup <name><!--NeedCopy-->
   ```

   Exemple

   ```
   1 > show cluster nodegroup NG0
   ```

Pour configurer un groupe de nœuds à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Groupes de nœuds.**
3. Dans le volet de détails, cliquez sur **Ajouter.**
4. Dans la boîte de dialogue **Créer un groupe de nœuds**, configurez le groupe de nœuds :
   a) Sous **Nœuds de cluster**, cliquez sur le bouton **Ajouter** .
      - La liste Disponible affiche les nœuds que vous pouvez lier au groupe de nœuds et la liste des nœuds configurés affiche les nœuds liés au groupe de nœuds.

- Cliquez sur le signe **+** dans la liste Disponible pour lier le nœud. De même, cliquez sur le signe **-** dans la liste des configurations pour dissocier le nœud.

b) Sous **Serveurs virtuels**, sélectionnez l'onglet correspondant au type de serveur virtuel que vous souhaitez lier au groupe de nœuds. Cliquez sur le bouton **Add**.

- La liste Disponible affiche les serveurs virtuels que vous pouvez lier au groupe de nœuds et la liste des serveurs configurés affiche les serveurs virtuels qui sont liés au groupe de nœuds.
- Cliquez sur le signe **+** dans la liste Disponible pour lier le serveur virtuel. De même, cliquez sur le signe - dans la liste des configurations pour dissocier le serveur virtuel.

Configuration de la redondance pour les groupes de nœuds

May 5, 2023

> **Remarque**
>
> Pris en charge à partir de NetScaler 10.5 Build 52.1115.e.

Les groupes de nœuds peuvent être configurés de telle sorte que lorsqu'un groupe de nœuds tombe en panne, un autre groupe de nœuds puisse prendre le relais et traiter le trafic. Par exemple, lorsqu'un groupe de nœuds NG1 tombe en panne, NG2 prend le relais.

> **Remarque**
>
> Cette fonctionnalité peut être utilisée pour configurer la redondance du centre de données où chaque groupe de nœuds est configuré en tant que centre de données.

Pour atteindre ce cas d'utilisation, les nœuds du cluster doivent être regroupés de manière logique en groupes de nœuds, certains groupes de nœuds devant être configurés comme ACTIFS et d'autres comme SPARE. Le groupe de nœuds actifs ayant la priorité la plus élevée (c'est-à-dire le numéro de priorité le plus bas) est rendu opérationnel et gère donc le trafic. Lorsqu'un nœud de ce groupe de nœuds actif sur le plan opérationnel tombe en panne, le nombre de nœuds de ce groupe de nœuds est comparé au nombre de nœuds des autres groupes de nœuds actifs par ordre de priorité. Si le nombre de nœuds d'un groupe de nœuds est supérieur ou égal, ce groupe de nœuds est rendu opérationnel. Sinon, les groupes de nœuds de rechange sont vérifiés.

> **Remarque**
>
> - Un seul groupe de nœuds spécifique à un État peut être actif à un moment donné.
> - Un nœud de cluster hérite de l'état du groupe de nœuds. Ainsi, si un nœud avec l'état « SPARE » est ajouté au groupe de nœuds avec l'état « ACTIVE », le nœud se comporte automatiquement comme un nœud actif.

- Le paramètre de préemption défini pour l'instance de cluster décide si le groupe de nœuds actif initial prend le contrôle lorsqu'il réapparaît.
- Un groupe de nœuds de rechange peut occuper un groupe de nœuds et héberger du trafic actif lorsqu'un groupe de nœuds actif tombe en panne.

La figure suivante montre une configuration de groupe de nœuds dans laquelle la redondance des groupes de nœuds est définie. NG1 est initialement le groupe de nœuds actif. Lorsqu'il perd l'un des nœuds, le groupe de nœuds de rechange (NG3) ayant la priorité la plus élevée commence à traiter le trafic.

Figure 1. Cluster NetScaler avec redondance des groupes de nœuds configurée.



Configuration de la redondance pour les groupes de nœuds

1. Connectez-vous à l'adresse IP du cluster.
2. Créez le groupe de nœuds actif et liez les nœuds de cluster requis.

```
1 > add cluster nodegroup NG1 -state ACTIVE
2 > bind cluster nodegroup NG1 -node n1
3 > bind cluster nodegroup NG1 -node n2
4 > bind cluster nodegroup NG1 -node n3
```


3. Créez le groupe de nœuds de rechange et liez les nœuds requis.

```
> add cluster nodegroup NG2 -state SPARE -priority 20
> bind cluster nodegroup NG2 -node n4
> bind cluster nodegroup NG2 -node n5
> bind cluster nodegroup NG2 -node n6
```

4. Créez un autre groupe de nœuds de rechange et liez les nœuds requis.

```
> add cluster nodegroup NG3 -state SPARE -priority 10
> bind cluster nodegroup NG3 -node n7
> bind cluster nodegroup NG3 -node n8
> bind cluster nodegroup NG3 -node n9
```

Désactivation de la direction sur le fond de panier du cluster

May 5, 2023

> **Remarque**
>
> Pris en charge à partir de NetScaler 11.

Le comportement par défaut d'un cluster NetScaler consiste à diriger le trafic qu'il reçoit (récepteur de flux) vers un autre nœud (processeur de flux). Le processeur de flux doit ensuite traiter le trafic. Ce processus qui consiste à diriger le trafic du récepteur de flux vers le processeur de flux s'effectue via le panneau arrière du cluster et est appelé pilotage.

Si nécessaire, vous pouvez désactiver le pilotage afin que le processus soit local par rapport au récepteur de débit et fasse ainsi du récepteur de débit le processeur de débit. Une telle configuration peut s'avérer utile lorsque vous disposez d'un lien à latence élevée.

> **Remarque**
>
> Cette configuration s'applique uniquement aux serveurs virtuels répartis par bandes.

- Pour les serveurs virtuels partiellement répartis par bandes, si le récepteur de flux est un nœud non propriétaire, le trafic est dirigé vers un nœud propriétaire. Si toutefois le récepteur de débit est un nœud propriétaire, le pilotage est désactivé.
- Pour les serveurs virtuels repérés, le récepteur de flux est le processeur de flux et il n'est donc pas nécessaire de le piloter.

Quelques points à retenir lors de la désactivation du mécanisme de direction :

- Les SNIP par bandes ne sont pas pris en charge car le pilotage est désactivé.
- MPTCP et FTP ne fonctionnent pas.

- Le mode L2 doit être désactivé.
- Si l'USIP est activé, le trafic risque de ne pas revenir au même nœud car le pilotage est désactivé.
- Le trafic dirigé vers l'adresse IP du cluster est dirigé vers le coordinateur de configuration.
- Lorsqu'un nœud rejoint ou quitte un cluster, il est possible que plus de 1/N de connexions soient affectées. Cela est dû au fait qu'une modification des nœuds disponibles peut entraîner le remaniement des routes. Par conséquent, le trafic est acheminé vers un autre nœud et, en raison de l'indisponibilité du pilotage, le trafic n'est pas traité.

Le pilotage peut être désactivé au niveau du serveur virtuel individuel ou au niveau mondial. La configuration globale est prioritaire par rapport au paramètre du serveur virtuel.

- Désactivation du pilotage du backplane pour tous les serveurs virtuels répartis par bandes

  Configuré au niveau de l'instance du cluster. Le trafic destiné à un serveur virtuel réparti par bandes n'est pas dirigé sur le panneau principal du cluster.

  ```
  add cluster instance \<clId\> -processLocal ENABLED<!--NeedCopy-->
  ```

- Désactivation du pilotage du backplane pour un serveur virtuel réparti par bandes spécifique

  Configuré sur un serveur virtuel réparti par bandes. Le trafic destiné au serveur virtuel n'est pas dirigé sur le backplane du cluster.

  ```
  add lb vserver <name> <serviceType> -processLocal ENABLED<!--NeedCopy
  -->
  ```

Synchronisation des configurations de cluster

May 5, 2023

Les configurations NetScaler disponibles sur le coordinateur de configuration sont synchronisées avec les autres nœuds du cluster lorsque :

- Un nœud rejoint le cluster
- Un nœud rejoint le cluster
- Une nouvelle commande est exécutée via l'adresse IP du cluster

Vous pouvez également synchroniser avec force les configurations disponibles sur le coordinateur de configuration (synchronisation complète) avec un nœud de cluster spécifique. Assurez-vous de synchroniser un nœud de cluster à la fois, sinon le cluster pourrait être affecté.

Pour synchroniser les configurations de cluster à l'aide de la CLI :

À l'invite de commandes de l'appliance sur laquelle vous souhaitez synchroniser les configurations, tapez :


```
force cluster sync
```

Pour synchroniser les configurations de cluster à l'aide de l'interface graphique :

1. Ouvrez une session sur l'appliance sur laquelle vous souhaitez synchroniser les configurations.
2. Accédez à **Système > Cluster.**
3. Dans le volet de détails, sous **Utilitaires**, cliquez sur Forcer la synchronisation du cluster.
4. Cliquez sur **OK.**

La liste d'affichage des commandes a échoué pendant la synchronisation de la configuration

Dans une configuration de cluster, avec le mode strict d'état de synchronisation `syncStatusStrictMode` activé, vous pouvez afficher la liste des commandes ayant échoué lors d'une synchronisation de cluster sur un nœud non CCO.

Vous pouvez déterminer l'état de synchronisation du cluster d'un nœud non CCO en exécutant l' `show node` opération. `PARTIAL SUCCESS` L'état de synchronisation indique que certaines commandes ont échoué sur le nœud autre que CCO lors de la synchronisation du cluster.

Pour afficher la liste des commandes ayant échoué sur un nœud lors de la synchronisation du cluster à l'aide de l'interface de ligne de commande :

- `show cluster syncFailures`

Exemple de configuration

```
    > show cluster node

    1) Node ID: 1
            IP:                  10.102.201.24
            Backplane:           1/1/1
            Health:              UP
            Admin State:         ACTIVE
            Operational State:   ACTIVE(Configuration Coordinator)
            Sync State:          ENABLED
            Priority:            31
            Tunnel Mode:         NONE
            Node Group:          DEFAULT_NG
    2) Node ID: 2
            IP:                  10.102.201.62*
            Backplane:           2/1/1
            Health:              UP
```



```
17              Admin State:          ACTIVE
18              Operational State:    ACTIVE
19              Sync State:           PARTIAL SUCCESS
20      (Refer the files clus_sync_batch_status.log, sync_route_status.log
           and sync_clusdiff_status.log in /var/nssynclog directory for
           list of commands failed)
21              Priority:             31
22              Tunnel Mode:          NONE
23              Node Group:           DEFAULT_NG
24      3) Node ID: 3
25              IP:                   10.102.201.64
26              Backplane:            3/1/1
27              Health:               UP
28              Admin State:          ACTIVE
29              Operational State:    ACTIVE
30              Sync State:           PARTIAL SUCCESS
31      (Refer the files clus_sync_batch_status.log, sync_route_status.log
           and sync_clusdiff_status.log in /var/nssynclog directory for
           list of commands failed)
32              Priority:             31
33              Tunnel Mode:          NONE
34              Node Group:           DEFAULT_NG
35      Done
36
37      > show cluster syncFailures
38
39      exec: add system user nsroot "********" -encrypted -externalAuth
           ENABLED -timeout 900 -logging ENABLED -maxsession 20 -
           allowedManagementInterface CLI API -devno 32768
40      ERROR: Resource already exists
41      --
42      exec: set interface 2/LO/1 -autoneg ENABLED -haMonitor OFF -
           haHeartbeat OFF -mtu 1500 -ringtype Elastic -tagall OFF -
           trunkmode OFF -state ENABLED -lagtype NODE -lacpPriority 32768 -
           lacpTimeout LONG -throughput 0 -linkRedundancy OFF -
           bandwidthHigh 0 -bandwidthNormal 0 -intftype Loopback -svmCmd 0
           -ifnum 2/LO/1 -lldpmode NONE -lrsetPriority 1024
43      ERROR: Operation not allowed on loopback interface.
```

Synchronisation du temps entre les nœuds de cluster

January 21, 2021

Le cluster utilise un protocole PTP (Precision Time Protocol) pour synchroniser l'heure entre les nœuds de cluster. PTP utilise des paquets de multidiffusion pour synchroniser l'heure. S'il y a des problèmes dans la synchronisation de l'heure, vous devez désactiver PTP et configurer NTP (Network Time Protocol) sur le cluster.

Pour activer/désactiver PTP à l'aide de l'interface de ligne de commande

À l'invite de commandes de l'adresse IP du cluster, tapez :

```
set ptp -state disable
```

Pour activer/désactiver PTP à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, sous **Utilitaires**, cliquez sur **Configurer les paramètres PTP.**
4. Dans la boîte de dialogue **Activer/Désactiver PTP**, indiquez si vous souhaitez activer ou désactiver PTP.
5. Cliquez sur **OK.**

Synchronisation des fichiers de cluster

October 5, 2021

Les fichiers disponibles sur le coordinateur de configuration sont appelés fichiers de cluster. Ces fichiers sont automatiquement synchronisés sur les autres nœuds de cluster lorsque le nœud est ajouté au cluster et périodiquement, pendant la durée de vie du cluster. Vous pouvez également synchroniser manuellement les fichiers de cluster.

Important : La suppression de tout certificat ou fichier clé dans un environnement de cluster limite la configuration de l'appliance ADC. Rajoutez les fichiers au même emplacement pour apporter des modifications de configuration.

Les répertoires et fichiers du coordinateur de configuration qui sont synchronisés sont les suivants :

- /nsconfig/ssl/
- /var/netscaler/ssl/
- /var/vpn/signet/
- /nsconfig/dns/
- /nsconfig/monitors/
- /nsconfig/nstemplates/

- /nsconfig/ssh/
- /nsconfig/rc.netscaler
- /nsconfig/resolv.conf
- /nsconfig/inetd.conf
- /nsconfig/syslog.conf
- /nsconfig/snmpd.conf
- /nsconfig/ntp.conf
- /nsconfig/httpd.conf
- /nsconfig/sshd_config
- /nsconfig/hosts
- /nsconfig/enckey
- /var/nslw.bin/etc/krb5.conf
- /var/nslw.bin/etc/krb5.keytab
- /var/lib/likewise/db/
- /var/download/
- /var/wi/tomcat/webapps/
- /var/wi/Tomcat/conf/Catalina/LocalHost/
- /var/wi/java_home/lib/security/cacerts
- /var/wi/java_home/jre/lib/security/cacerts
- /nsconfig/license/
- /nsconfig/rc.conf

> **Conseil**
>
> Les fichiers (certificats et fichiers clés) copiés manuellement sur le coordinateur de configuration du cluster (ou via le shell) ne sont pas automatiquement disponibles sur les autres nœuds de cluster. Exécutez la commande « synchroniser les fichiers de cluster » à partir de l'adresse IP du cluster avant d'exécuter une commande qui dépend de ces fichiers.

Pour synchroniser les fichiers de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes de l'adresse IP du cluster, tapez :

```
sync cluster files <mode>
```

Pour synchroniser des fichiers de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, sous **Utilitaires**, cliquez sur Synchroniser les fichiers de cluster.

4. Dans la boîte de dialogue **Synchroniser** les fichiers de cluster, sélectionnez les fichiers à synchroniser dans la liste déroulante Mode.
5. Cliquez sur **OK.**

Affichage des statistiques d'un cluster

January 21, 2021

Vous pouvez afficher les statistiques d'une instance de cluster et des nœuds de cluster pour évaluer les performances ou résoudre les problèmes de fonctionnement du cluster.

Pour afficher les statistiques d'une instance de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes de l'adresse IP du cluster, tapez :

```
stat cluster instance <clId>
```

Pour afficher les statistiques d'un nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes de l'adresse IP du cluster, tapez :

```
stat cluster node <nodeid>
```

> **Remarque**
>
> La `stat cluster node <nodeid>` commande affiche les statistiques de niveau cluster lorsque vous exécutez la commande à partir de l'adresse IP du cluster. Toutefois, lorsque vous exécutez à partir de l'adresse NSIP d'un nœud de cluster, la commande affiche des statistiques au niveau du nœud.

Pour afficher les statistiques d'une instance de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster.**
3. Dans le volet d'informations, au centre de la page, cliquez sur **Statistiques.**

Pour afficher les statistiques d'un nœud de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Nœuds.**
3. Dans le volet d'informations, sélectionnez un nœud et cliquez sur **Statistiques** pour afficher les statistiques du nœud. Pour afficher les statistiques de tous les nœuds, cliquez sur **Statistiques** sans sélectionner un nœud spécifique.

À la découverte des appliances NetScaler

May 5, 2023

Vous pouvez découvrir les appliances présentes dans le même sous-réseau que le nœud actuel. Les appliances découvertes requises peuvent ensuite être ajoutées de manière sélective au cluster. Cette opération peut être effectuée pour créer un cluster ou pour ajouter des nœuds à un cluster existant.

> **Remarque**
>
> - L'opération de découverte ne peut être effectuée que via l'utilitaire de configuration.
> - Cette opération ne permet pas de découvrir les appliances NetScaler provenant de différents réseaux.
> - Lorsque vous effectuez cette opération pour ajouter des nœuds à un cluster existant, les configurations VLAN L3 sont effacées du nœud. Assurez-vous de définir ces configurations une fois que l'appliance est ajoutée au cluster.

Pour découvrir les appliances à l'aide de l'interface graphique

1. Connectez-vous à l'adresse IP du cluster.
2. Accédez à **Système > Cluster > Nœuds.**
3. Dans le volet de détails, en bas de la page, cliquez sur **Découvrir NetScalers**.
4. Dans la boîte de dialogue **Discover NetScalers**, définissez les paramètres suivants :
   - **Plage d'adresses IP** : spécifiez la plage d'adresses IP dans laquelle vous souhaitez découvrir les appliances. Par exemple, vous pouvez rechercher toutes les adresses NSIP comprises entre 10.102.29.4 et 10.102.29.15 en spécifiant cette option sous la forme 10.102.29.4 - 15.
   - **Interface de fond** de panier : spécifiez les interfaces à utiliser comme interface de fond de panier. Il s'agit d'un paramètre facultatif. Si vous ne spécifiez pas ce paramètre, vous devez le mettre à jour une fois le nœud ajouté au cluster.
5. Cliquez sur **OK.**

6. Sélectionnez les appliances que vous souhaitez ajouter au cluster.
7. Cliquez sur **OK.**

Désactivation d'un nœud de cluster

August 20, 2021

Vous pouvez supprimer temporairement un nœud d'un cluster en désactivant l'instance de cluster sur ce nœud. Un nœud désactivé n'est pas synchronisé avec les configurations de cluster. Lorsque le nœud est à nouveau activé, les configurations de cluster sont automatiquement synchronisées dessus. Pour plus d'informations, voir Synchronisation entre les nœuds de cluster.

Un nœud désactivé ne peut pas servir le trafic et toutes les connexions existantes sur ce nœud sont terminées.

> **Remarque**
>
> Si les configurations d'un nœud coordinateur non configuré désactivé sont modifiées (via l'adresse NSIP du nœud), les configurations ne sont pas automatiquement synchronisées sur ce nœud. Vous pouvez synchroniser manuellement les configurations comme décrit dans Synchronisation des configurations de cluster.

Pour désactiver un nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes du nœud que vous souhaitez désactiver, tapez :

```
disable cluster instance <clId>
```

> **Remarque**
>
> Pour désactiver le cluster, exécutez la commande disable cluster instance sur l'adresse IP du cluster.

Pour désactiver un nœud de cluster à l'aide de l'utilitaire de configuration

1. Sur le nœud que vous souhaitez désactiver, accédez à **Système > Cluster**, puis cliquez sur **Gérer le cluster.**
2. Dans la boîte de dialogue **Configurer** l'instance de cluster, **désactivez** la case à cocher Activer l'instance de cluster.

> **Remarque**
>
> Pour désactiver l'instance de cluster sur tous les nœuds, exécutez la procédure précédente sur l'adresse IP du cluster.

Suppression d'un nœud de cluster

August 20, 2021

Lorsqu'un nœud est supprimé du cluster, les configurations de cluster sont effacées du nœud (en exécutant en interne la commande clear ns config -extended). Les adresses SNIP, les paramètres **MTU** de l'interface du fond de panier et toutes les configurations de VLAN (à l'exception du VLAN et du NSVLAN par défaut) sont également effacés de l'appliance.

> **Remarque**
>
> - Si le nœud supprimé était le coordinateur de configuration de cluster (CCO), un autre nœud est automatiquement sélectionné en tant que CCO et l'adresse IP du cluster est affectée à ce nœud. Toutes les sessions d'adresse IP de cluster actuelles ne sont pas valides et vous devez démarrer une nouvelle session.
> - Pour supprimer l'ensemble du cluster, vous devez supprimer chaque nœud individuellement. Lorsque vous supprimez le dernier nœud, les adresses IP du cluster sont supprimées.
> - Lorsqu'un nœud actif est supprimé, la capacité de service de trafic du cluster est réduite d'un nœud. Les connexions existantes sur ce nœud sont terminées.

Pour supprimer un nœud de cluster à l'aide de l'interface de ligne de commande

Pour NetScaler 10.1 et versions ultérieures

1. Connectez-vous à l'adresse IP du cluster et à l'invite de commandes, tapez :

```
rm cluster node <nodeId>

save ns config
```

2. Ouvrez une session sur le nœud supprimé, l'adresse NSIP et, à l'invite de commandes, tapez :

```
save ns config
```

> **Remarque**

> Si l'adresse IP du cluster est inaccessible depuis le nœud, exécutez la commande d'instance de cluster rm sur l'adresse NSIP de ce nœud lui-même.

Pour NetScaler 10

1. Ouvrez une session sur le nœud que vous souhaitez supprimer du cluster et supprimez la référence à l'instance de cluster.

```
rm cluster instance <clId>

save ns config
```

2. Ouvrez une session sur l'adresse IP du cluster et supprimez le nœud à partir duquel vous avez supprimé l'instance de cluster.

```
rm cluster node <nodeId>

save ns config
```

   Assurez-vous de ne pas exécuter la `rm cluster node` commande à partir du nœud local. Il en résulte des configurations incohérentes entre le CCO et le nœud.

Pour supprimer un nœud de cluster à l'aide de l'interface graphique

Sur l'adresse IP du cluster, accédez à **Système > Cluster > Nœuds**, sélectionnez le nœud à supprimer et cliquez sur **Supprimer.**

Suppression du nœud d'un cluster déployé à l'aide de l'agrégation de liens de cluster

August 20, 2021

Pour supprimer un nœud d'un cluster qui utilise l'agrégation de liens de cluster comme mécanisme de distribution du trafic, vous devez vous assurer que le nœud est rendu passif afin qu'il ne reçoive aucun trafic, puis, sur le commutateur en amont, supprimez l'interface correspondante du canal.

Pour plus d'informations sur l'agrégation de liens de cluster, voir Utilisation de l'agrégation de liens de cluster.

Pour supprimer un nœud d'un cluster qui utilise l'agrégation des liens de cluster comme mécanisme de distribution du trafic

1. Connectez-vous à l'adresse IP du cluster.
2. Définissez l'état du nœud de cluster que vous souhaitez supprimer sur PASSIVE.

```
set cluster node <nodeId> -state PASSIVE
```

3. Sur le commutateur en amont, supprimez l'interface correspondante du canal à l'aide de commandes spécifiques au commutateur.

> **Remarque**
>
> Vous n'avez pas besoin de supprimer manuellement l'interface des nœuds sur le canal d'agrégation des liens de cluster. Il est automatiquement supprimé lorsque le nœud est supprimé à l'étape suivante.

4. Supprimez le nœud du cluster.

```
rm cluster node <nodeId>
```

Détection d'une sonde jumbo sur un cluster

August 20, 2021

Si une trame Jumbo est activée sur une interface de cluster, l'interface du fond de panier doit être suffisamment grande pour prendre en charge tous les paquets dans le cadre Jumbo. Il est atteint en réglant l'unité de transmission maximale (MTU) du fond de panier comme suit :

Backplane_MTU = maximum (tous les MTU de l'interface de cluster) + 78

Pour vérifier la configuration précédente, vous devez envoyer une sonde jumbo (de la taille de calcul précédente) à tous les nœuds homologues d'une configuration de cluster. Si la sonde échoue, l'appliance affiche un message d'avertissement dans la sortie de la commande « show cluster instance ».

En mode interface de commande, tapez la commande suivante :

```
> show cluster instance
  Cluster ID: 1
  Dead Interval: 3 secs
  Hello Interval: 200 msecs
  Preemption: DISABLED
  Propagation: ENABLED
```



```
7         Quorum Type: MAJORITY
8         INC State: DISABLED
9         Process Local: DISABLED
10        Cluster Status: ENABLED(admin),    ENABLED(operational), UP
```

> **Avertissement**
>
> Le MTU d'une interface de backplane doit être suffisamment grand pour gérer tous les paquets du cadre. Il doit être égal à <MTU_VAL>. Si la valeur recommandée n'est pas configurable par l'utilisateur, vous devez vérifier la valeur MTU des interfaces jumbo.

Sl. non	Nœuds membres	Intégrité	État d'administration	État de l'opération
1	ID du nœud : 1 ; IP du nœud : 10.102.53.167	UP	Active	ACTIVE (Coordonnateur de configuration)
2	ID du nœud : 2 ; IP du nœud : 10.102.53.168	UP	Active	Actif

Surveillance des itinéraires pour les itinéraires dynamiques dans le cluster

January 21, 2021

Vous pouvez utiliser un moniteur d'itinéraires pour rendre un nœud de cluster dépendant de la table de routage interne, qu'il contienne ou non un itinéraire appris dynamiquement. Un moniteur de routage sur chaque nœud vérifie la table de routage interne pour s'assurer qu'une entrée d'itinéraire permettant d'atteindre un réseau particulier est toujours présente. Si l'entrée d'itinéraire n'est pas présente, l'état du moniteur d'itinéraire passe à DOWN.

Dans un déploiement de cluster, si la liaison latérale côté client ou serveur d'un nœud diminue, le trafic est dirigé vers ce nœud via les nœuds homologues pour traitement. La direction du trafic est implémentée en configurant le routage dynamique et en ajoutant des entrées ARP statiques, pointant vers l'adresse MAC spéciale de chaque nœud, sur tous les nœuds. S'il y a beaucoup de nœuds dans un déploiement de cluster, ajouter et gérer des entrées ARP statiques avec des adresses MAC spéciales sur tous les nœuds est une tâche lourde. Maintenant, les nœuds utilisent implicitement des adresses

MAC spéciales pour diriger les paquets. Par conséquent, les entrées ARP statiques pointant vers des adresses MAC spéciales ne doivent plus être ajoutées aux nœuds de cluster.

Pour lier un nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
unbind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
```

Considérons un scénario où le nœud 1 est lié au moniteur de routage 1.1.1.0 255.255.255.0. Lorsqu'un itinéraire dynamique échoue, le nœud 1 devient INACTIVE. L'état de santé est disponible dans la `show cluster node` commande par ID de nœud comme suit.

```
Node ID: 1
IP:  10.102.169.96
Backplane:  1/1/2
Health: NOT UP
Reason(s): Route Monitor(s) of the node have failed
Route Monitor -  Network: 1.1.1.0   Netmask: 255.255.255.0   State:
    DOWN
```

Surveillance de la configuration du cluster à l'aide de la MIB SNMP avec lien SNMP

May 5, 2023

Le MIB SNMP est une information spécifique à l'appareil qui est configurée sur l'agent SNMP pour identifier une appliance NetScaler. Il peut identifier des informations telles que le nom de l'appliance, l'administrateur et l'emplacement. Dans une configuration de cluster, vous pouvez désormais configurer la MIB SNMP dans n'importe quel nœud en incluant le paramètre « OwnerNode » dans la commande set SNMP MIB. Sans ce paramètre, la commande set SNMP MIB s'applique uniquement au nœud Cluster Coordinator (CCO).

Pour afficher la configuration MIB pour un nœud de cluster autre que le CCO, incluez le paramètre « OwnerNode » dans la commande show SNMP MIB.

Configuration du MIB SNMP sur CLIP

Pour configurer et afficher la configuration MIB sur CLIP à l'aide de l'interface de ligne de commande.

```
set snmp mib [-contact <string>] [-name <string>] [-location <string>]
      [-customID <string>] [-ownerNode <positive_integer>]
Done
show snmp mib [-ownerNode <positive_integer>]

 > set mib -contact John -name NS59 -location San Jose -customID 123 -
    ownerNode 3
Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
        NetScaler system MIB:
        sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun  7
           2016, 10:27:29
        sysUpTime:   124300
        sysObjectID: .1.3.6.1.4.1.5951.1.1
        sysContact:  John
        sysName:     NS59
        sysLocation: San Jose
        sysServices: 72
        Custom ID: 123
 Done

> unset mib -contact -name -location -customID -ownerNode 3
 Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
        NetScaler system MIB:
        sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun 7
           2016, 10:27:29
        sysUpTime:   146023
        sysObjectID: .1.3.6.1.4.1.5951.1.1
        sysContact:  WebMaster (default)
        sysName:     NetScaler
        sysLocation: POP (default)
        sysServices: 72
        Custom ID: Default
 Done
```


Messages d'interruption SNMP de cluster

Dans la configuration du cluster, les configurations des alarmes SNMP Trap doivent être effectuées à partir du CLIP. Les commandes sont propagées à chacun des nœuds.

Pour plus d'informations sur la configuration du SNMP, consultez la section Configuration de NetScaler pour générer desinterruptions SNMP.

Voici les interruptions spécifiques au cluster qui sont disponibles :

```
>sh snmp alarm | grep cluster
    CLUSTER-BACKPLANE-HB-MISSING N/A N/A 86400   ENABLED - ENABLED
    CLUSTER-CCO-CHANGE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-NODE-HEALTH N/A N/A 86400 ENABLED - ENABLED
    CLUSTER-NODE-QUORUM N/A N/A 86400 ENABLED - ENABLED
    CLUSTER-OVS-CHANGE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-PROP-FAILURE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-SYNC-FAILURE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-SYNC-PARTIAL-SUCCESS N/A N/A N/A ENABLED - ENABLED
    CLUSTER-VERSION-MISMATCH N/A N/A 86400 ENABLED - ENABLED
```

Surveillance des échecs de propagation des commandes dans un déploiement de cluster

May 5, 2023

Dans un déploiement de clusters, vous pouvez utiliser la nouvelle commande « show prop status » pour accélérer la surveillance et la résolution des problèmes. Les problèmes liés à l'échec de la propagation des commandes sur des nœuds autres que CCO. Cette commande affiche jusqu'à 20 des échecs de propagation de commandes les plus récents sur tous les nœuds autres que CCO. Vous pouvez utiliser la CLI ou l'interface graphique de l'appliance NetScaler pour effectuer cette opération. Vous pouvez y accéder via l'adresse CLIP ou via l'adresse NSIP de n'importe quel nœud du déploiement du cluster.

Arrêt progrestueux des nœuds

May 5, 2023

Dans une configuration de cluster, certaines des connexions existantes (1/Nth connexions, où N est la taille du cluster) au niveau du cluster ou au niveau d'un serveur virtuel spécifique sont perdues. Ce

comportement est observé si un nœud quitte le système ou le rejoint. Pour remédier à cette perte, vous devez gérer correctement les connexions existantes. Une gestion efficace s'effectue en configurant l'option « Conserver les connexions sur le cluster » dans l'adresse CLIP et en spécifiant un intervalle de temporisation dans le NSIP du nœud.

La gestion élégante des connexions est applicable dans deux scénarios :

1. Mise à niveau du cluster
2. Ajout d'un nouveau nœud

Gestion efficace des nœuds lors de la mise à niveau du cluster

Pour mettre à niveau un cluster, vous devez mettre à niveau un nœud à la fois. Avant de mettre à niveau un nœud, vous devez le mettre à l'état passif, puis le mettre à l'état actif après la mise à niveau. Pour éviter de mettre fin aux connexions existantes lors de la mise à niveau du nœud, arrêtez-le progressivement en respectant un intervalle de temporisation configuré. Sinon, 1/Nth (où N est la taille du cluster) des connexions du cluster sont interrompues.

> **Remarque**
>
> Si les sessions existantes ne sont pas terminées dans le délai d'expiration configuré, elles sont interrompues après le délai de grâce.

Voici les étapes à suivre pour gérer correctement les nœuds dans un scénario de mise à niveau d'un cluster :

1. Envisagez une configuration de cluster de cinq nœuds (n0, n1, n2, n3, n4).
2. Avant d'arrêter un nœud, vous devez configurer l'option « RetainConnectionsOnCluster ». Cela permet de conserver toutes les connexions existantes de ce nœud au niveau du cluster ou du serveur virtuel pendant un intervalle de temps spécifique.

   Exemple

   Sur CLIP

   "'set cluster instance –retainConnectionsOnCluster YES

   ```
   OU

   ```set lb vserver <vserver name>  - retainConnectionsOnCluster Yes
      <!--NeedCopy-->
   ```

3. Maintenant, connectez-vous à l'adresse NSIP du nœud n3 et définissez le nœud n3 sur PASSIVE avec un délai d'expiration interne.

   Exemple


   ```

“‘set cluster node n3 –state PASSIVE –delay 60

```
```saveconfig<!--NeedCopy-->
```

4. Une fois le délai de grâce expiré, fermez toutes les connexions, arrêtez n3 et redémarrez l’appliance NetScaler.
5. Mettez à niveau l’appliance. Ensuite, une fois la CLI connectée à l’adresse NSIP de l’appliance, définissez le nœud sur ACTIVE.

   Exemple

   “‘set cluster node n3 –state ACTIVE

```
```saveconfig<!--NeedCopy-->
```

6. Répétez les étapes 4 à 6 pour tous les nœuds du cluster.
7. Une fois que tous les nœuds sont mis à niveau et définis sur ACTIVE, réinitialisez l’option Retain-ConnectionsOnCluster à partir de l’adresse CLIP.

   Exemple

   “‘set cluster instance -retainConnectionsOnCluster NO

```
OU

```set lb vserver <vserver name>  - retainConnectionsOnCluster NO
   <!--NeedCopy-->
```

> **Remarque**
>
> En cas de non-concordance de version lors de la mise à niveau d’un cluster, la propagation du cluster est automatiquement désactivée et aucune commande n’est autorisée sur le CLIP.

Gestion élégante des nœuds lors de l’ajout d’un nouveau nœud

La gestion élégante des nœuds décrit comment un nouveau nœud peut être ajouté au cluster NetScaler existant. Supposons que vous disposez d’un cluster NetScaler qui gère déjà du trafic. Et vous souhaitez ajouter une appliance supplémentaire en tant que nœud au cluster sans mettre fin à ses connexions existantes. Pour réaliser le scénario précédent, définissez l’option permettant de conserver les connexions existantes soit au niveau global, soit au niveau d’un serveur virtuel spécifique. Une fois que c’est fait, enregistrez la configuration. Définissez maintenant l’option permettant de conserver les connexions sur NO, afin de permettre la réaffectation des connexions existantes d’autres nœuds au nouveau nœud.


```

Voici les étapes à suivre pour gérer correctement les nœuds si un nœud vient d'être ajouté :

1. Vous enregistrez la configuration existante dans laquelle l'option « RetainConnectionsOnCluster » est activée. Ce faisant, vous pouvez conserver toutes les connexions existantes de ce nœud au niveau du cluster ou du serveur virtuel pendant un intervalle de temps spécifique.

   Sur CLIP

   ```
   set cluster instance x - retainConnectionsOnCluster YES
   ```

   OU

   ```
   set lb vserver xxxx -retainConnectionsOnCluster Yes
   ```

2. Ajoutez un nœud 'n5' à la configuration du cluster.
3. Désactivez l'option « RetainConnectionOnCluster » sur « NON » pour distribuer les connexions existantes depuis d'autres nœuds vers le nœud n5 nouvellement ajouté.

   Sur CLIP

   ```
   set cluster instance x - retainConnectionsOnCluster NO
   ```

   OU

   ```
   set lb vserver xxxx -retainConnectionsOnCluster NO
   ```

> **Remarque**
>
> Le pilotage du backplane dépend du type de mécanisme de distribution du trafic (ECMP, CLAG et USIP) utilisé dans une configuration de cluster. L'augmentation du braquage du panneau arrière dépend du type de trafic.

Configuration de l'arrêt progressif des nœuds d'un cluster

Pour configurer l'arrêt progressif des nœuds d'un cluster, procédez comme suit :

1. Configurez l'option « RetainConnectionsOnCluster » au niveau global (cluster).
2. Configurez l'option « RetainConnectionsOnCluster » au niveau du serveur virtuel.
3. Réglez le nœud (quittant le système) sur l'état passif avec un intervalle de temporisation progressif spécifié dans l'adresse NSIP du nœud.
4. Surveillez les connexions existantes pour vous assurer que toutes les transactions sont terminées dans le délai de grâce.

Pour conserver les connexions existantes au niveau global (cluster) à l'aide de l'interface de ligne de commande

Vous pouvez conserver les connexions existantes au niveau global ou au niveau d'un serveur virtuel spécifique. Cette option est configurée pour conserver toutes les connexions existantes au niveau global. Par défaut, cette option est désactivée.

À l'invite de commandes, tapez :

```
1 - set cluster instance <clusterID> - retainConnectionsOnCluster YES
2
3 - set cluster instance 60 - retainConnectionsOnCluster YES
```

Pour conserver les connexions existantes d'un serveur virtuel spécifique dans le cluster à l'aide de l'interface de ligne de commande

Cette option est configurée pour conserver les connexions existantes spécifiques à un serveur virtuel d'équilibrage de charge. Pour conserver ces connexions, nous activons cette option au niveau du serveur virtuel. Par défaut, cette option est désactivée.

À l'invite de commande, tapez :

```
1 - set lb vserver <clusterID> - retainConnectionsOnCluster Yes
2
3 - set lb vserver v1 - retainConnectionsOnCluster Yes
```

Pour définir un nœud de cluster à l'état passif à l'aide de l'interface de ligne de commande

Pour mettre un nœud de cluster à l'état passif avec un intervalle de temporisation raisonnable. Ce paramètre est défini dans le NSIP du nœud car la propagation est désactivée lors de la mise à niveau du cluster.

À l'invite de commande, tapez :

```
1  - set cluster node <clusterID> -state passive
2 -backplane <interface_name>@
3 -priority <positive_integer>
4 -delay <mins>
5
6  - set cluster node 4 - state PASSIVE -delay 60
7
8  - set cluster instance 60 - retainConnectionsOnCluster YES
9  - set lb vserver v1 - retainConnectionsOnCluster Yes
10 - set cluster node 4 - state PASSIVE -delay 60
```


> **Remarque**
>
> Vous pouvez observer le comportement suivant sur un nœud de cluster lorsqu'il est défini sur passif avec une option de délai configurée à partir d'un CLIP :
>
> - Une fois le délai écoulé, le nœud apparaît comme passif à partir du NSIP du nœud.
> - La commande **show cluster instance** sur CLIP affiche le nœud comme étant actif à partir du CLIP. Alors que la commande **show cluster node** du CLIP affiche le nœud comme passif.

Pour configurer l'arrêt progressif des nœuds à l'aide de l'interface graphique

1. Accédez à **Configuration > Système > Cluster** et cliquez sur **Gérer le cluster.**
2. Sur la page **Gérer le cluster**, sélectionnez l'option **Conserver les connexions sur le cluster** .
3. Cliquez sur **OK**, puis sur **OK**.

Arrêt gracieux des services

May 5, 2023

À partir de NetScaler 12.1 build 49.xx, les clusters NetScaler prennent en charge l'arrêt progressif des services. Pour arrêter correctement les services, vous pouvez effectuer l'une des tâches suivantes.

- Désactivez explicitement le service, et
  - Définissez un délai (en secondes).
  - Activez l'arrêt progressif.
- Ajoutez un code ou une chaîne TROFS au moniteur.

Pour plus de détails, voir Arrêt gracieux des services.

Pour configurer l'arrêt progressif d'un service à l'aide de l'interface de ligne de commande

Désactiver avec l'option gracieuse uniquement :

À l'invite de commande, tapez :

```
disable service <name> [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Exemple


```
disable service svc1 -graceFul YES
Done
sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE   Graceful (number of
                   active clients: 1)
                Last state change was at Wed Jul 25 10:46:29 2018
                Time since last state change: 0 days, 00:00:02.680
                ... ... ... .
                ... ... ... .
                Traffic Domain: 0

1)            Monitor Name: tcp-default
                                State: UP              Weight: 1
                                                Passive: 0
                                Probes: 26           Failed [Total: 0
                                   Current: 0]
                                Last response: Success - TCP syn+ack
                                   received.
                                Response Time: 0.0 millisec
<!--NeedCopy-->
```

Désactiver avec timeout et option gracieuse :

À l'invite de commande, tapez :

```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Exemple

```
disable service svc1 2000 -graceFul YES

Done
> sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE (Graceful (number of active
                    clients: 1), Out Of Service in 1998 seconds)
                Last state change was at Wed Jul 25 10:49:08 2018
                Time since last state change: 0 days, 00:00:01.710
                ... ... ... .
                ... ... ... .
                Traffic Domain: 0
```



```
12
13 1)            Monitor Name: tcp-default
14                                 State: UP              Weight: 1
                                                      Passive: 0
15                                 Probes: 57           Failed [Total: 0
                                      Current: 0]
16                                 Last response: Success - TCP syn+ack
                                      received.
17                                 Response Time: 0.0 millisec
18 Done
19 <!--NeedCopy-->
```

Désactivez le groupe de services avec délai d'expiration et option gracieuse :

À l'invite de commande, tapez :

```
1 disable serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-delay
2 <secs>] [-graceFul ( YES | NO )]
3 Show service group <serviceGroupName>
4 <!--NeedCopy-->
```

Exemple :

```
1 disable servicegroup sg -delay 2000 -graceFul yes
2 sh servicegroup sg
3                  sg - HTTP
4                  State: DISABLED                Effective State: OUT OF
                      SERVICE Monitor Threshold : 0
5                  Max Conn: 0       Max Req: 0          Max Bandwidth: 0
                      kbits
6                  Use Source IP: NO
7                  Client Keepalive(CKA): NO
8                   … … … .
9                   … … …
10
11
12                 1)   200.200.10.21:80       Server Name: server3
                      Server ID: None Weight: 1
13                                 State:    GOING OUT OF SERVICE (learnt
                                      from node:2 )     Graceful (number
                                      of active clients: 6), Out Of
                                      Service in 1993 seconds
14                                 Last state change was at Mon Aug 13
                                      15:15:11 2018
15                                  … … …
16
```



```
17                  2)   200.200.10.22:80       Server Name: server4
                       Server ID: None Weight: 1
18                                  State:    GOING OUT OF SERVICE (learnt
                                       from node:2 )     Graceful (number
                                       of active clients: 7), Out Of
                                       Service in 1993 seconds
19                                  Last state change was at Mon Aug 13
                                       15:15:11 2018
20 <!--NeedCopy-->
```

> **Remarque :**
> CLIP affiche la valeur agrégée de toutes les connexions clients actives provenant de tous les nœuds du cluster.

Pour configurer l'arrêt progressif d'un service à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Ouvrez le service et, dans la liste des actions, cliquez sur **Désactiver**. Entrez un temps d'attente, puis sélectionnez Graceful.

Pour configurer un code ou une chaîne TROFS dans un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
1 add lb monitor <monitor-name> HTTP -trofsCode <respcode>
2 add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>
3 add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
4 <!--NeedCopy-->
```

Pour configurer un code ou une chaîne TROFS dans un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Dans le volet Moniteurs, cliquez sur Ajouter, puis effectuez l'une des étapes suivantes :
   - Sélectionnez Tapez HTTP et spécifiez un code TROFS.
   - Sélectionnez Type en tant que HTTP-ECV ou TCP-ECV, puis spécifiez une chaîne TROFS.

Prise en charge du logo IPv6 Ready pour les clusters

August 20, 2021

Vous pouvez tester les appliances en cluster pour la certification IPv6 Ready Logo. Les commandes modifiées pour tester les protocoles de base IPv6, comme pour les cas de test ND, le traitement de la sollicitation de routeur et l'envoi de messages de publicité d'itinéraire et de redirection de routeur, sont disponibles dans une configuration en cluster. Voici les fonctionnalités IPv6 disponibles pour tester les protocoles de base IPv6.

Voici les fonctionnalités modifiées disponibles pour passer les protocoles de base IPv6, tels que les cas de test ND, le traitement de la sollicitation de routeur et l'envoi de la publicité d'itinéraire et la messagerie de redirection de routeur dans la suite de tests IPv6ReadyLogo phase2.

- Lier des SNIP locaux
- Résolution des adresses et inaccessibilité des voisins
- Découverte du routeur et du préfixe
- Redirection du routeur
- DoDAD

Avec ces commandes modifiées, les configurations suivantes sont prises en charge dans une appliance en cluster.

Configurations supportables pour tester les protocoles de base IPv6

Pour qu'une configuration en cluster réussissent les cas de test du logo IPv6 Ready, vous pouvez exécuter les configurations suivantes sur l'adresse IP de gestion de cluster (CLIP).

- configuration IP6 globale
- configuration IPv6 de base
- plus de configurations IPv6

Configuration globale

Une configuration IPv6 globale vous permet de définir les paramètres IPv6 globaux (tels que relearning, routereDirection, ndBaseReachTime, nRetransmissionTime, `natprefix`, td et doodad) pour exécuter la configuration IPv6 de base.

À l'invite de commandes, tapez ce qui suit :

```
set ipv6 [-ralearning ( ENABLED | DISABLED )] [-routerRedirection (
    ENABLED | DISABLED )] [-ndBasereachTime<positive_integer>][-
    ndRetransmissionTime <positive_integer>] [-natprefix <ipv6_addr|*>[-
    td<positive_integer>]] [-doDAD ( ENABLED | DISABLED )]
```


Configuration IPv6 de base

La configuration IPv6 de base vous permet de créer une adresse IPv6 et de se lier à une interface VLAN. Vous pouvez effectuer les configurations suivantes pour tester les protocoles de base IPv6.

Pour ajouter un VLAN à la configuration en cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add vlan <id>
```

Pour ajouter un autre VLAN à la configuration en cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add vlan <id>
```

Pour lier une interface à un VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind vlan <id> -ifnum <interface_name>
```

Pour lier une interface à un VLAN à l'aide de l'interface de ligne de commande

Cette commande ajoute le préfixe global en tant que préfixe sur lien dans les informations RA pour les publicités de routeur suivantes. À l'invite de commandes, tapez :

```
bind vlan <id> -ifnum <interface_name>
```

Pour ajouter l'adresse SNIP IPv6 sur un VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```

Pour ajouter l'adresse IPv6 sur VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```

Pour lier une adresse IPv6 au VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
    ipv6_addr|
```


Pour lier l'adresse IPv6 au VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
    ipv6_addr|
```

Pour afficher l'adresse IPv6 locale de liaison attachée au VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
sh VLAN
```

Exemple 1

```
add vlan 2
add vlan 3
bind vlan 2 -ifnum 1/2
bind vlan 3 -ifnum 1/3
add ip6 fe80::9404:60ff:fedd:a464/64 -vlan 2 -scope link-local -type
    SNIP
add ip6 fe80::c0ee:7bff:fede:263f/64 -vlan 3 -scope link-local -type
    SNIP
add ip6 3ffe:501:ffff:100:9404:60ff:fedd:a464/64 -vlan 2
add ip6 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64 -vlan 3
bind vlan 2 -ipAddress 3ffe:501:ffff:100:9404:60ff:fedd:a464/64
bind vlan 3 -ipAddress 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64
```

Exemple 2

```
sh vlan
1)      VLAN ID: 2      VLAN Alias Name:
        Interfaces : 1/6
        IPs :
             3ffe:501:ffff:100:2e0:edff:fe15:ea2a/64
3)      VLAN ID: 3      VLAN Alias Name:
        Link-local IPv6 addr: fe80::9404:60ff:fedd:a464/64
        Interfaces : 1/5
        IPs :
             3ffe:501:ffff:101:2e0:edff:fe15:ea2b/64
 Done
```


Plus de configuration de cluster IPv6

Pour tester les protocoles de base IPv6, vous pouvez utiliser les configurations IPv6 nouvelles ou modifiées suivantes.

Pour définir les paramètres d'annonce de routeur spécifiques au VLAN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set nd6RAvariables -vlan <positive_integer> [-ceaseRouterAdv ( YES | NO )] [-sendRouterAdv ( YES | NO )] [-srcLinkLayerAddrOption ( YES | NO )][-onlyUnicastRtAdvResponse ( YES | NO )] [-managedAddrConfig ( YES | NO)] [-otherAddrConfig ( YES | NO )] [-currHopLimit <positive_integer>][-maxRtAdvInterval <positive_integer>] [-minRtAdvInterval<positive_integer>] [-linkMTU <positive_integer>] [-reachableTime<positive_integer>] [-retransTime <positive_integer>] [-defaultLifeTime<integer>]
```

Pour définir les paramètres configurables d'un préfixe global sur lien à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-decrementPrefixLifeTimes ( YES | NO )] [-prefixValideLifeTime <positive_integer>] [-prefixPreferredLifeTime <positive_integer>]
```

Pour ajouter des paramètres configurables à un préfixe global sur lien à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-decrementPrefixLifeTimes ( YES | NO )]-prefixValideLifeTime <positive_integer>][-prefixPreferredLifeTime <positive_integer>]
```

Pour définir une liaison sur lien vers les paramètres configurables du préfixe IPv6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
help set onLinkIPv6Prefix
```

Pour lier un lien on-link aux paramètres configurables du préfixe IPv6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
help bind nd6RAvariables
```

Pour afficher ND6RAVariables à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
help sh nd6RAvariables
```

Exemple

```
> sh nd6RAvariables
  1) Vlan : 1
     SendAdvert      : NO   CeaseAdv       : NO        SourceLLAddress: YES
     UnicastOnly     : NO   ManagedFlag    : NO        OtherConfigFlag: NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600       MinRtrAdvInterv: 198
     LinkMTU         : 0    ReachableTime  : 0          RetransTimer   : 0
     DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay    : 0

  2) Vlan : 2
     SendAdvert      : NO   CeaseAdv       : NO        SourceLLAddress: YES
     UnicastOnly     : NO   ManagedFlag    : NO        OtherConfigFlag: NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600       MinRtrAdvInterv: 198
     LinkMTU         : 0    ReachableTime  : 0          RetransTimer   : 0
     DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay    : 0
Done
>
> sh nd6Ravariables  -vlan 2
  1) Vlan : 2
     SendAdvert      : NO   CeaseAdv       : NO        SourceLLAddress: YES
     UnicastOnly     : NO   ManagedFlag    : NO        OtherConfigFlag: NO
```



```
21      CurHopLimit     : 64    MaxRtrAdvInterv: 600        MinRtrAdvInterv:
            198
22      LinkMTU         : 0     ReachableTime  : 0          RetransTimer    :
            0
23      DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay     :
            0
24      Prefix :
25  3ffe:501:ffff:100::/64
26  Done
```

Gestion des messages de pulsation du cluster

May 5, 2023

La gestion des messages de pulsation dans un cluster est similaire à leur gestion dans une configuration haute disponibilité (HA). Les nœuds peuvent envoyer et recevoir des messages de pulsation entre eux sur toutes les interfaces activées. Pour éviter l'augmentation du trafic résultant des messages de pulsation, vous pouvez désormais désactiver l'option de pulsation sur les interfaces des nœuds. Toutefois, l'option pulsation sur l'interface de backplane ne peut pas être désactivée, car elle est nécessaire pour maintenir la connectivité entre les nœuds de cluster.

Pour plus d'informations sur la gestion des messages cardiaques, voir Gestion des messages Heartbeat haute disponibilité sur un dispositif NetScaler Appliance.

Pour gérer les messages de pulsation sur une interface de nœud à l'aide de la CLI NetScaler

À l'invite de commande, tapez :

```
1  set interface <ID> [-HAHeartBeat (ON | OFF)]
2  Show interface <ID>
```

Configuration de l'état de la réponse du nœud propriétaire

May 5, 2023

Vous pouvez configurer l'option OwnerDownResponse sur un nœud dont l'adresse SNIP a été repérée. Par défaut, cette option est activée. Il permet à l'adresse IP repérée de répondre aux requêtes PING ou

ARP (provenant du routeur en amont) lorsque le nœud est inactif. Si vous désactivez l'option, l'adresse IP ne peut pas répondre aux demandes du routeur lorsque le nœud propriétaire est inactif.

Pour savoir comment cette fonctionnalité est utilisée pour surveiller les routes statiques dans le déploiement ECMP, reportez-vous à la rubrique Using Equal Cost Multiple Path (ECMP) .

Pour définir l'état de réponse du nœud propriétaire à l'aide de l'interface de ligne de commande NetScaler

À l'invite de commande, tapez :

```
add ns ip <IPAddress> [-ownerNode <positive_integer>] [-
    ownerDownResponse (YES | NO )] [-td <positive_integer>]
```

Exemple

```
add ns ip 2.2.2.2 255.255.255.0 -ownernode 6  - ownerdownResponse YES
```

Pour définir l'état de réponse du nœud propriétaire à l'aide de l'interface graphique NetScaler

1. Accédez à **Système > Réseau > IP** et cliquez sur **Ajouter** pour créer une adresse SNIP repérée.
2. Sur la page **Créer une adresse IP**, cochez ou décochez la case **OwnerDownResponse** .

Pour modifier l'état de réponse du nœud propriétaire à l'aide de l'interface graphique NetScaler

Accédez à **Système > Réseau > IP**, sélectionnez une adresse IP et cliquez sur **Modifier** pour activer ou désactiver la case à cocher **OwnerDownResponse** .

Surveillance de la prise en charge de la route statique (MSR) pour les nœuds inactifs dans une configuration de cluster spotted

January 21, 2021

Dans un cluster configuré avec l'option MSR activée sur la route, seuls les nœuds actifs peuvent sonder un itinéraire statique. Il peut atteindre un réseau alors que les nœuds inactifs et de secours n'ont aucun lien avec l'itinéraire et ne peuvent pas y sonder. Vous pouvez maintenant configurer un nœud

inactif ou de rechange pour envoyer une sonde PING et ARP à la route IPv4 et envoyer une sonde ping6 et nd6 à la route IPv6. Vous ne pouvez effectuer cette opération que dans une configuration de cluster repéré dans laquelle l'adresse SNIP est active et détenue exclusivement par un seul nœud.

Liaison d'interface VRRP dans un cluster actif à nœud unique

May 5, 2023

Lorsque vous migrez une configuration haute disponibilité (HA) vers une configuration de cluster, toutes les configurations doivent être compatibles et prises en charge dans le cluster. Pour ce faire, vous pouvez désormais configurer des ID de routeur virtuel (vRID et vRID6) sur une interface de nœud.

> **Important**
>
> Actuellement, seul un système de cluster actif à nœud unique prend en charge les VRID et les VRID6.

Pour obtenir des instructions sur la configuration des VRID et des VRID6, reportez-vous à la section Configuration des adresses MAC virtuelles.

Pour configurer un ID de routeur virtuel sur un cluster actif à nœud unique, ajoutez le VRID ou le VRID6 et liez-le à l'interface de nœud de cluster.

Pour ajouter un VRID à l'aide de l'interface de ligne de commande NetScaler

À l'invite de commande, tapez :

```
add vrID <ID>
```

Pour lier un VRID à l'interface cluster-node à l'aide de la CLI NetScaler

À l'invite de commande, tapez :

```
Bind vrid <ID> -ifnum <interface_name> | -trackifNum <interface_name

Add vrID 100
Bind vrid 100  - ifnum 1/1  1/2
done
```

Pour ajouter un VRID6 à l'aide de l'interface de ligne de commande NetScaler

À l'invite de commande, tapez :

```
add vrID6 <ID>
```

Pour lier un VRID6 à une interface de nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind vrid6 <ID> -ifnum <interface_name> | -trackifNum <interface_name>

Add vrID6 100
Bind vrid6 100  - ifnum 1/1  1/2
Done
```

Scénarios de configuration et d'utilisation du cluster

May 5, 2023

Cette section explique certains scénarios dans lesquels le cluster NetScaler peut être configuré et configuré pour différentes fonctionnalités et topologies de réseau. Faites-nous part de vos commentaires si vous souhaitez que d'autres scénarios soient documentés.

Création d'un cluster à deux nœuds

January 21, 2021

Un cluster à deux nœuds est une exception à la règle selon laquelle un cluster n'est fonctionnel que lorsqu'un minimum de nœuds (n/2 + 1), où n est le nombre de nœuds de cluster, sont capables de servir le trafic. Si la même formule est appliquée à un cluster à deux nœuds, le cluster échouerait si un nœud tombe en panne (n/2 +1=2).

Un cluster à deux nœuds est fonctionnel même si un seul nœud est capable de servir le trafic.

La création d'un cluster à deux nœuds est la même chose que la création d'un autre cluster. Vous ajoutez un nœud en tant que coordinateur de configuration et l'autre nœud comme autre nœud de cluster.

> **Remarque**
>
> La synchronisation incrémentielle de configuration n'est pas prise en charge dans un cluster à deux nœuds. Seule la synchronisation complète est prise en charge.

Migration d'une configuration HA vers une configuration de cluster

May 5, 2023

Pour migrer une configuration de haute disponibilité (HA) existante vers une configuration de cluster, vous devez d'abord supprimer les appliances NetScaler de la configuration HA et créer une sauvegarde du fichier de configuration HA. Vous pouvez ensuite utiliser les deux appliances pour créer un cluster et télécharger le fichier de configuration sauvegardé sur le cluster.

> **Remarque**
>
> - Avant de télécharger le fichier de configuration HA sauvegardé sur le cluster, vous devez le modifier pour le rendre compatible avec le cluster. Reportez-vous à l'étape correspondante de la procédure.
> - Utilisez la <backup_filename>commande **batch -f** pour charger le fichier de configuration sauvegardé.

L'approche précédente est une solution de migration de base qui entraîne des temps d'arrêt pour l'application déployée. En tant que tel, il doit être utilisé uniquement dans les déploiements où la disponibilité des applications n'est pas prise en compte.

Toutefois, dans la plupart des déploiements, la disponibilité de l'application est d'une importance capitale. Dans de tels cas, vous devez utiliser l'approche selon laquelle une configuration HA peut être migrée vers une configuration de cluster sans interruption de service. Dans cette approche, une configuration HA existante est migrée vers une configuration de cluster en supprimant d'abord l'appliance secondaire et en utilisant cette appliance pour créer un cluster à nœud unique. Une fois que le cluster est opérationnel et gère le trafic, l'appliance principale de la configuration HA est ajoutée au cluster.

Pour convertir une configuration HA en configuration de cluster (sans interruption de service) à l'aide de l'interface de ligne de commande

Prenons l'exemple d'une configuration HA avec l'appliance principale (NS1) - 10.102.97.131 et l'appliance secondaire (NS2) - 10.102.97.132.

1. Assurez-vous que les configurations de la paire HA sont stables.
2. Connectez-vous à l'un des dispositifs HA, accédez au shell et créez une copie du fichier ns.conf (par exemple, ns_backup.conf).
3. Ouvrez une session sur l'appliance secondaire, NS2, et effacez les configurations. Cette opération supprime NS2 de la configuration HA et en fait une appliance autonome.

```
1 > clear ns config full
```

> **Remarque**
>
> - Cette étape est requise pour s'assurer que NS2 ne commence pas à posséder des adresses VIP, maintenant qu'il s'agit d'une appliance autonome.
> - À ce stade, l'appliance principale, NS1, est toujours active et continue de servir le

> trafic.

4. Créez un cluster sur NS2 (désormais un dispositif secondaire) et configurez-le en tant que nœud PASSIF.

```
> add cluster instance 1

> add cluster node 0 10.102.97.132 -state PASSIVE -backplane
   0/1/1

> add ns ip 10.102.97.133 255.255.255.255 -type CLIP

> enable cluster instance 1

> save ns config

> reboot -warm
```

5. Modifiez le fichier de configuration sauvegardé comme suit :

   - Supprimez les entités qui ne sont pas prises en charge sur un cluster. Pour la liste des fonctionnalités non prises en charge, consultez la section Fonctionnalités de NetScaler prises en charge par uncluster. Il s'agit d'une étape facultative. Si vous n'effectuez pas cette étape, l'exécution des commandes non prises en charge échoue.
   - Supprimez les configurations qui ont des interfaces ou mettez à jour les noms d'interface de la convention c/u vers la convention n/c/u .

     Exemple

     ```
     > add vlan 10 -ifnum 0/1
     ```

     doit être changé en

     ```
     > add vlan 10 -ifnum 0/0/1 1/0/1
     ```

   - Le fichier de configuration de sauvegarde peut avoir des adresses SNIP. Ces adresses sont réparties par bandes sur tous les nœuds du cluster. Il est recommandé d'ajouter des adresses IP repérées pour chaque nœud.

     Exemple

     ```
     > add ns ip 1.1.1.1 255.255.255.0 -ownerNode 0

     > add ns ip 1.1.1.2 255.255.255.0 -ownerNode 1
     ```


- Mettez à jour le nom d'hôte pour spécifier le nœud propriétaire.

  Exemple

  ```
  > set ns hostname ns0 -ownerNode 0

  > set ns hostname ns1 -ownerNode 1
  ```

- Modifiez toutes les autres configurations réseau pertinentes qui dépendent des adresses IP repéré. Par exemple, le VLAN L3, la configuration RNAT (qui utilise les SNIP comme NATIP), les règles INAT (qui font référence aux SNIPS/MIP).

6. Sur le cluster, procédez comme suit :

   - Apportez les modifications topologiques au cluster en connectant le panneau arrière du cluster, le canal d'agrégation des liens du cluster, etc.
   - Appliquez les configurations du fichier de configuration sauvegardé et modifié au coordinateur de configuration via l'adresse IP du cluster.

     ```
     > batch -f ns_backup.conf
     ```

   - Configurez des mécanismes de distribution du trafic externe tels que ECMP ou l'agrégation de liens de cluster.

7. Transférez le trafic de la configuration HA vers le cluster.

   - Ouvrez une session sur l'appliance principale, NS1, et désactivez toutes les interfaces qui s'y trouve.

     ```
     > disable interface <interface_id>
     ```

   - Ouvrez une session sur l'adresse IP du cluster et configurez NS2 en tant que nœud ACTIVE.

     ```
     > set cluster node 0 -state ACTIVE
     ```

   > **Remarque**
   >
   > Il peut y avoir un léger temps d'arrêt (de l'ordre de quelques secondes) entre la désactivation des interfaces et l'activation du nœud du cluster.

8. Ouvrez une session sur l'appliance principale, NS1, et supprimez-la de la configuration HA.

   - Effacez toutes les configurations. Cette opération supprime NS1 de la configuration HA et en fait une appliance autonome.

     ```
     > clear ns config full
     ```


- Activez toutes les interfaces.

```
> enable interface <interface_id>
```

9. Ajoutez NS1 au cluster.
   - Ouvrez une session sur l'adresse IP du cluster et ajoutez NS1 au cluster.

```
> add cluster node 1 10.102.97.131 -state PASSIVE -backplane
   1/1/1
```

   - Connectez-vous à NS1 et joignez-le au cluster en exécutant séquentiellement les commandes suivantes :

```
> join cluster -clip 10.102.97.133 -password nsroot

> save ns config

> reboot -warm
```

10. Ouvrez une session sur NS1 et effectuez les modifications de topologie et de configuration requises.
11. Connectez-vous à l'adresse IP du cluster et définissez NS1 comme nœud ACTIVE.

```
> set cluster node 1 -state ACTIVE
```

Transition entre un cluster L2 et L3

May 5, 2023

> **Remarque**
>
> Pris en charge à partir de NetScaler 11.

Un cluster L2 est un cluster dont tous les nœuds proviennent du même réseau et un cluster L3 est un cluster qui peut inclure des nœuds de différents réseaux. Vous pouvez facilement passer d'un type de cluster à l'autre sans interruption de service pour les applications déployées sur NetScaler.

Transition d'un cluster de L2 à L3

Vous pouvez passer à un cluster L3 lorsque vous souhaitez que le cluster inclue des nœuds provenant d'autres réseaux.

Sur l'adresse IP du cluster, procédez comme suit :

1. Créez un groupe de nœuds.

   Exemple

   ```
   1 > add cluster nodegroup NG0
   ```

   Ce groupe de nœuds est utilisé à l'étape suivante pour regrouper tous les nœuds du cluster L2 existant.

2. Faites passer le cluster L2 à un cluster L3.

   Exemple

   ```
   1 > set cluster instance 1 -inc ENABLED -nodegroup NG0
   ```

   Cette commande atteint le double objectif de la transition vers le cluster L3 et également d'ajouter tous les nœuds du cluster L2 au groupe de nœuds.

3. Vous pouvez désormais ajouter d'autres nœuds au cluster, comme expliqué dans Ajout d'un nœud au cluster.

Transition d'un cluster de L3 à L2

Vous pouvez passer à un cluster L2 lorsque vous souhaitez conserver les nœuds qui appartiennent à un seul réseau.

Sur l'adresse IP du cluster, procédez comme suit :

1. Supprimez les nœuds de cluster des réseaux que vous ne souhaitez pas conserver.

   Exemple

   ```
   1 > rm cluster node <nodeId>
   ```

2. Transition du cluster L3 vers un cluster L2.

   Exemple

   ```
   1 > set cluster instance 1 -inc DISABLED
   ```

   Le cluster inclut désormais les nœuds d'un seul réseau.

Configuration de GSLB dans un cluster

August 20, 2021

> **Remarque**
>
> Prise en charge à partir de NetScaler 10.5 Build 52.11.

Pour configurer GSLB dans un cluster, vous devez lier les différentes entités GSLB à un groupe de nœuds. Le groupe de nœuds doit avoir un seul nœud membre.

> **Remarques**
>
> - Si vous avez configuré la méthode GSLB de proximité statique, assurez-vous que la base de données de proximité statique est présente sur tous les nœuds de cluster. Cela se produit par défaut si le fichier de base de données est disponible à l'emplacement par défaut. Toutefois, si le fichier de base de données est conservé dans un répertoire autre que /var/netscaler/locdb/, vous devez synchroniser manuellement le fichier sur tous les nœuds du cluster.
> - La `show gslb domain` commande n'est pas prise en charge dans une configuration de cluster.

Pour configurer GSLB dans un cluster à l'aide de l'interface de ligne de commande :

Ouvrez une session sur l'adresse IP du cluster et effectuez les opérations suivantes à l'invite de commandes :

1. Configurez les différentes entités GSLB. Pour plus d'informations, voir Entités de configuration GSLB.

   > **Remarque**
   >
   > Lors de la création du site GSLB, assurez-vous de spécifier l'adresse IP du cluster et l'adresse IP du cluster publique. L'adresse IP du cluster public n'est nécessaire que lorsque le cluster est déployé derrière un périphérique NAT. Lors de la configuration d'un site GSLB, vous devez utiliser l'adresse IP du cluster du même site. Ces paramètres sont nécessaires pour assurer la disponibilité de la fonctionnalité de synchronisation automatique GSLB.

   ```
   add gslb site <siteName> <siteType> <siteIPAddress> -publicIP <ip_addr>
    -clip <ip_addr> <publicCLIP><!--NeedCopy-->
   ```

2. Créez un groupe de nœuds de cluster.

   ```
   add cluster nodegroup <name> <name>@ [-strict ( YES | NO )] [-sticky (
   YES | NO )] [-state <state>] [-priority <positive_integer>]<!--NeedCopy
   -->
   ```

   > **Remarque**
   >
   > Activez l'option collante si vous souhaitez configurer GSLB basé pour les utilisateurs VPN.

3. Liez un nœud de cluster unique au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
   ```

4. Liez le site GSLB local au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -gslbSite <string><!--NeedCopy-->
   ```

   > **Remarque**
   >
   > Assurez-vous que l'adresse IP de l'adresse IP du site GSLB local est striped (disponible sur tous les nœuds de cluster).

5. Liez le service ADNS (ou ADNS-TCP) ou le serveur virtuel d'équilibrage de charge DNS (ou DNS-TCP) au groupe de nœuds.

   Pour lier le service ADNS :

   "'bind cluster nodegroup -service

   ```
   **Pour lier le serveur virtuel d'équilibrage de charge DNS :**

   ```bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

6. Liez le serveur virtuel GSLB au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

7. [Facultatif] Pour configurer GSLB en fonction des utilisateurs VPN, liez le serveur virtuel VPN au groupe de nœuds GSLB.

   ```
   bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

8. Vérifiez les configurations.

   ```
   show gslb runningConfig<!--NeedCopy-->
   ```

Pour configurer GSLB dans un cluster à l'aide de l'interface graphique :

Ouvrez une session sur l'adresse IP du cluster et effectuez les opérations suivantes dans l'onglet Configuration :

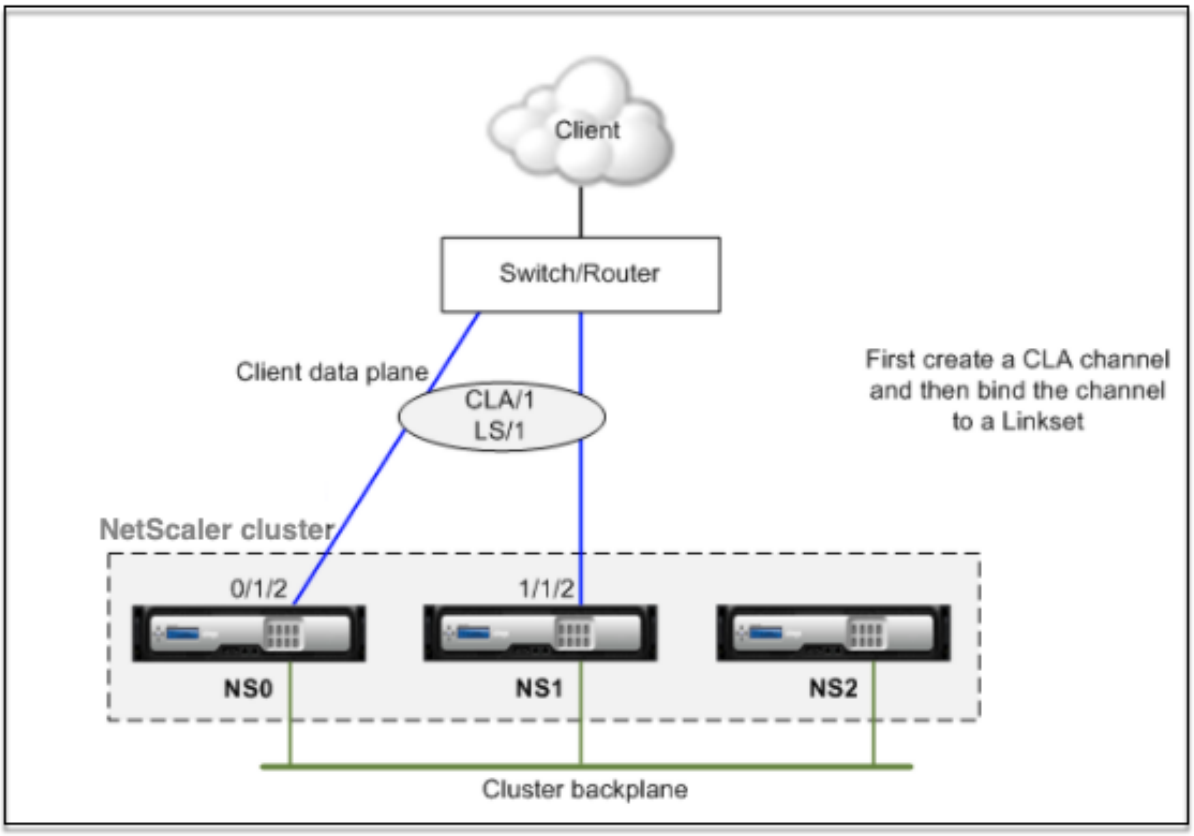
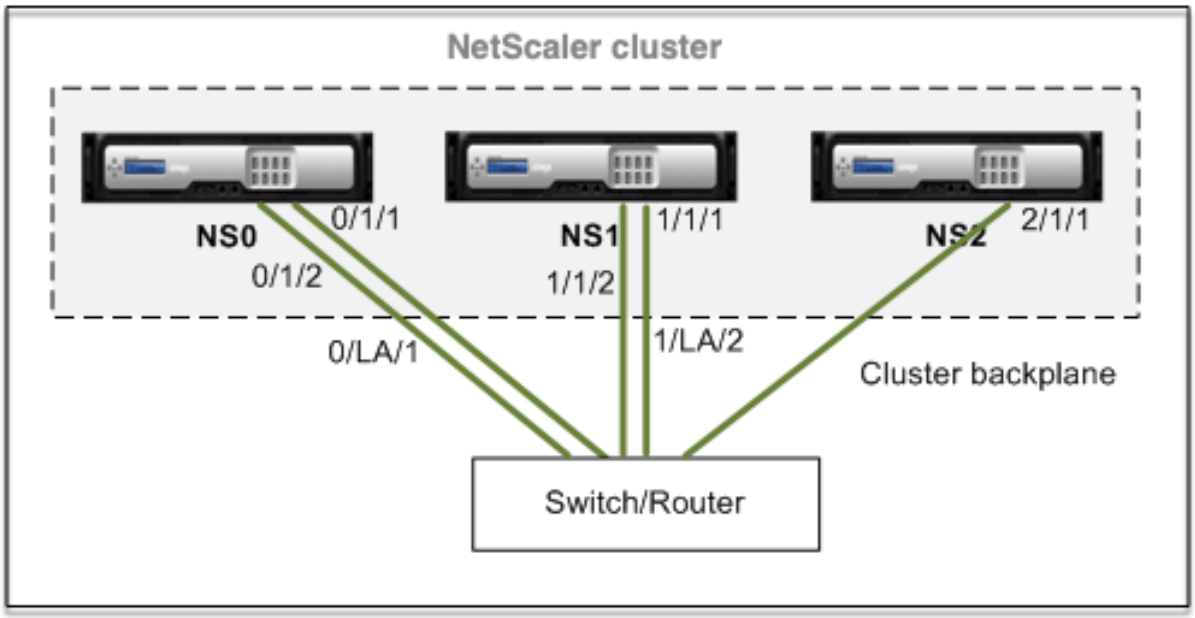
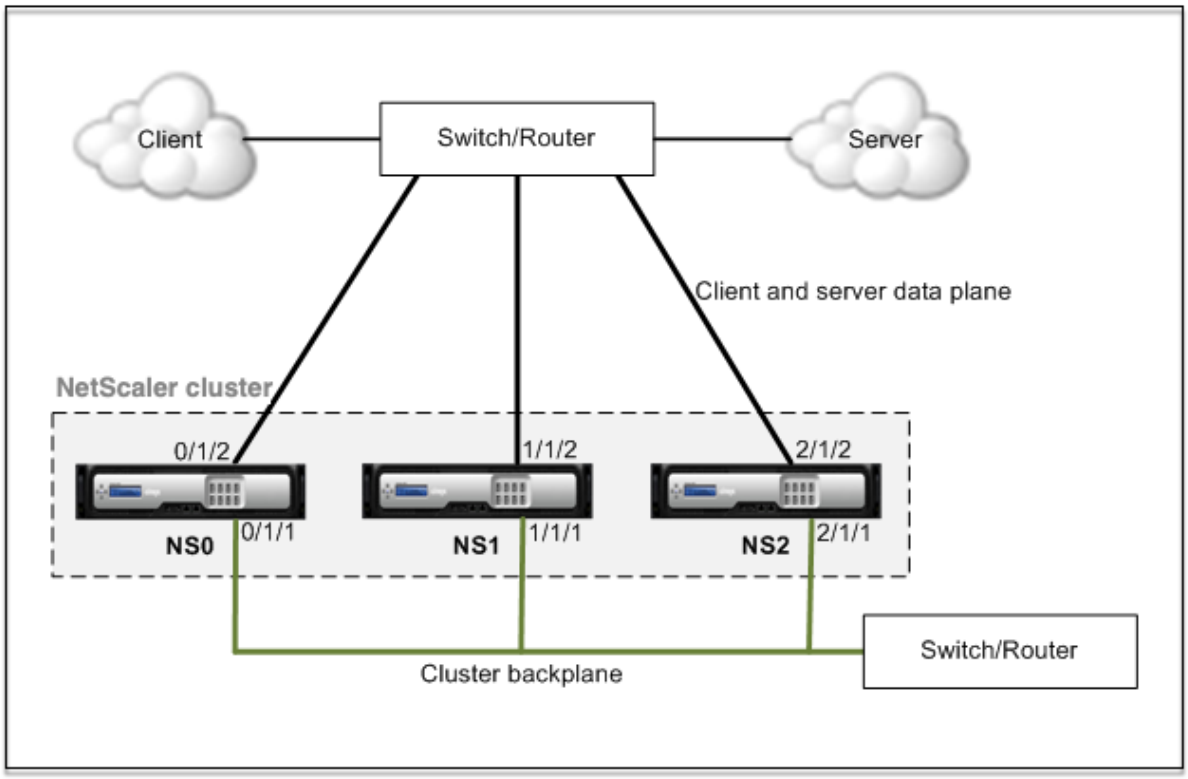
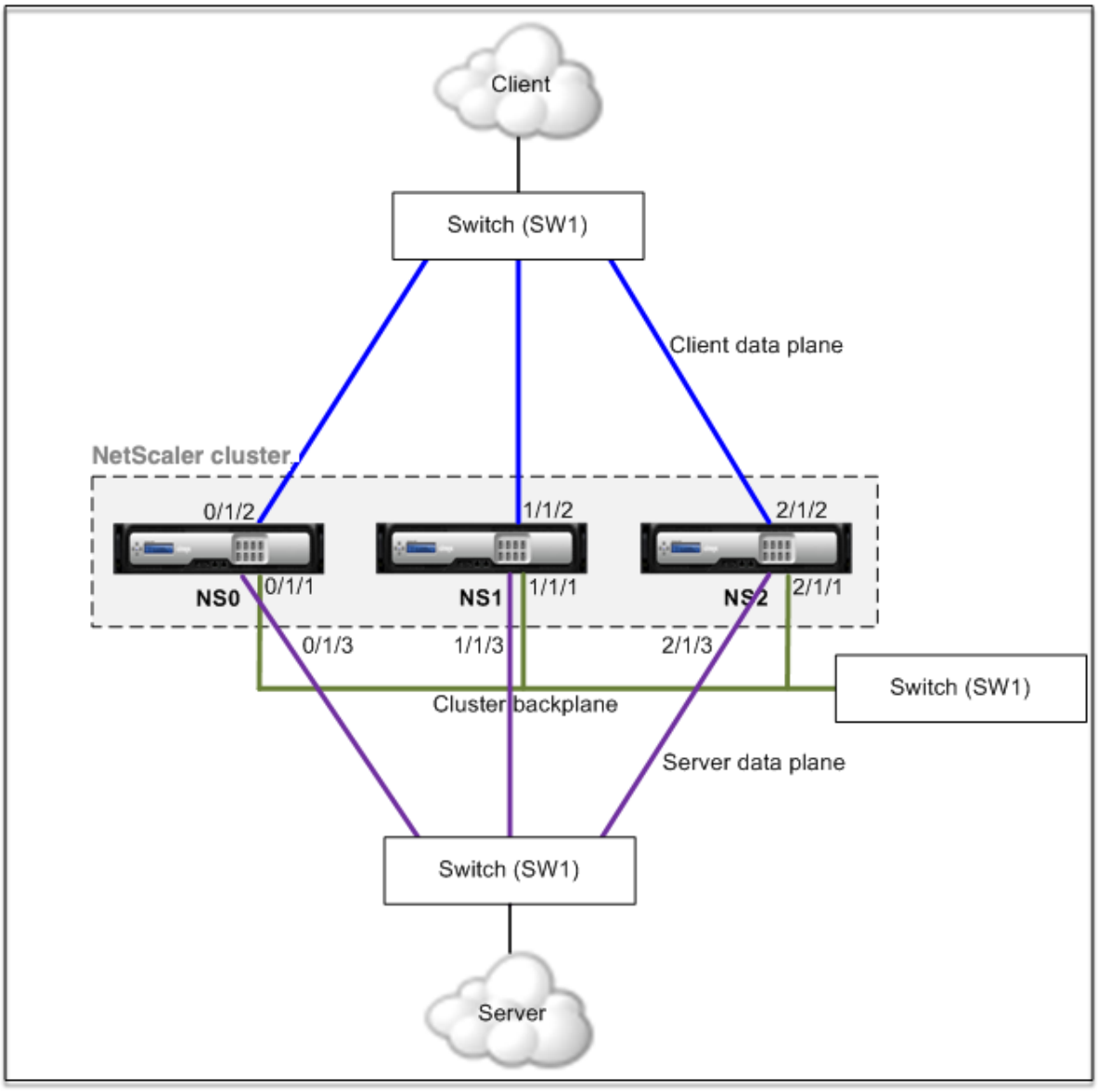
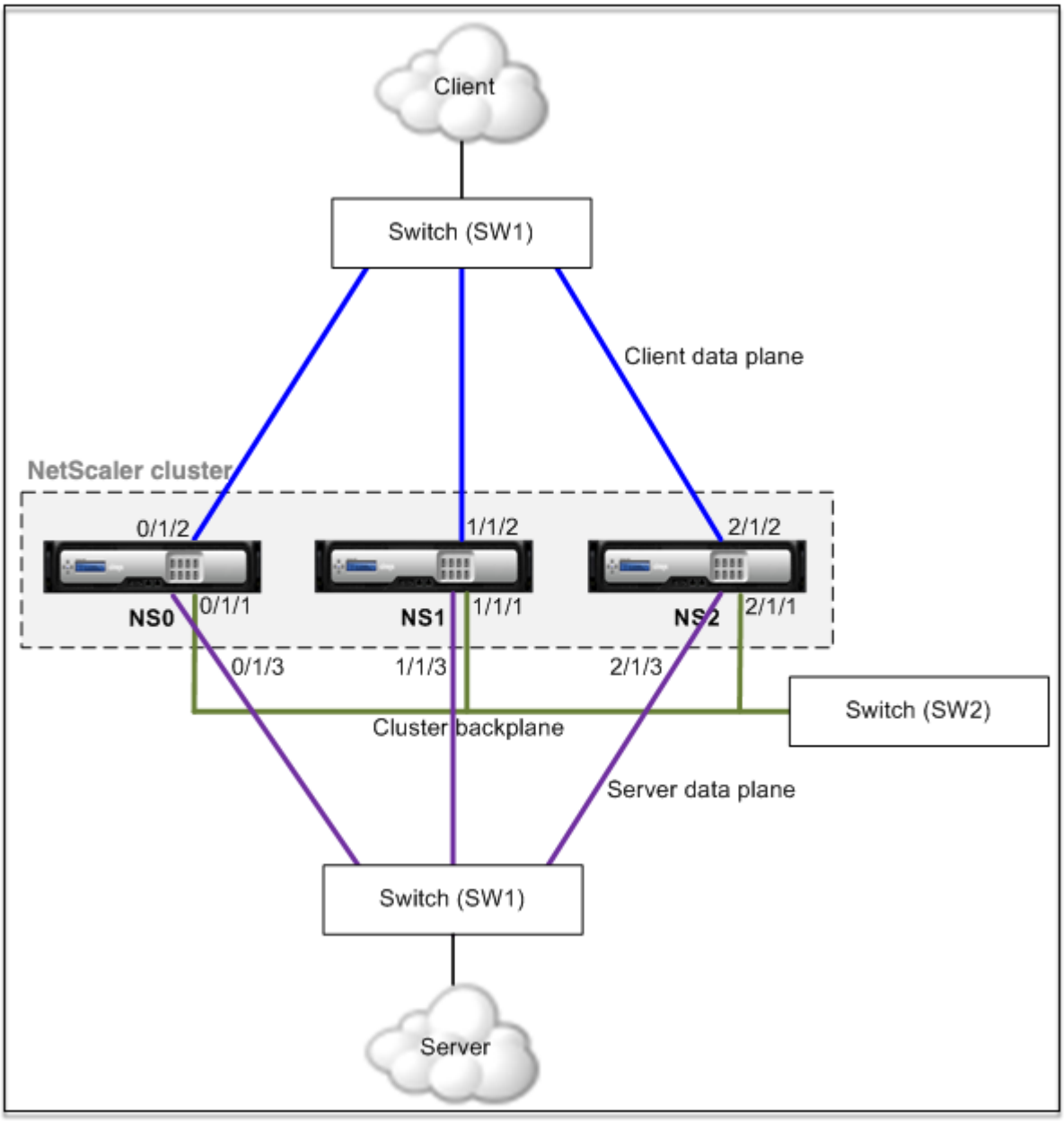
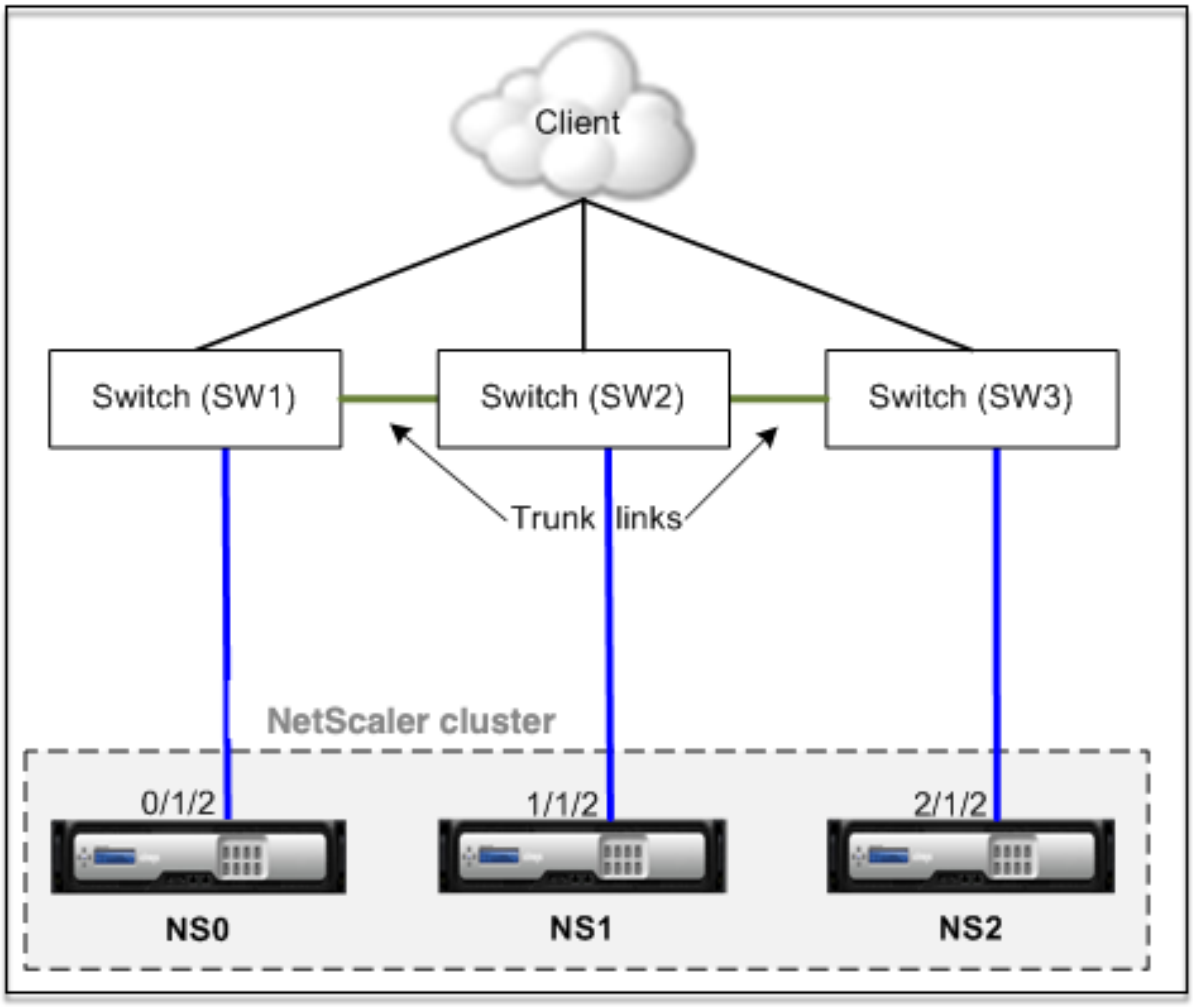
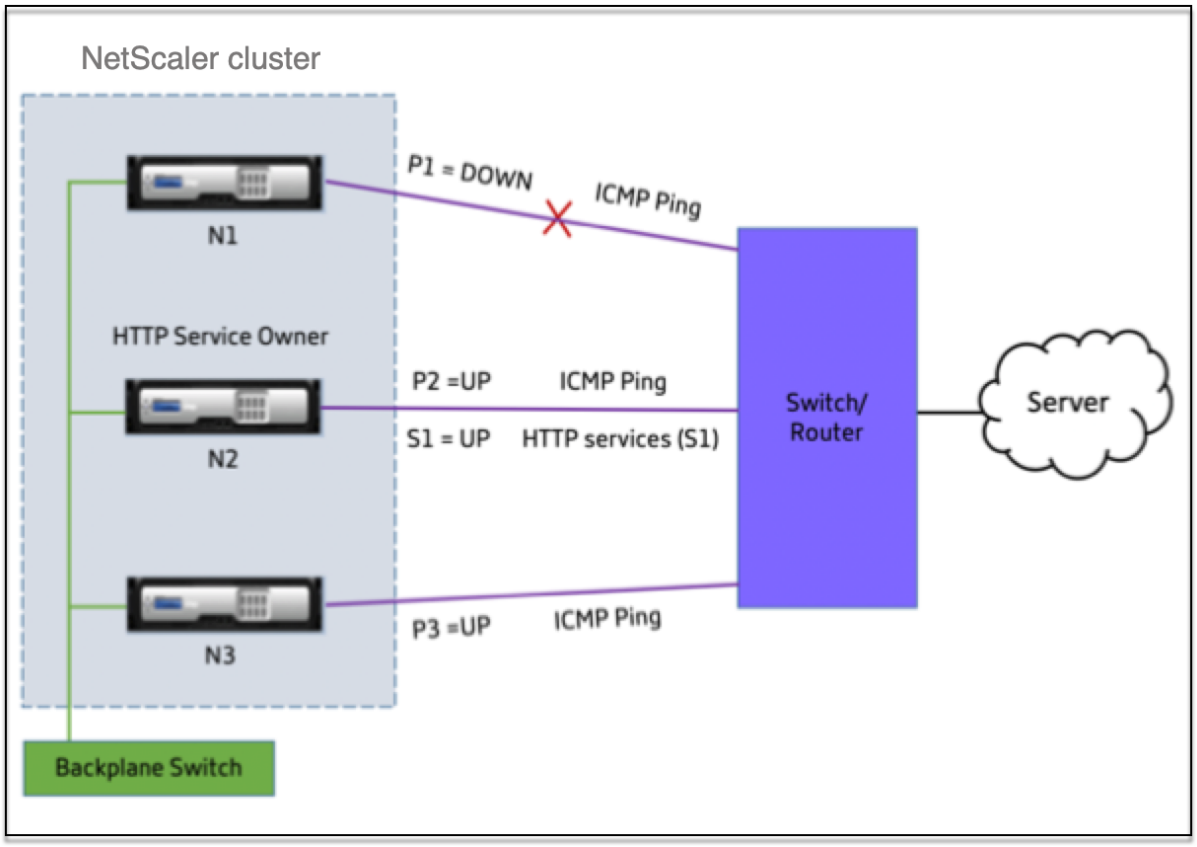
1. Configurez les entités GSLB.

   Accédez à **Gestion du trafic > GSLB** pour effectuer les configurations requises.

2. Créez un groupe de nœuds et effectuez d'autres configurations liées au groupe de nœuds.

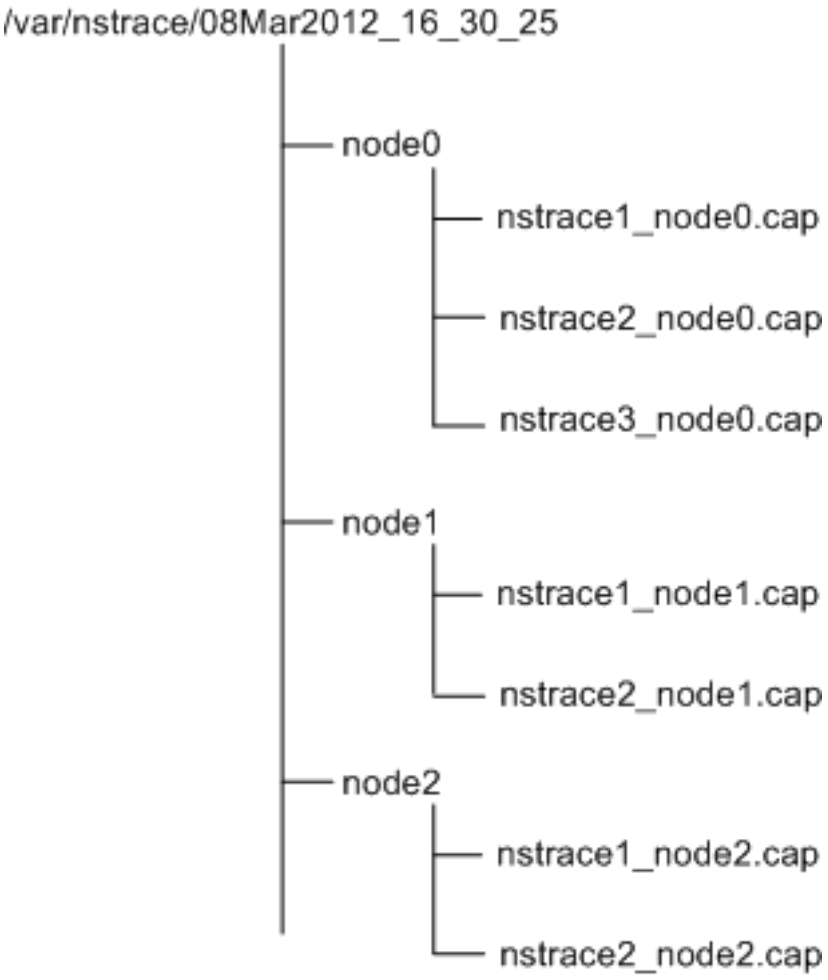
   Accédez à **Système > Cluster > Groupes de nœuds** pour effectuer les configurations requises.

Pour les configurations détaillées à effectuer, reportez-vous à la description fournie dans la procédure CLI précédente.


   ```

### Prise en charge de la topologie parent-enfant GSLB dans un cluster

À partir de NetScaler 12.1 build 49.xx, la topologie parent-enfant GSLB est prise en charge dans le cluster.

Pour plus d'informations sur la topologie parent-enfant, voir Déploiement de la topologie parent-enfant à l'aide du protocole MEP.

#### Pour configurer la topologie parent-enfant GSLB dans un cluster à l'aide de l'interface de ligne de commande

**Site parent**

Effectuez la configuration suivante :

1. Créez un groupe de nœuds de cluster.

   ```
   add cluster nodegroup <name>
   ```

   Exemple :

   ```
   add cluster nodegroup parentng
   ```

2. Liez un nœud de cluster unique au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```

   Exemple :

   ```
   bind cluster nodegroup parentng -node n2
   ```

3. Liez le site GSLB local au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Exemple :

   ```
   bind cluster nodegroup parentng -gslbSite site1
   ```

4. Liez le service ADNS (ou ADNS-TCP) ou le serveur virtuel d'équilibrage de charge DNS (ou DNS-TCP) au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -service <string>
   ```

   Exemple :

   ```
   bind cluster nodegroup parentng - service ADNS
   ```

5. Liez le serveur virtuel GSLB au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -vServer <string>
   ```

   Exemple :

   ```
   bind cluster nodegroup parentng -vServce gslbvs1
   ```


Site enfant

Effectuez la configuration suivante :

1. Créez un groupe de nœuds de cluster.

   ```
   add cluster nodegroup <name>
   ```

   Exemple :

   ```
   add cluster nodegroup childng
   ```

2. Liez un nœud de cluster unique au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```

   Exemple :

   ```
   bind cluster nodegroup childng -node -n3
   ```

3. Liez le site GSLB local au groupe de nœuds.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Exemple :

   ```
   bind cluster nodegroup childng -gslbSite site1
   ```

> **Remarque**
>
> Pour que les sites parents et enfants échangent des statistiques agrégées dans des méthodes d'équilibrage de charge basées sur des mesures, vous devez ajouter des services GSLB locaux sur le site enfant. Les méthodes d'équilibrage de charge basées sur des métriques sont le moins de connexion, la moins de bande passante et le moins de paquets.

Pour configurer la topologie parent-enfant GSLB dans un cluster à l'aide de l'interface graphique

1. Configurez les entités GSLB.

   Accédez à **Gestion du trafic** > **GSLB** pour effectuer les configurations requises.

2. Créez un groupe de nœuds.

   Accédez à **Système** > **Cluster** > **Groupes de nœuds** pour effectuer les configurations requises.

3. Dans la page Groupe de nœuds, sélectionnez le groupe de nœuds auquel vous souhaitez lier un nœud, cliquez sur **Modifier**, puis effectuez les tâches suivantes. Vous pouvez également effectuer ces tâches lors de l'ajout d'un groupe de nœuds.

   - Liez un nœud au groupe de nœuds.

     Dans **Paramètres avancés**, cliquez sur **Nœuds de cluster** et effectuez les tâches suivantes :

- Dans la section **Nœuds de cluster**, cliquez sur **Aucun nœud de cluster**.
- Dans **Sélectionner le nœud de cluster**, cliquez sur > et sélectionnez le nœud que vous souhaitez lier au groupe de nœuds. Vous pouvez également ajouter un nœud de cluster.

- Liez le site GSLB local au groupe de nœuds.

  Dans Paramètres avancés, cliquez sur Sites GSLB et effectuez les tâches suivantes :

  - Dans la section **Sites GSLB**, cliquez sur Aucun site GSLB.
  - Dans le **menu Sélectionner un site GSLB**, cliquez sur > et sélectionnez le site GSLB que vous souhaitez lier au groupe de nœuds. Vous pouvez également ajouter un site GSLB.

- Liez le serveur virtuel GSLB au groupe de nœuds.

  Dans **Paramètres avancés**, cliquez sur **Serveurs virtuels** et effectuez la tâche suivante :

  - Dans le volet **Serveurs virtuels**, cliquez sur +.
  - Dans **Choisir un serveur virtuel**, sélectionnez le serveur que vous souhaitez lier au groupe de nœuds.

- Liez le service ADNS (ou ADNS-TCP) ou le serveur virtuel d'équilibrage de charge DNS (ou DNS-TCP) au groupe de nœuds.

  Dans **Paramètres avancés**, cliquez sur **Services** et effectuez les tâches suivantes :

  - Dans la section **Services**, cliquez sur **Aucun service**.
  - Dans **Sélectionner un service**, sélectionnez le service que vous souhaitez lier au groupe de nœuds. Vous pouvez également ajouter un service.

> **Remarque**
>
> Pour les sites enfants, il suffit de lier le nœud de cluster et le site GSLB local au groupe de nœuds.

Utilisation de la redirection du cache dans un cluster

May 5, 2023

La redirection du cache dans un cluster fonctionne de la même manière que sur une appliance NetScaler autonome. La seule différence est que les configurations sont effectuées sur l'adresse IP du cluster. Pour plus d'informations sur la redirection du cache, voir Redirection du cache.

Points à retenir lors de l'utilisation de la redirection de cache en mode transparent sur un cluster :

- Avant de configurer la redirection du cache, assurez-vous que vous avez connecté tous les nœuds au commutateur externe et que vous avez configuré des jeux de liens. Dans le cas contraire, les demandes des clients sont abandonnées.
- Lorsque le mode MAC est activé sur un serveur virtuel d'équilibrage de charge, assurez-vous que le mode MBF est activé sur le cluster à l'aide de la commande enable ns mode MBF. Dans le cas contraire, les demandes sont envoyées directement au serveur d'origine au lieu d'être envoyées au serveur de cache.

Utilisation du mode L2 dans une configuration de cluster

January 21, 2021

> **Remarque**
>
> Prise en charge de NetScaler 10.5 et versions ultérieures.

Pour utiliser le mode L2 dans une configuration de cluster, vous devez vous assurer des éléments suivants :

- Les adresses IP spotted doivent être disponibles sur tous les nœuds, selon les besoins.
- Les jeux de liens doivent être utilisés pour communiquer avec le réseau externe.
- Les topologies asymétriques ou les groupes LA de cluster asymétrique ne sont pas pris en charge.
- Le groupe LA de cluster est recommandé.
- Le trafic est distribué entre les nœuds de cluster uniquement pour les déploiements où des services existent.

Utilisation du canal LA de cluster avec des jeux de liens

January 21, 2021

Dans une topologie de cluster asymétrique, certains nœuds de cluster ne sont pas connectés au réseau en amont. Dans ce cas, vous devez utiliser des jeux de liens. Pour optimiser les performances, vous pouvez lier les interfaces connectées au commutateur en tant que canal LA de cluster, puis lier le canal à un jeu de liens.

Pour comprendre comment une combinaison de canaux LA de cluster et de jeux de liens peut être utilisée, envisagez un cluster à trois nœuds pour lequel le commutateur en amont ne dispose que de deux ports. Vous pouvez connecter deux des nœuds de cluster au commutateur et laisser l'autre nœud non connecté.

> **Remarque**
>
> De même, vous pouvez également utiliser une combinaison d'ECMP et de jeux de liens dans une topologie asymétrique.

Figure 1. Linksets et topologie des canaux LA de cluster



Pour configurer le canal LA de cluster et les ensembles de liens à l'aide de l'interface de ligne de commande

1. Connectez-vous à l'adresse IP du cluster.
2. Liez les interfaces connectées à un canal LA de cluster.

```
add channel CLA/1 -ifnum 0/1/2 1/1/2
```

3. Liez le canal LA du cluster au jeu de liens.

```
add linkset LS/1 -ifnum CLA/1
```


backplane sur le canal LA

January 21, 2021

Dans ce déploiement, les canaux LA sont utilisés pour le backplane du cluster.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70
- NS2 - nodeId: 2, NSIP: 10.102.29.80

Pour déployer un cluster avec les interfaces de backplane en tant que canaux LA

1. Créez un cluster de nœuds NS0, NS1 et NS2.

   a) Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :

   ```
   > create cluster instance 1
   > add cluster node 0 10.102.29.60 -state ACTIVE
   > enable cluster instance 1
   > add ns ip 10.102.29.61 255.255.255.255 -type CLIP
   > save ns config
   > reboot -warm
   ```

   b) Connectez-vous à l'adresse IP du cluster et procédez comme suit :

   ```
   > add cluster node 1 10.102.29.70 -state ACTIVE
   ```



```
2 > add cluster node 2 10.102.29.80 -state ACTIVE
```

c) Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
1 > join cluster -clip 10.102.29.61 -password nsroot
2 > save ns config
3 > reboot -warm
```

Comme on le voit dans les commandes précédentes, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

2. Connectez-vous à l'adresse IP du cluster et procédez comme suit :

a) Créez les canaux LA pour les nœuds NS0 et NS1.

```
1 > add channel 0/LA/1 -ifnum 0/1/1 0/1/2
2 > add channel 1/LA/2 -ifnum 1/1/1 1/1/2
```

b) Configurez le backplane pour les nœuds de cluster.

```
1 > set cluster node 0 -backplane 0/LA/1
2 > set cluster node 1 -backplane 1/LA/2
3 > set cluster node 2 -backplane 2/1/1
```

Interfaces communes pour le client et le serveur et interfaces dédiées pour le fond de panier

May 5, 2023

Il s'agit d'un déploiement à bras unique du cluster NetScaler. Dans ce déploiement, les réseaux client et serveur utilisent les mêmes interfaces pour communiquer avec le cluster. Le backplane du cluster utilise des interfaces dédiées pour la communication entre les nœuds.



- NS0 - ID de nœud : 0, NSIP : 10.102.29.60
- NS1 - ID de nœud : 1, NSIP : 10.102.29.70
- NS2 - ID de nœud : 2, NSIP : 10.102.29.80

Pour déployer un cluster avec une interface commune pour le client et le serveur et une interface différente pour le backplane du cluster

1. Créez un cluster de nœuds NS0, NS1 et NS2.
2. Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :

```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

3. Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
```



```
2 > add cluster node 2 10.102.29.80 -state ACTIVE -backplane
      2/1/1
```

4. Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
1 > join cluster -clip 10.102.29.61 -password nsroot
2 > save ns config
3 > reboot -warm
```

Comme on le voit dans les commandes précédentes, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

1. Sur l'adresse IP du cluster, créez des VLAN pour les interfaces du backplane et pour les interfaces client et serveur.

   //Pour les interfaces de backplane

```
1 > add vlan 10
2 > bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Pour les interfaces connectées aux réseaux client et serveur.

```
1 > add vlan 20
2 > bind vlan 20 0/1/2 1/1/2 2/1/2
```

2. Sur le commutateur, créez des VLAN pour les interfaces correspondant aux interfaces de backplane et aux interfaces client et serveur. Les exemples de configuration suivants sont fournis pour le commutateur Cisco® Nexus 7000 C7010 version 5.2 (1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

   //Pour les interfaces du fond de panier. Répétez l'opération pour chaque interface…

```
1 > interface Ethernet2/47
2   switchport access vlan 100
3   switchport mode access
4   end
```

   //Pour les interfaces connectées aux réseaux client et serveur. Répétez l'opération pour chaque interface…

```
1 > interface Ethernet2/47
2   switchport access vlan 200
3   switchport mode access
4   end
```


Commutateur commun pour le client, le serveur et le fond de panier

May 5, 2023

Dans ce déploiement, le client, le serveur et le backplane utilisent des interfaces dédiées sur le même commutateur pour communiquer avec le cluster NetScaler.



- NS0 - ID de nœud : 0, NSIP : 10.102.29.60
- NS1 - ID de nœud : 1, NSIP : 10.102.29.70
- NS2 - ID de nœud : 2, NSIP : 10.102.29.80

Pour déployer un cluster avec un commutateur commun pour le client, le serveur et le

backplane

1. Créez un cluster de nœuds NS0, NS1 et NS2.
2. Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :

```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

3. Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
> add cluster node 2 10.102.29.80 -state ACTIVE -backplane
   2/1/1
```

4. Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```

Comme on le voit dans les commandes précédentes, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

1. Sur l'adresse IP du cluster, créez des VLAN pour les interfaces du backplane, du client et du serveur.

   //Pour les interfaces de backplane

```
> add vlan 10
> bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Pour les interfaces côté client

```
> add vlan 20
> bind vlan 20 0/1/2 1/1/2 2/1/2
```

   //Pour les interfaces côté serveur


```
> add vlan 30
> bind vlan 30 0/1/3 1/1/3 2/1/3
```

2. Sur le commutateur, créez des VLAN pour les interfaces correspondant aux interfaces de backplane et aux interfaces client et serveur. Les exemples de configuration suivants sont fournis pour le commutateur Cisco® Nexus 7000 C7010 version 5.2 (1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

   //Pour les interfaces du fond de panier. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/47
  switchport access vlan 100
  switchport mode access
  end
```

   //Pour les interfaces client. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/48
  switchport access vlan 200
  switchport mode access
  end
```

   //Pour les interfaces serveur. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/49
  switchport access vlan 300
  switchport mode access
  end
```

Commutateur commun pour client et serveur et commutateur dédié pour fond de panier

May 5, 2023

Dans ce déploiement, les clients et les serveurs utilisent différentes interfaces sur le même commutateur pour communiquer avec le cluster NetScaler. Le panneau arrière du cluster utilise un commutateur dédié pour la communication entre les nœuds.



- NS0 - ID de nœud : 0, NSIP : 10.102.29.60
- NS1 - ID de nœud : 1, NSIP : 10.102.29.70
- NS2 - ID de nœud : 2, NSIP : 10.102.29.80

Pour déployer un cluster avec le même commutateur pour les clients et les serveurs et un autre commutateur pour le backplane du cluster

1. Créez un cluster de nœuds NS0, NS1 et NS2.
    - Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :


```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

- Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
> add cluster node 2 10.102.29.80 -state ACTIVE -backplane
   2/1/1
```

- Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```

Comme on le voit dans les commandes précédentes, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

2. Sur l'adresse IP du cluster, créez des VLAN pour les interfaces du backplane, du client et du serveur.

   //Pour les interfaces de backplane

```
> add vlan 10
> bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Pour les interfaces côté client

```
> add vlan 20
> bind vlan 20 0/1/2 1/1/2 2/1/2
```

   //Pour les interfaces côté serveur

```
> add vlan 30
> bind vlan 30 0/1/3 1/1/3 2/1/3
```

3. Sur le commutateur, créez des VLAN pour les interfaces correspondant aux interfaces de backplane et aux interfaces client et serveur. Les exemples de configuration suivants sont fournis

pour le commutateur Cisco® Nexus 7000 C7010 version 5.2 (1). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

//Pour les interfaces du fond de panier. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/47
> switchport access vlan 100
> switchport mode access
> end
```

//Pour les interfaces client. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/48
> switchport access vlan 200
> switchport mode access
> end
```

//Pour les interfaces serveur. Répétez l'opération pour chaque interface…

```
> interface Ethernet2/49
> switchport access vlan 300
> switchport mode access
> end
```

Commutateur différent pour chaque nœud

January 21, 2021

Dans ce déploiement, chaque nœud de cluster est connecté à un commutateur différent et les liaisons de jonction sont configurées entre les commutateurs.



Les configurations de cluster sont les mêmes que les autres scénarios de déploiement. La plupart des configurations côté client sont effectuées sur les commutateurs côté client.

Exemples de configurations de cluster

May 5, 2023

L'exemple suivant peut être utilisé pour configurer un cluster à quatre nœuds avec ECMP, cluster LA ou Linksets.

1. Créez le cluster.
    - Ouvrez une session sur le premier nœud.
    - Ajoutez l'instance de cluster.

```
1   > add cluster instance 1
```


- Ajoutez le premier nœud au cluster.

```
1   > add cluster node 0 10.102.33.184 -backplane 0/1/1
```

- Activez l'instance de cluster.

```
1   > enable cluster instance 1
```

- Ajoutez l'adresse IP du cluster.

```
1   > add ns ip 10.102.33.185 255.255.255.255 -type CLIP
```

- Enregistrez les configurations.

```
1   > save ns config
```

- Redémarrez l'appliance à chaud.

```
1   > reboot -warm
```

2. Ajoutez les trois autres nœuds au cluster.
   - Connectez-vous à l'adresse IP du cluster.
   - Ajoutez le deuxième nœud au cluster.

```
1   > add cluster node 1 10.102.33.187 -backplane 1/1/1
```

   - Ajoutez le troisième nœud au cluster.

```
1   > add cluster node 2 10.102.33.188 -backplane 2/1/1
```

   - Ajoutez le quatrième nœud au cluster.

```
1   > add cluster node 3 10.102.33.189 -backplane 3/1/1
```

3. Joignez les nœuds ajoutés au cluster. Cette étape ne s'applique pas au premier nœud.
   - Connectez-vous à chaque nœud nouvellement ajouté.
   - Joignez le nœud au cluster.

```
1   > join cluster -clip 10.102.33.185 -password nsroot
```

   - Enregistrez la configuration.

```
1   > save ns config
```


- Redémarrez l'appliance à chaud.

```
1   > reboot -warm
```

4. Configurez le cluster NetScaler via l'adresse IP du cluster.

   // Activer la fonction d'équilibrage de charge

```
1      > enable ns feature lb
```

   // Ajout d'un serveur virtuel d'équilibrage de charge

```
1      > add lb vserver first_lbvserver http
2      ....
3      ....
```

5. Configurez l'un des mécanismes de distribution de trafic suivants (ECMP, LA de cluster ou Linkset) pour le cluster.

   ECMP

   - Connectez-vous à l'adresse IP du cluster.
   - Activez le protocole de routage OSPF.

```
1   > enable ns feature ospf
```

   - Ajoutez un VLAN.

```
1   > add vlan 97
```

   - Liez les interfaces des nœuds du cluster au VLAN.

```
1   > bind vlan 97 -ifnum 0/1/4 1/1/4 2/1/4 3/1/4
```

   - Ajoutez un SNIP repéré sur chaque nœud et activez le routage dynamique sur celui-ci.

```
1   > add ns ip 1.1.1.10 255.255.255.0 -ownerNode 0 -
       dynamicRouting ENABLED
2   > add ns ip 1.1.1.11 255.255.255.0 -ownerNode 1 -
       dynamicRouting ENABLED
3   > add ns ip 1.1.1.12 255.255.255.0 -ownerNode 2 -
       dynamicRouting ENABLED
4   > add ns ip 1.1.1.13 255.255.255.0 -ownerNode 3 -
       dynamicRouting ENABLED
```

   - Liez l'une des adresses SNIP au VLAN.


```
1   > bind vlan 97 -ipAddress 1.1.1.10 255.255.255.0
```

- Configurez le protocole de routage sur les ZEBOs à l'aide du shell VTYSH.

  Cluster statique LA

  - Connectez-vous à l'adresse IP du cluster.
  - Ajouter un canal LA de cluster.

    ```
    1   > add channel CLA/1 -speed 1000
    ```

  - Liez les interfaces au canal LA du cluster.

    ```
    1   > bind channel CLA/1 0/1/5 1/1/5 2/1/5 3/1/5
    ```

  - Effectuez une configuration équivalente sur le commutateur.

    Cluster dynamique LA

    * Connectez-vous à l'adresse IP du cluster.
    * Ajoutez les interfaces au canal LA du cluster.

      ```
      1   > set interface 0/1/5 -lacpmode active -lacpkey 5 -
          lagtype cluster
      2   > set interface 1/1/5 -lacpmode active -lacpkey 5 -
          lagtype cluster
      3   > set interface 2/1/5 -lacpmode active -lacpkey 5 -
          lagtype cluster
      4   > set interface 3/1/5 -lacpmode active -lacpkey 5 -
          lagtype  cluster
      ```

    * Effectuez une configuration équivalente sur le commutateur.

    Ensembles de liens. Supposons que le nœud portant l'ID de nœud 3 n'est pas connecté au commutateur. Vous devez configurer un jeu de liens afin que le nœud non connecté puisse utiliser les autres interfaces du nœud pour communiquer avec le commutateur.

  a) Connectez-vous à l'adresse IP du cluster.

  b) Ajouter un jeu de liens.

     ```
     1  > add linkset LS/1
     ```

  c) Liez les interfaces connectées au jeu de liens.


```
1 > bind linkset LS/1 -ifnum 0/1/6 1/1/6 2/1/6
```

6. Mettez à jour l'état des nœuds de cluster en ACTIVE.

```
1 > set cluster node 0 -state ACTIVE
2 > set cluster node 1 -state ACTIVE
3 > set cluster node 2 -state ACTIVE
4 > set cluster node 3 -state ACTIVE
```

Utilisation de VRRP dans une configuration de cluster

August 20, 2021

Virtual Router Redundancy Protocol (VRRP) est pris en charge dans une configuration de cluster pour IPv4 et IPv6. Les deux fonctionnalités VRRP prises en charge dans une configuration de cluster sont VRRP basé sur l'interface et VRRP basé sur IP.

VRRP basé sur IP

Dans VRRP basé sur IP, les adresses VIP par bandes liées au même VRID sont configurées sur tous les nœuds d'une configuration de cluster. Ces adresses VIP sont actives sur tous les nœuds

L'un des nœuds de cluster agit en tant que propriétaire VRID et envoie la publicité VRRP à d'autres nœuds. En cas d'échec du nœud propriétaire VRID, un autre nœud du cluster assume la propriété du VRID et commence à envoyer des publicités VRRP. Vous pouvez également affecter un nœud de cluster spécifique en tant que propriétaire du VRID.

> **Remarque**
>
> Citrix vous recommande d'utiliser la méthode basée sur IP pour le déploiement VRRP dans le cluster.

Configuration du VRRP basé sur IP pour IPv4

Effectuez les tâches suivantes sur une configuration de cluster pour configurer le VRRP basé sur IP pour IPv4 :

- **Ajoutez un VRID**. Un VRID est un entier utilisé par la configuration de cluster pour former une adresse MAC virtuelle. L'adresse VMAC générique est sous la forme de 00:00:5e:00:02:<VRID>.
- **(Facultatif) Affectez un nœud en tant que propriétaire de l'adresse MAC virtuelle**. Vous pouvez définir le paramètre de nœud propriétaire (lors de l'ajout ou de la modification de VRID6)

sur l'ID du nœud de cluster pour l'affecter en tant que propriétaire de l'adresse MAC virtuelle. Si le nœud propriétaire attribué échoue, l'un des nœuds de cluster UP est dynamiquement choisi comme propriétaire de l'adresse MAC virtuelle. Vous pouvez définir le nœud propriétaire à l'aide de la `set vrID <id> -ownerNode <positive_interger>` commande.

- **Liez le VRID à l'adresse VIP des nœuds**. Liez le VRID créé à l'adresse VIP entrelacée.

Pour ajouter un VRID à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 - add vrid <ID> [-ownerNode <positive_integer>]
2 - show vrid <ID>
```

Pour lier le VRID à l'adresse VIP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set ns ip <IPv4Address> -vrid <ID><!--NeedCopy-->`
- `show vrid <ID><!--NeedCopy-->`

Pour ajouter un VRID à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > VMAC** et, sous l'onglet **VMAC**, cliquez sur **Ajouter** .
2. Dans la page Créer un **VMAC**, spécifiez une valeur dans le champ **ID du routeur virtuel**, puis cliquez sur **Créer** .

Pour lier le VRID à une adresse VIP à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > IP**, sous l'onglet **IPv4s**, sélectionnez une adresse VIP et cliquez sur **Modifier**.
2. Définissez le paramètre **Virtual Router ID** lors de la modification de la configuration VIP.

```
1 > add vrid 90
2  Done
3 > set ns ip 192.0.2.90 - vrid 90
4  Done
```

Configuration du VRRP basé sur IP pour IPv6

Effectuez les tâches suivantes sur une configuration de cluster pour configurer le VRRP basé sur IP pour IPv6 :

- **Ajoutez un VRID6**. Un VRID6 est un entier utilisé par la configuration de cluster pour former une adresse MAC6 virtuelle. L'adresse générique VMAC6 est sous la forme de 00:00:5e:00:02:<VRID6>.
- **(Facultatif) Affectez un nœud en tant que propriétaire de l'adresse MAC6 virtuelle**. Vous pouvez définir le paramètre de nœud propriétaire (lors de l'ajout ou de la modification de VRID6) sur l'ID du nœud de cluster pour l'affecter en tant que propriétaire de l'adresse MAC6 virtuelle. Si le nœud propriétaire attribué échoue, l'un des nœuds de cluster UP est dynamiquement choisi comme propriétaire de l'adresse MAC6 virtuelle.
- **Liez le VRID6 à l'adresse VIP6 des nœuds**. Liez le VRID6 créé à l'adresse VIP6 entrelacée.

Pour ajouter un VRID6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `add vrid6 <ID> [-ownerNode <positive_integer>]<!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

Pour lier l'adresse VRID6 à VIP6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set ns ip6 <IPv6Address> -vrid6 <ID><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

Pour ajouter un VRID6 à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > VMAC** et, sous l'onglet **VMAC6**, cliquez sur **Ajouter** .
2. Sur la page **Créer MAC6 virtuel**, spécifiez une valeur dans le champ **ID du routeur virtuel**, puis cliquez sur **Créer** .

Pour lier le VRID6 à une adresse VIP6 à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > IP**, sous l'onglet **IPv6s**, sélectionnez une adresse VIP et cliquez sur **Modifier**.
2. Définissez le paramètre **Virtual Router ID** lors de la modification de la configuration VIP6.

```
1 > add vrid6 90
2  Done
3 > set ns ip6 2001:db8::5001  - vrid6 90
4  Done
```


VRRP basé sur l'interface

Dans la fonction VRRP basée sur l'interface, la même adresse MAC virtuelle est configurée sur les deux nœuds du cluster. Cette adresse MAC virtuelle est utilisée dans les annonces GARP et les réponses ARP pour les adresses IP configurées sur un nœud. Cette fonctionnalité est utile dans une configuration de cluster à deux nœuds active de secours qui dispose de périphériques/routeurs externes qui n'acceptent pas les publicités GARP.

> **Remarque**
>
> La fonction VRRP basée sur l'interface ne s'applique qu'à un cluster à deux nœuds dont un nœud est en état actif et l'autre noeud servant de rechange.

Avec la même adresse MAC virtuelle sur les deux nœuds de cluster, lorsque le nœud actif tombe en panne et que le nœud de secours prend le relais comme actif, l'adresse MAC des adresses IP du nouveau nœud actif reste inchangée et les tables ARP des périphériques/routeurs externes n'ont pas besoin d'être mises à jour.

Configuration de VRRP basé sur l'interface pour IPv4

Effectuez les tâches suivantes sur une configuration de cluster pour configurer VRRP basé sur l'interface pour IPv4 :

- **Ajoutez un VRID**. Un VRID est un entier utilisé par la configuration de cluster pour former une adresse MAC virtuelle.
- **Liez le VRID aux interfaces de nœud**. Liez les interfaces au VRID créé. Les interfaces liées (dans le nœud actif actuel) utilisent l'adresse MAC virtuelle dans les publicités GARP et les réponses ARP pour ses adresses IPv4. Vous devez associer le VRID aux interfaces des deux nœuds de la configuration du cluster de secours actif. En effet, contrairement à une configuration de haute disponibilité, les ID d'interface diffèrent dans une configuration de cluster.

Pour ajouter un VRID à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 - add vrid <ID>
2 - show vrid <ID>
```

Pour lier le VRID à une interface à l'aide de la CLI

À l'invite de commandes, tapez :

```
1 - bind vrid <ID> -ifnum <interface_name>
```



```
2 - show vrid <ID>
```

Pour ajouter un VRID et le lier à des interfaces à l'aide de l'interface graphique

1. Accédez à **Système > Réseau > VMAC** et, sous l'onglet **VMAC**, cliquez sur **Ajouter** .
2. Sur la page **Créer un MAC virtuel**, spécifiez une valeur dans le champ Identifiant du routeur ****virtuel*, liez les interfaces dans la section**Associer les interfaces**, puis cliquez sur**Créer**.

```
1 > add vrid 300
2  Done
3 > bind vrid 300 -ifnum 1/1/2 2/1/3
4  Done
```

Configuration du VRRP basé sur l'interface pour IPv6

Effectuez les tâches suivantes sur une configuration de cluster pour configurer le VRRP basé sur l'interface pour IPv6 :

- **Ajoutez un VRID6**. Un VRID6 est un entier utilisé par la configuration de cluster pour former une adresse MAC6 virtuelle. L'adresse générique VMAC6 est sous la forme de 00:00:5 e : 00:01 : <VRID6>.
- **Liez le VRID6 aux interfaces de nœud**. Liez les interfaces au VRID6 créé. Les interfaces liées (dans le nœud actif actuel) utilisent l'adresse MAC6 virtuelle dans les publicités GARP et les réponses ARP pour ses adresses IPv6. Vous devez associer le VRID6 aux interfaces des deux nœuds de la configuration du cluster de secours actif. En effet, contrairement à une configuration de haute disponibilité, les ID d'interface diffèrent dans une configuration de cluster.

Pour ajouter un VRID6 à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 - add vrid6 <ID>
2 - show vrid6 <ID>
```

Pour lier le VRID6 à une interface à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `bind vrid6 <ID> -ifnum <interface_name><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

Pour ajouter un VRID6 et le lier à des interfaces à l'aide de l'interface graphique

1. Naviguez **Système > Réseau > VMAC** et, sous l'onglet **VMAC6**, cliquez sur **Ajouter** .
2. Sur la page **Créer MAC6 virtuel**, spécifiez une valeur dans le champ **ID du routeur virtuel**, liez les interfaces dans la section **Associer les interfaces**, puis cliquez sur **Créer** .

```
> add vrid6 100
 Done
> bind vrid6 100 -ifnum 0/1/1 1/1/2 2/1/3
 Done
```

Services de surveillance dans un cluster à l'aide de la surveillance des chemins

May 5, 2023

Dans une configuration en cluster, la propriété des services de surveillance est répartie entre les nœuds. Par conséquent, différents nœuds surveillent différents services. Le nœud qui surveille un service est appelé propriétaire du service. Seul le propriétaire du service sonde le serveur pour surveiller l'état des services qui lui sont assignés. Il communique également l'état des services à tous les autres nœuds du cluster. L'inconvénient de la surveillance distribuée est que la connectivité réseau et l'état des liens entre tous les nœuds et le serveur ne sont pas déterminés. Pour pallier cet inconvénient, vous pouvez utiliser la surveillance des chemins.

> **Remarque**
>
> Vous ne pouvez pas sélectionner un nœud pour surveiller un service. La sélection des nœuds pour surveiller un service s'effectue par le biais d'un mécanisme interne. Vous pouvez voir le nœud propriétaire pour surveiller les services à l'aide de la `show serviceGroup <service group name>` commande `show service <service name>` and.

La surveillance des chemins vérifie la connectivité réseau et l'état du lien entre un nœud et le service fourni par le serveur. Un nœud envoie des pings ICMP pour vérifier si le serveur est accessible ou non.

Comment fonctionne la surveillance des chemins

Prenons l'exemple d'un cluster NetScaler composé de trois nœuds N1, N2 et N3. N2 est le propriétaire du service qui surveille l'état des services HTTP (S1). Il annonce l'état du service aux autres nœuds du cluster. La surveillance des chemins est activée sur tous les nœuds du cluster, pour tous les services. Chaque nœud envoie uniquement un ping ICMP au serveur. Le propriétaire du service envoie à la fois

la demande de service HTTP et un ping ICMP. Chaque nœud signale l'état de surveillance des chemins au propriétaire du service.



Les deux paramètres suivants déterminent l'état de service d'un nœud :

- S = état du service annoncé par le propriétaire du service
- P = état de surveillance du chemin de chaque nœud

Le fait qu'un nœud puisse accéder à un serveur ou non détermine l'état de surveillance des chemins pour ce nœud.

Le tableau suivant indique l'état du service défini en fonction de l'état de surveillance des chemins, lorsque le paramètre PathMonitorIndv est activé ou désactivé.

Paramètre	État de surveillance du chemin	État du service
PathMonitorIndv = NO ; Il s'agit de la configuration par défaut.	P1 = VERS LE BAS	S1 = VERS LE BAS
	P2 = VERS LE HAUT	S1 = VERS LE BAS
	P3 = VERS LE HAUT	S1 = VERS LE BAS

Paramètre	État de surveillance du chemin	État du service
PathMonitorIndv = OUI	P1 = VERS LE BAS	S1 = VERS LE BAS
	P2 = VERS LE HAUT	S1 = VERS LE HAUT
	P3 = VERS LE HAUT	S1 = VERS LE HAUT

Dans cet exemple, le propriétaire du service décide de l'état du service pour tous les nœuds en fonction du nœud dont l'état de surveillance des chemins est défini sur DOWN. Si l'état de surveillance des chemins pour l'un des nœuds est DOWN, le propriétaire du service définit l'état du service pour tous les nœuds comme DOWN. L'état de service de tous les nœuds est défini sur UP uniquement si l'état de surveillance des chemins pour chacun des nœuds est UP.

Vous pouvez utiliser la surveillance des chemins pour des nœuds individuels en activant le paramètre PathMonitorIndv. Ce paramètre permet au propriétaire du service de définir l'état du service pour chaque nœud en fonction de l'état de surveillance des chemins de ce nœud respectif.

> **Remarque**
>
> Si le paramètre PathMonitorIndv est défini, certaines fonctionnalités, telles que la persistance, peuvent être interrompues.

Configuration de la surveillance des chemins

La surveillance des chemins s'applique à tous les services et groupes de services. Le paramètre de surveillance des chemins est désactivé par défaut.

Pour activer la surveillance des chemins pour les services/groupes de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <service name> <IP address> <service type> <port> [-
    pathMonitor <YES | NO>] [-pathMonitorIndv <YES | NO>]

add servicegroup <servicegroup name> <service type> [-pathMonitor <YES
    | NO>] [-pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```

Exemple :

```
add service s1 1.1.1.1 HTTP 80 -pathMonitor YES
```



```
add servicegroup sg_1 HTTP -pathMonitor YES

add service s1 1.1.1.1 HTTP 80 -pathMonitor YES -pathMonitorIndv YES
add servicegroup sg_1 HTTP -pathMonitor YES -pathMonitorIndv YES
<!--NeedCopy-->
```

Vous pouvez également définir le paramètre de surveillance des chemins à l'aide de la commande set, comme suit :

```
set service <service name> [-pathMonitor <YES | NO>] [-pathMonitorIndv
   <YES | NO>]
set servicegroup <servicegroup name> [-pathMonitor <YES | NO>] [-
   pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```

Exemple :

```
set service s1 -pathMonitor YES
set servicegroup sg_1 -pathMonitor YES


set service s1 -pathMonitorIndv YES
set servicegroup sg_1 -pathMonitorIndv NO
<!--NeedCopy-->
```

Pour activer la surveillance des chemins pour les services/groupes de services à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.

   Pour les groupes de services, accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.

2. Dans le volet **Services/Groupes de services**, sélectionnez un service/groupe de services dans la liste, puis double-cliquez pour l'ouvrir.
3. Dans l'onglet **Paramètres du service**, cliquez sur **Modifier**.
4. Sélectionnez **Path Monitoring**.
5. Sélectionnez **Individual Path Monitoring**si vous souhaitez l'appliquer, puis cliquez sur **OK**.

> **Remarque**
>
> Vous pouvez activer la surveillance individuelle des chemins uniquement si vous activez la surveillance des chemins.

Sauvegarde et restauration de la configuration du cluster

May 5, 2023

Vous pouvez sauvegarder l'état actuel d'un nœud de cluster NetScaler. Plus tard, vous pouvez utiliser les fichiers sauvegardés pour restaurer le nœud dans le même état de cluster. Par mesure de précaution, vous devez utiliser cette fonctionnalité avant d'effectuer une mise à niveau sur les nœuds du cluster.

Sauvegarder la configuration d'un cluster

Vous pouvez effectuer une sauvegarde de base ou complète selon les critères suivants :

- Type de données à sauvegarder.
- Fréquence à laquelle vous créez une sauvegarde.
- **Sauvegarde de base.** Sauvegarde uniquement les fichiers de configuration. Vous souhaiterez peut-être effectuer ce type de sauvegarde fréquemment, car les fichiers qu'il sauvegarde changent constamment. Les fichiers sauvegardés sont répertoriés dans le tableau.

Répertoire

Sous-répertoire ou fichiers

/nsconfig/

- ns.conf
- ZEBOS.conf
- rc.netscaler
- snmpd.conf
- nsbefore.sh
- nsafter.sh
- inetd.conf
- ntp.conf
- syslog.conf
- newsyslog.conf
- crontab
- host.conf
- hôtes
- ttys
- sshd_config
- httpd.conf
- monitrc

- rc.conf
- ssh_config
- heure locale
- numéro
- issue.net

/var/

- télécharger/*
- log/wicmd.log
- av/tomcat/webapps/*
- avec/tomcat/logs/*
- wi/tomcat/conf/catalina/localhost/*
- nslw.bin/etc/krb.conf
- nslw.bin/etc/krb.keytab
- netscaler/locdb/*
- lib/likewise/db/*
- vpn/bookmark/*
- netscaler/crl
- Modèles/*
- données_d'apprentissage/*

/netscaler/

- custom.html
- vsr.html
- **Sauvegarde complète.** Outre les fichiers sauvegardés par une sauvegarde de base, une sauvegarde complète sauvegarde certains fichiers moins fréquemment mis à jour. Les fichiers qui sont sauvegardés lors de l'utilisation de l'option de sauvegarde complète sont répertoriés dans le tableau.

Répertoire

Sous-répertoire ou fichiers

/nsconfig/

- ssl/*
- licence/*
- conseils/*

/var/

- netscaler/ssl/*
- wi/java_home/jre/lib/security/cacerts/*

- wi/java_home/lib/security/cacerts/*

> **Important**
>
> La sauvegarde et la restauration ne fonctionnent pas si CLAG est configuré sur une configuration de cluster SDX.

La sauvegarde est stockée sous forme de fichier TAR compressé dans le répertoire /var/ns_sys_backup/. Pour éviter les problèmes liés à la non-disponibilité de l'espace disque, vous pouvez stocker un maximum de 50 fichiers de sauvegarde dans ce répertoire. Vous pouvez utiliser la commande rm system backup pour supprimer les fichiers de sauvegarde existants afin de pouvoir créer d'autres sauvegardes.

Lorsque vous effectuez l'opération de sauvegarde sur un CLIP d'une configuration de cluster, des fichiers de sauvegarde sont créés sur chacun des nœuds du cluster.

Comment sauvegarder la configuration d'un cluster

Pour sauvegarder la configuration du cluster sur CLIP à l'aide de l'interface de ligne de commande NetScaler.

À l'invite de commandes, procédez comme suit :

- Enregistrez la configuration.

  ```
  save ns config<!--NeedCopy-->
  ```

- Créez le fichier de sauvegarde (de base ou complet).

  "'create system backup [][–level (basic | full)][-comment]

  ```
  1  **Exemple**
  2
  3  ```create system backup cluster-backup-1  -level basic<!--
       NeedCopy-->
  ```

La commande précédente crée un fichier TAR de sauvegarde sur chaque nœud du cluster avec le nom de fichier spécifié. Par exemple, le fichier Cluster-Backup-1.tgz est créé sur chaque nœud du cluster.

> **Remarque**
>
> Si le nom du fichier n'est pas spécifié, des fichiers TAR de sauvegarde sont créés sur chacun des nœuds du cluster selon la convention de dénomination suivante :
>
> - backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp>.tgz<!--NeedCopy-->
> - backup_<level>_<nsip_address of the cluster node 1>_<date-timestamp>.tgz<!--NeedCopy-->

> Par exemple, dans une configuration de cluster à trois nœuds,
>
> - backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp >.tgz<!--NeedCopy--> est créé sur node0
> - backup _<level>_<nsip_address of the cluster node 1>_<date-timestamp >.tgz<!--NeedCopy--> est créé sur node1
> - backup_<level>_<nsip_address of the cluster node 2>_<date-timestamp >.tgz<!--NeedCopy--> est créé sur node2

- Vérifiez les fichiers de sauvegarde créés sur CLIP.

  ```
  show system backup<!--NeedCopy-->
  ```

Restaurer la configuration d'un cluster

Lorsqu'un nœud de cluster devient défectueux, vous pouvez le remplacer par un nouveau nœud. Vous pouvez définir le nouveau nœud pour un cluster à l'aide d'un fichier de sauvegarde du nœud défectueux.

Par exemple, dans une configuration de cluster à trois nœuds, si le nœud 1 devient défectueux, vous pouvez le remplacer par un nouveau nœud en tant que nœud 1. À l'aide de l'opération de restauration, vous pouvez restaurer l'un des fichiers de sauvegarde du nœud défectueux sur le nouveau nœud.

> **Remarque**
>
> L'opération de restauration échoue si le fichier de sauvegarde est renommé ou si le contenu du fichier est modifié.

Comment restaurer un nœud de cluster

Pour restaurer un nœud de cluster à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

- Obtenez la liste des fichiers de sauvegarde disponibles sur CLIP.

  ```
  show system backup<!--NeedCopy-->
  ```

- Copiez le fichier tar de sauvegarde dans le répertoire /var/ns_sys_backup du nœud du cluster, qui doit être restauré.
- Ajoutez le fichier tar de sauvegarde à la mémoire du nœud du cluster en exécutant la commande suivante sur le nœud du cluster.

  "'add system backup

  ```
  1  **Exemple**
  2
  ```



```
3  ```add system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
```

> **Remarque**
>
> La commande doit être exécutée sur le nœud de cluster pour être restaurée.

- Restaurez le nœud du cluster en spécifiant le fichier de sauvegarde.

  “‘restore system backup

```
1  **Exemple**
2
3  ```restore system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
```

> **Remarque**
>
> La commande doit être exécutée sur le nœud de cluster pour être restaurée.

- Redémarrez le nœud du cluster.

  reboot

> **Remarque**
>
> La commande doit être exécutée sur le nœud de cluster pour être restaurée.

Mise à niveau ou rétrogradation du cluster NetScaler

May 5, 2023

Tous les nœuds d’un cluster NetScaler doivent exécuter la même version logicielle. Par conséquent, pour mettre à niveau ou rétrograder le cluster, vous devez mettre à niveau ou rétrograder chaque appliance NetScaler du cluster, un nœud à la fois.

Un nœud en cours de mise à niveau ou de rétrogradation n’est pas supprimé du cluster. Le nœud fait toujours partie du cluster et dessert le trafic sans interruption, à l’exception du temps d’arrêt lorsque le nœud redémarre après sa mise à niveau ou sa rétrogradation.

Toutefois, en raison de l’incompatibilité des versions logicielles entre les nœuds du cluster, la propagation de la configuration est désactivée sur le cluster. La propagation de la configuration n’est activée que lorsque tous les nœuds du cluster sont de la même version. Étant donné que la propagation de la configuration est désactivée lors de la mise à niveau lors de la rétrogradation d’un cluster, vous ne pouvez pas effectuer de configurations via l’adresse IP du cluster pendant cette période.

Important

- Dans une configuration de cluster dont le paramètre global de connexion maximale (MaxConn) est défini sur une valeur différente de zéro, les connexions CLIP peuvent échouer si l'une des conditions suivantes est remplie :

```
- Upgrading the setup from NetScaler 13.0 76.x build to
  NetScaler 13.0 79.x build.
- Restarting the CCO node in a cluster setup running NetScaler
   13.0 76.x build.
```

Solutions :

```
\- Avant de mettre à niveau une configuration de cluster
   depuis la version NetScaler 13.0 76.x vers la version
   NetScaler 13.0 79.x, le paramétre global de connexion
   maximale (MaxConn) doit être défini sur zéro. Aprés la mise
   à niveau de la configuration, vous pouvez définir le paramé
   tre MaxConn sur la valeur souhaitée, puis enregistrer la
   configuration.
\- La version  NetScaler 13.0 76.x n'est pas adaptée aux
   configurations de clusters. Citrix recommande de ne pas
   utiliser la version NetScaler 13.0 76.x pour la
   configuration d'un cluster.
```

- Dans une configuration en cluster, une appliance NetScaler peut tomber en panne lorsque :

```
- upgrading the setup from NetScaler 13.0 47.x or 13.0 52.x
  build to a later build, or
- upgrading the setup to NetScaler 13.0 47.x or 13.0 52.x
  build
```

Solution : Pendant le processus de mise à niveau, effectuez les opérations suivantes :

```
\- Désactivez tous les nœuds de cluster, puis mettez à niveau
   chaque nœud de cluster.
\- Activez tous les nœuds de cluster aprés la mise à niveau de
    tous les nœuds.
```

Points à noter avant de mettre à niveau ou de rétrograder le cluster

- **IMPORTANT :**

  Il est important que les modifications de mise à niveau et vos personnalisations soient ap-

> pliquées à une appliance NetScaler mise à niveau. Par conséquent, si vous avez des fichiers de configuration personnalisés dans le répertoire `/etc`, consultez Considérations relatives à la mise à niveau pour les fichiers de configuration personnalisés avant de procéder à la mise à niveau.

- Vous ne pouvez pas ajouter de nœuds de cluster pendant la mise à niveau ou la rétrogradation de la version logicielle
- Vous pouvez effectuer des configurations au niveau des nœuds via l'adresse NSIP des nœuds individuels. Veillez à effectuer les mêmes configurations sur tous les nœuds pour les maintenir synchronisés.
- Vous ne pouvez pas exécuter la commande `start nstrace` à partir de l'adresse IP du cluster lors de la mise à niveau du cluster. Toutefois, vous pouvez obtenir la trace de nœuds individuels en effectuant cette opération sur des nœuds de cluster individuels à l'aide de leur adresse NSIP.
- La version NetScaler 13.0 76.x n'est pas adaptée aux configurations de clusters. Citrix recommande de ne pas utiliser la version NetScaler 13.0 76.x pour la configuration d'un cluster.
- Les versions NetScaler 13.0 47.x et 13.0 52.x ne conviennent pas à une configuration en cluster. C'est parce que les communications inter-nœuds ne sont pas compatibles dans ces versions.
- Lorsqu'un cluster est mis à niveau, il est possible que certaines fonctionnalités supplémentaires soient activées sur les nœuds mis à niveau qui ne sont pas encore disponibles sur les nœuds qui ne sont pas encore mis à niveau. Cela entraîne un avertissement de non-correspondance des licences pendant la mise à niveau du cluster. Cet avertissement est automatiquement résolu lorsque tous les nœuds du cluster sont mis à niveau.

> **Important**
>
> - Citrix vous recommande d'attendre que le nœud précédent soit actif avant de mettre à niveau ou de rétrograder le nœud suivant.
> - Citrix recommande que le nœud de configuration du cluster soit mis à niveau/rétrogradé en dernier pour éviter de multiples déconnexions des sessions IP du cluster.

Pour mettre à niveau ou rétrograder le logiciel des nœuds de cluster

1. Assurez-vous que le cluster est stable et que les configurations sont synchronisées sur tous les nœuds.
2. Accédez à chaque nœud via son adresse NSIP et effectuez les opérations suivantes :
   - Mettez à niveau ou rétrogradez le nœud du cluster. Pour obtenir des informations détaillées sur la mise à niveau et la rétrogradation du logiciel d'une appliance, consultez Mettre à niveau et rétrograder une appliance NetScaler.
   - Enregistrez les configurations.

- Redémarrez l'appliance.

3. Répétez l'étape 2 pour chacun des autres nœuds de cluster.

Opérations prises en charge sur des nœuds de cluster individuels

May 5, 2023

En règle générale, les appliances NetScaler qui font partie d'un cluster ne peuvent pas être configurées individuellement à partir de leur adresse NSIP. Certaines opérations font toutefois exception à cette règle. Ces opérations, lorsqu'elles sont exécutées à partir de l'adresse NSIP, ne sont pas propagées vers d'autres nœuds du cluster.

Les opérations sont les suivantes :

- instance de cluster (définir | rm | activer | désactiver)
- nœud de cluster (set | rm)
- ns trace (démarrer | afficher | arrêter)
- interface (définir | activer | désactiver)
- itinéraire (ajouter | rm | définir | annuler)
- ARP (ajouter | rm | tout envoyer)
- forcer la synchronisation du cluster
- synchroniser les fichiers du cluster
- désactiver la synchronisation NTP
- save ns config
- reboot
- fermer

Par exemple, lorsque vous exécutez la commande `disable interface 1/1/1` à partir de l'adresse NSIP d'un nœud de cluster, l'interface est désactivée uniquement sur ce nœud. Comme la commande n'est pas propagée, l'interface 1/1/1 reste activée sur tous les autres nœuds de cluster.

Prise en charge des clusters hétérogènes

May 5, 2023

L'appliance NetScaler prend en charge un cluster hétérogène dans le cadre d'un déploiement de clusters. Un cluster hétérogène couvre des nœuds de différents matériels NetScaler et vous pouvez avoir une combinaison de différentes plateformes dans le même cluster.

> **Important**
>
> La formation ou la prise en charge d'un cluster hétérogène sont possibles et limitées uniquement aux plateformes matérielles MPX.

La prise en charge et la formation du cluster hétérogène dépendent de certains modèles NetScaler. Le tableau suivant répertorie les plateformes prises en charge pour la formation d'un cluster hétérogène, avec un nombre égal de moteurs de paquets.

Nombre de moteurs de paquets	Plateformes matérielles MPX	Plateformes matérielles MPX prises en charge pour former un cluster hétérogène
5	MPX 11500	MPX 14020
7	MPX 11515	MPX 14040
9	MPX 11530	MPX 14060

Le tableau suivant répertorie les plateformes prises en charge dans la formation d'un cluster hétérogène, avec un nombre inégal de moteurs de paquets.

Plates-formes matérielles	Plateformes matérielles prises en charge pour former un cluster hétérogène
MPX 150XX	MPX 140XX

Pour plus d'informations sur la manière de former un déploiement en cluster hétérogène d'appliances NetScaler MPX avec un nombre différent de moteurs de paquets sur différents chipsets SSL, consultez la section **Déploiements de clusters hétérogènes dans Configuration** du déchargement SSL.

> **Remarque**
>
> Avant la version 13.0 build 47.x, si vous exécutez la commande « jointure cluster » à partir du nœud qui a un nombre inégal de moteurs de paquets, le message d'erreur suivant s'affiche : « Incompatibilité dans le nombre de PPE actifs entre CCO et nœud local ».

Points à noter

1. Le paramètre du processeur de gestion supplémentaire doit être identique sur tous les nœuds du cluster.

2. Le nœud nouvellement ajouté doit avoir la même capacité sur les plans de données et le fond de panier que celle des nœuds de cluster existants.
3. S'il existe des périphériques de plates-formes mixtes prenant en charge différents chiffrements, alors le cluster se mettrait d'accord sur une liste de chiffrement commune.

FAQ

May 8, 2023

Liste des FAQ sur le clustering.

Combien d'appliances NetScaler peuvent être incluses dans un seul cluster NetScaler ?

Un cluster NetScaler peut inclure une appliance ou jusqu'à 32 appliances matérielles ou virtuelles NetScaler nCore. Chacun de ces nœuds doit satisfaire aux critères spécifiés dans Prérequis pour les nœuds de cluster.

Une appliance NetScaler peut-elle faire partie de plusieurs clusters ?

Non. Une appliance NetScaler ne peut appartenir qu'à un seul cluster.

Qu'est-ce qu'une adresse IP de cluster ? Quel est son masque de sous-réseau ?

L'adresse IP du cluster est l'adresse de gestion d'un cluster NetScaler. Toutes les configurations de cluster doivent être effectuées en accédant au cluster via cette adresse. Le masque de sous-réseau de l'adresse IP du cluster est fixé à 255.255.255.255.

Comment puis-je créer un nœud de cluster spécifique en tant que coordinateur de configuration du cluster ?

Pour définir manuellement un nœud spécifique en tant que coordinateur de configuration du cluster, vous devez définir la priorité de ce nœud sur la valeur numérique la plus faible (priorité la plus élevée). Pour comprendre, considérons un cluster à trois nœuds qui ont les priorités suivantes :

n1 - 29, n2 - 30, n3 - 31

Ici, n1 est le coordinateur de configuration. Si vous souhaitez faire de n2 le coordinateur de configuration, vous devez définir sa priorité sur une valeur inférieure à n1, par exemple 28. Lors de l'enregistrement de la configuration, n2 devient le coordinateur de configuration.

> **Remarque**
>
> n2 avec sa valeur de priorité initiale de 30 devient le coordinateur de configuration lorsque n1 tombe en panne. Le nœud ayant la valeur de priorité la plus basse suivante est sélectionné en cas de panne du coordinateur de configuration.

Pourquoi les interfaces réseau d'un cluster sont-elles représentées en notation à 3 tuples (n/u/c) au lieu de la notation normale à 2 tuples (u/c) ?

Lorsqu'une appliance NetScaler fait partie d'un cluster, vous devez être en mesure d'identifier le nœud auquel appartient l'interface. Par conséquent, la convention de dénomination de l'interface réseau pour les nœuds du cluster est modifiée de u/c à n/u/c, où n désigne l'identifiant du nœud.

Comment définir le nom d'hôte d'un nœud de cluster ?

Le nom d'hôte d'un nœud de cluster doit être spécifié en exécutant la commande **set ns hostname** via l'adresse IP du cluster. Par exemple, pour définir le nom d'hôte du nœud de cluster avec l'ID 2, la commande est la suivante :

définir le nom d'hôte ns HostName1- OwnerNode 2

Puis-je détecter automatiquement les appliances NetScaler afin de les ajouter à un cluster ?

Oui. L'utilitaire de configuration vous permet de découvrir les appliances présentes dans le même sous-réseau que l'adresse NSIP du coordinateur de configuration. Pour plus d'informations, voir Découvrir les appliances NetScaler.

La capacité de service de trafic d'un cluster est-elle affectée si un nœud est supprimé ou désactivé, redémarré ou arrêté ou rendu inactif ?

Oui. Lorsque l'une de ces opérations est effectuée sur un nœud actif du cluster, le cluster dispose d'un nœud de moins pour acheminer le trafic. Les connexions existantes sur ce nœud sont également interrompues.

J'ai plusieurs appliances autonomes, chacune ayant des configurations différentes. Puis-je les ajouter à un seul cluster ?

Oui. Vous pouvez ajouter des appliances ayant des configurations différentes à un seul cluster. Toutefois, lorsque l'appliance est ajoutée au cluster, les configurations existantes sont effacées. Pour utiliser les configurations disponibles sur chaque appliance individuelle, vous devez :

1. Créez un seul fichier*.conf pour toutes les configurations.
2. Modifiez le fichier de configuration pour supprimer les fonctionnalités qui ne sont pas prises en charge dans un environnement de cluster.
3. Mettez à jour la convention de dénomination des interfaces du format à 2 tuples (u/c) au format à 3 tuples (n/u/c).
4. Appliquez les configurations au nœud coordinateur de configuration du cluster à l'aide de la commande batch .

Puis-je migrer les configurations d'une appliance NetScaler autonome ou d'une configuration HA vers la configuration en cluster ?

Non. Lorsqu'un nœud est ajouté à une configuration en cluster, ses configurations sont implicitement effacées à l'aide de la commande **clear ns config** (avec l'option **étendue**). De plus, les adresses SNIP et toutes les configurations VLAN (à l'exception du VLAN et du NSVLAN par défaut) sont effacées. Il est donc recommandé de sauvegarder les configurations avant d'ajouter l'appliance à un cluster. Avant d'utiliser le fichier de configuration sauvegardé pour le cluster, vous devez :

1. Modifiez le fichier de configuration pour supprimer les fonctionnalités qui ne sont pas prises en charge dans un environnement de cluster.
2. Mettez à jour la convention de dénomination des interfaces du format à deux tuples (x/y) au format à trois tuples (x/y/z).
3. Appliquez les configurations au nœud coordinateur de configuration du cluster à l'aide de la commande **batch** .

Les interfaces de fond de panier font-elles partie des VLAN L3 ?

Oui, par défaut, les interfaces de fond de panier sont présentes sur tous les VLAN L3 configurés sur le cluster.

Comment configurer un cluster qui inclut des nœuds provenant de différents réseaux ?

> **Remarque**
>
> Pris en charge à partir de NetScaler 11.0.

Un cluster qui inclut des nœuds provenant de différents réseaux est appelé cluster L3 (parfois appelé cluster en mode INC). Dans un cluster L3, tous les nœuds appartenant à un réseau unique doivent être regroupés dans un seul groupe de nœuds. Par conséquent, si un cluster comprend deux nœuds provenant chacun de trois réseaux différents, vous devez créer 3 groupes de nœuds (un pour chaque réseau) et associer chacun de ces groupes de nœuds aux nœuds appartenant à ce réseau. Pour plus d'informations sur la configuration, consultez les étapes de configuration d'un cluster.

Comment puis-je configurer/déconfigurer le NSVLAN sur un cluster ?

Procédez de l'une des manières suivantes :

- Pour rendre le NSVLAN disponible dans un cluster, assurez-vous que le même NSVLAN est configuré sur chaque appliance avant de l'ajouter à un cluster.
- Pour supprimer le NSVLAN d'un nœud de cluster, commencez par supprimer le nœud du cluster, puis supprimez le NSVLAN de l'appliance.

J'ai configuré un cluster dans lequel certains nœuds NetScaler ne sont pas connectés au réseau externe. Le cluster peut-il toujours fonctionner normalement ?

Oui. Le cluster prend en charge un mécanisme appelé linksets, qui permet aux nœuds non connectés de servir le trafic en utilisant les interfaces des nœuds connectés. Les nœuds non connectés communiquent avec les nœuds connectés via le backplane du cluster. Pour plus d'informations, voir Utilisation de jeux de liens.

Comment les déploiements nécessitant le transfert basé sur Mac (MBF) peuvent-ils être pris en charge dans une configuration en cluster ?

Les déploiements qui utilisent MBF doivent utiliser des jeux de liens. Pour plus d'informations, voir Utilisation de jeux de liens.

Puis-je exécuter des commandes à partir de l'adresse NSIP d'un nœud de cluster ?

Non. L'accès à des nœuds de cluster individuels via les adresses NSIP est en lecture seule. Par conséquent, lorsque vous vous connectez à l'adresse NSIP d'un nœud de cluster, vous ne pouvez consulter que les configurations et les statistiques. Vous ne pouvez rien configurer. Toutefois, il existe certaines opérations que vous pouvez exécuter à partir de l'adresse NSIP d'un nœud de cluster. Pour plus d'informations, voir Opérations prises en charge sur des nœuds individuels.

Puis-je désactiver la propagation de la configuration entre les nœuds de cluster ?

Non, vous ne pouvez pas désactiver explicitement la propagation des configurations de cluster entre les nœuds de cluster. Toutefois, lors d'une mise à niveau ou d'une rétrogradation logicielle, une erreur d'incompatibilité de version peut automatiquement désactiver la propagation de la configuration.

Puis-je modifier l'adresse NSIP ou le NSVLAN d'une appliance NetScaler lorsqu'elle fait partie du cluster ?

Non. Pour effectuer de telles modifications, vous devez d'abord supprimer l'appliance du cluster, effectuer les modifications, puis ajouter l'appliance au cluster.

Le cluster NetScaler prend-il en charge les VLAN L2 et L3 ?

Oui. Un cluster prend en charge les VLAN entre les nœuds du cluster. Les VLAN doivent être configurés sur l'adresse IP du cluster.

- **VLAN L2.** Vous pouvez créer un VLAN de couche 2 en liant des interfaces appartenant à différents nœuds du cluster.
- **VLAN L3.** Vous pouvez créer un VLAN de couche 3 en liant des adresses IP appartenant à différents nœuds du cluster. Les adresses IP doivent appartenir au même sous-réseau. Assurez-vous que l'un des critères suivants est satisfait. Sinon, les liaisons VLAN L3 peuvent échouer.
  - Tous les nœuds ont une adresse IP sur le même sous-réseau que celui lié au VLAN.
  - Le cluster possède une adresse IP par bandes et le sous-réseau de cette adresse IP est lié au VLAN.

Lorsque vous ajoutez un nœud à un cluster qui ne possède que des adresses IP repérées, la synchronisation se produit avant que les adresses IP repérées ne soient attribuées à ce nœud. Dans de tels cas, les liaisons VLAN L3 peuvent être perdues. Pour éviter cette perte, ajoutez une adresse IP par bandes ou ajoutez les liaisons VLAN L3 sur le NSIP du nœud nouvellement ajouté.

Comment configurer le SNMP sur un cluster NetScaler ?

Le protocole SNMP surveille le cluster et tous les nœuds du cluster de la même manière qu'il surveille un dispositif autonome. La seule différence est que le protocole SNMP d'un cluster doit être configuré via l'adresse IP du cluster. Lors de la génération d'interruptions spécifiques au matériel, deux varbinds supplémentaires sont inclus pour identifier le nœud du cluster : l'ID du nœud et l'adresse NSIP du nœud.

Quels détails dois-je disposer lorsque je contacte le support technique pour des problèmes liés au cluster ?

L'appliance NetScaler fournit une commande de **cluster show techsupport -scope** qui extrait les données de configuration, les informations statistiques et les journaux de tous les nœuds du cluster. Exécutez cette commande sur l'adresse IP du cluster.

*La sortie de cette commande est enregistrée dans un fichier nommé*collector_cluster_ _P_ .tar.gz qui est disponible dans le répertoire /var/tmp/support/cluster/*du coordinateur de configuration.* <nsip_CCO><date-timestamp>

Envoyez cette archive à l'équipe d'assistance technique pour résoudre le problème.

Puis-je utiliser des adresses IP réparties par bandes comme passerelle par défaut des serveurs ?

Dans les déploiements de clusters, assurez-vous que la passerelle par défaut du serveur pointe vers une adresse IP agrégée par bandes (si vous utilisez une adresse IP appartenant à Netscaler). Par exemple, dans le cas de déploiements LB avec l'USIP activé, la passerelle par défaut doit être une adresse SNIP entrelacée.

Puis-je consulter les configurations de routage d'un nœud de cluster spécifique à partir de l'adresse IP du cluster ?

Oui. Vous pouvez afficher et effacer les configurations spécifiques à un nœud en spécifiant le nœud propriétaire lors de l'accès au shell VTYSH.

Par exemple, pour afficher la sortie d'une commande sur les nœuds 0 et 1, la commande est la suivante :

```
\> vtysh
ns# owner-node 0 1
ns(node-0 1)\# show cluster state
ns(node-0 1)\# exit-cluster-node
ns\#
```

Comment puis-je spécifier le nœud pour lequel je veux définir la priorité système LACP ?

> **Remarque**
>
> Pris en charge à partir de NetScaler 10.1.

Dans un cluster, vous devez définir ce nœud comme nœud propriétaire à l'aide de la commande **set lacp** .

Par exemple,pour définir la priorité du système LACP pour un nœud dont l'ID est 2 :

```
set lacp -sysPriority 5 -ownerNode 2<!--NeedCopy-->
```


Comment les tunnels IP sont-ils configurés dans une configuration de cluster ?

> **Remarque**
>
> Pris en charge à partir de NetScaler 10.1.

La configuration des tunnels IP dans un cluster est la même que sur une appliance autonome. La seule différence est que dans une configuration de cluster, l'adresse IP locale doit être une adresse SNIP entrelacée.

Comment ajouter un ensemble d'interfaces de basculement (FIS) sur les nœuds d'un cluster NetScaler ?

> **Remarque**
>
> Pris en charge à partir de NetScaler 10.5.

Sur l'adresse IP du cluster, spécifiez l'ID du nœud de cluster sur lequel le FIS doit être ajouté, à l'aide de la commande suivante :

```
add fis <name> -ownerNode <nodeId>
```

> **Remarques**
>
> - Le nom FIS de chaque nœud de cluster doit être unique.
> - Un canal LA de cluster peut être ajouté à un FIS. Assurez-vous que le canal LA du cluster dispose d'une interface locale en tant qu'interface membre.

Pour plus d'informations sur FIS, voir Configuration du jeu d'interfaces de basculement.

Comment les profils réseau sont-ils configurés dans une configuration de cluster ?

> **Remarque**
>
> Pris en charge à partir de NetScaler 10.5.

Vous pouvez associer les adresses IP repérées à un profil réseau. Ce profil réseau peut ensuite être lié à un serveur ou à un service virtuel d'équilibrage de charge repéré (défini à l'aide d'un groupe de nœuds). Les recommandations suivantes doivent être suivies, faute de quoi les configurations du profil réseau ne sont pas respectées et les paramètres USIP/USNIP sont utilisés :

> **Remarque**
>
> - Si le paramètre **strict** du groupe de nœuds est défini sur **Oui**, le profil réseau doit contenir au moins une adresse IP de chaque membre du groupe de nœuds.
> - Si le paramètre **strict** du groupe de nœuds est défini sur **Non**, le profil réseau doit inclure au moins une adresse IP de chacun des nœuds du cluster.

Comment puis-je configurer WionNS dans une configuration de cluster ?

> **Remarque**
>
> Pris en charge à partir de NetScaler 11.0 Build 62.x.

Pour utiliser WionNS sur un cluster, vous devez effectuer les opérations suivantes :

1. Assurez-vous que le package Java et le package WI se trouvent dans le même répertoire sur tous les nœuds du cluster.
2. Créez un serveur virtuel d'équilibrage de charge dont la persistance est configurée.
3. Créez des services avec des adresses IP comme adresse NSIP de chacun des nœuds du cluster auxquels vous souhaitez acheminer le trafic Wi-Fi. Cette étape ne peut être configurée qu'à l'aide de l'interface de ligne de commande NetScaler.
4. Liez les services au serveur virtuel d'équilibrage de charge.

> **Remarque**
>
> Si vous utilisez WionNS via une connexion VPN, assurez-vous que le serveur virtuel d'équilibrage de charge est défini comme WIHOME.

Le canal LA du cluster peut-il être utilisé pour l'accès de gestion ?

Non. L'accès de gestion à un nœud de cluster ne doit pas être configuré sur un canal LA du cluster (par exemple, CLA/1) ou sur ses interfaces membres. En effet, lorsque le nœud est INACTIF, l'interface LA du cluster correspondante est marquée comme étant hors tension et perd donc l'accès à la gestion.

Comment les nœuds du cluster communiquent-ils entre eux et quels sont les différents types de trafic qui transitent par le backplane ?

Un backplane est un ensemble d'interfaces dans lequel une interface de chaque nœud est connectée à un commutateur commun, appelé commutateur de fond de cluster. Les différents types de trafic qui transitent par un fond de panier utilisé par la communication entre nœuds sont les suivants :

- Messagerie nœud à nœud (NNM)
- Trafic dirigé
- Propagation et synchronisation de la configuration

Chaque nœud du cluster utilise une adresse de commutateur de fond de cluster MAC spéciale pour communiquer avec les autres nœuds via le backplane. <cluster_id>Le MAC spécial du cluster est de la forme : **0x02 0x00 0x6F **<cluster _id> <node _id> <reserved>, où se trouve l'ID de l'instance du cluster. <node_id> Il s'agit du numéro de nœud de l'appliance NetScaler ajoutée à un cluster.

> **Remarque**
>
> La quantité de trafic gérée par un backplane représente une charge de processeur négligeable.

Qu'est-ce qui est acheminé via le tunnel GRE pour le cluster de couche 3 ?

Seul le trafic de données dirigé passe par le tunnel GRE. Les paquets sont dirigés via le tunnel GRE vers le nœud de l'autre sous-réseau.

Comment les messages de messagerie nœud à nœud (NNM) et les messages de battement de cœur sont-ils échangés et comment sont-ils acheminés ?

Le NNM, les messages de pulsation et le protocole de cluster ne dirigent pas le trafic. Ces messages ne sont pas envoyés via le tunnel, mais ils sont acheminés directement.

Quelles sont les recommandations du MTU pour le trafic tunnelé des clusters de couche 3 ?

Voici les recommandations relatives aux clusters de couche 3 du tunnel Jumbo MTU sur GRE :

- Le MTU Jumbo peut être configuré entre les nœuds du cluster le long du chemin L3 pour s'adapter à la surcharge du tunnel GRE.
- La fragmentation ne se produit pas pour les paquets de taille normale qui doivent être dirigés.
- La gestion du trafic continue de fonctionner même si les cadres Jumbo ne sont pas autorisés, mais avec une surcharge accrue en raison de la fragmentation.

Comment la clé de hachage globale est-elle générée et partagée entre tous les nœuds ?

Le `rsskey` pour un dispositif autonome est généré au moment du démarrage. Dans une configuration de cluster, le premier nœud contient le `rsskey` cluster. Chaque nouveau nœud rejoignant le cluster synchronise le `rsskey`.

Quel est le besoin d'une `set rsskeytype -rsskey symmetric` commande pour * : *, USIP activé, `useproxyport` désactivé, topologies ?

Il n'est pas spécifique à un cluster, mais s'applique également à une appliance autonome. Lorsque l'USIP est activé et que l'utilisation du port proxy est désactivée, Symetric `rsskey` réduit à la fois le pilotage Core to Core (C2C) et le pilotage nœud à nœud.

Quels sont les facteurs qui contribuent à modifier le nœud CCO ?

Le premier nœud ajouté pour former une configuration de cluster devient le nœud de coordinateur de configuration (CCO). Les facteurs suivants contribuent à modifier le nœud CCO dans la configuration du cluster :

- Lorsque le nœud CCO actuel est supprimé de la configuration du cluster
- Lorsque le nœud CCO actuel se bloque
- Lorsque la priorité du nœud non-CCO est modifiée (une priorité plus faible a une priorité plus élevée)
- Dans des conditions dynamiques telles que l'accessibilité du réseau entre les nœuds
- En cas de modification de l'état des nœuds : actif, de réserve et passif. Les nœuds actifs sont préférés en tant que CCO.
- Lorsqu'il y a un changement de configuration et que le nœud ayant la dernière configuration est préféré en tant que CCO.

Résolution des problèmes liés au cluster NetScaler

May 5, 2023

En cas de panne dans un cluster NetScaler, la première étape du dépannage consiste à obtenir des informations sur l'instance du cluster. Vous pouvez obtenir les informations en exécutant les `show cluster node nodeId` commandes `show cluster instance clId` et sur les nœuds du cluster respectivement.

Si vous ne parvenez pas à trouver le problème à l'aide des deux approches ci-dessus, vous pouvez utiliser l'une des méthodes suivantes :

- **Isolez la source de la panne.** Essayez de contourner le cluster pour accéder au serveur. Si la tentative aboutit, le problème vient probablement de la configuration du cluster.
- **Vérifiez les commandes récemment exécutées.** Exécutez la commande history pour vérifier les configurations récentes effectuées sur le cluster. Vous pouvez également consulter le fichier ns.conf pour vérifier les configurations qui ont été mises en œuvre.
- **Vérifiez les fichiers ns.log.** Utilisez les fichiers journaux, disponibles dans le répertoire /var/log/ de chaque nœud, pour identifier les commandes exécutées, l'état des commandes et les changements d'état.
- **Vérifiez les nouveaux fichiers slog.** Utilisez les `newnslog` fichiers disponibles dans le répertoire /var/nslog/ de chaque nœud pour identifier les événements qui se sont produits sur les nœuds du cluster. Vous pouvez afficher plusieurs fichiers `newnslog` sous la forme d'un seul fichier, en copiant les fichiers dans un seul répertoire, puis en exécutant la commande suivante :


```
nsconmsg -K newnslog-node<id> -K     newnslog.node<id> -d current
```

Si vous ne parvenez toujours pas à résoudre le problème, vous pouvez essayer de suivre les paquets sur le cluster ou utiliser la `techsupport -scope cluster` commande show. Vous pouvez utiliser la commande pour envoyer le rapport à l'équipe de support technique.

Suivi des paquets d'un cluster NetScaler

May 8, 2023

Le système d'exploitation NetScaler fournit un utilitaire appelé *ns trace* qui permet d'obtenir un vidage des paquets reçus et envoyés par une appliance. L'utilitaire stocke les paquets dans des fichiers de suivi. Vous pouvez utiliser ces fichiers pour résoudre les problèmes liés au flux de paquets vers les nœuds du cluster. Les fichiers de trace doivent être visualisés avec l'application Wireshark.

Les principaux aspects de l'utilitaire ns trace sont les suivants :

- Peut être configuré pour tracer les paquets de manière sélective à l'aide d'expressions classiques et d'expressions par défaut.
- Peut capturer la trace dans plusieurs formats : format ns trace (.cap) et format de dump TCP (.pcap).
- Peut agréger les fichiers de trace de tous les nœuds du cluster sur le coordinateur de configuration.
- Peut fusionner plusieurs fichiers de trace en un seul fichier de trace (uniquement pour les fichiers .cap).

Vous pouvez utiliser l'utilitaire ns trace à partir de la ligne de commande NetScaler ou du shell NetScaler.

Pour suivre les paquets d'une appliance autonome

Exécutez la commande start ns trace sur l'appliance. <date-timestamp>La commande crée des fichiers de trace dans le répertoire /var/nstrace/. <id>Les noms des fichiers de trace sont de la forme nstrace.cap.

Vous pouvez consulter l'état en exécutant la commande show ns trace. Vous pouvez arrêter le traçage des paquets en exécutant la commande stop ns trace.

> **Remarque**
>
> Vous pouvez également exécuter l'utilitaire ns trace à partir du shell NetScaler en exécutant le fichier nstrace.sh. Il est toutefois recommandé d'utiliser l'utilitaire ns trace via l'interface de ligne

> de commande NetScaler.

Pour suivre les paquets d'un cluster

Vous pouvez suivre les paquets sur tous les nœuds du cluster et obtenir tous les fichiers de suivi sur le coordinateur de configuration.

Exécutez la commande start ns trace sur l'adresse IP du cluster. La commande est propagée et exécutée sur tous les nœuds du cluster. Les fichiers de trace sont stockés dans des nœuds de cluster individuels du répertoire /var/nstrace/<date-timestamp> . <id>Les noms des fichiers de trace sont de la forme nstrace \ \ <id> _node \.cap.

Vous pouvez utiliser les fichiers de trace de chaque nœud pour déboguer les opérations des nœuds. Toutefois, si vous souhaitez que les fichiers de trace de tous les nœuds du cluster soient regroupés au même endroit, vous devez exécuter la commande stop ns trace sur l'adresse IP du cluster. Les fichiers de trace de tous les nœuds sont téléchargés sur le coordinateur de configuration du cluster dans le répertoire<date-timestamp> /var/nstrace/ comme suit :



Fusionner plusieurs fichiers de trace

Vous pouvez préparer un seul fichier à partir des fichiers de trace (pris en charge uniquement pour. Fichiers Cap) obtenus à partir des nœuds du cluster. Les fichiers de trace uniques vous offrent une vue cumulée de la trace des paquets du cluster. Les entrées de trace du fichier de trace unique sont triées en fonction de l'heure à laquelle les paquets ont été reçus sur le cluster.

Pour fusionner les fichiers de trace, dans le shell NetScaler, tapez :

```
1 > nstracemerge.sh -srcdir \<DIR\> -dstdir \<DIR\> -filename \<name\> -
     filesize \<num\>
```

Où,

- `srcdir` est le répertoire à partir duquel les fichiers de trace sont fusionnés. Tous les fichiers de trace de ce répertoire sont fusionnés en un seul fichier.
- `dstdir` est le répertoire dans lequel le fichier de trace fusionné est créé.
- `Filename` est le nom du fichier de trace créé.
- `Filesize` est la taille du fichier de trace.

Exemples

Vous trouverez ci-dessous quelques exemples d'utilisation de l'utilitaire ns trace pour filtrer les paquets.

- Pour suivre les paquets sur les interfaces de backplane de trois nœuds :

  À l'aide d'expressions classiques :

  ```
  1 > start nstrace -filter "INTF == 0/1/1 && INTF == 1/1/1 && INTF
       == 2/1/1"
  ```

  À l'aide d'expressions par défaut :

  ```
  1 > start nstrace -filter "CONNECTION.INTF.EQ("0/1/1") &&
       CONNECTION.INTF.EQ("1/1/1") && CONNECTION.INTF.EQ("2/1/1")"
  ```

- Pour suivre les paquets à partir d'une adresse IP source 10.102.34.201 ou d'un système dont le port source est supérieur à 80 et dont le nom de service n'est pas « s1 » :

  Utilisation d'expressions classiques

  ```
  1 > start nstrace -filter "SOURCEIP == 10.102.34.201 || (SVCNAME !=
       s1 && SOURCEPORT > 80)"
  ```

  Utilisation d'expressions par défaut


```
> start nstrace -filter "CONNECTION.SRCIP.EQ(10.102.34.201) || (
    CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.GT(80))"
```

> **Remarque**
>
> Pour plus d'informations sur les filtres utilisés dans ns trace, voir ns trace.

Capture des clés de session SSL lors d'une trace

Lorsque vous exécutez la commande « start ns trace », vous pouvez définir le nouveau `capsslkeys` paramètre pour capturer les clés principales SSL pour toutes les sessions SSL. Si vous incluez ce paramètre, un fichier nommé nstrace.sslkeys est généré avec la trace du paquet. Ce fichier peut être importé dans Wireshark pour déchiffrer le trafic SSL dans le fichier de trace correspondant.

Cette fonctionnalité est similaire à celle des navigateurs Web qui exportent des clés de session qui peuvent ensuite être importées dans Wireshark pour déchiffrer le trafic SSL.

Avantages de l'utilisation de clés de session SSL

Les avantages de l'utilisation des clés de session SSL sont les suivants :

1. Génère des fichiers de trace plus petits qui n'incluent pas les paquets supplémentaires créés par le mode de capture SSLPLAIN.
2. Permet de visualiser le texte en clair [SP (1]) à partir de la trace et de choisir de partager le fichier de clés principales ou de protéger les données sensibles en ne le partageant pas.

Limites de l'utilisation des clés de session SSL

Les limites de l'utilisation des clés de session SSL sont les suivantes :

1. Les sessions SSL ne peuvent pas être décryptées si les paquets initiaux de la session ne sont pas capturés.
2. Les sessions SSL ne peuvent pas être capturées si le mode FIPS (Federal Information Processing Standard) est activé.

Pour capturer des clés de session SSL à l'aide de l'interface de ligne de commande (CLI)

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver les clés de session SSL dans un fichier de suivi et vérifier l'opération de suivi.

```
> start nstrace -capsslkeys ENABLED
> show nstrace
Example
```



```
> start nstrace -capsslkeys ENABLED
> show nstrace
      State:  RUNNING          Scope:  LOCAL            TraceLocation:
          "/var/nstrace/04May2016_17_51_54/..."
      Nf:  24                  Time:  3600              Size:  164
                       Mode:  TXB NEW_RX
      Traceformat:  NSCAP      PerNIC:  DISABLED        FileName:  04
         May2016_17_51_54 Link:  DISABLED
      Merge:  ONSTOP           Doruntimecleanup:  ENABLED TraceBuffers:
           5000      SkipRPC:  DISABLED
      SkipLocalSSH:  DISABLED  Capsslkeys:  ENABLED     InMemoryTrace:
          DISABLED
 Done
```

Pour configurer les clés de session SSL à l'aide de l'interface graphique NetScaler

1. Accédez à **Configuration > Système > Diagnostics > Outils de support technique** et cliquez sur **Démarrer un nouveau suivi pour commencer à suivre** les paquets chiffrés sur une appliance.
2. Sur la page **Start Trace**, cochez la case **Capturer les clés principales SSL** .
3. Cliquez sur **OK** et **Terminé**.

Pour importer les clés principales SSL dans Wireshark

Dans l'interface graphique Wireshark, accédez à **Edition > Préférences > Protocoles > SSL > (Pre) -Master-Secret nom du fichier journal** et spécifiez les fichiers de clé principale obtenus à partir de l'appliance.

Résolution des problèmes courants

August 20, 2021

Lors de la jonction d'un nœud au cluster, je reçois le message suivant, "ERREUR : nom/numéro d'interface non valide." Que dois-je faire pour résoudre cette erreur ?

Cette erreur se produit si vous avez fourni une interface de fond de panier non valide ou incorrecte lors de l'utilisation de la commande add cluster node pour ajouter le nœud. Pour résoudre cette erreur, vérifiez l'interface que vous avez fournie lors de l'ajout du nœud. Assurez-vous que vous n'avez pas spécifié l'interface de gestion de l'appliance comme interface de backplane et que le <nodeId> bit de

l'interface est identique à l'ID du nœud. Par exemple, si le NodeID est 3, l'interface du fond de panier doit être 3/<c>/<u>.

Lors de la jonction d'un nœud au cluster, je reçois le message suivant : "ERREUR : Le clustering ne peut pas être activé, car le nœud local n'est pas membre du cluster." Que dois-je faire pour résoudre cette erreur ?

Cette erreur se produit lorsque vous essayez de joindre un nœud sans ajouter le NSIP du nœud au cluster. Pour résoudre cette erreur, vous devez d'abord ajouter l'adresse NSIP du nœud au cluster à l'aide de la commande **add cluster node**, puis exécuter la commande **jointure cluster**.

Lors de la jonction d'un nœud au cluster, je reçois le message suivant, "ERREUR : Connexion refusée." Que dois-je faire pour résoudre cette erreur ?

Cette erreur peut se produire pour les raisons suivantes :

- **Problèmes de connectivité.** Le nœud ne peut pas se connecter à l'adresse IP du cluster. Essayez d'effectuer un ping sur l'adresse IP du cluster à partir du nœud que vous essayez de joindre.
- **Dupliquer l'adresse IP du cluster.** Vérifiez si l'adresse IP du cluster existe sur un nœud non cluster. Si c'est le cas, créez une adresse IP de cluster et essayez de rejoindre le cluster.

En joignant un nœud au cluster, j'obtiens le message suivant, "ERROR: License mismatch between the configuration coordinator and the local node." Que dois-je faire pour résoudre cette erreur ?

L'appliance que vous joignez au cluster doit posséder les mêmes licences que le coordinateur de configuration. Cette erreur se produit lorsque les licences sur le nœud que vous rejoignez ne correspondent pas aux licences sur le coordinateur de configuration. Pour résoudre cette erreur, exécutez les commandes suivantes sur les deux nœuds et comparez les sorties.

À partir de la ligne de commande :

- `show ns hardware`
- `show ns license`

À partir de la coque :

- `nsconmsg -g feature -d stats`
- `ls /nsconfig/license`
- Afficher le contenu du fichier /var/log/license.log

Que dois-je faire lorsque les configurations d'un nœud de cluster ne sont pas synchronisées avec les configurations de cluster ?

Habituellement, les configurations sont automatiquement synchronisées entre tous les nœuds de cluster. Toutefois, si vous pensez que les configurations ne sont pas synchronisées sur un nœud spécifique, vous devez forcer la synchronisation en exécutant la commande forcer cluster sync à partir du nœud que vous souhaitez synchroniser. Pour plus d'informations, consultez Synchronisation des configurations de cluster.

Lors de la configuration d'un nœud de cluster, je reçois le message suivant : "ERREUR : La session est en lecture seule ; connectez-vous à l'adresse IP du cluster pour modifier la configuration."

Toutes les configurations d'un cluster doivent être effectuées via l'adresse IP du cluster et les configurations sont propagées aux autres nœuds de cluster. Toutes les sessions établies via l'adresse NSIP des nœuds individuels sont en lecture seule.

Pourquoi l'état du nœud affiche-t-il « INACTIVE » lorsque l'état du nœud affiche « UP » ?

Un nœud sain peut être dans l'état INACTIF pour diverses raisons. Une analyse du ns.log ou des compteurs d'erreurs peut vous aider à déterminer la raison exacte.

Comment puis-je résoudre la santé d'un nœud lorsque son état affiche « NOT UP » ?

La santé du**nœud "Not UP**" indique qu'il y a des problèmes avec le nœud. Pour connaître la cause première, vous devez exécuter la commande **show cluster node** . Cette commande affiche les propriétés du nœud et la raison de l'échec du nœud.

Que dois-je faire lorsque l'état d'un nœud apparaît comme « NOT UP » et que la raison indique que les commandes de configuration ont échoué sur un nœud ?

Ce problème se produit lorsque certaines commandes ne sont pas exécutées sur les nœuds de cluster. Dans de tels cas, vous devez vous assurer que les configurations sont synchronisées à l'aide de l'une des options suivantes :

- Si certains des nœuds de cluster sont dans cet état, vous devez effectuer l'opération de synchronisation forcée du cluster sur ces nœuds. Pour plus d'informations, consultez Synchronisation des configurations de cluster.
- Si tous les nœuds de cluster sont dans cet état, vous devez désactiver, puis activer l'instance de cluster sur tous les nœuds de cluster.

Lorsque j'exécute la commande set virtual server, j'obtiens le message suivant, « Aucune ressource de ce type.« Que dois-je faire pour résoudre ce problème ?

La commande **set vserver** n'est pas prise en charge dans le clustering. Les commandes **unset vserver, enable vserver, disable vserver** et **rm vserver** ne sont pas non plus prises en charge. Toutefois, la commande **show vserver** est prise en charge.

Je ne peux pas configurer le cluster sur une session Telnet. Que dois-je faire ?

Sur une session telnet, l'adresse IP du cluster est accessible uniquement en mode lecture seule. Par conséquent, vous ne pouvez pas configurer un cluster sur une session telnet.

Je remarque une différence d'heure significative entre les nœuds de cluster. Que dois-je faire pour résoudre ce problème ?

Lorsque des paquets PTP sont supprimés en raison du commutateur de fond de panier ou si les ressources physiques sont surexploitées dans un environnement virtuel, l'heure ne sera pas synchronisée.

Pour synchroniser les heures, vous devez effectuer les opérations suivantes sur l'adresse IP du cluster :

1. Désactivez PTP.

   set ptp -state disable

2. Configurer le protocole NTP (Network Time Protocol) pour le cluster. Pour plus d'informations, voir Configuration de la synchronisation de l'horloge.

Que dois-je faire, s'il n'y a pas de connectivité à l'adresse IP du cluster et à l'adresse NSIP d'un nœud de cluster ?

Si vous ne pouvez pas accéder à l'adresse IP du cluster ou au NSIP d'un nœud de cluster, vous devez accéder à l'appliance via la console série. Si l'adresse NSIP est accessible, vous pouvez SSH vers l'adresse IP du cluster à partir du shell en exécutant la commande suivante à l'invite shell :

"'# ssh nsroot@

```
## Que dois-je faire pour récupérer un nœud de cluster qui a des problé
   mes de connectivité ?

Pour restaurer un nœud qui présente des problémes de connectivité :

1.  Désactivez l'instance de cluster sur ce nœud (car vous ne pouvez
   pas exécuter de commandes à partir du NSIP d'un nœud de cluster).

```



```
1.  Exécutez les commandes requises pour restaurer le nœud.

1.  Activez l'instance de cluster sur ce nœud.

## Certains nœuds du cluster ont deux itinéraires par défaut. Comment
   puis-je supprimer la deuxiéme route par défaut du nœud de cluster ?

Pour supprimer l'itinéraire par défaut supplémentaire, procédez comme
   suit sur chaque nœud qui a l'itinéraire supplémentaire :

1.  Désactivez l'instance de cluster.

    ```disable cluster instance <clId><!--NeedCopy-->
```

1. Retirez l'itinéraire.

   ```
   rm route <network> <netmask> <gateway><!--NeedCopy-->
   ```

2. Activez l'instance de cluster.

   ```
   enable cluster instance <clId><!--NeedCopy-->
   ```

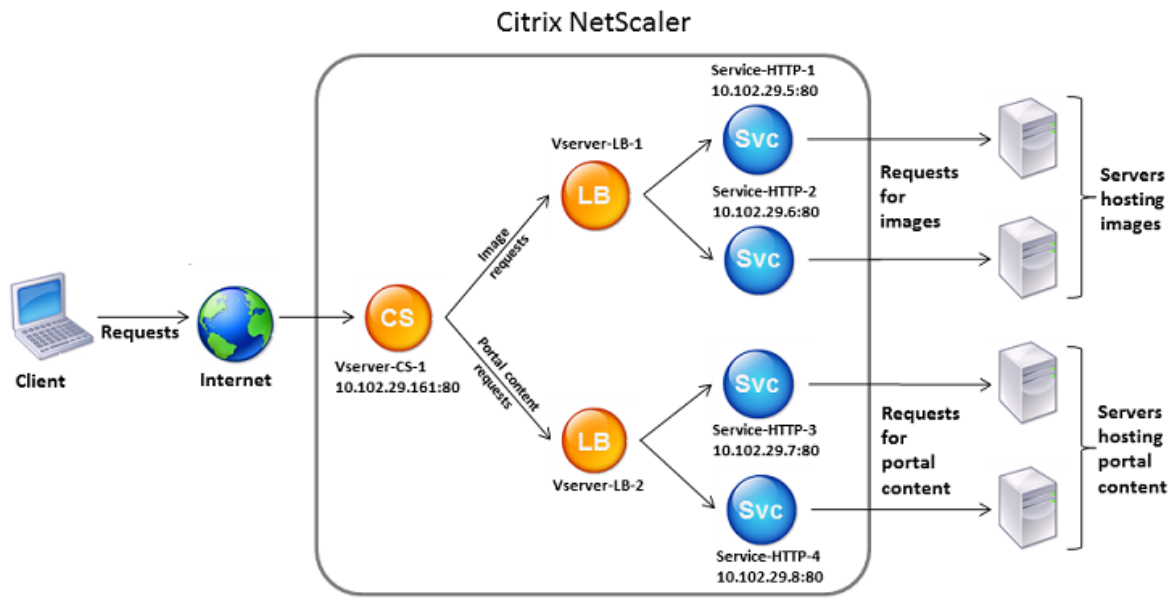
La fonctionnalité de cluster est affectée lorsqu'un nœud de cluster existant est mis en ligne. Que dois-je faire pour résoudre ce problème ?

Si le mot de passe RPC d'un nœud est modifié par rapport à l'adresse IP du cluster lorsque ce nœud est hors du cluster, alors, lorsque le nœud est en ligne, il y a une incompatibilité dans les informations d'identification RPC et peut affecter la fonctionnalité du cluster. Pour résoudre ce problème, utilisez la commande set ns RPCNode pour mettre à jour le mot de passe sur le NSIP du nœud qui est entré en ligne.

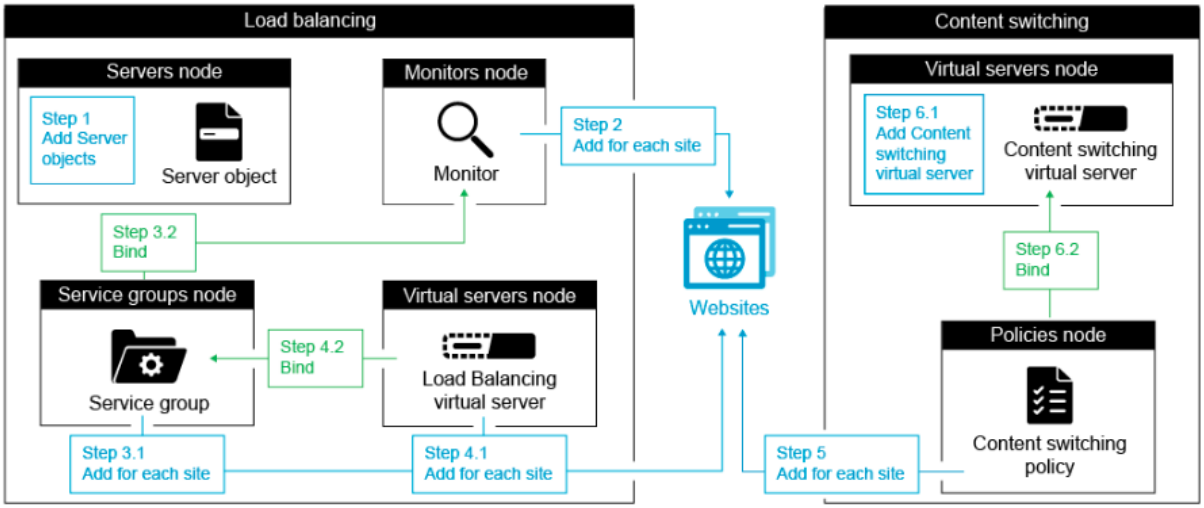
Commutation de contenu

May 5, 2023

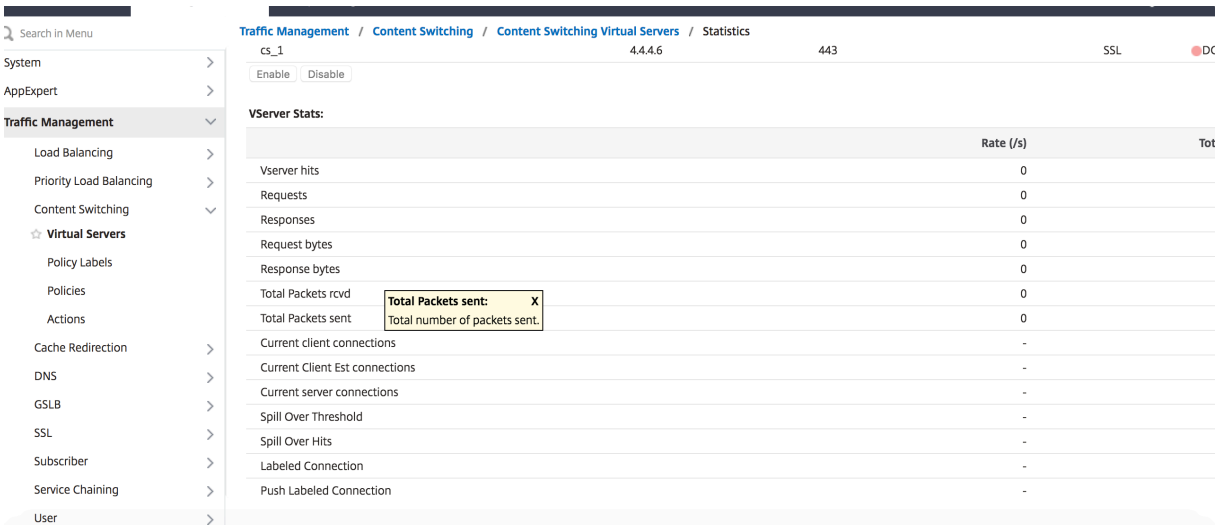
Dans les sites Web complexes d'aujourd'hui, vous souhaiterez peut-être présenter différents contenus à différents utilisateurs. Par exemple, vous pouvez souhaiter autoriser les utilisateurs de la plage d'adresses IP d'un client ou d'un partenaire à accéder à un portail Web spécial. Vous souhaiterez peut-être présenter du contenu pertinent à une zone géographique spécifique aux utilisateurs de cette zone. Vous souhaiterez peut-être présenter du contenu dans différentes langues aux locuteurs de ces langues. Vous souhaiterez peut-être présenter du contenu adapté à des appareils spécifiques, tels


   ```

que des smartphones, aux utilisateurs de ces appareils. La fonctionnalité de commutation de contenu de NetScaler permet à l'appliance de distribuer les demandes des clients sur plusieurs serveurs en fonction du contenu spécifique que vous souhaitez présenter à ces utilisateurs.

Pour configurer la commutation de contenu, créez d'abord une configuration de commutation de contenu de base, puis personnalisez-la en fonction de vos besoins. Cela implique l'activation de la fonctionnalité de commutation de contenu, la configuration de l'équilibrage de charge pour le ou les serveurs qui hébergent chaque version du contenu en cours de commutation, la création d'un serveur virtuel de commutation de contenu, la création de stratégies pour choisir les demandes qui sont dirigées vers quel serveur virtuel d'équilibrage de charge, et liaison des stratégies au serveur virtuel de commutation de contenu. Vous pouvez ensuite personnaliser la configuration en fonction de vos besoins en définissant la priorité de vos stratégies, en protégeant votre configuration en configurant un serveur virtuel de sauvegarde et en améliorant les performances de votre configuration en redirigeant les demandes vers un cache.

### Fonctionnement de la commutation de contenu

La commutation de contenu permet à l'appliance NetScaler de diriger les requêtes envoyées au même hôte Web vers différents serveurs avec un contenu différent. Par exemple, vous pouvez configurer la solution matérielle-logicielle pour diriger les demandes de contenu dynamique (telles que les URL avec un suffixe .asp, .dll ou .exe) vers un serveur et les demandes de contenu statique vers un autre serveur. Vous pouvez configurer la solution matérielle-logicielle pour qu'elle effectue une commutation de contenu en fonction des en-têtes TCP/IP et de la charge utile.

Vous pouvez également utiliser la commutation de contenu pour configurer la solution matérielle-logicielle afin de rediriger les demandes vers différents serveurs avec un contenu différent en fonction de divers attributs du client. Voici quelques-uns de ces attributs clients :

- **Type d'appareil.** La solution matérielle-logicielle examine l'agent utilisateur ou l'en-tête HTTP personnalisé dans la demande du client pour le type de périphérique à partir duquel la demande est originaire. En fonction du type d'appareil, il dirige la demande vers un serveur Web spécifique. Par exemple, si la demande provient d'un téléphone cellulaire, la demande est dirigée vers un serveur, capable de fournir un contenu que l'utilisateur peut consulter sur le téléphone cellulaire. Une demande émanant d'un ordinateur est dirigée vers un serveur différent, capable de diffuser un contenu conçu pour un écran d'ordinateur.
- **Langage.** La solution matérielle-logicielle examine l'en-tête HTTP Accept-Language dans la demande du client et détermine la langue utilisée par le navigateur du client. La solution matérielle-logicielle envoie ensuite la demande à un serveur qui diffuse du contenu dans cette langue. Par exemple, en utilisant la commutation de contenu en fonction de la langue, l'appliance peut envoyer une personne dont le navigateur est configuré pour demander du contenu en français à un serveur avec la version française d'un journal. Il peut envoyer une

 

autre personne dont le navigateur est configuré pour demander du contenu en anglais à un serveur avec la version anglaise.

- **Cookie.** La solution matérielle-logicielle examine les en-têtes de requête HTTP pour un cookie précédemment défini par le serveur. S'il trouve le cookie, il dirige les requêtes vers le serveur approprié, qui héberge du contenu personnalisé. Par exemple, si un cookie indique que le client est membre d'un programme de fidélisation de la clientèle, la demande est dirigée vers un serveur plus rapide ou un serveur doté d'un contenu spécial. S'il ne trouve pas de cookie, ou si le cookie indique que l'utilisateur n'est pas membre, la demande est dirigée vers un serveur destiné au grand public.
- **Méthode HTTP.** La solution matérielle-logicielle examine l'en-tête HTTP de la méthode utilisée et envoie la demande du client au bon serveur. Par exemple, les demandes GET d'images peuvent être dirigées vers un serveur d'images, tandis que les demandes POST peuvent être dirigées vers un serveur plus rapide qui gère le contenu dynamique.
- **Données de la couche 3/4.** L'appliance examine les demandes relatives à l'adresse IP source ou de destination, au port source ou de destination, ou à toute autre information présente dans les en-têtes TCP ou UDP, et dirige la demande du client vers le bon serveur. Par exemple, les demandes provenant d'adresses IP sources appartenant à des clients peuvent être dirigées vers un portail Web personnalisé sur un serveur plus rapide, ou vers un portail doté d'un contenu spécial.

Un déploiement de commutation de contenu typique comprend les entités décrites dans le diagramme suivant.

Figure 1. Architecture de commutation de contenu




 

Une configuration de commutation de contenu se compose d'un serveur virtuel de commutation de contenu, d'une configuration d'équilibrage de charge consistant en serveurs et services virtuels d'équilibrage de charge, et de stratégies de commutation de contenu. Pour configurer la commutation de contenu, vous devez configurer un serveur virtuel de commutation de contenu et l'associer à des stratégies et à des serveurs virtuels d'équilibrage de charge. Ce processus crée un *groupe de contenus*, un groupe de tous les serveurs virtuels et stratégies impliqués dans une configuration de commutation de contenu particulière.

La commutation de contenu peut être utilisée avec les connexions HTTP, HTTPS, TCP et UDP. Pour HTTPS, vous devez activer le déchargement SSL.

Lorsqu'une demande atteint le serveur virtuel de commutation de contenu, le serveur virtuel applique les stratégies de commutation de contenu associées à cette demande. La priorité de la stratégie définit l'ordre dans lequel les stratégies liées au serveur virtuel de commutation de contenu sont évaluées. Si vous utilisez des stratégies de stratégie avancées, lorsque vous liez une stratégie au serveur virtuel de commutation de contenu, vous devez attribuer une priorité à cette stratégie. Si vous utilisez les politiques classiques de NetScaler, vous pouvez attribuer une priorité à vos politiques, mais vous n'êtes pas obligé de le faire. Si vous attribuez des priorités, les stratégies sont évaluées dans l'ordre que vous avez défini. Dans le cas contraire, l'appliance NetScaler évalue vos politiques dans l'ordre dans lequel elles ont été créées.

Outre la configuration des priorités de stratégie, vous pouvez manipuler l'ordre d'évaluation de stratégie à l'aide d'expressions Goto et d'invocations de banque de stratégies. Pour plus d'informations sur la configuration avancée des stratégies, consultez Configuration des stratégies avancées.

Après avoir évalué les stratégies, le serveur virtuel de commutation de contenu achemine la demande vers le serveur virtuel d'équilibrage de charge approprié, qui l'envoie au service approprié.

Les serveurs virtuels de commutation de contenu peuvent uniquement envoyer des demandes à d'autres serveurs virtuels. Si vous utilisez un équilibreur de charge externe, vous devez créer un serveur virtuel d'équilibrage de charge pour celui-ci et lier son serveur virtuel en tant que service au serveur virtuel de commutation de contenu.

## Configuration de la commutation de contenu de base

May 5, 2023

Avant de configurer la commutation de contenu, vous devez comprendre comment la commutation de contenu est configurée et comment les services et les serveurs virtuels sont connectés.

Pour configurer une configuration de commutation de contenu de base et fonctionnelle, commencez par activer la fonction de commutation de contenu. Créez ensuite au moins un groupe de contenus.

 

Pour chaque groupe de contenus, créez un serveur virtuel de commutation de contenu pour accepter les demandes adressées à un groupe de sites Web qui utilisent la commutation de contenu. Créez également une configuration d'équilibrage de charge, qui inclut un groupe de serveurs virtuels d'équilibrage de charge vers lesquels le serveur virtuel de commutation de contenu dirige les demandes. Pour spécifier les demandes à diriger vers quel serveur virtuel d'équilibrage de charge, créez au moins deux stratégies de commutation de contenu, une pour chaque type de demande à rediriger. Lorsque vous avez créé les serveurs virtuels et les stratégies, liez les stratégies au serveur virtuel de commutation de contenu. Vous pouvez également lier une stratégie à plusieurs serveurs virtuels de commutation de contenu. Lorsque vous liez une stratégie, vous spécifiez le serveur virtuel d'équilibrage de charge vers lequel les demandes correspondant à la stratégie doivent être dirigées.

En plus de lier des stratégies individuelles à un serveur virtuel de commutation de contenu, vous pouvez lier des étiquettes de stratégie. Si vous créez plusieurs groupes de contenu, vous pouvez lier une stratégie ou une étiquette de stratégie à plusieurs des serveurs virtuels de commutation de contenu.

> **Remarque**
>
> Après avoir créé un groupe de contenus, vous pouvez modifier son serveur virtuel de commutation de contenu pour personnaliser la configuration.

### Activation du changement de contenu

Pour utiliser la fonctionnalité de changement de contenu, vous devez activer la commutation de contenu. Vous pouvez configurer des entités de changement de contenu même si la fonctionnalité de changement de contenu est désactivée. Toutefois, les entités ne fonctionneront pas.

### Pour activer la commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la commutation de contenu et vérifier la configuration :

```
enable ns feature CS

show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable  feature ContentSwitch
    Done
> show feature

    Feature                       Acronym             Status
    -------                       -------             ------
```



```
1)     Web Logging                    WL                  OFF
2)     Surge Protection               SP                  ON
3)     Load Balancing                 LB                  ON
4)     Content Switching              CS                  ON
.
.
.
22)    Responder                      RESPONDER           ON
23)    NetScaler Push                 push                OFF
Done
<!--NeedCopy-->
```

Pour activer la commutation de contenu à l'aide de l'interface graphique

Accédez à **Système > Paramètres** et, dans le groupe **Modes et fonctionnalités**, sélectionnez **Configurer les fonctionnalités de base**, puis sélectionnez **Changement de contenu**.

La figure suivante illustre la configuration pas à pas de Content Switching.



Création de serveurs virtuels de commutation de contenu

Vous pouvez ajouter, modifier et supprimer des serveurs virtuels de commutation de contenu. L'état d'un serveur virtuel est en panne lorsque vous le créez, car le serveur virtuel d'équilibrage de charge n'y est pas encore lié.

Pour créer un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Exemple :

```
add cs vserver Vserver-CS-1 HTTP 10.102.29.161 80
<!--NeedCopy-->
```

Pour ajouter un serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis ajoutez un serveur virtuel.
2. Spécifiez un nom pour le serveur virtuel de commutation de contenu.

   > **Remarque**
   >
   > Il existe différents serveurs virtuels de commutation de contenu pour chaque protocole. (Par exemple, HTTP et SSL).

3. Renseignez les champs pertinents, puis cliquez sur **OK**.

Statistiques du serveur virtuel de commutation de contenu

Les statistiques du serveur virtuel de commutation de contenu affichent des informations telles que la sélection du serveur virtuel, les octets de demande, les octets de réponse, le nombre total de paquets reçus, le nombre total de paquets envoyés, le seuil de débordement, la sélection de débordement, les connexions actuelles établies par le client et la sélection de sauvegarde du serveur virtuel en panne.

Les statistiques du serveur virtuel de commutation de contenu affichent également les détails récapitulatifs du serveur virtuel d'équilibrage de charge par défaut lié.

Pour afficher les statistiques du serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat cs vserver <name>
<!--NeedCopy-->
```

Exemple :


```
stat cs vserver CS_stats
<!--NeedCopy-->
```

```
Vserver Summary
                          IP  port     Protocol        State
CS_stats            1.1.1.1    80         HTTP           UP

VServer Stats:
                                          Rate (/s)                Total
Vserver hits                                      0                    0
Requests                                          0                    0
Responses                                         0                    0
Request bytes                                     0                    0
Response bytes                                    0                    0
Total Packets rcvd                                0                    0
Total Packets sent                                0                    0
Current client connections                       --                    0
Current Client Est connections                   --                    0
Current server connections                       --                    0
Spill Over Threshold                             --                    0
Spill Over Hits                                  --                    0
Labeled Connection                               --                    0
Push Labeled Connection                          --                    0
Deferred Request                                  0                    0
Invalid Request/Response                         --                    0
Invalid Request/Response Dropped                 --                    0
Vserver Down Backup Hits                         --                    0
Current Multipath TCP sessions                   --                    0
Current Multipath TCP subflows                   --                    0
Apdex for client response times.                 --                 1.00
Average client TTLB                              --                    0

 Done
```

Pour afficher les statistiques du serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels**.
2. Sélectionnez le serveur virtuel et cliquez sur **Statistiques**.



Configuration d'une configuration d'équilibrage de charge pour la commutation de contenu

Le serveur virtuel de commutation de contenu redirige toutes les demandes vers un serveur virtuel d'équilibrage de charge. Vous devez créer un serveur virtuel d'équilibrage de charge pour chaque version du contenu qui est commuté. Cela est vrai même si votre configuration ne comporte qu'un seul serveur pour chaque version du contenu et que vous n'effectuez donc aucun équilibrage de charge avec ces serveurs. Vous pouvez également configurer l'équilibrage de charge réel avec plusieurs serveurs à équilibrage de charge qui reflètent chaque version du contenu. Dans les deux scénarios, le serveur virtuel de commutation de contenu doit disposer d'un serveur virtuel d'équilibrage de charge spécifique affecté à chaque version du contenu en cours de commutation.

Le serveur virtuel d'équilibrage de charge transfère ensuite la demande à un service. Si un seul service lui est lié, il le sélectionne. Si plusieurs services lui sont liés, il utilise sa méthode d'équilibrage de charge configurée pour sélectionner un service pour la demande, et transfère cette demande au service qu'il a sélectionné.

Pour configurer une configuration d'équilibrage de charge de base, vous devez effectuer les tâches suivantes :

- Créer des serveurs virtuels d'équilibrage de charge
- Créer des services
- Liez les services au serveur virtuel d'équilibrage de charge

Pour plus d'informations sur l'équilibrage de charge, voir Fonctionnement de l'équilibrage de charge. Pour obtenir des instructions détaillées sur la configuration d'une configuration d'équilibrage de charge de base, voir Configurer l'équilibrage de charge de base.

Configuration d'une action de commutation de contenu

Vous spécifiez le serveur virtuel d'équilibrage de charge cible pour une stratégie de commutation de contenu lorsque vous liez la stratégie au serveur virtuel de commutation de contenu. Par conséquent, vous devez configurer une stratégie pour chaque serveur virtuel d'équilibrage de charge vers lequel diriger le trafic.

Toutefois, si votre stratégie de changement de contenu utilise une règle de stratégie avancée, vous pouvez configurer une action pour cette stratégie. Dans l'action, vous pouvez spécifier le nom du serveur virtuel d'équilibrage de charge cible ou configurer une expression basée sur la demande qui, au moment de l'exécution, calcule le nom du serveur virtuel d'équilibrage de charge auquel envoyer la demande. L'expression d'action doit être spécifiée dans la stratégie avancée.

L'option d'expression peut réduire considérablement la taille de votre configuration de commutation de contenu, car vous n'avez besoin que d'une seule stratégie par serveur virtuel de commutation de contenu. Les stratégies de commutation de contenu qui utilisent une action peuvent également être liées à plusieurs serveurs virtuels de commutation de contenu, car le serveur virtuel d'équilibrage de charge cible n'est plus spécifié dans la stratégie de commutation de contenu. La possibilité de lier une stratégie unique à plusieurs serveurs virtuels de commutation de contenu contribue à réduire davantage la taille de votre configuration de commutation de contenu.

Après avoir créé une action, vous créez une stratégie de changement de contenu et spécifiez l'action dans la stratégie, de sorte que l'action soit exécutée lorsque cette stratégie correspond à une demande.

> **Remarque**
>
> Vous pouvez également, pour une stratégie de commutation de contenu qui utilise une règle de stratégie avancée, spécifier le serveur virtuel d'équilibrage de charge cible lors de la liaison de la stratégie à un serveur virtuel de commutation de contenu, au lieu d'utiliser une action distincte. Pour les stratégies basées sur le domaine, les stratégies basées sur des URL et les stratégies basées sur des règles qui utilisent des expressions classiques, aucune action n'est disponible. Par conséquent, pour ces types de stratégies, vous spécifiez le nom du serveur virtuel d'équilibrage de charge cible lorsque vous liez la stratégie à un serveur virtuel de commutation de contenu.

Configuration d'une action qui spécifie le nom du serveur virtuel d'équilibrage de charge cible

Si vous choisissez de spécifier le nom du serveur virtuel d'équilibrage de charge cible dans une action de commutation de contenu, vous avez besoin d'autant de stratégies de commutation de contenu que de serveurs virtuels d'équilibrage de charge cible. Dans ce cas, les décisions de changement de contenu sont basées sur la règle de la stratégie de changement de contenu, et l'action spécifie simplement le serveur virtuel d'équilibrage de charge cible. Lorsqu'une demande correspond à la stratégie, elle est transférée au serveur virtuel d'équilibrage de charge spécifié.

Pour créer et vérifier une action de commutation de contenu qui spécifie le nom du serveur virtuel d'équilibrage de charge cible, à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add cs action <name> -targetLBVserver <string> [-comment <string>]

show cs action <name>
<!--NeedCopy-->
```

Exemple :

```
> add cs action mycsaction -targetLBVserver mylbvserver -comment "
    Forwards requests to mylbvserver."
 Done
> show cs action mycsaction
    Name: mycsaction
    Target LB Vserver: mylbvserver
    Hits: 0
    Undef Hits: 0
    Action Reference Count: 0
    Comment: "Forwards requests to mylbvserver."

 Done
>
<!--NeedCopy-->
```

Pour configurer une action de commutation de contenu qui spécifie le nom du serveur virtuel d'équilibrage de charge cible, à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Changement de contenu > Actions**.
2. Configurez une action de commutation de contenu et spécifiez le nom du serveur virtuel d'équilibrage de charge cible.

Configuration d'une action qui spécifie une expression pour sélectionner la cible au moment de l'exécution

Si vous choisissez de configurer une expression basée sur une demande qui peut calculer dynamiquement le nom du serveur virtuel d'équilibrage de charge cible, vous devez configurer une seule stratégie de commutation de contenu pour sélectionner le serveur virtuel approprié. La règle de la stratégie peut être un simple VRAI (la stratégie correspond à toutes les demandes) car, dans ce cas, les décisions de changement de contenu sont basées sur l'expression de l'action. En configurant une ex-

pression dans une action, vous pouvez réduire considérablement la taille de votre configuration de changement de contenu.

Si vous choisissez de configurer une expression basée sur la demande pour calculer le nom du serveur virtuel d'équilibrage de charge cible au moment de l'exécution, vous devez examiner attentivement comment nommer les serveurs virtuels d'équilibrage de charge dans la configuration. Vous devez être en mesure de dériver leurs noms à l'aide de l'expression de stratégie basée sur la demande dans l'action.

Par exemple, si vous changez de demande en fonction du suffixe d'URL (extension de la ressource demandée), lorsque vous nommez les serveurs virtuels d'équilibrage de charge, vous pouvez suivre la convention d'ajout du suffixe d'URL à une chaîne prédéterminée, par exemple `mylb_`. Par exemple, les serveurs virtuels d'équilibrage de charge pour les pages HTML et les fichiers PDF peuvent être nommés `mylb_html` et `mylb_pdf`, respectivement. Dans ce cas, la règle que vous pouvez utiliser dans l'action de changement de contenu pour sélectionner le serveur virtuel d'équilibrage de charge approprié est `"mylb_"+HTTP.REQ.URL.SUFFIX`. Si le serveur virtuel de commutation de contenu reçoit une demande de page HTML, l'expression est `mylb_html`renvoyée et la demande est basculée vers le serveur virtuel `mylb_html`.

Pour créer une action de changement de contenu qui spécifie une expression, à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour créer une action de changement de contenu qui spécifie une expression et vérifiez la configuration :

```
add cs action <name> -targetVserverExpr <expression>) [-comment <string
    >]

show cs action <name>
<!--NeedCopy-->
```

Exemple :

```
> add cs action mycsaction1 -targetvserverExpr '"mylb_" + HTTP.REQ.URL.
    SUFFIX'
 Done
> show cs action mycsaction1
    Name: mycsaction1
    Target Vserver Expression: "mylb_" + HTTP.REQ.URL.SUFFIX
    Target LB Vserver: No_Target
                ...
 Done
>
<!--NeedCopy-->
```


Pour configurer une action de changement de contenu qui spécifie une expression à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Changement de contenu > Actions**.
2. Configurez une action de commutation de contenu et spécifiez une expression qui calculera dynamiquement le nom du serveur virtuel d'équilibrage de charge cible.

Configuration des stratégies de changement de contenu

Une stratégie de commutation de contenu définit un type de demande qui doit être dirigée vers un serveur virtuel d'équilibrage de charge. Ces politiques sont appliquées dans l'ordre des priorités qui leur sont attribuées ou (si vous utilisez les politiques classiques de NetScaler et que vous n'attribuez pas de priorités lorsque vous les liez) dans l'ordre dans lequel les politiques ont été créées.

> **Remarque**
>
> Les paramètres d'**URL** et de **domaine** sont déconseillés et ne seront pas pris en charge à partir de la version 13.1. Utilisez les expressions de stratégie par défaut (avancées) ; l'utilitaire nspepi peut être utile pour la conversion.

Les politiques :

- **Stratégies basées sur des règles.** L'appliance compare les données entrantes aux expressions spécifiées dans les stratégies. Vous créez des stratégies basées sur des règles à l'aide d'une expression classique ou d'une expression de stratégie avancée. Les stratégies de stratégie classique et avancée sont prises en charge pour les stratégies de changement de contenu basées sur des règles.

  > **Remarque**
  >
  > Une stratégie basée sur des règles peut être configurée avec une action facultative. Une stratégie comportant une action peut être liée à plusieurs serveurs virtuels ou étiquettes de stratégie.

  Si vous définissez une priorité lorsque vous liez vos stratégies au serveur virtuel de commutation de contenu, les stratégies sont évaluées par ordre de priorité. Si vous ne définissez pas de priorités spécifiques lors de la liaison de vos stratégies, les stratégies sont évaluées dans l'ordre dans lequel elles ont été créées.

Pour plus d'informations sur les politiques et expressions classiques de NetScaler, consultez la section Configuration des politiques et des expressions classiques. Pour plus d'informations sur les stratégies de stratégie avancées, consultez Configuration des expressions de stratégie avancées.

Pour créer une stratégie de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
add cs policy <policyName> -rule <RULEValue>

add cs policy <policyName> -rule <RULEValue> -action <actionName>
<!--NeedCopy-->
```

Exemple :

```
add cs policy policy-CS-1 -rule "HTTP.REQ.URL.PATH.EQ("http://abcd.com
    ")"

add cs policy policy-CS-4 -rule "HTTP.REQ.HOSTNAME.EQ("example.com")"

add cs policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(24).EQ(10.217.84.0)"

add cs policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2009 Nov,GMT 2009 Dec)"

add cs policy-CS-3 -rule "http.req.method.eq(GET)" -action act1
<!--NeedCopy-->
```

Pour renommer une stratégie de changement de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rename cs policy <policyName> <newName>
<!--NeedCopy-->
```

Exemple :

```
rename cs policy myCSPolicy myCSPolicy1
<!--NeedCopy-->
```

Pour renommer une stratégie de changement de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Changement de contenu > Stratégies**, sélectionnez une stratégie et, dans la liste Action, sélectionnez Renommer.

Pour créer une stratégie de changement de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Stratégies**, puis cliquez sur **Ajouter**.
2. Renseignez les champs pertinents, puis cliquez sur **Créer**.

Configuration des étiquettes de stratégie de commutation de contenu

Une étiquette de stratégie est un point de liaison défini par l'utilisateur auquel les stratégies sont liées. Lorsqu'une étiquette de stratégie est appelée, toutes les stratégies qui lui sont liées sont évaluées dans l'ordre de priorité que vous leur avez attribué. Un libellé de stratégie peut inclure une ou plusieurs stratégies, chacune pouvant se voir attribuer son propre résultat. Une correspondance sur une stratégie dans l'étiquette de stratégie peut entraîner la poursuite de la stratégie suivante, l'appel d'un autre libellé de stratégie ou d'une ressource appropriée, ou la fin immédiate de l'évaluation de la stratégie et le retour du contrôle de la stratégie qui a appelé l'étiquette de stratégie. Vous pouvez créer des étiquettes de stratégie pour les stratégies avancées uniquement.

Une étiquette de stratégie de changement de contenu se compose d'un nom, d'un type d'étiquette et d'une liste de stratégies liées à l'étiquette de stratégie. Le type d'étiquette de stratégie spécifie le protocole qui a été affecté aux stratégies liées à l'étiquette. Il doit correspondre au type de service du serveur virtuel de commutation de contenu auquel la stratégie qui appelle l'étiquette de stratégie est liée. Par exemple, vous pouvez lier des stratégies de charge utile TCP à une étiquette de stratégie de type TCP uniquement. La liaison des stratégies de charge utile TCP à une étiquette de stratégie de type HTTP n'est pas prise en charge.

Chaque stratégie d'une étiquette de stratégie de changement de contenu est associée soit à une cible (qui est équivalente à l'action associée à d'autres types de stratégies, telles que les stratégies de réécriture et de répondeur), soit à une option GoToPriorityExpression et à une option d'appel. En d'autres termes, pour une stratégie donnée dans un libellé de stratégie de changement de contenu, vous pouvez spécifier une cible ou définir l'option GoToPriorityExpression et l'option invoke. De plus, si plusieurs stratégies sont évaluées sur true, seule la cible de la dernière stratégie évaluée sur true est prise en compte.

Vous pouvez utiliser l'interface de ligne de commande NetScaler ou l'interface graphique pour configurer les étiquettes de politique de commutation de contenu. Dans la CLI NetScaler, vous devez d'abord créer une étiquette de politique à l'aide de la commande add cs policy label. Ensuite, vous liez les stratégies à l'étiquette de stratégie, une stratégie à la fois, à l'aide de la commande bind cs policy label. Dans l'interface graphique de NetScaler, vous effectuez les deux tâches dans une seule boîte de dialogue.

Pour créer une étiquette de stratégie de changement de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add cs policylabel <labelName> <cspolicylabelTypetype>`
<!--NeedCopy-->
```

Exemple :

```
add cs policylabel testpollab http
<!--NeedCopy-->
```

Pour renommer une étiquette de stratégie de changement de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rename cs policylabel <labelName> <newName>`
<!--NeedCopy-->
```

Exemple :

```
rename cs policylabel oldPolicyLabelName newPolicyLabelName
<!--NeedCopy-->
```

Pour renommer une étiquette de stratégie de changement de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Changement de contenu > Étiquettes**de stratégie, sélectionnez une étiquette de stratégie et, dans la liste Action, sélectionnez Renommer.

Pour lier une stratégie à une étiquette de stratégie de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie à une étiquette de stratégie et vérifier la configuration :

```
bind cs policylabel <labelName> <policyName> <priority>[-targetVserver
    <string>] | [-gotoPriorityExpression <expression>] | [-invoke <
    labeltype> <labelName>] ]

show cs policylabel <labelName>
```



```
<!--NeedCopy-->
```

Exemple :

```
bind cs policylabel testpollab test_Pol 100 -targetVserver LBVIP
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 1
        Number of times invoked: 0
        Policy Name: test_Pol
        Priority: 100
        Target Virtual Server: LBVIP
<!--NeedCopy-->
```

> **Remarque**
>
> Si une stratégie est configurée avec une action, le serveur virtuel cible (TargetvServer), accédez à l'expression de priorité (GoToPriorityExpression) et les paramètres invoke (invoke) ne sont pas requis. Si une stratégie n'est pas configurée avec une action, vous devez configurer au moins l'un des paramètres suivants : TargetvServer, GoToPriorityExpression et invoke.

Pour délier une stratégie d'une étiquette de stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour délier une stratégie d'une étiquette de stratégie et vérifier la configuration :

```
unbind cs policylabel <labelName> <policyName>

show cs policylabel <labelName>
<!--NeedCopy-->
```

Exemple :

```
unbind cs policylabel testpollab test_Pol
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 0
        Number of times invoked: 0
<!--NeedCopy-->
```


Pour supprimer une étiquette de stratégie à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm cs policylabel <labelName>
<!--NeedCopy-->
```

Pour gérer une étiquette de stratégie de changement de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Étiquettes**de stratégie, configurez une étiquette de stratégie, liez des stratégies à l'étiquette et, le cas échéant, spécifiez une priorité, une expression GoToPriority et une option d'appel.

Stratégies de liaison à un serveur virtuel de commutation de contenu

Après avoir créé votre serveur virtuel de commutation de contenu et vos stratégies, vous liez chaque stratégie au serveur virtuel de commutation de contenu. Lorsque vous liez la stratégie au serveur virtuel de commutation de contenu, vous spécifiez le serveur virtuel d'équilibrage de charge cible.

> **Remarque**
>
> Si votre stratégie de changement de contenu utilise une règle de stratégie avancée, vous pouvez configurer une action de changement de contenu pour la stratégie. Si vous configurez une action, vous devez spécifier le serveur virtuel d'équilibrage de charge cible lorsque vous configurez l'action, et non lorsque vous liez la stratégie au serveur virtuel de commutation de contenu. Pour plus d'informations sur la configuration d'une action de changement de contenu, consultez la section
> Configuration d'une action de changement de contenu.

Pour lier une stratégie à un serveur virtuel de commutation de contenu et sélectionner un serveur virtuel d'équilibrage de charge cible à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind cs vserver <name>[-lbvserver<string> -targetLBVServer<string> -
    policyname <string> -priority <positive_integer>] [-
    gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )]
    [-invoke (<labelType> <labelName>)]
<!--NeedCopy-->
```

Exemple :


```
bind cs vserver csw-vip2 -policyname csw-ape-policy2 -priority 14 -
    gotoPriorityExpression NEXT

bind cs vserver csw-vip3 -policyname rewrite-policy1 -priority 17 -
    gotoPriorityExpression
'q.header("a").count' -flowtype REQUEST -invoke policylabel label1

bind cs vserver Vserver-CS-1 Vserver-LB-1 -policyname Policy-CS-1 -
    priority 20
<!--NeedCopy-->
```

> **Remarque**
>
> Les paramètres, serveur virtuel d'équilibrage de charge cible (TargetvServer), aller à l'expression de priorité (GoToPriorityExpression) et méthode invoke (invoke) ne peuvent pas être utilisés si une stratégie comporte une action.

Pour lier une stratégie à un serveur virtuel de commutation de contenu et sélectionner un serveur virtuel d'équilibrage de charge cible à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, ouvrez un serveur virtuel et, dans la section Liaison de stratégie de commutation de
contenu, liez une stratégie au serveur virtuel et spécifiez un serveur virtuel d'équilibrage de charge cible.

Configuration de la journalisation basée sur des stratégies pour la commutation de contenu

Vous pouvez configurer la journalisation basée sur une stratégie pour une stratégie de changement de contenu. La journalisation basée sur des stratégies vous permet de spécifier un format pour les messages de journal. Le contenu du message de journal est défini à l'aide d'une expression de stratégie avancée dans la stratégie de changement de contenu. Lorsque l'action de commutation de contenu spécifiée dans la politique est exécutée, l'appliance NetScaler construit le message de journal à partir de l'expression et écrit le message dans le fichier journal. La journalisation basée sur des stratégies est particulièrement utile si vous souhaitez tester et dépanner une configuration dans laquelle les actions de changement de contenu identifient le serveur virtuel d'équilibrage de charge cible au moment de l'exécution.

> **Remarque**
>
> Si plusieurs politiques liées à un serveur virtuel donné obtiennent la valeur TRUE et sont con-

> figurées avec une action de message d'audit, l'appliance NetScaler n'exécute pas toutes les actions du message d'audit. Il exécute uniquement l'action de message d'audit configurée pour la stratégie dont l'action de changement de contenu est effectuée.

Pour configurer la journalisation basée sur une stratégie pour une stratégie de changement de contenu, vous devez d'abord configurer une action de message d'audit. Pour plus d'informations sur la configuration d'une action de message d'audit, consultez la section Configuration de l'appliance NetScaler pour la journalisation des audits. Après avoir configuré l'action du message d'audit, vous spécifiez l'action dans une stratégie de changement de contenu.

Pour configurer la journalisation basée sur une stratégie pour une stratégie de commutation de contenu à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour configurer la journalisation basée sur une stratégie pour une stratégie de commutation de contenu et vérifier la configuration :

```
set cs policy <policyName> -logAction <string>

show cs policy <policyName>
<!--NeedCopy-->
```

Exemple :

```
> set cs policy cspol1 -logAction csLogAction
 Done
> show cs policy cspol1

    Policy: cspol1  Rule: TRUE  Action: csact1
    LogAction: csLogAction
    Hits: 0

1)  CS Vserver: csvs1
    Priority: 10
 Done
>
<!--NeedCopy-->
```

Pour configurer la journalisation basée sur une stratégie pour une stratégie de commutation de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Stratégies**, ouvrez une stratégie et, dans la liste Action du journal, sélectionnez une action de journal pour la stratégie.

Vérification de la configuration

Pour vérifier que la configuration de la commutation de contenu est correcte, vous devez afficher les entités de changement de contenu. Pour vérifier le bon fonctionnement après le déploiement de votre configuration de commutation de contenu, vous pouvez afficher les statistiques générées lors de l'accès aux serveurs.

Affichage des propriétés des serveurs virtuels de commutation de contenu

Vous pouvez consulter les propriétés des serveurs virtuels de commutation de contenu que vous avez configurés sur l'appliance NetScaler. Vous pouvez utiliser ces informations pour vérifier si le serveur virtuel est correctement configuré et, si nécessaire, pour résoudre les problèmes. Outre les détails tels que le nom, l'adresse IP et le port, vous pouvez afficher les différentes stratégies liées à un serveur virtuel et ses paramètres de gestion du trafic.

Les stratégies de changement de contenu sont affichées dans l'ordre de priorité. Si plusieurs stratégies ont la même priorité, elles sont affichées dans l'ordre dans lequel elles sont liées au serveur virtuel.

> **Remarque**
>
> Si vous avez configuré le serveur virtuel de commutation de contenu pour transférer le trafic vers un serveur virtuel d'équilibrage de charge, vous pouvez également afficher les stratégies de commutation de contenu en affichant les propriétés du serveur virtuel d'équilibrage de charge.

Pour afficher les propriétés des serveurs virtuels de commutation de contenu à l'aide de l'interface de ligne de commande

Pour répertorier les propriétés de base de tous les serveurs virtuels de commutation de contenu de votre configuration, ou les propriétés détaillées d'un serveur virtuel de commutation de contenu spécifique, à l'invite de commandes, tapez l'une des commandes suivantes :

```
show cs vserver

show cs vserver <name>
<!--NeedCopy-->
```

Exemple

```
1.
show cs vserver Vserver-CS-1
Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
Last state change was at Thu Jun 30 10:48:59 2011
```



```
Time since last state change: 6 days, 20:03:00.760
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
Default: Content Precedence: RULE
Vserver IP and Port insertion: OFF
Case Sensitivity: ON
Push: DISABLED Push VServer:
Push Label Rule: none

...
1) Policy : __ESNS_PREBODY_POLICY Priority:0
2) Policy : __ESNS_POSTBODY_POLICY Priority:0

1) Compression Policy Name: __ESNS_CMP_POLICY Priority: 2147483647
GotoPriority Expression: END
Flowtype: REQUEST

2) Rewrite Policy Name: __ESNS_REWRITE_POLICY Priority: 2147483647
GotoPriority Expression: END
Flowtype: REQUEST

3) Cache Policy Name: dfbx Priority: 10
GotoPriority Expression: END
Flowtype: REQUEST

4) Responder Policy Name: __ESNS_RESPONDER_POLICY Priority: 2147483647
GotoPriority Expression: END

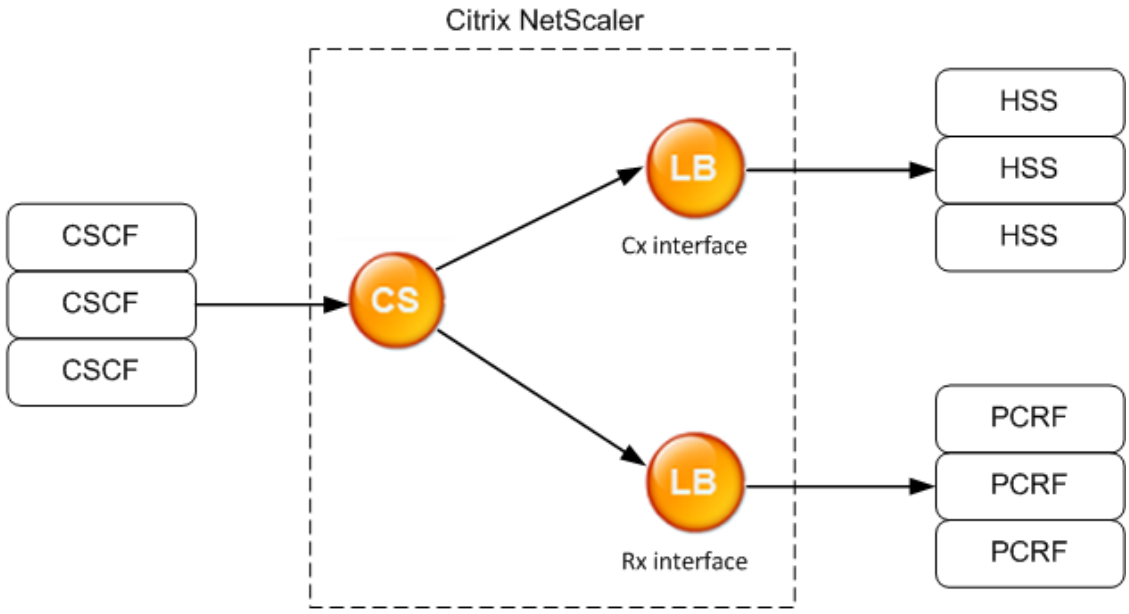
1) Policy: wiki Target: LBVIP2 Priority: 25 Hits: 0
2) Policy: plain Target: LBVIP1 Priority: 90 Hits: 0
3) Policy: DispOrderTest2 Target: KerbAuthLBVS Priority: 91 Hits: 0
4) Policy: test_Pol Target: LBVIP1 Priority: 92 Hits: 0
5) Policy: PolicyNameTesting Target: LBVIP1 Priority: 100 Hits: 0
 Done
>

show cs vserver
1) Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
…
Appflow logging: DISABLED
```



```
Port Rewrite : DISABLED
State Update: DISABLED

2) apubendpt (10.111.111.1:80) - HTTP Type: CONTENT
State: UP
…
Client Idle Timeout: 180 sec
Down state flush: DISABLED
…

3) apubendpt1 (10.111.111.2:80) - HTTP Type: CONTENT
State: UP
…
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
…
<!--NeedCopy-->
```

Affichage des stratégies de changement de contenu

Vous pouvez afficher les propriétés des stratégies de changement de contenu que vous avez définies, telles que le nom, le domaine, l'URL ou l'expression, et utiliser ces informations pour détecter toute erreur dans la configuration ou pour dépanner si quelque chose ne fonctionne pas correctement.

Pour afficher les propriétés des stratégies de changement de contenu à l'aide de l'interface de ligne de commande

Pour répertorier les propriétés de base de toutes les stratégies de commutation de contenu de votre configuration ou les propriétés détaillées d'une stratégie de commutation de contenu spécifique, à l'invite de commandes, tapez l'une des commandes suivantes :

```
show cs policy

show cs policy <PolicyName>
<!--NeedCopy-->
```

Exemple :

```
show cs policy

show cs policy-CS-1
```



```
<!--NeedCopy-->
```

Pour afficher les propriétés des stratégies de changement de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Changement de contenu** > **Stratégies**, sélectionnez une stratégie et, dans la liste Action, sélectionnez **Afficher les liaisons**.

Affichage d'une configuration de serveur virtuel de commutation de contenu à l'aide du visualiseur

Le visualiseur de commutation de contenu est un outil que vous pouvez utiliser pour afficher une configuration de changement de contenu au format graphique. Vous pouvez utiliser le visualiseur pour afficher les éléments de configuration suivants :

- Un résumé des serveurs virtuels d'équilibrage de charge auxquels le serveur virtuel de commutation de contenu est lié.
- Tous les services et groupes de services liés au serveur virtuel d'équilibrage de charge et tous les moniteurs liés aux services.
- Les détails de configuration de tout élément affiché.
- Toutes les stratégies liées au serveur virtuel de commutation de contenu. Il n'est pas nécessaire que ces stratégies soient des stratégies de changement de contenu. De nombreux types de stratégies, tels que les stratégies de réécriture, peuvent être liés à un serveur virtuel de commutation de contenu.

Après avoir configuré les différents éléments d'une configuration de commutation de contenu et d'équilibrage de charge, vous pouvez exporter l'intégralité de la configuration vers un fichier de modèle d'application.

> **Remarque**
>
> Le visualiseur nécessite une interface graphique, il n'est donc disponible que via l'interface graphique.

Pour afficher une configuration de commutation de contenu à l'aide du visualiseur dans l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez afficher, puis cliquez sur **Visualiseur**.

3. Dans la fenêtre **Visualiseur de changement de contenu**, vous pouvez ajuster la zone d'affichage comme suit :

    - Cliquez sur les icônes **Zoom avant** et **Zoom arrière** pour augmenter ou réduire la zone d'affichage.
    - Cliquez sur l'icône **Enregistrer l'image** pour enregistrer le graphique en tant que fichier image.
    - Dans le champ de texte Rechercher, commencez à taper le nom de l'élément que vous recherchez. Lorsque vous avez saisi suffisamment de caractères pour identifier l'élément, son emplacement est mis en surbrillance. Pour restreindre la recherche, cliquez sur le menu déroulant et sélectionnez le type d'élément que vous souhaitez rechercher.

4. Pour afficher les détails de configuration des entités liées à ce serveur virtuel, vous pouvez effectuer les opérations suivantes :

    - Pour afficher les stratégies liées au serveur virtuel, dans la barre d'outils située en haut de la boîte de dialogue, sélectionnez une ou plusieurs icônes de stratégie spécifiques aux fonctionnalités. Si les étiquettes de stratégie sont configurées, elles apparaissent dans la zone d'affichage principale.
    - Pour afficher les détails de configuration d'un service ou d'un groupe de services lié, cliquez sur l'icône du service, sur l'onglet Tâches associées, puis sur Afficher les services aux membres.
    - Pour afficher les détails de configuration d'un moniteur, cliquez sur l'icône du moniteur, cliquez sur l'onglet **Tâches associées**, puis cliquez sur **Afficher le moniteur**.

5. Pour afficher des statistiques détaillées pour n'importe quel serveur virtuel dans la configuration de commutation de contenu, cliquez sur le serveur virtuel pour lequel vous souhaitez afficher les statistiques, puis sur l'onglet Tâches associées, puis sur **Statistiques**.

6. Pour afficher une liste comparative des paramètres dont les valeurs diffèrent ou ne sont pas définies entre les conteneurs de services d'un serveur virtuel d'équilibrage de charge, cliquez sur l'icône d'un conteneur, cliquez sur l'onglet **Tâches associées**, puis sur **Différence des attributs de service**.

7. Pour afficher les détails de liaison de moniteur pour les services d'un conteneur, dans la boîte de dialogue Diff des attributs de service, dans la colonne Groupe du conteneur, cliquez sur **Détails**. Cette liste comparative vous aide à déterminer quel conteneur de services possède la configuration que vous souhaitez appliquer à tous les conteneurs de services.

8. Pour afficher le nombre de demandes reçues par seconde à un moment donné par les serveurs virtuels de la configuration, et le nombre de demandes sélectionnées par seconde à un moment donné pour les stratégies de réécriture, de répondeur et de cache, cliquez sur Afficher les statistiques. Les informations statistiques sont affichées sur les nœuds respectifs du visualiseur. Ces informations ne sont pas mises à jour en temps réel. Il est actualisé manuellement. Pour actu-

aliser les informations, cliquez sur Actualiser les statistiques.

> **Remarque**
>
> Cette option n'est disponible que sur les versions NetScaler nCore.

9. Pour copier les détails de configuration d'un élément dans un document ou une feuille de calcul, cliquez sur l'icône de cet élément, sur Tâches associées, sur Copier les propriétés, puis collez les informations dans un document.
10. Pour exporter l'intégralité de la configuration affichée dans le visualiseur vers un fichier de modèle d'application, cliquez sur l'icône du serveur virtuel de commutation de contenu, cliquez sur Tâches associées, puis sur Créer un modèle. Lors de la création du modèle d'application, vous pouvez configurer des variables dans certaines expressions de stratégie et actions. Pour plus d'informations sur la création du fichier de modèle d'application et la configuration des variables pour un modèle, consultez AppExpert.

Personnalisation de la configuration de base de la commutation de contenu

May 5, 2023

Après avoir configuré une configuration de commutation de contenu de base, il se peut que vous deviez la personnaliser en fonction de vos besoins. Vous pouvez configurer des serveurs virtuels de commutation de contenu HTTP et SSL pour qu'ils écoutent sur plusieurs ports au lieu de créer des serveurs virtuels distincts. Si vous souhaitez configurer la commutation de contenu pour un réseau local virtuel spécifique, vous pouvez configurer un serveur virtuel de commutation de contenu avec une politique d'écoute.

Prise en charge de plusieurs ports pour les serveurs virtuels de commutation de contenu de type HTTP et SSL

Vous pouvez configurer NetScaler de sorte que les serveurs virtuels de commutation de contenu HTTP et SSL écoutent sur plusieurs ports, sans avoir à configurer des serveurs virtuels distincts. Cette fonctionnalité est particulièrement utile si vous souhaitez baser une décision de changement de contenu sur une partie de l'URL et d'autres paramètres L7. Au lieu de configurer plusieurs serveurs virtuels avec la même adresse IP et différents ports, vous pouvez configurer une adresse IP et spécifier le port sous la forme *. Par conséquent, la taille de la configuration est également réduite.

Pour configurer un serveur virtuel de commutation de contenu HTTP ou SSL afin qu'il écoute sur plusieurs ports à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
add cs vserver \<name\> \<serviceType\> \<IPAddress\> Port \*
```

Exemple

```
> add cs vserver cs1 HTTP 10.102.92.215 *
 Done
> sh cs vserver cs1
        cs1 (10.102.92.215:*) - HTTP    Type: CONTENT
        State: UP
        Last state change was at Tue May 20 01:15:49 2014
        Time since last state change: 0 days, 00:00:03.270
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow logging: ENABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Vserver IP and Port insertion: OFF
        L2Conn: OFF     Case Sensitivity: ON
        Authentication: OFF
        401 Based Authentication: OFF
        Push: DISABLED  Push VServer:
        Push Label Rule: none
        IcmpResponse: PASSIVE
        RHIstate:  PASSIVE
        TD: 0
 Done
<!--NeedCopy-->
```

Pour configurer un serveur virtuel de commutation de contenu HTTP ou SSL afin qu'il écoute sur plusieurs ports à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis créez un serveur virtuel de type HTTP ou SSL.
2. Utilisez un astérisque (*) pour spécifier le port.

Configuration des serveurs virtuels génériques par VLAN

Si vous souhaitez configurer la commutation de contenu pour le trafic sur un VLAN spécifique, vous pouvez créer un serveur virtuel générique avec une stratégie d'écoute qui le limite au traitement du trafic uniquement sur le VLAN spécifié.

Pour configurer un serveur virtuel générique qui écoute un VLAN spécifique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add cs vserver \<name\> \<serviceType\> IPAddress `* Port *` -
   listenpolicy \<expression\> \[-listenpriority \<positive\_integer
   \>\]
<!--NeedCopy-->
```

Exemple :

```
add cs vserver Vserver-CS-vlan1 ANY * *
-listenpolicy "CLIENT.VLAN.ID.EQ(2)"  -listenpriority 10
<!--NeedCopy-->
```

Pour configurer un serveur virtuel générique qui écoute un VLAN spécifique à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis configurez un serveur virtuel. Spécifiez une stratégie d'écoute qui la limite au traitement du trafic uniquement sur le VLAN spécifié.

Une fois que vous avez créé ce serveur virtuel, vous le liez à un ou plusieurs services, comme décrit dans Configuration de l'équilibrage de charge de base.

Configuration du paramètre de version de Microsoft SQL Server

Vous pouvez spécifier la version de Microsoft® SQL Server® pour un serveur virtuel de commutation de contenu de type MSSQL. Le paramètre de version est recommandé si vous pensez que certains clients n'exécutent pas la même version que votre produit Microsoft SQL Server. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur.

Pour définir le paramètre de version de Microsoft SQL Server à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir le paramètre de version Microsoft SQL Server pour un serveur virtuel de commutation de contenu et vérifier la configuration :

- `set cs vserver \<name\> -mssqlServerVersion \<mssqlServerVersion\>`
- `show cs vserver \<name\>`

Exemple

```
1 > set cs vserver myMSSQLcsvip -mssqlServerVersion 2008R2 Done > show cs
      vserver myMSSQLcsvip myMSSQLcsvip (192.0.2.13:1433) - MSSQL Type:
     CONTENT State: UP . . . . . MSsql Server Version: 2008R2 . . . . .
      . Done >
2 <!--NeedCopy-->
```

Pour définir le paramètre de version de Microsoft SQL Server à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MSSQL.
2. Dans **les paramètres avancés**, spécifiez la **version du serveur**.

Activer la vérification de l'état TCP externe pour les serveurs virtuels UDP

Dans les clouds publics, vous pouvez utiliser l'appliance NetScaler comme équilibreur de charge de second niveau lorsque l'équilibreur de charge natif est utilisé comme premier niveau. L'équilibreur de charge natif peut être un équilibreur de charge d'application (ALB) ou un équilibreur de charge réseau (NLB). La plupart des clouds publics ne prennent pas en charge les sondes de santé UDP dans leurs équilibreurs de charge natifs. Pour surveiller l'état de l'application UDP, les clouds publics recommandent d'ajouter un point de terminaison TCP à votre service. Le point de terminaison reflète l'intégrité de l'application UDP.

L'appliance NetScaler prend en charge le contrôle de santé externe basé sur TCP pour un serveur virtuel UDP. Cette fonctionnalité introduit un écouteur TCP sur la VIP du serveur virtuel de commutation de contenu et du port configuré. L'écouteur TCP reflète l'état du serveur virtuel.

Pour activer la vérification de l'état TCP externe pour les serveurs virtuels UDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour activer une vérification d'intégrité TCP externe avec l'option tcpProbePort :

```
add cs vserver <name> <protocol> <IPAddress> <port> -tcpProbePort <
   tcpProbePort>
<!--NeedCopy-->
```

Exemple :

```
add cs vserver Vserver-CS-1 UDP 10.102.29.161 5002 -tcpProbePort 5000
<!--NeedCopy-->
```

Pour activer la vérification de l'état TCP externe pour les serveurs virtuels UDP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis créez un serveur virtuel.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel.
3. Dans le volet **Paramètres de base**, ajoutez le numéro de port dans le champ **Port de la sonde TCP** .
4. Cliquez sur **OK**.

Changement de contenu pour le protocole Diameter

May 5, 2023

Pour le trafic basé sur le protocole Diameter, vous pouvez configurer l'appliance NetScaler (ou l'appliance virtuelle) pour qu'elle agisse en tant qu'agent relais chargé d'équilibrer la charge et de transférer un paquet vers la destination appropriée sur la base du contenu du message (valeur AVP dans le message). Comme l'appliance n'effectue aucun traitement au niveau des applications, elle fournit des services de relais pour toutes les applications Diameter, conformément aux politiques de commutation de contenu configurées. Par conséquent, l'appliance annonce l'ID de l'application relais dans le message CEA (Capability Exchange Answer) lorsque le client établit une connexion Diameter. Vous devez configurer un serveur virtuel de commutation de contenu, des serveurs virtuels d'équilibrage de charge et des services pour représenter les nœuds Diameter. Lorsqu'une demande parvient au serveur virtuel de commutation de contenu, le serveur virtuel applique les politiques de commutation de contenu associées à ce type de demande. Après avoir évalué les

stratégies, le serveur virtuel de commutation de contenu achemine la demande vers le serveur virtuel d'équilibrage de charge approprié, qui l'envoie au service approprié.

Une interface de diamètre fournit une connexion entre les différents nœuds de diamètre. L'exemple de déploiement suivant utilise les interfaces Cx et Rx. Une interface Cx fournit une connexion entre un CSCF et un HSS. Une interface Rx fournit une connexion entre un CSCF et un PCRF. Tous les messages parviennent à l'appliance NetScaler. Selon que le message concerne une interface Cx ou Rx, et selon les politiques de commutation de contenu définies, NetScaler sélectionne un pool de serveurs d'équilibrage de charge approprié.



CSCF=Call Session Control Function
HSS=Home Subscriber Server
PCRF=Policy and Charging Rules Function

Exemple de configuration

1. Pour chaque entité, créez un service, un serveur d'équilibrage de charge et liez le service au serveur virtuel.

```
add service svc_pcrf[1-3] 1.1.1.1[1-3] DIAMETER 3868
add service svc_hss[1-3] 1.1.1.2[1-3] DIAMETER 3868
add lb vserver vs_rx DIAMETER -persistenceType DIAMETER -
   persistavpno 263
add lb vserver vs_cx DIAMETER -persistenceType DIAMETER -
   persistavpno 263
bind lb vserver vs_rx svc_pcrf[1-3]
bind lb vserver vs_cx svc_hss[1-3]
```



```
<!--NeedCopy-->
```

2. Créez un serveur virtuel de commutation de contenu et deux actions (une pour chaque serveur virtuel d'équilibrage de charge). Créez deux politiques de commutation de contenu et liez-les au serveur virtuel de commutation de contenu, en spécifiant une priorité pour chaque politique.

```
add cs vserver cs_diameter DIAMETER 10.1.1.10 3868
add cs action cx_action -targetLBVserver vs_cx
add cs action rx_action  - targetLBvserver vs_rx
add cs policy cx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777216)" -action cx_action
add cs policy rx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777236)" -action rx_action
bind cs vserver cs_diameter -policyName rx_policy -priority 100
bind cs vserver cs_diameter -policyName cx_policy -priority 110
<!--NeedCopy-->
```

Protection de la configuration de commutation de contenu contre les défaillances

May 8, 2023

La commutation de contenu peut échouer lorsque le serveur virtuel de commutation de contenu tombe en panne ou ne parvient pas à gérer un trafic excessif, ou pour d'autres raisons. Pour réduire les risques d'échec, vous pouvez prendre les mesures suivantes pour protéger la configuration de commutation de contenu contre les défaillances :

Configuration d'un serveur virtuel de sauvegarde

Si le serveur virtuel de commutation de contenu principal est marqué comme étant inactif ou DÉSACTIVÉ, l'appliance NetScaler peut diriger les demandes vers un serveur virtuel de commutation de contenu de sauvegarde. Il peut également envoyer un message de notification au client concernant la panne ou la maintenance du site. Le serveur virtuel de commutation de contenu de sauvegarde est un proxy transparent pour le client.

Lors de la configuration du serveur virtuel de sauvegarde, vous pouvez spécifier le paramètre de configuration Disable Primary When Down pour garantir que, lorsque le serveur virtuel principal revient, il reste le serveur secondaire jusqu'à ce que vous le forciez manuellement à prendre le relais en tant que serveur principal. C'est utile si vous voulez vous assurer que toutes les mises à jour de la base de

données sur le serveur pour la sauvegarde sont préservées, ce qui vous permet de synchroniser les bases de données avant de restaurer le serveur virtuel principal.

Vous pouvez configurer un serveur virtuel de commutation de contenu de sauvegarde lorsque vous créez un serveur virtuel de commutation de contenu ou lorsque vous modifiez les paramètres facultatifs d'un serveur virtuel de commutation de contenu existant. Vous pouvez également configurer un serveur virtuel de commutation de contenu de sauvegarde pour un serveur virtuel de commutation de contenu de sauvegarde existant, afin de créer des serveurs virtuels de commutation de contenu de sauvegarde en cascade. La profondeur maximale du contenu de sauvegarde en cascade passant par des serveurs virtuels est de 10. L'appliance recherche un serveur virtuel de commutation de contenu de sauvegarde actif et accède à ce serveur virtuel de commutation de contenu pour diffuser le contenu.

> **Remarque**
>
> Si un serveur virtuel de commutation de contenu est configuré avec à la fois un serveur virtuel de commutation de contenu de sauvegarde et une URL de redirection, le serveur virtuel de commutation de contenu de sauvegarde a la priorité sur l'URL de redirection. La redirection est utilisée lorsque le serveur virtuel principal et le serveur virtuel de sauvegarde sont hors service.

Pour configurer un serveur virtuel de sauvegarde et de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cs vserver <name> -backupVserver <string> -disablePrimaryOnDown (ON
    |OFF)
<!--NeedCopy-->
```

Exemple

```
set cs vserver Vserver-CS-1 -backupVserver Vserver-CS-2 -
    disablePrimaryOnDown ON
<!--NeedCopy-->
```

Pour configurer un serveur virtuel de sauvegarde et de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MYSQL.
2. Dans **Paramètres avancés**, sélectionnez **Protection**et spécifiez un **serveur virtuel de sauvegarde**.

Redirection du trafic excédentaire vers un serveur virtuel de sauvegarde

L'option de débordement redirige les nouvelles connexions arrivant sur un serveur virtuel de commutation de contenu vers un serveur virtuel de commutation de contenu de sauvegarde lorsque le nombre de connexions au serveur virtuel de commutation de contenu dépasse la valeur seuil configurée. La valeur du seuil est calculée dynamiquement ou vous pouvez définir la valeur. Le nombre de connexions établies (en TCP) sur le serveur virtuel est comparé à la valeur seuil. Lorsque le nombre de connexions atteint le seuil, les nouvelles connexions sont redirigées vers le serveur virtuel de commutation de contenu de sauvegarde.

Si les serveurs virtuels de commutation de contenu de sauvegarde atteignent le seuil configuré et ne sont pas en mesure de supporter la charge, le serveur virtuel de commutation de contenu principal redirige toutes les demandes vers l'URL de redirection. Si aucune URL de redirection n'est configurée sur le serveur virtuel de commutation de contenu principal, les demandes suivantes sont supprimées.

Pour configurer un serveur virtuel de commutation de contenu afin de rediriger les nouvelles connexions vers un serveur virtuel de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cs vserver \<name\> -soMethod \<methodType\> -soThreshold \<
    thresholdValue\> -soPersistence \<persistenceValue\> -
    soPersistenceTimeout \<timeoutValue\>
<!--NeedCopy-->
```

Exemple

```
set cs vserver Vserver-CS-1 -soMethod Connection -soThreshold 1000 -
    soPersistence enabled -soPersistenceTimeout 2
<!--NeedCopy-->
```

Pour configurer un serveur virtuel de commutation de contenu afin qu'il redirige les nouvelles connexions vers un serveur virtuel de sauvegarde à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MYSQL.
2. Dans **Paramètres avancés**, sélectionnez **Protection**et configurez le spillover.

Configuration d'une URL de redirection

Vous pouvez configurer une URL de redirection pour communiquer l'état de l'appliance NetScaler si un serveur virtuel de commutation de contenu de type HTTP ou HTTPS est en panne ou DÉSACTIVÉ.

Cette URL peut être locale ou distante.

Les URL de redirection peuvent être des URL absolues ou des URL relatives. Si l'URL de redirection configurée contient une URL absolue, la redirection HTTP est envoyée vers l'emplacement configuré, quelle que soit l'URL spécifiée dans la requête HTTP entrante. Si l'URL de redirection configurée contient uniquement le nom de domaine (URL relative), la redirection HTTP est envoyée vers un emplacement après avoir ajouté l'URL entrante au domaine configuré dans l'URL de redirection.

Citrix recommande d'utiliser une URL absolue. C'est-à-dire une URL se terminant par/, par exemple www.example.com/ au lieu d'une URL relative. Une redirection d'URL relative peut entraîner le signalement d'un faux positif par l'analyseur de vulnérabilités.

> **Remarque**
>
> Si un serveur virtuel de commutation de contenu est configuré avec à la fois un serveur virtuel de sauvegarde et une URL de redirection, le serveur virtuel de sauvegarde a la priorité sur l'URL de redirection. Une URL de redirection est utilisée lorsque le serveur virtuel principal et le serveur virtuel de sauvegarde sont hors service.

Lorsque la redirection est configurée et que le serveur virtuel de commutation de contenu n'est pas disponible, l'appliance émet une redirection HTTP 302 vers le navigateur de l'utilisateur.

Pour configurer une URL de redirection lorsque le serveur virtuel de commutation de contenu n'est pas disponible à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cs vserver \<name\> -redirectURL \<URLValue\>
<!--NeedCopy-->
```

Exemple

```
set cs vserver Vserver-CS-1 -redirectURL http://www.newdomain.com/
   mysite/maintenance
<!--NeedCopy-->
```

Pour configurer une URL de redirection lorsque le serveur virtuel de commutation de contenu n'est pas disponible à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MYSQL.
2. Dans **Paramètres avancés**, sélectionnez **Protection**et spécifiez une URL de redirection.

Configuration de l'option de mise à jour de l'état

La fonction de commutation de contenu permet de distribuer les demandes des clients sur plusieurs serveurs en fonction du contenu spécifique présenté aux utilisateurs. Pour une commutation de contenu efficace, le serveur virtuel de commutation de contenu distribue le trafic aux serveurs virtuels d'équilibrage de charge en fonction du type de contenu, et les serveurs virtuels d'équilibrage de charge distribuent le trafic aux serveurs physiques conformément à la méthode d'équilibrage de charge spécifiée.

Pour une gestion fluide du trafic, il est important que le serveur virtuel de commutation de contenu connaisse l'état des serveurs virtuels d'équilibrage de charge. L'option de mise à jour de l'état permet de marquer le serveur virtuel de commutation de contenu comme étant hors service si le serveur virtuel d'équilibrage de charge qui y est lié est marqué comme étant inactif. Un serveur virtuel d'équilibrage de charge est marqué comme étant inactif si tous les serveurs physiques qui y sont liés sont marqués comme étant hors service.

Lorsque la mise à jour de l'état est désactivée :

L'état du serveur virtuel de commutation de contenu est marqué comme UP. Il reste actif même si aucun serveur virtuel d'équilibrage de charge lié n'est actif.

Lorsque la mise à jour de l'état est activée :

Lorsque vous ajoutez un serveur virtuel de commutation de contenu, son état est initialement affiché comme étant inactif. Lorsque vous liez un serveur virtuel d'équilibrage de charge dont l'état est UP, l'état du serveur virtuel de commutation de contenu passe à UP.

Si plusieurs serveurs virtuels d'équilibrage de charge sont liés et si l'un d'entre eux est spécifié par défaut, l'état du serveur virtuel de commutation de contenu reflète l'état du serveur virtuel d'équilibrage de charge par défaut.

Si plusieurs serveurs virtuels d'équilibrage de charge sont liés sans qu'aucun d'entre eux ne soit spécifié par défaut, l'état du serveur virtuel de commutation de contenu est marqué UP uniquement si tous les serveurs virtuels d'équilibrage de charge liés sont actifs.

Pour configurer l'option de mise à jour de l'état à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add cs vserver \<name\> \<protocol\> \<ipAddress\> \<port\> -
     stateUpdate ENABLED
2 <!--NeedCopy-->
```

Exemple


```
1  add cs vserver csw_vserver HTTP 10.18.250.154 80 -stateupdate ENABLED
      -cltTimeout 180
2  <!--NeedCopy-->
```

Pour configurer l'option de mise à jour de l'état à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme MYSQL.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres du trafic**, puis sélectionnez **Mise à jour de l'état**.

Purger la file d'attente en cas de surtension

Lorsqu'un serveur physique reçoit une vague de demandes, il met du temps à répondre aux clients qui y sont actuellement connectés, ce qui laisse les utilisateurs insatisfaits et mécontents. Souvent, la surcharge provoque également les clients à recevoir des pages d'erreur. Pour éviter de telles surcharges, l'appliance NetScaler fournit des fonctionnalités telles que la protection contre les surtensions, qui contrôle la vitesse à laquelle de nouvelles connexions à un service peuvent être établies.

L'appliance effectue le multiplexage des connexions entre les clients et les serveurs physiques. Lorsqu'elle reçoit une demande d'un client pour accéder à un service sur un serveur, l'appliance recherche une connexion gratuite déjà établie avec le serveur. S'il trouve une connexion libre, il utilise cette connexion pour établir un lien virtuel entre le client et le serveur. Si aucune connexion gratuite n'est trouvée, l'appliance établit une nouvelle connexion avec le serveur et établit un lien virtuel entre le client et le serveur. Toutefois, si l'appliance ne peut pas établir de nouvelle connexion avec le serveur, elle envoie la demande client à une file d'attente de surtension. Si tous les serveurs physiques liés au serveur virtuel d'équilibrage de charge ou de commutation de contenu atteignent la limite supérieure du nombre de connexions client (valeur client maximale, seuil de protection contre les surtensions ou capacité maximale du service), l'appliance ne peut établir de connexion avec aucun serveur. La fonction de protection contre les surtensions utilise la file d'attente pour réguler la vitesse à laquelle les connexions sont ouvertes avec les serveurs physiques. L'appliance gère une file d'attente de surtension différente pour chaque service lié au serveur virtuel.

La longueur d'une file d'attente d'urgence augmente chaque fois qu'une demande arrive pour laquelle l'appliance ne peut pas établir de connexion, et elle diminue chaque fois qu'une demande de la file d'attente est envoyée au serveur ou qu'une demande arrive à expiration et est supprimée de la file d'attente.

Si la file d'attente de surtension d'un service ou d'un groupe de services devient trop longue, vous pouvez la vider. Vous pouvez vider la file d'attente d'un service ou d'un groupe de services spécifique, ou de tous les services et groupes de services liés à un serveur virtuel d'équilibrage de charge. Le

fait de vider une file d'attente d'urgence n'affecte pas les connexions existantes. Seules les demandes présentes dans la file d'attente d'urgence sont supprimées. Pour ces demandes, le client doit faire une nouvelle demande.

Vous pouvez également vider la file d'attente d'un serveur virtuel de commutation de contenu. Si un serveur virtuel de commutation de contenu transmet certaines demandes à un serveur virtuel d'équilibrage de charge particulier et que le serveur virtuel d'équilibrage de charge reçoit également d'autres demandes, lorsque vous videz la file d'attente du serveur virtuel de commutation de contenu, seules les demandes reçues de ce serveur virtuel de commutation de contenu sont vidées. Les autres requêtes de la file d'attente de surtension du serveur virtuel d'équilibrage de charge ne sont pas vidées.

> **Remarque**
>
> Vous ne pouvez pas vider les files d'attente de surtension des serveurs virtuels de redirection de cache, d'authentification, de VPN ou de serveurs virtuels GSLB ou des services GSLB.
> N'utilisez pas la fonctionnalité Protection contre les surtensions si USIP (USIP) est activée.

Pour vider une file d'attente d'urgence à l'aide de l'interface de ligne de commande

La commande flush ns SurgeQ fonctionne de la manière suivante :

- Vous pouvez spécifier le nom d'un service, d'un groupe de services ou d'un serveur virtuel dont la file d'attente doit être vidée.
- Si vous spécifiez un nom lors de l'exécution de la commande, la file d'attente de surtension de l'entité spécifiée est vidé. Si plusieurs entités portent le même nom, l'appliance vide les files d'attente de toutes ces entités.
- Si vous spécifiez le nom d'un groupe de services, ainsi qu'un nom de serveur et un port lors de l'exécution de la commande, l'appliance vide la file d'attente de surtension du membre du groupe de services spécifié uniquement.
- Vous ne pouvez pas spécifier directement un membre du groupe de services (<serverName> \ et \ <port>) sans spécifier le nom du groupe de services (\ <name>) et vous ne pouvez pas spécifier \ <port> sans \ <serverName>. Spécifiez les \ <serverName> et \ <port> si vous souhaitez vider la file d'attente d'urgence pour un membre spécifique du groupe de services.
- Si vous exécutez la commande sans spécifier de nom, l'appliance vide les files d'attente de surtension de toutes les entités présentes sur l'appliance.
- Si un membre du groupe de services est identifié par un nom de serveur, vous devez spécifier le nom du serveur dans cette commande ; vous ne pouvez pas spécifier son adresse IP.

À l'invite de commande, tapez :

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>].
<!--NeedCopy-->
```


Exemples

```
1. flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80
The above command flushes the surge queue of the service or virtual
    server that is named SVC1ANZGB and has IP address as 10.10.10

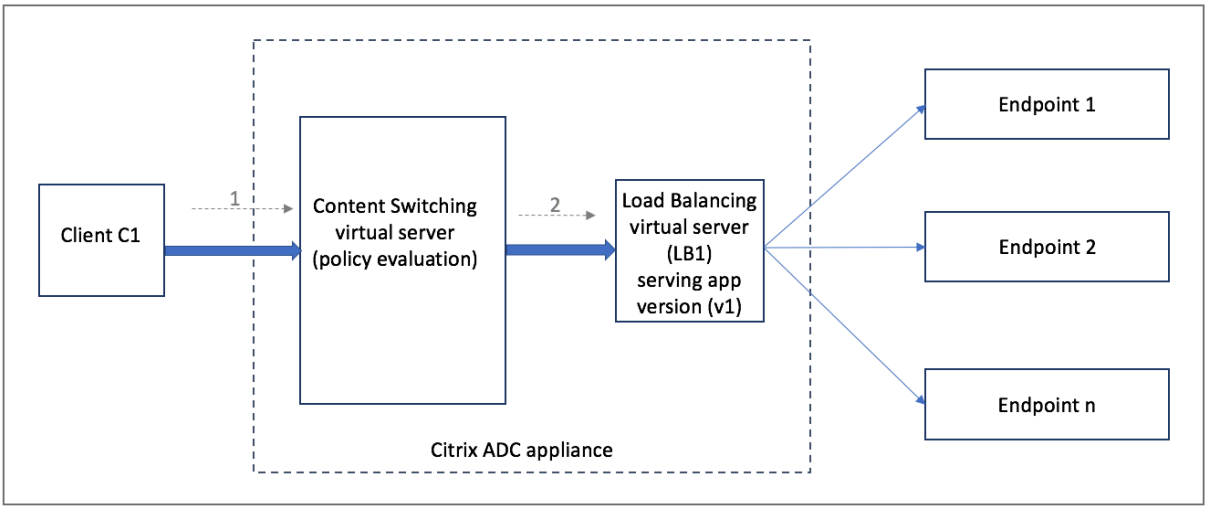
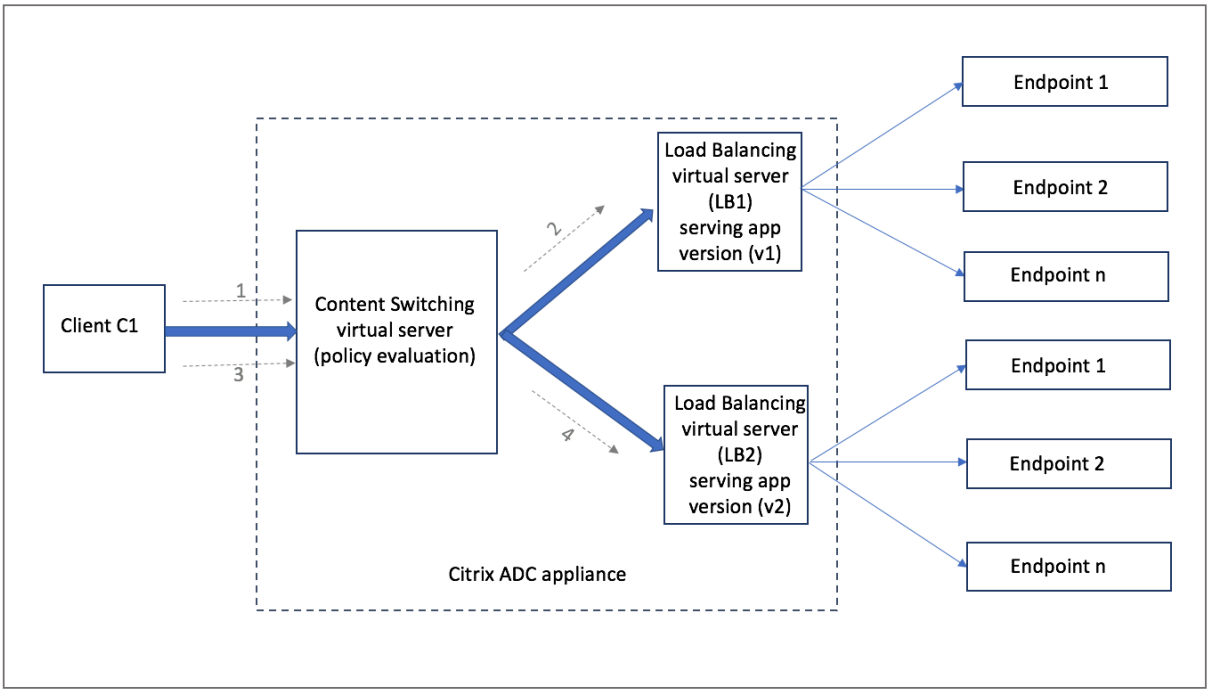
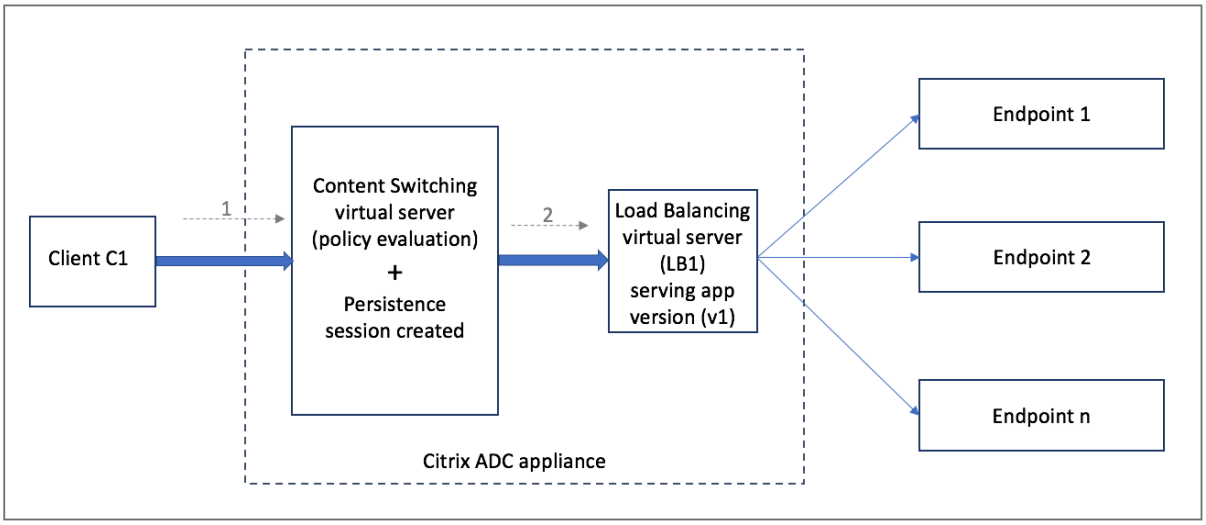
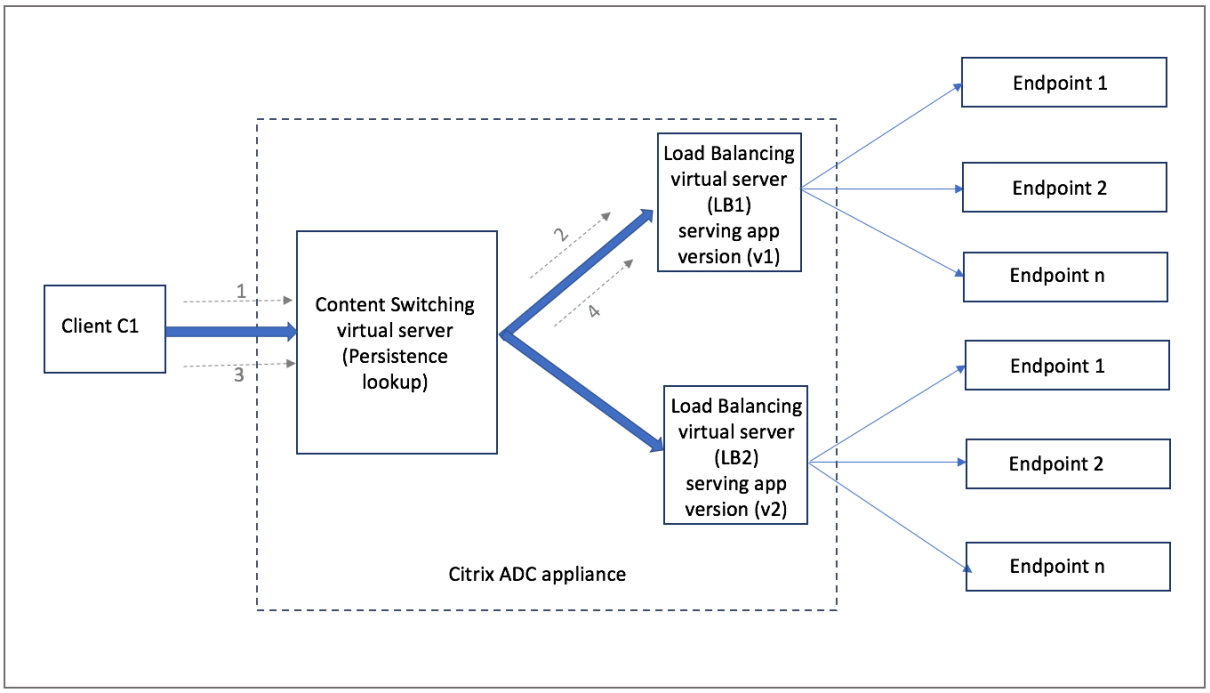
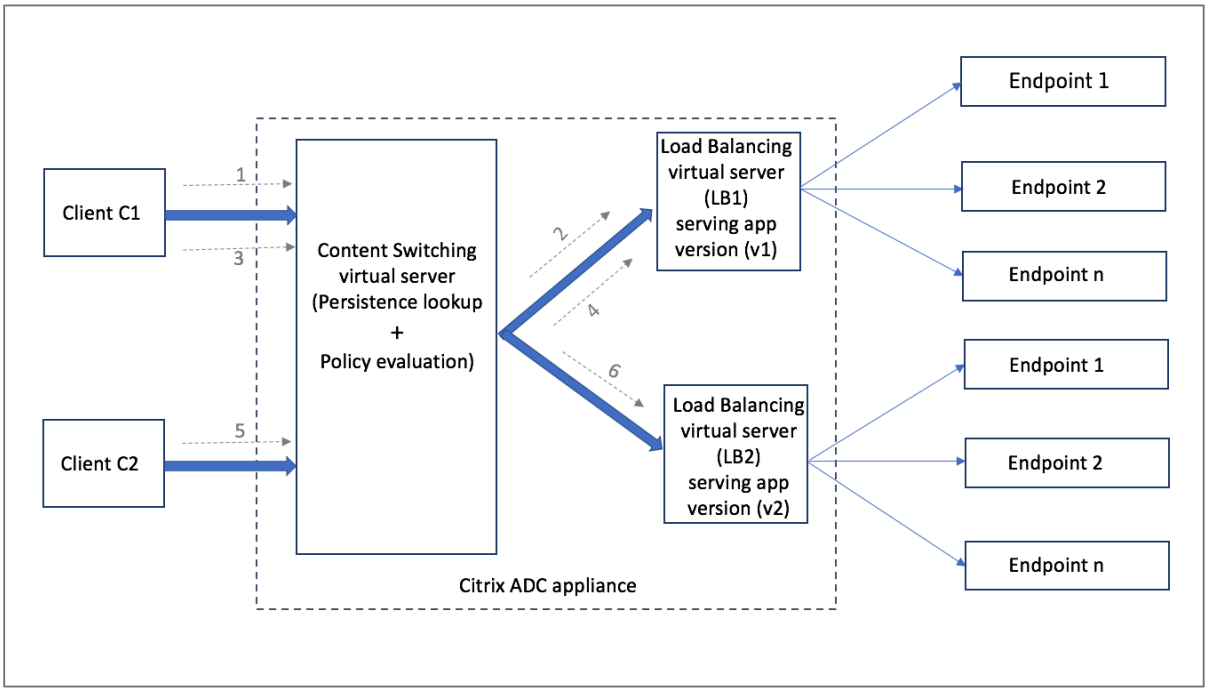
2. flush ns surgeQ
The above command flushes all the surge queues on the appliance.
<!--NeedCopy-->
```

Pour vider une file d'attente de surtension à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez un serveur virtuel et, dans la liste des actions, sélectionnez **Flush Surge Queue**.

Gestion d'une configuration de commutation de contenu

May 5, 2023

Une fois qu'une configuration de commutation de contenu est configurée, elle peut nécessiter des modifications périodiques. Lorsque des systèmes d'exploitation ou des logiciels sont mis à jour, ou que le matériel est épuisé et remplacé, il se peut que vous deviez arrêter votre configuration. La charge de votre configuration peut augmenter et nécessiter davantage de ressources. Vous pouvez également modifier la configuration pour améliorer les performances.

Ces tâches peuvent nécessiter des stratégies de dissociation du serveur virtuel de commutation de contenu, ou la désactivation ou la suppression des serveurs virtuels de commutation de contenu. Après avoir modifié votre configuration, vous devrez peut-être réactiver les serveurs et réassocier les stratégies. Vous pouvez également renommer vos serveurs virtuels.

Stratégies de déliement du serveur virtuel de commutation de contenu

Lorsque vous disposez d'une stratégie de changement de contenu de son serveur virtuel, le serveur virtuel n'inclut plus cette stratégie lorsqu'il détermine où diriger les demandes.

Pour délier une stratégie d'un serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
unbind cs vserver <name> -policyname <string>
```


Exemple :

```
unbind cs vserver Vserver-CS-1 -policyname Policy-CS-1
```

Pour délier une stratégie d'un serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Cliquez sur la section **Stratégies**, sélectionnez la stratégie, puis cliquez sur **Unbind**.

Supprimer les serveurs virtuels de commutation de contenu

Normalement, vous supprimez un serveur virtuel de commutation de contenu uniquement lorsque vous n'avez plus besoin du serveur virtuel. Lorsque vous supprimez un serveur virtuel de commutation de contenu, l'appliance NetScaler dissocie d'abord toutes les politiques du serveur virtuel de commutation de contenu, puis le supprime.

Pour supprimer un serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm cs vserver <name>
```

Exemple :

```
rm cs vserver Vserver-CS-1
```

Pour supprimer un serveur virtuel de commutation de contenu à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez un serveur virtuel, puis cliquez sur **Supprimer**.

Désactivation et réactivation des serveurs virtuels de commutation de contenu

Les serveurs virtuels de commutation de contenu sont activés par défaut lorsque vous les créez. Vous pouvez désactiver un serveur virtuel de commutation de contenu à des fins de maintenance. Si vous désactivez le serveur virtuel de commutation de contenu, l'état du serveur virtuel de commutation de contenu passe à Out of Service. Lorsqu'il est hors service, le serveur virtuel de commutation de contenu ne répond pas aux demandes.

Pour désactiver ou réactiver un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `disable cs vserver <name>`
- `enable cs vserver <name>`

Exemple :

```
disable cs vserver Vserver-CS-1
enable cs vserver Vserver-CS-1
```

Pour désactiver ou réactiver un serveur virtuel à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez un serveur virtuel et, dans la liste **Action**, sélectionnez **Activer** ou **désactiver**.

Changement de nom des serveurs virtuels de commutation de contenu

Vous pouvez renommer un serveur virtuel de commutation de contenu sans le délier. Le nouveau nom est automatiquement propagé à toutes les parties concernées de la configuration NetScaler.

Pour renommer un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rename cs vserver <name> <newName>
```

Exemple :

```
1 `rename cs vserver Vserver-CS-1 Vserver-CS-2`
```

Pour renommer un serveur virtuel à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez un serveur virtuel et, dans la liste **Action**, sélectionnez **Renommer**.

Gestion des stratégies de changement de contenu

Vous pouvez modifier une stratégie existante en configurant les règles ou en modifiant l'URL de la stratégie, ou vous pouvez supprimer une stratégie. Vous pouvez également renommer une stratégie de commutation de contenu avancée existante. Vous pouvez créer différentes stratégies en fonction de l'URL. Les stratégies basées sur l'URL peuvent être de différents types, comme décrit dans le tableau suivant.

Pour plus d'informations, voir Exemples de stratégies basées sur des URL.

> **Remarque**
>
> Vous pouvez configurer la commutation de contenu basée sur des règles à l'aide d'expressions de stratégie classiques ou d'expressions de stratégie avancées.

Pour modifier, supprimer ou renommer une stratégie à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `set cs policy <policyName> [-domain <domainValue>] [-rule <ruleValue>] [-url <URLValue>]`
- `rm cs policy <policyName>`
- `rename cs policy <policyName> <newPolicyName>`

Exemple :

```
set cs policy-CS-1 -domain "www.domainxyz.com"

set cs policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(22).EQ(10.100.148.0)"

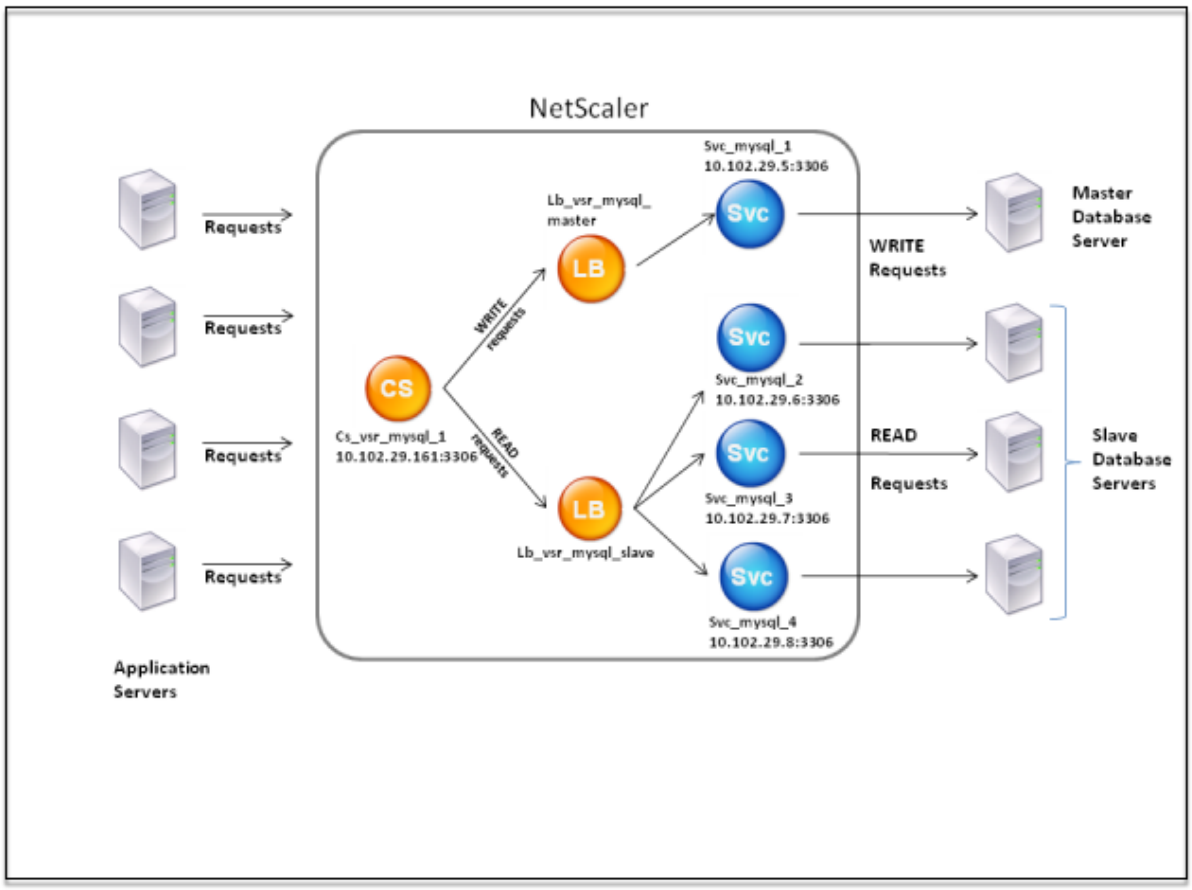
set cs policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2010 Jun,GMT 2010 Jul)"

set cs policy-CS-1 -url /sports/*

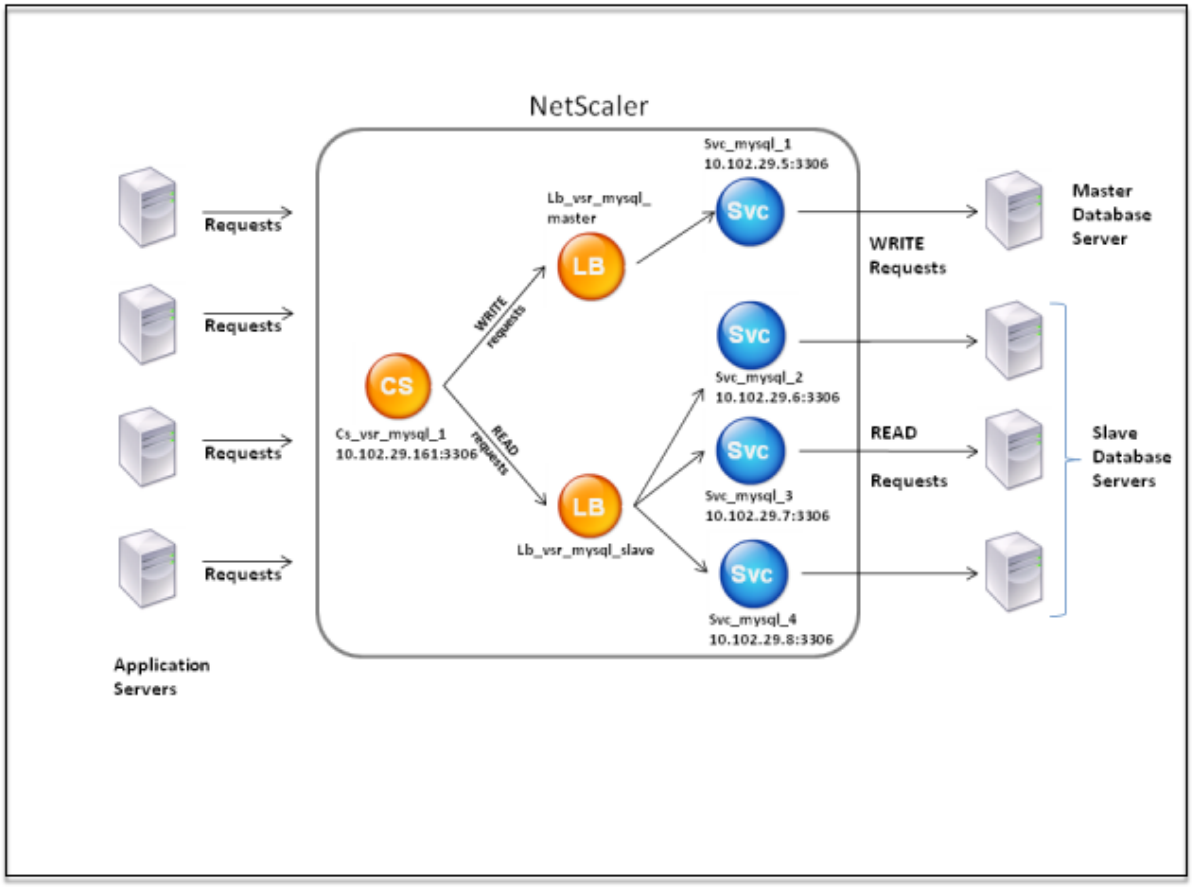
rename cs policy-CS-1 Policy-CS-11

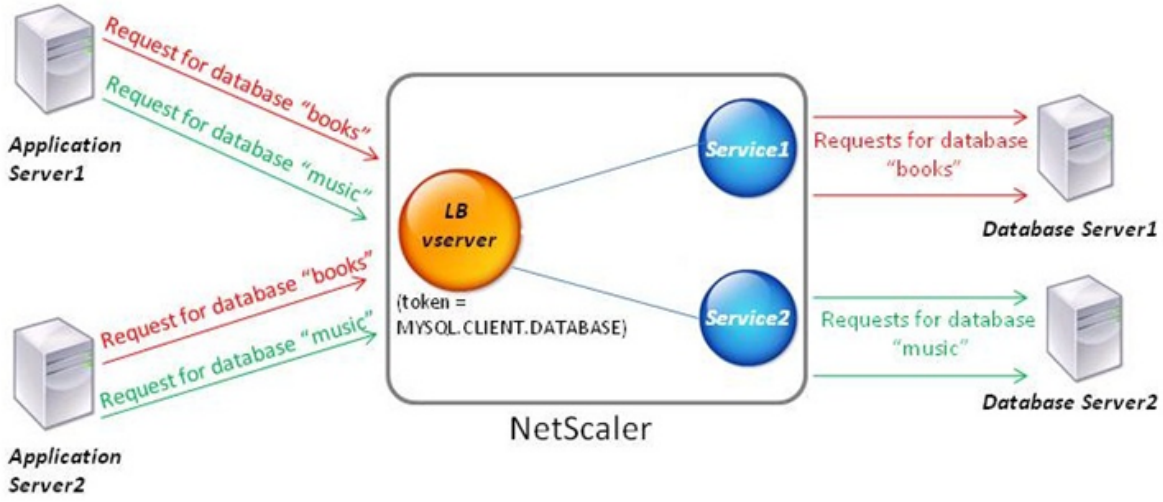
rm cs policy-CS-1
```

Pour modifier, supprimer ou renommer une stratégie à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Changement de contenu > Stratégies**.
2. Sélectionnez la stratégie, puis supprimez-la, modifiez-la ou, dans la liste **Action**, cliquez sur **Renommer**.

Gestion des connexions client

May 5, 2023

Pour garantir une gestion efficace des connexions client, vous pouvez configurer les serveurs virtuels de commutation de contenu sur l'appliance NetScaler pour utiliser les fonctionnalités suivantes :

- **Configuration de la réponse ICMP.** Vous pouvez configurer l'appliance NetScaler pour envoyer des réponses ICMP aux requêtes PING en fonction de vos paramètres. Sur l'adresse IP correspondant au serveur virtuel, définissez la réponse ICMP sur VSVR_CNTRLD, et sur le serveur virtuel, définissez la réponse du serveur virtuel ICMP.
  Les paramètres suivants peuvent être définis sur un serveur virtuel :
  - Lorsque vous définissez le paramètre RESPONSE du serveur virtuel ICMP sur PASSIVE sur tous les serveurs virtuels, l'appliance NetScaler répond toujours.
  - Lorsque vous définissez le paramètre RESPONSE du serveur virtuel ICMP sur ACTIVE sur tous les serveurs virtuels, l'appliance ADC répond même si l'un des serveurs virtuels est opérationnel.
  - Lorsque vous définissez le paramètre RESPONSE du serveur virtuel ICMP sur ACTIVE sur certains et PASSIVE sur d'autres, l'appliance ADC répond même si un serveur virtuel défini sur ACTIVE est activé.

Redirection des demandes du client vers un cache

La fonctionnalité de redirection du cache de NetScaler redirige les requêtes HTTP vers un cache. Vous pouvez réduire considérablement la charge que représente la réponse aux requêtes HTTP et améliorer les performances de votre site Web grâce à la mise en œuvre correcte de la fonctionnalité de redirection du cache.

Un cache stocke le contenu HTTP fréquemment demandé. Lorsque vous configurez la redirection du cache sur un serveur virtuel, l'appliance NetScaler envoie des requêtes HTTP pouvant être mises en cache vers le cache et des requêtes HTTP non mises en cache vers le serveur Web d'origine. Pour plus d'informations sur la redirection du cache, voir « Redirection du cache ».

Pour configurer la redirection du cache sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cs vserver \<name\> -cacheable \<Value\>
```

Exemple

```
set cs vserver Vserver-CS-1 -cacheable yes
```

Pour configurer la redirection du cache sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.

2. Dans **Paramètres avancés, sélectionnez Paramètresdu trafic**, puis sélectionnez**Peut être mis en cache**.

Activation du nettoyage différé des connexions aux serveurs virtuels

Dans certaines conditions, vous pouvez configurer le paramètre down state flush pour mettre fin aux connexions existantes lorsqu'un service ou un serveur virtuel est marqué comme étant inactif. L'arrêt des connexions existantes libère des ressources et, dans certains cas, accélère la restauration des configurations d'équilibrage de charge surchargées.

Pour configurer le paramètre de vidage d'état en panne sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cs vserver \<name\> -downStateFlush \<Value\>
```

Exemple

```
1 set cs vserver Vserver-CS-1 -downStateFlush enabled
2 <!--NeedCopy-->
```

Pour configurer le paramètre down state flush sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres du trafic**, puis sélectionnez **Down State Flush**.

Réécriture des ports et des protocoles pour la redirection

Les serveurs virtuels et les services qui y sont liés peuvent utiliser différents ports. Lorsqu'un service répond à une connexion HTTP par une redirection, vous devrez peut-être configurer l'appliance NetScaler pour modifier le port et le protocole afin de garantir le bon déroulement de la redirection. Vous le faites en activant et en configurant le paramètre redirectPortRewrite.

Pour configurer la redirection HTTP sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
set cs vserver \<name\> -redirectPortRewrite \<Value\>
```

Exemple

```
1 set cs vserver Vserver-CS-1 -redirectPortRewrite enabled
2 <!--NeedCopy-->
```

Pour configurer la redirection HTTP sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres du trafic**, puis sélectionnez **Réécrire**.

Insertion de l'adresse IP et du port d'un serveur virtuel dans l'en-tête de demande

Si vous disposez de plusieurs serveurs virtuels qui communiquent avec différentes applications sur le même service, vous devez configurer l'appliance NetScaler pour ajouter l'adresse IP et le numéro de port du serveur virtuel approprié aux requêtes HTTP envoyées à ce service. Ce paramètre permet aux applications exécutées sur le service d'identifier le serveur virtuel qui a envoyé la demande.

Si le serveur virtuel principal est en panne et que le serveur virtuel de sauvegarde est actif, les paramètres de configuration du serveur virtuel de sauvegarde sont ajoutés aux demandes du client. Si vous souhaitez ajouter la même balise d'en-tête, que les demandes proviennent du serveur virtuel principal ou du serveur virtuel de sauvegarde, vous devez configurer la balise d'en-tête requise sur les deux serveurs virtuels.

> **Remarque**
>
> Cette option n'est pas prise en charge pour les serveurs virtuels génériques ou les serveurs virtuels fictifs.

Pour insérer l'adresse IP et le port du serveur virtuel dans les demandes du client à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cs vserver \<name\> -insertVserverIPPort \<vServerIPPORT\>
```

Exemple

```
1 set cs vserver Vserver-CS-1 -insertVserverIPPort 10.201.25.136:80
2 <!--NeedCopy-->
```


Pour insérer l'adresse IP et le port du serveur virtuel dans les demandes du client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés, sélectionnez Paramètresdu trafic** et, dans la liste d'insertion des ports IP du serveur virtuel, sélectionnez VIPADDR ou V6TOV4MAPPING, puis spécifiez un en-tête de port dans la valeur d'insertion du port IP du serveur virtuel.

Définition d'une valeur de délai d'expiration pour les connexions client inactives

Vous pouvez configurer un serveur virtuel pour mettre fin à toute connexion client inactive une fois le délai d'expiration configuré écoulé. Lorsque vous configurez ce paramètre, l'appliance NetScaler attend le temps que vous spécifiez et, si le client est inactif après ce délai, elle ferme la connexion client.

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cs vserver \<name\> -cltTimeout \<Value\>
```

Exemple

```
1 set cs vserver Vserver-CS-1 -cltTimeout 100
2 <!--NeedCopy-->
```

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres du trafic**et spécifiez une valeur de **délai d'inactivité du client** .

Identification des connexions à l'aide des paramètres de connexion du tuple 4 et de la couche 2

Vous pouvez désormais définir l'option L2Conn pour un serveur virtuel de commutation de contenu. Lorsque l'option L2Conn est définie, les connexions au serveur virtuel de commutation de contenu

sont identifiées par la combinaison des paramètres de connexion du tuple 4 (<source IP> : \ : : <source port><destination IP > : <destination port >) et de la couche 2. Les paramètres de connexion de couche 2 sont l'adresse MAC, l'ID du VLAN et l'ID du canal.

Pour définir l'option L2Conn pour un serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour configurer le paramètre L2Conn pour un serveur virtuel de commutation de contenu et vérifier la configuration :

```
1 -  set cs vserver \<name\> -l2Conn (**ON** | **OFF**)
2 -  show cs vserver \<name\>
```

Exemple

```
1 > set cs vserver mycsvserver -l2Conn ON
2 Done
3 > show cs vserver mycsvserver
4      mycsvserver (192.0.2.56:80) - HTTP   Type: CONTENT
5      State: UP
6          . . .
7          . . .
8      L2Conn: ON Case Sensitivity: ON
9          . . .
10         . . .
11 Done
12 >
13 <!--NeedCopy-->
```

Pour définir l'option L2Conn pour un serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels** et ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres du trafic**, puis sélectionnez **Paramètres de couche 2**.

Prise en charge de la persistance pour le serveur virtuel de commutation de contenu

May 5, 2023

Les applications passent d'architectures monolithiques à une architecture de microservices. Différentes versions d'une même application peuvent coexister dans l'architecture des microservices. L'appliance NetScaler doit prendre en charge le déploiement continu d'applications. Cela est possible grâce à des plateformes qui exécutent des déploiements Canary (comme Spinnaker). Dans une configuration de déploiement continu, une version plus récente d'une application est déployée automatiquement et exposée au trafic client par étapes jusqu'à ce que l'application soit stable et prenne en charge la totalité du trafic. De plus, les services au client doivent être ininterrompus.

La fonctionnalité de commutation de contenu NetScaler permet à l'appliance NetScaler de distribuer les demandes des clients sur plusieurs serveurs virtuels d'équilibrage de charge en fonction des politiques liées au serveur virtuel de commutation de contenu.

Pour les déploiements continus, la commutation de contenu est utilisée pour sélectionner le serveur virtuel d'équilibrage de charge desservant différentes versions d'une application.

Lors de la commutation de contenu, la sélection d'un serveur virtuel d'équilibrage de charge pour une version d'application spécifique change lors de l'exécution en raison de la modification des politiques de commutation de contenu. Au cours de cette transition, si certaines sessions sont présentes avec d'anciennes versions de l'application, ce trafic doit continuer à être desservi uniquement par les anciennes versions. Pour répondre à cette exigence, l'appliance NetScaler maintient la persistance entre plusieurs groupes d'équilibrage de charge derrière un serveur virtuel de commutation de contenu. La persistance du serveur virtuel de commutation de contenu permet une transition fluide des clients d'une version à l'autre.

Types de persistance pris en charge sur le serveur virtuel de commutation de contenu

Les types de persistance suivants sont pris en charge sur les serveurs virtuels de commutation de contenu.

Type de persistance	Description
IP source	**ADRESSE IP SOURCE**. Les connexions provenant de la même adresse IP client font partie de la même session de persistance. Pour plus de détails, consultez la section Persistance de l'adresse IP source.

Type de persistance	Description
Cookie HTTP	ENCART À**BISCUITS.** Les connexions qui ont le même en-tête de cookie HTTP font partie de la même session de persistance. Le format du cookie inséré par l'appliance NetScaler est le suivant : **NSC_ = où NSC_XXXX** <vid_str of CSvserver><vid_str of Lbvserver>est l'ID du serveur virtuel dérivé du nom du serveur virtuel. Pour plus de détails, consultez la section Persistance des cookie HTTP.
ID de session SSL	**SESSION SSL**. Les connexions qui ont le même ID de session SSL font partie de la même session de persistance. Pour plus de détails, consultez la section Persistance des ID de session SSL.

Vous pouvez configurer une valeur de délai d'expiration pour la persistance basée sur les cookies HTTP. Si vous définissez la valeur du délai d'expiration sur 0, l'appliance ADC ne spécifie pas le délai d'expiration, quelle que soit la version du cookie HTTP utilisée. Le délai d'expiration dépend alors du logiciel client, et ces cookies ne sont valides que si le logiciel est en cours d'exécution.

Selon le type de persistance que vous avez configuré, le serveur virtuel peut prendre en charge 250 000 connexions persistantes simultanées ou un nombre quelconque de connexions persistantes dans les limites imposées par la quantité de mémoire de votre appliance NetScaler. Le tableau suivant indique les types de persistance qui entrent dans chaque catégorie.

Type de persistance	Nombre de connexions persistantes simultanées prises en charge
IP source, ID de session SSL	250,000
Cookie HTTP	Limite de mémoire. Dans CookieInsert, si le délai d'attente n'est pas égal à 0, le nombre de connexions est limité par la mémoire.

Certains types de persistance sont spécifiques à certains types de serveurs virtuels. Le tableau suivant répertorie chaque type de persistance et indique quels types de persistance sont pris en charge sur chaque type de serveur virtuel.

Type de persistance	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge	SSL_TCP	RTSP	SIP_UDP
SOURCEI	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
INSERT À BISCUITS	Oui	Oui	Non	Non	Non	Non	Non	Non
SESSION SSL	Non	Oui	Non	Non	Oui	Oui	Non	Non

Support de persistance des sauvegardes

Vous pouvez configurer le serveur virtuel de commutation de contenu pour qu'il utilise le type de persistance de l'adresse IP source comme type de persistance de sauvegarde lorsque le type de persistance des cookie échoue. Il est utile pour les déploiements Canary dans l'architecture des microservices.

Lorsque le type de persistance des cookies échoue, l'appliance revient à la persistance basée sur l'adresse IP source uniquement lorsque le navigateur client ne renvoie aucun cookie dans la demande. Toutefois, si le navigateur renvoie un cookie (pas nécessairement le cookie de persistance), il est supposé qu'il prend en charge les cookies et que la persistance des sauvegardes n'est donc pas déclenchée.

Vous pouvez également définir une valeur de délai d'expiration pour la persistance des sauvegardes. Le délai d'expiration est la période pendant laquelle une session de persistance est en vigueur.

Comment fonctionne la persistance sur le serveur virtuel de commutation de contenu

Scénario 1 : un serveur virtuel de commutation de contenu sans persistance

L'exemple suivant illustre le déploiement de plusieurs versions d'une application avec un serveur virtuel de commutation de contenu sans persistance.



Lorsque le client C1 envoie une demande à l'application, la demande est envoyée au serveur virtuel de commutation de contenu de l'appliance NetScaler. Le serveur virtuel de commutation de contenu évalue la politique et transmet la demande au serveur virtuel d'équilibrage de charge (LB1) qui fournit la version v1 de l'application.



Supposons qu'une nouvelle version v2 de l'application soit déployée et doive être exposée à un sous-ensemble d'utilisateurs. Le nouveau serveur virtuel d'équilibrage de charge (LB2) desservant la version v2 est lié au serveur virtuel de commutation de contenu par la politique de commutation de contenu appropriée.

Lorsque le client C1 envoie une nouvelle demande, la politique est à nouveau évaluée et la demande est transmise au serveur virtuel d'équilibrage de charge LB2. Ainsi, les transactions pour les applica-

tions statiques échouent si plusieurs versions de l'application sont déployées.

Scénario 2 : serveur virtuel de commutation de contenu avec persistance

L'exemple suivant illustre le déploiement de plusieurs versions de l'application avec un serveur virtuel de commutation de contenu avec persistance.



Lorsque le client C1 envoie une demande à l'application, la demande est envoyée au serveur virtuel de commutation de contenu de l'appliance NetScaler. Le serveur virtuel de commutation de contenu évalue la politique, crée une entrée de session de persistance et transmet la demande au serveur virtuel d'équilibrage de charge LB1 qui fournit la version v1 de l'application.



Le même client C1 demande à nouveau l'application, et la demande est envoyée au serveur virtuel de commutation de contenu de l'appliance NetScaler. Une recherche de la session de persistance est effectuée, et le serveur virtuel d'équilibrage de charge LB1 est extrait de la session de persistance existante et la demande est transmise à LB1. Aucune rupture de la transaction existante ne se produit avec cette solution, préservant ainsi le caractère dynamique de l'application.



Considérons un nouveau client C2. La nouvelle demande C2 est envoyée à la nouvelle version de l'application par le biais d'une évaluation des politiques car il n'existe aucune session de persistance pour ce client. Il en résulte un déploiement réussi de la nouvelle version de l'application sans en altérer le caractère dynamique.

Grâce à la prise en charge de la persistance, les clients peuvent déployer plusieurs contenus ou différentes versions de l'application de manière fluide sans affecter les transactions existantes, en particulier pour les applications statiques. Cela n'est pas possible sans persistance dans l'image.

Configurer le type de persistance sur le serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cs vserver <name> -PersistenceType <type> [-timeout <integer>]
<!--NeedCopy-->
```

Exemple :

```
set cs vserver Vserver-CS-1 -persistenceType SOURCEIP -timeout 60
```



```
<!--NeedCopy-->
```

Configurer le type de persistance sur le serveur virtuel de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels** et cliquez sur **Ajouter**.
2. Dans **Paramètres de base**, configurez les détails de persistance.

Dépannage

May 5, 2023

Si la fonctionnalité de commutation de contenu ne fonctionne pas comme prévu après l'avoir configurée, vous pouvez utiliser certains outils courants pour accéder aux ressources NetScaler et diagnostiquer le problème.

Ressources pour résoudre les problèmes liés au changement de contenu

Pour de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème de commutation de contenu sur une appliance NetScaler :

- Fichier de configuration
- `newnslog` Dossier pertinent
- Fichiers de traçage
- Schéma de topologie du réseau pour la configuration du réseau du client
- La documentation de NetScaler, telle que les notes de mise à jour, les articles du centre de connaissances et la documentation du produit.

Outre les ressources précédentes, les outils suivants accélèrent le dépannage :

- L'utilitaire `iehttpheaders` ou un utilitaire similaire
- L'application Wireshark personnalisée pour les fichiers de trace NetScaler
- Un utilitaire SSH pour l'accès en ligne de commande
- Un utilitaire HyperTerminal pour accéder à la console

Résolution des problèmes liés au changement de contenu

Les problèmes de changement de contenu les plus courants concernent le fait que la fonctionnalité de changement de contenu ne fonctionne pas du tout, ou ne fonctionne que de façon intermittente,

et les réponses « Service indisponible ».

- **Problème**

  La fonction de changement de contenu ne fonctionne pas.

  Résolution

  Vérifiez la configuration comme suit :

  - Vérifiez que l'appliance dispose d'une licence pour la commutation de contenu.
  - Vérifiez que la fonctionnalité est activée.
  - Dans le fichier de configuration, vérifiez que les politiques de commutation de contenu valides sont correctement liées aux serveurs virtuels d'équilibrage de charge.

- **Problème**

  Le client reçoit une réponse 503 indiquant que le service n'est pas disponible.

  Résolution

  - Vérifiez l'URL et les liaisons de politique. Le client reçoit la réponse 503 lorsqu'aucune des politiques que vous avez configurées n'est évaluée et qu'aucun serveur virtuel d'équilibrage de charge par défaut n'est défini et lié au serveur virtuel de commutation de contenu.
  - Dans la configuration, vérifiez les politiques et l'URL que le client accède à l'URL.
  - Vérifiez que la politique correspondante est évaluée pour chaque type de demande. Si la politique n'est pas évaluée, vérifiez l'expression de la politique et mettez-la à jour si nécessaire.
  - Vérifiez l'URL et les en-têtes de requête et de réponse HTTP. Pour ce faire, enregistrez une `HTTPHeader` trace et, si nécessaire, enregistrez les traces des paquets sur l'appliance et le client.

- **Problème**

  Par intermittence, la fonctionnalité de changement de contenu ne fonctionne pas comme prévu.

  Résolution

  - Étudiez le schéma de topologie du réseau, s'il est disponible, de la configuration pour comprendre les différents périphériques installés entre le client et les serveurs.
  - Vérifiez la configuration et les liens entre les politiques. Assurez-vous que l'URL de l'expression de politique correspond à celle de la demande du client.
  - Vérifiez que les priorités appropriées sont attribuées aux politiques. Une priorité ou une priorité incorrecte attribuée à une politique peut poser problème.

- Exécutez les commandes suivantes pour vérifier les liaisons et les valeurs des compteurs de sélection des politiques dans la sortie des commandes :

  ```
  show cs vserver \<CS VServer\>

  show cs policy \<CS Policy\>

  stat cs vserver \<CS VServer\>
  ```

- À l'aide `iehttpheaders` d'un utilitaire similaire, déterminez si les en-têtes HTTP des demandes ou des réponses fournissent des indications sur le problème.
- Consultez les notes de mise à jour et les articles du centre de connaissances.
- Si le problème n'est toujours pas résolu, contactez le support technique de Citrix en fournissant les données appropriées pour une enquête plus approfondie.

DataStream

May 5, 2023

La fonctionnalité NetScaler DataStream fournit un mécanisme intelligent de commutation des demandes au niveau de la couche de base de données en distribuant les demandes en fonction de la requête SQL envoyée.

Lorsqu'elle est déployée devant des serveurs de base de données, une appliance NetScaler garantit une distribution optimale du trafic en provenance des serveurs d'applications et des serveurs Web. Les administrateurs peuvent segmenter le trafic en fonction des informations contenues dans la requête SQL et en fonction des noms de base de données, des noms d'utilisateur, des jeux de caractères et de la taille des paquets.

Vous pouvez configurer l'équilibrage de charge pour commuter les demandes en fonction d'algorithmes d'équilibrage de charge. Vous pouvez également élaborer les critères de commutation en configurant la commutation de contenu pour prendre une décision en fonction d'un paramètre de requête SQL. Vous pouvez également configurer des moniteurs pour suivre l'état des serveurs de base de données.

> **Remarque**
>
> NetScaler DataStream est uniquement pris en charge pour les bases de données MySQL et MS SQL. Pour plus d'informations sur la version du protocole prise en charge, les jeux de caractères, les requêtes spéciales et les transactions, consultez DataStream Reference.

Comment fonctionne DataStream

Dans DataStream, l'appliance ADC est placée en ligne entre les serveurs d'applications ou Web et les serveurs de base de données. Sur l'appliance, les serveurs de base de données sont représentés par des services.

Un déploiement DataStream classique comprend les entités décrites dans le schéma suivant.

Figure 1. Modèle d'entité DataStream



Comme le montre cette figure, une configuration DataStream peut comprendre :

- Un serveur virtuel de commutation de contenu (CS) en option.
- Configuration d'équilibrage de charge composée de serveurs virtuels d'équilibrage de charge (LB1 et LB2).
- Services (Svc1, Svc2, Svc3 et Svc4).
- Politiques de changement de contenu (facultatif).

Les clients (serveurs d'applications ou serveurs Web) envoient des demandes à l'adresse IP d'un serveur virtuel de commutation de contenu (CS) configuré sur l'appliance NetScaler. L'appliance authentifie ensuite les clients à l'aide des informations d'identification utilisateur de base de données configurées sur l'appliance. Le serveur virtuel de commutation de contenu (CS) applique les

politiques de commutation de contenu associées aux demandes. Après avoir évalué les politiques, le serveur virtuel de commutation de contenu (CS) achemine les demandes vers le serveur virtuel d'équilibrage de charge approprié (LB1 ou LB2). Le serveur virtuel d'équilibrage de charge distribue ensuite les demandes aux serveurs de base de données appropriés (représentés par les services de l'appliance) en fonction de l'algorithme d'équilibrage de charge. L'appliance NetScaler utilise les mêmes informations d'identification utilisateur de base de données pour authentifier la connexion avec le serveur de base de données.

Si aucun serveur virtuel de commutation de contenu n'est configuré sur l'appliance, les clients (serveurs d'applications ou Web) envoient leurs demandes à un serveur virtuel d'équilibrage de charge configuré sur l'appliance. L'appliance NetScaler authentifie le client à l'aide des informations d'identification utilisateur de base de données configurées sur l'appliance, puis utilise les mêmes informations d'identification pour authentifier la connexion avec le serveur de base de données. Le serveur virtuel d'équilibrage de charge distribue les demandes aux serveurs de base de données conformément à l'algorithme d'équilibrage de charge. L'algorithme d'équilibrage de charge le plus efficace pour le changement de base de données est la méthode de moindre connexion.

DataStream utilise le multiplexage des connexions pour permettre à plusieurs demandes côté client d'être effectuées via la même connexion côté serveur. Les propriétés de connexion suivantes sont prises en compte :

- Nom d'utilisateur
- Database name
- Taille du paquet
- Set de caractères

Configurer les utilisateurs de base

August 20, 2021

Dans les bases de données, une connexion est toujours avec état, ce qui signifie que lorsqu'une connexion est établie, elle doit être authentifiée.

Configurez votre nom d'utilisateur et votre mot de passe de base de données sur l'appliance NetScaler. Par exemple, si vous avez un utilisateur John configuré sur la base de données, vous devez également configurer l'utilisateur John sur ADC. L'ajout de noms d'utilisateur et de mots de passe de base de données sur ADC les ajoute au fichier `nsconfig`.

> **Remarque**
>
> Les noms sont sensibles à la casse.

ADC utilise ces informations d'identification utilisateur pour authentifier les clients, puis authentifier les connexions serveur avec les serveurs de base de données.

Ajouter un utilisateur de base de données à l'aide de la CLI

À l'invite de commandes, tapez

```
add db user <username> - password <password>
```

Exemple :

```
1 add db user nsdbuser -password dd260427edf
2 <!--NeedCopy-->
```

Ajouter un utilisateur de base de données à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données** et configurez un utilisateur de base de données.

Si vous avez modifié le mot de passe de l'utilisateur de base de données sur le serveur de base de données, vous devez réinitialiser le mot de passe de l'utilisateur correspondant configuré sur l'appliance ADC.

Réinitialiser le mot de passe d'un utilisateur de base de données à l'aide de la CLI

À l'invite de commandes, tapez

```
1 set db user <username> -password <password>
2 <!--NeedCopy-->
```

Exemple :

```
1 set db user nsdbuser -password dd260538abs
2 <!--NeedCopy-->
```

Réinitialiser le mot de passe des utilisateurs de base de données en utilisant l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données**, sélectionnez un utilisateur et entrez de nouvelles valeurs pour le mot de passe.

Si un utilisateur de base de données n'existe plus sur le serveur de base de données, vous pouvez le supprimer de l'appliance ADC. Toutefois, si l'utilisateur continue d'exister sur le serveur de base

de données et que vous supprimez l'utilisateur de l'appliance ADC, toute demande du client portant ce nom d'utilisateur n'est pas authentifiée. Par conséquent, la demande n'est pas acheminée vers le serveur de base de données.

Supprimer un utilisateur de base de données à l'aide de la CLI

À l'invite de commandes, tapez

```
rm db user <username>
<!--NeedCopy-->
```

Exemple :

```
rm db user nsdbuser
<!--NeedCopy-->
```

Supprimer un utilisateur de base de données à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données**, sélectionnez un utilisateur et cliquez sur **Supprimer**.

Configurer un profil de base de données

August 20, 2021

Un profil de base de données est un ensemble nommé de paramètres configurés une fois mais appliqués à plusieurs serveurs virtuels qui nécessitent ces paramètres particuliers. Après avoir créé un profil de base de données, vous le liez à des serveurs virtuels d'équilibrage de charge ou de commutation de contenu. Vous pouvez créer autant de profils que vous le souhaitez.

Créer un profil de base de données à l'aide de la CLI

Sur la ligne de commande, tapez les commandes suivantes pour créer un profil de base de données et vérifier la configuration :

```
add db dbProfile <name> [-interpretQuery ( YES | NO )] [-stickiness (
    YES | NO )] [-kcdAccount <string>]

show db dbProfile
<!--NeedCopy-->
```


Exemple :

```
> add dbProfile myDBProfile -interpretQuery YES -stickiness YES -
    kcdAccount mykcdaccnt
 Done
> show dbProfile myDBProfile
    Name: myDBProfile
    Interpret Query: YES
    Stickyness: YES
    KCD Account: mykcdaccnt
    Reference count: 0

 Done
>
<!--NeedCopy-->
```

Créer un profil de base de données à l'aide de l'interface graphique

Accédez à **Système > Profils** et, sous l'onglet **Profils de base** de données, configurez un profil de base de données.

Liez un profil de base de données à un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez :

```
set (lb | cs) vserver <name> -dbProfileName <string>
<!--NeedCopy-->
```

Liez un profil de base de données à un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels ou Gestion du trafic > Commutation de contenu > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Profils**et, dans la liste **Profil DB**, sélectionnez un profil à lier au serveur virtuel. Pour créer un profil, cliquez sur plus (+).

Configurer l'équilibrage de charge pour DataStream

May 5, 2023

Avant de configurer une configuration d'équilibrage de charge, vous devez activer la fonctionnalité d'équilibrage de charge. Commencez ensuite par créer au moins un service pour chaque serveur de base de données du groupe d'équilibrage de charge. Une fois les services configurés, vous êtes prêt à créer un serveur virtuel d'équilibrage de charge et à lier les services au serveur virtuel.

> **Remarque** :
>
> Pour les bases de données, l'équilibrage de charge ne peut avoir lieu que sur des serveurs de base de données homogènes (serveurs de base de données qui contiennent exactement les mêmes bases de données). Pour une configuration qui contient des bases de données uniques sur différents serveurs, vous devez utiliser la commutation de contenu. Si certains de vos serveurs de base de données hébergent un contenu identique, vous pouvez utiliser l'équilibrage de charge sur ces serveurs uniquement. Vous pouvez ensuite utiliser des stratégies de commutation de contenu pour envoyer des demandes au serveur virtuel d'équilibrage de charge qui gère l'équilibrage de charge pour ces bases de données.
>
> L'appliance NetScaler stocke actuellement le nom de la base de données et les informations de connexion pendant la session de base de données. Lorsqu'une requête est effectuée dans la base de données, elle utilise ces informations pour se connecter au serveur de base de données spécifique.

Valeurs de paramètres spécifiques à DataStream

- Protocole

  Utilisez le type de protocole MYSQL pour les bases de données MySQL et le type de protocole MSSQL pour les bases de données MS SQL lors de la configuration des serveurs et services virtuels. Les protocoles MySQL et TDS sont utilisés par les clients pour communiquer avec les serveurs de base de données respectifs à l'aide de requêtes SQL. Pour plus d'informations sur le protocole MySQL, reportez-vous à la section http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Pour plus d'informations sur le protocole TDS, reportez-vous à la section http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Port sur lequel le serveur virtuel écoute les connexions client. Utilisez le port 3306 pour les serveurs de bases de données MySQL.

- Méthode

  Il est recommandé d'utiliser la méthode de moindre connexion pour un meilleur équilibrage de charge et une réduction de la charge du serveur. Toutefois, d'autres méthodes, telles que le Round Robin, le temps de réponse le plus court, le hachage IP source, le hachage IP source de destination, le minimum de bande passante, le moins de paquets et le hachage du port source IP source, sont également prises en charge.

Remarque : La méthode de hachage d'URL n'est pas prise en charge pour DataStream.

- Version de MS SQL Server

  Si vous utilisez Microsoft SQL Server et que vous pensez que certains clients exécutent une version différente de celle de votre produit Microsoft SQL Server, définissez le paramètre Version du serveur pour le serveur virtuel d'équilibrage de charge. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur. Pour plus d'informations sur la définition du paramètre Server Version, consultez Configuration du paramètre de version MySQL et Microsoft SQL Server.

- Version du serveur MySQL

  Si vous utilisez le serveur MySQL et que vous vous attendez à ce que certains clients exécutent une version différente de celle de votre produit MySQL Server, définissez le paramètre Version du serveur pour le serveur virtuel d'équilibrage de charge. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur. Pour plus d'informations sur la définition du paramètre Server Version, consultez Configuration du paramètre de version MySQL et Microsoft SQL Server.

Configurer la commutation de contenu pour DataStream

May 5, 2023

Vous pouvez segmenter le trafic en fonction des informations contenues dans la requête SQL, en fonction des noms de base de données, des noms d'utilisateur, des jeux de caractères et de la taille des paquets.

Vous pouvez configurer des stratégies de commutation de contenu avec des expressions de stratégie avancées pour basculer le contenu en fonction des propriétés de connexion. Par exemple, le nom d'utilisateur et le nom de la base de données, les paramètres de commande et la requête SQL pour sélectionner le serveur.

Les expressions de stratégie avancées évaluent le trafic associé aux serveurs de bases de données MYSQL et MS SQL. Utilisez des expressions basées sur les demandes dans les stratégies de stratégie avancées pour prendre des décisions de changement de demande au point de liaison du serveur virtuel de commutation de contenu. Utilisez des expressions basées sur les réponses (expressions commençant par MYSQL.RES) pour évaluer les réponses du serveur aux moniteurs d'intégrité configurés par l'utilisateur.

Pour plus d'informations sur les expressions de stratégie avancées, consultez Expressions de stratégie avancées : DataStream.

> **Remarque :**
>
> Pour les bases de données, l'équilibrage de charge ne peut avoir lieu que sur des serveurs de base de données homogènes (serveurs de base de données qui contiennent exactement les mêmes bases de données). Pour une configuration qui contient des bases de données uniques sur différents serveurs, vous devez utiliser la commutation de contenu. Si certains de vos serveurs de base de données hébergent un contenu identique, vous pouvez utiliser l'équilibrage de charge sur ces serveurs uniquement. Vous pouvez ensuite utiliser des stratégies de commutation de contenu pour envoyer des demandes au serveur virtuel d'équilibrage de charge qui gère l'équilibrage de charge pour ces bases de données.
>
> L'appliance NetScaler stocke actuellement le nom de la base de données et les informations de connexion pendant la session de base de données. Lorsqu'une requête est effectuée dans la base de données, elle utilise ces informations pour se connecter au serveur de base de données spécifique.

Valeurs de paramètres spécifiques à DataStream

- Protocole

  Utilisez le type de protocole MYSQL pour les bases de données MySQL et le type de protocole MSSQL pour les bases de données MS SQL lors de la configuration des serveurs et services virtuels. Les protocoles MySQL et TDS sont utilisés par les clients pour communiquer avec les serveurs de base de données respectifs à l'aide de requêtes SQL. Pour plus d'informations sur le protocole MySQL, reportez-vous à la section http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Pour plus d'informations sur le protocole TDS, reportez-vous à la section http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Port sur lequel le serveur virtuel écoute les connexions client. Utilisez le port 3306 pour les serveurs de bases de données MySQL.

- Version de MS SQL Server

  Si vous utilisez Microsoft SQL Server et que vous attendez que certains clients exécutent une version différente de celle de votre produit Microsoft SQL Server, définissez le paramètre Version du serveur pour le serveur virtuel de commutation de contenu. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur. Pour plus d'informations sur la définition du paramètre Server Version, consultez Configuration du paramètre de version Microsoft SQL Server.

Configurer des moniteurs pour DataStream

August 20, 2021

Pour suivre l'état de chaque serveur de base de données à charge équilibrée en temps réel, vous devez lier un moniteur à chaque service. Le moniteur est configuré pour tester le service en envoyant des sondes périodiques au service, parfois appelées exécution d'une vérification de l'état. Si le moniteur reçoit une réponse rapide à ses sondes, il marque le service comme UP. S'il ne reçoit pas de réponse en temps opportun au nombre désigné de sondes, il marque le service comme DOWN.

Pour DataStream, vous devez utiliser les moniteurs intégrés : MYSQL-ECV et MSSQL-ECV. À l'aide de ce moniteur, vous pouvez envoyer une requête SQL et analyser la réponse pour une chaîne.

Avant de configurer des moniteurs pour DataStream, vous devez ajouter des informations d'identification utilisateur de base de données à votre appliance NetScaler. Pour plus d'informations sur la configuration des moniteurs, voir Configurer les moniteurs dans une configuration d'équilibrage de charge.

Lorsque vous créez un moniteur, une connexion TCP est établie avec le serveur de base de données et la connexion est authentifiée à l'aide du nom d'utilisateur fourni lors de la création du moniteur. Vous pouvez ensuite exécuter une requête SQL sur le serveur de base de données et évaluer la réponse du serveur pour vérifier si elle correspond à la règle configurée.

Les exemples suivants concernent les serveurs MYSQL.

Exemples :

Dans l'exemple suivant, la valeur du message d'erreur est évaluée pour déterminer l'état du serveur.

```
add lb monitor lb_mon1 MYSQL-ECV -sqlQuery "select * from
table2;" -evalrule "mysql.res.error.message.contains("Invalid
User")"-database "NS" -userName "user1"
<!--NeedCopy-->
```

Dans l'exemple suivant, le nombre de lignes dans la réponse est évalué pour déterminer l'état du serveur.

```
add lb monitor lb_mon4 MYSQL-ECV -sqlQuery "select * from
table4;" -evalrule "mysql.res.atleast_rows_count(7)" -database "NS" -
   userName "user2"
<!--NeedCopy-->
```

Dans l'exemple suivant, la valeur d'une colonne particulière est évaluée pour déterminer l'état du serveur.

```
add lb monitor lb_mon3 MYSQL-ECV
```



```
-sqlQuery "select * from ABC;" -evalrule "mysql.res.row(1).double_elem
   (2) == 345.12"
-database "NS" -userName "user3"
<!--NeedCopy-->
```

Les exemples suivants concernent les serveurs MSSQL.

Exemples :

Dans l'exemple suivant, la valeur du message d'erreur est évaluée pour déterminer l'état du serveur.

```
add lb monitor lb_mon1 MSSQL-ECV -sqlQuery "select * from
table2;" -evalrule "mssql.res.error.message.contains("Invalid
User")"-database "NS" -userName "user1"
<!--NeedCopy-->
```

Dans l'exemple suivant, le nombre de lignes dans la réponse est évalué pour déterminer l'état du serveur.

```
add lb monitor lb_mon4 MSSQL-ECV -sqlQuery "select * from
table4;" -evalrule "mssql.res.atleast_rows_count(7)" -database "NS" -
   userName "user2"
<!--NeedCopy-->
```

Dans l'exemple suivant, la valeur d'une colonne particulière est évaluée pour déterminer l'état du serveur.

```
add lb monitor lb_mon3 MSSQL-ECV
-sqlQuery "select * from ABC;" -evalrule "mssql.res.row(1).double_elem
   (2) == 345.12"
-database "NS" -userName "user3"
<!--NeedCopy-->
```

Cas d'utilisation 1 : Configuration de DataStream pour une architecture de base de données primaire/secondaire

May 5, 2023

Un scénario de déploiement couramment utilisé est l'architecture de base de données principale/secondaire dans laquelle la base de données principale réplique toutes les informations vers les bases de données secondaires.

Pour l'architecture de base de données principale/secondaire, vous pouvez souhaiter que toutes les demandes WRITE soient envoyées à la base de données principale et toutes les demandes READ aux bases de données secondaires.

La figure suivante montre les entités et les valeurs des paramètres que vous devez configurer sur l'appliance.

Figure 1. Modèle d'entité DataStream pour la configuration de la base de données principale/secondaire



Dans cet exemple de scénario, un service (SVC_MySQL_1) est créé pour représenter la base de données principale et est lié à un serveur virtuel d'équilibrage de charge (LB_VSR_MySQL_Primary). Trois autres services (SVC_MySQL_2, SVC_MySQL_3 et SVC_MySQL_4) sont créés pour représenter les trois bases de données secondaires, et ils sont liés à un autre serveur virtuel d'équilibrage de charge (LB_vsr_MySQL_Secondary).

Un serveur virtuel de commutation de contenu (CS_VSR_MySQL_1) est configuré avec des stratégies associées pour envoyer toutes les demandes d'écriture au serveur virtuel d'équilibrage de charge, LB_VSR_MySQL_Primary. Toutes les demandes READ sont envoyées au serveur virtuel d'équilibrage de charge, LB_VSR_MySQL_Secondary.

Lorsqu'une demande atteint le serveur virtuel de commutation de contenu, le serveur virtuel ap-

plique les stratégies de commutation de contenu associées à cette demande. Après avoir évalué les stratégies, le serveur virtuel de commutation de contenu achemine la demande vers le serveur virtuel d'équilibrage de charge approprié, qui l'envoie au service approprié.

Le tableau suivant répertorie les noms et les valeurs des entités ainsi que la politique configurée sur l'appliance NetScaler.

Type d'entité	Nom	Adresse IP	Protocole	Port	Expression
Services	Svc_mysql_1	198.51.100.5	MYSQL	3306	SO
	Svc_mysql_2	198.51.100.6	MYSQL	3306	SO
	Svc_mysql_3	198.51.100.7	MYSQL	3306	SO
	Svc_mysql_4	198.51.100.8	MYSQL	3306	SO
Surveiller	lb_mon1	SO	MYSQL-ECV	SO	mysql.res.atleast_rows_cou
Équilibrage de charge des serveurs virtuels	Lb_vsr_mysql_primary	198.51.100.201	MYSQL	3306	SO
	Lb_vsr_mysql_	198.51.100.202	MYSQL	3306	SO
Serveur virtuel de commutation de contenu	Cs_vsr_mysql_1	198.51.100.161	MYSQL	3306	SO
Politique de commutation de contenu	Cs_select	SO	SO	SO	`MYSQL.REQ.QUERY.COMMAND.contains("select")`

Tableau 1. Noms et valeurs des entités et des politiques

Pour configurer DataStream pour une configuration de base de données principale/secondaire à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez

```
add db user user1 -password user1

add service Svc_mysql_1 198.51.100.5 mysql 3306
```



```
4
5  add service Svc_mysql_2 198.51.100.6 mysql 3306
6
7  add service Svc_mysql_3 198.51.100.7 mysql 3306
8
9  add service Svc_mysql_4 198.51.100.8 mysql 3306
10
11 add lb monitor lb_mon1 MYSQL-ECV -sqlQuery "select * from table1;" -
      evalrule "mysql.res.atleast_rows_count(1)" -database "NS" -userName
       "user1"
12
13 add lb vserver Lb_vsr_mysql_primary mysql 198.51.100.201 3306
14
15 add lb vserver Lb_vsr_mysql_secondary mysql 198.51.100.202 3306
16
17 bind lb vserver Lb_vsr_mysql_primary svc_mysql_1
18
19 bind lb vserver Lb_vsr_mysql_secondary svc_mysql_2
20
21 bind lb vserver Lb_vsr_mysql_secondary svc_mysql_3
22
23 bind lb vserver Lb_vsr_mysql_secondary svc_mysql_4
24
25 add cs vserver Cs_vsr_mysql_1 mysql 198.51.100.161 3306
26
27 add cs policy Cs_select  -rule "MYSQL.REQ.QUERY.COMMAND.contains("
      select")"
28
29 bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_primary
30
31 bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_secondary  -policy
      Cs_select  -priority 10
32
33 bind service Svc_mysql_1 -monitorName lb_mon1
34
35 bind service Svc_mysql_2 -monitorName lb_mon1
36
37 bind service Svc_mysql_3 -monitorName lb_mon1
38
39 bind service Svc_mysql_4 -monitorName lb_mon1
40 <!--NeedCopy-->
```


Cas d'utilisation 2 : Configuration de la méthode d'équilibrage de charge par jeton pour DataStream

May 5, 2023

Vous pouvez configurer la méthode d'équilibrage de charge par jeton pour DataStream afin de baser la sélection des serveurs de base de données sur la valeur du jeton extrait des demandes du client (application ou serveur Web). Ces jetons sont définis à l'aide d'expressions SQL. Pour les demandes suivantes avec le même jeton, l'appliance NetScaler envoie les demandes au même serveur de base de données qui a traité la demande initiale. Les demandes avec le même jeton sont envoyées au même serveur de base de données jusqu'à ce que la limite maximale de connexion soit atteinte ou que l'entrée de session soit dépassée.

Vous pouvez utiliser les exemples d'expressions SQL suivants pour définir des jetons :

MySQL	MS SQL
MYSQL.REQ.QUERY.TEXT	MSSQL.REQ.QUERY.TEXT
MYSQL.REQ.QUERY.TEXT (n)	MSSQL. REQ.QUERY.TEXT (n)
MYSQL.REQ.QUERY.COMMAND	MSSQL.REQ.QUERY.COMMAND
MYSQL.CLIENT.USER	MSSQL.CLIENT.USER
MYSQL.CLIENT.DATABASE	MSSQL.CLIENT.DATABASE
MYSQL.CLIENT.CAPABILITIES	

L'exemple suivant montre comment fonctionne la fonctionnalité NetScaler DataStream lorsque vous configurez la méthode d'équilibrage de charge par jeton.

Figure 1. DataStream et la méthode d'équilibrage de charge basée sur des jetons



Dans cet exemple, le jeton est le nom de la base de données. Une demande contenant des carnets de jetons est envoyée au serveur de base de données 1 et une demande contenant de la musique à jetons est envoyée au serveur de base de données 2. Toutes les demandes suivantes contenant des carnets de jetons sont envoyées au serveur de base de données 1 et les demandes contenant de la musique de jetons sont envoyées au serveur de base de données 2. Cette configuration fournit une pseudo-persistance avec les serveurs de base de données.

Configurez cet exemple à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service Service1 192.0.2.9 MYSQL 3306

add service Service2 192.0.2.11 MYSQL 3306

add lb vserver token_lb_vserver MYSQL 192.0.2.15 3306 -lbmethod token -
    rule MYSQL.CLIENT.DATABASE

bind lb vserver token_lb_vserver Service1

bind lb vserver token_lb_vserver Service2
<!--NeedCopy-->
```

Configurez cet exemple à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, configurez un serveur virtuel et spécifiez le protocole comme **MYSQL**.

2. Cliquez dans la section **Service** et configurez deux services en spécifiant le protocole comme MYSQL. Liez ces services au serveur virtuel.
3. Dans **Paramètres avancés**, cliquez sur **Méthode** et, dans la liste des méthodes d' **équilibrage de charge**, sélectionnez **TOKEN** et spécifiez l'expression **MYSQL.CLIENT.DATABASE**.

Cas d'utilisation 3 : consigner les transactions MSSQL en mode transparent

May 5, 2023

Vous pouvez configurer l'appliance NetScaler pour qu'elle fonctionne de manière transparente entre les clients et les serveurs MSSQL, et pour enregistrer ou analyser uniquement les détails de toutes les transactions client-serveur. Le mode transparent est conçu pour que l'appliance NetScaler transfère uniquement les requêtes MSSQL au serveur, puis relaie les réponses du serveur aux clients. Lorsque les demandes et les réponses transitent par l'appliance, celle-ci enregistre les informations collectées à partir de celles-ci, comme spécifié par la journalisation des audits ou la configuration AppFlow, ou collecte des statistiques, comme spécifié par la configuration d'Action Analytics. Il n'est pas nécessaire d'ajouter des utilisateurs de base de données à l'appliance.

Lorsqu'elle fonctionne en mode transparent, l'appliance NetScaler n'effectue pas d'équilibrage de charge, de commutation de contenu ou de multiplexage des connexions pour les demandes. Toutefois, il répond au paquet de pré-connexion d'un client pour le compte du serveur afin d'empêcher que le chiffrement ne soit convenu lors de l'établissement de contact préalable à la connexion. Le paquet de connexion et les paquets suivants sont transmis au serveur.

Récapitulatif des tâches de configuration

Pour enregistrer ou analyser les requêtes MSSQL en mode transparent, vous devez procéder comme suit :

- Configurez l'appliance NetScaler comme passerelle par défaut pour les clients et les serveurs.
- Effectuez l'une des opérations suivantes sur l'appliance NetScaler :
  - **Configurez l'option Utiliser l'adresse IP source (USIP) de manière globale :** créez un serveur virtuel d'équilibrage de charge avec une adresse IP générique et le numéro de port sur lequel les serveurs MSSQL écoutent les demandes (un serveur virtuel générique spécifique au port). Activez ensuite l'option USIP globalement. Si vous configurez un serveur virtuel générique spécifique à un port, il n'est pas nécessaire de créer des services MSSQL sur l'appliance. L'appliance découvre les services en fonction de l'adresse IP de destination figurant dans les demandes du client.

  - **Si vous ne souhaitez pas configurer l'option USIP de manière globale :** créez des services MSSQL en activant l'option USIP sur chacun d'eux. Si vous configurez des services, il n'est pas nécessaire de créer un serveur virtuel générique spécifique au port.
- Configurez la journalisation des audits, AppFlow ou Action Analytics pour enregistrer ou collecter des statistiques sur les demandes. Si vous configurez un serveur virtuel, vous pouvez lier vos politiques au serveur virtuel ou au point de liaison global. Si vous ne configurez pas de serveur virtuel, vous pouvez lier vos politiques uniquement au point de liaison global.

Configurer le mode transparent à l'aide d'un serveur virtuel à caractères génériques

Vous pouvez configurer le mode transparent en configurant un serveur virtuel générique spécifique au port et en activant le mode Utiliser l'adresse IP source (USIP) globalement. Lorsqu'un client envoie à sa passerelle par défaut (l'appliance NetScaler) une demande avec l'adresse IP d'un serveur MSSQL dans l'en-tête de l'adresse IP de destination, l'appliance vérifie si l'adresse IP de destination est disponible. Si l'adresse IP est disponible, le serveur virtuel transmet la demande au serveur. Dans le cas contraire, il supprime la demande.

Création d'un serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel générique et vérifier la configuration :

```
add lb vserver <name> <serviceType> <IPAddress> <port>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
> add lb vserver wildcardLbVs MSSQL * 1433
 Done
> show lb vserver wildcardLbVs
    wildcardLbVs (*:1433) - MSSQL   Type: ADDRESS
    State: UP
    . . .

 Done
>
<!--NeedCopy-->
```


Création d'un serveur virtuel générique à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis créez un serveur virtuel. Spécifiez MSSQL comme protocole et * comme adresse IP.

Activez le mode Utiliser l'adresse IP source (USIP) globalement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer le mode USIP de manière globale et vérifier la configuration :

```
enable ns mode USIP

show ns mode
<!--NeedCopy-->
```

Exemple :

```
> enable ns mode USIP
 Done
> show ns mode

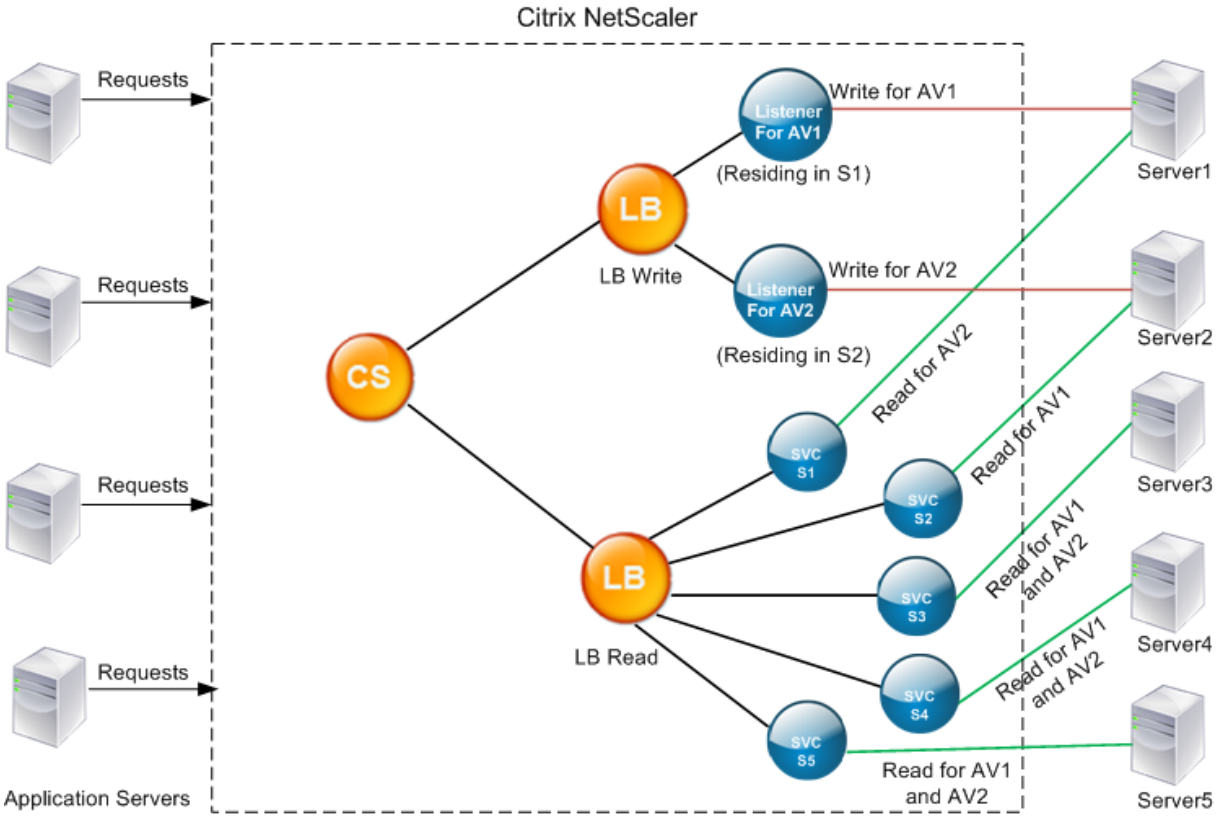
    Mode                                Acronym
       Status
    -------                             -------
       ------
                . . .
 3) Use Source IP                 USIP                            ON
                . . .
 Done
>
<!--NeedCopy-->
```

Activez le mode USIP globalement à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres** et, dans Modes et fonctionnalités, sélectionnez **Configurer les modes**.
2. Sélectionnez **Utiliser l'adresse IP source**.

Configuration du mode transparent à l'aide des services MSSQL

Vous pouvez configurer le mode transparent en configurant les services MSSQL et en activant USIP sur chaque service. Lorsqu'un client envoie à sa passerelle par défaut (l'appliance NetScaler) une de-

mande avec l'adresse IP d'un serveur MSSQL dans l'en-tête de l'adresse IP de destination, l'appliance transmet la demande au serveur de destination.

Créez un service MSSQL et activez le mode USIP sur le service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service MSSQL, avec USIP activé, et vérifiez la configuration :

```
add service <name> (<IP> | <serverName>) <serviceType> <port> -usip YES
    `

show service <name>
<!--NeedCopy-->
```

Exemple

```
> add service myDBservice 192.0.2.0 MSSQL 1433 -usip YES
 Done
> show service myDBservice
    myDBservice (192.0.2.0:1433) - MSSQL
    State: UP
                . . .
    Use Source IP: YES      Use Proxy Port: YES
                . . .
 Done
>
<!--NeedCopy-->
```

Créez un service MSSQL, avec USIP activé, à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis configurez un service.
2. Spécifiez le protocole **MSSQL** et, dans **Paramètres**, sélectionnez **Utiliser l'adresse IP source**.

Cas d'utilisation 4 : équilibrage de charge spécifique à la base de données

May 5, 2023

La charge d'un parc de serveurs de base de données doit être équilibrée non seulement en fonction de l'état des serveurs, mais également en fonction de la disponibilité de la base de données sur chaque serveur. Un service peut être actif et un dispositif d'équilibrage de charge peut indiquer qu'il est à l'état actif, mais la base de données demandée n'est peut-être pas disponible sur ce service. La demande n'est pas traitée si elle est transmise à un service sur lequel la base de données n'est pas disponible. Par conséquent, un dispositif d'équilibrage de charge doit être conscient de la disponibilité d'une base de données sur chaque service. Et lorsqu'il prend une décision d'équilibrage de charge, il doit uniquement prendre en compte les services sur lesquels la base de données est disponible.

À titre d'exemple, considérez que les serveurs de base de données serveur1, serveur2 et serveur3 hébergent les bases de données mydatabase1 et mydatabase2. Si mydatabase1 devient indisponible sur le serveur2, le dispositif d'équilibrage de charge doit être conscient de ce changement d'état. Il doit équilibrer la charge des demandes pour mydatabase1 uniquement sur le serveur1 et le serveur3. Une fois que mydatabase1 est disponible sur le serveur 2, le dispositif d'équilibrage de charge doit inclure le serveur 2 dans les décisions d'équilibrage de charge. De même, si mydatabase2 devient indisponible sur le serveur3, l'appareil doit équilibrer la charge des demandes pour mydatabase2 uniquement sur le serveur1 et le serveur2. Il doit inclure le serveur 3 dans ses décisions d'équilibrage de charge uniquement lorsque mydatabase2 sera disponible. Ce comportement d'équilibrage de charge doit être cohérent sur toutes les bases de données hébergées sur la batterie de serveurs.

L'appliance NetScaler met en œuvre ce comportement en récupérant la liste de toutes les bases de données actives sur un service. Pour récupérer la liste des bases de données actives, l'appliance utilise un moniteur configuré avec une requête SQL appropriée. Si la base de données demandée n'est pas disponible sur un service, l'appliance exclut le service des décisions d'équilibrage de charge jusqu'à ce qu'il soit disponible. Ce comportement garantit un service ininterrompu aux clients.

> **Remarque**
>
> L'équilibrage de charge spécifique à la base de données est pris en charge uniquement pour les types de service MSSQL et MySQL. Ce support est également disponible pour le déploiement de la haute disponibilité de Microsoft SQL Server 2012.

Pour configurer l'équilibrage de charge spécifique à la base de données, vous devez configurer les éléments suivants :

- Activez la fonctionnalité d'équilibrage de charge et configurez un serveur virtuel d'équilibrage de charge de type MSSQL ou MySQL.
- Configurez les services qui hébergent la base de données et liez-les au serveur virtuel. Le moniteur a besoin d'informations d'identification utilisateur valides pour se connecter au serveur de base de données. Vous devez donc configurer un compte utilisateur de base de données sur chacun des serveurs, puis ajouter le compte utilisateur à l'appliance NetScaler.
- Ensuite, vous configurez un moniteur MSSQL-ECV ou MYSQL-ECV et vous liez le moniteur à chaque service.

- Enfin, vous devez tester la configuration pour vous assurer qu'elle fonctionne comme prévu. Avant d'effectuer ces tâches de configuration, assurez-vous de bien comprendre le fonctionnement de l'équilibrage de charge spécifique à la base de données.

Comment fonctionne l'équilibrage de charge spécifique à la base de données

Pour un équilibrage de charge spécifique à une base de données, vous configurez un moniteur qui interroge régulièrement chaque serveur de base de données pour connaître les noms de toutes les bases de données actives qu'il contient. L'appliance NetScaler stocke les résultats et met régulièrement à jour les enregistrements en fonction des informations extraites lors de la surveillance. Lorsqu'un client interroge une base de données particulière, l'appliance utilise la méthode d'équilibrage de charge configurée pour sélectionner un service, puis vérifie ses enregistrements pour déterminer si la base de données est disponible sur ce service. Si les enregistrements indiquent que la base de données n'est pas disponible, elle utilise la méthode d'équilibrage de charge configurée pour sélectionner le prochain service disponible, puis répète la vérification. L'appliance transmet la requête au premier service disponible sur lequel la base de données est active.

Activer l'équilibrage de charge

Vous pouvez configurer des entités d'équilibrage de charge telles que des services et des serveurs virtuels lorsque la fonctionnalité d'équilibrage de charge est désactivée. Les entités ne fonctionnent pas tant que vous n'activez pas la fonctionnalité.

Activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

```
enable ns feature LB

show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
```



```
2)     Surge Protection                SP                    ON
3)     Load Balancing                  LB                    ON
.
.
.
24)    NetScaler Push                  push                  OFF
Done
<!--NeedCopy-->
```

Activer l'équilibrage de charge à l'aide de l'interface graphique

Accédez à **Système > Paramètres** et, dans **Configurer les fonctionnalités de base**, sélectionnez **Équilibrage de charge**.

Configurer un serveur virtuel d'équilibrage de charge pour un équilibrage de charge spécifique à la base de données

Pour configurer un serveur virtuel afin d'équilibrer la charge des bases de données en fonction de la disponibilité, vous activez le paramètre d'équilibrage de charge spécifique à la base de données sur le serveur virtuel. L'activation du paramètre modifie la logique d'équilibrage de charge afin que l'appliance NetScaler renvoie les résultats de la sonde de surveillance envoyée au service sélectionné, avant de transmettre la requête à ce service.

Configurer un serveur virtuel d'équilibrage de charge pour un équilibrage de charge spécifique à la base de données à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer un serveur virtuel d'équilibrage de charge pour un équilibrage de charge spécifique à la base de données et vérifier la configuration :

```
add lb vserver <name> <serviceType> <ipAddress> <port> -dbsLb ENABLED

show lb vserver <name>
<!--NeedCopy-->
```

Configurer les services

Après avoir activé la fonctionnalité d'équilibrage de charge, vous devez créer au moins un service pour chaque serveur d'applications à inclure dans votre configuration d'équilibrage de charge. Les services que vous configurez fournissent les connexions entre l'appliance NetScaler et les serveurs d'équilibrage de charge. Chaque service possède un nom et spécifie une adresse IP, un port et le type de données qui est servi.

Si vous créez un service sans créer au préalable un objet serveur, l'adresse IP du service est également le nom du serveur qui héberge le service. Si vous préférez identifier les serveurs par leur nom plutôt que par leur adresse IP, vous pouvez créer des objets serveur, puis spécifier le nom d'un serveur plutôt que son adresse IP lorsque vous créez un service.

Configuration des utilisateurs de la base

Dans les bases de données, une connexion est toujours active, ce qui signifie que lorsqu'une connexion est établie, elle doit être authentifiée.

Configurez le nom d'utilisateur et le mot de passe de votre base de données sur NetScaler. Par exemple, si vous avez configuré un utilisateur John sur la base de données, vous devez également configurer l'utilisateur John sur l'ADC. Les noms d'utilisateur et les mots de passe de base de données ajoutés à l'ADC sont ajoutés au `nsconfig` fichier.

> **Remarque**
>
> Les noms distinguent les majuscules et minuscules.

L'ADC utilise ces informations d'identification utilisateur pour authentifier les clients, puis authentifier les connexions aux serveurs de base de données.

Ajouter un utilisateur de base de données à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez

```
add db user <username> - password <password>
<!--NeedCopy-->
```

Exemple :

```
add db user nsdbuser -password dd260427edf
<!--NeedCopy-->
```

Ajouter un utilisateur de base de données à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base de données**, puis configurez un utilisateur de base de données.

Si vous avez modifié le mot de passe de l'utilisateur de base de données sur le serveur de base de données, vous devez réinitialiser le mot de passe de l'utilisateur correspondant configuré sur l'appliance NetScaler.

Réinitialisez le mot de passe d'un utilisateur de base de données à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez

```
set db user <username> -password <password>
<!--NeedCopy-->
```

Exemple :

```
set db user nsdbuser -password dd260538abs
<!--NeedCopy-->
```

Réinitialisez le mot de passe des utilisateurs de base de données à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de la base**de données, sélectionnez un utilisateur et entrez de nouvelles valeurs pour le mot de passe.

Si aucun utilisateur de base de données n'existe plus sur le serveur de base de données, vous pouvez le supprimer de l'appliance NetScaler. Toutefois, si l'utilisateur continue d'exister sur le serveur de base de données et que vous le supprimez de l'appliance ADC, aucune demande du client portant ce nom d'utilisateur n'est authentifiée. Par conséquent, le nom d'utilisateur n'est pas acheminé vers le serveur de base de données.

Supprimer un utilisateur de base de données à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez

```
rm db user <username>
<!--NeedCopy-->
```

Exemple :

```
rm db user nsdbuser
<!--NeedCopy-->
```

Supprimer un utilisateur de base de données à l'aide de l'interface graphique

Accédez à **Système > Administration des utilisateurs > Utilisateurs de base**de données, sélectionnez un utilisateur et cliquez sur **Supprimer**.

Configurer un moniteur pour récupérer les noms des bases de données actives

Vous pouvez créer un moniteur pour récupérer la liste de toutes les bases de données actives sur une instance de base de données. Le moniteur se connecte au serveur de base de données à l'aide d'informations d'identification utilisateur valides et exécute une requête SQL appropriée. La requête SQL que vous devez utiliser dépend du déploiement de votre serveur SQL. Par exemple, dans une configuration de mise en miroir de bases de données MSSQL, vous pouvez utiliser la requête suivante pour récupérer la liste des bases de données actives disponibles sur une instance de serveur.

```
select name from sys.databases where state=0
<!--NeedCopy-->
```

Dans une configuration de base de données MySQL, vous pouvez utiliser les requêtes suivantes pour récupérer la liste des bases de données actives disponibles sur une instance de serveur.

Afficher les bases de données :

Vous configurez également le moniteur pour évaluer la réponse à une condition d'erreur et pour stocker les résultats s'il n'y a pas d'erreur. Si la réponse contient une erreur, le moniteur marque le service comme étant hors service. L'appliance exclut le service des décisions d'équilibrage de charge jusqu'à ce qu'aucune erreur ne soit renvoyée.

> **Remarque**
>
> La fonctionnalité d'équilibrage de charge spécifique à la base de données est prise en charge uniquement pour les types de service MSSQL et MySQL. Par conséquent, le type de moniteur doit être MSSQL-ECV ou MYSQL-ECV.

Configurer un moniteur pour récupérer les noms de toutes les bases de données actives hébergées sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour récupérer les noms de toutes les bases de données actives hébergées sur un service et vérifier la configuration :

```
add lb monitor <monitorName> <type> -userName <string> -sqlQuery <text>
    -evalRule <expression> -storedb ENABLED

show lb monitor <monitorName>
<!--NeedCopy-->
```

Configurer un moniteur pour récupérer les noms de toutes les bases de données actives hébergées sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs** et configurez un moniteur de type MSSQL-ECV ou MYSQL-ECV.
2. Dans **Paramètres spéciaux**, spécifiez un nom d'utilisateur, une requête et une règle. Par exemple, pour MSSQL-ECV, la requête doit être « select name from sys.databases where state=0 ») et la règle doit être MSSQL.RES.TYPE.NE (ERROR). Pour MYSQL-ECV, la requête doit être « Afficher les bases de données » et la règle doit être MYSQL.RES.TYPE.NE (ERROR).

Prise en charge du déploiement de groupes de disponibilité pour MSSQL

Envisagez le scénario suivant dans lequel un équilibrage de charge spécifique à la base de données est configuré dans un déploiement de groupe de haute disponibilité. S1 à S5 sont les services de l'appliance ADC. DB1 à DB4 sont les bases de données sur les serveurs représentés par les services S1 à S5. AV1 et AV2 sont les groupes de disponibilité. Chaque groupe de disponibilité contient jusqu'à une instance de serveur de base de données principal et jusqu'à quatre instances de serveur de base de données secondaire. Un service, représentant les serveurs du groupe de disponibilité, peut être principal pour un groupe de disponibilité et secondaire pour un autre groupe de disponibilité. Chaque groupe de disponibilité contient différentes bases de données et un écouteur, qui est un service. Toutes les demandes arrivent sur le service d'écoute qui réside dans la base de données principale. AVI contient les bases de données DB1 et DB2. AV2 contient les bases de données DB3 et DB4. L1 et L2 sont les auditeurs d'AV1 et AV2 respectivement. S1 est le service principal pour AV1 et S2 est le service principal pour AV2.



Service	Liste des bases de données actives sur le service
S1	DB1, DB2, DB3, DB4
S2	DB3, DB4
S3	DB3, DB4
S4	DB1, DB2
S5	DB1, DB2

Groupe de disponibilité	Bases de données	Services représentant les serveurs du groupe de disponibilité
AV1	DB1, DB2	S1, S4, S5
AV2	DB3, DB4	S1, S2, S3

Les requêtes se déroulent comme suit :

1. Une requête READ pour AV1 est équilibrée en charge entre S4 et S5. S1 est le principal pour AV1.
2. Une requête WRITE pour AV1 est dirigée vers L1.
3. Une requête READ pour AV2 est équilibrée en charge entre S1 et S3. S2 est le principal pour AV2.
4. Une requête WRITE pour AV1 est dirigée vers L2.

Exemple de configuration

1. Configurez les serveurs virtuels d'équilibrage de charge et de commutation de contenu.
   - `add lb vserver lbwrite -dbslb enabled`
   - `add lbvserver lbread MSSQL -dbslb enabled`
   - `add csvserver csv MSSQL 1.1.1.10 1433`
2. Configurez deux services d'écoute, un pour chaque groupe de disponibilité, et cinq services S1 à S5 représentant les bases de données DB1 à DB4.
   - `add service L1 1.1.1.11 MSSQL 1433`
   - `add service L2 1.1.1.12 MSSQL 1433`
   - `add service s1 1.1.1.13 MSSQL 1433`
   - `add service s2 1.1.1.14 MSSQL 1433`
   - `add service s3 1.1.1.15 MSSQL 1433`
   - `add service s4 1.1.1.16 MSSQL 1433`
   - `add service s5 1.1.1.17 MSSQL 1433`
3. Liez les services aux serveurs virtuels d'équilibrage de charge.
   - `bind lbvserver lbwrite L1`
   - `bind lbvserver lbwrite L2`
   - `bind lbvserver lbread s1`
   - `bind lbvserver lbread s2`
   - `bind lbvserver lbread s3`
   - `bind lbvserver lbread s4`
   - `bind lbvserver lbread s5`
4. Configurer les utilisateurs de base de données.
   - `add db user nsdbuser1 -password dd260427edf`
   - `add db user nsdbuser2 -password ccd1234xyzw`
5. Configurez deux moniteurs, Monitor_L1 et Monitor_L2 pour chaque service d'écoute, afin de récupérer la liste des bases de données actives dans ce groupe de disponibilité. Ajoutez un moniteur, monitor1, pour récupérer la liste des bases de données pour l'instance de serveur de base de données secondaire.
   - ```
     add lb monitor monitor_L1 MSSQL-ECV -userName user1 -sqlQuery "
     SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_
      b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners
      c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a
      d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address
     ```


     ```

```
 like '1.1.1.11'"-evalRule "MSSQL.RES.TYPE.NE(ERROR)” -storedb
ENABLED
```

- `add lb monitor monitor_L2 MSSQL-ECV -userNameuser1 -sqlQuery "
SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replicca
 b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners
 c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a
 d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address
 like '1.1.1.12'"-evalRule "MSSQL.RES.TYPE.NE(ERROR)"-storedb
ENABLED`
- `add lb monitor monitor1 MSSQL-ECV -userNameuser1 -sqlQuery "SELECT
name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_states
 b ON a.replica_id=b.replica_id WHERE b.role = 2"-evalRule "MSSQL.
RES.TYPE.NE(ERROR)"-storedb ENABLED`

6. Configurez les politiques de lecture et d’écriture.
   - `add cs policy pol_write -rule "MSSQL.REQ.QUERY.TEXT.CONTAINS("
insert")"`
   - `add cs policy pol_read -rule "MSSQL.REQ.QUERY.TEXT.CONTAINS("select
")"`
7. Liez les politiques au serveur virtuel de commutation de contenu.
   - `bind csvserver csv -targetLBVserver lbwrite -policyName pol_write -
priority 11`
   - `bind csvserver csv -targetLBVserver lbread -policyName pol_read -
priority 12`
8. Liez les moniteurs aux services. Liez les moniteurs aux services L1 et L2 pour obtenir la liste des bases de données actives pour le groupe de disponibilité dont ils sont l’écouteur. Liez les moniteurs à tous les services liés au serveur virtuel en lecture seule.
   - `bind service L1 -monitorName monitor_L1`
   - `bind service L2 -monitorName monitor_L2`
   - `bind service s1 -monitorName monitor1`
   - `bind service s2 -monitorName monitor1`
   - `bind service s3 -monitorName monitor1`
   - `bind service s4 -monitorName monitor1`
   - `bind service s5 -monitorName monitor1`

Exemples de configuration pour le serveur virtuel MSSQL

Pour configurer un serveur virtuel d’équilibrage de charge pour un équilibrage de charge spécifique à la basede données :

```
1 add lb vserver DBSpecificLB1 MSSQL 192.0.2.10 1433 -dbsLb ENABLED
```



```
2
3 Done
4
5 show lb vserver DBSpecificLB1
6
7 DBSpecificLB1 (192.0.2.10:1433) - MSSQL Type: ADDRESS
8 . . .
9 DBS_LB: ENABLED
10
11 Done
12 <!--NeedCopy-->
```

Pour configurer les services :

ajouter le service msservice1 5.5.5.5 MSSQL 1433

Pour configurer un moniteur afin de récupérer les noms de toutes les bases de données actives hébergées sur un service à l'aide de la ligne de commande :

```
1 add lb monitor mssql-monitor1 MSSQL-ECV -userName user1 -sqlQuery "
     select name from sys.databases where state=0" -evalRule "MSSQL.RES.
     TYPE.NE(ERROR)" -storedb EN
2
3 Done
4
5 show lb monitor mssql-monitor1
6
7 1)   Name.......: mssql-monitor1    Type......: MSSQL-ECV
8
9 ...
10
11 Special parameters: Database.....:""
12
13 User name.....:"user1"
14
15 Query..:select name from sys.databases where state=0 EvalRule...:MSSQL.
     RES.TYPE.NE(ERROR)
16
17 Version...:70 STORE_DB...:ENABLED
18
19 Done
20 <!--NeedCopy-->
```


Exemples de configuration pour le serveur virtuel MySQL

Pour configurer un serveur virtuel d'équilibrage de charge pour un équilibrage de charge spécifique à la basede données :

```
add lb vserver DBSpecificLB1 MYSQL 192.0.2.10 3306 -dbsLb ENABLED

Done

show lb vserver DBSpecificLB1

DBSpecificLB1 (192.0.2.10:3306) - MYSQL Type: ADDRESS

. . .

DBS_LB: ENABLED

Done
<!--NeedCopy-->
```

Pour configurer les services :

```
add service msservice1 5.5.5.5 MYSQL 3306
<!--NeedCopy-->
```

Pour configurer un moniteur afin de récupérer les noms de toutes les bases de données actives hébergées sur un service à l'aide de la ligne de commande :

```
add lb monitor mysql-monitor1 MYSQL-ECV -userName user1 -sqlQuery "show
    databases" -evalRule "MYSQL.RES.TYPE.NE(ERROR)" -storedb ENABLED

Done

show lb monitor mysql-monitor1

1)     Name.......: mysql-monitor1  Type......: MYSQL-ECV  State....:
   ENABLED

...

Special parameters: Database.....:""

User name.....:"user1" Query..:show databases

EvalRule...:MYSQL.RES.TYPE.NE(ERROR) STORE_DB...:ENABLED
```



```
16
17 Done
18 <!--NeedCopy-->
```

Référence DataStream

May 5, 2023

Cette référence décrit les protocoles MySQL et TDS, les versions de base de données, les méthodes d'authentification et les jeux de caractères pris en charge par la fonctionnalité DataStream. Il décrit également la manière dont NetScaler gère les demandes de transaction et les requêtes spéciales qui modifient l'état d'une connexion.

Vous pouvez également configurer l'appliance NetScaler pour générer des messages de journal d'audit pour la fonctionnalité DataStream.

Versions de base de données, protocoles et méthodes d'authentification pris en charge

	Base de données MySQL	Base de données MS SQL
versions de base de données	Base de données MySQL versions 4.1, 5.0, 5.1, 5.4, 5.5, 5.6	Versions 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 de la base de données MS SQL (prise en charge de l'authentification Kerberos)
Protocoles	Protocole MySQL version 10. Pour plus d'informations sur le protocole MySQL, consultez MySQL Client/Server Protocol	Protocole TDS (Tabular Data Stream) version 7.1 et supérieure. Pour plus d'informations sur le protocole TDS, voir Tabular Data Stream Protocol.
Méthodes d'authentification	L'authentification native MySQL est prise en charge.	L'authentification SQL Server et l'authentification Windows (Kerberos/NTLM) sont prises en charge.

Ensembles de caractères

La fonctionnalité DataStream prend uniquement en charge le jeu de caractères UTF-8.

Le jeu de caractères utilisé par le client lors de l'envoi d'une demande peut être différent de celui utilisé dans les réponses du serveur de base de données. Bien que le paramètre charset soit défini lors de l'établissement de la connexion, il peut être modifié à tout moment en envoyant une requête SQL. Le jeu de caractères est associé à une connexion et, par conséquent, les demandes concernant des connexions utilisant un jeu de caractères ne peuvent pas être multiplexées sur une connexion avec un jeu de caractères différent.

L'appliance NetScaler analyse les requêtes envoyées par le client et les réponses envoyées par le serveur de base de données.

Le jeu de caractères associé à une connexion peut être modifié après la première prise de contact en utilisant les deux requêtes suivantes :

```
SET NAMES <charset> COLLATION <collation>

SET CHARACTER SET <charset>
<!--NeedCopy-->
```

Transactions

Dans MySQL, les transactions sont identifiées à l'aide du paramètre de connexion AUTOCOMMIT ou des requêtes BEGIN:COMMIT. Le paramètre AUTOCOMMIT peut être défini lors de l'établissement de la connexion initiale ou après l'établissement de la connexion à l'aide de la requête SET AUTOCOMMIT.

L'appliance NetScaler analyse explicitement chaque requête pour déterminer le début et la fin d'une transaction.

Dans le protocole MySQL, la réponse contient deux indicateurs pour indiquer si la connexion est une transaction : les indicateurs TRANSACTION et AUTOCOMMIT.

Si la connexion est une transaction, l'indicateur TRANSACTION est activé. Ou, si le mode AutoCommit est OFF, l'indicateur AUTOCOMMIT n'est pas défini. L'appliance ADC analyse la réponse et si l'indicateur TRANSACTION est défini ou si l'indicateur AUTOCOMMIT n'est pas défini, elle n'effectue pas de multiplexage des connexions. Lorsque ces conditions ne sont plus vraies, l'appliance ADC commence le multiplexage des connexions.

> **Remarque**
>
> Les transactions sont également prises en charge pour MS SQL.

Requêtes spéciales

Certaines requêtes spéciales, telles que SET et PREPARE, modifient l'état de la connexion et peuvent interrompre la commutation des requêtes. Par conséquent, ces requêtes doivent être traitées différemment.

À la réception d'une demande contenant des requêtes spéciales, l'appliance NetScaler envoie une réponse OK au client et enregistre également la demande dans la connexion.

Lorsqu'une requête non spéciale, telle que INSERT et SELECT, est reçue en même temps qu'une requête stockée, l'appliance ADC recherche la connexion côté serveur sur laquelle la requête stockée a déjà été envoyée au serveur de base de données. Si aucune connexion de ce type n'existe, l'appliance ADC crée une connexion et envoie d'abord la requête stockée, puis envoie la demande avec la requête non spéciale.

Dans les requêtes spéciales SET, USE db et INIT_DB, l'appliance modifie un champ de la connexion côté serveur correspondant à la requête spéciale. Cette modification permet une meilleure réutilisation de la connexion côté serveur.

Seules 16 requêtes sont stockées dans chaque connexion.

Vous trouverez ci-dessous une liste des requêtes spéciales pour lesquelles le comportement de l'appliance ADC a été modifié.

- Requête SET

  Les requêtes SQL SET définissent les variables associées à la connexion. Ces requêtes sont également utilisées pour définir des variables globales, mais pour l'instant, l'appliance ADC n'est pas en mesure de différencier les variables locales des variables globales. Pour cette requête, l'appliance ADC utilise le mécanisme de « stockage et transfert ».

- <db> Requête USE

  À l'aide de cette requête, l'utilisateur peut modifier la base de données associée à une connexion. Dans ce cas, l'appliance ADC analyse la <db> valeur envoyée et modifie un champ dans la connexion côté serveur pour refléter la nouvelle base de données à utiliser.

- Commande INIT_DB

  À l'aide de cette requête, l'utilisateur peut modifier la base de données associée à une connexion. Dans ce cas, l'appliance ADC analyse la <init_db> valeur envoyée et modifie un champ dans la connexion côté serveur pour refléter la nouvelle base de données à utiliser.

- COM_PREPARE

  L'appliance ADC arrête la commutation des requêtes à la réception de cette commande.

- Requête PREPARE

Cette requête est utilisée pour créer des instructions préparées associées à une connexion. Pour cette requête, l'appliance ADC utilise le mécanisme de « stockage et transfert ».

Prise en charge des messages du journal d'audit

Vous pouvez désormais configurer l'appliance NetScaler pour générer des messages de journal d'audit pour la fonctionnalité DataStream. Les messages du journal d'audit sont générés lorsque des connexions côté client et côté serveur sont établies, fermées ou abandonnées. Les catégories de messages que vous pouvez enregistrer et consulter sont ERROR et INFO. Les messages d'erreur pour les connexions côté client commencent par « CS » et les messages d'erreur pour les connexions côté serveur commencent par « SS ». « Des informations supplémentaires sont fournies si nécessaire. Par exemple, les messages de journal relatifs aux connexions fermées (CS_CONN_CLOSED) incluent uniquement l'ID de connexion. Toutefois, les messages de journal relatifs aux connexions établies (CS_CONN_ESTD) incluent des informations telles que le nom d'utilisateur, le nom de la base de données et l'adresse IP du client en plus de l'ID de connexion.

Système de noms de domaine

May 5, 2023

Remarque : à partir de la version 13.0 build 41.x, l'appliance NetScaler en mode ADNS et proxy est entièrement conforme au jour du drapeau DNS 2019.

Vous pouvez configurer l'appliance NetScaler pour qu'elle fonctionne comme un serveur de noms de domaine (serveur ADNS) faisant autorité pour un domaine. Ajoutez les enregistrements de ressources DNS qui appartiennent au domaine pour lequel l'appliance fait autorité et configurez les paramètres d'enregistrement de ressources. Vous pouvez également configurer l'appliance en tant que serveur DNS proxy qui équilibre la charge d'une batterie de serveurs de noms DNS situés à l'intérieur ou à l'extérieur de votre réseau. Configurez l'appliance en tant que résolveur d'extrémité et redirecteur. Vous pouvez configurer des suffixes DNS qui permettent la résolution de noms lorsque des noms de domaine complets ne sont pas configurés. L'appliance prend également en charge la requête DNS ANY qui récupère tous les enregistrements appartenant à un domaine.

Vous pouvez configurer l'appliance pour qu'elle fonctionne simultanément en tant que serveur DNS faisant autorité pour un domaine et en tant que serveur proxy DNS pour un autre domaine. Lorsque vous configurez l'appliance en tant que serveur DNS ou serveur proxy DNS faisant autorité pour une zone, vous pouvez permettre à l'appliance d'utiliser le protocole TCP pour les tailles de réponse qui dépassent la limite de taille spécifiée pour le protocole UDP (User Datagram Protocol).

Comment fonctionne le DNS sur NetScaler

Vous pouvez configurer l'appliance NetScaler pour qu'elle fonctionne en tant que serveur ADNS, serveur proxy DNS, résolveur final et redirecteur. Vous pouvez ajouter des enregistrements de ressources DNS sur l'appliance NetScaler, notamment les enregistrements suivants :

- Enregistrements de service (SRV)
- Enregistrements IPv6 (AAAA)
- Enregistrements d'adresse (A)
- Enregistrements d'échange de courrier (MX)
- Enregistrements de noms canoniques (CNAME)
- Enregistrements Pointer (PTR)
- Enregistrements de début d'autorité (SOA)
- Enregistrements texte (TXT)
- Enregistrements de pointeur d'autorité de nom (NAPTR)
- Dossiers DNSKEY
- Enregistrements d'autorisation de l'autorité de certification (CAA)

Vous pouvez également configurer NetScaler pour équilibrer la charge des serveurs de noms DNS externes.

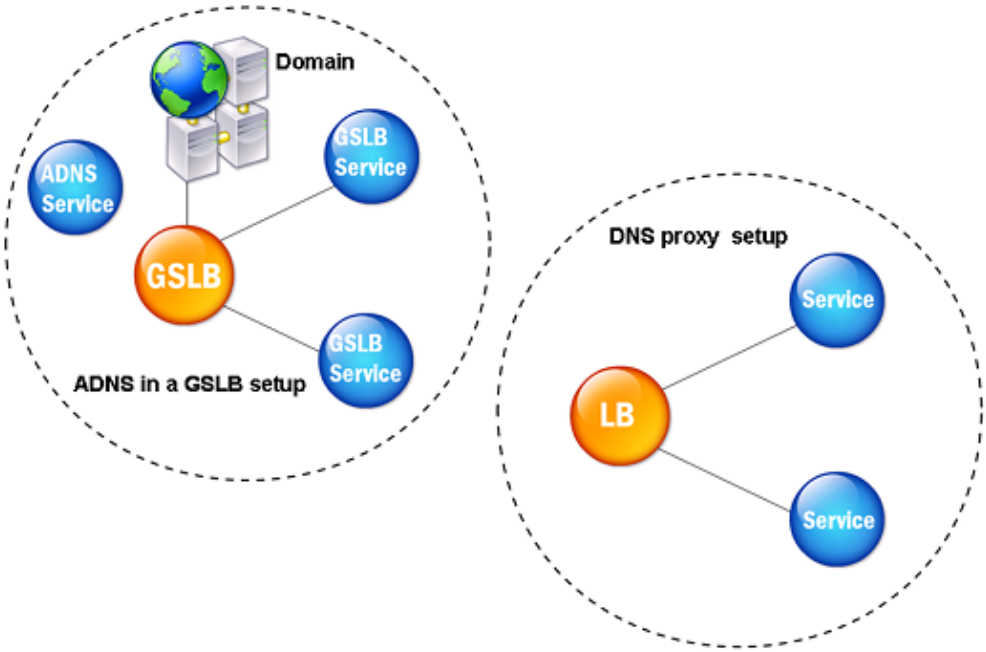
L'appliance NetScaler peut être configurée en tant qu'autorité pour un domaine. Ajoutez des enregistrements SOA et NS valides pour le domaine.

Un serveur ADNS est un serveur DNS qui contient des informations complètes sur une zone.

Pour configurer l'appliance NetScaler en tant que serveur ADNS pour une zone, vous devez ajouter un service ADNS, puis configurer la zone. Pour ce faire, vous devez ajouter des enregistrements SOA et NS valides pour le domaine. Lorsqu'un client envoie une demande DNS, l'appliance NetScaler recherche le nom de domaine dans les enregistrements de ressources configurés. Vous pouvez configurer le service ADNS à utiliser avec la fonctionnalité NetScaler Global Server Load Balancing (GSLB).

Vous pouvez déléguer un sous-domaine en ajoutant des enregistrements NS pour le sous-domaine à la zone du domaine parent. Vous pouvez ensuite faire en sorte que NetScaler fasse autorité pour le sous-domaine en ajoutant un « enregistrement colle » pour chacun des serveurs de noms de sous-domaines. Si le GSLB est configuré, NetScaler prend une décision d'équilibrage de charge GSLB en fonction de sa configuration et répond avec l'adresse IP du serveur virtuel sélectionné. La figure suivante montre les entités d'une configuration GSLB ADNS et d'une configuration de proxy DNS.

Figure 1. Modèle d'entité proxy DNS



L'appliance NetScaler peut fonctionner comme un proxy DNS. La mise en cache des enregistrements DNS, qui constitue une fonction importante d'un proxy DNS, est activée par défaut sur l'appliance NetScaler. La mise en cache permet à l'appliance NetScaler de fournir des réponses rapides pour les traductions répétées. Créez un serveur virtuel DNS d'équilibrage de charge et des services DNS, puis liez ces services au serveur virtuel.

NetScaler propose deux options, la durée de vie minimale (TTL) et la TTL maximale pour configurer la durée de vie des données mises en cache. Les données mises en cache expirent conformément à vos paramètres pour ces deux options. NetScaler vérifie le TTL de l'enregistrement DNS provenant du serveur. Si la durée de vie est inférieure à la durée de vie minimale configurée, elle est remplacée par la durée de vie minimale configurée. Si la durée de vie est supérieure à la durée de vie maximale configurée, elle est remplacée par la durée de vie maximale configurée.

NetScaler permet également la mise en cache des réponses négatives pour un domaine. Une réponse négative indique que les informations concernant un domaine demandé n'existent pas ou que le serveur ne peut pas fournir de réponse à la requête. Le stockage de ces informations est appelé *mise en cache négative*. La mise en cache négative permet d'accélérer les réponses aux requêtes sur un domaine et peut éventuellement fournir le type d'enregistrement.

Une réponse négative peut être l'une des suivantes :

- Message d'erreur NXDOMAIN - Si une réponse négative est présente dans le cache local, NetScaler renvoie un message d'erreur (NXDOMAIN). Si la réponse ne se trouve pas dans le cache local, la requête est transmise au serveur, qui renvoie une erreur NXDOMAIN à NetScaler. NetScaler met la réponse en cache localement, puis renvoie le message d'erreur au client.
- Message d'erreur NODATA : NetScaler envoie un message d'erreur NODATA si le nom de domaine de la requête est valide mais que les enregistrements du type indiqué ne sont pas disponibles.

NetScaler prend en charge la résolution récursive des requêtes DNS. En résolution récursive, le résolveur (client DNS) envoie une requête récursive à un serveur de noms pour un nom de domaine. Si le serveur de noms interrogé fait autorité pour le domaine, il répond avec le nom de domaine demandé. Sinon, NetScaler interroge les serveurs de noms de manière récursive jusqu'à ce que le nom de domaine demandé soit trouvé.

Avant de pouvoir appliquer l'option de requête récursive, vous devez d'abord l'activer. Vous pouvez également définir le nombre de fois où le résolveur DNS doit envoyer une demande de résolution (nouvelles tentatives DNS) en cas d'échec d'une recherche DNS.

Vous pouvez configurer NetScaler en tant que redirecteur DNS. Un redirecteur transmet les demandes DNS à des serveurs de noms externes. NetScaler vous permet d'ajouter des serveurs de noms externes et fournit une résolution de noms pour les domaines situés en dehors du réseau. NetScaler vous permet également de définir la priorité de recherche de noms sur DNS ou Windows Internet Name Service (WINS).

Permettre à l'appliance ADC d'utiliser DNS pour résoudre le nom d'hôte sur son adresse IP respective

Remarque : Vous avez besoin d'un utilitaire SSH pour accéder à l'interface de ligne de commande (CLI) de l'appliance.

Par défaut, l'appliance ADC ne peut pas résoudre le nom d'hôte sur son adresse IP respective. Effectuez les tâches suivantes pour activer la résolution de noms sur l'appliance :

1. Définissez des serveurs de noms.
2. Définissez un suffixe DNS.

Points à noter

Effectuez la recherche DNS depuis l'interface de ligne de commande. Les recherches DNS à partir de l'invite du shell du système d'exploitation FreeBSD échouent car l'entrée du fichier /etc/resolv.conf pointe vers l'adresse IP 127.0.0.2.

Les commandes suivantes sont remplacées par la commande `drill` de l'interface de ligne de commande FreeBSD de l'appliance accessible par la commande `shell`:


```
- host
- dig
- getent/MIP
- nslookup
<!--NeedCopy-->
```

Par exemple, au lieu d'exécuter `dig www.google.com @8.8.8.8` pour interroger l'enregistrement « A » « www.google.com » sur le serveur de noms « 8.8.8.8 », vous pouvez exécuter la commande `drill www.google.com @8.8.8.8`. La commande `drill` fonctionne exactement de la même manière que la commande `dig`.

```
root@lab# drill www.google.com @8.8.8.8
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 57980
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; www.google.com. IN A

;; ANSWER SECTION:
www.google.com. 300 IN A 142.250.187.196

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 53 msec
;; SERVER: 8.8.8.8
;; WHEN: Thu Jun 9 11:04:55 2022
;; MSG SIZE rcvd: 48
<!--NeedCopy-->
```

Si l'appliance ne parvient pas à effectuer une commande ping sur le serveur DNS sur son adresse SNIP, l'état du serveur indique « inactif ». La réussite du ping est importante lorsque l'appliance se trouve derrière un pare-feu.

Configuration CLI

À l'invite de commande, tapez :

```
add dns nameServer <Name_Server_IP_Address>
add dns suffix <DNS_Suffix>
<!--NeedCopy-->
```

Pour vérifier la configuration, tapez :


```
show dns nameServer
show dns suffix
<!--NeedCopy-->
```

Pour tester la résolution DNS, tapez :

```
show dns addrec <Host_Name>
<!--NeedCopy-->
```

Configuration graphique

1. Accédez à **Gestion du trafic > DNS > Serveurs de noms > Ajouter**.
2. Dans la boîte de dialogue **Créer un serveur** de noms, saisissez l'adresse IP du serveur de noms et cliquez sur **Créer**.
3. Accédez à **Gestion du trafic > DNS > Suffixe DNS > Ajouter**.
4. Dans la boîte de dialogue **Créer un suffixe DNS**, entrez le suffixe DNS, tel que exemple.com, à utiliser pour toutes les requêtes d'hôte, puis cliquez sur **Créer**.

DNS Round Robin

Lorsqu'un client envoie une demande DNS pour trouver l'enregistrement de ressource DNS, il reçoit une liste d'adresses IP correspondant au nom indiqué dans la demande DNS. Le client utilise ensuite l'une des adresses IP de la liste, généralement le premier enregistrement ou adresse IP. Par conséquent, un seul serveur est utilisé pour la durée de vie totale du cache et est surchargé lorsque de nombreuses demandes arrivent.

Lorsque NetScaler reçoit une demande DNS, il répond en modifiant l'ordre de la liste des enregistrements de ressources DNS selon une méthode circulaire. Cette fonctionnalité est appelée *DNS Round Robin*. Le Round Robin répartit le trafic de manière égale entre les centres de données. NetScaler exécute cette fonction automatiquement. Il n'est pas nécessaire de configurer ce comportement.

Vue d'ensemble fonctionnelle

Si NetScaler est configuré en tant que serveur ADNS, il renvoie les enregistrements DNS dans l'ordre dans lequel les enregistrements sont configurés. Lorsque NetScaler est configuré en tant que proxy DNS, il renvoie les enregistrements DNS dans l'ordre dans lequel il les reçoit du serveur. L'ordre des enregistrements présents dans le cache correspond à l'ordre dans lequel les enregistrements sont reçus du serveur.

NetScaler modifie ensuite l'ordre dans lequel les enregistrements sont envoyés dans la réponse DNS selon une méthode circulaire. La première réponse contient le premier enregistrement en séquence, la seconde réponse contient le second enregistrement en séquence, et l'ordre se poursuit dans la même séquence. Ainsi, les clients demandant le même nom peuvent se connecter à différentes adresses IP.

Exemple de DNS Round Robin

À titre d'exemple de DNS Round Robin, considérez les enregistrements DNS qui ont été ajoutés comme suit :

```
1   add dns addRec ns1 1.1.1.1  add dns addRec ns1 1.1.1.2  add dns
       addRec ns1 1.1.1.3  add dns addRec ns1 1.1.1.4
2 <!--NeedCopy-->
```

Le domaine, abc.com, est lié à un enregistrement NS comme suit :

```
1   add dns nsrec abc.com. ns1
2 <!--NeedCopy-->
```

Lorsque NetScaler reçoit une requête pour l'enregistrement A de ns1, les enregistrements d'adresses sont servis selon une méthode circulaire comme suit. Dans la première réponse DNS, 1.1.1.1 est servi comme premier enregistrement :

```
1   ns1.                    1H IN A         1.1.1.1  ns1.
                           1H IN A         1.1.1.2  ns1.
                           1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4
2 <!--NeedCopy-->
```

Dans la deuxième réponse DNS, la deuxième adresse IP, 1.1.1.2, est utilisée comme premier enregistrement :

```
1   ns1.                    1H IN A         1.1.1.2  ns1.
                           1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4  ns1.
                           1H IN A         1.1.1.1
2 <!--NeedCopy-->
```

Dans la troisième réponse DNS, la troisième adresse IP, 1.1.1.2, est utilisée comme premier enregistrement :

```
1   ns1.                    1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4  ns1.
```



```
                            1H IN A         1.1.1.1  ns1.
                            1H IN A         1.1.1.2
<!--NeedCopy-->
```

Configurer les enregistrements de ressources DNS

May 5, 2023

Vous configurez des enregistrements de ressources sur l'appliance Citrix® ADC lorsque vous configurez l'appliance en tant que serveur ADNS pour une zone. Vous pouvez également configurer des enregistrements de ressources sur l'appliance si les enregistrements de ressources appartiennent à une zone pour laquelle l'appliance est un serveur proxy DNS. Sur l'appliance, vous pouvez configurer les types d'enregistrement suivants :

- Dossiers de service
- Dossiers AAAA
- Enregistrements d'adresses
- Enregistrements Mail Exchange
- Enregistrements du serveur de noms
- Dossiers canoniques
- Enregistrements Pointer
- Disques NAPTR
- Début des notices d'autorité
- Enregistrements texte
- Enregistrements d'autorisation de l'autorité de certification (CAA)

Le tableau suivant répertorie les types d'enregistrement que vous pouvez configurer pour un enregistrement de nom de domaine sur l'appliance NetScaler. Par exemple, vous pouvez configurer un maximum de 25 adresses IP pour un enregistrement.

Tableau 1. Type et numéro d'enregistrement configurables

Record Type	Nombre d'enregistrements
Adresse (A)	25
IPv6 (AAAA)	5
Echange de courrier (MX)	12
Serveur de noms (NS)	16
Service (SRV)	8

Record Type	Nombre d'enregistrements
Pointeur (PTR)	20
Nom canonique (CNAME)	1
Début d'autorité (SOA)	1
Texte (TXT)	20
Pointeur d'autorité de dénomination (NAPTR)	20
Autorisation de l'autorité de certification (CAA)	20

> **Remarque :**
>
> Le nombre maximum d'adresses IP pour un nom d'hôte spécifique est de 25. Cependant, le nombre d'enregistrements d'adresses différents peut être supérieur à 25.

Créer des enregistrements SRV pour un service

May 5, 2023

L'enregistrement SRV fournit des informations sur les services disponibles sur l'appliance NetScaler. Un enregistrement SRV contient les informations suivantes :

- Nom du service et du protocole
- Nom de domaine
- TTL
- Classe DNS
- Priorité de la cible
- Poids des enregistrements ayant la même priorité
- Port du service
- Nom d'hôte du service.

NetScaler choisit d'abord l'enregistrement SRV dont le paramètre de priorité est le plus bas. Si un service possède plusieurs enregistrements SRV ayant la même priorité, les clients utilisent le champ de pondération pour déterminer quel hôte utiliser.

Ajouter un enregistrement SRV à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement SRV et vérifier la configuration :


```
- add dns srvRec <domain> <target> -priority <positive_integer> -
   weight <positive_integer> -port <positive_integer> [-TTL <secs>]
- sh dns srvRec <domain>
<!--NeedCopy-->
```

Exemple :

```
> add dns srvRec _http._tcp.example.com nameserver1.com -priority 1 -
   weight 1 -port 80
 Done
> show dns srvRec _http._tcp.example.com
1)      Domain Name : _http._tcp.example.com
        Target Host : nameserver1.com
        Priority : 1    Weight : 1
        Port : 80       TTL : 3600 secs
 Done
<!--NeedCopy-->
```

Modifier ou supprimer un enregistrement SRV à l'aide de l'interface de ligne de commande

- Pour modifier un enregistrement SRV, tapez :
  - La `set dns srvRec` commande
  - Le nom du domaine pour lequel l'enregistrement SRV est configuré
  - Le nom de l'hôte cible qui héberge le service associé
  - Les paramètres à modifier, avec leurs nouvelles valeurs
- Pour supprimer un enregistrement SRV, tapez :
  - La `rm dns srvRec` commande
  - Le nom du domaine pour lequel l'enregistrement SRV est configuré
  - Le nom de l'hôte cible qui héberge le service associé

Configuration d'un enregistrement SRV à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements SRV et créez un enregistrement** SRV.

Créer des enregistrements AAAA pour un nom de domaine

August 20, 2021

Un enregistrement de ressource AAAA stocke une adresse IPv6 unique.

Ajouter un enregistrement AAAA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement AAAA et vérifier la configuration :

```
1 -  add dns aaaaRec <hostName> <IPv6Address> ... [-TTL <secs>]
2 -  show dns aaaaRec <hostName>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns aaaaRec www.example.com 2001:0db8:0000:0000:0000:0000:1428:57
     ab
2  Done
3 > show dns aaaaRec www.example.com
4 1)      Host Name : www.example.com
5         Record Type : ADNS              TTL : 5 secs
6         IPV6 Address : 2001:db8::1428:57ab
7  Done
8 <!--NeedCopy-->
```

Pour supprimer un enregistrement AAAA et toutes les adresses IPv6 associées au nom de domaine, tapez la `rm dns aaaaRec` commande et le nom de domaine pour lesquels l'enregistrement AAAA est configuré. Pour supprimer uniquement un sous-ensemble des adresses IPv6 associées au nom de domaine dans un enregistrement AAAA, tapez ce qui suit :

- `rm dns aaaaRec` commande
- Nom de domaine pour lequel l'enregistrement AAAA est configuré
- Les adresses IPv6 que vous souhaitez supprimer

Ajouter un enregistrement AAAA à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements AAAA** et créez un enregistrement AAAA.

Créer des enregistrements d'adresses pour un nom de domaine

May 5, 2023

Les enregistrements d'adresse (A) sont des enregistrements DNS qui font correspondre un nom de domaine à une adresse IPv4.

Vous ne pouvez pas supprimer les enregistrements d'adresses d'un hôte participant à l'équilibrage de charge global des serveurs (GSLB). Toutefois, NetScaler supprime les enregistrements d'adresses ajoutés pour les domaines GSLB lorsque vous dissociez le domaine d'un serveur virtuel GSLB. Seuls les enregistrements configurés par l'utilisateur peuvent être supprimés manuellement. Vous ne pouvez pas supprimer un enregistrement pour un hôte référencé par des enregistrements tels que NS, MX ou CNAME.

Ajouter un enregistrement d'adresse à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement d'adresse et vérifier la configuration :

```
-  add dns addRec <hostName> <IPAddress> [-TTL <secs>]
-  show dns addRec <hostName>
<!--NeedCopy-->
```

Exemple :

```
> add dns addRec ns.example.com 192.0.2.0
 Done
> show dns addRec ns.example.com
1)      Host Name : ns.example.com
        Record Type : ADNS                      TTL : 5 secs
        IP Address : 192.0.2.0
 Done
<!--NeedCopy-->
```

Pour supprimer un enregistrement d'adresse et toutes les adresses IP associées au nom de domaine, tapez la `rm dns addRec` commande et le nom de domaine pour lequel l'enregistrement d'adresse est configuré. Pour supprimer uniquement un sous-ensemble des adresses IP associées au nom de domaine dans un enregistrement d'adresses, tapez ce qui suit :

- `rm dns addRec` commande
- Le nom de domaine pour lequel l'enregistrement d'adresse est configuré
- Les adresses IP que vous souhaitez supprimer

Ajouter un enregistrement d'adresse à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements d'adresses** et créez un enregistrement d'adresse.

Créer des enregistrements MX pour un serveur d'échange de messagerie

August 20, 2021

Les enregistrements Mail Exchange (MX) sont utilisés pour diriger les messages électroniques sur Internet. Un enregistrement MX contient une préférence MX qui spécifie le serveur MX à utiliser. Les valeurs de préférence MX varient de 0 à 65536. Un enregistrement MX contient un numéro de préférence MX unique. Vous pouvez définir la préférence MX et les valeurs TTL pour un enregistrement MX.

Lorsqu'un message électronique est envoyé via Internet, un agent de transfert de courrier envoie une requête DNS demandant l'enregistrement MX pour le nom de domaine. Cette requête renvoie une liste des noms d'hôte des serveurs d'échange de messagerie pour le domaine, ainsi qu'un numéro de préférence. S'il n'y a pas d'enregistrements MX, la demande est faite pour l'enregistrement Adresse de ce domaine. Un seul domaine peut avoir plusieurs serveurs d'échange de messagerie.

Ajouter un enregistrement MX à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement MX et vérifier la configuration :

```
1 -  add dns mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <
     secs>]
2 -  show dns mxRec <domain>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns mxRec example.com -mx mail.example.com -pref 1
2  Done
3 > show dns mxRec example.com
4 1)      Domain : example.com    MX Name : mail.example.com
5         Preference :   1        TTL : 5 secs
6  Done
7 <!--NeedCopy-->
```

Modifier ou supprimer un enregistrement MX à l'aide de l'interface de ligne de commande

- Pour modifier un enregistrement MX, tapez la `set dns mxRec` commande, le nom du domaine pour lequel l'enregistrement MX est configuré, le nom de l'enregistrement MX et les paramètres à modifier, avec leurs nouvelles valeurs.

- Pour définir la valeur par défaut du paramètre TTL, tapez la `unset dns mxRec` commande, le nom du domaine pour lequel l'enregistrement MX est configuré, le nom de l'enregistrement MX et -TTL sans valeur TTL. Vous pouvez utiliser la commande `unset dns mxRec` pour désactiver uniquement le paramètre TTL.
- Pour supprimer un enregistrement MX, tapez la `rm dns mxRec` commande, le nom du domaine pour lequel l'enregistrement MX est configuré et le nom de l'enregistrement MX.

Ajouter un enregistrement MX à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements d'échange de messagerie** et créez un enregistrement MX.

Créer des enregistrements NS pour un serveur faisant autorité

August 20, 2021

Les enregistrements NS (Name Server) spécifient le serveur faisant autorité pour un domaine. Vous pouvez configurer un maximum de 16 enregistrements NS. Vous pouvez utiliser un enregistrement NS pour déléguer le contrôle d'un sous-domaine à un serveur DNS.

Créer un enregistrement NS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un enregistrement NS et vérifier la configuration :

```
1 -  add dns nsRec <domain> <nameServer> [-TTL <secs>]
2 -  show dns nsRec <domain>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns nsRec example.com nameserver1.example.com
2  Done
3 > show dns nsRec example.com
4 1)      Domain : example.com    NameServer : nameserver1.example.com
5         TTL : 5 sec
6  Done
7 <!--NeedCopy-->
```

Pour supprimer un enregistrement NS, tapez la commande `rm dns nsRec`, le nom du domaine auquel appartient l'enregistrement NS et le nom du serveur de noms.

Créer un enregistrement NS à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements du serveur de noms** et créez un enregistrement NS.

Créer des enregistrements CNAME pour un sous-domaine

May 5, 2023

Un enregistrement de nom canonique (enregistrement CNAME) est un alias pour un nom DNS. Ces enregistrements sont utiles lorsque plusieurs services interrogent le serveur DNS. L'hôte qui possède un enregistrement d'adresse (A) ne peut pas avoir d'enregistrement CNAME.

Parfois, une appliance NetScaler en mode proxy demande un enregistrement d'adresse depuis le cache plutôt que depuis le serveur.

Ajouter un enregistrement CNAME à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un enregistrement CNAME et vérifier la configuration :

```
-  add dns cnameRec <aliasName> <canonicalName> [-TTL <secs>]
-  show dns cnameRec <aliasName>
<!--NeedCopy-->
```

Exemple :

```
> add dns cnameRec www.example.com www.examplenw.com
 Done
> show dns cnameRec www.example.com
        Alias Name      Canonical Name  TTL
1)      www.example.com        www.examplenw.com       5 secs
 Done
<!--NeedCopy-->
```

Pour supprimer un enregistrement CNAME pour un domaine donné, tapez la `rm dns cnameRec` commande et l'alias du nom de domaine.

Ajouter un enregistrement CNAME à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements canoniques et créez un enregistrement** CNAME.

Mettre en cache les enregistrements CNAME

Lorsqu'elle est déployée en mode proxy, l'appliance ADC n'envoie pas toujours la requête d'enregistrement d'adresse au serveur principal. Ce comportement se produit lorsque, pour répondre à une requête concernant un enregistrement d'adresse, une chaîne CNAME partielle est présente dans le cache. Il existe peu de conditions dans lesquelles l'ADC met en cache l'enregistrement CNAME partiel et sert la requête à partir du cache. Les conditions sont les suivantes :

- NetScaler doit être déployé en mode proxy.
- La réponse du serveur principal doit comporter une chaîne CNAME, pour laquelle le type d'enregistrement de la dernière entrée de la section de réponse doit être un CNAME et le type de question non un CNAME.
- La réponse du serveur principal ne peut pas être un No-Data ou un domaine NX.
- La réponse du serveur principal doit être une réponse faisant autorité.

Créer des enregistrements NAPTR pour le domaine des télécommunications

May 5, 2023

Le NAPTR (Naming Address Pointer) est l'un des enregistrements DNS les plus couramment utilisés dans le domaine des télécommunications. Les enregistrements NAPTR font correspondre l'espace d'adressage téléphonique Internet à l'espace d'adresses Internet. Ils permettent donc à un appareil mobile d'envoyer une demande au bon serveur. La combinaison des enregistrements NAPTR et des enregistrements de service (SRV) permet de chaîner plusieurs enregistrements afin de former des règles de réécriture complexes qui produisent de nouvelles étiquettes de domaine ou des identificateurs de ressources uniformes (URI). Le code DNS du NAPTR est 35.

NetScalers prend en charge le NAPTR selon deux modes : le mode ADNS et le mode proxy. En mode proxy, l'ADC met en cache la réponse des serveurs et utilise les enregistrements mis en cache pour traiter les requêtes futures. Un maximum de 20 enregistrements NAPTR peuvent être ajoutés pour un domaine particulier dans NetScaler. NetScaler met en cache la réponse à une requête d'enregistrement DNS NAPTR. Toutes les demandes ultérieures concernant l'enregistrement NAPTR sont traitées à partir du cache.

Création d'un enregistrement NAPTR à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement NAPTR et vérifier la configuration :

'ajouter DNS Naptrec [drapeaux][services](regexp|-replacement)\[-TTL]\'

Supprimer un enregistrement NAPTR à l'aide de la CLU

```
rm dns naptrRec<domain> (<order> <preference> [-flags <string>] [-services
 <string>] (-regexp <expression> | -replacement <string>))| -recordId <
positive_integer>@)
```

Configurer un enregistrement NAPTR à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements NAPTR et créez un enregistrement** NAPTR.

Créer des enregistrements PTR pour les adresses IPv4 et IPv6

August 20, 2021

Un enregistrement de pointeur (PTR) traduit une adresse IP en son nom de domaine. Les enregistrements IPv4 PTR sont représentés par les octets d'une adresse IP dans l'ordre inverse avec la chaîne "in-addr.arpa." joint à la fin. Par exemple, l'enregistrement PTR pour l'adresse IP 1.2.3.4 est 4.3.2.1.in-addr.arpa.

Les adresses IPv6 sont mappées inversement sous le domaine IP6.ARPA. Les cartes inverses IPv6 utilisent une séquence de quartets séparés par des points avec le suffixe ".IP6.ARPA" tel que défini dans la norme RFC 3596. Par exemple, le nom de domaine de recherche inverse correspondant à l'adresse 4321:0:1:2:3:4:567:89 ab serait b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA.

Ajouter un enregistrement PTR à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement PTR et vérifier la configuration :

```
1 -  add dns ptrRec <reverseDomain> <domain> [-TTL <secs>]
2 -  show dns ptrRec <reverseDomain>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns ptrRec 0.2.0.192.in-addr.arpa example.com
2  Done
3 > show dns ptrRec 0.2.0.192.in-addr.arpa
4 1)      Reverse Domain Name : 0.2.0.192.in-addr.arpa
5         Domain Name : example.com              TTL : 3600 secs
6  Done
```



```
<!--NeedCopy-->
```

Pour supprimer un enregistrement PTR, tapez la commande `rm dns ptrRec` et le nom de domaine inverse associé à l'enregistrement PTR

Ajouter un enregistrement PTR à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements PTR** et créez un enregistrement PTR.

Créer des enregistrements SOA pour les informations faisant autorité

August 20, 2021

Un enregistrement Start of Authority (SOA) est créé uniquement au sommet de la zone et contient des informations sur la zone. L'enregistrement inclut, entre autres paramètres, le serveur de noms principal, les informations de contact (e-mail) et les valeurs par défaut (minimum) de durée de vie (TTL) pour les enregistrements.

Créer un enregistrement SOA à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un enregistrement SOA et vérifier la configuration :

```
- add dns soaRec <domain> -originServer <originServerName> -contact <
   contactName>
- sh dns soaRec <do main>
<!--NeedCopy-->
```

Exemple :

```
> add dns soaRec example.com -originServer nameserver1.example.com -
   contact admin.example.com
 Done
> show dns soaRec example.com
1)      Domain Name : example.com
        Origin Server : nameserver1.example.com
        Contact : admin.example.com
        Serial No. : 100        Refresh : 3600 secs     Retry : 3 secs
        Expire : 3600 secs      Minimum : 5 secs        TTL : 3600 secs
 Done
<!--NeedCopy-->
```


Modifier ou supprimer un enregistrement SOA à l'aide de l'interface de ligne de commande

- Pour modifier un enregistrement SOA, tapez la commande `set dns soaRec`, le nom du domaine pour lequel l'enregistrement est configuré et les paramètres à modifier, avec leurs nouvelles valeurs.
- Pour supprimer un enregistrement SOA, tapez la commande `rm dns soaRec` et le nom du domaine pour lequel l'enregistrement est configuré.

Configurer un enregistrement SOA à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements SOA** et créez un enregistrement SOA.

Créer des enregistrements TXT pour contenir du texte descriptif

May 5, 2023

Les hôtes de domaine stockent les enregistrements TXT à des fins d'information. Le composant RDATA d'un enregistrement TXT, qui consiste en une ou plusieurs chaînes de caractères de longueur variable, peut stocker pratiquement toutes les informations dont un destinataire peut avoir besoin sur le domaine. Il peut également inclure des informations sur le fournisseur de services, la personne de contact, les adresses e-mail et les détails associés. La protection SPF (Sender Policy Framework) a été le principal cas d'utilisation de l'enregistrement TXT.

Tous les types de configuration (configurations DNS faisant autorité, proxy DNS, résolveur final et redirecteur) de l'appliance NetScaler prennent en charge les enregistrements TXT. Vous pouvez ajouter un maximum de 20 enregistrements de ressources TXT à un domaine. Chaque enregistrement de ressource est stocké avec un identifiant d'enregistrement unique généré en interne. Un enregistrement de ressource TXT peut contenir jusqu'à six chaînes, chacune pouvant contenir jusqu'à 255 caractères. Vous pouvez consulter l'ID d'un enregistrement et l'utiliser pour le supprimer. Toutefois, vous ne pouvez pas modifier un enregistrement de ressource TXT.

Créez un enregistrement de ressource TXT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un enregistrement de ressource TXT et vérifier la configuration :

```
1 -  add dns txtRec <domain> <string> ... [-TTL <secs>]
2 -  show dns txtRec [<domain> | -type <type>]
3 <!--NeedCopy-->
```


Exemple :

```
> add dns txtRec www.example.com "Contact: Mark" "Email: mark@example.com" -TTL 36000
 Done
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 13783       TTL : 36000 secs
     Record Type : ADNS
         "Contact: Mark"
         "Email: mark@example.com"
 Done
<!--NeedCopy-->
```

Divisez la chaîne dans un enregistrement de ressource TXT à l'aide de la CLI

Si vous avez une chaîne de plus de 255 caractères, vous pouvez fractionner les chaînes en tenant compte de la limite de six chaînes. Chaque chaîne peut avoir une longueur de 254 octets.

```
add dns txtrec domain.com "string1" "string2" string3" "string4"
<!--NeedCopy-->
```

Exemple :

```
add dns txtrec exampledomain.com "Contact: Evan" "Email: evan@example.com" "Contact: Mark" "Email: mark1@example.com"
<!--NeedCopy-->
```

Supprimer un enregistrement de ressource TXT à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour supprimer un enregistrement de ressource TXT et vérifier la configuration :

```
-  rm dns txtRec <domain> (<string> ... | -recordId <positive_integer>)
-  show dns txtRec [<domain> | -type <type>]
<!--NeedCopy-->
```

Exemple :
vous pouvez d'abord utiliser la `show dns txtRec` commande pour afficher l'ID d'enregistrement de l'enregistrement de ressource TXT que vous souhaitez supprimer, comme indiqué :

```
> show dns txtRec www.example.com
```



```
1)  Domain : www.example.com    Record id: 36865       TTL : 36000 secs
    Record Type : ADNS
        "Contact: Evan"
        "Email: evan@example.com"
2)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
    Record Type : ADNS
        "Contact: Mark"
        "Email: mark1@example.com"
 Done
<!--NeedCopy-->
```

La méthode la plus simple pour supprimer un enregistrement TXT consiste à utiliser l'ID de l'enregistrement. Si vous souhaitez fournir les chaînes, saisissez-les dans l'ordre dans lequel elles sont stockées dans l'enregistrement. Dans l'exemple suivant, l'enregistrement TXT est supprimé à l'aide de son ID d'enregistrement.

```
>rm dns txtRec www.example.com -recordID 36865
 Done
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
    Record Type : ADNS
        "Contact: Mark"
        "Email: mark1@example.com"
 Done
<!--NeedCopy-->
```

Configurer un enregistrement TXT à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements TXT** et créez un enregistrement TXT.

Création d'enregistrements CAA pour un nom de domaine

May 5, 2023

L'autorisation de l'autorité de certification (CAA) est un type d'enregistrement DNS qui permet aux propriétaires de domaine de spécifier quelle autorité de certification (CA) peut émettre des certificats SSL pour le domaine.

Une connexion sécurisée à un service nécessite des certificats SSL/TLS pour garantir l'identité de l'hôte et établir un canal sécurisé. Le fait de ne pas disposer d'enregistrements CAA peut entraîner

un risque de sécurité, car n'importe qui peut générer une demande de signature de certificat (CSR) pour le domaine et obtenir la signature du certificat par n'importe quelle autorité de certification.

Les enregistrements CAA fournissent un niveau de protection supplémentaire à votre présence sur le Web en permettant au propriétaire du domaine de déclarer quelles autorités de certification sont autorisées à délivrer un certificat pour le domaine. S'il existe une demande de certificat provenant d'une autorité de certification non autorisée, l'enregistrement CAA en informe le propriétaire du domaine. Si aucun enregistrement CAA n'est présent pour un domaine, toute autorité de certification est autorisée à émettre le certificat pour ce domaine.

L'appliance NetScaler prend en charge les enregistrements DNS CAA dans les modes suivants :

- **Proxy** : l'appliance met en cache les réponses aux enregistrements CAA des serveurs principaux et répond à d'autres requêtes du même type à partir du cache.
- **ADNS** : l'appliance répond aux requêtes DNS de type enregistrement CAA à partir des enregistrements DNS configurés.

Remarque :

> - Vous pouvez ajouter un maximum de 20 enregistrements CAA par nom de domaine.
> - Les modes résolveur et redirecteur récursifs ne sont pas pris en charge.

Ajouter un enregistrement CAA à l'aide de la CLI

À l'invite de commandes, tapez la commande suivante :

```
add dns caaRec <domain> <issuer-string> -tag <tag-string> -flag [None|
   Critical] [-TTL <secs>]
<!--NeedCopy-->
```

Exemple :

```
> add dns caaRec newdomain string1 -tag Issue -flag None [-TTL 3600]
<!--NeedCopy-->
```

Afficher les détails des commandes

```
> show dns caaRec

1)  Domain : newdomain  ECS Subnet : None      Record id: 39423 TTL :
   3600 secs Record Type : ADNS

Value: string1

Tag: issue

```



```
Flag: NONE

2)  Domain : test.com  ECS Subnet : None      Record id: 2572   TTL : 5
     secs    Record Type : ADNS

Value: ca1.test.com

Tag: issue

Flag: NONE
<!--NeedCopy-->
```

Pour supprimer un enregistrement CAA, tapez la commande suivante à l'invite de commandes :

```
rm dns caaRec <domain> <issuer-string> -tag <tag-string> | -recordId <
   positive_integer>@)
<!--NeedCopy-->
```

Exemple :

```
rm dns caaRec newdomain -recordId 39423
<!--NeedCopy-->
```

> **Remarque :**
>
> -recordId @ n'est pas pris en charge dans un cluster.

Ajouter un enregistrement CAA à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements CAA** et créez un enregistrement d'adresse.

Afficher les statistiques DNS

May 5, 2023

Vous pouvez consulter les statistiques DNS générées par l'appliance NetScaler. Les statistiques DNS incluent les statistiques d'exécution, de configuration et d'erreurs.

Afficher les statistiques des enregistrements DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
stat dns
```

Exemple :

```
> stat dns
DNS Statistics

Runtime Statistics
Dns queries                             21
NS queries                               8
SOA queries                             18
.
.
.
Configuration Statistics
AAAA records                            17
A records                               36
MX records                               9
.
.
.
Error Statistics
Nonexistent domain                      17
No AAAA records                          0
No A records                            13
.
.
.
Done
<!--NeedCopy-->
```

Afficher les statistiques des enregistrements DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet de détails, cliquez sur **Statistiques**.

Configurer une zone DNS

May 5, 2023

Une entité de zone DNS sur l'appliance NetScaler facilite la propriété d'un domaine sur l'appliance. Une zone de l'appliance vous permet également d'implémenter des extensions de sécurité DNS

(DNSSEC) pour la zone ou de décharger les opérations DNSSEC de la zone des serveurs DNS vers l'appliance. Les opérations de signature DNSSEC sont effectuées sur tous les enregistrements de ressources d'une zone DNS. Par conséquent, si vous souhaitez signer une zone ou si vous souhaitez décharger les opérations DNSSEC pour une zone, vous devez d'abord créer la zone sur l'appliance NetScaler.

Créez une zone DNS sur l'appliance dans les scénarios suivants :

- L'appliance NetScaler possède tous les enregistrements d'une zone, c'est-à-dire qu'elle fonctionne en tant que serveur DNS faisant autorité pour la zone. La zone doit être créée avec le paramètre ProxyMode défini sur NON.
- L'appliance NetScaler ne possède qu'un sous-ensemble des enregistrements d'une zone. Tous les autres enregistrements de ressources de la zone sont hébergés sur un ensemble de serveurs de noms principaux. L'appliance est configurée en tant que serveur proxy DNS pour ces serveurs principaux. Une configuration classique dans laquelle l'appliance NetScaler ne possède qu'un sous-ensemble des enregistrements de ressources de la zone est une configuration GSLB (Global Server Load Balancing). L'appliance NetScaler possède uniquement les noms de domaine GSLB, tandis que les serveurs de noms principaux possèdent tous les autres enregistrements. La zone doit être créée avec le paramètre ProxyMode défini sur YES.
- Vous souhaitez décharger les opérations DNSSEC pour une zone de vos serveurs DNS officiels vers l'appliance. La zone doit être créée avec le paramètre ProxyMode défini sur YES. Il se peut que vous deviez configurer d'autres paramètres pour la zone.

La rubrique actuelle décrit comment créer une zone pour les deux premiers scénarios. Pour plus d'informations sur la façon de configurer une zone pour le transfert des opérations DNSSEC vers l'appliance, voir Décharger les opérations DNSSECvers l'appliance NetScaler.

> **Remarque**
>
> Si l'appliance ADC fonctionne en tant que serveur DNS faisant autorité pour une zone, vous devez créer les enregistrements de début d'autorité (SOA) et de serveur de noms (NS) pour la zone avant de créer la zone. Si NetScaler fonctionne en tant que serveur proxy DNS pour une zone, les enregistrements SOA et NS ne doivent pas être créés sur l'appliance NetScaler. Pour plus d'informations sur la création d'enregistrements SOA et NS, voir Configurer les enregistrements de ressources DNS.

Lorsque vous créez une zone, tous les noms de domaine et enregistrements de ressources existants se terminant par le nom de la zone sont automatiquement traités comme faisant partie de la zone. De plus, tous les nouveaux enregistrements de ressources créés avec un suffixe correspondant au nom de la zone sont implicitement inclus dans la zone.

Créez une zone DNS sur l'appliance NetScaler à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour ajouter une zone DNS à l'appliance NetScaler et vérifier la configuration :

```
-  add dns zone <zoneName> -proxyMode ( YES | NO )
-  show dns zone [<zoneName> | -type <type>]
<!--NeedCopy-->
```

Exemple :

```
> add dns zone example.com -proxyMode Yes
 Done
> show dns zone example.com
         Zone Name : example.com
         Proxy Mode : YES
Done
<!--NeedCopy-->
```

Modifier ou supprimer une zone DNS à l'aide de l'interface de ligne de commande

- Pour modifier une zone DNS, tapez la `set dns zone` commande, le nom de la zone DNS et les paramètres à modifier, avec leurs nouvelles valeurs.
- Pour supprimer une zone DNS, saisissez la `rm dns zone` commande et le nom de la zone DNS.

Configuration d'une zone DNS à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Zones** et créez une zone DNS.

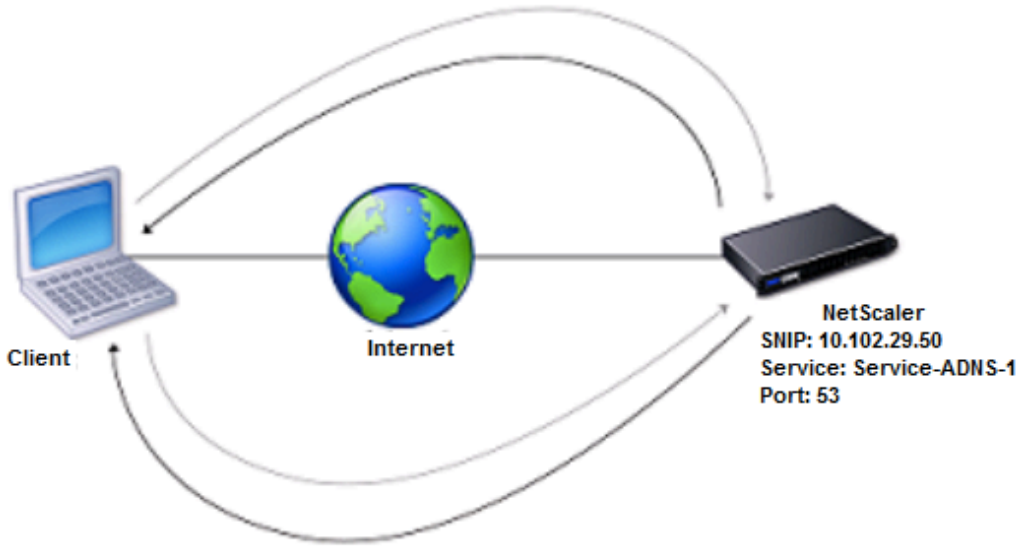
Configurer NetScaler en tant que serveur ADNS

May 5, 2023

Vous pouvez configurer l'appliance ADC pour qu'elle fonctionne comme un serveur de noms de domaine (ADNS) faisant autorité pour un domaine. En tant que serveur ADNS pour un domaine, NetScaler résout les demandes DNS pour tous les types d'enregistrements DNS appartenant au domaine. Pour configurer NetScaler afin qu'il fonctionne comme un serveur ADNS pour un domaine, vous devez créer un service ADNS et configurer les enregistrements NS et d'adresses pour le domaine sur NetScaler. Le service ADNS peut être configuré à l'aide de l'adresse IP du sous-réseau (SNIP) ou

d'une adresse IP distincte. Le diagramme de topologie suivant montre un exemple de configuration et le flux des demandes et des réponses.

Figure 1. NetScaler en tant qu'ADNS



Le tableau suivant présente les paramètres configurés pour le service ADNS illustré dans le diagramme topologique précédent.

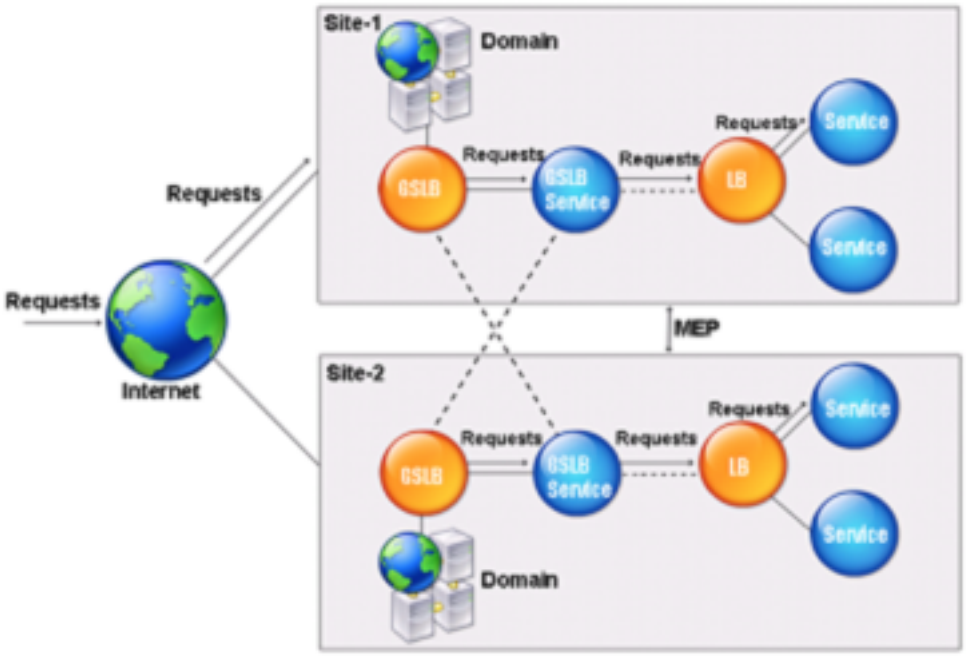
Type d'entité	Nom	Adresse IP	Type	Port
Service ADNS	Service-ADNS-1	10.102.29.51	ADNS	53

Tableau 1. Exemple de configuration du service ADNS

Pour configurer une configuration ADNS, vous devez configurer le service ADNS. Pour obtenir des instructions sur la configuration du service ADNS, voir Équilibrage de charge.

Lors de la résolution DNS, le serveur ADNS demande au proxy DNS ou au serveur DNS local de demander à NetScaler l'adresse IP du domaine. Étant donné que NetScaler fait autorité pour le domaine, il envoie l'adresse IP au proxy DNS ou au serveur DNS local. Le schéma suivant décrit le placement et le rôle du serveur ADNS dans une configuration GSLB.

Figure 2. Modèle d'entité GSLB



Remarque : En mode ADNS, si vous supprimez des enregistrements SOA et ADNS, les éléments suivants ne fonctionnent pas pour le domaine hébergé par NetScaler : N'IMPORTE quelle requête (pour plus d'informations sur la requête ANY, voir la requête DNS ANY) et réponses négatives, telles que NODATA et NXDOMAIN.

Créer un service ADNS

Un service ADNS est utilisé pour l'équilibrage global de la charge de service. Pour plus d'informations sur la création d'une configuration GSLB, reportez-vous à la section Équilibrage global de la charge des serveurs. Vous pouvez ajouter, modifier, activer, désactiver et supprimer un service ADNS. Pour obtenir des instructions sur la création d'un service ADNS, voir Configurer les services.

Remarque : Vous pouvez configurer le service ADNS pour utiliser SNIP ou toute nouvelle adresse IP.

Lorsque vous créez un service ADNS, NetScaler répond aux requêtes DNS sur l'adresse IP et le port du service ADNS configurés.

Vous pouvez vérifier la configuration en consultant les propriétés du service ADNS. Vous pouvez afficher des propriétés telles que le nom, l'état, l'adresse IP, le port, le protocole et le nombre maximum de connexions client.

Configurer la configuration ADNS pour utiliser le protocole TCP

Par défaut, certains clients utilisent le protocole UDP (User Datagram Protocol) pour le DNS, qui définit une limite de 512 octets pour la longueur de charge utile des paquets UDP. Pour gérer les charges utiles dont la taille dépasse 512 octets, le client doit utiliser le protocole TCP. Pour activer les communications DNS via TCP, vous devez configurer l'appliance NetScaler pour qu'elle utilise le protocole TCP pour le DNS. NetScaler définit ensuite le bit de troncature dans les paquets de réponse DNS. Le bit de troncature indique que la réponse est trop volumineuse pour le protocole UDP et que le client doit envoyer la demande via une connexion TCP. Le client utilise ensuite le protocole TCP sur le port 53 et ouvre une nouvelle connexion à NetScaler. NetScaler écoute sur le port 53 avec l'adresse IP du service ADNS pour accepter les nouvelles connexions TCP du client.

Pour configurer NetScaler afin qu'il utilise le protocole TCP, vous devez configurer un service ADNS_TCP. Pour obtenir des instructions sur la création d'un service ADNS_TCP, reportez-vous à la section Équilibrage de charge.

> **Important**
>
> Pour configurer NetScaler de manière à utiliser le protocole UDP pour le DNS et à n'utiliser le protocole TCP que lorsque la longueur de la charge utile du protocole UDP dépasse 512 octets, vous devez configurer les services ADNS et ADNS_TCP. L'adresse IP du service ADNS_TCP doit être identique à l'adresse IP du service ADNS.

Ajouter des enregistrements de ressources DNS

Après avoir créé un service ADNS, vous pouvez ajouter des enregistrements DNS. Pour obtenir des instructions sur l'ajout d'enregistrements DNS, voir Configurer les enregistrements de ressources DNS.

Supprimer les services ADNS

Pour obtenir des instructions sur la suppression des services, voir Équilibrage de charge.

Configurer la délégation de domaine

La délégation de domaine consiste à attribuer la responsabilité d'une partie de l'espace de domaine à un autre serveur de noms. Par conséquent, lors de la délégation de domaine, la responsabilité de répondre à la requête est déléguée à un autre serveur DNS. La délégation utilise des enregistrements NS.

Dans l'exemple suivant, sub1.abc.com est le sous-domaine d'abc.com. La procédure décrit les étapes permettant de déléguer le sous-domaine au serveur de noms ns2.sub1.abc.com et d'ajouter un enregistrement d'adresse pour ns2.sub1.abc.com.

Pour configurer la délégation de domaines, vous devez effectuer les tâches suivantes, qui sont décrites dans les sections suivantes :

1. Créez un enregistrement SOA pour un domaine.
2. Créez un enregistrement NS pour ajouter un serveur de noms pour le domaine.
3. Créez un enregistrement d'adresse pour le serveur de noms.
4. Créez un enregistrement NS pour déléguer le sous-domaine.
5. Créez un enregistrement Glue pour le serveur de noms.

Créer un enregistrement SOA

Pour obtenir des instructions sur la configuration des enregistrements SOA, reportez-vous à la section Créer des enregistrements SOA pour obtenir des informations faisant autorité.

Créer un enregistrement NS pour un serveur de noms

Pour obtenir des instructions sur la configuration d'un enregistrement NS, voir Créer des enregistrements NS pour un serveur faisant autorité. Dans la liste **Serveur de noms**, sélectionnez le serveur principal de noms faisant autorité, par exemple ns1.abc.com.

Créer un enregistrement d'adresse

Pour obtenir des instructions sur la configuration des enregistrements d'adresses, voir Créer des enregistrements d'adresses pour un nom de domaine. Dans les zones de texte Nom d'hôte et Adresse IP, tapez respectivement le nom de domaine de l'enregistrement Adresse DNS et l'adresse IP, par exemple ns1.abc.com et 10.102.11.135.

Créer un enregistrement NS pour la délégation de domaine

Pour obtenir des instructions sur la configuration des enregistrements NS, voir Créer des enregistrements NS pour un serveur faisant autorité. Dans la liste **Serveur de noms**, sélectionnez le serveur de noms principal faisant autorité, par exemple ns2.sub1.abc.com.

Créez un record de colle

Les enregistrements NS sont généralement définis immédiatement après l'enregistrement SOA (ce n'est pas une restriction). Un domaine doit comporter au moins deux enregistrements NS. Si un enregistrement NS est défini dans un domaine, il doit comporter un enregistrement d'adresse correspondant. Cet enregistrement d'adresses est appelé enregistrement colle. Les enregistrements de colle accélèrent les requêtes DNS.

Pour obtenir des instructions sur l'ajout d'enregistrements de colle pour un sous-domaine, reportez-vous à la procédure d'ajout d'un enregistrement Address (A), Configurer les enregistrements de ressources DNS.

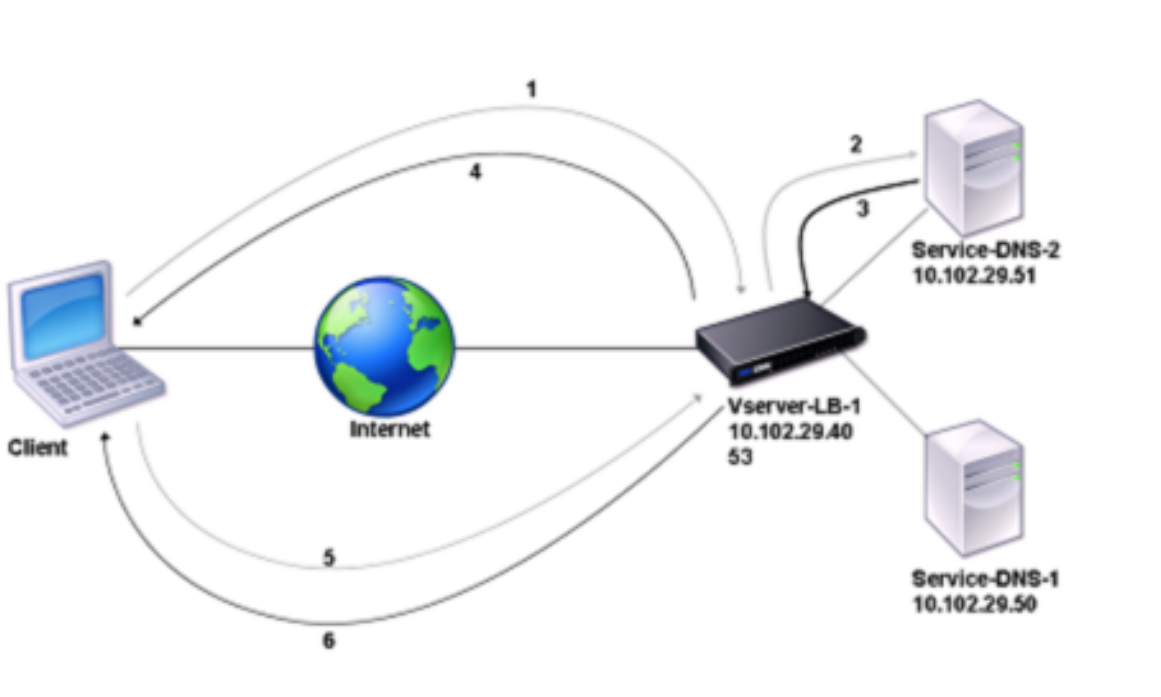
Pour obtenir des instructions sur la configuration des enregistrements d'adresses, voir Créer des enregistrements d'adresses pour un nom de domaine. Dans les zones de texte Nom d'hôte et Adresse IP, tapez le nom de domaine pour l'enregistrement Adresse DNS et l'adresse IP, par exemple ns2.sub1.abc.com et 10.102.12.135, respectivement.

Configurer l'appliance NetScaler en tant que serveur proxy DNS

May 5, 2023

En tant que serveur proxy DNS, l'appliance ADC peut fonctionner comme un proxy pour un seul serveur DNS ou pour un groupe de serveurs DNS. Le flux des demandes et des réponses est illustré dans l'exemple de diagramme topologique suivant.

Figure 1. NetScaler en tant que proxy DNS



Par défaut, l'appliance NetScaler met en cache les réponses des serveurs de noms DNS. Lorsque l'appliance reçoit une requête DNS, elle vérifie la présence du domaine interrogé dans son cache. Si l'adresse du domaine interrogé est présente dans son cache, NetScaler renvoie l'adresse correspondante au client. Sinon, il transmet la requête à un serveur de noms DNS qui vérifie la disponibilité de l'adresse et la renvoie à NetScaler. NetScaler renvoie ensuite l'adresse au client.

Pour les demandes concernant un domaine qui a déjà été mis en cache, NetScaler fournit l'enregistrement d'adresse du domaine à partir du cache sans interroger le serveur DNS configuré.

L'appliance supprime un enregistrement stocké dans son cache lorsque la valeur de durée de vie (TTL) de l'enregistrement atteint la valeur configurée. Un client qui demande un enregistrement expiré doit attendre que NetScaler récupère l'enregistrement sur le serveur et mette à jour son cache. Pour éviter ce retard, NetScaler met à jour le cache de manière proactive en récupérant l'enregistrement sur le serveur avant son expiration.

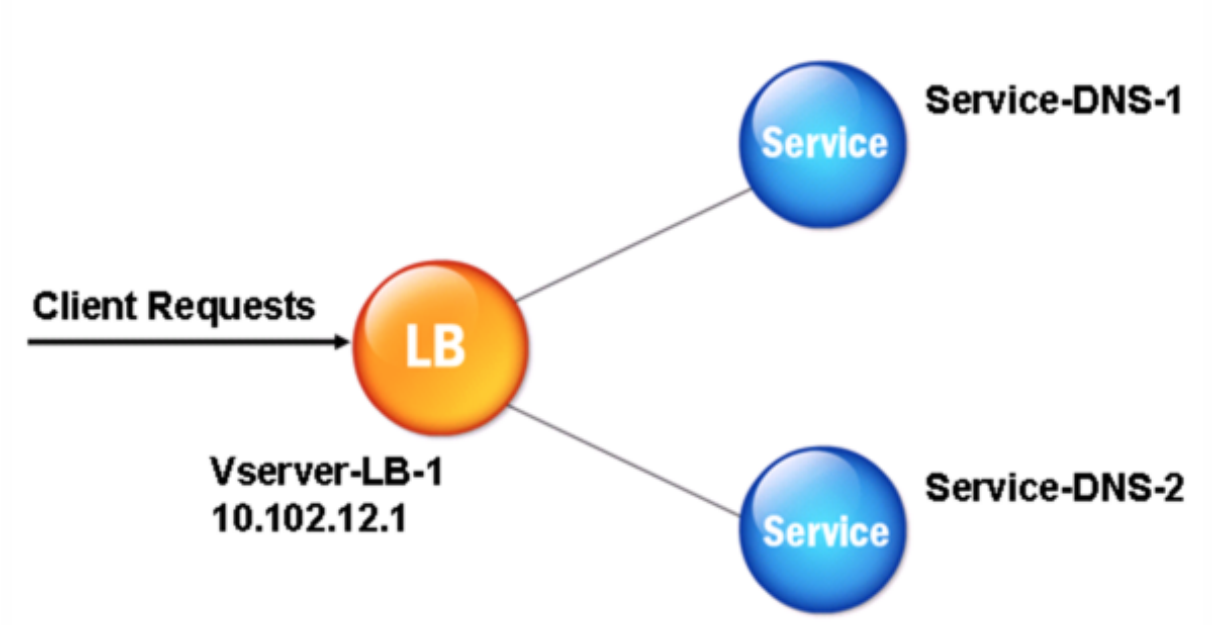
Le tableau suivant répertorie les exemples de noms et les valeurs des entités qui doivent être configurées sur NetScaler.

Tableau 1. Exemple de configuration de l'entité proxy DNS

Type d'entité	Nom	Adresse IP	Type	Port
Serveur virtuel LB	Vserver-DNS-1	10.102.29.40	DNS	53
Services	Service-DNS-1	10.102.29.50	DNS	53
Services	Service-DNS-2	10.102.29.51	DNS	53

Le schéma suivant montre les entités d'un proxy DNS et les valeurs des paramètres à configurer sur NetScaler.

Figure 2. Modèle d'entité proxy DNS



> **Remarque**
>
> Pour configurer la fonctionnalité de proxy DNS, vous devez savoir comment configurer les services d'équilibrage de charge et les serveurs virtuels.

Créer un serveur virtuel d'équilibrage de charge

Pour configurer un proxy DNS sur NetScaler, configurez un serveur virtuel d'équilibrage de charge de type DNS. Pour configurer un serveur virtuel DNS afin d'équilibrer la charge d'un ensemble de serveurs DNS prenant en charge les requêtes récursives, vous devez définir l'option Récursivité disponible. Avec cette option, le bit RA est défini sur ON dans les réponses DNS du serveur virtuel DNS.

Pour obtenir des instructions sur la création d'un serveur virtuel d'équilibrage de charge, voir Équilibrage decharge.

Créer des services DNS

Après avoir créé un serveur virtuel d'équilibrage de charge de type DNS, vous devez créer des services DNS. Vous pouvez ajouter, modifier, activer, désactiver et supprimer un service DNS. Pour obtenir des instructions sur la création d'un service DNS, voir Équilibrage de charge.

Lier un serveur virtuel d'équilibrage de charge aux services DNS

Pour terminer la configuration du proxy DNS, vous devez lier les services DNS au serveur virtuel d'équilibrage de charge. Pour obtenir des instructions sur la liaison d'un service à un serveur virtuel d'équilibrage de charge, reportez-vous à la section Équilibrage de charge.

Configurer la configuration du proxy DNS pour utiliser TCP

Certains clients utilisent le protocole UDP (User Datagram Protocol) pour les communications DNS. Toutefois, le protocole UDP spécifie une taille de paquet maximale de 512 octets. Lorsque la longueur de la charge utile dépasse 512 octets, le client doit utiliser le protocole TCP. Lorsqu'un client envoie une requête DNS à l'appliance NetScaler, l'appliance transmet la requête à l'un des serveurs de noms. Si la réponse est trop volumineuse pour un paquet UDP, le serveur de noms définit le bit de troncature dans sa réponse à NetScaler. Le bit de troncature indique que la réponse est trop volumineuse pour UDP et que le client doit envoyer la requête via une connexion TCP. L'appliance ADC transmet la réponse au client avec le bit de troncature intact. Il attend que le client initie une connexion TCP avec l'adresse IP du serveur virtuel d'équilibrage de charge DNS, sur le port 53. Le client envoie la demande via une connexion TCP. L'appliance NetScaler transmet ensuite la demande au serveur de noms et transmet la réponse au client.

Pour configurer NetScaler afin qu'il utilise le protocole TCP pour le DNS, vous devez configurer un serveur virtuel d'équilibrage de charge et des services, tous deux de type DNS_TCP. Vous pouvez configurer des moniteurs de type DNS_TCP pour vérifier l'état des services. Pour obtenir des instructions sur la création de serveurs virtuels, de services et de moniteurs DNS_TCP, reportez-vous à la section Équilibrage de charge.

Pour mettre à jour les enregistrements de manière proactive, NetScaler utilise une connexion TCP avec le serveur pour récupérer les enregistrements.

> **Important**
>
> Pour configurer NetScaler de manière à utiliser le protocole UDP pour le DNS et à n'utiliser le protocole TCP que lorsque la longueur de la charge utile du protocole UDP dépasse 512 octets, vous devez configurer à la fois les services DNS et DNS_TCP. L'adresse IP du service DNS_TCP doit être identique à l'adresse IP du service DNS.

Configurer les valeurs de durée de vie des entrées DNS

Le TTL est le même pour tous les enregistrements DNS ayant le même nom de domaine et le même type d'enregistrement. Si la valeur TTL est modifiée pour l'un des enregistrements, la nouvelle valeur est reflétée dans tous les enregistrements du même nom de domaine et du même type. La valeur TTL par défaut est de 3 600 secondes. Le minimum est 0 et le maximum est 604800. Si une entrée DNS possède une valeur TTL inférieure au minimum ou supérieure au maximum, elle est enregistrée en tant que valeur TTL minimale ou maximale, respectivement.

Spécifiez le TTL minimum et maximum à l'aide de l'interface de ligne de commande

À l'invite de commandes NetScaler, tapez les commandes suivantes pour spécifier le TTL minimum et maximum et vérifier la configuration :

```
1 -  set dns parameter [-minTTL <secs>] [-maxTTL <secs>]
2 -  show dns parameter
3 <!--NeedCopy-->
```

Exemple :

```
1 > set dns parameter -minTTL 1200 -maxTTL 1800
2  Done
3 > show dns parameter
4         DNS parameters:
5         DNS retries: 5
6         Minimum TTL: 1200               Maximum TTL: 1800
7             .
8             .
```



```
9                .
10  Done
11 >
12 <!--NeedCopy-->
```

Spécifiez le TTL minimum et maximum à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue Configurer les paramètres DNS, dans TTL, dans les zones de texte Minimum et Maximum, tapez respectivement la durée de vie minimale et maximale (en secondes), puis cliquez sur OK.

Remarque : Lorsque le TTL expire, l'enregistrement est supprimé du cache. NetScaler contacte les serveurs de manière proactive et obtient l'enregistrement DNS juste avant son expiration.

Effacer les enregistrements DNS

Vous pouvez supprimer tous les enregistrements DNS présents dans le cache. Par exemple, vous souhaiterez peut-être vider les enregistrements DNS lorsqu'un serveur est redémarré après que des modifications ont été apportées.

Supprimer tous les enregistrements de proxy à l'aide de l'interface de ligne de commande

À l'invite de commande NetScaler, tapez :

```
flush dns proxyRecords
```

Supprimer tous les enregistrements de proxy à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Enregistrements**.
2. Dans le volet de détails, cliquez sur Flush Proxy Records.

Ajouter des enregistrements de ressources DNS

Vous pouvez ajouter des enregistrements DNS à un domaine pour lequel l'appliance NetScaler est configurée en tant que serveur proxy DNS. Pour plus d'informations sur l'ajout d'enregistrements DNS, reportez-vous à la section Configuration des enregistrements de ressources DNS.

Suppression d'un serveur virtuel DNS équilibrage de charge

Pour plus d'informations sur la suppression d'un serveur virtuel d'équilibrage de charge, voir Équilibrage decharge.

Limiter le nombre de demandes DNS simultanées sur une connexion client

Vous pouvez limiter le nombre de requêtes DNS simultanées sur une seule connexion client, identifiée par le `<clientip:port>-<vserver ip:port>` tuple. Les demandes DNS simultanées sont les demandes que l'appliance NetScaler a transmises aux serveurs de noms et pour lesquelles l'appliance attend des réponses. La limitation du nombre de demandes simultanées sur une connexion client vous permet de protéger les serveurs de noms lorsqu'un client hostile tente une attaque par déni de service distribué (DDoS) en envoyant un flot de requêtes DNS. Lorsque la limite pour une connexion client est atteinte, les requêtes DNS suivantes sur la connexion sont abandonnées jusqu'à ce que le nombre de demandes en attente passe en dessous de la limite. Cette limite ne s'applique pas aux demandes que l'appliance NetScaler traite à partir de son cache.

La valeur par défaut de ce paramètre est 255. Cette valeur par défaut est suffisante dans la plupart des scénarios. Si les serveurs de noms traitent de nombreuses demandes DNS simultanées dans des conditions de fonctionnement normales, vous pouvez spécifier une valeur élevée ou une valeur nulle (0). La valeur 0 désactive cette fonctionnalité et indique qu'il n'y a pas de limite au nombre de requêtes DNS autorisées sur une seule connexion client. Ce paramètre est un paramètre global qui s'applique à tous les serveurs virtuels DNS configurés sur l'appliance NetScaler.
La valeur par défaut de ce paramètre est 255. Cette valeur par défaut est suffisante dans la plupart des scénarios. Si les serveurs de noms traitent de nombreuses demandes DNS simultanées dans des conditions de fonctionnement normales, vous pouvez spécifier une valeur élevée ou une valeur nulle (0). La valeur 0 désactive cette fonctionnalité et indique qu'il n'y a pas de limite au nombre de requêtes DNS autorisées sur une seule connexion client. Ce paramètre est un paramètre global qui s'applique à tous les serveurs virtuels DNS configurés sur l'appliance NetScaler.
La valeur par défaut de ce paramètre est 255. Cette valeur par défaut est suffisante dans la plupart des scénarios. Si les serveurs de noms traitent de nombreuses demandes DNS simultanées dans des conditions de fonctionnement normales, vous pouvez spécifier une valeur élevée ou une valeur nulle (0). La valeur 0 désactive cette fonctionnalité et indique qu'il n'y a pas de limite au nombre de requêtes DNS autorisées sur une seule connexion client. Ce paramètre est un paramètre global qui s'applique à tous les serveurs virtuels DNS configurés sur l'appliance NetScaler.

Spécifiez le nombre maximum de demandes DNS simultanées autorisées sur une seule connexion client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour spécifier le nombre maximum de demandes DNS simultanées autorisées sur une seule connexion client et vérifier la configuration :


```
-  set dns parameter -maxPipeline <positive_integer>
-  show dns parameter
<!--NeedCopy-->
```

Exemple :

```
> set dns parameter -maxPipeline 1000
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
        .
        .
        .
        Max DNS Pipeline Requests: 1000
 Done
<!--NeedCopy-->
```

Spécifiez le nombre maximum de requêtes DNS simultanées autorisées sur une seule connexion client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue Configurer les paramètres DNS, spécifiez une valeur pour le nombre maximum de demandes de pipeline DNS.
4. Cliquez sur OK.

Configurer NetScaler en tant que résolveur final

May 5, 2023

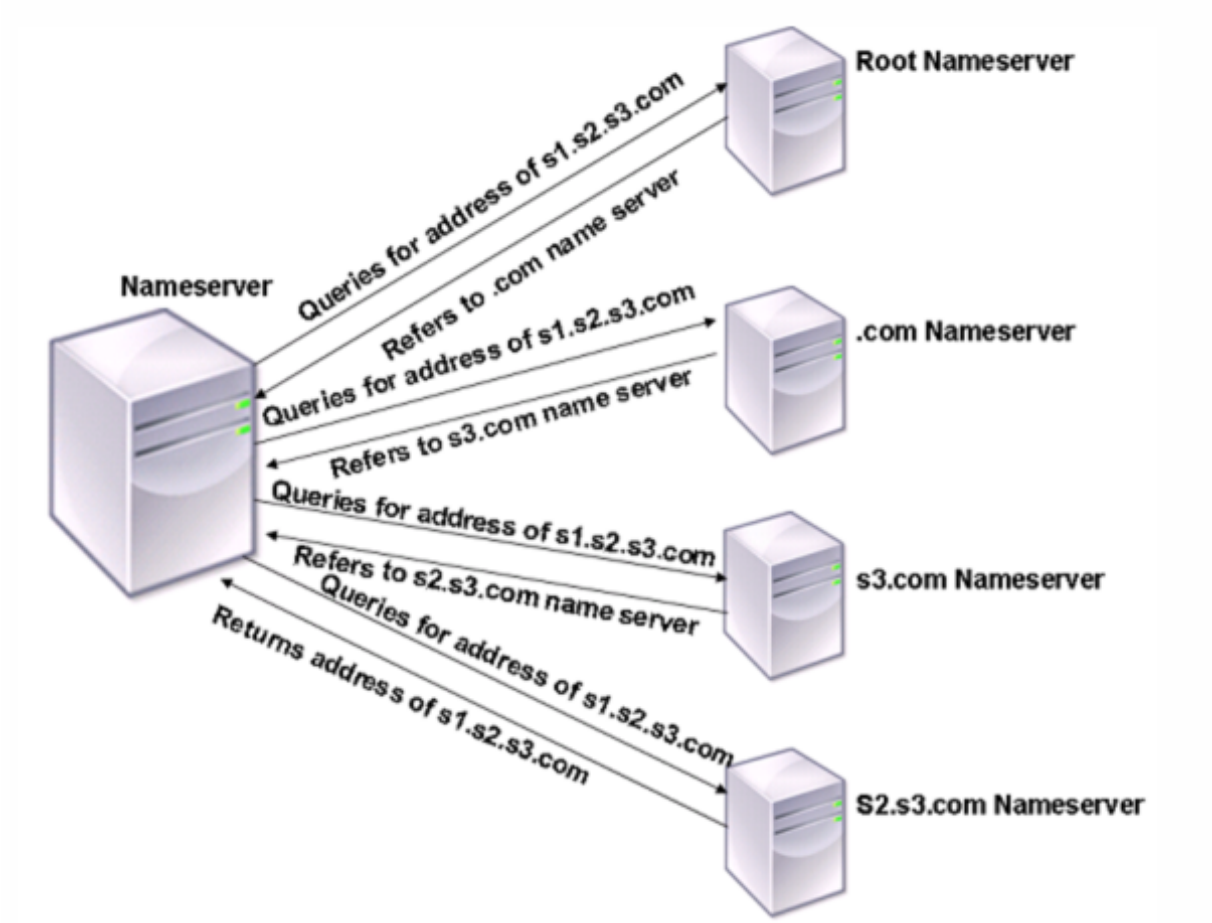
Un résolveur est une procédure invoquée par un programme d'application qui traduit un nom de domaine/hôte en son enregistrement de ressources. Le résolveur interagit avec le LDNS, qui recherche le nom de domaine pour obtenir son adresse IP. NetScaler peut fournir une résolution de bout en bout pour les requêtes DNS.

En résolution récursive, l'appliance NetScaler interroge différents serveurs de noms de manière récursive pour accéder à l'adresse IP d'un domaine. Lorsque NetScaler reçoit une demande DNS, il vérifie la présence de l'enregistrement DNS dans son cache. Si l'enregistrement n'est pas présent dans le cache, il interroge les serveurs racines configurés dans le fichier ns.conf. Le serveur de noms racine

renvoie l'adresse d'un serveur DNS contenant des informations détaillées sur le domaine de deuxième niveau. Le processus est répété jusqu'à ce que l'enregistrement requis soit trouvé.

Lorsque vous démarrez l'appliance NetScaler pour la première fois, 13 serveurs de noms root sont ajoutés au fichier ns.conf. Les enregistrements NS et Address pour les 13 serveurs racines sont également ajoutés. Vous pouvez modifier le fichier ns.conf, mais NetScaler ne vous permet pas de supprimer les 13 enregistrements. Au moins une entrée de serveur de noms est requise pour que l'appliance puisse effectuer la résolution des noms. Le schéma suivant illustre le processus de résolution des noms.

Figure 1. Résolution récursive



Dans le processus illustré dans le schéma, lorsque le serveur de noms reçoit une requête concernant l'adresse de s1.s2.s3.com, il vérifie d'abord les serveurs de noms racines pour détecter s1.s2.s3.com. Un serveur de noms racine indique l'adresse du serveur de noms .com. Si l'adresse de s1.s2.s3.com est trouvée dans le serveur de noms, il répond avec une adresse IP appropriée. Sinon, il interroge d'autres serveurs de noms pour s3.com, puis pour s2.s3.com pour récupérer l'adresse de s1.s2.s3.com. Ainsi, la résolution commence toujours par les serveurs de noms racines et se termine par le serveur de noms officiel du domaine.

> Remarque
>
> Pour la fonctionnalité de résolution récursive, la mise en cache doit être activée.

Activer la résolution récursive

Pour configurer l'appliance NetScaler afin qu'elle fonctionne comme un résolveur final, vous devez activer la résolution récursive sur l'appliance. Vous devez également ajouter un serveur de noms DNS avec l'option locale pour que la fonctionnalité fonctionne.

Activer la résolution récursive à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour activer la résolution récursive et vérifier la configuration :

```
-  set dns parameter -recursion ENABLED
-  show dns parameter
<!--NeedCopy-->
```

Exemple :

```
> set dns parameter -recursion ENABLED
 Done
> show dns parameter
        DNS parameters:
            .
            .
            .
        Recursive Resolution : ENABLED
            .
            .
            .
 Done
<!--NeedCopy-->
```

Activer la résolution récursive à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue Configurer les paramètres DNS, cochez la case Activer la récursivité, puis cliquez sur OK.

Ajoutez un serveur de noms (lorsque l'appliance NetScaler agit en tant que résolveur) à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>)
<!--NeedCopy-->
```

Exemple :

```
add dns nameServer 10.102.9.19 -local
show dns nameServer
1)  10.102.9.19 LOCAL -  State: UP  Protocol: UDP
Done
<!--NeedCopy-->
```

Local : marquez l'adresse IP comme appartenant à un serveur DNS récursif local sur l'appliance NetScaler. L'appliance résout de manière récursive les requêtes reçues sur une adresse IP marquée comme étant locale.
Pour que la résolution récursive fonctionne, le paramètre DNS global `recursion` doit également être défini.
Si aucun serveur de noms n'est marqué comme étant local, l'appliance fonctionne comme un résolveur de stub et équilibre la charge des serveurs de noms.

Ajouter un serveur de noms à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **DNS** > **Serveurs de noms** et créez un serveur de noms.

Activer le référencement root DNS

Le référencement root DNS est désactivé par défaut. Lorsqu'elle est activée, l'appliance ADC répond avec les enregistrements de référence root.

Envoyez une référence root si un client demande un nom de domaine qui n'est pas lié aux domaines configurés/mis en cache sur l'appliance NetScaler. Si le paramètre est désactivé, l'appliance envoie une réponse vide au lieu d'une référence root. Applicable aux domaines pour lesquels l'appliance fait autorité. Désactivez le paramètre lorsque l'appliance est attaquée par un client qui envoie un flot de requêtes pour des domaines non liés.

Activer le référencement root à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour activer la résolution récursive et vérifier la configuration :


```
-  set dns parameter -dnsrootReferral ENABLED
-  show dns parameter
<!--NeedCopy-->
```

Exemple :

```
> set dns parameter -recursion ENABLED
 Done
> show dns parameter
        DNS parameters:
            .
            .
            .
        DNS Root Referral : ENABLED
            .
            .
            .
 Done
<!--NeedCopy-->
```

Activer le référencement root à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres DNS**.
3. Dans la boîte de dialogue **Configurer les paramètres DNS**, cochez la case **Activer le référencement root**, puis cliquez sur **OK**.

Définissez le nombre de nouvelles tentatives

Configurez l'appliance ADC pour qu'elle effectue un nombre préconfiguré de tentatives (appelées nouvelles tentatives DNS) lorsqu'elle ne reçoit pas de réponse du serveur auquel elle envoie une requête. Par défaut, le nombre de nouvelles tentatives DNS est défini sur 5.

Définissez le nombre de nouvelles tentatives DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir le nombre de nouvelles tentatives et vérifier la configuration :

```
-  set dns parameter -retries <positive_integer>
-  show dns parameter
<!--NeedCopy-->
```


Exemple :

```
> set DNS parameter -retries 3
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 3
            .
            .
            .
 Done
<!--NeedCopy-->
```

Définissez le nombre de nouvelles tentatives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres DNS.
3. Dans la boîte de dialogue Configurer les paramètres DNS, dans la zone de texte Retentatives DNS, tapez le nombre de nouvelles tentatives du résolveur DNS, puis cliquez sur OK.

Configurer l'appliance NetScaler en tant que redirecteur

May 5, 2023

Un redirecteur est un serveur qui transmet des requêtes DNS à des serveurs DNS situés en dehors du réseau du serveur de redirecteur. Les requêtes qui ne peuvent pas être résolues localement sont transmises à d'autres serveurs DNS. Un redirecteur accumule des informations DNS externes dans son cache lorsqu'il résout des requêtes DNS. Pour configurer l'appliance NetScaler en tant que redirecteur, vous devez ajouter un serveur de noms externe.

L'appliance NetScaler vous permet d'ajouter des serveurs de noms externes auxquels elle peut transmettre les requêtes de résolution de noms qui ne peuvent pas être résolues localement. Pour configurer l'appliance NetScaler en tant que redirecteur, vous devez ajouter les serveurs de noms auxquels elle doit transmettre les requêtes de résolution de noms. Vous pouvez spécifier la priorité de recherche pour spécifier le service de noms que l'appliance NetScaler doit utiliser pour la résolution des noms.

Pour plus d'informations sur la configuration de l'appliance NetScaler en tant que redirecteur, voir Ajouter un serveur de noms (lorsque l'appliance NetScaler agit en tant que redirecteur) à l'aide de l'interface de ligne decommande.

> **Remarque :**
>
> L'appliance NetScaler en mode redirecteur prend en charge les serveurs de noms TCP, UDP et UDP-TCP.
>
> - Si vous avez configuré un serveur de noms TCP, l'appliance NetScaler envoie la demande DNS via TCP.
> - Si vous avez configuré un serveur de noms UDP, l'appliance NetScaler envoie la demande DNS via UDP.
> - Si vous avez configuré un serveur de noms UDP-TCP, l'appliance NetScaler envoie la demande DNS via UDP. Toutefois, si le bit tronqué est défini dans la réponse DNS, l'appliance envoie ces demandes DNS via TCP.

Ajouter un serveur de noms

Vous pouvez créer un serveur de noms en spécifiant son adresse IP ou en configurant un serveur virtuel existant comme serveur de noms.

- Serveur de**noms basé sur les adresses IP : serveur** de noms externe à contacter pour la résolution des noms de domaine. Si plusieurs serveurs de noms basés sur des adresses IP sont configurés sur l'appliance et que le paramètre local n'est défini sur aucun d'entre eux, la charge des requêtes DNS entrantes est équilibrée sur tous les serveurs de noms, de manière circulaire.
- **Serveur de noms basé sur un serveur virtuel** : serveur virtuel DNS configuré dans NetScaler. Pour un contrôle plus précis de la manière dont les serveurs de noms DNS externes sont équilibrés (par exemple, vous souhaitez utiliser une méthode d'équilibrage de charge autre que la méthode Round Robin), procédez comme suit :
- Configuration d'un serveur virtuel DNS sur l'appliance
- Liez les serveurs de noms externes en tant que services
- Spécifiez le nom du serveur virtuel dans cette commande.

Pour vérifier la configuration, vous pouvez utiliser la commande `show dns nameServer`.

Pour supprimer un serveur de noms, dans l'interface de ligne de commande NetScaler, tapez la `rm dns nameServer` commande suivie de l'adresse IP du serveur de noms.

Pour afficher les détails du serveur de noms DNS, sur l'interface de ligne de commande NetScaler, tapez la `show dns nameServer` commande suivie de l'adresse IP du serveur de noms.

Ajoutez un serveur de noms (lorsque l'appliance NetScaler agit en tant que redirecteur) à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
1 add dns nameServer ((<IP>) | <dnsVserverName>)
```



```
<!--NeedCopy-->
```

Ou

```
add dns nameServer ((<IP> | <dnsVserverName>) [-type <type>]
<!--NeedCopy-->
```

Exemples :

```
add dns nameServer dnsVirtualNS

add dns nameServer 192.0.2.11 -type TCP

add dns nameServer 192.0.2.12 -type UDP_TCP


add dns nameServer 192.0.2.10
show dns nameServer 192.0.2.10

1) 192.0.2.10  -  State: UP  Protocol: UDP
Done
<!--NeedCopy-->
```

> **Remarque :**
>
> Si le type de serveur de noms n'est pas spécifié, un serveur de noms UDP est créé par défaut. Pour créer un serveur de noms de type TCP ou UDP_TCP, vous devez spécifier le type.
>
> Lorsque vous spécifiez le type UDP_TCP, deux serveurs de noms (un serveur de noms UDP et un serveur de noms TCP) sont créés pour l'adresse IP donnée.

Ajoutez un serveur de noms (lorsque l'appliance NetScaler agit en tant que résolveur) à l'aide de l'interface de ligne de commande

Spécifiez le paramètre `local` d'un résolveur récursif. Activez la récursivité en utilisant la commande `set dns parameter`.

À l'invite de commande, tapez :

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>)
show dns nameServer
set dns parameter -recursion ENABLED
show dns parameter
<!--NeedCopy-->
```

Exemple :


```
add dns nameServer 10.102.9.19 -local
show dns nameServer
1)  10.102.9.19 LOCAL -  State: UP  Protocol: UDP
Done
set dns parameter -recursion ENABLED
Done
show dns parameter
        DNS parameters:
            .
            .
            .
        Recursive Resolution : ENABLED
            .
            .
            .
Done
<!--NeedCopy-->
```

Local : marquez l'adresse IP comme appartenant à un serveur DNS récursif local sur l'appliance NetScaler. L'appliance résout de manière récursive les requêtes reçues sur une adresse IP marquée comme étant locale.
Pour que la résolution récursive fonctionne, le paramètre DNS global `recursion` doit également être défini.
Si aucun serveur de noms n'est marqué comme étant local, l'appliance fonctionne comme un résolveur de stub et équilibre la charge des serveurs de noms.

Ajouter un serveur de noms à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **DNS** > **Serveurs de noms** et créez un serveur de noms.

Définir la priorité de recherche DNS

Vous pouvez définir la priorité de recherche sur DNS ou WINS. Cette option est utilisée dans le mode de fonctionnement du VPN SSL.

Définissez la priorité de recherche sur le DNS à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour définir la priorité de recherche du DNS et vérifier la configuration :

```
-  set dns parameter -nameLookupPriority (DNS | WINS)
-  show dns parameter
```



```
<!--NeedCopy-->
```

Exemple :

```
> set dns parameter -nameLookupPriority DNS
 Done
> show dns parameter
                .
                .
                .
         Name lookup priority : DNS
                .
                .
                .
 Done
<!--NeedCopy-->
```

Définissez la priorité de recherche du DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres DNS**.
3. Dans la boîte de dialogue **Configurer les paramètres DNS**, sous **Priorité de recherche de noms**, sélectionnez DNS ou WINS, puis cliquez sur **OK.**

> **Remarque**
>
> Si le serveur virtuel DNS que vous avez configuré est en panne et si vous le définissez sur `-nameLookupPriority` DNS, NetScaler ne tente pas de rechercher WINS. Par conséquent, si un serveur virtuel DNS n'est pas configuré ou est désactivé, définissez`-nameLookupPriority` la sur WINS.

Désactiver et activer les serveurs de noms

La procédure suivante décrit les étapes à suivre pour activer ou désactiver un serveur de noms existant.

Activer ou désactiver un serveur de noms à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver un serveur de noms et vérifier la configuration :

```
-  (enable | disable) dns nameServer <IPAddress>
-  show dns nameServer <IPAddress>
```



```
<!--NeedCopy-->
```

Exemple :

```
> disable dns nameServer 10.102.9.19
 Done
> show dns nameServer 10.102.9.19
1)       10.102.9.19: LOCAL  -  State: OUT OF SERVICE
 Done
<!--NeedCopy-->
```

Activer ou désactiver un serveur de noms à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Serveurs de noms**.
2. Dans le volet d'informations, sélectionnez le serveur de noms que vous souhaitez activer ou désactiver.
3. Cliquez sur **Activer** ou **Désactiver**. Si un serveur de noms est activé, l'option **Désactiver** est disponible. Si un serveur de noms est désactivé, l'option **Activer** est disponible.

Configurer NetScaler en tant que résolveur de stubs non validant et sensible à la sécurité

May 5, 2023

À partir de NetScaler 12.1 build 49.xx, NetScaler agit comme un résolveur de stubs non validant et soucieux de la sécurité. Pour activer cette prise en charge, le bit AD est défini dans l'en-tête DNS et le bit DO n'est pas défini dans l'en-tête OPT. Lorsque le bit AD est défini et que le bit DO n'est pas défini, le résolveur récursif en amont valide la réponse DNSSEC. Si la validation est réussie, le résolveur récursif répond sans les RR DNSSEC. Si la validation DNSSEC échoue, le résolveur récursif renvoie une réponse SERVFAIL.

> **Important :**
>
> Le bit AD est défini par défaut dans le redirecteur ADC. Le bit AD n'est pas défini pour les requêtes initiées par DBS.

Prise en charge des trames Jumbo pour le DNS pour gérer les réponses de grande taille

May 5, 2023

À partir de NetScaler 12.1 build 49.xx, le DNS prend en charge les trames jumbo pour gérer les réponses UDP supérieures à 1 280 octets. Auparavant, l'appliance NetScaler ne prenait en charge que des paquets UDP d'une taille maximale de 1 280 octets.

Vous pouvez définir la taille maximale des paquets UDP que l'appliance peut gérer en modes proxy, ADNS et redirecteur en configurant la valeur du paramètre Taille maximale des paquets UDP. Par exemple, si la valeur du paramètre Taille maximale des paquets UDP est définie sur 4 096, l'appliance peut gérer une réponse DNS d'une taille de 4 096 octets.

> **Important**
>
> - En mode proxy, la taille la plus faible entre la taille de la charge utile OPT de la demande client et la valeur de taille maximale des paquets UDP est prise en compte pour l'envoi de requêtes DNS au serveur principal. Par exemple, si la taille de la charge utile OPT de la demande client est de 3 000 et que la valeur de la taille maximale des paquets UDP est de 4 096, des requêtes DNS de 3 000 octets sont envoyées au serveur principal.
>
> De plus, depuis le serveur principal, l'appliance peut recevoir des réponses de grande taille et traiter des réponses de grande taille.
> - En mode redirecteur, l'appliance définit la taille de la charge utile OPT égale à la valeur du paramètre de taille de paquet UDP.
> - Si les enregistrements DNS sont locaux, l'appliance peut composer des tailles de réponse aussi élevées que la valeur du paramètre Taille maximale des paquets UDP. Ce paramètre s'applique aux résolveurs ADNS, proxy et récursifs.

Pour configurer la taille de paquet UDP maximale à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set dns parameter [-maxUDPPacketSize <positive_integer>]
<!--NeedCopy-->
```

Exemple :

```
set dns parameter -maxUDPPacketSize 10000
<!--NeedCopy-->
```


> **Remarque :**
>
> Les valeurs minimales et maximales que vous pouvez définir pour le paramètre Taille maximale des paquets UDP sont 512 et 16384 respectivement. La valeur par défaut est 1280.

Pour configurer la taille maximale des paquets UDP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **DNS**.
2. Dans le volet d'informations, cliquez sur **Modifier les paramètres DNS**.
3. Dans Taille maximale des paquets UDP, spécifiez la taille maximale des paquets UDP.
4. Cliquez sur **OK**.

Configurer la journalisation DNS

May 8, 2023

Vous pouvez configurer l'appliance NetScaler pour qu'elle enregistre les demandes et les réponses DNS qu'elle gère. La solution matérielle-logicielle consigne les demandes et réponses DNS au format SYSLOG. Vous pouvez choisir de consigner les demandes DNS ou les réponses DNS, ou les deux, et d'envoyer les messages Syslog à un serveur de journaux distant. Les messages de journal peuvent être utilisés pour :

- Audit des réponses DNS au client
- Audit des clients DNS
- Détecter et prévenir les attaques DNS
- Dépanner

Une appliance NetScaler peut enregistrer les sections suivantes dans la demande ou la réponse DNS, en fonction de votre configuration :

- Section d'en-tête
- Section des questions
- Section Réponses
- Section de l'autorité
- Section **supplémentaire**

Profils DNS

Vous pouvez utiliser un profil DNS pour configurer les différents paramètres DNS que vous souhaitez que le point de terminaison DNS applique au trafic DNS. Dans le profil, vous pouvez activer la journalisation, la mise en cache et la mise en cache négative.

Important : Depuis la version NetScaler 11.0, l'activation de la mise en cache DNS à l'aide des paramètres DNS globaux est obsolète. Vous pouvez activer ou désactiver la mise en cache DNS à l'aide de profils DNS. Vous pouvez désormais activer la mise en cache DNS pour un serveur virtuel individuel en activant la mise en cache DNS dans un profil DNS et en définissant le profil DNS sur le serveur virtuel individuel.

Les profils DNS prennent en charge les types de journalisation DNS suivants :

- Journalisation des requêtes DNS
- Journalisation de la section de réponses DNS
- Journalisation étendue DNS
- Journalisation des erreurs DNS

Journalisation des requêtes DNS

Vous pouvez configurer une appliance NetScaler pour qu'elle enregistre uniquement les requêtes DNS reçues par les points de terminaison DNS de l'appliance.

Remarque : Si des erreurs se produisent pendant le traitement d'une requête, elles sont consignées si cette option est définie dans le profil DNS.

Voici un exemple de message de journal des requêtes :

```
1 DNS DNS_QUERY 143 0 :  U:10.102.27.70#61297:10.102.27.73#53/22142/Q/
2 (RD)/NO/1/0/0/0#test.com./1#
3 <!--NeedCopy-->
```

Journalisation de la section de réponses DNS

Vous pouvez configurer une appliance NetScaler pour enregistrer toutes les sections de **réponse** dans les réponses DNS que l'appliance envoie au client. La journalisation de la section des réponses DNS est utile lorsque NetScaler est configuré en tant que résolveur DNS ou dans les cas d'utilisation de GLSB.

Voici un exemple de journal de section de réponses DNS :

```
1 DNS DNS_RESPONSE 6678 0 :  U:100.100.100.210#32776:100.100.100.10#
2 53/61373/Q/(RD,AA,RA,R)/NO/1/1/2/4#n1.citrix.com1./
3 28#ANS#AAAA/120/1111:2345:6789:ffab:abcd:effa:1234:3212##
4 <!--NeedCopy-->
```


Journalisation étendue DNS

Pour configurer une appliance NetScaler afin de consigner l'autorité et les sections **supplémentaires** dans les réponses DNS, activez la journalisation étendue avec la journalisation des sections de réponses.

Remarque : Si des erreurs se produisent pendant le traitement des requêtes ou des réponses, elles sont consignées si cette option est définie dans le profil DNS.

Voici un exemple de message consigné lorsque la recherche du cache est terminée et que la réponse est incorporée dans le paquet :

```
DNS DNS_RESPONSE 2252 0 :  T:100.100.100.118#21411:100.100.100.10
#53/48537/Q/(RD,AA,CD,RA,R)/NO/1/1/2/6#a1.citrix.com1./1#ANS#A/
120/1.1.1.1##AUTH#citrix.com1/NS/120/n2.citrix.com1#n1.citrix.com1##ADD
   #n1.citrix.com1
/A/120/1.1.1.1#1.1.1.2##n1.citrix.com1/AAAA/120/
1111:2345:6789:ffab:abcd:effa:1234:3212##n2.citrix.com1/A/120/2.1.1.2
##n2.citrix.com1/AAAA/120/2222:faff:3212:8976:123:1241:64:ff9b##OPT
   /0/1280/DO##
<!--NeedCopy-->
```

Journalisation des erreurs DNS

Vous pouvez configurer une appliance NetScaler pour consigner les erreurs ou les échecs qui se produisent lorsqu'elle traite une requête ou une réponse DNS. Pour ces erreurs, la solution matérielle-logicielle consigne l'en-tête DNS, les sections **Question** et les enregistrements OPT.

Voici un exemple de message consigné lorsqu'une erreur se produit pendant le traitement d'une demande ou d'une réponse DNS :

```
DNS DNS_ERROR 149 0 :  U:10.102.27.70#27832:10.102.27.73#53/61153/Q/
(RD)/NO/1/0/0/0#test.com./1140#Packet Dropped
<!--NeedCopy-->
```

Journalisation basée sur des stratégies

Vous pouvez configurer la journalisation personnalisée basée sur des expressions DNS en configurant les stratégies LogAction on DNS, Rewrite ou Responder. Vous pouvez spécifier que la journalisation se produit uniquement lorsqu'une stratégie DNS particulière est évaluée à true. Pour plus d'informations, voir Configurer la journalisation basée sur des stratégies pour DNS.

Comprendre le format des messages du journal Syslog de NetScaler

L'appliance NetScaler enregistre les demandes et les réponses DNS au format Syslog suivant :

```
<transport> :<client IP>#<client ephemeral port>:<DNS endpoint IP>#<
   port>
 : <query id> /opcode/header flags/rcode/question section count/answer
    section count
/ auth section count / additional section count #<queried domain name>
/<queried type>#...
<!--NeedCopy-->
```

- **<transport>:**
  - T = TCP
  - U = UDP
- **<client IP>#< client ephemeral port >:** adresse IP et numéro de port du client DNS
- **\# \ : Adresse IP et numéro de port du point de terminaison DNS NetScaler** <DNS endpoint IP> <port>
- **<query id>:**
  ID de requête
- **<opcode>:** code d'opération. Valeurs prises en charge :
  - Q : requête
  - I : requête inverse
  - S : état
  - X0 : non affecté
  - N : notifier
  - U : mise à jour
  - X1-10 : valeurs non attribuées
- **<header flags>:** drapeaux. Valeurs prises en charge :
  - RD : récursion souhaitée
  - TC : tronqué
  - AA : réponse faisant autorité
  - CD : vérification désactivée
  - AD : données authentifiées
  - Z : non affecté
  - RA : récursion disponible
  - R : réponse
- **<rcode>:** code de réponse. Valeurs prises en charge :

  - NO : aucune erreur
  - F Erreur de format
  - S : défaillance du serveur
  - NX : domaine inexistant
  - NI : non implémenté
  - R : requête refusée
  - YX : le nom existe alors qu'il ne doit pas
  - YXR : RR Set existe alors qu'il ne doit pas
  - NXR : Le jeu de RR qui doit exister n'existe pas
  - NAS : le serveur ne fait pas autorité pour la zone
  - NA : Non autorisé
  - NZ : nom non contenu dans la zone
  - X1-5 : non affecté

- **/nombre de sections de questions/nombre de sections de réponse/nombre de sections auth/nombre de sections supplémentaires :** section de question, nombre de sections d'autorité et nombre de sections **supplémentaires** dans la requête DNS
- **<queried domain name>/<queried type>:** domaine interrogé et type interrogé dans la requête DNS
- **#ANS#<record type>/<ttl>/.. #AUTH#<domain name>/<record type>/<ttl>.. #ADD#<domain name>/<record type>/<ttl>...:**

  Dans les réponses DNS :

  La section Réponses est consignée si la journalisation de la section de réponses est activée dans le profil DNS. Les sections Authority et **Additional** sont consignées si la journalisation étendue est activée dans le profil DNS. Le format du journal diffère en fonction du type d'enregistrement. Pour plus d'informations, consultez la rubrique Présentation du format de journalisation des enregistrements.

  - ANS : section réponse
  - AUTH : autorité
  - ADD : section **supplémentaire**

- **OPT/<edns version>/UDP max payload size/DO:** format d'enregistrement OPT dans le journal DNS
- **OPT/<EDNS version>/<UDP payload size>/<"DO"ou vide selon que le bit OK DNSSEC est défini ou non>/<value of RDLEN>/ECS/<Q/R>/<option length>/<Family>/<Source Prefix-Length>/<Scope Prefix-Length>/<ECS Address>:**

  Si la requête ou la réponse DNS inclut l'option EDNS Client Subnet (ECS), elle est également consignée dans le format d'enregistrement OPT dans le fichier journal DNS.

Lorsqu'une requête DNS avec une option ECS incluant une adresse IPv4 ou IPv6 est envoyée, l'option ECS est consignée avec l'une des options suivantes :

- « ECS/Q » indiquant que les valeurs du journal proviennent de la requête
- « ECS/R » indiquant que les valeurs du journal proviennent de la réponse.

La valeur de Scope Prefix-Length est également définie de manière appropriée. Dans la requête DNS, elle est définie sur zéro, et pour la réponse, elle est définie sur la valeur calculée.

Le tableau suivant décrit les détails consignés dans différents scénarios :

Scénario	Option ECS définie dans la requête DNS	Option ECS définie dans la réponse DNS	Détails consignés
La journalisation des requêtes et la journalisation étendue sont toutes deux activées	Oui	Oui	L'option ECS est consignée avec la chaîne « ECS/R/ » et la longueur du préfixe de portée est définie sur la valeur calculée.
La journalisation des requêtes et la journalisation étendue sont toutes deux activées	Oui	Non	L'option ECS est consignée avec la chaîne « ECS/Q » et la longueur du préfixe de portée est définie sur zéro.
La journalisation des requêtes est activée, mais la journalisation étendue n'est pas activée	Oui	Oui	L'option ECS est consignée avec la chaîne « ECS/Q/ » et la longueur du préfixe de portée est définie sur zéro.
La journalisation des requêtes et la journalisation étendue ne sont pas activées	Oui	Oui	L'option ECS n'est pas consignée.

Scénario	Option ECS définie dans la requête DNS	Option ECS définie dans la réponse DNS	Détails consignés
La journalisation des requêtes est activée, mais la journalisation étendue n'est pas activée	Oui	Non	L'option ECS est consignée avec la chaîne « ECS/Q/ » et la longueur du préfixe de portée est définie sur zéro.
La journalisation des requêtes n'est pas activée, mais la journalisation étendue est activée	Oui	Oui	L'option ECS est consignée avec la chaîne « ECS/R/ » et la longueur du préfixe de portée est définie sur la valeur calculée.
La journalisation des requêtes n'est pas activée, mais la journalisation étendue est activée	Oui	Non	L'option ECS n'est pas consignée.

Comprendre le format de journalisation des enregistrements

Voici un exemple du format de journalisation des enregistrements dans un message Syslog :

```
1 <domainname>/<record type>/ <record ttl> / <resource record data>#<
     resource record data>#......##
2 <!--NeedCopy-->
```

Où :

Record Type	Exemple de format	Données et format des enregistrements de ressources
Enregistrement de l'adresse (A)	A/5/1.1.1.1#1.1.1.2#1.1.1.3##	Adresse IPv4
Record AAAA	AAAA/5/1::1#1::2#1::3##	adresse IPv6

Record Type	Exemple de format	Données et format des enregistrements de ressources
Record SOA	SOA/3600/ns1.dnslogging.test./ …3/3600/5##	Serveur Origin, contact et autres détails. Le format d'enregistrement des ressources est : <originServer>/<contact>/<serial number>/<refresh rate>/<retry>/<expire>/<minimum>##
Enregistrement NS	NS/5/ns1.dnslogging.test	Nom d'hôte du serveur de noms.
Record MX	#MX/5/10/host1.dnslogging.test	Préférence suivie du nom d'hôte du serveur d'échange de messagerie
Enregistrement CNAME	CNAME/5/host1.dnslogging.test.##	Nom canonique
Enregistrement SRV	SRV/5/1/2/3/host1.dnslogging.t …##	Format d'enregistrement des ressources : <priority>/<weight>/<port>/<target>#
Enregistrement TXT	TXT/5/dns+logging##	Les données comprennent tous les textes.
Enregistrement NAPTR	NAPTR/5/10/11////dnslogging#… ##	Format d'enregistrement des ressources : <order>/<preference>/<flags>/<services>/<re… expression>/<replacement string>#
Enregistrement DNSKEY	DNSKEY/5/1/3/5/AwEAAanP0K+i5ofv5SUd78L760EtjemPq2Cx6JZgiDBZhSON	Format d'enregistrement des ressources : <flags>/<protocol>/<algorithm>/<public key in base64 encoding>#
Enregistrement PTR	PTR/3600/test.com.#test4.com.	Nom de domaine

Limitations de la journalisation DNS

La journalisation DNS présente les limitations suivantes :

- Si la journalisation des réponses est activée, seuls les types d'enregistrement suivants sont con-

signés :

- Enregistrement de l'adresse (A)
- Record AAAA
- Record SOA
- Enregistrement NS
- Record MX
- Enregistrement CNAME
- Enregistrement SRV
- Enregistrement TXT
- Enregistrement NAPTR
- Enregistrement DNSKEY
- Enregistrement PTR

Pour tous les autres types d'enregistrement, seuls les paramètres L3/L4, l'en-tête DNS et la section Question sont consignés.

- Les enregistrements RRSIG ne sont pas consignés même si la journalisation des réponses est activée.
- Le DNS64 n'est pas pris en charge.
- Les demandes ou réponses de mise à jour proactive DNS sont consignées en fonction des paramètres du profil par défaut.
- Sur le serveur virtuel, si l'option sans session et la journalisation des réponses sont activées, les paramètres L3/L4, l'en-tête DNS et la section Question DNS sont consignés à la place de la réponse.
- La taille maximale du message Syslog est de 1 024 octets.
- Si vous avez défini un profil DNS pour une politique DNS avec le type d'action Rewrite Response, l'appliance NetScaler n'enregistre pas la requête ni les réponses manipulées. Pour consigner les informations requises, vous devez utiliser une action de message d'audit dans la stratégie DNS.
- Les transactions DNS dues au trafic de surveillance DNS ne sont pas consignées.

Configuration de la journalisation DNS

Voici un aperçu de la configuration de la journalisation DNS :

1. Créez une action Syslog et activez le DNS dans l'action.
2. Créez une stratégie Syslog et spécifiez l'action Syslog dans la stratégie.
3. Liez globalement la politique Syslog pour permettre la journalisation de tous les événements du système NetScaler. Vous pouvez également lier la stratégie Syslog à un serveur virtuel d'équilibrage de charge spécifique.

4. Créez un profil DNS et définissez l'un des types de journalisation suivants que vous souhaitez activer :
   - Journalisation des requêtes DNS
   - Journalisation de la section de réponses DNS
   - Journalisation étendue DNS
   - Journalisation des erreurs DNS
5. Configurez l'un des éléments suivants, en fonction de vos besoins :
   - Service DNS et serveur virtuel pour DNS
   - Service ADNS
   - NetScaler en tant que transitaire
   - NetScaler en tant que résolveur
6. Définissez le profil DNS créé sur l'une des entités DNS.

Configurer la journalisation DNS pour NetScaler configuré en tant que proxy DNS à l'aide de l'interface de ligne de commande

1. Ajoutez une action Syslog et activez le DNS dans l'action. À l'invite de commande, tapez :

```
add audit syslogAction <name> (<serverIP> | -lbVserverName <string
    >) [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat <
    dateFormat>] [-logFacility <logFacility>] [-tcp ( NONE | ALL )]
     [-acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME |
    LOCAL_TIME )] [-userDefinedAuditlog ( YES | NO )] [-
    appflowExport ( ENABLED |DISABLED )] [-lsn ( ENABLED | DISABLED
     )] [-alg ( ENABLED | DISABLED )] [-transport ( TCP | UDP )] [-
    tcpProfileName <string>] [-maxLogDataSizeToHold <
    positive_integer>] [-dns ( ENABLED | DISABLED)]
<!--NeedCopy-->
```

   Exemple :

```
add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
LOCAL_TIME -dns ENABLED
```

2. Créez une stratégie Syslog et spécifiez l'action Syslog créée dans la stratégie. À l'invite de commande, tapez :

```
add audit syslogPolicy <name> <rule> <action>
```

   Exemple :

```
add audit syslogPolicy syslogpol1 ns_true nssyslogact1
```

3. Liez la stratégie Syslog globalement. À l'invite de commande, tapez :


```
bind system global [<policyName> [-priority <positive_integer>]]
```

Exemple :

```
bind system global syslogpol1
```

4. Créez un profil DNS et activez l'un des types de journaux suivants que vous souhaitez configurer :
   - Journalisation des requêtes DNS
   - Journalisation de la section de réponses DNS
   - Journalisation étendue DNS
   - Journalisation des erreurs DNS

   À l'invite de commande, tapez :

   ```
   add dns profile <dnsProfileName> [-dnsQueryLogging ( ENABLED | DISABLED )] [-dnsAnswerSecLogging ( ENABLED | DISABLED )] [-dnsExtendedLogging (ENABLED | DISABLED )] [-dnsErrorLogging ( ENABLED | DISABLED )] [-cacheRecords ( ENABLED | DISABLED )] [-cacheNegativeResponses ( ENABLED | DISABLED )]
   ```

   Exemple :

   ```
   add dns profile dnsprofile1 -dnsQueryLogging ENABLED
   ```

5. Configurez le service de type DNS. À l'invite de commande, tapez :

   ```
   add service <name> <serverName> <serviceType> <port>
   ```

   Exemple :

   ```
   add service svc1 10.102.84.140 dns 53
   ```

6. Configurez un serveur virtuel d'équilibrage de charge de type DNS de type de service.

   ```
   add lb vserver <name> <serviceType> <ip> <port>
   ```

   Exemple :

   ```
   add lb vserver lb1 dns 100.100.100.10 53
   ```

7. Liez le service au serveur virtuel. À l'invite de commande, tapez :

   ```
   bind lb vserver <name> <serviceName>
   ```

   Exemple :

   ```
   bind lb vserver lb1 svc1
   ```

8. Définissez le profil DNS créé sur le serveur virtuel. À l'invite de commande, tapez :

   ```
   set lb vserver <name> [ - dnsProfileName <string>]
   ```

   Exemple :

   ```
   set lb vserver lb1 -dnsProfileName dnsprofile1
   ```


Exemple de configuration de journalisation DNS pour l'appliance NetScaler configurée en tant que proxy DNS

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel
CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -
    timeZone
LOCAL_TIME -dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
Done
> add service svc1 10.102.84.140 dns 53
Done
> bind lb vserver lb1 svc1
Done
<!--NeedCopy-->
```

Exemple de configuration de journalisation DNS pour l'appliance NetScaler configurée en tant qu'ADNS

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
    LOCAL_TIME
-dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
Done
> add service svc1 10.102.84.140 dns 53
Done
> bind lb vserver lb1 svc1
Done
<!--NeedCopy-->
```


Exemple de configuration de journalisation DNS pour l'appliance NetScaler configurée en tant que redirecteur

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
    LOCAL_TIME
-dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add dns nameserver 8.8.8.8  - dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```

Exemple de configuration de journalisation DNS pour une appliance NetScaler configurée en tant que résolveur

```
> add audit syslogAction nssyslogact1 10.102.151.136
-logLevel CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -
    logFacility LOCAL4
-timeZone LOCAL_TIME -dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> set dns parameter -recursion enABLED
Done
> add nameserver 1.1.1.100 -local dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```

Configurer la journalisation basée sur des stratégies pour DNS

La journalisation basée sur des stratégies vous permet de spécifier un format pour les messages de journal. Le contenu d'un message de journal est défini à l'aide d'une expression de stratégie avancée.

Lorsque l'action de message spécifiée dans la politique est exécutée, l'appliance NetScaler construit le message de journal à partir de l'expression et écrit le message dans le fichier journal. Vous pouvez configurer la solution matérielle-logicielle pour qu'elle se connecte uniquement lorsqu'une stratégie DNS particulière est évaluée à True.

> **Remarque**
>
> Si vous avez défini une politique DNS avec un profil DNS pour le côté demande, l'appliance NetScaler enregistre uniquement la requête.

Pour configurer la journalisation basée sur une stratégie pour une stratégie DNS, vous devez d'abord configurer une action de message d'audit. Pour plus d'informations sur la configuration d'une action de message d'audit, voir Configurer l'appliance NetScaler pour la journalisation des audits. Après avoir configuré l'action du message d'audit, spécifiez l'action du message dans une stratégie DNS.

Configurer la journalisation basée sur une stratégie pour une stratégie DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la journalisation basée sur une stratégie pour une stratégie DNS et vérifier la configuration :

```
1 - add dns action <actionName> <actionType> [-IPAddress <ip_addr|
    ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
    ...] [-TTL <secs>] [-dnsProfileName <string>]
2 - set dns policy <name> [<rule>] [-actionName <string>] [-logAction <
    string>]
3 - show dns policy [<name>]
4 <!--NeedCopy-->
```

Exemple 1 :

Dans un déploiement GSLB, si vous souhaitez répondre avec des adresses IP différentes aux demandes des clients provenant d'un sous-réseau particulier, au lieu de répondre avec des adresses IP utilisées à des fins générales (telles que les adresses IP des utilisateurs internes), vous pouvez configurer une stratégie DNS avec le type d'action comme vue DNS. Dans ce cas, vous pouvez configurer la journalisation DNS sur l'action DNS spécifiée afin de pouvoir consigner les réponses spécifiques.

```
1 > add dns profile dns_prof1 -dnsqueryLogging enABLED -
    dnsanswerSecLogging enABLED
2  Done
3 > add dns view dns_view1
4  Done
5 > add dns action dns_act1 viewName -view dns_view1  - dnsprofilename
    dns_prof1
6  Done
```



```
> add dns policy dns_pol1 "CLIENT.IP.SRC.APPLY_MASK(255.255.255.0).EQ
   (100.100.100.0)”
dns_act1
 Done
> bind dns global dns_pol1 100 -gotoPriorityExpression END -type
   REQ_DEFAULT
 Done
> bind gslb service site_1_svc -viewName dns_view1 123.1.1.1
 Done
> bind gslb service site_5_svc -view dns_view1 132.1.1.1
 Done
<!--NeedCopy-->
```

Remarque : Dans la configuration précédente, si vous recherchez le domaine configuré sur un serveur virtuel GSLB, par exemple, *sampletest.com*, tous les utilisateurs internes du sous-réseau 100.100.100.0/24 sont servis avec les adresses IP de la vue DNS et les réponses sont consignées. Les demandes des clients pour d'autres sous-réseaux ne sont pas consignées.

Exemple 2 :

Si vous souhaitez consigner uniquement les requêtes pour le domaine *exemple.com*, vous pouvez créer un profil DNS avec la journalisation des requêtes activée et définir le profil DNS sur une action DNS avec le type d'action
NOOP, puis créer une stratégie DNS et définir l'action DNS. Par exemple :

```
>add dns profile query_logging -dnsqueryLogging ENABLED
Done
>add dns action dns_act1 NOOP -dnsprofileName query_logging
Done
>add dns policy dns_pol1 DNS.REQ.QUESTION.DOMAIN.EQ("example.com")
   dns_act1
Done
<!--NeedCopy-->
```

Configurer l'action de journalisation pour la stratégie DNS afin d'enregistrer l'adresse IP du client

L'action de journalisation peut être utilisée pour consigner les adresses IP sources pour les requêtes DNS à l'aide de l'expression suivante et l'utiliser dans le cadre de l'action de journalisation dans la stratégie DNS.

```
> add audit messageaction log_act_custom INFORMATIONAL ""ClientIP:"
   CLIENT.IP.SRC" ECS IP:"+((DNS.REQ.OPT.ECS.IP).typecast_text_t ALT "
   NONE")"
```



```
Done
<!--NeedCopy-->
```

L'expression précédente capture à la fois l'adresse IP source telle que dans l'en-tête IP et l'adresse IP ECS à partir de l'option DNS ECS, et l'une ou l'autre d'entre elles peut être exclue si nécessaire.

Exemple de configuration de journalisation DNS pour une appliance NetScaler permettant d'enregistrer l'adresse IP du client

Si vous souhaitez échantillonner la journalisation des requêtes DNS, vous pouvez le faire à l'aide de l'expression suivante. Cela déconnectera une requête sur 10.

```
> add audit messageaction log_action_srcip_1of10 INFORMATIONAL ""
   OneOf10: Source IP : "+client.ip.src"
Done
> add responder policy logsrcip_1of10 "sys.random.mul(10).lt(1)" NOOP -
   logAction log_action_srcip_1of10
Done
<!--NeedCopy-->
```

Configuration des suffixes DNS

May 5, 2023

Vous pouvez configurer des suffixes DNS qui permettent à l'appliance NetScaler de compléter les noms de domaine non complets lors de la résolution des noms. Par exemple, lors de la résolution d'un nom de domaine abc non entièrement qualifié, si un suffixe DNS example.com est configuré, l'appliance ajoute le suffixe au nom de domaine. Ensuite, il résout le nom de domaine. Dans ce cas, cela résoudrait abc.example.com. Si les suffixes DNS ne sont pas configurés, l'appliance ajoute un point aux noms de domaine non entièrement qualifiés et résout le nom de domaine.

Création de suffixes DNS

Les suffixes DNS sont importants et ne sont valides que lorsque NetScaler est configuré en tant que résolveur final ou redirecteur. Vous pouvez spécifier un suffixe de 127 caractères maximum.

> **Remarques :**
>
> - L'ordre des suffixes DNS est important. L'appliance ADC essaie les suffixes configurés dans un ordre série et s'arrête lorsqu'elle obtient une réponse positive pour un suffixe.

> - Un seul nom de domaine est traité à la fois. Tous les suffixes disponibles sont ajoutés au nom de domaine jusqu'à ce qu'une réponse soit reçue.
>
> **Par exemple :** si le nom de domaine est `www` et que les suffixes sont `abc.com` et `abc`. L'appliance NetScaler essaie `www.abc.com` d'abord et si elle ne renvoie pas de réponse positive, elle essaie. `www.abc` Si `www.abc.com` la réponse est positive, l'appliance n'essaiera pas d'utiliser le suffixe suivant.
> - L'appliance utilise tous les suffixes dans l'ordre dans lequel ils sont ajoutés jusqu'à ce qu'elle reçoive une réponse positive.

Création de suffixes DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez les commandes suivantes pour créer un suffixe DNS et vérifier la configuration :

```
1 -  add dns suffix <dnsSuffix>
2 -  show dns suffix <dnsSuffix>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns suffix example.com
2  Done
3 > show dns suffix example.com
4 1)      Suffix: example.com
5 Done
6
7 <!--NeedCopy-->
```

Pour supprimer un suffixe DNS à l'aide de la ligne de commande NetScaler, à l'invite de commandes, tapez la `rm dns suffix` commande et le nom du suffixe DNS.

Création de suffixes DNS à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Suffixe DNS** et créez des suffixes DNS.

Requête DNS ANY

May 5, 2023

Une requête ANY est un type de requête DNS qui extrait tous les enregistrements disponibles pour un nom de domaine. La requête ANY doit être envoyée à un serveur de noms faisant autorité pour un

domaine.

Comportement en mode ADNS

En mode ADNS, l'appliance NetScaler renvoie les enregistrements contenus dans son cache local. S'il n'y a aucun enregistrement dans le cache, l'appliance renvoie la réponse NXDOMAIN (négative).

Si NetScaler peut correspondre aux enregistrements de délégation de domaine, il renvoie les enregistrements NS. Dans le cas contraire, il renvoie les enregistrements NS du domaine racine.

Comportement en mode proxy DNS

En mode proxy, l'appliance NetScaler vérifie son cache local. S'il n'y a aucun enregistrement dans le cache, l'appliance transmet la requête au serveur.

Comportement des domaines GSLB (Global Server Load Balancing)

Si un domaine GSLB est configuré sur l'appliance ADC et qu'une requête ANY est envoyée pour le domaine GSLB (site), l'appliance renvoie l'adresse IP du service GSLB. Il sélectionne ce service par le biais d'une décision d'équilibrage de charge. Si l'option de réponse IP multiple (MIR) est activée, les adresses IP de tous les services GSLB sont envoyées.

Pour que NetScaler renvoie ces enregistrements lorsqu'il répond à la requête ANY, tous les enregistrements correspondant à un domaine GSLB doivent être configurés sur NetScaler.

> **Remarque**
>
> Si les enregistrements d'un domaine sont distribués entre NetScaler et un serveur, seuls les enregistrements configurés sur NetScaler sont renvoyés.

NetScaler offre la possibilité de configurer les vues DNS et les politiques DNS. Ces vues et stratégies sont utilisées pour effectuer l'équilibrage global de la charge du serveur. Pour plus d'informations, voir Global Server Load Balancing.

Configurer la mise en cache négative des enregistrements DNS

May 5, 2023

L'appliance NetScaler prend en charge la mise en cache des réponses négatives pour un domaine. Une réponse négative indique que les informations concernant un domaine demandé n'existent pas

ou que le serveur ne peut pas fournir de réponse à la requête. Le stockage de ces informations est appelé mise en cache négative. La mise en cache négative permet d'accélérer les réponses aux requêtes concernant un domaine.

> **Remarque :**
>
> La mise en cache négative n'est prise en charge que lorsque le serveur principal est configuré en tant que serveur DNS (ADNS) faisant autorité pour le domaine interrogé.

Une réponse négative peut être l'une des suivantes :

- Message d'erreur NXDOMAIN — Les serveurs DNS faisant autorité répondent par le message d'erreur NXDOMAIN lorsque aucun enregistrement n'est configuré sur le serveur pour le nom de domaine demandé. Ce message implique que le domaine demandé est un nom de domaine non valide ou inexistant.
- Message d'erreur NODATA : si le nom de domaine indiqué dans la requête est valide mais que les enregistrements du type indiqué ne sont pas disponibles, l'appliance envoie un message d'erreur NODATA.

Lorsque la mise en cache négative est activée, l'appliance met en cache la réponse négative du serveur DNS et traite les demandes futures uniquement à partir du cache. Cette action permet d'accélérer les réponses aux requêtes et de réduire le trafic DNS principal. La mise en cache négative peut être utilisée dans tous les déploiements, c'est-à-dire lorsqu'une appliance NetScaler fait office de proxy, de résolveur final ou de redirecteur.

Vous pouvez activer ou désactiver la mise en cache négative à l'aide d'un profil DNS. Pour plus d'informations, voir Profils DNS. Par défaut, la mise en cache négative est activée dans le profil DNS par défaut (**default**-dns-profile) qui sont liés par défaut à un serveur virtuel DNS ou dans le profil DNS nouvellement créé.

Activer ou désactiver la mise en cache négative à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver la mise en cache négative et vérifier la configuration :

```
1 -  add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED
     )] [-cacheNegativeResponses (ENABLED | DISABLED )]
2 -  show dns profile [<dnsProfileName>]
3 <!--NeedCopy-->
```

Exemple de profil DNS par défaut :

```
1 > sh dns profile default-dns-profile
2     1)   default-dns-profile
```



```
3          Query logging : DISABLED        Answer section logging :
               DISABLED
4          Extended logging : DISABLED     Error logging : DISABLED
5          Cache Records : ENABLED     Cache Negative Responses: ENABLED
6  Done
7  <!--NeedCopy-->
```

Exemple de profil DNS récemment créé :

```
1  > add dnsprofile dns_profile1 -cacheRecords ENABLED -
       cacheNegativeResponses ENABLED
2  Done
3  > show dns profile dns_profile1
4      1)   dns_profile1
5          Query logging : DISABLED        Answer section logging :
               DISABLED
6          Extended logging : DISABLED     Error logging : DISABLED
7          Cache Records : ENABLED     Cache Negative Responses: ENABLED
8  Done
9  <!--NeedCopy-->
```

Spécifiez les paramètres DNS au niveau du service ou du serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, effectuez les opérations suivantes :

1. Configurez le profil DNS.

   ```
   add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED )]
    [-cacheNegativeResponses (ENABLED | DISABLED )]
   ```

2. Liez le profil DNS au service ou au serveur virtuel.

   Pour lier le profil DNS au service :

   ```
   set service <name> [-dnsProfileName <string>]
   ```

Exemple :

```
1  >set service service1 -dnsProfileName dns_profile1
2  Done
3  <!--NeedCopy-->
```

Pour lier le profil DNS au serveur virtuel :

```
set lb vserver <name> [-dnsProfileName <string>]
```

Exemple :


```
>set lb vserver lbvserver1 -dnsProfileName dns_profile1
Done
<!--NeedCopy-->
```

Spécifiez les paramètres DNS au niveau du service ou du serveur virtuel à l'aide de l'interface graphique

1. Configurez le profil HTTP.

   Accédez à **Système** > **Profils**> **Profil DNS**, puis créez le profil DNS.

2. Liez le profil HTTP au service ou au serveur virtuel.

   Accédez à **Gestion du trafic** > **Équilibrage de charge**> **Services/Serveurs virtuels**, puis créez le profil DNS qui doit être lié au service ou au serveur virtuel.

Limitation du débit : réponse négative fournie par l'appliance

Vous pouvez définir un seuil pour les réponses négatives envoyées par l'appliance NetScaler à partir du cache. Lorsque le seuil est défini, l'appliance transmet la réponse depuis le cache jusqu'à ce que le seuil soit atteint. Une fois le seuil atteint, l'appliance abandonne les demandes au lieu de répondre par une réponse NXDOMAIN.

La définition d'une limite de taux pour les réponses négatives présente les avantages suivants.

- Enregistrez les ressources sur l'appliance NetScaler.
- Empêchez toute requête malveillante concernant des noms de domaine inexistants.

> **Remarque :** Vous pouvez définir un seuil pour les réponses négatives uniquement pour les domaines pour lesquels l'appliance ADC est configurée en tant que serveur de noms de domaine faisant autorité. Vous ne pouvez pas définir de seuil pour les enregistrements mis en cache provenant des serveurs de noms principaux faisant autorité.

Limitation du débit de réponses négatives fournies par le cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez

```
set dns parameter -NXDOMainRateLimitThreshold <positive-integer>
<!--NeedCopy-->
```

Exemple :


```
set dns parameter -NXDOMainRateLimitThreshold 1000
<!--NeedCopy-->
```

NxDomainRateLimitThreshold : lorsque ce paramètre est défini sur une valeur entière positive, les réponses sont servies depuis le cache jusqu'à ce que ce seuil (en secondes) soit atteint. Une fois le seuil dépassé, les demandes sont abandonnées. Le seuil configuré est par moteur de paquets.

Limitation du débit de réponses négatives fournies par le cache à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS** et cliquez sur **Modifier les paramètres DNS**.
2. Sur la page **Configurer les paramètres DNS**, dans le champ **NXDOMAIN Rate Limit Threshold**, entrez la valeur seuil jusqu'à laquelle les réponses doivent être transmises depuis le cache.

Remarque : La valeur du **seuil de NXDOMAIN Croisé** affiche le nombre de fois où les demandes sont supprimées une fois le seuil atteint.

Mettre en cache les données du sous-réseau du client EDNS0 lorsque l'appliance NetScaler est en mode proxy

May 5, 2023

En mode Proxy NetScaler, si un serveur principal prenant en charge un sous-réseau client EDNS0 (ECS) envoie une réponse contenant l'option ECS, l'appliance NetScaler effectue les opérations suivantes :

- Il transmet la réponse telle quelle au client et
- Stocke la réponse dans le cache, ainsi que les informations du sous-réseau client.

Les requêtes DNS qui proviennent du même sous-réseau du même domaine et pour lesquelles le serveur enverrait la même réponse sont ensuite traitées à partir du cache.

Remarque :

- La mise en cache ECS est désactivée par défaut. Activez la mise en cache des données du sous-réseau client EDNS0 dans le profil DNS associé.
- Le nombre de sous-réseaux que vous pouvez mettre en cache pour un domaine est limité aux ID de sous-réseau disponibles, c'est-à-dire 1 270 dans l'appliance NetScaler. Vous pouvez éventuellement définir la limite sur un nombre inférieur (valeur minimale : 1 ipv4/ipv6).

Activer la mise en cache des réponses ECS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

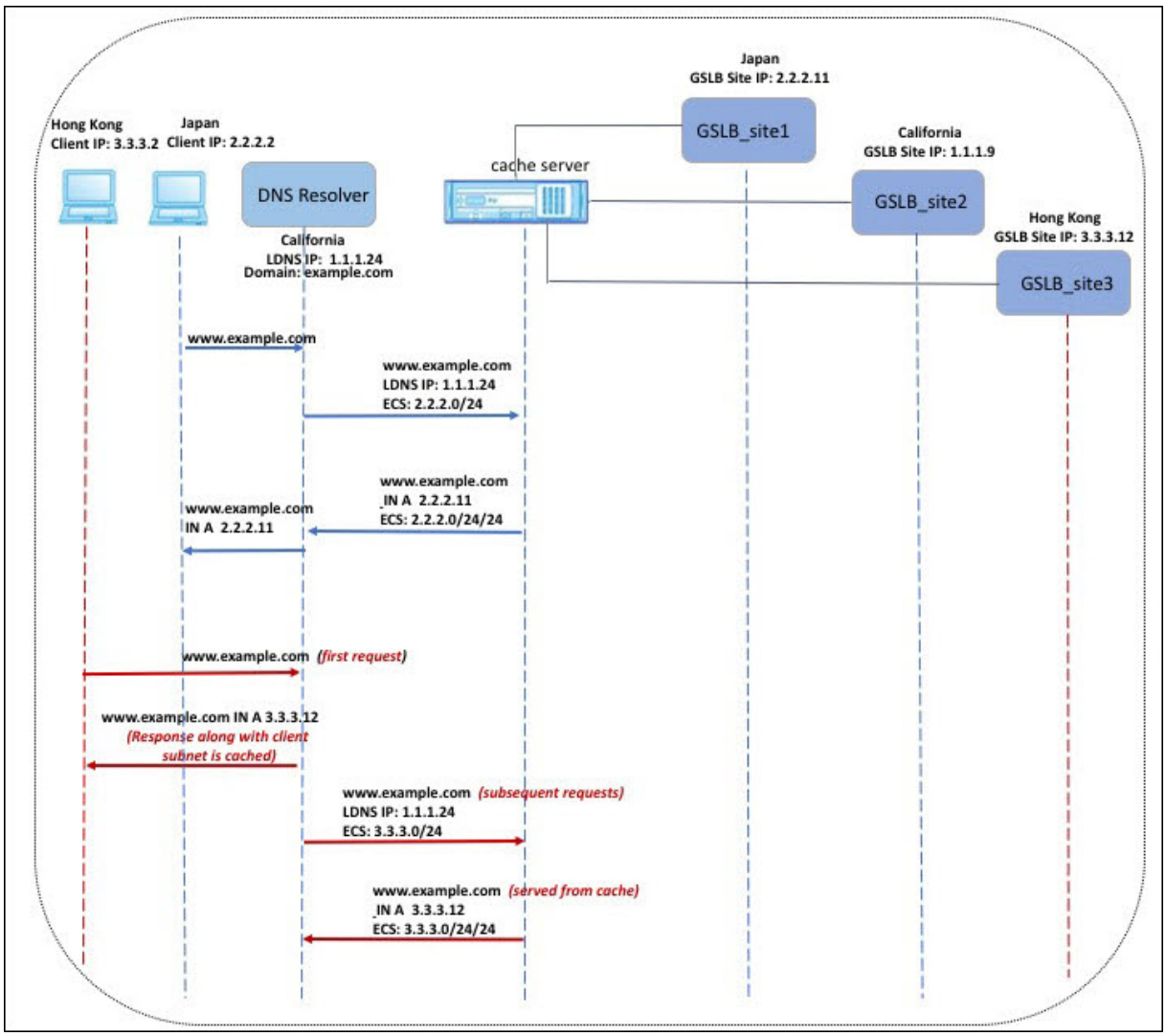

```
set dns profile <dnsProfileName> -cacheECSSubnet ( ENABLED | DISABLED )
```

Limitez le nombre de sous-réseaux pouvant être mis en cache par domaine à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set dns profile <dnsProfileName> -maxSubnetsPerDomain <positive_integer>
```

Exemple :



Dans l'exemple illustré dans la figure précédente, le client à l'adresse IP 2.2.2.2 envoie une requête pour www.example.com au résolveur DNS. Le résolveur DNS envoie la réponse suivante :

www.example.com DANS A, L'IP est 2.2.2.11, et ECS 2.2.2.0/24/24

À ce stade, la réponse et l'identifiant du sous-réseau client (2.2.2.0/24) sont mis en cache. D'autres demandes provenant du même sous-réseau et du même domaine sont traitées à partir du cache.

Par exemple, si l'adresse IP du client est 2.2.2.100 et que la requête concerne www.example.com, la requête est diffusée depuis le cache au lieu d'être envoyée au serveur principal.

extensions de sécurité du système de noms de domaine

May 5, 2023

Les extensions de sécurité DNS (DNSSEC) sont une norme de l'Internet Engineering Task Force (IETF). Il vise à garantir l'intégrité des données et l'authentification de l'origine des données dans les communications entre les serveurs de noms et les clients tout en transmettant les réponses UDP en texte clair. Le DNSSEC spécifie un mécanisme qui utilise la cryptographie à clé asymétrique et un ensemble de nouveaux enregistrements de ressources spécifiques à sa mise en œuvre.

La spécification DNSSEC est décrite dans :

- RFC 4033, « Introduction et exigences relatives à la sécurité du DNS »
- RFC 4034, « Enregistrements de ressources pour les extensions de sécurité DNS »
- RFC 4035, « Modifications du protocole pour les extensions de sécurité DNS »

Les aspects opérationnels de la mise en œuvre du DNSSEC dans le DNS sont abordés dans la RFC 4641, « Pratiques opérationnelles du DNSSEC ».

Vous pouvez configurer DNSSEC sur NetScaler. Vous pouvez générer et importer des clés pour signer des zones DNS. Vous pouvez configurer DNSSEC pour les zones pour lesquelles NetScaler fait autorité. Vous pouvez configurer l'ADC en tant que serveur proxy DNS pour les zones signées hébergées sur une batterie de serveurs de noms principaux. Si ADC fait autorité pour un sous-ensemble d'enregistrements appartenant à une zone pour laquelle ADC est configuré en tant que serveur proxy DNS, vous pouvez inclure le sous-ensemble d'enregistrements dans l'implémentation DNSSEC.

Configurer DNSSEC

May 5, 2023

Procédez comme suit pour configurer DNSSEC :

1. Activez DNSSEC sur l'appliance NetScaler.
2. Créez une clé de signature de zone et une clé de signature pour la zone.
3. Ajoutez les deux clés à la zone.
4. Signer la zone avec les clés.

L'appliance NetScaler n'agit pas en tant que résolveur DNSSEC. Le protocole DNSSEC sur l'ADC n'est pris en charge que dans les scénarios de déploiement suivants :

1. ADNS : NetScaler est l'ADNS et génère lui-même les signatures.
2. Proxy : NetScaler agit en tant que proxy DNSSEC. On suppose que le NetScaler est placé devant les serveurs ADNS/LDNS en mode sécurisé. L'ADC agit uniquement en tant qu'entité de mise en cache par proxy et ne valide aucune signature.

Activer et désactiver DNSSEC

Activez DNSSEC sur NetScaler pour que l'ADC réponde aux clients compatibles DNSSEC. Par défaut, DNSSEC est activé.

Vous pouvez désactiver la fonctionnalité DNSSEC si vous ne souhaitez pas que NetScaler réponde aux clients avec des informations spécifiques au DNSSEC.

Activer ou désactiver DNSSEC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver DNSSEC et vérifier la configuration :

```
-  set dns parameter -dnssec ( ENABLED | DISABLED )
-  show dns parameter
<!--NeedCopy-->
```

Exemple :

```
> set dns parameter -dnssec ENABLED
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
         .
         .
         .
         DNSEC Extension: ENABLED
        Max DNS Pipeline Requests: 255
 Done

<!--NeedCopy-->
```

Activer ou désactiver DNSSEC à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans le volet d'informations, cliquez sur Modifier les paramètres DNS.

3. Dans la boîte de dialogue **Configurer les paramètres DNS**, cochez ou décochez la case **Activer l'extension DNSSEC** .

Création de clés DNS pour une zone

Pour chaque zone DNS que vous souhaitez signer, vous devez créer deux paires de clés asymétriques. Une paire, appelée clé de signature de zone (ZSK), est utilisée pour signer tous les ensembles d'enregistrements de ressources de la zone. La seconde paire est appelée clé de signature (KSK) et est utilisée pour signer uniquement les enregistrements de ressources DNSKEY de la zone.

Lorsque le ZSK et le KSK sont créés, le `suffix.key` est ajouté aux noms des composants publics des clés. Le `suffix.private` est ajouté aux noms de leurs composants privés. L'ajout se fait automatiquement.

NetScaler crée également un enregistrement de délégation de signature (DS) et ajoute le suffixe .ds au nom de l'enregistrement. Si la zone parent est une zone signée, vous devez publier l'enregistrement DS dans la zone parent pour établir la chaîne de confiance.

Lorsque vous créez une clé, celle-ci est stockée dans le `/nsconfig/dns/` répertoire, mais elle n'est pas automatiquement publiée dans la zone. Après avoir créé une clé à l'aide de la `create dns key` commande, vous devez publier la clé de manière explicite dans la zone à l'aide de la `add dns key` commande. Le processus de génération d'une clé est distinct du processus de publication de la clé dans une zone afin de vous permettre d'utiliser d'autres moyens pour générer des clés. Par exemple, vous pouvez importer des clés générées par d'autres programmes de génération de clés (tels que `bind -keygen`) à l'aide de Secure FTP (SFTP), puis publier les clés dans la zone. Pour plus d'informations sur la publication d'une clé dans une zone, voir Publier une clé DNS dans une zone.

Effectuez les étapes décrites dans cette rubrique pour créer une clé de signature de zone, puis répétez les étapes pour créer une clé de signature de clé. L'exemple qui suit la syntaxe de commande crée d'abord une paire de clés de signature de zone pour la zone example.com. L'exemple utilise ensuite la commande pour créer une paire de clés de signature pour la zone.

À partir de la version 13.0 build 61.x, l'appliance NetScaler prend désormais en charge des algorithmes de chiffrement plus puissants, tels que RSASHA256 et RSASHA512, pour authentifier une zone DNS. Auparavant, seul l'algorithme RSASHA1 était pris en charge.

Création d'une clé DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

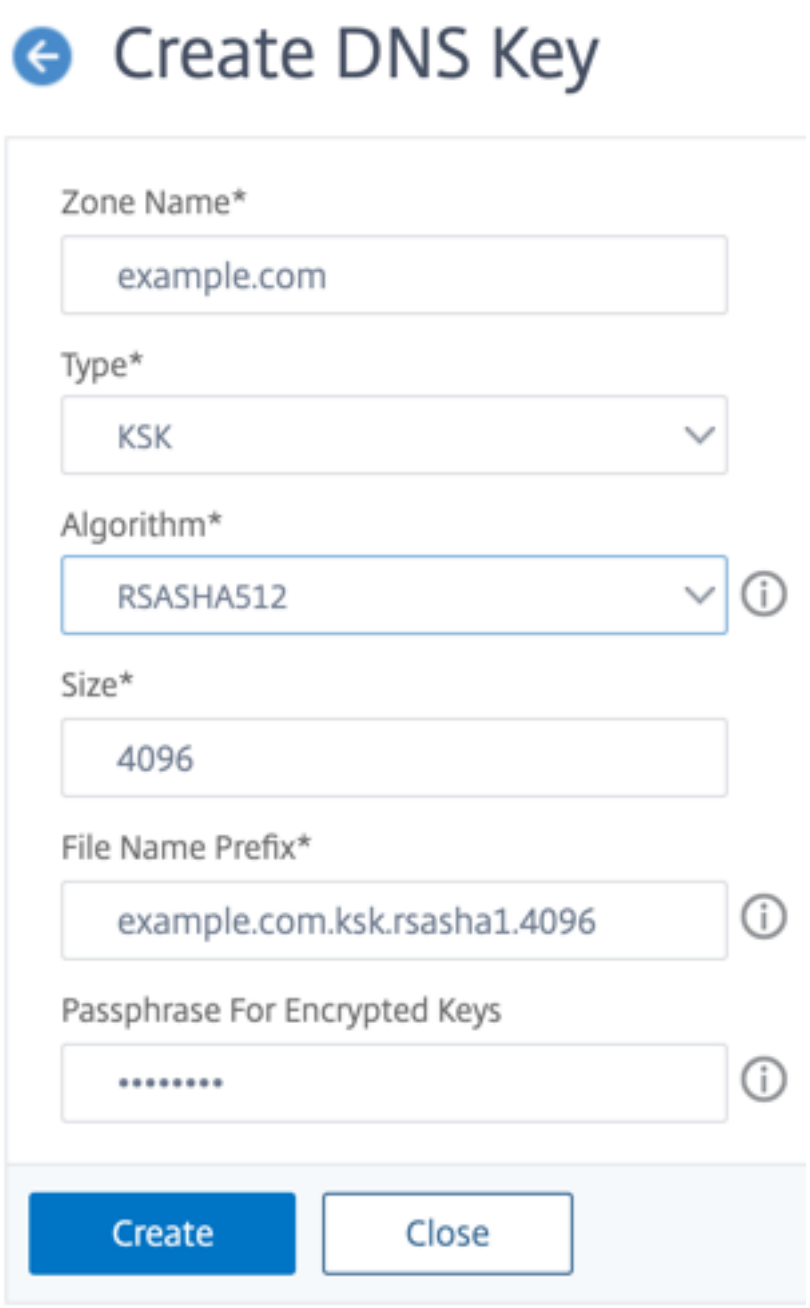
```
create dns key -zoneName <string> -keyType <keyType> -algorithm <algorithm>
 -keySize <positive_integer> -fileNamePrefix <string>
```

Exemple :


```
> create dns key -zoneName example.com -keyType zsk -algorithm
   RSASHA256 -keySize 1024 -fileNamePrefix example.com.zsk.rsasha1.1024
File Name: /nsconfig/dns/example.com.zsk.rsasha1.1024.key (public); /
   nsconfig/dns/example.com.zsk.rsasha1.1024.private (private); /
   nsconfig/dns/example.com.zsk.rsasha1.1024.ds (ds)
This operation may take some time, Please wait...
 Done
> create dns key -zoneName example.com -keyType ksk -algorithm
   RSASHA512 -keySize 4096 -fileNamePrefix example.com.ksk.rsasha1.4096
File Name: /nsconfig/dns/example.com.ksk.rsasha1.4096.key (public); /
   nsconfig/dns/example.com.ksk.rsasha1.4096.private (private); /
   nsconfig/dns/example.com.ksk.rsasha1.4096.ds (ds)
This operation may take some time, Please wait...
 Done
<!--NeedCopy-->
```

Création d'une clé DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS**.
2. Dans la zone de détails, cliquez sur **Créer une clé DNS**.
3. Entrez les valeurs des différents paramètres et cliquez sur **Créer**.



Remarque : Pour modifier le préfixe du nom de fichier d'une clé existante :

- Cliquez sur la flèche à côté du bouton **Parcourir** .
- Cliquez sur **Local** ou sur **Appliance** (selon que la clé existante est stockée sur votre ordinateur local ou dans le `/nsconfig/dns/` répertoire de l'appliance)
- Naviguez jusqu'à l'emplacement de la clé, puis double-cliquez sur la touche.
  La zone **Préfixe du nom de fichier** est remplie uniquement avec le préfixe de la clé existante. Modifiez le préfixe en conséquence.

Publier une clé DNS dans une zone

Une clé (clé de signature de zone ou clé de signature par clé) est publiée dans une zone en ajoutant la clé à l'appliance ADC. Une clé doit être publiée dans une zone avant de signer la zone.

Avant de publier une clé dans une zone, celle-ci doit être disponible dans le répertoire **/nsconfig/dns/** . Si vous avez créé la clé DNS sur un autre ordinateur (par exemple, à l'aide du `bind-keygen` programme), assurez-vous que la clé est ajoutée au `/nsconfig/dns/` répertoire. Publiez ensuite la clé dans la zone. Utilisez l'interface graphique ADC pour ajouter la clé au `/nsconfig/dns/` répertoire. Vous pouvez également utiliser un autre programme pour importer la clé dans le répertoire, tel que le FTP sécurisé (SFTP).

Utilisez la `add dns key` commande pour chaque paire de clés publique-privée que vous souhaitez publier dans une zone donnée. Si vous avez créé une paire ZSK et une paire KSK pour une zone, utilisez la `add dns key` commande pour publier d'abord l'une des paires de clés de la zone. Répétez la commande pour publier l'autre paire de clés. Pour chaque clé que vous publiez dans une zone, un enregistrement de ressource DNSKEY est créé dans la zone.

L'exemple qui suit la syntaxe de commande publie d'abord la paire de clés de signature de zone (qui a été créée pour la zone example.com) dans la zone. L'exemple utilise ensuite la commande pour publier la paire de clés de signature dans la zone.

Publier une clé dans une zone à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour publier une clé dans une zone et vérifier la configuration :

```
1 -  add dns key <keyName> <publickey> <privatekey> [-expires <
    positive_integer> [<units>]] [-notificationPeriod <positive_integer>
     [<units>]] [-TTL <secs>]
2 -  show dns zone [<zoneName> | -type <type>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > add dns key example.com.zsk example.com.zsk.rsasha1.1024.key example.
    com.zsk.rsasha1.1024.private
2  Done
3 > add dns key example.com.ksk example.com.ksk.rsasha1.4096.key example.
    com.ksk.rsasha1.4096.private
4  Done
5 > show dns zone example.com
6          Zone Name : example.com
7          Proxy Mode : NO
8          Domain Name : example.com
```



```
                    Record Types : NS SOA DNSKEY
            Domain Name : ns1.example.com
                    Record Types : A
            Domain Name : ns2.example.com
                    Record Types : A
 Done
<!--NeedCopy-->
```

Publier une clé dans une zone DNS à l'aide de l'interface graphique

Accédez à **Gestion du trafic > DNS > Clés**.

Remarque : Pour la clé publique et la clé privée, pour ajouter une clé stockée sur votre ordinateur local, cliquez sur la flèche à côté du bouton **Parcourir**, cliquez sur **Local**, accédez à l'emplacement de la clé, puis double-cliquez sur la clé.

Configuration d'une clé DNS

Vous pouvez configurer les paramètres d'une clé qui a été publiée dans une zone. Vous pouvez modifier la période d'expiration, la période de notification et les paramètres de durée de vie (TTL) de la clé. Si vous modifiez la période d'expiration d'une clé, l'appliance signe automatiquement à nouveau tous les enregistrements de ressources de la zone contenant la clé. La nouvelle signature se produit si la zone est signée avec la clé en question.

Configurer une clé à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer une clé et vérifier la configuration :

```
-  set dns key <keyName> [-expires <positive_integer> [<units>]] [-
   notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]
-  show dns key [<keyName>]
<!--NeedCopy-->
```

Exemple :

```
> set dns key example.com.ksk -expires 30 DAYS -notificationPeriod 3
   DAYS -TTL 3600
 Done
> show dns key example.com.ksk
1)      Key Name: example.com.ksk
        Expires: 30 DAYS        Notification: 3 DAYS    TTL: 3600
        Public Key File: example.com.ksk.rsasha1.4096.key
```



```
        Private Key File: example.com.ksk.rsasha1.4096.private
 Done
<!--NeedCopy-->
```

Configuration d'une clé à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Clés**.
2. Dans le volet de détails, cliquez sur la touche que vous souhaitez configurer, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer la clé DNS, modifiez les valeurs des paramètres suivants comme indiqué :
   - Expire : expire
   - Période de notification — notificationPeriod
   - TTL — TTL
4. Cliquez sur OK.

Signer et annuler la signature d'une zone DNS

Pour sécuriser une zone DNS, vous devez signer la zone avec les clés qui y ont été publiées. Lorsque vous signez une zone, NetScaler crée un enregistrement de ressource Next Secure (NSEC) pour chaque nom de propriétaire. Il utilise ensuite la clé de signature pour signer le jeu d'enregistrements de ressources DNSKEY. Enfin, il utilise le ZSK pour signer tous les jeux d'enregistrements de ressources de la zone, y compris les jeux d'enregistrements de ressources DNSKEY et les jeux d'enregistrements de ressources NSEC. Chaque opération de signature génère une signature pour les ensembles d'enregistrements de ressources de la zone. La signature est capturée dans un nouvel enregistrement de ressource appelé enregistrement de ressource RRSIG.

Après avoir signé une zone, enregistrez la configuration.

Signer une zone à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour signer une zone et vérifier la configuration :

```
-  sign dns zone <zoneName> [-keyName <string> ...]
-  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
-  save config
<!--NeedCopy-->
```

Exemple :


```
> sign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
         Zone Name : example.com
         Proxy Mode : NO
         Domain Name : example.com
                 Record Types : NS SOA DNSKEY RRSIG NSEC
         Domain Name : ns1.example.com
                 Record Types : A RRSIG NSEC
         Domain Name : ns2.example.com
                 Record Types : A RRSIG
         Domain Name : ns2.example.com
                 Record Types : RRSIG NSEC
Done
> save config
 Done
<!--NeedCopy-->
```

Annuler la signature d'une zone à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour annuler la signature d'une zone et vérifier la configuration :

```
-  unsign dns zone <zoneName> [-keyName <string> ...]
-  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
<!--NeedCopy-->
```

Exemple :

```
> unsign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
         Zone Name : example.com
         Proxy Mode : NO
         Domain Name : example.com
                 Record Types : NS SOA DNSKEY
         Domain Name : ns1.example.com
                 Record Types : A
         Domain Name : ns2.example.com
                 Record Types : A
 Done
<!--NeedCopy-->
```


Signer ou annuler la signature d'une zone à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Zones**.
2. Dans le volet d'informations, cliquez sur la zone que vous souhaitez signer, puis cliquez sur Signer/Annuler la signature.
3. Dans la boîte de dialogue Sign/Unsign DNS Zone, effectuez l'une des opérations suivantes :
   - Pour signer la zone, cochez les cases correspondant aux clés (clé de signature de zone et clé de signature de clé) avec lesquelles vous souhaitez signer la zone.
     Vous pouvez signer la zone à l'aide de plusieurs clés de signature de zone ou de plusieurs paires de clés de signature de zone.
   - Pour annuler la signature de la zone, décochez les cases correspondant aux clés (clé de signature de zone et clé de signature de clé) avec lesquelles vous souhaitez annuler la signature de la zone.
     Vous pouvez annuler la signature de la zone à l'aide de plusieurs clés de signature de zone ou de plusieurs paires de clés de signature de zone.
4. Cliquez sur OK.

Afficher les enregistrements NSEC pour un enregistrement donné dans une zone

Vous pouvez consulter les enregistrements NSEC que NetScaler crée automatiquement pour chaque nom de propriétaire de la zone.

Afficher l'enregistrement NSEC pour un enregistrement donné dans une zone à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour afficher l'enregistrement NSEC pour un enregistrement donné dans une zone :

```
show dns nsecRec [<hostName> | -type (ADNS | PROXY | ALL)]
```

Exemple :

```
1 > show dns nsecRec example.com
2 1)      Domain Name : example.com
3         Next Nsec Name: ns1.example.com
4         Record Types : NS SOA DNSKEY RRSIG NSEC
5  Done
6 <!--NeedCopy-->
```

Afficher l'enregistrement NSEC pour un enregistrement donné dans une zone à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Enregistrements > Enregistrements sécurisés suivants**.

2. Dans le volet de détails, cliquez sur le nom de l'enregistrement pour lequel vous souhaitez consulter l'enregistrement NSEC. L'enregistrement NSEC correspondant à l'enregistrement que vous sélectionnez s'affiche dans la zone Détails.

Supprimer une clé DNS

Supprimez une clé de la zone dans laquelle elle est publiée lorsqu'elle a expiré ou si elle a été compromise. Lorsque vous supprimez une clé de la zone, la zone est automatiquement désignée avec la clé. La suppression de la clé à l'aide de cette commande ne supprime pas les fichiers clés présents dans le répertoire /nsconfig/dns/. Si les fichiers clés ne sont plus nécessaires, ils doivent être explicitement supprimés du répertoire.

Supprimer une clé de NetScaler à l'aide de la CLI

À l'invite de commandes, tapez la commande suivante pour supprimer une clé et vérifier la configuration :

```
1 -  rm dns key <keyName>
2 -  show dns key <keyName>
3 <!--NeedCopy-->
```

Exemple :

```
1 > rm dns key example.com.zsk
2  Done
3 > show dns key example.com.zsk
4 ERROR: No such resource [keyName, example.com.zsk]
5
6 <!--NeedCopy-->
```

Supprimer une clé de NetScaler à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Clés**.
2. Dans le volet de détails, cliquez sur le nom de la clé que vous souhaitez supprimer de l'ADC, puis cliquez sur Supprimer.

Configurer DNSSEC lorsque NetScaler fait autorité pour une zone

May 5, 2023

Lorsque NetScaler fait autorité pour une zone donnée, tous les enregistrements de ressources de la zone sont configurés sur l'ADC. Pour signer la zone faisant autorité, vous devez créer la signature de zone et les clés de signature pour la zone, ajouter les clés à l'ADC, puis signer la zone. Pour plus d'informations, consultez :

- Création de clés DNS pour une zone
- Publier une clé DNS dans une zone
- Signez et désignez une zone DNS.

Si des domaines GSLB configurés sur ADC appartiennent à la zone en cours de signature, les noms de domaine GSLB sont signés avec les autres enregistrements qui appartiennent à la zone.

Une fois que vous avez signé une zone, les réponses aux demandes des clients compatibles DNSSEC incluent les enregistrements de ressources RRSIG ainsi que les enregistrements de ressources demandés. Le DNSSEC doit être activé sur ADC. Pour plus d'informations sur l'activation de DNSSEC, voir Activer et désactiver DNSSEC.

Enfin, après avoir configuré DNSSEC pour la zone officielle, vous devez enregistrer la configuration de NetScaler.

Configurer DNSSEC pour une zone pour laquelle NetScaler est un serveur proxy DNS

May 5, 2023

La procédure de signature d'une zone pour laquelle NetScaler est configuré en tant que serveur proxy DNS dépend du fait que l'ADC possède ou non un sous-ensemble des informations de zone détenues par les serveurs de noms principaux. Si tel est le cas, la configuration est considérée comme une configuration de propriété partielle de la zone. Si l'ADC ne possède aucun sous-ensemble des informations de zone, la configuration NetScaler pour la gestion des serveurs principaux est considérée comme une configuration de serveur proxy DNS sans zone. Les tâches de configuration DNSSEC de base pour les deux configurations NetScaler sont les mêmes. Toutefois, la signature de la zone partielle sur NetScaler nécessite quelques étapes de configuration supplémentaires.

Remarque : Les termes configuration de serveur proxy sans zone et zone partielle sont utilisés uniquement dans le contexte de l'appliance NetScaler.

Important : lorsqu'il est configuré en mode proxy, l'ADC ne vérifie pas la signature des réponses DNSSEC avant de mettre à jour le cache.

Si vous configurez l'ADC en tant que proxy DNS pour équilibrer la charge des résolveurs (serveurs) compatibles DNSSEC, vous devez définir l'option Récursion disponible lors de la configuration du serveur

virtuel DNS. Si une requête DNSSEC arrive avec le bit Checking Disabled (CD) défini, la requête est transmise au serveur avec le bit CD conservé. La réponse du serveur n'est pas mise en cache.

Configurer DNSSEC pour une configuration de serveur proxy DNS sans zone

Pour une configuration de serveur proxy DNS sans zone, la signature de zone doit être effectuée sur les serveurs de noms principaux. Sur NetScaler, vous configurez l'ADC en tant que serveur proxy DNS pour la zone. Créez un serveur virtuel d'équilibrage de charge de type de protocole DNS. Configurez les services sur l'ADC pour représenter les serveurs de noms. Ensuite, liez les services au serveur virtuel d'équilibrage de charge. Pour plus d'informations sur ces tâches de configuration, voir Configurer NetScaler en tant que serveur proxy DNS.

Lorsqu'un client envoie à ADC une demande DNS avec le bit OK (DO) DNSSEC défini, ADC vérifie son cache pour les informations demandées. Si les enregistrements de ressources ne sont pas disponibles dans son cache, l'ADC transmet la demande à l'un des serveurs de noms DNS. Il transmet ensuite la réponse du serveur de noms au client. L'ADC met également en cache les enregistrements de ressources RRSIG ainsi que la réponse du serveur de noms. Les demandes suivantes émanant de clients compatibles DNSSEC sont traitées à partir du cache (y compris les enregistrements de ressources RRSIG), en fonction du paramètre de durée de vie (TTL). Si un client envoie une requête DNS sans définir le bit DO, l'ADC répond avec uniquement les enregistrements de ressources demandés. Il n'inclut pas les enregistrements de ressources RRSIG spécifiques à DNSSEC.

Configurer DNSSEC pour une configuration de propriété partielle de la zone

Dans certaines configurations ADC, même si l'autorité d'une zone appartient aux serveurs de noms principaux, un sous-ensemble des enregistrements de ressources appartenant à la zone peut être configuré sur l'ADC. L'ADC possède (ou fait autorité pour) uniquement ce sous-ensemble d'enregistrements. Un tel sous-ensemble d'enregistrements peut être considéré comme constituant une *zone partielle* sur l'ADC. L'ADC est propriétaire de la zone partielle. Tous les autres enregistrements appartiennent aux serveurs de noms principaux.

Une configuration de zone partielle typique sur NetScaler s'affiche lorsque :

- Les domaines GSLB (Global Server Load Balancing) sont configurés sur l'ADC
- Les domaines GSLB font partie d'une zone pour laquelle les serveurs de noms principaux font autorité.

La signature d'une zone qui inclut uniquement une zone partielle sur l'ADC implique :

- Inclusion des informations de zone partielles dans les fichiers de zone du serveur de noms principal
- Signature de la zone sur les serveurs de noms principaux
- Signature de la zone partielle sur l'ADC.

Le même jeu de clés doit être utilisé pour signer la zone sur les serveurs de noms et la zone partielle sur l'ADC.

Signez la zone sur les serveurs de noms principaux

1. Incluez les enregistrements de ressources contenus dans la zone partielle, dans les fichiers de zone des serveurs de noms.
2. Créez des clés et utilisez-les pour signer la zone sur les serveurs de noms principaux.

Signez la zone partielle sur NetScaler

1. Créez une zone avec le nom de la zone appartenant aux serveurs de noms principaux. Lors de la configuration de la zone partielle, définissez le paramètre ProxyMode sur YES. Cette zone est la zone partielle qui contient les enregistrements de ressources détenus par l'ADC.

   Par exemple, si le nom de la zone configurée sur les serveurs de noms principaux est exemple.com, vous devez créer une zone nommée exemple.com sur l'ADC. Définissez le paramètre ProxyMode sur YES. Pour plus d'informations sur l'ajout d'une zone, voir Configurer une zone DNS.

   > **Remarque**
   >
   > N'ajoutez pas d'enregistrements SOA et NS pour la zone. Ces enregistrements doivent exister sur l'ADC pour une zone pour laquelle l'ADC fait autorité.

2. Importez les clés (depuis l'un des serveurs de noms dorsaux) vers ADC, puis ajoutez-les au répertoire /nsconfig/dns/. Pour plus d'informations sur la façon dont vous pouvez importer une clé et l'ajouter à ADC, consultez Publier une clé DNS dans une zone.
3. Signez la zone partielle avec les clés importées. Lorsque vous signez la zone partielle avec les clés, ADC génère des enregistrements RRSIG et NSEC pour les jeux d'enregistrements de ressources et les enregistrements de ressources individuels dans la zone partielle, respectivement. Pour plus d'informations sur la signature d'une zone, voir Signer et désigner une zone DNS.

Configurer DNSSEC pour les noms de domaine GSLB (Global Server Load Balancing)

May 5, 2023

Si le GSLB est configuré sur NetScaler et que l'ADC fait autorité pour la zone à laquelle appartiennent les noms de domaine GSLB, tous les noms de domaine GLSB sont signés lorsque la zone est signée.

Pour plus d'informations sur la signature d'une zone pour laquelle l'ADC fait autorité, voir Configurer DNSSEC lorsque l'appliance NetScalerfait autorité pour une zone.

Si les domaines GSLB appartiennent à une zone pour laquelle les serveurs de noms principaux font autorité, vous devez :

- Commencez par signer la zone sur les serveurs de noms.
- Signez ensuite la zone partielle sur ADC pour terminer la configuration DNSSEC de la zone.

Pour plus d'informations, voir Configurer DNSSEC pour une configuration de propriété de zone partielle.

Entretien de zone

May 5, 2023

Du point de vue du DNSSEC, la maintenance de zone implique le renouvellement des clés de signature de zone et des clés de signature lorsque l'expiration de la clé est imminente. Ces tâches de maintenance de zone doivent être effectuées manuellement. La zone est resignée automatiquement et ne nécessite aucune intervention manuelle.

Resigner une zone mise à jour

Lorsqu'une zone est mise à jour (ajout d'un enregistrement ou modification d'un enregistrement existant), l'appliance signe automatiquement à nouveau le nouvel enregistrement (ou le nouvel enregistrement modifié). Si une zone contient plusieurs clés de signature de zone, l'appliance signe à nouveau le nouvel enregistrement (ou le nouvel enregistrement modifié) à l'aide de la clé utilisée pour signer la zone.

Survolez les clés DNSSEC

Remarque : Passez manuellement le curseur sur les clés DNSSEC (KSK, ZSK) avant leur expiration.

Sur NetScaler, vous pouvez utiliser les méthodes de prépublication et de double signature pour effectuer un transfert de la clé de signature de zone et de la clé de signature de la clé. Plus d'informations sur ces deux méthodes de basculement sont disponibles dans la RFC 4641, « Pratiques opérationnelles DNSSEC ».

Les rubriques suivantes mettent en correspondance les commandes de l'ADC avec les étapes des procédures de basculement décrites dans la RFC 4641.

La notification d'expiration de la clé est envoyée via une interruption SNMP appelée DNSKeyExpiration. Trois variables MIB, DNSKeyName, DNSKeyTimeToExpiration et DNSKeyUnitsofExpiration sont

envoyées avec l'interruption SNMP DNSKeyExpiration. Pour plus d'informations, consultez la section *NetScaler SNMP OID Reference* sur NetScaler12.0 SNMP OID Reference.

Prépublication du survol des clés

La RFC 4641, « Pratiques opérationnelles DNSSEC », définit quatre étapes pour la méthode de remplacement des clés de prépublication : initiale, nouvelle DNSKEY, nouveaux RRSIG et suppression de DNSKEY. Chaque étape est associée à un ensemble de tâches que vous devez effectuer sur l'ADC. Vous trouverez ci-dessous la description de chaque étape et des tâches que vous devez effectuer. La procédure de transfert décrite ici peut être utilisée à la fois pour les clés de signature par clé et pour les clés de signature de zone.

- **Étape 1 : Initiale.** La zone contient uniquement les jeux de clés avec lesquels la zone est actuellement signée. L'état de la zone au stade initial est l'état de la zone juste avant que vous ne commenciez le processus de changement de touches.

  Exemple :

  Examinez la clé, example.com.zsk1, avec laquelle la zone example.com est signée. La zone contient uniquement les RRSIG générés par la clé example.com.zsk1, dont l'expiration est imminente. La clé de signature est example.com.ksk1.

- **Étape 2 : Nouveau DNSKEY.** Une nouvelle clé est créée et publiée dans la zone. C'est-à-dire que la clé est ajoutée à l'ADC, mais que la zone n'est pas signée avec la nouvelle clé tant que la phase de pré-lancement n'est pas terminée. À ce stade, la zone contient l'ancienne clé, la nouvelle clé et les RRSIG générés par l'ancienne clé. La publication de la nouvelle clé pendant toute la durée de la phase préalable à l'enregistrement permet d'obtenir l'enregistrement de ressources DNSKEY correspondant à la nouvelle clé et de le transmettre aux serveurs de noms secondaires.

  Exemple :

  Une nouvelle clé example.com.zsk2 est ajoutée à la zone example.com. La zone n'est pas signée avec example.com.zsk2 tant que la phase préalable à l'enregistrement n'est pas terminée. La zone example.com contient des enregistrements de ressources DNSKEY pour example.com.zsk1 et example.com.zsk2.

  Commandes NetScaler :

  Effectuez les tâches suivantes sur l'ADC :

  - Créez une clé DNS à l'aide de la commande `create dns key`.

    Pour plus d'informations sur la création d'une clé DNS, y compris un exemple, voir Créer des clés DNS pour une zone.

- Publiez la nouvelle clé DNS dans la zone à l'aide de la commande `add dns key`.

  Pour plus d'informations sur la publication de la clé dans la zone, y compris un exemple, voir Publier une clé DNS dans une zone.

- **Étape 3 : Nouveaux RRSIG.** La zone est signée avec la nouvelle clé DNS, puis désignée avec l'ancienne clé DNS. L'ancienne clé DNS n'est pas supprimée de la zone et reste publiée jusqu'à ce que les RRSIG générés par l'ancienne clé expirent.

  Exemple :

  La zone est signée avec example.com.zsk2, puis désignée avec example.com.zsk1. La zone continue de publier example.com.zsk1 jusqu'à ce que les RRSIG générés par example.com.zsk1 expirent.

  Commandes NetScaler :

  Effectuez les tâches suivantes sur l'ADC :

  - Signez la zone avec la nouvelle clé DNS à l'aide de la `sign dns zone` commande.
  - Déconnectez la zone avec l'ancienne clé DNS à l'aide de la commande `unsign dns zone`.

  Pour plus d'informations sur la signature et la désignature d'une zone, y compris des exemples, voir Signer et désigner une zone DNS.

- **Étape 4 : Suppression de DNSKEY.** Lorsque les RRSIG générés par l'ancienne clé DNS expirent, l'ancienne clé DNS est supprimée de la zone.

  Exemple :

  L'ancienne clé DNS example.com.zsk1 est supprimée de la zone example.com.

  Commandes NetScaler

  Sur ADC, vous supprimez l'ancienne clé DNS à l'aide de la commande `rm dns key`. Pour plus d'informations sur la suppression d'une clé d'une zone, y compris un exemple, voir Supprimer une clé DNS.

Clé-clé à double signature

La RFC 4641, « Pratiques opérationnelles DNSSEC », définit trois étapes pour le transfert de clés à double signature : la clé initiale, la nouvelle DNSKEY et la suppression de DNSKEY. Chaque étape est associée à un ensemble de tâches que vous devez effectuer sur l'ADC. Vous trouverez ci-dessous la description de chaque étape et des tâches que vous devez effectuer. La procédure de transfert décrite ici peut être utilisée à la fois pour les clés de signature par clé et pour les clés de signature de zone.

- **Étape 1 : Initiale.** La zone contient uniquement les jeux de clés avec lesquels la zone est actuellement signée. L'état de la zone au stade initial est l'état de la zone juste avant que vous ne commenciez le processus de changement de touches.

Exemple :

Examinez la clé, example.com.zsk1, avec laquelle la zone example.com est signée. La zone contient uniquement les RRSIG générés par la clé example.com.zsk1, dont l'expiration est imminente. La clé de signature est example.com.ksk1.

- **Étape 2 : Nouveau DNSKEY.** La nouvelle clé est publiée dans la zone et la zone est signée avec la nouvelle clé. La zone contient les RRSIG générés par l'ancienne et la nouvelle clé. La durée minimale pendant laquelle la zone doit contenir les deux ensembles de RRSIG est le temps nécessaire pour que tous les RRSIG expirent.

  Exemple :

  Une nouvelle clé example.com.zsk2 est ajoutée à la zone example.com. La zone est signée avec example.com.zsk2. La zone example.com contient désormais les RRSIG générés à partir des deux clés.

  Commandes NetScaler

  Effectuez les tâches suivantes sur l'ADC :

  - Créez une clé DNS à l'aide de la commande `create dns key`.

    Pour plus d'informations sur la création d'une clé DNS, y compris un exemple, voir Créer des clés DNS pour une zone.

  - Publiez la nouvelle clé dans la zone à l'aide de la commande `add dns key`.

    Pour plus d'informations sur la publication de la clé dans la zone, y compris un exemple, voir Publier une clé DNS dans une zone.

  - Signez la zone avec la nouvelle clé à l'aide de la commande `sign dns zone`.

    Pour plus d'informations sur la signature d'une zone, y compris des exemples, voir Signer et désigner une zone DNS.

- **Étape 3 : Suppression de DNSKEY.** Lorsque les RRSIG générés par l'ancienne clé DNS expirent, l'ancienne clé DNS est supprimée de la zone.

  Exemple :

  L'ancienne clé DNS example.com.zsk1 est supprimée de la zone example.com.

  Commandes NetScaler :

  Sur ADC, vous supprimez l'ancienne clé DNS à l'aide de la commande `rm dns key`.

  Pour plus d'informations sur la suppression d'une clé d'une zone, y compris un exemple, voir Supprimer une clé DNS.

Transférez les opérations DNSSEC vers NetScaler

May 5, 2023

Pour les zones DNS pour lesquelles vos serveurs DNS font autorité, les opérations DNSSEC peuvent être déchargées vers l'appliance ADC. Dans un déploiement de déchargement DNSSEC, un serveur DNS envoie des réponses non signées. L'ADC signe la réponse de manière dynamique avant de la transmettre au client. L'ADC met également en cache la réponse signée. Outre la réduction de la charge sur les serveurs DNS, le transfert des opérations DNSSEC vers l'ADC vous offre les avantages suivants :

- Vous pouvez signer les enregistrements que les serveurs DNS génèrent par programmation. Ces enregistrements ne peuvent pas être signés par des opérations de signature de zone de routine effectuées sur les serveurs DNS.
- Vous pouvez fournir des réponses signées aux clients même si vous n'avez pas implémenté le protocole DNSSEC sur vos serveurs.

Pour configurer le déchargement DNSSEC, vous devez configurer un serveur virtuel d'équilibrage de charge DNS, configurer les services qui représentent les serveurs DNS, puis lier les services au serveur virtuel. Pour plus d'informations sur la configuration d'un serveur virtuel d'équilibrage de charge DNS, la configuration des services et la liaison des services au serveur virtuel, voir Configurer une zone DNS.

Créez une entité de zone sur ADC pour chaque zone DNS dont vous souhaitez décharger les opérations DNSSEC. Pour chaque zone DNS, vous devez activer les paramètres du mode proxy et du déchargement DNSSEC. Vous pouvez éventuellement configurer la génération d'enregistrements NSEC pour une zone déchargée. Pour créer une entité de zone DNS pour le déchargement DNSSEC, suivez les instructions de cette rubrique.

Pour terminer la configuration, vous devez générer des clés DNS pour la zone, ajouter les clés à la zone, puis signer la zone avec les clés. Ce processus est le même que pour le DNSSEC normal. Pour plus d'informations sur la création de clés, l'ajout de clés à une zone et la signature de la zone, voir Extensions de sécurité du système de noms de domaine.

Après avoir configuré le déchargement DNS, vous devez vider le cache DNS sur NetScaler. Le vidage du cache DNS garantit que tous les enregistrements non signés dans le cache sont supprimés puis remplacés par des enregistrements signés. Pour plus d'informations sur le vidage du cache DNS, voir Vider les enregistrements DNS.

Activer le déchargement DNSSEC pour une zone à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour activer le déchargement DNSSEC pour une zone et vérifier la configuration :


```
-  add dns zone <zoneName> -proxyMode YES -dnssecOffload ENABLED [-nsec
    ( ENABLED | DISABLED )
-  show dns zone
<!--NeedCopy-->
```

Exemple :

```
> add dns zone example.com -proxyMode YES -dnssecOffload ENABLED nsec
   ENABLED
 Done
> show dns zone example.com
     Zone Name : example.com
     Proxy Mode : YES
     DNSSEC Offload: ENABLED    NSEC: ENABLED
 Done
<!--NeedCopy-->
```

Activer le déchargement DNSSEC pour une zone à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Zones**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Pour créer une zone sur NetScaler, cliquez sur Ajouter.
   - Pour configurer le déchargement DNSSEC pour une zone existante, double-cliquez sur la zone.
3. Dans la boîte de dialogue Créer une zone DNS ou Configurer une zone DNS, cochez les cases Mode proxy et Déchargement DNSSEC.
4. Si vous souhaitez que NetScaler génère des enregistrements NSEC pour la zone, cochez la case NSEC.

Prise en charge de la partition d'administration pour DNSSEC

May 8, 2023

Dans une appliance NetScaler partitionnée, les clés DNS générées sont stockées aux emplacements suivants :

- Partition par défaut : /nsconfig/dns/
- <partitionname>Partition autre que celle par défaut : /nsconfig/partitions/ \/dns/

Vous pouvez désormais ajouter un mot de passe à la clé DNS. Pour ajouter un mot de passe à la clé DNS, vous devez d'abord ajouter le mot de passe dans la `create dns key` commande. Entrez

ensuite le même mot de passe dans la `add dns key` commande lors de l'ajout de la clé DNS à l'appliance ADC. Par exemple :

```
create dns key -zoneName com -keytype ksK -algorithm rsASHA1 -keysize 4096
- fileNamePrefix com.ksk.rsasha1.4096 -password 1jsfd3Wa

add dns key com.zsk.4096 /nsconfig/dns/com.zsk.rsasha1.4096.private -
password 1jsfd3Wa
```

Remarque :

- Pour un environnement partitionné par défaut, les clés sont lues à partir de l'emplacement par défaut/nsconfig/dns/. Toutefois, si les clés sont stockées dans un emplacement différent, le nom du chemin doit être fourni dans la `add dns key -private` commande. Par exemple, `add dns key -private <path name>`.
- Pour un environnement partitionné autre que par défaut, les clés sont lues à partir de l'emplacement par défaut `/nsconfig/partitions/<partitionname>/dns/`.

Supporte les domaines DNS génériques

May 5, 2023

Les domaines DNS Wildcard sont utilisés pour traiter les demandes concernant des domaines et des sous-domaines inexistants. Dans une zone, utilisez des domaines génériques pour rediriger les requêtes relatives à tous les domaines ou sous-domaines inexistants vers un serveur particulier, au lieu de créer un enregistrement de ressource (RR) distinct pour chaque domaine. L'utilisation la plus courante d'un domaine DNS générique est de créer une zone qui peut être utilisée pour transférer du courrier depuis Internet vers un autre système de messagerie.

Dans la résolution DNS, les RR génériques prennent en charge le domaine générique. Les RR génériques sont utilisés pour synthétiser les réponses aux requêtes concernant un nom de domaine inexistant. Par exemple, si vous avez effectué une requête et que `http://image.example.com`le sous-domaine « image » n'existe pas, il se peut que vous soyez redirigé vers exemple.com.

Un enregistrement générique comporte un astérisque (*) comme étiquette la plus à gauche d'un nom de domaine. Par exemple, `*.example.com`. Un astérisque à n'importe quel autre endroit du nom de domaine signifie qu'il s'agit d'un enregistrement DNS générique. Par exemple, `new.*.example.com` il ne s'agit pas d'un enregistrement DNS générique valide.

> **Remarque**
>
> - Le domaine Wildcard est pris en charge uniquement lorsque l'appliance NetScaler fait autorité pour la zone et est configurée en tant que serveur proxy ADNS ou DNS.

- Le domaine Wildcard n'est pas pris en charge pour les enregistrements NS et SOA.
- Le domaine Wildcard ne peut pas être appliqué lorsque la requête se trouve dans une autre zone.
- Le domaine générique ne peut pas être appliqué lorsque l'existence du QNAME ou d'un nom compris entre le domaine générique et le QNAME est connue.

Exemple de configuration

```
add dns soaRec example.com -originServer n1.example.com -contact admin.
   example.com

add dns nsRec example.com n1.example.com

add dns nsRec example.com n2.example.com

add dns zone example.com  -proxyMode no

add dns addrec www.example.com 2.2.2.2

add dns addrec *.example.com 10.10.10.10

add dns addrec *.example.com 10.10.10.11

add dns aaaarec *.example.com 2001::1
<!--NeedCopy-->
```

Dans l'exemple, un nom de domaine générique est ajouté pour un enregistrement A et AAAA.

Lorsqu'une requête est reçue pour un nom de domaine qui existe dans la zone, l'appliance NetScaler répond avec la réponse correspondante. Par exemple, pour `www.example.com`, l'appliance répond avec 2.2.2.2 dans l'exemple.

Pour un nom de domaine inexistant qui correspond à un type de caractère générique, une réponse synthétisée est délivrée.

Dans l'exemple, l'appliance NetScaler répond avec 10.10.10.10 et 10.10.11 pour un nom de domaine nonexist.example.com ou xyz.example.com.

La synthèse des caractères génériques ne s'applique pas à un nom de domaine qui existe dans la zone.

Par exemple, pour la requête `www.example.com` et le type AAAA, l'appliance NetScaler ne synthétise pas avec un caractère générique, car elle `www.example.com` existe avec le type A. Dans cet exemple, l'appliance NetScaler répond par une réponse NODATA.

Pour une requête, dites abc.example.com et tapez AAAA, l'appliance NetScaler répond par une

réponse synthétisée. Par exemple, pour `www.example.com`, l'appliance répond avec 2001 : :1 dans l'exemple.

Atténuez les attaques DDoS DNS

May 5, 2023

Les serveurs DNS sont l'un des composants les plus critiques d'un réseau et ils doivent être défendus contre les attaques. L'attaque DDoS est l'un des types les plus élémentaires d'attaques DNS. Les attaques de ce type se multiplient et peuvent être destructrices. Pour atténuer les attaques DDoS, vous pouvez procéder comme suit :

- Videz les enregistrements négatifs.
- Limitez la durée de vie (TTL) des enregistrements négatifs.
- Préservez la mémoire NetScaler en limitant la consommation de mémoire par le cache DNS.
- Conservez les enregistrements DNS dans le cache.
- Activez le contournement du cache DNS.

Rincer les enregistrements négatifs

Une attaque DNS remplit le cache d'enregistrements négatifs (NXDOMAIN et NODATA). Par conséquent, les réponses aux demandes légitimes ne sont pas mises en cache. Les nouvelles demandes sont donc envoyées à un serveur principal pour résolution DNS. Les réponses sont donc différées.

Vous pouvez désormais vider les enregistrements DNS négatifs du cache DNS de l'appliance NetScaler.

Videz les enregistrements de cache négatifs à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
flush dns proxyrecords -type (dnsRecordType | negRecType)NXDOMAIN | NODATA
```

Exemple :

```
flush dns proxyrecords -negRecType NODATA
```

Effacement des enregistrements de cache négatifs à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS >**Enregistrements**.
2. Dans le volet de détails, cliquez sur **Flush Proxy Records**.
3. Dans la zone **Type de rinçage**, sélectionnez **Negative Records**.
4. **Dans la zone**Type d'enregistrements négatifs**, sélectionnez**NXDOMAIN**ou NODATA.**

Protection contre les attaques aléatoires par sous-domaine et NXDOMAIN

Pour empêcher les attaques aléatoires par sous-domaine et NXDOMAIN, vous pouvez restreindre la mémoire cache du DNS et ajuster les valeurs TTL pour les enregistrements négatifs.

Pour limiter la quantité de mémoire consommée par le cache DNS, spécifiez la taille maximale du cache (en Mo), ainsi que la taille du cache (en Mo) pour le stockage des réponses négatives. Lorsque l'une des limites est atteinte, aucune autre entrée n'est ajoutée au cache. Les messages Syslog sont également enregistrés et, si vous avez configuré des interruptions SNMP, des interruptions SNMP sont générées. Si ces limites ne sont pas définies, la mise en cache se poursuit jusqu'à épuisement de la mémoire système.

Une valeur TTL plus élevée pour les enregistrements négatifs peut entraîner le stockage d'enregistrements qui ne sont pas utiles pendant une longue période. Une valeur TTL plus faible entraîne l'envoi d'un plus grand nombre de demandes au serveur principal.

Le TTL de l'enregistrement négatif est défini sur une valeur qui peut être la moins élevée entre la valeur TTL ou la valeur « Expire » de l'enregistrement SOA.

Remarque :

- Cette limitation est ajoutée par moteur de paquets. Par exemple, si la valeur MaxCacheSize est définie sur 5 Mo et que l'appliance possède 3 moteurs de paquets, la taille totale du cache est de 15 Mo.
- La taille du cache pour les enregistrements négatifs doit être inférieure ou égale à la taille maximale du cache.
- Si vous réduisez la limite de mémoire cache DNS à une valeur inférieure à la quantité de données déjà mises en cache, la taille du cache reste supérieure à la limite jusqu'à ce que les données expirent. C'est-à-dire qu'il dépasse son TTL0 ou qu'il est vidé (`flush dns proxyrecords` commande ou Flush Proxy Records dans l'interface graphique de NetScaler).
- Pour configurer les interruptions SNMP, reportez-vous à la section Configuration de NetScaler pour générer des interruptions SNMP.

Limiter la mémoire consommée par le cache DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set dns parameter -maxCacheSize <MBytes> -maxNegativeCacheSize <MBytes>
```

Exemple :

```
set dns parameter - maxCacheSize 100 -maxNegativeCacheSize 25
```


Limitez la mémoire consommée par le cache DNS à l'aide de l'interface graphique

Accédez à **Configuration** > **Gestion du trafic** > **DNS**, cliquez sur **Modifier les paramètres DNS**et définissez les paramètres suivants :

- Taille maximale du cache en Mo
- Taille de cache négative maximale en Mo

Restreindre le TTL des enregistrements négatifs à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set dns parameter -maxnegcacheTTL <secs>
```

Exemple :

```
set dns parameter -maxnegcacheTTL 360
```

Restreindre le TTL des enregistrements négatifs à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS**.
2. Cliquez sur **Modifier les paramètres DNS** et définissez le paramètre **Max Negative Cache TTL en secondes** .

Conserver les enregistrements DNS dans le cache

Une attaque peut inonder le cache DNS d'entrées non importantes, mais peut également provoquer le vidage des enregistrements légitimes déjà mis en cache pour faire de la place aux nouvelles entrées. Pour empêcher les attaques de remplir le cache avec des données non valides, vous pouvez conserver les enregistrements légitimes même s'ils dépassent leurs valeurs TTL.

Si vous activez le paramètre CacheNoExpire, les enregistrements actuellement dans le cache sont conservés jusqu'à ce que vous désactiviez le paramètre.

Remarque :

- Cette option ne peut être utilisée que lorsque la taille maximale du cache est spécifiée (paramètre MaxCacheSize).
- Si MaxNegCacheTtl est configuré et que CacheNoExpire est activé, CachNoExpire est prioritaire.

Conservez les enregistrements DNS dans le cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set dns parameter -cacheNoExpire ( ENABLED | DISABLED)
```


Exemple :

```
set dns parameter -cacheNoExpire ENABLED
```

Conservez les enregistrements DNS dans le cache à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS** et cliquez sur **Modifier les paramètres DNS**.
2. Sélectionnez **Cache No Expire**.

Activer le contournement du cache DNS

Pour une meilleure visibilité et un meilleur contrôle des requêtes DNS, définissez le paramètre CacheHitBypass pour transmettre toutes les demandes aux serveurs principaux et autoriser la création du cache sans toutefois l'utiliser. Une fois le cache créé, vous pouvez désactiver le paramètre afin que les requêtes soient traitées à partir du cache.

Activer le contournement du cache DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set dns parameter -cacheHitBypass ( ENABLED | DISABLED )
```

Exemple :

```
set dns parameter -cacheHitBypass ENABLED
```

Activer le contournement du cache DNS à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS** et cliquez sur **Modifier les paramètres DNS**.
2. Sélectionnez **Cache Hit Bypass**.

Prévenir l'`Slowloris` attaque

Une requête DNS couvrant plusieurs paquets représente la menace potentielle d'une `Slowloris` attaque. L'appliance NetScaler peut supprimer silencieusement les requêtes DNS qui sont divisées en plusieurs paquets.

Vous pouvez définir le `splitPktQueryProcessing` paramètre sur AUTORISER ou SUPPRIMER une requête DNS si la requête est divisée en plusieurs paquets.

Remarque : Ce paramètre s'applique uniquement au DNS TCP.

Limitez les requêtes DNS à un seul paquet à l'aide de la CLI

À l'invite de commande, tapez :

```
set dns parameter -splitPktQueryProcessing ( ALLOW | DROP )
```

Exemple :

```
set dns parameter -splitPktQueryProcessing DROP
```

Limitez les requêtes DNS à un seul paquet à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **DNS** et cliquez sur **Modifier les paramètres DNS**.
2. Dans la zone **Traitement des requêtes par paquets fractionnés**, choisissez **ALLOW** ou **DROP**.

Collectez des statistiques sur les réponses DNS envoyées depuis le cache

Vous pouvez collecter des statistiques sur les réponses DNS envoyées à partir du cache. Utilisez ensuite ces statistiques pour créer un seuil au-delà duquel davantage de trafic DNS est supprimé et appliquez ce seuil à l'aide d'une politique basée sur la bande passante. Auparavant, le calcul de la bande passante pour un serveur virtuel d'équilibrage de charge DNS n'était pas précis, car le nombre de demandes traitées à partir du cache n'était pas indiqué.

En mode proxy, les statistiques relatives aux octets de demande, aux octets de réponse, au nombre total de paquets reçus et au nombre total de paquets envoyés sont mises à jour en permanence. Auparavant, ces statistiques n'étaient pas toujours mises à jour, en particulier pour un serveur virtuel d'équilibrage de charge DNS.

Le mode proxy vous permet également désormais de déterminer le nombre de réponses DNS envoyées à partir du cache. Pour collecter ces statistiques, les options suivantes ont été ajoutées à la `stat lb vserver <DNSvirtualServerName>` commande :

- **Demandes** : nombre total de demandes reçues par le serveur virtuel DNS ou DNS_TCP. Inclut les demandes transférées vers le serveur principal et les demandes auxquelles il a été répondu depuis le cache.
- Nombre d'**accès au serveur virtuel** : nombre total de demandes transmises au backend. Le nombre de demandes traitées depuis le cache est la différence entre le nombre total de demandes et le nombre de demandes traitées depuis le serveur virtuel.
- **Réponses** : nombre total de réponses envoyées par ce serveur virtuel. Par exemple, si un serveur virtuel DNS LB reçoit 5 requêtes DNS, en transmet 3 au serveur principal et en transmet 2 depuis le cache, la valeur correspondante de chacune de ces statistiques serait la suivante :
  - **Nombre de visites du serveur virtuel** : 3
  - **Demandes** : 5

- **Réponses** : 5

Équilibrage de la charge du

May 5, 2023

L'équilibrage de charge du pare-feu répartit le trafic entre plusieurs pare-feux, offrant ainsi une tolérance aux pannes et un débit accru. L'équilibrage de charge du pare-feu protège votre réseau en :

- Répartir la charge entre les pare-feux, ce qui élimine un point de défaillance unique et permet au réseau d'évoluer.
- Augmenter la haute disponibilité.

La configuration d'une appliance NetScaler pour l'équilibrage de charge du pare-feu est similaire à la configuration de l'équilibrage de charge, à l'exception du fait que le type de service recommandé est ANY, le type de moniteur recommandé est PING et le mode serveur virtuel d'équilibrage de charge est défini sur MAC.

Vous pouvez configurer l'équilibrage de charge du pare-feu dans une configuration d'environnement sandwich, d'entreprise ou à plusieurs pare-feux. L'environnement sandwich est utilisé pour équilibrer la charge du trafic entrant sur le réseau depuis l'extérieur et le trafic sortant du réseau vers Internet. Il implique la configuration de deux appliances NetScaler, une de chaque côté d'un ensemble de pare-feux. Vous configurez un environnement d'entreprise pour équilibrer la charge du trafic quittant le réseau vers Internet. L'environnement d'entreprise implique la configuration d'une appliance NetScaler unique entre le réseau interne et les pare-feux qui fournissent un accès à Internet. L'environnement à plusieurs pare-feux est utilisé pour équilibrer la charge du trafic provenant d'un autre pare-feu. L'activation de l'équilibrage de charge du pare-feu des deux côtés de l'appliance NetScaler améliore le flux de trafic à la fois dans le sens de sortie et d'entrée et garantit un traitement plus rapide du trafic. L'environnement à plusieurs pare-feux implique la configuration d'une appliance NetScaler intercalée entre deux pare-feux.

Important : si vous configurez des itinéraires statiques sur l'appliance NetScaler pour l'adresse IP de destination et activez le mode L3, l'appliance NetScaler utilise sa table de routage pour acheminer le trafic au lieu de l'envoyer au serveur vserver d'équilibrage de charge.

Remarque : Pour que le FTP fonctionne, un serveur ou un service virtuel supplémentaire doit être configuré sur l'appliance NetScaler avec l'adresse IP et le port sous la forme * et 21 respectivement, et le type de service spécifié comme FTP. Dans ce cas, l'appliance NetScaler gère le protocole FTP en acceptant la connexion de contrôle FTP, en modifiant la charge utile et en gérant la connexion de données, le tout via le même pare-feu.

L'équilibrage de charge du pare-feu ne prend en charge que certaines des méthodes d'équilibrage de charge prises en charge par l'appliance NetScaler. En outre, vous ne pouvez configurer que quelques

types de persistance et de moniteurs.

Méthodes d'équilibrage de charge du pare-feu

Les méthodes d'équilibrage de charge suivantes sont prises en charge pour l'équilibrage de charge du pare-feu.

- Connexions moindres
- Round Robin
- Moins de paquets
- Moins de bande passante
- Hash IP source
- Hachage IP de destination
- IP source, hachage IP de destination
- IP source Hachage du port source
- Méthode du temps de réponse le plus court (LRTM)
- Chargement personnalisé

Persistance du pare-feu

Seule la persistance basée sur SOURCEIP, DESTIP et SOURCEIPDESTIP est prise en charge pour l'équilibrage de charge du pare-feu.

Surveillance des serveurs de pare-feu

Seuls le PING et les moniteurs transparents sont pris en charge dans l'équilibrage de charge du pare-feu. Vous pouvez lier un moniteur PING (par défaut) au service principal qui représente le pare-feu. Si un pare-feu est configuré pour ne pas répondre aux paquets ping, vous pouvez configurer des moniteurs transparents pour surveiller les hôtes du côté approuvé via des pare-feu individuels.

Environnement Sandwich

May 5, 2023

Un déploiement NetScaler en mode sandwich permet d'équilibrer la charge du trafic réseau via les pare-feux dans les deux sens : entrée (trafic entrant sur le réseau depuis l'extérieur, tel qu'Internet) et sortie (trafic sortant du réseau vers Internet).

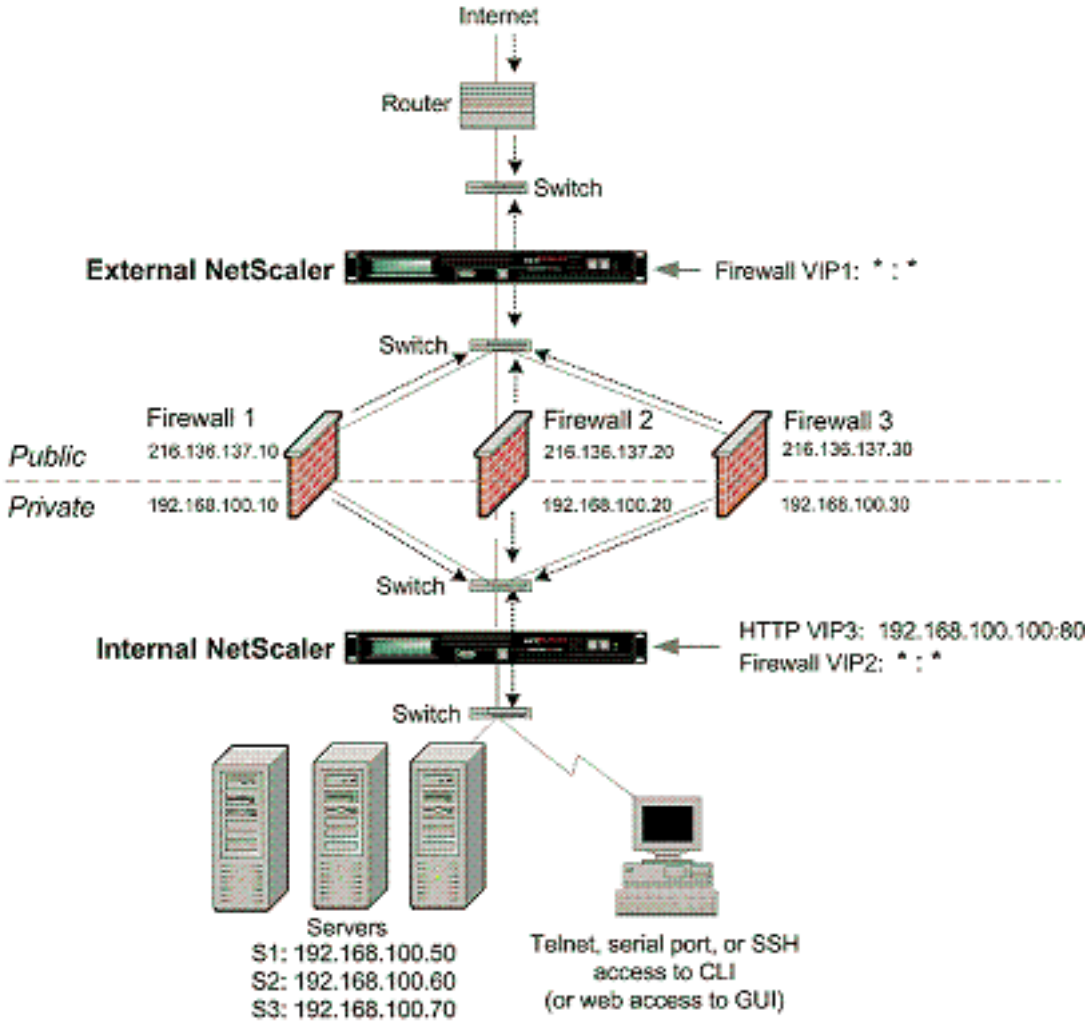
Dans cette configuration, un NetScaler est situé de chaque côté d'un ensemble de pare-feux. Le NetScaler placé entre les pare-feux et Internet, appelé NetScaler externe qui gère le trafic entrant,

sélectionne le meilleur pare-feu en fonction de la méthode configurée. Le NetScaler situé entre les pare-feux et le réseau privé, appelé NetScaler interne, suit le pare-feu à partir duquel le paquet initial d'une session est reçu. Il s'assure ensuite que tous les paquets suivants pour cette session sont envoyés au même pare-feu.

Le NetScaler interne peut être configuré comme un gestionnaire de trafic normal pour équilibrer la charge du trafic sur les serveurs du réseau privé. Cette configuration permet également d'équilibrer la charge du trafic provenant du réseau privé (sortie) entre les pare-feux.

Le schéma suivant montre l'environnement d'équilibrage de charge du pare-feu sandwich.

Figure 1. Équilibrage de charge du pare-feu (Sandwich)



Le type de service ANY configure NetScaler pour qu'il accepte tout le trafic.

Pour bénéficier des avantages liés au HTTP et au TCP, configurez le service et le serveur virtuel avec le type HTTP ou TCP. Pour que FTP fonctionne, configurez le service avec le type FTP.

Configuration du NetScaler externe dans un environnement sandwich

Effectuez les tâches suivantes pour configurer le NetScaler externe dans un environnement sandwich

- Activez la fonction d'équilibrage de charge.
- Configurez un service générique pour chaque pare-feu.
- Configurez un moniteur pour chaque service générique.
- Configurez un serveur virtuel générique pour le trafic provenant d'Internet.
- Configurez le serveur virtuel en mode de réécriture MAC.
- Liez les services au serveur virtuel Wildcard.
- Enregistrez et vérifiez la configuration.

Activer la fonction d'équilibrage de charge

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

```
enable ns feature LB
show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                       Acronym             Status
        -------                       -------             ------
 1)     Web Logging                   WL                  OFF
 2)     Surge Protection              SP                  ON
 3)     Load Balancing                LB                  ON
 .
 .
 .
 24)    NetScaler Push                push                OFF
 Done
<!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres** et, dans **Configurer les fonctionnalités de base**, sélectionnez **Équilibrage de charge**.

Configurer un service générique pour chaque pare-feu

Pour configurer un service générique pour chaque pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

Pour configurer un service générique pour chaque pare-feu à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services** et ajoutez un service. Spécifiez **ANY** dans le champ **Protocole** et * dans le champ Port.

Configurer un moniteur pour chaque service générique

Un moniteur PING est lié par défaut au service. Vous devez configurer un moniteur transparent pour surveiller les hôtes fiables via des pare-feux individuels. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance NetScaler et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existant dans le chemin allant de l'appliance au périphérique qui possède l'adresse IP de destination spécifiée dans le moniteur. Si aucun moniteur transparent n'est configuré et que l'état du pare-feu est UP mais que l'un des périphériques de saut suivant de ce pare-feu est en panne, l'appliance inclut le pare-feu lors de l'équilibrage de charge et transmet le paquet au pare-feu. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivant est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le pare-feu) est en panne, le service est marqué comme étant DOWN et le pare-feu n'est pas inclus lorsque l'appliance effectue l'équilibrage de charge du pare-feu.

La liaison d'un moniteur transparent remplace le moniteur PING. Pour configurer un moniteur PING en plus d'un moniteur transparent, après avoir créé et lié un moniteur transparent, vous devez lier un moniteur PING au service.

Pour configurer un moniteur transparent à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
   transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
To bind a PING monitor, type the following command:
bind monitor PING fw-svc1
<!--NeedCopy-->
```

Pour créer et lier un moniteur transparent à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**, puis créez et liez un moniteur transparent.

Configurer un serveur virtuel générique pour le trafic provenant d'Internet

Pour configurer un serveur virtuel générique pour le trafic provenant d'Internet à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Pour configurer un serveur virtuel générique pour le trafic provenant d'Internet à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et créez un serveur virtuel générique. Spécifiez **ANY** dans le champ **Protocole** et * dans le champ Port.

Configurer le serveur virtuel en mode de réécriture MAC

Pour configurer le serveur virtuel en mode de réécriture MAC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Pour configurer le serveur virtuel en mode de réécriture MAC à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-LB-1).
2. Modifiez la section **Paramètres de base**, puis cliquez sur **Plus**.
3. Dans la liste déroulante **Mode de redirection**, sélectionnez **Basé sur MAC**.

Liez les services au serveur virtuel Wildcard

Pour lier un service au serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier un service au serveur virtuel générique à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et sélectionnez le serveur virtuel auquel vous souhaitez lier le service.
2. Cliquez dans la section **Services** et sélectionnez le service à lier.

Enregistrer et vérifier la configuration

Lorsque vous avez terminé les tâches de configuration, veillez à enregistrer la configuration. Assurez-vous que les paramètres sont corrects.

Pour enregistrer et vérifier la configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

```
save ns config
show vserver
<!--NeedCopy-->
```

Exemple :

```
save config
sh lb vserver FWLBVIP1
FWLBVIP1 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 06:40:14 2010
        Time since last state change: 0 days, 00:00:11.240
        Effective State: UP  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: SRCIPDESTIPHASH
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw_svc_1 (10.102.29.251: *) - ANY State: UP  Weight: 1
2) fw_svc_2 (10.102.29.18: \*) - ANY State: UP   Weight: 1
 Done
show service fw-svc1
        fw-svc1 (10.102.29.251:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 10:04:50 2010
        Time since last state change: 0 days, 00:00:38.120
        Server Name: 10.102.29.251
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
```



```
30          Access Down Service: NO
31          TCP Buffering(TCPB): YES
32          HTTP Compression(CMP): NO
33          Idle timeout: Client: 120 sec   Server: 120 sec
34          Client IP: DISABLED
35          Cacheable: NO
36          SC: OFF
37          SP: OFF
38          Down state flush: ENABLED
39
40  1)      Monitor Name: monitor-HTTP-1
41                  State: DOWN     Weight: 1
42                  Probes: 5       Failed [Total: 5 Current: 5]
43                  Last response: Failure - Time out during TCP connection
                        establishment stage
44                  Response Time: 2000.0 millisec
45  2)      Monitor Name: ping
46                  State: UP       Weight: 1
47                  Probes: 3       Failed [Total: 0 Current: 0]
48                  Last response: Success - ICMP echo reply received.
49                  Response Time: 1.415 millisec
50   Done
51  <!--NeedCopy-->
```

Configuration du NetScaler interne dans un environnement sandwich

Effectuez les tâches suivantes pour configurer le NetScaler interne dans un environnement sandwich

Pour le trafic provenant du serveur (sortie)

- Activez la fonction d'équilibrage de charge.
- Configurez un service générique pour chaque pare-feu.
- Configurez un moniteur pour chaque service générique.
- Configurez un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu.
- Configurez le serveur virtuel en mode de réécriture MAC.
- Liez les services de pare-feu au serveur virtuel générique.

Pour le trafic sur les serveurs de réseaux privés

- Configurez un service pour chaque serveur virtuel.
- Configurez un moniteur pour chaque service.
- Configurez un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs.
- Liez les services HTTP au serveur virtuel HTTP.
- Enregistrez et vérifiez la configuration.

Activer la fonction d'équilibrage de charge

Vous pouvez configurer des entités d'équilibrage de charge telles que des services et des serveurs virtuels lorsque la fonctionnalité d'équilibrage de charge est désactivée. Mais ils ne fonctionneront pas tant que vous n'aurez pas activé la fonctionnalité.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

```
enable ns feature LB
show ns feature
<!--NeedCopy-->
```

Exemple :

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres** et, dans Configurer les fonctionnalités de base, sélectionnez **Équilibrage de charge**.

Configurer un service générique pour chaque pare-feu

Pour configurer un service générique pour chaque pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

Pour configurer un service générique pour chaque pare-feu à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services** et ajoutez un service. Spécifiez **ANY** dans le champ **Protocole** et * dans le champ Port.

Configurer un moniteur pour chaque service générique

Un moniteur PING est lié par défaut au service. Vous devez configurer un moniteur transparent pour surveiller les hôtes fiables via des pare-feux individuels. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance NetScaler et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existant dans le chemin allant de l'appliance au périphérique qui possède l'adresse IP de destination spécifiée dans le moniteur. Si aucun moniteur transparent n'est configuré et que l'état du pare-feu est UP mais que l'un des périphériques de saut suivant de ce pare-feu est en panne, l'appliance inclut le pare-feu lors de l'équilibrage de charge et transmet le paquet au pare-feu. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivant est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le pare-feu) est en panne, le service est marqué comme étant DOWN et le pare-feu n'est pas inclus lorsque l'appliance effectue l'équilibrage de charge du pare-feu.

La liaison d'un moniteur transparent remplace le moniteur PING. Pour configurer un moniteur PING en plus d'un moniteur transparent, après avoir créé et lié un moniteur transparent, vous devez lier un moniteur PING au service.

Pour configurer un moniteur transparent à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
```



```
<!--NeedCopy-->
```

Exemple :

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```

Pour créer et lier un moniteur transparent à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs** et créez un moniteur.
2. Dans la boîte de dialogue **Créer un moniteur**, entrez les paramètres requis, puis sélectionnez **Transparent**.

Configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu

Pour configurer un serveur virtuel générique afin d'équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Pour configurer un serveur virtuel générique pour le trafic provenant d'Internet à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et créez un serveur virtuel générique.
2. Spécifiez **ANY** dans le champ Protocole et ***** dans le champ Port.

Pour configurer un serveur virtuel générique afin d'équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet de détails, cliquez sur Ajouter.

3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants, comme indiqué :
   - Nom—nom
4. Dans Protocole, sélectionnez ANY, et dans IP Address and Port, sélectionnez *.
5. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Configurer le serveur virtuel en mode de réécriture MAC

Pour configurer le serveur virtuel en mode de réécriture MAC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Pour configurer le serveur virtuel en mode de réécriture MAC à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-LB-1).
2. Modifiez la section **Paramètres de base**, puis cliquez sur **Plus**.
3. Dans la liste déroulante **Mode de redirection**, sélectionnez **Basé sur MAC**.

Liez les services de pare-feu au serveur virtuel générique

Pour lier les services de pare-feu au serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :


```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier les services de pare-feu au serveur virtuel générique à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez un serveur virtuel.
2. Cliquez sur dans la section Service, puis sélectionnez le service à lier.

Remarque : Vous pouvez lier un service à plusieurs serveurs virtuels.

Configurer un service pour chaque serveur virtuel

Pour configurer un service pour chaque serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 10.102.29.5 HTTP 80
<!--NeedCopy-->
```

Pour configurer un service pour chaque serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis configurez un service pour chaque serveur virtuel.
2. Spécifiez **HTTP** dans le champ **Protocole**, puis sélectionnez **HTTP** sous **Moniteurs disponibles**.

Pour configurer un service pour chaque serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez des valeurs pour les paramètres suivants, comme indiqué :

- Nom du service : nom
- Serveur—Nom du serveur
- Port-port

4. Dans Protocole, spécifiez HTTP. Sous Moniteurs disponibles, sélectionnez HTTP.
5. Cliquez sur Créer, puis sur Fermer. Le service que vous avez créé apparaît dans le volet Services.

Configurer un moniteur pour chaque service

Pour lier un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Exemple :

```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier un moniteur à un service à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, double-cliquez sur un service et ajoutez un moniteur.

Configurer un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs

Pour configurer un serveur virtuel HTTP afin d'équilibrer le trafic envoyé aux serveurs à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

Pour configurer un serveur virtuel HTTP afin d'équilibrer le trafic envoyé aux serveurs à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services virtuels**, puis configurez un serveur virtuel HTTP.
2. Spécifiez **HTTP** dans le champ **Protocole** .

Pour configurer un serveur virtuel HTTP afin d'équilibrer le trafic envoyé aux serveurs à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants, comme indiqué :
   - Nom—nom
   - Adresse IP : adresse IP
     Remarque : Si le serveur virtuel utilise IPv6, cochez la case IPv6 et entrez l'adresse au format
     IPv6 (par exemple,
     1000:0000:0000:0000:0005:0600:700a:888b).
   - Port-port
4. Sous Protocole, sélectionnez HTTP.
5. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Enregistrer et vérifier la configuration

Lorsque vous avez terminé les tâches de configuration, veillez à enregistrer la configuration. Vous devez également vérifier que les paramètres sont corrects.

Pour enregistrer et vérifier la configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

- `save ns config`
- `show vserver`

Exemple :

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
```



```
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 9       Failed [Total: 9 Current: 9]
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: 2000.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.275 millisec
```



```
51   Done
52 <!--NeedCopy-->
```

Pour enregistrer et vérifier la configuration à l'aide de l'utilitaire de configuration

1. Dans le volet **Détails**, cliquez sur **Enregistrer**.
2. Dans la boîte de dialogue **Enregistrer la configuration**, cliquez sur **Oui**.
3. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
4. Dans le volet **Détails**, sélectionnez le serveur virtuel que vous avez créé à l'étape 5.
5. Vérifiez que les paramètres affichés dans le volet **Détails** sont corrects.
6. Accédez à **Traffic Management > Load Balancing > Services**.
7. Dans le volet **Détails**, sélectionnez les services que vous avez créés à l'étape 5.
8. Vérifiez que les paramètres affichés dans le volet **Détails** sont corrects.

Surveillance de l'équilibrage de charge d'un pare-feu configuré dans un environnement sandwich

Une fois la configuration installée et exécutée, vous devez consulter les statistiques de chaque service et serveur virtuel afin de vérifier les éventuels problèmes.

Affichage des statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre des problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance NetScaler. Vous pouvez afficher un résumé des statistiques pour tous les serveurs virtuels, ou vous pouvez spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les informations suivantes :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel
- Taux de demandes reçues
- Taux de succès

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques pour tous les serveurs virtuels actuellement configurés sur NetScaler, ou pour un seul serveur virtuel, à l'invite de commande, tapez :


```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Exemple :

```
>stat lb vserver -detail
Virtual Server(s) Summary
                       vsvrIP  port     Protocol        State    Req/s
                            Hits/s
One                         *    80         HTTP           UP      5/s
        0/s
Two                         *     0          TCP         DOWN      0/s
        0/s
Three                       *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done

<!--NeedCopy-->
```

Pour afficher les statistiques du serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Statistiques**.
2. Si vous souhaitez afficher les statistiques d'un seul serveur virtuel, dans le volet de détails, sélectionnez le serveur virtuel, puis cliquez sur **Statistiques**.

Affichage des statistiques d'un service

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions au serveur en cours, etc. à l'aide des statistiques de service.

Pour afficher les statistiques d'un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat service <name>
```



```
<!--NeedCopy-->
```

Exemple :

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Pour afficher les statistiques d'un service à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services > Statistiques**.
2. Si vous souhaitez afficher les statistiques d'un seul service, sélectionnez le service et cliquez sur **Statistiques**.

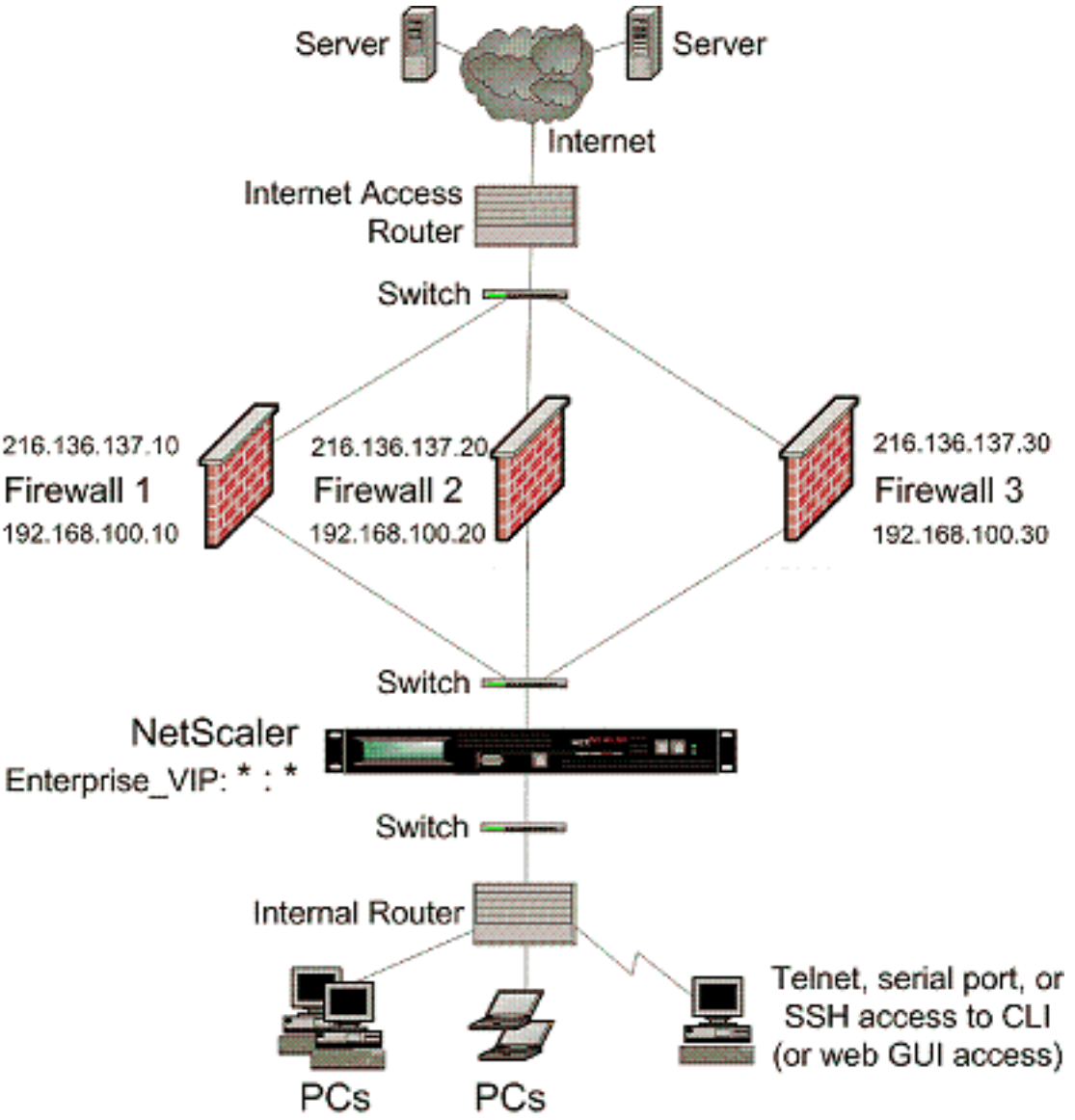
Environnement d'entreprise

May 5, 2023

Dans la configuration de l'entreprise, le NetScaler est placé entre les pare-feux se connectant à l'Internet public et au réseau privé interne et gère le trafic sortant. NetScaler sélectionne le meilleur pare-feu en fonction de la politique d'équilibrage de charge configurée.

Le schéma suivant illustre l'environnement d'équilibrage de charge du pare-feu d'entreprise.

Figure 1. Équilibrage de charge du pare-feu (Enterprise)



Le type de service ANY configure NetScaler pour qu'il accepte tout le trafic.

Pour bénéficier des avantages liés à HTTP et TCP, configurez le service et vserver avec le type HTTP ou TCP. Pour que FTP fonctionne, configurez le service avec le type FTP.

Configuration de NetScaler dans un environnement d'entreprise

Effectuez les tâches suivantes pour configurer un NetScaler dans un environnement d'entreprise.

Pour le trafic provenant du serveur (sortie)

- Activez la fonction d'équilibrage de charge.
- Configurez un service générique pour chaque pare-feu.
- Configurez un moniteur pour chaque service générique.

- Configurez un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu.
- Configurez le serveur virtuel en mode de réécriture MAC.
- Liez les services de pare-feu au serveur virtuel générique.

Pour le trafic sur les serveurs de réseaux privés

- Configurez un service pour chaque serveur virtuel.
- Configurez un moniteur pour chaque service.
- Configurez un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs.
- Liez les services HTTP au serveur virtuel HTTP.
- Enregistrez et vérifiez la configuration.

Dans l'exemple de configuration ci-dessous, l'un des serveurs de pare-feu est représenté dans le diagramme de topologie du réseau (Figure 1) est considéré.

Activer la fonction d'équilibrage de charge

Vous pouvez configurer des entités d'équilibrage de charge telles que des services et des serveurs virtuels lorsque la fonction d'équilibrage de charge est désactivée, mais elles ne fonctionneront pas tant que vous n'aurez pas activé la fonctionnalité.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

- enable ns feature LB
- show ns feature

Exemple :

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
```



```
<!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'utilitaire de configuration

Accédez à Système > Paramètres et, dans Configurer les fonctionnalités de base, sélectionnez Équilibrage de charge.

Configurer un service générique pour chaque pare-feu

Pour configurer un service générique pour chaque pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 192.168.100.10 ANY *
<!--NeedCopy-->
```

Pour configurer un service générique pour chaque pare-feu à l'aide de l'utilitaire de configuration

1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez des valeurs pour les paramètres suivants, comme indiqué :
   - Nom du service : nom
   - Serveur—Nom du serveur
4. Dans Protocole, sélectionnez ANY, et dans Port, sélectionnez *.
5. Cliquez sur Créer, puis sur Fermer. Le service que vous avez créé apparaît dans le volet Services.

Configurer un moniteur pour chaque service générique

Un moniteur PING est lié par défaut au service. Vous devrez configurer un moniteur transparent pour surveiller les hôtes du côté de confiance via des pare-feu individuels. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance NetScaler et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existant dans le chemin allant de l'appliance au périphérique qui possède l'adresse

IP de destination spécifiée dans le moniteur. Si aucun moniteur transparent n'est configuré et que l'état du pare-feu est UP mais que l'un des périphériques de saut suivant de ce pare-feu est en panne, l'appliance inclut le pare-feu lors de l'équilibrage de charge et transmet le paquet au pare-feu. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivant est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le pare-feu) est en panne, le service est marqué comme étant DOWN et le pare-feu n'est pas inclus lorsque l'appliance effectue l'équilibrage de charge du pare-feu.

La liaison d'un moniteur transparent remplacera le moniteur PING. Pour configurer un moniteur PING en plus d'un moniteur transparent, après avoir créé et lié un moniteur transparent, vous devez lier un moniteur PING au service.

Pour configurer un moniteur transparent à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -destport 80 -
    transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```

Pour créer et lier un moniteur transparent à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un moniteur, spécifiez les valeurs comme indiqué :
   - Nom*
   - Type*—Type
   - IP destination
   - Transparent

   -* Un paramètre obligatoire
4. Cliquez sur Créer, puis sur Fermer. Dans le volet Moniteurs, sélectionnez le moniteur que vous venez de configurer et vérifiez que les paramètres affichés en bas de l'écran sont corrects.

Configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu

Le trafic passant par les pare-feux est destiné à différents proxys ou serveurs placés derrière les pare-feu. Ces serveurs proxy ou serveurs peuvent avoir des adresses IP et des ports différents. Pour que le trafic passe de manière transparente par les pare-feu, l'adresse IP et le port du serveur virtuel d'équilibrage de charge des pare-feu doivent être définis sur * afin d'accepter le trafic pour n'importe quelle adresse IP et port.

Pour configurer un serveur virtuel générique afin d'équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Pour configurer un serveur virtuel générique afin d'équilibrer la charge du trafic envoyé aux pare-feu à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants, comme indiqué :
   - Nom—nom
4. Dans Protocole, sélectionnez ANY, et dans IP Address and Port, sélectionnez *.
5. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Configurer le serveur virtuel en mode de réécriture MAC

Pour configurer le serveur virtuel en mode de réécriture MAC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```


Exemple :

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Pour configurer le serveur virtuel en mode de réécriture MAC à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet de détails, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-LB-1), puis cliquez sur Ouvrir.
3. Dans l'onglet Avancé, sous Mode de redirection, cliquez sur Mac.
4. Cliquez sur OK.

Liez les services de pare-feu au serveur virtuel générique

Pour lier les services de pare-feu au serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier les services de pare-feu au serveur virtuel générique à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels, puis sélectionnez un serveur virtuel.
2. Cliquez sur dans la section Service, puis sélectionnez le service à lier.

Remarque : Vous pouvez lier un service à plusieurs serveurs virtuels.

Configurer un service pour chaque serveur virtuel

Pour configurer un service pour chaque serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 192.168.100.10 HTTP 80
<!--NeedCopy-->
```

Pour configurer un service pour chaque serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez des valeurs pour les paramètres suivants, comme indiqué :
   - Nom du service : nom
   - Serveur—Nom du serveur
   - Port-port
4. Dans Protocole, spécifiez HTTP. Sous Moniteurs disponibles, sélectionnez HTTP.
5. Cliquez sur Créer, puis sur Fermer. Le service que vous avez créé apparaît dans le volet Services.

Configurer un moniteur pour chaque service

Pour lier un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Exemple :

```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier un moniteur à un service à l'aide de l'utilitaire de configuration

1. Accédez à Traffic Management > Load Balancing > Services.
2. Ouvrez le service et ajoutez un moniteur.

Configurer un serveur virtuel HTTP pour équilibrer le trafic envoyé aux serveurs

Pour configurer un serveur virtuel HTTP afin d'équilibrer le trafic envoyé aux serveurs à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

Pour configurer un serveur virtuel HTTP afin d'équilibrer le trafic envoyé aux serveurs à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), spécifiez les valeurs des paramètres suivants, comme indiqué :
   - Nom—nom
   - Adresse IP—Adresse IP
     Remarque : Si le serveur virtuel utilise IPv6, cochez la case IPv6 et entrez l'adresse au format IPv6 (par exemple, **1000:0000:0000:0000:0005:0600:700 a:888b**).
   - Port-port
4. Sous Protocole, sélectionnez HTTP.
5. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Liez les services HTTP au serveur virtuel HTTP

Pour lier des services HTTP au serveur virtuel générique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :


```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier des services HTTP au serveur virtuel générique à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels, puis sélectionnez un serveur virtuel.
2. Cliquez sur dans la section Service, puis sélectionnez le service à lier.

Remarque : Vous pouvez lier un service à plusieurs serveurs virtuels.

Enregistrer et vérifier la configuration

Lorsque vous avez terminé les tâches de configuration, veillez à enregistrer la configuration. Vous devez également vérifier que les paramètres sont corrects.

Pour enregistrer et vérifier la configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

- save ns config
- show vserver

Exemple :

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED
```



```
17
18 1) fw-int-svc1 (192.168.100.10: \*) - ANY State: UP Weight: 1
19  Done
20 show service fw-int-svc1
21         fw-int-svc1 (192.168.100.10:\*) - ANY
22         State: UP
23         Last state change was at Thu Jul  8 14:44:51 2010
24         Time since last state change: 0 days, 00:01:50.240
25         Server Name: 192.168.100.10
26         Server ID : 0   Monitor Threshold : 0
27         Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
28         Use Source IP: NO
29         Client Keepalive(CKA): NO
30         Access Down Service: NO
31         TCP Buffering(TCPB): NO
32         HTTP Compression(CMP): NO
33         Idle timeout: Client: 120 sec   Server: 120 sec
34         Client IP: DISABLED
35         Cacheable: NO
36         SC: OFF
37         SP: OFF
38         Down state flush: ENABLED
39
40 1)      Monitor Name: monitor-HTTP-1
41                 State: UP     Weight: 1
42                 Probes: 9       Failed [Total: 0 Current: 0]
43                 Last response: Success - HTTP response code 200
        received
44                 Response Time: 100.0 millisec
45 2)      Monitor Name: ping
46                 State: UP       Weight: 1
47                 Probes: 3       Failed [Total: 0 Current: 0]
48                 Last response: Success - ICMP echo reply received.
49                 Response Time: 1.275 millisec
50  Done
51 <!--NeedCopy-->
```

Pour enregistrer et vérifier la configuration à l'aide de l'utilitaire de configuration

1. Dans le volet d'informations, cliquez sur Enregistrer.
2. Dans la boîte de dialogue Enregistrer la configuration, cliquez sur Oui.
3. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
4. Dans le volet de détails, sélectionnez le serveur virtuel que vous avez créé à l'étape 5 et vérifiez

que les paramètres affichés dans le volet Détails sont corrects.

5. Accédez à Traffic Management > Load Balancing > Services.
6. Dans le volet de détails, sélectionnez le service que vous avez créé à l'étape 5 et vérifiez que les paramètres affichés dans le volet Détails sont corrects.

Surveillance de la configuration d'un équilibrage de charge de pare-feu dans un environnement d'entreprise

Une fois la configuration installée et exécutée, vous devez consulter les statistiques de chaque service et serveur virtuel afin de vérifier les éventuels problèmes.

Affichage des statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre des problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance NetScaler. Vous pouvez afficher un résumé des statistiques pour tous les serveurs virtuels, ou vous pouvez spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les informations suivantes :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel
- Taux de demandes reçues
- Taux de succès

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques pour tous les serveurs virtuels actuellement configurés sur l'appliance NetScaler, ou pour un seul serveur virtuel, à l'invite de commande, tapez :

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Exemple :

```
>stat lb vserver -detail
Virtual Server(s) Summary
                      vsvrIP  port     Protocol        State    Req/s
                           Hits/s
One                        *    80         HTTP           UP      5/s
          0/s
```



```
5  Two                          *      0          TCP          DOWN       0/s
           0/s
6  Three                        *   2598          TCP          DOWN       0/s
           0/s
7  dnsVirtualNS     10.102.29.90     53          DNS          DOWN       0/s
           0/s
8  BRVSERV             10.10.1.1     80         HTTP          DOWN       0/s
           0/s
9  LBVIP            10.102.29.66     80         HTTP            UP       0/s
           0/s
10  Done
11
12
13 <!--NeedCopy-->
```

Pour afficher les statistiques du serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Statistiques.
2. Si vous souhaitez afficher les statistiques d'un seul serveur virtuel, dans le volet de détails, sélectionnez le serveur virtuel, puis cliquez sur Statistiques.

Affichage des statistiques d'un service

Mise à jour : 2013-08-28

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions au serveur en cours, etc. à l'aide des statistiques de service.

Pour afficher les statistiques d'un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 stat service <name>
2 <!--NeedCopy-->
```

Exemple :

```
1 stat service Service-HTTP-1
2 <!--NeedCopy-->
```


Pour afficher les statistiques d'un service à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Services > Statistiques.
2. Si vous souhaitez afficher les statistiques d'un seul service, sélectionnez-le et cliquez sur Statistiques.

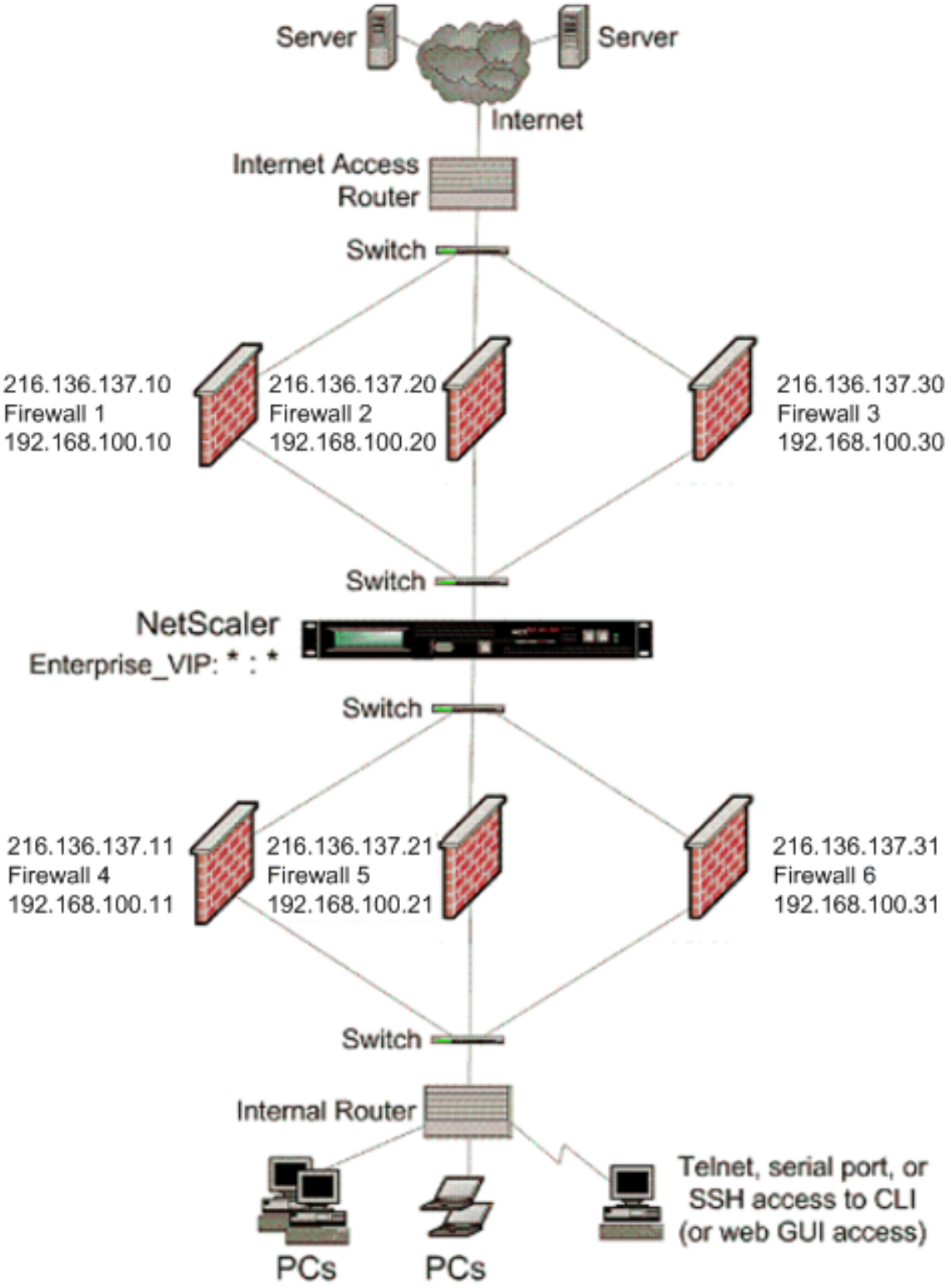
Environnement à pare-feu multiple

May 5, 2023

Dans un environnement à plusieurs pare-feux, l'appliance NetScaler est placée entre deux ensembles de pare-feux, l'ensemble externe se connectant à l'Internet public et l'ensemble interne se connectant au réseau privé interne. L'ensemble externe gère généralement le trafic sortant. Ces pare-feux implémentent principalement des listes de contrôle d'accès pour autoriser ou refuser l'accès à des ressources externes. L'ensemble interne gère généralement le trafic entrant. Ces pare-feux mettent en œuvre des mesures de sécurité destinées à protéger l'intranet contre les attaques malveillantes, en plus d'équilibrer la charge du trafic entrant. L'environnement à plusieurs pare-feux vous permet d'équilibrer la charge du trafic provenant d'un autre pare-feu. Par défaut, le trafic provenant d'un pare-feu n'est pas équilibré sur l'autre pare-feu d'une appliance NetScaler. L'activation de l'équilibrage de charge du pare-feu des deux côtés de NetScaler améliore le flux de trafic à la fois dans le sens de sortie et d'entrée et garantit un traitement plus rapide du trafic.

La figure suivante montre un environnement d'équilibrage de charge à plusieurs pare-feux

Figure 1. Équilibrage de charge du pare-feu (pare-feu multiple)



Avec une configuration telle que celle illustrée à la Figure 1, vous pouvez configurer NetScaler pour équilibrer la charge du trafic via un pare-feu interne, même si la charge est équilibrée par un pare-feu

externe. Par exemple, lorsque cette fonctionnalité est configurée, le trafic provenant des pare-feux externes (pare-feux 1, 2 et 3) est équilibré sur les pare-feux internes (pare-feux 4, 5 et 6) et vice versa.

L'équilibrage de charge du pare-feu est pris en charge uniquement pour le serveur virtuel LB en mode MAC.

Le type de service ANY configure NetScaler pour qu'il accepte tout le trafic.

Pour bénéficier des avantages liés au HTTP et au TCP, configurez le service et le serveur virtuel avec le type HTTP ou TCP. Pour que FTP fonctionne, configurez le service avec le type FTP.

Configuration de NetScaler dans un environnement à plusieurs pare-feux

Pour configurer une appliance NetScaler dans un environnement à plusieurs pare-feux, vous devez activer la fonctionnalité d'équilibrage de charge, configurer un serveur virtuel pour équilibrer la charge du trafic sortant à travers les pare-feux externes, configurer un serveur virtuel pour équilibrer la charge du trafic entrant à travers les pare-feux internes et activer l'équilibrage de charge du pare-feu sur l'appliance NetScaler. Pour configurer un serveur virtuel afin d'équilibrer la charge du trafic à travers un pare-feu dans un environnement à plusieurs pare-feux, vous devez :

1. Configurer un service générique pour chaque pare-feu
2. Configurer un moniteur pour chaque service générique
3. Configurer un serveur virtuel générique pour équilibrer la charge du trafic envoyé aux pare-feu
4. Configurer le serveur virtuel en mode de réécriture MAC
5. Liez les services de pare-feu au serveur virtuel générique

Activation de la fonction d'équilibrage de charge

Pour configurer et implémenter des entités d'équilibrage de charge telles que des services et des serveurs virtuels, vous devez activer la fonctionnalité d'équilibrage de charge sur le périphérique NetScaler.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

```
enable ns feature <featureName>
show ns feature
<!--NeedCopy-->
```

Exemple :

```
enable ns feature LoadBalancing
Done
```



```
show ns feature
Feature Acronym Status
------- ------- ------
1) Web Logging WL OFF
2) Surge Protection SP ON
3) Load Balancing LB ON
.
.
.
24) NetScaler Push push OFF
Done
<!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'interface graphique :

1. Dans le volet de navigation, développez Système, puis cliquez sur Paramètres.
2. Dans le volet Paramètres, sous Modes et fonctionnalités, cliquez sur Modifier les fonctionnalités de base.
3. Dans la boîte de dialogue Configurer les fonctionnalités de base, cochez la case Équilibrage de charge, puis cliquez sur Ok.

Configuration d'un service de caractères génériques pour chaque pare-feu

Pour accepter le trafic provenant de tous les protocoles, vous devez configurer le service de caractères génériques pour chaque pare-feu en spécifiant la prise en charge de tous les protocoles et ports.

Pour configurer un service de caractères génériques pour chaque pare-feu à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante pour configurer la prise en charge de tous les protocoles et ports :

```
add service <name>@ <serverName> <serviceType> <port_number>
<!--NeedCopy-->
```

Exemple :

```
add service fw-svc1 10.102.29.5 ANY *
<!--NeedCopy-->
```

Pour configurer un service de caractères génériques pour chaque pare-feu à l'aide de l'interface graphique :

1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans le volet de détails, cliquez sur Ajouter.

3. Dans la boîte de dialogue Créer des services, spécifiez les valeurs des paramètres suivants comme indiqué :

   - Nom du service : nom
   - Serveur—Nom du serveur

   -* Un paramètre obligatoire

4. Dans Protocole, sélectionnez N'importe quel et dans Port, sélectionnez*.
5. Cliquez sur Créer, puis sur Fermer. Le service que vous avez créé apparaît dans le volet Services.

Configuration d'un moniteur pour chaque service

Un moniteur PING est lié par défaut au service. Vous devrez configurer un moniteur transparent pour surveiller les hôtes du côté de confiance via des pare-feu individuels. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance NetScaler et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existant dans le chemin allant de l'appliance au périphérique qui possède l'adresse IP de destination spécifiée dans le moniteur. Si aucun moniteur transparent n'est configuré et que l'état du pare-feu est UP mais que l'un des périphériques de saut suivant de ce pare-feu est en panne, l'appliance inclut le pare-feu lors de l'équilibrage de charge et transmet le paquet au pare-feu. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivant est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le pare-feu) est en panne, le service est marqué comme étant DOWN et le pare-feu n'est pas inclus lorsque l'appliance effectue l'équilibrage de charge du pare-feu.

La liaison d'un moniteur transparent remplacera le moniteur PING. Pour configurer un moniteur PING en plus d'un moniteur transparent, après avoir créé et lié un moniteur transparent, vous devez lier un moniteur PING au service.

Pour configurer un moniteur transparent à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```


L'appliance NetScaler apprend les paramètres L2 du serveur à partir du moniteur lié au service. Pour les moniteurs UDP-ECV, configurez une chaîne de réception pour permettre à l'appliance d'apprendre les paramètres L2 du serveur. Si la chaîne de réception n'est pas configurée et que le serveur ne répond pas, l'appliance n'apprend pas les paramètres L2 mais le service est configuré sur UP. Le trafic de ce service est bloqué.

Pour configurer une chaîne de réception à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )] [-send <string>] [-recv <string>]
<!--NeedCopy-->
```

Exemple :

```
add lb monitor monitor-udp-1 udp-ecv -destip 10.10.10.11 -transparent
    YES  - send "test message"  - recv "site_is_up"
<!--NeedCopy-->
```

Pour créer et lier un moniteur transparent à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Create Monitor, spécifiez les valeurs des paramètres suivants, comme indiqué :
   - Nom*
   - Type*—Type
   - IP destination
   - Transparent

   -* Un paramètre obligatoire
4. Cliquez sur Créer, puis sur Fermer. Dans le volet Moniteurs, sélectionnez le moniteur que vous venez de configurer et vérifiez que les paramètres affichés en bas de l'écran sont corrects.

Configuration d'un serveur virtuel pour équilibrer la charge du trafic envoyé aux pare-feux

Pour équilibrer la charge de tout type de trafic, vous devez configurer un serveur virtuel générique en spécifiant le protocole et le port comme n'importe quelle valeur.

Pour configurer un serveur virtuel afin d'équilibrer la charge du trafic envoyé aux pare-feux à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :


```
add lb vserver <name>@ <serviceType> <IPAddress> <port_number>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Pour configurer un serveur virtuel afin d'équilibrer la charge du trafic envoyé aux pare-feux à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans Protocole, sélectionnez N'importe lequel, et dans Adresse IP et port, sélectionnez*.
4. Cliquez sur Créer, puis sur Fermer. Le serveur virtuel que vous avez créé apparaît dans le volet Serveurs virtuels d'équilibrage de charge.

Configuration du serveur virtuel en mode de réécriture MAC

Pour configurer le serveur virtuel afin qu'il utilise l'adresse MAC pour transférer le trafic entrant, vous devez activer le mode de réécriture MAC.

Pour configurer le serveur virtuel en mode de réécriture MAC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

Pour configurer le serveur virtuel en mode de réécriture MAC à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet de détails, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-LB1), puis cliquez sur Ouvrir.
3. Dans l'onglet Avancé, sous le mode Mode de redirection, cliquez sur Ouvrir.
4. Cliquez sur OK.

Lier les services de pare-feu au serveur virtuel

Pour accéder à un service sur l'appliance NetScaler, vous devez le lier à un serveur virtuel générique.

Pour lier les services de pare-feu au serveur virtuel à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
bind lb vserver <name>@ <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier les services de pare-feu au serveur virtuel à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet de détails, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, vServer-LB1), puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel (équilibrage de charge), sous l'onglet Services, cochez la case Actif à côté du service que vous souhaitez lier au serveur virtuel (par exemple, Service-HTTP-1).
4. Cliquez sur OK.

Configuration de l'équilibrage de charge à plusieurs pare-feux sur l'appliance NetScaler

Pour équilibrer la charge du trafic des deux côtés d'un NetScaler à l'aide de l'équilibrage de charge du pare-feu, vous devez activer l'équilibrage de charge multipl-firewall à l'aide du paramètre vServer-SpecificMac.

Pour configurer l'équilibrage de charge entre plusieurs pare-feux à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
set lb parameter -vServerSpecificMac <status>
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -vServerSpecificMac ENABLED
<!--NeedCopy-->
```

Pour configurer l'équilibrage de charge entre plusieurs pare-feux à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet de détails, sélectionnez le serveur virtuel pour lequel vous souhaitez configurer le mode de redirection (par exemple, Configurer les paramètres d'équilibrage de charge).
3. Dans la boîte de dialogue Définir les paramètres d'équilibrage de charge, cochez la case MAC spécifique au serveur virtuel.
4. Cliquez sur OK.

Sauvegarde et vérification de la configuration

Lorsque vous avez terminé les tâches de configuration, veillez à enregistrer la configuration. Vous devez également vérifier que les paramètres sont corrects.

Pour enregistrer et vérifier la configuration à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur transparent et vérifier la configuration :

- save ns config
- show vserver

Exemple :

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
```



```
25          Time since last state change: 0 days, 00:01:50.240
26          Server Name: 10.102.29.5
27          Server ID : 0   Monitor Threshold : 0
28          Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
29          Use Source IP: NO
30          Client Keepalive(CKA): NO
31          Access Down Service: NO
32          TCP Buffering(TCPB): NO
33          HTTP Compression(CMP): NO
34          Idle timeout: Client: 120 sec   Server: 120 sec
35          Client IP: DISABLED
36          Cacheable: NO
37          SC: OFF
38          SP: OFF
39          Down state flush: ENABLED
40
41  1)      Monitor Name: monitor-HTTP-1
42                  State: DOWN     Weight: 1
43                  Probes: 9       Failed [Total: 9 Current: 9]
44                  Last response: Failure - Time out during TCP connection
                        establishment stage
45                  Response Time: 2000.0 millisec
46  2)      Monitor Name: ping
47                  State: UP       Weight: 1
48                  Probes: 3       Failed [Total: 0 Current: 0]
49                  Last response: Success - ICMP echo reply received.
50                  Response Time: 1.275 millisec
51   Done
52  <!--NeedCopy-->
```

Pour enregistrer et vérifier la configuration à l'aide de l'interface graphique :

1. Dans le volet d'informations, cliquez sur Enregistrer.
2. Dans la boîte de dialogue Enregistrer la configuration, cliquez sur Oui.
3. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
4. Dans le volet de détails, sélectionnez le serveur virtuel que vous avez créé à l'étape 5 et vérifiez que les paramètres affichés dans le volet Détails sont corrects.
5. Accédez à Traffic Management > Load Balancing > Services.
6. Dans le volet de détails, sélectionnez le service que vous avez créé à l'étape 5 et vérifiez que les paramètres affichés dans le volet Détails sont corrects.

Surveillance de la configuration d'équilibrage de charge d'un pare-feu dans un environnement à plusieurs pare-feux

Une fois la configuration installée et exécutée, vous devez consulter les statistiques de chaque service et serveur virtuel afin de vérifier les éventuels problèmes.

Affichage des statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre des problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance NetScaler. Vous pouvez afficher un résumé des statistiques pour tous les serveurs virtuels, ou vous pouvez spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les informations suivantes :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel
- Taux de demandes reçues
- Taux de succès

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques pour tous les serveurs virtuels actuellement configurés sur l'appliance NetScaler, ou pour un seul serveur virtuel, à l'invite de commande, tapez :

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Exemple :

```
>stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
```



```
8  BRVSERV             10.10.1.1     80          HTTP          DOWN       0/s
          0/s
9  LBVIP            10.102.29.66     80          HTTP            UP       0/s
          0/s
10  Done
11
12
13 <!--NeedCopy-->
```

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Statistiques.
2. Si vous souhaitez afficher les statistiques d'un seul serveur virtuel, dans le volet de détails, sélectionnez le serveur virtuel, puis cliquez sur Statistiques.

Affichage des statistiques d'un service

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions au serveur en cours, etc. à l'aide des statistiques de service.

Pour consulter les statistiques d'un service à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
1 stat service <name>
2 <!--NeedCopy-->
```

Exemple :

```
1 stat service Service-HTTP-1
2 <!--NeedCopy-->
```

Pour consulter les statistiques d'un service à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Services > Statistiques.
2. Si vous souhaitez afficher les statistiques d'un seul service, sélectionnez-le et cliquez sur Statistiques.

Équilibrage de charge de serveur global

May 5, 2023

> **Remarques :**
>
> - À partir de la version 13.0 build 41.x, les déploiements mondiaux d'équilibrage de charge des serveurs (GSLB) à l'aide de l'appliance NetScaler sont entièrement conformes au jour du drapeau DNS 2019.
> - La fonctionnalité GSLB est incluse dans les licences des éditions NetScaler Advance et Premium. La licence optionnelle NetScaler est prise en charge avec l'édition Standard.

Les appliances NetScaler configurées pour GSLB assurent la reprise après sinistre et garantissent la disponibilité continue des applications en les protégeant contre les points de défaillance d'un réseau étendu. GSLB équilibre la charge entre les centres de données en dirigeant les demandes des clients vers le centre de données le plus proche ou le plus performant, ou vers les centres de données survivants en cas de panne.

Dans une configuration classique, un serveur DNS local envoie les demandes des clients à un serveur virtuel GSLB, auquel sont liés les services GSLB. Un service GSLB identifie un serveur virtuel d'équilibrage de charge ou de commutation de contenu, qui peut se trouver sur le site local ou distant. Si le serveur virtuel GSLB sélectionne un serveur virtuel d'équilibrage de charge ou de commutation de contenu sur un site distant, il envoie l'adresse IP du serveur virtuel au serveur DNS. Le serveur DNS l'envoie au client. Le client renvoie ensuite la demande au nouveau serveur virtuel à la nouvelle adresse IP.

Les entités GSLB que vous devez configurer sont les sites GSLB, les services GSLB, les serveurs virtuels GSLB, les serveurs virtuels d'équilibrage de charge ou de commutation de contenu et les services DNS (ADNS) faisant autorité. Vous devez également configurer MEP. Vous pouvez également configurer des vues DNS pour exposer différentes parties de votre réseau aux clients accédant au réseau depuis différents emplacements.

> **Remarque :**
>
> Pour tirer pleinement parti des fonctionnalités GSLB, utilisez des appliances ADC pour l'équilibrage de charge ou la commutation de contenu dans chaque centre de données, afin que votre configuration GSLB puisse utiliser le MEP propriétaire pour échanger les métriques du site.

Comment fonctionne le GSLB

Avec le DNS ordinaire, lorsqu'un client envoie une demande DNS (Domain Name System), il reçoit une liste d'adresses IP du domaine ou du service. En général, le client choisit la première adresse IP de la liste et établit une connexion avec ce serveur. Le serveur DNS utilise une technique appelée DNS Round Robin pour faire alterner les adresses IP de la liste. Il envoie la première adresse IP à la fin de la liste et promeut les autres après avoir répondu à chaque requête DNS. Cette technique assure une

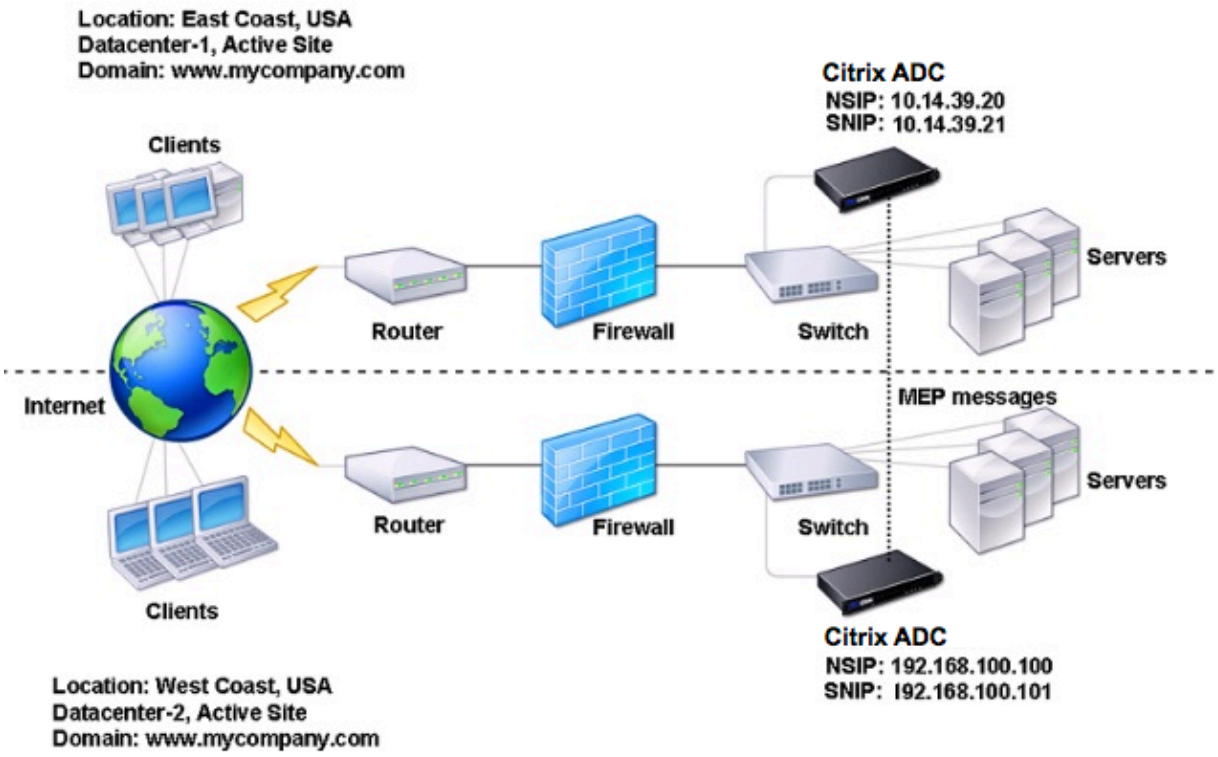
répartition égale de la charge, mais elle ne prend pas en charge la reprise après sinistre, l'équilibrage de charge basé sur la charge ou la proximité des serveurs, ou la persistance.

Lorsque vous configurez GSLB sur des appliances ADC et activez MEP, l'infrastructure DNS est utilisée pour connecter le client au centre de données qui répond le mieux aux critères définis. Les critères peuvent désigner les éléments suivants :

- Centre de données le moins chargé
- Centre de données le plus proche
- Centre de données qui répond le plus rapidement aux demandes depuis le site du client
- Une combinaison de ces mesures et de mesures SNMP.

Une appliance assure le suivi de l'emplacement, des performances, de la charge et de la disponibilité de chaque centre de données. Il utilise ces facteurs pour sélectionner le centre de données à envoyer la demande du client.

La figure suivante illustre une topologie GSLB de base.



Une configuration GSLB consiste en un groupe d'entités GSLB sur chaque appliance de la configuration. Ces entités incluent les sites GSLB, les services GSLB, les groupes de services GSLB, les serveurs virtuels GSLB, les serveurs d'équilibrage de charge, les serveurs de commutation de contenu et les services ADNS.

Types de déploiement GSLB

May 5, 2023

Les appliances NetScaler configurées pour l'équilibrage global de la charge des serveurs (GSLB) assurent la reprise après sinistre et garantissent la disponibilité continue des applications en les protégeant contre les points de défaillance d'un réseau étendu (WAN). GSLB peut équilibrer la charge entre les centres de données en dirigeant les demandes des clients vers le centre de données le plus proche ou le plus performant, ou vers les centres de données survivants en cas de panne.

Voici quelques-uns des types de déploiement GSLB typiques :

- Déploiement de sites actifs-actifs
- Déploiement de site actif-passif
- Déploiement de la topologie parent-enfant

Déploiement de sites actifs-actifs

May 5, 2023

Un site actif-actif se compose de plusieurs centres de données actifs. Les demandes des clients sont équilibrées de charge entre les datacenters actifs. Ce type de déploiement peut être utilisé lorsque vous avez besoin d'une distribution globale du trafic dans un environnement distribué.

Tous les sites d'un déploiement actif-actif sont actifs, et tous les services d'une application/domaine particulier sont liés au même serveur virtuel GSLB. Les sites échangent des mesures via le protocole MEP (Metrics Exchange Protocol). Les métriques de site échangées entre les sites incluent l'état de chaque serveur virtuel d'équilibrage de charge et de commutation de contenu, le nombre actuel de connexions, le débit de paquets actuel et l'utilisation actuelle de la bande passante. L'appliance NetScaler a besoin de ces informations pour effectuer un équilibrage de charge sur les sites.

Un déploiement actif-actif peut inclure un maximum de 32 sites GSLB, car MEP ne peut pas synchroniser plus de 32 sites. Aucun site de sauvegarde n'est configuré dans ce type de déploiement.

L'appliance NetScaler envoie les demandes des clients au site GSLB approprié, tel que déterminé par la méthode GSLB spécifiée dans la configuration GSLB.

Pour un déploiement actif-actif, vous pouvez configurer les méthodes GSLB suivantes.

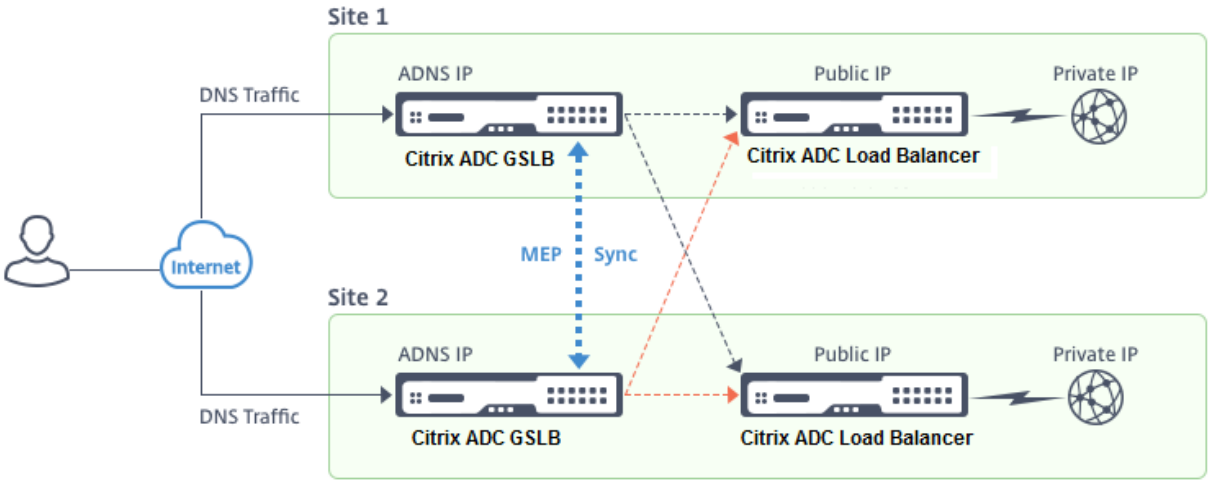
- Round Robin
- Connexions moindres
- Temps de réponse le plus faible
- Moins de bande passante

- Moins de paquets
- Hash IP source
- Chargement personnalisé
- Temps aller-retour (RTT)
- Proximité statique

> Remarque :
>
> - Si MEP est désactivé, les méthodes GSLB suivantes sont par défaut la méthode Round Robin.
>   - RTT
>   - Moins de connexions
>   - Moins de bande passante
>   - Moins de paquets
>   - Temps de réponse minimal
> - Dans la méthode GLSB de proximité statique, l'appliance envoie la demande à l'adresse IP du site qui correspond le mieux aux critères de proximité.
> - Dans la méthode Round Trip Time, les valeurs du temps aller-retour dynamique (RTT) servent à sélectionner l'adresse IP du site le plus performant. RTT est une mesure du retard dans le réseau entre le serveur DNS local du client et une ressource de données.

Topologie de centre de données actif-actif GSLB

Dans le diagramme, le site 1 et le site 2 sont des sites actifs de la DGGLSB.



Lorsque le client envoie une requête DNS, il atterrit sur l'un des sites actifs.

Si le site 1 reçoit la demande du client, le serveur virtuel GSLB du site 1 sélectionne un serveur virtuel d'équilibrage de charge ou de commutation de contenu et envoie l'adresse IP du serveur virtuel au serveur DNS, qui l'envoie au client. Le client renvoie ensuite la demande au nouveau serveur virtuel à la nouvelle adresse IP.

Comme les deux sites sont actifs, l'algorithme GSLB évalue les services des deux sites lorsqu'il effectue une sélection telle que déterminée par la méthode GSLB configurée.

Déploiement de site actif-passif

August 20, 2021

Un site actif-passif est constitué d'un centre de données actif et passif. Ce type de déploiement est idéal pour la reprise après sinistre.

Dans ce type de déploiement, certains sites (sites distants) sont réservés uniquement à la reprise après sinistre. Ces sites ne participent à aucune prise de décision tant que tous les sites actifs ne sont pas en panne. Un site passif ne devient opérationnel que si un événement de sinistre déclenche un basculement.

Une fois que vous avez configuré le centre de données principal, répliquez la configuration du centre de données de sauvegarde et désignez-le comme site GSLB passif en désignant un serveur virtuel GSLB sur ce site comme serveur virtuel de sauvegarde.

Un déploiement actif-passif peut inclure un maximum de 32 sites GSLB, car le MEP ne peut pas synchroniser plus de 32 sites.

Pour un déploiement actif-passif, vous pouvez configurer les méthodes GSLB suivantes.

- Round Robin
- Connexions moindres
- Temps de réponse le plus faible
- Moins de bande passante
- Moins de paquets
- Hash IP source
- Chargement personnalisé
- Temps aller-retour (RTT)
- Proximité statique

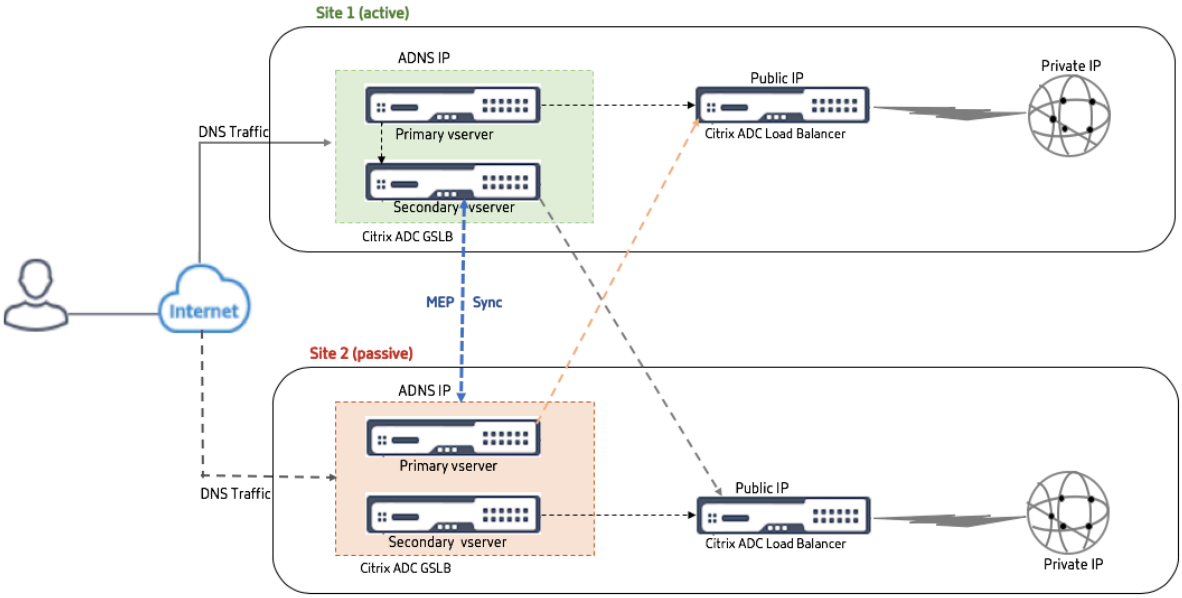
Remarque :

- Si MEP est désactivé, les méthodes d'algorithme suivantes sont par défaut Round Robin.
  - RTT
  - Connexions moindres
  - Moins de bande passante
  - Moins de paquets
  - Temps de réponse le plus faible

- Dans la méthode GLSB de proximité statique, l'appliance envoie la demande à l'adresse IP du site qui correspond le mieux aux critères de proximité.
- Dans la méthode Round Trip Time, les valeurs de temps d'aller-retour dynamique (RTT) sont de sélectionner l'adresse IP du site le plus performant. RTT est une mesure du retard dans le réseau entre le serveur DNS local du client et une ressource de données.

Topologie de centre de données actif-passif GSLB

Dans le diagramme, le site 1 est un site actif et le site 2 est un site passif, dont la configuration est identique à celle du Site 1.



Si le site 1 tombe en panne, le site 2 devient opérationnel.

Lorsque le client envoie une demande DNS, la demande peut atterrir sur n'importe lequel des sites. Cependant, les services sont sélectionnés uniquement à partir du site actif (Site1) tant qu'il est UP.

Les services du site passif (Site 2) ne sont sélectionnés que si le site actif (Site 1) est DOWN.

Déploiement de la topologie parent-enfant à l'aide du protocole MEP

May 5, 2023

NetScaler GSLB assure l'équilibrage global de la charge des serveurs et la reprise après sinistre en créant des connexions maillées entre tous les sites concernés et en prenant des décisions intelligentes en matière d'équilibrage de charge. Chaque site communique avec les autres pour échanger

des métriques de serveur et de réseau via le Metric Exchange Protocol (MEP), à intervalles réguliers. Cependant, avec l'augmentation du nombre de sites homologues, le volume de trafic MEP augmente de façon exponentielle en raison de la topologie maillée. Pour résoudre ce problème, vous pouvez utiliser une topologie parent-enfant. La topologie parent-enfant prend également en charge des déploiements plus importants. En plus des 32 sites parents, vous pouvez configurer 1024 sites enfants.

La topologie parent-enfant GSLB est une conception hiérarchique à deux niveaux présentant les caractéristiques suivantes :

- Au niveau supérieur se trouvent les sites parents, qui entretiennent des relations avec les pairs avec d'autres parents.
- Chaque parent peut avoir plusieurs sites enfants.
- Chaque site parent échange des informations de santé avec ses sites enfants et avec d'autres sites parents.
- Un site enfant communique uniquement avec son site parent.
- Dans une relation parent-enfant pour GSLB, seul le site parent répond aux requêtes ADNS. Les sites enfants agissent comme des sites d'équilibrage de charge normaux.
- Configurez un service ADNS ou un serveur virtuel d'équilibrage de charge DNS uniquement sur le site parent.
- Un site parent peut avoir une configuration GSLB normale, c'est-à-dire des services provenant de sites locaux et de tous les sites distants, mais un site enfant ne peut avoir que des services locaux. En outre, seuls les sites parents ont des serveurs virtuels GSLB configurés.

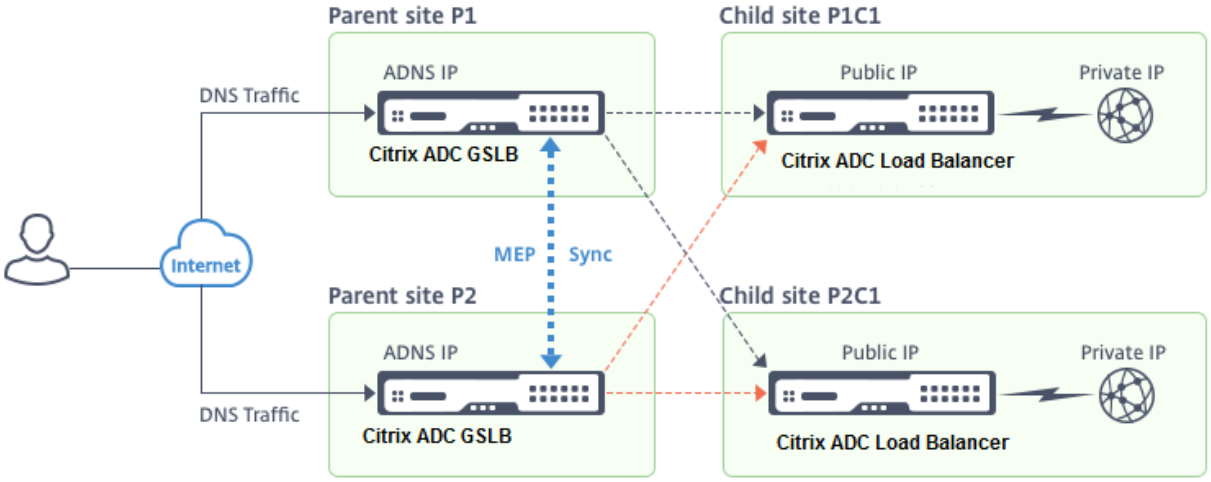
> **Remarque**
>
> - Dans une topologie parent-enfant, l'échange de mesures de site est initié à partir de la plus faible des deux adresses IP. Toutefois, à partir de la version 11.1 build 51.x de NetScaler, les sites parents établissent des connexions avec les sites enfants, et non l'inverse. Parce que les sites parents contiennent des informations sur tous les sites enfants de la configuration GSLB.

- Dans une connexion parent-parent, l'échange de mesures de site est toujours initié à partir de l'adresse IP inférieure de deux adresses IP.
- Dans une topologie parent-enfant, les services GSLB ne doivent pas toujours être configurés sur un site enfant. Toutefois, si vous avez d'autres configurations, telles que l'authentification client, l'insertion d'adresse IP du client ou toute autre exigence spécifique à SSL, vous devez ajouter un service GSLB explicite sur le site enfant et le configurer en conséquence.
- Dans une topologie parent-enfant, le site parent et le site enfant peuvent se trouver sur différentes versions du logiciel NetScaler. Toutefois, pour utiliser l'option GSLB Automatic-ConfigSync afin de synchroniser la configuration entre les sites parents, tous les sites parents doivent utiliser les mêmes versions du logiciel NetScaler. Si vous n'utilisez pas l'option Auto-

maticConfigSync, le site parent et le site enfant peuvent utiliser différentes versions du logiciel NetScaler, mais assurez-vous de ne pas utiliser les nouvelles fonctionnalités de la dernière version. Cela s'applique également, en général, à deux nœuds NetScaler participant au GSLB.

Topologie parent-enfant de base

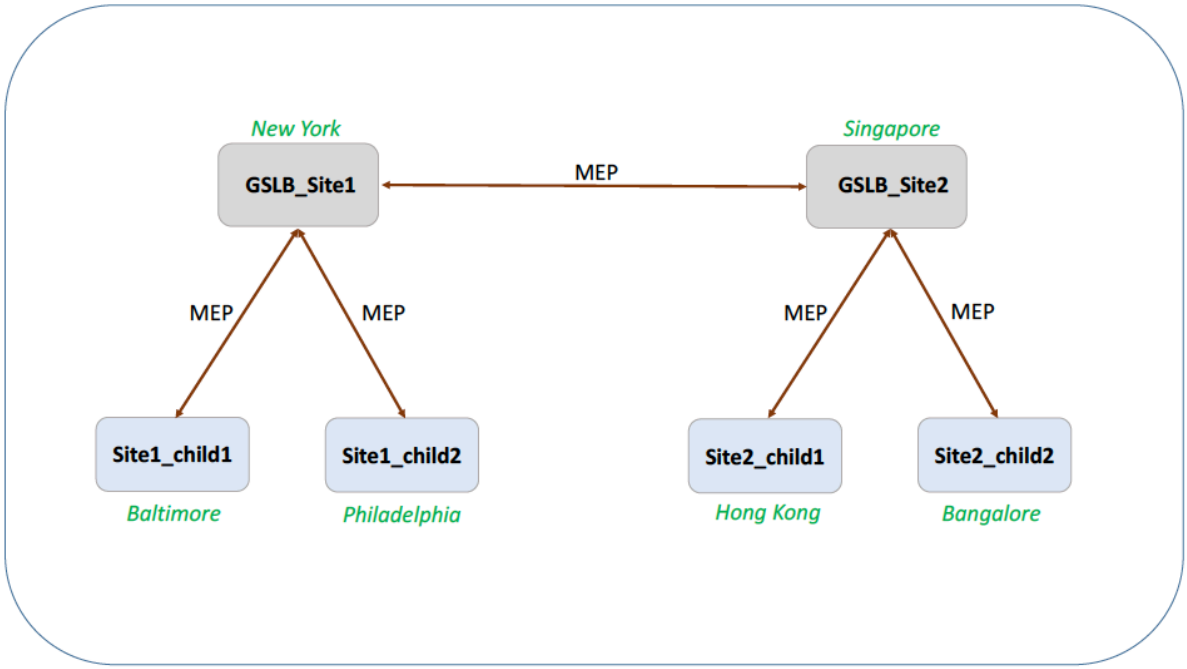
Dans le diagramme, SiteP1 et SiteP2 sont des sites parents dans une relation homologue. Les sites P1C1 et P2C1 sont les sites enfants de P1 et P2 respectivement.



Configuration d'une configuration parent-enfant pour GSLB

Si un pare-feu est configuré sur un site GSLB, assurez-vous que le port 3011 est ouvert.

Le schéma suivant présente un exemple de configuration parent-enfant.



- La configuration d'un site enfant inclut le site enfant et son site parent, mais aucun autre site parent ou enfant.
- Les mesures réseau, telles que les informations de RTT et de session de persistance, sont synchronisées uniquement sur les sites parents. Par conséquent, les paramètres tels que NWMetricExchange et SessionExchange sont désactivés par défaut sur tous les sites enfants.
- Pour vérifier la bonne configuration parent-enfant, vérifiez les états de tous les services GSLB liés aux sites parents.

Pour configurer une configuration parent-enfant pour GSLB à l'aide de l'interface de ligne de commande :

1. Sur chaque site parent, configurez tous ses sites enfants, ses sites parents homologues et les sites enfants associés aux sites homologues :

   Utilisez la commande suivante lors de l'ajout d'un site parent :

   ```
   add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
      ipv6_addr|*>]
   <!--NeedCopy-->
   ```

   Utilisez la commande suivante lors de l'ajout d'un site enfant :

   ```
   add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
      ipv6_addr|*>] [-parentSite <string>]
   <!--NeedCopy-->
   ```

2. Sur les sites enfants, configurez le site enfant et associez également le site enfant à son parent :

> **Remarque :**
>
> Configurez correctement l'association du site parent et du site enfant. Par exemple, vous devez configurer Site1_Child1 avec GSLB_Site1. Vous ne pouvez pas configurer Site1_Child1 avec GSLB_Site2.

Utilisez la commande suivante pour configurer le site parent auquel le site enfant est associé :

```
add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
    ipv6_addr|*>]
<!--NeedCopy-->
```

Utilisez la commande suivante pour ajouter un site enfant et l'associer à son site parent :

```
add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
    ipv6_addr|*>] [-parentSite <string>]
<!--NeedCopy-->
```

Pour obtenir un exemple complet de configuration parent-enfant, à l'aide de l'interface de ligne de commande, reportez-vous à Exemple de configuration parent-enfant complète, à l'aide de l'interface de ligne de commande.

> **Remarque**
>
> Si l'adresse IP du serveur virtuel d'équilibrage de charge est une adresse IP privée et que l'adresse IP publique est différente de cette adresse IP, vous devez configurer un service GSLB pour le serveur virtuel d'équilibrage de charge local sur le site enfant. Cela est nécessaire pour la collecte de statistiques entre le site parent et le site enfant.
>
> Sur le site enfant, à l'invite de commandes, tapez :
>
> `add gslb service <name> <private IP/lb vserver IP> http 80 -sitename <childsite name> -publicip <public IP of LB vserver>`
>
> **Exemple :**
>
> `add gslb service Service-GSLB 192.168.1.3 http 80 -GSLB_Site11 site 11_lb1 172.16.1.1`
>
> Où 192.168.1.3 est une adresse IP privée du serveur virtuel d'équilibrage de charge et 172.16.1.1 est une adresse IP publique du serveur virtuel d'équilibrage de charge.

Sauvegarde d'un site parent

Remarque : Cette fonctionnalité a été introduite dans NetScaler version 11.1 build 51.x. Pour utiliser la topologie du site parent de sauvegarde, assurez-vous que le site parent et les sites enfants se trouvent sur NetScaler 11.1 build 51.x et versions ultérieures.

La topologie de site parent de sauvegarde est utile dans les scénarios dans lesquels de nombreux sites enfants sont associés à un site parent. Si ce site parent tombe en panne, tous ses sites enfants deviennent indisponibles. Pour éviter cela, vous pouvez désormais configurer un site parent de sauvegarde auquel les sites enfants peuvent se connecter si le site parent d'origine est ARRÊTÉ. Le site parent envoie la liste parente de sauvegarde aux sites enfants par le biais des messages MEP.

Lorsqu'un site parent est DOWN, les autres sites parents du GSLB apprennent qu'un site parent particulier est DOWN via MEP car MEP vers ce site parent est DOWN. Les autres sites parents de la configuration GSLB recherchent la chaîne de sauvegarde du parent homologue. Le site parent ayant la préférence la plus élevée adopte les sites enfants du parent qui est tombé en panne. Le nouveau parent initie ensuite une connexion avec le site enfant. Un site enfant peut accepter ou rejeter la connexion après avoir évalué ses connexions existantes et les informations de la liste de sauvegarde. L'adoption des sites enfants par le parent de sauvegarde prend quelques secondes.
Lorsque le site parent d'origine est rétabli, il essaie d'établir des connexions avec ses sites enfants qui ont migré vers un autre parent. Lorsqu'une tentative de connexion aboutit, le site enfant est réaffecté à son site parent d'origine.

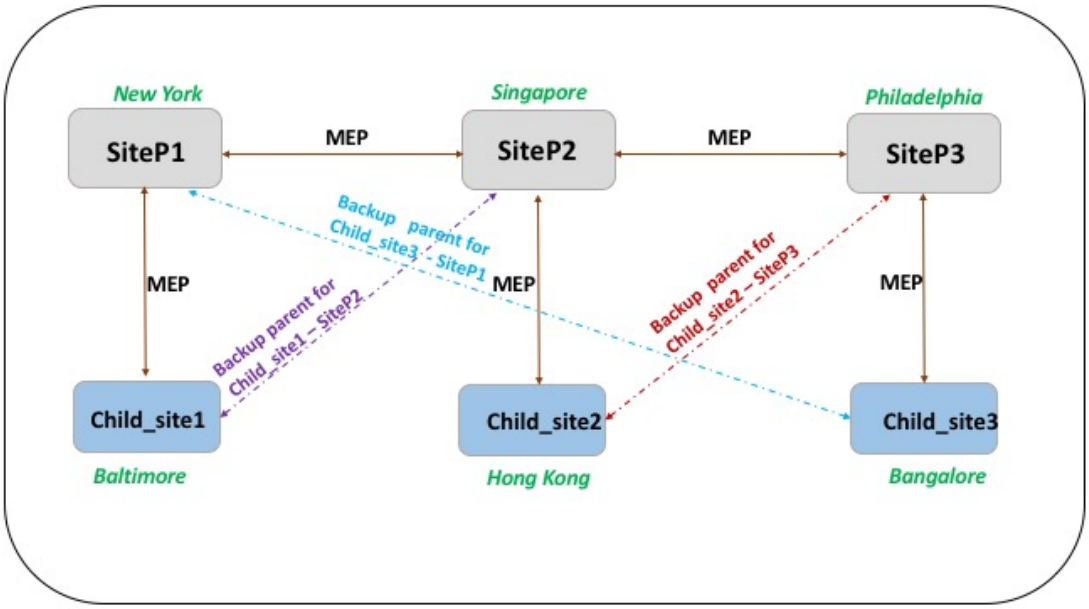
Remarque :

- Seuls les sites parents peuvent être configurés en tant que sauvegardes, et cette configuration ne peut être effectuée que sur le site parent.
- Tous les sites enfants utilisent le jeu parent de sauvegarde.
- La synchronisation est effectuée uniquement sur les sites parents. La configuration des sites enfants GSLB n'est pas affectée par la synchronisation. En effet, les configurations de site parent et de site enfant ne sont pas identiques. La configuration des sites enfants comprend uniquement ses propres informations et celle de son site parent. En outre, les services GSLB ne doivent pas toujours être configurés dans les sites enfants.

Considérez la configuration illustrée dans la figure suivante, dans laquelle :

- SiteP1, SiteP2 et SiteP3 sont les sites parents.
- Child_Site1, Child_Site2 et Child_Site3 sont les sites enfants de SiteP1, SiteP2 et SiteP3 respectivement.
- sites parents de sauvegarde ;
  - Parents de sauvegarde SiteP1 : SiteP2 (préférence supérieure) et SiteP3
  - Parents de sauvegarde SiteP2 : SiteP3 (préférence supérieure) et SiteP1
  - Parents de sauvegarde SiteP3 : SiteP1 (préférence supérieure) et SiteP2

Remarque : À des fins d'illustration, la figure montre un seul parent de sauvegarde pour chaque site parent.



La liste suivante récapitule le comportement des sites parents et enfants dans différents scénarios :

- Scénario 1 : le site P1 tombe en panne.
  - SiteP2 et SiteP3 détectent que la connexion MEP de SiteP1 est DOWN. SiteP2 est plus haut dans la liste de préférences des parents de sauvegarde pour SiteP1, il essaie donc d'établir une connexion à Child_Site1. SiteP3 suppose que Child_Site1 est désormais le site enfant du site SiteP2 parent.
  - SiteP2 envoie à Child_Site1 la liste des parents de sauvegarde de SiteP1 (SiteP2 et SiteP3) à Child_Site1. Child_Site1 utilise la liste pour décider d'accepter ou de rejeter la connexion à partir de SiteP2. Il accepte la connexion et devient enfant de SiteP2.
  - Lorsque SiteP1 est rétabli, il envoie une demande de connexion à Child_Site1. La nouvelle demande est prioritaire et Child_site 1 migre vers SiteP1.
- Scénario 2 : Seule la connexion MEP entre SiteP1 et SiteP2 a été interrompue. Child_Site1 rejette la demande de connexion de SiteP2, car son parent, SiteP1, est toujours actif.
- Scénario 3 : SiteP3 et Child_Site1 détectent que SiteP1 est DOWN, et la connexion MEP entre SiteP3 et SiteP2 est également DOWN. Cependant, SiteP2 détecte que SiteP1 est actif et que la connexion MEP entre SiteP1 et SiteP2 est active.
  - SiteP2 ne prend aucune mesure.
  - SiteP3 vérifie la liste de sauvegarde de SiteP1 et constate que SiteP2 a une préférence plus élevée que SiteP3. Mais SiteP2 est DOWN, donc SiteP3 essaie d'établir une connexion avec Child_Site1. Child_Site1 a détecté que SiteP1 est DOWN, il accepte donc la demande de connexion de SiteP3.

- Maintenant, la connexion entre SiteP1 et SiteP2 est INTERROMPUE. SiteP2 vérifie la liste de sauvegarde de SiteP1 et se trouve comme la sauvegarde préférée. Il essaie donc de se connecter à Child_Site1. Child_Site1 évalue la nouvelle demande de connexion en fonction de la liste de SiteP1 et trouve SiteP2 comme la sauvegarde préférée, de sorte qu'il migre vers SiteP2 à partir de SiteP3.

Pour configurer un site parent de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set gslb site <sitename> -backupParentlist <bkp_site1> <bkp_site2> ... <
   bkp_site5>
<!--NeedCopy-->
```

<sitename> est le site parent actuel.

Exemple :

Pour le site parent (SiteP1), les sites (SiteP2 et SiteP3) sont configurés en tant que sites parents de sauvegarde.

```
set gslb site SiteP1 -backupParentlist SiteP2 SiteP3
<!--NeedCopy-->
```

Remarque :

- Vous ne pouvez pas ajouter de nouveau site en tant que parent de sauvegarde. Vous devez d'abord ajouter tous les sites, puis configurer le site en tant que parent de sauvegarde.
- Pour supprimer un parent de sauvegarde, vous devez utiliser la commande unset, qui désactive tous les sites précédemment configurés en tant que sites parents de sauvegarde.

Pour configurer un site parent de sauvegarde à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Sites**.
2. Ajoutez un nouveau site ou sélectionnez un site existant.
3. Sélectionnez la zone d'option **Sauvegarder les sites parents** lors de la création ou de la configuration du site GSLB.

Entités de configuration GSLB

May 5, 2023

Une configuration GSLB consiste en un groupe d'entités GSLB sur chaque appliance de la configuration. Ces entités sont notamment les suivantes :

- Sites GSLB
- Services GSLB
- Serveurs virtuels GSLB
- Serveurs virtuels d'équilibrage de charge ou de commutation de contenu
- Services ADNS
- VIP DNS

Sites GSLB

Une configuration GSLB classique comprend des centres de données, chacun étant doté de divers dispositifs réseau qui peuvent être des appareils NetScaler ou non. Les centres de données sont appelés sites GSLB. Chaque site GSLB est géré par une appliance NetScaler locale sur ce site. Chacune de ces appliances traite son propre site comme site local et tous les autres sites, gérés par d'autres appliances, comme des sites distants.

Si l'appliance qui gère un site est la seule appliance NetScaler de ce centre de données, le site GSLB hébergé sur cette appliance fait office d'espace comptable à des fins d'audit, car aucune métrique ne peut être collectée. Cela se produit généralement lorsque l'appliance est utilisée uniquement pour le GSLB et que d'autres produits du centre de données sont utilisés pour l'équilibrage de charge ou la commutation de contenu.

Relations entre les sites GSLB

Le concept de sites est au cœur des implémentations de NetScaler GSLB. Sauf indication contraire, les sites établissent une relation de pair entre eux. Cette relation est d'abord utilisée pour échanger des informations de santé, puis pour répartir la charge selon l'algorithme sélectionné. Toutefois, dans de nombreuses situations, il n'est pas souhaitable d'établir une relation entre les pairs entre tous les sites du GSLB. Les raisons de l'absence d'une implémentation entièrement par les pairs peuvent être les suivantes :

- Pour séparer clairement les sites GSLB. Par exemple, pour séparer les sites qui participent à la résolution des requêtes DNS des sites de gestion du trafic.
- Réduire le volume du trafic MEP (Metric Exchange Protocol), qui augmente de façon exponentielle avec l'augmentation du nombre de sites homologues.

Ces objectifs peuvent être atteints en utilisant les sites GSLB parents et enfants.

Services GSLB

Un service GSLB est généralement une représentation d'un serveur virtuel d'équilibrage de charge ou de commutation de contenu, bien qu'il puisse représenter n'importe quel type de serveur virtuel. Le service GSLB identifie l'adresse IP, le numéro de port et le type de service du serveur virtuel. Les services GSLB sont liés aux serveurs virtuels GSLB sur les appliances NetScaler qui gèrent les sites GSLB. Un service GSLB lié à un serveur virtuel GSLB dans le même centre de données est local au serveur virtuel GSLB. Un service GSLB lié à un serveur virtuel GSLB dans un centre de données différent est distant de ce serveur virtuel GSLB.

> **Remarque**
>
> Les sites et les services sont intrinsèquement liés pour indiquer la proximité entre les deux. En d'autres termes, tous les services doivent appartenir à un site et sont supposés se trouver au même endroit que le site GSLB à des fins de proximité. De même, les services et les serveurs virtuels sont liés, de sorte que la logique est liée aux ressources disponibles.

Serveurs virtuels GSLB

Un ou plusieurs services GSLB sont liés à un serveur virtuel GSLB et répartit la charge du trafic entre ces services. Il évalue les méthodes GSLB configurées (algorithmes) pour sélectionner le service approprié auquel envoyer une demande client. Étant donné que les services GSLB peuvent représenter des serveurs locaux ou distants, la sélection du service GSLB optimal pour une requête a pour effet de sélectionner le centre de données qui doit servir la demande client.

Le domaine pour lequel l'équilibrage de charge global du serveur est configuré doit être lié au serveur virtuel GSLB, car un ou plusieurs services liés au serveur virtuel répondront aux demandes effectuées pour ce domaine.

Contrairement aux autres serveurs virtuels configurés sur une appliance NetScaler, un serveur virtuel GSLB ne possède pas sa propre adresse IP virtuelle (VIP).

Serveurs virtuels d'équilibrage de charge ou de commutation de contenu

Un serveur virtuel d'équilibrage de charge ou de commutation de contenu représente un ou plusieurs serveurs physiques sur le réseau local. Les clients envoient leurs demandes à l'adresse IP virtuelle (VIP) du serveur virtuel d'équilibrage de charge ou de commutation de contenu, et le serveur virtuel répartit la charge entre les serveurs physiques. Après qu'un serveur virtuel GSLB sélectionne un service GSLB représentant un serveur virtuel d'équilibrage de charge ou de commutation de contenu local ou distant, le client envoie la demande à l'adresse VIP de ce serveur virtuel.

Pour plus d'informations sur l'équilibrage de charge ou les serveurs et services virtuels de commutation de contenu, voir Équilibrage de charge ou commutation de contenu.

Services ADNS

Un service ADNS est un type particulier de service qui répond uniquement aux demandes DNS pour les domaines pour lesquels l'appliance NetScaler fait autorité. Lorsqu'un service ADNS est configuré, l'appliance possède l'adresse IP du service ADNS et en fait la publicité. Lors de la réception d'une demande DNS par un service ADNS, l'appliance vérifie la présence d'un serveur virtuel GSLB lié à ce domaine. Si un serveur virtuel GSLB est lié au domaine, il est interrogé pour obtenir la meilleure adresse IP à laquelle envoyer la réponse DNS.

VIP DNS

Une adresse IP virtuelle DNS est une adresse IP virtuelle (VIP) qui représente un serveur virtuel DNS d'équilibrage de charge sur l'appliance NetScaler. Les demandes DNS pour les domaines pour lesquels l'appliance NetScaler fait autorité peuvent être envoyées à un DNS VIP.

Méthodes GSLB

May 5, 2023

Contrairement aux serveurs DNS traditionnels qui répondent simplement avec les adresses IP des serveurs configurés, une appliance NetScaler configurée pour le GSLB répond avec les adresses IP des services, telles que déterminées par la méthode GSLB configurée. Par défaut, le serveur virtuel GSLB est défini sur la méthode de connexion minimale. Si tous les services GSLB sont indisponibles, l'appliance répond avec les adresses IP de tous les services GSLB configurés.

Les méthodes GSLB sont des algorithmes que le serveur virtuel GSLB utilise pour sélectionner le service GSLB le plus performant. Une fois le nom d'hôte indiqué dans l'adresse Web résolu, le client envoie le trafic directement à l'adresse IP du service résolu.

L'appliance NetScaler fournit les méthodes GSLB suivantes :

- Round Robin
- Connexions moindres
- Temps de réponse le plus faible
- Moins de bande passante
- Moins de paquets
- Hash IP source
- Chargement personnalisé
- Temps aller-retour (RTT)
- Proximité statique

Pour que les méthodes GSLB fonctionnent avec un site distant, MEP doit être activé ou des moniteurs explicites doivent être liés aux services distants. Si MEP est désactivé, les méthodes RTT, Least Connections, Least Bandwidth, Least Packets et Least Response Time sont définies par défaut sur Round Robin.

Les méthodes d'équilibrage de charge Static Proximity et RTT sont spécifiques au GSLB.

Spécification d'une méthode GSLB autre que la proximité statique ou la RTT dynamique

Pour plus d'informations sur la méthode Round Robin, Last Connections, Moindres Temps de réponse, Moins de bande passante, Moins de paquets, Hash IP source ou Charge personnalisée, reportez-vous à la section Équilibrage de charge.

Pour modifier la méthode GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb vserver <name> -lbMethod GSLBMethod
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -lbMethod ROUNDROBIN
<!--NeedCopy-->
```

Pour modifier la méthode GSLB à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB > Serveursvirtuels**.
2. **Dans le volet de détails, sélectionnez un serveur virtuel GSLB et cliquez sur Ouvrir.**
3. Dans la boîte de dialogue Configurer le serveur virtuel GSLB, sous l'onglet Méthode et persistance, sous Méthode, sélectionnez une méthode dans la liste Choisir une méthode.
4. Cliquez sur **OK**et vérifiez que la méthode sélectionnée apparaît sous Détails au bas de l'écran.

Algorithmes GSLB

May 5, 2023

Les algorithmes suivants sont pris en charge pour GSLB.

- **Round Robin** : lorsqu'un serveur virtuel GSLB est configuré pour utiliser la méthode Round Robin, il fait pivoter en permanence la liste des services qui lui sont liés. Lorsque le serveur virtuel reçoit une demande, il attribue la connexion au premier service de la liste, puis déplace ce service vers le bas de la liste.
- **Temps de réponse minimal** : lorsque le serveur virtuel GSLB est configuré pour utiliser la méthode du temps de réponse le plus faible, il sélectionne le service ayant la valeur la plus faible. Où, valeur la plus basse = connexions actives actuelles X temps de réponse moyen.

  Vous pouvez configurer cette méthode uniquement pour les services HTTP et SSL (Secure Sockets Layer). Le temps de réponse (également appelé Time to First Byte, ou TTFB) est l'intervalle de temps entre l'envoi d'un paquet de demande à un service et la réception du premier paquet de réponse du service. L'appliance NetScaler utilise le code de réponse 200 pour calculer le TTFB.
- **Moins de connexions** : lorsqu'un serveur virtuel GSLB est configuré pour utiliser l'algorithme (ou la méthode) GSLB le moins de connexions, il sélectionne le service avec le moins de connexions actives. Il s'agit de la méthode par défaut, car, dans la plupart des cas, elle fournit les meilleures performances.
- **Bande passante minimale** : Un serveur virtuel GSLB configuré pour utiliser la méthode de la bande passante la plus faible sélectionne le service qui dessert actuellement le moins de trafic, mesuré en mégabits par seconde (Mbps).
- **Moins de paquets** : un serveur virtuel GSLB configuré pour utiliser la méthode du moins de paquets sélectionne le service qui a reçu le moins de paquets au cours des 14 dernières secondes.
- **Hachage IP source** : Un serveur virtuel GSLB configuré pour utiliser la méthode de hachage IP source utilise la valeur hachée de l'adresse IPv4 ou IPv6 du client pour sélectionner un service. Pour diriger toutes les demandes provenant d'adresses IP source appartenant à un réseau particulier vers un serveur de destination spécifique, vous devez masquer l'adresse IP source. Pour les adresses IPv4, utilisez le paramètre NetMask. Pour les adresses IPv6, utilisez le paramètre V6NetMaskLength.
- **Charge personnalisée** : L'équilibrage de charge personnalisé est effectué sur les paramètres du serveur tels que l'utilisation du processeur, la mémoire et le temps de réponse. Lorsque vous utilisez la méthode de chargement personnalisée, l'appliance NetScaler sélectionne généralement un service qui ne gère aucune transaction active. Si tous les services de la configuration GSLB gèrent des transactions actives, l'appliance sélectionne le service dont la charge est la plus faible. Un type spécial de moniteur, connu sous le nom de moniteur de charge, calcule la charge sur chaque service du réseau. Les moniteurs de charge ne marquent pas l'état d'un service, mais ils retirent les services de la décision GSLB lorsque ces services ne sont pas UP.
- **Proximité statique** : GSLB utilise une base de données de proximité statique basée sur les adresses IP pour déterminer la proximité entre le serveur DNS local du client et les sites GSLB.

L'appliance NetScaler répond avec l'adresse IP du site qui correspond le mieux aux critères de proximité.

- **Temps aller-retour** : Le RTT est une mesure du temps ou du délai dans le réseau entre le serveur DNS local du client et une ressource de données. L'appliance NetScaler sonde le serveur DNS local du client et recueille des informations métriques RTT. L'appliance utilise ensuite cette métrique pour prendre sa décision d'équilibrage de charge. L'équilibrage de charge global des serveurs surveille l'état en temps réel du réseau et dirige dynamiquement la demande du client vers le centre de données présentant la valeur RTT la plus faible.
- **Méthode API** : GSLB utilise une API REST pour déterminer le service GSLB le plus performant. Dans la méthode API, lorsque GSLB reçoit une requête DNS d'un client, il évalue la demande par rapport à la règle spécifiée.

Pour plus de détails, voir Équilibrage de charge.

Proximité statique

May 5, 2023

La méthode de proximité statique pour GSLB utilise une base de données de proximité statique basée sur des adresses IP pour déterminer la proximité entre le serveur DNS local du client et les sites GSLB. L'appliance NetScaler répond avec l'adresse IP du site qui correspond le mieux aux critères de proximité.

Si deux sites GSLB ou plus situés à des emplacements géographiques différents diffusent le même contenu, l'appliance NetScaler gère une base de données de plages d'adresses IP et utilise cette base de données pour prendre des décisions concernant les sites GSLB vers lesquels diriger les demandes des clients entrantes.

Pour que la méthode de proximité statique fonctionne, vous devez soit configurer l'appliance NetScaler pour qu'elle utilise une base de données de proximité statique existante remplie via un fichier d'emplacement, soit ajouter des entrées personnalisées à la base de données de proximité statique. Après avoir ajouté des entrées personnalisées, vous pouvez définir leurs qualificatifs de localisation. Après avoir configuré la base de données, vous êtes prêt à spécifier la proximité statique comme méthode GSLB.

Pour plus d'informations sur la configuration de la proximité statique, reportez-vous à la section Configuration de la proximité statique.

Méthode de temps aller-retour dynamique

May 5, 2023

Le temps d'aller-retour dynamique (RTT) est une mesure du temps ou du délai sur le réseau entre le serveur DNS local du client et une ressource de données. Pour mesurer le RTT dynamique, l'appliance NetScaler sonde le serveur DNS local du client et recueille des informations métriques RTT. L'appliance utilise ensuite cette métrique pour prendre sa décision d'équilibrage de charge. L'équilibrage de charge global des serveurs surveille l'état en temps réel du réseau et dirige dynamiquement la demande du client vers le centre de données présentant la valeur RTT la plus faible.

Lorsque la demande DNS d'un client pour un domaine parvient à l'appliance NetScaler configurée en tant que DNS faisant autorité pour ce domaine, l'appliance utilise la valeur RTT pour sélectionner l'adresse IP du site le plus performant à envoyer en réponse à la demande DNS.

L'appliance NetScaler utilise différents mécanismes, tels que la demande ou la réponse d'écho ICMP (PING), l'UDP et le protocole TCP pour collecter les métriques RTT relatives aux connexions entre le serveur DNS local et les sites participants. L'appliance envoie d'abord une sonde ping pour déterminer le RTT. Si la sonde ping échoue, une sonde DNS UDP est utilisée. Si cette sonde échoue également, l'appliance utilise une sonde DNS TCP.

Ces mécanismes sont représentés sur l'appliance NetScaler sous la forme de moniteurs d'équilibrage de charge et sont facilement identifiables grâce à leur utilisation du préfixe « ldns ». Les trois écrans, dans leur ordre par défaut, sont les suivants :

- `ldns-ping`
- `ldns-dns`
- `ldns-tcp`

Ces moniteurs sont intégrés à l'appliance et sont réglés sur des paramètres sécurisés par défaut. Mais ils sont personnalisables comme n'importe quel autre moniteur de l'appliance.

Vous pouvez modifier l'ordre par défaut en le définissant explicitement en tant que paramètre GSLB. Par exemple, pour définir l'ordre dans lequel la requête DNS UDP sera suivie du PING puis du TCP, tapez la commande suivante :

```
1 set gslb parameter -ldnsprobeOrder DNS PING TCP
2 <!--NeedCopy-->
```

À moins qu'elles n'aient été personnalisées, l'appliance NetScaler effectue des tests UDP et TCP sur le port 53. Toutefois, contrairement aux moniteurs d'équilibrage de charge classiques, les sondes n'ont pas besoin d'être couronnées de succès pour fournir des informations RTT valides. Les messages

d'indisponibilité du port ICMP, les réinitialisations TCP et les réponses d'erreur DNS, qui constituent généralement un échec, sont tous acceptables pour le calcul de la valeur RTT.

Une fois les données RTT compilées, l'appliance utilise le protocole propriétaire d'échange de métriques (MEP) pour échanger des valeurs RTT entre les sites participants. Après avoir calculé les métriques RTT, l'appliance trie les valeurs RTT pour identifier le centre de données présentant la meilleure (la plus petite) métrique RTT. «

Si les informations RTT ne sont pas disponibles (par exemple, lorsque le serveur DNS local d'un client accède au site pour la première fois), l'appliance NetScaler sélectionne un site en utilisant la méthode du round robin et dirige le client vers le site.

Pour configurer la méthode dynamique, vous devez configurer le serveur virtuel GSLB du site pour le RTT dynamique. Vous pouvez également définir l'intervalle auquel les serveurs DNS locaux sont sondés à une valeur autre que la valeur par défaut.

Configurer un serveur virtuel GSLB pour le RTT dynamique

Pour configurer un serveur virtuel GSLB pour le RTT dynamique, vous devez spécifier la méthode d'équilibrage de charge RTT.

L'appliance NetScaler valide régulièrement les informations de synchronisation pour un serveur local donné. Si une modification de la latence dépasse le facteur de tolérance configuré, l'appliance met à jour sa base de données avec les nouvelles informations de synchronisation et envoie la nouvelle valeur à d'autres sites GSLB en effectuant un échange MEP. Le facteur de tolérance par défaut est de 5 millisecondes (ms).

Le facteur de tolérance RTT doit être le même dans tout le domaine GSLB. Si vous le modifiez pour un site, vous devez configurer des facteurs de tolérance RTT identiques sur toutes les appliances NetScaler déployées dans le domaine GSLB.

Pour configurer un serveur virtuel GSLB pour le RTT dynamique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb vserver <name> -lbMethod RTT -tolerance <value>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -lbMethod RTT -tolerance 10
<!--NeedCopy-->
```


Pour configurer un serveur virtuel GSLB pour le RTT dynamique à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel.

Définissez l'intervalle d'analyse des serveurs DNS locaux

L'appliance NetScaler utilise différents mécanismes, tels que la demande ou la réponse d'écho ICMP (PING), le TCP et l'UDP pour obtenir des métriques RTT pour les connexions entre le serveur DNS local et les sites GSLB participants. Par défaut, l'appliance utilise un moniteur de ping et sonde le serveur DNS local toutes les 5 secondes. L'appliance attend ensuite la réponse pendant 2 secondes. Si aucune réponse n'est reçue dans ce délai, il utilise le moniteur DNS TCP pour l'analyse.

Vous pouvez toutefois modifier l'intervalle de temps pour sonder le serveur DNS local en fonction de votre configuration.

Pour modifier l'intervalle de sondage à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb monitor <monitorName> <type> -interval <integer> <units> -
   resptimeout <integer> <units>
<!--NeedCopy-->
```

Exemple :

```
set lb monitor ldns-tcp LDNS-TCP -interval 10 sec -resptimeout 5 sec
<!--NeedCopy-->
```

Pour modifier l'intervalle de sondage à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**, puis double-cliquez sur le moniteur que vous souhaitez modifier (par exemple, ping).

Méthode API

June 2, 2023

Vous pouvez utiliser la méthode API pour déterminer le service GSLB le plus performant. La méthode API pour GSLB utilise une API REST pour déterminer le service GSLB le plus performant.

Dans la méthode API, lorsque GSLB reçoit une requête DNS d'un client, il évalue la demande par rapport à la règle spécifiée. Si GSLB rencontre l'expression de légende HTTP SYS.HTTP_CALLOUT (<name>), il appelle une requête d'API REST à destination d'un agent de légende HTTP. GSLB utilise la réponse de l'agent de légende HTTP pour choisir le service le plus performant. Dans la réponse DNS, GSLB renvoie au client l'adresse IP du service le plus performant.

Pour configurer une méthode d'API GSLB à l'aide de l'interface de ligne de commande

Procédez comme suit pour configurer la méthode de l'API GSLB :

1. Configurez une légende HTTP.

   Pour plus d'informations, voir Configuration d'une légende HTTP.

   À l'invite de commande, tapez :

```
add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port <port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (GET | POST)] [-hostExpr <string>] [-urlStemExpr <string>] [-headers <name(value)> ...] [-parameters <name(value)> ...] [-bodyExpr <string>] [-fullReqExpr <string>] [-scheme (http | https)] [-resultExpr <string>] [-cacheForSecs <secs>] [-comment <string>]
<!--NeedCopy-->
```

   Exemple :

```
add policy httpCallout GSLB_Method_API -IPAddress 208.111.39.237 -port 443 -returnType TEXT -hostExpr  "\" hopx.gslb.com\ ""  -urlStemExpr  "\" /zones/1/customers/92395/apps/6/decision\ "" -headers Authorization( "Basic 19fbe6db-4332-4e3f-a8bc-ee47bdc726f8") -parameters ip(DNS.REQ.OPT.ECS.IP.TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme https -resultExpr  "HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).XPATH_JSON(xp%/providers/Val[1]/provider%)"  -cacheForSecs 30
<!--NeedCopy-->
```

2. Spécifiez la méthode d'API pour l'équilibrage de charge. GSLB évalue la demande DNS par rapport à la règle spécifiée.

   À l'invite de commande, tapez :

```
add gslb vserver <name> <serviceType>  [-lbMethod <lbMethod>] [-backupLBMethod <backupLBMethod>] -rule <expression>
<!--NeedCopy-->
```


Exemple :

```
add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN
    -rule  “sys.http_callout(GSLB_Method_API)”
<!--NeedCopy-->
```

Exemple de configuration pour intégrer GSLB et ITM en utilisant l’API comme méthode LB

Cette configuration permet à GSLB d’utiliser les aspects de visibilité sur Internet de la gestion intelligente du trafic (ITM) de Citrix pour déterminer le service GSLB le plus performant.

```
/* Enable ns features */

enable ns feature lb gslb cs

/* This is a named expression that is used in the HTTP callout, used
   for result expression. */

add policy expression exp1 "HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).
   XPATH_JSON(xp%/providers/Val[1]/provider%)"

/* This is a named expression that is used in HTTP callout, used for
   host expression. */

add policy expression exp2 ""hopx.cedexis.com""

/* This is the HTTP callout configured to request the ITM for the GSLB
   decision. */

add policy httpCallout ITM_OpenMix_API -IPAddress 208.111.39.237 -port
   80 -returnType TEXT -hostExpr exp2 -urlStemExpr ""/zones/1/customers
   /61770/apps/3/decision"" -headers Authorization("Basic a310697a-1d69
   -48bf-8f36-55742a8e894e") -parameters ip(DNS.REQ.OPT.ECS.IP.
   TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme http -
   resultExpr exp1 -cacheForSecs 30

/* Add service 1 */
add service sg1 98.136.103.24 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
    -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -
   svrTimeout 360 -CKA NO -TCPB NO -CMP NO

/* Add service 2 */
add service sg2 172.217.194.113 HTTP 80 -gslb NONE -maxClient 0 -maxReq
```



```
      0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180
    -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

/* Add ADNS service */

add service adns1 10.102.217.106 ADNS 53 -gslb NONE -maxClient 0 -
    maxReq 0 -cip DISABLED -usip NO -useproxyport NO -sp OFF -cltTimeout
     120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO

/* Add lb vserver 1 for service 1 */
add lb vserver lbvs1 HTTP 10.102.217.116 80 -persistenceType NONE -
    cltTimeout 180

/* Add lb vserver 2 for service 2 */
add lb vserver lbvs2 HTTP 10.102.217.117 80 -persistenceType NONE -
    cltTimeout 180

/* Bind service 1 to lb vserver 1 */

bind lb vserver lbvs1 sg1

/* Bind service 2 to lb vserver 2 */

bind lb vserver lbvs2 sg2

/* Configure API GSLB method on GSLB virtual server to call the HTTP
    callout. This HTTP callout requests the ITM for the GSLB decision
    and returns GSLB service name, which should serve the request. */

add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN -
    rule "sys.http_callout(ITM_OpenMix_API)" -tolerance 0 -ECS ENABLED

/* Add GSLB site */

add gslb site site1 10.102.217.106 -publicIP 10.102.217.106

/* Add GSLB service 1 */

add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai_1
    10.102.217.116 HTTP 80 -publicIP 10.102.217.116 -publicPort 80 -
    maxClient 0 -siteName site1 -sitePersistence HTTPRedirect -
    sitePrefix gs2. -cltTimeout 180 -svrTimeout 360 -downStateFlush
    ENABLED

/* Add GSLB service 2 */
```



```
54
55 add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai 10.102.217.117
      HTTP 80 -publicIP 10.102.217.117 -publicPort 80 -maxClient 0 -
      siteName site1 -sitePersistence HTTPRedirect -sitePrefix gs1. -
      cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
56
57 /* Bind the GSLB service 1 to GSLB server 1 */
58 bind gslb vserver vs1 -serviceName
      aws_ec2_ap_south_1_asia_pacific_mumbai_1
59
60 /* Bind the GSLB service 2 to GSLB server 2 */
61 bind gslb vserver vs1 -serviceName
      aws_ec2_ap_south_1_asia_pacific_mumbai
62
63 /* Bind a domain name to the GSLB virtual server */
64 bind gslb vserver vs1 -domainName testruchit104.com -TTL 5
65
66 <!--NeedCopy-->
```

Configurer la proximité statique

May 5, 2023

Pour que la méthode de proximité statique fonctionne, vous devez soit configurer l'appliance NetScaler pour qu'elle utilise une base de données de proximité statique existante remplie via un fichier d'emplacement, soit ajouter des entrées personnalisées à la base de données de proximité statique. Après avoir ajouté des entrées personnalisées, vous pouvez définir leurs qualificatifs de localisation. Après avoir configuré la base de données, vous êtes prêt à spécifier la proximité statique comme méthode GSLB.

Ce document contient les informations suivantes :

- Ajout d'un fichier de position pour créer une base de données de proximité statique
- Ajouter des entrées personnalisées à une base de données de proximité statique
- Configuration des qualificatifs de localisation
- Spécification de la méthode de proximité
- Synchronisation de la base de données de proximité statique GSLB

Ajouter un fichier d'emplacement pour créer une base de données de proximité statique

June 20, 2023

Une base de données de proximité statique est un fichier ASCII basé sur UNIX. Les entrées ajoutées à cette base de données à partir d'un fichier d'emplacements sont appelées entrées statiques. Un seul fichier d'emplacement peut être chargé sur une appliance NetScaler. L'ajout d'un nouveau fichier d'emplacement remplace le fichier existant. Le nombre d'entrées dans la base de données de proximité statique est limité par la mémoire configurée dans l'appliance NetScaler.

La base de données de proximité statique peut être créée dans le format par défaut ou dans un format dérivé de bases de données tierces configurées commercialement (telles que www.maxmind.com et www.ip2location.com).

L'appliance NetScaler inclut les deux fichiers de base de données de géolocalisation IP suivants. Ce sont des fichiers GeoLite2, publiés par MaxMind.

- Citrix_Netscaler_InBuilt_GeoIP_DB_IPv4
- Citrix_Netscaler_InBuilt_GeoIP_DB_IPv6

Ces fichiers de base de données sont disponibles dans un format pris en charge par l'appliance NetScaler dans le répertoire /var/netscaler/inbuilt_db.

Vous pouvez utiliser ces bases de données de géolocalisation IP comme fichier d'emplacement pour la méthode GSLB basée sur la proximité statique ou dans des stratégies basées sur l'emplacement.

Ces bases de données varient dans les détails qu'elles fournissent. Le format de fichier de base de données n'est pas strictement appliqué, sauf que le fichier par défaut possède des balises de format. Les fichiers de base de données sont des fichiers ASCII qui utilisent une virgule comme délimiteur de champ. Il existe des différences dans la structure des champs et la représentation des adresses IP dans les emplacements.

Le paramètre format décrit la structure du fichier à l'appliance NetScaler. La spécification d'une valeur incorrecte pour l'option de format peut endommager les données internes.

> **Remarque**
>
> - Après une mise à niveau, si le répertoire /var/netscaler/inbuilt_db/ contient le fichier de base de données (Citrix_Netscaler_InBuilt_GeoIP_DB.csv) des versions antérieures du logiciel NetScaler, le fichier est conservé.
> - L'emplacement par défaut du fichier de base de données est /var/netscaler/locdb, et dans une configuration haute disponibilité (HA), une copie identique du fichier doit se trouver au même emplacement sur les deux appliances NetScaler.

- Si le fichier d'emplacements est stocké dans un emplacement autre que l'emplacement par défaut, spécifiez le chemin d'accès du fichier d'emplacements.
- Pour les partitions d'administration, le chemin par défaut est : /var/partitions/<partitionName>/netscaler/locdb.
- Certaines bases de données fournissent des noms de pays courts selon la norme ISO-3166 ainsi que des noms de pays longs. NetScaler utilise des noms courts lors du stockage et de la mise en correspondance des qualificatifs.
- Pour créer une base de données de proximité statique, connectez-vous au shell UNIX de l'appliance NetScaler et utilisez un éditeur pour créer un fichier contenant les détails de localisation dans l'un des formats pris en charge par NetScaler.
- L'appliance NetScaler est livrée avec la base de données GeoLite2 (IPv4 et IPv6) mais NetScaler ne gère ni ne met à jour régulièrement la base de données MaxMind GeoLite2. Si nécessaire, vous pouvez obtenir la base de données GeoLite2 sur www.maxmind.com et la convertir au format de base de données NetScaler. Pour plus d'informations, voir Script pour convertir le format de base de données MaxMind GeoLite2 au format de base de données NetScaler.

Pour ajouter un fichier d'emplacement statique à l'aide de la CLI

À l'invite de commande, tapez :

```
add locationFile <locationFile> [-format <format>]
-  show locationFile
<!--NeedCopy-->
```

Exemple :

```
add locationFile /var/netscaler/locdb/nsgeo1.0 -format netscaler
Done

show locationFile
Location File: /var/netscaler/locdb/nsgeo1.0
Format: netscaler
 Done
>
<!--NeedCopy-->
```

Exemple :

```
add locationFile /var/netscaler/inbuilt_db/
    Citrix_Netscaler_InBuilt_GeoIP_DB_IPv4 -format netscaler

```



```
add locationFile6 /var/netscaler/inbuilt_db/
   Citrix_Netscaler_InBuilt_GeoIP_DB_IPv6 -format netscaler
<!--NeedCopy-->
```

Pour ajouter un fichier d'emplacements statiques à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Emplacement**, puis cliquez sur l'onglet **Base de données statique** .
2. Cliquez sur **Ajouter** pour ajouter un fichier d'emplacements statiques.

Vous pouvez afficher une base de données de fichiers d'emplacements importée en utilisant la boîte de dialogue **Afficher la base** de données de l'utilitaire de configuration. Il n'y a pas d'équivalent CLI.

Pour afficher un fichier d'emplacements statiques à l'aide de l'interface graphique :

1. Accédez à **AppExpert** > **Emplacement**, puis cliquez sur l'onglet **Base de données statique** .
2. Sélectionnez un fichier d'emplacement statique, puis dans la liste **Action**, cliquez sur **Afficher la base de données**.

Pour convertir un fichier de localisation au format NetScaler :

Par défaut, lorsque vous ajoutez un fichier d'emplacement, il est enregistré au format NetScaler. Vous pouvez convertir un fichier de localisation d'autres formats au format NetScaler.

> **Remarque** : L'option `nsmap` n'est accessible que depuis l'interface de ligne de commande. La conversion n'est possible qu'au format NetScaler.

Pour convertir le format de base de données statique, tapez la commande suivante à l'invite de l'interface de ligne de commande :

```
nsmap -f <inputFileFormat> -o <outputFileName> <inputFileName>
<!--NeedCopy-->
```

Exemple :

```
 nsmap -f ip-country-region-city -o nsfile.ns ip-country-region-city.
    csv
<!--NeedCopy-->
```

Script pour convertir le format de base de données MaxMind GeoLite2 au format de base de données NetScaler

La base de données MaxMind GeoIP ne peut pas être utilisée directement dans NetScaler. La base de données MaxMind GeoIP doit être convertie au format NetScaler, puis chargée pour la détection de la localisation IP à l'aide de la méthode de proximité statique GSLB et d'autres fonctionnalités telles que les stratégies.
Vous pouvez utiliser un script pour convertir le format de base de données GeoLite2 au format de

base de données NetScaler. Ce script peut être utilisé pour convertir des fichiers IPv4 et IPv6.
Le script est disponible à l'emplacement suivant : https://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format

Étapes pour convertir la base de données GeoIP2 au format NetScaler

1. Téléchargez la base de données GeoLite2 City ou GeoLite2 Country au format .csv à partir de https://dev.maxmind.com/geoip/geoip2/geolite2/.
2. Copiez le fichier dans un répertoire NetScaler (disons /var). Décompressez le fichier à l'aide de la commande shell suivante, qui créerait un répertoire portant le même nom.

   ```
   tar -xf <filename>
   ```

3. Téléchargez le script Convert_GeoIPDB_to_Netscaler_format.pl depuis https://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format et copiez-le dans le répertoire créé à l'étape #2.
4. Pour vérifier les options acceptables pour l'exécution du script, exécutez la commande suivante :

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl -help
   ```

   Les différentes options disponibles sont les suivantes :

   - `<filename>` Fichier de sortie IPv4. Nom du fichier de sortie par défaut : Netscaler_Maxmind_GeoIP_DB
   - `-p <filename>` Fichier de sortie IPv6. Nom du fichier de sortie par défaut : Netscaler_Maxmind_GeoIP_DB_IPv6.csv
   - `-logfile <filename>` Fichier contenant la liste des événements/messages
   - `-debug` Affiche tous les messages sur STDOUT

5. Exécutez la commande suivante pour convertir le format de base de données GeoLite2 au format de base de données NetScaler.

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl
   ```

   > **Remarque :** L'opération peut prendre jusqu'à 5 minutes.

   Les noms de fichiers par défaut utilisés dans le script sont ceux de la base de données basée sur MaxMind GeoLite2 City. Si vous avez téléchargé la base de données GeoLite2 Country, vous devez fournir les noms des fichiers d'entrée en conséquence, tels qu'ils figurent dans la liste.

   - `-b <filename>` nom du fichier de blocs IPv4 à convertir. Nom de fichier par défaut : GeoLite2-City-Blocks-IPv4.csv
   - `-i <filename>` nom du fichier de blocs IPv6 à convertir. Nom de fichier par défaut : GeoLite2-City-Blocks-IPv6.csv

- `-l <filename>` nom du fichier d'emplacement à convertir. Nom de fichier par défaut : GeoLite2-City-Locations-en.csv

Exemple :

```
perl Convert_GeoIPDB_To_Netscaler_Format.pl -b GeoLite2-City-Blocks-IPv4.csv -i GeoLite2-City-Blocks-IPv6.csv -l  GeoLite2-City-Locations-en.csv
<!--NeedCopy-->
```

Voici les fichiers de sortie générés après l'exécution du script.

- Netscaler_Maxmind_GeoIP_DB_IPv4.csv
- Netscaler_Maxmind_GeoIP_DB_IPv6.csv

6. Une fois la conversion de la base de données au format NetScaler terminée, utilisez la commande suivante pour commencer à l'utiliser.

   ```
   add locationFile <locationFile>
   ```

Ajouter un fichier de base de données statique tiers sur une appliance NetScaler

Procédez comme suit pour ajouter un fichier de base de données statique tiers sur une appliance NetScaler.

1. Procurez-vous le fichier de base de données d'emplacements auprès d'un fournisseur tiers, tel que www.maxmind.com.

   > **Remarque :**
   >
   > Si vous téléchargez le fichier de base de données de localisation depuis www.maxmind.com, vous pouvez utiliser le script facilement disponible pour le convertir au format de base de données NetScaler. Pour plus d'informations sur l'utilisation du script, voir Script pour convertir le format de base de données MaxMind GeoLite2 au format de base de données NetScaler.
   >
   > Pour les bases de données de localisation téléchargées auprès d'autres fournisseurs tiers, vous devez les convertir au format de base de données NetScaler avant de les ajouter à une appliance NetScaler.

2. Exécutez la commande suivante pour ajouter un fichier d'emplacements statiques :

   ```
   add location file <locationfile Name>
   <!--NeedCopy-->
   ```


> **Remarque :**
>
> - Si le fichier de base de données d'emplacements n'est pas placé dans l'emplacement par défaut **/var/netscaler/locdb**, le fichier `<locationfile Name>` doit contenir l'emplacement du fichier ainsi que le nom du fichier.
> - Avant d'exécuter la commande `add location file <locationfile Name>` :
>   - Make sure that the location database file is present in one of the directories of the NetScaler appliance.
>   - Run the `sync HA files` command on the high availability setup and the `sync cluster files` command in a cluster setup. These commands ensure that the location database file is copied to the secondary appliance of the high availability pair and peer nodes of the cluster.

3. Exécutez la commande suivante pour vous assurer que la base de données d'emplacements est chargée :

```
1 show location parameter
2 <!--NeedCopy-->
```

Cette commande affiche les paramètres, tels que le nombre d'entrées statiques. Un maximum de 3 M-1 (3 millions moins un) entrées peuvent être chargées. Lorsque le chargement de la base de données est en cours, la commande s'affiche `Loading: In progress`. Une fois le chargement terminé, la commande s'affiche `Loading: Idle`. Si la base de données n'est pas chargée correctement, cette commande affiche également un message d'erreur.

4. Exécutez la commande suivante pour afficher l'emplacement du site GSLB :

```
1 show gslb service
2 <!--NeedCopy-->
```

> **Remarque**
>
> - Si la base de données est chargée correctement, l'emplacement des sites GSLB est automatiquement renseigné dans la base de données.
> - Vous ne pouvez spécifier qu'un seul fichier d'emplacement dans la configuration de l'appliance.
> - Si aucune correspondance n'est trouvée pour une adresse IP entrante, la demande est traitée à l'aide de la méthode Round Robin.

5. Exécutez la commande suivante pour configurer la méthode GSLB sur l'appliance :

```
1 set gslb vserver GSLBVserverName -lbMethod MethodType
2 <!--NeedCopy-->
```


Ajouter des entrées personnalisées à une base de données de proximité statique

May 5, 2023

Les entrées personnalisées ont la priorité sur les entrées statiques de la base de données de proximité. Vous pouvez ajouter un maximum de 3 000 entrées personnalisées. Pour une entrée personnalisée, signalez tous les qualificatifs omis par un astérisque (*) et, si le nom des qualificatifs comporte un point ou un espace, placez le paramètre entre guillemets doubles. Les 31 premiers caractères sont évalués pour chaque qualificatif. Vous pouvez également fournir la longitude et la latitude de l'emplacement géographique de la plage d'adresses IP pour sélectionner un service à l'aide de la méthode GSLB de proximité statique.

Pour ajouter des entrées personnalisées à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une entrée personnalisée à la base de données de proximité statique et vérifier la configuration.

```
add location < IPfrom> < IPto> <preferredLocation> [-longitude <integer
   >[-latitude <integer>]]
show location
<!--NeedCopy-->
```

Exemple :

```
> add location 192.168.100.1 192.168.100.100 *.us.ca.mycity
Done
<!--NeedCopy-->
```

```
> show location
1) IP from 192.168.100.1    IP to 192.168.100.100
Continent.Country.REgion.City.ISP.Organization =
North America.us.ca.mycity.*.
Coordinated: Not specified
Done
<!--NeedCopy-->
```

Paramètres d'ajout d'entrées personnalisées

- **À partir de l'adresse IP** : première adresse IP de la plage en notation décimale avec points.

  Il s'agit d'un argument obligatoire.

- **À l'adresse IP** : dernière adresse IP de la plage qui est en notation décimale avec points.

  Il s'agit d'un argument obligatoire.

- **Nom de l'emplacement** : La chaîne de qualificatifs en notation pointillée décrit l'emplacement géographique de la plage d'adresses IP. Chaque qualificatif est plus spécifique que celui qui le précède, comme dans continent.country.region.city.isp.organization. Par exemple, « NA.US.CA.San Jose.att.Citrix ».

  Il s'agit d'un argument obligatoire. Longueur maximale : 197

  > **Remarque :**
  >
  > Un qualificatif qui inclut un point (.) ou un espace () doit être placé entre guillemets doubles.

- **longitude** : la valeur numérique exprimée en degrés indique la longitude de l'emplacement géographique de la plage d'adresses IP.
  Valeur maximale : 180

- **latitude** : la valeur numérique exprimée en degrés indique la latitude de l'emplacement géographique de la plage d'adresses IP.
  Valeur maximale : 180

  > **Remarque :**
  >
  > Les paramètres de longitude et de latitude sont utilisés pour sélectionner un service à l'aide de la méthode GSLB de proximité statique. S'ils ne sont pas spécifiés, la sélection est basée sur les qualificatifs spécifiés pour le lieu.

Pour ajouter des entrées personnalisées à l'aide de l'utilitaire de configuration

Accédez à **AppExpert** > **Emplacement**, cliquez sur l'onglet **Entrées personnalisées** et ajoutez les entrées personnalisées.

Définir les qualificatifs d'emplacement

May 5, 2023

La base de données utilisée pour implémenter la proximité statique contient l'emplacement des sites GSLB. Chaque emplacement possède une plage d'adresses IP et jusqu'à six qualificatifs pour cette plage. Les qualificatifs sont des chaînes littérales et sont comparés dans un ordre prescrit au moment de l'exécution. Chaque emplacement doit comporter au moins un qualificatif. Les étiquettes de qualificatifs définissent la signification des qualificatifs (contexte), qui sont définis par l'utilisateur. NetScaler possède deux contextes intégrés :

Contexte géographique, qui comporte les libellés de qualificateurs suivants :

- Qualificateur 1 — « Continent »
- Qualificateur 2 — « Pays »
- Qualificateur 3 — « État »
- Qualificateur 4 — « Ville »
- Qualificateur 5 — « FAI »
- Qualificateur 6 — « Organisation »

Entrées personnalisées, qui comportent les étiquettes de qualificateur suivantes :

- Qualificateur 1 — « Qualifier 1 »
- Qualificateur 2 — « Qualifier 2 »
- Qualificateur 3 — « Qualifier 3 »
- Qualificateur 4 — « Qualifier 4 »
- Qualificateur 5 — « Qualifier 5 »
- Qualificateur 6 — « Qualifier 6 »

Si le contexte géographique est défini sans qualificateur de continent, Continent est dérivé de Country. Même les libellés de qualificatifs intégrés sont basés sur le contexte, et les étiquettes peuvent être modifiées. Ces étiquettes de qualificatifs spécifient les emplacements mappés avec les adresses IP utilisées pour prendre des décisions de proximité statiques.

Pour prendre une décision statique basée sur la proximité, l'appliance NetScaler compare les attributs de localisation (qualificatifs) dérivés de l'adresse IP du résolveur de serveur DNS local avec les attributs de localisation des sites participants. Si un seul site correspond, l'applliance renvoie l'adresse IP de ce site. S'il y a plusieurs correspondances, le site sélectionné est le résultat d'un tournoi à la ronde sur les sites GSLB correspondants. S'il n'y a pas de correspondance, le site sélectionné est le résultat d'un tourniquet sur tous les sites configurés. Un site qui n'a pas de qualificatifs est considéré comme une correspondance.

Les règles GEO pour l'expression de stratégie basée sur l'emplacement vous permettent de vérifier les correspondances avec des caractères génériques. Cette fonctionnalité vérifie si les qualificatifs génériques correspondent à n'importe quel autre qualificatif, y compris non générique ou non. La correspondance générique est effectuée à l'aide de l'attribut `matchWildcardtoany` ajouté à la commande `set locationParameter`.

L' `matchWildcardtoany` attribut peut être défini sur les valeurs suivantes :

- **Oui :** les qualifications Wildcard correspondent à toutes les autres qualifications.
- **Non :** les qualificatifs génériques ne correspondent pas aux qualificatifs non génériques, mais à d'autres qualificatifs génériques. L'option par défaut est **Non**.
- **Expression :** les qualificatifs génériques d'une expression correspondent à n'importe quel qualificatif d'un emplacement LDNS, mais les qualificatifs génériques de l'emplacement LDNS ne correspondent pas aux qualificatifs non génériques d'une expression.

Exemple :

```
1 add dns policy1 "CLIENT.IP.SRC.MATCHES_LOCATION("Continent.country
     \*.\*.\*.\* \ “)”  <action>
2 <!--NeedCopy-->
```

Pour définir les paramètres d’emplacement à l’aide de l’interface de ligne de commande

À l’invite de commande, tapez :

```
1 set locationparameter -context <context> -q1label <string> [-q2label <
     string>] [-q3label <string>] [-q4label <string>] [-q5label <string>]
      [-q6label <string>] -matchWildcardtoany [Yes | No | Expression]
2 <!--NeedCopy-->
```

Exemple :

```
1 set locationparameter -context custom -q1label asia -matchWildcardtoany
     Yes
2 <!--NeedCopy-->
```

Pour définir les paramètres de localisation à l’aide de l’interface graphique

1. Accédez à **Gestion du trafic > GSLB > Base de données et entrées**.
2. Sous **Paramètres**, cliquez sur **Modifier les paramètres d’emplacement**.
3. Dans la page **Configurer les paramètres d’emplacement**, définissez les paramètres d’emplacement.

Exemple de configuration (en utilisant CLI)

Considérez la configuration réseau suivante :

- Nom du serveur virtuel GSLB : gv1
- Adresse IP du serveur virtuel GSLB : 1.1.1.2
- Service GSLB : gsvc1 lié à gv1
- Nom du fichier de la base de données d’emplacement sample.csv
- Qualificatifs de géolocalisation : les qualificatifs 1 et 2 sont configurés. Le repos est défini pour correspondre au caractère générique.
  - Qualifier 1 — Asie
  - Qualifier 2 — IR
  - Qualifications 3-*

  - Qualifications 4-*
  - Qualifications 5-*
  - Qualifications 6-*
- Stratégie DNS - La stratégie, pol1, est définie pour supprimer les paquets s'il y a correspondance.

Définissez le paramètre d'emplacement et configurez la stratégie DNS comme suit :

```
set locationParameter -q2label Country_Code -q3label Subdivision_1_Name
    -q4label Subdivision_2_Name -q5label City

add locationFile "/var/netscaler/inbuilt_db/sample.csv"

add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0

add dns policy pol1 "CLIENT.IP.SRC.MATCHES_LOCATION("Asia.IR
    .\*.\*.\*.\*")||CLIENT.IP.SRC.MATCHES_LOCATION("Asia.SY.\*.\*.\*.\*"
    )||CLIENT.IP.SRC.MATCHES_LOCATION("Asia.SD.\*.\*.\*.\*")||CLIENT.IP.
    SRC.MATCHES_LOCATION("Asia.KP.\*.\*.\*.\*")||CLIENT.IP.SRC.
    MATCHES_LOCATION("North America.CU.\*.\*.\*.\*")||CLIENT.IP.SRC.
    MATCHES_LOCATION("Europe.UA.Crimea.\*.\*.\*.\*")"
    dns_default_act_Drop

bind dns global pol1 1 -gotoPriorityExpression 65535 -type REQ_DEFAULT

add gslb service gsvc1 1.1.1.2 HTTP 80 -publicIP 1.1.1.2 -publicPort 80
    -maxClient 0 -healthMonitor NO -siteName s1 -cltTimeout 180 -
    svrTimeout 360 -downStateFlush ENABLED

bind gslb vserver gv1 -serviceName gsvc1

bind gslb vserver gv1 -domainName www.gslbnew.com -TTL 5
<!--NeedCopy-->
```

Ajoutez les entrées client suivantes dans le fichier de base de données d'emplacement. Dans cet exemple, le nom du fichier de base de données d'emplacement est sample.csv :

```
10.106.24.170,10.106.24.190,,,,,,,8.0000,47.0000

10.102.82.170,10.102.82.190,Asia,,,,,,-73.9924,40.7553

10.106.24.140,10.106.24.150,,IR,,,,,51.4231,35.6961
<!--NeedCopy-->
```

Selon la configuration précédente, les clients compris entre 10.106.24.170 et 10.106.24.190 n'ont aucun qualificatif générique défini. Les clients entre 10.106.24.140 et 10.106.24.150 ont le qualificatif 2

comme IR.

Définissez le qualificatif générique de correspondance sur NON :

```
set locationparameter -matchWildcardtoany no
<!--NeedCopy-->
```

Lorsque le qualificatif générique de correspondance est défini sur NON, les qualificatifs génériques correspondent uniquement aux qualificatifs génériques définis. Il ne correspond à aucun autre qualificatif non générique.

- Les requêtes DNS provenant de 10.106.24.147 correspondent au qualificatif générique défini (qualificatif 2 = IR). Par conséquent, la stratégie DNS entre en vigueur et supprime les requêtes.

  Lorsque vous exécutez la commande `dig @10.102.82.13 www.gslbnew.com` sur le client 10.106.24.147, la sortie indique que les serveurs n'étaient pas accessibles.

  ```
  root@ns#  dig @10.102.82.13 www.gslbnew.com

  ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
  ; (1 server found)
  ;; global options: +cmd
  ;; connection timed out; no servers could be reached
  <!--NeedCopy-->
  ```

- Les requêtes DNS provenant de 10.106.24.180 ne correspondent pas aux qualificatifs définis. La politique DNS n'entre pas en vigueur et les requêtes sont traitées.

  Exécutez la commande `dig @10.102.82.13 www.gslbnew.com` sur le client 10.106.24.180. La sortie indique l'adresse IP du serveur virtuel GSLB.

  ```
  root@ns# dig @10.102.82.13 www.gslbnew.com

  ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
  ; (1 server found)
  ;; global options: +cmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64265
  ;; flags: qr aa rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
     ADDITIONAL: 1
  ;; WARNING: recursion requested but not available

  ;; OPT PSEUDOSECTION:
  ; EDNS: version: 0, flags:; udp: 1280
  ;; QUESTION SECTION:
  ;www.gslbnew.com. IN    A
  ```



```
15
16  ;; ANSWER SECTION:
17  www.gslbnew.com.    5   IN  A   1.1.1.2
18
19  ;; Query time: 12 msec
20  ;; SERVER: 10.102.82.13#53(10.102.82.13)
21  ;; WHEN: Tue Mar 29 22:46:40 UTC 2022
22  ;; MSG SIZE  rcvd: 60
23  <!--NeedCopy-->
```

Définissez le qualificatif générique de correspondance sur Oui :

```
1 set locationparameter -matchWildcardtoany yes
2 <!--NeedCopy-->
```

Lorsque le qualificatif générique de correspondance est défini sur yes, les qualificatifs génériques correspondent à n'importe quel qualificatif générique (qualificatif défini et non générique).

- Les requêtes DNS provenant de 10.106.24.147 correspondent au qualificatif défini (qualificatif 2 = IR). Par conséquent, la stratégie DNS entre en vigueur et supprime les requêtes.

  Exécutez la commande `dig @10.102.82.13 www.gslbnew.com` sur le client 10.106.24.147. La sortie indique que les serveurs n'étaient pas accessibles.

  ```
  1  root@ns#  dig @10.102.82.13 www.gslbnew.com
  2
  3  ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
  4  ; (1 server found)
  5  ;; global options: +cmd
  6  ;; connection timed out; no servers could be reached
  7  <!--NeedCopy-->
  ```

- Les requêtes provenant de 10.106.24.180 correspondent aux qualificatifs non génériques. Par conséquent, la stratégie DNS entre en vigueur et supprime les requêtes.

  Exécutez la commande `dig @10.102.82.13 www.gslbnew.com` sur le client 10.106.24.180. La sortie indique que les serveurs n'étaient pas accessibles.

  ```
  1  root@ns# dig @10.102.82.13 www.gslbnew.com
  2
  3  ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
  4  ; (1 server found)
  5  ;; global options: +cmd
  6  ;; connection timed out; no servers could be reached
  7  <!--NeedCopy-->
  ```


Définissez le qualificatif générique de correspondance sur Expression :

```
set locationparameter -matchWildcardtoany expression
<!--NeedCopy-->
```

Lorsque le qualificatif générique de correspondance est défini sur expression, les qualificatifs génériques correspondent soit au qualificateur disponible dans la stratégie DNS, soit aux qualificateurs disponibles dans le fichier de base de données d'emplacement.

- Les requêtes DNS provenant de 10.106.24.147 correspondent aux qualificatifs génériques définis dans la stratégie DNS. Par conséquent, la stratégie DNS entre en vigueur et supprime les requêtes.

  Exécutez la commande `dig @10.102.82.13 www.gslbnew.com` sur le client 10.106.24.147. La sortie indique que les serveurs n'étaient pas accessibles.

  ```
  root@ns#  dig @10.102.82.13 www.gslbnew.com

  ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
  ; (1 server found)
  ;; global options: +cmd
  ;; connection timed out; no servers could be reached
  <!--NeedCopy-->
  ```

- Les requêtes provenant de 10.106.24.180 ne correspondent pas aux qualificatifs de la stratégie DNS. Par conséquent, la stratégie DNS n'entre pas en vigueur et les requêtes sont traitées.

  Exécutez la commande `dig @10.102.82.13 www.gslbnew.com` sur le client 10.106.24.180. La sortie indique l'adresse IP du serveur virtuel GSLB.

  ```
  root@ns# dig @10.102.82.13 www.gslbnew.com

  ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
  ; (1 server found)
  ;; global options: +cmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64265
  ;; flags: qr aa rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
     ADDITIONAL: 1
  ;; WARNING: recursion requested but not available

  ;; OPT PSEUDOSECTION:
  ; EDNS: version: 0, flags:; udp: 1280
  ;; QUESTION SECTION:
  ;www.gslbnew.com.  IN   A

  ```



```
;; ANSWER SECTION:
www.gslbnew.com.    5   IN  A   1.1.1.2

;; Query time: 12 msec
;; SERVER: 10.102.82.13#53(10.102.82.13)
;; WHEN: Tue Mar 29 22:46:40 UTC 2022
;; MSG SIZE  rcvd: 60
<!--NeedCopy-->
```

Spécifier la méthode de proximité

August 20, 2021

Lorsque vous avez configuré la base de données de proximité statique, vous êtes prêt à spécifier la proximité statique comme méthode GLSB.

Pour spécifier la proximité statique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la proximité statique et vérifier la configuration :

```
set gslb vserver <name> -lbMethod STATICPROXIMITY
show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -lbMethod STATICPROXIMITY
show gslb vserver
<!--NeedCopy-->
```

Pour spécifier la proximité statique à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels et double-cliquez sur le serveur virtuel.
2. Cliquez sur la section **Méthode** et, dans la liste déroulante **Choisir une méthode**, sélectionnez **STATICPROXIMITY**.

Synchroniser la base de données de proximité statique GSLB

January 21, 2021

La synchronisation d'une base de données de proximité statique GSLB (Global Server Load Balancing) nécessite que l'un des sites soit identifié comme étant le nœud GSLB maître. Tout site de la topologie peut être désigné comme nœud maître. Le reste des nœuds GSLB sont automatiquement désignés comme nœuds esclaves.

La synchronisation des bases de données de proximité statique GSLB synchronise les fichiers du répertoire /var/netscaler/locdb sur les nœuds esclaves. Pendant le processus de synchronisation, le nœud maître récupère la configuration en cours d'exécution à partir de chacun des nœuds esclaves et la compare à la configuration du nœud maître. Le nœud GSLB maître utilise le programme rsync pour synchroniser la base de données de proximité statique entre les nœuds esclaves. Pour accélérer le processus de synchronisation, le programme rsync ne fait que suffisamment de modifications pour éliminer les différences entre les deux fichiers. Le processus de synchronisation ne peut pas être annulé.

L'exemple suivant synchronise Site2, qui est un site esclave, avec le site maître Site1. L'administrateur entre la commande **sync gslb config** sur Site1 :

```
sync gslb config -nowarn
Sync Time: Feb 24 2014 14:56:16
Retrieving local site info: ok
Retrieving all participating gslb sites info:
0 bytes in 0 blocks
ok
site1[Master]:
        Getting Config: ok
site2[Slave]:
        Syncing gslb static proximity database: ok
        Getting Config: ok
        Comparing config: ok
        Applying changes: ok
 Done
<!--NeedCopy-->
```

Configurer la communication de site à site

May 5, 2023

La communication GSLB de site à site s'effectue entre les nœuds d'appel de procédure distante (RPC) associés aux sites communicants. Un site GSLB principal établit des connexions avec des sites esclaves afin de synchroniser les informations de configuration du GSLB et d'échanger des métriques de site.

Un nœud RPC est créé automatiquement lors de la création d'un site GSLB et se voit attribuer un nom d'utilisateur et un mot de passe générés en interne. L'appliance NetScaler utilise ce nom d'utilisateur et ce mot de passe pour s'authentifier auprès des sites GSLB distants lors de l'établissement de la connexion. Aucune étape de configuration n'est nécessaire pour un nœud RPC, mais vous pouvez spécifier le mot de passe de votre choix, renforcer la sécurité en chiffrant les informations échangées par les sites GSLB et spécifier une adresse IP source pour le nœud RPC.

L'appliance a besoin d'une adresse IP appartenant à NetScaler à utiliser comme adresse IP source lors de la communication avec d'autres sites GSLB. Par défaut, les nœuds RPC utilisent soit une adresse IP de sous-réseau (SNIP), mais vous pouvez spécifier l'adresse IP de votre choix.

Les rubriques suivantes décrivent le comportement et la configuration des nœuds RPC sur l'appliance NetScaler :

Changer le mot de passe d'un nœud RPC

Citrix vous recommande de sécuriser la communication entre les sites de votre configuration GSLB en modifiant le mot de passe de chaque nœud RPC. Après avoir modifié le mot de passe du nœud RPC du site local, vous devez propager manuellement la modification au nœud RPC de chacun des sites distants.

Le mot de passe est enregistré sous forme cryptée. Vous pouvez vérifier que le mot de passe a changé en utilisant la commande show RPCNode pour comparer la forme cryptée du mot de passe avant et après la modification.

> **Remarque :** GSLB utilise un compte utilisateur interne. Pour une sécurité renforcée, Citrix vous recommande de modifier également le mot de passe du compte utilisateur interne. Le mot de passe du compte d'utilisateur interne est modifié via le mot de passe du nœud RPC.

Pour modifier le mot de passe d'un nœud RPC à l'aide de l'interface de ligne de commande

Sur la ligne de commande, tapez les commandes suivantes pour modifier le mot de passe d'un nœud RPC :

```
set ns rpcNode <IPAddress> {
 -password }

show ns rpcNode
<!--NeedCopy-->
```


Exemple :

```
> set rpcNode 192.0.2.4 -password mypassword
 Done
> show rpcNode
.
.
.
2)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
    SrcIP:  *               Secure:  OFF
Done
>

<!--NeedCopy-->
```

Pour annuler la définition du mot de passe d'un nœud RPC à l'aide de l'interface de ligne de commande

Pour annuler le mot de passe d'un nœud RPC à l'aide de l'interface de ligne de commande, tapez la commande unset RPCNode, l'adresse IP du nœud RPC et le paramètre de mot de passe, sans valeur.

Pour modifier le mot de passe d'un nœud RPC à l'aide de l'utilitaire de configuration

Accédez à Système > Réseau > RPC, sélectionnez le nœud RPC et modifiez le mot de passe.

Chiffrer l'échange de statistiques du site

Vous pouvez sécuriser les informations échangées entre les sites GSLB en définissant l'option sécurisée pour les nœuds RPC dans la configuration GSLB. Lorsque l'option sécurisée est définie, l'appliance NetScaler chiffre toutes les communications envoyées depuis le nœud vers d'autres nœuds RPC.

Pour crypter l'échange de métriques de site à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour chiffrer l'échange de métriques du site et vérifier la configuration :

```
set ns rpcNode <IPAddress> [-secure ( YES | NO )]
show rpcNode
<!--NeedCopy-->
```

Exemple :


```
> set rpcNode 192.0.2.4 -secure YES
 Done
>
> show rpcNode
.
.
.
3)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e SrcIP:
    192.0.2.3     Secure:  ON
 Done
>
<!--NeedCopy-->
```

Pour annuler la définition du paramètre sécurisé à l'aide de l'interface de ligne de commande

Pour annuler la définition du paramètre sécurisé à l'aide de l'interface de ligne de commande, tapez la commande unset RPCNode, l'adresse IP du nœud RPC et le paramètre sécurisé, sans valeur.

Pour crypter l'échange de métriques de site à l'aide de l'utilitaire de configuration NetScaler

1. Accédez à Système > Réseau > RPC et double-cliquez sur un nœud RPC.
2. Sélectionnez l'option **Sécurisé**, puis cliquez sur **OK**.

Configurer l'adresse IP source pour un nœud RPC

Par défaut, l'appliance NetScaler utilise une adresse IP de sous-réseau appartenant à NetScaler (SNIP) comme adresse IP source pour un nœud RPC, mais vous pouvez configurer l'appliance pour qu'elle utilise une adresse SNIP spécifique. Si aucune adresse SNIP n'est disponible, le site GSLB ne peut pas communiquer avec d'autres sites. Dans un tel scénario, vous devez configurer l'adresse NSIP ou une adresse IP virtuelle (VIP) comme adresse IP source pour un nœud RPC. Une adresse VIP peut être utilisée comme adresse IP source d'un nœud RPC uniquement si le nœud RPC est un nœud distant. Si vous configurez une adresse VIP comme adresse IP source et que vous supprimez l'adresse VIP, l'appliance utilise une adresse SNIP.

> **Remarque**
>
> À partir de la version 11.0.64.x de NetScaler, vous pouvez configurer l'appliance pour qu'elle utilise l'adresse IP du site GSLB comme adresse IP source pour un nœud RPC.

Pour spécifier une adresse IP source pour un nœud RPC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour modifier l'adresse IP source d'un nœud RPC et vérifier la configuration :

```
set ns rpcNode <IPAddress> [-srcIP <ip_addr|ipv6_addr|*>]
show ns rpcNode
<!--NeedCopy-->
```

Exemple :

```
set rpcNode 192.0.2.4 -srcIP 192.0.2.3
Done
show rpcNode
<!--NeedCopy-->
```

```
IPAddress: 192.0.2.4 Password: d336004164d4352ce39e SrcIP: 192.0.2.3
   Secure: OFF
Done
<!--NeedCopy-->
```

Pour annuler la définition du paramètre d'adresse IP source à l'aide de l'interface de ligne de commande

Pour annuler la définition du paramètre d'adresse IP source à l'aide de l'interface de ligne de commande, tapez la commande RPCNodeCommand non définie, l'adresse IP du nœud RPC et le paramètre srCip, sans valeur.

Pour spécifier une adresse IP source pour un nœud RPC à l'aide de l'utilitaire de configuration NetScaler

1. Accédez à Système > Réseau > RPC et double-cliquez sur un nœud RPC.
2. Dans le champ Adresse IP source, entrez l'adresse IP que vous souhaitez que le nœud RPC utilise comme adresse IP source et cliquez sur OK.

> **Important**
>
> L'adresse IP source ne peut pas être synchronisée entre les sites participant au GSLB car l'adresse IP source d'un nœud RPC est spécifique à chaque appliance NetScaler. Par conséquent, après avoir forcé une synchronisation (à l'aide de la commande sync gslb config —ForceSync ou en sélectionnant l'option ForceSync dans l'interface graphique), vous devez

> modifier manuellement les adresses IP sources sur les autres appliances NetScaler.

Configurer le protocole d'échange de mesures

May 5, 2023

Les centres de données d'une configuration GSLB échangent des métriques entre eux via le protocole d'échange de métriques (MEP), qui est un protocole propriétaire pour l'appliance NetScaler. L'échange des informations de mesure commence lorsque vous créez un site GSLB. Ces mesures comprennent des informations de charge, de réseau et de persistance.

Le MEP est requis pour le contrôle de santé des centres de données afin de garantir leur disponibilité. Une connexion pour échanger des métriques réseau (temps aller-retour) peut être initiée par l'un des centres de données impliqués dans l'échange, mais une connexion pour échanger des métriques de site est toujours initiée par le centre de données dont l'adresse IP est la plus basse. Par défaut, le centre de données utilise une adresse IP de sous-réseau (SNIP) pour établir une connexion à l'adresse IP d'un autre centre de données. Toutefois, vous pouvez configurer une adresse SNIP, une adresse IP virtuelle (VIP) ou une adresse NSIP spécifique comme adresse IP source pour l'échange de métriques. Le processus de communication entre les sites GSLB utilise le port TCP 3011 ou 3009. Ce port doit donc être ouvert sur les pare-feux situés entre les appliances NetScaler.

Remarque : Vous pouvez configurer une adresse IP de site SNIP ou GSLB comme adresse IP source pour l'échange de mesures. Pour plus d'informations, voir Configurer l'adresse IP source pour un nœud RPC.

Si les sites source et cible (le site qui initie une connexion MEP et le site qui reçoit la demande de connexion, respectivement) ont des adresses IP privées et publiques configurées, les sites échangent des informations MEP à l'aide des adresses IP publiques.

Vous pouvez également lier des moniteurs pour vérifier l'état de santé des services distants, comme décrit dans « Surveillance des services GSLB ». « Lorsque les moniteurs sont liés, l'échange de mesures ne contrôle pas l'état du service distant. Si un moniteur est lié à un service distant et que l'échange de métriques est activé, le moniteur contrôle l'état de santé. La liaison des moniteurs au service distant permet à l'appliance NetScaler d'interagir avec un dispositif d'équilibrage de charge autre que NetScaler. L'appliance NetScaler peut surveiller des appareils non NetScaler mais ne peut pas effectuer d'équilibrage de charge sur ceux-ci à moins que les moniteurs ne soient liés à tous les services GSLB et que seules des méthodes d'équilibrage de charge statiques (telles que le round robin, la proximité statique ou les méthodes basées sur le hachage) soient utilisées.

Avec NetScaler version 11.1.51.x ou ultérieure, pour éviter toute interruption inutile des services, vous pouvez définir un délai pour marquer les services GSLB comme étant hors service lorsqu'une connexion MEP est interrompue.

État MEP dans une configuration à haute disponibilité

Dans une configuration à haute disponibilité, le nœud principal établit des connexions avec les sites distants et l'état du MEP n'est pas synchronisé entre le nœud principal et les nœuds secondaires. Par conséquent, l'état MEP du nœud secondaire reste inactif. Lorsque le nœud secondaire devient principal, il établit des connexions MEP avec le nouveau site GSLB et met à jour l'état du MEP en conséquence.

Activer l'échange de métriques du site

Les métriques de site échangées entre les sites GSLB incluent l'état de chaque serveur virtuel d'équilibrage de charge ou de commutation de contenu, le nombre actuel de connexions, le débit de paquets actuel et les informations d'utilisation actuelle de la bande passante.

L'appliance NetScaler a besoin de ces informations pour effectuer l'équilibrage de charge entre les sites. L'intervalle d'échange des métriques du site est de 1 seconde. Un service GSLB distant doit être lié à un serveur virtuel GSLB local pour permettre l'échange de métriques de site avec le service distant.

Pour activer ou désactiver l'échange de métriques du site à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver l'échange de métriques du site et vérifier la configuration :

```
set gslb site <siteName> -metricExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Exemple :

```
set gslb site Site-GSLB-East-Coast -metricExchange ENABLED
set gslb site Site-GSLB-East-Coast -metricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour activer ou désactiver l'échange de métriques du site à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Sites**, puis sélectionnez le site.
2. Dans la boîte de dialogue **Configurer le site GSLB**, sélectionnez l'option **Metric Exchange** .

Activer l'échange de métriques réseau

Si vos sites GSLB utilisent la méthode d'équilibrage de charge RTT (aller-retour), vous pouvez activer ou désactiver l'échange d'informations RTT concernant le service DNS local du client. Ces informations sont échangées toutes les 5 secondes.

Pour plus d'informations sur la modification de la méthode GSLB par une méthode basée sur RTT, voir Méthodes GSLB.

Pour activer ou désactiver l'échange d'informations de mesure réseau à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver l'échange d'informations sur les métriques du réseau et vérifier la configuration :

```
set gslb site <siteName> -nwmetricExchange (ENABLED|DISABLED)
show gslb site <<siteName>
<!--NeedCopy-->
```

Exemple :

```
set gslb site Site-GSLB-East-Coast -nwmetricExchange ENABLED
set gslb site Site-GSLB-East-Coast -nwmetricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour activer ou désactiver l'échange d'informations sur les métriques réseau à l'aide de l'interface graphique

1. **Accédez à**Gestion du trafic**>**GSLB > Sites**.**
2. Dans la boîte de dialogue **Configurer le site GSLB**, sélectionnez l'option **Network Metric Exchange** .

Configuration d'un délai pour que les services GSLB soient marqués comme étant hors service lorsqu'une connexion MEP tombe en panne

Si l'état d'une connexion MEP à un site distant passe à DOWN, l'état de chaque service GSLB de ce site distant est marqué comme étant INACTIF, bien que le site ne soit peut-être pas réellement INACTIF.

Vous pouvez désormais définir un délai afin de permettre le rétablissement de la connexion MEP avant que le site ne soit marqué comme étant inactif. Si la connexion MEP est rétablie avant l'expiration du délai, les services ne sont pas affectés.

Par exemple, si vous définissez le délai de 10, les services GSLB sont marqués comme étant hors service jusqu'à ce que la connexion MEP soit interrompue pendant 10 secondes. Si la connexion MEP est rétablie dans les 10 secondes, les services GSLB restent à l'état actif.

Remarque : Ce délai s'applique uniquement aux services qui ne sont pas liés à un moniteur. Le délai n'affecte pas les moniteurs de déclenchement.

Pour définir un délai à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set gslb parameter** - GSLBSvcStateDelayTime <sec>
<!--NeedCopy-->
```

Exemple :

définir le paramètre gslb - GSLBSVCStateDelayTime 10

> **Remarque**
>
> Dans un déploiement hiérarchique (topologie parent-enfant), si vous configurez le service GSLB à la fois sur les sites parent et enfant, définissez le paramètre GSLB sur les sites parent et enfant. Si vous ne configurez pas le service GSLB sur le site enfant, définissez le paramètre GSLB uniquement sur le site parent.

Pour définir un délai à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Modifier les paramètres GSLB**.
2. Dans la zone **Temps de retard (secondes) de l'état du service GSLB**, tapez le délai en secondes.

Configurer un temps d'apprentissage pour les services GSLB lorsque l'état de la connexion MEP apparaît pour éviter les volets sur les services GSLB

Lorsqu'un nœud redémarre ou pendant le basculement HA, le système est initialisé. Ensuite, le nœud doit connaître les informations actuelles sur les services locaux et enfants configurés pour communiquer l'état du service aux nœuds distants via MEP. Le nœud prend un certain temps pour apprendre les informations correctes. Dans le même temps, si un nœud homologue se connecte à ce nœud et demande une mise à jour, le nœud peut envoyer un état de service et des statistiques incorrects. Ces informations incorrectes peuvent entraîner des problèmes liés à la fonctionnalité et à d'autres problèmes liés aux fonctionnalités sur les nœuds homologues distants. Pour éviter ce scénario, vous pouvez désormais définir un temps d'apprentissage pour le service GSLB local et enfant.

Lorsqu'un délai d'attente d'apprentissage est configuré, le site GSLB reçoit un certain temps de tampon (délai d'attente d'apprentissage) pour connaître les statistiques correctes sur ses services locaux et enfants. Lorsqu'un service est en phase d'apprentissage, le site GSLB distant obtient ces informations dans la mise à jour MEP, et ne respecte pas l'état du site principal et les statistiques reçues via MEP pour ce service.

Les services GSLB entrent dans la phase d'apprentissage dans l'un des scénarios suivants.

- L'appliance NetScaler est redémarrée
- Le basculement à haute disponibilité s'est produit
- Le nœud propriétaire d'une configuration GSLB de cluster est modifié
- MEP est activé sur un nœud local
- Le site GSLB est issu d'un scénario insulaire. Un site GSLB devient un îlot lorsqu'il n'est connecté à aucun autre site.

Dans un déploiement parent-enfant, le parent de sauvegarde (s'il est configuré) déplace sélectivement les services GSLB du site enfant adopté vers la phase d'apprentissage lorsque le parent principal tombe en panne.

Pour définir un temps d'apprentissage de l'état du service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set gslb parameter - SvcStateLearningTime <sec>
<!--NeedCopy-->
```

Vous pouvez définir « SVCStateLearningTime » en quelques secondes. La valeur par défaut est 0 et la valeur maximale est 3600. Ce paramètre est applicable uniquement si les moniteurs ne sont pas liés aux services GSLB.

Exemple :

```
set gslb parameter - SvcStateLearningTime 10
<!--NeedCopy-->
```

Pour définir un temps d'apprentissage de l'état du service à l'aide de l'interface graphique

1. Accédez à **Configuration > Gestion du trafic > GSLB > Tableau de bord > Modifier les paramètres GSLB**.

   La page **Définir les paramètres GSLB** apparaît.

2. Dans le champ **Durée d'apprentissage de l'état du service GSLB (secondes)**, saisissez le temps d'apprentissage en secondes.

Activer l'échange d'informations de persistance

Vous pouvez configurer l'appliance NetScaler pour fournir des connexions persistantes, de sorte qu'une transmission client vers n'importe quel serveur virtuel d'un groupe puisse être dirigée vers un serveur ayant reçu des transmissions précédentes du même client.

Vous pouvez activer ou désactiver l'échange d'informations de persistance sur chaque site. Ces informations sont échangées toutes les 5 secondes entre les appliances NetScaler participant au GSLB.

Pour plus d'informations sur la configuration de la persistance, voir Configuration des connexions persistantes.

Pour activer ou désactiver l'échange d'informations de persistance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer ou désactiver l'échange d'informations persistantes et vérifier la configuration :

```
set gslb site <siteName> -sessionExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Exemple :

```
set gslb site Site-GSLB-East-Coast -sessionExchange  ENABLED
set gslb site Site-GSLB-East-Coast -sessionExchange  DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour activer ou désactiver l'échange d'informations de persistance à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Sites, puis**double-cliquez sur le site.
2. Dans la boîte de dialogue **Configurer le site GSLB**, cochez ou décochez la case **Persistence Session Entry Exchange** .

Configurer GSLB à l'aide d'un assistant

January 21, 2021

Vous pouvez maintenant utiliser un assistant pour configurer les types de déploiement GSLB : actif-actif, actif-passif et parent-enfant.

Cet Assistant est disponible dans l'interface graphique. Pour accéder à l'Assistant, accédez à **Configuration** > **Gestion du trafic** > **GSLB** et cliquez sur **Démarrer** .

Vous pouvez également accéder à cet Assistant à partir du tableau de bord GSLB. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Tableau de bord** et cliquez sur **Configurer GSLB** .

Remarque : Vous pouvez également configurer les entités GSLB individuellement.

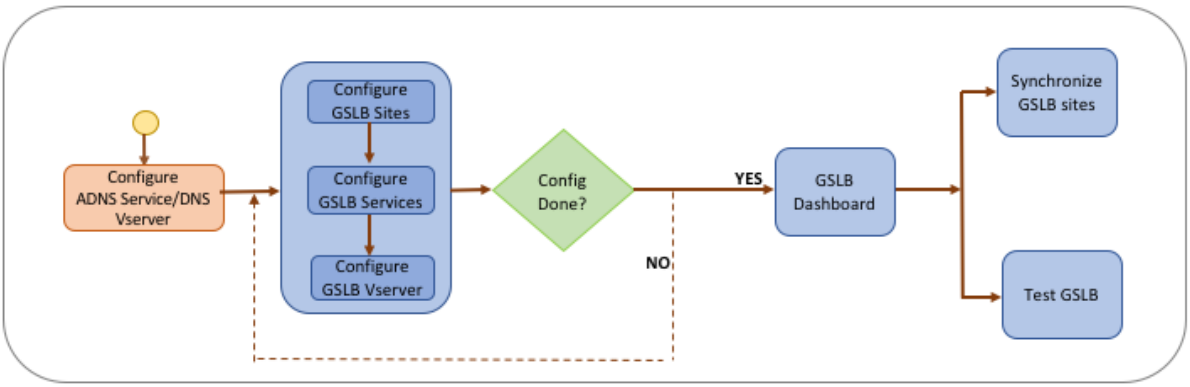
- Configuration active du site
- Configuration du site actif-passif
- Configuration de la topologie parent-enfant

> **Important**
>
> Cette fonctionnalité est prise en charge dans le déploiement haute disponibilité et non dans les déploiements de partition d'administration et de cluster.

Configurer le site actif-actif

May 5, 2023

La figure suivante montre le flux de travail impliqué dans la configuration d'un site GSLB actif-actif.



Avant de commencer à configurer un site actif-actif, assurez-vous d'avoir configuré une configuration d'équilibrage de charge standard pour chaque parc de serveurs ou centre de données.

En outre, pour synchroniser la configuration GSLB entre les sites GSLB du déploiement, assurez-vous que :

- Les sites GLSB locaux sont configurés sur toutes les appliances de la configuration GSLB.
- Vous avez activé l'accès à la gestion sur tous les sites GSLB dans la configuration.
- Vous avez configuré le pare-feu pour qu'il accepte la synchronisation automatique et les connexions MEP.
- Les appliances NetScaler maître et esclave exécutent les mêmes versions du logiciel NetScaler.

- Toutes les appliances NetScaler participant en tant que sites doivent disposer de la même version du logiciel NetScaler (les sites ne sont pas dans une relation maître-esclave).
- Le mot de passe du nœud RPC est le même pour tous les sites GSLB de la configuration GSLB.

Pour configurer un site actif-actif à l'aide de l'assistant

Dans l'onglet Configuration, procédez comme suit :

1. Accédez à **Gestion du trafic** > **GSLB**, puis cliquez sur **Commencer**.
2. Si vous n'avez pas configuré de service ADNS ou de serveur virtuel DNS pour le site, vous pouvez le faire dès maintenant.
   a) Cliquez sur **Afficher**, puis sur **Ajouter**.
   b) Entrez le nom du service, l'adresse IP et sélectionnez le protocole (ADNS/ADNS_TCP) via lequel les données sont échangées avec le service.
3. Sélectionnez **Active-Active Site**.
4. Entrez le nom de domaine complet et spécifiez la période pendant laquelle l'enregistrement doit être mis en cache par les proxies DNS.
5. Configurez les sites GSLB. Chaque site doit être configuré avec un site GSLB local, et la configuration de chaque site doit inclure tous les autres sites en tant que sites GSLB distants. Il ne peut y avoir qu'un seul site local et tous les autres sites sont des sites distants.
   a) Entrez les détails du site, tels que le nom du site et l'adresse IP du site.
   b) Sélectionnez le type de site DISTANT ou LOCAL.
   c) Modifiez éventuellement le mot de passe RPC et, si nécessaire, sécurisez-le.
   d) Si un moniteur doit être lié au service GSLB, sélectionnez la condition dans laquelle le moniteur doit surveiller le service. Cela ne sera effectif qu'une fois qu'un moniteur sera lié aux services. Les conditions possibles sont les suivantes :
      - **TOUJOURS**. Surveillez le service GSLB à tout moment.
      - **MEP échoue**. Surveillez le service GSLB uniquement lorsque l'échange de métriques via MEP échoue.
      - **Le MEP échoue et l'ID de service est en panne.** L'échange de métriques via MEP est activé mais l'état du service, mis à jour via l'échange de métriques, est DOWN.
6. Configurez les services GSLB. Pour créer un site actif, vous devez ajouter au moins deux services GSLB.
   a) Entrez les détails du service, tels que le nom du service, le type de service et le numéro de port.
   b) Associez le service à un site (local ou distant) en sélectionnant le site GSLB auquel appartient le service GSLB.
   c) Sélectionnez le moniteur qui doit être lié au service en cas de défaillance du MEP, si nécessaire. Le service peut être un serveur existant ou vous pouvez créer un nouveau serveur ou un serveur virtuel.

d) Pour associer un serveur existant, sélectionnez le nom du serveur. L'adresse IP du service est automatiquement renseignée.
   - Si l'adresse IP publique est différente de l'adresse IP du serveur, ce qui peut se produire dans un environnement NAT, entrez l'adresse IP publique et le numéro de port du port public.
   - Pour associer un nouveau serveur, créez-en un en saisissant les détails IP du serveur, son adresse IP publique et le numéro de port public.
   - Pour associer un serveur virtuel, sélectionnez un serveur virtuel existant ou cliquez sur + et ajoutez un nouveau serveur virtuel. Ce serveur virtuel est le serveur virtuel d'équilibrage de charge auquel ce service GSLB sera associé.

7. Configurez les serveurs virtuels GSLB.
   a) Entrez le nom du serveur virtuel GSLB et sélectionnez le type d'enregistrement DNS.
   b) Cliquez sur **** dans la zone **Sélectionner un service** et choisissez les services GSLB à lier au serveur virtuel GSLB.
   c) Cliquez sur **** dans la zone **Liaison de domaine** pour sélectionner le domaine à lier à ce serveur virtuel GSLB.
   d) Choisissez la méthode GSLB pour sélectionner le service GSLB le plus performant. Les valeurs par défaut de la méthode GSLB, de la méthode de sauvegarde et de la pondération dynamique sont renseignées automatiquement par défaut. Vous pouvez les modifier si nécessaire.
      - Si vous choisissez la méthode **basée sur un algorithme**, sélectionnez la méthode principale et la méthode de sauvegarde et spécifiez également l'option de pondération dynamique.
      - Si vous choisissez la méthode de **proximité statique**, sélectionnez la méthode de sauvegarde et la méthode de pondération dynamique. Indiquez également l'emplacement du fichier de base de données en cliquant sur l'icône > ou ajoutez un nouvel emplacement en cliquant sur **+** dans la zone Sélectionner une base de données d'emplacement.
      - Si vous choisissez la méthode de **proximité dynamique (RTT)**, sélectionnez la méthode de sauvegarde et spécifiez l'option de pondération dynamique et la valeur de temps aller-retour en fonction de laquelle le service le plus performant doit être sélectionné.
8. Cliquez sur **Terminé** si la configuration est terminée. Le tableau de bord GSLB s'affiche.
9. Si vous avez modifié la configuration du site GSLB, cliquez sur **Synchroniser automatiquement GSLB** dans le tableau de bord pour synchroniser la configuration avec les autres sites de la configuration GSLB.
   - Avant la synchronisation, assurez-vous que la configuration du site local inclut des informations sur les sites distants. De plus, pour que la synchronisation soit réussie, le site local doit être configuré sur les autres appliances NetScaler.

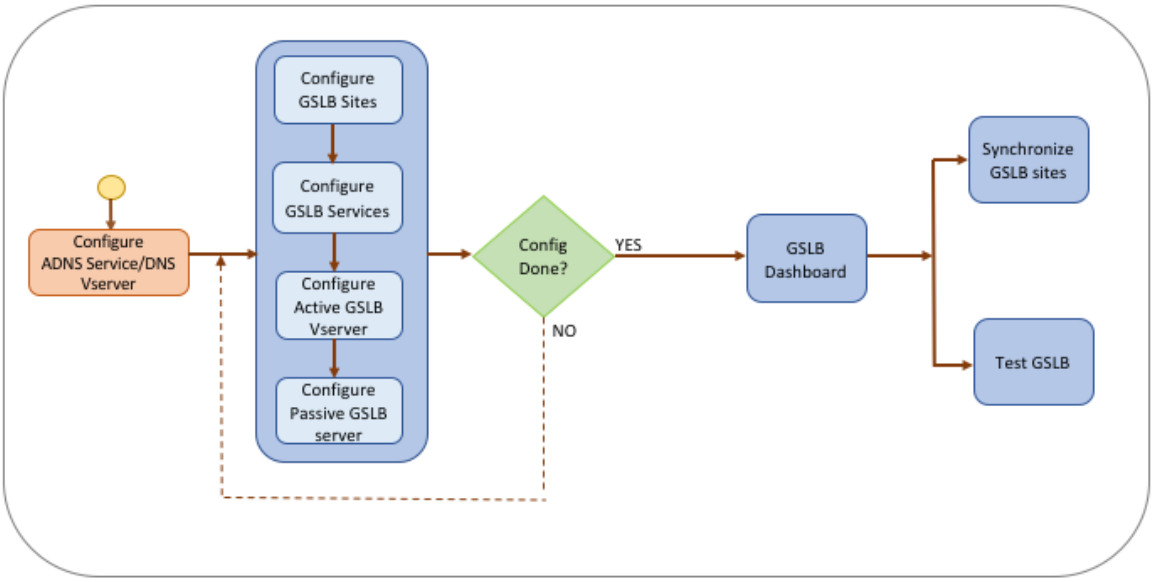
- Si la synchronisation en temps réel est activée, il n'est pas nécessaire de cliquer sur **Synchroniser automatiquement GSLB**. La synchronisation s'effectue automatiquement. Pour activer la synchronisation en temps réel, procédez comme suit :
  a) Accédez à **Gestion du trafic** > **GSLB** > **Tableau de bord** et cliquez sur **Modifier les paramètres GSLB**.
  b) Cochez la case **Synchronisation automatique** des configurations.

10. Cliquez sur **Tester l'installation GSLB** pour vous assurer que les services ADNS ou les serveurs DNS répondent avec l'adresse IP correcte pour le nom de domaine configuré dans la configuration GSLB.

Configurer le site actif-passif

May 5, 2023

La figure suivante montre le flux de travail impliqué dans la configuration active-passive du site.



Avant de commencer à configurer un site actif-passif, assurez-vous d'avoir configuré une configuration d'équilibrage de charge standard pour chaque parc de serveurs ou centre de données.

En outre, pour synchroniser la configuration GSLB entre les sites GSLB du déploiement, assurez-vous que :

- Les sites GLSB locaux sont configurés sur toutes les appliances de la configuration GSLB.
- Vous avez activé l'accès à la gestion sur tous les sites GSLB dans la configuration.
- Vous avez configuré le pare-feu pour qu'il accepte la synchronisation automatique et les connexions MEP.

- Les appliances NetScaler maître et esclave exécutent les mêmes versions du logiciel NetScaler.
- Toutes les appliances NetScaler participant en tant que sites doivent disposer de la même version du logiciel NetScaler (les sites ne sont pas dans une relation maître-esclave).
- Le mot de passe du nœud RPC est le même pour tous les sites GSLB de la configuration GSLB.

Pour configurer un site actif-passif à l'aide de l'assistant

Dans l'onglet Configuration, procédez comme suit :

1. Accédez à **Gestion du trafic** > **GSLB**, puis cliquez sur **Commencer**.
2. Si vous n'avez pas configuré de service ADNS ou de serveur virtuel DNS pour le site, vous pouvez le faire dès maintenant.
   a) Cliquez sur **Afficher**, puis sur **Ajouter**.
   b) Entrez le nom du service, l'adresse IP et sélectionnez le protocole (ADNS/ADNS_TCP) via lequel les données sont échangées avec le service.
3. Sélectionnez Site **actif-passif**.
4. Entrez le nom de domaine complet et spécifiez la période pendant laquelle l'enregistrement doit être mis en cache par les proxies DNS.
5. Configurez les sites GSLB. Chaque site doit être configuré avec un site GSLB local, et la configuration de chaque site doit inclure tous les autres sites en tant que sites GSLB distants. Il ne peut y avoir qu'un seul site local et tous les autres sites sont des sites distants.
   a) Entrez les détails du site, tels que le nom du site et l'adresse IP du site.
   b) Sélectionnez le type de site DISTANT ou LOCAL.
   c) Modifiez éventuellement le mot de passe RPC et, si nécessaire, sécurisez-le.
   d) Si un moniteur doit être lié au service GSLB, sélectionnez la condition dans laquelle le moniteur doit surveiller le service. Cela ne sera effectif qu'une fois qu'un moniteur sera lié aux services. Les conditions possibles sont les suivantes :
      - **TOUJOURS**. Surveillez le service GSLB à tout moment.
      - **MEP échoue**. Surveillez le service GSLB uniquement lorsque l'échange de métriques via MEP échoue.
      - **Le MEP échoue et l'ID de service est en panne.** L'échange de métriques via MEP est activé mais l'état du service, mis à jour via l'échange de métriques, est DOWN.
6. Configurez les services GSLB.
   a) Entrez les détails du service, tels que le nom du service, le type de service et le numéro de port.
   b) Associez le service à un site (local ou distant) en sélectionnant le site GSLB auquel appartient le service GSLB.
   c) Sélectionnez le moniteur qui doit être lié au service en cas de défaillance du MEP, si nécessaire. Le service peut être un serveur existant ou vous pouvez créer un nouveau serveur ou un serveur virtuel.

d) Pour associer un serveur existant, sélectionnez le nom du serveur. L'adresse IP du service est automatiquement renseignée.
   - Si l'adresse IP publique est différente de l'adresse IP du serveur, ce qui peut se produire dans un environnement NAT, entrez l'adresse IP publique et le numéro de port du port public.
   - Pour associer un nouveau serveur, créez-en un en saisissant les détails IP du serveur, son adresse IP publique et le numéro de port public.
   - Pour associer un serveur virtuel, sélectionnez un serveur virtuel existant ou cliquez sur **+** et ajoutez un nouveau serveur virtuel. Ce serveur virtuel est le serveur virtuel d'équilibrage de charge auquel ce service GSLB sera associé.

7. Configurez les serveurs virtuels de sauvegarde GSLB. Les serveurs virtuels de sauvegarde GSLB ne deviennent opérationnels que lorsque les serveurs virtuels GSLB principaux sont inaccessibles ou qu'ils sont marqués comme étant hors service pour une raison quelconque.
   a) Entrez le nom du serveur virtuel GSLB et sélectionnez le type d'enregistrement DNS.
   b) Cliquez sur **** dans **Service Binding**, puis choisissez les services GSLB qui doivent être liés au serveur virtuel GSLB.
   c) Choisissez la méthode GSLB pour sélectionner le service GSLB le plus performant. Les valeurs par défaut de la méthode GSLB, de la méthode de sauvegarde et de la pondération dynamique sont renseignées automatiquement par défaut. Vous pouvez les modifier si nécessaire.
      - Si vous choisissez la méthode **basée sur un algorithme**, sélectionnez la méthode principale et la méthode de sauvegarde.
      - Si vous choisissez la méthode de **proximité statique**, sélectionnez la méthode de sauvegarde et indiquez l'emplacement du fichier de base de données.
      - Si vous choisissez la méthode de **proximité dynamique (RTT)**, sélectionnez la méthode de sauvegarde et spécifiez le poids du service et la valeur RTT en fonction desquels le service le plus performant doit être sélectionné.

8. Configurez les serveurs virtuels GSLB.
   a) Entrez le nom du serveur virtuel GSLB et sélectionnez le type d'enregistrement DNS.
   b) Cliquez sur **** dans la zone **Sélectionner un service** et choisissez les services GSLB à lier au serveur virtuel GSLB.
   c) Cliquez sur **** dans la zone **Liaison de domaine** pour sélectionner le domaine à lier à ce serveur virtuel GSLB.
   d) Choisissez la méthode GSLB pour sélectionner le service GSLB le plus performant. Les valeurs par défaut de la méthode GSLB, de la méthode de sauvegarde et de la pondération dynamique sont renseignées automatiquement par défaut. Vous pouvez les modifier si nécessaire.
      - Si vous choisissez la méthode **basée sur un algorithme**, sélectionnez la méthode principale et la méthode de sauvegarde et spécifiez également l'option de pondéra-

tion dynamique.

- Si vous choisissez la méthode de **proximité statique**, sélectionnez la méthode de sauvegarde et la méthode de pondération dynamique. Indiquez également l'emplacement du fichier de base de données en cliquant sur l'icône **** ou ajoutez un nouvel emplacement en cliquant sur **+** dans la zone Sélectionner une base de données d'emplacements.
- Si vous choisissez la méthode de **proximité dynamique (RTT)**, sélectionnez la méthode de sauvegarde et spécifiez l'option de pondération dynamique et la valeur de temps aller-retour en fonction de laquelle le service le plus performant doit être sélectionné.

9. Cliquez sur **Terminé** si la configuration est terminée. Le tableau de bord GSLB s'affiche.
10. Si vous avez modifié la configuration du site GSLB, cliquez sur **Synchroniser automatiquement GSLB** dans le tableau de bord pour synchroniser la configuration avec les autres sites de la configuration GSLB.
    - Avant la synchronisation, assurez-vous que la configuration du site local inclut des informations sur les sites distants. De plus, pour que la synchronisation soit réussie, le site local doit être configuré sur les autres appliances NetScaler.
    - Si la synchronisation en temps réel est activée, il n'est pas nécessaire de cliquer sur **Synchroniser automatiquement GSLB**. La synchronisation s'effectue automatiquement. Pour activer la synchronisation en temps réel, procédez comme suit :
        a) Accédez à **Gestion du trafic** > **GSLB** > **Tableau de bord** et cliquez sur **Modifier les paramètres GSLB**.
        b) Cochez la case **Synchronisation automatique** des configurations.
11. Cliquez sur **Tester l'installation GSLB** pour vous assurer que les services ADNS ou les serveurs DNS répondent avec l'adresse IP correcte pour le nom de domaine configuré dans la configuration GSLB.

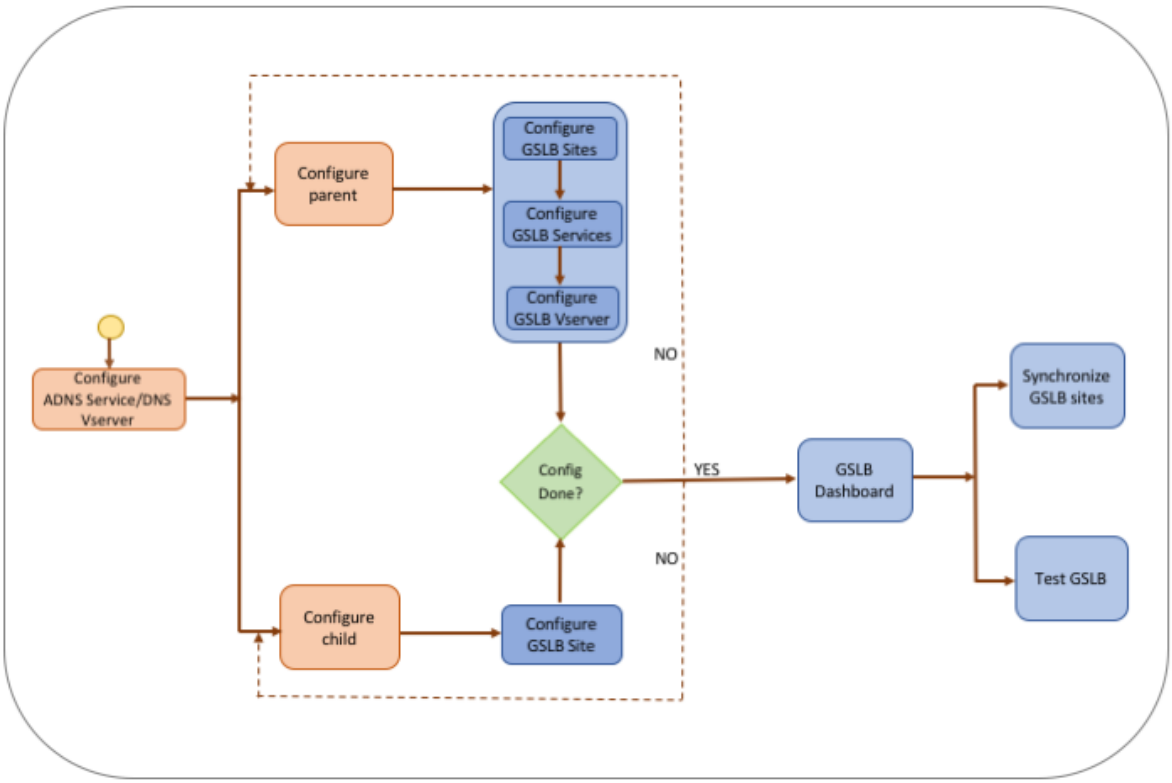
> **Remarque**
>
> Pour plus d'informations sur la configuration des entités GSLB d'une configuration GSLB actif-passive pour la reprise après sinistre, voir Configuration de GSLB pour la reprise après sinistre.

Configuration de la topologie parent-enfant

May 5, 2023

Dans une topologie parent-enfant, au niveau supérieur se trouvent les sites parents, qui entretiennent des relations entre pairs et d'autres parents. Chaque parent peut disposer de plusieurs sites pour enfants, et chaque site parent échange des informations de santé avec ses sites pour enfants et avec d'autres sites parents. Toutefois, un site enfant communique uniquement avec son site parent.

La figure suivante montre le flux de travail impliqué dans une configuration de topologie parent-enfant GSLB.



Avant de commencer à configurer le déploiement de la topologie parent-enfant, assurez-vous d'avoir configuré une configuration d'équilibrage de charge standard pour chaque parc de serveurs ou centre de données.

En outre, pour synchroniser la configuration GSLB entre les sites GSLB du déploiement, assurez-vous que :

- Les sites GLSB locaux sont configurés sur toutes les appliances de la configuration GSLB.
- Vous avez activé l'accès à la gestion sur tous les sites GSLB dans la configuration.
- Vous avez configuré le pare-feu pour qu'il accepte la synchronisation automatique et les connexions MEP.
- Toutes les appliances NetScaler participant en tant que sites doivent disposer de la même version du logiciel NetScaler (les sites ne sont pas dans une relation maître-esclave).
- Le mot de passe du nœud RPC est le même pour tous les sites GSLB de la configuration GSLB.

Pour configurer un déploiement parent-enfant à l'aide de l'assistant

Dans l'onglet Configuration, procédez comme suit :

1. Accédez à **Gestion du trafic** > **GSLB**, puis cliquez sur **Commencer**.

2. Si vous n'avez pas configuré de serveur ADNS ou de serveur virtuel DNS pour le site, vous pouvez le faire dès maintenant.
   a) Cliquez sur **Afficher**, puis sur **Ajouter**.
   b) Entrez le nom du service, l'adresse IP et sélectionnez le protocole (ADNS/ADNS_TCP) via lequel les données sont échangées avec le service.
3. Sélectionnez la **topologie parent-enfant.**
4. Dans le champ Sélectionnez le type de site, choisissez ;
   - **Parent** : lors de la configuration du site parent, vous devez configurer ses sites enfants associés ainsi que les autres sites parents dans la configuration GSLB.
   - **Enfant** : lors de la configuration du site enfant, vous devez configurer uniquement le site enfant et son site parent.

Pour configurer un site parent

1. Entrez le nom de domaine complet et spécifiez la période pendant laquelle l'enregistrement doit être mis en cache par les proxies DNS.
2. Configurez les sites GSLB. Chaque site doit être configuré avec un site GSLB local, et la configuration de chaque site doit inclure tous les autres sites en tant que sites GSLB distants. Il ne peut y avoir qu'un seul site local. Tous les autres sites sont des sites distants. Si l'adresse IP du site spécifiée appartient à l'appliance (par exemple, une adresse MIP ou une adresse SNIP), le site est un site local. Dans le cas contraire, il s'agit d'un site distant.
3. Entrez les détails du site, tels que le nom du site et l'adresse IP du site.
   a) Sélectionnez le type de site.
   b) Modifiez éventuellement le mot de passe RPC et, si nécessaire, sécurisez-le.
   c) Si un moniteur doit être lié au service GSLB, sélectionnez la condition dans laquelle le moniteur doit surveiller le service. Cela ne sera effectif qu'une fois qu'un moniteur sera lié aux services. Les conditions possibles sont les suivantes :
      - **Always**. Surveillez le service GSLB à tout moment.
      - **MEP échoue**. Surveillez le service GSLB uniquement lorsque l'échange de métriques via MEP échoue.
      - **Le MEP échoue et le service est en panne.** L'échange de métriques via MEP est activé mais l'état du service, mis à jour via l'échange de métriques, est DOWN.
4. Configurez les services GSLB.
   a) Entrez les détails du service tels que le nom du service, le type de service et le numéro de port.
   b) Associez le service à un site (local ou distant) en sélectionnant le site GSLB auquel appartient le service GSLB.
   c) Sélectionnez le moniteur qui doit être lié au service en cas de défaillance du MEP, si nécessaire. Le service peut être un serveur existant ou vous pouvez créer un nouveau serveur ou un serveur virtuel.

- Pour associer un serveur existant, sélectionnez le nom du serveur. L'adresse IP du service est renseignée automatiquement.
- Pour associer un nouveau serveur, créez-en un en saisissant les détails IP du serveur, son adresse IP publique et le numéro de port public.
- Pour associer un serveur virtuel, sélectionnez un serveur virtuel existant ou cliquez sur **+** et ajoutez un nouveau serveur virtuel. Ce serveur virtuel est le serveur virtuel d'équilibrage de charge auquel ce service GSLB sera associé. Si l'adresse IP publique est différente de l'adresse IP du serveur, ce qui peut se produire dans un environnement NAT, entrez l'adresse IP publique et le numéro de port public.

5. Configurez les serveurs virtuels GSLB.
   a) Entrez le nom du serveur virtuel GSLB et sélectionnez le type d'enregistrement DNS.
   b) Cliquez sur **** dans la zone **Sélectionner un service** et choisissez les services GSLB à lier au serveur virtuel GSLB.
   c) Cliquez sur **** dans la zone **Liaison** de domaine pour afficher le nom de domaine lié au serveur virtuel GSLB.
   d) Choisissez la méthode GSLB pour sélectionner le service GSLB le plus performant. Les valeurs par défaut de la méthode GSLB, de la méthode de sauvegarde et de la pondération dynamique sont automatiquement renseignées par défaut. Vous pouvez les modifier si nécessaire.
      - Si vous choisissez la méthode **basée sur un algorithme**, sélectionnez la méthode principale et la méthode de sauvegarde et spécifiez également l'option de pondération dynamique.
      - Si vous choisissez la méthode de **proximité statique**, sélectionnez la méthode de sauvegarde et la méthode de pondération dynamique. Indiquez également l'emplacement du fichier de base de données en cliquant sur l'icône **** ou ajoutez un nouvel emplacement en cliquant sur **+** dans la zone Sélectionner une base de données d'emplacements.
      - Si vous choisissez la méthode de **proximité dynamique (RTT)**, sélectionnez la méthode de sauvegarde et spécifiez le poids du service et la valeur RTT en fonction desquels le service le plus performant doit être sélectionné.
6. Cliquez sur **Terminé** si la configuration est terminée. Le tableau de bord GSLB s'affiche.
7. Si vous avez modifié la configuration du site parent GSLB, cliquez sur Synchroniser **automatiquement GSLB pour synchroniser** la configuration avec les autres sites parents de la configuration GSLB. Dans une topologie parent-enfant, la synchronisation des sites enfants est ignorée.
   - Avant la synchronisation, assurez-vous que la configuration du site local inclut des informations sur les sites distants.
   - Si la synchronisation en temps réel est activée, il n'est pas nécessaire de cliquer sur **Synchroniser automatiquement GSLB**. La synchronisation s'effectue automatiquement.

Pour activer la synchronisation en temps réel, procédez comme suit :

a) Accédez à **Gestion du trafic** > **GSLB** > **Tableau de bord** et cliquez sur **Modifier les paramètres GSLB**.

b) Cochez la case **Synchronisation automatique** des configurations.

8. Cliquez sur **Tester l'installation GSLB** pour vous assurer que les services ADNS ou les serveurs DNS répondent avec l'adresse IP correcte pour le nom de domaine configuré dans la configuration GSLB.

Pour configurer un site enfant

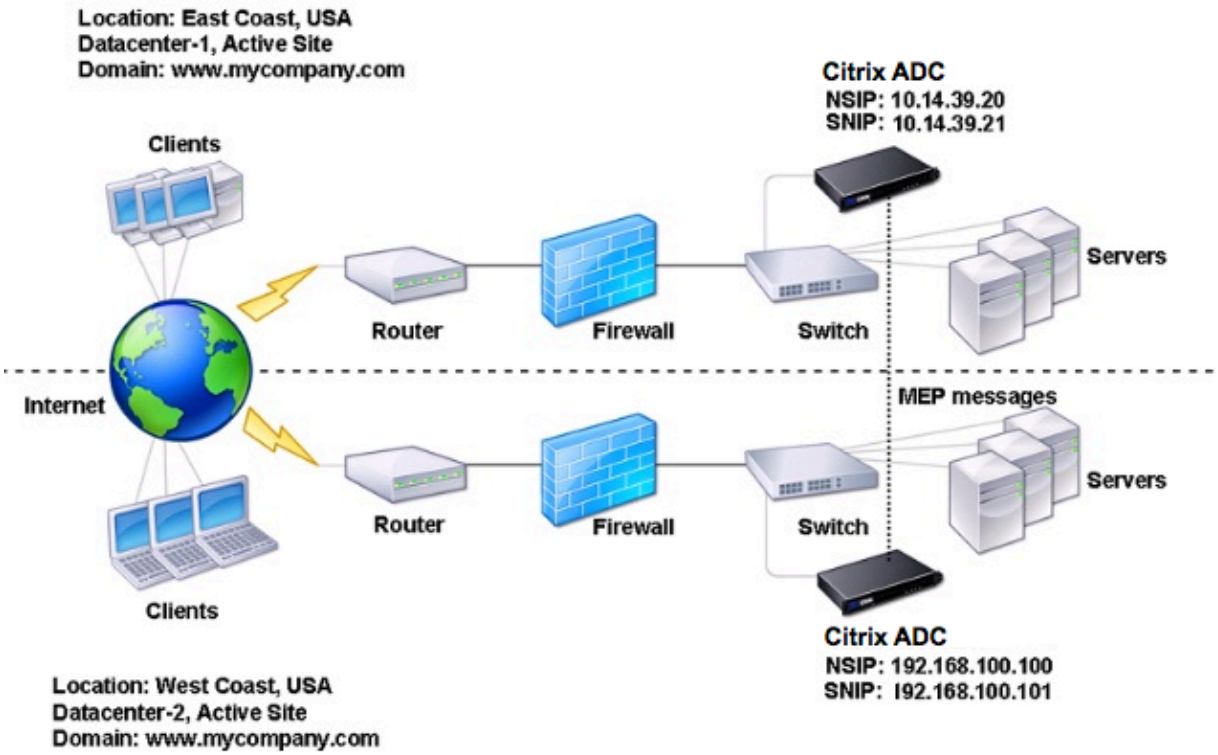
1. Configurez les sites GSLB.
   a) Entrez les détails du site, tels que le nom du site et l'adresse IP du site.
   b) Sélectionnez le type de site.
   c) Modifiez éventuellement le mot de passe RPC et, si nécessaire, sécurisez-le. 4. Si un moniteur est lié au service GSLB, sélectionnez la condition dans laquelle le moniteur doit surveiller le service. Les conditions possibles sont les suivantes :
      - **Always**. Surveillez le service GSLB à tout moment.
      - **MEP échoue**. Surveillez le service GSLB uniquement lorsque l'échange de métriques via MEP échoue.
      - **Le MEP échoue et le service est en panne.** L'échange de métriques via MEP est activé mais l'état du service, mis à jour via l'échange de métriques, est DOWN.
2. Cliquez sur **Terminé** si la configuration est terminée. Le tableau de bord GSLB s'affiche.
3. Cliquez sur **Tester l'installation GSLB** pour vous assurer que les services ADNS ou les serveurs DNS répondent avec l'adresse IP correcte pour le nom de domaine configuré dans la configuration GSLB.

Configurez les entités GSLB individuellement

May 5, 2023

L'équilibrage global de la charge des serveurs est utilisé pour gérer le flux de trafic vers un site Web hébergé sur deux batteries de serveurs distinctes, idéalement situées dans des emplacements géographiques différents. Prenons l'exemple d'un site Web, www.mycompany.com, qui est hébergé sur deux batteries de serveurs ou centres de données géographiquement séparés. Les deux batteries de serveurs utilisent des appliances NetScaler. Les appliances NetScaler de ces batteries de serveurs sont configurées en mode bras unique et fonctionnent comme des serveurs DNS faisant autorité pour le domaine www.mycompany.com. La figure suivante illustre cette configuration.

Figure 1. Topologie GSLB de base



Pour configurer une telle configuration GSLB, vous devez d'abord configurer une configuration d'équilibrage de charge standard pour chaque parc de serveurs ou centre de données. Cela vous permet d'équilibrer la charge entre les différents serveurs de chaque parc de serveurs. Configurez ensuite les deux appliances NetScaler en tant que serveurs DNS (ADNS) faisant autorité. Ensuite, créez un site GSLB pour chaque parc de serveurs, configurez des serveurs virtuels GSLB pour chaque site, créez des services GLSB et liez les services GSLB aux serveurs virtuels GSLB. Enfin, liez le domaine aux serveurs virtuels GSLB. Les configurations GSLB sur les deux appliances sur les deux sites différents sont identiques, bien que les configurations d'équilibrage de charge pour chaque site soient spécifiques à ce site.

Remarque : Pour configurer un site GSLB dans une configuration de cluster NetScaler, consultez Configuration de GSLBdans un cluster.

Configuration d'une configuration d'équilibrage de charge standard

Un serveur virtuel d'équilibrage de charge équilibre la charge entre les différents serveurs physiques du centre de données. Ces serveurs sont représentés sous forme de services sur l'appliance NetScaler, et les services sont liés au serveur virtuel d'équilibrage de charge.

Pour plus d'informations sur la configuration d'une configuration d'équilibrage de charge de base, voir Équilibrage de charge.

Configurer un service DNS faisant autorité

May 5, 2023

Lorsque vous configurez l'appliance NetScaler en tant que serveur DNS faisant autorité, elle accepte les demandes DNS du client et répond avec l'adresse IP du centre de données auquel le client doit envoyer les demandes.

Remarque : Pour que l'appliance NetScaler fasse autorité, vous devez également créer des enregistrements SOA et NS. Pour plus d'informations sur les enregistrements SOA et NS, voir Système de noms de domaine.

Pour créer un service ADNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service ADNS et vérifier la configuration :

```
add service <name> <IP>@ ADNS <port>

show service <name>
<!--NeedCopy-->
```

Exemple :

```
add service Service-ADNS-1 10.14.39.21 ADNS 53

show service Service-ADNS-1
<!--NeedCopy-->
```

Pour modifier un service ADNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set service <name> <IPAddress> ADNS <port>
<!--NeedCopy-->
```

Exemple :

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```


Pour supprimer un service ADNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
rm service <name>
<!--NeedCopy-->
```

Exemple :

```
rm service Service-ADNS-1
<!--NeedCopy-->
```

Pour configurer un service ADNS à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Ajoutez un nouveau service ADNS ou sélectionnez un service existant et modifiez ses paramètres.

Configuration d'un site GSLB de base

May 5, 2023

Un site GSLB est une représentation d'un centre de données de votre réseau et un regroupement logique de serveurs virtuels GSLB, de services et d'autres entités du réseau. Généralement, dans une configuration GSLB, de nombreux sites GSLB sont équipés pour diffuser le même contenu à un client. Ils sont généralement séparés géographiquement pour garantir que le domaine est actif même si un site tombe complètement en panne. Tous les sites de la configuration GSLB doivent être configurés sur chaque appliance NetScaler hébergeant un site GSLB. En d'autres termes, sur chaque site, vous configurez le site GSLB local et chaque site GSLB distant.

Une fois que les sites GSLB sont créés pour un domaine, l'appliance NetScaler envoie les demandes des clients au site GSLB approprié, selon les algorithmes GSLB configurés.

Pour créer un site GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un site GSLB et vérifier la configuration :

```
add gslb site <siteName> <siteIPAddress>
show gslb site <siteName>
<!--NeedCopy-->
```


Exemple :

```
add gslb site Site-GSLB-East-Coast 10.14.39.21
show glsb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour modifier ou supprimer un site GSLB à l'aide de l'interface de ligne de commande

- Pour modifier un site GSLB, utilisez la commande set gslb site, comme si vous utilisiez la commande add gslb site, sauf que vous entrez le nom d'un site GSLB existant.
- Pour annuler la définition d'un paramètre de site, utilisez la commande unset gslb site, suivie de la valeur siteName et du nom du paramètre à rétablir à sa valeur par défaut.
- Pour supprimer un site GSLB, utilisez la commande rm gslb site, qui accepte uniquement l'argument. <name>

Pour configurer un site GSLB de base à l'aide de l'utilitaire de configuration

1. **Accédez à**Gestion du trafic**>**GSLB > Sites**.**
2. Ajoutez un nouveau site GSLB ou sélectionnez un site GSLB existant et modifiez ses paramètres.

Pour consulter les statistiques d'un site GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat gslb site <siteName>
<!--NeedCopy-->
```

Exemple :

```
stat gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Pour consulter les statistiques d'un site GSLB à l'aide de l'utilitaire de configuration

1. **Accédez à**Gestion du trafic**>**GSLB > Sites**.**
2. Sélectionnez le site GSLB et cliquez sur **Statistiques**.

Configurer un service GSLB

August 20, 2021

Un service GSLB est une représentation d'un serveur virtuel d'équilibrage de charge ou de commutation de contenu. Un service GSLB local représente un serveur virtuel d'équilibrage de charge ou de commutation de contenu local. Un service GSLB distant représente un serveur virtuel d'équilibrage de charge ou de commutation de contenu configuré sur l'un des autres sites de la configuration GSLB. Sur chaque site de la configuration GSLB, vous pouvez créer un service GSLB local et n'importe quel nombre de services GSLB distants.

> **Important**
>
> Si le serveur virtuel d'équilibrage de charge se trouve dans un nœud GSLB lui-même ou dans un nœud enfant (dans le déploiement parent-enfant) et qu'aucun moniteur n'est lié au service GSLB, assurez-vous que les éléments suivants :
>
> L'adresse IP du service GLSB, le numéro de port et le protocole correspondent au que le service représente. Sinon, l'état du service est marqué comme étant DOWN.

Pour créer un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service GSLB et vérifier la configuration :

```
1 add gslb service <serviceName> <serverName | IP> <serviceType> <port>-
     siteName <string>
2 show gslb service <serviceName>
3 <!--NeedCopy-->
```

Exemple :

```
1 add gslb service Service-GSLB-1 10.14.39.14 HTTP 80  - siteName Site-
     GSLB-East-Coast
2 show gslb service Service-GSLB-1
3 <!--NeedCopy-->
```

Pour modifier ou supprimer un service GSLB à l'aide de l'interface de ligne de commande

- Pour modifier un service GSLB, utilisez la commande <serviceName> set gslb service. Pour cette commande, spécifiez le nom du service GSLB dont vous souhaitez modifier la configuration. Vous pouvez modifier les valeurs existantes des paramètres spécifiés par vous ou définis

par défaut. Vous pouvez modifier la valeur de plusieurs paramètres dans la même commande. Reportez-vous à la commande add gslb service pour plus de détails sur les paramètres. Exemple

```
> set gslb service SKP_GSLB_NOTCNAME_SVC2 -maxBandWidth 25 -
   maxClient 8
Done
> sh gslb service SKP_GSLB_NOTCNAME_SVC2
SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
...
Max Conn: 8  Max Bandwidth: 25 kbits
<!--NeedCopy-->
```

- Pour réinitialiser un paramètre à sa valeur par défaut, vous pouvez utiliser la commande <serviceName> unset gslb service et les paramètres à annuler. Exemple

```
> unset gslb service SKP_GSLB_NOTCNAME_SVC2 maxBandWidth
Done
> sh gslb service SKP_GSLB_NOTCNAME_SVC2
SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
...
Max Conn: 8  Max Bandwidth: 0 kbits
<!--NeedCopy-->
```

- Pour supprimer un service GSLB, utilisez la commande <serviceName> rm gslb service.

Pour créer un service GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services**.
2. Ajoutez un nouveau service GSLB ou sélectionnez un service existant et modifiez ses paramètres.

Pour afficher les statistiques d'un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
stat gslb service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
stat gslb service Service-GSLB-1
<!--NeedCopy-->
```


Pour afficher les statistiques d'un service GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services**.
2. Sélectionnez le service GSLB et cliquez sur **Statistiques**.

Configurer un groupe de services GSLB

May 5, 2023

Le groupe de services vous permet de gérer un groupe de services aussi facilement qu'un seul service. Si vous activez ou désactivez une option pour un groupe de services, l'option est activée ou désactivée pour tous les membres du groupe de services. Par exemple, vous pouvez appliquer cette fonctionnalité à des options telles que la compression, la surveillance de l'état et l'arrêt progressif.

Après avoir créé un groupe de services, vous pouvez effectuer l'une des opérations suivantes :

- Liez le groupe de services à un serveur virtuel.
- Ajoutez des services au groupe de services.
- Liez les moniteurs aux groupes de services.

> **Important**
>
> Si le serveur virtuel d'équilibrage de charge se trouve soit dans un nœud GSLB lui-même, soit dans un nœud enfant (dans un déploiement parent-enfant) et qu'aucun moniteur n'est lié au service GSLB, vérifiez les points suivants : L'adresse IP,
>
> le numéro de port et le protocole du groupe de services GLSB correspondent au serveur virtuel sur lequel le service est représentant. Sinon, l'état du service est marqué comme DOWN.

NetScaler prend en charge les types de groupes de services GSLB suivants.

- Groupes de services basés sur l'adresse IP
- Groupes de services basés sur le nom de
- Groupes de services autoscale basés sur le nom de domaine

Groupes de services autoscale basés sur le nom de domaine GSLB

La solution d'équilibrage de charge globale des serveurs (GSLB) hybride et multicloud de NetScaler permet aux clients de répartir le trafic applicatif entre plusieurs centres de données dans des clouds hybrides, plusieurs clouds et sur site. La solution NetScaler GSLB prend en charge diverses solutions d'équilibrage de charge, telles que l'équilibreur de charge NetScaler, Elastic Load Balancing (ELB) pour AWS et d'autres équilibreurs de charge tiers. En outre, la solution GSLB effectue un équilibrage de charge global même si les couches GSLB et d'équilibrage de charge sont gérées indépendamment.

Dans les déploiements cloud, les utilisateurs reçoivent un nom de domaine comme référence lorsqu'ils accèdent à la solution d'équilibrage de charge à des fins de gestion. Il est recommandé que les entités externes n'utilisent pas les adresses IP vers lesquelles ces noms de domaine sont résolus. En outre, les couches d'équilibrage de charge augmentent ou diminuent en fonction de la charge, et il n'est pas garanti que les adresses IP soient statiques. Par conséquent, il est recommandé d'utiliser le nom de domaine pour faire référence aux points de terminaison d'équilibrage de charge au lieu des adresses IP. Cela nécessite que les services GSLB soient référencés à l'aide du nom de domaine au lieu d'adresses IP et qu'ils doivent consommer toutes les adresses IP renvoyées pour le nom de domaine de la couche d'équilibrage de charge et avoir une représentation de celles-ci dans GSLB.

Pour utiliser des noms de domaine au lieu d'adresses IP lorsque vous faites référence aux points de terminaison d'équilibrage de charge, vous pouvez utiliser les groupes de services basés sur le nom de domaine pour GSLB.

Surveiller les groupes de services basés sur les noms de domaine GSL

L'appliance NetScaler possède deux moniteurs intégrés qui surveillent les applications basées sur le protocole TCP ; et. `tcp-default`ping-`default` Le `tcp-default` moniteur est lié à tous les services TCP et le `ping-default` moniteur est lié à tous les services non TCP. Les moniteurs intégrés sont liés par défaut aux groupes de services GSLB. Toutefois, il est recommandé de lier un moniteur spécifique à l'application aux groupes de services GSLB.

Recommandation pour régler l'option des moniteurs de déclenchement sur MEPDOWN

L'option Trigger Monitors peut être utilisée pour indiquer si le site GSLB doit toujours utiliser les moniteurs, ou utiliser des moniteurs lorsque le protocole d'échange de métriques (MEP) est DOWN.

L'option Trigger Monitors est définie sur TOUJOURS par défaut.

Lorsque l'option Trigger Monitors est réglée sur TOUJOURS, chaque nœud GSLB déclenche les moniteurs indépendamment. Si chaque nœud GSLB déclenche les moniteurs indépendamment, chaque nœud GSLB peut fonctionner sur un ensemble différent de services GSLB. Cela peut entraîner des incohérences dans les réponses DNS pour les requêtes DNS arrivant sur ces nœuds GSLB. En outre, si chaque nœud GSLB surveille indépendamment, le nombre de sondes de surveillance atteignant l'entité d'équilibrage de charge augmente. Les entrées de persistance deviennent également incompatibles entre les nœuds GSLB.

Par conséquent, il est recommandé que l'option Trigger Monitors de l'entité de site GSLB soit définie sur MEPDOWN. Lorsque l'option Trigger Monitors est définie sur MEPDOWN, la résolution du domaine d'équilibrage de charge et la propriété de surveillance appartiennent au nœud GSLB local. Lorsque l'option Trigger Monitors est définie sur MEPDOWN, la résolution du domaine d'équilibrage de charge et la surveillance ultérieure sont effectuées par le nœud GSLB local d'un groupe de services GSLB. Les

résultats sont ensuite propagés à tous les autres nœuds participant au GSLB en utilisant le protocole d'échange de métriques (MEP).

En outre, chaque fois que l'ensemble d'adresses IP associé à un domaine d'équilibrage de charge est mis à jour, il est notifié via MEP.

Limitations des groupes de services GSLB

- Pour un domaine d'équilibrage de charge, l'adresse IP renvoyée dans la réponse DNS est généralement l'adresse IP publique. L'adresse IP privée ne peut pas être appliquée dynamiquement lorsque le domaine d'équilibrage de charge est résolu. Par conséquent, le port IP public et le port IP privé pour les liaisons de port IP des groupes de services autoscale basés sur le nom de domaine GSLB sont identiques. Ces paramètres ne peuvent pas être définis explicitement pour les groupes de services autoscale basés sur le nom de domaine.
- La persistance du site, les vues DNS et le clustering ne sont pas pris en charge pour les groupes de services GSLB.

Configurer et gérer les groupes de services GSLB à l'aide de la CLI

Pour ajouter un groupe de services GSLB :

```
add gslb serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (
    DISABLED | DNS )] -siteName <string>
<!--NeedCopy-->
```

Exemple :

```
add gslb serviceGroup Service-Group-1 http -autoScale DNS -siteName
    Site1
<!--NeedCopy-->
```

Pour lier un groupe de services GSLB à un serveur virtuel :

```
bind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <serverName
    >@ | (-monitorName <string>@))
<!--NeedCopy-->
```

Exemple :

```
bind gslb serviceGroup Service-Group-1 203.0.113.2
bind gslb serviceGroup Service-Group-1 S1 80
bind gslb serviceGroup** Service-Group-1 -monitorName Mon1
<!--NeedCopy-->
```


Pour dissocier un groupe de services GSLB à un serveur virtuel :

```
unbind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <
    serverName>@ | -monitorName <string>@)
<!--NeedCopy-->
```

Exemple :

```
unbind gslb serviceGroup Service-Group-1 -monitorName Mon1
<!--NeedCopy-->
```

Pour définir les paramètres d'un groupe de services GSLB :

```
set gslb serviceGroup <serviceGroupName>@ [(<serverName>@ <port> [-
    weight <positive_integer>] [-hashId <positive_integer>] [-publicIP <
    ip_addr|ipv6_addr|*>] [-publicPort <port>]) | -maxClient <
    positive_integer> | -cip ( ENABLED | DISABLED ) | <cipHeader> | -
    cltTimeout <secs> | -svrTimeout <secs> | -maxBandwidth <
    positive_integer> | -monThreshold <positive_integer> | -
    downStateFlush ( ENABLED | DISABLED )] [-monitorName <string> -
    weight <positive_integer>] [-healthMonitor ( YES | NO )] [-comment <
    string>] [-appflowLog ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Pour annuler la définition des paramètres d'un groupe de services GSLB :

```
unset gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port> [-
    weight] [-hashId] [-publicIP] [-publicPort]] [-maxClient] [-cip] [-
    cltTimeout] [-svrTimeout] [-maxBandwidth] [-monThreshold] [-
    appflowLog] [-monitorName] [-weight] [-healthMonitor] [-cipHeader]
    [-downStateFlush] [-comment]
<!--NeedCopy-->
```

Pour activer un groupe de services GSLB

```
enable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```

Exemple :

```
enable gslb serviceGroup SG1 S1 80
<!--NeedCopy-->
```

Pour désactiver un groupe de services GSLB


```
disable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-
    delay <secs>] [-graceFul ( YES /| NO )]
<!--NeedCopy-->
```

Exemple :

```
disable gslb serviceGroup SRG2 S1 80
<!--NeedCopy-->
```

> **Remarque**
>
> Le groupe de services qui doit être désactivé doit être un groupe de services DBS et non un groupe de services de mise à l'échelle automatique.

Pour supprimer un groupe de services GSLB :

```
rm gslb serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
rm gslb serviceGroup Service-Group-1
<!--NeedCopy-->
```

Pour afficher les statistiques d'un groupe de services GSLB :

```
stat gslb serviceGroup [<serviceGroupName>]
<!--NeedCopy-->
```

Exemple :

```
stat gslb serviceGroup Service-Group-1
<!--NeedCopy-->
```

Pour afficher les propriétés d'un groupe de services GSLB :

```
show gslb serviceGroup [<serviceGroupName>  -includeMembers]
<!--NeedCopy-->
```

Exemple :

```
show gslb serviceGroup SG1
show gslb serviceGroup -includeMembers
<!--NeedCopy-->
```


Activer ou désactiver les membres du groupe de services GSLB

Vous pouvez activer ou désactiver de manière sélective un membre individuel d'un groupe de services GSLB (basé sur DNS) au lieu d'activer ou de désactiver l'ensemble du groupe de services. Cette fonctionnalité est disponible à la fois dans les groupes de services autoscale et dans les groupes de services non autoscale. Par conséquent, la gestion d'un groupe de services GSLB est facilitée.

Par exemple, vous devez éviter le trafic vers un serveur particulier sur un site GSLB. Supposons que 10 services ou serveurs GSLB (S1 à S10) sont liés à un groupe de services (SG1). Vous souhaitez désactiver uniquement le service 5 (S5), c'est-à-dire éviter le trafic vers le serveur 5. Sans cette fonctionnalité, vous devez lier séparément les services S1 à S4 et les services S6 à S10. Ce processus devient fastidieux dans un grand groupe de services GSLB où vous devez désactiver ou activer un grand nombre de services. Cette fonctionnalité vous permet de désactiver directement le service 5 (S5) sans affecter les autres services du groupe de services.

Pour activer un membre du groupe de services GSLB à l'aide de la CLI :

```
enable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour activer un groupe de services GSLB, fournissez uniquement le nom du groupe de services. Pour activer un membre d'un groupe de services, en plus du nom du groupe de services GSLB, fournissez le nom du serveur qui héberge le service et le numéro de port du service.

Exemple :

```
enable gslb serviceGroup http_svc_group 10.102.27.153 80
<!--NeedCopy-->
```

Pour désactiver un groupe de services GSLB ou un membre du groupe de services GSLB à l'aide de l'interface de ligne de commande :

```
disable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```

Exemple :

```
disable gslb serviceGroup http_svc_group 10.102.27.153 80
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour désactiver un groupe de services GSLB, fournissez uniquement le nom du groupe de services. Pour désactiver un membre d'un groupe de services, en plus du nom du groupe de services

> GSLB, fournissez le nom du serveur qui héberge le service et le numéro de port du service.

Modifications apportées aux commandes CLI GSLB existantes

Voici les modifications apportées aux commandes GSLB existantes après l'introduction des groupes de services GSLB :

- `bind gslb vserver` - Le nom du groupe de services est ajouté à la commande de liaison.

  Exemple :

```
bind gslb vserver <name> ((-serviceName <string> [-weight <
    positive_integer>] ) | <serviceGroupName>@ | | (-domainName <
    string> [-TTL <secs>] [-backupIP<ip_addr|ipv6_addr|*>] [-
    cookieDomain <string>] [-cookieTimeout <mins>][-sitedomainTTL
    <secs>]) | (-policyName <string>@ [-priority<positive_integer
    >] [-gotoPriorityExpression <expression>] [-type REQUEST |
    RESPONSE )]))
<!--NeedCopy-->
```

- `unbind gslb vserver` - Le groupe de services est ajouté à la commande unbind.

  Exemple :

```
unbind gslb vserver <name> (-serviceName <string> <
    serviceGroupName> @ /(-domainName <string> [-backupIP] [-
    cookieDomain]) | -policyName <string>@)
<!--NeedCopy-->
```

- `show gslb site` - Lorsque cette commande est exécutée, les groupes de services GSLB sont également affichés.
- `show gslb vs` - Lorsque cette commande est exécutée, les groupes de services GSLB sont affichés.
- `stat gslb vs` - Lorsque cette commande est exécutée, les statistiques des groupes de services GSLB sont également affichées.
- `show lb monitor bindings` - Lorsque cette commande est exécutée, les liaisons du groupe de services GSLB sont également affichées.

Configurer les groupes de services GSLB à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB > Groupes** de **services.**
2. Créez un groupe de services et définissez le mode AutoScale sur DNS.

Configurer la persistance du site pour les groupes de services GSLB

Vous pouvez configurer la persistance du site pour les groupes de services basés sur l'adresse IP et le nom de domaine. La persistance du site n'est pas prise en charge pour les groupes de services de mise à l'échelle automatique basés

Pour définir la persistance du site en fonction des cookies HTTP à l'aide de la CLI

- Pour la persistance du proxy de connexion, il n'est pas nécessaire de définir le préfixe du site.

  À l'invite de commande, tapez :

```
set gslb service group <serviceGroupName> [-sitePersistence <
    sitePersistence>]
<!--NeedCopy-->
```

- Pour la persistance de la redirection HTTP, vous devez d'abord définir le préfixe de site d'un membre du groupe de services, puis définir le paramètre de `HTTPRedirect` persistance pour le groupe de services.

  À l'invite de commande, tapez :

```
set gslb servicegroup <serviceGroupName>  <serviceGroup member
    name|Ip> <port>  [-sitePrefix <string>]

set gslb servicegroup <serviceGroupName> [-sitePersistence <
    sitePersistence>]
<!--NeedCopy-->
```

Exemples :

- persistance du proxy de connexion

```
set gslbservicegroup sg1 -sitePersistence connectionProxy
<!--NeedCopy-->
```

- Persistance de redirection HTTP

```
set gslb servicegroup sg2 test1 80 -sitePrefix vserver-GSLB-1

set gslb servicegroup sg2 -sitePersistence HTTPRedirect
<!--NeedCopy-->
```

Pour définir la persistance du site en fonction des cookies à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Groupes de services** et sélectionnez le groupe de services que vous souhaitez configurer pour la persistance du site (par exemple, ServiceGroup-GSLB-1).
2. Cliquez sur la section **Persistance du site** et définissez la persistance qui répond à vos besoins.

> **Conseil**
>
> Pour obtenir un scénario de déploiement et un exemple de configuration de groupes de services GSLB, consultez les rubriques suivantes :
>
> - Cas d'utilisation : déploiement d'un groupe de services Autoscale basé sur un nom de domaine
> - Cas d'utilisation : Déploiement d'un groupe de services de mise à l'échelle automatique basé sur l'adresse IP

Configuration d'un serveur virtuel GSLB

May 5, 2023

Un serveur virtuel GSLB est une entité qui représente un ou plusieurs services GSLB et équilibre le trafic entre eux. Il évalue les méthodes ou algorithmes GSLB configurés pour sélectionner un service GSLB auquel envoyer la demande du client.

> **Remarque**
>
> Une exigence du protocole de serveur virtuel GSLB consiste principalement à créer une relation entre le serveur virtuel et les services qui sont liés au serveur virtuel. Cela permet également de garantir la cohérence des CLI et des API pour les autres types de serveurs virtuels. Le paramètre Type de service sur un service ou un serveur virtuel n'est pas utilisé lors du traitement des requêtes DNS. Il est plutôt référencé lors de la persistance du site, de la surveillance et pour effectuer des recherches via MEP.

Pour créer un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez les commandes suivantes pour ajouter un serveur virtuel GSLB et vérifier la configuration :

```
1 -  add gslb vserver <name> <serviceType> -ipType (IPv4 | IPv6)
2 -  show gslb vserver <name>
3 <!--NeedCopy-->
```

Exemple :

```
1 add gslb vserver Vserver-GSLB-1 HTTP -ipType IPv4
```



```
add gslb vserver Vserver-GSLB-2 HTTP -ipType IPv6
show gslb vserver Vserver-GSLB-1
show gslb vserver Vserver-GSLB-2
<!--NeedCopy-->
```

Pour modifier ou supprimer un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

- Pour modifier un serveur virtuel GSLB, utilisez la `set gslb vserver` commande. Cette commande fonctionne de la même manière que la `add gslb vserver` commande, sauf que vous entrez le nom d'un serveur virtuel GSLB existant.
- Pour rétablir la valeur par défaut d'un paramètre, vous pouvez utiliser la `unset gslb vserver` commande suivie de la valeur vServerName et du nom du paramètre à supprimer.
- Pour supprimer un serveur virtuel GSLB, utilisez la `rm gslb vserver` commande, qui accepte uniquement l'argument name.

Pour configurer un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB > Serveursvirtuels**.
2. Ajoutez un nouveau serveur virtuel GSLB ou sélectionnez un serveur virtuel GSLB existant et modifiez ses paramètres.

Pour afficher les statistiques d'un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
stat gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Pour afficher les statistiques d'un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

Accédez à Gestion du trafic**>**GSLB**>**Serveurs virtuels**, sélectionnez le serveur virtuel et cliquez sur Statistiques.**

Statistiques du serveur virtuel GSLB

À partir de NetScaler version 12.1 build 51.xx et versions ultérieures, les statistiques du serveur virtuel GSLB affichent également les informations suivantes en plus des détails tels que les accès au serveur virtuel, la session de persistance en cours, les octets de requête, les octets de réponse, le seuil de débordement, les accès de débordement, les connexions actuellement établies par le client et les accès de sauvegarde inactifs du serveur virtuel.

- **Échecs de la méthode LB principale** : nombre de fois que la méthode GSLB principale a échoué.
- **Échecs de la méthode Backup LB** : nombre de fois que la méthode GSLB de sauvegarde a échoué.
- Résultats de**persistance du serveur Vserver** : nombre de fois que la demande est traitée par le biais des sessions de persistance.

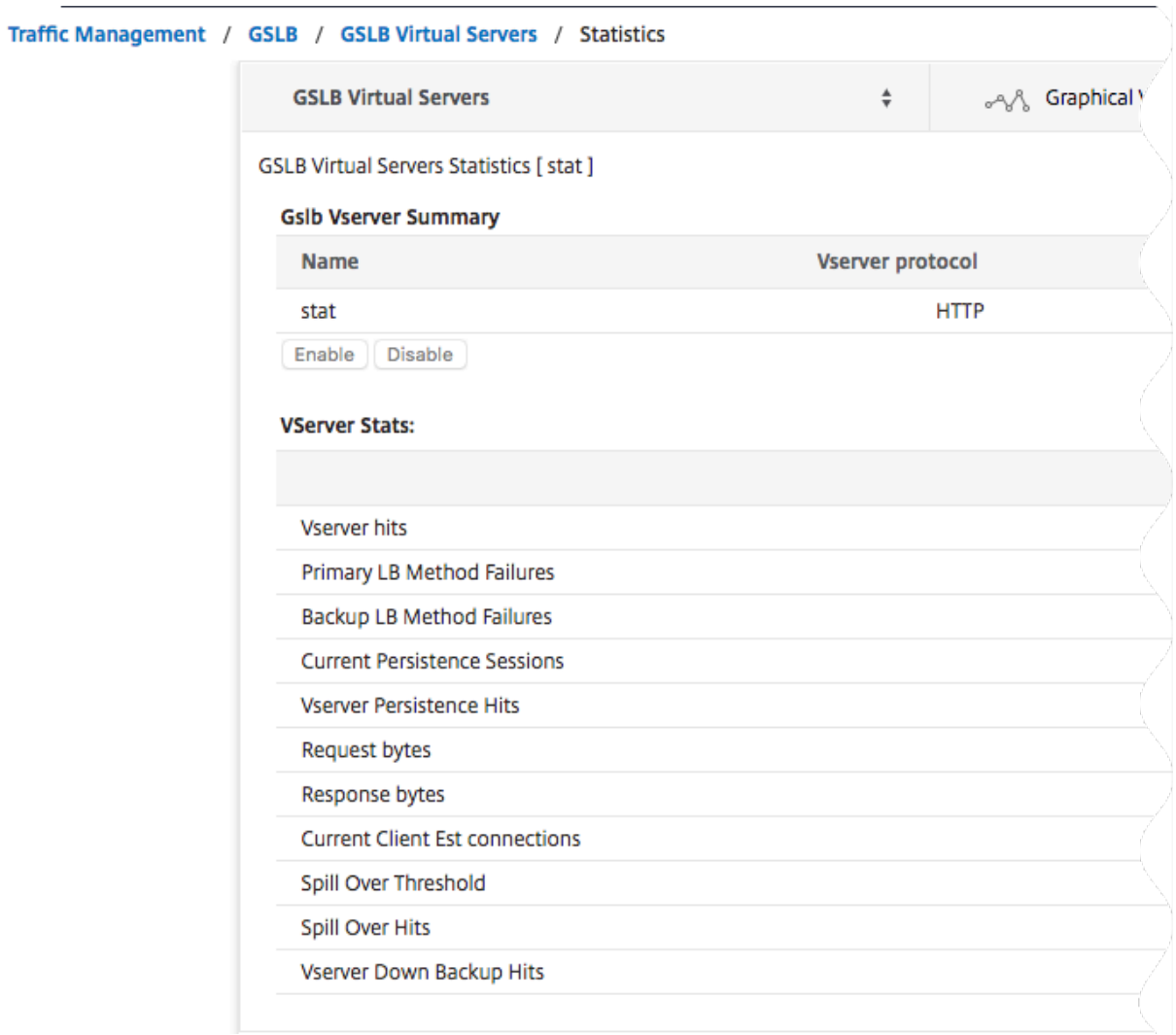
Les statistiques du serveur virtuel GSLB affichent également les statistiques des membres du groupe de services liés au serveur virtuel.

> **Remarque :**
> La méthode principale ou la méthode de sauvegarde peut échouer lorsque la méthode principale est la proximité statique et la méthode de sauvegarde est RTT. Dans ce scénario, si aucun emplacement ne correspond à l'adresse IP du LDNS, la proximité statique échoue et la méthode de sauvegarde est tentée. Les statistiques sont mises à jour sur la base des éléments suivants :
>
> - Si la méthode de sauvegarde aboutit, seules les statistiques d'échec de la méthode principale sont incrémentées.
> - Si le calcul du RTT échoue, la méthode de sauvegarde échoue également. Dans ce cas, les statistiques d'échec de la méthode principale et de sauvegarde sont incrémentées.
>
> Lorsque la méthode de sauvegarde échoue, la méthode de dernier recours, le round robin, est utilisée.

L'image suivante est un exemple des statistiques du serveur virtuel GSLB provenant de l'interface de ligne de commande.


```
Gslb Vserver Summary
                Protocol        State   Health  actSvcs inactSvc
gslbvip             HTTP         DOWN        0        0        0

VServer Stats:
                                        Rate (/s)               Total
Vserver hits                                 0                      0
Primary LB Method Failures                  --                      0
Backup LB Method Failures                   --                      0
Current Persistence Sessions                --                      0
Vserver Persistence Hits                    --                      0
Request bytes                                0                      0
Response bytes                               0                      0
Current Client Est connections              --                      0
Spill Over Threshold                        --                      0
Spill Over Hits                             --                      0
Vserver Down Backup Hits                    --                      0

Note: The above counters are the sum of all bound GSLB services
 Done
```

L’image suivante est un exemple des statistiques du serveur virtuel GSLB issues de l’interface graphique.



Statistiques du service GSLB

Lorsque vous exécutez la `stat gslb service` commande à partir de la ligne de commande ou que vous cliquez sur le **lien Statistiques** de l'utilitaire de configuration, les informations suivantes concernant le service s'affichent :

- **Octets de requête.** Nombre total d'octets de demande reçus sur ce service ou serveur virtuel.
- **Octets de réponse.** Nombre d'octets de réponse reçus par ce service ou serveur virtuel.
- **Connexions établies par le client actuel.** Nombre de connexions client dans l'état ÉTABLI.
- **Charge actuelle du service.** Charge sur le service (calculée à partir du moniteur de charge lié au service).

Les données relatives au nombre de demandes et de réponses et au nombre de connexions client et serveur actuelles peuvent ne pas être affichées ou ne pas être synchronisées avec les données du serveur virtuel d'équilibrage de charge correspondant.

Effacer les statistiques du serveur virtuel ou du service GSLB

Remarque : Cette fonctionnalité est disponible dans la version 10.5.e de NetScaler.

Vous pouvez désormais effacer les statistiques d'un serveur et d'un service virtuels GSLB. NetScaler propose les deux options suivantes pour effacer les statistiques :

- De**base** : efface les statistiques spécifiques au serveur virtuel mais conserve les statistiques fournies par le service GLSB lié.
- **Complet** : efface à la fois les statistiques du serveur virtuel et du service GSLB lié.

Pour effacer les statistiques d'un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat gslb vserver <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Exemple :

```
stat gslb vserver Vserver-GSLB-1 - clearstats basic
<!--NeedCopy-->
```

Pour effacer les statistiques d'un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat gslb service <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Exemple :

```
stat gslb service service-GSLB-1 - clearstats basic
<!--NeedCopy-->
```

Pour effacer les statistiques d'un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB > Serveursvirtuels**.
2. Sélectionnez le serveur virtuel GSLB et cliquez sur **Statistiques**, puis sur **Effacer**.
3. Dans la liste déroulante **Effacer**, sélectionnez **Basique** ou **Complet**, puis cliquez sur **OK**.

Pour effacer les statistiques d'un service GSLB à l'aide de l'utilitaire de configuration

1. **Accédez à**Gestion du trafic**>**GSLB > Services**.**
2. Sélectionnez le service GSLB et cliquez sur **Statistiques**, puis sur **Effacer**.
3. Dans la liste déroulante **Effacer**, sélectionnez **Basique** ou **Complet**, puis cliquez sur **OK**.

Activation et désactivation des serveurs virtuels GSLB

Lorsque vous créez un serveur virtuel GSLB, il est activé par défaut. Si vous désactivez le serveur virtuel GSLB, lors de la réception d'une demande DNS, l'appliance NetScaler ne prend aucune décision GSLB en fonction de la méthode GSLB configurée. La réponse à la requête DNS contient plutôt les adresses IP de tous les services liés au serveur virtuel.

Pour activer ou désactiver un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
enable gslb vserver <name>@

disable gslb vserver <name>@
<!--NeedCopy-->
```

Exemple :

```
enable gslb vserver Vserver-GSLB-1
disable gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Pour activer ou désactiver un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB > Serveursvirtuels**.
2. Sélectionnez un serveur virtuel et, dans la liste des **actions**, sélectionnez **activer** ou **désactiver**.

Cas d'utilisation - Serveur virtuel GSLB

Voici quelques exemples d'utilisation dans lesquels vous pouvez configurer des serveurs virtuels GSLB :

- Configurer le serveur virtuel GSLB pour protéger l'installation GSLB contre les pannes
- Configurer la persistance dans GSLB
- Configurer la méthode d'API GSLB

Lier les services GSLB à un serveur virtuel GSLB

August 20, 2021

Une fois les services GSLB et le serveur virtuel configurés, les services GSLB pertinents doivent être liés au serveur virtuel GSLB pour activer la configuration.

Pour lier un service GSLB à un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier un service GSLB à un serveur virtuel GSLB et vérifiez la configuration :

```
bind gslb vserver <name> -serviceName <string>

show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
bind gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Pour délier un service GSLB d'un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind gslb vserver <name> -serviceName <string>
<!--NeedCopy-->
```

Pour lier des services GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur un serveur virtuel.
2. Cliquez dans la section **Domaines**, puis configurez un domaine et liez le domaine.

Liaison d'un domaine à un serveur virtuel GSLB

May 5, 2023

Pour faire d'une appliance NetScaler le serveur DNS faisant autorité pour un domaine, vous devez lier le domaine au serveur virtuel GSLB. Lorsque vous liez un domaine à un serveur virtuel GSLB, l'appliance NetScaler ajoute un enregistrement d'adresse pour le domaine, contenant le nom du serveur virtuel GSLB. Les enregistrements de début d'autorité (SOA) et de serveur de noms (NS) pour le domaine GSLB doivent être ajoutés manuellement.

Pour plus d'informations sur la configuration des enregistrements SOA et NS, voir Système de noms de domaine.

Pour lier un domaine à un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier un domaine à un serveur virtuel GSLB et vérifier la configuration :

```
bind gslb vserver <name> -domainName <string>
show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
bind gslb vserver Vserver-GSLB-1 -domainName www.mycompany.com
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

Pour dissocier un domaine GSLB d'un serveur virtuel GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
unbind gslb vserver <name> -domainName <string>
<!--NeedCopy-->
```

Pour lier un domaine à un serveur virtuel GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB > Serveursvirtuels**.
2. Dans le volet Serveurs virtuels GSLB, sélectionnez le serveur virtuel GSLB auquel vous souhaitez lier le domaine (par exemple, vServer-GSLB-1) et cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel GSLB, sous l'onglet Domaines, effectuez l'une des opérations suivantes :

- Pour créer un nouveau domaine, cliquez sur **Ajouter**.
- Pour modifier un domaine existant, sélectionnez le domaine, puis cliquez sur **Ouvrir**.

4. Dans la boîte de dialogue Créer un domaine GSLB ou Configurer un domaine GSLB, spécifiez des valeurs pour les paramètres suivants comme indiqué :

   - Nom de domaine* : nom de domaine (par exemple, www.mycompany.com)

   * Un paramètre obligatoire

5. Cliquez sur Create.
6. Cliquez sur OK.

Pour afficher les statistiques d'un domaine à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat gslb domain <name>
<!--NeedCopy-->
```

Exemple :

```
stat gslb domain www.mycompany.com
<!--NeedCopy-->
```

Remarque : Pour afficher les statistiques d'un domaine GSLB particulier, entrez le nom du domaine exactement tel qu'il a été ajouté à l'appliance NetScaler. Si vous ne spécifiez pas le nom de domaine ou si vous spécifiez un nom de domaine incorrect, les statistiques de tous les domaines GSLB configurés s'affichent.

Pour afficher les statistiques d'un domaine à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB > Serveursvirtuels**.
2. Dans le volet Serveurs virtuels GSLB, sélectionnez le serveur virtuel GSLB (par exemple, vServer-GSLB-1) et cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le serveur virtuel GSLB, sous l'onglet Domaines, sélectionnez le domaine, puis cliquez sur **Statistiques s.**

Pour afficher les détails de configuration des entités liées à un domaine GSLB à l'aide de la ligne de commande

Remarque : Cette fonctionnalité est disponible dans la version 10.5.e de NetScaler.

À l'invite de commande, tapez :

```
show gslb domain <name>
<!--NeedCopy-->
```

Exemple :

```
show gslb domain gslb1.com
       gslb1.com
       gvs1 - HTTP    state: DOWN
       DNS Record Type: A
       Configured Method: LEASTCONNECTION
       Backup Method: ROUNDROBIN
       Persistence Type: NONE
       Empty Down Response: DISABLED
       Multi IP Response: DISABLED
       Dynamic Weights: DISABLED

       gsvc1 (10.102.239.165: 80)- HTTP State: DOWN    Weight: 1
              Dynamic Weight: 0    Cumulative Weight: 1
              Effective State: DOWN
              Threshold : BELOW

              Monitor Name : http
                     State: DOWN   Weight: 1
                     Probes: 144   Failed [Total: 144 Current: 144]
                     Last response: Failure - TCP syn sent, reset
                        received.
                     Response Time: 2000 millisec

       gsvc2 (10.102.239.179: 80)- HTTP State: DOWN    Weight: 1
              Dynamic Weight: 0    Cumulative Weight: 1
              Effective State: DOWN
              Threshold : BELOW

              Monitor Name : http-ecv
                     State: DOWN   Weight: 1
                     Probes: 141   Failed [Total: 141 Current: 141]
                     Last response: Failure - TCP syn sent, reset
                        received.
                     Response Time: 2000 millisec
Done
<!--NeedCopy-->
```


Pour afficher les détails de configuration des entités liées à un domaine GSLB à l'aide de l'utilitaire de configuration

Remarque : Cette fonctionnalité est disponible dans la version 10.5.e de NetScaler.

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur un serveur virtuel.
2. Cliquez sur le champ situé sous le volet **Domaines** .
3. Dans la boîte de dialogue **Liaison de domaine du serveur virtuel GSLB**, sélectionnez un domaine, puis cliquez sur **Afficher**les liaisons.

Exemple de configuration et de configuration GSLB

May 5, 2023

Une organisation dispose d'un réseau géographiquement dispersé et possède trois centres de données situés aux États-Unis, au Mexique et en Colombie. Dans la configuration associée à ces emplacements, ceux-ci sont appelés respectivement US, MX et CO. Sur chaque site, l'entreprise dispose d'un parc de serveurs qui fournit le même contenu et la configuration fonctionne comme prévu. L'appliance NetScaler de chaque emplacement est configurée via un serveur virtuel avec le protocole HTTP sur le port 80.

L'organisation a mis en œuvre la configuration GSLB en ajoutant un identifiant de site sur chaque site. L'identifiant du site inclut un nom de site et une adresse IP appartenant à l'appliance NetScaler et utilisée pour les communications GSLB.
Chaque site possède un site local à l'appliance. En outre, chaque site possède deux sites distants de l'appliance locale. Sur chaque site, un serveur virtuel GSLB portant le même nom est créé. Ce serveur virtuel identifie le site Web de l'organisation dans le monde entier et aucune adresse IP ne lui est associée.
La configuration comporte également des services GSLB configurés qui pointent vers les serveurs virtuels d'équilibrage de charge configurés sur chaque site GSLB en spécifiant l'adresse IP, le protocole et le numéro de port du serveur virtuel correspondant. Ces services sont liés au serveur virtuel GSLB.

Remarque : Dans la procédure ci-dessous, les commandes utilisent des adresses IP privées pour les sites GSLB. Pour les sites publics et les services GSLB, veillez à utiliser des adresses IP publiques pour ces sites.

Le tableau suivant répertorie les adresses IP et les emplacements utilisés dans l'exemple :

Adresse IP	Emplacement
10.3.1.101	Adresse IP du site NetScaler local.
172.16.1.101	IP du site distant Site-MX.
192.168.1.101	IP du site distant Site-co.
172.16.1.100	IP du service de localisation distante Site-MX.
10.3.1.100	IP de service du NetScaler local.
192.168.1.100	IP du service de localisation distante Site-co.

Lorsque vous ajoutez un site GSLB, si le site communique uniquement via Internet, utilisez le champ « IP publique ». Par exemple, lorsqu'il n'existe aucune connectivité VPN de site à site entre les sites GSLB.

Pour configurer la configuration GSLB avec les appliances NetScaler à l'aide des commandes CLI

1. Activez la fonction GSLB, si ce n'est pas déjà fait.

```
enable ns feature gslb
<!--NeedCopy-->
```

2. Identifiez un SNIP pour ajouter un site GSLB local.
3. Ajoutez le site GSLB pour l'appliance NetScaler locale.

```
add gslb site site-US 10.3.1.101
<!--NeedCopy-->
```

4. Ajoutez les sites GSLB pour les appliances NetScaler distantes.

```
add gslb site site-MX 172.16.1.101
add gslb site site-CO 192.168.1.101
<!--NeedCopy-->
```

5. Ajoutez le serveur virtuel GSLB qui fait référence à un service utilisé dans la configuration GSLB :

```
add gslb vserver gslb-lb HTTP
<!--NeedCopy-->
```

6. Ajoutez les services GSLB pour chaque site participant à la configuration du GSLB :


```
add gslb service gslb_SVC30 172.16.1.100 HTTP 80 -siteName site-MX
add gslb service gslb_SVC10 10.3.1.100 HTTP 80 -siteName site-US
add gslb service gslb_SVC20 192.168.1.100 HTTP 80 -siteName site-
   CO
<!--NeedCopy-->
```

7. Liez les services GSLB au serveur virtuel GSLB :

```
bind gslb vserver gslb-lb -serviceName gslb_SVC10
bind gslb vserver gslb-lb -serviceName gslb_SVC20
bind gslb vserver gslb-lb -serviceName gslb_SVC30
<!--NeedCopy-->
```

8. Liez le domaine au serveur virtuel GSLB.

```
bind gslb vserver gslb-lb -domainName www.mycompany.com -TTL 30
<!--NeedCopy-->
```

9. Ajoutez un service ADNS qui écoute les requêtes DNS.

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

Synchronisation de la configuration dans une configuration GSLB

May 5, 2023

Généralement, une configuration GSLB comporte quelques centres de données avec un site GSLB configuré pour chaque centre de données. Dans chaque NetScaler participant à GSLB, configurez un site GSLB en tant que site local et les autres en tant que sites distants. Lorsque vous ajoutez un autre site GSLB ultérieurement, vous devez vous assurer que la configuration sur tous les sites GSLB est identique. Vous pouvez utiliser l'option de synchronisation de configuration GSLB de NetScaler pour synchroniser la configuration entre les sites GSLB.

L'appliance NetScaler à partir de laquelle vous utilisez l'option de synchronisation est appelée « site principal » et les sites GSLB sur lesquels la configuration est copiée sont appelés « sites subordonnés ». Lorsque vous synchronisez une configuration GSLB, les configurations de tous les sites GSLB participant à la configuration GSLB sont similaires à celles du site principal.

La synchronisation est effectuée uniquement sur les sites parents. La synchronisation n'affecte pas la configuration des sites enfants GSLB. En effet, les configurations de site parent et de site enfant ne sont

pas identiques. La configuration des sites enfants comprend uniquement ses propres informations et celle de son site parent. En outre, les services GSLB ne doivent pas toujours être configurés dans les sites enfants.

- Le nœud principal détecte les différences entre la configuration du nœud principal et du nœud subordonné, et modifie la configuration du nœud subordonné pour le rendre similaire au nœud principal.

  Si vous forcez une synchronisation (utilisez l'option « forcer la synchronisation »), l'appliance supprime la configuration GSLB du nœud subordonné, puis configure le subordonné pour qu'elle soit similaire au nœud principal.

- Pendant la synchronisation, si une commande échoue, la synchronisation n'est pas interrompue et le message d'erreur est enregistré dans un fichier **.err** dans le répertoire **/var/netscaler/gslb** .

- La synchronisation est effectuée uniquement sur les sites parents. La synchronisation n'affecte pas la configuration des sites enfants GSLB. En effet, les configurations de site parent et de site enfant ne sont pas identiques. La configuration des sites enfants comprend uniquement ses propres informations et celle de son site parent. En outre, les services GSLB ne doivent pas toujours être configurés dans les sites enfants.

- Si vous désactivez la connexion utilisateur interne, la synchronisation automatique GSLB utilise les clés SSH pour synchroniser la configuration. Toutefois, pour utiliser la synchronisation automatique GSLB dans l'environnement de partition, vous devez activer la connexion utilisateur interne et vous assurer que le nom d'utilisateur de la partition dans les sites GSLB locaux et distants est le même.

> **Remarque**
>
> - Sur le nœud RPC du site GSLB distant, configurez le pare-feu pour qu'il accepte les connexions de synchronisation automatique en spécifiant l'adresse IP du site distant (adresse IP du cluster pour la configuration du cluster) et le port (3010 pour RPC et 3008 pour RPC sécurisé). Si la route par défaut pour atteindre les sites distants se trouve dans le sous-réseau de gestion, comme dans la plupart des cas, NSIP est utilisé comme adresse IP source.
>
> Pour configurer une adresse IP source différente, vous devez disposer de l'adresse IP du site GSLB et du SNIP dans un sous-réseau différent. En outre, vous devez disposer d'une route explicite définie vers l'adresse IP du site distant via un sous-réseau IP de site GSLB.
>
> Pour une sécurité renforcée, Citrix vous recommande de modifier le compte d'utilisateur interne et les mots de passe du nœud RPC. Le mot de passe du compte d'utilisateur interne est modifié via le mot de passe du nœud RPC. Pour plus de détails, voir Modifier le mot de passe d'un nœud RPC.

Si vous utilisez l'option saveconfig, les sites qui participent au processus de synchronisation enregistrent automatiquement leur configuration, de la manière suivante :

Sur le nœud RPC du site GSLB distant, configurez le pare-feu pour qu'il accepte les connexions de synchronisation automatique en spécifiant l'adresse IP du site distant (adresse IP du cluster pour la configuration du cluster) et le port (3010 pour RPC et 3008 pour RPC sécurisé). Si la route par défaut pour atteindre les sites distants se trouve dans un sous-réseau de gestion, comme dans la plupart des cas, NSIP est utilisé comme adresse IP source.

Pour configurer une adresse IP source différente, vous devez disposer de l'adresse IP du site GSLB et du SNIP dans un sous-réseau différent. Vous devez également disposer d'une route explicite définie vers l'adresse IP du site distant via le sous-réseau IP du site GSLB. L'adresse IP source ne peut pas être synchronisée entre les sites participant au GSLB car l'adresse IP source d'un nœud RPC est spécifique à chaque appliance NetScaler. Par conséquent, après avoir forcé une synchronisation (à l'aide de la commande sync gslb config -ForceSync ou en sélectionnant l'option ForceSync dans l'interface graphique), vous devez modifier manuellement les adresses IP sources sur les autres appliances NetScaler. Le port 22 est également requis pour synchroniser les fichiers de base de données sur le site distant.

Pour améliorer le temps nécessaire à la synchronisation de la configuration sur tous les sites GSLB

Configurez les paramètres du profil TCP à l'invite de commandes comme suit :

```
1 set tcpprofile nstcp_internal_apps -bufferSize 4194304 -sendBuffsize
     4194304 -tcpmode ENDPOINT
2 <!--NeedCopy-->
```

Limites de la synchronisation

- Sur le site principal, les noms des sites GSLB distants doivent être identiques aux noms des sites configurés sur les appliances NetScaler hébergeant ces sites.
- Pendant la synchronisation, des perturbations de trafic peuvent se produire.
- NetScaler a été testé pour synchroniser jusqu'à 200 000 lignes de la configuration.
- La synchronisation peut échouer :
  - Si la méthode de déversement est passée de CONNECTION à CONNECTION DYNAMIC CONNECTION.
  - Si vous échangez le préfixe de site des services GSLB liés à un serveur virtuel GSLB sur le nœud principal, puis essayez de synchroniser.
  - Si les mots de passe du nœud RPC sont différents pour NSIP et l'adresse IP de bouclage.

  - Si vous effectuez une synchronisation sur des sites GSLB configurés dans différentes partitions du même dispositif NetScaler.
- Si vous avez configuré les sites GSLB en tant que paires haute disponibilité (HA), les mots de passe des nœuds RPC des nœuds principal et secondaire doivent être identiques.
- Si vous renommez une entité GLSB faisant partie de votre configuration GSLB (utilisez la commande « show gslb RunningConfig » pour afficher la configuration GSLB). Vous devez utiliser l'option de synchronisation forcée pour synchroniser la configuration avec d'autres sites GSLB.

> **Remarque :**
>
> - Dans la synchronisation incrémentielle, vous n'avez pas besoin d'utiliser l'option de synchronisation forcée pour synchroniser la configuration avec d'autres sites GSLB. Cela s'applique à partir de la version 13.0 de NetScaler build 79.x.

Remarque : Pour surmonter les limitations dues à certains paramètres de la configuration GSLB, vous pouvez utiliser l'option de synchronisation forcée. Toutefois, si vous utilisez l'option de synchronisation forcée, les entités GSLB sont supprimées et ajoutées à la configuration et les statistiques GSLB sont remises à zéro. Le trafic est donc perturbé lors du changement de configuration.

Points à noter avant de commencer la synchronisation d'une configuration GSLB

Avant de commencer la synchronisation d'une configuration GSLB, assurez-vous que :

- Sur tous les sites GSLB, y compris le site principal, l'accès à la gestion et SSH doivent être activés pour l'adresse IP du site GSLB correspondant. L'adresse IP d'un site GSLB doit être une adresse IP appartenant à l'appliance NetScaler. Pour plus d'informations sur l'ajout des adresses IP du site GSLB et l'activation de l'accès à la gestion, voir « Configuration d'un site GSLB de base ».
- La configuration GSLB sur l'appliance NetScaler considérée comme le site principal est complète et peut être copiée sur tous les sites.
- Si vous synchronisez la configuration GSLB pour la première fois, tous les sites participant à GSLB doivent posséder l'entité de site GSLB de leurs sites locaux respectifs.
- Vous ne synchronisez pas les sites qui, par conception, n'ont pas la même configuration.
- Le site principal et les sites subordonnés exécutent les mêmes versions de NetScaler. À partir de la version 12.1, version 50.x, l'appliance vérifie la version du micrologiciel sur les sites principaux et subordonnés avant de lancer la synchronisation. Si les sites principal et les sites subordonnés exécutent différentes versions, la synchronisation est interrompue pour ce site distant afin d'éviter toute modification incompatible entre les versions. En outre, un message d'erreur affichant les détails du site sur lequel la synchronisation a été interrompue s'affiche.

  Les figures suivantes présentent des exemples de messages d'erreur provenant de l'interface de ligne de commande et de l'interface graphique.


```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name                Status      Reason
-------------------------------------------------------------------------------------------------------------
        s2                       Failure     Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                       Success     All Done
        s3                       Success     All Done
Done
>
```

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name                Status      Reason
-------------------------------------------------------------------------------------------------------------
        s2                       Failure     Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                       Success     All Done
        s3                       Success     All Done
Done
>
```

> **Important**
>
> Les répertoires suivants sont synchronisés dans le cadre de la synchronisation de la configuration GSLB.
>
> - /var/netscaler/locdb/
> - /var/netscaler/ssl/
> - /var/netscaler/inbuilt_db/

Synchronisation manuelle entre les sites participant au GSLB

May 5, 2023

La synchronisation manuelle de la configuration GSLB entre le site principal et les sites esclaves s'effectue de la manière suivante :

- Le site principal détecte les différences entre la configuration de son propre site et celle du site esclave.
- Le site principal applique la différence de configuration au site esclave.
- Le site principal effectue la synchronisation de la configuration avec tous les sites esclaves de la configuration GSLB et termine le processus de synchronisation.

Important : Une fois qu'une configuration GSLB est synchronisée, elle ne peut être annulée sur aucun des sites GSLB. Effectuez la synchronisation uniquement si vous êtes certain que le processus de synchronisation ne remplace pas la configuration sur le site distant. La synchronisation des sites n'est

pas souhaitable lorsque les sites locaux et distants ont des configurations différentes par conception, ce qui entraîne une panne du site. Si certaines commandes échouent et que d'autres réussissent, les commandes réussies ne sont pas annulées.

Points à noter

- Si vous forcez une synchronisation (utilisez l'option « forcer la synchronisation »), l'appliance NetScaler supprime la configuration GSLB du site esclave. Le site principal configure ensuite le site esclave pour le rendre similaire à son propre site.
- Pendant la synchronisation, si une commande échoue, la synchronisation n'est pas abandonnée. Les messages d'erreur sont enregistrés dans un fichier .err du répertoire /var/netscaler/gslb.
- Si vous utilisez `saveconfig` cette option, les sites participant au processus de synchronisation enregistrent automatiquement leur configuration de la manière suivante :
  - Le site principal enregistre sa configuration juste avant de lancer le processus de synchronisation.
  - Les sites esclaves enregistrent leur configuration une fois le processus de synchronisation terminé. Un site esclave enregistre sa configuration uniquement si la différence de configuration lui a été appliquée correctement. Si la synchronisation échoue sur un site esclave, vous devez rechercher manuellement la cause de l'échec et prendre des mesures correctives.

Pour synchroniser une configuration GSLB à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour synchroniser les sites GSLB et vérifier la configuration :

```
sync gslb config [-preview | -forceSync <string> | -nowarn | -
   saveconfig] [-debug]
show gslb syncStatus
<!--NeedCopy-->
```

Exemple :

```
sync gslb config

[WARNING]: Syncing config may cause configuration loss on other site.

Please confirm whether you want to sync-config (Y/N)? [N]:y

Sync Time: Dec 9 2011 10:56:9

Retrieving local site info: ok
```



```
10
11 Retrieving all participating gslb sites info: ok
12
13 Gslb_site1[Master]:
14
15 Getting Config: ok
16
17 Gslb_site2[Slave]:
18
19 Getting Config: ok
20
21 Comparing config: ok
22
23 Applying changes: ok
24
25 Done
26 <!--NeedCopy-->
```

Pour synchroniser une configuration GSLB à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > GSLB**Tableau de bord.
2. **Cliquez sur**Synchronisation automatique GSLB**et sélectionnez ForceSyn.**
3. Dans **Nom du site GSLB**, sélectionnez les sites GSLB qui doivent être synchronisés avec la configuration du nœud principal.

Aperçu de la synchronisation GSLB

En prévisualisant l'opération de synchronisation GSLB, vous pouvez voir les différences entre le nœud maître et chaque nœud esclave. En cas de divergence, vous pouvez résoudre les problèmes avant de synchroniser la configuration GSLB.

Pour prévisualiser la sortie de synchronisation GSLB à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
1 sync gslb config -preview
2 <!--NeedCopy-->
```

Pour prévisualiser la sortie de synchronisation GSLB à l'aide de l'interface graphique :

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Tableau de bord**.
2. **Cliquez sur**Synchronisation automatique GSLB**et sélectionnez Aperçu.**
3. Cliquez sur **Exécuter**.
   Une fenêtre de progression affiche les éventuelles incohérences dans la configuration.

Débogage des commandes déclenchées lors du processus de synchronisation

Vous pouvez consulter l'état (réussite ou échec) de chaque commande déclenchée pendant le processus de synchronisation et résoudre les problèmes en conséquence.

Pour déboguer les commandes de synchronisation GSLB à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande suivante :

```
sync gslb config -debug
<!--NeedCopy-->
```

Pour déboguer les commandes de synchronisation GSLB à l'aide de l'interface graphique :

1. **Accédez à**Configuration**>**Gestion du trafic**>**GSLB**> Tableau de bord.**
2. **Cliquez sur**Synchronisation automatique GSLB**et sélectionnez Debug.**
3. Cliquez sur **Exécuter**. Une fenêtre de progression affiche l'état de chaque commande déclenchée lors de la synchronisation.

Synchronisation en temps réel entre les sites participant à GSLB

May 5, 2023

Vous pouvez utiliser ce `AutomaticConfigSync` paramètre pour synchroniser automatiquement la configuration GSLB en temps réel du site principal avec tous les sites subordonnés. Il n'est pas nécessaire de déclencher manuellement l'option AutoSync pour synchroniser la configuration.

Vous pouvez synchroniser automatiquement la configuration GSLB du site principal avec tous les sites subordonnés en utilisant la synchronisation incrémentielle ou la synchronisation complète. Le `GSLBSyncMode` paramètre permet de choisir le mode de synchronisation.

> Remarque :
>
> À partir de NetScaler version 13.0 build 79.x, la synchronisation incrémentielle de la synchronisation GSLB est prise en charge. Par défaut, la synchronisation est effectuée à l'aide d'une synchronisation incrémentielle. La synchronisation incrémentielle peut être effectuée en activant le `IncrementalSync` paramètre. Pour plus de détails, consultez la section Synchronisation incrémentielle de la configuration GSLB.

Meilleures pratiques pour l'utilisation de la fonction de synchronisation en temps réel

- Il est recommandé que toutes les appliances NetScaler participant en tant que sites disposent de la même version logicielle NetScaler.

- Pour modifier le mot de passe du nœud RPC, commencez par modifier le mot de passe sur le site subordonné, puis sur le site principal.
- Configurez les sites GSLB locaux sur chaque site participant à GSLB.
- Activez AutomaticConfigSync sur l'un des sites où la configuration est effectuée. Ce site est finalement synchronisé avec d'autres sites GSLB.
- S'il y a une nouvelle configuration ou si des modifications sont apportées à la configuration existante, vérifiez l'état à l'aide de la `show gslb syncStatus` commande pour confirmer si les modifications sont synchronisées sur tous les sites ou s'il y a eu une erreur.
- La surveillance des ports RSYNC doit être activée.

Pour activer la synchronisation en temps réel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb parameter [ - automaticConfigSync (ENABLED | DISABLED)] [-
    MEPKeepAliveTimeout <secs>]  [-GSLBSyncMode ( IncrementalSync |
    FullSync )] [-GSLBSyncLocFiles ( ENABLED | DISABLED)] [-
    GslbConfigSyncMonitor ( ENABLED | DISABLED )] [-GSLBSyncInterval <
    secs>] [-GSLBSyncSaveConfigCommand ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Exemple :

```
set gslb parameter  - automaticConfigSync ENABLED
<!--NeedCopy-->
```

La synchronisation en temps réel fournit les paramètres configurables suivants :

- **GSLBSyncMode -Mode**dans lequel la configuration est synchronisée du site principal vers les sites distants.
  - Valeurs possibles : IncrementalSync, FullSync
  - Valeur par défaut : IncrementalSync
- **GSLBSynclocFiles**—Lors de la synchronisation de la configuration GSLB, par défaut, les modifications apportées aux fichiers DB d'emplacement sont détectées et synchronisées automatiquement. Étant donné que les répertoires DB d'emplacement ne changent pas souvent, les administrateurs peuvent désactiver la synchronisation automatique des fichiers DB de localisation. Les administrateurs doivent plutôt copier manuellement les fichiers DB d'emplacement sur les sites subordonnés GSLB. La synchronisation des fichiers DB d'emplacement prend beaucoup de temps. Ainsi, le fait de l'éviter réduit le temps global de synchronisation.

  Exemple de désactivation de la synchronisation automatique des fichiers DB d'emplacement :


```
set gslb parameter -GSLBSyncMode IncrementalSync -
   GSLBSyncLocFiles DISABLED
<!--NeedCopy-->
```

- **GSLBConfigSyncMonitor**—Activez le paramètre GSLB Config Sync Monitor pour surveiller l'état du port RSYNC des sites subordonnés, qui est le port SSH 22 sur l'adresse IP du site GSLB distant. Si le moniteur affiche l'état du site subordonné comme DOWN, l'opération RSYNC vers ce site est ignorée. Cela réduit les retards de synchronisation causés par la tentative de connexion aux sites distants en panne.

  Exemple pour activer la surveillance des ports RSYNC dans l'interface de ligne de commande :

```
set gslb parameter -GSLBSyncMode IncrementalSync -
   GslbConfigSyncMonitor ENABLED
<!--NeedCopy-->
```

- **GSLBSyncInterval**—Définit l'intervalle de temps (en secondes) auquel se produit la synchronisation de la configuration GSLB. Par défaut, la fonction de synchronisation automatique de configuration GSLB synchronise automatiquement la configuration GSLB toutes les 10 secondes. Vous pouvez modifier l'intervalle de temps sur n'importe quelle valeur souhaitée. Ne pas définir cette valeur sur une valeur inférieure, par exemple, au moins 5 secondes. Parce que la synchronisation fréquente peut augmenter la consommation du processeur de gestion.

  > Remarque :
  >
  > Dans une configuration de partition d'administration, l'intervalle de temps ne peut être défini que dans la partition par défaut car il s'agit d'un paramètre global.

  Exemple de définition de l'intervalle de synchronisation :

```
set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
   IncrementalSync -GSLBSyncInterval 7
<!--NeedCopy-->
```

- **GSLBSyncSaveConfigCommand**—Activez ce paramètre pour synchroniser la `save ns config` commande avec les sites subordonnés, si l' `AutomaticConfigSync` option est activée.

  Exemple pour activer la synchronisation de la commande « Enregistrer la configuration » :

```
set gslb parameter -AutomaticConfigSync ENABLED -
   GSLBSyncSaveConfigCommand ENABLED
<!--NeedCopy-->
```


La `save ns config` commande n'est pas synchronisée sur les sites subordonnés dans certains scénarios, comme suit :

- Le site subordonné est en panne ou inaccessible lorsque la configuration est enregistrée sur le site principal.
- La configuration a échoué sur un site subordonné.

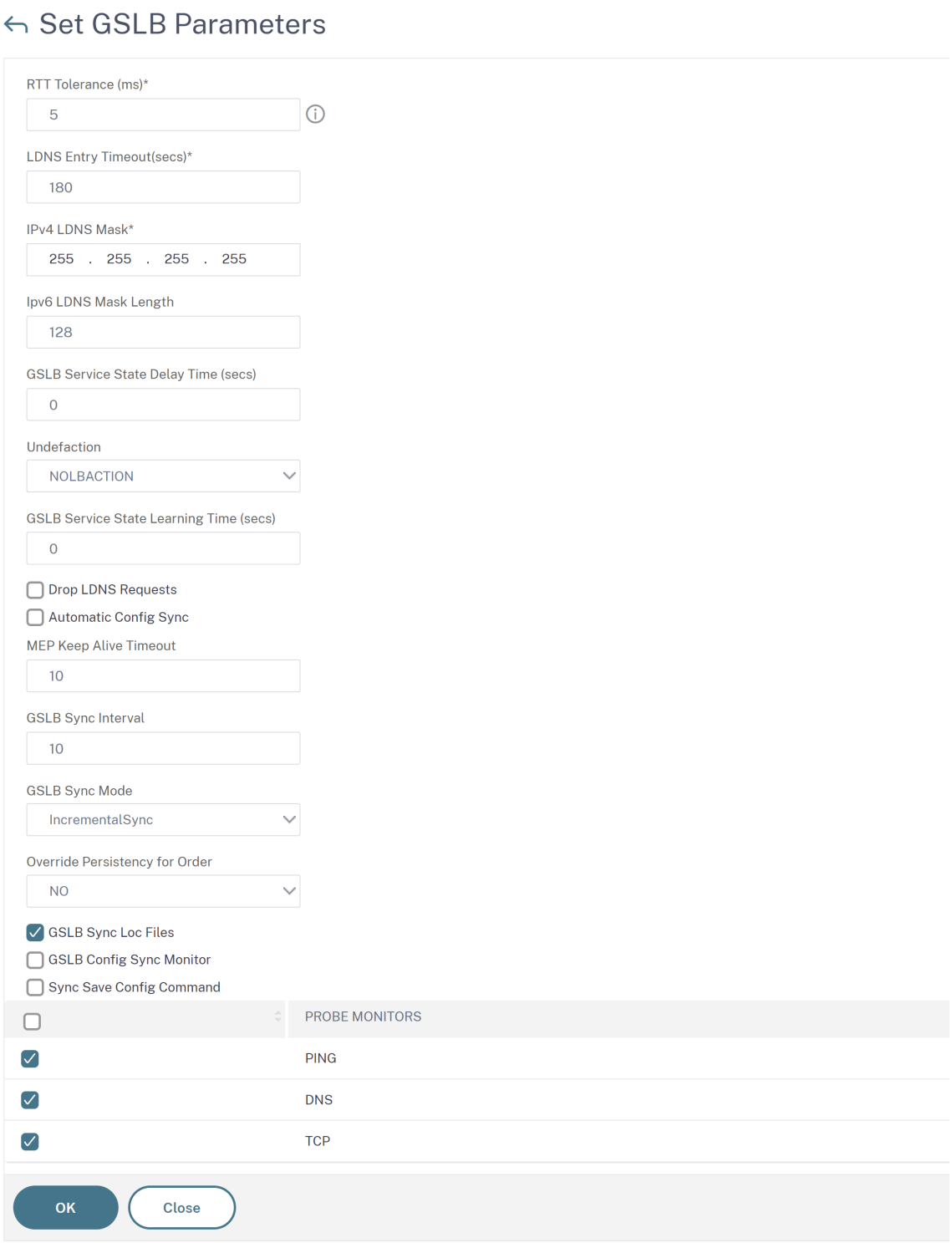
Pour activer la synchronisation en temps réel à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Modifier les paramètres GSLB**.
2. Dans la page **Définir les paramètres GSLB**, vous pouvez effectuer les opérations suivantes :

   - Pour synchroniser automatiquement la configuration GSLB en temps réel, sélectionnez **ConfigSync automatique**.

   Remarque : Cette option doit être activée uniquement sur le site où la configuration est effectuée.

   - Pour définir l'intervalle de synchronisation automatique de configuration GSLB, entrez le temps en secondes dans le champ **Intervalle de synchronisation GSLB** .
   - Pour activer la surveillance des ports RSYNC, activez la case à cocher **GSLB Config Sync Monitor** .
   - Pour désactiver la synchronisation automatique des fichiers DB d'emplacement, désactivez la case à cocher **GSLB Sync Loc Files** .
   - Pour activer la synchronisation de la `save ns config` commande sur les sites subordonnés, activez la case à cocher **Synchroniser la commande Enregistrer la configuration** .



Pour plus d'informations sur les rubriques suivantes, reportez-vous à la section Synchronisation manuelle entre les sites participant à GSLB.

- Aperçu de la synchronisation GSLB
- Débogage des commandes déclenchées pendant le processus de synchronisation

Points à noter

- Le fichier journal consolidé lié à la synchronisation en temps réel est stocké dans le répertoire /var/netscaler/gslb/periodic_sync.log.
- Le fichier de configuration par défaut est stocké dans le répertoire /var/netscaler/gslb_sync/.
- Le site principal utilise la structure de répertoires suivante :
  - Le site principal stocke tous ses fichiers dans le répertoire /var/netscaler/gslb_sync/master.
  - Le site principal stocke son fichier de configuration qui doit être synchronisé avec les sites subordonnés, dans le répertoire /var/netscaler/gslb_sync/master/gslbconf/.
  - Les fichiers d'état extraits de tous les sites subordonnés sont stockés dans le répertoire /var/netscaler/gslb_sync/master/slavestatus/.
- Le site subordonné utilise la structure de répertoires suivante :
  - Le site subordonné reprend le dernier fichier de configuration à appliquer depuis le répertoire /var/netscaler/gslb_sync/slave/gslbconf.
  - Le site subordonné stocke son fichier d'état dans le répertoire /var/netscaler/gslb_sync/slave/gslbstatus
- Dans la configuration d'une partition d'administration, la même structure de répertoire est maintenue à l'emplacement : /var/partitions/`partition name`/netscaler/gslb_sync.
- Les horloges de tous les sites doivent être réglées avec précision selon une norme en temps réel telle que le temps universel coordonné (UTC).

Synchronisation incrémentielle de la configuration GSLB

La fonction de synchronisation automatique de la configuration GSLB vérifie les modifications de configuration sur le site principal toutes les 10 secondes et effectue une synchronisation. Cette valeur d'intervalle de synchronisation est configurable.

Dans la synchronisation incrémentielle, seules les configurations qui ont changé sur le site principal entre la dernière synchronisation et l'intervalle de synchronisation suivant (10 secondes) sont synchronisées sur tous les sites subordonnés. La synchronisation incrémentielle est le comportement par défaut. Le fait de pousser uniquement les configurations incrémentielles réduit considérablement la taille du fichier de configuration, et donc le temps de synchronisation. Si une synchronisation incrémentielle échoue, le système effectue automatiquement une synchronisation complète de la configuration.

La synchronisation incrémentielle est effectuée de la manière suivante :

- Le site principal envoie le fichier de configuration comprenant uniquement ses dernières modifications sur tous les sites subordonnés. La dernière modification concerne les configurations qui ont changé entre la dernière synchronisation et l'intervalle de synchronisation suivant (10 secondes).
- Chaque site subordonné applique la dernière modification à son propre site.

- La synchronisation incrémentielle n'est pas tentée sur les sites subordonnés, qui sont en état DOWN. Lorsque le site revient, la synchronisation est à nouveau effectuée.
- Le site subordonné génère des journaux d'état à chaque étape et les copie dans un fichier à un emplacement spécifique.
- Le site principal extrait les fichiers journaux d'état de l'emplacement spécifié.
- Le site principal prépare un fichier journal avec des journaux combinés à partir de tous les sites subordonnés.
- Ce fichier journal combiné est stocké dans le fichier "/var/netscaler/gslb/periodic_sync.log".

Pour plus d'informations sur les répertoires dans lesquels les fichiers de configuration sont stockés, consultez la section Points à noter .

Pour activer la synchronisation incrémentielle de configuration GSLB à l'aide de l'interface de ligne de commande

```
set gslb parameter -AutomaticConfigSync (ENABLED | DISABLED) -
    GSLBSyncMode (IncrementalSync | FullSync) -GslbConfigSyncMonitor (
    ENABLED | DISABLED) -GSLBSyncInterval <secs> -GSLBSyncLocFiles (
    ENABLED | DISABLED)
<!--NeedCopy-->
```

Exemple :

```
set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
    IncrementalSync
<!--NeedCopy-->
```

Pour activer la synchronisation incrémentielle GSLB à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > GSLB > Tableau de bord > Modifier les paramètres GSLB**.
2. Dans la page **Définir les paramètres GSLB**, choisissez **IncrementalSync** dans le menu déroulant **Mode de synchronisation GSLB** .

Synchronisation complète de la configuration GSLB

Chaque fois qu'il y a un changement de configuration sur le site principal, la configuration complète en cours d'exécution du GSLB sur le site principal est transférée vers tous les sites subordonnés. Même si la synchronisation incrémentielle est configurée, une synchronisation complète est effectuée lorsque le site principal ne connaît pas l'état de configuration du site subordonné. Certains de ces scénarios sont les suivants :

- Activez la fonction de synchronisation automatique de la configuration GSLB pour la première fois.
- Redémarrez l'appliance NetScaler.
- Le déploiement de GSLB comporte plusieurs sites principaux, et un autre site principal devient le site principal actif.
- Ajoutez un nouveau site subordonné au déploiement GSLB.

La synchronisation complète de la configuration GSLB s'effectue de la manière suivante :

- Le site principal envoie son dernier fichier de configuration vers tous les sites subordonnés.
- Chaque site subordonné compare sa propre configuration au dernier fichier de configuration envoyé par le site principal. Le site subordonné identifie la différence de configuration et applique la configuration delta à son propre site.
- Le site subordonné génère des journaux d'état à chaque étape et les copie dans un fichier à un emplacement spécifique.
- Le site principal extrait les fichiers journaux d'état de l'emplacement spécifié.
- Le site principal prépare un fichier journal avec des journaux combinés à partir de tous les sites subordonnés.
- Ce fichier journal combiné est stocké dans le fichier "/var/netscaler/gslb/periodic_sync.log".

Si vous tentez de synchroniser manuellement (avec la `sync gslb config` commande) un site en cours de synchronisation automatique, un message d'erreur « Synchronisation en cours » apparaît. La synchronisation automatique ne peut pas être déclenchée pour un site en cours de synchronisation manuelle.

> **Attention :**
>
> À partir de NetScaler 12.1 build 49.37, les interruptions SNMP sont générées lorsque vous synchronisez la configuration GSLB. Dans la synchronisation en temps réel, l'état de synchronisation dans la première interruption SNMP est capturé en tant qu'échec. Vous pouvez ignorer cet état car une deuxième interruption SNMP est automatiquement générée immédiatement après la première interruption avec l'état de synchronisation réel. Toutefois, si la synchronisation a également échoué lors de la deuxième tentative, l'interruption SNMP n'est pas générée car l'état de synchronisation n'a pas changé par rapport à l'état de synchronisation précédent.

Pour plus de détails sur la configuration de l'appliance NetScaler pour générer des interruptions, voir Configuration de NetScaler pourgénérer des interruptions SNMP.

Pour activer la synchronisation complète GSLB à l'aide de l'interface de ligne de commande

```
set gslb parameter -GSLBSyncMode (IncrementalSync | FullSync)
<!--NeedCopy-->
```

Exemple :


```
set gslb parameter -GSLBSyncMode FullSync
<!--NeedCopy-->
```

Pour activer la synchronisation incrémentielle GSLB à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > GSLB > Tableau de bord > Modifier les paramètres GSLB**.
2. Dans la page **Définir les paramètres GSLB**, choisissez **FullSync** dans le menu déroulant **Mode de synchronisation GSLB** .

Plusieurs sites principaux dans un déploiement GSLB

L'appliance NetScaler prend en charge plusieurs sites principaux dans le cadre d'un déploiement actif-passif. Il est recommandé d'avoir deux sites principaux dans un déploiement GSLB pour faire face à la défaillance du site principal GSLB. Le fait de disposer de deux sites principaux peut éviter un point de défaillance unique de la synchronisation de la configuration GSLB. À tout moment, un seul site principal peut traiter activement la configuration GSLB à partir de l'utilisateur. Si les modifications de configuration sont effectuées simultanément sur plusieurs sites principaux, cela peut entraîner des incohérences de configuration ou des pertes de configuration. Par conséquent, il est recommandé d'effectuer des modifications de configuration à partir d'un seul site principal à la fois et d'utiliser l'autre site principal comme sauvegarde en cas de défaillance du site principal actif.

> Remarque :
>
> Lorsque plusieurs sites principaux sont utilisés dans un déploiement GSLB, la surveillance RSYNC doit être activée.

Pour faire d'un nœud GSLB l'un des principaux sites de synchronisation de configuration GSLB, exécutez la commande suivante :

```
set gslb parameter -automaticConfigSync Enabled
<!--NeedCopy-->
```

Afficher l'état et le résumé de la synchronisation GSLB

January 21, 2021

Une fois la configuration GSLB synchronisée sur les sites GSLB, vous pouvez afficher l'état détaillé et le résumé de la dernière opération de synchronisation GSLB. Ceci est applicable à la synchronisation GSLB manuelle et en temps réel.

Pour afficher l'état ou le résumé de la synchronisation GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
show gslb sync status
<!--NeedCopy-->
```

ou

```
show gslb syncStatus -summary
<!--NeedCopy-->
```

Exemple de sortie de configuration pour la synchronisation manuelle GSLB

La sortie suivante affiche l'état de la synchronisation manuelle de la configuration GSLB.

```
> sh gslb syncStatus
Displaying the status of the manual GSLB configuration synchronization:

gslb_site1[Master]:
        Getting Config:  ok
gslb_site2[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
gslb_natsite1[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
 Done
>
```

La sortie suivante affiche le récapitulatif de l'état de la synchronisation manuelle de la configuration GSLB.


```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name                Status          Reason
-------------------------------------------------------------------------------------------------------------
        gslb_site1               Success         All Done
        gslb_site2               Failure         Error executing command on gslb site...ERROR: Connection failed
        gslb_natsite1            Success         All Done
Done
>
```

Exemple de sortie de configuration pour la synchronisation en temps réel GSLB

La sortie suivante affiche l'état de la synchronisation de configuration GSLB en temps réel pour le site maître :

```
> sh gslb syncStatus
Displaying the status of the real time GSLB configuration
    synchronization as master node:

site2[Master]:
                New GSLB configuration detected at Fri Jan 23 20:54:24
                    2020
                Fetching current configuration: Done
                Updating default.conf file: Done
site1[Slave]:
                Syncing gslb static proximity database to node site1:
                    Done
                Syncing inbuilt GSLB static proximity database to node
                    site1: Done
                Syncing ssl certificates, keys and CRLS to node site1:
                    Done
                Syncing current configuration to site1: Done
                Pulling status files from site1: Status file not
                    available yet(Sync in progress)
                Pulling status files from site1: Done
                site1 received new configuration from 10.102.217.205 in
                     file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
                    conf
                Firing set gslb parameter -startConfigSync ENABLED
                    command: Done
                Fetching running GSLB Config: Done
                Comparing config: Done
```



```
19                 Applying changes: Done
20                 Firing set gslb parameter -startConfigSync DISABLED
                      command: Done
21                 Updating default.conf file: Done
22 Done
23 <!--NeedCopy-->
```

La sortie suivante affiche l'état de la synchronisation de configuration GSLB en temps réel pour le site esclave :

```
1  > sh gslb syncStatus
2  Displaying the status of the real time GSLB configuration
      synchronization as slave node:
3
4                  site1 received new configuration from 10.102.217.205 in
                        file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
                      conf
5                  Firing set gslb parameter -startConfigSync ENABLED
                      command: Done
6                  Fetching running GSLB Config: Done
7                  Comparing config: Done
8                  Applying changes: Done
9                  Firing set gslb parameter -startConfigSync DISABLED
                      command: Done
10                 Updating default.conf file: Done
11 Done
12 <!--NeedCopy-->
```

La sortie suivante affiche le récapitulatif de l'état de la synchronisation de configuration GSLB en temps réel pour le site maître :

```
1  > sh gslb syncStatus -summary
2  Displaying the status summary of the real time GSLB configuration
      synchronization as master node:
3
4  ------------------------------------------------------------------------------

5                  Site Name                                   Status
                                Reason
6  ------------------------------------------------------------------------------

7                  site2                                       Success
                               All Done
8                  site1                                       Success
                               All Done
```



```
9
10 Done
11 <!--NeedCopy-->
```

La sortie suivante affiche le récapitulatif de l'état de la synchronisation de configuration GSLB en temps réel pour le site esclave :

```
1 > sh gslb syncStatus  -summary
2 Displaying the status summary of the real time GSLB configuration
     synchronization as slave node:
3
4 ------------------------------------------------------------------------------

5                  Site Name                                    Status
                                  Reason
6 ------------------------------------------------------------------------------

7                  site1                                        Success
                                All Done
8
9 Done
10 <!--NeedCopy-->
```

Pour afficher l'état ou le résumé de la synchronisation GSLB à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Tableau de bord**.
2. Cliquez sur **Afficher le résumé de la synchronisationou Afficher l'état de la synchronisation**, selon les besoins.

Traps SNMP pour la synchronisation de la configuration GSLB

May 5, 2023

À partir de NetScaler 12.1 build 49.xx, l'appliance NetScaler génère des interruptions SNMP pour les sites locaux et distants lorsque vous synchronisez la configuration GSLB. Les interruptions SNMP sont générées à la fois pour la synchronisation manuelle et la synchronisation en temps réel.

Lorsque vous synchronisez la configuration GSLB pour la première fois, des interruptions SNMP sont générées. Lors des tentatives de synchronisation suivantes, les interruptions SNMP sont générées uniquement en cas de modification de l'état de synchronisation par rapport à l'état de synchronisation précédent. De plus, les interruptions SNMP sont générées uniquement pour les sites dont l'état de synchronisation a changé par rapport à l'état précédent.

Supposons, par exemple, que la première synchronisation de configuration GSLB soit réussie. Lorsque vous synchronisez la configuration pour la deuxième fois et si la synchronisation réussit à nouveau, les interruptions SNMP ne sont pas générées car l'état n'est pas modifié. Toutefois, lors de la troisième tentative, si la synchronisation échoue pour l'un des sites, le piège SNMP est généré uniquement pour ce site.

Dans une configuration à haute disponibilité et en cluster, l'appliance génère les interruptions SNMP lorsque vous synchronisez la configuration GSLB à partir du nouveau nœud, quel que soit l'état de synchronisation précédent. En outre, si l'option d'interruption SNMP a été précédemment désactivée puis activée, les interruptions SNMP sont générées à partir de ce point, quel que soit l'état de synchronisation précédent.

Les interruptions SNMP de la synchronisation de configuration GSLB fournissent les détails suivants :

- Nom du site GSLB pour lequel l'interruption SNMP est envoyée.
- État de synchronisation de la configuration GSLB : succès ou échec.
- Mode de synchronisation de configuration GSLB : synchronisation incrémentielle ou synchronisation complète.
- (Facultatif) Informations détaillées sur les interruptions SNMP.

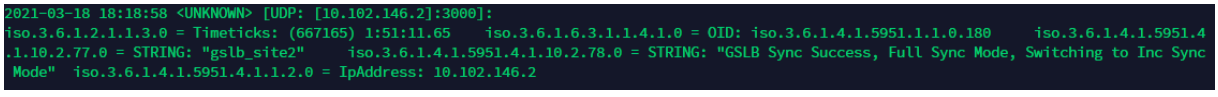
Les interruptions SNMP sont générées dans les scénarios suivants :

- L'état de synchronisation GSLB pour un site GSLB passe de Success to Failure, et inversement.
- Le mode de synchronisation GSLB passe de la synchronisation incrémentielle à la synchronisation complète, et inversement.

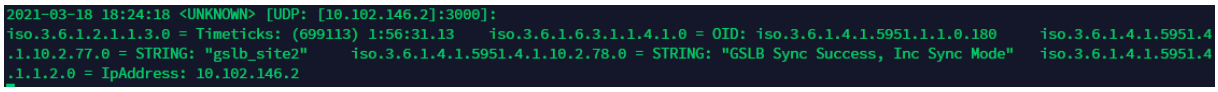
> Remarque :
>
> Même lorsque la synchronisation incrémentielle est activée, si la synchronisation complète est effectuée sur un site GSLB pour une raison quelconque, la raison de la synchronisation complète est mentionnée dans la section « Informations détaillées » du message d'interruption. Par exemple, lorsqu'un nouveau site GSLB est ajouté à la configuration GSLB.

Exemples de messages d'interruption SNMP

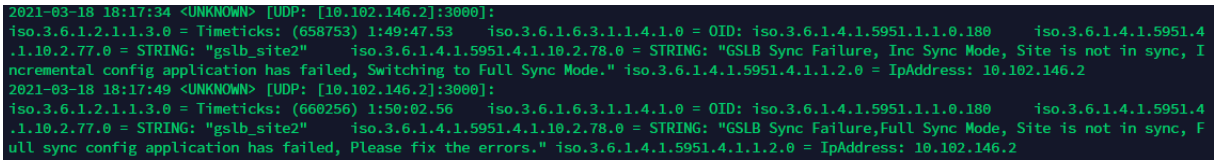
La figure suivante présente un exemple d'interruption SNMP pour gslb_site2, où la synchronisation de la configuration GSLB réussit en mode Synchronisation complète.



La figure suivante présente un exemple d'interruption SNMP pour gslb_site2, où la synchronisation de la configuration GSLB réussit à l'aide du mode de synchronisation incrémentielle.



La figure suivante présente un exemple d'interruption SNMP pour gslb_site2, où la synchronisation de la configuration GSLB à l'aide du mode de synchronisation incrémentielle a échoué. Le message d'erreur indique que vous devez corriger manuellement les erreurs pour terminer la synchronisation.



La figure suivante présente un exemple d'interruption SNMP pour gslb_site2, où la synchronisation de la configuration GSLB à l'aide du mode de synchronisation incrémentielle a échoué. Il indique également la raison de l'échec de la synchronisation, c'est-à-dire que le moniteur de site est en panne.

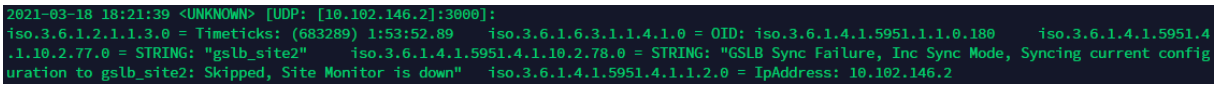


Tableau de bord GSLB

January 21, 2021

Vous pouvez afficher l'état général des sites GSLB participant à GSLB sur le tableau de bord GSLB.

Vous pouvez accéder aux paramètres GSLB à partir du tableau de bord. Vous pouvez également démarrer l'assistant de configuration GSLB à partir du tableau de bord. En outre, vous pouvez effectuer la synchronisation et tester la configuration GSLB à partir du tableau de bord.

Pour accéder au tableau de bord GSLB, accédez à **Configuration** > **Gestion du trafic** > **GSLB** > **Tableau de bord**.

Surveillance des services GSLB

May 5, 2023

Lorsque vous liez un service distant à un serveur virtuel GSLB, les sites GSLB échangent des informations de mesure, y compris des informations de mesure réseau, qui sont les informations de temps d'arrêt et de persistance.

Si une connexion d'échange métrique est momentanément perdue entre l'un des sites participants, le site distant est marqué comme étant hors service et un équilibrage de charge est effectué sur les autres sites actifs. Lorsque l'échange de métriques pour un site est inactif, les services distants appartenant au site sont également marqués comme étant hors service.

L'appliance NetScaler évalue régulièrement l'état des services GSLB distants à l'aide de MEP ou de moniteurs explicitement liés aux services distants. Il n'est pas nécessaire de lier des moniteurs explicites à des services locaux, car l'état du service GSLB local est mis à jour par défaut à l'aide du MEP. Vous pouvez toutefois lier des moniteurs explicites à un service distant. Lorsque les moniteurs sont explicitement liés, l'état du service distant n'est pas contrôlé par l'échange de mesures.

Par défaut, lorsque vous liez un moniteur à un service GSLB distant, l'appliance NetScaler utilise l'état du service indiqué par le moniteur. Vous pouvez toutefois configurer l'appliance NetScaler pour qu'elle utilise des moniteurs afin d'évaluer les services dans les situations suivantes :

- Utilisez toujours des moniteurs (réglage par défaut).
- Utilisez les écrans lorsque MEP est en panne.
- Utilisez les écrans lorsque les services distants et MEP sont hors service.

Les deuxième et troisième paramètres ci-dessus permettent à l'appliance d'arrêter la surveillance lorsque MEP est activé. Par exemple, dans une configuration GSLB hiérarchique, un site GSLB fournit les informations MEP concernant ses sites enfants à son site parent. Un tel site intermédiaire peut évaluer l'état du site enfant comme étant hors service en raison de problèmes de réseau, bien que l'état réel du site soit ouvert. Dans ce cas, vous pouvez lier les moniteurs aux services du site parent et désactiver MEP pour déterminer l'état réel du service distant. Cette option vous permet de contrôler la manière dont les états des services distants sont déterminés.

Pour utiliser des moniteurs, créez-les d'abord, puis liez-les aux services GSLB.

Configurer le déclencheur du moniteur

Vous pouvez configurer un site GSLB pour toujours utiliser des moniteurs (option par défaut), utiliser des moniteurs lorsque MEP est en panne ou utiliser des moniteurs lorsque le service distant et MEP sont en panne. Dans les deux derniers cas, l'appliance NetScaler arrête la surveillance lorsque MEP revient à l'état UP.

Pour configurer le déclenchement du moniteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb site <siteName> -triggerMonitor (ALWAYS | MEPDOWN |
   MEPDOWN_SVCDOWN)
<!--NeedCopy-->
```

Exemple :

```
set gslb site Site-GSLB-North-America -triggerMonitor Always
<!--NeedCopy-->
```


Pour configurer le déclenchement du moniteur à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Sites, puis**double-cliquez sur le site.
2. Dans la liste déroulante **Trigger Monitors**, sélectionnez une option indiquant quand déclencher la surveillance.

Ajouter ou supprimer des moniteurs

Pour ajouter un moniteur, vous devez spécifier le type et le port. Vous ne pouvez pas supprimer un moniteur lié à un service. Vous devez d'abord dissocier le moniteur du service.

Pour ajouter un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un moniteur et vérifier la configuration :

```
add lb monitor <monitorName> -type <monitorType> -destPort <portNumber>

show lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor monitor-HTTP-1 -type HTTP -destPort 80
show lb monitor monitor-HTTP-1
<!--NeedCopy-->
```

Pour supprimer un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm lb monitor <monitorName>
<!--NeedCopy-->
```

Pour ajouter un moniteur à l'aide de l'utilitaire de configuration

Accédez à Gestion
du trafic > Équilibrage de charge > Moniteurs, puis ajoutez ou supprimez un moniteur.

Liez des moniteurs à un service GSLB

Une fois que vous avez créé des moniteurs, vous devez les lier aux services GSLB. Lorsque vous liez des moniteurs aux services, vous pouvez spécifier un poids pour le moniteur. Après avoir lié un ou plusieurs moniteurs pondérés, vous pouvez configurer un seuil de surveillance pour le service. Ce seuil fait baisser le service si la somme des poids des moniteurs liés tombe en dessous de la valeur seuil.

Remarque : Dans l'utilitaire de configuration, vous pouvez définir le poids et le seuil de surveillance en même temps que vous liez le moniteur. Lorsque vous utilisez la ligne de commande, vous devez émettre une commande distincte pour définir le seuil de surveillance du service.

Pour lier le moniteur au service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind monitor <name> <serviceName> [ -state (Enabled | Disabled) ] -
   weight <positiveInteger>
<!--NeedCopy-->
```

Exemple :

```
bind monitor monitor-HTTP-1 service-GSLB-1 -state enabled -weight 2
<!--NeedCopy-->
```

Pour définir le seuil de surveillance d'un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb service <ServiceName> -monThreshold <PositiveInteger>
<!--NeedCopy-->
```

Exemple :

```
set gslb service service-GSLB-1 -monThreshold 9
<!--NeedCopy-->
```

Pour lier le moniteur au service GSLB à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Services.
2. Cliquez sur la section **Monitor** et liez le moniteur au service GSLB.

Pour définir le seuil de surveillance d'un service GSLB à l'aide de l'utilitaire de configuration

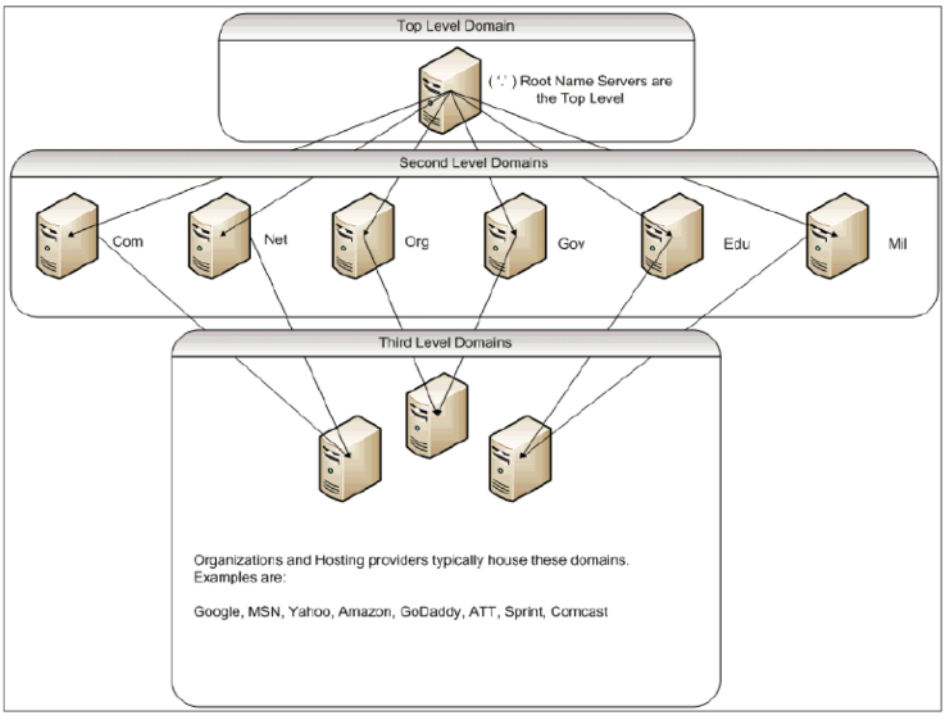
1. Accédez à Gestion du trafic > GSLB > Services.
2. Cliquez sur la section **Surveiller le seuil** et entrez une valeur de seuil.

Comment le système de noms de domaine prend en charge GSLB

May 5, 2023

Le système de noms de domaine (DNS) est considéré comme une base de données distribuée, qui utilise l'architecture Client/Serveur. Les serveurs de noms sont les serveurs de l'architecture, et les résolveurs sont les clients qui sont des routines de bibliothèque installées sur un système d'exploitation qui créent et envoient des requêtes sur le réseau.

La hiérarchie logique du DNS est illustrée dans le diagramme suivant :



> Remarque :
>
> Les serveurs racine de deuxième niveau sont responsables de la gestion des mappages Name Server to Address pour les délégations de serveurs de noms dans les domaines .com, .net, .org, .gov, etc. Chaque domaine des domaines de deuxième niveau est responsable de la gestion des mappages Serveur de noms à adresse pour les domaines organisationnels de niveau inférieur. Au niveau de l'organisation, les adresses d'hôte individuelles sont résolues pour les hôtes www,

> FTP et autres hôtes fournissant des services.

Délégation

L'objectif principal de la topologie DNS actuelle est d'alléger la charge de gestion de tous les enregistrements d'adresses sur une seule autorité. Cela permet de déléguer un espace de noms d'organisation à cette organisation particulière. L'organisation peut ensuite déléguer davantage son espace à des sous-domaines au sein de l'organisation. Par exemple, sous citrix.com, vous pouvez créer des sous-domaines appelés `sales.citrix.comeducation.citrix.com`, et `support.citrix.com`. Les services correspondants peuvent conserver leur propre ensemble de serveurs de noms qui font autorité pour leur sous-domaine, puis conserver leur propre ensemble de noms d'hôte pour les mappages d'adresses. Aucun service n'est responsable de la gestion de tous les enregistrements d'adresses Citrix. Chaque département peut modifier les adresses et modifier les topologies, sans imposer davantage de travail au domaine ou à l'organisation de niveau supérieur.

Avantages de la topologie hiérarchique

Voici quelques-uns des avantages de la topologie hiérarchique :

- Scalabilité
- Ajout d'une fonctionnalité de mise en cache dans les serveurs de noms à chaque niveau, où une requête DNS est gérée par un hôte qui ne fait pas autorité pour un domaine particulier, mais qui peut contribuer à la réponse à la requête et réduire la congestion et le temps de réponse.
- La mise en cache crée également une redondance et une résilience face aux défaillances du serveur. Si un serveur de noms échoue, il est toujours possible que des enregistrements soient diffusés à partir d'autres serveurs disposant de copies mises en cache récentes des mêmes enregistrements.

Résolveurs

Les résolveurs sont le composant client du système DNS. Les programmes exécutés sur un hôte qui ont besoin d'informations provenant de l'espace de noms de domaine utilisent le résolveur. Le résolveur gère :

- Interrogation d'un serveur de noms.
- Interprétation des réponses (qui peuvent être des enregistrements de ressources ou une erreur).
- Renvoyer l'information aux programmes qui en ont fait la demande.

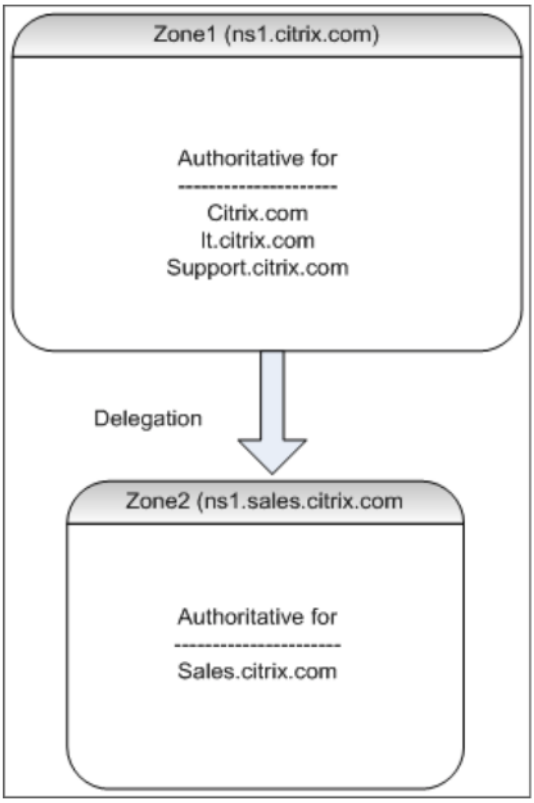
Le résolveur est un ensemble de routines de bibliothèque compilées dans des programmes tels que telnet, FTP et ping. Il ne s'agit pas de processus distincts. Les résolveurs peuvent créer une requête, l'envoyer et attendre une réponse. Et, envoyez-le à nouveau (éventuellement à un serveur de noms secondaire) s'il n'y a pas de réponse dans un certain temps. Ces types de résolveurs sont appelés

résolveurs de talon. Certains résolveurs ont la fonctionnalité ajoutée pour mettre en cache les enregistrements et respectent le temps de vie (TTL). Sous Windows, cette fonctionnalité est disponible via le service Client DNS ; elle peut être consultée via la console « services.msc ».

Serveurs de noms

Les serveurs de noms stockent généralement des informations complètes sur une partie particulière d'un espace de noms de domaine (appelée zone). On dit alors que le serveur de noms est autorisé pour cette zone. Ils peuvent également faire autorité pour plusieurs zones.

La différence entre un domaine et une zone est subtile. Un domaine est l'ensemble complet des entités, y compris ses sous-domaines, tandis qu'une zone est uniquement l'information d'un domaine qui n'est pas déléguée à un autre serveur de noms. Un exemple de zone est `citrix.com`, alors qu'il s' `sales.citrix.com` agit d'une zone distincte si cette zone est déléguée à un autre serveur de noms au sein du sous-domaine. Dans ce cas, la zone Citrix principale peut inclure `citrix.comit.citrix.com`, et `support.citrix.com`. Étant donné que le `sales.citrix.com` est délégué, il ne fait pas partie de la zone sur laquelle le serveur de `citrix.com` noms fait autorité. Le diagramme suivant montre les deux zones.



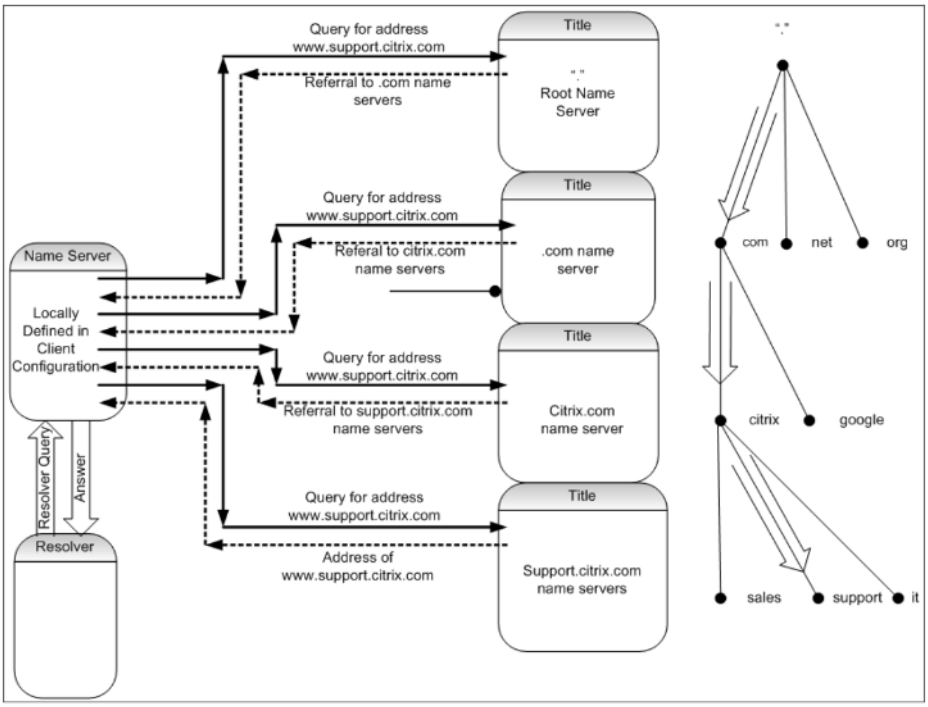
Pour déléguer correctement un sous-domaine, vous devez attribuer des pouvoirs pour ce sous-domaine à différents serveurs de noms. Dans l'exemple précédent, le `ns1.citrix.com` ne contient

pas d'informations sur le `sales.citrix.com` sous-domaine. Il contient plutôt des pointeurs vers les serveurs de noms qui font autorité pour le `ns1.sales.citrix.com` sous-domaine.

Serveurs de noms racine et résolution des requêtes

Les serveurs de noms racine connaissent les adresses IP de tous les serveurs de noms faisant autorité pour les domaines de deuxième niveau. Si un serveur de noms ne dispose pas d'informations sur un domaine donné dans ses propres fichiers de données, il n'a qu'à contacter un serveur racine pour commencer à parcourir la branche appropriée de l'arborescence **DNS** afin d'accéder au domaine donné. Il s'agit d'une série de demandes adressées à plusieurs serveurs de noms afin de faciliter la traversée de l'arborescence afin de trouver le prochain serveur de noms faisant autorité, qui doit être contacté pour une résolution ultérieure.

Le diagramme suivant montre une requête DNS typique, en supposant qu'il n'y ait pas d'enregistrement mis en cache pour le nom demandé pendant la traversée. L'exemple suivant utilise une maquette du domaine Citrix.



Requêtes récursives et non récursives

L'exemple précédent illustre les deux types de requêtes pouvant survenir.

- Requête récursive : La requête entre le résolveur et le serveur de noms configuré localement est récursive. Cela signifie que le serveur de noms reçoit la requête et ne répond pas au résolveur tant que la requête n'a pas reçu une réponse complète ou qu'une erreur n'a pas été renvoyée.

Si le serveur de noms reçoit une référence vers la requête, le serveur de noms suit la référence jusqu'à ce que le serveur de noms reçoive enfin la réponse (adresse IP) renvoyée.

- Requête non récursive : La requête que le serveur de noms configuré localement effectue sur le serveur de noms de domaine faisant autorité ultérieur est non récursive (ou itérative). Chaque demande est immédiatement répondue par un renvoi vers un serveur faisant autorité de niveau inférieur ou la réponse à la requête, si le serveur de noms interrogé contient la réponse dans ses fichiers de données ou dans son cache.

Mise en cache

Bien que le processus de résolution soit impliqué et peut nécessiter de petites requêtes à plusieurs hôtes, il est rapide. L'un des facteurs qui augmente la vitesse de résolution DNS est la mise en cache. Chaque fois qu'un serveur Name reçoit une requête récursive, il peut devoir communiquer avec d'autres serveurs pour accéder au serveur faisant autorité approprié pour la demande spécifique. Il stocke toutes les informations qu'il reçoit pour référence ultérieure. Lorsque le client suivant émet une demande similaire, par exemple un hôte différent mais dans le même domaine, il connaît déjà le serveur de noms qui fait autorité pour ce domaine et peut envoyer une demande directement là au lieu de commencer par le serveur de noms racine.

La mise en cache peut également se produire pour les réponses négatives, telles que les requêtes pour les hôtes qui n'existent pas. Dans ce cas, le serveur ne doit pas interroger le serveur de noms faisant autorité pour le domaine demandé pour déterminer que l'hôte n'existe pas. Pour gagner du temps, le serveur de noms vérifie simplement le cache et réagit avec l'enregistrement négatif.

Les serveurs de noms ne mettent pas en cache les enregistrements indéfiniment, sinon vous ne pouvez jamais mettre à jour les adresses IP. Pour éviter les problèmes de synchronisation, les réponses DNS contiennent une durée de vie (TTL). Ce champ décrit l'intervalle de temps pendant lequel le cache peut stocker un enregistrement avant qu'il ne doive l'abandonner et vérifier auprès du serveur de noms faisant autorité pour les enregistrements mis à jour. Si les enregistrements n'ont pas été modifiés, l'utilisation de TTL permet également des réponses dynamiques rapides des appareils exécutant GSLB.

Types d'enregistrements de ressources

Divers RFC fournissent une liste complète des types d'enregistrements de ressources DNS et de leur description. Le tableau suivant répertorie les types d'enregistrements de ressources courants.

Type d'enregistrement de ressource	Description	RFC
Une	Une adresse d'hôte	RFC 1035

Type d'enregistrement de ressource	Description	RFC
NS	Un serveur de noms faisant autorité	RFC 1035
MD	Une destination de messagerie (obsolète - utiliser MX)	RFC 1035
MF	Un redirecteur de courrier (obsolète - utiliser MX)	RFC 1035
CNAME	Le nom canonique d'un alias	RFC 1035
SOA	Marque le début d'une zone d'autorité	RFC 1035
WKS	Une description de service bien connue	RFC 1035
PTR	Un pointeur de nom de domaine	RFC 1035
HINFO	Informations sur l'hôte	RFC 1035
MINFO	Informations sur la boîte aux lettres ou la liste de diffusion	RFC 1035
MX	Échange de courrier	RFC 1035
TXT	chaînes de texte	RFC 1035
AAAA	Adresse IP6	RFC 3596
SRV	Sélection de serveurs	RFC 2782]

Comment GSLB prend en charge le DNS

GSLB utilise des algorithmes et des protocoles qui décident quelle adresse IP doit être envoyée pour une requête DNS. Les sites GSLB sont répartis géographiquement et il existe un serveur de noms DNS faisant autorité sur chaque site qui s'exécute en tant que service sur l'appliance NetScaler. Tous les serveurs de noms des différents sites concernés font autorité pour le même domaine. Chacun des domaines GSLB est un sous-domaine pour lequel une délégation est configurée. Par conséquent, les serveurs de noms GSLB font autorité et peuvent utiliser l'un des différents algorithmes d'équilibrage de charge pour décider de l'adresse IP à renvoyer.

Une délégation est créée en ajoutant un enregistrement de serveur de noms pour le domaine GSLB dans les fichiers de base de données du domaine parent et un enregistrement d'adresse ultérieur

pour les serveurs de noms utilisés pour la délégation. Par exemple, si vous souhaitez utiliser GSLB pour `www.citrix.com`, le fichier SOA Bind suivant peut être utilisé pour déléguer des demandes `www.citrix.com` à des serveurs de noms : Netscaler1 et Netscaler2.

```
; ###########################################################################

@ IN SOA citrix.com. hostmaster.citrix.com. (
1 ; serial
3h ; refresh
1h ; retry
1w ; expire
1h ) ; negative caching TTL
IN NS ns1
IN NS ns2
IN MX 10 mail

ns1   IN A 10.10.10.10
ns2   IN A 10.10.10.20
mail  IN A 10.20.20.50

### Old Configuration if www was not delegated to a GSLB name server
www IN A 10.20.20.50

### Updated Configuration
Netscaler1 IN A xxx.xxx.xxx.xxx
Netscaler2 IN A yyy.yyy.yyy.yyy
www IN NS Netscaler1.citrix.com.
www IN NS Netscaler2.citrix.com.
###
IN MX 20 mail2
mail2 IN A 10.50.50.20
; ###########################################################################


<!--NeedCopy-->
```

La compréhension de BIND n'est pas obligatoire pour configurer DNS. Toutes les implémentations de serveur DNS conformes disposent d'une méthode permettant de créer la délégation équivalente. Les serveurs DNS Microsoft peuvent être configurés pour délégation en utilisant les instructions de la section Créer une délégation de zone.

Ce qui différencie le GSLB sur l'appliance NetScaler de l'utilisation du service DNS standard pour la distribution du trafic est que les sites NetScaler GSLB échangent des données à l'aide d'un protocole propriétaire appelé Metric Exchange Protocol (MEP). Avec MEP, les sites GSLB sont en mesure de con-

server des informations sur tous les autres sites. Lorsqu'une demande DNS est reçue, le MEP prend en compte les mesures GSLB pour déterminer les informations suivantes :

- Site avec le moins de connexions actuelles
- Site le plus proche du serveur LDNS, qui a envoyé la demande en fonction des temps aller-retour (RTT).

Plusieurs algorithmes d'équilibrage de charge peuvent être utilisés, mais le GSLB est un DNS dans lequel le cerveau sous-jacent indique au serveur de noms (hébergé sur l'appliance NetScaler) quelle adresse doit être envoyée en fonction des métriques des sites participants.

Les autres avantages que GSLB offre sont la capacité de maintenir la persistance (ou l'affinité du site). Les réponses aux requêtes DNS entrantes peuvent être comparées à l'adresse IP source pour déterminer si cette adresse a été dirigée vers un site particulier dans un passé récent. Si c'est le cas, la même adresse est envoyée dans la réponse DNS pour s'assurer que la session client est maintenue.

Une autre forme de persistance est obtenue au niveau du site à l'aide de redirections HTTP ou de proxy HTTP. Ces formes de persistance se produisent après la réponse DNS. Par conséquent, si vous recevez une demande HTTP sur un site contenant un cookie pour diriger la demande vers un autre site participant, vous pouvez répondre par une redirection ou envoyer un proxy à la demande vers le site approprié.

Protocole d'échange de mesures

Le protocole MEP (Metric Exchange Protocol) est utilisé pour partager les données utilisées dans les calculs GSLB entre sites. À l'aide de connexions MEP, vous échangez trois types de données. Ces connexions n'ont pas besoin d'être sécurisées via le port TCP 3011 ou peuvent être sécurisées à l'aide du port SSL sur le port TCP 3009.

Les trois types de données suivants sont échangés et possèdent leurs propres intervalles et méthodes d'échange.

- **Échange de mesures de site :** Il s'agit d'un modèle d'échange d'interrogation. Par exemple, si site1 dispose d'une configuration pour les services site2, un site1 demande à site2 l'état des services GSLB chaque seconde. Site2 répond avec l'état et d'autres détails de chargement.
- **Échange de mesures réseau :** Il s'agit de l'échange d'informations LDNS RTT, utilisé dans l'algorithme d'équilibrage de charge de proximité dynamique. Il s'agit d'un modèle d'échange push. Toutes les cinq secondes, chaque site transmet ses données vers d'autres sites participants.
- **Échange de persistance :** Il s'agit de l'échange de persistance SOURCEIP. Il s'agit également d'un modèle d'échange push. Toutes les cinq secondes, chaque site transmet ses données vers d'autres sites participants.

Par défaut, les services de site sont surveillés par MEP sur la base des informations d'interrogation uniquement. Si vous liez des moniteurs en fonction de l'intervalle de surveillance, l'état est mis à jour et vous pouvez contrôler la fréquence des mises à jour en définissant l'intervalle de surveillance en conséquence.

Ordre de priorité pour les services GSLB

May 5, 2023

La fonction Ordre de priorité pour les services vous permet de hiérarchiser l'ordre des services ou des groupes de services en fonction des préférences de sélection de l'équilibrage de charge. Vous pouvez configurer l'ordre de priorité lorsque vous effectuez les opérations suivantes :

- Liez un service à un serveur virtuel GSLB.
- Liez un groupe de services à un serveur virtuel GSLB.
- Liez un membre du groupe de services au groupe de services GSLB.

Actuellement, vous pouvez configurer l'ordre de priorité des services à l'aide des approches suivantes. Toutefois, ces approches présentent les limites suivantes :

- Configuration d'une chaîne de serveurs virtuels de sauvegarde : Le nombre de lignes de configuration est élevé et vous devez exécuter la commande `show` plusieurs fois pour connaître l'état de tous les services GSLB pour chaque serveur virtuel.
- Configuration de l'emplacement préféré : vous devez créer des entrées d'emplacement pour tous les points de terminaison de votre application.

La fonctionnalité Ordre de priorité pour les services résout les limitations précédentes avec moins de commandes de configuration et vous aide à effectuer la configuration de l'emplacement préféré sans avoir besoin de représentation de l'emplacement de toutes les adresses IP des services GSLB.

Configurer l'ordre de priorité pour les services GSLB

Pour configurer l'ordre de priorité des services GSLB, le paramètre `-order <number>` est ajouté aux commandes de liaison.

> **Remarque :**
>
> Le numéro de commande le plus bas a la priorité la plus élevée.

Commande :

```
bind gslb vserver <vservername> -servicename/servicegroupname <servicename/
servicegroupname> -order <number>
```


Prenons l'exemple d'un ensemble de services liés à un serveur virtuel GSLB (gv1). À l'aide du paramètre
– `order <number>`, vous pouvez hiérarchiser l'ordre de sélection des services comme suit :

- Set 1 (s1, s2) bound to gv1 – order 1
- Set 2 (s3, s4) bound to gv1 – order 2
- Set 3 (s5, s6) bound to gv1 – order 3

Une fois que vous avez lié les services à gv1 et que gv1 reçoit le trafic client, l'ordre de sélection des services est le suivant :

- Le serveur virtuel (gv1) sélectionne les services de l'ensemble 1 (s1 et s2) avec le numéro d'ordre 1, car cet ensemble se voit attribuer le numéro d'ordre le plus bas. Par défaut, le numéro de commande le plus bas a la priorité la plus élevée.
- Si tous les services de l'ensemble 1 sont DOWN, gv1 sélectionne l'ensemble 2 (s3 et s4) avec le numéro d'ordre 2.
- Si tous les services des ensembles 1 et 2 sont hors service, gv1 sélectionne l'ensemble 3 (s5 et s6) avec le numéro d'ordre 3.

Configurer l'ordre de priorité pour les services GSLB à l'aide du CLI

Pour configurer l'ordre de priorité des services GSLB, tapez les commandes suivantes à l'invite de commandes :

1. Ajoutez des sites GSLB.

```
add gslb site site1 1.1.1.1

add gslb site site2 1.1.1.2
```

2. Ajoutez un serveur virtuel GSLB.

```
add gslb vserver gv1 HTTP
```

3. Ajoutez des services GSLB.

```
add gslb service gsvc1 1.1.1.3 http 80 -sitename site1

add gslb service gsvc2 1.1.1.4 http 80 -sitename site2

add gslb service gsvc3 1.1.1.5 http 80 -sitename site1

add gslb service gsvc4 1.1.1.6 http 80 -sitename site2

add gslb service gsvc5 1.1.1.7 http 80 -sitename site1

add gslb service gsvc6 1.1.1.8 http 80 -sitename site2
```

4. Définissez le numéro de commande et liez les services au serveur virtuel GSLB.

```
bind gslb vserver gv1 gsvc1 -order 1
```



```
bind gslb vserver gv1 gsvc2 -order 1

bind gslb vserver gv1 gsvc3 -order 2

bind gslb vserver gv1 gsvc4 -order 2

bind gslb vserver gv1 gsvc5 -order 3

bind gslb vserver gv1 gsvc6 -order 3
```

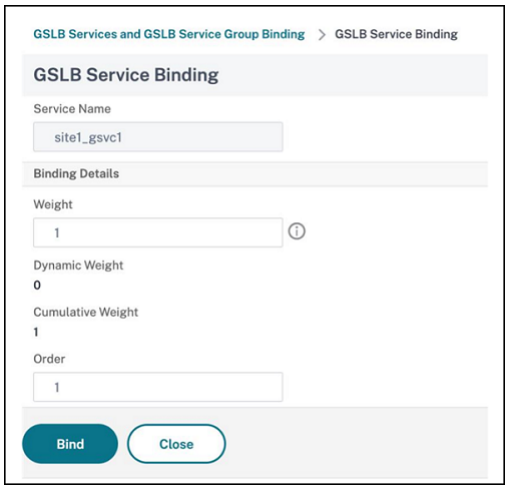
Configurer l'ordre de priorité des services GSLB à l'aide de l'interface graphique

Pré-requis :

- Vous avez créé des sites GSLB.
- Vous avez créé un serveur virtuel GSLB.
- Vous avez créé des services GSLB.

Pour configurer l'ordre de priorité des services GSLB et les lier au serveur virtuel GSLB, procédez comme suit :

1. Accédez à**Gestion du trafic > GSLB > Serveurs virtuels**et double-cliquez sur le serveur virtuel GSLB.
2. Dans **Serveur virtuel GSLB**, sous la section**Services GSLB et liaison de groupe de services GSLB**, cliquez sur **Liaisons de serveur virtuel GSLB à GSLB Service**.
3. Dans la boîte de dialogue**Services GSLB et Liaison de groupe de services GSLB**, cliquez sur**Ajouter une liaison**.
4. Dans la boîte de dialogue**Liaison de service GSLB**, sélectionnez un service.
5. Saisissez un nombre dans le champ**Ordre**pour définir l'ordre de priorité du service.



6. Cliquez sur**Bind**.

7. Répétez les étapes 1 à 6 pour configurer un numéro d'ordre de priorité différent pour différents services.

Configurer l'ordre de priorité pour les services GSLB à l'aide des commandes de stratégie LB

Par défaut, le numéro de commande le plus bas a la priorité la plus élevée. Toutefois, vous pouvez différer ce comportement par défaut à l'aide des nouvelles commandes d'action et de stratégie LB. Vous pouvez configurer l'ordre de sélection des services en fonction du trafic client entrant ou des données client.

Prenons l'exemple d'un ensemble de services liés à un serveur virtuel GSLB (gv1). À l'aide du paramètre – `order <number>`, vous avez configuré l'ordre de priorité des services comme suit :

- Ensemble 1 (s1, s2) lié à gv1 — ordre 1
- Ensemble 2 (s3, s4) lié à gv1 — ordre 2
- Set 3 (s5, s6) lié à gv1 — ordre 3

Par défaut, le numéro de commande le plus bas a la priorité la plus élevée. Par conséquent, l'ordre de priorité par défaut est 1, 2 et 3 pour les services de l'ensemble 1, ensemble2 et ensemble3, respectivement. Toutefois, pour un trafic client spécifique, vous souhaitez modifier l'ordre de priorité sur 3, 1 et 2. Pour ce faire, vous pouvez ajouter une stratégie LB et la lier à gv1.

Une commande de stratégie LB se compose de deux éléments : une règle et une action. La règle est associée à une action, qui est exécutée si une demande correspond à la règle.

> **Remarque :**
>
> Les commandes de politique LB sont communes à la fois à la configuration LB et GSLB et s'appliquent aux demandes traitées par l'appliance NetScaler.

Action LB

Expression :

```
add lb action <name> <type> <string>
```

Exemple :

```
add lb action act1 -type SELECTIONORDER -value 3 2 1
```

Paramètres :

- `name`: nom de l'action.
- `type`: Type d'action.
- `string`: valeur de l'action spécifiée.

Politique LB

Expression :

```
add lb policy <name> <rule> <action> <undefaction>
```

Exemple :

```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
```

Paramètres :

- `name`: nom de la stratégie.
- `rule`: une règle se compose d'une ou plusieurs expressions. La règle est associée à une action, qui est exécutée si la demande correspond à la règle.
- `action`: DROP, NOLBACTION et RESET sont pris en charge.
- `undefaction`: l'appliance NetScaler génère un événement non défini (événement UNDEF) lorsqu'une demande ne correspond pas à une politique. Vous pouvez utiliser la `set lb param -undefAction <action>`commande pour définir l'action non définie. Vous pouvez attribuer ces actions à un événement non défini : DROP, NOLBACTION et RESET.

Prenons un exemple dans lequel vous ajoutez une action LB, une stratégie LB et liez la stratégie à un serveur virtuel GSLB (gv1) comme suit :

```
add lb action act1 -type SELECTIONORDER -value 3 1 2
```

```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
```

```
bind gslb vserver gv1 -policyName pol1 -priority 20 - gotoPriorityExpression
 END -type REQUEST
```

La règle sélectionne le trafic client correspondant à l'adresse IP et envoie ce trafic à gv1. `8.8.8.8` Le type d'action LB (`SELECTIONORDER`) définit l'ordre de sélection du service. Après avoir lié la stratégie LB à gv1, et lorsque gv1 reçoit le trafic client de l'adresse IP`8.8.8.8`, les services sont sélectionnés dans l'ordre suivant :

1. Le serveur virtuel (gv1) sélectionne les services de l'ensemble 3 (s5 et s6) avec un ordre de priorité 3.
2. Si tous les services de l'ensemble 3 sont DOWN, gv1 sélectionne l'ensemble 1 (s1 et s2) avec un ordre de priorité 2.
3. Si tous les services de l'ensemble 3 et de l'ensemble 2 sont hors service, le gv1 sélectionne l'ensemble 1 (s1 et s2) avec l'ordre 1.

Configurer l'ordre de priorité pour les services GSLB avec les commandes de stratégie LB à l'aide de l'interface

Pour configurer l'ordre de priorité des services GSLB à l'aide des commandes de stratégie LB, tapez les commandes suivantes à l'invite de commandes :

1. Ajoutez une action LB.

```
add lb action act1 -type SELECTIONORDER -value 3 1 2
```

2. Ajoutez une stratégie LB.

```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
```

3. Ajoutez des sites GSLB.

```
add gslb site site1 1.1.1.1

add gslb site site2 1.1.1.2
```

4. Ajoutez un serveur virtuel GSLB.

```
add gslb vserver gv1 HTTP
```

5. Liez la stratégie LB au serveur virtuel GSLB.

```
bind gslb vserver gv1 -policyName pol1 -priority 20 - gotoPriorityExpression
 END -type REQUEST
```

6. Ajoutez des services GSLB.

```
add gslb service gsvc1 1.1.1.3 http 80 -sitename site1

add gslb service gsvc2 1.1.1.4 http 80 -sitename site2

add gslb service gsvc3 1.1.1.5 http 80 -sitename site1

add gslb service gsvc4 1.1.1.6 http 80 -sitename site2

add gslb service gsvc5 1.1.1.7 http 80 -sitename site1

add gslb service gsvc6 1.1.1.8 http 80 -sitename site2
```

7. Définissez l'ordre et liez les services au serveur virtuel GSLB.

```
bind gslb vserver gv1 gsvc1 -order 1

bind gslb vserver gv1 gsvc2 -order 1

bind gslb vserver gv1 gsvc3 -order 2

bind gslb vserver gv1 gsvc4 -order 2

bind gslb vserver gv1 gsvc5 -order 3

bind gslb vserver gv1 gsvc6 -order 3
```


Configurez l'ordre de priorité pour les services GSLB avec les commandes de stratégie LB à l'aide de l'interface graphique

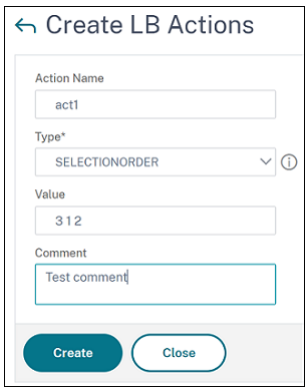
Pré-requis :

- Vous avez créé des sites GSLB.
- Vous avez créé un serveur virtuel GSLB.
- Vous avez créé des services.

Étape 1 - Créer une action LB :

1. Accédez à **AppExpert > LB > Actions**.
2. Dans**Actions LB**, cliquez sur**Ajouter**.
3. Dans la boîte de dialogue**Créer des actions LB**, spécifiez des valeurs pour les paramètres suivants :
   - **Nom de l'action** : act1
   - **Type** : SELECTIONORDER
   - **Valeur** : 3 1 2

     > **Remarque :**
     >
     > Les chiffres du champ **Valeur**sont séparés par un espace.

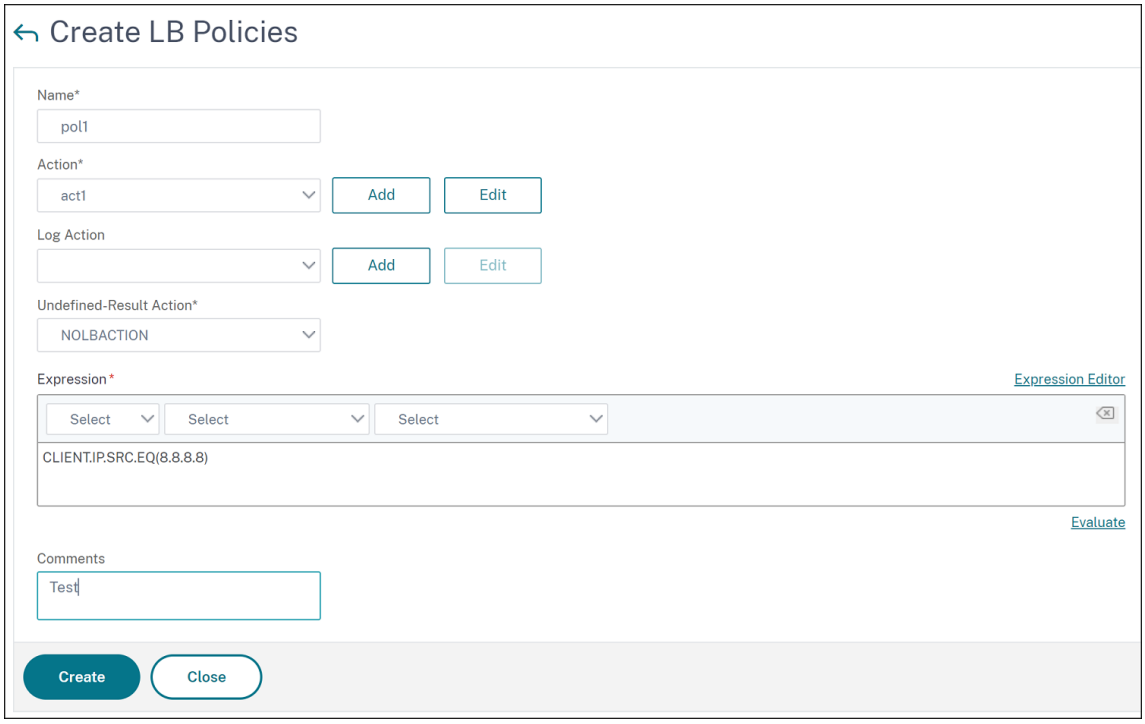


4. Cliquez sur **Create**.

Étape 2 - Créer une stratégie LB :

1. Accédez à **AppExpert > LB > Stratégies**.
2. Dans**Stratégies LB**, cliquez sur**Ajouter**.
3. Dans la boîte de dialogue**Créer des stratégies LB**, spécifiez des valeurs pour les paramètres suivants :
   - **Nom** : pol1
   - **Action** : acte 1

- **Action à résultat non défini** : NOLBACTION
- **Expression** : CLIENT.IP.SRC.EQ (8.8.8.8)

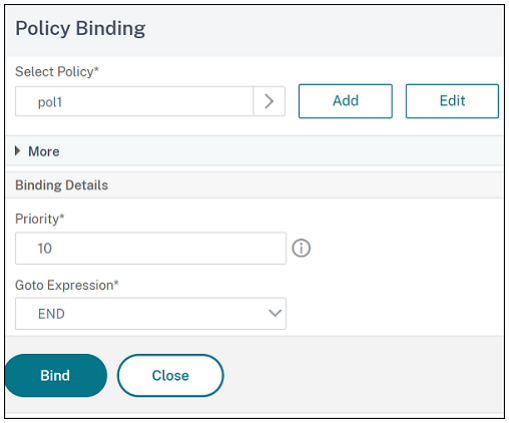


4. Cliquez sur**Créer**.

Étape 3 - Liez la stratégie LB au serveur virtuel GSLB :

1. Accédez à**Gestion du trafic > GSLB > Serveurs virtuels**et double-cliquez sur le serveur virtuel GSLB.
2. Dans le **serveur virtuel GSLB**, sous la section **Paramètres avancés**, cliquez sur**Stratégies**.
3. Dans la section**Stratégies**, cliquez sur **Liaison de stratégie LB du serveur virtuel GSLB**.
4. Dans la boîte de dialogue **Liaison de stratégie**, spécifiez des valeurs pour les paramètres suivants :

   - **Sélectionnez la stratégie** : pol 1
   - **Priorité** : 10
   - **Accédez à Expression** : FIN



5. Cliquez sur **Bind**.

Étape 4 - Configurez l'ordre de priorité pour les services GSLB :

Pour configurer l'ordre de priorité pour GSLB, reportez-vous à la procédure **Configurer l'ordre de priorité pour les services GSLB à l'aide de l'interface graphique** .

Paramètres de persistance pour les services

Si la persistance est configurée pour un service, la préférence est toujours donnée à la persistance, par défaut.

Prenons l'exemple d'un service dont la persistance est configurée et dont l'ordre de priorité est 1. Si un service d'ordre de priorité 0 est UP, la préférence est toujours donnée au service d'ordre de priorité 1.

Toutefois, vous pouvez remplacer ce comportement par défaut à l'aide de la commande CLI suivante :

```
set gslb param -overridePersistencyforOrder<YES/NO>
```

Prenons l'exemple suivant :

Un ensemble de services est lié à un serveur virtuel GSLB (gv1) avec l'ordre de priorité suivant :

- Ensemble 1 (s1, s2) lié à gv1 — ordre 1
- Ensemble 2 (s3, s4) lié à gv1 — ordre 2

Tapez la commande suivante à l'invite de commandes pour remplacer la persistance :

```
set gslb parameter -overridePersistencyforOrder YES
```

Si l'ensemble 1 (les services avec persistance sont configurés) est DOWN, les services de l'ensemble 2 traitent toutes les demandes jusqu'à ce que les services de l'ensemble 1 soient actifs. Une entrée de persistance pour la priorité 2 est créée.

Supposons qu'après un certain temps, les services de l'ensemble 1 soient actifs. Désormais, les services de l'ensemble 1 et de l'ensemble 2 sont prêts à traiter les demandes. Dans ce scénario, de nou-

velles décisions d'équilibrage de charge sont prises lorsque les services d'ordre supérieur sont actifs. L'entrée de persistance est remplacée par une nouvelle entrée d'équilibrage de charge.

Bascule de priorité

Avec la fonctionnalité de basculement de priorité, vous pouvez basculer tout le trafic vers un service de faible priorité pendant la mise à niveau de version pour un service avec un ordre de priorité plus élevé. Vous pouvez utiliser les commandes suivantes pour basculer la priorité :

- `set gslb vserver -toggleorder <Ascending/Descending>`
- `set gslb vserver v1 -orderthreshold 80`

Par exemple, considérons qu'il existe deux services ayant les priorités suivantes :

- Service 1- order 0
- Service 2 — commande 1

Par défaut, le service 1 gère tout le trafic. Si le service 1 doit être mis à niveau, le trafic doit être redirigé vers le service 2.

À l'invite de commandes, tapez les commandes suivantes pour basculer la priorité :

```
set gslb vserver -toggleorder Descending
```

Par défaut, 0 a une priorité supérieure. Cependant, après le basculement de priorité, 1 est considéré comme une priorité supérieure. Si une entrée de persistance est présente pour le service, le comportement de préférence de persistance est tel qu'expliqué dans la section**Paramètres de persistance pour les services** .

Recommandations de mise à niveau pour le déploiement GSLB

May 5, 2023

Cette section fournit des recommandations sur la séquence dans laquelle les nœuds GSLB doivent être mis à niveau dans diverses configurations GSLB. Il aborde également quelques questions fréquentes.

Remarque : L'appliance NetScaler à partir de laquelle la synchronisation GSLB est démarrée est appelée « site principal » et les sites GSLB sur lesquels la configuration est copiée sont appelés « sites subordonnés ».

Avant de commencer le processus de mise à niveau, lisez les conditions préalables mentionnées dans les rubriques suivantes :

- Avant de commencer

- Mettez à niveau une paire haute disponibilité.
- Mettez à niveau un cluster.

Points à noter lors de la mise à niveau des configurations GSLB

- Dans une configuration HA, commencez par mettre à niveau les sites subordonnés, puis le site principal.
- Dans une configuration HA, les états de service peuvent ne pas se propager d'un nœud principal de génération antérieure vers un nœud secondaire de génération plus récent. Toutefois, si les versions sont de versions différentes, mais qu'elles ont la même version HA, l'état du service peut toujours se propager.
- Si GSLB est configuré au sein d'un cluster, mettez d'abord à niveau les nœuds non propriétaires, puis mettez à niveau le nœud propriétaire. S'il existe un ou plusieurs sites dans un cluster, suivez la même séquence de mise à niveau dans chacun des sites.
- Activez les nouvelles fonctionnalités GSLB uniquement après avoir mis à niveau tous les nœuds vers une version plus récente.
- Mettez à niveau tous les nœuds GSLB vers la dernière version. Il n'y a pas d'impact fonctionnel sur les fonctionnalités disponibles lorsque certains nœuds GSLB utilisent une version plus ancienne et que certains nœuds GSLB sont mis à niveau vers une version plus récente.

FAQ

- **Les états du service GSLB sont-ils propagés lorsque les instances exécutent des versions logicielles différentes ?**

  Le MEP GSLB est fonctionnel lorsque les instances sont exécutées sur différentes versions et que les états de service GSLB sont propagés sur les sites GSLB. Il n'y a aucun impact sur la communication MEP lorsque les instances exécutent différentes versions après une mise à niveau.

- **Est-il recommandé de modifier la configuration pendant une mise à niveau ?**

  Dans une configuration GSLB, lorsqu'un site principal est en cours de mise à niveau, il n'est pas recommandé d'effectuer des modifications de configuration sur d'autres nœuds GSLB.

Ressources connexes

Les ressources suivantes fournissent des informations sur la mise à niveau d'une instance NetScaler à l'aide de NetScaler ADM :

- 10 manières dont le service NetScaler ADM facilite les mises à niveau de NetScaler
- Utiliser le service NetScaler ADM pour mettre à niveau les instances NetScaler

- Utiliser le logiciel NetScaler ADM pour mettre à niveau les instances NetScaler

Cas d'utilisation : Déploiement d'un groupe de services de mise à l'échelle automatique basé sur un nom de domaine

May 5, 2023

> **Conseil**
>
> Pour plus d'informations sur les groupes de services GSLB, voir Configuration d'un groupe de services GSLB.

Scénario de déploiement

Deux centres de données sont déployés dans deux régions AWS, l'un à Sydney et l'autre en Virginie du Nord. Un autre centre de données est déployé dans Azure. Un ELB AWS dans chaque région AWS est utilisé pour équilibrer la charge des serveurs d'applications. L'ALB est utilisé par Azure pour équilibrer la charge du serveur d'applications. Les appliances NetScaler sont configurées pour GSLB pour les ELB et ALB à l'aide d'un groupe de services autoscale basé sur le nom de domaine GSLB.

> **Important**
>
> Vous devez configurer les groupes de sécurité requis dans AWS et les associer à l'instance GSLB. Le port 53 doit être autorisé dans les règles entrantes et sortantes du groupe de sécurité. De plus, les ports (3009 ou 3011 selon la configuration MEP sécurisée) pour la communication MEP doivent être ouverts. Pour la surveillance des applications, les ports correspondants doivent être autorisés dans les règles sortantes du groupe de sécurité.

Les étapes de configuration du scénario de déploiement ci-dessus et les commandes CLI correspondantes sont les suivantes :

1. Créez des centres de données (représentés par des sites GSLB).

   ```
   add gslb site aws-sydney 192.0.2.2

   add gslb site aws-nvirginia 198.51.100.111

   add gslb site alb-southindia 203.0.113.6
   ```

2. Ajoutez un serveur de noms avec l'adresse IP de la passerelle DNS où le nœud GSLB est ajouté. Cela doit être fait dans tous les centres de données.

   ```
   add dns nameServer 8.8.8.8
   ```

3. Ajoutez des serveurs pour ELB et ALB.


```
add server aws-sydney_server lb-sydney-1052691850.ap-southeast-2.elb.
amazonaws.com

add server aws-nvirginia_server LB-nvirginia-860559595.us-east-1.elb.
amazonaws.com

add server alb-southindia_server alb.southindia.cloudapp.azure.com
```

4. Ajoutez des groupes de services GSLB autoscale pour chaque ELB et ALB et liez chaque serveur au groupe de services correspondant.

```
add gslb serviceGroup aws-nvirginia_sg HTTP -autoScale DNS -siteName
aws-nvirginia

add gslb serviceGroup aws-sydney_sg HTTP -autoScale DNS -siteName aws-
sydney

add gslb serviceGroup alb-southindia_sg HTTP -autoScale DNS -siteName
alb-southindia

bind gslb serviceGroup aws-nvirginia_sg aws-nvirginia_server 80

bind gslb serviceGroup aws-sydney_sg aws-sydney_server 80

bind gslb serviceGroup alb-southindia_sg alb-southindia_server 80
```

5. Ajoutez un serveur virtuel GSLB et liez le domaine de l'application et les groupes de services à ce serveur virtuel.

```
add gslb vserver gv1 HTTP

bind gslb vserver gv1 -serviceGroupName aws-nvirginia_sg

bind gslb vserver gv1 -serviceGroupName aws-sydney_sg

bind gslb vserver gv1 -serviceGroupName alb-southindia_sg
```

Cas d'utilisation : déploiement d'un groupe de services GSLB basé sur une adresse IP

August 20, 2021

> **Conseil**
>
> Pour plus d'informations sur les groupes de services GSLB, voir Configuration d'un groupe de services GSLB.

Scénario de déploiement

S'il existe plusieurs applications hébergées sur le même serveur d'applications, le GSLB doit sonder ces applications pour voir si elles répondent ou non. Si une application ne répond pas, l'utilisateur doit être dirigé vers le serveur sur lequel l'application est UP. En outre, si l'une des applications est DOWN, le serveur ne doit pas être marqué DOWN, car les autres applications sont UP.

Dans l'exemple suivant, plusieurs applications (HTTPS) sont hébergées sur un serveur dans chaque site GSLB et donc toutes ces applications se résolvent en une seule adresse IP du site respectif.

À l'aide des groupes de services GSLB, vous pouvez avoir le même serveur avec une adresse IP et un port liés à plusieurs groupes de services où chaque groupe de services représente une application différente.

Un moniteur spécifique à l'application est lié aux groupes de services qui marque le groupe de services comme DOWN si l'application est en panne. Ainsi, chaque fois qu'une application est DOWN, seule cette application est retirée de l'installation et non du serveur.

```
```
add gslb serviceGroup app1_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app2_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app1_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add gslb serviceGroup app2_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add lb monitor http_app2 HTTP -respCode 200 -httpRequest "GET /testsite
    /app2.html"

add lb monitor http_app1 HTTP -respCode 200 -httpRequest "GET /testsite
    /app1.html"

bind gslb serviceGroup app1_site1 192.0.2.140 80

bind gslb serviceGroup app1_site1 -monitorName http_app1

bind gslb serviceGroup app2_site1 192.0.2.140 80

bind gslb serviceGroup app2_site1 -monitorName http_app2

bind gslb serviceGroup app1_site2 192.0.2.142 80
```

 
```

```
23
24 bind gslb serviceGroup app1_site2 -monitorName http_app1
25
26 bind gslb serviceGroup app2_site2 192.0.2.142 80
27
28 bind gslb serviceGroup app2_site2 -monitorName http_app2
29 <!--NeedCopy--> ```
```

Articles pratiques

January 21, 2021

Les articles pratiques GSLB contiennent des informations sur certaines des configurations GSLB importantes telles que la personnalisation de la configuration GSLB, la configuration des connexions persistantes, la reprise après sinistre, etc.

Personnalisation de votre configuration GSLB

Configuration des connexions persistantes

Gestion des connexions client

Configurer GSLB pour la proximité

Protection de la configuration GSLB contre les défaillances

Configuration de GSLB pour la reprise après sinistre

Remplacer le comportement de proximité statique en configurant les emplacements préférés

Configuration de la sélection de service GSLB à l'aide de la commutation de contenu

Configuration de l'équilibrage de la charge du serveur global pour les requêtes DNS avec les enregistrements NAPTR

Utilisation de l'option de sous-réseau client EDNS0 pour l'équilibrage de la charge du serveur global

Exemple de configuration parent-enfant complète à l'aide du protocole Exchange de mesures

Personnalisez votre configuration GSLB

May 5, 2023

Une fois que votre configuration GSLB de base est opérationnelle, vous pouvez la personnaliser en modifiant la bande passante d'un service GSLB, en configurant les services GSLB basés sur CNAME, la

proximité statique, le RTT dynamique, les connexions persistantes ou les pondérations dynamiques pour les services, ou en modifiant la méthode GSLB.

Vous pouvez également configurer la surveillance des services GSLB afin de déterminer leur état.

Ces paramètres dépendent du déploiement de votre réseau et des types de clients que vous souhaitez connecter à vos serveurs.

Modifier le nombre maximum de connexions ou la bande passante maximale pour un service GSLB

Vous pouvez limiter le nombre de nouveaux clients pouvant se connecter simultanément à un serveur virtuel d'équilibrage de charge ou de commutation de contenu en configurant le nombre maximum de clients et/ou la bande passante maximale pour le service GSLB qui représente le serveur virtuel.

Pour modifier le nombre maximum de clients ou la bande passante d'un service GSLB à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour modifier le nombre maximum de connexions client ou la bande passante maximale d'un service GSLB et vérifier la configuration :

```
set gslb service <serviceName> [-maxClients <positive_integer>] [-
    maxBandwidth <positive_integer>]
show gslb service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
set glsb service Service-GSLB-1 -maxBandwidth 100 -maxClients 100
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

Pour modifier le nombre maximum de clients ou la bande passante d'un service GSLB à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services, puis**double-cliquez sur un service.
2. Cliquez dans la section **Autres paramètres** et définissez les paramètres suivants :
   - Nombre maximum de clients : nombre maximum de clients
   - Bande passante maximale : bande passante maximale

Création de services GSLB basés sur CNAME

Pour configurer un service GSLB, vous pouvez utiliser l'adresse IP du serveur ou un nom canonique du serveur. Si vous souhaitez exécuter plusieurs services (comme un serveur FTP et un serveur Web, chacun s'exécutant sur des ports différents) à partir d'une seule adresse IP ou exécuter plusieurs services HTTP sur le même port, avec des noms différents, sur le même hôte physique, vous pouvez utiliser des noms canoniques (CNAMES) pour les services.

Par exemple, vous pouvez avoir deux entrées dans le DNS, ftp.example.com et www.example.com pour les services FTP et les services HTTP sur le même domaine, exemple.com. Les services GSLB basés sur CNAME sont utiles dans une configuration de résolveur de domaine multiniveaux ou dans l'équilibrage de charge de domaines multiniveaux. La configuration d'un service GSLB basé sur CNAME peut également être utile si l'adresse IP du serveur physique est susceptible de changer.

Si vous configurez des services GSLB basés sur CNAME pour un domaine GSLB, lorsqu'une requête est envoyée pour le domaine GSLB, l'appliance NetScaler fournit un CNAME au lieu d'une adresse IP. Si l'enregistrement A pour cet enregistrement CNAME n'est pas configuré, le client doit interroger le domaine CNAME pour l'adresse IP. Si l'enregistrement A pour cet enregistrement CNAME est configuré, l'appliance NetScaler fournit au CNAME l'enregistrement A correspondant (adresse IP). L'appliance NetScaler gère la résolution finale de la requête DNS, telle que déterminée par la méthode GSLB. Les enregistrements CNAME peuvent être conservés sur une autre appliance NetScaler ou sur un système tiers.

Dans un service GSLB basé sur une adresse IP, l'état d'un service est déterminé par l'état du serveur qu'il représente. Toutefois, l'état d'un service GSLB basé sur CNAME est défini par défaut sur UP ; l'adresse IP (VIP) du serveur virtuel ou le protocole d'échange métrique (MEP) ne sont pas utilisés pour déterminer son état. Si un moniteur de bureau est lié à un service GSLB basé sur CNAME, l'état du service est déterminé en fonction du résultat des sondes du moniteur.

Vous pouvez lier un service GSLB basé sur CNAME uniquement à un serveur virtuel GSLB dont le type d'enregistrement DNS est CNAME. En outre, une appliance NetScaler peut contenir au plus un service GSLB avec une entrée CNAME donnée.

Voici certaines des fonctionnalités prises en charge pour un service GSLB basé sur CNAME :

- L'affinité de site basée sur la politique GSLB est prise en charge, le CNAME étant l'emplacement préféré.
- La persistance de l'adresse IP source est prise en charge. L'entrée de persistance contient les informations CNAME au lieu de l'adresse IP et du port du service sélectionné.

Les limites des services GSLB basés sur CNAME sont les suivantes :

- La persistance du site n'est pas prise en charge, car le service référencé par un CNAME peut être présent sur n'importe quel emplacement tiers.

- La réponse à plusieurs adresses IP n'est pas prise en charge car un domaine ne peut pas comporter plusieurs entrées CNAME.
- Le hachage IP source et le Round Robin sont les seules méthodes d'équilibrage de charge prises en charge. La méthode de proximité statique n'est pas prise en charge car aucun CNAME n'est associé à une adresse IP et la proximité statique ne peut être maintenue qu'en fonction des adresses IP.

Remarque : La fonctionnalité Empty-Down-Response doit être activée sur le serveur virtuel GSLB auquel vous liez le service GSLB basé sur CNAME. Si vous activez la fonctionnalité Empty-Down-Response, lorsqu'un serveur virtuel GSLB est en panne ou désactivé, la réponse à une requête DNS, pour les domaines liés à ce serveur virtuel, contient un enregistrement vide sans aucune adresse IP, au lieu d'un code d'erreur.

Pour créer un service GSLB basé sur CNAME à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add gslb service <serviceName> -cnameEntry <string> -siteName <string>
2 <!--NeedCopy-->
```

Exemple :

```
1 add gslb service Service-GSLB-1 -cnameEntry transport.mycompany.com -
     siteName Site-GSLB-East-Coast
2 add gslb service Service-GSLB-2 -cnameEntry finance.mycompany.com -
     siteName Site-GSLB-West-Coast
3 <!--NeedCopy-->
```

Pour créer un service GSLB basé sur CNAME à l'aide de l'utilitaire de configuration

1. **Accédez à**Gestion du trafic**>**GSLB > Services**.**
2. Créez un service et définissez le **type sur Canonical Name Based**.

Configurer l'état de transition hors service (TROFS) dans GSLB

Lorsque vous configurez la persistance sur un serveur virtuel GSLB auquel un service est lié, le service continue de traiter les demandes du client même après sa désactivation, en acceptant de nouvelles demandes ou connexions uniquement pour respecter la persistance. Après une période configurée, connue sous le nom de période d'arrêt progressif, aucune nouvelle demande ou connexion n'est dirigée vers le service et toutes les connexions existantes sont fermées.

Lorsque vous désactivez un service, vous pouvez spécifier une période d'arrêt progressive, en secondes, à l'aide de l'argument delay. Pendant la période d'arrêt progressif, si le service est lié à un serveur virtuel, son état apparaît comme Hors service.

Configurer des pondérations dynamiques pour les services

Dans un réseau classique, certains serveurs ont une capacité de trafic plus élevée que d'autres. Toutefois, avec une configuration d'équilibrage de charge régulière, la charge est répartie de manière uniforme entre tous les services, même si les différents services représentent des serveurs dotés de capacités différentes.

Pour optimiser vos ressources GSLB, vous pouvez configurer des pondérations dynamiques sur un serveur virtuel GSLB. Les poids dynamiques peuvent être basés soit sur le nombre total de services liés au serveur virtuel, soit sur la somme des poids des services individuels liés au serveur virtuel. La répartition du trafic est alors basée sur les poids configurés pour les services.

Lorsque des poids dynamiques sont configurés sur le serveur virtuel GSLB, les demandes sont distribuées en fonction de la méthode d'équilibrage de charge, du poids du service GSLB et du poids dynamique. Le produit du poids du service GSLB et du poids dynamique est appelé poids cumulé. Par conséquent, lorsque le poids dynamique est configuré sur le serveur virtuel GSLB, les demandes sont distribuées sur la base de la méthode d'équilibrage de charge et du poids cumulé.

Lorsque la pondération dynamique d'un serveur virtuel est désactivée, la valeur numérique est définie sur 1. Cela garantit que le poids cumulé est un entier différent de zéro à tout moment.

La pondération dynamique peut être basée sur le nombre total de services actifs liés aux serveurs virtuels d'équilibrage de charge ou sur les pondérations attribuées aux services.

Envisagez une configuration avec deux sites GSLB configurés pour un domaine et chaque site disposant de deux services pouvant servir le client. Si un service de l'un des sites tombe en panne, l'autre serveur de ce site doit gérer deux fois plus de trafic qu'un service de l'autre site. Si la pondération dynamique est basée sur le nombre de services actifs, le site dont les deux services sont actifs a deux fois plus de poids que le site dont l'un des services est en panne et reçoit donc deux fois plus de trafic.

Vous pouvez également envisager une configuration dans laquelle les services du premier site représentent des serveurs deux fois plus puissants que ceux du second site. Si la pondération dynamique est basée sur les poids attribués aux services, le trafic peut être envoyé deux fois plus important au premier site que au second.

Remarque : Pour plus d'informations sur l'attribution de poids aux services d'équilibrage de charge, voir Assignation de poids aux services.

Pour illustrer la façon dont le poids dynamique est calculé, considérez un serveur virtuel GSLB auquel un service GSLB est lié. Le service GSLB représente un serveur virtuel d'équilibrage de charge auquel deux services sont liés. Le poids attribué au service GSLB est de 3. Les pondérations attribuées aux

deux services sont respectivement de 1 et 2. Dans cet exemple, lorsque la pondération dynamique est définie sur :

- **Désactivé : le**poids cumulé du serveur virtuel GSLB est le produit du poids dynamique (désactivé = 1) et du poids du service GSLB (3). Le poids cumulé est donc de 3.
- **SERVICECOUNT** : Le décompte est la somme du nombre de services liés aux serveurs virtuels d'équilibrage de charge correspondant au service GSLB (2), et le poids cumulé est le produit du poids dynamique (2) et du poids du service GSLB (3), qui est de 6.
- **POIDS DU SERVICE** : Le poids dynamique est la somme des poids des services liés aux serveurs virtuels d'équilibrage de charge correspondant au service GSLB (3), et le poids cumulé est le produit du poids dynamique (3) et du poids du service GSLB (3), qui est de 9.

Remarque : Les pondérations dynamiques ne sont pas applicables lorsque des serveurs virtuels de commutation de contenu sont configurés.

Pour configurer un serveur virtuel GSLB afin qu'il utilise des poids dynamiques à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb vserver <name> -dynamicWeight SERVICECOUNT | SERVICEWEIGHT
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver vserver-GSLB-1 -dynamicWeight SERVICECOUNT
<!--NeedCopy-->
```

Pour configurer le serveur virtuel GSLB afin qu'il utilise des poids dynamiques à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels, puis double-cliquez sur le serveur virtuel GSLB dont vous souhaitez modifier la méthode (par exemple, vServer-GSLB-1).
2. **Cliquez sur la section**Méthode**et, dans la liste déroulante**Dynamic Weight**, sélectionnez**SERVICECOUNT ou SERVICEWEIGHT**.**

Comment configurer la persistance dans GSLB

May 5, 2023

La persistance garantit qu'une série de demandes de clients pour un nom de domaine particulier sont envoyées au même centre de données au lieu d'être rééquilibrées. Si la persistance est configurée pour un domaine particulier, elle est prioritaire par rapport à la méthode GSLB configurée. Vous pouvez utiliser la persistance pour les déploiements dans lesquels les informations relatives à une transaction client sont stockées localement sur une instance qui a traité les demandes initiales. Par exemple, les déploiements pour le commerce électronique qui utilisent un panier d'achat, où le serveur doit maintenir l'état de la connexion pour suivre la transaction. L'appliance NetScaler sélectionne un centre de données pour traiter une demande client. Lorsque la persistance est activée, il transmet la même adresse IP du centre de données sélectionné pour toutes les demandes DNS (Domain Name System) suivantes. Si une session de persistance pointe vers un centre de données hors service, l'appliance NetScaler utilise la méthode GSLB configurée pour sélectionner un nouveau centre de données. Il devient alors persistant pour les demandes ultérieures du client.
Pour la persistance dans GSLB, le même ensemble d'identifiants de persistance (PersistID) doit être configuré sur les serveurs virtuels GSLB de tous les centres de données. Le module GSLB utilise l'identifiant de persistance pour identifier de manière unique un serveur virtuel GSLB. Lorsque la persistance de l'adresse IP source est activée sur le serveur virtuel GSLB, les sessions de persistance sont également échangées dans le cadre de l'échange de métriques. Pour que l'appliance NetScaler prenne en charge la persistance entre les sites, la configuration liée à la persistance doit être effectuée sur tous les sites GSLB participants. Citrix recommande la persistance dans GSLB pour les applications statiques, ce qui oblige les clients à se reconnecter à la même instance d'application pour les demandes suivantes.

Vous pouvez obtenir la persistance dans GSLB de la manière suivante :

- Persistance sur le serveur virtuel GSLB
- Persistance du site sur les services GSLB

Persistance sur le serveur virtuel GSLB

La persistance sur le serveur virtuel GSLB est utilisée lors des requêtes DNS. L'adresse IP source de la requête DNS est utilisée pour créer une session de persistance entre le client et le centre de données. Les clients DNS sont généralement des DNS locaux (LDNS) ou des passerelles DNS qui fournissent un proxy à un ensemble de clients assis derrière eux (dans les FAI). La persistance sur un serveur virtuel GSLB est indépendante du protocole d'application.
En général, plusieurs passerelles DNS ou serveurs de noms de domaine locaux (LDNS) sont configurés sur le réseau client. Citrix vous recommande de configurer un masque de persistance approprié car pour les demandes DNS suivantes, quels que soient les appareils LDNS en amont utilisés pour se connecter à l'appliance ADC, le client peut persister dans le même centre de données que celui qui avait traité les demandes précédentes. Une fois la session de persistance créée pour une adresse IP LDNS, tous les clients finaux qui se connectent à l'aide de cette adresse LDNS reçoivent la même adresse IP de centre de données.

Persistance du site sur les services GSLB

La persistance du site devient effective lors du traitement des demandes de l'application. La persistance du site ne fonctionne que pour le trafic HTTP et HTTPS car elle est obtenue à l'aide d'un cookie HTTP. Comme les cookies sont conservés sur les clients HTTP (navigateurs), ils permettent de voir quels clients se trouvent derrière les passerelles DNS. Lorsque vous utilisez des cookies pour garantir la persistance des clients, aucune ressource n'est consommée sur l'appliance ADC pour chaque client entrant. Lorsque vous interdisez un service GSLB avec un certain délai, le service passe à l'état hors service (TROFS). La persistance est prise en charge tant que le service est à l'état UP ou TROFS. En d'autres termes, si le même client envoie une demande pour le même service dans le délai spécifié après qu'un service est marqué TROFS, le même site GSLB (centre de données) traite la demande.

Si vous accédez à une application via un alias, assurez-vous que l'enregistrement CNAME est également configuré sur l'appliance NetScaler. Dans une topologie parent-enfant, la persistance du site ne fonctionne pas lorsque vous accédez à une application via un alias.

> Remarque
>
> Si le proxy de connexion est spécifié comme méthode de persistance du site et que vous souhaitez également configurer la persistance sur les serveurs virtuels LB, la persistance de l'adresse IP source n'est pas recommandée. Lorsque la connexion est établie par proxy, une adresse IP appartenant à l'appliance ADC est utilisée, et non l'adresse IP réelle du client.
> Configurez une persistance appropriée, qui n'utilise pas l'adresse IP source de la requête HTTP (S) pour identifier le client, par exemple, la persistance des cookie ou la persistance basée sur des règles.

Configurer la persistance en fonction de l'adresse IP source

Si la persistance de l'adresse IP source est configurée sur le serveur virtuel GSLB, des sessions de persistance sont créées pour l'adresse IP source de la demande DNS. Selon la fonctionnalité ECS (Extended Client Subnet), l'adresse IP source de la demande DNS provient de l'une des sources suivantes :

- L'adresse IP source dans l'en-tête IP du paquet de requête DNS entrant
- L'option ECS de la requête DNS Pour plus d'informations sur ECS, voir Utiliser l'option de sous-réseau client EDNS0 pour Global Server Load Balancing.

Les sessions de persistance d'un client durent jusqu'au délai d'expiration de la persistance. Une fois le délai expiré, les sessions de persistance existantes sont effacées. Pour les demandes suivantes, une nouvelle décision GSLB est prise et une adresse IP de service GSLB différente peut être sélectionnée. La persistance de l'adresse IP source sur le serveur virtuel GSLB et la persistance du site sur le service GSLB se complètent mutuellement. Si la persistance de l'adresse IP source est désactivée sur le serveur virtuel GSLB, le serveur virtuel GSLB choisit un service GSLB différent chaque fois que le DNS essaie d'effectuer la résolution. Le client se connecte également à un autre service GSLB et le centre de

données qui reçoit la demande d'application transmet par proxy la connexion au centre de données qui a servi le client en premier. Cela peut ajouter une certaine latence. Ainsi, en activant la persistance de l'adresse IP source sur le serveur virtuel GSLB, vous pouvez éviter de tels sauts multiples fréquents pour les demandes d'applications. Si la session de persistance de l'adresse IP source a expiré et que le client se reconnecte par la suite, la persistance du site reconnecte le client au centre de données qui l'avait initialement desservi. De plus, si le client se reconnecte via une passerelle DNS, qui ne fait pas partie de la plage de masques de persistance configurée, la persistance du site aide également les clients à s'en tenir au centre de données qui a répondu à la première demande.

Pour configurer la persistance en fonction de l'adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb vserver <name> -persistenceType (SOURCEIP|NONE) -persistenceId
    <positive_integer> [-persistMask <netmask>] - [timeout <mins>]
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver vserver-GSLB-1 -persistenceType SOURCEIP -
   persistenceId 23 -persistMask 255.255.255.255 - timeout 2
<!--NeedCopy-->
```

Pour configurer la persistance en fonction de l'adresse IP source à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel GSLB dont vous souhaitez modifier la méthode (par exemple, vServer-GSLB-1).
2. Cliquez sur la section **Persistance** et, dans la liste déroulante **Persistance**, sélectionnez **SOURCEIP** et définissez les paramètres suivants :
   - ID de persistance : ID de persistance
   - Délai d'expiration : délai d'expiration
   - Longueur du masque de réseau IPv4 ou du masque IPv6 : PersistMask

Configurer la persistance du site en fonction des cookies HTTP

La persistance du site est obtenue à l'aide de cookies HTTP (appelés « cookie de site ») pour reconnecter le client au même serveur. Lorsque l'appliance GSLB répond à une demande DNS du client en envoyant l'adresse IP du site GSLB sélectionné, le client envoie une requête HTTP à ce site GSLB. Le point de terminaison de l'application sur ce site GSLB ajoute un cookie de site à l'en-tête HTTP, et la

persistance du site est effective.
Si le client envoie une requête DNS après l'expiration du cache du client, la demande DNS peut être dirigée vers un autre site GSLB. Le nouveau site GSLB utilise le cookie du site présent dans l'en-tête de demande du client pour implémenter la persistance. La fonctionnalité de persistance du site devient active dans les conditions suivantes :

- Lorsque le nom de domaine figurant dans l'en-tête de l'hôte correspond à l'un des domaines GSLB
- Lorsque la persistance du site est activée sur le service GSLB qui représente le serveur virtuel recevant le trafic de l'application.

Le cookie du site contient des informations sur le service GSLB sélectionné sur lequel le client dispose d'une connexion permanente. Si le service GSLB pointé par le cookie est hors service ou supprimé de la configuration GLSB, le serveur virtuel qui reçoit le trafic continue de traiter le trafic. L'expiration des cookie est basée sur le délai d'expiration des cookie configuré sur l'appliance NetScaler. Si les noms des serveurs virtuels ne sont pas identiques sur tous les sites, vous devez utiliser l'identifiant de persistance. Les cookies insérés sont conformes à la norme RFC 2109.

NetScaler prend en charge deux types de persistance des sites :

- Proxy de connexion
- Redirection HTTP

Proxy de connexion

En mode de persistance du site en mode Proxy de connexion, le centre de données qui reçoit la demande d'application suivante exécute les tâches suivantes pour établir une connexion :

1. Crée une connexion au site GSLB qui a inséré le cookie du site.
2. Proxie la demande du client vers le site d'origine.

   > **Remarque :**
   >
   > Le serveur proxy établit la connexion avec le site d'origine à l'aide des informations suivantes :
   >
   > - Le SNIP du nouveau site est l'adresse IP source.
   > - L'adresse IP publique du service GSLB du site d'origine est l'adresse IP de destination.
   > - Un port éphémère est le port source et le port de service GSLB est le port de destination.
   > - Utilise les protocoles HTTP ou HTTPS selon le type de service GSLB.

3. Reçoit une réponse du site GSLB d'origine.
4. Transmet cette réponse au client.
5. Ferme la connexion.

Redirection HTTP

Si la configuration GSLB utilise la persistance des redirections HTTP, le nouveau site redirige la demande vers le site qui a initialement inséré le cookie. Le nom de domaine indiqué dans l'URL de redirection est le domaine du site. Assurez-vous que les cookies et les certificats SSL s'appliquent à la fois au domaine GSLB et au domaine du site. Pour appliquer des cookies à la fois pour GSLB et pour le domaine du site, le domaine du cookie doit être le domaine site vers GSLB. Pour appliquer des certificats SSL à la fois au GSLB et au domaine du site, le certificat lié au serveur virtuel SSL doit être un certificat générique.

Le proxy de connexion se produit lorsque les conditions suivantes sont remplies :

- Les demandes sont envoyées pour un domaine participant au GSLB. Le domaine est obtenu à partir de l'en-tête URL/host.
- Le proxy de connexion est activé pour le service GSLB local.
- La demande inclut un cookie valide qui contient l'adresse IP d'un service GSLB distant actif.

> **Remarque**
>
> Dans une configuration parent-enfant GSLB, le proxy de connexion fonctionne comme prévu même lorsqu'aucun service GSLB n'est configuré sur un site enfant. Toutefois, si vous disposez d'une configuration supplémentaire telle que l'authentification client, l'insertion d'adresse IP du client ou toute autre exigence spécifique à SSL, vous devez ajouter un service GSLB explicite sur le site et le configurer en conséquence.
>
> Pour plus d'informations sur la topologie parent-enfant, voir Déploiement de la topologie parent-enfant à l'aide du protocole MEP.

Pour définir la persistance en fonction des cookies HTTP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb service <serviceName> -sitePersistence (ConnectionProxy [-
   sitePrefix <prefix>] | HTTPredirect -sitePrefix <prefix>)
<!--NeedCopy-->
```

Exemple :

```
set gslb service service-GSLB-1 -sitePersistence ConnectionProxy
set gslb service service-GSLB-1 -sitePersistence HTTPRedirect -
   sitePrefix vserver-GSLB-1
<!--NeedCopy-->
```


Pour définir la persistance en fonction des cookies à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **GSLB** > **Services** et sélectionnez le service que vous souhaitez configurer pour la persistance du site (par exemple, Service-GSLB-1).
2. Cliquez sur la section **Persistance du site** et définissez la persistance en fonction des cookies.

Gérer les connexions client

May 5, 2023

Pour faciliter la gestion des connexions client, vous pouvez activer le nettoyage différé des connexions au serveur virtuel. Vous pouvez ensuite gérer le trafic DNS local en configurant des stratégies DNS.

Activer le nettoyage différé des connexions aux serveurs virtuels

L'état d'un serveur virtuel dépend des états des services qui lui sont liés, et l'état de chaque service dépend des moniteurs qui lui sont liés. En cas de ralentissement ou d'arrêt d'un serveur, le délai des sondes de surveillance est dépassé et le service qui représente le serveur est marqué comme étant EN PANNE. Un serveur virtuel est marqué comme étant en panne uniquement lorsque tous les services qui lui sont liés sont marqués comme étant en panne. Vous pouvez configurer des services et des serveurs virtuels pour qu'ils mettent fin à toutes les connexions lorsqu'elles tombent en panne ou qu'elles autorisent le passage des connexions. Ce dernier paramètre est destiné aux situations dans lesquelles un service est marqué comme étant en panne en raison d'un serveur lent.

Lorsque vous configurez l'option down state flush, l'appliance NetScaler effectue un nettoyage différé des connexions à un service GSLB en panne.

Pour activer le nettoyage différé des connexions au serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le nettoyage des connexions différées et vérifier la configuration :

```
set gslb service <name> -downStateFlush (ENABLED | DISABLED)
show gslb service <name>
<!--NeedCopy-->
```

Exemple :

```
set gslb service Service-GSLB-1 -downStateFlush ENABLED
Done
```



```
3
4 show gslb service Service-GSLB-1
5 Done
6 <!--NeedCopy-->
```

Pour activer le nettoyage différé des connexions au serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Services** et double-cliquez sur le service.
2. Cliquez sur la section **Autres paramètres** et **sélectionnez l'option Flush de l'état désactivée** .

Gérez le trafic DNS local à l'aide de stratégies DNS

Vous pouvez utiliser des stratégies DNS pour implémenter l'affinité de site en dirigeant le trafic depuis l'adresse IP d'un résolveur DNS local ou d'un réseau vers un site GSLB cible prédéfini. Ceci est configuré en créant des politiques DNS avec des expressions DNS et en liant les politiques globalement sur l'appliance NetScaler.

Expressions DNS

L'appliance NetScaler fournit certaines expressions DNS prédéfinies qui peuvent être utilisées pour configurer des actions spécifiques à un domaine. Ces actions peuvent, par exemple, supprimer certaines demandes, sélectionner une vue spécifique pour un domaine spécifique ou rediriger certaines demandes vers un emplacement spécifique.

Ces expressions DNS (également appelées *règles*) sont combinées pour créer des politiques DNS qui sont ensuite liées globalement à l'appliance NetScaler.

Voici la liste des qualificatifs DNS prédéfinis disponibles sur l'appliance NetScaler :

- CLIENT.UDP.DNS.DOMAIN.EQ (« nom de domaine »)
- CLIENT.UDP.DNS.IS_AREC
- CLIENT.UDP.DNS.IS_AAAAREC
- CLIENT.UDP.DNS.IS_SRVREC
- CLIENT.UDP.DNS.IS_MXREC
- CLIENT.UDP.DNS.IS_SOAREC
- CLIENT.UDP.DNS.IS_PTRREC
- CLIENT.UDP.DNS.IS_CNAME
- CLIENT.UDP.DNS.IS_NSREC
- CLIENT.UDP.DNS.IS_ANYREC

L'expression DNS CLIENT.UDP.DNS.DOMAIN peut être utilisée avec des expressions de chaîne. Si vous utilisez des noms de domaine dans l'expression, ils doivent se terminer par un point (.). Par exemple, CLIENT.UDP.DNS.DOMAIN.ENDSWITH (« abc.com. »)

Pour créer une expression à l'aide de l'utilitaire de configuration

1. Cliquez sur l'icône en regard de la zone de texte Expression. Cliquez sur Ajouter. (Laissez les zones de liste déroulante Type de flux et protocole vides.) Suivez ces étapes pour créer une règle.
2. Dans la zone Qualificatif, sélectionnez un qualificatif (par exemple, EMPLACEMENT).
3. Dans la zone Opérateur, sélectionnez un opérateur (par exemple, ==).
4. Dans la zone Valeur, tapez une valeur (par exemple, Asie, Japon…).
5. Cliquez sur OK. Cliquez sur Créer, puis sur Fermer. La règle est créée.
6. Cliquez sur OK.

Configurer les actions DNS

Une stratégie DNS inclut le nom d'une action DNS à exécuter lorsque la règle de stratégie est évaluée à TRUE. Une action DNS peut effectuer l'une des opérations suivantes :

- Envoyez au client une adresse IP pour laquelle vous avez configuré une vue DNS. Pour plus d'informations sur les vues DNS, voir Ajout de vues DNS.
- Envoyez au client l'adresse IP d'un service GSLB après avoir fait référence à une liste d'emplacements préférés qui remplace le comportement de proximité statique. Pour plus d'informations sur les emplacements préférés, reportez-vous à la section Remplace le comportement de proximité statique par configuration des emplacements préférés.
- Envoyez au client une adresse IP spécifique telle que déterminée par l'évaluation de la requête ou de la réponse DNS (réécriture de la réponse DNS).
- Transmettez une demande au serveur de noms sans effectuer de recherche dans le cache DNS de la solution matérielle-logicielle.
- Déposez une demande.

Vous ne pouvez pas créer d'action DNS pour supprimer une demande DNS ou pour contourner le cache DNS sur l'appliance. Si vous souhaitez supprimer une demande DNS, utilisez l'action intégrée DNS_Default_Act_Drop. Si vous souhaitez contourner le cache DNS, utilisez l'action intégrée DNS_Default_Act_CacheBypass. Les deux actions sont disponibles avec les actions personnalisées dans les boîtes de dialogue Créer une stratégie DNS et Configurer la stratégie DNS. Ces actions intégrées ne peuvent pas être modifiées ou supprimées.

Pour configurer une action DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une action DNS et vérifier la configuration :

```
add dns action <actionName> <actionType> (-IPAddress <ip_addr |
    ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
    ...) [-TTL <secs>]

show dns action [<actionName>]
<!--NeedCopy-->
```

Exemples

Exemple 1 : Configuration de la réécriture de la réponse DNS. L'action DNS suivante envoie au client une adresse IP préconfigurée lorsque la stratégie à laquelle l'action est liée est évaluée à true :

```
add dns action dns_act_response_rewrite Rewrite_Response -IPAddress
    192.0.2.20 192.0.2.56 198.51.100.10
 Done

show dns action dns_act_response_rewrite
1)  ActionName:  dns_act_response_rewrite ActionType:  Rewrite_Response
     TTL:  3600              IPAddress:  192.0.2.20 192.0.2.56
    198.51.100.10
 Done
<!--NeedCopy-->
```

Exemple 2 : Configuration d'une réponse basée sur la vue DNS. L'action DNS suivante envoie au client une adresse IP pour laquelle vous avez configuré une vue DNS :

```
add dns action send_ip_from_view_internal_ip ViewName -viewName
    view_internal_ip
Done

show dns action send_ip_from_view_internal_ip
1)  ActionName:  send_ip_from_view_internal_ip ActionType:  ViewName
       ViewName:  view_internal_ip
 Done
<!--NeedCopy-->
```

Exemple 3 : Configuration d'une réponse basée sur une liste d'emplacements préférés. L'action DNS suivante envoie au client l'adresse IP qui correspond à l'emplacement préféré qu'il sélectionne dans la liste d'emplacements spécifiée :


```
add dns action send_preferred_location GslbPrefLoc -preferredLocList NA
    .tx.ns1.\*.\*.* NA.tx.ns2.\*.\*.* NA.tx.ns3.\*.\*.*
Done

show dns action  send_preferred_location
1)  ActionName:  send_preferred_location ActionType:  GslbPrefLoc
    PreferredLocList:  "NA.tx.ns1.\*.\*.\*" "NA.tx.ns2.\*.\*.\*" "NA.tx.
    ns3.\*.\*.*"
 Done
<!--NeedCopy-->
```

Pour configurer une action DNS à l'aide de l'utilitaire de configuration NetScaler

1. Accédez à Gestion du trafic > DNS > Actions, créez ou modifiez une action DNS.
2. Dans la boîte de dialogue Créer une action DNS ou Configurer une action DNS, définissez les paramètres suivants :
   - Nom de l'action (ne peut pas être modifié pour une action DNS existante)
   - Type (ne peut pas être modifié pour une action DNS existante)
     Pour définir le paramètre
     Type, effectuez l'une des opérations suivantes :
     - Pour créer une action DNS associée à une vue DNS, sélectionnez Nom de la vue. Ensuite, dans la liste Nom de la vue, sélectionnez la vue DNS que vous souhaitez utiliser dans l'action.
     - Pour créer une action DNS avec une liste d'emplacements préférés, sélectionnez Liste des emplacements préférés. Dans Emplacement préféré, saisissez un lieu, puis cliquez sur Ajouter. Ajoutez autant d'emplacements DNS que vous le souhaitez.
     - Pour configurer une action DNS de réécriture d'une réponse DNS sur la base de l'évaluation de la stratégie, sélectionnez Réécrire la réponse. Dans Adresse IP, saisissez une adresse IP, puis cliquez sur Ajouter. Ajoutez autant d'adresses IP que vous le souhaitez.
   - TTL (applicable uniquement au type d'action Réécrire la réponse)

Configurer les stratégies DNS

Les stratégies DNS fonctionnent sur une base de données d'emplacements qui utilise des adresses IP statiques et personnalisées. Les attributs de la demande DNS locale entrante sont définis dans le cadre d'une expression, et le site cible est défini dans le cadre d'une stratégie DNS. Lorsque vous définissez des actions et des expressions, vous pouvez utiliser une paire de guillemets simples (« ») comme qualificatif générique pour spécifier plusieurs emplacements. Lorsqu'une stratégie DNS est configurée et qu'une demande GSLB est reçue, la base de données d'adresses IP personnalisée est d'abord interrogée pour obtenir une entrée qui définit les attributs d'emplacement de la source :

- Lorsqu'une requête DNS provient d'un LDNS, les caractéristiques du LDNS sont évaluées par rapport aux stratégies configurées. Si elles correspondent, une action appropriée (affinité de site) est exécutée. Si les caractéristiques LDNS correspondent à plusieurs sites, la charge de la demande est équilibrée entre les sites qui correspondent aux caractéristiques LDNS.
- Si l'entrée est introuvable dans la base de données personnalisée, la base de données d'adresses IP statique est interrogée pour une entrée et, en cas de correspondance, l'évaluation de stratégie ci-dessus est répétée.
- Si l'entrée n'est pas trouvée dans les bases de données personnalisées ou statiques, le meilleur site est sélectionné et envoyé dans la réponse DNS sur la base de la méthode d'équilibrage de charge configurée.

Les restrictions suivantes s'appliquent aux politiques DNS créées sur l'appliance NetScaler.

- 64 stratégies au maximum sont prises en charge.
- Les politiques DNS sont globales pour l'appliance NetScaler et ne peuvent pas être appliquées à un serveur virtuel ou à un domaine spécifique.
- La liaison de stratégie spécifique au domaine ou au serveur virtuel n'est pas prise en charge.

Vous pouvez utiliser des stratégies DNS pour diriger les clients qui correspondent à une certaine plage d'adresses IP vers un site spécifique. Par exemple, si vous avez une configuration GSLB avec plusieurs sites GSLB séparés géographiquement, vous pouvez diriger tous les clients dont l'adresse IP se trouve dans une plage spécifique vers un centre de données particulier.

Le trafic DNS basé sur TCP et UDP peut être évalué. Les expressions de stratégie sont disponibles pour le trafic DNS basé sur UDP sur le serveur et pour le trafic DNS UDP et le trafic DNS TCP côté client. En outre, vous pouvez configurer des expressions pour évaluer les requêtes et les réponses qui impliquent uniquement les types de questions DNS (ou valeurs QTYPE) suivants :

- Une
- AAAA
- NS
- SRV
- PTR
- CNAME
- SOA
- MX
- ANY

Les codes de réponse suivants (valeurs RCODE) sont également pris en charge :

- NOERROR - Aucune erreur
- FORMERR - Erreur de format
- SERVFAIL - Défaillance du serveur

- NXDOMAIN - Domaine inexistant
- NOTIMP - Type de requête non implémenté
- REFUSÉ - Requête refusée

Vous pouvez configurer des expressions pour évaluer le trafic DNS. Une expression DNS commence par les préfixes DNS.REQ ou DNS.RES. Des fonctions sont disponibles pour évaluer le domaine interrogé, le type de requête et le protocole transporteur. Pour plus d'informations sur les expressions DNS, voir « Expressions pour évaluer un message DNS et identifier son protocole de transporteur » dans « Configuration et référence des stratégies ».

Pour ajouter une stratégie DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une stratégie DNS et vérifier la configuration :

```
add dns policy <name> <rule> <actionName>
show dns policy <name>
<!--NeedCopy-->
```

Exemple :

```
> add dns policy-GSLB-1 'CLIENT.UDP.DNS.DOMAIN.EQ("domainname")'
   my_dns_action
 Done
> show dns policy-GSLB-1
    Name: policy-GSLB-1
    Rule: CLIENT.UDP.DNS.DOMAIN.EQ("domainname")
    Action Name: my_dns_action
    Hits: 0
    Undef Hits: 0

 Done
<!--NeedCopy-->
```

Pour supprimer une stratégie DNS configurée à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm dns policy <name>
<!--NeedCopy-->
```

Pour configurer une politique DNS à l'aide de l'utilitaire de configuration NetScaler

1. Accédez à Gestion du trafic > DNS > Stratégies et créez une stratégie DNS.
2. Dans la boîte de dialogue Créer une stratégie DNS ou Configurer une stratégie DNS, définissez les paramètres suivants :
   - Nom de la stratégie (ne peut pas être modifié pour une stratégie existante)
   - Action
   - Expression

     Pour spécifier une expression, procédez comme suit :
     a) Cliquez sur Ajouter, puis, dans la zone de liste déroulante qui apparaît, sélectionnez l'élément d'expression par lequel vous souhaitez commencer l'expression. Une deuxième liste apparaît. La liste contient un ensemble d'éléments d'expression que vous pouvez utiliser immédiatement après le premier élément d'expression.
     b) Dans la deuxième liste, sélectionnez l'élément d'expression souhaité, puis entrez un point.
     c) Après chaque sélection, si vous entrez une période, le prochain ensemble d'éléments d'expression valides apparaît dans une liste. Sélectionnez des éléments d'expression et remplissez les arguments des fonctions jusqu'à ce que vous obteniez l'expression souhaitée.
3. Cliquez sur Créer ou sur OK, puis sur Fermer.

Stratégies de liaison DNS

Les politiques DNS sont liées globalement à l'appliance NetScaler et sont disponibles pour tous les serveurs virtuels GSLB configurés. Même si les stratégies DNS sont globalement liées, l'exécution des stratégies peut être limitée à un serveur virtuel GSLB spécifique en spécifiant le domaine dans l'expression.

Remarque : Même si la commande bind dns global accepte REQ_OVERRIDE et RES_OVERRIDE comme points de liaison valides, ces points de liaison sont redondants, car les stratégies DNS ne peuvent être liées que globalement. Liez vos stratégies DNS uniquement aux points de liaison REQ_DEFAULT et RES_DEFAULT.

Pour lier une stratégie DNS globalement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie DNS globalement et vérifier la configuration :

```
bind dns global <policyName> <priority> [-gotoPriorityExpression <
    string>] [-type <type>]
show dns global -type <type>
<!--NeedCopy-->
```

Exemple :


```
bind dns global policy-GSLB-1 10 -gotoPriorityExpression END
 Done
show dns global -type REQ_DEFAULT
1)  Policy Name: policy-GSLB-1
    Priority: 10
    GotoPriorityExpression: END
 Done
<!--NeedCopy-->
```

Pour lier une stratégie DNS globalement à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > DNS > Stratégies.
2. Dans le volet d'informations, cliquez sur Liaisons globales.
3. Dans la boîte de dialogue Lier/délier les stratégies DNS à la stratégie globale, cliquez sur Insérer une stratégie.
4. Dans la colonne Nom de la stratégie, sélectionnez, dans la liste, la stratégie que vous souhaitez lier. Sinon, dans la liste, cliquez sur Nouvelle stratégie, puis créez une stratégie DNS en définissant des paramètres dans la boîte de dialogue Créer une stratégie DNS.
5. Pour modifier une stratégie déjà liée globalement, cliquez sur le nom de la stratégie, puis sur Modifier la stratégie. Ensuite, dans la boîte de dialogue Configurer la stratégie DNS, modifiez la stratégie, puis cliquez sur OK.
6. Pour délier une stratégie, cliquez sur le nom de la stratégie, puis cliquez sur Délier la stratégie.
7. Pour modifier la priorité attribuée à une stratégie, double-cliquez sur la valeur de priorité, puis saisissez une nouvelle valeur.
8. Pour régénérer les priorités attribuées, cliquez sur Régénérer les priorités. Les valeurs de priorité sont modifiées pour commencer à 100, avec des incréments de 10, sans affecter l'ordre d'évaluation.
9. Cliquez sur OK.

Pour afficher les liaisons globales d'une stratégie DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show dns global
```

Pour afficher les liaisons globales d'une stratégie DNS à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **DNS** > **Stratégies**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales**. Les liaisons globales de toutes les stratégies DNS apparaissent dans cette boîte de dialogue.

Ajout de vues DNS

Vous pouvez configurer des vues DNS pour identifier différents types de clients et fournir une adresse IP appropriée à un groupe de clients qui interrogent le même domaine GSLB. Les vues DNS sont configurées à l'aide de stratégies DNS qui sélectionnent les adresses IP renvoyées au client.

Par exemple, si vous avez configuré GSLB pour le domaine de votre entreprise et que le serveur est hébergé sur le réseau de votre entreprise, les clients qui demandent le domaine depuis le réseau interne de votre entreprise peuvent recevoir l'adresse IP interne du serveur au lieu de l'adresse IP publique. En revanche, les clients qui interrogent le DNS pour le domaine à partir d'Internet peuvent obtenir l'adresse IP publique du domaine.

Pour ajouter une vue DNS, vous lui attribuez un nom de 31 caractères maximum. Le premier caractère doit être un chiffre ou une lettre. Les caractères suivants sont également autorisés : @ _ -. (point) : (deux-points) # et espace (). Après avoir ajouté la vue, vous configurez une stratégie pour l'associer aux clients et à une partie du réseau, et vous liez la stratégie globalement. Pour configurer et lier une stratégie DNS, consultez **Gestion du trafic DNS local à l'aide de stratégies DNS**.

Pour ajouter une vue DNS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer une vue DNS et vérifier la configuration :

```
add dns view <viewName>
show dns view <viewName>
<!--NeedCopy-->
```

Exemple :

```
add dns view PrivateSubnet
show dns view PrivateSubnet
<!--NeedCopy-->
```

Pour supprimer une vue DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm dns view <viewName>
<!--NeedCopy-->
```

Pour ajouter une vue DNS à l'aide de l'utilitaire de configuration

Accédez à Gestion du trafic > DNS > Vues et ajoutez une vue DNS.

Pour plus d'informations sur la création d'une stratégie DNS et sur la façon de lier des stratégies DNS globalement, voir **Gestion du trafic DNS local à l'aide de stratégies DNS**.

Configurer le GSLB pour la proximité

May 5, 2023

Lorsque vous configurez GSLB pour la proximité, les demandes des clients sont transmises au centre de données le plus proche. Le principal avantage de la méthode GSLB basée sur la proximité est la réduction des temps de réponse grâce à la sélection du centre de données disponible le plus proche. Un tel déploiement est essentiel pour les applications nécessitant un accès rapide à de grands volumes de données.

Vous pouvez configurer le GSLB pour la proximité en fonction du temps aller-retour (RTT), de la proximité statique ou d'une combinaison des deux.

Configurer la méthode de temps aller-retour dynamique (RTT)

Le temps d'aller-retour dynamique (RTT) est une mesure du temps ou du délai sur le réseau entre le serveur DNS local du client et une ressource de données. Pour mesurer le RTT dynamique, l'appliance NetScaler sonde le serveur DNS local du client et recueille des informations métriques RTT. L'appliance utilise ensuite cette métrique pour prendre sa décision d'équilibrage de charge. L'équilibrage global de la charge des serveurs surveille l'état en temps réel du réseau et dirige dynamiquement la demande du client vers le centre de données présentant la valeur RTT la plus faible

Pour configurer le GSLB pour la proximité avec la méthode dynamique, vous devez d'abord configurer la configuration GSLB de base, puis configurer le RTT dynamique.

Créez d'abord deux sites GSLB, local et distant. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB, puis liez les services au serveur virtuel. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB sur le site local. Enfin, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, configurez la méthode RTT dynamique.

Pour plus d'informations sur la configuration du serveur virtuel GSLB pour utiliser la méthode RTT dynamique pour l'équilibrage de charge, voir Configuration du RTT dynamique.

Configurer la proximité statique

La méthode de proximité statique pour GSLB utilise une base de données de proximité statique basée sur l'adresse IP pour déterminer la proximité entre le serveur DNS local du client et les sites GSLB. L'appliance NetScaler répond avec l'adresse IP du site qui correspond le mieux aux critères de proximité.

Si deux sites GSLB ou plus situés à des emplacements géographiques différents diffusent le même contenu, l'appliance NetScaler gère une base de données de plages d'adresses IP et utilise cette base de données pour prendre des décisions concernant les sites GSLB vers lesquels diriger les demandes des clients entrantes.

Pour configurer le GSLB pour la proximité avec proximité statique, vous devez d'abord configurer la configuration GSLB de base, puis configurer la proximité statique.

Créez d'abord deux sites GSLB, local et distant. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB, puis liez les services au serveur virtuel. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB sur le site local. Enfin, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, configurez la proximité statique.

Pour plus d'informations sur la configuration du serveur virtuel GSLB pour utiliser la proximité statique pour l'équilibrage de charge, reportez-vous à la section Configuration de la proximité statique.

Configurer la proximité statique et la RTT dynamique

Vous pouvez configurer le serveur virtuel GSLB pour qu'il utilise une combinaison de proximité statique et de RTT dynamique lorsque certains clients proviennent d'un réseau interne tel qu'une succursale. Vous pouvez configurer GSLB de telle sorte que les clients provenant de la succursale ou de tout autre réseau interne soient dirigés vers un site GSLB particulier qui est géographiquement proche du réseau client. Pour toutes les autres demandes, vous pouvez utiliser le RTT dynamique.

Créez d'abord deux sites GSLB, local et distant. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB, puis liez les services au serveur virtuel. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB sur le site local. Enfin, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, configurez le serveur virtuel GSLB pour qu'il utilise la proximité statique pour tout le trafic provenant d'un réseau interne, puis utilisez RTT dynamique pour tout autre trafic.

Pour plus d'informations sur la configuration de la proximité statique, reportez-vous à la section Configuration de la proximité statique et pour plus d'informations sur la configuration du RTT dynamique, voir Configuration du RTT dynamique.

Protéger la configuration GSLB contre les défaillances

May 5, 2023

Vous pouvez protéger votre configuration GSLB contre les défaillances d'un site GSLB ou d'un serveur virtuel GSLB en configurant les éléments suivants :

- Un serveur virtuel GSLB de sauvegarde
- Une appliance NetScaler capable de répondre avec plusieurs adresses IP
- Une adresse IP de sauvegarde pour un domaine GSLB

Vous pouvez également détourner le trafic excédentaire vers un serveur virtuel de sauvegarde à l'aide de spillover.

Configuration d'un serveur virtuel GSLB de sauvegarde

La configuration d'une entité de sauvegarde pour un serveur virtuel GSLB garantit que le trafic DNS vers un site n'est pas interrompu en cas de panne du serveur virtuel GSLB. L'entité de sauvegarde peut être un autre serveur virtuel GSLB ou une adresse IP de sauvegarde. Avec une entité de sauvegarde configurée, si le serveur virtuel GSLB principal tombe en panne, l'entité de sauvegarde gère les demandes DNS. Pour spécifier ce qui doit se produire lorsque le serveur virtuel GSLB principal revient à nouveau, vous pouvez configurer l'entité de sauvegarde pour continuer à gérer le trafic jusqu'à ce que vous autorisiez manuellement le serveur virtuel principal à prendre le relais (à l'aide de l'option DisablePrimaryOnDown).

Remarque : Vous pouvez configurer une seule entité de sauvegarde comme sauvegarde pour plusieurs serveurs virtuels GSLB.

Pour configurer un serveur virtuel GSLB de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel GSLB en tant que serveur virtuel de sauvegarde et vérifier la configuration :


```
set gslb vserver <name> -backupVServer <name> [-disablePrimaryOnDown (
    ENABLED | DISABLED)]

show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2 -
    disablePrimaryOnDown ENABLED
show gslb vserver vserver-GSLB-1
<!--NeedCopy-->
```

Pour définir le serveur virtuel GSLB comme serveur virtuel de sauvegarde à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels**, puis double-cliquez sur le serveur virtuel GSLB.
2. Sélectionnez la section **Sauvegarde Virtual Server** et choisissez le serveur virtuel de sauvegarde.

Configurer une configuration GSLB pour répondre avec plusieurs adresses IP

Une réponse DNS typique contient l'adresse IP du service GSLB le plus performant. Toutefois, si vous activez les réponses IP multiples (MIR), l'appliance NetScaler envoie le meilleur service GSLB en tant que premier enregistrement de la réponse et ajoute les services actifs restants sous forme d'enregistrements supplémentaires. Si MIR est désactivé (valeur par défaut), l'appliance NetScaler envoie le meilleur service en tant que seul enregistrement en réponse.

Pour configurer un serveur virtuel GSLB pour plusieurs réponses IP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel GSLB pour plusieurs réponses IP et vérifier la configuration :

```
set gslb vserver<name> -MIR (ENABLED | DISABLED)
-  show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :


```
set gslb vserver vserver-GSLB-1 -MIR ENABLED
 show gslb vserver <vserverName>
<!--NeedCopy-->
```

Pour configurer un serveur virtuel GSLB pour plusieurs réponses IP à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel GSLB pour lequel vous souhaitez configurer un serveur virtuel de sauvegarde (par exemple, vServer-GSLB-1).
2. Dans l'onglet **Avancé**, sous Lorsque ce serveur virtuel est « UP », activez la case à cocher Envoyer toutes les adresses IP de service « actives » en réponse (MIR), puis sélectionnez **OK**.

Configuration d'un serveur virtuel GSLB pour répondre avec un enregistrement d'adresse vide en cas de panne

Une réponse DNS peut contenir l'adresse IP du domaine demandé ou une réponse indiquant que l'adresse IP du domaine n'est pas connue du serveur DNS, auquel cas la requête est transmise à un autre serveur de noms. Ce sont les seules réponses possibles à une requête DNS.

Lorsqu'un serveur virtuel GSLB est désactivé ou à l'état DOWN, la réponse à une requête DNS pour le domaine GSLB lié à ce serveur virtuel contient les adresses IP de tous les services liés au serveur virtuel. Toutefois, vous pouvez configurer le serveur virtuel GSLB pour, dans ce cas, envoyer une réponse vide (EDR). Lorsque cette option est définie, une réponse DNS provenant d'un serveur virtuel GSLB à l'état DOWN ne contient pas d'enregistrements d'adresses IP, mais le code de réponse est correct. Cela empêche les clients de tenter de se connecter à des sites GSLB inactifs.

Remarque : Vous devez configurer ce paramètre pour chaque serveur virtuel auquel vous souhaitez qu'il s'applique.

Pour configurer un serveur virtuel GSLB pour des réponses vides à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb vserver<name> -EDR (ENABLED | DISABLED)
<!--NeedCopy-->
```

Exemple :

```
> set gslb vserver vserver-GSLB-1 -EDR ENABLED
```



```
2   Done
3 <!--NeedCopy-->
```

Pour configurer un serveur virtuel GSLB pour les réponses vides à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel GSLB pour lequel vous souhaitez configurer un serveur virtuel de sauvegarde (par exemple, vServer-GSLB-1).
2. Dans l'onglet Avancé, sous Lorsque ce serveur virtuel est en panne, activez la case à cocher Ne pas envoyer d'adresse IP de service en réponse (EDR).
3. Cliquez sur **OK**.

Configuration d'une adresse IP de sauvegarde pour un domaine GSLB

Vous pouvez configurer un site de sauvegarde pour votre configuration GSLB. Lorsque cette configuration est en place, si tous les sites principaux tombent en panne, l'adresse IP du site de sauvegarde est fournie dans la réponse DNS.

En règle générale, si un serveur virtuel GSLB est actif, ce serveur virtuel envoie une réponse DNS avec l'une des adresses IP de site actives sélectionnées par la méthode GSLB configurée. Si tous les sites principaux configurés sur le serveur virtuel GSLB sont inactifs (à l'état DOWN), le serveur ADNS (Domain Name System) ou le serveur DNS autoritaire envoie une réponse DNS avec l'adresse IP du site de sauvegarde.

Remarque : Lorsqu'une adresse IP de sauvegarde est envoyée, la persistance n'est pas respectée.

Pour définir une adresse IP de sauvegarde pour un domaine à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir une adresse IP de sauvegarde et vérifier la configuration :

```
1 set gslb vserver <name> -domainName <string> -backupIP <IPAddress>
2 show gslb vserver <name>
3 <!--NeedCopy-->
```

Exemple :

```
1 set gslb vserver vserver-GSLB-1 -domainName www.abc.com -backupIP
     10.102.29.66
2 show gslb vserver vserver-GSLB-1
```



```
<!--NeedCopy-->
```

Pour définir une adresse IP de sauvegarde pour un domaine à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel GSLB auquel vous souhaitez lier le domaine de sauvegarde (par exemple, vServer-GSLB-1).
2. Cliquez sur la section **Domaines**, configurez le domaine GSLB et spécifiez l'adresse IP du domaine de sauvegarde dans le champ **IP de sauvegarde** .

Rediriger le trafic excédentaire vers un serveur virtuel de sauvegarde

Une fois que le nombre de connexions à un serveur virtuel GSLB principal dépasse la valeur seuil configurée, vous pouvez utiliser l'option spillover pour rediriger les nouvelles connexions vers un serveur virtuel GSLB de sauvegarde. Cette valeur de seuil peut être calculée dynamiquement ou définie manuellement. Une fois que le nombre de connexions au serveur virtuel principal tombe en dessous du seuil, le serveur virtuel GSLB principal reprend le traitement des demandes des clients.

Vous pouvez configurer la persistance avec le spillover. Lorsque la persistance est configurée, les nouveaux clients sont redirigés vers le serveur virtuel de sauvegarde si ce client n'est pas déjà connecté à un serveur virtuel principal. Lorsque la persistance est configurée, les connexions qui ont été redirigées vers le serveur virtuel de sauvegarde ne sont pas renvoyées vers le serveur virtuel principal une fois que le nombre de connexions au serveur virtuel principal est tombé en dessous du seuil. Au lieu de cela, le serveur virtuel de sauvegarde continue de traiter ces connexions jusqu'à ce qu'elles soient interrompues par l'utilisateur. Pendant ce temps, le serveur virtuel principal accepte de nouveaux clients.

Le seuil peut être mesuré en fonction du nombre de connexions, de la bande passante et de l'état de santé des services.

Si le serveur virtuel de sauvegarde atteint le seuil configuré et ne peut supporter aucune charge supplémentaire, le serveur virtuel principal redirige toutes les demandes vers l'URL de redirection désignée. Si aucune URL de redirection n'est configurée sur le serveur virtuel principal, les demandes suivantes sont supprimées.

La fonctionnalité de débordement empêche le service GSLB de sauvegarde à distance (site GSLB de sauvegarde) d'être inondé de demandes clients en cas de défaillance du serveur virtuel GSLB principal. Cela se produit lorsqu'un moniteur est lié à un service GSLB distant et que le service rencontre une défaillance qui entraîne la panne de son état. Le moniteur continue toutefois de maintenir l'état du service GSLB distant actif, en raison de la fonction de propagation.

Dans le cadre de la résolution de ce problème, deux états sont maintenus pour un service GSLB, l'état principal et l'état effectif. L'état principal est l'état du serveur virtuel principal et l'état effectif est l'état

cumulé des serveurs virtuels (chaîne principale et de sauvegarde). L'état effectif est défini sur UP si l'un des serveurs virtuels de la chaîne de serveurs virtuels est actif. Un drapeau indiquant que le VIP principal a atteint le seuil est également fourni. Le seuil peut être mesuré soit par le nombre de connexions, soit par la bande passante.

Un service n'est considéré pour GSLB que si son état principal est UP. Le trafic est dirigé vers le service GSLB de sauvegarde uniquement lorsque tous les serveurs virtuels principaux sont DOWN. En règle générale, ces déploiements ne comportent qu'un seul service GSLB de sauvegarde.

L'ajout d'états primaires et effectifs à un service GSLB a les effets suivants :

- Lorsque la persistance de l'adresse IP source est configurée, le DNS local est dirigé vers le site précédemment sélectionné uniquement si le serveur virtuel principal du site sélectionné est actif et inférieur au seuil. La persistance peut être ignorée en mode round robin.
- Si la persistance basée sur les cookies est configurée, les requêtes client sont redirigées uniquement lorsque le serveur virtuel principal sur le site sélectionné est UP.
- Si le serveur virtuel principal a atteint sa saturation et que les VIP de sauvegarde sont absents ou inexistants, l'état effectif est défini sur DOWN.
- Si les moniteurs externes sont liés à un serveur virtuel HTTP-HTTPS, le moniteur décide de l'état principal.
- S'il n'y a pas de serveur virtuel de sauvegarde sur le serveur virtuel principal et que le serveur virtuel principal a atteint son seuil, l'état effectif est défini sur DOWN.

Pour configurer un serveur virtuel GSLB de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le serveur virtuel GSLB de sauvegarde et vérifier la configuration :

```
set gslb vserver <name> -soMethod <method> -soThreshold <threshold> -
    soPersistence ( \*\*ENABLED\*\* | \*\*DISABLED\*\* ) -
    soPersistenceTimeout <timeout>
show gslb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -soMethod CONNECTION -soThreshold 1000
    -soPersistence ENABLED -soPersistenceTimeout 2
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```


Pour configurer un serveur virtuel GSLB de sauvegarde à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **GSLB** > **Serveurs virtuels** et double-cliquez sur le serveur virtuel que vous souhaitez configurer en tant que sauvegarde (par exemple, vServer-LB-1).
2. Cliquez sur la section **Spillover** et définissez les paramètres suivants :
   - Méthode — SomeMod
   - Seuil — SoThreshold
   - Délai de persistance (min) — SoPersistenceTimeout
3. Sélectionnez l'option Persistance et cliquez sur **OK**.

Configurer GSLB pour la reprise après sinistre

May 5, 2023

La capacité de reprise après sinistre est essentielle, car les temps d'arrêt sont coûteux. Une appliance NetScaler configurée pour le GSLB transfère le trafic vers le centre de données le moins chargé ou le plus performant. Cette configuration, appelée configuration active-active, améliore non seulement les performances, mais assure également une reprise après sinistre immédiate en acheminant le trafic vers d'autres centres de données si un centre de données faisant partie de la configuration est en panne. Vous pouvez également configurer une configuration GSLB active en veille uniquement pour la reprise après sinistre.

Configuration du GSLB pour la reprise après sinistre dans une configuration de centre de données actif en veille

Une configuration de reprise après sinistre classique comprend un centre de données actif et un centre de données de secours. Le centre de données de secours est un site distant. Lorsqu'un basculement survient à la suite d'un sinistre qui rend le centre de données actif principal inactif, le centre de données de secours devient opérationnel.

La configuration de la reprise après sinistre dans une configuration de centre de données actif en veille comprend les tâches suivantes.

- Créez le centre de données actif.
  - Ajoutez un site GSLB local.
  - Ajoutez un serveur virtuel GSLB, qui représente le centre de données actif.
  - Liez le domaine au serveur virtuel GSLB.
  - Ajoutez des services gslb et liez les services au serveur virtuel GSLB actif.
- Créez le centre de données de secours.
  - Ajoutez un site gslb distant.
  - Ajoutez un vserver gslb, qui représente un centre de données de secours.

- Ajoutez les services gslb qui représentent le centre de données de secours et liez les services au vserver gslb de secours.
- Désignez le centre de données de secours en configurant le serveur virtuel GSLB de secours en tant que serveur virtuel de sauvegarde pour le serveur virtuel GSLB actif.

Une fois que vous avez configuré le centre de données principal, répliquez la configuration du centre de données de sauvegarde et désignez-la comme site GSLB de secours en désignant un serveur virtuel GSLB sur ce site comme serveur virtuel de sauvegarde.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Pour désigner le site GSLB de secours à l'aide de l'interface de ligne de commande

Sur le site actif et sur le site distant, à l'invite de commande, tapez :

```
set gslb vserver <name> -backupVserver <string>
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2
<!--NeedCopy-->
```

Pour configurer le site de secours à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels et double-cliquez sur le serveur virtuel GSLB du site principal.
2. Cliquez sur la section **Serveur virtuel de sauvegarde** et sélectionnez un serveur virtuel de sauvegarde.

Par défaut, une fois que le serveur virtuel principal est actif, il commence à recevoir du trafic. Toutefois, si vous souhaitez que le trafic soit dirigé vers le serveur virtuel de sauvegarde même après que le serveur virtuel principal soit activé, utilisez l'
option « Désactiver le serveur principal en cas d'arrêt ».

Configuration pour la reprise après sinistre dans une configuration de centre de données actif-actif

Un déploiement GSLB actif-actif, dans lequel les deux sites GSLB sont actifs, élimine tout risque pouvant découler de la mise en place d'un centre de données de secours. Avec une telle configuration, le contenu du Web ou de l'application peut être reflété dans des emplacements géographiquement distincts. Cela garantit la disponibilité constante des données dans chaque centre de données distribué.

Pour configurer le GSLB pour la reprise après sinistre dans une configuration de centre de données actif-actif, vous devez d'abord configurer la configuration GSLB de base sur le premier centre de données, puis configurer tous les autres centres de données.

Créez d'abord au moins deux sites GSLB. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB, puis liez les services au serveur virtuel. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB du site local. Enfin, sur le site local, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP du serveur virtuel que le service GSLB.

Une fois que vous avez configuré le premier centre de données, répliquez la configuration pour les autres centres de données partie de la configuration.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Configuration pour la reprise après sinistre avec Weighted Round Robin

Lorsque vous configurez GSLB pour utiliser la méthode circulaire pondérée, des poids sont ajoutés aux services GSLB et le pourcentage configuré du trafic entrant est envoyé à chaque site GSLB. Par exemple, vous pouvez configurer votre configuration GSLB pour transférer 80 % du trafic vers un site et 20 % du trafic vers un autre. Ensuite, l'appliance NetScaler envoie quatre demandes au premier site pour chaque demande qu'elle envoie au second.

Pour configurer la méthode circulaire pondérée, créez d'abord deux sites GSLB, local et distant. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB, puis liez les services au serveur virtuel. Configurez la méthode GSLB comme méthode Round Robin. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB. Enfin, créez un serveur virtuel d'équilibrage de charge avec la même adresse IP de serveur virtuel que le service GSLB.

Chaque service qui représente un serveur physique sur le réseau est associé à des pondérations. Par conséquent, le service GSLB se voit attribuer un poids dynamique qui est la somme des poids de tous les services qui lui sont liés. Le trafic est ensuite réparti entre les services GSLB sur la base du rapport entre le poids dynamique du service particulier et le poids total. Vous pouvez également configurer des pondérations individuelles pour chaque service GSLB au lieu de la pondération dynamique.

Si les services n'ont pas de poids associés, vous pouvez configurer le serveur virtuel GSLB pour qu'il utilise le nombre de services qui lui sont liés pour calculer la pondération dynamiquement.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, vous devez configurer la méthode pondérée de manière à ce que le trafic soit réparti entre les sites GSLB configurés en fonction des

pondérations configurées pour les services individuels.

Pour configurer un serveur virtuel afin d'attribuer des poids aux services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes, selon que vous souhaitez créer un nouveau serveur virtuel d'équilibrage de charge ou configurer un serveur existant :

```
add lb vserver <name>@ -weight <WeightValue> <ServiceName>
set lb vserver <name>@ -weight <WeightValue> <ServiceName>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
set lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
<!--NeedCopy-->
```

Pour définir la pondération dynamique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb vserver <name> -dynamicWeight DynamicWeightType
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -dynamicWeight ServiceWeight
<!--NeedCopy-->
```

Pour ajouter des poids aux services GSLB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set gslb vserver <name> -serviceName GSLBServiceName -weight
   WeightValue
<!--NeedCopy-->
```

Exemple :

```
set gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1 -weight 1
<!--NeedCopy-->
```


Pour configurer un serveur virtuel afin d'attribuer des poids aux services à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels et double-cliquez sur le serveur virtuel (par exemple, vServer-LB-1).
2. Cliquez sur la section Services et définissez le poids d'un service.

Pour ajouter des poids aux services GSLB à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels et double-cliquez sur le serveur virtuel (par exemple, vServer-GSLB-1)
2. Cliquez sur la section Services et définissez le poids du service dans le champ Poids.

Pour définir la pondération dynamique à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Serveurs virtuels et double-cliquez sur le serveur virtuel (par exemple, vServer-GSLB-1).
2. Cliquez sur la section **Méthode** et, dans la liste déroulante **Dynamic Weight**, sélectionnez **SERVICEWEIGHT**.

Configuration pour la reprise après sinistre avec Data Center Persistence

La persistance du datacenter est requise pour les applications Web qui nécessitent de maintenir une connexion avec le même serveur au lieu d'équilibrer la charge des demandes. Par exemple, dans un portail de commerce électronique, le maintien d'une connexion entre le client et le même serveur est essentiel. Pour de telles applications, la persistance des redirections HTTP peut être configurée dans une configuration active-active.

Pour configurer GSLB pour la reprise après sinistre avec persistance du centre de données, vous devez d'abord configurer la configuration de base du GSLB, puis configurer la persistance des redirections HTTP.

Créez d'abord deux sites GSLB, local et distant. Ensuite, pour le site local, créez un serveur virtuel GSLB et des services GSLB, puis liez les services au serveur virtuel. Créez ensuite des services ADNS et liez le domaine pour lequel vous configurez GSLB au serveur virtuel GSLB sur le site local. Créez ensuite un serveur virtuel d'équilibrage de charge avec la même adresse IP du serveur virtuel que le service GSLB. Enfin, dupliquez les étapes précédentes pour la configuration à distance ou configurez l'appliance NetScaler pour synchroniser automatiquement votre configuration GSLB.

Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Une fois que vous avez configuré une configuration GSLB de base, configurez la priorité de redirection HTTP pour activer la persistance du centre de données.

Pour configurer la redirection HTTP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la redirection HTTP et vérifier la configuration :

```
set gslb service <serviceName> -sitePersistence <sitePersistence> -
   sitePrefix <string>
show gslb service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
set gslb service Service-GSLB-1 -sitePersistence HTTPRedirect -
   sitePrefix vserver-GSLB-1
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

Pour configurer la redirection HTTP à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > GSLB > Services et double-cliquez sur le service GSLB à configurer.
2. Cliquez sur la section **Persistance du site**, sélectionnez l'option **HttpRedirect et, dans la zone de texte Préfixe** du **site, entrez le préfixe** du site (par exemple, vServer-GSLB-1).

> **Remarque**
>
> Lorsque la persistance du site n'est pas configurée et si un serveur virtuel d'équilibrage de charge configuré en tant que service GSLB local est DOWN, les requêtes HTTP sont redirigées vers d'autres sites GSLB sains à l'aide d'une redirection 302.

Remplacer le comportement de proximité statique en configurant les emplacements préférés

May 5, 2023

Vous souhaiterez peut-être diriger le trafic d'un serveur ou d'un réseau DNS (LDNS) local vers un service GSLB autre que le service GSLB sélectionné par la méthode de proximité statique pour ce trafic. C'est-à-dire que vous avez un

emplacement préféré pour ce trafic. Pour remplacer la méthode de proximité statique par des emplacements préférés, vous pouvez procéder comme suit :

1. Configurez une action DNS qui consiste en une liste d'emplacements préférés. Pour plus d'informations sur la configuration d'une action DNS, voir Configuration d'une action DNS.
2. Configurez une stratégie DNS pour identifier le trafic en provenance du serveur ou du réseau LDNS pour lequel vous souhaitez remplacer la proximité statique, et appliquez l'action dans la stratégie.
3. Liez la politique au point de liaison global de la demande.

Dans l'action DNS, vous pouvez configurer une liste contenant jusqu'à 8 emplacements préférés. Les emplacements doivent être fournis dans la notation qualificative en pointillés, qui est la notation dans laquelle vous ajoutez des emplacements personnalisés à la base de données de proximité statique. Les emplacements peuvent inclure des caractères génériques pour les qualificatifs que vous souhaitez omettre. Pour plus d'informations sur la notation de qualificatif pointillé pour les emplacements, voir Ajout d'entrées personnalisées à une base de données de proximité statique. Lorsque vous saisissez les emplacements préférés, vous devez les saisir dans l'ordre décroissant de priorité.

Lorsqu'une politique est évaluée à
TRUE, l'appliance NetScaler fait correspondre les emplacements préférés, par ordre de priorité, aux emplacements des services GSLB. Les matchs sont des deux types suivants :

- Si tous les qualificatifs non génériques d'un emplacement préféré correspondent aux qualificatifs correspondants du site d'un service GSLB, la correspondance est considérée comme parfaite. Par exemple, un emplacement de service GSLB de *.UK.*.* ou Europe.UK.*.* correspond parfaitement à l'emplacement préféré *.UK.*.*.
- Si seul un sous-ensemble des qualificatifs non génériques correspond, la correspondance est considérée comme une correspondance partielle. Par exemple, l'emplacement du service GSLB Europe.eg correspond partiellement à l'emplacement préféré Europe.uk.

Lorsqu'une politique DNS est évaluée à
TRUE, l'algorithme suivant est utilisé pour sélectionner un service GSLB :

1. L'appliance évalue l'emplacement préféré ayant la priorité la plus élevée et descend par ordre de priorité jusqu'à ce qu'une correspondance parfaite soit trouvée entre un emplacement préféré et l'emplacement d'un service GSLB.

   Si une correspondance parfaite est trouvée, l'appliance vérifie si le service GSLB correspondant est actif. S'il fonctionne, il renvoie l'adresse IP du service GSLB dans la réponse DNS. Si plusieurs correspondances parfaites sont trouvées (ce qui peut se produire lorsqu'un ou plusieurs caractères génériques sont utilisés à un emplacement préféré), l'appliance vérifie l'état de chacun des services GSLB correspondants et équilibre la charge des services GSLB actifs.

2. Si aucune correspondance parfaite n'est trouvée pour aucun des emplacements préférés, l'appliance revient à l'emplacement préféré ayant la priorité la plus élevée et descend

dans l'ordre de priorité jusqu'à ce qu'une correspondance partielle soit trouvée entre un emplacement préféré et l'emplacement d'un service GSLB.

Si une correspondance partielle est trouvée, l'appliance vérifie si le service GSLB correspondant est actif. S'il fonctionne, il renvoie l'adresse IP du service GSLB dans la réponse DNS. Si plusieurs correspondances partielles sont détectées, l'appliance vérifie l'état de chacun des services GSLB correspondants et équilibre la charge des services GSLB actifs.

3. Si aucune correspondance parfaite ou partielle n'est trouvée, l'appliance équilibre la charge de tous les autres services GSLB disponibles.

   De cette manière, l'appliance met en œuvre un type d'affinité de site pour le trafic qui correspond à la politique DNS.

Exemple

Envisagez une configuration GSLB composée des huit services GSLB suivants :

- Asia.in
- Asie.JPN
- Asia.hk
- Europe.UK
- Europe.ru
- Europe.eg
- Afrique.sd
- Afrique.zmb

Examinez plus en détail l'action et la configuration de la politique DNS suivantes :

```
1 > add dns action prefLoc11 GslbPrefLoc -preferredLocList "Asia.HK" "
     Europe.UK"
2  Done
3 > add dns policy dnsPolPrefLoc "CLIENT.IP.SRC.MATCHES_LOCATION("\*.ZMB
     .\*.*")" prefLoc11
4  Done
5 <!--NeedCopy-->
```

Lorsque l'appliance reçoit une demande provenant de l'emplacement *.ZMB..**, les emplacements préférés sont évalués comme suit :

1. L'appliance tente de trouver un service GSLB dont l'emplacement correspond parfaitement à Asia.hk, qui est l'emplacement préféré ayant la priorité la plus élevée. Elle constate que le service GSLB d'Asia.hk est parfaitement adapté. Si le service GSLB est actif, il envoie au client l'adresse IP du service GSLB.

2. Si le service GSLB sur Asia.hk est hors service, l'appliance tente de trouver la solution idéale pour le deuxième emplacement préféré, Europe.UK. Elle constate que le service GSLB proposé par Europe.uk est parfaitement adapté. Si le service GSLB fonctionne, il envoie au client l'adresse IP du service.
3. Si le service GSLB sur Europe.uk est en panne, il retourne à l'emplacement préféré ayant la priorité la plus élevée, Asia.hk, et recherche des correspondances partielles. Pour Asia.hk, il constate que Asia.in et Asia.JPN sont des correspondances partielles. Si un seul des services GSLB correspondants est actif, il envoie au client l'adresse IP du service. Si les deux sites fonctionnent, il équilibre la charge des deux services.
4. Si toutes les correspondances partielles pour Asia.hk sont indisponibles, l'appliance recherche des correspondances partielles pour Europe.uk. Elle constate que Europe.ru et Europe.eg ne correspondent que partiellement à l'emplacement préféré. Si un seul des services GSLB correspondants est actif, il envoie au client l'adresse IP du service. Si les deux sites fonctionnent, il équilibre la charge des deux services.
5. Si toutes les correspondances partielles pour Europe.uk sont indisponibles, l'appliance équilibre la charge de tous les autres services GSLB disponibles. Dans l'exemple actuel, la charge de l'appareil équilibre Africa.sd et Africa.zmb parce que les six autres services GSLB ont été trouvés en panne.

Configurer la sélection du service GSLB à l'aide du changement de contenu

August 20, 2021

Dans un déploiement GSLB typique, vous pouvez hiérarchiser la sélection d'un ensemble de services GSLB liés à un serveur virtuel GSLB, mais vous ne pouvez pas effectuer les opérations suivantes :

- Restreindre la sélection d'un service GSLB à partir d'un sous-ensemble de services GSLB liés à un serveur virtuel GSLB pour le domaine donné.
- Appliquez différentes méthodes d'équilibrage de charge sur les différents sous-ensembles de services GSLB dans le déploiement.
- Appliquez des stratégies de débordement sur un sous-ensemble de services GSLB et vous ne pouvez pas avoir de sauvegarde pour un sous-ensemble de services GSLB.
- Configurez un sous-ensemble de services GSLB pour servir un contenu différent. Autrement dit, vous ne pouvez pas basculer de contenu entre les serveurs de différents sites GSLB. La configuration GSLB suppose que les serveurs contiennent le même contenu.
- Définissez un service GSLB de sous-ensemble avec des priorités différentes et spécifiez un ordre dans lequel les services du sous-ensemble sont appliqués à une demande.

Vous pouvez maintenant configurer une stratégie de commutation de contenu (CS) pour person-

naliser le déploiement GSLB. Configurez d'abord un ensemble de services GSLB et liez-le à un serveur virtuel GSLB. Ensuite, configurez un serveur virtuel CS de type cible GSLB, définissez une stratégie CS et une action avec le serveur virtuel GSLB comme serveur virtuel cible, et liez la stratégie CS au serveur virtuel CS.

> **Important**
>
> - Seules les stratégies CS avec des expressions basées sur DNS peuvent être liées à un serveur virtuel CS de type cible GSLB.
> - Si un service GLSB est lié à un serveur virtuel CS via un serveur virtuel GSLB, vous ne pouvez pas lier un autre serveur virtuel GSLB lié au même service GSLB au serveur virtuel CS.

Exemple

Considérez un déploiement GLSB qui comprend deux sites GSLB. Sur chaque site, quatre services GSLB (S-1, S-2, S-3 et S-4) sont liés au serveur virtuel GSLB VS-1. Vous pouvez configurer un serveur virtuel de commutation de contenu (CS) de type cible GSLB et définir une stratégie et une action CS avec VS-1 comme serveur virtuel cible, de sorte que les demandes de contenu en anglais ne soient traitées que par S-1 et S-2, et que les demandes de contenu dans la langue locale ne soient traitées que par S-3 et S-4.

Vous pouvez donner la priorité S-1 en configurant un serveur virtuel de sauvegarde sur VS-1 et en liant S-2 au serveur virtuel de sauvegarde. S-1 répond aux demandes du client. Si le serveur S-1 représente tombe en panne, S-2 sert les requêtes. Si S-1 et S-2 sont en panne, les clients reçoivent une réponse vide.

Pour configurer la sélection de service GSLB à l'aide de la commutation de contenu :

1. Configurez GSLB. Pour obtenir des instructions, voir Configuration de l'équilibrage de charge global du serveur.
2. Configurez un serveur virtuel CS (Content Switching) de type cible GSLB. Pour plus d'informations, voir Création de serveurs virtuels de commutation de contenu.
3. Configurer les stratégies CS (Content Switching). Pour plus d'informations, voir Configuration des stratégies de commutation de contenu.
4. Configurez les actions CS qui désignent un serveur virtuel GSLB comme serveur virtuel cible. Pour plus d'informations, voir Configuration d'une action de changement de contenu.
5. Liez les stratégies CS au serveur virtuel CS. Pour plus d'informations, voir Liaison de stratégies à un serveur virtuel de commutation de contenu.
6. Liez le domaine au serveur virtuel CS au lieu du serveur virtuel GSLB.

Exemple de configuration

L'exemple de configuration suivant envoie les demandes du client avec l'adresse IP 5.5.5.5 à SERVICE_GSLB1 et SERVICE_GSLB2. SERVICE_GSLB1 a une priorité plus élevée que SERVICE_GSLB2, et SERVICE_GSLB2 ne sert les demandes du client que lorsque SERVICE_GSLB1 est en panne. Si les deux

SERVICE_GSLB1 et SERVICE_GSLB2 sont en panne, SERVICE_GSLB3 et Service-GSLB4 ne sont pas pris en compte et une réponse vide est envoyée au client.

```
add cs vs CSVSERVER_GSLB http  -targettype GSLB
Done
add gslb vs VSERVER_GSLB1 http
Done
add gslb vs VSERVER_GSLB2 http
Done
add gslb vs VSERVER_GSLB_BACKUP1 http
Done
set gslb vs VSERVER_GSLB1 -backupvserver VSERVER_GSLB_BACKUP1
Done
add gslb service SERVICE_GSLB1 1.1.1.1 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB2 1.1.1.2 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB3 1.1.1.3 HTTP 80 -sitename site2
Done
add gslb service SERVICE_GSLB4 1.1.1.4 HTTP 80 -sitename site2
Done
bind gslb vs VSERVER_GSLB1 -servicename SERVICE_GSLB1
Done
bind gslb vs VSERVER_GSLB_BACKUP1 -servicename SERVICE_GSLB2
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB3
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB4
Done
add cs action a1 -targetvserver VSERVER_GSLB1
Done
add cs policy p1 -rule "CLIENT.IP.SRC.EQ(5.5.5.5)" -action a1
Done
bind cs vs CSVSERVER_GSLB -domainName www.abc.com
Done
bind cs vs CSVSERVER_GSLB -policyname p1 -priority 1
Done
add cs action a2 -targetvserver VSERVER_GSLB2
Done
add cs policy p2 -rule "CLIENT.IP.SRC.EQ(6.6.6.6)" -action a2
Done
bind cs vs CSVSERVER_GSLB -policyname p2 -priority 2
Done
<!--NeedCopy-->
```


Associer une expression de serveur virtuel cible à une action de commutation de contenu GSLB

Vous pouvez maintenant associer une expression de serveur virtuel cible à une action de commutation de contenu GSLB. Cela permet au serveur virtuel de commutation de contenu GSLB d'utiliser des expressions de stratégie pour composer le nom du serveur virtuel GSLB cible lors du traitement des demandes DNS.

Pour configurer une action de commutation de contenu qui spécifie une expression à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer l'action de commutation de contenu afin de récupérer la réponse de légende HTTP.

```
1 add cs action <name> -targetVserverExpr <expression>
2 <!--NeedCopy-->
```

Exemple :

```
1 add cs action csact_GSLB_VServer -targetVserverExpr "SYS.HTTP_CALLOUT(
     GSLB_Method_API)"
2 <!--NeedCopy-->
```

Pour configurer une action de commutation de contenu qui spécifie une expression à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Commutation de contenu > Actions**.
2. Configurez une action de commutation de contenu et spécifiez une **expression** qui calcule dynamiquement le nom du serveur virtuel d'équilibrage de charge cible.

Configurer GSLB pour les requêtes DNS avec des enregistrements NAPTR

May 5, 2023

Dans un déploiement GSLB (Global Server Load Balancing) classique, l'appliance NetScaler reçoit des requêtes DNS pour des enregistrements A/AAAA, sélectionne le service GSLB le plus approprié en fonction de la méthode d'équilibrage de charge configurée et renvoie l'adresse IP du service en réponse à la requête DNS. Vous pouvez désormais configurer l'appliance pour qu'elle reçoive des requêtes DNS

pour les enregistrements NAPTR et qu'elle y réponde avec la liste des services configurés pour un domaine. L'appliance surveille également l'état des services et, dans sa réponse, fournit une liste des seuls services actifs.

Exemple :

Dans les déploiements de télécommunications, vous pouvez configurer une appliance NetScaler pour recevoir des requêtes DNS avec des enregistrements NAPTR provenant de clients tels que des entités de gestion mobile (MME), qui jouent le rôle d'un résolveur DNS pour découvrir tous les services proposés par le nom de domaine. L'appliance répond à la requête avec des enregistrements NAPTR pour tous les services actifs. La MME peut utiliser cette réponse NAPTR pour exécuter la procédure S-NAPTR afin de sélectionner les nœuds sur la base du service offert, de la colocation, de la proximité topologique, etc.

Si plusieurs nœuds peuvent être sélectionnés, la MME peut utiliser le champ de préférence de l'enregistrement NAPTR de l'appliance NetScaler pour déterminer le nœud.

Format d'enregistrement NAPTR

Tout en répondant à une requête DNS avec un enregistrement NAPTR, une appliance NetScaler crée un enregistrement NAPTR de réponse pour chaque service GSLB.

Le tableau suivant répertorie les fichiers de l'enregistrement NAPTR :

Champ	
Domaine	Le domaine GSLB
TTL	Durée pendant laquelle l'enregistrement NAPTR peut être mis en cache.
Classe	La classe de l'enregistrement. Par défaut, cette valeur est définie sur IN.
Type	Type d'enregistrement DNS.
Order	Spécifie l'ordre dans lequel l'enregistrement NAPTR DOIT être traité. Vous pouvez spécifier la commande dans le service GSLB. Dans le cas contraire, il est défini sur 1.
Préférence	Spécifie l'ordre dans lequel les enregistrements NAPTR ayant des valeurs « d'ordre » égales DEVRAIENT être traités, les nombres faibles devant être traités avant les nombres élevés. Si l'ordre n'est pas spécifié dans le service GSLB, il est défini sur 1.

Champ	
Indicateurs	Contrôle les aspects de la réécriture et de l'interprétation des champs de l'enregistrement. L'appliance NetScaler définit cette valeur sur A.
Service	Spécifie le ou les services disponibles.
Expression régulière	Les expressions régulières ne sont pas prises en charge. Cette valeur est donc définie sur NULL.
Remplacement	Le nom de domaine du nœud qui héberge les services.

Procédure de configuration

Pour obtenir des instructions détaillées de configuration GSLB, reportez-vous à la section Configuration de l'équilibrage de charge globale du serveur (GSLB). Assurez-vous d'effectuer les opérations suivantes :

- Définissez les paramètres suivants lors de l'ajout du serveur virtuel GSLB :
  - Type de service : N'IMPORTE LEQUEL
  - Type d'enregistrement DNS : NAPTR
  - Méthode LB : CHARGEMENT PERSONNALISÉ

Exemple :

```
1 add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD
2 <!--NeedCopy-->
```

- Lors de l'ajout d'un site GSLB, définissez le paramètre *NAPTRReplacementSuffix* sur le nom de domaine que vous souhaitez intégrer dans les enregistrements NAPTR.

Exemple :

```
1 add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com
2 <!--NeedCopy-->
```

- Définissez les paramètres suivants lors de l'ajout du service GSLB :
  - remplacement du naptr
  - Ordre NAPT
  - Services NAPTR
  - TTL du domaine NAPTR

- Préférence NAPTR

Exemple de configuration

```
add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD

Done

add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com

Done

add gslb service sgw1 3.3.3.13 ANY *  -siteName site1 -naptrreplacement
    sgw1.site1. -naptrOrder 2 -naptrServices x-3gpp-sgw:x-s5-gtp -
   naptrDomainTTL 20 -naptrPreference   200

Done

add gslb service sgw2 3.3.3.11 ANY *  -siteName site1 -naptrreplacement
    sgw2.site1. -naptrOrder 5 -naptrServices x-3gpp-sgw:x-s5-gtp  -
   naptrDomainTTL 20  naptrPreference  100

Done

add gslb service sgw3 3.3.3.12 ANY *  -siteName site2 -naptrreplacement
    sgw3.site1. -naptrOrder 10 -naptrServices x-3gpp-sgw:x-s5-gtp  -
   naptrDomainTTL 20 naptrPreference   300

bind gslb vserver gslb_vs -serviceName sgw1

Done

bind gslb vserver gslb_vs -serviceName sgw2

Done

bind gslb vserver gslb_vs -serviceName sgw3

Done

bind gslb service sgw1 -monitorName ping

Done

```



```
bind gslb service sgw2 -monitorName ping

Done

bind gslb service sgw3 -monitorName ping

Done

bind gslb vserver gslb_vs -domainName gslb.com -TTL 5

Done
<!--NeedCopy-->
```

> **Remarque**
>
> Les requêtes DNS avec enregistrements NAPTR ne sont pas prises en charge dans la configuration parent-enfant.

Configurer GSLB pour le domaine générique

July 12, 2022

Vous pouvez lier un domaine DNS générique à un serveur virtuel GSLB. Les utilisateurs qui accèdent aux applications derrière un domaine générique sont acheminés vers le meilleur centre de données optimal, qui héberge ces applications. Le domaine générique gère les demandes de domaines et de sous-domaines inexistants. Pour plus d'informations sur les domaines génériques, voir Prise en charge des domaines DNS génériques. Pour plus d'informations sur les zones DNS, consultez la section Configurer une zone DNS.

Pour configurer GSLB pour un domaine générique, vous devez d'abord configurer la configuration GSLB de base. Pour plus d'informations sur la configuration d'une configuration GSLB de base, reportez-vous à la section Configuration des entités GSLB individuellement.

Pour configurer une configuration GSLB pour le domaine générique à l'aide de l'interface de ligne de commande

Effectuez les étapes suivantes pour configurer une configuration GSLB pour un domaine générique :

1. Créez les sites GSLB.

```
add gslb site site1 10.0.1.10
add gslb site site2 20.0.1.10
<!--NeedCopy-->
```


2. Ajoutez les services GSLB pour chaque site participant à la configuration du GSLB.

```
add gslb service svc1 -sitename site1 10.0.1.10  http 80
add gslb service svc2 -sitename site1 10.0.1.10  http 80
add gslb service svc3 -sitename site2 20.0.1.10  http 80
add gslb service svc4 -sitename site2 20.0.1.10  http 80
<!--NeedCopy-->
```

3. Ajoutez le serveur virtuel GSLB qui fait référence à un service utilisé dans la configuration du GSLB.

```
add gslb vserver gslb_vs http
<!--NeedCopy-->
```

4. Ajoutez un service ADNS qui écoute les requêtes DNS.

```
add service adns_udp 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

5. Liez les services GSLB au serveur virtuel GSLB.

```
bind gslb vserver gslb_vs -service svc1
bind gslb vserver gslb_vs -service svc2
bind gslb vserver gslb_vs -service svc3
bind gslb vserver gslb_vs -service svc4
<!--NeedCopy-->
```

6. Créez une zone.

```
add dns soaRec test.com -originServer n1.test.com -contact n1.test
    .com
add dns nsrec test.com n1.test.com
add dns nsrec test.com n2.test.com
add dns zone test.com -proxymode no
<!--NeedCopy-->
```

7. Liez le nom de domaine au serveur virtuel GSLB.

```
bind gslb vserver gslb_vs -domainName *.test.com
<!--NeedCopy-->
```


Utilisez l'option de sous-réseau client EDNS0 pour l'équilibrage global de la charge du serveur

May 5, 2023

Le sous-réseau client EDNS (ECS) est une extension d'en-tête du serveur de noms de domaine (DNS) qui fournit les détails du sous-réseau client. Vous pouvez utiliser ces informations pour améliorer la précision de NetScaler Global Server Load Balancing (GSLB) en utilisant l'emplacement réseau du client plutôt que l'emplacement du résolveur DNS pour déterminer la proximité topologique du client.

> **Remarque**
>
> NetScaler prend uniquement en charge EDNS0.

Important :

> Assurez-vous que le serveur de noms de domaine local (LDNS) de votre déploiement prend en charge le sous-réseau client EDNS0 afin que les requêtes DNS entrantes contiennent l'option de sous-réseau client EDNS0 et que l'appliance NetScaler utilise l'adresse ECS lors du traitement de la requête DNS.

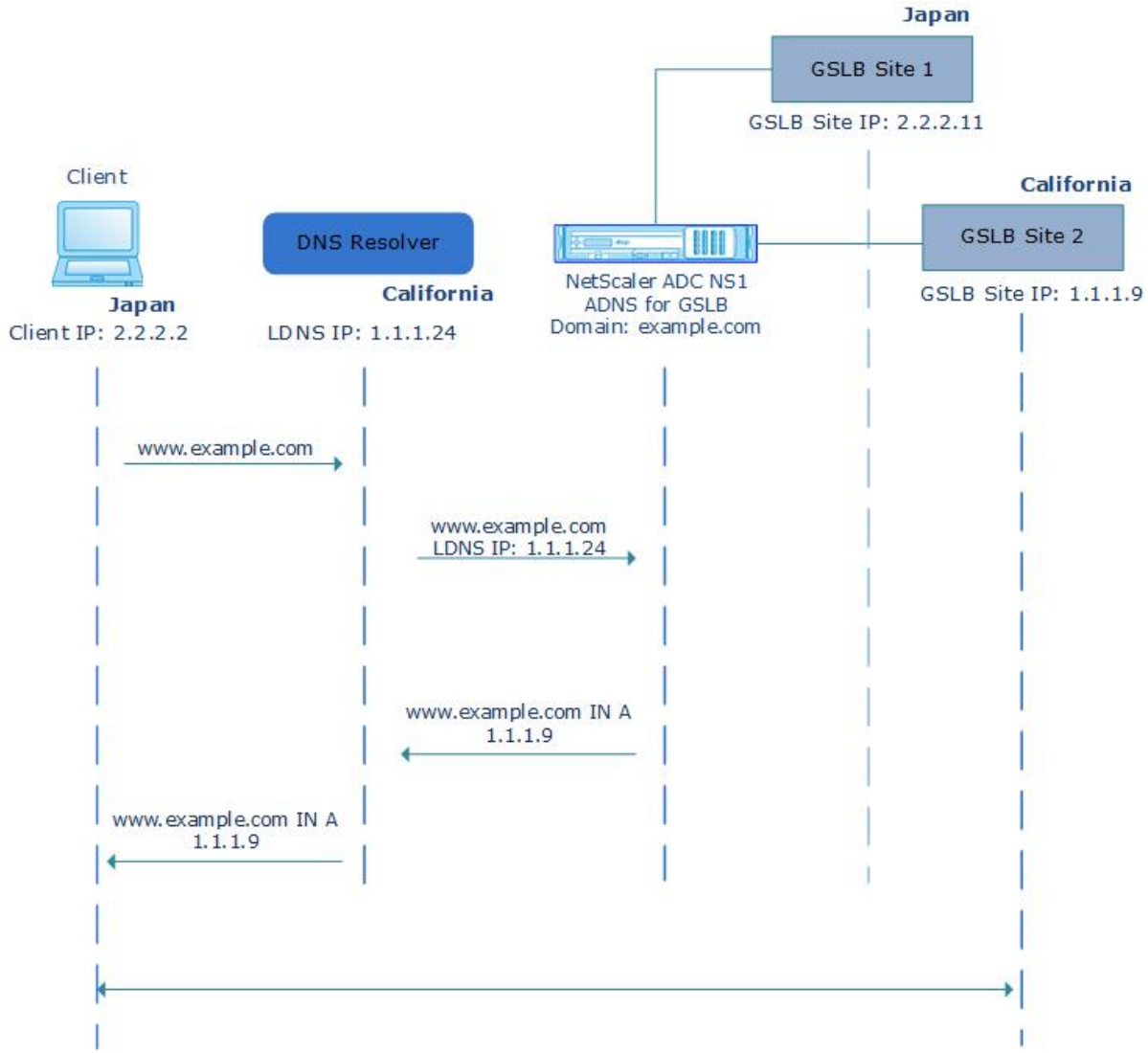
L'appliance NetScaler utilise l'adresse IP LDNS pour déterminer la proximité topologique du client et exécute le GSLB, donc lorsque vous utilisez des méthodes d'équilibrage de charge basées sur la proximité, telles que la proximité statique ou le temps aller-retour dynamique (RTT). Cela se produit dans le cadre d'un déploiement GSLB classique. Mais lorsqu'un résolveur DNS centralisé, tel que Google DNS ou OpenDNS, est impliqué dans le déploiement, l'appliance NetScaler envoie la demande DNS à un centre de données proche du résolveur DNS centralisé, qui n'est peut-être pas proche du client. Par exemple, dans un déploiement NetScaler GSLB classique utilisant la méthode d'équilibrage de charge de proximité statique, une demande d'utilisateur final en provenance du Japon est envoyée à un centre de données au Japon et une demande d'utilisateur final en provenance de Californie est envoyée à un centre de données en Californie. Mais si un résolveur DNS centralisé est impliqué, l'appliance NetScaler peut envoyer une demande depuis le Japon vers un centre de données en Californie.

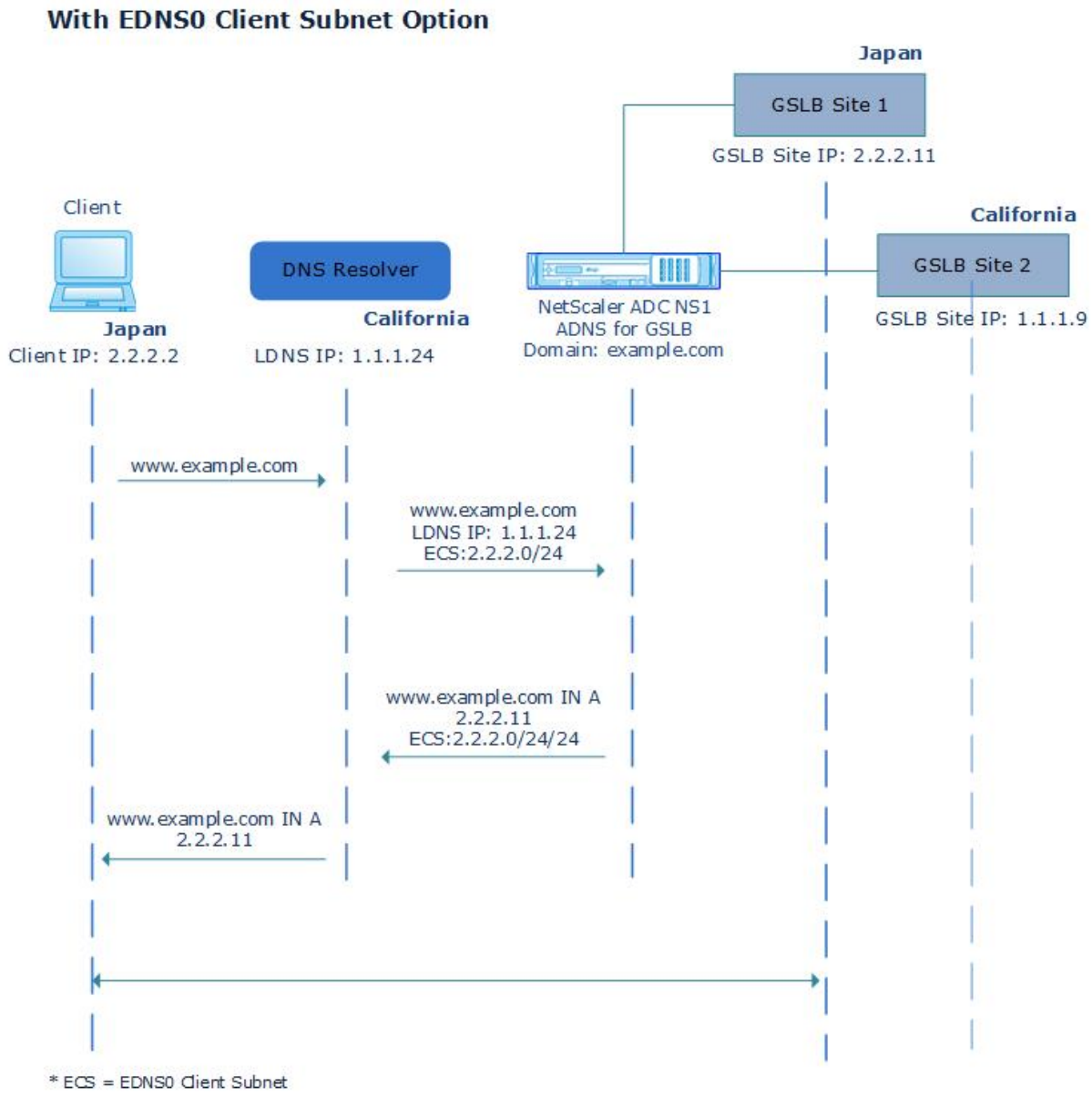
Vous pouvez utiliser l'option ECS dans les déploiements qui incluent l'appliance NetScaler configurée en tant que serveur DNS officiel (ADNS) pour un domaine GSLB. Si vous utilisez la proximité statique comme méthode d'équilibrage de charge, vous pouvez utiliser le sous-réseau IP dans l'en-tête EDNS au lieu de l'adresse IP LDNS. Cela permet de déterminer la proximité géographique du client. Lors du déploiement en mode proxy, l'appliance NetScaler transmet telle quelle une requête DNS compatible ECS aux serveurs principaux. L'appliance ne met pas en cache les réponses DNS compatibles ECS.

> **Remarque**
>
> L'option ECS ne s'applique pas à tous les autres modes de déploiement, tels que le mode ADNS

pour les domaines non GSLB, le mode résolveur et le mode redirecteur. L'option ECS est ignorée par l'appliance NetScaler dans les modes mentionnés ci-dessus. De plus, par défaut, ECS est désactivé pour le déploiement du GSLB.

Without EDNS0 Client Subnet Option





Pour activer l'option de sous-réseau client EDNS0 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
set gslb vserver <vserver_name> **-ECS ENABLED

set gslb vserver vserver-GSLB-1 -ECS ENABLED
<!--NeedCopy-->
```


Validation d’adresse

Vous pouvez configurer un serveur virtuel GSLB pour vérifier que l’adresse renvoyée par l’option EDNS0 Client Subnet (ECS) de la requête DNS n’est pas une adresse IP privée ou non routable. Lorsque la validation d’adresse est activée, l’appliance NetScaler ignore l’adresse ECS dans la requête DNS si elle est répertoriée dans le tableau suivant et utilise à la place l’adresse IP LDNS pour l’équilibrage de charge global du serveur.

> **Remarque**
>
> Par défaut, la validation des adresses est désactivée.

Type d’adresse	Adresse	Description
IPV4	10,0.0.0/8	Pour un usage privé
	172.16.0.0/12	Pour un usage privé
	192.168.0.0/16	Pour un usage privé
	0,0,0,0/8	Fait référence à l’hôte sur le réseau
	100,64,0,0/10	Espace d’adressage partagé
	127,0.0.0/8	Adresse de bouclage
	169,254,0,0/16	Adresse IPv4 locale du lien telle que définie dans la RFC 3927
	192.0.0.0/24	Utilisé pour les attributions de protocoles IETF, inclut l’espace privé 192.168.0.0/16
	192.0.2.0/24	Utilisé à des fins de documentation
	192.88.99.0/24	Utilisé pour 6to4 Relay Anycast
	198.18,0,0/15	Utilisé dans les tests de performance des appareils
	198.51.100,0/24	Utilisé à des fins de documentation
	203,0.113,0/24	Utilisé à des fins de documentation
	240,0.0.0/4	Utilisé comme réservé

Type d'adresse	Adresse	Description
	255.255.255.255/32	Utilisé pour la diffusion
IPv6	::1/128	adresse de bouclage
	::/128	adresse non spécifiée
	::ffff:0:0/96	Adresse mappée IPv4
	100::/64	bloc d'adresses à supprimer uniquement
	2001::/23	Utilisé pour les attributions de protocoles IETF
	2001::/32	TEREDO
	2001:2::/48	Utilisé pour l'analyse comparative
	2001:db8::/32	Utilisé à des fins de documentation
	2001:10::/28	ORCHIDÉE
	2002::/16	Utilisé pour 6to4 Relay Anycast
	fc00::/7	Unique-local
	fe80::/10	Adresses Unicast locales du lien

Pour activer la validation des adresses à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

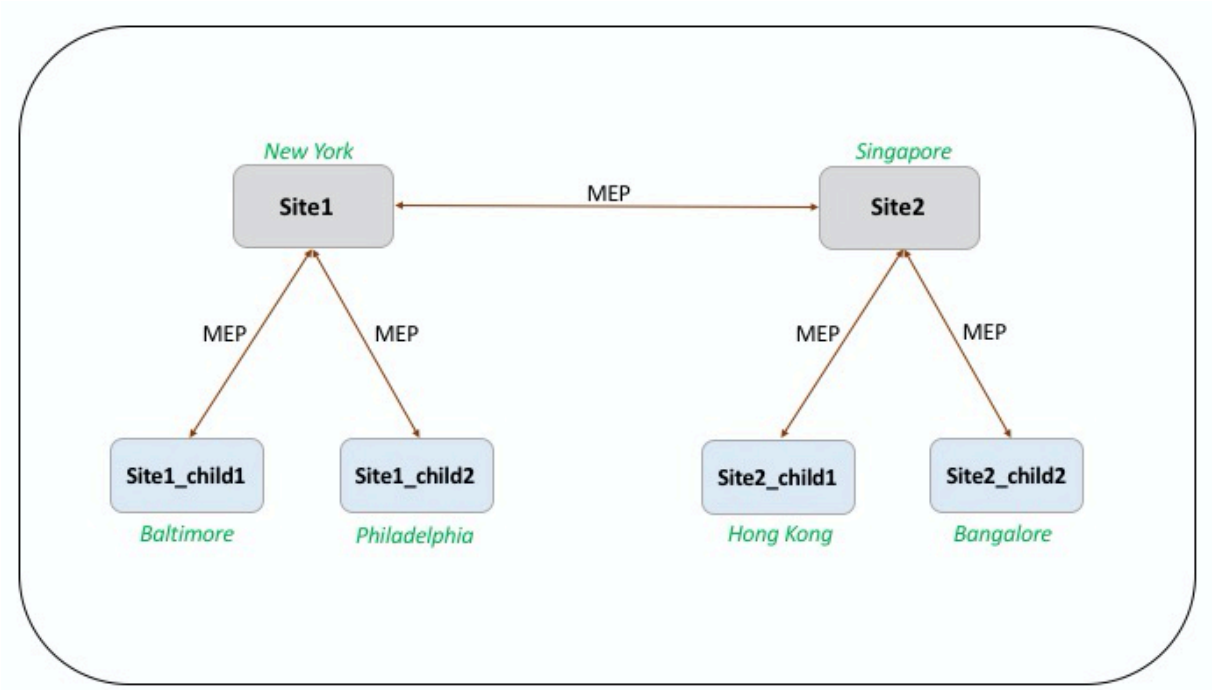
```
set gslb vserver <vserver_name> -ecsAddrValidation ENABLED

set gslb vserver vserver-GSLB-1 -ecsAddrValidation ENABLED
<!--NeedCopy-->
```


Exemple de configuration parent-enfant complète à l'aide du protocole d'échange de mesures

August 20, 2021

Considérons la topologie parent-enfant suivante dans laquelle les sites GSLB sont distribués globalement.

- Site1 et Site2 sont les sites parents.
- Site1_child1 et Site1_child2 sont les sites enfants de Site1.
- Site2_child1 et Site2_child2 sont les sites enfants de Site2.



Les commandes suivantes illustrent la configuration complète de la topologie parent-enfant.

site1

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site2 10.106.24.164 -publicIP 10.106.24.164

add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

```



```
7  add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site1
8
9  add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
10
11 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
12
13 add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
       publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
       site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
14
15 add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
        10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
16
17 add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
       publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
       site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
18
19 add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
        10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
20
21 add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
       appflowLog DISABLED
22
23 bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1
24
25 bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1
26
27 bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1
28
29 bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1
30
31 bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
32 <!--NeedCopy-->
```

site1_child1


```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1
<!--NeedCopy-->
```

Vous pouvez ajouter les commandes suivantes pour la configuration de l'équilibrage de charge :

```
add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.132 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```

site1_child2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

You can add the following commands for load balancing configuration:

add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.68 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```

site2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164
```



```
2
3  add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
4
5  add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site1
6
7  add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site1
8
9  add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
10
11 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
12
13 add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
       publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
       site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
14
15 add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
        10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
16
17 add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
       publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
       site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
18
19 add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
        10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
20
21 add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
       appflowLog DISABLED
22
23 bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1
24
25 bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1
26
27 bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1
28
29 bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1
```



```
30
31 bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
32 <!--NeedCopy-->
```

site2_child1

```
1 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
2
3 add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
     nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
     site2
4 <!--NeedCopy-->
```

You can add the following commands for load balancing configuration:

```
1 add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
      -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
     svrTimeout 360 -CKA NO -TCPB NO -CMP NO
2
3 add lb vserver lb1 HTTP 10.106.24.134 80 -persistenceType NONE -
     cltTimeout 180
4
5 bind lb vserver lb1 svc1
6 <!--NeedCopy-->
```

site2_child2

```
1 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
2
3 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
     nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
     site2
4 <!--NeedCopy-->
```

You can add the following commands for load balancing configuration:

```
1 add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
      -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
     svrTimeout 360 -CKA NO -TCPB NO -CMP NO
2
3 add lb vserver lb1 HTTP 10.106.24.68 80 -persistenceType NONE -
     cltTimeout 180
```



```
4
5 bind lb vserver lb1 svc1
6 \`\`\`
7 <!--NeedCopy-->
```

Équilibrage de charge de liaison

May 5, 2023

L'équilibrage de charge des liens (LLB) équilibre le trafic sortant entre plusieurs connexions Internet fournies par différents fournisseurs de services. LLB permet à l'appliance NetScaler de surveiller et de contrôler le trafic afin que les paquets soient transmis de manière fluide via la meilleure liaison possible. Contrairement à l'équilibrage de charge des serveurs, où un service représente un serveur, avec LLB, un service représente un routeur ou le saut suivant. Un lien est une connexion entre l'appliance NetScaler et le routeur.

Pour configurer l'équilibrage de charge des liens, de nombreux utilisateurs commencent par configurer une configuration de base avec les paramètres par défaut. Une configuration de base implique des services, des serveurs virtuels, des moniteurs, des itinéraires, une méthode LLB et la persistance (facultatif). Une fois qu'une configuration de base est opérationnelle, vous pouvez la personnaliser en fonction de votre environnement.

Les méthodes d'équilibrage de charge applicables à LLB sont les suivantes : le round robin, le hachage IP de destination, le minimum de bande passante et le minimum de paquets. Vous pouvez éventuellement configurer la persistance pour que les connexions soient maintenues sur un lien spécifique. Les types de persistance disponibles sont basés sur l'adresse IP source, basés sur l'adresse IP de destination et basés sur l'IP source et l'adresse IP de destination. PING est le moniteur par défaut, mais il est recommandé de configurer un moniteur transparent.

Vous pouvez personnaliser votre configuration en configurant le NAT inversé (RNAT) et des liens de sauvegarde.

Configuration d'une configuration LLB de base

May 5, 2023

Pour configurer LLB, vous devez d'abord créer des services représentant chaque routeur auprès des fournisseurs de services Internet (ISP). Un moniteur PING est lié par défaut à chaque service. La fixation d'un moniteur transparent est facultative mais recommandée. Ensuite, vous créez un serveur

virtuel, vous liez les services au serveur virtuel et vous configurez un itinéraire pour le serveur virtuel. L'itinéraire identifie le serveur virtuel en tant que passerelle vers les routeurs physiques représentés par les services. Le serveur virtuel sélectionne un routeur à l'aide de la méthode d'équilibrage de charge que vous avez spécifiée. Vous pouvez éventuellement configurer la persistance pour vous assurer que tout le trafic d'une session particulière est envoyé via un lien spécifique.

Pour configurer une configuration LLB de base, procédez comme suit :

- Configurer les services
- Configurer un serveur virtuel LLB et lier un service
- Configuration de la méthode LLB et de la persistance
- Configuration d'un itinéraire LLB
- Création et liaison d'un moniteur transparent

Configurer les services

Un moniteur par défaut (PING) est automatiquement lié à un type de service ANY lors de la création du service, mais vous pouvez remplacer le moniteur par défaut par un moniteur transparent, comme décrit dans Création et liaison d'un moniteur transparent.

Pour créer un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <name> <IP> <serviceType> <port>

show service <name>
<!--NeedCopy-->
```

Exemple :

```
add service ISP1R_svc_any 10.10.10.254 any *
show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: DOWN
        Last state change was at Tue Aug 31 04:31:13 2010
        Time since last state change: 2 days, 05:34:18.600
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
```



```
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 244705  Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

Pour créer des services à l'aide de l'utilitaire de configuration

Accédez à Gestion du trafic > Équilibrage de charge > Services, puis créez un service.

Pour créer des services à l'aide de l'utilitaire de configuration

1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer un service, spécifiez les valeurs des paramètres suivants :
   - Nom du service*—Nom
   - Serveur—IP
   - Protocol* : type de service (sélectionnez N'IMPORTE QUEL dans la liste déroulante.)
   - Port*—port

Un paramètre obligatoire

1. Cliquez sur Create.
2. Répétez les étapes 2 à 4 pour créer un autre service.
3. Cliquez sur Fermer.
4. Dans le volet Services, sélectionnez les services que vous venez de configurer et vérifiez que les paramètres affichés en bas de l'écran sont corrects.

Configurer un serveur virtuel LLB et lier un service

Après avoir créé un service, créez un serveur virtuel et liez les services au serveur virtuel. La méthode LB par défaut des connexions minimales n'est pas prise en charge dans LLB. Pour plus d'informations sur la modification de la méthode LB, voir Configuration de la méthode LLB et de la persistance.

Pour créer un serveur virtuel d'équilibrage de charge de liaison et lier un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> <serviceType>

bind lb vserver < name> <serviceName>

show lb vserver < name>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver LLB-vip any
bind lb vserver LLB-vip ISP1R_svc_any
sh lb vserver LLB-vip
        LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Thu Sep  2 10:51:32 2010
        Time since last state change: 0 days, 17:51:46.770
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
        Mode: IP
        Persistence: NONE
        Connection Failover: DISABLED

1) ISP1R_svc_any (10.10.10.254: *) - ANY State: DOWN    Weight: 1
 Done
<!--NeedCopy-->
```


Pour créer un serveur virtuel d'équilibrage de charge de liens et lier un service à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis créez un serveur virtuel pour l'équilibrage de charge des liens. Spécifiez **ANY** dans le champ **Protocole** .
2. Dans la liste déroulante **Type d'adresse IP**, sélectionnez l'option souhaitée. Sélectionnez **Non adressable** pour créer un serveur virtuel qui n'est pas directement accessible.
3. Sous l'onglet **Services**, dans la colonne **Actif**, cochez la case correspondant au service que vous souhaitez lier au serveur virtuel.

Configuration de la méthode LLB et de la persistance

Par défaut, l'appliance NetScaler utilise la méthode du moins de connexions pour sélectionner le service pour rediriger chaque demande client, mais vous devez définir la méthode LLB sur l'une des méthodes prises en charge. Vous pouvez également configurer la persistance afin que différentes transmissions provenant du même client soient dirigées vers le même serveur.

Pour configurer la méthode LLB et/ou la persistance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set lb vserver <name> -lbMethod <lbMethod> -persistenceType <
   persistenceType>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver LLB-vip -lbmethod ROUNDROBIN -persistencetype SOURCEIP

show lb vserver LLB-vip
        LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 00:52:21.200
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
```



```
14          Mode: IP
15          Persistence: SOURCEIP
16       Persistence Mask: 255.255.255.255       Persistence v6MaskLength:
            128   Persistence Timeout: 2 min
17          Connection Failover: DISABLED
18 <!--NeedCopy-->
```

Pour configurer la méthode d'équilibrage de charge des liens et/ou la persistance à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels et sélectionnez le serveur virtuel pour lequel vous souhaitez configurer la méthode d'équilibrage de charge et/ou les paramètres de persistance.
2. Dans la section **Paramètres avancés**, sélectionnez Méthode et configurez la méthode d'équilibrage de charge.
3. Dans la section **Paramètres avancés**, sélectionnez **Persistance** et configurez les paramètres de persistance.

Configuration d'un itinéraire LLB

Après avoir configuré les services IPv4 ou IPv6, les serveurs virtuels, les méthodes LLB et la persistance, vous configurez un itinéraire LLB IPv4 ou IPv6 pour le réseau en spécifiant le serveur virtuel LLB comme passerelle. Un itinéraire est un ensemble de liens dont la charge est équilibrée. Les demandes sont envoyées à l'adresse IP du serveur virtuel LLB qui fait office de passerelle pour tout le trafic sortant et sélectionne le routeur en fonction de la méthode LLB configurée.

Pour configurer une route LLB IPv4 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add lb route <network> <netmask> <gatewayName>
2
3 show lb route [<network> <netmask>]
4 <!--NeedCopy-->
```

Exemple :

```
1 add lb route 0.0.0.0 0.0.0.0 LLB-vip
2 show lb route 0.0.0.0 0.0.0.0
3        Network          Netmask        Gateway/VIP              Flags
4      -----------      -------------   ---------------          --------
5 1)     0.0.0.0          0.0.0.0        LLB-vip                UP
```



```
<!--NeedCopy-->
```

Pour configurer un itinéraire LLB IPv6 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb route6 <network> <gatewayName>

show lb route6
<!--NeedCopy-->
```

Exemple :

```
add lb route6 ::/0 llb6_vs show lb route6 Network VIP Flags -----------
    --------- -------- 1) ::/0 llb6_vs UP
<!--NeedCopy-->
```

Pour configurer un itinéraire LLB à l'aide de l'utilitaire de configuration

Accédez à Système > Réseau > Routes, sélectionnez **LLB**et configurez l'itinéraire LLB.

Remarque : Sélectionnez LLBV6 pour configurer un itinéraire IPV6.

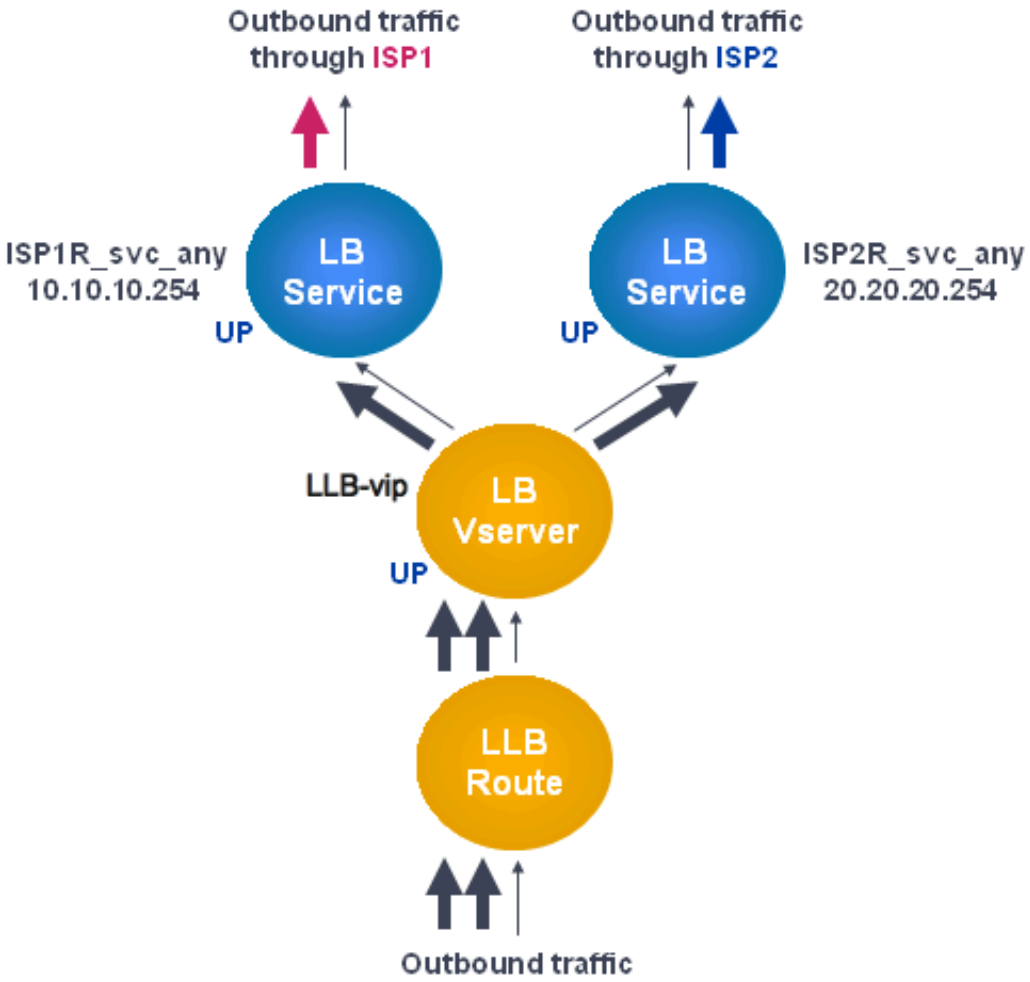
Pour configurer un itinéraire LLB à l'aide de l'utilitaire de configuration

1. Accédez à Système > Réseau > Routes.
2. Dans le volet de détails, sélectionnez l'une des options suivantes :
   - Cliquez sur LLB pour configurer un itinéraire IPv4.
   - Cliquez sur LLBV6 pour configurer un itinéraire IPv4.
3. Dans la boîte de dialogue Créer une route LB ou Créer une route IPV6 LB, définissez les paramètres suivants :
   - Réseau*
   - Masque de réseau* : obligatoire pour les routes IPV4.
   - Nom de passerelle* : nom de passerelle

     *Paramètre obligatoire
4. Cliquez sur Créer, puis sur Fermer. L'itinéraire que vous venez de créer apparaît dans l'onglet LLB ou LLB6 du volet Itinéraires.

Le schéma suivant montre une configuration LLB de base. Un service est configuré pour chacune des deux liaisons (ISP) et les moniteurs PING sont liés par défaut à ces services. Un lien est sélectionné en fonction de la méthode LLB configurée.

Figure 1. Configuration de base de LLB



> **Remarque**
>
> Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure ci-dessus.

Création et liaison d'un moniteur transparent

Vous créez un moniteur transparent pour surveiller l'état des appareils en amont, tels que les routeurs. Vous pouvez ensuite lier le moniteur transparent aux services. Le moniteur PING par défaut surveille la connectivité uniquement entre l'appliance NetScaler et le périphérique en amont. Le moniteur transparent surveille tous les périphériques existant dans le chemin allant de l'appliance au périphérique

qui possède l'adresse IP de destination spécifiée dans le moniteur. Si aucun moniteur transparent n'est configuré et que l'état du routeur est activé mais que l'un des périphériques de saut suivant ce routeur est hors service, l'appliance inclut le routeur lors de l'équilibrage de charge et transmet le paquet au routeur. Cependant, le paquet n'est pas livré à la destination finale car l'un des périphériques de saut suivant est en panne. En liant un moniteur transparent, si l'un des périphériques (y compris le routeur) est en panne, le service est marqué comme étant hors service et le routeur n'est pas inclus lorsque l'appliance effectue un équilibrage de charge des liaisons.

Pour créer un moniteur transparent à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb monitor <monitorName> <type> -destIP <ip_addr|*> -transparent
   YES

show lb monitor [<monitorName>]
<!--NeedCopy-->
```

Exemple :

```
add lb monitor monitor-1 PING -destIP 10.10.10.11 -transparent YES
> show lb monitor monitor-1
1)   Name.......: monitor-1  Type......:      PING   State....:
   ENABLED
Standard parameters:
  Interval.........:            5 sec   Retries...........:
                    3
  Response timeout.:            2 sec   Down time.........:
      30 sec
  Reverse..........:              NO   Transparent.......:
                  YES
  Secure...........:              NO   LRTM..............:
      ENABLED
  Action...........:   Not applicable   Deviation.........:
      0 sec
  Destination IP...:      10.10.10.11
  Destination port.:    Bound service
  Iptunnel.........:              NO
  TOS..............:              NO   TOS ID............:
                    0
  SNMP Alert Retries:               0     Success Retries..:
                    1
  Failure Retries..:                0
<!--NeedCopy-->
```


Pour créer un moniteur transparent à l'aide de l'utilitaire de configuration

Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs et configurez un moniteur transparent.

Pour créer un moniteur transparent à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs.
2. Dans le volet Moniteurs, cliquez sur Ajouter.
3. Dans la boîte de dialogue Create Monitor, définissez les paramètres suivants :
   - Nom*
   - Type*
   - IP destination
   - Transparent

   *Paramètre obligatoire
4. Cliquez sur Créer, puis sur Fermer.
5. Dans le volet Moniteurs, sélectionnez le moniteur que vous venez de configurer et vérifiez que les paramètres affichés dans le volet Détails sont corrects.

Pour lier un moniteur à un service à l'aide de l'utilitaire de configuration

1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans l'onglet **Moniteurs**, sous **Disponible**, sélectionnez le moniteur que vous souhaitez lier au service, puis cliquez sur **Ajouter**.

Pour lier un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb monitor <monitorName> <serviceName>

show service <name>
<!--NeedCopy-->
```

Exemple :

```
bind lb monitor monitor-HTTP-1 ISP1R_svc_any
 Done
> show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
```



```
        State: UP
        Last state change was at Thu Sep  2 10:51:07 2010
        Time since last state change: 0 days, 18:41:55.130
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: UP  Weight: 1
                Probes: 1256       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

Pour lier un moniteur à un service à l'aide de l'utilitaire de configuration

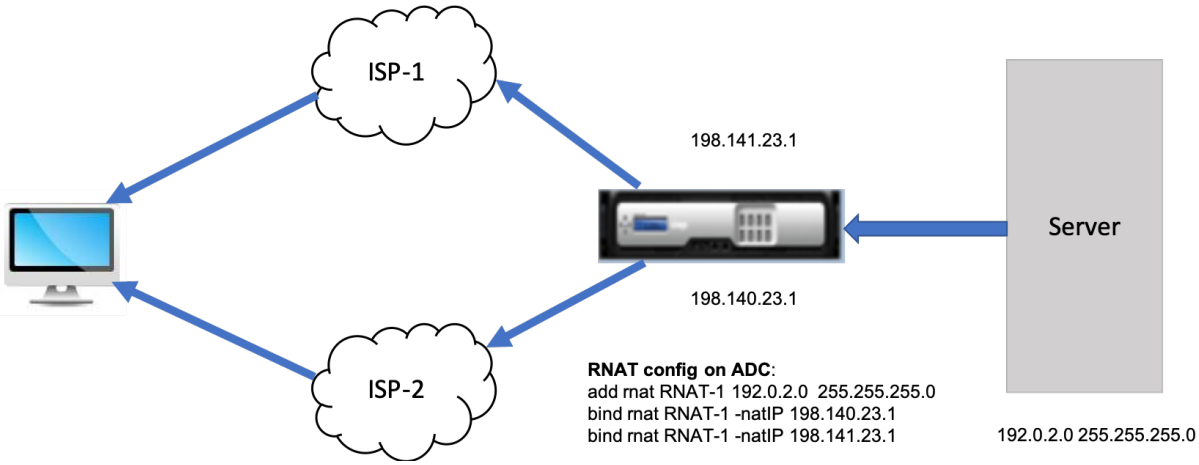
1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans le volet de détails, sélectionnez le service auquel vous souhaitez lier un moniteur, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le service, sous l'onglet Moniteurs, sous Disponible, sélectionnez le moniteur que vous souhaitez lier au service, puis cliquez sur Ajouter.
4. Cliquez sur OK.
5. Dans le volet Services, sélectionnez le service que vous venez de configurer et vérifiez que les paramètres affichés dans le volet Détails sont corrects.

Configurer RNAT avec LLB

May 5, 2023

Vous pouvez configurer une configuration LLB pour la traduction inverse des adresses réseau (RNAT) pour le trafic sortant. Il garantit que le trafic réseau de retour pour un flux spécifique est acheminé via le même chemin. Configurez d'abord la LLB de base, comme décrit dans Configuration d'un programme d'installation LLB de base, puis configurez RNAT comme décrit dans Configurer RNAT. Activez ensuite le mode « utiliser le sous-réseau IP (USNIP) ».

Dans le schéma suivant, l'appliance NetScaler utilise LLB pour acheminer le trafic sortant vers différents liens. Pendant l'opération RNAT, l'appliance ADC remplace les adresses IP sources du trafic sortant par l'adresse IP NAT publique (198.141.23.1) pour acheminer le trafic via ISP-1. De même, l'appliance ADC remplace les adresses IP sources par 198.140.23.1 pour acheminer le trafic via ISP-2.



Pour ajouter des SNIP aux routeurs ISP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add NS IP <subnet of first ISP in the IP router> <subnet mask> -type
    SNIP

add NS IP <subnet of second ISP in the IP router> <subnet mask> -type
    SNIP
<!--NeedCopy-->
```

Exemple :

```
add ns ip 198.140.23.1 255.255.255.0 -type snip

add ns ip 198.141.23.1 255.255.255.0 -type snip
<!--NeedCopy-->
```


Pour configurer RNAT à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ …

show rnat <name>
<!--NeedCopy-->
```

Exemple :

```
add rnat RNAT-1 192.0.2.0 255.255.255.0
bind rnat RNAT-1 -natIP 198.140.23.1
bind rnat RNAT-1 -natIP 198.141.23.1

> show rnat RNAT-1
    1) RNAT Name: RNAT-1     Network: 192.0.2.0      Netmask:
       255.255.255.0     Traffic Domain: 0
        UseProxyPort: ENABLED

        NatIP: 198.140.23.1
        NatIP: 198.141.23.1
<!--NeedCopy-->
```

Pour configurer RNAT à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **NATS.**
2. Dans l'onglet **RNAT**, cliquez sur **Configurer RNAT**.
3. Spécifiez le réseau sur lequel effectuer le RNAT.

> **Remarque**
>
> Vous pouvez également configurer RNAT à l'aide des listes de contrôle d'accès (ACL). Pour plus de détails, reportez-vous à Configuration de RNAT .

Pour activer l'utilisation du mode IP de sous-réseau à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
enable ns mode USNIP

```



```
show ns mode
<!--NeedCopy-->
```

Exemple :

```
enable ns mode USNIP

show ns mode
        Mode                            Acronym             Status
        -------                         -------             ------
 1)     Fast Ramp                       FR                  ON
 2)     ….
 8)     Use Subnet IP                   USNIP               ON
 9)     …
<!--NeedCopy-->
```

Pour activer le mode Utiliser l'adresse IP du sous-réseau à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres** et, sous **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.
2. Dans la boîte de dialogue **Configurer les modes**, sélectionnez **Utiliser l'adresse IP du sous-réseau**, puis cliquez sur **OK.**

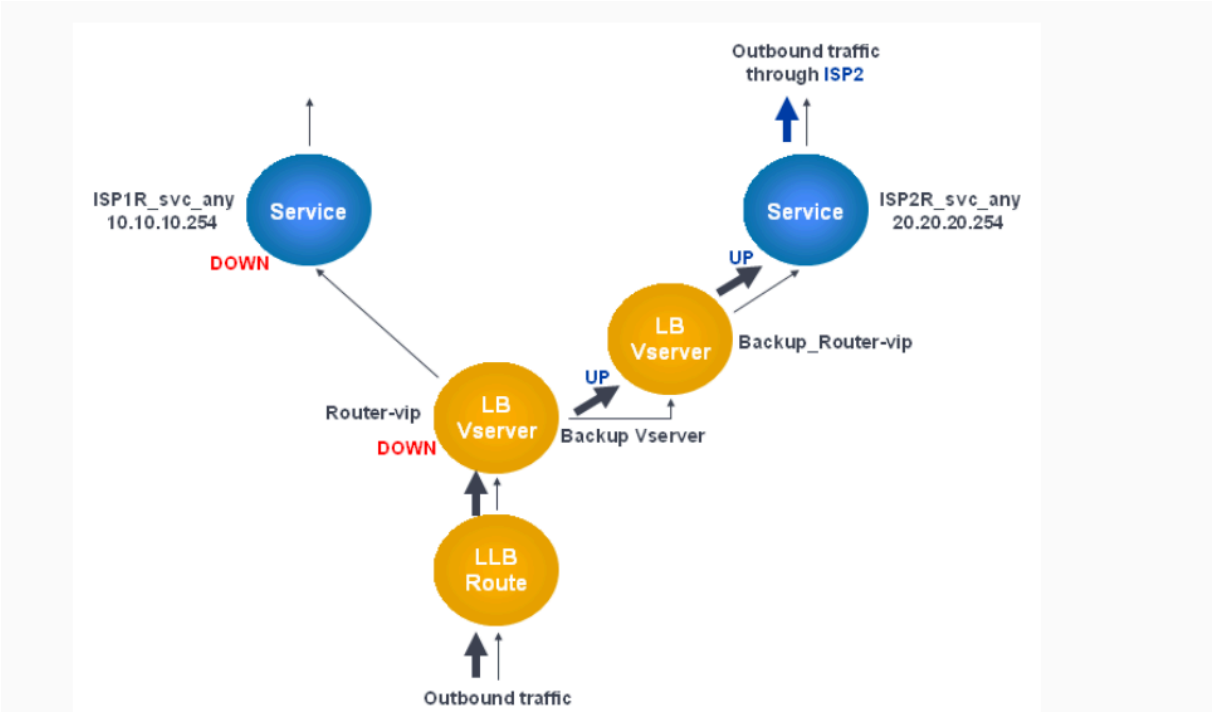
Configuration d'un itinéraire de sauvegarde

May 5, 2023

Pour éviter toute interruption des services lorsque l'itinéraire principal est en panne, vous pouvez configurer un itinéraire de secours. Une fois la route de sauvegarde configurée, l'appliance NetScaler l'utilise automatiquement lorsque la route principale échoue. Commencez par créer un serveur virtuel principal, comme décrit dans Configuration d'un serveur virtuel LLB et liaison d'un service. Pour configurer une route de sauvegarde, créez un serveur virtuel secondaire similaire à un serveur virtuel principal, puis définissez ce serveur virtuel comme serveur virtuel de sauvegarde (route).

Dans le schéma suivant, **Router-VIP** est le serveur virtuel principal et **Backup_Router-VIP** est le serveur virtuel secondaire désigné comme serveur virtuel de sauvegarde.

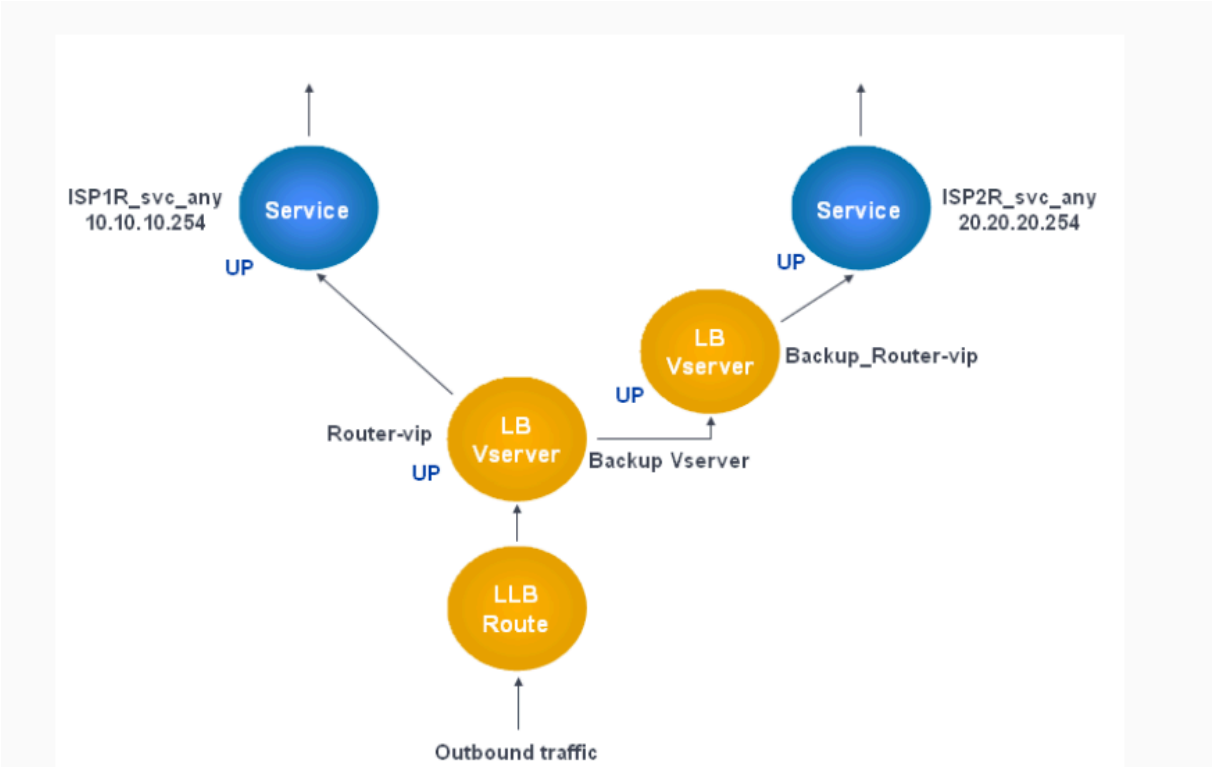
Figure 1. Configuration de l'itinéraire de sauvegarde



Remarque : Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure précédente.

Par défaut, tout le trafic est envoyé via l'itinéraire principal. Toutefois, en cas de défaillance de l'itinéraire principal, tout le trafic est redirigé vers l'itinéraire de secours, comme le montre le schéma suivant.

Figure 2. Routage de secours en cours de fonctionnement



Remarque : Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure précédente.

Pour définir le serveur virtuel secondaire comme serveur virtuel de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -backupVserver <string>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Router-vip -backupVServer Backup_Router-vip
> show lb vserver Router-vip
        Router-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 03:09:45.600
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       1 (Active)
```



```
12          Configured Method: ROUNDROBIN
13          Mode: IP
14          Persistence: DESTIP     Persistence Mask: 255.255.255.255
                      Persistence v6MaskLength: 128   Persistence Timeout: 2
                min
15          Backup: Router2-vip
16          Connection Failover: DISABLED
17   Done
18  <!--NeedCopy-->
```

Pour définir le serveur virtuel secondaire comme serveur virtuel de sauvegarde à l'aide de l'utilitaire de configuration

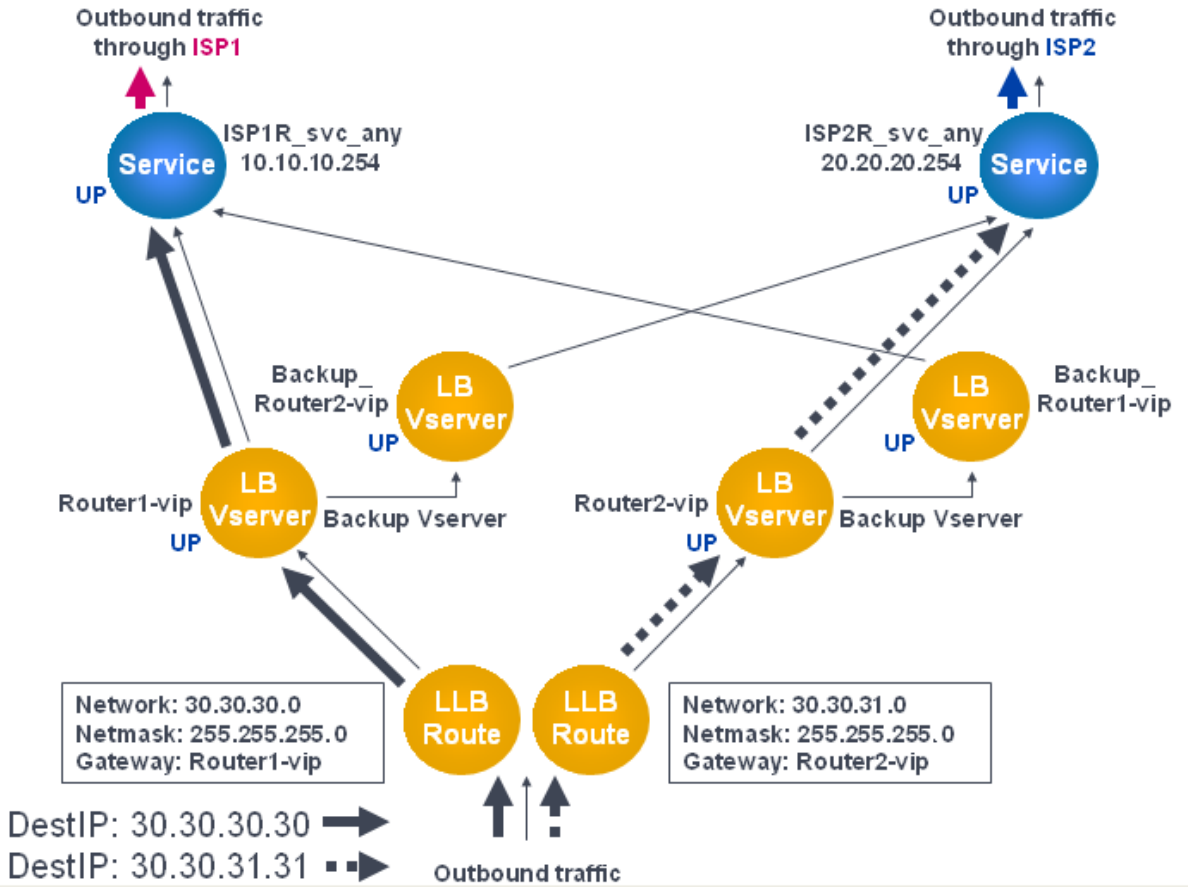
1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et sélectionnez le serveur virtuel secondaire pour lequel vous souhaitez configurer le serveur virtuel de sauvegarde.
2. Dans la boîte de dialogue **du serveur virtuel d'équilibrage** de charge, sous **Avancé**, sélectionnez **Protection**.
3. Dans la liste déroulante **Serveur virtuel de sauvegarde**, sélectionnez le serveur virtuel de sauvegarde secondaire, puis cliquez sur **OK**.

Scénario de déploiement de LLB résilient

January 21, 2021

Dans le diagramme suivant, il y a deux réseaux : 30.30.30.0 et 30.30.31.0. L'équilibrage de charge de liaison est configuré en fonction de l'adresse IP de destination. Deux itinéraires sont configurés avec les passerelles **Router1-VIP** et **Router2-VIP**, respectivement. **Router1-VIP** est configuré comme une sauvegarde sur **Router2-VIP** et de la manière opposée. Tout le trafic avec l'adresse IP de destination spécifiée comme 30.30.30.30 est envoyé via **Router1-VIP** et le trafic avec l'adresse IP de destination spécifiée comme 30.30.31.31 est envoyé via **Router2-VIP** .

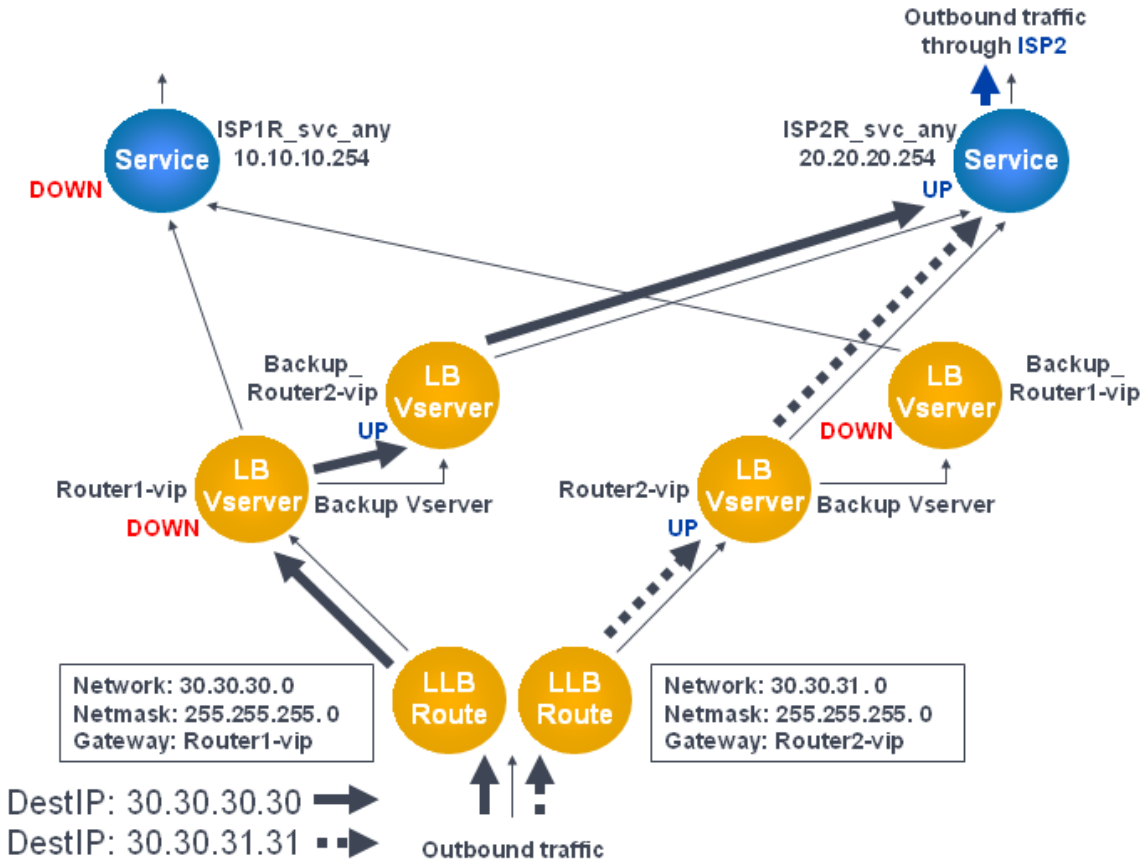
Figure 1. Configuration du déploiement LLB résilient



Remarque : Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure précédente.

Toutefois, si l'une des passerelles (**Router1-VIP** ou **Router2-VIP**) est DOWN, le trafic est acheminé via le routeur de sauvegarde. Dans le diagramme suivant, **Router1-VIP** pour ISP1 est DOWN, donc tout le trafic avec l'adresse IP de destination spécifiée comme 30.30.30.30 est également envoyé via ISP2.

Figure 2. Scénario de déploiement LLB résilient



Remarque : Si votre fournisseur de services Internet a fourni une adresse IPv6, remplacez le service IPv4 par un service IPv6 dans la figure précédente.

Surveiller une configuration LLB

May 5, 2023

Une fois la configuration opérationnelle, vous pouvez consulter les statistiques de chaque service et serveur virtuel afin de détecter d'éventuels problèmes.

Afficher les statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre des problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance NetScaler. Vous pouvez afficher un résumé des statistiques pour tous les serveurs virtuels. Vous pouvez également spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les informations suivantes :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel
- Taux de demandes reçues
- Rate of hits

Afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques pour tous les serveurs virtuels actuellement configurés sur NetScaler, ou pour un seul serveur virtuel, à l'invite de commande, tapez :

```
stat lb vserver -detail] [<name>]
<!--NeedCopy-->
```

Exemple :

```
stat lb vserver -detail
Virtual Server(s) Summary
                       vsvrIP  port     Protocol        State    Req/s
                            Hits/s
One                         *    80         HTTP           UP      5/s
        0/s
Two                         *     0          TCP         DOWN      0/s
        0/s
Three                       *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done
<!--NeedCopy-->
```

Afficher les statistiques du serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels > Statistiques**.
2. Si vous souhaitez afficher les statistiques d'un seul serveur virtuel, dans le volet de détails, sélectionnez le serveur virtuel, puis cliquez sur Statistiques.

Afficher les statistiques d'un service

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions au serveur en cours, etc. à l'aide des statistiques de service.

Afficher les statistiques d'un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat service <name>
<!--NeedCopy-->
```

Exemple :

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Afficher les statistiques d'un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services > Statistiques**.
2. Si vous souhaitez afficher les statistiques d'un seul service, sélectionnez-le et cliquez sur Statistiques.

Équilibrage de charge

May 5, 2023

La fonction d'équilibrage de charge distribue les demandes des utilisateurs pour des pages Web et autres applications protégées sur plusieurs serveurs hébergeant (ou miroir) le même contenu. Vous utilisez l'équilibrage de charge principalement pour gérer les demandes des utilisateurs vers des applications fortement utilisées, évitant les mauvaises performances et les pannes et vous assurant que les utilisateurs peuvent accéder à vos applications protégées. L'équilibrage de charge offre également une tolérance aux pannes. Lorsqu'un serveur hébergeant une application protégée devient indisponible, la fonctionnalité distribue les demandes des utilisateurs aux autres serveurs hébergeant la même application.

Vous pouvez configurer la fonction d'équilibrage de charge pour :

- Distribuez toutes les demandes pour un site Web, une application ou une ressource protégé spécifique entre deux ou plusieurs serveurs configurés de manière identique.

- Utilisez l'un de plusieurs algorithmes différents pour déterminer quel serveur doit recevoir chaque demande d'utilisateur entrante, en basant la décision sur différents facteurs, tels que le serveur qui possède le moins de connexions utilisateur actuelles ou quel serveur a la charge la plus faible.

La fonction d'équilibrage de charge est une fonctionnalité essentielle de l'appliance NetScaler. La plupart des utilisateurs mettent d'abord en place une configuration de base fonctionnelle, puis personnalisent divers paramètres, notamment la persistance des connexions. En outre, vous pouvez configurer des fonctionnalités pour protéger la configuration contre les pannes, gérer le trafic client, gérer et surveiller les serveurs et gérer un déploiement à grande échelle.

Fonctionnement de l'équilibrage de charge

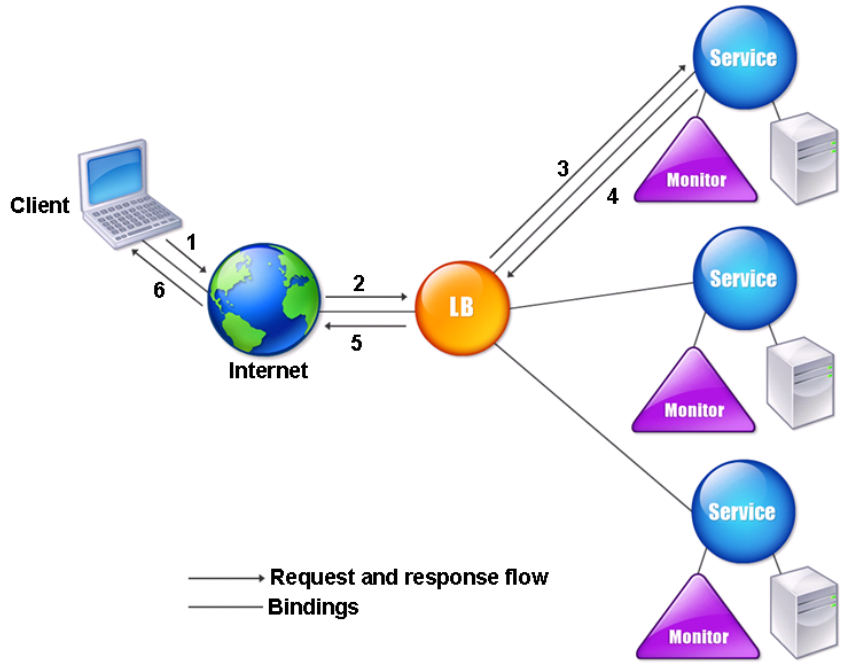
May 5, 2023

Dans une configuration d'équilibrage de charge de base, les clients envoient leurs demandes à l'adresse IP d'un serveur virtuel configuré sur l'appliance NetScaler. Le serveur virtuel les distribue aux serveurs d'applications à équilibrage de charge selon un modèle prédéfini, appelé algorithme d'équilibrage de charge. Il peut arriver que vous souhaitiez attribuer au serveur virtuel d'équilibrage de charge une adresse générique au lieu d'une adresse IP spécifique. Pour obtenir des instructions sur la spécification d'un port HTTP global sur l'appliance, consultez **Ports HTTP globaux**.

Les bases de l'équilibrage de charge

Une configuration d'équilibrage de charge comprend un serveur virtuel d'équilibrage de charge et plusieurs serveurs d'applications d'équilibrage de charge. Le serveur virtuel reçoit les demandes des clients entrants, utilise l'algorithme d'équilibrage de charge pour sélectionner un serveur d'applications et transmet les demandes au serveur d'applications sélectionné. Le dessin conceptuel suivant illustre un déploiement d'équilibrage de charge typique. Une autre variante consiste à attribuer un port HTTP global.

Figure 1. Architecture d'équilibrage de charge



Le serveur virtuel d'équilibrage de charge peut utiliser plusieurs algorithmes (ou méthodes) pour déterminer comment répartir la charge entre les serveurs à charge équilibrée qu'il gère. La méthode d'équilibrage de charge par défaut est la méthode de moindre connexion, dans laquelle l'appliance NetScaler transmet chaque connexion client entrante au serveur d'applications à équilibrage de charge qui possède actuellement le moins de connexions utilisateur actives.

Les entités que vous configurez dans une configuration d'équilibrage de charge NetScaler classique sont les suivantes :

- **Serveur virtuel d'équilibrage de charge.** La combinaison d'adresse IP, de port et de protocole à laquelle un client envoie des demandes de connexion pour un site Web ou une application à charge équilibrée en particulier. Si l'application est accessible à partir d'Internet, l'adresse IP du serveur virtuel (VIP) est une adresse IP publique. Si l'application est accessible uniquement à partir du réseau local ou du WAN, le VIP est généralement une adresse IP privée (non routable de l'ICANN).
- **Service.** La combinaison d'adresse IP, de port et de protocole utilisée pour acheminer les demandes vers un serveur d'applications à charge équilibrée spécifique. Un service peut être une représentation logique du serveur d'applications lui-même ou d'une application exécutée sur un serveur hébergeant plusieurs applications. Après avoir créé un service, vous le liez à un serveur virtuel d'équilibrage de charge.

- **Objet serveur.** Entité virtuelle qui vous permet d'attribuer un nom à un serveur physique au lieu de l'identifier par son adresse IP. Si vous créez un objet serveur, vous pouvez spécifier son nom au lieu de l'adresse IP du serveur lorsque vous créez un service. Sinon, vous devez spécifier l'adresse IP du serveur lorsque vous créez un service, et l'adresse IP devient le nom du serveur.
- **Moniteur.** Entité de l'appliance NetScaler qui assure le suivi d'un service et s'assure qu'il fonctionne correctement. Le moniteur sonde régulièrement (ou effectue un bilan de santé) de chaque service auquel vous l'attribuez. Si le service ne répond pas dans le délai spécifié par le délai d'expiration et qu'un certain nombre de contrôles de santé échouent, ce service est marqué comme étant inactif. L'appliance NetScaler ignore ensuite ce service lors de l'équilibrage de charge, jusqu'à ce que les problèmes à l'origine de l'arrêt de réponse du service soient résolus.

Le serveur virtuel, les services et les serveurs d'applications à charge équilibrée d'une configuration d'équilibrage de charge peuvent utiliser des adresses IP IPv4 (Internet Protocol version 4) ou IPv6 (Internet Protocol version 6). Vous pouvez combiner des adresses IPv4 et IPv6 dans une seule configuration d'équilibrage de charge.

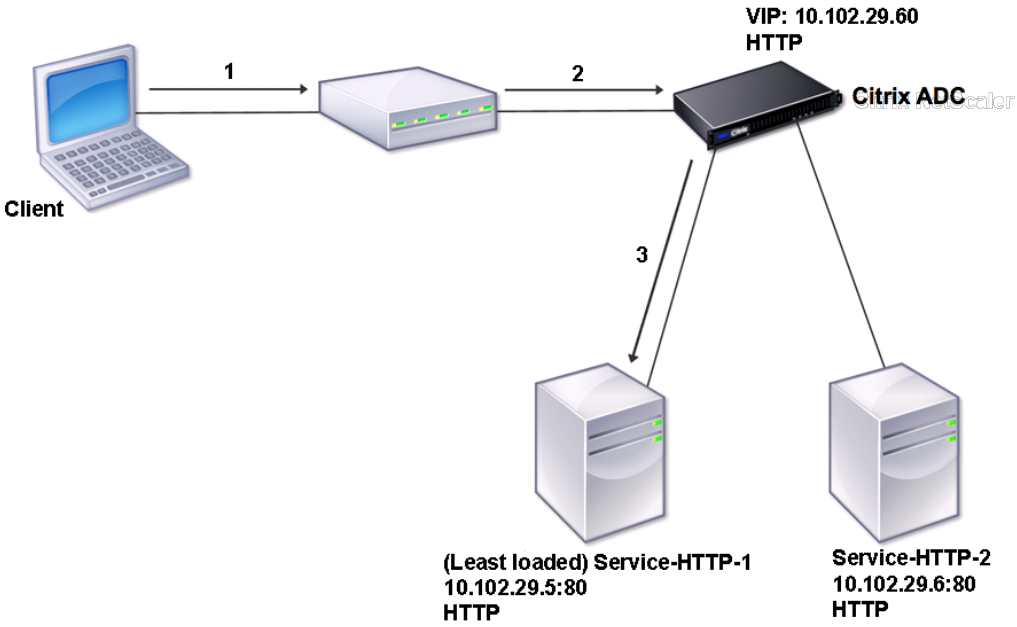
Pour connaître les variations de configuration de l'équilibrage de charge, consultez les cas d'utilisation suivants :

- Configuration de l'équilibrage de charge en mode Direct Server Return
- Configuration de serveurs LINUX en mode DSR
- Configuration du mode DSR lors de l'utilisation de TOS
- Configuration de l'équilibrage de charge en mode DSR à l'aide d'IP over IP
- Configuration de l'équilibrage de charge en mode One-Arm
- Configuration de l'équilibrage de charge en mode intégré
- Équilibrage de charge des serveurs du système de détection des intrusions
- Équilibrer la charge des serveurs de protocole Bureau à distance

Comprendre la topologie

Dans une configuration d'équilibrage de charge, le serveur d'équilibrage de charge est logiquement situé entre le client et la batterie de serveurs et gère le flux de trafic vers les serveurs de la batterie de serveurs. Sur l'appliance NetScaler, les serveurs d'applications sont représentés par des entités virtuelles appelées services. Le schéma suivant montre la topologie d'une configuration d'équilibrage de charge de base.

Figure 2. Topologie d'équilibrage de charge de base

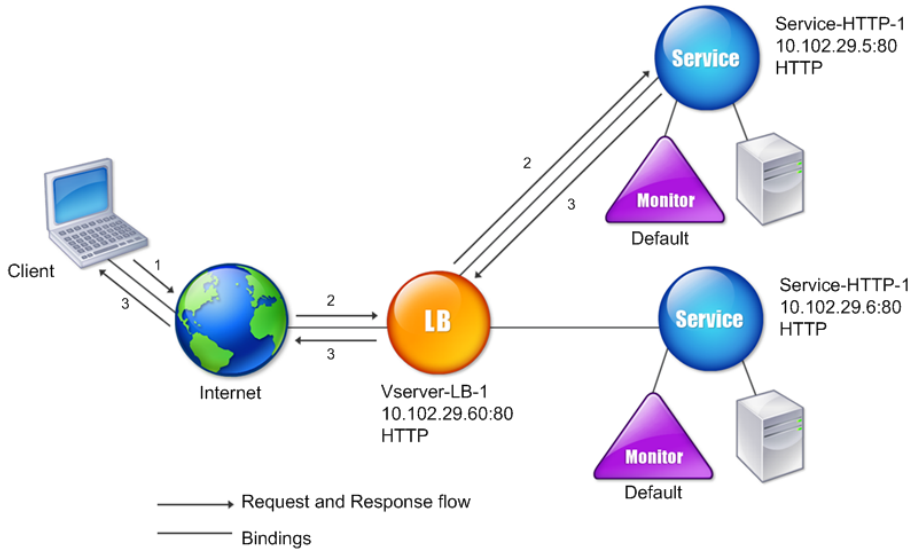


Dans le diagramme, l'équilibrage de charge est utilisé pour gérer le flux de trafic vers les serveurs. Le serveur virtuel sélectionne le service et l'attribue pour répondre aux demandes des clients. Imaginons un scénario dans lequel les services Service-HTTP-1 et Service-HTTP-2 sont créés et liés au serveur virtuel nommé vServer-LB-1. vServer-LB-1 transmet la demande du client à Service-HTTP-1 ou Service-HTTP-2. L'appliance NetScaler utilise la méthode d'équilibrage de charge de moindre connexion pour sélectionner le service pour chaque demande. Le tableau suivant répertorie les noms et les valeurs des entités de base qui doivent être configurées sur l'appliance.

Entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.60	80	HTTP
Services	Service-HTTP-1	10.102.29,5	80	HTTP
	Service-HTTP-2	10.102.29.6	80	HTTP
Moniteurs	Valeur par défaut	Aucun	Aucun	Aucun

Le diagramme suivant montre les valeurs d'échantillon d'équilibrage de charge et les paramètres obligatoires décrits dans le tableau précédent.

Figure 3. Modèle d'entité d'équilibrage de charge



Utilisation de caractères génériques au lieu d'adresses IP et de ports

Il peut arriver que vous deviez utiliser un caractère générique pour l'adresse IP ou le port d'un serveur virtuel ou pour le port d'un service. Les cas suivants peuvent nécessiter l'utilisation d'un caractère générique :

- Si l'appliance NetScaler est configurée en tant que passerelle transparente, elle doit accepter tout le trafic qui lui est envoyé, quel que soit l'adresse IP ou le port vers lequel il est envoyé.
- Si un ou plusieurs services écoutent sur des ports peu connus.
- Si un ou plusieurs services modifient au fil du temps les ports sur lesquels ils écoutent.
- Si vous atteignez la limite du nombre d'adresses IP et de ports que vous pouvez configurer sur une seule appliance NetScaler.
- Si vous souhaitez créer des serveurs virtuels qui écoutent tout le trafic sur un réseau local virtuel spécifique.

Lorsqu'un serveur ou un service virtuel configuré par caractères génériques reçoit du trafic, l'appliance NetScaler détermine l'adresse IP ou le port réel et crée des enregistrements pour le service et le serveur d'applications à équilibrage de charge associé. Ces enregistrements créés

dynamiquement sont appelés enregistrements de serveur et de service appris dynamiquement.

Par exemple, une configuration d'équilibrage de charge de pare-feu peut utiliser des caractères génériques à la fois pour l'adresse IP et pour le port. Si vous liez un service TCP générique à ce type de serveur virtuel d'équilibrage de charge, le serveur virtuel reçoit et traite tout le trafic TCP qui ne correspond à aucun autre service ou serveur virtuel.

Le tableau suivant décrit certains des différents types de configurations génériques et le moment où chacune doit être utilisée.

IP	Port	Protocole	Description
*	*	TCP	Un serveur virtuel générique qui accepte le trafic envoyé vers n'importe quelle adresse IP et n'importe quel port de l'appliance NetScaler. Lors de l'utilisation d'un serveur virtuel générique, l'appliance apprend dynamiquement l'adresse IP et le port de chaque service et crée les enregistrements nécessaires au cours du traitement du trafic.

IP	Port	Protocole	Description
*	*	TCP	Un serveur virtuel d'équilibrage de charge de pare-feu. Vous pouvez lier des services de pare-feu à ce serveur virtuel et l'appliance NetScaler fait passer le trafic à travers le pare-feu jusqu'à la destination.
Adresse IP	*	TCP, UDP et ANY	Serveur virtuel qui accepte tout le trafic envoyé à l'adresse IP spécifiée, quel que soit le port. Vous devez lier explicitement à ce type de serveur virtuel les services vers lesquels il redirigera le trafic. Il ne les apprend pas dynamiquement.

IP	Port	Protocole	Description
			Remarque : vous ne configurez pas de services ou de serveurs virtuels pour un port HTTP global. Dans ce cas, vous configurez un port spécifique en tant que port HTTP global (par exemple, définissez ns param -HttpPort 80). L'appliance accepte ensuite tout le trafic correspondant au numéro de port et le traite comme du trafic HTTP. L'appliance apprend et crée des services de manière dynamique pour ce trafic.

IP	Port	Protocole	Description
*	port	SSL, SSL_TCP	Serveur virtuel qui accepte tout le trafic envoyé vers n'importe quelle adresse IP sur un port spécifique. Utilisé pour le déchargement SSL transparent global. Tout le traitement SSL, HTTP et TCP qui est généralement effectué pour un service du même type de protocole est appliqué au trafic qui est dirigé vers ce port spécifique. L'appliance utilise le port pour connaître dynamiquement l'adresse IP du service qu'elle doit utiliser. Si —cleartext n'est pas spécifié, l'appliance NetScaler utilise le protocole SSL de bout en bout.

IP	Port	Protocole	Description
*	port	Non applicable	Tous les autres serveurs virtuels pouvant accepter le trafic vers le port. Vous ne liez pas de services à ces serveurs virtuels. L'appliance NetScaler les apprend de manière dynamique.

Remarque : Si vous avez configuré votre appliance NetScaler en tant que passerelle transparente utilisant des ports globaux (caractères génériques), vous pouvez activer le mode Edge.
Pour plus d'informations, reportez-vous à lasection « Configuration du mode Edge ». «

L'appliance NetScaler tente de localiser des serveurs et des services virtuels en tentant d'abord de trouver une correspondance exacte. Si aucune correspondance n'est trouvée, il continue à rechercher une correspondance à l'aide de caractères génériques, dans l'ordre suivant :

1. Adresse IP et numéro de port spécifiques
2. Adresse IP spécifique et port * (caractère générique)
3. • Adresse IP (caractère générique) et port spécifique
4. • (caractère générique) adresse IP et un port * (caractère générique)

Si l'appliance ne peut pas sélectionner un serveur virtuel par adresse IP ou numéro de port, elle recherche un serveur virtuel basé sur le protocole utilisé dans la demande, dans l'ordre suivant :

1. HTTP
2. TCP
3. ANY

Configuration des ports HTTP globaux

Vous ne configurez pas de services ou de serveurs virtuels pour un port HTTP global. Au lieu de cela, vous configurez un port spécifique à l'aide de la commande set ns param. Après avoir configuré ce port, l'appliance NetScaler accepte tout le trafic correspondant au numéro de port et le traite comme du trafic HTTP, en apprenant de manière dynamique et en créant des services pour ce trafic.

Vous pouvez configurer plusieurs numéros de port en tant que port HTTP global. Si vous spécifiez plusieurs numéros de port dans une seule commande set ns param, séparez les numéros de port par

un seul espace blanc. Si un ou plusieurs ports ont déjà été spécifiés comme ports HTTP globaux et que vous souhaitez ajouter un ou plusieurs ports sans supprimer les ports actuellement configurés, vous devez spécifier tous les numéros de port, actuels et nouveaux, dans la commande. Avant d'ajouter des numéros de port, utilisez la commande show ns param pour afficher les ports actuellement configurés.

Pour configurer un port HTTP global à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un port HTTP global et vérifier la configuration :

```
set ns param  -httpPort <port>

show ns param
<!--NeedCopy-->
```

Exemple 1 : Configuration d'un port en tant que port HTTP global

Dans cet exemple, le port 80 est configuré en tant que port HTTP global.

```
set ns param -httpPort 80
Done
show ns param
         Global configuration settings:
                           HTTP port(s): 80
                       Max connections: 0
            Max requests per connection: 0
                    Client IP insertion: DISABLED
                         Cookie version: 0
         Persistence Cookie Secure Flag: ENABLED
         ...
         ...
<!--NeedCopy-->
```

Exemple 2 : Ajouter des ports lorsqu'un ou plusieurs ports HTTP globaux sont déjà configurés**

Dans cet exemple, le port 8888 est ajouté à la liste globale des ports HTTP. Le port 80 est déjà configuré en tant que port HTTP global.

```
> show ns param
         Global configuration settings:
```



```
                            HTTP port(s): 80
                         Max connections: 0
               Max requests per connection: 0
                       Client IP insertion: DISABLED
                            Cookie version: 0
           Persistence Cookie Secure Flag: ENABLED
                            Min Path MTU: 576
           ...
           ...
 Done
> set ns param -httpPort 80 8888
 Done
>  show ns param

           Global configuration settings:
                            HTTP port(s): 80,8888
                         Max connections: 0
               Max requests per connection: 0
                       Client IP insertion: DISABLED
                            Cookie version: 0
           Persistence Cookie Secure Flag: ENABLED
                            Min Path MTU: 576

           ...
           ...
 Done
>
<!--NeedCopy-->
```

Pour configurer un port HTTP global à l'aide de l'utilitaire de configuration

1. Accédez à **Système > Paramètres > Modifier les paramètres HTTP**, puis ajoutez un numéro de port HTTP.

Configurer l'équilibrage de charge de base

May 5, 2023

Avant de configurer votre configuration initiale d'équilibrage de charge, activez la fonction d'équilibrage de charge. Commencez ensuite par créer au moins un service pour chaque serveur du groupe d'équilibrage de charge. Une fois les services configurés, vous êtes prêt à créer un

serveur virtuel d'équilibrage de charge et à lier chaque service au serveur virtuel. Cela termine la configuration initiale. Avant de poursuivre la configuration, vérifiez votre configuration pour vous assurer que chaque élément a été correctement configuré et fonctionne comme prévu.

Activation de l'équilibrage de charge

Vous pouvez configurer des entités d'équilibrage de charge telles que des services et des serveurs virtuels lorsque la fonction d'équilibrage de charge est désactivée, mais elles ne fonctionneront pas tant que vous n'aurez pas activé la fonctionnalité.

Pour activer l'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez la commande suivante pour activer l'équilibrage de charge et vérifier la configuration :

- enable ns feature LB
- show ns feature

Exemple

```
> enable ns feature LoadBalancing

 Done

> show ns feature


        Feature                         Acronym             Status

        -------                         -------             ------

 1)     Web Logging                     WL                  OFF

 2)     Surge Protection                SP                  ON

 3) Load Balancing LB ON

 .

 .

 .
```



```
24
25      24)    NetScaler Push                  push                  OFF
26
27      Done
28 <!--NeedCopy-->
```

Pour activer l'équilibrage de charge à l'aide de l'interface graphique

Accédez à **Système** > **Paramètres** et, dans **Configurer les fonctionnalités de base**, sélectionnez **Équilibrage de charge**.

Configuration d'un objet serveur

Créez une entrée pour votre serveur sur l'appliance NetScaler. L'appliance NetScaler prend en charge les serveurs basés sur des adresses IP et les serveurs basés sur des domaines. Si vous créez un serveur basé sur l'adresse IP, vous pouvez spécifier le nom du serveur au lieu de son adresse IP lorsque vous créez un service. Pour plus d'informations sur la configuration du DNS pour un serveur basé sur un domaine, voir Système de noms de domaine.

Pour créer un objet serveur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add server `<name>`@ `<IPAddress>`@ | `<domain>`
2 <!--NeedCopy-->
```

Exemple d'ajout d'un serveur de noms basé sur l'adresse IP :

```
1 add server web_serv 10.102.27.150
2 <!--NeedCopy-->
```

Exemple d'ajout d'un serveur basé sur un domaine :

```
1 add server web_serv test.com
2 <!--NeedCopy-->
```

Pour créer un objet serveur à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs**, puis ajoutez un objet serveur.

Configuration des services

Après avoir activé la fonctionnalité d'équilibrage de charge, vous devez créer au moins un service pour chaque serveur d'applications à inclure dans votre configuration d'équilibrage de charge. Les services que vous configurez fournissent les connexions entre l'appliance NetScaler et les serveurs d'équilibrage de charge. Chaque service possède un nom et spécifie une adresse IP, un port et le type de données qui est servi.

Si vous créez un service sans créer au préalable un objet serveur, l'adresse IP du service est également le nom du serveur qui héberge le service. Si vous préférez identifier les serveurs par leur nom plutôt que par leur adresse IP, vous pouvez créer des objets serveur, puis spécifier le nom d'un serveur plutôt que son adresse IP lorsque vous créez un service.

Lorsque vous créez un service qui utilise UDP comme protocole de couche transport, un moniteur de ping est automatiquement lié au service. Un moniteur ping est le moniteur intégré le plus élémentaire. Lorsque vous créez un service qui utilise TCP comme protocole de couche transport, un moniteur TCP_Default est automatiquement lié au service. Lorsque vous développez une stratégie pour gérer votre configuration d'équilibrage de charge, vous pouvez décider de lier un autre type de moniteur, ou plusieurs moniteurs, au service.

Création d'un service

Avant de créer un service, vous devez comprendre les différents types de services et la façon dont chacun est utilisé. La liste suivante décrit les types de services pris en charge sur l'appliance NetScaler.

HTTP

Utilisé pour les serveurs à charge équilibrée qui acceptent le trafic HTTP, tels que les sites Web et les applications Web standard. Le type de service HTTP permet à l'appliance NetScaler de fournir des services de compression, de filtrage de contenu, de mise en cache et de prise en charge du maintien en activité des clients pour vos serveurs Web de couche 7. Ce type de service prend également en charge l'insertion de ports IP de serveurs virtuels, la réécriture de ports de redirection, le Web 2.0 Push et la prise en charge de la redirection d'URL.

Le protocole HTTP étant un protocole d'application basé sur le protocole TCP, vous pouvez également utiliser le type de service TCP pour les serveurs Web. Toutefois, si vous le faites, l'appliance NetScaler est en mesure d'effectuer uniquement un équilibrage de charge de couche 4. Il ne peut fournir aucun des supports de couche 7 décrits précédemment.

SSL

Utilisé pour les serveurs qui acceptent le trafic HTTPS, tels que les sites Web de commerce électronique et les applications de panier d'achat. Le type de service SSL permet à l'appliance NetScaler

de chiffrer et de déchiffrer le trafic SSL (effectuer un déchargement SSL) pour vos applications Web sécurisées. Il prend également en charge la persistance HTTP, la commutation de contenu, la réécriture, l'insertion du port IP du serveur virtuel, le Web 2.0 Push et la redirection d'URL.

Vous pouvez également utiliser les types de service SSL_BRIDGE, SSL_TCP ou TCP. Toutefois, si vous le faites, l'appliance effectue uniquement un équilibrage de charge de couche 4. Il ne peut pas fournir de déchargement SSL ni aucun des supports de couche 7 décrits.

FTP

Utilisé pour les serveurs qui acceptent le trafic FTP. Le type de service FTP permet à l'appliance NetScaler de prendre en charge des détails spécifiques du protocole FTP.

Vous pouvez également utiliser TCP ou N'importe quel type de service pour les serveurs FTP.

TCP

Utilisé pour les serveurs qui acceptent différents types de trafic TCP ou qui acceptent un type de trafic TCP pour lequel aucun type de service plus spécifique n'est disponible.

Vous pouvez également utiliser le type de service ANY pour ces serveurs.

SSL_TCP

Utilisé pour les serveurs qui acceptent le trafic SSL non basé sur HTTP, afin de prendre en charge le déchargement SSL.

Vous pouvez également utiliser le type de service TCP pour ces services. Dans ce cas, l'appliance NetScaler effectue à la fois l'équilibrage de charge de couche 4 et le déchargement SSL.

UDP

Utilisé pour les serveurs qui acceptent le trafic UDP. Vous pouvez également utiliser le type de service ANY.

PONT SSL

Utilisé pour les serveurs qui acceptent le trafic SSL lorsque vous ne souhaitez pas que l'appliance NetScaler effectue un déchargement SSL. Vous pouvez également utiliser le type de service SSL_TCP.

NNTP

Utilisé pour les serveurs qui acceptent le trafic NNTP (Network News Transfer Protocol), généralement les sites Usenet.

DNS

Utilisé pour les serveurs qui acceptent le trafic DNS, généralement des serveurs de noms. Avec le type de service DNS, l'appliance NetScaler valide le format de paquet de chaque demande et réponse DNS. Il peut également mettre en cache les réponses DNS. Vous pouvez appliquer des politiques DNS aux services DNS.

Vous pouvez également utiliser le type de service UDP pour ces services. Toutefois, si vous le faites, l'appliance NetScaler ne peut effectuer qu'un équilibrage de charge de couche 4. Il ne peut pas fournir de support pour les fonctionnalités spécifiques au DNS.

ANY

Utilisé pour les serveurs qui acceptent tout type de trafic TCP, UDP ou ICMP. Le paramètre ANY est principalement utilisé avec l'équilibrage de charge du pare-feu et l'équilibrage de charge des liens.

SIP-UDP

Utilisé pour les serveurs qui acceptent le trafic SIP (Session Initiation Protocol) basé sur UDP. Le protocole SIP initie, gère et met fin à des sessions de communication multimédia et est devenu la norme pour la téléphonie Internet (VoIP).

Vous pouvez également utiliser le type de service UDP pour ces services. Toutefois, si vous le faites, l'appliance NetScaler effectue uniquement un équilibrage de charge de couche 4. Il ne peut pas fournir de support pour les fonctionnalités spécifiques au SIP.

DNS-TCP

Utilisé pour les serveurs qui acceptent le trafic DNS, où l'appliance NetScaler agit en tant que proxy pour le trafic TCP envoyé aux serveurs DNS. Avec les services du type de service DNS-TCP, l'appliance NetScaler valide le format de paquet de chaque demande et réponse DNS et peut mettre en cache les réponses DNS, comme pour le type de service DNS.

Vous pouvez également utiliser le type de service TCP pour ces services. Toutefois, si vous le faites, l'appliance NetScaler effectue uniquement l'équilibrage de charge de couche 4 des serveurs de noms DNS externes. Il ne peut fournir de support pour aucune fonctionnalité spécifique au DNS.

RTSP

Utilisé pour les serveurs qui acceptent le trafic RTSP (Real Time Streaming Protocol). Le RTSP fournit du multimédia et d'autres données de streaming. Sélectionnez ce type pour prendre en charge le son, la vidéo et d'autres types de contenu multimédia en streaming.

Vous pouvez également utiliser le type de service TCP pour ces services. Toutefois, si vous le faites, l'appliance NetScaler effectue uniquement un équilibrage de charge de couche 4. Il ne peut pas analyser le flux RTSP ni fournir la prise en charge de la persistance RTSPID ou du NAT RTSP.

DHCPRA

Utilisé pour les serveurs qui acceptent le trafic DHCP. Le type de service DHCPRA peut être utilisé pour relayer les demandes et les réponses DHCP entre les VLAN.

DIAMÈTRE

Utilisé pour équilibrer la charge du trafic Diameter entre plusieurs serveurs Diameter. Diameter utilise un équilibrage de charge basé sur des messages.

DIAMÈTRE_SSL

Utilisé pour équilibrer la charge du trafic Diameter via SSL.

Les services sont désignés comme DÉSACTIVÉS jusqu'à ce que l'appliance NetScaler se connecte au serveur d'équilibrage de charge associé et vérifie qu'il est opérationnel. À ce stade, le service est désigné comme ACTIVÉ. Ensuite, l'appliance NetScaler surveille régulièrement l'état des serveurs et remet à l'état DISABLED ceux qui ne répondent pas aux sondes de surveillance (appelées contrôles de santé) jusqu'à ce qu'ils répondent.

Remarque : Vous pouvez créer une gamme de services à partir d'une seule commande CLI ou de la même boîte de dialogue. Les noms de la gamme varient selon un nombre utilisé comme suffixe/préfixe. Par exemple, service1, service2, etc. Dans l'utilitaire de configuration, vous pouvez spécifier une plage uniquement dans le dernier octet de l'adresse IP, c'est-à-dire le quatrième dans le cas d'une adresse IPv4 et le huitième dans le cas d'une adresse IPv6. À partir de la ligne de commande, vous pouvez spécifier la plage dans n'importe quel octet de l'adresse IP.

QUIC

Utilisé par les serveurs d'équilibrage de charge qui acceptent le trafic vidéo QUIC basé sur UDP. Le service permet à l'appliance NetScaler d'optimiser le trafic vidéo ABR crypté via le protocole UDP.

Pour créer un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <name> <serverName> <serviceType> <port>

add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

Pour créer un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic**> **Équilibrage de charge** > **Services**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Créer un service, spécifiez les valeurs des paramètres suivants :
   - Nom du service : nom
   - Serveur—Nom du serveur
   - Protocole — Type de service
   - Port-port
4. Cliquez sur **Créer**, puis sur **Fermer**. Le service que vous avez créé apparaît dans le volet Services.

Création d'un serveur virtuel

Après avoir créé vos services, vous devez créer un serveur virtuel pour accepter le trafic pour les sites Web, les applications ou les serveurs à charge équilibrée. Une fois l'équilibrage de charge configuré, les utilisateurs se connectent au site Web, à l'application ou au serveur soumis à l'équilibrage de charge via l'adresse IP ou le nom de domaine complet du serveur virtuel.

Remarque :

- Les noms de serveurs virtuels préfixés par « app_ » n'apparaissent pas dans l'interface graphique bien qu'ils soient présents dans le fichier ns.conf et s'affichent lorsque vous exécutez la commande show. Toutefois, les noms de serveurs virtuels préfixés par « app » sont affichés dans l'interface graphique.
- Le serveur virtuel est désigné comme étant hors service jusqu'à ce que vous y liez les services que vous avez créés et jusqu'à ce que l'appliance NetScaler se connecte à ces services et vérifie qu'ils sont opérationnels. Ce n'est qu'alors que le serveur virtuel est désigné comme étant UP.

Pour créer un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add lb vserver <name> <serviceType> <ip> <port>

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

Pour créer un serveur virtuel à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis créez un serveur virtuel.

Liaison des services au serveur virtuel

Remarque : Un service peut être lié à un maximum de 500 serveurs virtuels.

Après avoir créé des services et un serveur virtuel, vous devez lier les services au serveur virtuel. Généralement, les services sont liés à des serveurs virtuels du même type, mais vous pouvez lier certains types de services à différents types de serveurs virtuels, comme illustré ci-dessous.

Type de serveur virtuel	Type de service	Commentaire
HTTP	SSL	Vous devez normalement lier un service SSL à un serveur virtuel HTTP pour effectuer le chiffrement.
SSL	HTTP	Vous devez normalement lier un service HTTP à un serveur virtuel SSL pour effectuer le déchargement SSL.
SSL_TCP	TCP	Vous devez normalement lier un service TCP à un serveur virtuel SSL_TCP pour effectuer un déchargement SSL pour un autre TCP (déchiffrement SSL sans connaissance du contenu).

L'état des services liés à un serveur virtuel détermine l'état du serveur virtuel : si tous les services liés sont hors service, le serveur virtuel est marqué comme étant inactif, et si l'un des services liés est ACTIF ou HORS SERVICE, l'état du serveur virtuel est ACTIF.

Pour lier un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb vserver <name> <serviceName>

bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour lier un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic**> **Équilibrage de charge** > **Serveurs virtuels**, puis sélectionnez un serveur virtuel.
2. Cliquez dans la section **Service** et sélectionnez le service à lier.

Remarque : Vous pouvez lier un service à plusieurs serveurs virtuels.

Vérification de la configuration

Une fois votre configuration de base terminée, vous pouvez afficher les propriétés de chaque serveur virtuel d'équilibrage de charge et de service dans votre configuration d'équilibrage de charge pour vérifier que chacun est correctement configuré. Une fois la configuration en cours d'exécution, vous pouvez afficher les statistiques de chaque serveur virtuel d'équilibrage de charge et de service pour vérifier les problèmes éventuels.

Affichage des propriétés d'un objet serveur

Vous pouvez afficher des propriétés telles que le nom, l'état et l'adresse IP de n'importe quel objet serveur dans la configuration de votre appliance NetScaler.

Pour afficher les propriétés des objets du serveur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show server <serverName>

show server server-1
<!--NeedCopy-->
```


Pour afficher les propriétés des objets du serveur à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs**. Les valeurs des paramètres des serveurs disponibles apparaissent dans le volet de détails.

Affichage des propriétés d'un serveur virtuel

Vous pouvez afficher des propriétés telles que le nom, l'état, l'état effectif, l'adresse IP, le port, le protocole, la méthode et le nombre de services liés pour vos serveurs virtuels. Si vous avez configuré d'autres paramètres que les paramètres d'équilibrage de charge de base, vous pouvez consulter les paramètres de persistance de vos serveurs virtuels, toutes les politiques qui leur sont liées, ainsi que tous les serveurs virtuels de redirection du cache et de commutation de contenu qui ont été liés aux serveurs virtuels.

Pour afficher les propriétés d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show lb vserver <name>

show lb vserver Vserver-LB-1
<!--NeedCopy-->
```

Pour afficher les propriétés d'un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel pour afficher ses propriétés en bas du volet d'informations.
3. Pour afficher les serveurs virtuels de redirection du cache et de commutation de contenu liés à ce serveur virtuel, cliquez sur **Afficher les liaisons CS/CR**.

Affichage des propriétés d'un service

Vous pouvez consulter le nom, l'état, l'adresse IP, le port, le protocole, le nombre maximal de connexions client, le nombre maximum de demandes par connexion et le type de serveur des services configurés, et utiliser ces informations pour résoudre toute erreur dans la configuration du service.

Pour afficher les propriétés des services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show service <name>

show service Service-HTTP-1
<!--NeedCopy-->
```

Pour afficher les propriétés des services à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**. Les détails des services disponibles apparaissent dans le volet Services.

Affichage des liaisons d'un service

Vous pouvez consulter la liste des serveurs virtuels auxquels le service est lié. Les informations de liaison fournissent également le nom, l'adresse IP, le port et l'état des serveurs virtuels auxquels les services sont liés. Vous pouvez utiliser les informations de liaison pour résoudre tout problème lié à la liaison des services à des serveurs virtuels.

Pour afficher les liaisons d'un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show service bindings <name>

show service bindings Service-HTTP-1
<!--NeedCopy-->
```

Pour afficher les liaisons d'un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Dans le volet de détails, sélectionnez le service dont vous souhaitez consulter les informations de liaison.
3. Dans l'onglet **Action**, cliquez sur **Afficher les liaisons**.

Affichage des statistiques d'un serveur virtuel

Pour évaluer les performances des serveurs virtuels ou pour résoudre des problèmes, vous pouvez afficher les détails des serveurs virtuels configurés sur l'appliance NetScaler. Vous pouvez afficher un

résumé des statistiques pour tous les serveurs virtuels, ou vous pouvez spécifier le nom d'un serveur virtuel pour afficher les statistiques uniquement pour ce serveur virtuel. Vous pouvez afficher les informations suivantes :

- Nom
- Adresse IP
- Port
- Protocole
- État du serveur virtuel
- Taux de demandes reçues
- Taux de succès

Pour afficher les statistiques du serveur virtuel à l'aide de l'interface de ligne de commande

Pour afficher un résumé des statistiques pour tous les serveurs virtuels actuellement configurés sur l'appliance, ou pour un seul serveur virtuel, à l'invite de commande, tapez :

```
stat lb vserver [`<name>`]
<!--NeedCopy-->
```

Exemple :

```
stat lb vserver server-1
<!--NeedCopy-->
```

La figure suivante présente un exemple de statistique.


```
> stat lbvserver
[
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
vserver1        10.102.20.200    80          SSL         DOWN      0/s

lb1               203.1.113.5   443         DTLS         DOWN      0/s

vicap                       *     0          TCP         DOWN      0/s

lbicap                2.2.3.4  1344          TCP         DOWN      0/s

app_...stest          0.0.0.0     0         HTTP         DOWN      0/s

app_...ttest          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...test1          0.0.0.0     0         HTTP         DOWN      0/s

app_...1test          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...est12          0.0.0.0     0         HTTP         DOWN      0/s

app_...sting          0.0.0.0     0         HTTP         DOWN      0/s

test                  2.2.2.2    80         HTTP         DOWN      0/s

shar...lt-lb          0.0.0.0     0         HTTP         DOWN      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ts-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ns-lb          0.0.0.0     0         HTTP           UP      0/s

shar...as-lb          0.0.0.0     0         HTTP           UP      0/s

forward-vs            0.0.0.0     0          TCP         DOWN      0/s

tcpcs                 0.0.0.0     0          TCP         DOWN      0/s

test124               0.0.0.0     0          SSL         DOWN      0/s

testssl               0.0.0.0     0          SSL         DOWN      0/s
```


Pour afficher les statistiques du serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Si vous souhaitez afficher les statistiques d'un seul serveur virtuel, dans le volet de détails, sélectionnez le serveur virtuel dont vous souhaitez afficher les statistiques.
3. Dans le volet de détails, cliquez sur **Statistiques**.

Affichage des statistiques d'un service

Vous pouvez afficher le taux de demandes, de réponses, d'octets de demande, d'octets de réponse, de connexions client actuelles, de demandes dans la file d'attente de surtension, de connexions au serveur en cours, etc. à l'aide des statistiques de service.

Pour afficher les statistiques d'un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat service <name>
<!--NeedCopy-->
```

Exemple :

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Pour afficher les statistiques d'un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Dans le volet d'informations, sélectionnez le service dont vous souhaitez consulter les statistiques (par exemple, Service-HTTP-1).
3. Cliquez sur **Statistiques**. Les statistiques apparaissent dans une nouvelle fenêtre.

Équilibrer la charge du serveur virtuel et des états de service

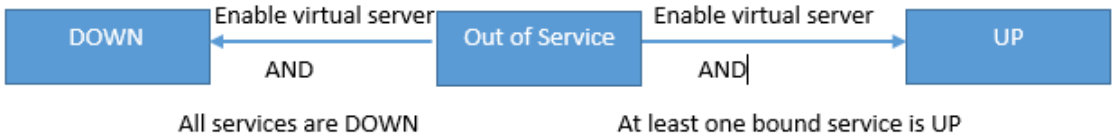
August 20, 2021

Un serveur virtuel d'équilibrage de charge qui ne possède pas de serveur virtuel de sauvegarde peut prendre les états suivants, en fonction de l'état des services qui y sont liés et de sa désactivation administrative :

- **UP** : Au moins un des services liés au serveur virtuel est UP.
- **DOWN** : tous les services liés au serveur virtuel sont DOWN, ou la fonctionnalité d'équilibrage de charge n'est pas activée.
- **Out of Service (OFS)** : Si vous désactivez administrativement le serveur virtuel, il entre dans l'état OFS mais son état effectif est DOWN. L'administrateur peut contrôler la transition vers l'état OFS à partir de l'état DOWN ou UP, ou vers l'état DOWN ou UP à partir de l'état OFS.

L'état et l'état effectif d'un serveur virtuel sont les mêmes si un serveur virtuel de sauvegarde n'est pas configuré. Toutefois, si un serveur virtuel de sauvegarde ou une chaîne de serveurs virtuels de sauvegarde est configuré, l'état effectif est dérivé des états des services liés au serveur virtuel principal et aux serveurs virtuels de sauvegarde. Si l'un des serveurs virtuels de sauvegarde de la chaîne est UP, l'état effectif du serveur virtuel principal est UP, même si tous les services liés au serveur virtuel principal sont DOWN.

Les diagrammes suivants montrent les conditions dans lesquelles un serveur virtuel passe d'un état à un autre.



Un service peut prendre les états suivants :

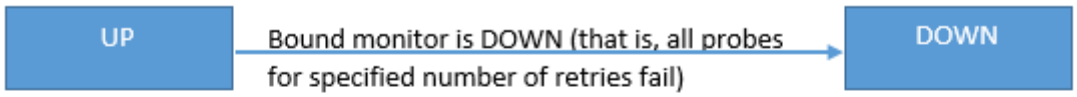
- **UP :** Si les sondes de tous les moniteurs liés au service réussissent.
- **DOWN** : Si les sondes de surveillance vers le service ne sont pas répondues dans le délai configuré.

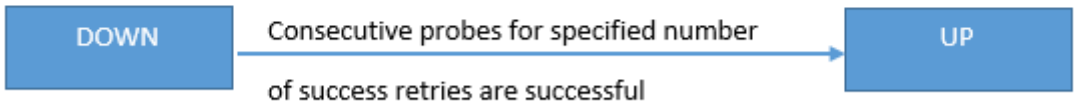
- **OUT OF SERVICE** : si vous désactivez administrativement le service, ou si vous arrêtez correctement le service et qu'il n'y a pas de transactions actives sur le service
- **GOING OUT OF SERVICE (TROFS)** : Si vous désactivez administrativement le service avec un délai, ou si vous arrêtez gracieusement le service et qu'il y a des transactions actives sur le service. Pour plus d'informations, voir Arrêt gracieux des services.
- **ARRÊT EN CAS DE SORTIE DU SERVICE (TROFS_DOWN)[]** Une sonde de surveillance échoue alors que le service est dans l'état « OUT OF SERVICE ».

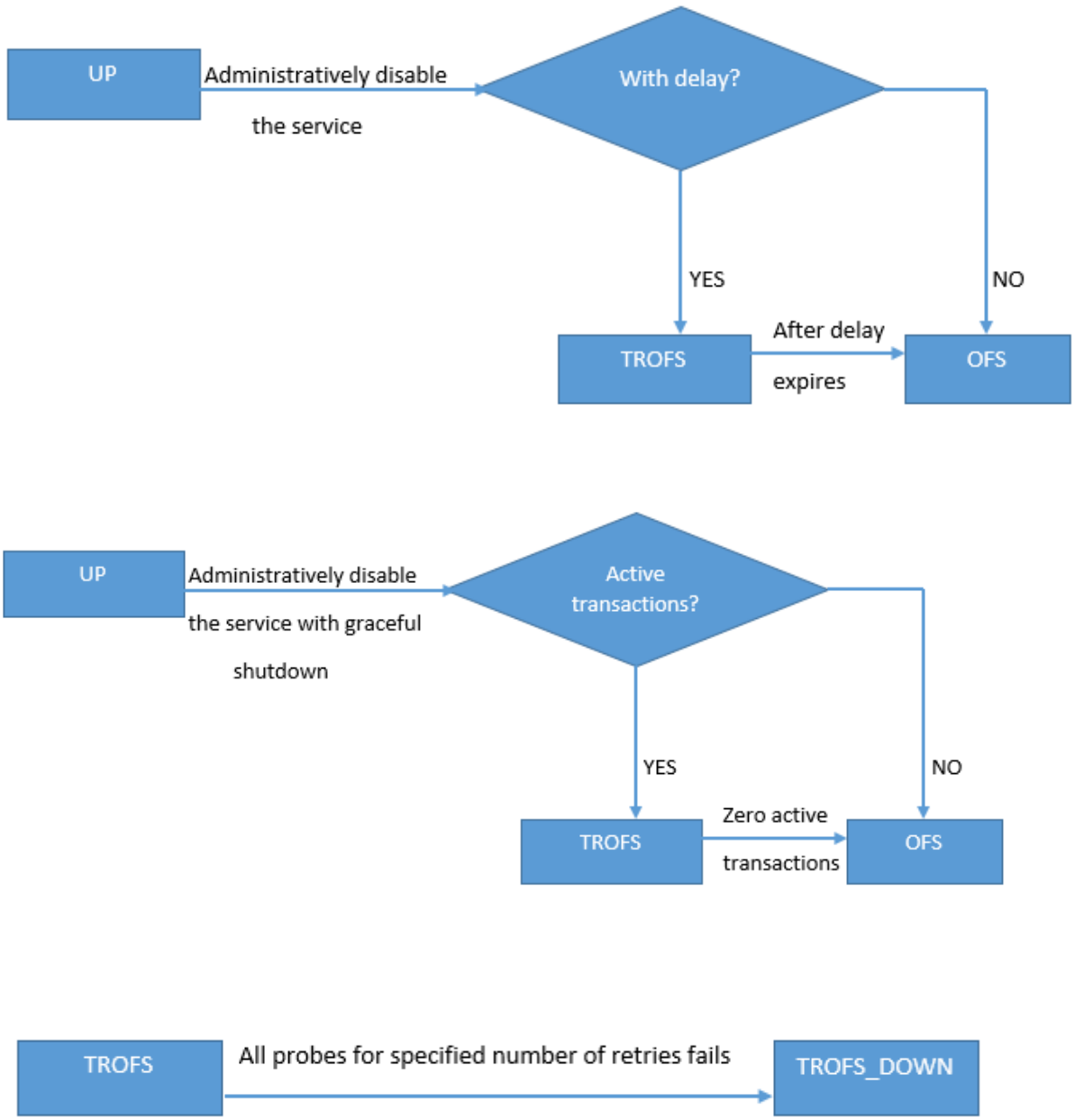
Un service en cours de transition de UP à OFS est dans l'état OUT DU SERVICE. Un service faisant la transition de DOWN à OFS est dans l'état DOWN WHEN GOING OUT OF SERVICE. Par exemple, si un service est DOWN et que vous le désactivez avec un délai, le service passe à DOWN WHEN GOING OUT OF SERVICE, puis à l'état OUT OF SERVICE. Si un service est OUT et que vous le désactivez avec un délai, le service passe à OUT DE SERVICE. Pendant ce temps, si une sonde de surveillance sur le serveur échoue, le service passe à DOWN WHEN GOING OUT OF SERVICE et, après l'expiration du délai, passe à l'état OFS.

> **Remarque**
>
> Vous pouvez configurer le débordement sur un serveur virtuel de sauvegarde en définissant le paramètre « HealthThreshold » sur une valeur positive non nulle. Ensuite, si un service unique lié au serveur virtuel principal passe à l'état DOWN lorsque vous sortez du service et que le seuil d'intégrité n'est pas atteint, le serveur virtuel principal est marqué « DOWN » et les nouvelles connexions sont dirigées vers le serveur virtuel de sauvegarde.

Les diagrammes suivants montrent les conditions dans lesquelles un service passe d'un état à un autre.







Prise en charge du profil d'équilibrage de charge

June 20, 2023

Une configuration d'équilibrage de charge comporte de nombreux paramètres, de sorte que la définition des mêmes paramètres sur plusieurs serveurs virtuels peut devenir fastidieuse. À partir de la

version 11.1, un profil d'équilibrage de charge (LB) facilite cette tâche. Vous pouvez désormais définir des paramètres d'équilibrage de charge dans un profil et associer ce profil à des serveurs virtuels, au lieu de définir ces paramètres sur chaque serveur virtuel.

Les paramètres suivants sont actuellement pris en charge dans un profil LB :

- `HTTPonlyflag`: incluez l'attribut HttpOnly dans les cookies de persistance. L'attribut HttpOnly limite la portée d'un cookie aux requêtes HTTP et contribue à atténuer le risque d'attaques par script intersite.
- UseSecuredPersistenceCookie : chiffrez les valeurs des cookie de persistance à l'aide de l'algorithme de hachage SHA2.
- `Cookiepassphrase`: spécifiez la phrase secrète utilisée pour générer une valeur de cookie de persistance sécurisée.
- DBS_LB : activez l'équilibrage de charge spécifique à la base de données pour les types de service MySQL et MSSQL.
- cl_process_local—Les paquets destinés à un serveur virtuel dans un cluster ne sont pas dirigés. Activez l'option pour le mode de réponse à une demande de paquet unique ou lorsque le périphérique amont exécute un RSS approprié pour la distribution basée sur la connexion.
- LBHashalgorithm : spécifiez l'algorithme de hachage à utiliser pour les méthodes d'équilibrage de charge basées sur le hachage suivantes :
  - Méthode de hachage d'URL
  - Méthode de hachage du domaine
  - Méthode de hachage IP de destination
  - Méthode de hachage de l'adresse IP source
  - Méthode de hachage IP source et adresse IP de destination
  - Méthode de hachage du port source IP source
  - Méthode de hachage de l'ID d'appel
  - Méthode de jeton

  Valeurs possibles : DEFAULT, PRAC, JARH Valeur
  par défaut : DEFAULT
- LBHashfingers : spécifiez le nombre de doigts à utiliser dans les algorithmes PRAC et JARH pour les méthodes LB basées sur le hachage. L'augmentation du nombre de doigts permet une meilleure répartition du trafic au détriment de la mémoire supplémentaire.

  Valeur par défaut : 256 Valeur
  minimale : 1 Valeur
  maximale : 1024
- ProximityFromSelf-Enable permet d'utiliser l'adresse IP de bouclage du Netscaler au lieu de

l'adresse IP du client afin de récupérer l'emplacement du serveur le plus proche à des fins d'équilibrage de charge de proximité statique ou de décision GSLB.

> **Remarque**
>
> Vous pouvez définir les paramètres DBS_LB et CL_Process_Local sur un serveur virtuel et dans le profil. Si vous activez ces paramètres sur un serveur virtuel, puis que vous définissez un profil sur ce serveur virtuel, les paramètres apparaissent comme désactivés dans la sortie de la "show lb vserver" commande de ce serveur virtuel. Vérifiez le profil pour voir l'état réel de ces paramètres. En outre, si vous définissez puis désactivez un profil sur un serveur virtuel, les paramètres sont définis avec les valeurs par défaut pour ce serveur virtuel.

Pour créer un profil LB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb profile <lbprofilename> -dbsLb ( ENABLED | DISABLED ) -
    processLocal ( ENABLED | DISABLED ) -httpOnlyCookieFlag ( ENABLED |
    DISABLED ) -cookiePassphrase -useSecuredPersistenceCookie ( ENABLED
    | DISABLED ) -lbHashAlgorithm <lbHashAlgorithm> -lbHashFingers <
    positive_integer>- proximityFromSelf <NO/YES>
<!--NeedCopy-->
```

Exemple :

```
> sh lb profile p1
LB Profile name:  p1
DBS LB : DISABLED   Process Local: DISABLED
Persistence Cookie HttpOnly Flag: ENABLED
Use Encrypted Persistence Cookie: DISABLED
Proximity From Self: ENABLED
No of vservers bound: 0
Store MQTT clientid and username in transactional logs: NO
Hash LB algorithm used in LB decision: DEFAULT
Number of fingers for Hash LB algorithm: 256
Done

<!--NeedCopy-->
```

Pour créer un profil LB à l'aide de l'interface graphique

Accédez à **Système** > **Profils** > **Profil LB**, puis ajoutez un profil.

Pour associer un profil LB à un serveur virtuel LB à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -lbprofilename <string>
<!--NeedCopy-->
```

Exemple

```
set lbvserver lbvip1 -lbprofile p1

Done

sh lb vserver lbvip1

lbvip1 (203.0.113.1:80) - HTTP       Type: ADDRESS
State: UP
Last state change was at Wed May 25 12:36:20 2016
Time since last state change: 0 days, 00:01:26.140
Effective State: UP  ARP:DISABLED
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: ENABLED
Port Rewrite : DISABLED
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION      BackupMethod: ROUNDROBIN
Mode: IP
Persistence: NONE
Vserver IP and Port insertion: OFF
Push: DISABLED  Push VServer:
Push Multi Clients: NO
Push Label Rule: none
L2Conn: OFF
Skip Persistency: None
Listen Policy: NONE
IcmpResponse: PASSIVE
RHIstate: PASSIVE
New Service Startup Request Rate: 0 PER_SECOND, Increment Interval: 0
Mac mode Retain Vlan: DISABLED
DBS_LB: DISABLED
Process Local: DISABLED
Traffic Domain: 0
LB Profile: p1
```



```
Done
<!--NeedCopy-->
```

Pour associer un profil LB à un serveur virtuel LB à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sélectionnez un serveur virtuel, puis cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, cliquez sur **Profils**.
4. Dans la liste des **profils LB**, sélectionnez le profil à associer à ce serveur virtuel.

Pour configurer le paramètre Proximity from Self dans le profil d'équilibrage de charge à l'aide de l'interface graphique

Configurez le paramètre Proximity from Self dans le profil de sorte que lorsque le profil est associé à l'entité, le paramètre soit activé pour l'entité.

1. Accédez à **Système** > **Profil > ProfilLB**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Proximity from Self**.
4. Cliquez sur **OK**.

Algorithmes d'équilibrage de charge

May 5, 2023

L'algorithme d'équilibrage de charge définit les critères que l'appliance NetScaler utilise pour sélectionner le service vers lequel rediriger chaque demande client. Différents algorithmes d'équilibrage de charge utilisent des critères différents. Par exemple, l'algorithme de moindre connexion sélectionne le service avec le moins de connexions actives, tandis que l'algorithme Round Robin gère une file d'attente de services actifs, distribue chaque connexion au service suivant de la file d'attente, puis envoie ce service à la fin de la file d'attente.

Certains algorithmes d'équilibrage de charge sont les mieux adaptés à la gestion du trafic sur les sites Web, d'autres à la gestion du trafic vers les serveurs DNS et d'autres à la gestion d'applications Web complexes utilisées dans le commerce électronique ou sur les réseaux locaux ou WAN de l'entreprise. Le tableau suivant répertorie chaque algorithme d'équilibrage de charge pris en charge par l'appliance NetScaler, avec une brève description du fonctionnement de chacun d'entre eux.

Nom	Sélection du serveur basée sur
LE MOINS DE CONNEXION	Quel service possède actuellement le moins de connexions client ? Il s'agit de l'algorithme d'équilibrage de charge par défaut.
ROUNDROBIN	Quel service figure en haut de la liste des services ? Une fois que ce service est sélectionné pour une connexion, il se déplace vers le bas de la liste.
TEMPS DE RÉPONSE LE PLUS COURT	Quel serveur à charge équilibrée présente actuellement le temps de réponse le plus rapide ?
HACHAGE D'URL	Un hachage de l'URL de destination.
HACHAGE DE DOMAINE	Un hachage du domaine de destination.
DESTINATIONIPHASH	Un hachage de l'adresse IP de destination.
SOURCEIPHASH	Un hachage de l'adresse IP source.
SRCIPDESTIPHASH	Un hachage des adresses IP source et de destination.
CALLIDHASH	Un hachage de l'ID d'appel dans l'en-tête SIP.
SRCIPSRCPORTHASH	Un hachage de l'adresse IP et du port du client.
LEASTBANDWIDTH	Quel service présente actuellement le moins de contraintes de bande passante ?
LEASTPACKETS	Quel service reçoit actuellement le moins de paquets ?
CHARGEMENT PERSONNALISÉ	Données provenant d'un moniteur de charge.
JETON	Le jeton configuré.
LRTM	Le moins de connexions actives et le temps de réponse moyen le plus bas.

En fonction du protocole du service utilisé pour l'équilibrage de charge, l'appliance NetScaler configure chaque connexion entre le client et le serveur pour qu'elle dure pendant un intervalle de temps différent. C'est ce que l'on appelle la granularité d'équilibrage de charge, qui se divise en trois types : granularité basée sur les demandes, basée sur les connexions et basée sur le temps. Le tableau suivant décrit chaque type de granularité et indique quand chacun est utilisé.

Granularité	Types de service d'équilibrage de charge	Spécifie
Basé sur des demandes	HTTP ou HTTPS	Un nouveau service est choisi pour chaque requête HTTP, indépendamment des connexions TCP. Comme pour toutes les requêtes HTTP, une fois que le serveur Web répond à la demande, la connexion est fermée.
Basé sur la connexion	Protocoles TCP et TCP autres que HTTP	Un service est choisi pour chaque nouvelle connexion TCP. La connexion persiste jusqu'à ce que le service ou le client y mette fin.
Basé sur le temps	UDP et autres protocoles IP	Un nouveau service est choisi pour chaque paquet UDP. Lors de la sélection d'un service, une session est créée entre le service et un client pendant une période spécifiée. Lorsque le temps expire, la session est supprimée et un nouveau service est choisi pour les paquets supplémentaires, même si ces paquets proviennent du même client.

Lors du démarrage d'un serveur virtuel, ou chaque fois que l'état d'un serveur virtuel change, le serveur virtuel peut initialement utiliser la méthode du round robin pour distribuer les demandes des clients entre les serveurs physiques. Ce type de distribution, appelé « *start round robin »,* permet d'éviter toute charge inutile sur un seul serveur lorsque les demandes initiales sont traitées. Après avoir utilisé la méthode Round Robin au démarrage, le serveur virtuel passe à la méthode d'équilibrage de charge spécifiée sur le serveur virtuel.

Le Startup RR Factor fonctionne de la manière suivante :

- Si le facteur RR de démarrage est défini sur zéro, l'appliance passe à la méthode d'équilibrage

de charge spécifiée en fonction du taux de demandes.
- Si le facteur RR de démarrage est un nombre autre que zéro, l'appliance utilise la méthode circulaire pour le nombre de demandes spécifié avant de passer à la méthode d'équilibrage de charge spécifiée.
- Par défaut, le facteur RR de démarrage est défini sur zéro.

Remarque : Vous ne pouvez pas définir le facteur RR de démarrage pour un serveur virtuel individuel. La valeur que vous spécifiez s'applique à tous les serveurs virtuels de l'appliance NetScaler.

Pour définir le facteur de démarrage à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb parameter -startupRRFactor <positive_integer>
```

Exemple

```
set lb parameter -startupRRFactor 25000
```

Pour définir le facteur de démarrage à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**et définissez le facteur RR de démarrage.

Méthode de connexion la moins

May 5, 2023

Lorsqu'un serveur virtuel est configuré pour utiliser l'algorithme (ou la méthode) d'équilibrage de charge le moins élevé de connexions, il sélectionne le service avec le moins de connexions actives. Il s'agit de la méthode par défaut, car, dans la plupart des cas, elle fournit les meilleures performances.

Pour les services TCP, HTTP, HTTPS et SSL_TCP, l'appliance NetScaler inclut les types de connexion suivants dans sa liste de connexions existantes :

- **Connexions actives à un service.** Connexions représentant les demandes qu'un client a envoyées au serveur virtuel et que le serveur virtuel a transmises à un service. Pour les services HTTP et HTTPS, les connexions actives représentent uniquement les requêtes HTTP ou HTTPS qui n'ont pas encore reçu de réponse.
- **Connexions en attente dans la file d'attente.** Toutes les connexions au serveur virtuel qui sont en attente dans une file d'attente d'urgence et qui n'ont pas encore été transférées vers un service. Les connexions peuvent s'accumuler dans la file d'attente de surtension à tout moment, pour l'une des raisons suivantes :

- Vos services sont soumis à des limites de connexion, et tous les services de votre configuration d'équilibrage de charge respectent cette limite.
- La fonction de protection contre les surtensions est configurée et a été activée par une augmentation du nombre de demandes adressées au serveur virtuel.
- Le serveur à charge équilibrée a atteint une limite interne et n'ouvre donc aucune nouvelle connexion. (Par exemple, la limite de connexion d'un serveur Apache est atteinte.)

Lorsqu'un serveur virtuel utilise la méthode de moindre connexion, il considère les connexions en attente comme appartenant au service spécifique. Par conséquent, il n'ouvre pas de nouvelles connexions à ces services.

Pour les services UDP, les connexions prises en compte par l'algorithme de moindre connexion incluent toutes les sessions entre le client et un service. Ces sessions sont des entités logiques basées sur le temps. Lorsque le premier paquet UDP d'une session arrive, l'appliance NetScaler crée une session entre l'adresse IP et le port source et l'adresse IP et le port de destination.

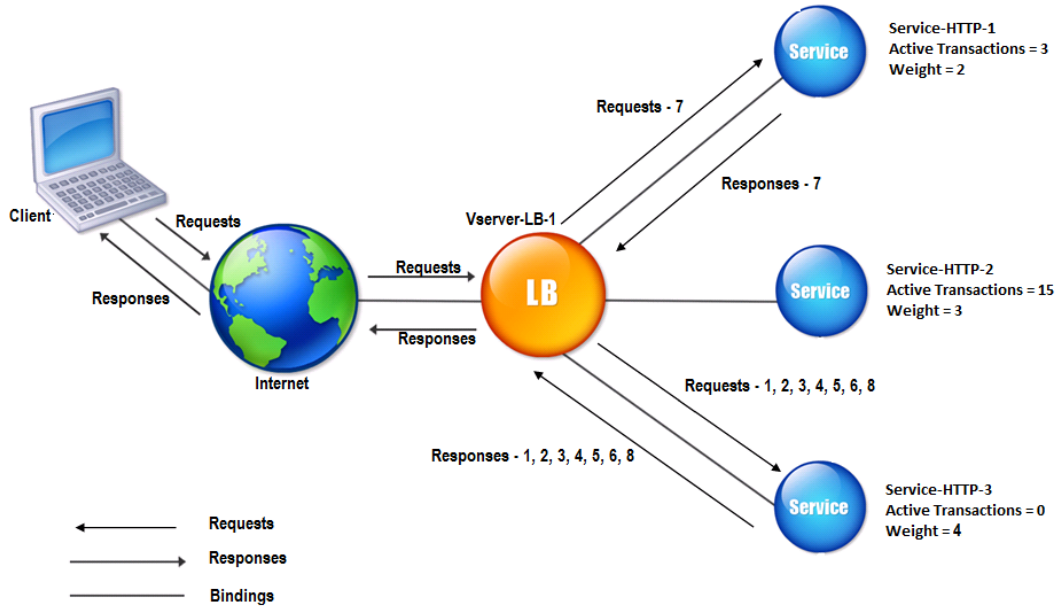
Pour les connexions RTSP (Real-Time Streaming Protocol), l'appliance NetScaler utilise le nombre de connexions de contrôle actives pour déterminer le plus petit nombre de connexions à un service RTSP.

L'exemple suivant montre comment un serveur virtuel sélectionne un service pour l'équilibrage de charge en utilisant la méthode de moindre connexion. Prenez en compte les trois services suivants :

- Service-HTTP-1 gère 3 transactions actives.
- Service-HTTP-2 gère 15 transactions actives.
- Service-HTTP-3 ne gère aucune transaction active.

Le schéma suivant montre comment l'appliance NetScaler transmet les demandes entrantes lorsque la méthode de moindre connexion est utilisée.

Figure 1. Mécanisme de la méthode d'équilibrage de charge basée sur le moindre nombre de connexions



Dans ce schéma, le serveur virtuel sélectionne le service pour chaque connexion entrante en choisissant le serveur avec le moins de transactions actives.

Les connexions sont transférées comme suit :

- Service-HTTP-3 reçoit la première requête, car il ne gère aucune transaction active.

  Remarque : Le service sans transaction active est sélectionné en premier.

- Service-HTTP-3 reçoit les deuxième et troisième requêtes parce que le service a le plus petit nombre de transactions actives.
- Service-HTTP-1 reçoit la quatrième demande car Service-HTTP-1 et Service-HTTP-3 ont le même nombre de transactions actives, le serveur virtuel utilise la méthode Round Robin pour choisir entre elles.
- Service-HTTP-3 reçoit la cinquième requête.
- Service-HTTP-1 reçoit la sixième requête, et ainsi de suite, jusqu'à ce que Service-HTTP-1 et Service-HTTP-3 traitent le même nombre de requêtes que Service-HTTP-2. Ensuite, l'appliance NetScaler commence à transférer les demandes vers Service-HTTP-2 lorsqu'il s'agit du service le moins chargé ou lorsque son tour apparaît dans la file d'attente circulaire.

  Remarque : si les connexions à Service-HTTP-2 se ferment, il peut obtenir de nouvelles connexions avant que chacun des deux autres services ait 15 transactions actives.

Le tableau suivant explique comment les connexions sont distribuées dans la configuration d'équilibrage de charge à trois services décrite précédemment.

Connexion entrante	Service sélectionné	Nombre actuel de connexions actives	Remarques
Request-1	Service-HTTP-3 ; (N = 0)	1	Le Service-HTTP-3 possède le moins de connexions actives.
Request-2	Service-HTTP-3 ; (N = 1)	2	Le Service-HTTP-3 possède le moins de connexions actives.
Request-3	Service-HTTP-3 ; (N = 2)	3	-
Request-4	Service-HTTP-1 ; (N = 3)	4	Service-HTTP-1 et Service-HTTP-3 ont le même nombre de connexions actives.
Request-5	Service-HTTP-3 ; (N = 3)	4	Service-HTTP-1 et Service-HTTP-3 ont le même nombre de connexions actives.
Request-6	Service-HTTP-1 ; (N = 4)	5	-
Request-7	Service-HTTP-3 ; (N = 4)	5	-
Request-8	Service-HTTP-1 ; (N = 5)	6	-

Le Service-HTTP-2 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives et que les connexions en cours avec celui-ci se ferment, ou lorsque les autres services (Service-HTTP-1 et Service-HTTP-3) disposent chacun de 15 connexions ou plus.

L'appliance NetScaler peut également utiliser la méthode de moindre connexion lorsque des poids sont attribués aux services. Il sélectionne un service en utilisant la valeur (Nw) de l'expression suivante :

Nw = (Nombre de transactions actives) * (10000/poids)

L'exemple suivant montre comment l'appliance NetScaler sélectionne un service pour l'équilibrage de

charge en utilisant la méthode de moindre connexion lorsque des poids sont attribués aux services. Dans l'exemple précédent, supposons que Service-HTTP-1 se voit attribuer un poids de 2, Service-HTTP-2 un poids de 3 et Service-HTTP-3 un poids de 4. Les connexions sont transférées comme suit :

- Service-HTTP-3 reçoit le premier car le service ne gère aucune transaction active.

  Remarque : Si les services ne traitent aucune transaction active, l'appliance NetScaler utilise la méthode du round robin indépendamment des pondérations attribuées à chacun des services.

- Service-HTTP-3 reçoit les deuxième, troisième, quatrième, cinquième, sixième et septième demandes car le service a la valeur Nw la plus faible.
- Service-HTTP-1 reçoit la huitième requête. Étant donné que Service-HTTP-1 et Service-HTTP-3 ont désormais la même valeur Nw, l'appliance effectue un équilibrage de charge de manière ronde. Par conséquent, Service-HTTP-3 reçoit la neuvième requête.

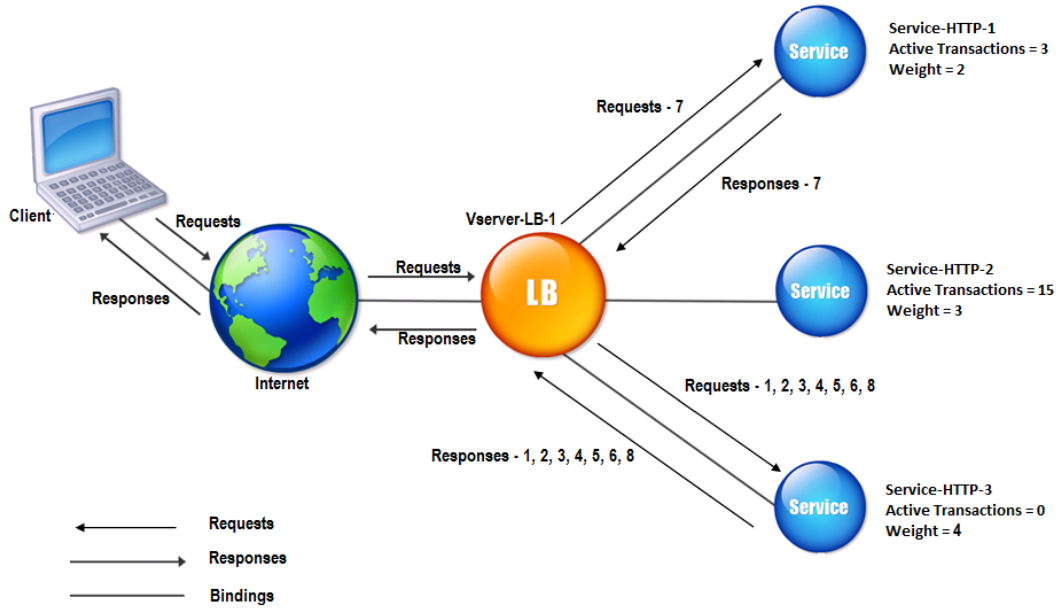
Le tableau suivant explique comment les connexions sont distribuées sur la configuration d'équilibrage de charge à trois services décrite précédemment.

Demande reçue	Service sélectionné	Valeur actuelle Nw (nombre de transactions actives) * (10000/poids)	Remarques
Request-1	Service-HTTP-3 ; (Nouveau = 0)	Nw = 2500	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-2	Service-HTTP-3 ; (Nw = 2500)	Nw = 5000	
Request-3	Service-HTTP-3 ; (Nw = 5000)	Nouveau = 7500	
Request-4	Service-HTTP-3 ; (Nw = 7500)	Nw = 10 000	
Request-5	Service-HTTP-3 ; (Nw = 10000)	Nouveau = 12 500	
Request-6	Service-HTTP-3 ; (Nw = 12500)	Nouveau = 15 000	
Request-7	Service-HTTP-1 ; (Nw = 15000)	Nw = 20 000	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs Nw
Request-8	Service-HTTP-3 ; (Nw = 15000)	Nouveau = 17 500	

Le Service-HTTP-2 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque la valeur Nw des autres services (Service-HTTP-1 et Service-HTTP-3) est égale à 50000.

Le schéma suivant montre comment l'appliance NetScaler utilise la méthode de moindre connexion lorsque des poids sont attribués aux services.

Figure 2. Mécanisme de la méthode d'équilibrage de charge des connexions moindres lorsque des poids sont affectés



Pour configurer la méthode de connexion la plus faible, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode Round Robin

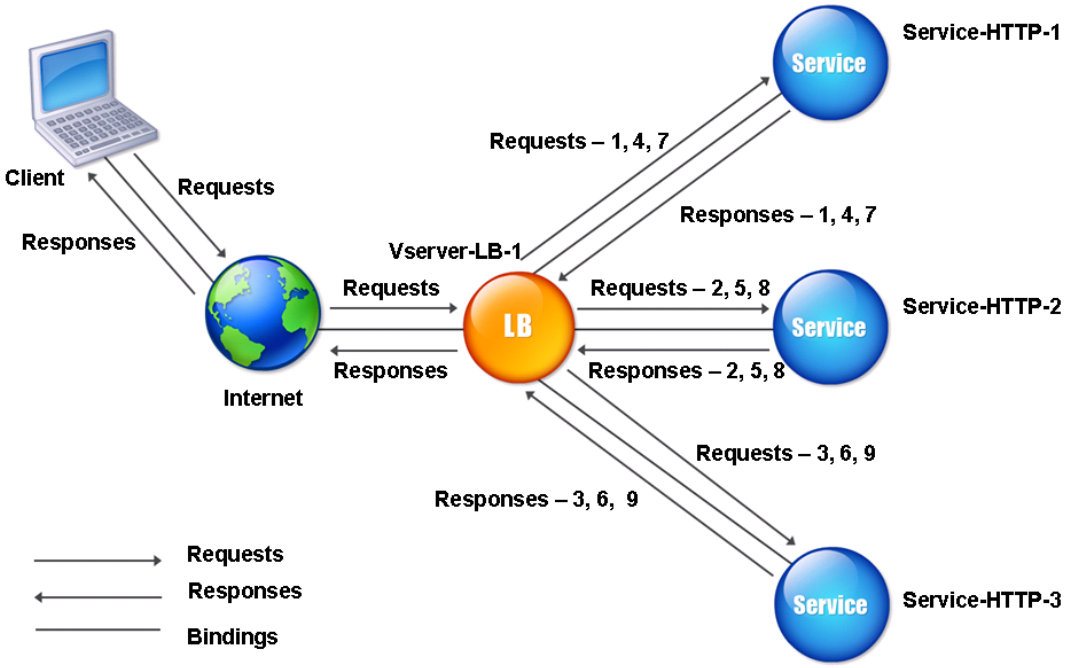
May 5, 2023

Lorsqu'un serveur virtuel d'équilibrage de charge est configuré pour utiliser la méthode circulaire, il fait pivoter en permanence la liste des services qui lui sont liés. Lorsque le serveur virtuel reçoit une demande, il attribue la connexion au premier service de la liste, puis déplace ce service vers le bas de la liste.

Le schéma suivant montre comment l'appliance NetScaler utilise la méthode circulaire avec une configuration d'équilibrage de charge qui contient trois serveurs à équilibrage de charge et leurs services

associés.

Figure 1. Fonctionnement de la méthode d'équilibrage de charge Round Robin



Si vous attribuez une pondération différente à chaque service, l'appliance NetScaler effectue la distribution circulaire pondérée des connexions entrantes. Pour ce faire, il saute les services moins pondérés à des intervalles appropriés.

Supposons, par exemple, que vous disposiez d'une configuration d'équilibrage de charge avec trois services. Vous définissez Service-HTTP-1 sur une pondération de 2, Service-HTTP-2 sur une pondération de 3 et Service-HTTP-3 sur une pondération de 4. Les services sont liés à vServer-LB-1, qui est configuré pour utiliser la méthode Round Robin. Avec cette configuration, les demandes entrantes sont transmises comme suit :

- Service-HTTP-1 reçoit la première demande.
- Service-HTTP-2 reçoit la deuxième demande.
- Service-HTTP-3 reçoit la troisième demande.
- Service-HTTP-1 reçoit la quatrième requête.
- Service-HTTP-2 reçoit la cinquième requête.
- Service-HTTP-3 reçoit la sixième demande.
- Service-HTTP-2 reçoit la septième demande.

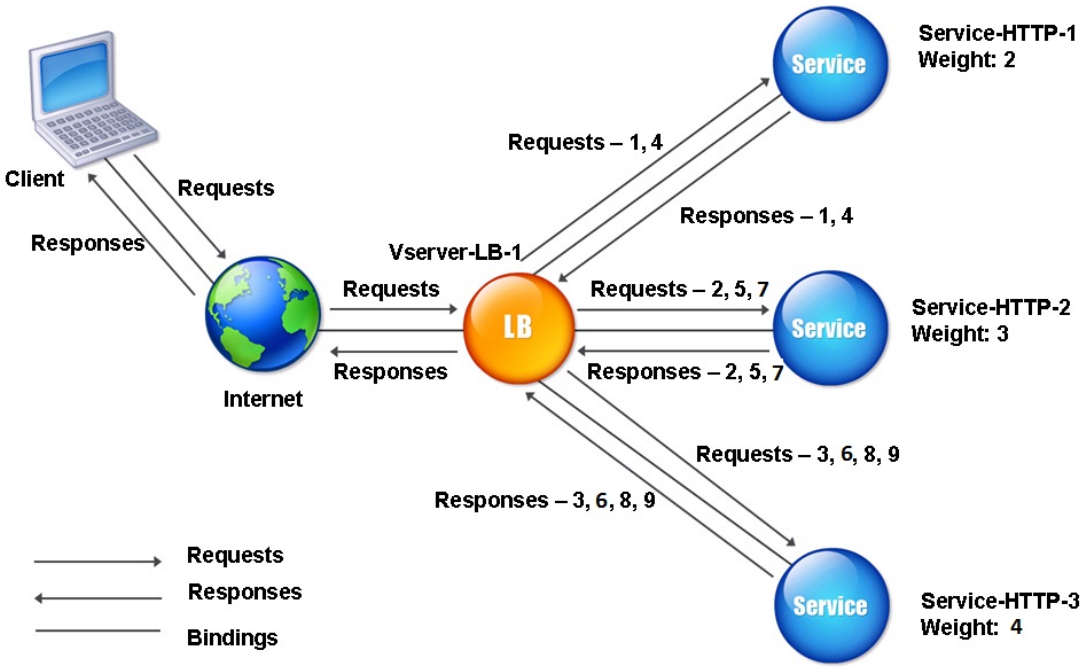
- Service-HTTP-3 reçoit à la fois les huitième et neuvième requêtes.

> **Remarque** :
>
> Vous pouvez également configurer des pondérations pour les services afin d'éviter que plusieurs services n'utilisent le même serveur et ne le surchargent.

Un nouveau cycle commence alors, selon le même schéma.

Le schéma suivant illustre la méthode de sondage à tour pondéré.

Figure 2. Comment la méthode d'équilibrage de charge Round Robin prend en charge les services pondérés



Pour configurer la méthode ronde, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de temps de réponse minimal

May 5, 2023

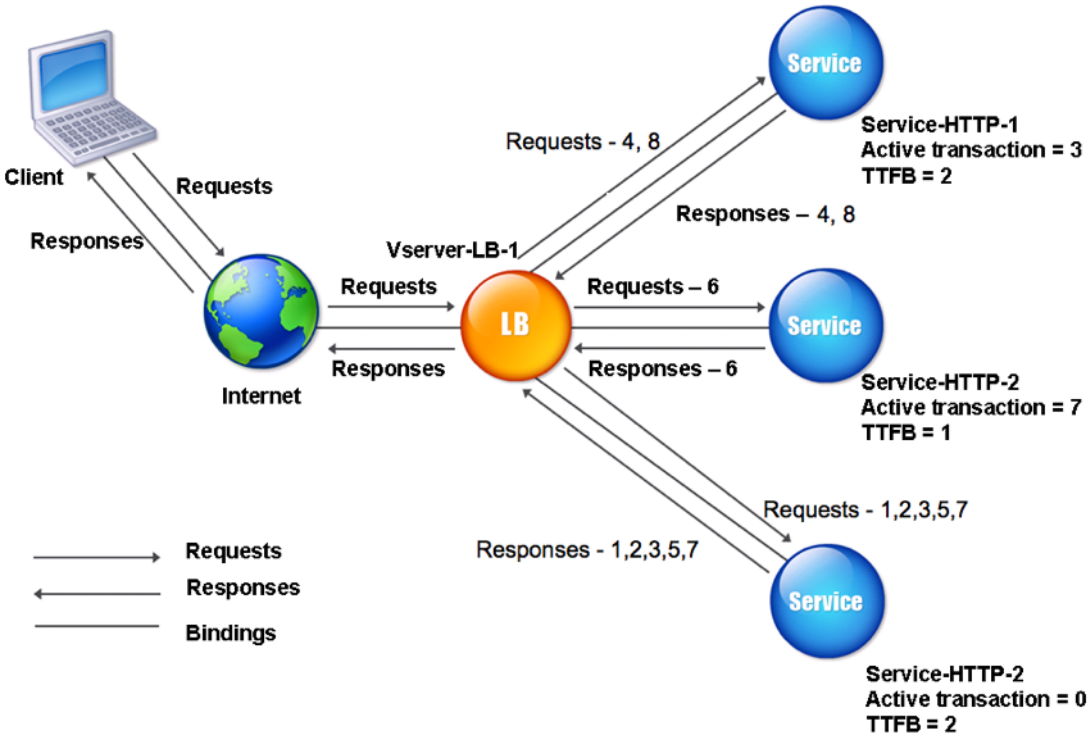
Lorsque le serveur virtuel d'équilibrage de charge est configuré pour utiliser la méthode du temps de réponse le plus court, il sélectionne le service avec le moins de connexions actives et le temps de réponse moyen le plus bas. Vous pouvez configurer cette méthode uniquement pour les serveurs virtuels d'équilibrage de charge HTTP et SSL (Secure Sockets Layer). Le temps de réponse (également appelé Time to First Byte, ou TTFB) est l'intervalle de temps entre l'envoi d'un paquet de demande à un service et la réception du premier paquet de réponse du service. L'appliance NetScaler utilise le code de réponse 200 pour calculer le TTFB.

L'exemple suivant montre comment un serveur virtuel sélectionne un service pour l'équilibrage de charge en utilisant la méthode du temps de réponse le plus court. Prenez en compte les trois services suivants :

- Service-HTTP-1 gère trois transactions actives et TTFB dure deux secondes.
- Service-HTTP-2 gère sept transactions actives et TTFB en une seconde.
- Service-HTTP-3 ne gère aucune transaction active et le TTFB dure deux secondes.

Le schéma suivant montre comment l'appliance NetScaler utilise la méthode du temps de réponse le plus court pour transférer les connexions.

Figure 1. Fonctionnement de la méthode d'équilibrage de charge au moindre temps de réponse



Le serveur virtuel sélectionne un service en multipliant le nombre de transactions actives par le TTFB

pour chaque service, puis en sélectionnant le service avec le résultat le plus bas. Dans l'exemple ci-dessus, le serveur virtuel transmet les demandes comme suit :

- Service-HTTP-3 reçoit la première demande, car le service ne gère aucune transaction active.
- Service-HTTP-3 reçoit également les deuxième et troisième demandes, car le résultat est le plus bas des trois services.
- Service-HTTP-1 reçoit la quatrième requête. Étant donné que Service-HTTP-1 et Service-HTTP-3 obtiennent le même résultat, l'appliance NetScaler choisit entre les deux en appliquant la méthode Round Robin.
- Service-HTTP-3 reçoit la cinquième requête.
- Service-HTTP-2 reçoit la sixième requête car, à ce stade, elle a le résultat le plus faible.
- Étant donné que Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont tous le même résultat à ce stade, l'appliance passe à la méthode round robin et continue à distribuer les connexions à l'aide de cette méthode.

Le tableau suivant explique comment les connexions sont distribuées dans la configuration d'équilibrage de charge à trois services décrite précédemment.

Demande reçue	Service sélectionné	Valeur N actuelle (nombre de transactions actives* TTFB)	Remarques
Request-1	Service-HTTP-3 ; (N = 0)	N = 2	Service-HTTP-3 a la valeur N la plus faible.
Request-2	Service-HTTP-3 ; (N = 2)	N = 4	Service-HTTP-3 a la valeur N la plus faible.
Request-3	Service-HTTP-3 ; (N = 4)	N = 6	Service-HTTP-3 a la valeur N la plus faible.
Request-4	Service-HTTP-1 ; (N = 6)	N = 8	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N. L'appliance utilise la méthode Round Robin pour distribuer les demandes.
Request-5	Service-HTTP-3 ; (N = 6)	N = 8	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-6	Service-HTTP-2 ; (N = 7)	N = 8	Service-HTTP-2 a la valeur N la plus faible.

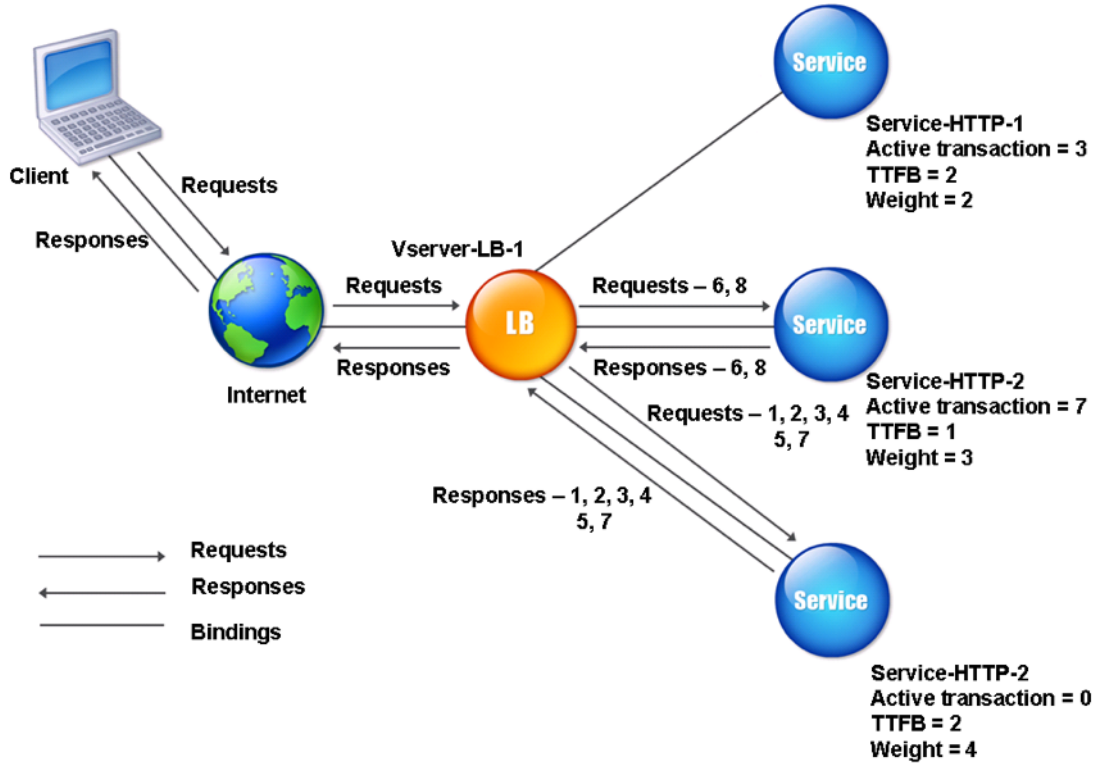
Demande reçue	Service sélectionné	Valeur N actuelle (nombre de transactions actives* TTFB)	Remarques
Request-7	Service-HTTP-3 ; (N = 8)	N = 10	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N. L'appliance NetScaler utilise la méthode Round Robin pour distribuer les demandes.
Request-8	Service-HTTP-1 ; (N = 8)	N = 10	Service-HTTP-1 et Service-HTTP-2 ont les mêmes valeurs N ; l'appliance utilise la méthode circulaire pour distribuer les demandes.

Le Service-HTTP-1 est à nouveau sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque sa valeur N est inférieure à celle des autres services (Service-HTTP-2 et Service-HTTP-3).

Sélection des services lors de l'attribution de poids

Le schéma suivant montre comment l'appliance NetScaler utilise la méthode du temps de réponse le plus court lorsque des poids sont attribués.

Figure 2. Fonctionnement de la méthode d'équilibrage de charge du temps de réponse le moins important lorsque des poids sont affectés



Le serveur virtuel sélectionne un service en utilisant la valeur (Nw) dans l'expression suivante :

Nw = (N) ⋆ (10000/poids), où N = (nombre de transactions actives ⋆ TTFB)

Supposons que Service-HTTP-1 se voit attribuer un poids de 2, Service-HTTP-2 un poids de 3 et Service-HTTP-3 un poids de 4.

L'appliance NetScaler distribue les demandes comme suit :

- Service-HTTP-3 reçoit la première requête, car il ne gère aucune transaction active.

  Si les services ne gèrent aucune transaction active, l'appliance les sélectionne indépendamment des poids qui leur sont attribués.
- Service-HTTP-3 reçoit les deuxième, troisième, quatrième et cinquième requêtes, car ce service a la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la sixième demande, car ce service possède la valeur Nw la plus faible.
- Service-HTTP-3 reçoit la septième requête, car ce service possède la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la huitième requête, car ce service possède la valeur Nw la plus faible.

Service-HTTP-1 a le poids le plus faible et donc la valeur Nw la plus élevée, de sorte que le serveur virtuel ne le sélectionne pas pour l'équilibrage de charge.

Le tableau suivant explique comment les connexions sont distribuées dans la configuration d'équilibrage de charge à trois services décrite précédemment.

Demande reçue	Service sélectionné	Nouvelle valeur actuelle = (N) * (10000/poids)	Remarques
Request-1	Service-HTTP-3 ; (Nouveau = 0)	Nw = 5000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-2	Service-HTTP-3 ; (Nw = 5000)	Nw = 10 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-3	Service-HTTP-3 ; (Nw = 10000)	Nouveau = 15 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-4	Service-HTTP-3 ; (Nw = 15000)	Nw = 20 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-5	Service-HTTP-3 ; (Nouveau = 20 000)	Nw = 25 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-6	Service-HTTP-2 ; (Nw = 23333,34)	Nouveau = 2666,67	Service-HTTP-2 possède la valeur Nw la plus faible.
Request-7	Service-HTTP-3 ; (Nw = 25 000)	Nw = 30 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-8	Service-HTTP-2 ; (Nw = 26666,67)	Nw = 30 000	Service-HTTP-2 possède la valeur Nw la plus faible.

Le Service-HTTP-1 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque sa valeur Nw est inférieure à celle des autres services (Service-HTTP-2 et Service-HTTP-3).

Pour configurer la méthode d'équilibrage de charge avec le temps de réponse le plus court à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
set lb vserver <name> -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```

Pour configurer la méthode d'équilibrage de charge avec le temps de réponse le plus court à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **LEASTRESPONSETIME**.

Pour plus d'informations sur la configuration des moniteurs, voir Configuration des moniteurs dans une configuration d'équilibrage de charge.

Méthode LRTM

May 5, 2023

Remarque : LRTM est l'abréviation de Least Response Time Method using monitor (LRTM).

Lorsqu'un serveur virtuel d'équilibrage de charge est configuré pour utiliser la méthode LRTM, il utilise l'infrastructure de surveillance existante pour obtenir le temps de réponse le plus rapide. Le serveur virtuel d'équilibrage de charge sélectionne ensuite le service présentant le plus petit nombre de transactions actives et le temps de réponse le plus faible. Avant d'utiliser la méthode LRTM, vous devez lier des moniteurs spécifiques à l'application à chaque service et activer le mode LRTM sur ces moniteurs. L'appliance NetScaler prend ensuite des décisions d'équilibrage de charge en fonction des temps de réponse qu'elle calcule à partir des sondes de surveillance.

Vous pouvez également utiliser la méthode LRTM pour équilibrer la charge des services non HTTP et non HTTPS. Vous pouvez également utiliser cette méthode lorsque plusieurs moniteurs sont liés à un service. Chaque moniteur détermine le temps de réponse en utilisant le protocole qu'il mesure pour le service auquel il est lié. Le serveur virtuel calcule ensuite un temps de réponse moyen pour ce service en calculant la moyenne des résultats.

Le tableau suivant résume comment les temps de réponse sont calculés pour les différents moniteurs.

Surveiller	Calcul du temps de réponse
PING	Différence de temps entre la demande ICMP ECHO et la réponse ICMP ECHO.
TCP	Différence de temps entre la demande SYN et la réponse SYN+ACK.
HTTP	Décalage horaire entre la requête HTTP (après l'établissement de la connexion TCP) et la réponse HTTP.
TCP-ECV	Différence de temps entre le moment où la chaîne d'envoi des données est envoyée et la chaîne de réception des données est renvoyée. Un moniteur TCP-ECV sans chaînes d'envoi et de réception est considéré comme ayant une configuration incorrecte.
HTTP-ECV	Décalage horaire entre la requête HTTP et la réponse HTTP.
UDP-ECV	Décalage horaire entre la chaîne d'envoi de l'UDP et la chaîne de réception. Un moniteur UDP-ECV sans chaîne de réception est considéré comme ayant une configuration incorrecte.
DNS	Décalage horaire entre une requête DNS et la réponse DNS.
TCPS	Décalage horaire entre une demande SYN et la fin de l'établissement de connexion SSL.
FTP	Décalage horaire entre l'envoi du nom d'utilisateur et la fin de l'authentification de l'utilisateur.
HTTPS (surveille les demandes HTTPS)	Le décalage horaire est le même que pour le moniteur HTTP.
HTTS-ECV (surveille les requêtes HTTPS)	Le décalage horaire est le même que pour le moniteur HTTP-ECV

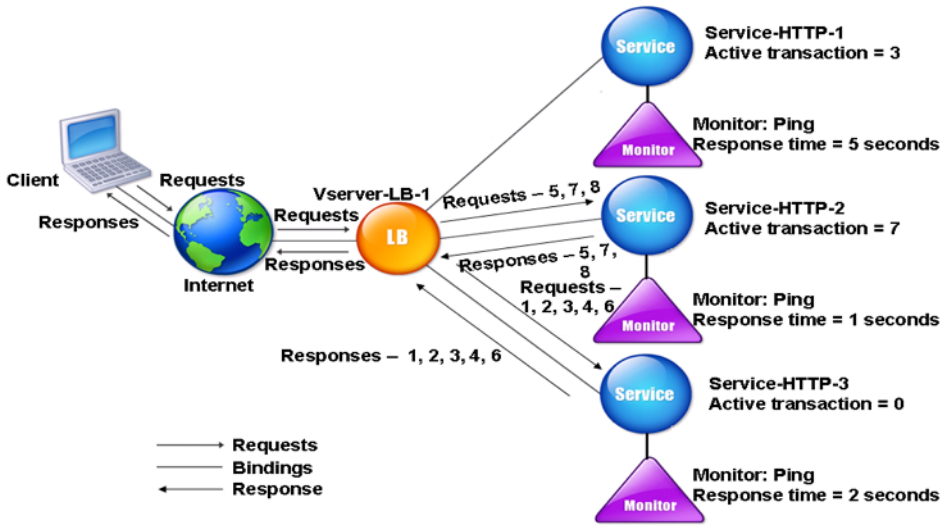
Surveiller	Calcul du temps de réponse
USER	Décalage horaire entre l'heure à laquelle une demande est envoyée au répartiteur et l'heure à laquelle la réponse du répartiteur est reçue.

L'exemple suivant montre comment l'appliance NetScaler sélectionne un service pour l'équilibrage de charge à l'aide de la méthode LRTM. Prenez en compte les trois services suivants :

- Service-HTTP-1 gère 3 transactions actives et le temps de réponse est de cinq secondes.
- Service-HTTP-2 gère 7 transactions actives et le temps de réponse est d'une seconde.
- Service-HTTP-3 ne gère aucune transaction active et le temps de réponse est de deux secondes.

Le schéma suivant illustre le processus suivi par l'appliance NetScaler lorsqu'elle transmet des demandes.

Figure 1. Fonctionnement de la méthode LRTM



Le serveur virtuel sélectionne un service en utilisant la valeur (N) dans l'expression suivante :

N = (Nombre de transactions actives* Temps de réponse déterminé par le moniteur)

Le serveur virtuel envoie les demandes comme suit :

- Service-HTTP-3 reçoit la première demande, car ce service ne gère aucune transaction active.
- Service-HTTP-3 reçoit les deuxième, troisième et quatrième requêtes, car ce service possède la valeur N la plus faible.

- Service-HTTP-2 reçoit la cinquième requête, car ce service a la valeur N la plus faible.
- Étant donné que Service-HTTP-2 et Service-HTTP-3 ont actuellement la même valeur N, l'appliance NetScaler passe à la méthode round robin. Par conséquent, Service-HTTP-3 reçoit la sixième demande.
- Service-HTTP-2 reçoit les septième et huitième requêtes, car ce service a la valeur N la plus faible.

Le service-HTTP-1 n'est pas pris en compte pour l'équilibrage de charge, car il est plus chargé (possède la valeur N la plus élevée) par rapport aux deux autres services. Toutefois, si Service-HTTP-1 termine ses transactions actives, l'appliance NetScaler considère à nouveau ce service pour l'équilibrage de charge.

Le tableau suivant résume la façon dont N est calculé pour les services.

Demande reçue	Service sélectionné	Valeur N actuelle (nombre de transactions actives* TTFB)	Remarques
Request-1	Service-HTTP-3 ; (N = 0)	N = 2	Service-HTTP-3 a la valeur N la plus faible.
Request-2	Service-HTTP-3 ; (N = 2)	N = 4	Service-HTTP-3 a la valeur N la plus faible.
Request-3	Service-HTTP-3 ; (N = 4)	N = 6	Service-HTTP-3 a la valeur N la plus faible.
Request-4	Service-HTTP-3 ; (N = 6)	N = 8	Service-HTTP-3 a la valeur N la plus faible.
Request-5	Service-HTTP-2 ; (N = 7)	N = 8	Service-HTTP-2 a la valeur N la plus faible.
Request-6	Service-HTTP-3 ; (N = 8)	N = 10	Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N. L'appliance NetScaler passe à la méthode Round Robin et sélectionne Service-HTTP-3
Request-7	Service-HTTP-2 ; (N = 8)	N = 9	Service-HTTP-2 a la valeur N la plus faible.

Demande reçue	Service sélectionné	Valeur N actuelle (nombre de transactions actives* TTFB)	Remarques
Request-8	Service-HTTP-2 ; (N = 9)	N = 10	Service-HTTP-2 a la valeur N la plus faible.

Le Service-HTTP-1 est à nouveau sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque sa valeur N est inférieure à celle des autres services (Service-HTTP-2 et Service-HTTP-3).

Sélection des services lors de l'attribution de poids

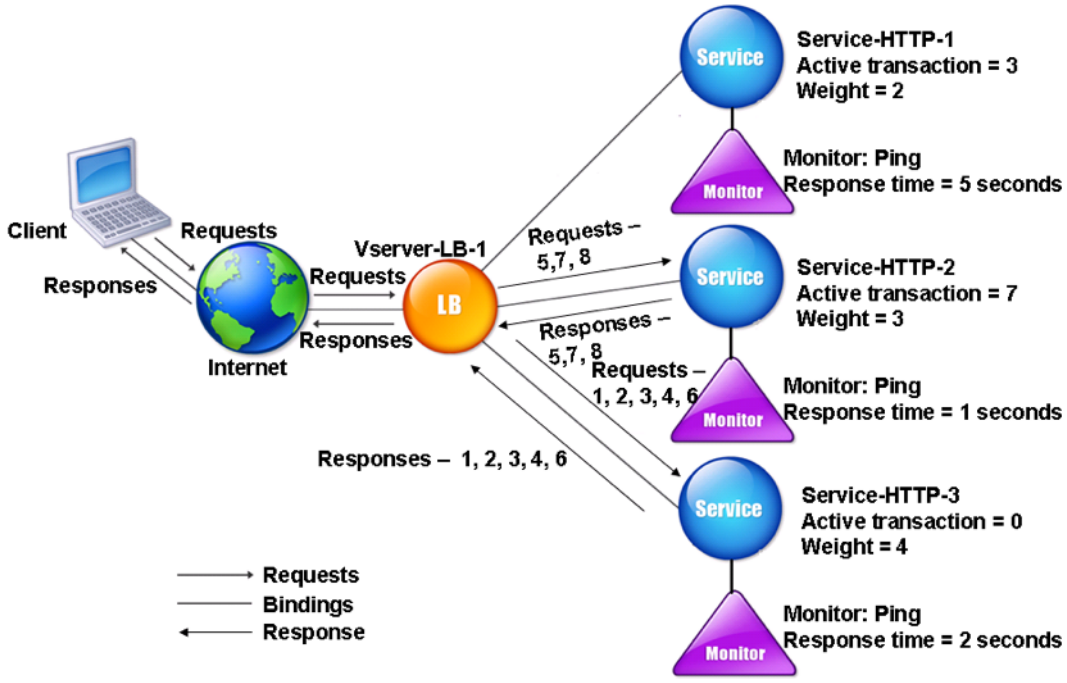
L'appliance NetScaler effectue également un équilibrage de charge en utilisant le nombre de transactions actives, le temps de réponse et les poids si différents poids sont attribués aux services. L'appliance NetScaler sélectionne le service à l'aide de la valeur (Nw) de l'expression suivante :

Nw = (N) * (10 000/poids)

Où N = (Nombre de transactions actives* Temps de réponse déterminé par le moniteur)

Le schéma suivant montre comment le serveur virtuel utilise la méthode LRTM lorsque des poids sont attribués.

Figure 2. Fonctionnement de la méthode d'équilibrage de charge du temps de réponse le moins important lorsque des poids sont affectés



Dans cet exemple, supposons que Service-HTTP-1 se voit attribuer un poids de 2, Service-HTTP-2 se voit attribuer un poids de 3 et Service-HTTP-3 un poids de 4.

L'appliance NetScaler fournit les demandes comme suit :

- Service-HTTP-3 reçoit la première requête, car il ne gère aucune transaction active.
- Service-HTTP-3 reçoit les deuxième, troisième, quatrième et cinquième requêtes, car ce service a la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la sixième demande, car ce service possède la valeur Nw la plus faible.
- Service-HTTP-3 reçoit la septième requête, car ce service possède la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la huitième requête, car ce service possède la valeur Nw la plus faible.

Le Service-HTTP-1 a le poids le plus faible et la valeur Nw la plus élevée. L'appliance NetScaler ne le sélectionne donc pas pour l'équilibrage de charge.

Le tableau suivant résume la façon dont Nw est calculé pour différents moniteurs.

Demande reçue	Service sélectionné	Nouvelle valeur actuelle (N) * (10000/poids)	Remarques
Request-1	Service-HTTP-3 ; (Nouveau = 0)	Nw = 5000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-2	Service-HTTP-3 ; (Nw = 5000)	Nw = 10 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-3	Service-HTTP-3 ; (Nw = 10000)	Nouveau = 15 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-4	Service-HTTP-3 ; (Nw = 15000)	Nw = 20 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-5	Service-HTTP-3 ; (Nouveau = 20 000)	Nw = 25 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-6	Service-HTTP-2 ; (Nw = 23333,34)	Nouveau = 2666,67	Service-HTTP-2 possède la valeur Nw la plus faible.
Request-7	Service-HTTP-3 ; (Nw = 25 000)	Nw = 30 000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-8	Service-HTTP-2 ; (Nw = 26666,67)	Nw = 30 000	Service-HTTP-2 possède la valeur Nw la plus faible.

Le Service-HTTP-1 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque sa valeur Nw est inférieure à celle des autres services (Service-HTTP-2 et Service-HTTP-3).

Pour configurer la méthode d'équilibrage de charge LRTM à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;


```
set lb vserver <name> [-lbMethod <lbMethod>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod LRTM
<!--NeedCopy-->
```

Pour configurer la méthode d'équilibrage de charge LRTM à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **LRTM**.

Pour activer l'option LRTM dans les moniteurs à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
set lb monitor <monitorName> <type> [-LRTM ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Exemple :

```
set lb monitor monitor-HTTP-1 HTTP -LRTM ENABLED
<!--NeedCopy-->
```

Pour activer l'option LRTM sur les moniteurs à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**, puis ouvrez un moniteur.
2. Dans Paramètres avancés, sélectionnez **LRTM (Temps de réponse minimum à l'aide de la surveillance)**.

Pour plus d'informations sur la configuration des moniteurs, voir Configuration des moniteurs dans une configuration d'équilibrage de charge.

Méthodes de hachage

May 5, 2023

Les méthodes d'équilibrage de charge basées sur le hachage de certaines informations de connexion ou d'en-tête constituent la plupart des méthodes d'équilibrage de charge de l'appliance NetScaler. Les hachages sont plus courts et plus faciles à utiliser que les informations sur lesquelles ils sont basés, tout en conservant suffisamment d'informations pour s'assurer qu'aucun élément d'information différent ne génère le même hachage et sont donc confondus les uns avec les autres.

Vous pouvez utiliser les méthodes d'équilibrage de charge de hachage dans un environnement où un cache sert une large gamme de contenu provenant d'Internet ou de serveurs d'origine spécifiés. La mise en cache des demandes réduit la latence des demandes et des réponses et garantit une meilleure utilisation des ressources (CPU), rendant la mise en cache populaire sur les sites Web et serveurs d'applications très utilisés. Comme ces sites bénéficient également de l'équilibrage de charge, les méthodes d'équilibrage de charge de hachage sont largement utiles.

L'appliance NetScaler fournit les méthodes de hachage suivantes :

- Méthode de hachage d'URL
- Méthode de hachage du domaine
- Méthode de hachage IP de destination
- Méthode de hachage de l'adresse IP source
- Méthode de hachage IP source et adresse IP de destination
- Méthode de hachage du port source IP source
- Méthode de hachage de l'ID d'appel
- Méthode de jeton

La plupart des algorithmes de hachage calculent deux valeurs de hachage :

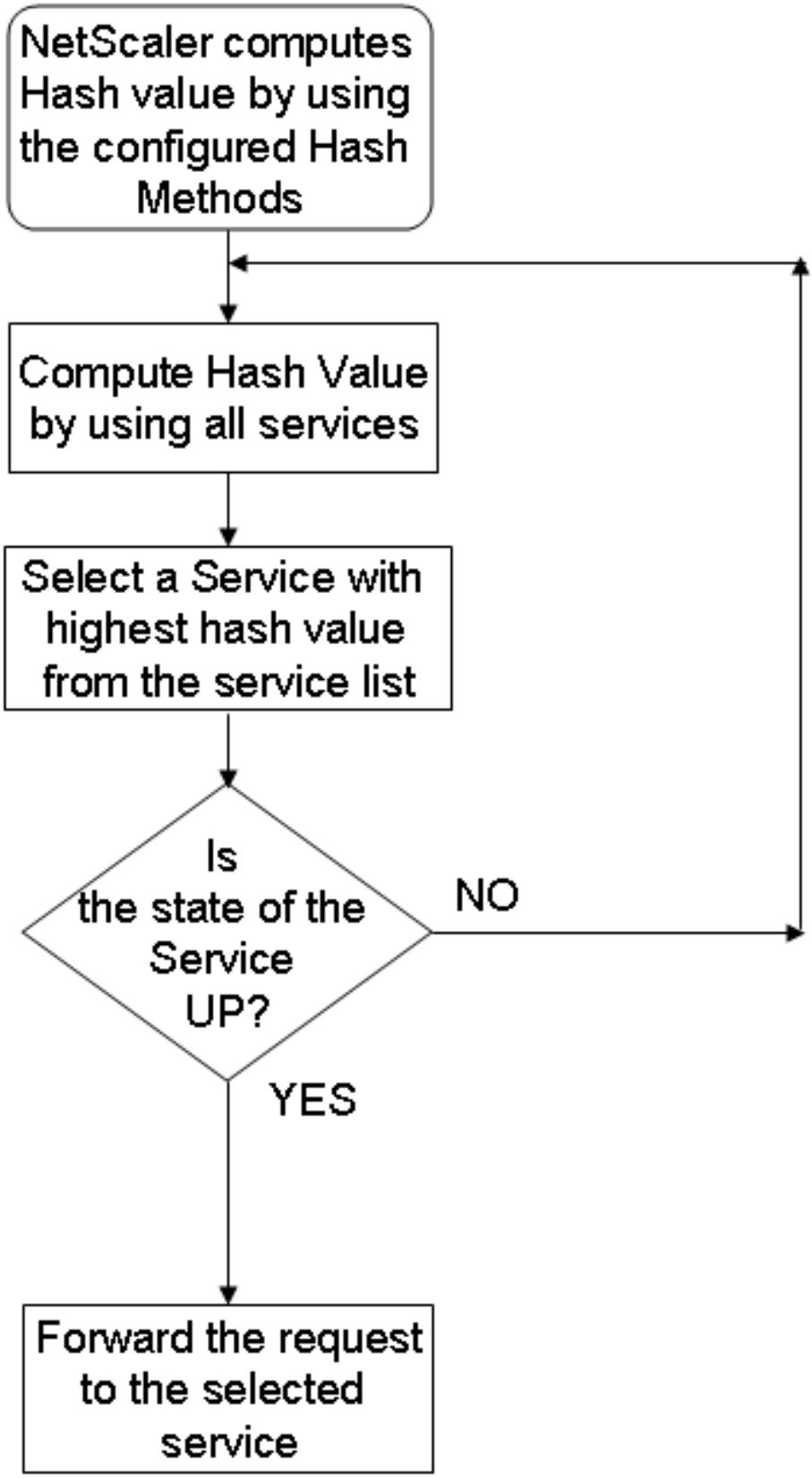
- Un hachage de l'adresse IP et du port du service.
- Un hachage de l'URL entrante, du nom de domaine, de l'adresse IP source, de l'adresse IP de destination ou des adresses IP source et de destination, selon la méthode de hachage configurée.

L'appliance NetScaler génère ensuite une nouvelle valeur de hachage en utilisant ces deux valeurs de hachage. Enfin, il transmet la demande au service ayant la valeur de hachage la plus élevée. Lorsque l'appliance calcule une valeur de hachage pour chaque demande et sélectionne le service qui traite la demande, il remplit un cache. Les requêtes suivantes avec la même valeur de hachage sont envoyées au même service. L'organigramme suivant illustre ce processus.

> Remarque
>
> À partir de la version 13.0 build 79.x de NetScaler, les algorithmes de hachage cohérents Prime Re-Shuffled Assisted CARP (PRAC) et Jump table Assisted Ring Hash (JARH) sont pris en charge. Les algorithmes de hachage cohérents garantissent une interruption minimale lorsque des services sont ajoutés ou supprimés de votre configuration d'équilibrage de charge, ou lors d'un événement de clapet de service dans la configuration d'équilibrage de charge. Pour plus de détails,

> voir Algorithmes de hachage cohérents.

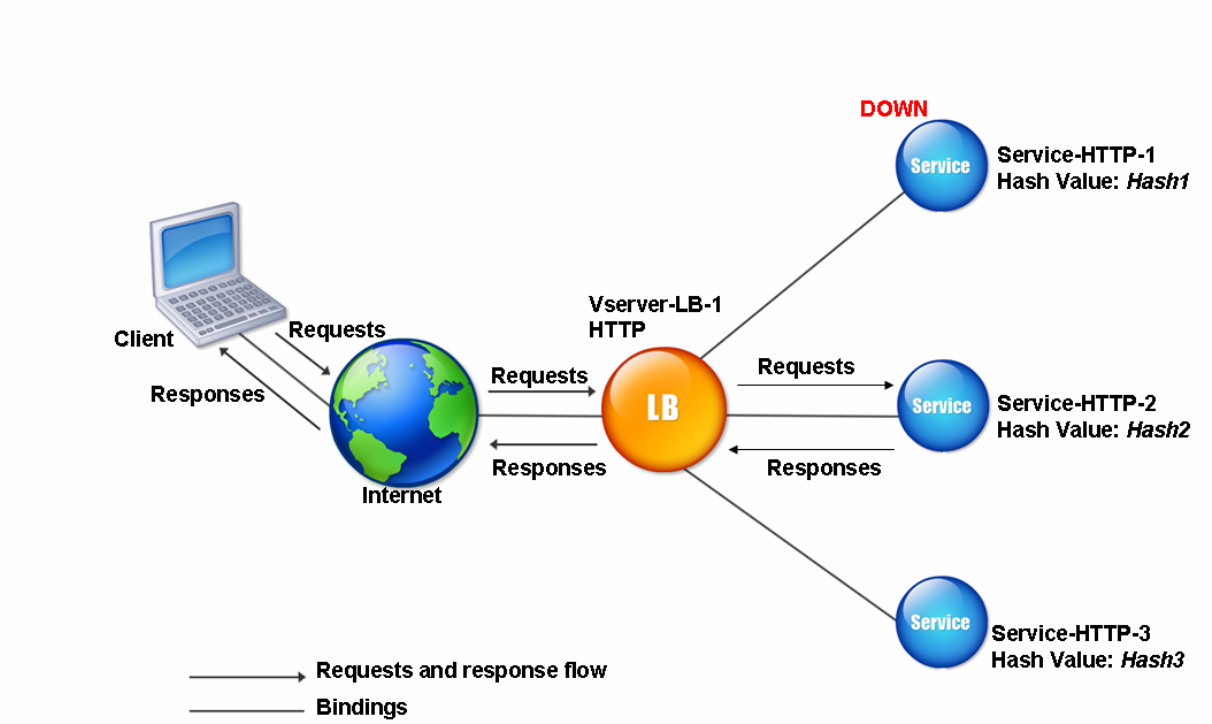
Figure 1. Comment les méthodes de hachage distribuent les demandes



Les méthodes de hachage peuvent être appliquées aux adresses IPv4 et IPv6.

Imaginons un scénario dans lequel trois services (Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3) sont liés à un serveur virtuel, n'importe quelle méthode de hachage est configurée et la valeur de hachage est Hash1. Lorsque les services configurés sont actifs, la demande est envoyée à Service-HTTP-1. Si Service-HTTP-1 est hors service, l'appliance NetScaler calcule la valeur de hachage du dernier journal du nombre de services. L'appliance sélectionne ensuite le service dont la valeur de hachage est la plus élevée, tel que Service-HTTP-2. Le schéma suivant illustre ce processus.

Figure 2. Modèle d'entité pour les méthodes de hachage



> Remarque
>
> Si l'appliance NetScaler ne parvient pas à sélectionner un service à l'aide d'une méthode de hachage, elle utilise par défaut la méthode de moindre connexion pour sélectionner un service pour la demande entrante. Ajustez les pools de serveurs en supprimant les services pendant les périodes de faible trafic pour permettre aux caches de se repeupler sans affecter les performances de votre configuration d'équilibrage de charge.

Algorithmes de hachage cohérents

Les algorithmes de hachage cohérents sont utilisés pour obtenir une persistance sans état. Les méthodes LB basées sur le hachage utilisent l'un des trois algorithmes de hachage cohérents suivants :

- **Cache Array Routing Protocol (CARP)**

L'algorithme CARP est utilisé dans l'équilibrage de charge des requêtes HTTP sur plusieurs serveurs de cache proxy. Cet algorithme est activé par défaut.

- **Prime Re-Shuffled Assisted CARP (PRAC)**

  L'appliance NetScaler utilise l'algorithme propriétaire PRAC pour fournir une distribution uniforme du trafic.

- **Jump table Assisted Ring Hash (JARH)**

  L'appliance NetScaler utilise l'algorithme propriétaire JARH pour assurer la cohérence et la distribution uniforme du trafic. Cet algorithme utilise des doigts de hachage. Un nombre plus élevé de doigts permet une meilleure répartition du trafic. Cependant, l'augmentation du nombre de doigts augmente également l'utilisation de la mémoire.

Pour choisir l'algorithme de hachage cohérent à l'aide de l'interface de ligne de commande

```
set lb parameter [-lbHashAlgorithm [DEFAULT|JARH|PRAC] [-lbHashFingers
   <positive_integer>]
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -lbHashAlgorithm JARH -lbHashFingers 10
<!--NeedCopy-->
```

ARGUMENTS :

- **lbHashAlgorithm**-Spécifiez l'algorithme de hachage à utiliser pour les méthodes d'équilibrage de charge basées sur le hachage suivantes :
  - Méthode de hachage d'URL
  - Méthode de hachage du domaine
  - Méthode de hachage IP de destination
  - Méthode de hachage de l'adresse IP source
  - Méthode de hachage IP source et adresse IP de destination
  - Méthode de hachage du port source IP source
  - Méthode de hachage de l'ID d'appel
  - Méthode de jeton

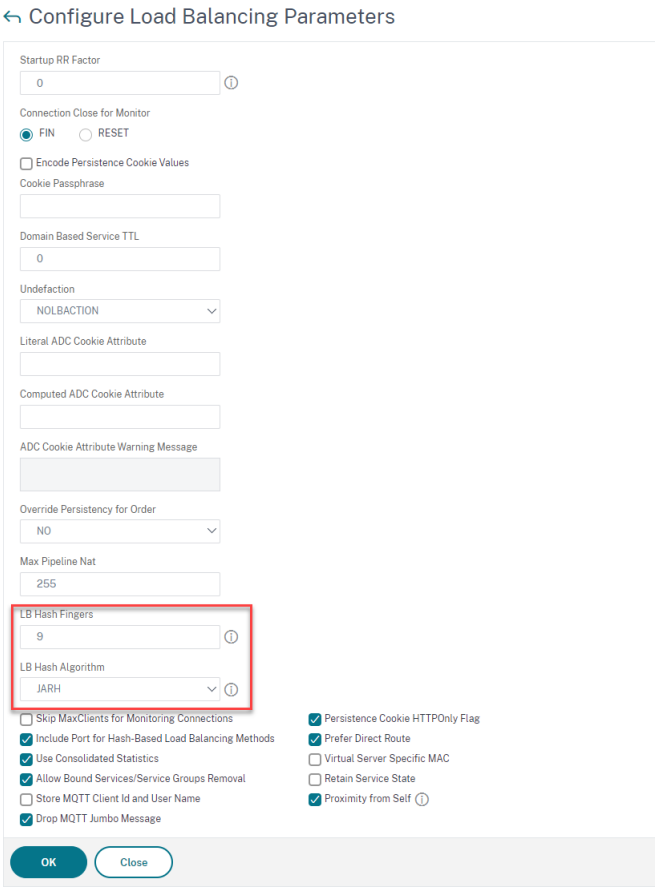
  Valeurs possibles : DEFAULT, PRAC, JARH Valeur
  par défaut : DEFAULT

- **LBHashFingers**-Spécifiez le nombre de doigts à utiliser dans les algorithmes PRAC et JARH pour les méthodes LB basées sur le hachage. L'augmentation du nombre de doigts permet une meilleure répartition du trafic au détriment de la mémoire supplémentaire.

Valeur par défaut : 256 Valeur
minimale : 1 Valeur
maximale : 1024

Pour choisir l'algorithme de hachage cohérent à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Modifier les paramètres d'équilibrage de charge**.
2. Dans le volet **Configurer les paramètres d'équilibrage de charge**, entrez les valeurs appropriées pour les champs suivants en fonction de vos besoins :
   - doigts de hachage LB
   - Dans le champ **Algorithme de hachage LB**, choisissez l'algorithme de hachage cohérent dans le menu déroulant.



La méthode de hachage de l'URL

Lorsque vous configurez l'appliance NetScaler pour utiliser la méthode de hachage d'URL pour équilibrer la charge des services, pour sélectionner un service, l'appliance génère une valeur de hachage de

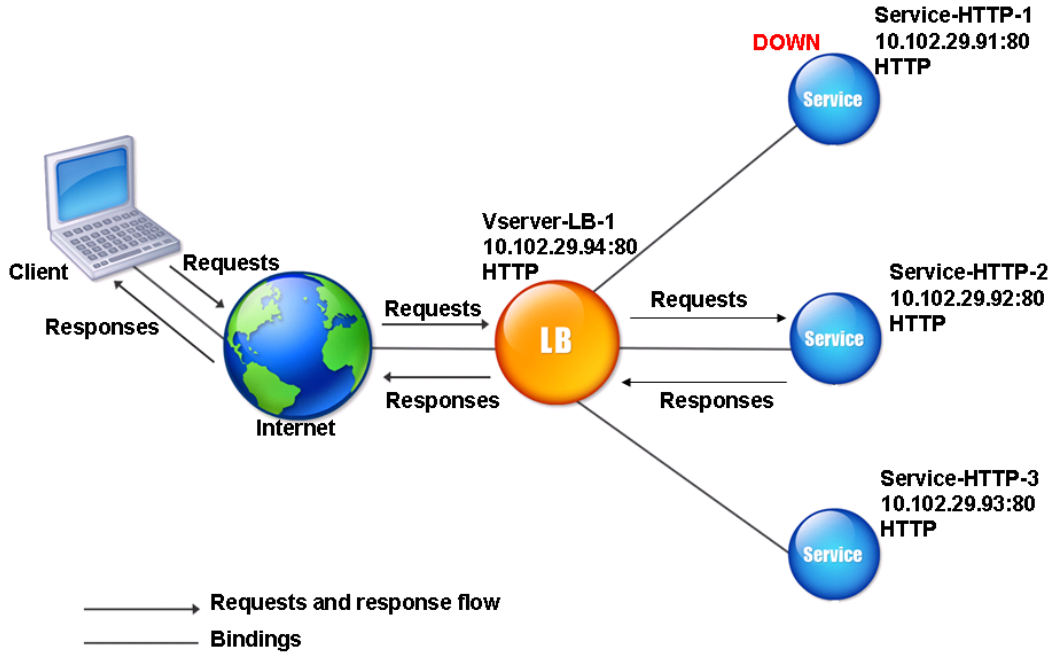
l'URL HTTP présente dans la demande entrante. Si le service sélectionné par la valeur de hachage est DOWN, l'algorithme dispose d'une méthode pour sélectionner un autre service dans la liste des services actifs. L'appliance met en cache la valeur hachée de l'URL et, lorsqu'elle reçoit des demandes ultérieures utilisant la même URL, elle les transmet au même service. Si l'appliance ne parvient pas à analyser une demande entrante, elle utilise la méthode Round Robin pour l'équilibrage de charge au lieu de la méthode de hachage d'URL.

Pour générer la valeur de hachage, l'appliance utilise un algorithme spécifique et prend en compte une partie de l'URL. Par défaut, l'appliance prend en compte les 80 premiers octets de l'URL. Si l'URL est inférieure à 80 octets, c'est l'URL complète qui est utilisée. Vous pouvez spécifier une longueur différente. La longueur de hachage peut aller de 1 octet à 4096 octets. En règle générale, si des URL longues sont utilisées lorsque seuls quelques caractères sont différents, il est judicieux de rendre la longueur de hachage la plus élevée possible afin d'assurer une répartition plus uniforme de la charge.

Considérons un scénario dans lequel trois services, Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3, sont liés à un serveur virtuel, et la méthode d'équilibrage de charge configurée sur le serveur virtuel est la méthode de hachage URL. Le serveur virtuel reçoit une demande et la valeur de hachage de l'URL est U1. L'appliance sélectionne Service-HTTP-1. Si Service-HTTP-1 est DOWN, l'appliance sélectionne Service-HTTP-2.

Le schéma suivant illustre ce processus.

Figure 3. Comment fonctionne le hachage d'URL



Si Service-HTTP-1 et Service-HTTP-2 sont tous deux en panne, l'appliance envoie les demandes avec la valeur de hachage U1 à Service-HTTP-3.

Si Service-HTTP-1 et Service-HTTP-2 sont en panne, les requêtes qui génèrent l'URL1 de hachage sont envoyées à Service-HTTP-3. Si ces services sont UP, les demandes qui génèrent l'URL de hachage 1 sont distribuées de la manière suivante :

- Si le Service-HTTP-2 est en service, la demande est envoyée à Service-HTTP-2.
- Si le Service-HTTP-1 est actif, la demande est envoyée à Service-HTTP-1.
- Si Service-HTTP-1 et Service-HTTP-2 sont mis en service en même temps, la demande est envoyée à Service-HTTP-1.

Pour configurer la méthode de hachage d'URL, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie. Sélectionnez la méthode d'équilibrage de charge en tant qu'URL Hash et définissez la longueur de hachage sur le nombre d'octets à utiliser pour générer la valeur de hachage.

La méthode de hachage du domaine

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage de domaine utilise la valeur hachée du nom de domaine dans la requête HTTP pour sélectionner un service. Le

nom de domaine est extrait de l'URL entrante ou de l'en-tête Host de la requête HTTP. Si le nom de domaine apparaît à la fois dans l'URL et dans l'en-tête Host, l'appliance donne la préférence à l'URL.

Si vous configurez le hachage d'un nom de domaine et qu'une requête HTTP entrante ne contient aucun nom de domaine, l'appliance NetScaler utilise par défaut la méthode round robin pour cette demande.

Le calcul de la valeur de hachage utilise la longueur du nom ou la valeur de longueur de hachage, la valeur la plus petite étant retenue. Par défaut, l'appliance NetScaler calcule la valeur de hachage à partir des 80 premiers octets du nom de domaine. Pour spécifier un nombre différent d'octets dans le nom de domaine lors du calcul de la valeur de hachage, vous pouvez définir le paramètre hash-Length (longueur de hachage dans l'utilitaire de configuration) sur une valeur comprise entre 1 et 4096 (octets).

Pour configurer la méthode de hachage de domaine, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de hachage IP de destination

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage IP de destination utilise la valeur hachée de l'adresse IP de destination pour sélectionner un serveur. Vous pouvez masquer l'adresse IP de destination pour spécifier la partie de celle-ci à utiliser dans le calcul de la valeur de hachage, de sorte que les demandes provenant de réseaux différents mais destinées au même sous-réseau soient toutes dirigées vers le même serveur. Cette méthode prend en charge les serveurs de destination IPv4 et IPv6.

Cette méthode d'équilibrage de charge convient à une utilisation avec la fonctionnalité de redirection du cache.

Pour configurer la méthode de hachage IP de destination pour un serveur de destination IPv4, vous devez définir le paramètre NetMask. Pour configurer cette méthode pour un serveur de destination IPv6, vous devez utiliser le paramètre V6NetMasklen. Dans l'utilitaire de configuration, les zones de texte permettant de définir ces paramètres apparaissent lorsque vous sélectionnez la **méthode de hachage IP de destination**.

Pour configurer la méthode de hachage IP de destination, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

La méthode de hachage IP source

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage IP source utilise la valeur hachée de l'adresse IPv4 ou IPv6 du client pour sélectionner un service. Pour diriger toutes les demandes provenant d'adresses IP source appartenant à un réseau particulier vers un

serveur de destination spécifique, vous devez masquer l'adresse IP source. Pour les adresses IPv4, utilisez le paramètre NetMask. Pour les adresses IPv6, utilisez le paramètre V6NetMaskLength.

Pour configurer la méthode de hachage IP source, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de hachage IP de destination IP source

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage IP de destination IP source utilise la valeur hachée des adresses IP source et destination (IPv4 ou IPv6) pour sélectionner un service. Le hachage est symétrique. La valeur de hachage est la même quel que soit l'ordre des adresses IP source et de destination. Cela garantit que tous les paquets circulant d'un client particulier vers la même destination sont dirigés vers le même serveur.

Pour diriger toutes les demandes appartenant à un réseau particulier vers un serveur de destination spécifique, vous devez masquer l'adresse IP source. Pour les adresses IPv4, utilisez le paramètre NetMask. Pour les adresses IPv6, utilisez le paramètre V6NetMaskLength.

Pour configurer la méthode de hachage IP de destination IP source, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de hachage du port source IP source

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage du port source IP source utilise la valeur de hachage de l'IP source (IPv4 ou IPv6) et du port source pour sélectionner un service. Cela garantit que tous les paquets d'une connexion particulière sont dirigés vers le même service.

Cette méthode est utilisée dans la mise en miroir des connexions et l'équilibrage de charge du pare-feu. Pour plus d'informations sur la mise en miroir des connexions, voir Basculement de connexion.

Pour diriger toutes les demandes appartenant à un réseau particulier vers un serveur de destination spécifique, vous devez masquer l'adresse IP source. Pour les adresses IPv4, utilisez le paramètre NetMask. Pour les adresses IPv6, utilisez le paramètre V6NetMaskLength.

Pour configurer la méthode de hachage du port source IP source source, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

La méthode de hachage de l'ID d'appel

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de hachage de l'ID d'appel utilise la valeur de hachage de l'ID d'appel dans l'en-tête SIP pour sélectionner un service. Les paquets pour une session SIP particulière sont donc toujours dirigés vers le même serveur proxy.

Cette méthode est applicable à l'équilibrage de charge SIP. Pour plus d'informations sur l'équilibrage de charge SIP, voir Surveillance des services SIP.

Pour configurer la méthode de hachage de l'ID d'appel, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de bande passante minimale

May 5, 2023

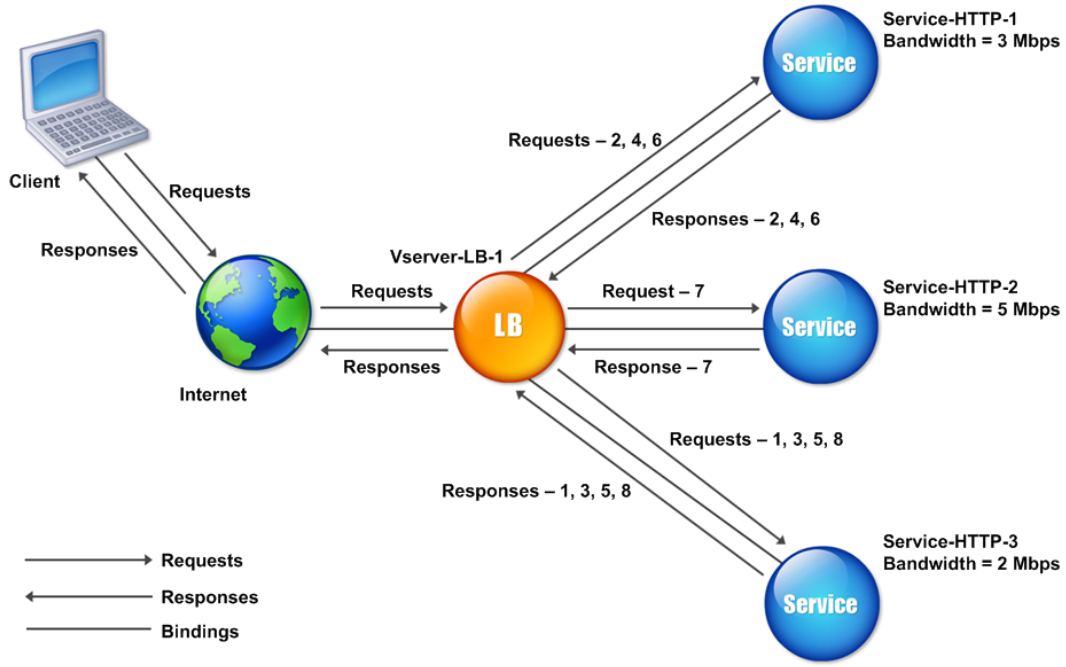
Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode de moindre bande passante sélectionne le service qui dessert actuellement le moins de trafic, mesuré en mégabits par seconde (Mbit/s). L'exemple suivant montre comment le serveur virtuel sélectionne un service pour l'équilibrage de charge en utilisant la méthode de moindre bande passante.

Considérons trois services, Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3.

- Service-http-1 dispose d'une bande passante de 3 Mbps.
- Service-http-2 dispose d'une bande passante de 5 Mbps.
- Service-http-3 dispose d'une bande passante de 2 Mbps.

Le schéma suivant montre comment le serveur virtuel utilise la méthode la moins passante pour transmettre les demandes aux trois services.

Figure 1. Fonctionnement de la méthode d'équilibrage de charge la plus faible bande passante



Le serveur virtuel sélectionne le service en utilisant la valeur de bande passante (N), qui est la somme du nombre d'octets transmis et reçus au cours des 14 secondes précédentes. Si chaque demande nécessite une bande passante de 1 Mbit/s, l'appliance NetScaler transmet les demandes comme suit :

- Service-HTTP-3 reçoit la première requête, car ce service a la valeur N la plus faible.
- Étant donné que Service-HTTP-1 et Service-HTTP-3 ont désormais la même valeur N, le serveur virtuel passe à la méthode Round Robin pour ces serveurs, en alternant entre eux. Service-HTTP-1 reçoit la deuxième requête, Service-HTTP-3 reçoit la troisième requête, Service-HTTP-1 reçoit la quatrième requête, Service-HTTP-3 reçoit la cinquième requête et Service-HTTP-1 reçoit la sixième requête.
- Puisque Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont désormais la même valeur N, le serveur virtuel inclut Service-HTTP-2 dans la liste ronde. Par conséquent, Service-HTTP-2 reçoit la septième requête, Service-HTTP-3 reçoit la huitième requête, et ainsi de suite.

Le tableau suivant récapitule le mode de calcul de N.

Demande reçue	Service sélectionné	Valeur N actuelle	Remarques
Request-1	Service-HTTP-3 ; (N = 2)	N = 3	Service-HTTP-3 a la valeur N la plus faible.

Demande reçue	Service sélectionné	Valeur N actuelle	Remarques
Request-2	Service-HTTP-1 ; (N = 3)	N = 4	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-3	Service-HTTP-3 ; (N = 3)	N = 4	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-4	Service-HTTP-1 ; (N = 4)	N = 5	-
Request-5	Service-HTTP-3 ; (N = 4)	N = 5	-
Request-6	Service-HTTP-1 ; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-7	Service-HTTP-2 ; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-8	Service-HTTP-3 ; (N = 5)	N = 6	-

Remarque : Si vous activez l'option RTSP NAT sur le serveur virtuel, l'appliance NetScaler utilise le nombre de données et d'octets de contrôle échangés pour déterminer l'utilisation de la bande passante pour les services RTSP. Pour plus d'informations sur l'option NAT RTSP, consultez Gestion des connexions RTSP.

L'appliance NetScaler effectue également un équilibrage de charge en utilisant la bande passante et les poids si des poids différents sont attribués aux services. Il sélectionne un service en utilisant la valeur (Nw) dans l'expression suivante :

Nw = (N) * (10 000/poids)

Comme dans l'exemple précédent, supposons qu'un poids de 2 soit attribué à Service-HTTP-1, un poids de 3 et un poids de 4 à Service-HTTP-3. L'appliance NetScaler fournit les demandes comme suit :

- Le service HTTP-3 reçoit les premières, deuxième, troisième, quatrième et cinquième requêtes, car ce service possède la valeur Nw la plus faible.

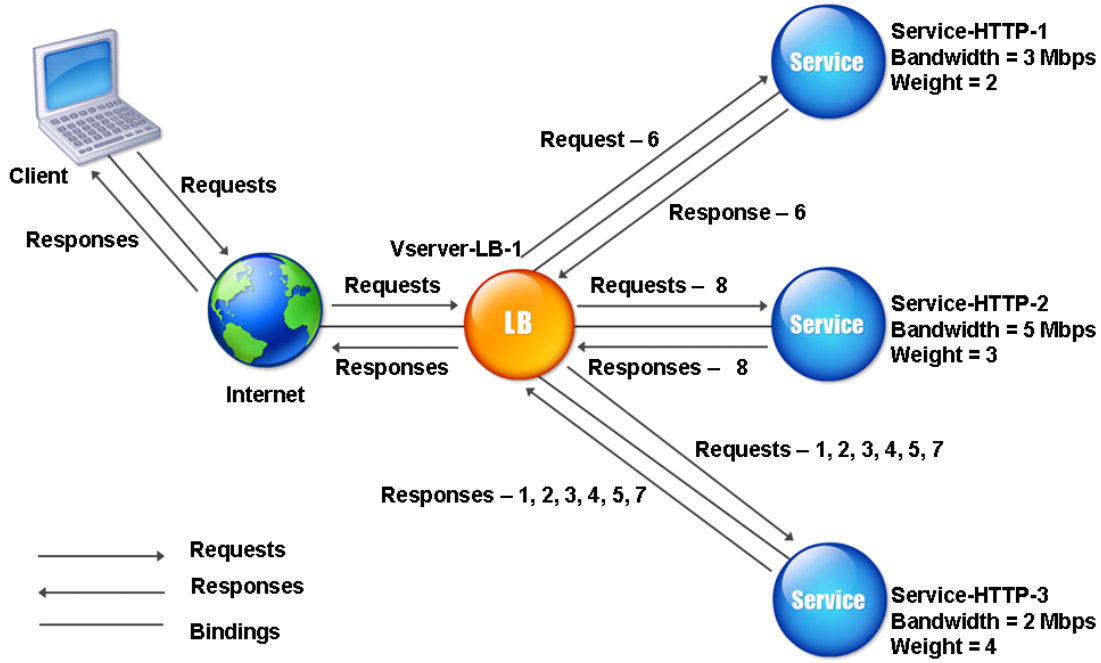
- Service-HTTP-1 reçoit la sixième demande, car ce service possède la valeur Nw la plus faible.
- Service-HTTP-3 reçoit la septième requête, car ce service possède la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la huitième requête, car ce service possède la valeur Nw la plus faible.

Le tableau suivant récapitule le mode de calcul de Nw.

Demande reçue	Service sélectionné	Nouvelle valeur actuelle (nombre de transactions actives) * (10 000/ poids)	Remarques
Request-1	Service-HTTP-3 ; (Nw = 5000)	Nw = 5000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-2	Service-HTTP-3 ; (Nw = 5000)	Nouveau = 7500	-
Request-3	Service-HTTP-3 ; (Nw = 7500)	Nw = 10 000	-
Request-4	Service-HTTP-3 ; (Nw = 10000)	Nouveau = 12 500	-
Request-5	Service-HTTP-3 ; (Nw = 12500)	Nouveau = 15 000	-
Request-6	Service-HTTP-1 ; (Nw = 15000)	Nw = 20 000	Service-HTTP-1 et Service-HTTP-3 ont la même valeur Nw.
Request-7	Service-HTTP-3 ; (Nw = 15000)	Nouveau = 17 500	Service-HTTP-1 et Service-HTTP-3 ont la même valeur Nw.
Request-8	Service-HTTP-2 ; (Nw = 16666,67)	Nw = 20 000	Service-HTTP-2 possède la valeur Nw la plus faible.

Le schéma suivant montre comment le serveur virtuel utilise la méthode de moindre bande passante lorsque des poids sont attribués aux services.

Figure 2. Fonctionnement de la méthode d'équilibrage de charge de la bande passante minimale lorsque des poids sont affectés



Pour configurer la méthode de la moindre bande passante, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode des moindres paquets

May 5, 2023

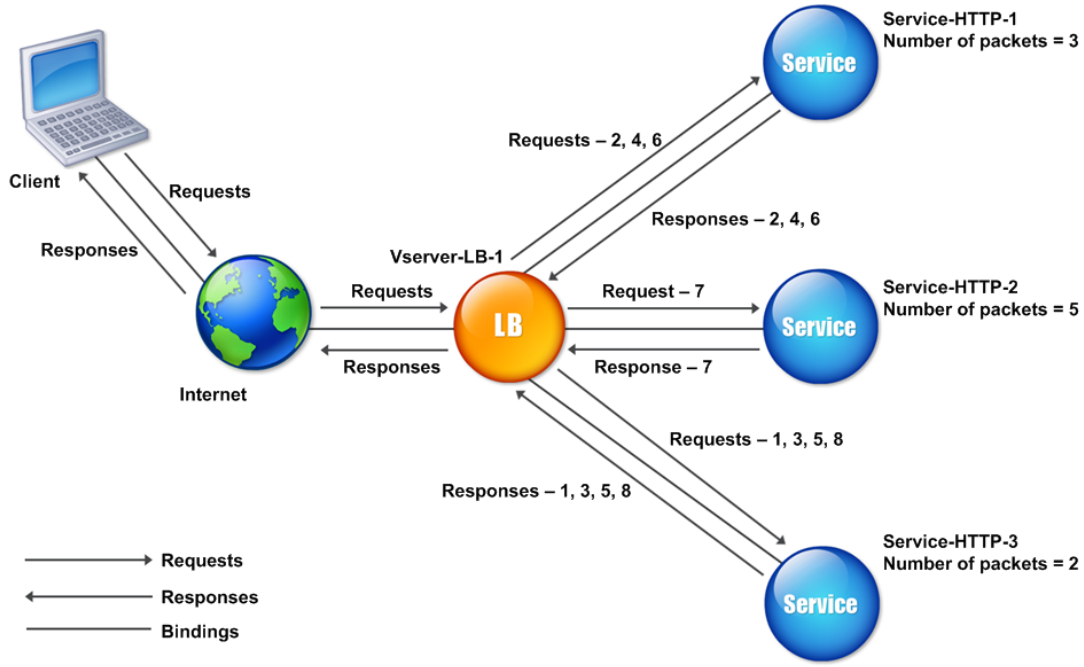
Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode du moins de paquets sélectionne le service qui a reçu le moins de paquets au cours des 14 dernières secondes.

Par exemple, considérez trois services, Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3.

- Service-HTTP-1 a traité trois paquets au cours des 14 dernières secondes.
- Service-HTTP-2 a traité cinq paquets au cours des 14 dernières secondes.
- Service-HTTP-3 a traité deux paquets au cours des 14 dernières secondes.

Le schéma suivant montre comment l'appliance NetScaler utilise la méthode des moindres paquets pour choisir un service pour chaque demande qu'elle reçoit.

Figure 1. Comment fonctionne la méthode d'équilibrage de charge basée sur le moindre nombre de paquets



L'appliance NetScaler sélectionne un service en utilisant le nombre de paquets (N) transmis et reçus par chaque service au cours des 14 dernières secondes. À l'aide de cette méthode, il envoie les demandes comme suit :

- Service-HTTP-3 reçoit la première requête, car ce service a la valeur N la plus faible.
- Comme Service-HTTP-1 et Service-HTTP-3 ont désormais la même valeur N, le serveur virtuel passe à la méthode Round Robin. Service-HTTP-1 reçoit donc la deuxième requête, Service-HTTP-3 reçoit la troisième requête, Service-HTTP-1 reçoit la quatrième requête, Service-HTTP-3 reçoit la cinquième requête et Service-HTTP-1 reçoit la sixième requête.
- Puisque Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont tous la même valeur N, le serveur virtuel passe également à la méthode round robin pour Service-HTTP-2, y compris dans la liste ronde. Par conséquent, Service-HTTP-2 reçoit la septième requête, Service-HTTP-3 reçoit la huitième requête, et ainsi de suite.

Le tableau suivant récapitule le mode de calcul de N.

Demande reçue	Service sélectionné	Valeur N actuelle	Remarques
Request-1	Service-HTTP-3 ; (N = 2)	N = 3	Service-HTTP-3 a la valeur N la plus faible.

Demande reçue	Service sélectionné	Valeur N actuelle	Remarques
Request-2	Service-HTTP-1 ; (N = 3)	N = 4	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-3	Service-HTTP-3 ; (N = 3)	N = 4	Service-HTTP-1 et Service-HTTP-3 ont les mêmes valeurs N.
Request-4	Service-HTTP-1 ; (N = 4)	N = 5	-
Request-5	Service-HTTP-3 ; (N = 4)	N = 5	-
Request-6	Service-HTTP-1 ; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-7	Service-HTTP-2 ; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-8	Service-HTTP-3 ; (N = 5)	N = 6	-

Remarque : Si vous activez l'option NAT RTSP sur le serveur virtuel, l'appliance utilise le nombre de paquets de données et de contrôle pour calculer le nombre de paquets pour les services RTSP. Pour plus d'informations sur l'option NAT RTSP, consultez Gestion des connexions RTSP.

L'appliance NetScaler effectue également un équilibrage de charge en utilisant le nombre de paquets et les poids lorsqu'un poids différent est attribué à chaque service. Il sélectionne un service en utilisant la valeur (Nw) dans l'expression suivante :

Nw = (N) * (10 000/poids)

Comme dans l'exemple précédent, supposons qu'un poids de 2 soit attribué à Service-HTTP-1, un poids de 3 et un poids de 4 à Service-HTTP-3. L'appliance NetScaler fournit les demandes comme suit :

- Le service HTTP-3 reçoit les premières, deuxième, troisième, quatrième et cinquième requêtes, car ce service possède la valeur Nw la plus faible.
- Service-HTTP-1 reçoit la sixième demande, car ce service possède la valeur Nw la plus faible.

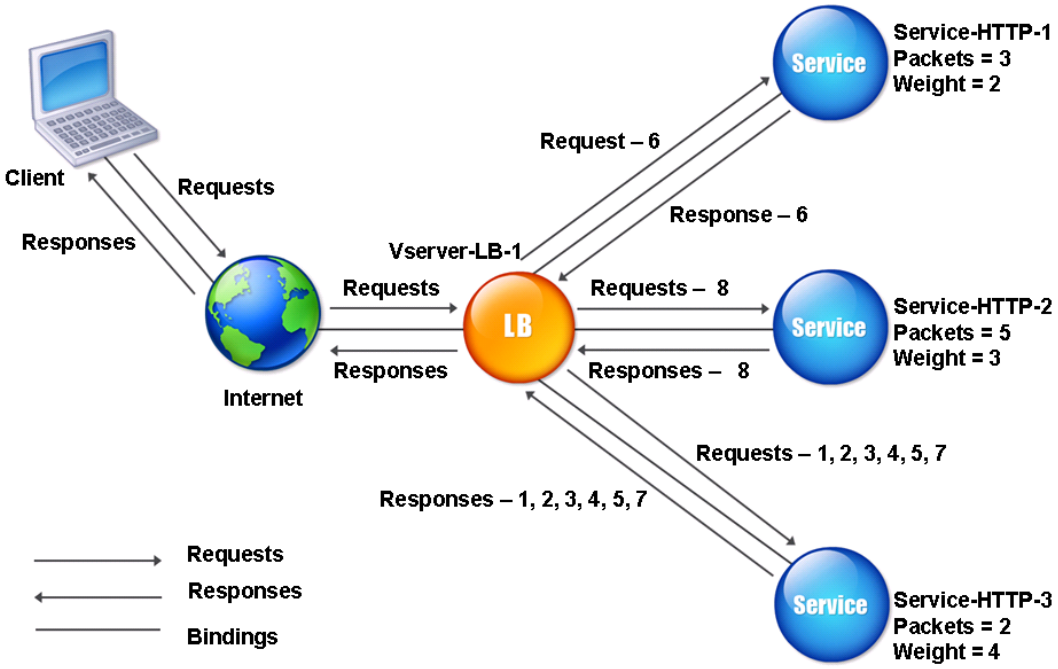
- Service-HTTP-3 reçoit la septième requête, car ce service possède la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la huitième requête, car ce service possède la valeur Nw la plus faible.

Le tableau suivant récapitule le mode de calcul de Nw.

Demande reçue	Service sélectionné	Nouvelle valeur actuelle (nombre de transactions actives) * (10 000/poids)	Remarques
Request-1	Service-HTTP-3 ; (Nw = 5000)	Nw = 5000	Service-HTTP-3 possède la valeur Nw la plus faible.
Request-2	Service-HTTP-3 ; (Nw = 5000)	Nouveau = 7500	-
Request-3	Service-HTTP-3 ; (Nw = 7500)	Nw = 10 000	-
Request-4	Service-HTTP-3 ; (Nw = 10000)	Nouveau = 12 500	-
Request-5	Service-HTTP-3 ; (Nw = 12500)	Nouveau = 15 000	-
Request-6	Service-HTTP-1 ; (Nw = 15000)	Nw = 20 000	Service-HTTP-1 et Service-HTTP-3 ont la même valeur Nw.
Request-7	Service-HTTP-3 ; (Nw = 15000)	Nouveau = 17 500	Service-HTTP-1 et Service-HTTP-3 ont la même valeur Nw.
Request-8	Service-HTTP-2 ; (Nw = 16666,67)	Nw = 20 000	Service-HTTP-2 possède la valeur Nw la plus faible.

Le schéma suivant montre comment le serveur virtuel utilise la méthode du moins de paquets lors de l'attribution de poids.

Figure 2. Comment fonctionne la méthode du plus petit nombre de paquets lorsque des poids sont attribués



Pour configurer la méthode des moindres paquets, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

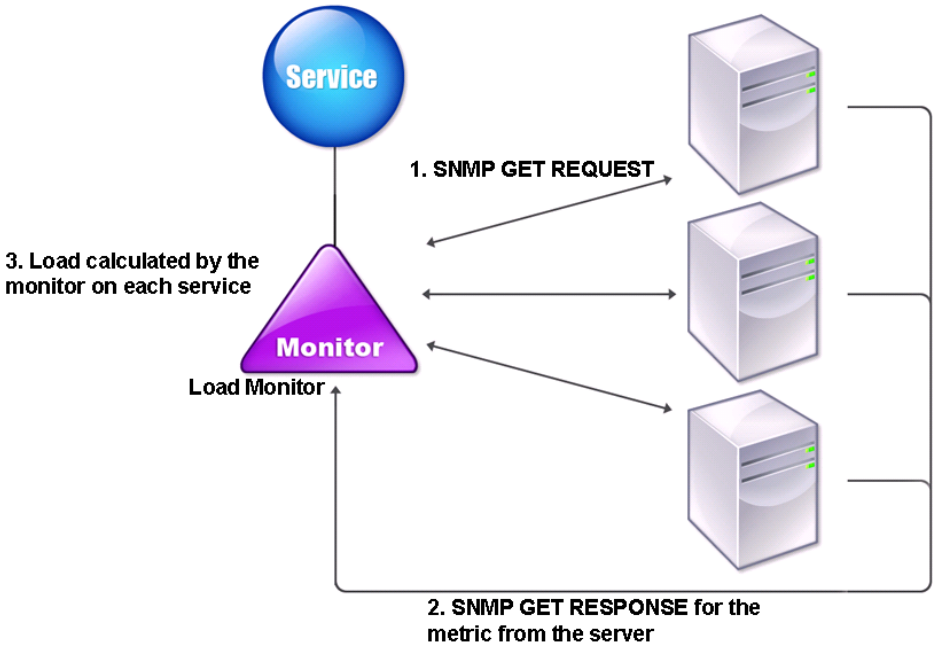
Méthode de chargement personnalisée

May 5, 2023

L'équilibrage de charge personnalisé est effectué sur les paramètres du serveur tels que l'utilisation du processeur, la mémoire et le temps de réponse. Lorsque vous utilisez la méthode de chargement personnalisée, l'appliance NetScaler sélectionne généralement un service qui ne gère aucune transaction active. Si tous les services de la configuration d'équilibrage de charge gèrent les transactions actives, l'appliance sélectionne le service avec la charge la plus faible. Un type spécial de moniteur, connu sous le nom de moniteur de charge, calcule la charge sur chaque service du réseau. Les moniteurs de charge ne marquent pas l'état d'un service, mais ils retirent les services de la décision d'équilibrage de charge lorsque ces services ne sont pas UP.

Pour plus d'informations sur les moniteurs de charge, voir Présentation des moniteurs de charge. Le diagramme suivant illustre le fonctionnement d'un moniteur de charge.

Figure 1. Comment fonctionnent les moniteurs de charge



Le moniteur de charge utilise des sondes SNMP pour calculer la charge sur chaque service en envoyant une demande GET SNMP au service. Cette demande contient un ou plusieurs ID d'objet (OID). Le service répond avec une réponse SNMP GET, avec des mesures correspondant aux OID SNMP. Le moniteur de charge utilise les mesures de réponse pour calculer la charge sur le service.

Le moniteur de charge calcule la charge sur un service en utilisant les paramètres suivants :

- Valeurs de mesures extraites via des sondes SNMP qui existent sous forme de tables dans l'appliance NetScaler.
- Valeur de seuil définie pour chaque métrique.
- Poids attribué à chaque métrique.

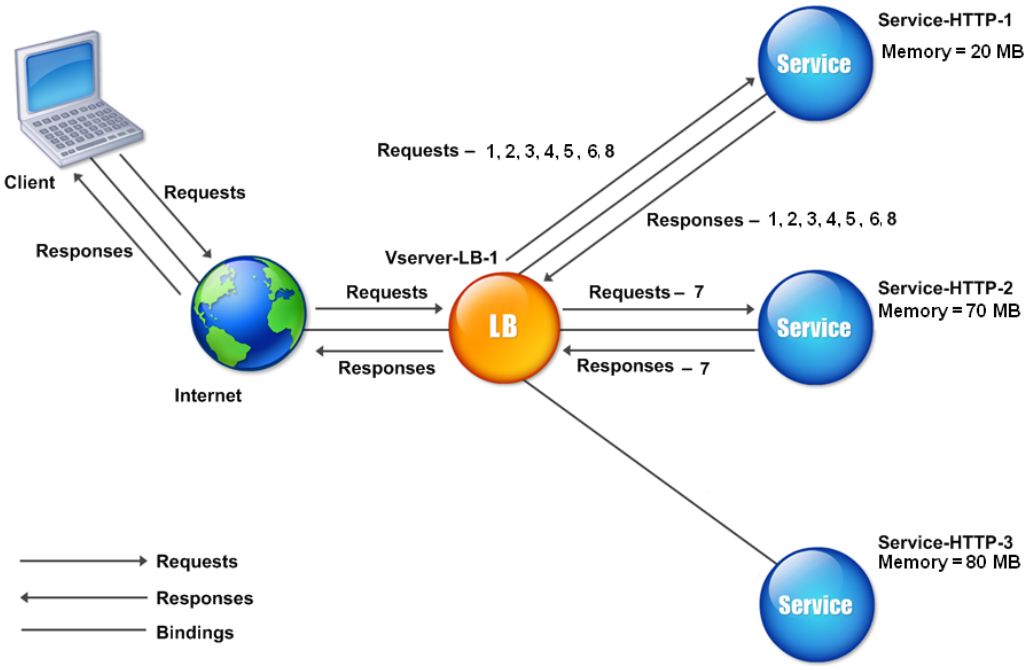
Par exemple, considérez trois services, Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3.

- Le service HTTP-1 utilise 20 Mo de mémoire.
- Service-HTTP-2 utilise 70 Mo de mémoire.
- Le Service-HTTP-3 utilise 80 Mo de mémoire.

Les serveurs à charge équilibrée peuvent exporter des mesures telles que l'utilisation du processeur et de la mémoire vers les services, qui peuvent à leur tour les fournir au moniteur de charge. Le moniteur de charge envoie une requête SNMP GET contenant les OID 1.3.6.1.4.1.5951.4.1.1.41.1.5,

1.3.6.1.4.1.5951.4.1.1.41.1.4 et 1.3.6.1.4.1.5951.4.1.1.41.1.3 aux services. Les OID SNMP de type STRING ne sont pas pris en charge car vous ne pouvez pas calculer la charge à l'aide d'un OID STRING. Les charges peuvent être calculées à l'aide d'autres types de données, tels que INT et gauge32. Les trois services répondent à la demande. L'appliance NetScaler compare les mesures exportées, puis sélectionne Service-HTTP-1 car elle dispose d'une plus grande quantité de mémoire disponible. Le schéma suivant illustre ce processus.

Figure 2. Fonctionnement de la méthode de chargement personnalisé



Si chaque demande utilise 10 Mo de mémoire, l'appliance NetScaler transmet les demandes comme suit :

- Service-HTTP-1 reçoit les première, deuxième, troisième, quatrième et cinquième requêtes, car ce service possède la valeur N la plus faible.
- Service-HTTP-1 et Service-HTTP-2 ont désormais la même charge, de sorte que le serveur virtuel revient à la méthode circulaire pour ces serveurs. Par conséquent, Service-HTTP-2 reçoit la sixième requête, et Service-HTTP-1 reçoit la septième requête.
- Puisque Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont tous la même charge, le serveur virtuel revient également à la méthode round robin pour Service-HTTP-3. Par conséquent, Service-HTTP-3 reçoit la huitième requête.

Le tableau suivant récapitule le mode de calcul de N.

Demande reçue	Service sélectionné	Valeur N actuelle (nombre de transactions actives)	Remarques
Request-1	Service-HTTP-1 ; (N = 20)	N = 30	Service-HTTP-3 a la valeur N la plus faible.
Request-2	Service-HTTP-1 ; (N = 30)	N = 40	-
Request-3	Service-HTTP-1 ; (N = 40)	N = 50	-
Request-4	Service-HTTP-1 ; (N = 50)	N = 60	-
Request-5	Service-HTTP-1 ; (N = 60)	N = 70	-
Request-6	Service-HTTP-1 ; (N = 70)	N = 80	Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.
Request-7	Service-HTTP-2 ; (N = 70)	N = 80	Service-HTTP-3 possède les mêmes valeurs N.
Request-8	Service-HTTP-1 ; (N = 80)	N = 90	Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 ont les mêmes valeurs N.

Si différents poids sont attribués aux services, l'algorithme de charge personnalisé prend en compte à la fois la charge de chaque service et le poids attribué à chaque service. Il sélectionne un service en utilisant la valeur (Nw) dans l'expression suivante :

Nw = (N) * (10 000/poids)

Comme dans l'exemple précédent, supposons que Service-HTTP-1 se voit attribuer un poids de 4, Service-HTTP-2 un poids de 3 et Service-HTTP-3 un poids de 2. Si chaque demande utilise 10 Mo de mémoire, l'appliance NetScaler transmet les demandes comme suit :

- Service-HTTP-1 reçoit les première, deuxième, troisième, quatrième, cinquième, sixième, septième et huitième requêtes, car ce service possède la valeur Nw la plus faible.
- Service-HTTP-2 reçoit la neuvième requête, car ce service possède la valeur Nw la plus faible.

Le Service-HTTP-3 possède la valeur Nw la plus élevée et n'est donc pas pris en compte pour l'équilibrage de charge.

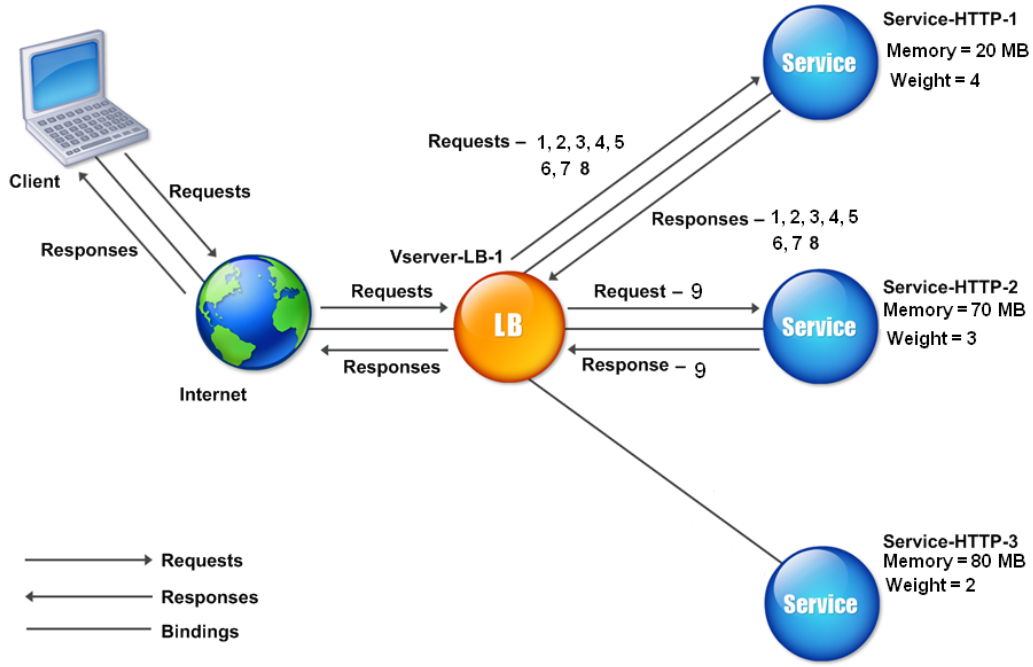
Le tableau suivant récapitule le mode de calcul de Nw.

Demande reçue	Service sélectionné	Nouvelle valeur actuelle (nombre de transactions actives) * (10 000/ poids)	Remarques
Request-1	Service-HTTP-1 ; (Nw = 50 000)	Nw = 75 000	Service-HTTP-1 possède la valeur Nw la plus faible.
Request-2	Service-HTTP-1 ; (Nw = 5000)	Nw = 100 000	-
Request-3	Service-HTTP-1 ; (Nw = 15000)	Nouveau = 125 000	-
Request-4	Service-HTTP-1 ; (Nouveau = 20 000)	Nouveau = 150 000	-
Request-5	Service-HTTP-1 ; (Nw = 23333,34)	Nouveau = 175 000	-
Request-6	Service-HTTP-1 ; (Nw = 25 000)	Nw = 200 000	-
Request-7	Service-HTTP-1 ; (Nw = 23333,34)	Nw = 225 000	-
Request-8|Service-HTTP-1 ; (Nw = 25000) |Nw = 250000||-| |Request-9|Service-HTTP-2 ; (Nw = 233333.34) |Nw = 266666.67|Service-HTTP-2 possède la valeur Nw la plus faible
.

Le Service-HTTP-1 est sélectionné pour l'équilibrage de charge lorsqu'il termine ses transactions actives ou lorsque la valeur Nw des autres services (Service-HTTP-2 et Service-HTTP-3) est égale à 400 000.

Le schéma suivant montre comment l'appliance NetScaler utilise la méthode de chargement personnalisée lorsque des poids sont attribués.

Figure 3. Fonctionnement de la méthode de chargement personnalisée lorsque des poids sont affectés



Pour configurer la méthode de chargement personnalisée, reportez-vous à la section Configuration d'une méthode d'équilibrage de charge qui n'inclut pas de stratégie.

Méthode de proximité statique

June 20, 2023

Lorsqu'un serveur virtuel est configuré pour utiliser la méthode de proximité statique, il sélectionne le service qui correspond le mieux aux critères de proximité.

Pour que la méthode de proximité statique fonctionne, vous devez soit configurer l'appliance NetScaler pour qu'elle utilise une base de données de proximité statique existante remplie via un fichier d'emplacement, soit ajouter des entrées personnalisées à la base de données de proximité statique. Après avoir ajouté des entrées personnalisées, vous pouvez définir leurs qualificatifs de localisation. Après avoir configuré la base de données, vous êtes prêt à spécifier la proximité statique comme méthode d'équilibrage de charge.

Pour plus de détails, consultez les rubriques suivantes.

- Ajout d'un fichier de position pour créer une base de données de proximité statique

- Ajouter des entrées personnalisées à une base de données de proximité statique
- Configuration des qualificatifs de localisation
- Spécification de la méthode de proximité statique

Spécification de la méthode de proximité

Lorsque vous avez configuré la base de données de proximité statique, vous êtes prêt à spécifier la proximité statique comme méthode GLSB.

Pour spécifier la proximité statique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la proximité statique et vérifier la configuration :

```
set lb vserver <name> -lbMethod STATICPROXIMITY

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod STATICPROXIMITY

show lb vserver
<!--NeedCopy-->
```

Pour spécifier la proximité statique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et sélectionnez le serveur virtuel.
2. Cliquez sur **Modifier** et développez la section **Méthode** .
3. Dans la liste des **méthodes d'équilibrage** de charge, sélectionnez **STATICPROXIMITY**.

> **Remarque**
>
> Activez le paramètre ProximityFromSelf pour utiliser l'adresse IP de bouclage du Netscaler au lieu de l'adresse IP du client afin de récupérer l'emplacement du serveur le plus proche pour un équilibrage de charge de proximité statique ou une décision GSLB.

Méthode de jeton

May 5, 2023

Un serveur virtuel d'équilibrage de charge configuré pour utiliser la méthode des jetons base sa sélection d'un service sur la valeur d'un segment de données extrait de la demande du client. Le segment de données s'appelle le jeton. Vous configurez l'emplacement et la taille du jeton. Pour les demandes suivantes avec le même jeton, le serveur virtuel choisit le même service qui a traité la demande initiale.

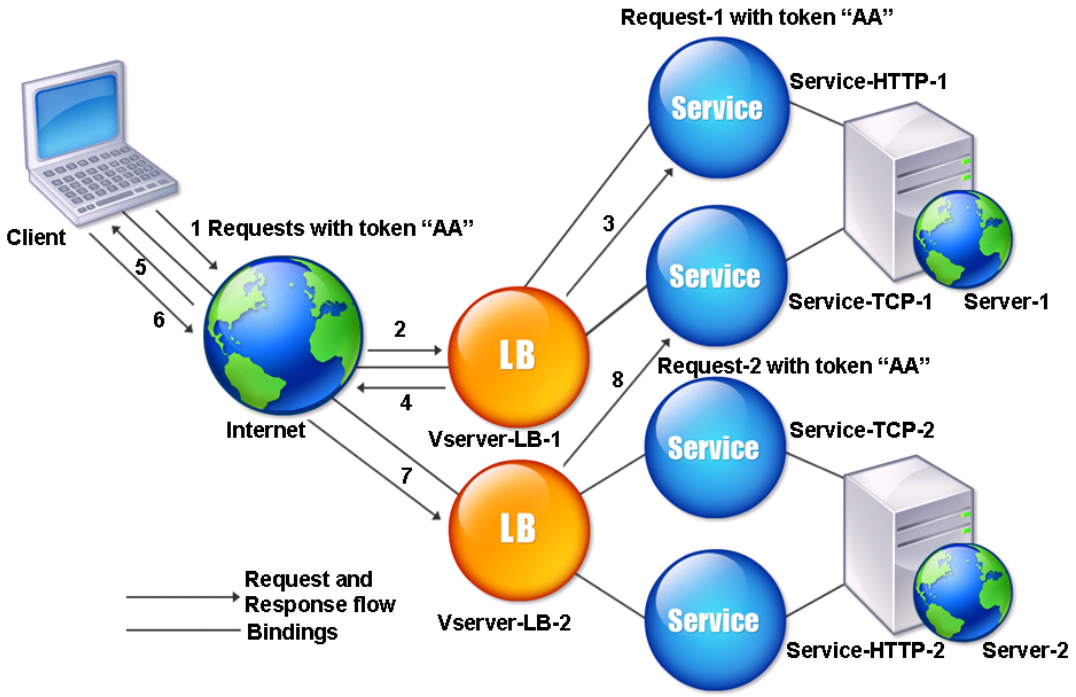
Cette méthode est consciente du contenu. Il fonctionne différemment pour les connexions TCP, HTTP et HTTPS. Pour les services HTTP ou HTTPS, le jeton se trouve dans les en-têtes HTTP, l'URL ou le BODY. Pour localiser le jeton, vous spécifiez ou créez une expression classique ou avancée. Pour plus d'informations sur les expressions classiques ou avancées, voir Configuration et référence des stratégies.

Pour les services HTTP, le serveur virtuel recherche le jeton configuré dans les 24 premiers kilo-octets (Ko) de la charge utile TCP. Pour les services non HTTP (TCP, SSL et SSL_TCP), le serveur virtuel recherche le jeton configuré dans les 16 premiers paquets si la taille totale des 16 paquets est inférieure à 24 Ko. Toutefois, si la taille totale des 16 paquets est supérieure à 24 Ko, l'appliance recherche le jeton dans les 24 premiers Ko de charge utile. Vous pouvez utiliser cette méthode d'équilibrage de charge sur des serveurs virtuels de différents types pour vous assurer que les demandes présentant le même jeton sont dirigées vers les services appropriés, quel que soit le protocole utilisé.

Par exemple, considérez une configuration d'équilibrage de charge composée de serveurs contenant du contenu Web. Vous souhaitez configurer l'appliance NetScaler pour qu'elle recherche une chaîne spécifique (le jeton) dans la partie requête URL de la demande. Le serveur 1 possède deux services, le service HTTP-1 et le service TCP-1, et le serveur 2 possède deux services, le service HTTP-2 et le service TCP-2. Les services TCP sont liés à vServer-LB-2 et les services HTTP sont liés à vServer-LB-1.

Si vServer-LB-1 reçoit une demande avec le jeton AA, il sélectionne le service Service-HTTP-1 (lié au serveur-1) pour traiter la demande. Si vServer-LB-2 reçoit une demande différente avec le même jeton (AA), il dirige cette demande vers le service Service-TCP-1. Le schéma suivant illustre ce processus.

Figure 1. Fonctionnement de la méthode jeton



Pour configurer la méthode d’équilibrage de charge Token à l’aide de l’interface de ligne de commande

À l’invite de commandes, tapez les commandes suivantes pour configurer la méthode d’équilibrage de charge des jetons et vérifier la configuration :

```
set lb vserver <name> -lbMethod TOKEN -rule <rule> -datalength <length>
    -dataoffset <offset>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver LB-VServer-1 -lbMethod TOKEN -rule 'AA' -datalength 2 -
   dataoffset 25

show lb vserver LB-VServer-1
<!--NeedCopy-->
```


Pour configurer la méthode d'équilibrage de charge des jetons à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, cliquez sur Méthode
3. Dans la liste Méthode d'équilibrage de charge, sélectionnez Token et spécifiez une expression.

Configurer une méthode d'équilibrage de charge qui n'inclut pas de stratégie

May 5, 2023

Après avoir sélectionné un algorithme d'équilibrage de charge pour votre configuration d'équilibrage de charge, vous devez configurer l'appliance NetScaler pour qu'elle utilise cet algorithme. Vous pouvez le configurer à l'aide de l'interface de ligne de commande ou de l'utilitaire de configuration.

Remarque :

La méthode jeton est basée sur une stratégie et nécessite plus de configuration que ce qui est décrit ici. Pour configurer la méthode du jeton, reportez-vous à la section Méthode Token.

Pour certaines méthodes basées sur le hachage, vous pouvez masquer une adresse IP pour diriger les requêtes appartenant au même sous-réseau vers le même serveur. Pour plus d'informations, voir Méthodes de hachage.

Pour définir la méthode d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -lbMethod <method>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod LeastConnection
<!--NeedCopy-->
```


Pour définir la méthode d'équilibrage de charge à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, cliquez sur **Méthode**et dans la liste Méthode d'équilibrage de charge, sélectionnez une méthode.

Persistance et connexions persistantes

May 5, 2023

Un protocole sans état d'équilibrage de charge, tel que HTTP, perturbe la maintenance des informations d'état relatives aux connexions client si la persistance n'est pas configurée. Différentes transmissions provenant d'un même client peuvent être dirigées vers différents serveurs, même si toutes les transmissions font partie de la même session. Vous pouvez configurer la persistance sur un serveur virtuel d'équilibrage de charge qui gère certains types d'applications Web, telles que les applications de panier d'achat.

Avant de pouvoir configurer la persistance, vous devez comprendre les différents types de persistance, comment ils sont utilisés et quelles sont leurs implications. Vous devez ensuite configurer l'appliance NetScaler pour fournir des connexions persistantes aux sites Web et aux applications Web qui en ont besoin.

Vous pouvez également configurer la persistance des sauvegardes, qui prend effet si le type principal de persistance configuré pour un serveur virtuel d'équilibrage de charge échoue. Vous pouvez configurer des groupes de persistance afin qu'une transmission client vers n'importe quel serveur virtuel d'un groupe puisse être dirigée vers un serveur qui a reçu des transmissions précédentes du même client.

Pour plus d'informations sur la persistance avec l'équilibrage de charge RADIUS, voir Configuration de l'équilibrage de charge RADIUS avec persistance.

À propos de la persistance

May 5, 2023

Vous pouvez choisir parmi plusieurs types de persistance pour un serveur virtuel d'équilibrage de charge donné, qui achemine ensuite vers le même service toutes les connexions du même utilisateur vers votre application de panier, votre messagerie Web ou toute autre application réseau. La session de persistance reste en vigueur pendant la durée spécifiée.

Si un serveur participant à une session de persistance est désactivé, le serveur virtuel d'équilibrage de charge utilise la méthode d'équilibrage de charge configurée pour sélectionner un nouveau service et établit une nouvelle session de persistance avec le serveur représenté par ce service. Si le serveur est HORS SERVICE, il continue à traiter les sessions de persistance existantes, mais le serveur virtuel n'y dirige aucun nouveau trafic. Une fois la période d'arrêt écoulée, le serveur virtuel cesse de diriger les connexions des clients existants vers le service, ferme les connexions existantes et redirige ces clients vers de nouveaux services si nécessaire.

Selon le type de persistance que vous configurez, l'appliance NetScaler peut examiner les adresses IP source, les adresses IP de destination, les ID de session SSL, les en-têtes d'hôte ou d'URL, ou une combinaison de ces éléments pour placer chaque connexion dans la session de persistance appropriée. Elle peut également baser la persistance sur un cookie émis par le serveur Web, sur un jeton assigné arbitrairement ou sur une règle logique. Presque tout ce qui permet à l'appliance de faire correspondre les connexions à la session de persistance appropriée et sert de base à la persistance.

Le tableau suivant récapitule les types de persistance disponibles sur l'appliance NetScaler.

Type de persistance	Description
IP source	ADRESSE IP DE LA SOURCE. Les connexions provenant de la même adresse IP client font partie de la même session de persistance.
Cookie HTTP	INSERT À BISCUITS. Les connexions qui ont le même en-tête de cookie HTTP font partie de la même session de persistance.
ID de session SSL	SESSION DE SESSION. Les connexions qui ont le même ID de session SSL font partie de la même session de persistance.
URL passive	URLPASSIVE. Les connexions à la même URL sont traitées comme faisant partie de la même session de persistance.
ID de serveur personnalisé	IDENTIFIANT DU SERVEUR PERSONNALISÉ. Les connexions ayant le même en-tête HTTP HOST sont traitées comme faisant partie de la même session de persistance.
IP destination	DESTIP. Les connexions à la même adresse IP de destination sont traitées comme faisant partie de la même session de persistance.

Type de persistance	Description
IP source et adresse IP de destination	SCRIPT TIP. Les connexions qui proviennent à la fois de la même adresse IP source et de la même adresse IP de destination sont traitées comme faisant partie de la même session de persistance.
ID d'appel SIP	CALLID. Les connexions qui ont le même ID d'appel dans l'en-tête SIP sont traitées comme faisant partie de la même session de persistance.
ID de session RTSP	RTSPSID. Les connexions qui ont le même ID de session RTSP sont traitées comme faisant partie de la même session de persistance.
Règle définie par l'utilisateur	RÈGLE. Les connexions qui correspondent à une règle définie par l'utilisateur sont traitées comme faisant partie de la même session de persistance.

Tableau 1. Types de persistance

Selon le type de persistance que vous avez configuré, le serveur virtuel peut prendre en charge 250 000 connexions persistantes simultanées ou un nombre quelconque de connexions persistantes dans les limites imposées par la quantité de RAM de votre appliance NetScaler. Le tableau suivant indique les types de persistance qui entrent dans chaque catégorie.

Type de persistance	Nombre de connexions persistantes simultanées prises en charge
IP source, ID de session SSL, règle, adresse IP de destination, adresse IP source/adresse IP de destination, identifiant d'appel SIP, identifiant de session RTSP	250 K
Cookie, ID du serveur URL, ID du serveur personnalisé	Limite de mémoire. Dans CookieInsert, si le délai d'expiration n'est pas 0, le nombre de connexions est limité par la mémoire.

Tableau 2 Types de persistance et nombre de connexions simultanées prises en charge

Certains types de persistance sont spécifiques à certains types de serveurs virtuels. Le tableau suivant

répertorie chaque type de persistance et indique quels types de persistance sont pris en charge sur chaque type de serveur virtuel.

Type de persis-tance	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge	SSL_TCP	RTSP	SIP_UDP
SOURCEI	OUI	OUI	OUI	OUI	OUI	OUI	NON	NON
INSERT À BIS-CUITS	OUI	OUI	NON	NON	NON	NON	NON	NON
SESSION SSL	NON	OUI	NON	NON	OUI	OUI	NON	NON
URL PAS-SIVE	OUI	OUI	NON	NON	NON	NON	NON	NON
ID DE SERVEUF PER-SON-NALISÉ	OUI	OUI	NON	NON	NON	NON	NON	NON
RÈGLE	OUI	OUI	OUI	NON	NON		NON	NON
SRCIPDE	OUI	OUI	OUI	OUI	OUI	OUI	NON	NON
DESTIP	OUI	OUI	OUI	OUI	OUI	OUI	NON	NON
CALLID	NON	NON	NON	NON	NON	NON	NON	OUI
RTSPID	NON	NON	NON	NON	NON	NON	OUI	NON

Tableau 3. Relation entre le type de persistance et le type de serveur virtuel

Persistance de l’adresse IP source

May 5, 2023

Lorsque la persistance de l’adresse IP source est configurée, le serveur virtuel d’équilibrage de charge utilise la méthode d’équilibrage de charge configurée pour sélectionner un service pour la demande initiale, puis utilise l’adresse IP source (adresse IP du client) pour identifier les demandes suivantes de

ce client et les envoyer au même service. Vous pouvez définir une valeur de délai d'expiration qui indique la période d'inactivité maximale pour la session. Lorsque la valeur du délai d'expiration expire, la session est supprimée et l'algorithme d'équilibrage de charge configuré est utilisé pour sélectionner un nouveau serveur.

Attention : Dans certains cas, l'utilisation de la persistance basée sur l'adresse IP source peut surcharger vos serveurs. Toutes les demandes adressées à un seul site Web ou à une seule application sont acheminées via la passerelle unique vers l'appliance NetScaler, même si elles sont ensuite redirigées vers plusieurs emplacements. Dans plusieurs environnements proxy, les demandes des clients ont souvent des adresses IP source différentes, même lorsqu'elles sont envoyées à partir du même client, ce qui entraîne une multiplication rapide des sessions de persistance où une seule session doit être créée. Ce problème s'appelle "Mega Proxy problem". Vous pouvez utiliser la persistance basée sur les cookies HTTP au lieu de la persistance basée sur l'IP source pour empêcher cela de se produire.

Pour configurer la persistance en fonction de l'adresse IP source, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Remarque : Si tout le trafic entrant provient d'un périphérique de traduction d'adresses réseau (NAT) ou d'un proxy, le trafic apparaît à l'appliance NetScaler comme provenant d'une adresse IP source unique. Cela empêche la persistance de l'adresse IP source de fonctionner correctement. Dans ce cas, vous devez sélectionner un autre type de persistance.

Persistance des cookie HTTP

May 5, 2023

Lorsque la persistance des cookies HTTP est configurée, l'appliance NetScaler définit un cookie dans les en-têtes HTTP de la demande initiale du client. Le cookie contient l'adresse IP et le port du service sélectionné par l'algorithme d'équilibrage de charge. Comme pour toute connexion HTTP, le client inclut ensuite ce cookie dans toutes les demandes ultérieures.

Lorsque l'appliance NetScaler détecte le cookie, elle transmet la demande à l'adresse IP du service et au port contenus dans le cookie, préservant ainsi la persistance de la connexion. Vous pouvez utiliser ce type de persistance avec des serveurs virtuels de type HTTP ou HTTPS. Ce type de persistance ne consomme pas de ressources d'appliance et peut donc accueillir un nombre illimité de clients persistants.

Remarque : Si le navigateur Web du client est configuré pour refuser les cookies, la persistance basée sur les cookies HTTP ne fonctionne pas. Il peut être conseillé de configurer une vérification des cookie sur le site Web et d'avertir les clients qui ne semblent pas stocker correctement les cookies qu'ils doivent activer les cookies pour le site Web s'ils souhaitent les utiliser.

Le format du cookie que l'appliance NetScaler insère est le suivant :

```
NSC_XXXX=<ServiceIP ><ServicePort>
```

Où :

- NSC_XXXX est l'ID du serveur virtuel dérivé du nom du serveur virtuel.
- ServiceIP et ServicePort sont des représentations codées de l'adresse IP et du port du service, respectivement. L'adresse IP et le port sont codés séparément.

Vous pouvez définir une valeur de délai d'attente pour ce type de persistance afin de spécifier une période d'inactivité pour la session. Lorsque la connexion est restée inactive pendant la période spécifiée, l'appliance NetScaler supprime la session de persistance. Toute connexion ultérieure à partir du même client entraîne la sélection d'un nouveau serveur en fonction de la méthode d'équilibrage de charge configurée et l'établissement d'une nouvelle session de persistance.

Remarque : Si vous définissez la valeur du délai d'expiration sur 0, l'appliance NetScaler ne spécifie pas de délai d'expiration, mais définit un cookie de session qui n'est pas enregistré lorsque le navigateur du client est fermé.

Par défaut, l'appliance NetScaler définit des cookies HTTP version 0 pour une compatibilité maximale avec les navigateurs clients. (Seuls certains proxys HTTP comprennent les cookies de la version 1 ; les navigateurs les plus couramment utilisés ne le comprennent pas.) Vous pouvez configurer l'appliance pour définir des cookies HTTP version 1, conformément à la RFC2109. Pour les cookies HTTP version 0, l'appliance insère la date et l'heure d'expiration du cookie sous forme de temps universel coordonné (GMT) absolu. Il calcule cette valeur comme la somme de l'heure GMT actuelle sur l'appliance et de la valeur du délai d'expiration. Pour les cookies HTTP version 1, l'appliance insère un délai d'expiration relatif en définissant l'attribut « Max-Age » du cookie HTTP. Dans ce cas, le navigateur du client calcule le temps d'expiration réel.

Pour configurer la persistance en fonction d'un cookie inséré par l'appliance, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Dans le cookie HTTP, l'appliance définit par défaut l'`HTTPOnly` indicateur pour indiquer que le cookie n'est pas scriptable et ne doit pas être révélé à l'application cliente. Par conséquent, un script côté client ne peut pas accéder au cookie et le client n'est pas sensible aux scripts intersites.

Cependant, certains navigateurs ne prennent pas en charge l'`HTTPOnly` indicateur et, par conséquent, risquent de ne pas renvoyer le cookie. En conséquence, la persistance est brisée. Pour les navigateurs qui ne prennent pas en charge l'indicateur, vous pouvez omettre l'`HTTPOnly` indicateur dans le cookie de persistance.

Pour modifier le paramètre d'`HTTPOnly` indicateur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
set lb parameter -httpOnlyCookieFlag (ENABLED|DISABLED)
<!--NeedCopy-->
```

Exemple :

```
>  set lb parameter -httpOnlyCookieFlag disabled
   Done
> show lb parameter
  Global LB parameters:
       Persistence Cookie HttpOnly Flag: DISABLED
       Use port for hash LB: YES
 Done
<!--NeedCopy-->
```

Pour modifier le paramètre d' HTTPOnly indicateur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**, puis sélectionnez ou désactivez l'indicateur **HttpOnly Cookie de persistance** .

Cryptage du cookie

À partir de la version 10.5 build 55.8, vous pouvez crypter le cookie en plus de tout cryptage SSL.

Pour crypter le cookie à l'aide de l'interface de ligne de commande, à l'invite de commande, tapez

```
set lb parameter -UseEncryptedPersistenceCookie ENABLED -
   cookiePassphrase test
<!--NeedCopy-->
```

Pour crypter le cookie à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Modifier les paramètres d'équilibrage** de la charge, puis sélectionnez **Encoder les valeurs de cookie de persistance** et entrez une phrase secrète dans la **phrase secrète de cookie** .

Persistance de l'ID de session SSL

May 5, 2023

Lorsque la persistance de l'ID de session SSL est configurée, l'appliance NetScaler utilise l'ID de session SSL, qui fait partie du processus d'établissement de connexion SSL, pour créer une session de persistance avant que la demande initiale ne soit dirigée vers un service. Le serveur virtuel d'équilibrage de charge dirige les demandes suivantes qui ont le même ID de session SSL vers le même service. Ce type de persistance est utilisé pour les services de pont SSL.

Remarque :

Les utilisateurs doivent prendre en compte deux problèmes avant de choisir ce type de persistance. Tout d'abord, ce type de persistance consomme des ressources sur l'appliance NetScaler, ce qui limite le nombre de sessions de persistance simultanées qu'elle peut prendre en charge. Si vous prévoyez de prendre en charge plusieurs sessions de persistance, vous pouvez choisir un autre type de persistance.

Deuxièmement, si le client et le serveur à charge équilibrée doivent renégocier l'ID de session pendant leurs transactions, la persistance n'est pas maintenue et une nouvelle session de persistance est créée lors de la réception de la prochaine demande du client. Cela peut entraîner l'interruption de l'activité du client sur le site Web et il peut être demandé au client de se réauthentifier ou de redémarrer la session. Cela peut également entraîner un grand nombre de sessions abandonnées si le délai d'attente est défini sur une valeur trop importante.

Pour configurer la persistance en fonction de l'ID de session SSL, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

> **Remarque**
>
> La persistance des ID de session SSL n'est pas prise en charge avec les tickets de session.

Prise en charge de la persistance de sauvegarde pour l'ID de session SSL

À partir de NetScaler version 12.0 build 56.20, la persistance IP source est prise en charge en tant que type de persistance de sauvegarde pour la persistance de l'ID de session SSL. Si le client et le serveur à équilibrage de charge renégocient la session et que la persistance de l'adresse IP source est configurée comme persistance de sauvegarde, les demandes du client sont transmises au même serveur.

Pour prendre en charge la persistance de la sauvegarde pour l'ID de session SSL, l'appliance NetScaler crée des entrées de session pour l'IP source et l'ID de session SSL lorsqu'une demande client est reçue pour la première fois. Pour les demandes suivantes contenant le même ID de session, l'ID de session SSL est utilisé. Toutefois, lorsque le client et le serveur à équilibrage de charge renégocient la session, la demande du client est transmise au même serveur à l'aide de la persistance IP source et une nouvelle entrée de persistance SSL ID de session est créée.

Pour plus d'informations sur la configuration de la persistance des sauvegardes, voir Configuration de la persistance des sauvegardes.

Persistance du nombre AVP de diamètre

May 5, 2023

Vous pouvez utiliser la persistance en fonction du numéro de paire attribut-valeur (AVP) d'un message Diameter pour créer des sessions Diameter persistantes. Lorsque l'appliance NetScaler trouve l'AVP dans le message Diameter, elle crée une session de persistance basée sur la valeur de l'AVP. Tous les messages suivants qui correspondent à la valeur de l'AVP sont dirigés vers le serveur précédemment sélectionné. Si la valeur de l'AVP ne correspond pas à la session de persistance, une nouvelle session est créée pour la nouvelle valeur.

Remarque : Si le numéro AVP n'est pas défini dans le protocole de base de diamètre RFC 6733, et si le numéro est imbriqué dans un AVP groupé, vous devez définir une séquence de numéros AVP (maximum 3) dans l'ordre parent-enfant. Par exemple, si le numéro AVP X persiste est imbriqué dans AVP Y, qui est imbriqué dans Z, définissez la liste comme Z Y X.

Pour configurer la persistance basée sur le Diameter sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set lb vserver <name> -PersistenceType <type-> persistAVPno <
   positive_integer>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver diameter_vs -persistenceType DIAMETER -persistAVPno 263
<!--NeedCopy-->
```

Persistance de l'ID de serveur personnalisé

May 5, 2023

Dans la méthode de persistance de l'ID de serveur personnalisé, l'ID de serveur spécifié dans la demande du client est utilisé pour maintenir la persistance. Pour que ce type de persistance fonctionne,

vous devez d'abord définir un ID de serveur sur les services. L'appliance NetScaler vérifie l'URL de la demande du client et se connecte au serveur associé à l'ID de serveur spécifié. Le fournisseur de services doit s'assurer que les utilisateurs connaissent les ID de serveur à fournir dans leurs demandes de services spécifiques.

Par exemple, si votre site fournit différents types de données, tels que des images, du texte et du multimédia, provenant de différents serveurs, vous pouvez attribuer un ID de serveur à chaque serveur. Sur l'appliance NetScaler, vous spécifiez ces ID de serveur pour les services correspondants et vous configurez la persistance personnalisée des ID de serveur sur le serveur virtuel d'équilibrage de charge correspondant. Lors de l'envoi d'une demande, le client insère l'ID du serveur dans l'URL indiquant le type de données requis.

Pour configurer la persistance des ID de serveur personnalisés :

- Dans votre configuration d'équilibrage de charge, attribuez un ID de serveur à chaque service pour lequel vous souhaitez utiliser l'ID de serveur défini par l'utilisateur afin de maintenir la persistance. Les identifiants de serveur alphanumériques sont autorisés.
- Spécifiez des règles, dans le langage d'expression de syntaxe par défaut, pour examiner les requêtes URL relatives à l'ID du serveur et transférer le trafic vers le serveur correspondant.
- Configurez la persistance des ID de serveur personnalisés.

Remarque : La valeur du délai d'expiration de la persistance n'affecte pas le type de persistance de l'ID de serveur personnalisé. Le nombre maximum de clients persistants n'est pas limité car ce type de persistance ne stocke aucune information client.

Exemple :

Dans une configuration d'équilibrage de charge avec deux services, attribuez l'ID de serveur 2345-photo-56789 au Service-1 et l'ID de serveur 2345-drawing-abb123 au Service-2. Liez ces services à un serveur virtuel nommé Web11.

```
set service Service-1 10.102.29.5 -CustomServerID 2345-photo-56789

set service Service-2 10.102.29.6 -CustomServerID 2345-drawing-abb123
<!--NeedCopy-->
```

Sur le serveur virtuel Web11, activez la persistance de l'ID de serveur personnalisé.

Créez l'expression suivante afin que toutes les requêtes d'URL contenant la chaîne « sid= » soient examinées.

HTTP.REQ.URL.AFTER_STR (« sid= »)

Exemple :

```
set lb vserver Web11 -persistenceType customserverID -rule "HTTP.REQ.
    URL.AFTER_STR("sid=")"
```



```
2
3 bind lb vserver Web11 Service-[1-2]
4 <!--NeedCopy-->
```

Lorsqu'un client envoie une demande avec l'URL suivante à l'adresse IP de Web11, l'appliance dirige la demande vers Service-2 et respecte la persistance.

Exemple :

```
http://www.example.com/index.asp?&sid=2345-drawing-abb123
```

Pour plus d'informations sur les expressions de stratégie de syntaxe par défaut, reportez-vous à la section Configuration et référence des stratégies.

Pour configurer la persistance de l'ID de serveur personnalisé à l'aide de l'utilitaire de configuration

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Ouvrez le service et définissez un ID de serveur.
3. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.
4. Dans Paramètres avancés, sélectionnez Persistance.
5. Sélectionnez CUSTOMESERVERID et spécifiez une expression.

Persistance de l'adresse IP

May 5, 2023

Vous pouvez baser la persistance sur les adresses IP de destination, ou à la fois sur les adresses IP source et de destination.

Persistance basée sur les adresses IP de destination

Avec la persistance basée sur l'adresse IP de destination, lorsque l'appliance NetScaler reçoit une demande d'un nouveau client, elle crée une session de persistance basée sur l'adresse IP du service sélectionné par le serveur virtuel (l'adresse IP de destination). Plus tard, il dirige les demandes vers la même adresse IP de destination vers le même service. Ce type de persistance est utilisé avec l'équilibrage de charge de liaison. Pour plus d'informations sur l'équilibrage de charge des liaisons, voir Équilibrage de charge de liaison.

La valeur de délai d'expiration pour la persistance IP de destination est la même que pour la persistance IP source, décrite dans Persistance basée sur l'adresse IP source.

Pour configurer la persistance en fonction de l'adresse IP de destination, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Persistance basée sur les adresses IP source et destination

Avec la persistance basée sur les adresses IP source et destination, lorsque l'appliance NetScaler reçoit une demande, elle crée une session de persistance basée à la fois sur l'adresse IP du client (l'adresse IP source) et sur l'adresse IP du service sélectionné par le serveur virtuel (l'adresse IP de destination). Plus tard, il dirige les demandes provenant de la même adresse IP source et vers la même adresse IP de destination vers le même service.

La valeur de délai d'expiration pour la persistance IP de destination est la même que pour la persistance IP source, décrite dans Persistance basée sur l'adresse IP source.

Pour configurer la persistance en fonction des adresses IP source et de destination, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Persistance de l'ID d'appel SIP

May 5, 2023

Avec la persistance de l'ID d'appel SIP, l'appliance NetScaler choisit un service en fonction de l'ID d'appel figurant dans l'en-tête SIP. Cela lui permet de diriger les paquets d'une session SIP particulière vers le même service et, par conséquent, vers le même serveur d'équilibrage de charge. Ce type de persistance s'applique spécifiquement à l'équilibrage de charge SIP. Pour plus d'informations sur l'équilibrage de charge SIP, voir Surveillance des services SIP.

Pour configurer la persistance en fonction de l'ID d'appel SIP, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Persistance de l'ID de session RTSP

May 5, 2023

Avec la persistance des ID de session RTSP, lorsque l'appliance NetScaler reçoit une demande d'un nouveau client, elle crée une session de persistance basée sur l'ID de session RTSP (Real-Time Streaming Protocol) figurant dans l'en-tête du paquet RTSP, puis dirige la demande vers le service RTSP sélectionné par la méthode d'équilibrage de charge configurée. Il dirige les demandes suivantes qui contiennent le même ID de session vers le même service. Ce type de persistance s'applique spécifiquement

à l'équilibrage de charge SIP. Pour plus d'informations sur l'équilibrage de charge SIP, voir Surveillance des services SIP.

Remarque : la persistance de l'ID de session RTSP est configurée par défaut sur les serveurs virtuels RTSP, et vous ne pouvez pas modifier ce paramètre.

Il arrive que différents serveurs RTSP émettent les mêmes identifiants de session. Lorsque cela se produit, des sessions uniques ne peuvent pas être créées entre le client et le serveur RTSP en utilisant uniquement l'ID de session RTSP. Si plusieurs serveurs RTSP peuvent émettre les mêmes ID de session, vous pouvez configurer l'appliance pour ajouter l'adresse IP du serveur et le port à l'ID de session, créant ainsi un jeton unique qui peut être utilisé pour établir la persistance. Il s'agit du mappage des ID de session.

Pour configurer la persistance en fonction des ID de session RTSP, reportez-vous à la section Configuration des types de persistance qui ne nécessitent pas de règle.

Important : si vous devez utiliser le mappage d'ID de session, vous devez définir le paramètre suivant lors de la configuration de chaque service au sein de la configuration d'équilibrage de charge. Assurez-vous également qu'aucune connexion non persistante n'est routée via le serveur virtuel RTSP.

Configurer la persistance passive des URL

May 5, 2023

Avec la persistance passive des URL, lorsque l'appliance NetScaler reçoit une demande d'un client, elle extrait les informations relatives au port de l'adresse IP du serveur (exprimées sous la forme d'un nombre hexadécimal unique) de la demande du client.

La persistance passive des URL nécessite la configuration d'une expression avancée qui spécifie l'élément de requête contenant les informations de port d'adresse IP du serveur. Pour plus d'informations sur les expressions de stratégie classiques et avancées, voir Stratégies et expressions.

L'expression suivante configure l'appliance pour qu'elle examine les requêtes d'URL contenant la chaîne « urlp= », extraire les informations de port d'adresse IP du serveur, les convertit d'une chaîne hexadécimale en adresse IP et numéro de port, puis transfère la requête au service configuré avec cette adresse IP et numéro de port.

HTTP.REQ.URL.AFTER_STR (« urlp= »)

Si la persistance passive d'URL est activée et que l'expression précédente est configurée, une demande avec l'URL et la chaîne de port d'adresse IP du serveur suivantes est dirigée vers 10.102.29.10:80.

```
http://www.example.com/index.asp?&urlp=0A661D0A0050
```


La valeur du délai d'attente de persistance n'affecte pas ce type de persistance. La persistance est maintenue tant que les informations du port d'adresse IP du serveur peuvent être extraites des demandes des clients. Ce type de persistance ne consomme pas de ressources d'appliance, de sorte qu'il peut accueillir un nombre illimité de clients persistants.

Pour configurer la persistance passive des URL, vous devez d'abord configurer la persistance comme décrit dans Configuration des types de persistance qui ne nécessitent pas de règle. Vous définissez le type de persistance sur URLPASSIVE. Vous effectuez ensuite les procédures suivantes.

Pour configurer la persistance passive des URL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

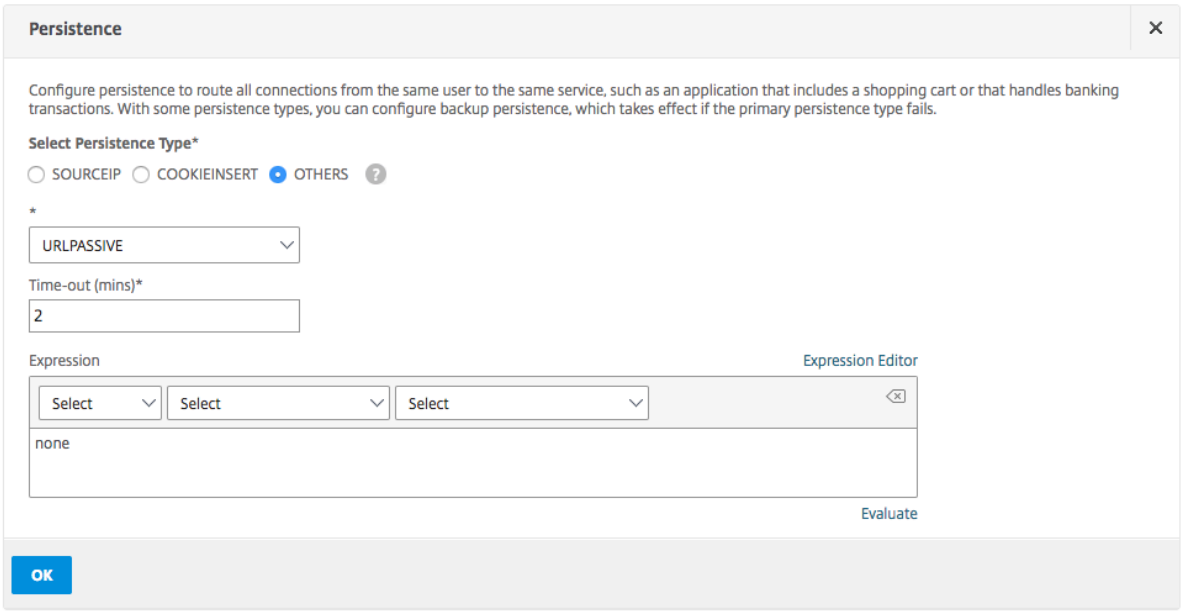
```
set lb vserver <vserverName>  [-persistenceType <persistenceType>]  [-
    rule <expression>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver LB-VServer-1 -persistenceType URLPASSIVE  -rule HTTP.REQ
    .URL.AFTER_STR( "urlp=" )
<!--NeedCopy-->
```

Pour configurer la persistance sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestiondu trafic**>**Équilibrage**de**charge**>**Serveursvirtuels**, puis ouvrez le serveur virtuel.
2. Dans la section Persistence, choisissez le type de persistance qui répond à vos besoins. Le type de persistance le plus approprié pour le serveur virtuel est disponible sous forme de boutons d'option. D'autres types de persistance applicables au type de serveur virtuel spécifique peuvent être sélectionnés dans la liste Autres.



> **Remarque :**
>
> Avant NetScaler version 12.0 build 56.20, tous les types de persistance sont disponibles dans une seule liste déroulante Persistence sans boutons d'option.

Configuration de la persistance en fonction de règles définies par l'utilisateur

May 5, 2023

> **Avertissement :**
>
> L'utilisation d'expressions classiques pour la règle de persistance dans la fonctionnalité d'équilibrage de charge a été supprimée et n'est plus disponible pour la règle de filtrage sur les versions 13.1 et ultérieures de l'appliance NetScaler. Citrix recommande de ne pas utiliser ces expressions de politique via l'interface de ligne de commande NetScaler, l'interface graphique NetScaler ou Nitro Automation. Pour plus d'informations, consultez les tableaux 1 et 2 de la page FAQ sur la dépréciation des stratégies classiques .

Lorsque la persistance basée sur des règles est configurée, l'appliance NetScaler crée une session de persistance basée sur le contenu de la règle correspondante avant de diriger la demande vers le service sélectionné par la méthode d'équilibrage de charge configurée. Plus tard, il dirige toutes les demandes correspondant à la règle vers le même service. Vous pouvez configurer la persistance basée sur des règles pour les services de type HTTP, SSL, RADIUS, ANY, TCP et SSL_TCP.

La persistance basée sur des règles nécessite une expression de stratégie classique ou avancée. Vous

pouvez utiliser une expression classique pour évaluer les en-têtes de demande, ou vous pouvez utiliser une expression de stratégie avancée pour évaluer les en-têtes de demande, les données de formulaire Web d'une demande, les en-têtes de réponse ou les corps de réponse. Par exemple, vous pouvez utiliser une expression classique pour configurer la persistance en fonction du contenu de l'en-tête de l'hôte HTTP. Vous pouvez également utiliser une expression de stratégie avancée pour configurer la persistance en fonction des informations de session d'application contenues dans un cookie de réponse ou un en-tête personnalisé. Pour plus d'informations sur la création et l'utilisation d'expressions de stratégie classiques et avancées, consultez la section Stratégies et expressions.

Les expressions que vous pouvez configurer dépendent du type de service pour lequel vous configurez la persistance basée sur des règles. Par exemple, certaines expressions spécifiques à RADIUS ne sont pas autorisées pour des protocoles autres que RADIUS, et les expressions basées sur des options TCP ne sont pas autorisées pour des types de service autres que le type AUY. Pour les types de service TCP et SSL_TCP, vous pouvez utiliser des expressions qui évaluent les données du protocole TCP/IP, les données de couche 2, les options TCP et les charges utiles TCP.

Remarque : Pour un cas d'utilisation impliquant la configuration de la persistance basée sur des règles basées sur les données du protocole Financial Information ExCHANGE (« FIX ») transmises via TCP, reportez-vous à la section Configuration de la persistance basée sur une paire nom-valeur dans un flux d'octets TCP.

La persistance basée sur des règles peut être utilisée pour maintenir la persistance avec des entités telles que les appliances Citrix SD-WAN, les plug-ins Citrix SD-WAN, les serveurs de cache et les serveurs d'applications.

Remarque : Sur un serveur virtuel ANY, vous ne pouvez pas configurer la persistance basée sur des règles pour les réponses.

Pour configurer la persistance en fonction d'une règle définie par l'utilisateur, vous devez d'abord configurer la persistance comme décrit dans Configuration des types de persistance qui ne nécessitent pas de règle, puis définissez le type de persistance sur RULE. Vous pouvez ensuite effectuer les procédures suivantes. Vous pouvez configurer la persistance basée sur des règles à l'aide de l'utilitaire de configuration ou de l'interface de ligne de commande.

Pour configurer la persistance en fonction de règles définies par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

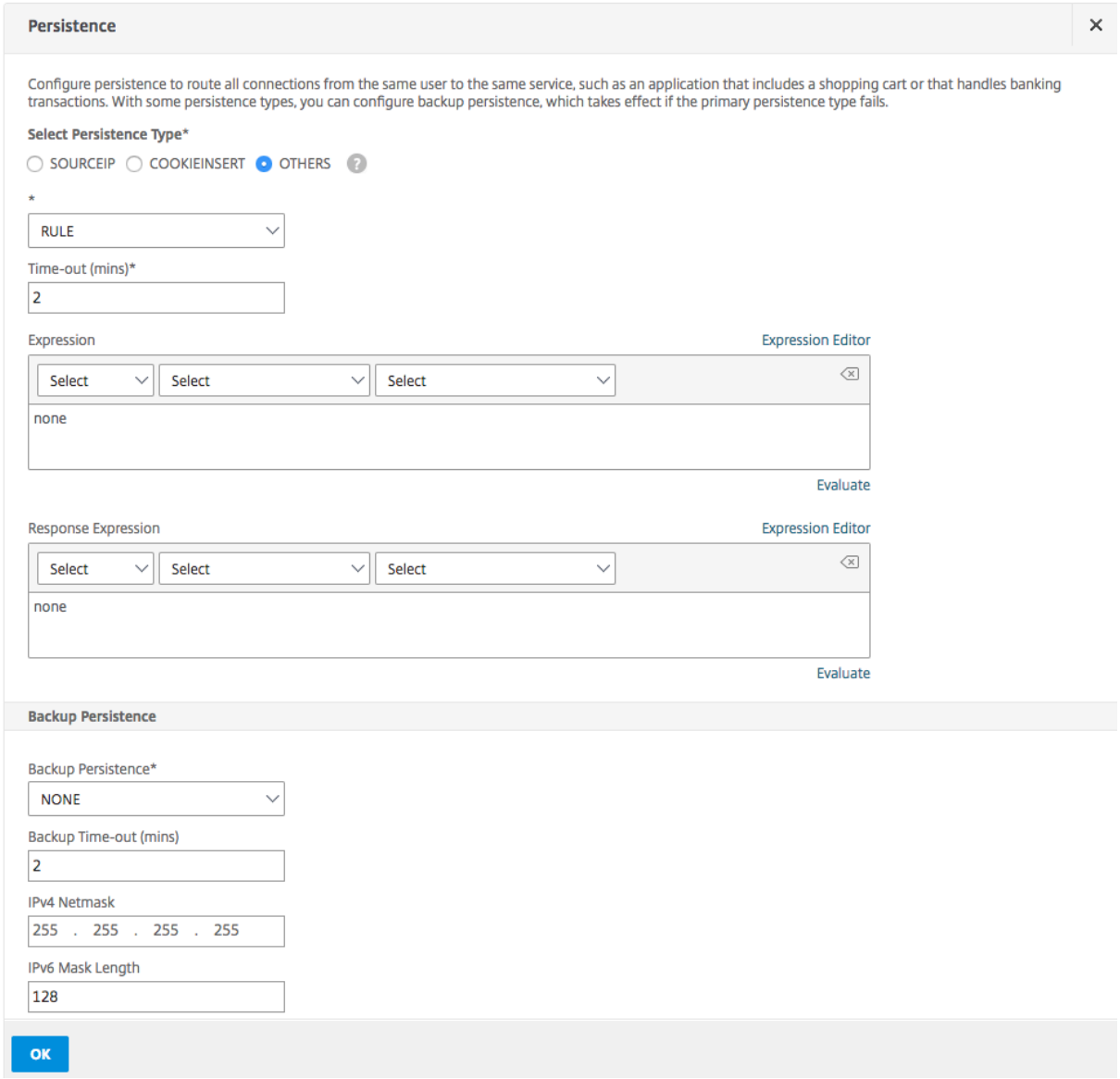
```
set lb vserver <vserverName> [-rule <expression>][-resRule <expression
    >]
<!--NeedCopy-->
```

Exemple :


```
set lb vserver vsvr_name -rule http.req.header("cookie").value(0).
    typecast_nvlist_t('=',';').value("server")

set lb vserver vsvr_name -resrule http.res.header("set-cookie").value
    (0).typecast_nvlist_t('=',';').value("server")

<!--NeedCopy-->
```

Pour configurer la persistance en fonction de règles définies par l'utilisateur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans la section Persistence, choisissez le type de persistance qui répond à vos besoins. Le type de persistance le plus approprié pour le serveur virtuel est disponible sous forme de boutons d'option. D'autres types de persistance applicables au type de serveur virtuel spécifique peuvent être sélectionnés dans la liste Autres.



> **Remarque**
>
> Avant NetScaler version 12.0 build 56.20, tous les types de persistance sont disponibles dans une seule liste déroulante Persistence sans boutons d'option.

Exemple : Expression classique pour une charge utile de demande

L'expression classique suivante crée une session de persistance basée sur la présence d'un en-tête HTTP User-Agent contenant la chaîne « MyBrowser » et dirige toutes les demandes client ultérieures contenant cet en-tête et cette chaîne vers le même serveur qui a été sélectionné pour la demande initiale.

```
1 http header User-Agent contains MyBrowser
```



```
<!--NeedCopy-->
```

Exemple : Expression de stratégie avancée pour un en-tête de demande

L'expression de stratégie avancée suivante fait la même chose que l'expression classique précédente.

HTTP.REQ.HEADER("User-Agent").CONTAINS ("MyBrowser")

Exemple : Expression de stratégie avancée pour un cookie de réponse

L'expression suivante examine les réponses pour les cookies « serveur », puis dirige toutes les demandes contenant ce cookie vers le même serveur qui a été sélectionné pour la demande initiale.

HTTP.RES.HEADER("SET-COOKIE").VALUE(0).TYPECAST_NVLIST_T('=';';').VALUE("server")

Configurer les types de persistance qui ne nécessitent pas de règle

June 20, 2023

Pour configurer la persistance, vous devez d'abord configurer un serveur virtuel d'équilibrage de charge, comme décrit dans Configuration de l'équilibrage de charge de base. Vous configurez ensuite la persistance sur le serveur virtuel.

Pour configurer la persistance sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la persistance et vérifier la configuration :

```
set lb vserver <name> -PersistenceType <type> [-timeout <integer>]

show lb vserver
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -persistenceType SOURCEIP -timeout 60

show lb vserver
<!--NeedCopy-->
```


Le délai d'expiration est la période pendant laquelle une session de persistance est en vigueur. Les valeurs par défaut et minimales du délai d'expiration (en minutes) varient en fonction du type de persistance, comme indiqué dans le tableau suivant.

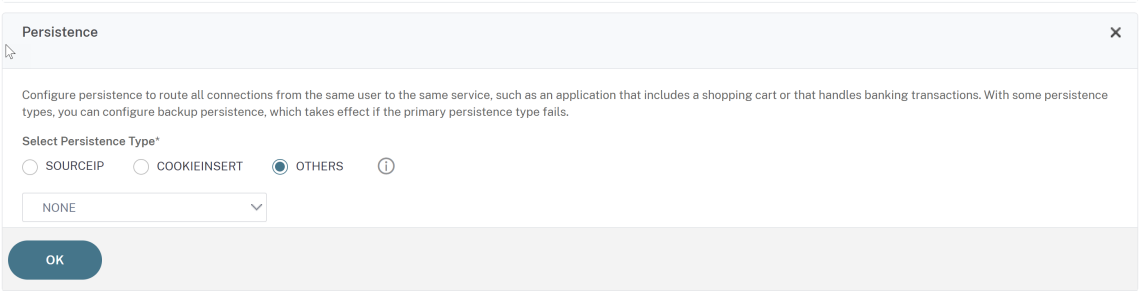
type de persistance	Valeur par défaut	Valeur minimale	Valeur maximale
Insertion de cookies/insertion de cookies de groupe	2	0	1440
Autres types de persistance	2	2	1440

Remarque

- Le type de persistance de l'insertion des cookie de groupe peut être défini sur le groupe d'équilibrage de charge.
- Pour la persistance basée sur l'adresse IP, vous pouvez également définir le paramètre PersistMask.
- Le type de persistance par défaut est défini sur AUCUN.

Pour configurer la persistance sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans la section Persistence, choisissez le type de persistance qui répond à vos besoins. Le type de persistance le plus approprié pour le serveur virtuel est disponible sous forme de boutons d'option. Les autres types de persistance applicables au type de serveur virtuel spécifique peuvent être sélectionnés dans la liste **Autres** .



Remarque Avant la version 12.0 build 56.20 de NetScaler, tous les types de persistance étaient disponibles dans une seule liste déroulante de persistance sans aucun bouton d'option.

Configurer la persistance des sauvegardes

August 20, 2021

Vous pouvez configurer un serveur virtuel pour qu'il utilise le type de persistance IP source lorsque le type de persistance principal échoue.

Le tableau suivant décrit les combinaisons de types de persistance de sauvegarde primaire et secondaire, ainsi que les conditions d'utilisation de la persistance de sauvegarde.

Persistance primaire	Persistance des sauvegardes	Lorsque la recherche de persistance principale échoue…
Insertion de cookie	IP source	L'appliance revient à la persistance basée sur la source IP uniquement lorsque le navigateur client ne renvoie aucun cookie dans la requête. Cependant, si le navigateur renvoie un cookie (pas nécessairement le cookie de persistance), il est supposé que le navigateur supporte les cookies et donc la persistance de sauvegarde n'est pas déclenchée.
Règle	IP source	L'appliance utilise la persistance basée sur la source IP lorsque le paramètre spécifié dans la règle est manquant dans la requête entrante.

Remarque

- Si le type de persistance principal est la persistance basée sur un cookie HTTP et que le type de persistance de sauvegarde est basé sur IP source, vous pouvez définir une valeur de délai d'expiration pour la persistance de la sauvegarde. Pour obtenir des instructions, reportez-vous à la section Définition d'une valeur de délai d'attente pour les connexions

clientinactives.

- Vous ne pouvez pas définir de valeur de délai d'attente pour la persistance de sauvegarde lorsque la persistance principale est basée sur des règles, car dans ce cas, la valeur de délai d'attente pour la persistance secondaire doit être la même que pour la persistance principale. Par conséquent, le primaire et le secondaire expirent en même temps.

Pour définir la persistance des sauvegardes pour un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb vserver <name> -persistenceType <PersistenceType> -
    persistenceBackup <BackupPersistenceType>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -persistenceType CookieInsert -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1  -persistenceType RULE  -rule http.req.
    header("User-Agent").value(0).contains("MyBrowser")  -
    persistenceBackup SOURCEIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP
<!--NeedCopy-->
```

Pour définir la persistance des sauvegardes pour un serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans **Paramètres avancés**, sélectionnez **Persistance**et spécifiez un type de persistance de sauvegarde.

Remarque : La persistance principale doit être définie sur COOKIEINSERT, RULE ou SSLSESSION.

Configurer les groupes de persistance

August 20, 2021

Lorsque vous disposez de serveurs équilibrés de charge qui gèrent plusieurs types de connexions différents (tels que des serveurs Web qui hébergent du multimédia), vous pouvez configurer un groupe de serveurs virtuels pour gérer ces connexions. Pour créer un groupe de serveurs virtuels, vous liez différents types de serveurs virtuels, un pour chaque type de connexion accepté par vos serveurs équilibrés de charge, en un seul groupe. Vous configurez ensuite un type de persistance pour l'ensemble du groupe.

Vous pouvez configurer la persistance basée sur IP source ou la persistance basée sur les cookies HTTP pour les groupes de persistance. Après avoir défini la persistance pour l'ensemble du groupe, vous ne pouvez pas la modifier pour les serveurs virtuels individuels du groupe. Si vous configurez la persistance sur un groupe, puis ajoutez un nouveau serveur virtuel au groupe, la persistance du nouveau serveur virtuel est modifiée pour correspondre au paramètre de persistance du groupe.

Lorsque la persistance est configurée sur un groupe de serveurs virtuels, des sessions de persistance sont créées pour les demandes initiales et les demandes suivantes sont dirigées vers le même service que la demande initiale, quel que soit le serveur virtuel du groupe qui reçoit chaque demande client.

Lorsque vous ajoutez un serveur virtuel qui possède des sessions de persistance à un groupe d'équilibrage de charge avec un type de persistance différent, les sessions persistantes existantes spécifiques à un ancien type de persistance sont supprimées. Les sessions persistantes déterminent si le trafic doit être acheminé vers le même serveur virtuel ou vers un autre serveur. Par conséquent, les connexions établies existantes ne sont pas affectées.

Le type de persistance d'un groupe d'équilibrage de charge est appliqué à tous les serveurs virtuels liés à ce groupe, quel que soit le type de protocole des serveurs virtuels. Un groupe d'équilibrage de charge prend en charge les types de persistance suivants :

- IP sourceIP
- CookieInsert
- Règle

Certains serveurs virtuels ne prennent en charge que certains types de persistance. Par exemple, un serveur virtuel de type SSL_BRIDGE peut utiliser uniquement le type de persistance SourceIP pour un groupe LB.

Si vous configurez la persistance basée sur les cookies HTTP, l'attribut de domaine du cookie HTTP est défini. Ce paramètre entraîne le logiciel client à ajouter le cookie HTTP dans les requêtes client si différents serveurs virtuels ont des noms d'hôte publics différents. Pour plus d'informations sur le type de persistance CookieInsert, voir Persistance basée sur les cookies HTTP.

Pour créer un groupe de persistance de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
bind lb group <vServerGroupName> <vServerName> -persistenceType <
   PersistenceType>
<!--NeedCopy-->
```

Exemple :

```
bind lb group Vserver-Group-1 Vserver-LB-1 -persistenceType
   CookieInsert
<!--NeedCopy-->
```

Pour modifier un groupe de serveurs virtuels à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes**de persistance, créez un groupe de persistance et spécifiez les serveurs virtuels qui doivent faire partie de ce groupe.

Pour modifier un groupe de serveurs virtuels à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb group <vServerGroupName> -PersistenceBackup <
   BackupPersistenceType> -persistMask <SubnetMaskAddress>
<!--NeedCopy-->
```

Exemple :

```
set lb group vserver-Group-1 -PersistenceBackup SourceIP -persistMask
   255.255.255.255
<!--NeedCopy-->
```

Partage de sessions persistantes entre serveurs virtuels

May 5, 2023

Dans certains environnements clients (télécommunications et FAI), un seul serveur gère à la fois le contrôle et le trafic de données. Pour une adresse IP client donnée, le contrôle et le trafic de données

doivent être dirigés vers le même serveur principal. Pour cela, un serveur virtuel est requis pour gérer le trafic d'authentification des clients, et la persistance basée sur des règles est généralement configurée sur ce serveur. Par exemple, radius.req.avp (8) .value.typecast_text_t'. Le deuxième serveur virtuel pour la gestion du trafic de données. Généralement, la persistance SourceIP est configurée dessus.

Auparavant, les entrées de persistance étaient locales sur le serveur virtuel. Si vous deviez appliquer la persistance sur plusieurs serveurs virtuels, vous deviez ajouter le serveur virtuel à un groupe d'équilibrage de charge, puis appliquer un type de persistance commun au groupe. Cette exigence ne peut pas être atteinte, car tous les serveurs virtuels liés à un groupe d'équilibrage de charge ont hérité de la persistance configurée sur le groupe.

Avec la fonctionnalité de partage de persistance entre serveurs virtuels, vous pouvez définir le nouveau `useVserverPersistency` paramètre pour un groupe d'équilibrage de charge afin de permettre au serveur virtuel du groupe d'utiliser ses propres paramètres de persistance au lieu de les hériter des paramètres de groupe. Vous pouvez configurer une persistance basée sur des règles distinctes sur chaque serveur virtuel.

Vous pouvez également désigner l'un des serveurs virtuels du groupe en tant que serveur virtuel principal. Lorsqu'un serveur virtuel est désigné comme serveur virtuel principal, seul ce serveur virtuel crée les entrées de persistance, qui sont utilisées par tous les serveurs virtuels du groupe. Si le serveur virtuel principal est en panne, l'appliance NetScaler ne crée aucune entrée de persistance.

Remarque : Le partage de persistance entre les serveurs virtuels est pris en charge uniquement pour les méthodes de persistance basées sur des règles. Configurez des paramètres de persistance basés sur des règles compatibles sur les serveurs virtuels membres.

Exemple :

Supposons que les v1 et v2 soient liées à un groupe d'équilibrage de charge, la v1 est un serveur virtuel de type RADIUS et v2 est un serveur virtuel de type HTTP. 'Radius.req.avp (8) .value.typecast_text_t' persistency est configuré sur v1 et 'client.ip.src' est configuré sur v2.

Lorsque le trafic passe par le serveur virtuel RADIUS v1, il crée une entrée persistante basée sur la chaîne de règle évaluée. Plus tard, lorsque le trafic atteint le serveur virtuel de type HTTP v2, v2 vérifie les entrées de persistance sur le groupe d'équilibrage de charge et utilise la même session de persistance pour diriger le trafic vers le même serveur principal.

Configuration du partage des sessions persistantes

Pour partager des paramètres de persistance sur le serveur virtuel dans un groupe d'équilibrage de charge, vous devez d'abord activer le paramètre UsevServerPersistency, puis désigner l'un des serveurs virtuels du groupe comme serveur principal.

Pour activer le paramètre USEVServerPersistency à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb group <name> -useVserverPersistency ( ENABLED)
<!--NeedCopy-->
```

Exemple :

```
set lb group lb_grp1 -useVserverPersistency ENABLED
<!--NeedCopy-->
```

Pour activer le paramètre UseVServerPersistency à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Groupes de persistance**.
2. Cliquez sur **Ajouter** pour ajouter un nouveau groupe ou sélectionnez un groupe existant et cliquez sur **Modifier**.
3. Sélectionnez **Utiliser la persistance Vserver**.

Pour désigner un serveur virtuel comme serveur virtuel principal à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb group <name> -useVserverPersistency ( ENABLED ) -masterVserver <
   string>
<!--NeedCopy-->
```

Exemple :

```
set lb group lb_grp1 -useVserverPersistency ENABLED - masterVserver vs1
<!--NeedCopy-->
```

Pour désigner un serveur virtuel comme serveur virtuel principal à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Groupes de persistance**.
2. Cliquez sur **Ajouter** pour ajouter un nouveau groupe ou sélectionnez un groupe existant et cliquez sur **Modifier**.

3. Sélectionnez **Utiliser la persistance Vserver**.
4. Dans la zone **Nom du serveur virtuel**, cliquez sur **+** pour ajouter le serveur virtuel au groupe. Vous pouvez sélectionner le serveur virtuel disponible ou créer un serveur virtuel.
5. Cliquez sur **Créer** si vous ajoutez un nouveau groupe ou sur **Fermer** si vous modifiez un groupe existant.
6. Sélectionnez le groupe pour lequel vous avez activé le paramètre UsevServerPersistency et cliquez sur **Modifier** pour définir un serveur virtuel comme principal afin de créer des entrées de persistance.
7. Dans la liste **Master vServer**, sélectionnez le serveur virtuel qui doit être désigné comme serveur virtuel principal.

Arguments

Utiliser la persistance du serveur V

Autorisez les serveurs virtuels d'un groupe à utiliser leurs propres paramètres de persistance pour créer des sessions persistantes, au lieu d'hériter des paramètres de persistance des paramètres du groupe. Lorsque ce paramètre est activé, la persistance ne peut pas être définie sur le groupe d'équilibrage de charge.

Lorsque ce paramètre est désactivé, les serveurs virtuels du groupe héritent des paramètres de persistance des paramètres du groupe.

Lorsque ce paramètre est activé sur le groupe d'équilibrage de charge, l'appliance NetScaler vide toutes les entrées de persistance correspondantes du groupe et des serveurs virtuels membres.

Valeurs possibles : ENABLED, DISABLED

Par défaut : DÉSACTIVÉ

Exemple :

```
set lb group lb_grp1 -useVserverPersistency ENABLED
<!--NeedCopy-->
```

masterVserver

Désignez un serveur virtuel comme serveur virtuel principal dans son groupe d'équilibrage de charge. Une fois désigné, seul le serveur virtuel principal peut créer les entrées persistantes utilisées par le groupe.

Remarque : Ce paramètre ne peut être défini que si le paramètre useVserverPersistency est activé.

Exemple :


```
set lb group lb_grp1 -masterVserver vs1
<!--NeedCopy-->
```

Exemple de configuration du partage de sessions persistantes à l'aide de l'interface de ligne de commande

Les serveurs virtuels sont créés

```
add lb vs vs1 http 10.1.10.11 80 -persistence rule -rule 'client.ip.src'

add lb vs vs2 radius 10.2.2.2 1812 -persistenceType rule -rule 'Radius.req.avp(8).value.typecast_text_t'
<!--NeedCopy-->
```

Les groupes sont créés.

```
add lb group lb_grp1 -persistenceType NONE -useVserverPersistency ENABLED
<!--NeedCopy-->
```

Un serveur virtuel d'un groupe est désigné comme serveur virtuel principal.

```
set lb group lb_grp1 -masterVserver vs1
<!--NeedCopy-->
```

Les serveurs virtuels sont liés au groupe.

```
bind lb group lb_grp1 vs1
bind lb group lb_grp1 vs2
<!--NeedCopy-->
```

Pour plus de détails, voir Configuration de l'équilibrage de charge de base et configuration des groupes de persistance.

Configurer l'équilibrage de charge RADIUS avec persistance

May 5, 2023

L'environnement réseau complexe d'aujourd'hui nécessite souvent la coordination d'une configuration d'équilibrage de charge à haut volume et haute capacité avec une authentification et une autorisation robustes. Les utilisateurs d'applications peuvent se connecter à un VPN via des points d'accès

mobiles tels que des connexions DSL ou câble de qualité grand public, WiFi ou même des nœuds d'accès à distance. Ces connexions utilisent généralement des adresses IP dynamiques, qui peuvent changer pendant la connexion.

Si vous configurez l'équilibrage de charge RADIUS sur l'appliance NetScaler pour prendre en charge les connexions clients persistantes aux serveurs d'authentification RADIUS, l'appliance utilise l'ouverture de session utilisateur ou l'attribut RADIUS spécifié au lieu de l'adresse IP du client comme ID de session, dirigeant toutes les connexions et tous les enregistrements associés à cette session utilisateur vers le même serveur RADIUS. Les utilisateurs peuvent ainsi se connecter à votre VPN à partir d'emplacements d'accès mobiles sans être déconnectés lorsque l'adresse IP du client ou le point d'accès WiFi change.

Pour configurer l'équilibrage de charge RADIUS avec persistance, vous devez d'abord configurer l'authentification RADIUS pour votre VPN. Pour plus d'informations et instructions, reportez-vous au chapitre Authentification, Authentication, Auditing (AAA) dans le trafic d'applications AAA. Choisissez également la fonction d'équilibrage de charge ou de commutation de contenu comme base de votre configuration, et assurez-vous que la fonctionnalité que vous avez choisie est activée. Le processus de configuration avec l'une ou l'autre des fonctions est presque le même.

Ensuite, vous configurez deux serveurs virtuels d'équilibrage de charge ou de commutation de contenu, l'un pour gérer le trafic d'authentification RADIUS et l'autre pour gérer le trafic de comptabilité RADIUS. Ensuite, vous configurez deux services, un pour chaque serveur virtuel d'équilibrage de charge, et vous liez chaque serveur virtuel d'équilibrage de charge à son service. Enfin, vous créez un groupe de persistance d'équilibrage de charge et définissez le type de persistance sur RULE.

Activation de la fonctionnalité d'équilibrage de charge ou de commutation de contenu

Pour utiliser la fonctionnalité d'équilibrage de charge ou de commutation de contenu, vous devez d'abord vous assurer que la fonctionnalité est activée. Si vous configurez une nouvelle appliance NetScaler qui n'a pas encore été configurée, ces deux fonctionnalités sont déjà activées. Vous pouvez donc passer à la section suivante. Si vous configurez une appliance NetScaler avec une configuration précédente et que vous n'êtes pas certain que la fonctionnalité que vous utilisez est activée, vous devez le faire maintenant.

- Pour obtenir des instructions sur l'activation de la fonction d'équilibrage de charge, reportez-vous à Activation de l'équilibra
- Pour obtenir des instructions sur l'activation de la fonction de commutation de contenu, voir Activation du changement

Configuration des serveurs virtuels

Après avoir activé la fonctionnalité d'équilibrage de charge ou de commutation de contenu, vous devez ensuite configurer deux serveurs virtuels pour prendre en charge l'authentification RADIUS :

- **Serveur virtuel d'authentification RADIUS.** Ce serveur virtuel et son service associé traitent le trafic d'authentification vers votre serveur RADIUS. Le trafic d'authentification consiste en des connexions associées aux utilisateurs qui se connectent à votre application protégée ou à votre réseau privé virtuel (VPN).
- **Serveur virtuel de comptabilité RADIUS.** Ce serveur virtuel et son service associé gère les connexions comptables à votre serveur RADIUS. Le trafic comptable est constitué de connexions qui suivent les activités d'un utilisateur authentifié sur votre application protégée ou VPN.

Important : Vous devez créer une paire de serveurs virtuels d'équilibrage de charge ou une paire de serveurs virtuels de commutation de contenu à utiliser dans votre configuration de persistance RADIUS. Vous ne pouvez pas mélanger les types de serveurs virtuels.

Pour configurer un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel d'équilibrage de charge et vérifier la configuration :

```
1 add lb vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
      <rule>
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Pour configurer un serveur virtuel d'équilibrage de charge existant, remplacez la `add lb virtual server` commande précédente par la `set lb vserver` commande, qui prend les mêmes arguments.

Pour configurer un serveur virtuel de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel de commutation de contenu et vérifier la configuration :

```
1 add cs vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
      <rule>
2
3 show cs vserver <name>
4 <!--NeedCopy-->
```

Pour configurer un serveur virtuel de commutation de contenu existant, remplacez la `add cs vserver` commande précédente par la `set cs vserver` commande, qui prend les mêmes arguments.

Exemple :

```
add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
<!--NeedCopy-->
```

Pour configurer un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** ou accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels>**, puis configurez un serveur virtuel.

Configuration des services

Après avoir configuré vos serveurs virtuels, vous devez ensuite configurer deux services, un pour chacun des serveurs virtuels que vous avez créés.

Remarque : Une fois configurés, ces services sont à l'état DÉSACTIVÉ jusqu'à ce que l'appliance NetScaler puisse se connecter aux adresses IP d'authentification et de comptabilité de votre serveur RADIUS et surveiller leur état. Pour obtenir des instructions, reportez-vous à la section Configuration des services.

Liaison de serveurs virtuels aux services

Après avoir configuré vos services, vous devez ensuite lier chacun des serveurs virtuels que vous avez créés au service approprié.Pour obtenir des instructions, reportez-vous à la section Liaison des services au serveur virtuel.

Configuration d'un groupe de persistance pour Rayon

Après avoir lié vos serveurs virtuels d'équilibrage de charge aux services correspondants, vous devez configurer votre configuration d'équilibrage de charge RADIUS pour prendre en charge la persistance. Pour ce faire, vous configurez un groupe de persistance d'équilibrage de charge qui contient

vos serveurs et services virtuels d'équilibrage de charge RADIUS, et vous configurez ce groupe de persistance d'équilibrage de charge pour utiliser la persistance basée sur des règles. Un groupe de persistance est requis car les serveurs virtuels d'authentification et de comptabilité sont différents et le message d'authentification et de comptabilisation pour un seul utilisateur doit atteindre le même serveur RADIUS. Le groupe de persistance permet d'utiliser la même session pour les deux serveurs virtuels. Pour obtenir des instructions, reportez-vous à la section Configuration des groupes de persistance.

Configuration du secret partagé RADIUS

À partir de la version 12.0, une appliance NetScaler prend en charge le secret partagé RADIUS. Un client et un serveur RADIUS communiquent entre eux à l'aide d'un secret partagé configuré sur le client et sur le serveur. Les transactions entre un client RADIUS et un serveur sont authentifiées à l'aide d'un secret partagé. Ce secret est également utilisé pour crypter certaines informations dans le paquet RADIUS.

Scénarios de validation de clés secrètes partagées RADIUS

La validation de la clé **secrète partagée RADIUS** se produit dans les scénarios suivants :

- La**clé secrète partagée RADIUS est configurée à la fois pour le client Radius et pour le serveur Radius :** l'appliance NetScaler utilise la clé secrète RADIUS à la fois côté client et côté serveur. Si la vérification aboutit, l'appliance autorise le message RADIUS à passer. Dans le cas contraire, il supprime le message RADIUS.
- La**clé secrète partagée RADIUS n'est configurée ni pour le client Radius ni pour le serveur Radius : l'** appliance NetScaler supprime le message RADIUS, car la validation de la clé secrète partagée ne peut pas être effectuée sur un nœud sur lequel aucune clé radkey n'est configurée.
- **La clé secrète partagée RADIUS n'est pas configurée à la fois pour le client RADIUS et pour le serveur RADIUS :** l'appliance NetScaler contourne la validation de la clé secrète RADIUS et autorise le passage des messages RADIUS.

Vous pouvez configurer un secret partagé RADIUS par défaut ou le configurer par client ou par sous-réseau. Il est recommandé d'ajouter une clé secrète partagée RADIUS pour tous les déploiements pour lesquels la politique RADIUS est configurée. L'appliance utilise l'adresse IP source du paquet RADIUS pour décider quel secret partagé utiliser. Vous pouvez configurer un client et un serveur RADIUS ainsi que le secret partagé correspondant comme suit :

À l'invite CLI, tapez :

```
add radiusNode <clientPrefix/Subnet> -radKey <Shared_secret_key>
<!--NeedCopy-->
```


Arguments

Adresse IP

Adresse IP ou sous-réseau du client RADIUS au format CIDR. L'appliance utilise l'adresse IP source d'un paquet de demande entrant pour correspondre à l'adresse IP du client. Au lieu de configurer une adresse IP client, vous pouvez configurer l'adresse réseau du client. Le préfixe le plus long est mis en correspondance pour identifier le secret partagé pour une demande client entrante.

Radkey

Secret partagé entre le client, l'appliance NetScaler et le serveur. Longueur maximale : 31.

```
add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
   TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
   TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add service radius_auth_service1 192.168.41.68 RADIUS 1812

add service radius_acct_service1 192.168.41.70 RADIUS 1813

bind lb vserver radius_auth_vs1 radius_auth_service1

bind lb vserver radius_acct_vs1 radius_acct_service[1-3]

add radiusNode 192.168.41.0/24 -radKey  serverkey123

add radiusNode 203.0.113.0/24 -radkey clientkey123
<!--NeedCopy-->
```

Un secret partagé doit être configuré à la fois pour un client et un serveur RADIUS. La commande est la même. Le sous-réseau détermine si le secret partagé est destiné à un client ou à un serveur.

Par exemple, si le sous-réseau spécifié est un sous-réseau client, le secret partagé est pour le client. Si le sous-réseau spécifié est un sous-réseau serveur (192.168.41.0/24 dans l'exemple précédent), le secret partagé concerne le serveur.

Un sous-réseau de 0.0.0.0/0 implique qu'il s'agit du secret partagé par défaut pour tous les clients et serveurs.

> **Remarque :**
>
> Seules les méthodes d'authentification PAP et CHAP sont prises en charge avec le secret partagé RADIUS.

Afficher les sessions de persistance

May 5, 2023

Vous pouvez consulter les différentes sessions de persistance qui sont en vigueur globalement ou pour un serveur virtuel en particulier.

> **Remarque** : Une appliance NetScaler nCore utilise plusieurs cœurs de processeur pour la gestion des paquets. Le cœur du processeur est propriétaire de chaque session de l'appliance. Si l'appliance reçoit une demande pour laquelle aucune session n'existe, une session est créée et l'un des cœurs est désigné comme propriétaire de cette session.
>
> Les demandes ultérieures qui appartiennent à cette session peuvent ne pas toujours arriver et être traitées par le noyau du propriétaire. Dans ce cas, la messagerie inter-cœur garantit que les informations de session sur le cœur propriétaire sont toujours à jour.

Toutefois, lorsqu'un noyau reçoit une demande appartenant à une session de persistance appartenant à un autre noyau, la messagerie inter-cœur n'actualise pas la valeur de délai d'expiration de la session de persistance.

Par conséquent, dans la sortie des commandes show lb PersistentSessions exécutées successivement, qui affichent uniquement les valeurs de délai d'expiration provenant des cœurs propriétaires, la valeur de délai d'expiration d'une session de persistance peut diminuer à 0 (zéro), même si la session de persistance reste active.

Pour afficher les sessions de persistance à l'aide de l'interface de ligne de commande

À l'invite de commandes, pour afficher les sessions de persistance associées à tous les serveurs virtuels, tapez :

```
show lb persistentSessions [<vServer>]
<!--NeedCopy-->
```

À l'invite de commandes, pour afficher les sessions de persistance liées à un serveur virtuel, tapez :

```
show lb persistentSessions <vServername>
<!--NeedCopy-->
```

Exemple :

```
show lb persistentSessions myVserver
<!--NeedCopy-->
```


Pour afficher les sessions de persistance à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Sessions persistantes du serveur virtuel**.

Séances de persistance claires

May 5, 2023

Vous devrez peut-être effacer les sessions de persistance de l'appliance NetScaler si les sessions n'arrivent pas à expiration. Vous pouvez effectuer l'une des opérations suivantes :

- Effacez simultanément toutes les sessions de tous les serveurs virtuels.
- Effacez toutes les sessions d'un serveur virtuel donné en une seule fois.
- Efface une session particulière associée à un serveur virtuel donné.

Pour effacer une session de persistance à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour effacer les sessions de persistance et vérifier la configuration :

```
clear lb persistentSessions [<vServer> [-persistenceParam <string>]]

show persistentSessions <vServer>
<!--NeedCopy-->
```

Exemples :

L'exemple 1 efface toutes les sessions de persistance pour le serveur virtuel lbvip1 d'équilibrage de charge.

L'exemple 2 affiche d'abord les sessions de persistance pour le serveur virtuel d'équilibrage de charge lbvip1, efface la session avec le paramètre de persistance xls, puis affiche les sessions de persistance pour vérifier que la session a été effacée.

Exemple 1 :

```
> clear persistentSessions lbvip1
 Done
> show persistentSessions
 Done
>
<!--NeedCopy-->
```

Exemple 2 :


```
> show persistentSessions lbvip1
Type        SRC-IP    ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0   ...    xls
RULE        0.0.0.0   ...    txt
RULE        0.0.0.0   ...    html
 Done
> clear persistentSessions lbvip1 -persistenceParam xls
 Done
> show persistentSessions lbvip1
Type        SRC-IP    ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0   ...    txt
RULE        0.0.0.0   ...    html
 Done
>
<!--NeedCopy-->
```

Pour effacer les sessions de persistance à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Effacer les sessions persistantes**.

Remplacer les paramètres de persistance pour les services surchargés

May 5, 2023

Lorsqu'un service est chargé ou n'est pas disponible, le service aux clients est dégradé. Dans ce cas, vous devrez peut-être configurer l'appliance NetScaler pour transférer temporairement vers d'autres services les demandes qui seraient autrement incluses dans la session de persistance associée au service surchargé. En d'autres termes, vous devrez peut-être remplacer le paramètre de persistance configuré pour le serveur virtuel d'équilibrage de charge. Vous pouvez obtenir cette fonctionnalité en définissant le paramètre skippersistency. Lorsque ce paramètre de saut de persistance est défini et si le serveur virtuel reçoit de nouvelles connexions pour un service surchargé, ce qui suit se produit.

- Le serveur virtuel ignore les sessions de persistance existantes associées à ce service, jusqu'à ce que le service retourne à un état auquel il peut accepter les demandes.
- Les sessions de persistance associées à d'autres services ne sont pas affectées.

Cette fonctionnalité est disponible uniquement pour les serveurs virtuels de type ANY ou UDP.

Dans les configurations d'équilibrage de charge du répéteur de branche, vous devez également configurer un moniteur de charge et le lier au service. Le moniteur supporte le service des décisions d'équilibrage de charge suivantes jusqu'à ce que la charge sur le service soit ramenée en dessous du

seuil configuré. Pour plus d'informations sur la configuration d'un moniteur de charge pour votre serveur virtuel, voir Présentation des moniteurs de charge.

Vous pouvez configurer le serveur virtuel pour effectuer l'une des actions suivantes avec les demandes qui, autrement, feraient partie de la session de persistance :

- **Envoyez chaque demande à l'un des autres services.** Le serveur virtuel prend une décision d'équilibrage de charge et envoie chaque demande à l'un des autres services en fonction de la méthode d'équilibrage de charge. Si tous les services sont surchargés, les demandes sont abandonnées jusqu'à ce qu'un service devienne disponible.

  Les serveurs virtuels basés sur des caractères génériques et basés sur des adresses IP prennent en charge cette option. Cette action est appropriée pour tous les déploiements, y compris les déploiements dans lesquels le serveur virtuel équilibre la charge, les appliances Branch Repeater ou les pare-feux.

- **Contournez la configuration du service serveur virtuel.** Le serveur virtuel ne prend pas de décision d'équilibrage de charge. Au lieu de cela, il relie simplement chaque demande à un serveur physique en fonction de l'adresse IP de destination dans la demande.

  Seuls les serveurs virtuels génériques de type ANY et UDP prennent en charge l'option de contournement. Les serveurs virtuels Wildcard ont une combinaison *:* IP et port. Cette action est appropriée pour les déploiements dans lesquels vous utilisez le serveur virtuel pour équilibrer la charge des appliances Branch Repeater ou des pare-feux. Dans ces déploiements, l'appliance NetScaler transmet d'abord une demande à une appliance Branch Repeater ou à un pare-feu, puis transmet la réponse traitée à un serveur physique. Le serveur virtuel envoie des demandes directement à ses adresses IP de destination dans les conditions suivantes.

  - Vous configurez le serveur virtuel pour contourner la configuration du serveur virtuel—service pour les services surchargés.
  - L'appliance ou le pare-feu Branch Repeater est surchargé.

  Le serveur virtuel envoie des requêtes directement à leurs adresses IP de destination jusqu'à ce que l'appliance Branch Repeater ou le pare-feu puisse accepter les demandes.

Pour remplacer les paramètres de persistance des services surchargés à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour remplacer les paramètres de persistance des services surchargés et vérifier la configuration :

```
set lb vserver <name> -skippersistency <skippersistency>

show lb vserver <name>
<!--NeedCopy-->
```


Exemple

```
> set lb vserver mylbvserver -skippersistency ReLb
 Done
> show lb vserver mylbvserver
    mylbvserver (\*:\*) - ANY Type: ADDRESS
       . . .
       . . .
 Skip Persistency: ReLb
       . . .
 Done
>
<!--NeedCopy-->
```

Pour remplacer les paramètres de persistance des services surchargés à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et sélectionnez le serveur virtuel de type UDP ou ANY.
2. Dans le volet Paramètres avancés, sélectionnez Paramètres de trafic et spécifiez le type d'Ignorer la persistance.

Dépannage

May 5, 2023

- **Les statistiques de l'appliance NetScaler VPX indiquent que l'appliance a atteint la limite de persistance de session. Par conséquent, les sessions de persistance échouent. Est-il possible d'augmenter la limite de persistance des sessions ?**

  Cause : L'appliance NetScaler a la limite système de 250 000 sessions de persistance pour un cœur.

  Résolution : Pour résoudre ce problème, vous pouvez effectuer l'une des tâches suivantes :

  - Réduisez la valeur du délai d'attente pour la persistance
  - Augmenter le nombre de cœurs de l'appliance

- **Après avoir configuré la persistance de l'insertion de cookies sur l'appliance NetScaler, les utilisateurs signalent que les connexions fonctionnent correctement pendant un certain temps, puis commencent à être déconnectées. Quelles sont les meilleures pratiques à suivre lors de la configuration de la persistance ?**

Cause : Par défaut, la valeur du délai d'expiration pour la persistance de l'insertion de cookies est de 120 secondes.

Résolution : lorsque vous configurez la persistance pour des applications pour lesquelles le temps d'inactivité ne peut pas être déterminé, définissez la valeur du délai d'expiration de la persistance de l'insertion des cookies sur 0. Avec ce paramètre, la connexion n'est pas interrompue.

- **Après avoir configuré un serveur virtuel HTTP sur l'appliance NetScaler, je dois m'assurer qu'un utilisateur se connecte toujours au même serveur pour le contenu demandé. J'ai donc configuré la persistance SourceIP. Désormais, l'augmentation de la valeur du délai d'expiration pour la persistance introduit de la latence. Comment puis-je augmenter la valeur du délai d'attente sans affecter les performances ?**

  Résolution : Envisagez d'utiliser la persistance de l'insertion des cookies avec la valeur du délai d'expiration définie sur 0. Ce paramètre active les paramètres de persistance de longue durée, car l'appliance ne précise pas de délai d'expiration du cookie.

- **Après avoir configuré la persistance de l'insertion de cookies sur l'appliance NetScaler, cela fonctionne comme prévu lorsque des clients du même fuseau horaire accèdent au contenu. Toutefois, lorsqu'un client d'un autre fuseau horaire tente de se connecter, le délai de connexion est immédiatement dépassé.**

  Cause : La persistance de l'insertion de cookies basée sur le temps fonctionne comme prévu lorsqu'un client du même fuseau horaire établit une connexion. Toutefois, lorsque la machine cliente et l'appliance NetScaler se trouvent dans des fuseaux horaires différents, le cookie n'est pas valide. Par exemple, lorsqu'un client situé dans le fuseau horaire EST envoie un cookie à 11 h 00 EST à une appliance NetScaler située dans le fuseau horaire PST, l'appliance reçoit le cookie à 14 h 00 PST. En raison de la différence de temps, le cookie n'est pas valide et la connexion est immédiatement expiré.

  Résolution : définissez la valeur du délai d'expiration pour la persistance de l'insertion de cookies sur 0.

- **Une appliance NetScaler est utilisée pour équilibrer la charge des serveurs d'applications, tels que le serveur Oracle Weblogic. Pour garantir que les clients obtiennent des connexions persistantes à ces serveurs, la persistance SourceIP est configurée. Il fonctionne comme prévu lorsqu'une connexion est établie à partir d'un ordinateur. Toutefois, lorsque des clients légers tentent d'établir une connexion via un serveur Terminal Server et que, par conséquent, l'appliance reçoit des demandes de plusieurs clients provenant de la même adresse IP (l'adresse IP du serveur de terminal). Par conséquent, les connexions provenant de tous les clients légers sont dirigées vers le même serveur d'applications. Est-il possible de configurer la persistance des demandes provenant de clients légers individuels en fonction de l'adresse IP du client ?**

Cause : l'appliance NetScaler reçoit des demandes du serveur de terminaux et l'adresse IP source de la demande reste la même. Par conséquent, l'appliance ne peut pas faire la distinction entre les demandes reçues des clients légers et assurer la persistance en fonction des demandes provenant des clients légers.

Résolution : Pour éviter ce problème, vous pouvez configurer la persistance des règles en fonction d'une valeur de paramètre unique pour chaque client léger.

- **L'appliance NetScaler est utilisée pour équilibrer la charge des serveurs d'interface Web. Lors de l'accès aux serveurs, l'utilisateur reçoit le message d'erreur « State Error ». En outre, lorsque l'un des serveurs d'interface Web est arrêté ou n'est pas disponible, certains utilisateurs reçoivent un message d'erreur.**

  Cause : Le manque de persistance des serveurs d'interface Web peut entraîner des messages d'erreur lorsqu'un utilisateur tente de se connecter au serveur.

  Résolution : Citrix vous recommande de spécifier la méthode de persistance de l'insertion de cookies sur l'appliance NetScaler lors de l'équilibrage de charge des serveurs d'interface Web.

Insérer des attributs de cookie aux cookies générés par ADC

May 5, 2023

Les administrateurs Web peuvent insérer d'autres attributs de cookie dans les cookies générés par l'appliance NetScaler. Ces attributs de cookies supplémentaires aident à appliquer les politiques requises pour les cookies générés par ADC en fonction du modèle d'accès à l'application.

Les fonctionnalités suivantes utilisent les cookies générés par l'ADC pour assurer la persistance.

- Persistance des cookie d'équilibrage de charge
- Persistance des cookie du groupe d'équilibrage de charge
- Persistance du site GSLB
- Persistance des cookies de commutation de contenu

Vous pouvez insérer d'autres attributs de cookie dans les cookies générés par ADC à l'aide des paramètres suivants :

- **LiteralAdcCookieAttribute :** ajoutez d'autres attributs de cookie au cookie généré par ADC, sous forme de chaîne.
- **ComputedAdcCookieAttribute :** Utilisez une variable ADC ns pour ajouter conditionnellement des attributs de cookie au cookie généré par ADC, en fonction des attributs client ou serveur, par exemple, la version de l'agent utilisateur.

> **Remarque**
>
> Vous ne pouvez pas configurer à la fois l'attribut de cookie ADC littéral et l'attribut de cookie ADC calculé simultanément sur le paramètre d'équilibrage de charge ou dans un seul profil d'équilibrage de charge.

Cas d'utilisation : configurer l'attribut de cookie SameSite

Chaque cookie est associé à un domaine. Lorsque le domaine d'un cookie correspond au domaine du site Web indiqué dans la barre d'adresse de l'utilisateur, cela est considéré comme un contexte de même site (ou de première partie). Si le domaine associé à un cookie correspond à un service externe et non au site Web indiqué dans la barre d'adresse de l'utilisateur, cela est considéré comme un contexte intersite (ou tiers).

L'attribut **SameSite** indique au navigateur si le cookie peut être utilisé pour un contexte intersite ou uniquement pour un contexte de même site. De plus, si une application a l'intention d'être consultée dans un contexte intersite, elle ne peut le faire que via la connexion HTTPS. Pour plus de détails, voir la RFC6265.

Jusqu'en février 2020, la propriété **SameSite** n'était pas définie de manière explicite dans NetScaler. Le navigateur a pris la valeur par défaut None et n'a pas eu d'impact sur les déploiements de NetScaler.

Toutefois, la mise à niveau de certains navigateurs, tels que Google Chrome 80, modifie le comportement par défaut des cookies entre domaines. L'attribut **SameSite** peut être défini sur l'une des valeurs suivantes. La valeur par défaut de Google Chrome est définie sur Lax.

- **Aucun :** indique que le navigateur doit utiliser un cookie dans un contexte intersite uniquement sur les connexions sécurisées.
- **Lax :** indique que le navigateur doit utiliser un cookie pour les demandes dans le même contexte de site. Dans le contexte inter-site, seules les méthodes HTTP sûres comme la requête GET peuvent utiliser le cookie.
- **Strict :** Utilisez le cookie uniquement dans le contexte du même site.

S'il n'y a pas d'attribut SameSite dans le cookie, Google Chrome suppose la fonctionnalité SameSite=LAX.

> **Remarque**
>
> Pour certaines versions d'autres navigateurs, la valeur par défaut de l'attribut SameSite peut être définie sur **Aucun**. Dans certaines versions du navigateur, « Samesite = none » peut être traité différemment. Par exemple, les navigateurs suivants rejettent un cookie avec « SameSite = none » :
>
> - Versions de Chrome de Chrome 51 à Chrome 66 (inclus sur les deux extrémités)
> - Versions du navigateur UC sur Android antérieures à la version 12.13.2

Configurer les cookies générés par ADC

Pour configurer les attributs des cookie générés par ADC, vous devez effectuer les opérations suivantes :

1. Créer un serveur virtuel d'équilibrage de charge
2. Définissez les attributs du cookie ADC pour le serveur virtuel d'équilibrage de charge, via les paramètres LB ou le profil LB.
3. Si vous utilisez un profil LB, définissez le profil LB sur un serveur virtuel d'équilibrage de charge.
4. Si vous choisissez d'utiliser l'attribut de cookie ADC calculé, configurez la politique de réécriture associée.

> **Remarque**
>
> Si un profil LB est lié à un serveur virtuel LB, la configuration du paramètre de profil est prise en compte au lieu de la configuration globale des paramètres LB.

Vous pouvez définir les attributs de cookie générés par ADC par les méthodes suivantes :

- Définition des attributs des cookie ADC dans les paramètres d'équilibrage de charge
- Définition des attributs des cookie ADC dans le profil d'équilibrage de charge

Définition des attributs des cookie ADC dans les paramètres d'équilibrage de charge à l'aide de l'interface de ligne de commande

Pour appliquer une politique de manière uniforme aux cookies générés par ADC pour toutes les applications configurées sur l'appliance NetScaler, vous pouvez définir l'attribut du cookie ADC dans les paramètres LB globaux.

Le paramètre **Literal ADC Cookie Attribut** vous permet d'insérer inconditionnellement les attributs de cookie dans le cookie généré par ADC.

À l'invite de commande, tapez :

```
set lb parameter -LiteralADCCookieAttribute <string>
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -LiteralADCCookieAttribute SameSite=None
<!--NeedCopy-->
```

Le paramètre d' **attribut de cookie ADC calculé** vous permet d'insérer de manière conditionnelle les attributs du cookie, en fonction des attributs du client ou du serveur, dans le cookie généré par l'ADC.

À l'invite de commande, tapez :

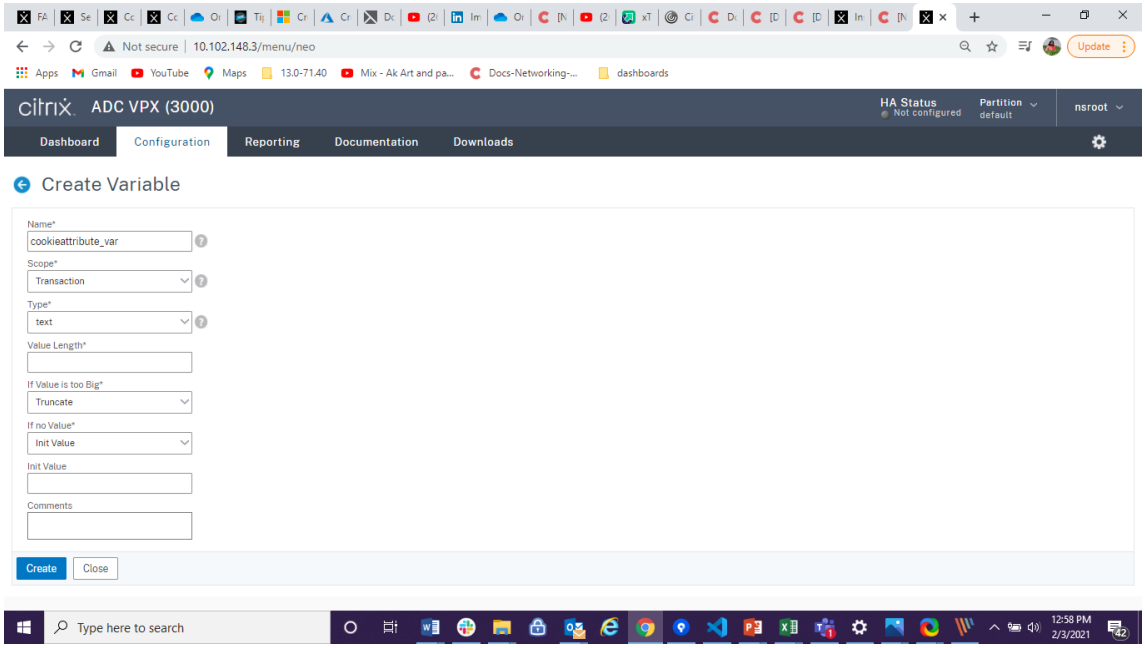

```
set lb parameter -ComputedADCCookieAttribute <ns variable>
<!--NeedCopy-->
```

Exemple :

```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
set lb parameter -ComputedADCCookieAttributE "$cookieattribute_var"
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
add rewrite policy append_samesite_attribute true samesiteassign

bind rewrite global exception_samesite_attribute 90 110 -type
    RES_OVERRIDE
bind rewrite global append_samesite_attribute 100 110 -type
    RES_OVERRIDE
<!--NeedCopy-->
```

Configuration des variables à l'aide de l'interface graphique

1. Accédez à **AppExpert > Variables**, puis cliquez sur **Ajouter**.
2. Sur la page **Créer une variable**, sélectionnez **Étendue** en tant que **transaction** et **Type** en tant que **texte** dans le menu déroulant.

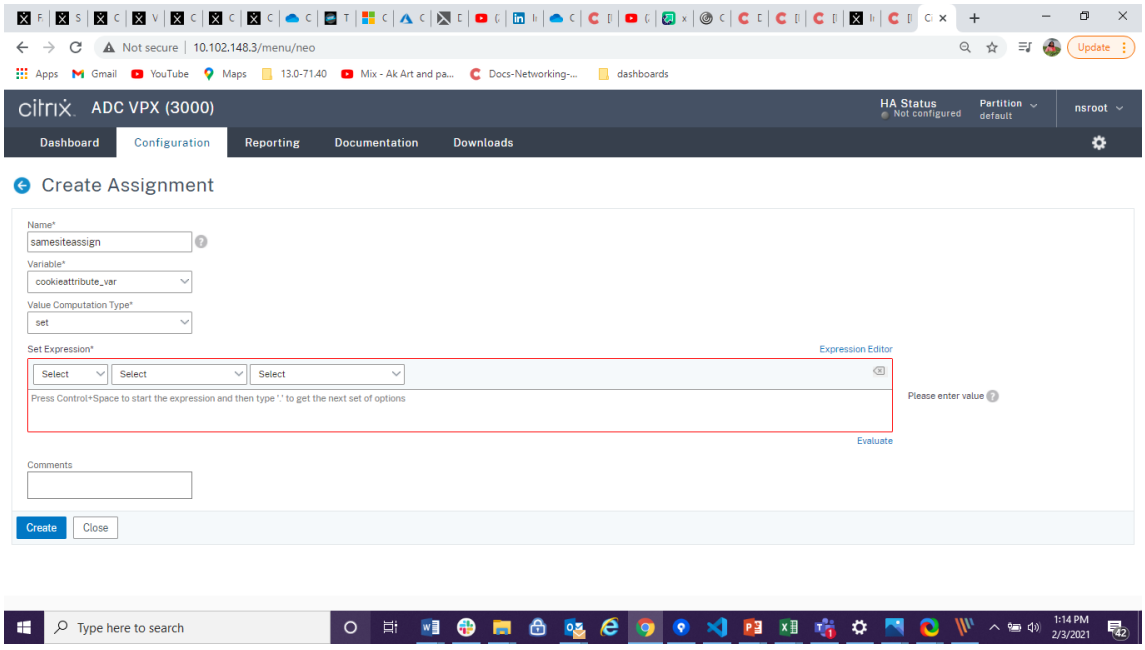


3. Entrez d'autres détails, puis cliquez sur **Créer**.

Création d'un devoir à l'aide de l'interface graphique

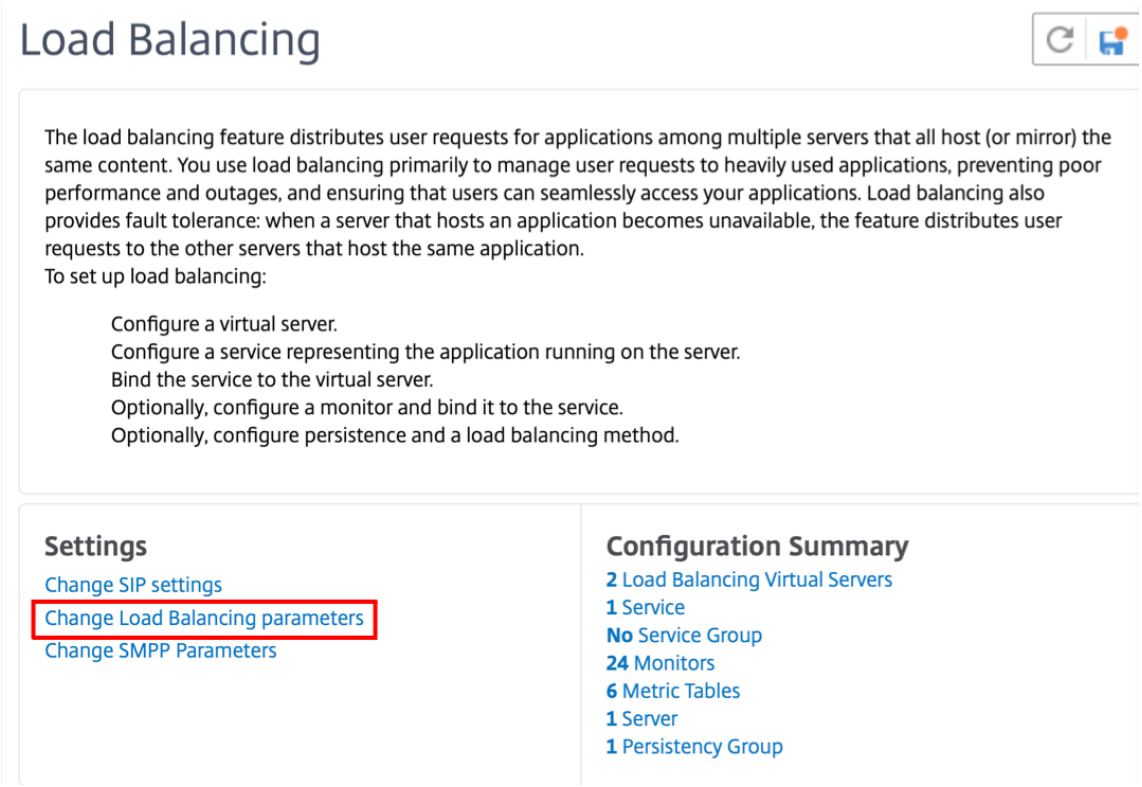
Après avoir configuré une variable, vous pouvez lui attribuer une valeur ou spécifier l'opération à effectuer sur la variable en créant une affectation.

1. Accédez à **AppExpert > Affectations**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un devoir**, entrez les détails, puis cliquez sur **Créer**.



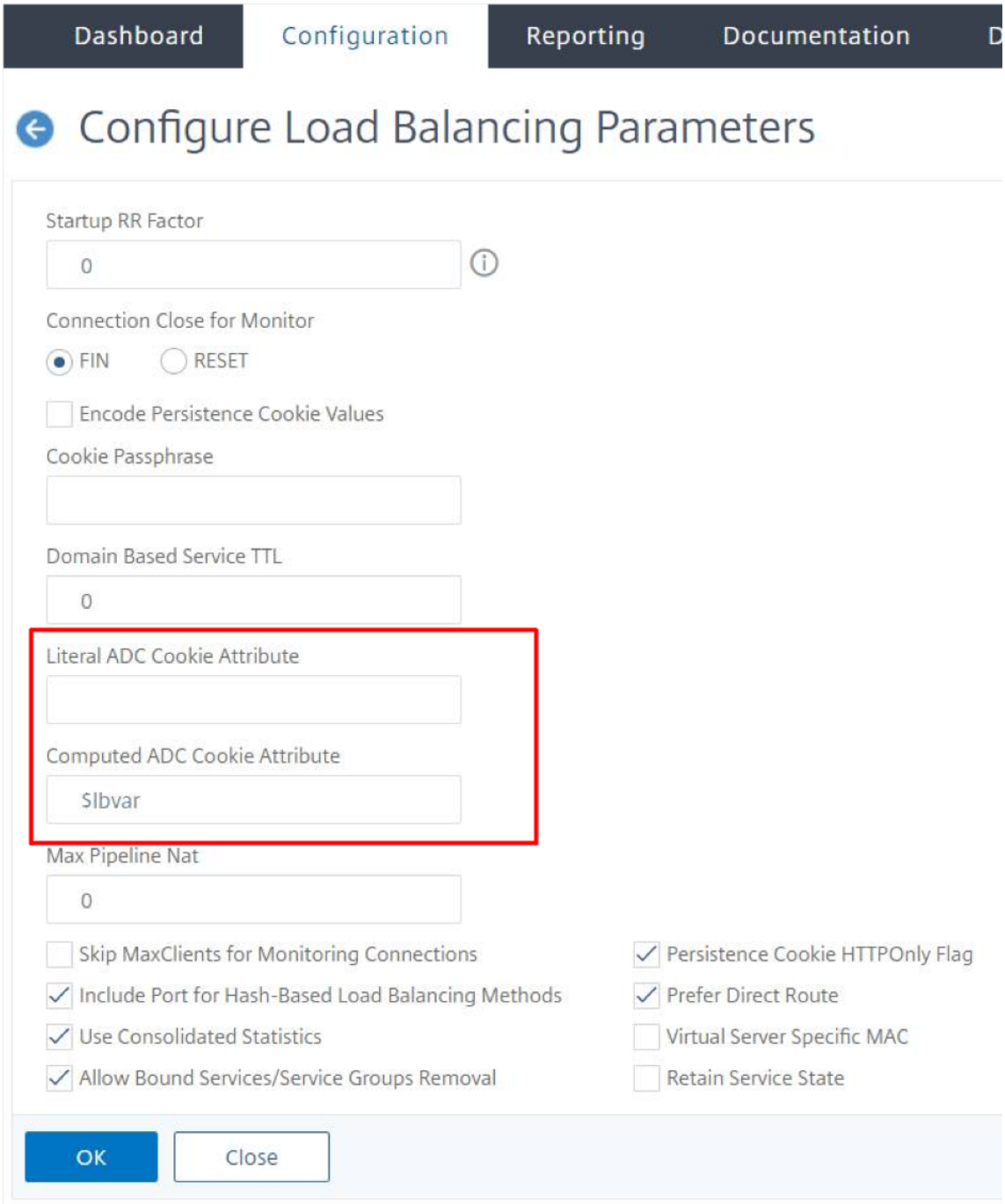
Définition des attributs des cookie ADC dans les paramètres d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Modifier les paramètres d'équilibrage de charge**.



2. Dans le volet **Configurer les paramètres d'équilibrage de charge**, entrez les valeurs appropriées pour l'un des champs en fonction de vos besoins :

   - **Literal ADC Cookie Attribute**
   - **Computed ADC Cookie Attribute**



3. Cliquez sur **OK**.

Définition des attributs des cookie ADC dans le profil d'équilibrage de charge à l'aide de l'interface de ligne de commande

Pour appliquer une politique à une application spécifique configurée sur l'appliance NetScaler, vous pouvez définir les paramètres d'attribut des cookie dans le profil LB lié au serveur virtuel LB spécifique

à l'application.

Le paramètre d' **attribut Cookie ADC Literal** dans le profil LB vous permet d'insérer inconditionnellement les attributs de cookie dans le cookie généré par ADC spécifique à un serveur virtuel.

À l'invite de commande, tapez :

```
add lb profile <profile name> -LiteralADCCookieAttribute <string>
<!--NeedCopy-->
```

Exemple :

```
add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite
    =None
add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
<!--NeedCopy-->
```

Le paramètre d' **attribut de cookie ADC calculé** dans le profil LB vous permet d'insérer de manière conditionnelle les attributs du cookie en fonction des attributs du client ou du serveur, dans le cookie généré par l'ADC. Définissez ensuite ce profil LB sur un serveur virtuel LB.

À l'invite de commande, tapez :

```
add lb profile <profile name> -ComputedADCCookieAttribute <ns variable>
<!--NeedCopy-->
```

Exemple :

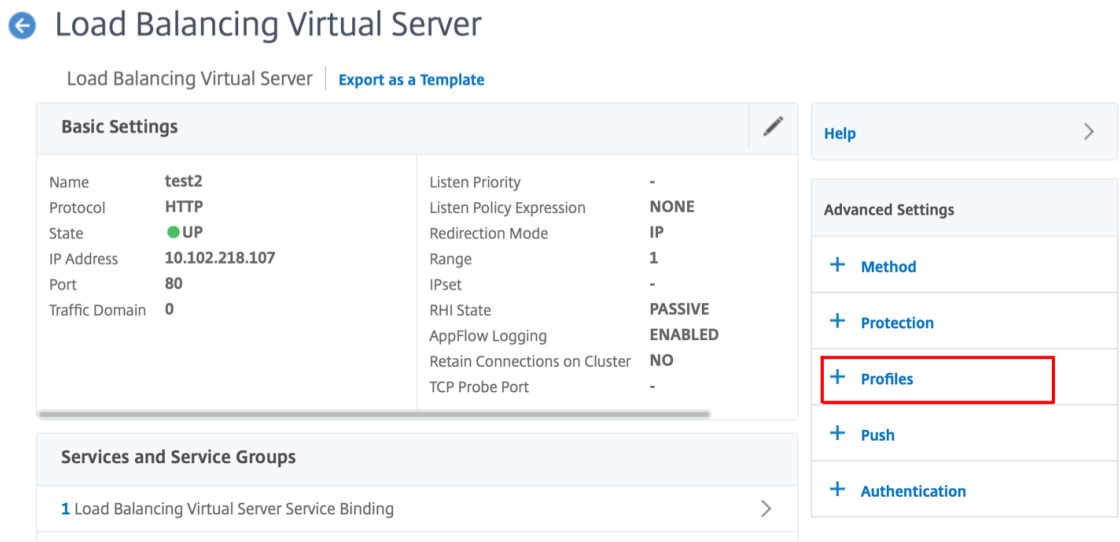
```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""
add lb profile LB-Vserver-Profile-1 -ComputedADCCookieAttributE "
    $cookieattribute_var"

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
```



```
add rewrite policy append_samesite_attribute true samesiteassign

add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
bind lb vserver LB-VServer-1 -policyName exception_samesite_attribute -
    priority 90 -gotoPriorityExpression 110 -type RESPONSE
bind lb vserver LB-VServer-1 -policyName append_samesite_attribute -
    priority 100 -gotoPriorityExpression 110 -type RESPONSE
<!--NeedCopy-->
```

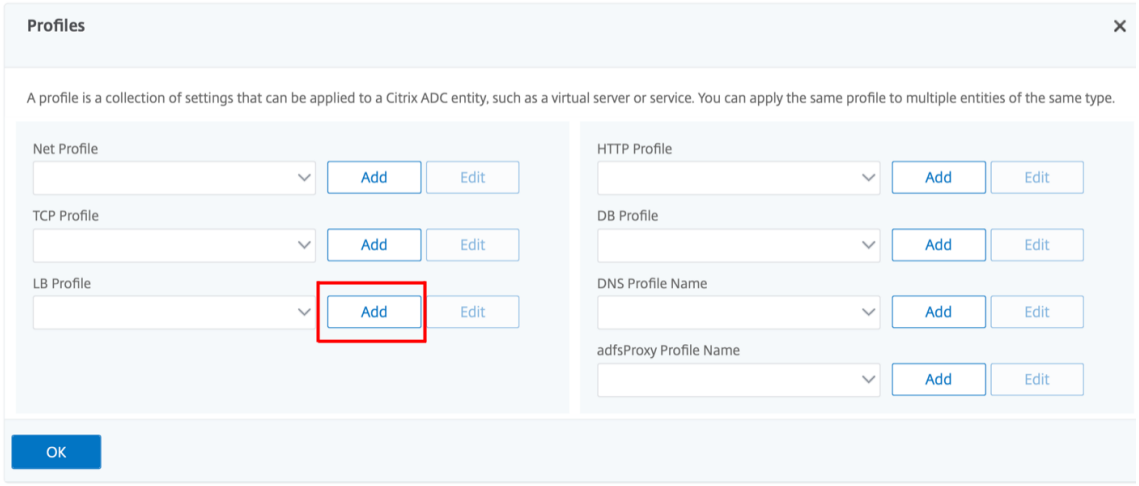
Définition des attributs ADC Cookie dans le profil d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.
3. Dans la section **Paramètres avancés**, cliquez sur **Ajouter des profils**.



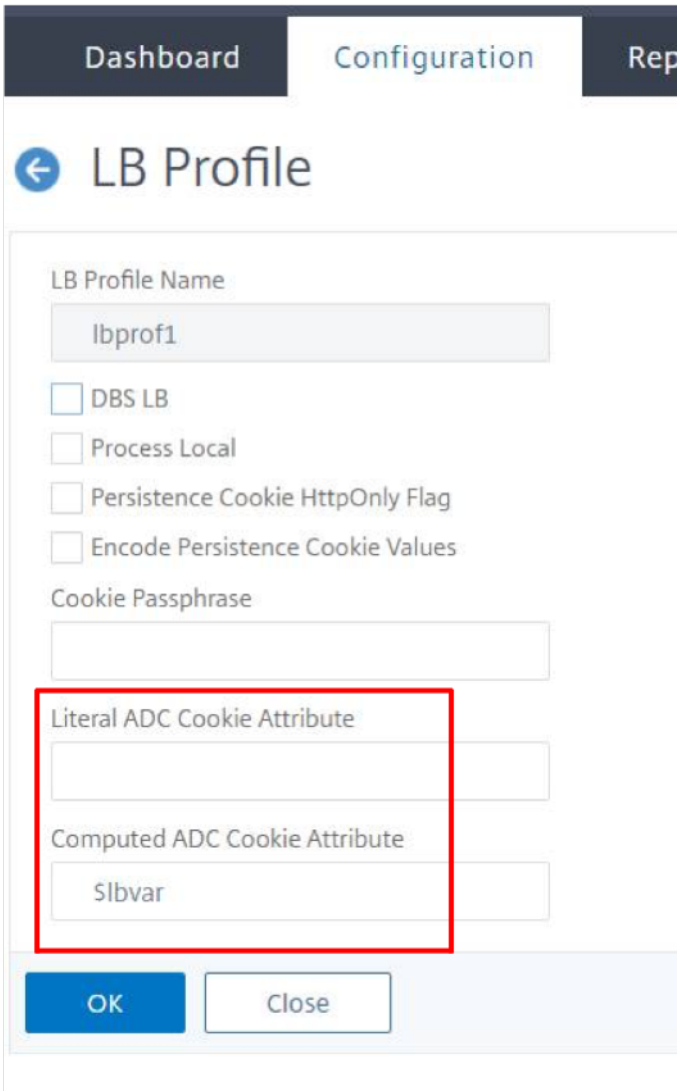
4. Dans la section **Profils**, cliquez sur **Ajouter** pour créer un profil LB.

   Si vous avez déjà créé un profil, choisissez-le dans le menu déroulant **Profil LB**.



5. Dans le volet **Profil LB**, entrez les valeurs appropriées pour l'un des champs en fonction de vos besoins :

- **Literal ADC Cookie Attribute**
- **Computed ADC Cookie Attribute**



1. Cliquez sur **OK**.
2. Définissez le profil LB créé sur le serveur virtuel LB créé à **l'étape 1**.

Vérifier la configuration de la variable ns

Pour vérifier que la variable ADC ns est configurée correctement dans les paramètres LB ou le profil LB, utilisez les commandes show lb parameter ou show lb profile.

Le tableau suivant répertorie les différents messages d'avertissement et leur cause, lorsque la variable ns n'est pas correctement configurée.

Message d'avertissement	Raisons
La variable NS n'est pas configurée. Configurez-le avec le type text () et étendez la transaction pour la variable	La variable NS n'est pas encore configurée.
La portée de la variable NS configurée n'est pas une transaction.	La variable est configurée mais la portée n'est pas définie sur « transaction ».
Le type de variable n'est pas Text ().	La variable est configurée mais le type n'est pas défini sur « Texte ».
La taille maximale de valeur configurée pour la variable NS est supérieure à 255.	La valeur configurée pour la variable NS est supérieure à 255 caractères. **Remarque :** une longueur maximale de 255 caractères peut être ajoutée à un cookie généré par ADC. Les caractères qui dépassent la longueur maximale sont tronqués.

Sortie d'échantillon

Dans l'exemple suivant, le message d'avertissement s'affiche lorsque la variable ns n'est pas configurée.

```
1 set lb parameter -ComputedADCCookieAttribute "$lbvar"
2
3 Warning: NS Variable is not configured. Please configure it with type
     text() and scope transaction
4 Done
5 <!--NeedCopy-->
```

Le message d'avertissement s'affiche dans la sortie suivante de la `show lb parameter` commande.

```
1  show lb parameter
2
3  Global LB parameters:
4  Persistence Cookie HttpOnly Flag: ENABLED
5  Use Encrypted Persistence Cookie: DISABLED
6  Use Port For Hash LB: YES
7  Prefer direct route: YES
8  Retain Service State: OFF
9  Start RR Factor: 0
10 Skip Maxclient for Monitoring: DISABLED
11 Monitor Connection Close: FIN
```



```
Use consolidated stats for LeastConnection: YES
Allow mac mode based vserver to pick thereturn traffic from services: DISABLED
Allow bound service removal: ENABLED
TTL for Domain Based Server: 0 secs

NetScaler Cookie Variable Name: $lbvar(NS Variable is not configured. Please configure it with type text() and scope transaction)

Done
<!--NeedCopy-->
```

Exemple de configuration pour l'insertion d'attributs de cookie dans le déploiement de GSLB

L'exemple de configuration suivant s'applique à la persistance du site configurée sur les services GSLB correspondant à un serveur virtuel LB. Pour ajouter des attributs de cookie supplémentaires aux cookies GSLB, effectuez la configuration suivante.

- Définissez les attributs du cookie ADC dans le profil LB (LB-VServer-Profile-1).
- Définissez la valeur de l'attribut de cookie Literal ADC, par exemple « SameSite=None », dans le profil LB.
- Définissez le profil LB sur le serveur virtuel d'équilibrage de charge (LB-vServer-1), qui représente le service GSLB.

```
add gslb vserver GSLB-VServer-1 SSL -backupLBMethod ROUNDROBIN -tolerance 0 -appflowLog DISABLED
add gslb site site1 10.102.148.4 -publicIP 10.102.148.4
add gslb service site1_gsvc1 10.102.148.35 SSL 443 -publicIP 10.102.148.35 -publicPort 443 -maxClient 0 -siteName site1 -sitePersistence HTTPRedirect -sitePrefix ss1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

bind gslb vserver GSLB-VServer-1 -serviceName site1_gsvc1
bind gslb vserver GSLB-VServer-1 -domainName www.gslb.com -TTL 5

add service service-1 10.102.84.140 SSL 443

add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite=None
add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType COOKIEINSERT -lbprofilename LB-Vserver-Profile-1

bind lb vserver LB-VServer-1 service-1
```



```
<!--NeedCopy-->
```

> **Remarque**
>
> Vous pouvez également insérer de manière conditionnelle les attributs de cookie à l'aide de l'attribut de cookie ADC calculé.

Exemple de configuration pour l'insertion d'un attribut de cookie dans un déploiement de commutation de contenu

L'exemple de configuration suivant s'applique lorsque plusieurs applications sont hébergées derrière un serveur virtuel de commutation de contenu. Pour appliquer la même politique à toutes les applications, liez les politiques de réécriture au serveur virtuel de commutation de contenu plutôt qu'au serveur virtuel LB, comme suit :

- Définissez les attributs du cookie ADC dans les paramètres LB.

  > **Remarque :**
  >
  > Vous pouvez également définir les attributs des cookie ADC dans le profil LB.

- Configurez la variable ns (cookieattribute_var) dont le type est défini sur Texte et l'étendue sur Transaction.
- Définissez l'attribut de cookie ADC calculé dans les paramètres LB globaux à l'aide de la variable ns.
- Définissez les politiques de réécriture (exception_samesite_attribute et append_samesite_attribute) sur les serveurs virtuels de commutation de contenu pour insérer les attributs des cookie.

```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
set lb parameter -ComputedADCCookieAttributE "$cookieattribute_var"
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
```



```
add rewrite policy append_samesite_attribute true samesiteassign

add lb vserver LB-VServer-1 SSL 10.102.148.35 443
add lb vserver LB-VServer-2 SSL 10.102.148.36 443

add cs vserver CS-VServer-1 SSL 10.102.148.42 443 -persistenceType
    COOKIEINSERT

add cs action act1 -targetLBVserver v1
add cs action act2 -targetLBVserver v2
add cs policy CS-policy-1 -rule "HTTP.REQ.URL.CONTAINS("file1.html")" -
    action act1
add cs policy CS-policy-2 -rule "HTTP.REQ.URL.CONTAINS("file2.html")" -
    action act2

bind cs vserver CS-VServer-1 -policyName CS-policy-1 -priority 1
bind cs vserver CS-VServer-1 -policyName CS-policy-2 -priority 2

bind cs vserver -policyname exception_samesite_attribute 90 110 -type
    RES_OVERRIDE
bind cs vserver -policyname append_samesite_attribute 100 110 -type
    RES_OVERRIDE
<!--NeedCopy-->
```

Personnaliser une configuration d'équilibrage de charge

May 5, 2023

Après avoir configuré une configuration d'équilibrage de charge de base, vous pouvez y apporter plusieurs modifications afin qu'elle répartit la charge exactement comme vous le souhaitez. La fonction d'équilibrage de charge est complexe. Vous pouvez modifier les éléments de base en effectuant une ou plusieurs des opérations suivantes :

- Modification de l'algorithme d'équilibrage de charge
- Configuration des groupes d'équilibrage de charge et utilisation de ces groupes pour créer votre configuration d'équilibrage de charge
- Configuration des connexions client-serveur persistantes
- Configuration du mode de redirection
- Affectation de différentes pondérations à différents services ayant des capacités différentes.

L'algorithme d'équilibrage de charge par défaut de l'appliance NetScaler est la méthode de moindre connexion. Dans la méthode de connexion la plus faible, l'appliance envoie chaque connexion en-

trante au service qui gère actuellement le moins de connexions. Vous pouvez spécifier différents algorithmes d'équilibrage de charge, chacun étant adapté à différentes conditions.

Pour prendre en charge des applications telles que les chariots d'achat, qui requièrent que toutes les demandes du même utilisateur soient dirigées vers le même serveur, vous pouvez configurer l'appliance pour qu'elle conserve les connexions persistantes entre les clients et les serveurs. Vous pouvez également spécifier la persistance d'un groupe de serveurs virtuels. La persistance permet à l'appliance de diriger les demandes client individuelles vers le même service, quel que soit le serveur virtuel du groupe qui reçoit la demande du client.

Vous pouvez activer et configurer le mode de redirection utilisé par l'appliance lors de la redirection des demandes des utilisateurs, en choisissant entre le transfert sur IP et le transfert sur Mac. Vous pouvez également attribuer des poids à différents services, en spécifiant quel pourcentage de charge entrante doit être dirigé vers chaque service. L'attribution de poids vous permet d'inclure des serveurs de capacités différentes dans la même configuration d'équilibrage de charge sans :

- surcharge des serveurs à faible capacité ou
- ce qui permet aux serveurs de plus grande capacité de rester inactifs.

Personnalisation de l'algorithme de hachage pour assurer la persistance sur les serveurs virtuels

May 5, 2023

L'appliance NetScaler utilise des algorithmes basés sur le hachage pour maintenir la persistance sur les serveurs virtuels. Par défaut, la méthode d'équilibrage de charge basée sur le hachage utilise la valeur de hachage de l'adresse IP et du numéro de port du service. Si un service est mis à disposition sur différents ports du même serveur, l'algorithme génère différentes valeurs de hachage. Par conséquent, différents serveurs virtuels d'équilibrage de charge peuvent envoyer des demandes pour la même application à différents services, brisant ainsi la pseudo-persistance.

Au lieu d'utiliser le numéro de port pour générer la valeur de hachage, vous pouvez spécifier un identifiant de hachage unique pour chaque service. Pour un service, la même valeur d'identifiant de hachage doit être spécifiée sur tous les serveurs virtuels. Si un serveur physique dessert plusieurs types d'applications, chaque type d'application doit disposer d'un identifiant de hachage unique.

L'algorithme de calcul de la valeur de hachage d'un service fonctionne comme suit :

- Par défaut, un paramètre global spécifie l'utilisation du numéro de port dans un calcul de hachage.
- Si vous configurez un identifiant de hachage pour un service, il est utilisé, mais pas le numéro de port, quel que soit le paramètre global.

- Si vous ne configurez pas d'identifiant de hachage, mais que vous modifiez la valeur par défaut du paramètre global afin qu'il ne spécifie pas l'utilisation du numéro de port, la valeur de hachage est basée uniquement sur l'adresse IP du service.
- Si vous ne configurez pas d'identifiant de hachage ou si vous ne modifiez pas la valeur par défaut du paramètre global pour utiliser le numéro de port, la valeur de hachage est basée sur l'adresse IP et le numéro de port du service.

Vous pouvez également spécifier des identifiants de hachage lorsque vous utilisez l'interface de ligne de commande pour lier des services à un groupe de services. Dans l'utilitaire de configuration, vous pouvez ouvrir un groupe de services et ajouter des identifiants de hachage dans l'onglet Membres.

Pour modifier le paramètre global use-port-number à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
définir le paramètre lb -usePortForHashLB          NO)
(OUI)
```

Exemple :

```
1 > set lb parameter -usePortForHashLb NO
2  Done
3 >show lb parameter
4 Global LB parameters:
5         Persistence Cookie HttpOnly Flag: DISABLED
6         Use port for hash LB: NO
7  Done
8 <!--NeedCopy-->
```

Pour modifier le paramètre global use-port-number à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge.
2. Sélectionnez ou désactivez Utiliser le port pour les méthodes LB basées sur le hachage.

Pour créer un nouveau service et spécifier un identifiant de hachage pour un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir l'ID de hachage et vérifier le paramètre :

ajouter un service < name > (< ip >	< serverName >) < serviceType > < port > -Hashid < positive_integer >

```
show service <name>
<!--NeedCopy-->
```

Exemple :

```
> add service flbkng 10.101.10.1 http 80 -hashId 12345
 Done
>show service flbkng
        flbkng (10.101.10.1:80) - HTTP
        State: DOWN
        Last state change was at Thu Nov  4 10:14:52 2010
        Time since last state change: 0 days, 00:00:15.990
        Server Name: 10.101.10.1
        Server ID : 0   Monitor Threshold : 0

        Down state flush: ENABLED
        Hash Id: 12345

1)      Monitor Name: tcp-default
                State: DOWN     Weight: 1

 Done
<!--NeedCopy-->
```

Pour spécifier un identifiant de hachage pour un service existant à l'aide de l'interface de ligne de commande

Tapez la commande set service, le nom du service et **-HashiD** suivi de la valeur de l'ID.

Pour spécifier un identifiant de hachage lors de l'ajout d'un membre du groupe de services

Pour spécifier un identifiant de hachage pour chaque membre à ajouter au groupe et vérifier le paramètre, à l'invite de commandes, tapez les commandes suivantes (Veillez à spécifier un HashiD unique pour chaque membre).) :

```
bind servicegroup <serviceGroupName> <memberName> <port> -hashId <
    positive_integer>
```



```
2
3 show servicegroup <serviceGroupName>
4 <!--NeedCopy-->
```

Exemple :

```
1  bind servicegroup http_svc_group 10.102.27.153 80 -hashId 2222222
2
3 >show servicegroup SRV
4         SRV - HTTP
5         State: ENABLED  Monitor Threshold : 0
6         ...
7
8         1)         1.1.1.1:80   State: DOWN     Server Name: 1.1.1.1
                Server ID: 123  Weight: 1
9         Hash Id: 32211
10
11                  Monitor Name: tcp-default       State: DOWN
12        ...
13
14        2)         2.2.2.2:80   State: DOWN     Server Name: 2.2.2.2
                Server ID: 123  Weight: 1
15        Hash Id: 12345
16
17                  Monitor Name: tcp-default       State: DOWN
18        ...
19 Done
20
21 <!--NeedCopy-->
```

Pour spécifier un identifiant de hachage pour un service à l'aide de l'interface graphique

1. Accédez à Traffic Management > Load Balancing > Services.
2. Créez un nouveau service ou ouvrez un service existant et spécifiez l'ID de hachage.

Pour spécifier un identifiant de hachage pour un membre du groupe de services déjà configuré à l'aide de l'interface graphique

1. Accédez à Gestion du trafic > Équilibrage de charge > Groupes de services.
2. Ouvrez un membre et tapez un ID de hachage unique.

Configurer le mode de redirection

May 5, 2023

Le mode de redirection configure la méthode utilisée par un serveur virtuel pour déterminer où transférer le trafic entrant. L'appliance NetScaler prend en charge les modes de redirection suivants. Avant de transférer la demande vers un serveur, les modes de redirection fonctionnent comme suit :

- Transfert basé sur IP (par défaut) : l'adresse IP de destination est remplacée par l'adresse IP du serveur.
- Transfert sur Mac : l'adresse MAC de destination est remplacée par l'adresse MAC du serveur. Toutefois, l'adresse IP de destination n'est pas modifiée. Le mode de redirection basé sur Mac est principalement utilisé dans les déploiements d'équilibrage de charge de pare-feu.
- Basé sur le TUNNEL IP : Une encapsulation IP dans IP est effectuée pour les paquets IP clients. Dans les en-têtes IP externes, l'adresse IP de destination est définie sur l'adresse IP du serveur et l'adresse IP source est définie sur l'adresse IP du sous-réseau (SNIP). Les paquets IP du client ne sont pas modifiés. Cela s'applique aux paquets IPv4 et IPv6.
- Basé sur l'ID TOS : L'ID TOS du serveur virtuel est codé dans le champ TOS de l'en-tête IP.

Vous pouvez utiliser l'option IP TUNNEL ou TOS pour implémenter le retour direct du serveur (DSR). Pour plus d'informations, voir :

- Configuration du mode DSR lors de l'utilisation de TOS
- Configurez l'équilibrage de charge en mode DSR pour les réseaux IPv6 à l'aide du champ TOS
- Configurez l'équilibrage de charge en mode DSR à l'aide d'IP sur IP

Vous pouvez configurer le transfert Mac sur les réseaux qui utilisent la topologie DSR, l'équilibrage de charge des liens ou l'équilibrage de charge du pare-feu. Pour plus d'informations sur le transfert Mac pour l'équilibrage de charge, consultez Configurer MBF pour la configuration de l'équilibrage de charge.

Pour configurer le mode de redirection à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -m <RedirectionMode>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```


> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l' `-m MAC` option est activée, vous devez lier un moniteur non utilisateur.

Pour configurer le mode de redirection à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et sélectionnez le mode de redirection.

Configurer des serveurs virtuels génériques par VLAN

August 20, 2021

Si vous souhaitez configurer l'équilibrage de charge pour le trafic sur un réseau local virtuel (VLAN) spécifique, vous pouvez créer un serveur virtuel avec une stratégie d'écoute qui le limite au traitement du trafic uniquement sur le VLAN spécifié.

Pour configurer un serveur virtuel avec caractères génériques qui écoute un VLAN spécifique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel génériques qui écoute un VLAN spécifique et vérifier la configuration :

```
add lb vserver <name> <serviceType> IPAddress * Port * -listenpolicy <
    expression> [-listenpriority <positive_integer>]

show vserver
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-vlan1 ANY -listenpolicy "CLIENT.VLAN.ID.EQ(2)
    " -listenpriority 10

show vserver Vserver-LB-vlan1
<!--NeedCopy-->
```


Pour configurer un serveur virtuel avec caractères génériques qui écoute un VLAN spécifique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Créez un nouveau serveur virtuel ou ouvrez un serveur virtuel existant.
3. Spécifiez une priorité et une expression de stratégie d'écoute.

Une fois que vous avez créé ce serveur virtuel, vous le liez à un ou plusieurs services, comme décrit dans Configuration de l'équilibrage de charge de base.

Attribuer des pondérations aux services

May 5, 2023

Dans une configuration d'équilibrage de charge, vous attribuez des poids aux services pour indiquer le pourcentage de trafic qui doit être envoyé à chaque service. Les services avec des pondérations plus élevées peuvent traiter davantage de demandes, tandis que les services avec des pondérations plus faibles peuvent traiter moins de demandes. L'attribution de poids aux services permet à l'appliance NetScaler de déterminer la quantité de trafic que chaque serveur d'équilibrage de charge peut gérer, et donc d'équilibrer la charge de manière plus efficace.

Remarque : Si vous utilisez une méthode d'équilibrage de charge qui prend en charge la pondération des services (par exemple, la méthode Round Robin), vous pouvez attribuer une pondération au service.

Le tableau suivant décrit les méthodes d'équilibrage de charge qui prennent en charge la pondération et décrit brièvement la manière dont la pondération affecte la manière dont un service est sélectionné pour chacune d'entre elles.

Méthodes d'équilibrage de charge	Sélection des services avec poids
Round Robin	Le serveur virtuel donne la priorité à la file d'attente des services disponibles de telle sorte que les services ayant les poids les plus élevés arrivent plus fréquemment à l'avant de la file d'attente que ceux ayant les poids les plus faibles et reçoivent proportionnellement plus de trafic. Pour une description complète, voir La méthode Round Robin.

Méthodes d'équilibrage de charge	Sélection des services avec poids
Moins de connexion	Le serveur virtuel sélectionne le service avec la meilleure combinaison de transactions actives et le poids le plus élevé. Pour une description complète, reportez-vous à la section Méthode de connexion la plus faible.
Moins de temps de réponse et moins de temps de réponse à l'aide de moniteurs	Le serveur virtuel sélectionne le service avec la meilleure combinaison de transactions actives et de temps de réponse moyen le plus rapide. Pour une description complète, reportez-vous à la section Méthode du temps de réponse le plus faible.
Moins de bande passante	Le serveur virtuel sélectionne le service avec la meilleure combinaison de moins de trafic et de bande passante la plus élevée. Pour une description complète, reportez-vous à la section Méthode de la moindre bande passante.
Moins de paquets	Le serveur virtuel sélectionne le service avec la meilleure combinaison de paquets le plus faible et de poids le plus élevé. Pour une description complète, reportez-vous à la section Méthode The Moast Packets.
Chargement personnalisé	Le serveur virtuel sélectionne le service avec la meilleure combinaison de charge la plus faible et de poids le plus élevé. Pour obtenir une description complète, reportez-vous à la section Méthode de chargement personnalisée.
Méthodes de hachage et méthode Token	La pondération n'est pas prise en charge par ces méthodes d'équilibrage de charge.

Pour configurer un serveur virtuel afin d'attribuer des poids aux services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
set lb vserver <name> -weight <Value> <ServiceName>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -weight 10 Service-HTTP-1
<!--NeedCopy-->
```

Pour configurer un serveur virtuel afin d'attribuer des poids aux services à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ouvrez le serveur virtuel, puis cliquez dans la section **Services** .
3. Dans la colonne Poids du service, affectez une pondération au service.

Configurer le paramètre de version de serveur MySQL et Microsoft SQL

January 21, 2021

Vous pouvez spécifier la version de Microsoft® SQL Server® et le serveur MySQL pour un serveur virtuel d'équilibrage de charge de type MSSQL et MySQL respectivement. Le paramètre de version est recommandé si vous vous attendez à ce que certains clients n'exécutent pas la même version que votre produit MySQL ou Microsoft SQL Server. Le paramètre de version assure la compatibilité entre les connexions côté client et côté serveur en veillant à ce que toutes les communications soient conformes à la version du serveur.

Pour définir le paramètre de version du serveur Microsoft SQL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir le paramètre de version de Microsoft SQL Server pour un serveur virtuel d'équilibrage de charge et vérifiez la configuration :

```
set lb vserver <name> -mssqlServerVersion <mssqlServerVersion>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple


```
> set lb vserver myMSSQLvip -mssqlServerVersion 2008R2
 Done
> show lb vserver myMSSQLvip
    myMSSQLvip (190.0.2.12:1433) - MSSQL    Type: ADDRESS
 . . .
 . . .
    MSsql Server Version: 2008R2
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```

Pour définir le paramètre de version du serveur MySQL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir le paramètre de version de MySQL Server pour un serveur virtuel d'équilibrage de charge et vérifiez la configuration :

```
set lb vserver <name> -mysqlServerVersion <string>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple

```
> set lb vserver mysqlsvr -mysqlserverversion 5.5.30
 Done
> sh lb vserver mysqlsvr
     mysqlsvr (2.22.2.222:3306) - MYSQL      Type: ADDRESS
 . . .
 . . .
     Mysql Server Version: 5.5.30
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```


Pour définir le paramètre de version du serveur MySQL ou Microsoft SQL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ouvrez un serveur virtuel de type MySQL ou MSSQL et définissez la version du serveur.

Serveurs virtuels multi-IP

May 5, 2023

NetScaler prend en charge la création d'un serveur virtuel d'équilibrage de charge unique avec plusieurs adresses IPv4 et IPv6 non consécutives/consécutives de type VIP. Chaque adresse VIP liée à un serveur virtuel est traitée comme un serveur virtuel individuel. Ces serveurs virtuels ont le même protocole et d'autres paramètres de niveau serveur virtuel. Un serveur virtuel avec plusieurs adresses VIP est également appelé serveur virtuel multi-IP.

L'utilisation de serveurs virtuels multi-IP présente les avantages suivants :

- Un serveur virtuel multi-IP permet de ne pas créer de nombreux serveurs virtuels avec les mêmes paramètres et liaisons de service.
- Les serveurs virtuels multi-IP réduisent efficacement la possibilité d'atteindre la limite maximale des entités de serveurs virtuels.
- Un serveur virtuel multi-IP peut être utilisé pour les clients de différents sous-réseaux afin de se connecter au même ensemble de serveurs.
- Un seul serveur virtuel multi-IP peut être utilisé pour les clients IPv6 et IPv4 afin de se connecter au même ensemble de serveurs.

Configuration d'un serveur virtuel multi-IP

La configuration d'un serveur virtuel multi-IP comprend les tâches suivantes :

- Créez un IPSet et associez-le à plusieurs adresses IP.
- Liez l'IPSet aux serveurs virtuels d'équilibrage de charge.

Notez les points suivants relatifs à la configuration d'IPSet :

- Un IPSet peut avoir :
  - adresses IPv4 et adresses IPv6 non consécutives/consécutives
  - combinaisons d'adresses IPv4 et IPv6.
- Toutes les adresses IPv4/IPv6 à associer à des serveurs virtuels utilisant IPSet doivent être de type VIP.
- Un même IPSet peut être lié à plusieurs serveurs virtuels.

- Les adresses IPv4/IPv6 peuvent être liées/dissociées depuis/vers IPSet indépendamment des liaisons IPSet existantes avec des serveurs virtuels.
- Vous devez annuler la liaison IPSet à un serveur virtuel avant de lui lier un nouvel IPSet.

Pour ajouter un IPSet et y associer plusieurs adresses VIP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ipset <name>

bind ipset <name> <IPaddress1 ... >

bind ipset <name> <IPaddress2... >

show ipset <name>
<!--NeedCopy-->
```

Pour lier l'IPSet à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -ipset <ipset name>

show lb vserver <name>
<!--NeedCopy-->
```

Pour ajouter un IPSet et y associer plusieurs adresses VIP à l'aide de l'interface graphique

Accédez à **Système** > **Réseau** > **IPSet**, puis créez un IPSet avec plusieurs adresses VIP.

Pour lier l'IPSet à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**et ouvrez un serveur virtuel auquel vous souhaitez lier l'IPSet créé.
2. Dans **Paramètres de base**, définissez le paramètre **IPSet**sur le nom de l'IPSet créé.

```
> add ipset IPSET-1


Done

```



```
> bind ipset IPSET-1 9.9.9.10

Done
> bind ipset IPSET-1 1000::20

Done
> add lb vserver LBVS-1 HTTP 8.8.8.10 80  -ipset IPSET-1

Done
> add service SVC-1 3.3.3.10 HTTP 80

Done
> add service SVC-2 3.3.3.100 HTTP 80

Done
> bind lb vserver LBVS-1 SVC-1

Done
> bind lb vserver LBVS-1 SVC-2

Done
```

Prise en charge de GSLB pour les serveurs virtuels multi-IP

Les adresses IP flottantes sont requises pour les déploiements haute disponibilité. Les déploiements cloud ne prennent pas en charge les adresses IP flottantes. Ainsi, la fonctionnalité d'ensemble d'adresses IP vous aide à prendre en charge la haute disponibilité dans les déploiements cloud. La fonction d'ensemble d'adresses IP vous permet d'associer une adresse IP privée à chacune des instances principale et secondaire. L'une des adresses IP privées est ajoutée lors de la création du serveur virtuel. L'autre adresse IP est liée à un ensemble d'adresses IP. L'ensemble d'adresses IP

est ensuite associé au serveur virtuel. Généralement, une adresse IP publique est mappée à l'une des adresses IP privées en fonction de l'appliance qui reçoit le trafic. Pendant le basculement, ce mappage change dynamiquement pour acheminer le trafic vers le nouveau serveur principal.

Dans les déploiements GSLB, le service GSLB représente le serveur virtuel et nécessite l'adresse IP privée et publique du serveur virtuel. Dans les déploiements cloud, plusieurs adresses IP privées sont représentées sous la forme d'un ensemble d'adresses IP, mais le service GSLB ne peut accepter qu'une seule adresse IP privée. Ainsi, lors de la configuration du service GSLB, il est recommandé de donner l'adresse IP configurée lors de l'ajout du serveur virtuel ou l'une des adresses IP du jeu d'adresses IP. Il n'est pas nécessaire de configurer la fonction d'ensemble d'adresses IP sur le service GSLB. L'ensemble d'adresses IP configuré sur le serveur virtuel d'équilibrage de charge associé au service GSLB est suffisant.

Dans la topologie parent-enfant GSLB, l'adresse IP définie peut être associée aux serveurs virtuels d'équilibrage de charge sur les sites enfants. Le service GSLB correspondant à cette topologie porte l'adresse IP publique et l'une des adresses IP privées. L'adresse IP privée peut être une adresse IP de l'ensemble d'adresses IP ou celle configurée lors de l'ajout du serveur virtuel sur le site enfant. La communication entre le site parent et le site enfant utilise toujours l'adresse IP publique et le port public du service GSLB.

De plus, avec la prise en charge des ensembles d'adresses IP, vous pouvez disposer d'un seul point de terminaison de serveur virtuel pour le trafic IPv4 et IPv6. Auparavant, vous deviez configurer différents serveurs virtuels pour le trafic IPv4 et IPv6. Avec la prise en charge des ensembles d'adresses IP, vous pouvez associer des adresses IP IPv4 et IPv6 au même ensemble d'adresses IP. Vous pouvez ajouter différents services GSLB représentant les points de terminaison IPv4 et IPv6.

Limiter le nombre de demandes simultanées sur une connexion client

May 5, 2023

Vous pouvez limiter le nombre de demandes simultanées sur une seule connexion client. Vous pouvez protéger les serveurs contre les failles de sécurité en limitant le nombre de demandes simultanées. Lorsque la connexion client atteint la limite maximale spécifiée, l'appliance NetScaler abandonne les demandes suivantes sur la connexion jusqu'à ce que le nombre de demandes en suspens passe en dessous de la limite.

Vous pouvez configurer le paramètre MaxPipelineNat pour limiter le nombre de demandes simultanées sur une seule connexion client. Ce paramètre s'applique uniquement aux types de service suivants et lorsque « SvrTimeout » est défini sur zéro :

- ANY
- Tous les types de services UDP à l'exception du DNS

La valeur par défaut du paramètre MaxPipelineNat est 255. La valeur zéro (0) n'applique aucune limite au nombre de demandes simultanées. Lorsqu'aucune limite n'est définie, l'appliance NetScaler exécute toutes les demandes.

> **Remarque**
>
> Si vous attribuez à MaxPipelineNat une valeur plus élevée, la probabilité d'une attaque par usurpation d'identité peut être plus élevée. Par conséquent, il est recommandé de définir MaxPipelineNat sur une valeur inférieure.

Pour limiter le nombre de connexions simultanées pour un client à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb parameter -maxPipelineNat <positive_integer>
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -maxPipelineNat 199
<!--NeedCopy-->
```

Pour limiter le nombre de connexions simultanées pour un client à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage**de charge, spécifiez une valeur pour les requêtes NAT Max Pipeline.

Configuration de l'équilibrage de charge de diamètre

May 5, 2023

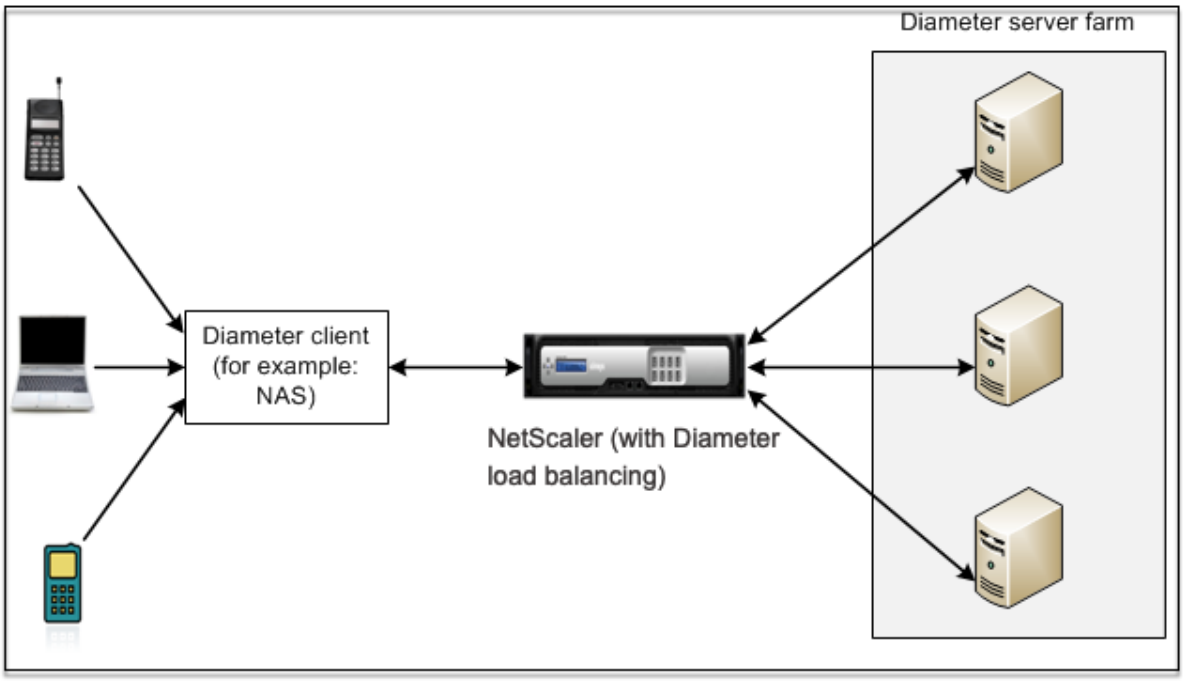
Le protocole Diameter est un protocole de signalisation AAA (Authentication, Authorization, and Accounting) de nouvelle génération utilisé principalement sur les appareils mobiles tels que les ordinateurs portables et les téléphones portables. Il s'agit d'un protocole peer-to-peer, par opposition au modèle client-serveur traditionnel utilisé par la plupart des autres protocoles. Toutefois, dans la plupart des déploiements de Diameter, les clients sont à l'origine de la demande et le serveur y répond.

Lorsque des messages Diameter sont échangés, le serveur Diameter effectue généralement beaucoup plus de traitement que le client Diameter. Avec l'augmentation du volume de signalisation du plan

de contrôle, le serveur Diameter devient un goulot d'étranglement. Par conséquent, la charge des messages Diameter doit être répartie entre plusieurs serveurs. Un serveur virtuel effectuant un équilibrage de charge des messages Diameter offre les avantages suivants :

- Allégement de la charge sur les serveurs Diameter, ce qui se traduit par un temps de réponse plus rapide pour les utilisateurs finaux.
- Surveillance de l'état du serveur et meilleures fonctionnalités de basculement.
- Meilleure évolutivité en termes d'ajout de serveurs sans modification de la configuration du client.
- Haute disponibilité.
- Déchargement au Diameter SSL.

La figure suivante montre un système Diameter dans un déploiement NetScaler :



Un système Diameter comprend les composants suivants :

- **Client Diameter.** Prend en charge les applications clientes Diameter en plus du protocole de base. Les clients Diameter sont souvent implémentés dans des appareils situés à la périphérie d'un réseau et fournissent des services de contrôle d'accès pour ce réseau. Des exemples typiques de clients Diameter sont un serveur d'accès réseau (NAS) et l'agent étranger (FA) Mobile IP.
- **Agent de Diameter.** Fournit des services de relais, de proxy, de redirection ou de traduction. L'appliance NetScaler (configurée avec un serveur virtuel d'équilibrage de charge Diameter) joue le rôle d'un agent Diameter.
- **Serveur Diameter.** Gère les demandes d'authentification, d'autorisation et de comptabilité pour un domaine particulier. Un serveur Diameter doit prendre en charge les applications du

serveur Diameter en plus du protocole de base.

Dans une topologie Diameter classique, lorsqu'un appareil utilisateur final (tel qu'un téléphone portable) a besoin d'un service, il envoie une demande à un client Diameter. Chaque client Diameter établit une connexion unique (connexion TCP, le protocole SCTP n'est pas encore pris en charge) avec un serveur Diameter tel que spécifié par le protocole de base Diameter RFC 6733. La connexion est de longue durée et tous les messages entre les deux nœuds Diameter (client et serveur) sont échangés via cette connexion. NetScaler utilise un équilibrage de charge basé sur des messages.

Exemple :

Un fournisseur de services mobiles utilise Diameter pour son système de facturation. Lorsqu'un abonné utilise un numéro prépayé, le client Diameter envoie à plusieurs reprises des demandes au serveur pour vérifier le solde disponible. Le protocole Diameter établit une connexion entre le client et le serveur, et toutes les demandes sont échangées via cette connexion. L'équilibrage de charge basé sur les connexions serait inutile, car il n'existe qu'une seule connexion. Toutefois, compte tenu du grand nombre de messages sur la connexion, l'équilibrage de charge basé sur les messages accélère le processus de facturation de l'abonné mobile prépayé.

Comment fonctionne l'équilibrage de la charge en diamètre

Une demande DPR (Disconnect Peer Request) indique l'intention du pair de fermer la connexion, ainsi que la raison de la fermeture de la connexion. L'homologue répond par un DPA (TCP fournit toujours un DPA réussi).

- Lorsque l'appliance reçoit un DPR du client, elle diffuse le DPR à tous les serveurs et répond immédiatement par un DPA au client. Les serveurs répondent par des DPA, mais l'appliance les ignore. Le client envoie un FIN, que l'appliance diffuse à tous les serveurs.
- Lorsque l'appliance reçoit un DPR du serveur, elle répond par un DPA uniquement à ce serveur et ne supprime pas le serveur du pool de réutilisation. Lorsque le serveur envoie un FIN, l'appliance répond par FIN/ACK et supprime les connexions du pool de réutilisation.
- Si l'appliance reçoit un FIN du client, elle envoie un FIN/ACK au client, diffuse le FIN et supprime immédiatement la connexion au serveur du pool de réutilisation.
- Si l'appliance reçoit un FIN du serveur, elle envoie un FIN/ACK et le supprime du pool de réutilisation. Tout nouveau message destiné à ce serveur est envoyé lors d'une nouvelle connexion.

Trafic de Diameter d'équilibrage de charge

Lorsqu'un client envoie une demande à l'appliance NetScaler, l'appliance analyse la demande et l'équilibre de charge contextuellement vers un serveur Diameter sur la base d'un AVP persistant. L'appliance a annoncé l'identité du client sur le serveur, de sorte qu'elle n'ajoute pas d'entrées de routage, car le serveur attend des messages directement du client.

Les demandes initiées par le serveur ne sont pas aussi fréquentes que les demandes des clients. Les demandes initiées par le serveur sont similaires aux demandes initiées par le client, sauf que :

- Étant donné que les messages sont reçus de plusieurs serveurs, l'appliance conserve l'état de la transaction en ajoutant un numéro HbyH (Hop by Hop) unique à chaque message de demande transféré. Lorsque la réponse au message arrive (avec le même numéro HByH), l'appliance traduit ce numéro HByH en numéro HByH reçu sur le serveur lorsque la demande est arrivée.
- L'appliance NetScaler ajoute une entrée de route en indiquant son identité, car le client considère l'appliance comme un agent relais.

Remarque : Si un message Diameter couvre plusieurs paquets, l'appliance accumule les paquets dans une file d'en-tête incomplète et les transmet au serveur lorsque le message complet est accumulé. De même, si un paquet contient plusieurs messages Diameter, l'appliance divise le paquet et transmet les messages aux serveurs selon les instructions du serveur virtuel d'équilibrage de charge.

Déconnecter une session

Une demande DPR (Disconnect Peer Request) indique l'intention du pair de fermer la connexion, ainsi que la raison de la fermeture de la connexion. L'homologue répond par un DPA (TCP fournit toujours un DPA réussi).

- Lorsque l'appliance NetScaler reçoit un DPR du client, elle diffuse le DPR à tous les serveurs et répond immédiatement par un DPA au client. Les serveurs répondent par des DPA, mais l'appliance les ignore. Le client envoie un FIN, que l'appliance diffuse à tous les serveurs.
- Lorsque l'appliance reçoit un DPR du serveur, elle répond par un DPA uniquement à ce serveur et ne supprime pas le serveur du pool de réutilisation. Lorsque le serveur envoie un FIN, l'appliance répond par FIN/ACK et supprime les connexions du pool de réutilisation.
- Si l'appliance reçoit un FIN du client, elle envoie un FIN/ACK au client, diffuse le FIN et supprime immédiatement la connexion au serveur du pool de réutilisation.
- Si l'appliance reçoit un FIN du serveur, elle envoie un FIN/ACK et le supprime du pool de réutilisation. Tout nouveau message destiné à ce serveur est envoyé lors d'une nouvelle connexion.

Configurer l'équilibrage de charge pour le trafic de diamètre

Pour configurer l'appliance NetScaler afin d'équilibrer la charge du trafic de diameter, vous devez d'abord définir les paramètres Diameter sur l'appliance, puis ajouter le moniteur de diamètre, ajouter les services de diamètre, lier les services au moniteur, ajouter le serveur virtuel d'équilibrage de charge Diameter et lier les services au serveur virtuel.

Pour configurer l'équilibrage de charge pour le trafic de diamètre à l'aide de l'interface de ligne de commande

Configurez les paramètres de diamètre.

```
set ns diameter -identity <string> -realm <string> -
   serverClosePropagation <YES|NO>
<!--NeedCopy-->
```

Exemple :

```
set ns diameter -identity mydomain.org -realm org -
   serverClosePropagation YES
<!--NeedCopy-->
```

Ajoutez un moniteur Diameter.

```
add lb monitor <monitorName> DIAMETER -originHost <string> -originRealm
    <string>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor diameter_mon DIAMETER -originHost mydomain.org -
   originRealm org
<!--NeedCopy-->
```

Créez les services Diameter.

```
add service <name> <IP> DIAMETER <port>
<!--NeedCopy-->
```

Exemple :

```
add service diameter_svc0 10.102.82.86 DIAMETER 3868

add service diameter_svc1 10.102.82.87 DIAMETER 3868

add service diameter_svc2 10.102.82.88 DIAMETER 3868

add service diameter_svc3 10.102.82.89 DIAMETER 3868
<!--NeedCopy-->
```

Liez les services Diameter au moniteur Diameter.

```
bind service <name>@ monitorName <monitorName>
```



```
<!--NeedCopy-->
```

Exemple :

```
bind service diameter_svc0 -monitorName diameter_mon

bind service diameter_svc1 -monitorName diameter_mon

bind service diameter_svc2 -monitorName diameter_mon

bind service diameter_svc3 -monitorName diameter_mon
<!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge Diameter avec persistance Diameter.

```
add lb vserver <name> DIAMETER <IPAddress> <port> -persistenceType
   DIAMETER -persistAVPno <positive_integer>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver diameter_vs DIAMETER 10.102.112.152 3868 -
   persistenceType DIAMETER -persistAVPno 263
<!--NeedCopy-->
```

Liez les services Diameter au serveur virtuel d'équilibrage de charge Diameter.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver diameter_vs diameter_svc0

bind lb vserver diameter_vs diameter_svc1

bind lb vserver diameter_vs diameter_svc2

bind lb vserver diameter_vs diameter_svc3
<!--NeedCopy-->
```

Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```


Remarque : Vous pouvez également configurer l'équilibrage de charge du trafic Diameter via SSL à l'aide du type de service **SSL_DIAMETER** .

Pour configurer l'équilibrage de charge pour le trafic Diameter à l'aide de l'utilitaire de configuration

1. Accédez à **Système** > **Paramètres** > **Modifier les paramètres de Diameter** et définissez les paramètres de diamètre.
2. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis créez un serveur virtuel d'équilibrage de charge de type Diameter.
3. Créez un service de type Diameter.
4. Créez un moniteur de type Diameter. Dans Paramètres spéciaux, définissez l'hôte d'origine et le domaine d'origine.
5. Liez le moniteur au service et liez le service au serveur virtuel Diameter.
6. Dans Paramètres avancés, cliquez sur **Persistance**, spécifiez le diamètre et entrez un numéro AVP de persistance.
7. Cliquez sur **Enregistrer**, puis sur **Terminé**.

Configurer l'équilibrage de charge FIX

May 5, 2023

Le protocole FIX (Financial Information Exchange) est une norme de message ouvert utilisée dans le secteur financier pour l'échange électronique d'informations relatives aux transactions de titres entre partenaires commerciaux. Le protocole FIX/SSL_FIX est largement utilisé par les entreprises acheteur et vendeur, les plates-formes de négociation et les régulateurs pour communiquer des informations commerciales.

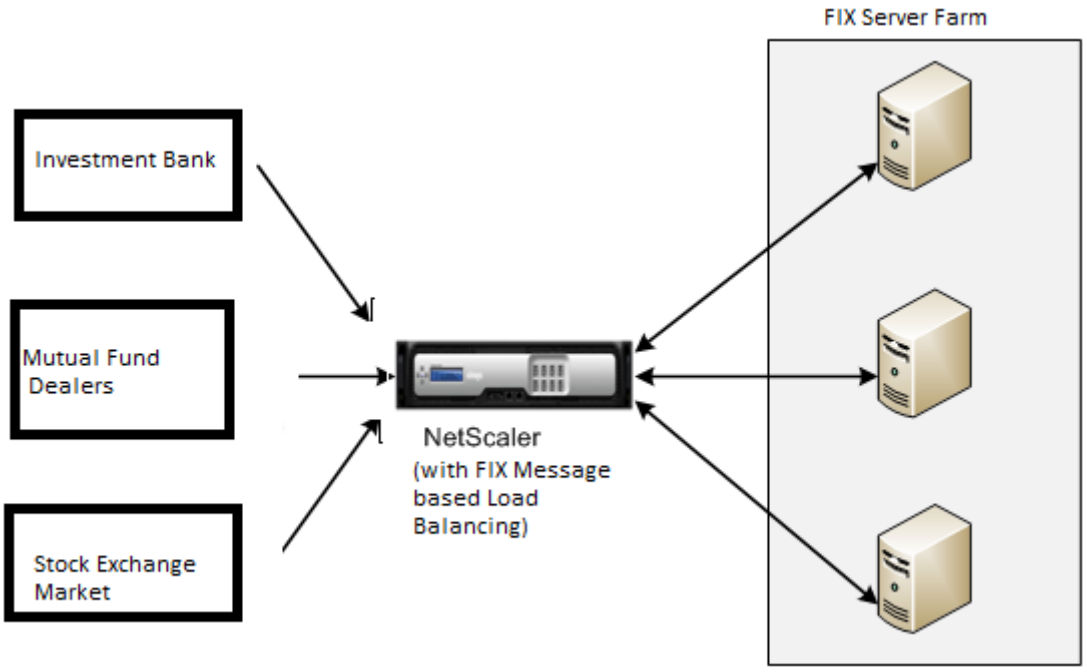
Cette fonctionnalité vous permet de configurer un serveur virtuel d'équilibrage de charge FIX ou SSL_FIX pour distribuer les messages FIX entrants et assurer la sécurité dans la messagerie FIX. NetScaler prend en charge l'équilibrage de charge basé sur les messages FIX (MBLB) pour les versions FIX 4.1, FIX 4.2, FIX 4.3 et FIX 4.4.

FIX MBLB sur une appliance NetScaler offre les avantages suivants :

1. Gestion efficace des serveurs FIX ou SSL_FIX avec une haute disponibilité et une surveillance de l'état de santé supérieures.
2. Protection SYN pour tous les serveurs FIX ou SSL_FIX.
3. CORRIGE la persistance des sessions.

Comment fonctionne l'équilibrage de charge FIX

Une configuration FIX MBLB inclut un serveur virtuel d'équilibrage de charge FIX et plusieurs serveurs FIX équilibrés de charge. Le serveur virtuel FIX reçoit le trafic client entrant, analyse le trafic entrant en messages FIX, sélectionne un serveur FIX pour chaque message FIX et transmet le message au serveur FIX sélectionné. Le dessin conceptuel suivant illustre une configuration typique d'équilibrage de charge FIX.



Dans une configuration de base de FIX MBLB, le serveur virtuel FIX distribue les messages FIX provenant des clients vers les serveurs FIX à charge équilibrée à l'aide de la méthode d'équilibrage de charge ronde. Lorsque la persistance de type FIXSESSION est activée, le serveur virtuel FIX sélectionne le même serveur pour différents messages FIX appartenant à la même session FIX. La session FIX est déterminée en fonction des valeurs des champs **FIX** SenderCompid (balise 49) et TargetCompid (balise 56).

Configurer et surveiller l'équilibrage de charge pour le trafic FIX

Les configurations que vous devez effectuer pour équilibrer la charge du trafic de messages FIX sont les suivantes :

1. Configuration du serveur virtuel d'équilibrage de charge FIX
2. Configuration du serveur virtuel d'équilibrage de charge SSL_FIX
3. Configuration du service d'équilibrage de charge FIX
4. Configuration du service d'équilibrage de charge SSL_FIX
5. Configuration de la persistance de FIXSESSION

6. Définition du délai d'expiration de la persistance
7. Affichage des statistiques FIX/SSL_FIX
8. Surveillance des sessions persistantes FIX/SSL_FIX

Pour configurer un serveur d'équilibrage de charge FIX à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> FIX <IP> <PORT>
<!--NeedCopy-->
```

Exemple

```
add lb vserver vs1 FIX 10.102.82.86 3868
<!--NeedCopy-->
```

Pour configurer un serveur virtuel d'équilibrage de charge SSL_FIX à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> SSL_FIX <IP> <PORT>
<!--NeedCopy-->
```

Exemple

```
add lb vserver vs1 SSL_FIX 10.102.82.86 3868
<!--NeedCopy-->
```

Pour configurer un service FIX à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <name> <ip-addr> FIX <port>
<!--NeedCopy-->
```

Exemple

```
add service_svc1 10.102.82.86 FIX 3868
<!--NeedCopy-->
```


Pour configurer un service SSL_FIX à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <name> <ip-addr> SSL_FIX <port>
<!--NeedCopy-->
```

Exemple

```
add service svc1 10.102.82.86 SSL_FIX 3868
<!--NeedCopy-->
```

Pour configurer la persistance de FIXSESSION à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -persistenceType FIXSESSION
<!--NeedCopy-->
```

Exemple

```
set lb vserver vs1 -persistenceType FIXSESSION
<!--NeedCopy-->
```

Pour définir le délai d'expiration de la persistance à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -timeout <value>
<!--NeedCopy-->
```

Exemple

```
set lb vserver vs1  - timeout 2
<!--NeedCopy-->
```

Pour afficher les statistiques FIX à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat lb vserver <name>
<!--NeedCopy-->
```


Exemple

```
stat lb vserver_svc1
<!--NeedCopy-->
```

Pour lier le service FIX au serveur virtuel FIX à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb vserver <name> <service name>
<!--NeedCopy-->
```

Exemple

```
bind lb vserver vs1 svc1
<!--NeedCopy-->
```

Pour afficher les sessions persistantes FIX à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show lb persistentSessions <name>
<!--NeedCopy-->
```

Exemple

```
show lb persistentSessions vs1
<!--NeedCopy-->
```

> **Remarque**
>
> Remarque : Vous pouvez désormais configurer l'équilibrage de charge du trafic FIX via SSL à l'aide du type de service SSL_FIX. Ce service fournit une communication sécurisée pour les messages FIX.

Pour configurer le serveur virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

1. Accédez à la page **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et cliquez sur **Ajouter** pour créer un serveur virtuel FIX Load Balancing.
2. Sur la page **Serveur virtuel d'équilibrage** de charge, définissez les paramètres du serveur :
   a) Nom du serveur virtuel
   b) Type de protocole « FIX »

c) Type d'adresse IP du serveur
d) Adresse IP du serveur
e) Numéro de port du serveur

3. Cliquez sur **OK** et **Continuer** pour définir d'autres paramètres.
4. Dans la section **Services**, sélectionnez ou ajoutez un nouveau service virtuel d'équilibrage de charge FIX et liez-le au serveur FIX.
5. Dans la section **Persistance**, définissez les paramètres suivants :
   a) Type de persistance « FIXSESSION »
   b) Intervalle de temporisation
6. Cliquez sur **OK**, puis sur **Terminé**.

Pour modifier un serveur virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez un serveur FIX et cliquez sur **Modifier**.

Pour supprimer un serveur virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez un serveur FIX, puis cliquez sur **Supprimer**.

Pour configurer FIX Load Balancing Virtual Service à l'aide de l'interface graphique

1. Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services** et cliquez sur **Ajouter** pour créer un service virtuel FIX Load Balancing.
2. Dans la page **Services**, définissez les paramètres suivants. Vous pouvez cliquer sur la flèche « Plus » pour définir d'autres paramètres tels que Domaine du trafic, ID de hachage, ID du serveur, Type de cache et Nombre de connexions actives.
   a) Nom du service — Nom du service virtuel FIX
   b) Choisissez le type de serveur virtuel comme (nouveau ou existant)
   c) Protocole : type de protocole « FIX »
   d) Serveur : adresse IP du serveur virtuel
   e) Port : numéro de port du serveur
3. Cliquez sur **OK** et **continuez** pour définir d'autres paramètres tels que les moniteurs, le seuil et le délai d'expiration, les profils et les politiques.
4. Cliquez sur **OK**, puis sur **Terminé**.

Pour modifier un service virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services**, sélectionnez un **service FIX** et cliquez sur **Modifier**.

Pour supprimer un service virtuel d'équilibrage de charge FIX à l'aide de l'interface graphique

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services**, sélectionnez un service FIX, puis cliquez sur **Supprimer**.

Pour afficher les statistiques du serveur d'équilibrage de charge FIX

Accédez à **la page Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis cliquez sur **Statistiques** pour afficher les statistiques du serveur FIX.

Pour afficher les sessions persistantes pour un serveur FIX à l'aide de l'interface graphique

Accédez à **la page Configuration** > **Gestion du trafic** et, sous **Surveiller les sessions, cliquez sur Sessionspersistantes du serveur virtuel**.

Pour effacer les sessions persistantes d'un serveur FIX à l'aide de l'interface graphique

1. Accédez à **la page Configuration** > **Gestion du trafic** et, sous **Surveiller les sessions**, cliquez sur **Effacer les sessions persistantes**.
2. Sur la page **Effacer les sessions persistantes**, définissez les paramètres suivants :
   a) Serveur virtuel — Choisissez un serveur virtuel FIX
   b) Paramètre de persistance — Choisissez un paramètre de persistance FIX
3. Cliquez sur **OK**.

équilibrage de charge MQTT

May 5, 2023

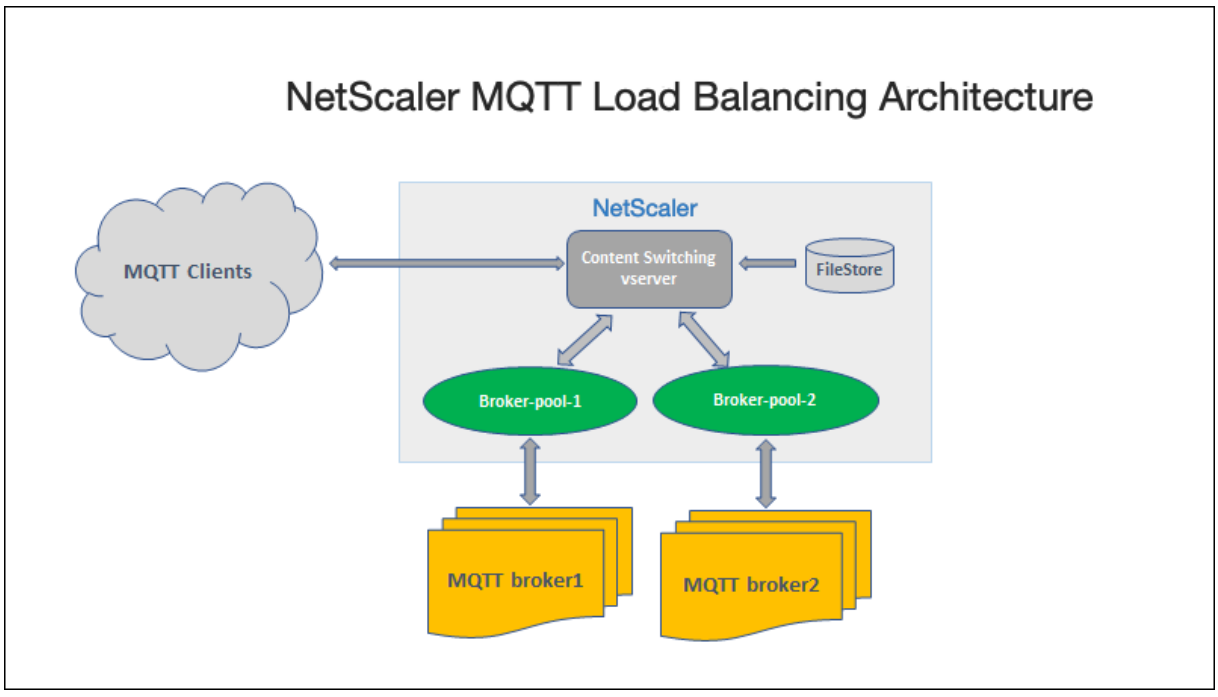
Le transport télémétrique MQTT (Message Queuing Telemetry Transport) est un protocole de messagerie standard OASIS pour l'Internet des objets (IoT). Le MQTT est une technologie flexible et facile à utiliser qui permet une communication efficace au sein d'un système IoT. Le MQTT est un protocole basé sur un courtier et est largement utilisé pour faciliter l'échange de messages entre les clients et le courtier.

Les principaux avantages suivants du MQTT en font une option parfaitement adaptée à votre appareil IoT :

- Fiabilité
- Temps de réponse rapide
- Possibilité de prendre en charge un nombre illimité d'appareils
- Messagerie de publication/d'abonnement idéale pour les communications entre plusieurs utilisateurs

L'IoT est un réseau d'appareils interconnectés intégrant des capteurs, des logiciels, une connectivité réseau et les composants électroniques nécessaires. Les composants intégrés permettent aux appareils IoT de collecter et d'échanger des données. L'utilisation croissante des appareils IoT pose de multiples défis à l'infrastructure réseau, le principal étant Scale. Dans le cadre d'un déploiement à grande échelle d'appareils IoT, les données générées par chaque appareil IoT doivent être analysées rapidement. Pour atteindre les exigences d'échelle et l'utilisation efficace des ressources, la charge sur le pool de courtiers doit être répartie uniformément. Grâce à la prise en charge du protocole MQTT, vous pouvez utiliser l'appliance NetScaler dans les déploiements IoT pour équilibrer la charge du trafic MQTT.

La figure suivante décrit l'architecture MQTT utilisant une appliance NetScaler pour équilibrer la charge du trafic MQTT.



Un déploiement IoT avec le protocole MQTT comporte les composants suivants :

- **Courtier MQTT.** Un serveur qui reçoit tous les messages des clients, puis les achemine vers les clients de destination appropriés. Le courtier est chargé de recevoir tous les messages, de

les filtrer, de déterminer qui est abonné à chaque message et d'envoyer le message aux clients abonnés. Le courtier est le hub central par lequel chaque message doit passer.

- **Client MQTT.** Tout appareil, qu'il s'agisse d'un microcontrôleur ou d'un serveur à part entière, qui exécute une bibliothèque MQTT et se connecte à un courtier MQTT via un réseau. Les éditeurs et les abonnés sont des clients MQTT. Les étiquettes d'éditeur et d'abonné indiquent si le client publie des messages ou s'il est abonné pour recevoir des messages.
- **Équilibreur de charge MQTT.** L'appliance NetScaler est configurée avec un serveur virtuel d'équilibrage de charge MQTT pour équilibrer la charge du trafic MQTT.

Dans un déploiement IoT typique, le broker (cluster de serveurs) gère le groupe de périphériques IoT (clients IoT). L'appliance NetScaler équilibre la charge du trafic MQTT vers les courtiers en fonction de divers paramètres, tels que l'ID client, la rubrique et le nom d'utilisateur.

Configurer l'équilibrage de charge pour le trafic MQTT

Pour que l'appliance NetScaler équilibre la charge du trafic MQTT, effectuez les tâches de configuration suivantes :

1. Configurez les services ou groupes de services MQTT/MQTT_TLS.
2. Configurez le serveur virtuel d'équilibrage de charge MQTT/MQTT_TLS.
3. Liez les services MQTT/MQTT_TLS au serveur virtuel d'équilibrage de charge MQTT/MQTT_TLS.
4. Configurez le serveur virtuel de commutation de contenu MQTT/MQTT_TLS.
5. Configurer une action de commutation de contenu qui spécifie le serveur virtuel d'équilibrage de charge cible
6. Configurez une politique de commutation de contenu.
7. Liez la politique de commutation de contenu à un serveur virtuel de commutation de contenu déjà configuré pour rediriger vers le serveur virtuel d'équilibrage de charge spécifique.
8. Enregistrez la configuration.

Pour configurer l'équilibrage de charge pour le trafic MQTT à l'aide de l'interface de ligne de commande

Configurez les services ou groupes de services MQTT/MQTT_TLS.

```
add service <name> <IP> <protocol> <port>
add servicegroup <ServiceGroupName> <Protocol>
bind servicegroup <serviceGroupName> <IP> <port>
<!--NeedCopy-->
```

Exemple :

```
add service srvc1 10.106.163.3 MQTT 1883
add servicegroup srvcg1 MQTT
```



```
bind servicegroup srvcg1 10.106.163.3 1883
<!--NeedCopy-->
```

Configurez le serveur virtuel d'équilibrage de charge MQTT/MQTT_TLS.

```
add lb vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver lb1 MQTT 10.106.163.9 1883
<!--NeedCopy-->
```

Liez les services ou groupes de services MQTT/MQTT_TLS au serveur virtuel d'équilibrage de charge MQTT.

```
bind lb vserver <name> <serviceName>
bind lb vserver <name> <servicegroupName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb1 srvc1
bind lb vserver lb1 srvcg1
<!--NeedCopy-->
```

Configurez le serveur virtuel de commutation de contenu MQTT/MQTT_TLS.

```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Exemple :

```
add cs vserver cs1 MQTT 10.106.163.13 1883
<!--NeedCopy-->
```

Configurez une action de commutation de contenu qui spécifie le serveur virtuel d'équilibrage de charge cible.

```
add cs action <name> -targetLBVserver <string> [-comment <string>]
<!--NeedCopy-->
```

Exemple :

```
add cs action act1 -targetlbvserver lbv1
<!--NeedCopy-->
```


Configurez une politique de commutation de contenu.

```
add cs policy <policyName> [-url <string> | -rule <expression>] -
    action <actName>
<!--NeedCopy-->
```

Exemple :

```
add cs policy cspol1  -rule   "MQTT.COMMAND.EQ(CONNECT) && MQTT.CONNECT
    .FLAGS.QOS.eq(2)"  -action act1
<!--NeedCopy-->
```

Liez la politique de commutation de contenu à un serveur virtuel de commutation de contenu déjà configuré pour rediriger vers le serveur virtuel d'équilibrage de charge spécifique.

```
bind cs vserver <virtualServerName> -policyName <policyName> -priority
    <positiveInteger>
<!--NeedCopy-->
```

Exemple :

```
bind cs vserver cs1  - policyName cspol1 -priority 20
<!--NeedCopy-->
```

Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```

Pour configurer l'équilibrage de charge pour le trafic MQTT à l'aide de l'interface graphique

1. **Accédez à**Gestion du trafic**>**Équilibrage de charge**>**Serveurs virtuels**, puis créez un serveur virtuel d'équilibrage de charge de type**MQTT ou MQTT_TLS**.**
2. Créez un service ou un groupe de services de type MQTT.
3. Liez le service au serveur virtuel MQTT.
4. Cliquez sur **Enregistrer**.

Limite de longueur des messages MQTT

L'appliance NetScaler traite les messages dont la longueur est supérieure à 65 536 octets comme des paquets Jumbo et les supprime par défaut. Le paramètre `dropmqttjumbomessage` lb décide s'il faut traiter les paquets Jumbo ou non. Ce paramètre est défini par défaut sur **YES**, ce qui implique que les

paquets MQTT jumbo sont supprimés par défaut. Si ce paramètre est défini sur **NON**, l'appliance ADC gère même les paquets dont la longueur du message est supérieure à 65 536 octets.

Pour configurer l'appliance ADC afin qu'elle gère les paquets Jumbo à l'aide de l'interface de ligne de commande :

```
Set lb parameter -dropMqttJumboMessage [YES | NO]
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -dropMqttJumboMessage no
<!--NeedCopy-->
```

Protection d'une configuration d'équilibrage de charge contre les défaillances

May 5, 2023

Lorsqu'un serveur virtuel d'équilibrage de charge échoue ou lorsque le serveur virtuel est incapable de gérer un trafic excessif, la configuration d'équilibrage de charge peut échouer. Vous pouvez protéger votre configuration d'équilibrage de charge contre les défaillances en configurant ;

- l'appliance NetScaler pour rediriger le trafic excédentaire vers une autre URL,
- un serveur virtuel d'équilibrage de charge de sauvegarde, et
- un basculement de connexion avec état.

Rediriger les demandes du client vers une autre URL

August 20, 2021

Vous pouvez rediriger les requêtes vers une autre URL à l'aide d'une redirection HTTP 302 si un serveur virtuel d'équilibrage de charge de type HTTP ou HTTPS tombe en panne ou est désactivé. L'URL alternative peut fournir des informations sur l'état du serveur. L'URL de redirection configurée est spécifiée dans l'en-tête d'emplacement de la réponse HTTP. L'URL exacte spécifiée dans la réponse dépend des options de configuration suivantes :

- Si l'URL de redirection configurée contient uniquement le nom de domaine, par exemple http://www.sample1.example.com, l'URL de redirection spécifiée dans la réponse HTTP ajoute l'URI (Uniform Resource Identifier). Il est spécifié dans la requête HTTP au nom de domaine

configuré. Par exemple, si la requête contient l'en-tête GET http://www.sample2.example.com/images/site_nav.png, l'en-tête d'emplacement dans la réponse de redirection spécifie l'emplacement : en-tête http://www.sample1.example.com/images/site_nav.png.

> **Remarque**
>
> Les noms de domaine dans la demande et la réponse peuvent différer. Dans cette rubrique, les deux domaines sont appelés sample1.example.com et sample2.example.com pour expliquer le concept.

- Si l'URL de redirection configurée contient un chemin complet, la réponse de redirection spécifie l'URL configurée complète, indépendamment de l'URI de la requête. Par exemple, les URL suivantes sont :
  - URL demandée - http://www.redirect.com/en/index.html
  - URL de redirection - http://www.redirect.com/en/site_down.html

Le tableau suivant répertorie les options de configuration précédentes :

URL de redirection configurée	URL dans la requête HTTP	En-tête dans la réponse HTTP
http://www.sample1.example.com	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/index.html
http://www.sample1.example.com/en/error.html	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/error.html

> **Remarque**
>
> - Lors de la configuration d'une URL de redirection, l' http://example.com URL n'est pas la même que l' http://example.com/ URL, car cette dernière contient le chemin complet du chemin d'accès Webroot, /.
> - Si un serveur virtuel d'équilibrage de charge est configuré avec un serveur virtuel de sauvegarde et une URL de redirection, le serveur virtuel de sauvegarde a priorité sur l'URL de redirection. Une redirection n'est utilisée que lorsque les serveurs virtuels principaux et les serveurs virtuels de sauvegarde sont DOWN.

Pour configurer un serveur virtuel pour rediriger la demande du client vers une URL à l'aide de l'interface de ligne de commande

1. Créez un serveur virtuel d'équilibrage de charge.

   ```
   set lb vserver -redirect url
   ```

2. Vérifiez que l'option URL de redirection fonctionne comme prévu. Désactivez le serveur virtuel.

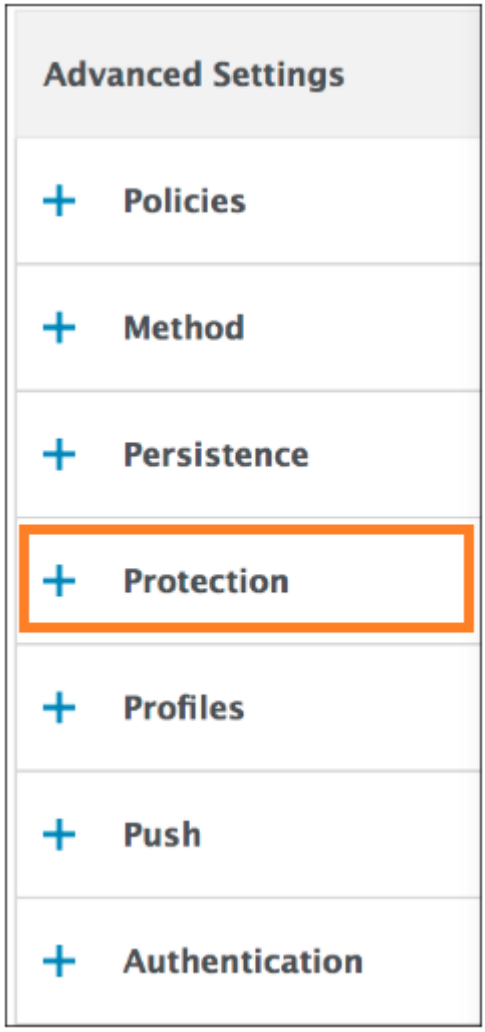

```
disable vserver <vserver_name>
```

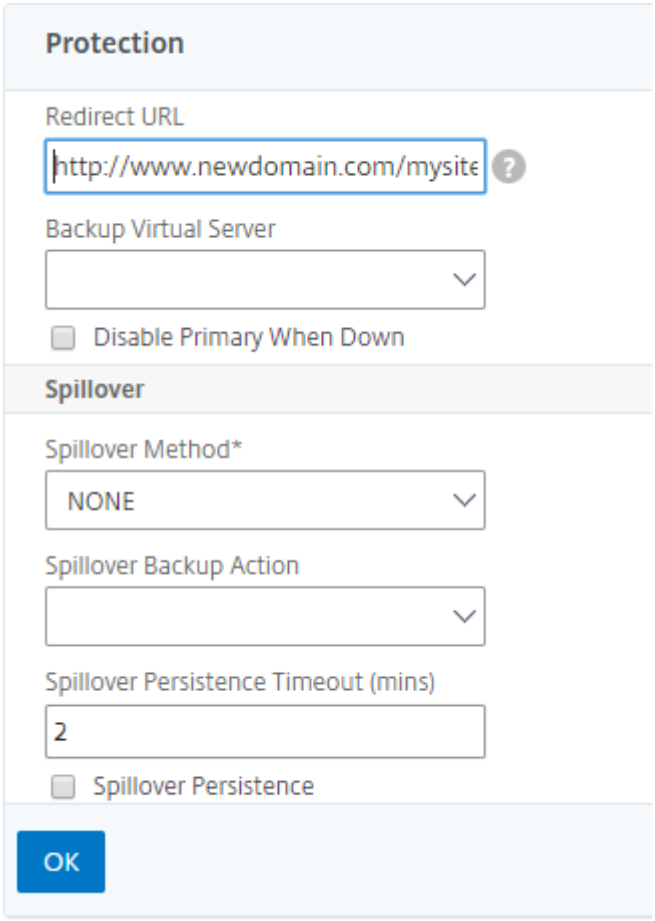
3. Accédez à l'URL du site Web à partir d'un navigateur Web pour vérifier que la demande est redirigée comme prévu. Vous devrez peut-être effacer le cache du navigateur Web et établir une nouvelle connexion avant d'accéder au site Web.
4. Activer le serveur virtuel.

```
enable vserver <vserver_name>
```

Pour configurer un serveur virtuel pour rediriger la demande client vers une URL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, pour ajouter un nouveau serveur virtuel, cliquez sur **Ajouter**.
3. Pour modifier un serveur virtuel existant, sélectionnez-le dans la liste et cliquez sur **Modifier**.
4. Sous l'onglet **Paramètres avancés**, cliquez sur **Protection**. Dans le champ **URL de redirection**, tapez l'URL de redirection (par exemple, http://www.newdomain.com/mysite/maintenance).





5. Cliquez sur **OK**.

Configurer un serveur virtuel d'équilibrage de charge de sauvegarde

June 20, 2023

Vous pouvez configurer l'appliance NetScaler pour qu'elle dirige les demandes vers un serveur virtuel de sauvegarde lorsque le serveur virtuel d'équilibrage de charge principal est en panne ou indisponible. Le serveur virtuel de sauvegarde est un proxy et est transparent pour le client. L'appliance peut également envoyer un message de notification au client concernant la panne du site.

Le serveur virtuel d'équilibrage de charge de sauvegarde garantit une interruption minimale lorsque la méthode principale n'est pas disponible, augmentant ainsi la disponibilité et la fiabilité de l'environnement d'équilibrage de charge.

> Remarque :
>
> Le serveur virtuel de sauvegarde continue de gérer les connexions existantes, même après la suppression ou la désactivation du serveur virtuel principal.

Vous pouvez configurer un serveur virtuel d'équilibrage de charge de sauvegarde lorsque vous le créez ou modifier les paramètres facultatifs d'un serveur virtuel existant. Vous pouvez également configurer un serveur virtuel de sauvegarde pour un serveur virtuel de sauvegarde existant, afin de créer des serveurs virtuels de sauvegarde en cascade. La profondeur maximale des serveurs virtuels de sauvegarde en cascade est de 10.

Si plusieurs serveurs virtuels se connectent à deux serveurs, vous pouvez choisir ce qui se passe si le serveur virtuel principal tombe en panne puis redémarre. Le comportement par défaut consiste à ce que le serveur virtuel principal reprenne son rôle en tant que serveur principal. Toutefois, vous pouvez configurer le serveur virtuel de sauvegarde pour qu'il reste en contrôle lorsqu'il prend le relais. Par exemple, vous pouvez synchroniser les mises à jour du serveur virtuel de sauvegarde avec le serveur virtuel principal, puis forcer manuellement le serveur principal d'origine à reprendre son rôle. Dans ce cas, vous pouvez désigner le serveur virtuel de sauvegarde pour qu'il reste en contrôle lorsque le serveur virtuel principal tombe en panne, puis revient.

Vous pouvez configurer une URL de redirection sur le serveur virtuel d'équilibrage de charge principal comme solution de secours lorsque le serveur virtuel principal et le serveur virtuel de sauvegarde sont hors service ou ont atteint leur seuil de traitement des demandes. Lorsque les services liés à des serveurs virtuels sont HORS SERVICE, l'appliance utilise l'URL de redirection.

La méthode Backup LB s'affiche si les méthodes d'équilibrage de charge suivantes sont sélectionnées :

- Moins de connexion
- Temps de réponse le plus court
- Robin à la ronde
- Bande passante minimale
- Moins de paquets
- Charge personnalisée
- Demande minimale
- Proximité statique

> Remarque
>
> Si un serveur virtuel d'équilibrage de charge est configuré avec à la fois un serveur virtuel de sauvegarde et une URL de redirection, le serveur virtuel de sauvegarde est prioritaire par rapport à l'URL de redirection. Une redirection est utilisée uniquement lorsque les serveurs virtuels principal et de sauvegarde sont hors service.

Pour définir un serveur virtuel de sauvegarde à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <vServerName> -backupVserver <BackupVServerName> [-
   disablePrimaryOnDown]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -backupVserver Vserver-LB-2 -
   disablePrimaryOnDown
<!--NeedCopy-->
```

Pour définir un serveur virtuel de sauvegarde à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur **Protection**et sélectionnez un serveur virtuel de sauvegarde.
3. Si vous souhaitez que le serveur virtuel de sauvegarde garde le contrôle jusqu'à ce que vous activiez manuellement le serveur virtuel principal, même si le serveur virtuel principal revient, sélectionnez **Désactiver le serveur principal en cas d'arrêt**.

> **Remarque :** À partir de NetScaler version 12.1 build 51.xx, l'interface graphique affiche l'état effectif de ce serveur en indiquant si la sauvegarde est active ou non.
>
> L'état effectif du serveur actuel peut être l'un des suivants :
>
> - **UP** — Indique que le serveur est opérationnel
> - **EN PANNE** — Indique que le serveur est en panne
> - **UP (sauvegarde active)** : indique que le serveur virtuel principal ou secondaire est opérationnel et que le trafic est dirigé vers le serveur virtuel de sauvegarde.
> - **DOWN (sauvegarde active)** : indique que le serveur virtuel principal et le serveur virtuel de sauvegarde sont en panne et que le trafic est acheminé vers le serveur virtuel de sauvegarde.
>
> Lorsque l'option **Désactiver le serveur principal en cas** d'arrêt est activée sur le serveur virtuel principal et que le serveur principal tombe en panne puis redémarre, le trafic est toujours servi par le serveur virtuel de sauvegarde jusqu'à ce que le serveur virtuel principal soit réactivé de manière explicite. Vous pouvez utiliser la commande de `enable lb vserver <vserver_name>` commande pour réactiver le serveur virtuel principal.

Configurer le débordement

May 5, 2023

Une configuration de débordement sur l'appliance comprend un serveur virtuel principal configuré avec une méthode de débordement, un seuil de débordement et un serveur virtuel de sauvegarde. Les serveurs virtuels de sauvegarde peuvent également être configurés en vue d'un débordement, créant ainsi une chaîne de serveurs virtuels de sauvegarde.

La méthode du spillover spécifie les conditions opérationnelles sur lesquelles vous souhaitez baser votre configuration de spillover (par exemple, le nombre de connexions établies, la bande passante ou l'état de santé combiné du parc de serveurs). Lorsqu'une nouvelle connexion arrive, l'appliance vérifie que le serveur virtuel principal est opérationnel et compare l'état de fonctionnement au seuil de débordement configuré. Si le seuil est atteint, la fonction de propagation redirige les nouvelles connexions vers le premier serveur virtuel disponible dans la chaîne de sauvegarde. Le serveur virtuel de sauvegarde gère les connexions qu'il reçoit jusqu'à ce que la charge sur le serveur principal tombe en dessous du seuil.

Si vous configurez la persistance des débordements, le serveur virtuel de sauvegarde continue de traiter les connexions qu'il a reçues, même lorsque la charge sur le serveur principal tombe en dessous du seuil. Si vous configurez la persistance des débordements et un délai d'expiration de la persistance des débordements, le serveur virtuel de sauvegarde traite les connexions uniquement pendant la période spécifiée une fois que la charge sur le serveur principal tombe en dessous du seuil.

Remarque : Généralement, le débordement est déclenché si la valeur associée à la méthode de débordement dépasse le seuil (par exemple, le nombre de connexions). Toutefois, avec la méthode de débordement sur l'état du serveur, le débordement est déclenché si l'état de santé du parc de serveurs tombe en dessous du seuil.

Vous pouvez configurer le débordement de l'une des manières suivantes :

- Spécifiez une méthode de propagation prédéfinie. Quatre méthodes prédéfinies sont disponibles et elles répondent aux exigences courantes en matière de répercussions.
- Configurez les retombées basées sur des politiques. Dans le cas d'un débordement basé sur des politiques, vous utilisez une règle NetScaler pour spécifier les conditions dans lesquelles le débordement se produit. Les règles NetScaler vous offrent la flexibilité nécessaire pour configurer les retombées en fonction de différentes conditions opérationnelles.

Utilisez les retombées basées sur des politiques si une méthode prédéfinie ne répond pas à vos exigences. Si vous configurez les deux pour un serveur virtuel principal, la configuration de débordement basée sur des règles prévaut sur la méthode prédéfinie.

Tout d'abord, vous créez le serveur virtuel principal et les serveurs virtuels dont vous avez besoin pour la chaîne de sauvegarde. Vous configurez la chaîne de sauvegarde en spécifiant un serveur virtuel

comme serveur de sauvegarde pour le serveur principal (c'est-à-dire que vous créez un serveur virtuel secondaire), un serveur virtuel comme serveur de sauvegarde pour le serveur secondaire (c'est-à-dire que vous créez un serveur virtuel tertiaire), etc. Ensuite, vous configurez le spillover en spécifiant une méthode de spillover prédéfinie ou en créant et en liant des stratégies de spillover.

Pour obtenir des instructions sur l'attribution d'un serveur virtuel comme sauvegarde pour un autre serveur virtuel, reportez-vous à la section Configuration d'un serveur virtuel d'équilibrage de charge de sauvegarde.

Configurer une méthode de débordement prédéfinie

Les méthodes de propagation prédéfinies répondent à certaines des exigences de diffusion les plus courantes. Pour utiliser l'une des méthodes de débordement prédéfinies, vous devez configurer les paramètres de débordement sur le serveur virtuel principal. Pour créer une chaîne de serveurs virtuels de sauvegarde, vous devez également configurer les paramètres de débordement sur les serveurs virtuels de sauvegarde.

Si les serveurs virtuels de sauvegarde atteignent leurs propres valeurs de seuil et que le type de service est TCP, l'appliance NetScaler envoie aux clients une réinitialisation TCP. Pour les types de service HTTP, SSL et RTSP, il redirige les nouvelles demandes vers l'URL de redirection configurée pour le serveur virtuel principal. Une URL de redirection ne peut être spécifiée que pour les serveurs virtuels HTTP, SSL et RTSP. Si aucune URL de redirection n'est configurée, l'appliance NetScaler envoie aux clients une réinitialisation TCP (si le serveur virtuel est de type TCP) ou une réponse HTTP 503 (si le serveur virtuel est de type HTTP ou SSL).

Remarque : avec les serveurs virtuels RTSP, l'appliance NetScaler utilise uniquement des connexions de données pour le débordement. Si le serveur virtuel RTSP de sauvegarde n'est pas disponible, les demandes sont redirigées vers une URL RTSP et un message de redirection RTSP est envoyé au client.

Pour configurer une méthode de propagation prédéfinie pour un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <vServerName> -soMethod <spillOverType> -soThreshold <
    positiveInteger> -soPersistence ENABLED -soPersistenceTimeout <
    positiveInteger>
<!--NeedCopy-->
```

Exemple


```
set lb vserver Vserver-LB-1 -soMethod Connection -soThreshold 1000 -
    soPersistence enabled -soPersistenceTimeout 2
<!--NeedCopy-->
```

Pour configurer une méthode de propagation prédéfinie pour un serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur **Protection**et définissez les paramètres de débordement.

Configurer les retombées basées sur des politiques

Les stratégies de débordement, basées sur des règles (expressions), vous permettent de configurer l'appliance pour un plus grand nombre de scénarios de débordement. Par exemple, vous pouvez configurer des retombées en fonction du temps de réponse du serveur virtuel ou en fonction du nombre de connexions dans la file d'attente de surtension du serveur virtuel.

Pour configurer le débordement basé sur une stratégie, commencez par créer une action de débordement. Vous sélectionnez ensuite l'expression que vous souhaitez utiliser dans la politique de débordement, configurez la politique et associez l'action à celle-ci. Enfin, vous liez la politique de débordement à un serveur virtuel d'équilibrage de charge, de commutation de contenu ou d'équilibrage de charge global du serveur. Vous pouvez lier plusieurs politiques de débordement à un serveur virtuel, avec des numéros de priorité. L'appliance évalue les politiques de débordement par ordre croissant de priorité et exécute l'action associée à la dernière politique à évaluer comme TRUE.

Un serveur virtuel peut également avoir une action de sauvegarde. L'action de sauvegarde est exécutée si le serveur virtuel ne possède pas un ou plusieurs serveurs virtuels de sauvegarde, ou si tous les serveurs virtuels de sauvegarde sont hors service, désactivés ou ont atteint leurs propres limites de débordement.

Lorsqu'une politique de débordement entraîne une condition UNDEF (une exception déclenchée lorsque le résultat de l'évaluation de la politique n'est pas défini), une action UNDEF est exécutée. L'action UNDEF est toujours ACCEPT. Vous ne pouvez pas spécifier l'action UNDEF de votre choix.

Configuration d'une action de débordement

Une action de débordement est exécutée lorsque la politique de débordement à laquelle elle est associée est évaluée à TRUE. Actuellement, SPILLOVER est la seule action de débordement prise en charge.

Pour configurer les retombées basées sur des politiques à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une politique de débordement et vérifier la configuration :

```
add spillover action <name> -action SPILLOVER

show spillover action <name>
<!--NeedCopy-->
```

Exemple

```
add spillover action mySoAction -action SPILLOVER
Done
<!--NeedCopy-->
```

```
show spillover action mySoAction
1) Name: mySoAction Action: SPILLOVER
Done
<!--NeedCopy-->
```

Sélection d'une expression pour la politique de débordement

Dans l'expression de politique, vous pouvez utiliser n'importe quelle expression basée sur un serveur virtuel qui renvoie une valeur booléenne. Par exemple, vous pouvez utiliser l'une des expressions suivantes :

```
SYS.VSERVER("vserver").RESPTIME.GT(<int>)
SYS.VSERVER("vserver").STATE.EQ( " <string> " ), and
SYS.VSERVER("vserver").THROUGHPUT.LT    (<int>)
<!--NeedCopy-->
```

Outre les fonctions existantes telles que RESPTIME, STATE et THROUGHPUT, vous pouvez utiliser les fonctions serveur virtuel suivantes qui ont été introduites avec cette fonctionnalité :

`Averagesurgecount`

Renvoie le nombre moyen de requêtes dans les files d'attente de surtension des services actifs. Renvoie 0 (zéro) s'il n'y a aucun service actif. Lance une condition UNDEF si elle est utilisée avec un serveur virtuel de commutation de contenu ou d'équilibrage de charge de serveur global.

Activeservices

Renvoie le nombre de services actifs. Lance une condition UNDEF si elle est utilisée avec un serveur virtuel de commutation de contenu ou d'équilibrage de charge de serveur global.

Activetransactions

Renvoie la valeur du compteur de niveau serveur virtuel pour les transactions actives en cours.

est_dynamic_limit_atteinte

Renvoie une valeur booléenne TRUE si le nombre de connexions gérées par le serveur virtuel est égal au seuil calculé dynamiquement. Le seuil dynamique est la somme des paramètres clients maximaux (Nombre maximum de clients) des services liés actifs.

Vous pouvez utiliser une expression de politique pour implémenter n'importe laquelle des méthodes d'entraînement prédéfinies. Le tableau suivant fait correspondre les méthodes de propagation prédéfinies aux expressions que vous pouvez utiliser pour les implémenter :

Tableau 1. Conversion de méthodes de propagation prédéfinies en expressions de politique

Méthode de débordement prédéfinie	Expression correspondante
CONNEXION	SYS.VSERVER (»<vserver-name>«) .CONNECTIONS, utilisé avec la fonction arithmétique GT (int).
BANDE PASSANTE	SYS.VSERVER (»<vserver-name>«) .THROUGHPUT, utilisé avec la fonction arithmétique GT (int).
HEALTH	SYS.VSERVER (»<vserver-name>«) .HEALTH, utilisé avec la fonction arithmétique LT (int).
DYNAMICCONNECTION	SYS.VSERVER (»<vserver-name>«) .IS_DYNAMIC_LIMIT_READED **Remarque** : Si vous implémentez un débordement basé sur des stratégies à l'aide de la fonction IS_DYNAMIC_LIMIT_READED, vous devez également configurer la méthode DYNAMICCONNECTION prédéfinie pour le serveur virtuel, de sorte que les statistiques nécessaires au débordement fonctionnent. sont collectés.

Configuration d'une stratégie de débordement

Une politique de débordement utilise généralement une expression booléenne pour spécifier les conditions qui doivent être remplies pour que le débordement se produise.

Pour configurer une politique de débordement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une politique de débordement et vérifier la configuration :

```
add spillover policy <name> -rule <expression> -action <string> [-
    comment <string>]

show spillover policy <name>
<!--NeedCopy-->
```

Exemple

```
> add spillover policy mySoPolicy -rule SYS.VSERVER("v1").RESPTIME.GT
    (50) -action mySoAction -comment "Triggers spillover when the
    vserver's response time is greater than 50 ms."
Done

> show spillover policy mySoPolicy

1)  Name: mySoPolicy Rule: "SYS.VSERVER("v1").RESPTIME.GT(50)" Action:
    mySoAction Hits: 0 ActivePolicy: 0
Comment: "Triggers spillover when the vserver's response time is
    greater than 50 ms."
Done
>
<!--NeedCopy-->
```

Lier une politique de débordement à un serveur virtuel

Vous pouvez lier une politique de débordement à l'équilibrage de charge, à la commutation de contenu ou à l'équilibrage de charge global des serveurs (serveurs virtuels). Vous pouvez lier plusieurs politiques à un serveur virtuel, les expressions Goto contrôlant le flux d'évaluation.

Pour lier une politique de débordement à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une politique de débordement à un serveur virtuel d'équilibrage de charge, de commutation de contenu ou d'équilibrage de charge global du serveur et vérifiez la configuration :

```
bind (lb | cs | gslb) vserver <name> -policyName <string> -priority <
    positive_integer> [-gotoPriorityExpression <expression>]

show (lb | cs | gslb) vserver <name>
<!--NeedCopy-->
```

Exemple

```
> bind lb vserver vserver1 -policyName mySoPolicy -priority 5
Done
> show lb vserver vserver1
vserver1 (2.2.2.12:80) - HTTP Type: ADDRESS
. . .

1)  Spillover Policy Name: mySoPolicy Priority: 5
GotoPriority Expression: END
Flowtype: REQUEST
Done
>
<!--NeedCopy-->
```

Configuration d'une action de sauvegarde pour un événement de débordement

Une action de sauvegarde indique la marche à suivre lorsque le seuil de propagation est atteint mais qu'un ou plusieurs serveurs virtuels de sauvegarde ne sont pas configurés, sont hors service, sont désactivés ou ont atteint leurs propres seuils.

Remarque : Pour les méthodes de propagation prédéfinies qui sont configurées directement sur le serveur virtuel (en tant que valeurs du paramètre Spillover Method), l'action de sauvegarde n'est pas configurable. Par défaut, l'appliance envoie aux clients une réinitialisation TCP (si le serveur virtuel est de type TCP) ou une réponse HTTP 503 (si le serveur virtuel est de type HTTP ou SSL).

L'action de sauvegarde est configurée sur le serveur virtuel. Vous pouvez configurer le serveur virtuel pour qu'il accepte les demandes (une fois le seuil spécifié par la politique atteint), redirige les clients vers une URL ou simplement abandonne les demandes avant même d'établir des connexions TCP ou SSL jusqu'à ce que le nombre de demandes tombe en dessous du seuil. Par conséquent, moins de ressources de mémoire sont utilisées car les connexions sont réinitialisées avant même d'allouer des structures de données.

Pour configurer une action de sauvegarde en cas de débordement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une action de sauvegarde et vérifier la configuration :

```
set lb vserver <name> -soBackupAction <soBackupAction>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vs1 -soBackupAction REDIRECT -redirectURL `http://www.
   mysite.com/maintenance`
Done
> show lb vserver vs1
vs1 (10.102.29.76:80) - HTTP Type: ADDRESS
State: UP
. . .
Redirect URL: `http://www.mysite.com/maintenance`
. . .
Done
<!--NeedCopy-->
```

Pour configurer une action de sauvegarde pour le débordement à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur **Protection**, puis spécifiez une action de sauvegarde de débordement.

Basculement de connexion

May 5, 2023

Le basculement de connexion permet d'éviter toute interruption de l'accès aux applications déployées dans un environnement distribué. Dans une configuration NetScaler High Availability (HA), le *basculement de connexion* (ou mise en *miroir des connexions-CM*) fait référence au maintien actif d'une connexion TCP ou UDP établie en cas de basculement. Le nouveau dispositif NetScaler principal contient des informations sur les connexions établies avant le basculement et continue de fournir

ces connexions. Après le basculement, le client reste connecté au même serveur physique. La nouvelle appliance principale synchronise les informations avec la nouvelle appliance secondaire. Si le paramètre L2Conn est défini, les paramètres de connexion de couche 2 sont également synchronisés avec le paramètre secondaire.

> Remarque :
>
> Pensez à une configuration HA, dans laquelle un client établit une session avec le nœud principal, qui à son tour établit une session avec le serveur principal. Lorsqu'un basculement est déclenché dans cet état, les paquets reçus sur un nouveau nœud principal à partir du client et des nœuds serveur existants sont traités comme des paquets défectueux, et les connexions client et serveur sont réinitialisées. Si le basculement de connexion sans état est activé (USIP est activé), après le basculement, les connexions ne sont pas réinitialisées lorsque vous recevez des paquets provenant de nœuds client ou serveur. Au lieu de cela, les connexions client et serveur sont créées dynamiquement.

Vous pouvez configurer le basculement de connexion en mode stateless ou stateful. En mode de basculement de connexion sans état, les nœuds HA n'échangent aucune information sur les connexions qui sont basculées. Cette méthode n'entraîne aucune surcharge d'exécution.

En mode de basculement de connexion dynamique, l'appliance principale synchronise les données des connexions avec basculement avec la nouvelle appliance secondaire.

Le basculement de connexion est utile si votre déploiement possède des connexions de longue durée. Par exemple, si vous téléchargez un fichier volumineux sur FTP et qu'un basculement se produit pendant le téléchargement, la connexion se rompt et le téléchargement est interrompu. Toutefois, si vous configurez le basculement de connexion en mode avec état, le téléchargement se poursuit même après le basculement.

Comment fonctionne le basculement de connexion sur les appliances NetScaler

Dans un basculement de connexion sans état, la nouvelle appliance principale tente de recréer le flux de paquets en fonction des informations contenues dans les paquets qu'elle reçoit.

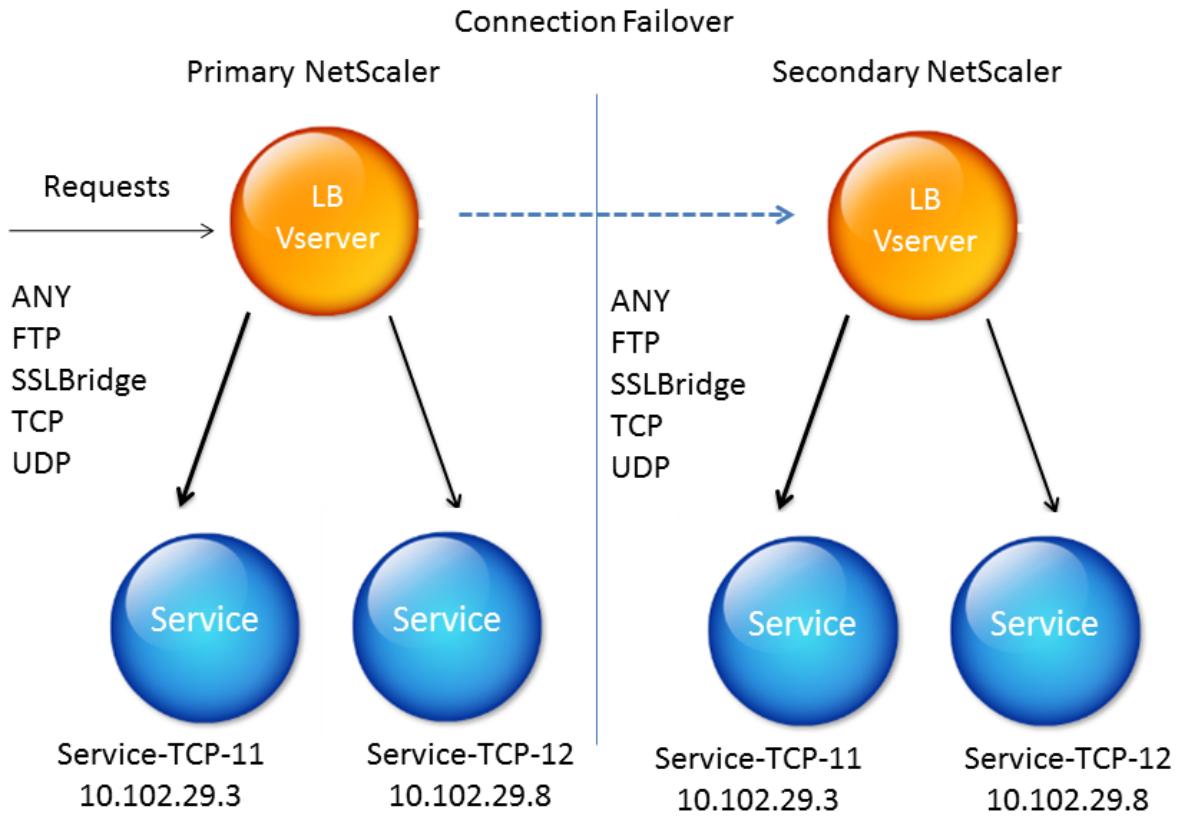
En cas de basculement sur incident avec état, pour gérer les informations actuelles sur les connexions mises en miroir, l'appliance principale envoie des messages à l'appliance secondaire. L'appliance secondaire conserve les données relatives aux paquets mais ne les utilise qu'en cas de basculement. En cas de basculement sur incident, la nouvelle appliance principale (ancienne solution secondaire) commence à utiliser les données stockées sur les connexions en miroir et à accepter le trafic. Pendant la période de transition, le client et le serveur peuvent rencontrer une brève interruption et retransmissions.

Remarque :

Vérifiez que l'appliance principale est en mesure de s'autoriser sur l'appliance secondaire. Pour vérifier la configuration correcte des mots de passe, utilisez la commande `rpcnode` show depuis la ligne de commande ou utilisez l'option RPC du menu **Réseau** de l'interface graphique.

Une configuration HA de base avec basculement de connexion contient les entités illustrées dans la figure suivante.

Figure 1. Diagramme d'entité de basculement de connexion



> **Remarque**
>
> Le basculement de connexion n'est pas pris en charge après l'un des événements suivants :
>
> ```
> - An upgrade to a later release.
> - An upgrade to a later build within the same release, if the new
>   build uses a different HA version.
> ```

Configuration prise en charge

Le basculement de connexion peut être configuré uniquement sur des serveurs virtuels d'équilibrage de charge. Il ne peut pas être configuré sur des serveurs virtuels de commutation de contenu. Si vous

activez le basculement de connexion sur des serveurs virtuels d'équilibrage de charge connectés à un serveur virtuel de commutation de contenu, le basculement de connexion ne fonctionne pas car les serveurs virtuels d'équilibrage de charge n'acceptent pas initialement le trafic.

Le tableau suivant décrit le programme d'installation pris en charge pour le basculement de connexion.

Tableau 1. Basculement de connexion - Configuration prise en charge

Paramètre	Apatride	État
Type de service	ANY.	ANY, UDP, TCP, FTP, SSL_BRIDGE.
Méthodes d'équilibrage de charge	Toutes les méthodes prises en charge pour le type de service ANY. Toutefois, si la persistance de l'adresse IP source n'est pas définie, la méthode SRCIPSRCPORTHASH doit être utilisée.	Toutes les méthodes applicables aux types de services pris en charge.
Types de persistance	Persistance SOURCEIP.	Tous les types applicables aux types de services pris en charge sont pris en charge.
USIP	Il doit être activé.	Aucune restriction. Il peut être activé ou désactivé.
Fixations de service	Le service ne peut être lié qu'à un seul serveur virtuel.	Le service peut être lié à un ou plusieurs serveurs virtuels.
Versions du protocole Internet (IP)	IPv4 et IPv6	IPV4 et IPv6
Support de redondance	Clustering et haute disponibilité	Haute disponibilité
Mode INC	Non pris en charge	Pris en charge lorsque le type de service du serveur virtuel est ANY, que le mode est DSR (MAC, IPTUNNEL, TOS) et que USIP est activé sur les services liés au serveur virtuel.

> **Remarque :**
>
> Le basculement dynamique de connexion est uniquement pris en charge pour les services de commutation basés sur la connexion, par exemple TCP. Étant donné que HTTP utilise la commutation basée sur les requêtes, il ne prend pas en charge le basculement de connexion. Dans SSL, les connexions existantes sont réinitialisées après le basculement.

Fonctionnalités affectées par le basculement de connexion

Le tableau suivant répertorie les fonctionnalités affectées si le basculement de connexion est configuré.

Tableau 2 Comment le basculement de connexion affecte les fonctionnalités de NetScaler

Fonctionnalité	Impact du basculement de connexion
Protection SYN	Pour n'importe quelle connexion, si un basculement survient après la sortie de SYN-ACK par l'appliance, mais avant qu'elle ne reçoive l'ACK final, la connexion n'est pas prise en charge par le basculement de connexion. Le client doit réémettre la demande pour établir la connexion.
Protection contre les surtensions	Si le basculement se produit avant l'établissement d'une connexion avec le serveur, le nouveau dispositif principal tente d'établir la connexion avec le serveur. Il retransmet également tous les paquets détenus pendant la protection contre les surtensions.
Access down	Si cette option est activée, la fonctionnalité d'accès est prioritaire sur le basculement de connexion.
Pare-feu d'application	La fonction de pare-feu d'application n'est pas prise en charge.

Fonctionnalité	Impact du basculement de connexion
INC	La configuration réseau indépendante (INC) est prise en charge en mode haute disponibilité uniquement lorsque le type de service du serveur virtuel est ANY, que le mode est DSR (MAC, IPTUNNEL, TOS) et que USIP est activé sur les services liés au serveur virtuel. Dans tous les autres scénarios, INC n'est pas pris en charge.
TCP mise en mémoire tampon	La mise en mémoire tampon TCP n'est pas compatible avec la mise en miroir des connexions.
Clôture de la réponse	Après basculement, les NATPCB peuvent ne pas être fermés lors de la réponse.

Pour configurer le basculement de connexion à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**. Ouvrez le serveur virtuel, puis dans **Paramètres avancés**, cliquez sur **Protection**, puis sélectionnez **Basculement de connexion surétat**.

Pour configurer le basculement de connexion à l'aide de la CLI

À l'invite de commandes :

```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -connFailover stateful
Done
<!--NeedCopy-->
```

Lorsque le basculement de connexion est désactivé sur un serveur virtuel, les ressources allouées au serveur virtuel sont libérées.

Pour désactiver le basculement de connexion à l'aide de la CLI

À l'invite de commandes :

```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -connFailover disable
Done
<!--NeedCopy-->
```

Pour désactiver le basculement de connexion à l'aide de l'interface graphique

Accédez à **Gestion du trafic**> **Équilibrage de charge**> **Serveurs virtuels**. Ouvrez le serveur virtuel, dans **Protection**, sélectionnez **Basculement de connexion en**tant que désactivé.

Éviter la file d'attente de surtension

May 5, 2023

Lorsqu'un serveur physique reçoit une vague de demandes, il met du temps à répondre aux clients qui y sont actuellement connectés, ce qui laisse les utilisateurs insatisfaits et mécontents. Souvent, la surcharge provoque également les clients à recevoir des pages d'erreur. L'appliance NetScaler fournit des fonctionnalités telles que la protection contre les surtensions, qui contrôle la vitesse à laquelle de nouvelles connexions à un service peuvent être établies et évite ainsi les surcharges.

L'appliance effectue le multiplexage des connexions entre les clients et les serveurs physiques. Lorsqu'elle reçoit une demande d'un client pour accéder à un service sur un serveur, l'appliance recherche une connexion gratuite déjà établie avec le serveur. S'il trouve une connexion libre, il utilise cette connexion pour établir un lien virtuel entre le client et le serveur. Si aucune connexion gratuite n'est trouvée, l'appliance établit une nouvelle connexion avec le serveur et établit un lien virtuel entre le client et le serveur. Toutefois, si l'appliance ne peut pas établir de nouvelle connexion avec le serveur, elle envoie la demande client à une file d'attente de surtension. Si tous les serveurs physiques liés au serveur virtuel d'équilibrage de charge ou de commutation de contenu atteignent la limite supérieure du nombre de connexions client (valeur client maximale, seuil de protection contre les surtensions ou capacité maximale du service), l'appliance ne peut établir de connexion avec aucun serveur. La fonction de protection contre les surtensions utilise la file d'attente pour

réguler la vitesse à laquelle les connexions sont ouvertes avec les serveurs physiques. L'appliance gère une file d'attente de surtension différente pour chaque service lié au serveur virtuel.

La longueur d'une file d'attente de surtension augmente chaque fois qu'une demande survient pour laquelle l'appliance ne peut pas établir de connexion. La longueur d'une file d'attente de surtension diminue dans l'une des conditions suivantes :

- Une demande dans la file d'attente est envoyée au serveur.
- Une demande est dépassée et est supprimée de la file d'attente.

Si la file d'attente de surtension d'un service ou d'un groupe de services devient trop longue, vous pouvez la vider. Vous pouvez vider la file d'attente d'un service ou d'un groupe de services spécifique, ou de tous les services et groupes de services liés à un serveur virtuel d'équilibrage de charge. Le fait de vider une file d'attente d'urgence n'affecte pas les connexions existantes. Seules les demandes présentes dans la file d'attente d'urgence sont supprimées. Pour ces demandes, le client doit faire une nouvelle demande.

Vous pouvez également vider la file d'attente d'un serveur virtuel de commutation de contenu. Si un serveur virtuel de commutation de contenu transmet certaines demandes à un serveur virtuel d'équilibrage de charge particulier et que le serveur virtuel d'équilibrage de charge reçoit également d'autres demandes, lorsque vous videz la file d'attente du serveur virtuel de commutation de contenu, seules les demandes reçues de ce serveur virtuel de commutation de contenu sont vidées. Les autres requêtes de la file d'attente de surtension du serveur virtuel d'équilibrage de charge ne sont pas vidées.

Remarque : Vous ne pouvez pas vider les files d'attente de redirection de cache, d'authentification, de VPN ou de serveurs virtuels GSLB ou de services GSLB.

Remarque : N'utilisez pas la fonction de protection contre les surtensions si l'option Use Source IP (USIP) est activée.

Pour vider une file d'attente d'urgence à l'aide de l'interface de ligne de commande

La commande flush ns SurgeQ fonctionne de la manière suivante :

- Vous pouvez spécifier le nom d'un service, d'un groupe de services ou d'un serveur virtuel dont la file d'attente doit être vidée.
- Si vous spécifiez un nom lors de l'exécution de la commande, la file d'attente de surtension de l'entité spécifiée est vidé. Si plusieurs entités portent le même nom, l'appliance vide les files d'attente de toutes ces entités.
- Si vous spécifiez le nom d'un groupe de services, ainsi qu'un nom de serveur et un port lors de l'exécution de la commande, l'appliance vide la file d'attente de surtension du membre du groupe de services spécifié uniquement.

- Vous ne pouvez pas spécifier directement un membre du groupe de services (<serverName> et <port>) sans spécifier le nom du groupe de services (<name>) et vous ne pouvez pas spécifier <port> sans un <serverName>. Spécifiez le <serverName> et <port> si vous souhaitez vider la file d'attente de surtension pour un membre du groupe de services spécifique.
- Si vous exécutez la commande sans spécifier de nom, l'appliance vide les files d'attente de surtension de toutes les entités présentes sur l'appliance.
- Si un membre du groupe de services est identifié par un nom de serveur, vous devez spécifier le nom du serveur dans cette commande ; vous ne pouvez pas spécifier son adresse IP.

À l'invite de commande, tapez :

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
<!--NeedCopy-->
```

Exemples

```
flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80
<!--NeedCopy-->
```

La commande précédente vide la file d'attente de surtension du service ou du serveur virtuel appelé SVC1ANZGB et dont l'adresse IP est 10.10.10.

```
flush ns surgeQ
<!--NeedCopy-->
```

La commande précédente vide toutes les files d'attente de surtension de l'appliance.

Pour vider une file d'attente de surtension à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels**, sélectionnez un serveur virtuel et, dans la liste Action, sélectionnez **Vider la file d'attente de surtension**.

Gérer une configuration d'équilibrage de charge

May 5, 2023

La maintenance d'une configuration d'équilibrage de charge existante ne nécessite pas beaucoup de travail tant qu'elle reste inchangée, mais la plupart ne le restent pas longtemps. L'augmentation de la charge nécessite de nouveaux serveurs à équilibrage de charge et, à terme, de nouvelles appliances NetScaler, qui doivent être configurées et ajoutées à la configuration existante. Les anciens

serveurs s'usent et doivent être remplacés, ce qui nécessite la suppression de certains serveurs et l'ajout d'autres. Les mises à niveau de votre équipement réseau ou les modifications apportées à la topologie peuvent également nécessiter des modifications de votre configuration d'équilibrage de charge. Par conséquent, vous devez effectuer des opérations sur des objets serveur, des services et des serveurs virtuels. Le Visualizer peut afficher votre configuration graphiquement et vous pouvez effectuer des opérations sur les entités de l'affichage. Vous pouvez également profiter d'autres fonctionnalités qui facilitent la gestion du trafic via votre configuration d'équilibrage de charge.

Gérer les objets serveur

May 5, 2023

Lors de la configuration de base de l'équilibrage de charge, lorsque vous créez un service, un objet serveur avec l'adresse IP du service est créé, s'il n'en existe pas. Si vous préférez les objets de service nommés avec des noms de domaine plutôt que des adresses IP, vous pouvez également avoir créé manuellement un ou plusieurs objets serveur. Vous pouvez activer, désactiver ou supprimer n'importe quel objet serveur.

Lorsque vous activez ou désactivez un objet serveur, vous activez ou désactivez tous les services associés à cet objet serveur. Lorsque vous actualisez l'appliance NetScaler après avoir désactivé un objet serveur, l'état de son service apparaît comme HORS SERVICE. Si vous spécifiez un délai d'attente lors de la désactivation d'un objet serveur, l'objet serveur continue à gérer les connexions établies pendant la durée spécifiée, mais rejette les nouvelles connexions. Si vous supprimez un objet serveur, le service auquel il est lié est également supprimé.

Pour activer un serveur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
enable server <name>
<!--NeedCopy-->
```

Exemple :

```
enable server 10.102.29.5
<!--NeedCopy-->
```

Pour activer ou désactiver un objet serveur à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Servers**.
2. Sélectionnez le serveur et, dans la liste Action, sélectionnez **Activer** ou **Désactiver**.

Pour désactiver un objet serveur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
disable server <name> <delay>
<!--NeedCopy-->
```

Exemple :

```
disable server 10.102.29.5 30
<!--NeedCopy-->
```

Pour supprimer un objet serveur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm server <name>
<!--NeedCopy-->
```

Exemple :

```
rm server 10.102.29.5
<!--NeedCopy-->
```

Pour supprimer un objet serveur à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Servers**.
2. Sélectionnez un serveur, puis cliquez sur **Supprimer**.

Gérer les services

May 5, 2023

Les services sont activés par défaut lorsque vous les créez. Vous pouvez désactiver ou activer chaque service individuellement. Lorsque vous désactivez un service, vous spécifiez normalement un délai d'attente pendant lequel le service continue de traiter les connexions établies, mais rejette les nouvelles, avant de s'arrêter. Si vous ne spécifiez pas de temps d'attente, le service s'arrête immédiatement. Pendant le temps d'attente, l'état du service est HORS SERVICE.

Vous pouvez supprimer un service lorsqu'il n'est plus utilisé. Lorsque vous supprimez un service, il est dissocié de son serveur virtuel et supprimé de la configuration NetScaler.

Pour activer ou désactiver un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
enable service <name>

disable service <name> <DelayInSeconds>
<!--NeedCopy-->
```

Exemples :

```
enable service Service-HTTP-1
disable service Service-HTTP-1 30
<!--NeedCopy-->
```

Pour activer ou désactiver un service à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Ouvrez un service et, dans la liste des **actions**, sélectionnez **Activer** ou **Désactiver**.

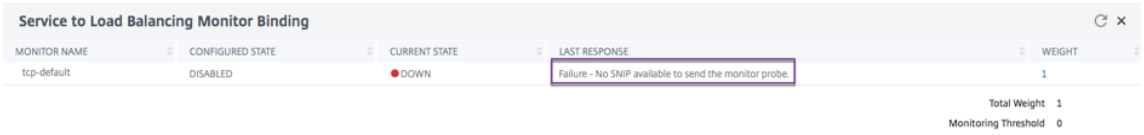
Identifiez la cause de l'état du service marqué « BAS » à l'aide de l'interface graphique

À partir de NetScaler version 13.0 build 41.20, vous pouvez consulter les informations de sonde du moniteur sur l'interface graphique pour les services qui sont hors service sans accéder à l'interface de liaison du moniteur. La valeur de la colonne **État du serveur** de la page Services est cliquable. Vous pouvez cliquer sur **le bouton VERS LE BAS** pour identifier la cause première à cause de laquelle le service est marqué comme NON FONCTIONNEL.

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Cliquez sur **BAS** dans la colonne **État du serveur** correspondant au service qui est en panne.

La page Service to Load Balancing Monitor Binding s'affiche.

La colonne **Dernière réponse** indique la raison pour laquelle le service est marqué comme étant inactif.



Gestion d'un serveur virtuel d'équilibrage de charge

May 5, 2023

Les serveurs virtuels sont activés par défaut lorsque vous les créez. Vous pouvez désactiver et activer les serveurs virtuels manuellement. Si vous désactivez un serveur virtuel, l'état du service virtuel apparaît comme HORS SERVICE. Dans ce cas, le serveur virtuel met fin à toutes les connexions, soit immédiatement, soit après avoir autorisé la fin des connexions existantes, en fonction du paramètre DownStateFlush. Si DownStateFlush est activé (par défaut), toutes les connexions sont vidées. Si cette option est DÉSACTIVÉE, le serveur virtuel continue de traiter les demandes sur les connexions existantes.

Vous supprimez un serveur virtuel uniquement lorsque vous n'en avez plus besoin. Avant de le supprimer, vous devez en dissocier tous les services.

Pour activer ou désactiver un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
enable lb vserver <name>
<!--NeedCopy-->
```

```
disable lb vserver <name>
<!--NeedCopy-->
```

Exemples :

```
enable lb vserver Vserver-LB-1
disable lb vserver Vserver-LB-1
<!--NeedCopy-->
```

Pour activer ou désactiver un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel et, dans la liste des **actions**, sélectionnez **Activer** ou **Désactiver**.

Pour dissocier un service d'un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
unbind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
unbind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

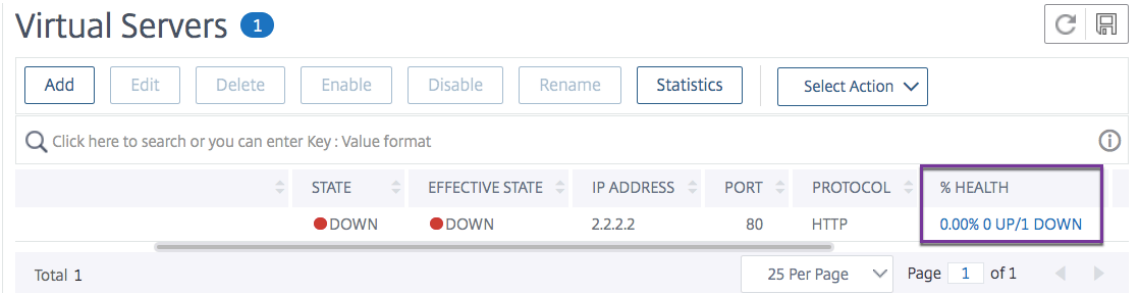
Pour dissocier un service d'un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et cliquez dans la section **Services** .
3. Sélectionnez un service et cliquez sur **Dissocier.**

Identifier la cause de l'état du serveur virtuel marqué comme DOWN à l'aide de l'interface graphique

À partir de NetScaler version 13.0 build 41.20, vous pouvez consulter les informations de sonde du moniteur sur l'interface graphique des serveurs virtuels qui sont hors service sans accéder à l'interface de liaison du moniteur. La valeur de la colonne **% HEALTH** de la page Serveur virtuel est cliquable. Vous pouvez cliquer sur la valeur dans la colonne **% HEALTH** pour identifier la cause première à cause de laquelle le serveur virtuel est marqué comme étant inactif.

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur la valeur dans la colonne **% HEALTH** correspondant au serveur virtuel en panne.

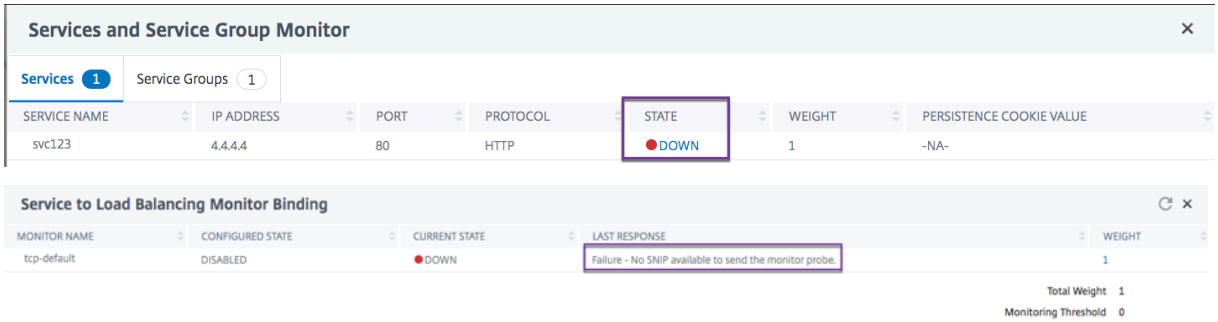


La page Moniteur des services et des groupes de services s'affiche. Les services et groupes de services liés à ce serveur virtuel sont affichés dans les onglets correspondants.

Si vous utilisez des services liés à l'équilibrage de charge virtuel, procédez comme suit :

Dans l'onglet **Services**, cliquez sur **VERS LE BAS** correspondant au service qui est en panne.

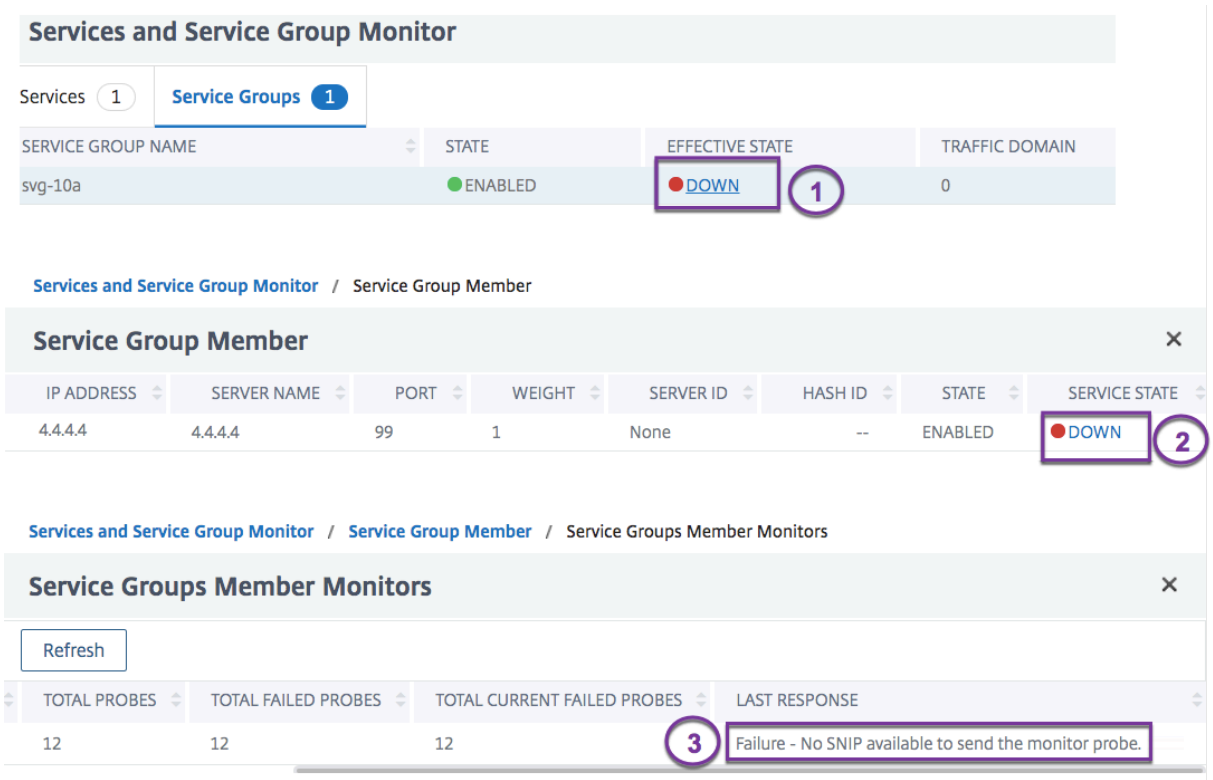
La colonne **Dernière réponse** de la page de liaison entre Service et Load Balancing Monitor affiche la raison pour laquelle le serveur virtuel est classé comme étant en baisse.



Si vous utilisez des groupes de services liés à un équilibrage de charge virtuel, procédez comme suit :

Dans l'onglet **Groupes de services**, cliquez sur **VERS LE BAS** dans la page Services et Moniteur des groupes de services, puis cliquez sur **BAS** dans la page Membres du groupe de services.

La colonne **Dernière réponse** de la page Service Groups Member Monitors indique la raison pour laquelle le serveur virtuel est classé comme étant inférieur.



Visualiseur d'équilibrage de charge

April 11, 2023

Le visualiseur d'équilibrage de charge est un outil que vous pouvez utiliser pour afficher et modifier la configuration d'équilibrage de charge dans un format graphique. Voici un exemple de l'affichage Visualizer.

Figure 1. Affichage du visualiseur d'équilibrage de charge

Vous pouvez utiliser le visualiseur pour afficher les éléments suivants :

- Services et groupes de services liés à un serveur virtuel.
- Les moniteurs liés à chaque service.
- Stratégies liées au serveur virtuel.
- Les étiquettes de stratégie, si elles sont configurées.
- Détails de configuration de tout élément affiché.

Vous pouvez également utiliser le visualiseur pour ajouter et lier de nouveaux objets, modifier des objets existants et activer ou désactiver des objets. La plupart des éléments de configuration affichés dans Visualizer apparaissent sous les mêmes noms que dans d'autres parties de l'utilitaire de configuration. Toutefois, contrairement au reste de l'utilitaire de configuration, Visualizer regroupe les services qui ont les mêmes détails de configuration et surveillent les liaisons dans une entité appelée conteneur de service.

Un conteneur de service est un ensemble de services et de groupes de services similaires liés à un seul serveur virtuel d'équilibrage de charge. Les services du conteneur ont les mêmes propriétés, à l'exception du nom, de l'adresse IP et du port, et leurs liaisons de moniteur doivent avoir le même poids et l'état de liaison. Lorsque vous liez un nouveau service à un serveur virtuel, il est placé dans un conteneur existant si ses liaisons de configuration et de surveillance correspondent à celles d'autres services. Sinon, il est placé dans son propre conteneur.

Les procédures suivantes fournissent uniquement les étapes de base de l'utilisation du visualiseur. Étant donné que le Visualizer duplique des fonctionnalités dans d'autres zones de la fonction d'équilibrage de charge, d'autres méthodes d'affichage ou de configuration de tous les paramètres pouvant être configurés dans le Visualizer sont fournies dans la documentation d'équilibrage de charge.

Remarque : Le Visualizer nécessite une interface graphique, de sorte qu'il n'est disponible que via l'utilitaire de configuration.

Pour afficher les propriétés du serveur virtuel d'équilibrage de charge à l'aide du Visualizer

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez afficher, puis cliquez sur **Visualiseur**.

Pour afficher les détails de configuration des services, des groupes de services et des moniteurs à l'aide du Visualizer

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez afficher, puis cliquez sur **Visualiseur**.
3. Dans la boîte de dialogue Load Balancing Visualizer, double-cliquez sur l'entité pour afficher les détails de configuration de l'entité liée à ce serveur virtuel, vous pouvez effectuer les opérations suivantes :

Pour afficher les détails de configuration des stratégies et des étiquettes de stratégie à l'aide du Visualizer dans l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel que vous souhaitez afficher, puis cliquez sur Visualiseur.
3. Dans la boîte de dialogue Visualiseur d'équilibrage de charge, double-cliquez sur l'entité de stratégies pour afficher les stratégies liées à ce serveur virtuel.

Pour modifier une ressource dans une configuration d'équilibrage de charge à l'aide du Visualizer

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel à configurer, puis cliquez sur Visualizer.
3. Dans la boîte de dialogue Load Balancing Visualizer, sur l'image Visualizer, double-cliquez sur la ressource à modifier.

Pour ajouter une configuration d'équilibrage de charge à l'aide du Visualizer

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez le serveur virtuel à configurer, puis cliquez sur Visualizer.

3. Dans la boîte de dialogue Load Balancing Visualizer, cliquez sur **+** pour ajouter la ressource.

Gérer le trafic client

May 5, 2023

La gestion correcte des connexions client permet de garantir que vos applications restent disponibles pour les utilisateurs même lorsque votre appliance NetScaler est confrontée à des charges élevées. Diverses fonctions d'équilibrage de charge et autres fonctionnalités disponibles sur l'appliance peuvent être intégrées dans une configuration d'équilibrage de charge pour traiter la charge plus efficacement, la détourner si nécessaire et hiérarchiser les tâches que l'appliance doit effectuer :

- **Équilibrage de charge sans session.** Vous pouvez configurer des serveurs virtuels d'équilibrage de charge sans session et effectuer l'équilibrage de charge sans créer de sessions dans des configurations utilisant DSR ou des systèmes de détection d'intrusion (IDS).
- **Mise en cache intégrée.** Vous pouvez rediriger les requêtes HTTP vers un cache.
- **Nettoyage retardé.** Vous pouvez configurer le nettoyage différé des connexions au serveur virtuel pour empêcher le processus de nettoyage d'utiliser les cycles du processeur pendant les périodes où l'appliance NetScaler est confrontée à des charges élevées.
- **Réécriture.** Vous pouvez utiliser la fonction de réécriture pour modifier le port et le protocole lors de la redirection HTTP, ou insérer l'adresse IP et le port du serveur virtuel dans un en-tête de demande personnalisé.
- **RTSP NAT.**
- **Surveillance basée sur les tarifs.** Vous pouvez activer la surveillance basée sur le débit pour détourner le trafic excédentaire.
- **Paramètres de la couche 2.** Vous pouvez configurer un serveur virtuel pour qu'il utilise les paramètres L2 pour identifier une connexion.
- **Réponse ICMP**. Vous pouvez configurer l'appliance pour qu'elle envoie des réponses ICMP aux demandes PING en fonction de vos paramètres. Sur l'adresse IP correspondant au serveur virtuel, définissez la RÉPONSE ICMP sur VSVR_CNTRLD et, sur le serveur virtuel, définissez le `ICMP VSERVER RESPONSE`.

  Les paramètres suivants peuvent être définis sur un serveur virtuel :
  - Lorsque vous définissez `ICMP VSERVER RESPONSE` la valeur PASSIVE sur tous les serveurs virtuels, l'appliance répond toujours.
  - Lorsque vous définissez `ICMP VSERVER RESPONSE` la valeur ACTIVE sur tous les serveurs virtuels, l'appliance répond même si un serveur virtuel est activé.
  - Lorsque vous définissez `ICMP VSERVER RESPONSE` la valeur ACTIVE sur certains et PASSIVE sur d'autres, l'appliance répond même si un serveur virtuel défini sur ACTIVE est activé.

Configuration des serveurs virtuels d'équilibrage de charge sans session

May 5, 2023

Lorsque l'appliance NetScaler effectue un équilibrage de charge, elle crée et gère des sessions entre les clients et les serveurs. La maintenance des informations de session sollicite considérablement les ressources de l'appliance, et les sessions peuvent ne pas être nécessaires dans des scénarios tels que la configuration d'un retour direct au serveur (DSR) et l'équilibrage de charge des systèmes de détection d'intrusion (IDS). Pour éviter de créer des sessions lorsqu'elles ne sont pas nécessaires, vous pouvez configurer un serveur virtuel sur l'appliance pour un équilibrage de charge sans session. Dans le cadre de l'équilibrage de charge sans session, l'appliance effectue un équilibrage de charge par paquet.

L'équilibrage de charge sans session peut fonctionner en mode de transfert basé sur Mac ou en mode de transfert basé sur IP.

Pour le transfert basé sur Mac, l'adresse IP du serveur virtuel sans session doit être spécifiée sur tous les serveurs physiques vers lesquels le trafic est transféré.

Pour le transfert basé sur IP dans le cadre de l'équilibrage de charge sans session, il n'est pas nécessaire de spécifier l'adresse IP et le port du serveur virtuel sur les serveurs physiques, car ces informations sont incluses dans les paquets transférés. Lors du transfert d'un paquet du client vers le serveur physique, l'appliance laisse inchangés les détails du client tels que l'adresse IP et le port et ajoute l'adresse IP et le port de la destination.

Configuration prise en charge

L'équilibrage de charge sans session NetScaler prend en charge les types de service et les méthodes d'équilibrage de charge suivants :

Types de services

- ANY pour la redirection basée sur Mac
- ANY, DNS et UDP pour la redirection basée sur IP

Méthodes d'équilibrage de charge

- Round Robin
- Moins de bande passante
- LRTM (méthode du temps de réponse le plus court)
- Hash IP source
- Hachage IP de destination

- IP source, hachage IP de destination
- Adresse IP source Hachage du port source
- Chargement personnalisé

Limitations

L'équilibrage de charge sans session présente les limites suivantes :

- L'appliance doit être déployée en mode à deux bras.
- Un service doit être lié à un seul serveur virtuel.
- L'équilibrage de charge sans session n'est pas pris en charge pour les groupes de services.
- L'équilibrage de charge sans session n'est pas pris en charge pour les services basés sur des domaines (services DBS).
- L'équilibrage de charge sans session en mode IP n'est pas pris en charge pour un serveur virtuel configuré comme sauvegarde sur un serveur virtuel principal.
- Vous ne pouvez pas activer le mode spillover.
- Pour tous les services liés à un serveur virtuel d'équilibrage de charge sans session, l'option Use Source IP (USIP) doit être activée.
- Pour un serveur ou un service virtuel générique, l'adresse IP de destination n'est pas modifiée.

Remarque :

- Lors de la configuration d'un serveur virtuel pour un équilibrage de charge sans session, spécifiez explicitement une méthode d'équilibrage de charge prise en charge. La méthode par défaut, Least Connection, ne peut pas être utilisée pour l'équilibrage de charge sans session.
- Pour configurer l'équilibrage de charge sans session en mode de redirection basé sur Mac sur un serveur virtuel, l'option de transfert basée sur MAC doit être activée sur l'appliance NetScaler.

Pour ajouter un serveur virtuel sans session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un serveur virtuel sans session et vérifier la configuration :

```
add lb vserver <name>@ <serviceType> <IPAddress>@ <port> -m <
    redirectionMode> -sessionless <(ENABLED|DISABLED)> -lbMethod <
    load_balancing_method>

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :


```
1  add lb vserver sesslessv1 any 11.11.12.123 54 -sessionless ENABLED -
      lbMethod roundrobin -m ip
2       Done
3  show lb vserver sesslessv1
4       sesslessv1 (11.11.12.123:54) - ANY Type: ADDRESS
5       State: DOWN
6       ...
7       Effective State: DOWN
8       Client Idle Timeout: 120 sec
9       Down state flush: ENABLED
10      ...
11      Persistence: NONE
12      Sessionless LB: ENABLED
13      Connection Failover: DISABLED
14      L2Conn: OFF
15      1) Policy : cmp_text Priority:8680 Inherited
16      2) Policy : cmp_nocmp_ie60 Priority:8690 Inherited
17 <!--NeedCopy-->
```

Pour configurer l'équilibrage de charge sans session sur un serveur virtuel existant

À l'invite de commande, tapez :

```
1 set lb vserver <name>@ -m <redirectionMode> -sessionless <(ENABLED|
     DISABLED)> -lbMethod <load_balancing_method>
2 <!--NeedCopy-->
```

Exemple

```
1 set lb vserver sesslessv1 -m mac -sessionless ENABLED -lbmethod lrtm
2   Done
3 <!--NeedCopy-->
```

> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l' `-m MAC` option est activée, vous devez lier un moniteur non utilisateur.

Pour configurer un serveur virtuel sans session à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

2. Ouvrez le serveur virtuel, puis dans Paramètres avancés, cliquez sur Paramètres de trafic, puis sélectionnez Équilibrage de charge sans session.

Rediriger les requêtes HTTP vers un cache

May 5, 2023

La fonctionnalité de redirection du cache de NetScaler redirige les requêtes HTTP vers un cache. Vous pouvez réduire considérablement l'impact de la réponse aux demandes HTTP et améliorer les performances de votre site Web grâce à la mise en œuvre correcte de la fonctionnalité de redirection du cache.

Un cache stocke le contenu HTTP fréquemment demandé. Lorsque vous configurez la redirection du cache sur un serveur virtuel, l'appliance NetScaler envoie des requêtes HTTP pouvant être mises en cache au cache et des requêtes HTTP non mises en cache au serveur Web d'origine.

Pour configurer la redirection du cache sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -cacheable <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -cacheable yes
<!--NeedCopy-->
```

Pour configurer la redirection du cache sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur Paramètres de trafic, puis sélectionnez Cacheable.

Activer le nettoyage des connexions au serveur virtuel

May 5, 2023

Sous certaines conditions, vous pouvez configurer le paramètre DownStateFlush pour mettre fin immédiatement aux connexions existantes lorsqu'un service ou un serveur virtuel est marqué « DOWN ». La fin des connexions existantes libère des ressources et, dans certains cas, accélère la récupération des configurations d'équilibrage de charge surchargées.

L'état d'un serveur virtuel dépend de l'état des services qui y sont liés. L'état de chaque service dépend des réponses des serveurs à charge équilibrée aux sondes et aux contrôles de santé envoyés par les moniteurs liés à ce service. Parfois, les serveurs à charge équilibrée ne répondent pas. Si un serveur est lent ou occupé, le temps imparti aux sondes de surveillance peut être dépassé. Si les sondes de surveillance répétées ne sont pas répondues dans le délai d'expiration configuré, le service est marqué DOWN.

Un serveur virtuel est marqué comme étant inactif uniquement lorsque tous les services qui y sont liés sont marqués comme étant hors service. Lorsqu'un serveur virtuel est en panne, il met fin à toutes les connexions, soit immédiatement, soit après avoir autorisé les connexions existantes à se terminer.

N'activez pas le paramètre DownStateFlush sur les serveurs d'applications qui doivent terminer leurs transactions. Vous pouvez activer ce paramètre sur les serveurs Web dont les connexions peuvent être interrompues en toute sécurité lorsqu'ils sont marqués comme DOWN.

Le tableau suivant résume l'effet de ce paramètre sur un exemple de configuration consistant en un serveur virtuel, vServer-LB-1, auquel est lié un service, Service-TCP-1. Dans le tableau, E et D indiquent l'état du paramètre DownStateFlush : E signifie Activé et D signifie Désactivé.

Vserver-LB-1	Service-TCP-1	État des connexions
E	E	Les connexions client et serveur sont interrompues.

Vserver-LB-1	Service-TCP-1	État des connexions
E	D	Pour certains types de services, tels que TCP, pour lesquels l'appliance NetScaler ne prend pas en charge la réutilisation des connexions, les connexions client et serveur sont interrompues. Pour les types de service, tels que HTTP, pour lesquels l'appliance prend en charge la réutilisation des connexions, les connexions client et serveur ne sont interrompues que si une transaction est active sur ces connexions. Si une transaction n'est pas active, seules les connexions client sont interrompues.
D	E	Pour certains types de services, tels que TCP, pour lesquels l'appliance NetScaler ne prend pas en charge la réutilisation des connexions, les connexions client et serveur sont interrompues. Pour les types de service, tels que HTTP, pour lesquels l'appliance prend en charge la réutilisation des connexions, les connexions client et serveur ne sont interrompues que si une transaction est active sur ces connexions. Si une transaction n'est pas active, seules les connexions au serveur sont interrompues.

Vserver-LB-1	Service-TCP-1	État des connexions
D	D	Ni les connexions client ni serveur ne sont interrompues.

Si vous souhaitez désactiver un service uniquement lorsque toutes les connexions établies sont fermées par le serveur ou le client, vous pouvez utiliser l'option d'arrêt gracieux. Pour plus d'informations sur l'arrêt gracieux d'un service, voir Arrêt gracieux des services.

Pour configurer le paramètre de vidage d'état en panne sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -downStateFlush <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -downStateFlush enabled
<!--NeedCopy-->
```

Pour configurer le paramètre down state flush sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur Paramètres de trafic, puis sélectionnez Déclenchement de l'état.

Réécriture des ports et des protocoles pour la redirection HTTP

May 5, 2023

Les serveurs virtuels et les services qui y sont liés peuvent utiliser différents ports. Lorsqu'un service répond à une connexion HTTP par une redirection, vous devrez peut-être configurer l'appliance NetScaler pour modifier le port et le protocole afin de garantir le bon déroulement de la redirection. Pour ce faire, activez et configurez le paramètre redirectPortRewrite.

Ce paramètre ne concerne que le trafic HTTP et HTTPS. Si ce paramètre est activé sur un serveur virtuel, le serveur virtuel réécrit le port lors des redirections, en remplaçant le port utilisé par le service par le port utilisé par le serveur virtuel.

Si le serveur ou le service virtuel est de type SSL, vous devez activer la redirection SSL sur le serveur ou le service virtuel. Si le serveur virtuel et le service sont de type SSL, activez la redirection SSL sur le serveur virtuel.

Le paramètre redirectPortRewrite peut être utilisé dans les scénarios suivants :

- Le serveur virtuel est de type HTTP et les services sont de type SSL.
- Le serveur virtuel est de type SSL et les services sont de type HTTP.
- Le serveur virtuel est de type HTTP et les services sont de type HTTP.
- Le serveur virtuel est de type SSL et les services sont de type SSL.

Scénario 1 : Le serveur virtuel est de type HTTP et les services sont de type SSL. La redirection SSL, et éventuellement la réécriture des ports, sont activées sur le service. Si la réécriture de port est activée, le port des URL HTTPS est réécrit. Les URL HTTP du serveur sont envoyées telles quelles au client.

Seule la redirection SSL est activée. Le serveur virtuel peut être configuré sur n'importe quel port. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirection SSL et la réécriture des ports sont activées. Le serveur virtuel est configuré sur le port 80. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com/

La redirection SSL et la réécriture des ports sont activées. Le serveur virtuel est configuré sur le port 8080. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	http://domain.com:8080/
https://domain.com:444/	http://domain.com:8080/

Scénario 2 : Le serveur virtuel est de type SSL et les services sont de type HTTP. Si la réécriture de port est activée, seul le port des URL HTTP est réécrit. Les URL HTTPS du serveur sont envoyées telles quelles au client.

La redirection SSL est activée sur le serveur virtuel. Le serveur virtuel peut être configuré sur n'importe quel port. Voir le tableau suivant.

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirection SSL et la réécriture des ports sont activées sur le serveur virtuel. Le serveur virtuel est configuré sur le port 443. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirection SSL et la réécriture des ports sont activées. Le serveur virtuel est configuré sur le port 444. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	https://domain.com:444/
http://domain.com:8080/	https://domain.com:444/
https://domain.com/	https://domain.com/
https://domain.com:445/	https://domain.com:445/

Scénario 3 : Le serveur virtuel et le service sont de type HTTP. La réécriture des ports doit être activée sur le serveur virtuel. Seul le port des URL HTTP est réécrit. Les URL HTTPS du serveur sont envoyées telles quelles au client.

Le serveur virtuel est configuré sur le port 80. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

Le serveur virtuel est configuré sur le port 8080. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	http://domain.com:8080/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:445/	https://domain.com:445/

Scénario 4 : Le serveur virtuel et le service sont de type SSL. Si la réécriture de port est activée, seul le port des URL HTTPS est réécrit. Les URL HTTP du serveur sont envoyées telles quelles au client.

La redirection SSL est activée sur le serveur virtuel. Le serveur virtuel peut être configuré sur n'importe quel port. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

La redirection SSL et la réécriture des ports sont activées sur le serveur virtuel. Le serveur virtuel est configuré sur le port 443. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com/

La redirection SSL et la réécriture des ports sont activées sur le serveur virtuel. Le serveur virtuel est configuré sur le port 444. Consultez le tableau suivant :

URL de redirection depuis le serveur	URL de redirection envoyée au client
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com:444/
https://domain.com:445/	https://domain.com:444/

Pour configurer la redirection HTTP sur un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -redirectPortRewrite (ENABLED | DISABLED)
<!--NeedCopy-->
```

Exemple :


```
set lb vserver Vserver-LB-1 -redirectPortRewrite enabled
<!--NeedCopy-->
```

Pour configurer la redirection HTTP sur un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez le serveur virtuel et, dans le volet Paramètres avancés, cliquez sur Paramètres du trafic, puis sélectionnez Réécrire.

Pour configurer la redirection SSL sur un serveur virtuel ou un service SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl vserver <vServerName> - sslRedirect (ENABLED | DISABLED)

set ssl service <serviceName> - sslRedirect (ENABLED | DISABLED)
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver Vserver-SSL-1 -sslRedirect enabled

set ssl service service-SSL-1 -sslRedirect enabled
<!--NeedCopy-->
```

Pour configurer la redirection SSL et la réécriture du port SSL sur un serveur virtuel ou un service SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans Paramètres avancés, cliquez sur Paramètres SSL, puis sélectionnez Redirection SSL.

Insérer l'adresse IP et le port d'un serveur virtuel dans l'en-tête de requête

May 5, 2023

Si plusieurs serveurs virtuels communiquent avec différentes applications sur le même service, vous devez effectuer les opérations suivantes :

Configurez l'appliance NetScaler pour ajouter l'adresse IP et le numéro de port du serveur virtuel approprié aux requêtes HTTP envoyées à ce service. Ce paramètre permet aux applications exécutées sur le service d'identifier le serveur virtuel qui a envoyé la demande.

Si le serveur virtuel principal est en panne et que le serveur virtuel de sauvegarde est actif, les paramètres de configuration du serveur virtuel de sauvegarde sont ajoutés aux demandes du client. Si vous souhaitez ajouter la même balise d'en-tête, que les demandes proviennent du serveur virtuel principal ou du serveur virtuel de sauvegarde, vous devez configurer la balise d'en-tête requise sur les deux serveurs virtuels.

Remarque : Cette option n'est pas prise en charge pour les serveurs virtuels génériques ou les serveurs virtuels fictifs.

Pour insérer l'adresse IP et le port du serveur virtuel dans les demandes du client à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -insertVserverIPPort <insertVserverIPPort> [<
    vipHeader>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -insertVserverIPPort VipAddr
<!--NeedCopy-->
```

Pour insérer l'adresse IP et le port du serveur virtuel dans les demandes du client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez le serveur virtuel et, dans le volet Paramètres avancés, cliquez sur Paramètres de **trafic**, puis sélectionnez Insertion de port IP Virtual Server et spécifiez un en-tête de port IP du serveur virtuel.

Utiliser une adresse IP source spécifiée pour la communication back-end

May 5, 2023

Pour communiquer avec les serveurs physiques ou d'autres appareils homologues, l'appliance NetScaler utilise une adresse IP qui lui appartient comme adresse IP source. L'appliance NetScaler gère un pool d'adresses IP et sélectionne dynamiquement une adresse IP lors de la connexion à un serveur. En fonction du sous-réseau dans lequel le serveur physique est placé, l'appliance décide de l'adresse IP à utiliser. Ce pool d'adresses est utilisé pour envoyer du trafic et surveiller les sondes.

Dans de nombreux cas, vous pouvez souhaiter que l'appliance utilise une adresse IP spécifique ou n'importe quelle adresse IP provenant d'un ensemble spécifique d'adresses IP pour les communications back-end. Voici quelques exemples :

- Un serveur peut distinguer les sondes de surveillance du trafic si l'adresse IP source utilisée pour les sondes de surveillance appartient à un ensemble spécifique.
- Pour améliorer la sécurité du serveur, un serveur peut être configuré pour répondre à des demandes provenant d'un ensemble spécifique d'adresses IP ou, parfois, d'une seule adresse IP spécifique. Dans ce cas, l'appliance peut utiliser uniquement les adresses IP acceptées par le serveur comme adresse IP source.
- L'appliance peut gérer efficacement ses connexions internes si elle peut distribuer ses adresses IP en ensembles IP et utiliser une adresse d'un ensemble uniquement pour se connecter à un service spécifique.

Pour configurer l'appliance pour qu'elle utilise une adresse IP source spécifiée, créez des profils réseau (profils réseau) et configurez les entités de l'appliance pour qu'elles utilisent le profil. Un profil réseau peut être lié à des serveurs virtuels d'équilibrage de charge ou de commutation de contenu, à des serveurs virtuels VPN NetScaler Gateway, à des services, à des groupes de services ou à des moniteurs. Un profil réseau possède des adresses IP appartenant à NetScaler (SNIP et VIP) qui peuvent être utilisées comme adresse IP source. Il peut s'agir d'une adresse IP unique ou d'un ensemble d'adresses IP, appelé ensemble d'adresses IP. Si un profil réseau possède un ensemble d'adresses IP, l'appliance sélectionne dynamiquement une adresse IP parmi l'ensemble d'adresses IP au moment de la connexion. Si un profil possède une seule adresse IP, la même adresse IP est utilisée comme adresse IP source.

Si un profil réseau est lié à un serveur virtuel d'équilibrage de charge ou de commutation de contenu, le profil est utilisé pour envoyer du trafic vers tous les services qui lui sont liés. Si un profil réseau est lié à un groupe de services, l'appliance utilise le profil pour tous les membres du groupe de services. Si un profil réseau est lié à un moniteur, l'appliance utilise le profil pour toutes les sondes envoyées à partir du moniteur.

Remarque :

- Lorsqu'une appliance NetScaler utilise une adresse VIP pour communiquer avec un serveur, elle utilise les entrées de session pour identifier si le trafic destiné à l'adresse VIP est une réponse d'un serveur ou une demande d'un client.
- Vous pouvez lier un profil réseau aux serveurs virtuels VPN NetScaler Gateway. Toutefois, vous devez noter certains points lorsque vous liez un profil net. Pour plus d'informations, voir Points à noter lors de la liaison d'un profil réseau à un serveur virtuel VPN.
- Les adresses IP de profil réseau liées à un service ou à un groupe de services sont utilisées non seulement pour envoyer du trafic vers les serveurs principaux correspondants, mais également pour les demandes DNS qui sont déclenchées par tout nom de domaine complet principal non résolu.

Utilisation d'un profil net pour l'envoi de trafic

Si l'option Utiliser l'adresse IP source (USIP) est activée, l'appliance utilise l'adresse IP du client et ignore tous les profils réseau. Si l'option USIP n'est pas activée, l'appliance sélectionne l'adresse IP source de la manière suivante :

- S'il n'existe aucun profil réseau sur le serveur virtuel ou le groupe de services/services, l'appliance utilise la méthode par défaut.
- S'il existe un profil réseau uniquement sur le groupe de services/services, l'appliance utilise ce profil réseau.
- S'il existe un profil réseau uniquement sur le serveur virtuel, l'appliance utilise le profil réseau.
- S'il existe un profil réseau à la fois sur le serveur virtuel et sur le groupe de services/services, l'appliance utilise le profil réseau lié au service/groupe de services.

Utilisation d'un profil réseau pour l'envoi de sondes de moniteur :

Pour les sondes de surveillance, l'appliance sélectionne l'adresse IP source de la manière suivante :

- Si un profil réseau est lié au moniteur, l'appliance utilise le profil net du moniteur. Il ignore les profils réseau liés au serveur virtuel ou au groupe de services/services.
- Si aucun profil réseau n'est lié au moniteur,
  - S'il existe un profil réseau sur le groupe de services/services, l'appliance utilise le profil réseau du service/groupe de services.
  - S'il n'existe aucun profil réseau, même sur le groupe de service/service, l'appliance utilise la méthode par défaut de sélection d'une adresse IP source.

Remarque : S'il n'existe aucun profil réseau lié à un service, l'appliance recherche un profil réseau sur le groupe de services si le service est lié à un groupe de services.

Pour utiliser une adresse IP source spécifiée pour la communication, procédez comme suit :

1. Créez des ensembles d'adresses IP à partir du pool de SNIP et de VIP appartenant à l'appliance NetScaler. Un jeu d'adresses IP peut être constitué à la fois d'adresses SNIP et VIP. Pour obtenir des instructions, voir Création de jeux d'adresses IP.
2. Créez des profils réseau. Pour obtenir des instructions, reportez-vous à la section Création d'un profil réseau.
3. Liez les profils réseau aux entités de l'appliance. Pour obtenir des instructions, consultez Liaison d'un profil réseau à une entité NetScaler.

> **Remarque :**
>
> - Un profil réseau ne peut avoir que les adresses IP spécifiées comme SNIP et VIP sur l'appliance NetScaler.
> - La persistance de l'adresse IP source n'est pas respectée pour les paquets initiés par NetScaler.

Gérer les profils de réseau

Un profil réseau (ou profil réseau) contient une adresse IP ou un ensemble d'adresses IP. Lors de la communication avec des serveurs physiques ou des homologues, l'appliance NetScaler utilise les adresses spécifiées dans le profil comme adresse IP source.

- Pour obtenir des instructions sur la création d'un profil réseau, reportez-vous à la section Création d'un profil réseau.
- Pour obtenir des instructions sur la liaison d'un profil réseau à une entité NetScaler, consultez Liaison d'un profil réseau à une entité NetScaler.

Créer un jeu d'adresses IP

Un ensemble d'adresses IP est un ensemble d'adresses IP configurées sur l'appliance NetScaler sous forme d'adresses IP de sous-réseau (SNIP) ou d'adresses IP virtuelles (VIP). Un ensemble d'adresses IP est identifié avec un nom significatif qui aide à identifier l'utilisation des adresses IP qu'il contient. Pour créer un ensemble d'adresses IP, ajoutez-en un et liez-y les adresses IP appartenant à NetScaler. Les adresses SNIP et VIP peuvent être présentes dans le même ensemble d'adresses IP.

Pour créer un ensemble d'adresses IP à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes :

```
add ipset <name>

bind ipset <name> <IPAddress>
<!--NeedCopy-->
```


Ou

```
bind ipset <name> <IPAddress>

show ipset [<name>]
<!--NeedCopy-->
```

La commande précédente affiche les noms de tous les ensembles d'adresses IP de l'appliance si vous ne transmettez aucun nom. Il affiche les adresses IP liées au jeu d'adresses IP spécifié si vous transmettez un nom.

Exemples

```
1.
> add ipset skpnwipset
 Done
> bind ipset skpnwipset 21.21.20.1
 Done

2.
 > add ipset testnwipset
 Done
> bind ipset testnwipset 21.21.21.[21-25]
 IPAddress "21.21.21.21" bound
 IPAddress "21.21.21.22" bound
 IPAddress "21.21.21.23" bound
 IPAddress "21.21.21.24" bound
 IPAddress "21.21.21.25" bound
 Done

3.
 > bind ipset skpipset 11.11.11.101
 ERROR: Invalid IP address
[This IP address could not be added because this is not an IP address
   owned by the NetScaler appliance]
 > add ns ip 11.11.11.101 255.255.255.0 -type SNIP
 ip "11.11.11.101" added
 Done
 > bind ipset skpipset 11.11.11.101
 IPAddress "11.11.11.101" bound
 Done
4.
> sh ipset
1) Name: ipset-1
```



```
2) Name: ipset-2
3) Name: ipset-3
4) Name: skpnewipset
 Done

5.
> sh ipset skpnewipset
IP:21.21.21.21
IP:21.21.21.22
IP:21.21.21.23
IP:21.21.21.24
IP:21.21.21.25
 Done
<!--NeedCopy-->
```

Pour créer un ensemble d'adresses IP à l'aide de l'interface graphique

Accédez à **Système > Réseau > Jeux d'adresses IP**et créez un ensemble d'adresses IP.

Créer un profil net

Un profil réseau (profil réseau) comprend une ou plusieurs adresses SNIP ou VIP de l'appliance NetScaler.

Pour créer un profil réseau à l'aide de la CLI

À l'invite de commande, tapez :

```
add netprofile <name> [-srcIp <srcIpVal>]
<!--NeedCopy-->
```

Si le srcIpVal n'est pas fourni dans cette commande, il peut être fourni ultérieurement à l'aide de la commande `set netprofile`.

Exemples

```
add netprofile skpnetprofile1 -srcIp 21.21.20.1
Done

add netprofile baksnp -srcIp bakipset
Done

```



```
set netprofile yahnp -srcIp 12.12.23.1
Done

set netprofile citkbnp -srcIp citkbipset
Done
<!--NeedCopy-->
```

Lier un profil réseau à une entité NetScaler

Un profil réseau peut être lié à un serveur virtuel d'équilibrage de charge, un service, un groupe de services ou un moniteur.

Remarque : Vous pouvez lier un profil réseau au moment de la création d'une entité NetScaler ou le lier à une entité existante.

Pour lier un profil réseau à un serveur à l'aide de l'interface de ligne de commande

Vous pouvez lier un profil réseau à des serveurs virtuels d'équilibrage de charge et à des serveurs virtuels de commutation de contenu. Spécifiez le serveur virtuel approprié.

À l'invite de commande, tapez :

```
set lb vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Ou

```
set cs vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Exemples

```
set lb vserver skpnwvs1 -netProfile gntnp
 Done
set cs vserver mmdcsv -netProfile mmdnp
 Done
<!--NeedCopy-->
```

Pour lier un profil réseau à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez le serveur virtuel.

2. Dans Paramètres avancés, cliquez sur **Profils**et définissez un profil réseau.

Pour lier un profil réseau à un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Exemple

```
set service brnssvc1 -netProfile brnsnp
 Done
<!--NeedCopy-->
```

Pour lier un profil réseau à un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, cliquez sur **Profils**et définissez un profil réseau.

Pour lier un profil réseau à un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set servicegroup <serviceGroupName> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Exemple

```
set servicegroup ndhsvcgrp -netProfile ndhnp
 Done
<!--NeedCopy-->
```

Pour lier un profil réseau à un groupe de services à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services**et ouvrez un groupe de services.
2. Dans Paramètres avancés, cliquez sur **Profils**et définissez un profil réseau.

Pour lier un profil réseau à un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set monitor <monitor_name> -netProfile <net_profile_name>
```

Exemple

```
set monitor brnsecvmon1 -netProfile brnsmonnp
 Done
<!--NeedCopy-->
```

Pour lier un profil réseau à un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Ouvrez un moniteur et définissez le profil net.

Définir une valeur de délai d'expiration pour les connexions client inactives

May 5, 2023

Vous pouvez configurer un serveur virtuel pour mettre fin à toute connexion client inactive après l'expiration d'un délai configuré (en secondes). Lorsque vous configurez ce paramètre, l'appliance NetScaler attend le temps que vous spécifiez et, si le client est inactif après ce délai, elle ferme la connexion client. Par défaut, la valeur du délai d'inactivité du client est définie sur 180 secondes.

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name> -cltTimeout <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -cltTimeout 100
<!--NeedCopy-->
```


Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans **Paramètres avancés,** cliquez sur **Paramètres du trafic**et définissez la valeur du délai d'inactivité du client en secondes.

Gérer les connexions RTSP

May 5, 2023

L'appliance NetScaler peut utiliser l'une des deux topologies (mode NAT-on ou mode NAT-off) pour équilibrer la charge des serveurs RTSP. En mode NAT-on, la traduction d'adresses réseau (NAT) est activée et configurée sur l'appliance. Les requêtes et les réponses RTSP transitent toutes deux par l'appliance. Vous devez donc configurer l'appliance pour effectuer la traduction d'adresses réseau (NAT) afin d'identifier la connexion de données.

Pour plus d'informations sur l'activation et la configuration de NAT, consultez Addressage IP.

En mode NAT désactivé, NAT n'est pas activé et configuré. L'appliance reçoit des demandes RTSP du client et les achemine vers le service qu'elle sélectionne à l'aide de la méthode d'équilibrage de charge configurée. Les serveurs RTSP à charge équilibrée envoient leurs réponses directement au client, en contournant l'appliance. Vous devez donc configurer l'appliance pour qu'elle utilise le mode DSR (Direct Server Return) et attribuer des noms de domaine complets accessibles au public dans DNS à vos serveurs RTSP à charge équilibrée.

Pour plus d'informations sur l'activation et la configuration du mode DSR, reportez-vous à la section Configuration de l'équilibrage de charge en mode de retour direct du serveur. Pour plus d'informations sur la configuration du DNS, voir Système de noms de domaine. Dans les deux cas, lorsque vous configurez l'équilibrage de charge RTSP, vous devez également configurer RTSPnat pour qu'il corresponde à la topologie de votre configuration d'équilibrage de charge.

Pour configurer le NAT RTSP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name>  -RTSPNAT <ValueOfRTSPNAT>
<!--NeedCopy-->
```

Exemple :


```
set lb vserver vserver-LB-1  -RTSPNAT ON
<!--NeedCopy-->
```

Pour configurer RTSP NAT à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel de type RTSP.
2. Dans Paramètres avancés, cliquez sur **Paramètres de trafic**, puis sélectionnez **Natting RTSP**.

Gérer le trafic client en fonction du taux de trafic

May 5, 2023

Vous pouvez surveiller le débit de trafic qui traverse les serveurs virtuels d'équilibrage de charge et contrôler le comportement de l'appliance NetScaler en fonction du débit de trafic. Par exemple :

- Régulez le flux de trafic s'il est trop élevé.
- Les informations de cache sont basées sur le débit de trafic.
- Si le taux de trafic est trop élevé, redirigez le trafic excédentaire vers un autre serveur virtuel d'équilibrage de charge.
- Appliquez une surveillance basée sur les taux aux demandes HTTP et DNS (Domain Name System).

Pour plus d'informations sur les stratégies basées sur les taux, voir Limitation de taux.

Identifier une connexion avec les paramètres de couche 2

May 5, 2023

Généralement, pour identifier une connexion, l'appliance NetScaler utilise les quatre tuples suivants : adresse IP du client, port client, adresse IP de destination et port de destination. Lorsque vous activez l'option Connexion L2, les paramètres de couche 2 de la connexion (numéro de canal, adresse MAC et ID VLAN) sont utilisés en plus du 4-tuple normal.

L'activation du paramètre L2Conn pour un serveur virtuel d'équilibrage de charge permet à plusieurs connexions TCP et non TCP avec le même tuple à 4 (<source IP>:::<source port><destination IP> :<destination port>) de coexister sur l'appliance NetScaler. L'appliance utilise à la fois les paramètres du tuple 4 et de la couche 2 pour identifier les connexions TCP et non TCP.

Vous pouvez activer l'option L2Conn dans les scénarios suivants :

- Plusieurs VLAN sont configurés sur l'appliance NetScaler et un pare-feu est configuré pour chaque VLAN.
- Vous souhaitez que le trafic provenant des serveurs d'un VLAN et destiné à un serveur virtuel d'un autre VLAN passe par les pare-feux configurés pour les deux VLAN.

Par conséquent, lorsqu'une appliance nCore NetScaler sur laquelle le paramètre L2conn est défini pour un ou plusieurs serveurs virtuels d'équilibrage de charge est rétrogradée vers une version classique ou vers une version nCore qui ne prend pas en charge le paramètre L2conn, les configurations d'équilibrage de charge qui utilisent le paramètre L2Conn deviennent inefficaces.

Pour configurer l'option de connexion L2 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name> <serviceType> <IPAddress>@ <port> -l2Conn ON
<!--NeedCopy-->
```

Exemple

```
 add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -l2Conn ON
<!--NeedCopy-->
```

Pour configurer l'option de connexion L2 à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez Paramètres de trafic, puis Paramètres de couche 2.

Configurer l'option Préférer le routage direct

May 5, 2023

Sur un serveur virtuel d'équilibrage de charge générique, si vous configurez explicitement un itinéraire vers une destination, par défaut, l'appliance NetScaler transfère le trafic en fonction de l'itinéraire configuré. Si vous souhaitez que l'appliance ne recherche pas l'itinéraire configuré, vous pouvez définir l'option Préférer l'itinéraire direct sur NON.

Si un appareil est directement connecté à une appliance NetScaler, l'appliance transmet directement le trafic à l'appareil. Par exemple, si la destination d'un paquet est un pare-feu, le paquet n'a pas besoin d'être routé via un autre pare-feu. Cependant, il se peut que vous souhaitiez parfois que le

trafic passe par le pare-feu même si l'appareil y est directement connecté. Dans de tels cas, vous pouvez définir l'option Préférer un itinéraire direct sur NO.

Remarque : Le paramètre PreferDirectRoute s'applique à tous les serveurs virtuels génériques de l'appliance NetScaler.

Pour définir l'option Préférer l'itinéraire direct à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb parameter -preferDirectRoute (YES | NO)
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -preferDirectRoute YES
<!--NeedCopy-->
```

Pour définir l'option Préférer l'itinéraire direct à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**.
2. Sélectionnez Préférer un itinéraire direct.

Utiliser un port source provenant d'une plage de ports spécifiée pour la communication back-end

May 5, 2023

Par défaut, pour les configurations pour lesquelles l'option USIP est désactivée ou pour lesquelles les options USIP et utilisation du port proxy sont activées, l'appliance NetScaler communique avec les serveurs à partir d'un port source aléatoire (supérieur à 1024).

L'appliance prend en charge l'utilisation d'un port source à partir d'une plage de ports spécifiée pour communiquer avec les serveurs. L'un des cas d'utilisation de cette fonctionnalité concerne les serveurs configurés pour identifier le trafic reçu appartenant à un ensemble spécifique basé sur le port source à des fins de journalisation et de surveillance. Par exemple, identifier le trafic interne et externe à des fins de journalisation.

La configuration de l'appliance NetScaler pour qu'elle utilise un port source d'une plage de ports pour communiquer avec les serveurs comprend les tâches suivantes :

- **Créez un profil réseau et définissez le paramètre de plage de ports source**. Un paramètre de plage de ports source spécifie une ou plusieurs plages de ports. L'appliance sélectionne de manière aléatoire l'un des ports libres parmi les plages de ports spécifiées et l'utilise comme port source pour chaque connexion aux serveurs.
- **Liez le profil réseau à des serveurs virtuels, des services ou des groupes de services d'équilibrage de charge** : Un profil réseau avec un paramètre de plage de ports source peut être lié à un serveur virtuel, un service ou un groupe de services d'une configuration d'équilibrage de charge. Pour une connexion à un serveur virtuel, l'appliance sélectionne aléatoirement l'un des ports libres parmi les plages de ports spécifiées d'un profil réseau et utilise ce port comme port source pour se connecter à l'un des serveurs liés.

Pour spécifier une ou plusieurs plages de ports source à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind netProfile <name> (-srcPortRange <int[-int]> ...)

show netprofile <name>
<!--NeedCopy-->
```

Pour spécifier une ou plusieurs plages de ports source à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Profils réseau**.
2. Définissez le paramètre **Source Port Range** lors de l'ajout ou de la modification de NetProfiles.

Exemple de configuration

Dans l'exemple de configuration suivant, le profil réseau PARTIAL-NAT-1 possède des paramètres NAT partiels et est lié au serveur virtuel d'équilibrage de charge LBVS-1, de type ANY. Pour les paquets reçus sur LBVS-1 à partir de 192.0.0.0/8, l'appliance NetScaler traduit le dernier octet de l'adresse IP source du paquet en 100. Par exemple, s'il s'agit d'un paquet dont l'adresse IP source est 192.0.2.30 reçu sur LBVS-1, l'appliance NetScaler traduit l'adresse IP source en 100.0.2.30 avant de l'envoyer à l'un des serveurs liés.

```
```
> add netprofile CUSTOM-SRCPORT-NP-1
Done
> bind netprofile CUSTOM-SRCPRT-NP-1 - srcportrange 2000-3000

Done
```

 
```

```
> bind netprofile CUSTOM-SRCPRT-NP-1  - srcportrange 5000-6000

Done
> add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1

Done
<!--NeedCopy--> ```
```

Configurer la persistance IP source pour les communications back-end

May 5, 2023

Par défaut, pour une configuration d'équilibrage de charge avec l'option USIP désactivée et un profil réseau lié à un serveur virtuel ou à des services ou à des groupes de services, l'appliance NetScaler utilise l'algorithme round robin pour sélectionner une adresse IP dans le profil réseau pour communiquer avec les serveurs. En raison de cette méthode de sélection, l'adresse IP sélectionnée peut être différente pour différentes sessions d'un client spécifique.

Certaines situations nécessitent que l'appliance NetScaler achemine tout le trafic d'un client spécifique à partir de la même adresse IP lors de l'envoi du trafic vers des serveurs. Les serveurs peuvent alors, par exemple, identifier le trafic appartenant à un ensemble spécifique à des fins de journalisation et de surveillance.

L'option de persistance de l'adresse IP source d'un profil réseau permet à l'appliance NetScaler d'utiliser la même adresse, spécifiée dans le profil réseau, pour communiquer avec les serveurs au sujet de toutes les sessions initiées depuis un client spécifique vers un serveur virtuel.

Pour activer la persistance de l'adresse IP source dans un profil réseau à l'aide de l'interface de ligne de commande

Pour activer la persistance de l'adresse IP source lors de l'ajout d'un profil réseau, à l'invite de commande, tapez :

```
add netProfile <name> -srcippersistency ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Pour activer la persistance de l'adresse IP source dans un profil réseau existant, à l'invite de commande, tapez :


```
set netProfile <name> -srcippersistency ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Pour activer la persistance de l'adresse IP source dans un profil réseau à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Profils réseau**.
2. Sélectionnez **Persistency de l'adresse IP source** lors de l'ajout ou de la modification d'un profil réseau.

Exemple

Dans l'exemple de configuration suivant, le profil net NETPROFILE-IPPRSTNCY-1 a l'option de persistance IP source activée et est lié à l'équilibrage de charge du serveur virtuel LBVS-1.

L'appliance NetScaler utilise toujours la même adresse IP (dans cet exemple, 192.0.2.11) pour communiquer avec les serveurs liés à LBVS-1, pour toutes les sessions initiées depuis un client spécifique vers le serveur virtuel.

```
```
> add ipset IPSET-1

Done
> bind ipset IPSET-1 192.0.2.[11-15]
 IPAddress "192.0.2.11" bound
 IPAddress "192.0.2.12" bound
 IPAddress "192.0.2.13" bound
 IPAddress "192.0.2.14" bound
 IPAddress "192.0.2.15" bound
 Done
> add netprofile NETPROFILE-IPPRSTNCY-1 -srcIp IPSET-1 -
    srcippersistency ENABLED

Done
> set lb vserver LBVS-1 -netprofile NETPROFILE-IPPRSTNCY-1

 Done
<!--NeedCopy--> ```
```

 
```

Utiliser les adresses locales de liaison IPv6 côté serveur d'une configuration d'équilibrage de charge

May 5, 2023

L'adresse locale de liaison IPv6 est prise en charge pour les services, les groupes de services et les serveurs d'une configuration d'équilibrage de charge. Vous pouvez spécifier une adresse IPv6 locale de liaison avec l'ID VLAN associé dans les configurations de services, de groupes de services et de serveurs. L'appliance NetScaler utilise l'adresse SNIP6 locale du lien provenant du même VLAN que celui spécifié dans les configurations des services, des groupes de services et des serveurs pour communiquer avec elles.

Une adresse IPv6 locale de liaison et l'ID VLAN associé sont spécifiés dans le format suivant dans les configurations des services, des groupes de services et des serveurs :`<IPv6_Addrs>%<vlan_id>`

Par exemple, `fe80:123:4567::a%2048:`, `fe80:123:4567::a` est l'adresse locale du lien ET 2048 est l'ID VLAN.

```
> add service SERVICE-1 fe80:123:4567::a%2048 HTTP 80

Done
> bind servicegroup SERVICE-GROUP-1 fe80::1%24 80

Done
> add server SERVER-1 fe80:b:c:d::e:f:a/64%1028

Done
```

Paramètres avancés d'équilibrage de charge

January 21, 2021

Outre la configuration des serveurs virtuels, vous pouvez configurer des paramètres avancés pour les services.

Pour configurer des paramètres avancés d'équilibrage de charge, consultez les sections suivantes :

- Augmenter progressivement la charge sur un nouveau service avec un démarrage lent au niveau du serveur virtuel
- Option sans moniteur pour les services
- Protéger les applications sur les serveurs protégés contre les surtensions de trafic
- Activer le nettoyage des connexions de serveur virtuel et de service

- Arrêt gracieux des services
- Activer ou désactiver la session de persistance sur les services TROFS
- Demandes directes vers une page Web personnalisée
- Activer l'accès aux services en cas de panne
- Activer la mise en mémoire tampon TCP des réponses
- Activer la compression
- Maintenir la connexion client pour plusieurs demandes client
- Insérer l'adresse IP du client dans l'en-tête de la requête
- Récupérer les détails de localisation à partir de l'adresse IP de l'utilisateur à l'aide de la base de données de géolocalisation
- Utiliser l'adresse IP source du client lors de la connexion au serveur
- Configurer le port source pour les connexions côté serveur
- Définir une limite sur le nombre de connexions client
- Définir une limite sur le nombre de requêtes par connexion au serveur
- Définir une valeur de seuil pour les moniteurs liés à un service
- Définir une valeur de délai d'attente pour les connexions client inactives
- Définir une valeur de délai d'attente pour les connexions au serveur inactif
- Définir une limite sur l'utilisation de la bande passante par les clients
- Rediriger les requêtes client vers un cache
- Conserver l'identificateur VLAN pour la transparence VLAN
- Configurer la transition automatique de l'état en fonction du pourcentage d'intégrité des services liés

Augmenter progressivement la charge sur un nouveau service avec un démarrage lent au niveau du serveur virtuel

May 5, 2023

Vous pouvez configurer l'appliance NetScaler pour augmenter progressivement la charge d'un service (le nombre de demandes que le service reçoit par seconde) immédiatement après que le service est ajouté à une configuration d'équilibrage de charge ou que son état passe de DOWN à UP (dans ce document, le terme « nouveau service » est utilisé dans les deux cas). Vous pouvez augmenter la charge manuellement avec les valeurs de charge et les intervalles de votre choix (démarrage lent manuel) ou configurer l'appliance pour augmenter la charge à un intervalle spécifié (démarrage lent automatisé) jusqu'à ce que le service reçoive autant de demandes que les autres services de la configuration. Pendant la période de mise en service du nouveau service, l'appliance utilise la méthode d'équilibrage de charge configurée.

Cette fonctionnalité n'est pas disponible dans le monde entier. Il doit être configuré pour chaque

serveur virtuel. La fonctionnalité n'est disponible que pour les serveurs virtuels qui utilisent l'une des méthodes d'équilibrage de charge suivantes :

- Robin à la ronde
- Moins de connexion
- Temps de réponse le plus court
- Bande passante minimale
- Moins de paquets
- LRTM (méthode du temps de réponse le plus court)
- Charge personnalisée

Pour cette fonctionnalité, vous devez définir les paramètres suivants :

- Le nouveau taux de demandes de service, qui est le montant permettant d'augmenter le nombre ou le pourcentage de demandes envoyées à un nouveau service chaque fois que le taux est incrémenté. C'est-à-dire que vous spécifiez la taille de l'incrément en termes de nombre de demandes par seconde ou de pourcentage de la charge supportée, à ce moment-là, par les services existants. Si cette valeur est définie sur 0 (zéro), le démarrage lent n'est pas effectué sur les nouveaux services.

  Remarque : Dans un mode de démarrage lent automatisé, l'incrément final est inférieur à la valeur spécifiée si la valeur spécifiée entraînerait une charge plus lourde sur le nouveau service que sur les autres services.

- Intervalle d'incrément, en secondes. Si cette valeur est définie sur 0 (zéro), la charge n'est pas incrémentée automatiquement. Vous devez l'incrémenter manuellement.

Avec un démarrage lent automatisé, un service est retiré de la phase de démarrage lent lorsque l'une des conditions suivantes s'applique :

- Le tarif réel des demandes est inférieur au nouveau tarif des demandes de service.
- Le service ne reçoit pas de trafic pendant trois intervalles d'incrémentation successifs.
- Le taux de demandes a été augmenté 200 fois.
- Le pourcentage de trafic que le nouveau service doit recevoir est supérieur ou égal à 100.

Avec le démarrage lent manuel, le service reste en phase de démarrage lent jusqu'à ce que vous le sortiez de cette phase.

Démarrage lent manuel

Si vous souhaitez augmenter manuellement la charge d'un nouveau service, ne spécifiez pas d'intervalle d'incrémentation pour le serveur virtuel d'équilibrage de charge. Spécifiez uniquement le nouveau taux de demande de service et les unités. Aucun intervalle n'étant spécifié, l'appliance n'incrémente pas la charge périodiquement. Il maintient la charge du nouveau service à la valeur spécifiée par la combinaison du nouveau taux de demande de service et des unités jusqu'à ce que

vous modifiiez manuellement l'un des paramètres. Par exemple, si vous définissez le nouveau taux de demandes de service et les paramètres d'unité sur 25 et « par seconde », respectivement, l'appliance maintient la charge du nouveau service à 25 demandes par seconde jusqu'à ce que vous modifiiez l'un ou l'autre de ces paramètres. Lorsque vous souhaitez que le nouveau service quitte le mode de démarrage lent et reçoive autant de demandes que les services existants, définissez le nouveau paramètre de taux de demandes de service sur 0.

Par exemple, supposons que vous utilisiez un serveur virtuel pour équilibrer la charge de deux services, Service1 et Service2, en mode round robin. Supposons également que le serveur virtuel reçoit 240 demandes par seconde et qu'il répartit la charge de manière uniforme entre les services. Lorsqu'un nouveau service, Service3, est ajouté à la configuration, vous pouvez augmenter sa charge manuellement en utilisant des valeurs de 10, 20 et 40 demandes par seconde avant de lui envoyer la totalité de la charge. Le tableau suivant indique les valeurs auxquelles vous avez défini les trois paramètres.

Tableau 1. Valeurs des paramètres

Paramètre	Valeur
Intervalle en secondes	0
Nouveau taux de demande de service	10, 20, 40 et 0, aux intervalles que vous choisissez
Unités correspondant au nouveau taux de demande de service	Demandes par seconde

Lorsque vous définissez le nouveau paramètre de taux de demande de service sur 0, Service3 n'est plus considéré comme un nouveau service et reçoit sa part complète de la charge.

Supposons que vous ajoutiez un autre service, Service4, pendant la période de montée en puissance de Service3. Dans cet exemple, Service4 est ajouté lorsque le nouveau paramètre de taux de demande de service est défini sur 40. Par conséquent, Service4 commence à recevoir 40 demandes par seconde.

Le tableau suivant montre la répartition de la charge sur les services au cours de la période décrite dans cet exemple.

Tableau 2 Répartition de la charge sur les services lors de l'augmentation manuelle de la charge

	nouveau taux de demande de service = 10 req/sec (Service3added)	nouveau taux de demande de service = 20 req/sec	nouveau taux de demande de service = 40 req/sec (Service4added)	taux de nouvelles demandes de service = 0 req/sec (les nouveaux services quittent le mode de démarrage lent)
Service1	115	110	80	60
Service2	115	110	80	60
Service3	10	20	40	60
Service4	-	-	40	60
Nombre total de requêtes par seconde (charge sur le serveur virtuel)	240	240	240	240

Démarrage lent automatique

Si vous souhaitez que l'appliance augmente automatiquement la charge sur un nouveau service à intervalles spécifiés jusqu'à ce que le service puisse être considéré comme capable de gérer sa part entière de la charge, définissez le nouveau paramètre de débit de demande de service, le paramètre unités et l'intervalle d'incrémentation. Lorsque tous les paramètres sont définis sur des valeurs autres que 0, l'appliance incrémente la charge sur un nouveau service en fonction de la valeur du nouveau taux de demande de service, à l'intervalle spécifié, jusqu'à ce que le service reçoive toute sa part de la charge.

Par exemple, supposons que quatre services, Service1, Service2, Service3 et Service4, sont liés à un serveur virtuel d'équilibrage de charge, vserver1. Supposons également que vserver1 reçoit 100 demandes par seconde et qu'il répartit la charge de manière uniforme entre les services (25 demandes par seconde et par service). Lorsque vous ajoutez un cinquième service, Service5, à la configuration, vous souhaiterez peut-être que l'appliance envoie au nouveau service 4 demandes par seconde pendant les 10 premières secondes, 8 demandes par seconde pendant les 10 secondes suivantes, et ainsi de suite, jusqu'à ce qu'elle reçoive 20 demandes par seconde. Pour cette exigence, le tableau suivant indique les valeurs sur lesquelles vous définissez les trois paramètres :

Tableau 3. Valeurs des paramètres

Paramètre	**Valeur**
Intervalle en secondes	10
Valeur d'incrémentation	4
Unités correspondant au nouveau taux de demande de service	Demandes par seconde

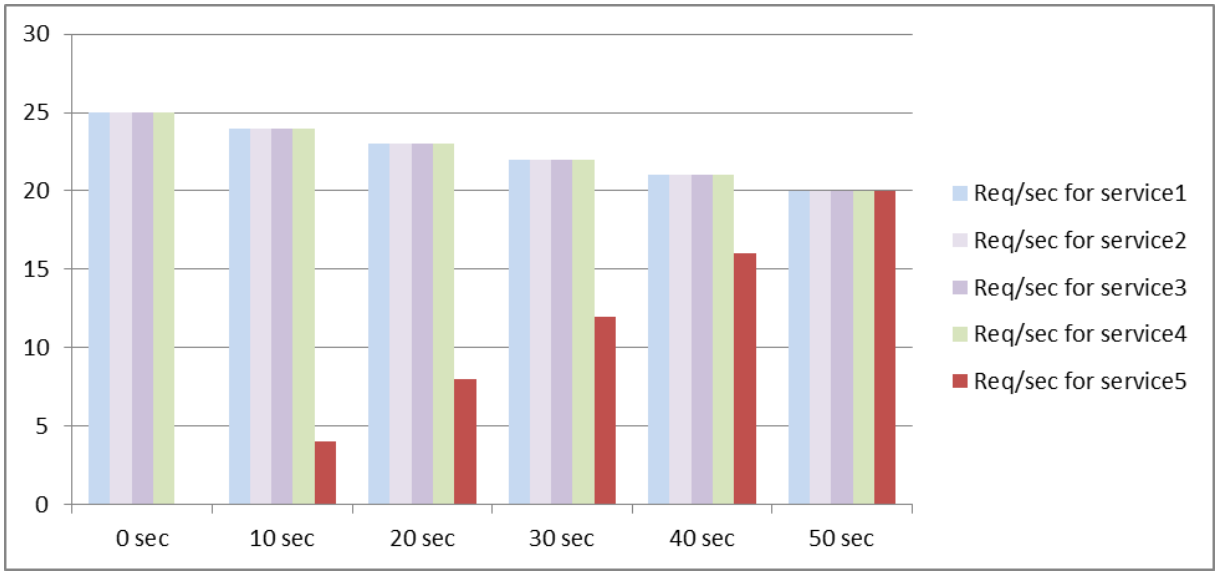
Avec cette configuration, le nouveau service commence à recevoir autant de demandes que les services existants 50 secondes après son ajout ou son passage de DOWN à UP. Au cours de chaque intervalle de cette période, l'appliance distribue aux serveurs existants l'excédent de demandes qui auraient été envoyées au nouveau service en l'absence d'incréments progressifs. Par exemple, en l'absence d'incréments progressifs, chaque service, y compris Service5, aurait reçu 20 demandes par seconde. Par incréments progressifs, pendant les 10 premières secondes, lorsque Service5 ne reçoit que 4 demandes par seconde, l'appliance distribue l'excédent de 16 demandes par seconde aux services existants, ce qui donne le modèle de distribution illustré dans le tableau et la figure suivants sur une période de 50 secondes. Après la période de 50 secondes, Service5 n'est plus considéré comme un nouveau service et reçoit sa part normale de trafic.

Tableau 4. Modèle de distribution des charges sur tous les services pendant la période de 50 secondes immédiatement après l'ajout du Service5

	0 seconde	10 secondes	20 secondes	30 secondes	40 secondes	50 secondes
Req/sec pour Service1	25	24	23	22	21	20
Req/sec pour Service2	25	24	23	22	21	20
Req/sec pour Service3	25	24	23	22	21	20
Req/sec pour Service4	25	24	23	22	21	20
Req/sec pour Service5	0	4	8	12	16	20

	0 seconde	10 secondes	20 secondes	30 secondes	40 secondes	50 secondes
Nombre total de requêtes par seconde (charge sur le serveur virtuel)	100	100	100	100	100	100

Figure 1. Graphique du modèle de répartition de charge sur tous les services pour la période de 50 secondes immédiatement après l'ajout du service5



Une autre exigence pourrait consister à ce que l'appliance envoie le Service5 25 % de la charge sur les services existants dans les 5 premières secondes, 50 % dans les 5 secondes suivantes, etc., jusqu'à ce qu'elle reçoive 20 demandes par seconde. Pour cette exigence, le tableau suivant indique les valeurs auxquelles vous avez défini les trois paramètres.

Tableau 5. Valeurs des paramètres

Paramètre	Valeur
Intervalle en secondes	5
Valeur d'incrémentation	25

Paramètre	Valeur
Unités correspondant au nouveau taux de demande de service	Pourcentage

Avec cette configuration, le service commence à recevoir autant de demandes que les services existants 20 secondes après son ajout ou le passage de son état de DOWN à UP. La répartition du trafic pendant la période de montée en puissance du nouveau service est identique à celle décrite précédemment, où l'unité utilisée pour les incréments était le nombre de « demandes par seconde ».

Définir les paramètres de démarrage lent

Vous définissez les paramètres de démarrage lent à l'aide de la commande `set lb vserver` ou de la `add lb vserver` commande. La commande suivante permet de définir des paramètres de démarrage lent lors de l'ajout d'un serveur virtuel.

Pour configurer des incréments de charge par étapes pour un nouveau service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer des incréments progressifs de la charge d'un service et vérifier la configuration :

```
add lb vserver <name> <serviceType> <IPAddress> <port> [-
   newServiceRequest <positive_integer>] [<newServiceRequestUnit>] [-
   newServiceRequestIncrementInterval <positive_integer>]

show lb vserver <name>
<!--NeedCopy-->
```

Exemple

```
set lb vserver BR_LB -newServiceRequest 5 PER_SECOND -
   newServiceRequestIncrementInterval 10
Done

show lb vserver BR_LB
BR_LB (192.0.2.33:80) - HTTP Type: ADDRESS
State: UP
...
...
New Service Startup Request Rate: 5 PER_SECOND, Increment Interval: 10
```



```
...
...
Done
<!--NeedCopy-->
```

Pour configurer des incréments de charge par étapes pour un nouveau service à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez Méthode et définissez les paramètres de démarrage lent suivants :
   - Taux de demandes de démarrage de nouveaux services.
   - Nouvelle unité de demande de service.
   - Intervalle d'incrémentation.

L'option sans surveillance pour les services

May 5, 2023

Si vous utilisez un système externe pour effectuer des contrôles de santé sur les services et que vous ne souhaitez pas que l'appliance NetScaler surveille l'état d'un service, vous pouvez définir l'option d'absence de surveillance pour le service. Dans ce cas, l'appliance n'envoie pas de sondes pour vérifier l'état du service, mais indique que le service est actif. Même si le service tombe en panne, l'appliance continue d'envoyer le trafic du client vers le service conformément à la méthode d'équilibrage de charge.

Le moniteur peut être à l'état ACTIVÉ ou DÉSACTIVÉ lorsque vous définissez l'option sans surveillance, et lorsque vous supprimez l'option sans surveillance, l'état antérieur du moniteur est rétabli.

Vous pouvez définir l'option sans surveillance pour un service lors de sa création. Vous pouvez également définir l'option d'absence de surveillance sur un service existant.

Les conséquences de la définition de l'option sans moniteur sont les suivantes :

- Si un service pour lequel vous avez activé l'option d'absence de surveillance tombe en panne, l'appliance continue d'afficher le service comme étant actif et continue de transférer le trafic vers ce service. Une connexion permanente au service peut aggraver la situation. Dans ce cas, ou si de nombreux services affichés comme UP sont réellement DOWN, le système peut échouer. Pour éviter une telle situation, lorsque le mécanisme externe qui surveille les services signale qu'un service est hors service, supprimez le service de la configuration NetScaler.

- Si vous configurez l'option sans moniteur sur un service, vous ne pouvez pas configurer l'équilibrage de charge en mode DSR (Direct Server Return). Pour un service existant, si vous définissez l'option sans surveillance, vous ne pouvez pas configurer le mode DSR pour le service.

Pour définir l'option no-monitor pour un nouveau service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service avec l'option de surveillance de l'état et vérifiez la configuration :

```
add service <serviceName> <IP | serverName> <serviceType> <port> -
   healthMonitor (YES|NO)
<!--NeedCopy-->
```

Exemple :

```
add service nomonsrvc 10.102.21.21 http 80 -healthMonitor no
Done

show service nomonsrvc
nomonsrvc (10.102.21.21:80) - HTTP
State: UP
Last state change was at Mon Nov 15 22:41:29 2010
Time since last state change: 0 days, 00:00:00.970
Server Name: 10.102.21.21
 Server ID : 0 Monitor Threshold : 0
...
Access Down Service: NO
...
Down state flush: ENABLED
Health monitoring: OFF

1 bound monitor:
1) Monitor Name: tcp-default
State: UNKNOWN Weight: 1
Probes: 3 Failed [Total: 3 Current: 3]
Last response: Probe skipped - Health monitoring is turned off.
Response Time: N/A
Done
<!--NeedCopy-->
```


Pour définir l'option sans surveillance pour un service existant à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour définir l'option du moniteur de santé :

```
set service <name> -healthMonitor (YES|NO)
<!--NeedCopy-->
```

Exemple :

```
By default, the state of a service and the state of the corresponding
   monitor are UP.
 >show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP


1) Monitor Name: http-ecv
 State: UP Weight: 1
Probes: 99992 Failed [Total: 0 Current: 0]
Last response: Success - Pattern found in response.
Response Time: 3.76 millisec
Done

When the no-monitor option is set on a service, the state of the
   monitor changes to UNKNOWN.
set service LB-SVC1 -healthMonitor NO
Done

show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
Last state change was at Fri Dec 10 10:17:37 2010.
Time since last state change: 5 days, 18:55:48.710
Health monitoring: OFF

1) Monitor Name: http-ecv
   State: UNKNOWN Weight: 1
         Probes: 100028 Failed [Total: 0 Current: 0]
   Last response: Probe skipped - Health monitoring is turned off.
     Response Time: 0.0 millisec
  Done
When the no-monitor option is removed, the earlier state of the monitor
    is resumed.
> set service LB-SVC1 -healthMonitor YES
```



```
Done
>show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
Last state change was at Fri Dec 10 10:17:37 2010
Time since last state change: 5 days, 18:57:47.880
1) Monitor Name: http-ecv
   State: UP Weight: 1
   Probes: 100029 Failed [Total: 0 Current: 0]
   Last response: Success - Pattern found in response.
   Response Time: 5.690 millisec
   Done
<!--NeedCopy-->
```

Pour définir l'option sans surveillance pour un service à l'aide de l'interface graphique

1. Accédez à Traffic Management > Load Balancing > Services.
2. Ouvrez le service et désactivez la case Surveillance de l'état de santé.

Protégez les applications sur les serveurs protégés contre les pics de trafic

May 5, 2023

L'appliance NetScaler fournit l'option de protection contre les surtensions pour maintenir la capacité d'un serveur ou d'un cache. L'appliance régule le flux des demandes des clients vers les serveurs et contrôle le nombre de clients pouvant accéder simultanément aux serveurs. L'appliance bloque toutes les surtensions transmises au serveur, empêchant ainsi la surcharge du serveur.

Pour que la protection contre les surtensions fonctionne correctement, vous devez l'activer globalement. Pour plus d'informations sur la protection contre les surtensions, voir Protection contre les surtensions.

Pour définir la protection contre les surtensions sur le service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -sp <Value>
<!--NeedCopy-->
```


Exemple :

```
set service Service-HTTP-1 -sp ON
<!--NeedCopy-->
```

Pour configurer la protection contre les surtensions sur le service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez une source.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Protection contre les surtensions**.

Activer le nettoyage des connexions de serveur virtuel et de service

May 5, 2023

L'état d'un serveur virtuel dépend de l'état des services qui y sont liés. L'état de chaque service dépend des réponses des serveurs à charge équilibrée aux sondes ou aux contrôles de santé envoyés par les moniteurs liés à ce service. Parfois, les serveurs à charge équilibrée ne répondent pas. Si un serveur est lent ou occupé, le temps imparti aux sondes de surveillance peut être dépassé. Si les sondes de surveillance répétées ne sont pas répondues dans le délai d'expiration configuré, le service est marqué DOWN. Si un service ou un serveur virtuel est marqué BAS, les connexions côté serveur et client doivent être vides. La fin des connexions existantes libère des ressources et, dans certains cas, accélère la récupération des configurations d'équilibrage de charge surchargées.

Sous certaines conditions, vous pouvez configurer le paramètre **DownStateFlush** pour mettre fin immédiatement aux connexions existantes lorsqu'un service ou un serveur virtuel est marqué « DOWN ». N'activez pas le paramètre DownStateFlush sur les serveurs d'applications qui doivent terminer leurs transactions. Vous pouvez activer ce paramètre sur les serveurs Web dont les connexions peuvent être interrompues en toute sécurité lorsqu'ils sont marqués comme DOWN.

Le tableau suivant résume l'effet de ce paramètre sur un exemple de configuration consistant en un serveur virtuel, vServer-LB-1, auquel est lié un service, Service-1. Dans le tableau, E et D indiquent l'état du paramètre DownStateFlush : E signifie Activé et D signifie Désactivé.

Vserver-LB-1	Service-1	État des connexions
E	E	Les connexions client et serveur sont interrompues.

Vserver-LB-1	Service-1	État des connexions
E	D	Pour certains types de services, tels que TCP, pour lesquels l'appliance NetScaler ne prend pas en charge la réutilisation des connexions, les connexions client et serveur sont interrompues. Pour les types de service, tels que HTTP, pour lesquels l'appliance prend en charge la réutilisation des connexions, les connexions client et serveur ne sont interrompues que si une transaction est active sur ces connexions. Si une transaction n'est pas active, seules les connexions client sont interrompues.
D	E	Pour certains types de services, tels que TCP, pour lesquels l'appliance NetScaler ne prend pas en charge la réutilisation des connexions, les connexions client et serveur sont interrompues. Pour les types de service, tels que HTTP, pour lesquels l'appliance prend en charge la réutilisation des connexions, les connexions client et serveur ne sont interrompues que si une transaction est active sur ces connexions. Si une transaction n'est pas active, seules les connexions au serveur sont interrompues.

Vserver-LB-1	Service-1	État des connexions
D	D	Ni les connexions client ni serveur ne sont interrompues.

Si vous souhaitez désactiver un service uniquement lorsque toutes les connexions établies sont fermées par le serveur ou le client, vous pouvez utiliser l'option d'arrêt gracieux. Pour plus d'informations sur l'arrêt gracieux d'un service, voir Arrêt gracieux des services.

Pour définir le vidage d'état sur le service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -downStateFlush enabled
<!--NeedCopy-->
```

Pour configurer le vidage de l'état du service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**et sélectionnez **Vidage de l'état dévalant**.

Pour configurer le transfert d'état sur le serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Exemple :

```
set lb vserver vsvr1 -downStateFlush enabled
<!--NeedCopy-->
```


Pour configurer le transfert d'état sur le serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**et sélectionnez **Vidage de l'état dévalant**.

Arrêt gracieux des services

May 5, 2023

Lors de pannes réseau planifiées, telles que les mises à niveau du système ou la maintenance matérielle, vous devrez peut-être fermer ou désactiver certains services. Vous pouvez activer le service ultérieurement à l'aide de la <name> commande « enable service ».

Pour éviter de perturber les sessions établies, vous pouvez placer un service dans l'état Transition Out of Service (TROFS) en procédant de l'une des manières suivantes :

- Ajouter un code ou une chaîne TROFS au moniteur : configurez le serveur pour qu'il envoie un code ou une chaîne spécifique en réponse à une sonde de surveillance.
- Désactivez explicitement le service et :
  - Définissez un délai (en secondes).
  - Activez l'arrêt progressif.

Ajout d'un code ou d'une chaîne TROFS

Si vous ne liez qu'un seul moniteur à un service et que le moniteur est activé par TROFS, il peut placer le service dans l'état TROFS sur la base de la réponse du serveur à une sonde de surveillance. Cette réponse est comparée à la valeur du paramètre TroFSCode pour un moniteur HTTP ou du paramètre TroFSString pour un moniteur HTTP-ECV ou TCP-ECV. Si le code correspond, le service est placé dans l'état TROFS. Dans cet état, il continue de respecter les connexions persistantes.

Si plusieurs moniteurs sont liés à un service, l'état effectif du service est calculé sur la base de l'état de tous les moniteurs liés au service. Lors de la réception d'une réponse TROFS, l'état du moniteur compatible TROFS est considéré comme UP aux fins de ce calcul. Pour plus d'informations sur la manière dont une appliance NetScaler désigne un service comme étant actif, consultez la section Définition d'une valeur seuil pour les moniteurs liés àun service.

Important :

- Vous pouvez lier plusieurs moniteurs à un service, mais vous ne devez pas activer TROFS pour plusieurs d'entre eux.

- Vous pouvez convertir un moniteur compatible TroFS en un moniteur qui ne l'est pas, mais pas l'inverse.

Pour configurer un code ou une chaîne TROFS dans un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
add lb monitor <monitor-name> HTTP -trofsCode <respcode>

add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>

add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
<!--NeedCopy-->
```

Pour modifier le code ou la chaîne TROFS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
set lb monitor <trofs monitorname> HTTP -trofscode <newcode>

set lb monitor <trofs monitorname> HTTP-ECV -trofsstring <new string>

set lb monitor <trofs monitorname> TCP-ECV -trofsstring <new string>
<!--NeedCopy-->
```

Remarque : Vous ne pouvez utiliser la commande set que si un moniteur compatible TroFS a été ajouté précédemment. Vous ne pouvez pas utiliser cette commande pour définir le code ou la chaîne TROFS pour un moniteur qui n'est pas compatible avec TROFS.

Pour configurer un code ou une chaîne TROFS dans un moniteur à l'aide de l'utilitaire de configuration

1. Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs.
2. Dans le volet Moniteurs, cliquez sur Ajouter, puis effectuez l'une des opérations suivantes :
   - Sélectionnez Tapez HTTP et spécifiez un code TROFS.
   - Sélectionnez Type en tant que HTTP-ECV ou TCP-ECV, puis spécifiez une chaîne TROFS.

Désactiver un service

Toutefois, il arrive souvent que vous ne puissiez pas estimer le temps nécessaire à toutes les connexions à un service pour terminer les transactions existantes. Si une transaction n'est pas terminée à

l'expiration du délai d'attente, l'arrêt du service peut entraîner une perte de données. Dans ce cas, vous pouvez spécifier un arrêt progressif du service, de sorte que le service ne soit désactivé que lorsque toutes les connexions clientes actives en cours sont fermées par le serveur ou le client. Consultez le tableau suivant pour connaître le comportement si vous spécifiez un temps d'attente en plus d'un arrêt progressif.

La persistance est maintenue selon la méthode spécifiée même si vous activez l'arrêt progressif. Le système continue de servir tous les clients persistants, y compris les nouvelles connexions des clients, sauf si le service est marqué comme DOWN pendant l'état d'arrêt gracieux à la suite des vérifications effectuées par un moniteur.

Le tableau suivant décrit les options d'arrêt gracieuses.

State	Résultats
L'arrêt progressif est activé et un temps d'attente est spécifié.	Le service est arrêté une fois que la dernière des connexions clientes actives en cours a été effectuée, même si le délai d'attente n'a pas expiré. L'appliance vérifie l'état des connexions une fois par seconde. Si le délai d'attente expire, toutes les sessions ouvertes sont fermées.
L'arrêt progressif est désactivé et un temps d'attente est spécifié.	Le service est arrêté uniquement après l'expiration du délai d'attente, même si toutes les connexions établies sont assurées avant l'expiration.
L'arrêt progressif est activé et aucun temps d'attente n'est spécifié.	Le service est arrêté uniquement lorsque la dernière des connexions précédemment établies a été traitée, quel que soit le temps nécessaire pour traiter la dernière connexion.
L'arrêt progressif est désactivé et aucun délai d'attente n'est spécifié.	Pas d'arrêt gracieux. Le service est arrêté immédiatement après le choix de l'option de désactivation ou l'émission de la commande de désactivation. (Le temps d'attente par défaut est de zéro seconde.)

Pour mettre fin à des connexions existantes lorsqu'un service ou un serveur virtuel est marqué comme DOWN, vous pouvez utiliser l'option Down State Flush. Pour plus d'informations, reportez-vous à la section Activation du nettoyage des connexions aux serveurs virtuels.

Pour configurer l'arrêt progressif d'un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour arrêter correctement un service et vérifier la configuration :

```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Exemple :

```
> disable service svc1 6000 -graceFul YES
Done
>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: GOING OUT OF SERVICE (Graceful, Out Of Service in 5998 seconds)
Last state change was at Mon Nov 15 22:44:15 2010
Time since last state change: 0 days, 00:00:01.160
...
Down state flush: ENABLED

1 bound monitor:
1) Monitor Name: tcp-default
State: UP              Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - live traffic to service.
Response Time: N/A
Done

>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: OUT OF SERVICE
Last state change was at Mon Nov 15 22:44:19 2010
Time since last state change: 0 days, 00:00:03.250
Down state flush: ENABLED

1 bound monitor:
1)  Monitor Name: tcp-default
State: UNKNOWN           Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - service state OFS.
Response Time: N/A
Done
```



```
<!--NeedCopy-->
```

Pour configurer l'arrêt progressif d'un service à l'aide de l'utilitaire de configuration

1. Accédez à Traffic Management > Load Balancing > Services.
2. Ouvrez le service et, dans la liste des actions, cliquez sur Désactiver. Entrez un temps d'attente, puis sélectionnez Graceful.

Activer ou désactiver la session de persistance sur les services TROFS

August 20, 2021

Vous pouvez définir l'indicateur TrofsPersistence pour spécifier si un service en état de transition hors service (TROFS) doit conserver des sessions persistantes. Lorsqu'un moniteur est activé par TROFS, il peut placer un service dans l'état TROFS en fonction de la réponse du serveur à une sonde de moniteur. Cette réponse est comparée à la valeur du paramètre trofsCode pour un moniteur HTTP ou le paramètre trofsString pour un moniteur HTTP ECV ou TCP-ECV. Si le code correspond, le service est placé dans l'état TROFS. Dans cet état, il continue d'honorer les connexions clientes actives. Dans certains cas, les sessions actives honorées peuvent devoir inclure des sessions persistantes. Mais dans d'autres cas, en particulier ceux impliquant des sessions de persistance de longue durée ou des méthodes de persistance telles que l'ID de serveur personnalisé, le respect des sessions persistantes peut empêcher le service de passer à l'état hors service.

Si vous définissez l'indicateur TrofsPersistence sur Enabled, les sessions persistantes sont honorées. Si vous le définissez sur DISABLED, ils ne le sont pas.

Pour définir l'indicateur TrofsPersistence à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour définir l'indicateur `trofsPersistence` d'un nouveau serveur virtuel ou d'un serveur virtuel existant, ou pour renvoyer le paramètre à sa valeur par défaut :

```
add lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

set lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

unset lb vserver <name> [-trofsPersistence]
<!--NeedCopy-->
```


Argument

trofsPersistence. Honorer les connexions clientes actives actuelles et les nouvelles demandes sur les sessions de persistance lorsque le service est dans l'état TROFS.

Valeurs possibles : ENABLED, DISABLED. Par défaut : ENABLED.

Exemples :

```
add lb vserver v1 http 10.102.217.42 80 -persistencetype SOURCEIP -
   trofsPersistence ENABLED

set lb vserver v1 -trofsPersistence DISABLED

unset lb vserver v1 -trofsPersistence
<!--NeedCopy-->
```

Demandes directes vers une page Web personnalisée

May 5, 2023

> **Avertissement**
>
> SureConnect (SC) est obsolète à partir de NetScaler 12.0 build 56.20 et Citrix vous recommande d'utiliser la fonctionnalité AppQoE. Pour plus d'informations, consultezAppQoE.

Pour que SureConnect fonctionne correctement, vous devez le définir globalement. NetScaler fournit l'option SureConnect pour garantir la réponse d'une application.

Pour définir SureConnect sur le service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -sc <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -sc ON
<!--NeedCopy-->
```

Pour configurer SureConnect sur le service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.

2. Dans Paramètres avancés, sélectionnez Paramètres de trafic, puis **Sure Connect**.

Activer l'accès aux services en cas de panne

May 5, 2023

Vous pouvez activer l'accès à un service lorsqu'il est désactivé ou lorsqu'il est hors service en configurant l'appliance NetScaler pour qu'elle utilise le mode de couche 2 pour relier les paquets envoyés au service. Normalement, lorsque les demandes sont transmises à des services qui sont hors service, les paquets de demandes sont supprimés. Toutefois, lorsque vous activez le paramètre **Access Down**, ces paquets de demandes sont envoyés directement aux serveurs à charge équilibrée.

Pour plus d'informations sur les modes de couche 2 et de couche 3, voir Adressage IP.

Pour que l'appliance relie les paquets envoyés aux services DOWN, activez le mode Couche 2 avec le paramètre AccessDown.

Pour activer l'accès à un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -accessDown <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -accessDown YES
<!--NeedCopy-->
```

Pour activer l'accès à un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Access Down**.

Activer la mise en mémoire tampon TCP des réponses

May 5, 2023

L'appliance NetScaler fournit une option de mise en mémoire tampon TCP qui met en mémoire tampon uniquement les réponses provenant du serveur d'équilibrage de charge. Cela permet à

l'appliance de fournir des réponses serveur au client à la vitesse maximale que le client peut accepter. L'appliance alloue de 0 à 4 095 Mo (Mo) de mémoire tampon pour la mise en mémoire tampon TCP et de 4 à 2 480 kilo-octets (Ko) de mémoire par connexion.

Remarque : La mise en mémoire tampon TCP au niveau du service a priorité sur le paramètre global. Pour plus d'informations sur la configuration globale de la mise en mémoire tampon TCP, voir TCP Buffering.

Pour activer la mise en mémoire tampon TCP sur un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -TCPB <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -TCPB YES
<!--NeedCopy-->
```

Pour activer la mise en mémoire tampon TCP sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Buffering TCP**.

Activer la compression

May 5, 2023

L'appliance NetScaler fournit une option de compression permettant de compresser de manière transparente les fichiers HTML et texte à l'aide d'un ensemble de politiques de compression intégrées. La compression réduit les besoins en bande passante et peut améliorer de manière significative la réactivité du serveur dans les configurations à bande passante limitée. Les politiques de compression sont associées aux services liés au serveur virtuel. Les politiques déterminent si une réponse peut être compressée et envoient du contenu compressible à l'appliance, qui le compresse et l'envoie au client.

Remarque : Pour que la compression fonctionne correctement, vous devez l'activer globalement. Pour plus d'informations sur la configuration globale de la compression, voir Compression.

Pour activer la compression sur un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -CMP <YES | NO>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -CMP YES
<!--NeedCopy-->
```

Pour activer la compression sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Compression**.

Activer la vérification de l'état TCP externe pour les serveurs virtuels UDP

May 5, 2023

Dans les clouds publics, vous pouvez utiliser l'appliance NetScaler comme équilibreur de charge de second niveau lorsque l'équilibreur de charge natif est utilisé comme premier niveau. L'équilibreur de charge natif peut être un équilibreur de charge d'application (ALB) ou un équilibreur de charge réseau (NLB). La plupart des clouds publics ne prennent pas en charge les sondes de santé UDP dans leurs équilibreurs de charge natifs. Pour surveiller l'état de l'application UDP, les clouds publics recommandent d'ajouter un point de terminaison TCP à votre service. Le point de terminaison reflète l'intégrité de l'application UDP.

L'appliance NetScaler prend en charge le contrôle de santé externe basé sur TCP pour un serveur virtuel UDP. Cette fonctionnalité introduit un écouteur TCP sur le VIP du serveur virtuel et le port configuré. L'écouteur TCP reflète l'état du serveur virtuel.

Pour activer un contrôle de santé TCP externe pour les serveurs virtuels UDP par CLI

À l'invite de commandes, tapez la commande suivante pour activer une vérification d'intégrité TCP externe avec l'option tcpProbePort :

```
add lb vserver <name> <serviceType> <IPAddress> <port> -tcpProbePort <
    tcpProbePort>
```



```
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-UDP-1 UDP 10.102.29.60 80 tcpProbePort 5000
<!--NeedCopy-->
```

Pour activer un contrôle de santé TCP externe pour les serveurs virtuels UDP par interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis créez un serveur virtuel.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel.
3. Dans le volet **Paramètres de base**, ajoutez le numéro de port dans le champ **Port de la sonde TCP** .
4. Cliquez sur **OK**.

Maintenir la connexion client pour plusieurs demandes client

May 5, 2023

Vous pouvez définir le paramètre Keep-Alive du client pour configurer un service HTTP ou SSL afin de maintenir une connexion client à un site Web ouverte sur plusieurs demandes client. Si le maintien en activité du client est activé, même lorsque le serveur Web à charge équilibrée ferme une connexion, l'appliance NetScaler maintient ouverte la connexion entre le client et lui-même. Ce paramètre permet aux services de servir plusieurs requêtes client sur une seule connexion client.

Si vous n'activez pas ce paramètre, le client ouvre une nouvelle connexion pour chaque demande envoyée au site Web. Le paramètre Keep-alive du client permet d'économiser le temps de trajet aller-retour des paquets requis pour établir et fermer les connexions. Ce paramètre réduit également le temps nécessaire pour terminer chaque transaction. Le maintien en vie du client ne peut être activé que sur les types de service HTTP ou SSL.

Client keep-alive défini au niveau du service a priorité sur le paramètre global keep-alive du client. Pour plus d'informations sur le service Keep-Alive du client, voir Keep-Alivedu client.

Pour activer le maintien en vie du client sur un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
set service <name> -CKA <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -CKA YES
<!--NeedCopy-->
```

Pour activer le maintien en vie du client sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**et sélectionnez **Client Keep-Alive**.

Insérez l'adresse IP du client dans l'en-tête de la demande

May 5, 2023

Un NetScaler utilise l'adresse IP du sous-réseau (SNIP) pour se connecter au serveur. Le serveur n'a pas besoin de connaître le client.

Toutefois, dans certaines situations, le serveur doit connaître le client qu'il doit servir. Lorsque vous activez le paramètre IP du client, l'appliance insère l'adresse IPv4 ou IPv6 du client tout en transmettant les demandes au serveur. Le serveur insère cette adresse IP du client dans l'en-tête des réponses. Le serveur connaît donc le client.

> **Remarque** : Pour insérer plusieurs en-têtes, vous devez effectuer l'une des opérations suivantes :
>
> - Ajoutez des politiques de réécriture pour vérifier CLIENT.IS_SSL et insérer l'en-tête approprié.
> - Liez la stratégie de réécriture appropriée pour chaque serveur virtuel en fonction du type.

Pour insérer l'adresse IP du client dans la demande du client à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -CIP <Value> <cipHeader>
<!--NeedCopy-->
```

Exemple :


```
set service Service-HTTP-1 -CIP enabled X-Forwarded-For
<!--NeedCopy-->
```

Pour insérer l'adresse IP du client dans la demande du client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services** et modifiez un service.
2. Dans le volet **Paramètres du service**, cliquez sur l' **icône de modification**.
3. Dans le volet **Service d'équilibrage de charge**, cochez la case **Insérer l'adresse IP du client** .

Récupérer les détails de localisation à partir de l'adresse IP de l'utilisateur à l'aide de la base de données

May 5, 2023

> **Remarque** Cette fonctionnalité est disponible à partir de NetScaler version 12.1 build 50.x et versions ultérieures.

L'appliance NetScaler peut obtenir les informations de localisation des utilisateurs, telles que le continent, le comté et la ville. Pour toute adresse IP publique provenant d'une base de données de géolocalisation. Il est exécuté à l'aide de l'infrastructure de stratégie avancée. Les détails de localisation récupérés sont ensuite utilisés dans une action de réécriture ou une action de répondeur pour effectuer les cas d'utilisation suivants.

- Insérez un en-tête HTTP avec les détails de l'emplacement de l'utilisateur (tels que le pays, la ville) lors de l'envoi de la demande du client au serveur principal.
- Ajoutez le nom du pays dans la réponse de la page HTML pour un utilisateur non valide.

La solution matérielle-logicielle peut également consigner les détails de l'emplacement à l'aide du mécanisme de journalisation d'audit.

Obtention des détails de localisation des utilisateurs à l'aide des fonctions de géolocalisation

Les composants interagissent comme suit :

1. L'utilisateur envoie une demande client à partir d'un emplacement géographique particulier.
2. L'appliance NetScaler recherche l'adresse IP de l'utilisateur à partir de la demande du client et récupère les détails de géolocalisation. Les détails incluent le continent, le pays, la région, la

ville, le FAI, l'organisation ou les détails personnalisés d'une base de données de géolocalisation.

3. Une fois les détails de l'emplacement récupérés, la solution matérielle-logicielle utilise une stratégie de répondeur ou une stratégie de réécriture pour évaluer la demande.
4. Dans une stratégie de réécriture, la solution matérielle-logicielle ajoute un en-tête avec les détails de l'emplacement géographique et l'envoie au serveur principal. Par exemple, insérez un en-tête HTTP personnalisé avec des informations de pays.
5. Dans une stratégie de répondeur, la solution matérielle-logicielle évalue la demande HTTP et, en fonction de l'évaluation de la stratégie, autorise l'accès aux utilisateurs ou redirige l'utilisateur vers une page d'erreur. Il indique que la région à partir de laquelle ils accèdent à l'application n'a pas accès.

Configuration de la base de données de géolocalisation

Au préalable, vous devez disposer d'une base de données de géolocalisation à exécuter sur l'appliance NetScaler. Les fichiers de base de données de géolocalisation sont disponibles avec le microprogramme NetScaler. Pour télécharger les fichiers de base de données auprès d'un fournisseur, convertissez-les au format NetScaler et importez-les dans votre appliance.
Pour plus d'informations sur la base de données de géolocalisation, consultez la rubrique Ajouter un fichier d'emplacement pour créer une base de données de proximité statique .

Fonctions de géolocalisation

Le tableau suivant répertorie les fonctions de géolocalisation qui récupèrent les détails de localisation de n'importe quelle adresse IP publique. Ces fonctions peuvent être utilisées dans les stratégies de réécriture ou de répondeur.

Fonction de géolocalisation	Exemple
CLIENT.IP.SRC.LOCATION	Asia.In.Karnataka.Bangalore
CLIENT.IP.SRC.LOCATION.GET (1) .LOCATION_LONG	Inde
CLIENT.IP.SRC.LOCATION (3)	Asia.In.Karnataka
CLIENT.IP.SRC.LAT_LONG	12,77
CLIENT.IPV6.SRC.LOCATION	Amérique du Nord .US.Californie.Santa Clara.Verizon.Citrix
CLIENT.IPV6.SRC.LOCATION(3)	Amérique du Nord, États-Unis, Californie
CLIENT.IPV6.SRC.LOCATION.GET (1) .LOCATION_LONG	États-Unis

Fonction de géolocalisation	Exemple
CLIENT.IPV6.SRC.LOCATION.GET (3)	Californie
CLIENT.IPV6.SRC.LAT_LONG	36, -119

Configuration des fonctions de géolocalisation

Pour configurer les fonctions de géolocalisation à l'aide d'une infrastructure de stratégie avancée, vous devez activer les fonctionnalités d'équilibrage de charge, de réécriture et de répondeur, puis compléter les cas d'utilisation suivants.

Activer les fonctionnalités d'équilibrage de charge, de répondeur et de réécriture

Si vous souhaitez que l'appliance NetScaler autorise l'accès des utilisateurs à partir d'un emplacement géographique particulier, vous devez activer les fonctionnalités d'équilibrage de charge, de réécriture et de réponse.

```
enable ns feature loadbalancing rewrite responder
<!--NeedCopy-->
```

Cas d'utilisation 1 : Configuration de la fonction de géolocalisation pour rediriger les utilisateurs non valides en dehors de la géolocalisation

Lorsqu'un utilisateur indien demande l'accès à une page Web, bloquez la demande et répondez avec une page HTML avec le nom du pays.

Les étapes suivantes vous aident à terminer la configuration de ce cas d'utilisation.

- Add responder action
- Add responder policy
- Lier la stratégie du répondeur au serveur d'équilibrage de charge

Pour plus d'informations sur les procédures de l'interface graphique pour l'action de réécriture et la configuration de la stratégie de réécriture, consultez la rubrique Responder

Add responder action

Ajoutez une action de répondeur pour répondre avec une page HTML avec le nom du pays.
À l'invite de commande, tapez :


```
add responder action <name> <type> (<target> | <htmlpage>) [-comment <
    string>] [-responseStatusCode <positive_integer>][-reasonPhrase <
    string>]
<!--NeedCopy-->
```

Exemple :

```
add responder action responder_act respondwith "HTTP.REQ.VERSION + "
    304 Requested Page not allowed in your country - " + CLIENT.IP.SRC.
    LOCATION.GET (1).LOCATION_LONG + "\r\n""
<!--NeedCopy-->
```

Ajouter une action de message journal d'audit

Vous pouvez configurer les actions de message d'audit pour consigner les messages à différents niveaux de journal, soit au format Syslog uniquement, soit en syslog et en `newnslog` formats. Les actions de message d'audit utilisent des expressions pour spécifier le format des messages d'audit.
Pour créer une action de message d'audit à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add audit messageaction <name> <logLevel> <stringBuilderExpr> [-logtoNewnslog
 (YES|NO)]
```

Exemple :

```
add audit messageaction msg1 DEBUG ""Request Location: "+CLIENT.IP.SRC.
    LOCATION"
<!--NeedCopy-->
```

Add responder policy

Ajoutez une stratégie de répondeur pour identifier les demandes provenant de l'Inde et associez l'action de répondeur à cette stratégie.
À l'invite de commande, tapez :

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>] [-appflowAction <string>]
<!--NeedCopy-->
```

Exemple :

```
add responder policy responder_pol CLIENT.IP.SRC.MATCHES_LOCATION("Asia
    .India.\*.\*.\*.\*") responder_act -logaction msg1
```



```
<!--NeedCopy-->
```

Lier la stratégie du répondeur au serveur d'équilibrage de charge

Liez la stratégie de répondeur à un serveur virtuel d'équilibrage de charge de type HTTP/SSL.
À l'invite de commande, tapez :

```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
    <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver http_vserver -policyName responder_pol -priority 100 -
    type REQUEST
<!--NeedCopy-->
```

Cas d'utilisation 2 : Configuration de la fonction de géolocalisation pour insérer un nouvel en-tête HTTP avec des détails d'emplacement pour que le back-end réponde

Imaginons un scénario dans lequel une appliance NetScaler doit insérer l'emplacement de l'utilisateur dans l'en-tête HTTP d'une demande envoyée au serveur d'applications afin que le serveur puisse utiliser les informations pour une certaine logique métier.
Les étapes suivantes vous aident à terminer la configuration de ce cas d'utilisation.

- Add rewrite action
- Add rewrite policy
- Lier la stratégie de réécriture à l'équilibrage de charge

Pour plus d'informations sur les procédures de l'interface graphique pour l'action de réécriture et la configuration de la stratégie de réécriture, consultez la rubrique Répondeur .

Add rewrite action

Ajoutez une action de réécriture pour insérer un en-tête HTTP personnalisé avec les détails de géolocalisation de l'utilisateur dans la demande et envoyez-lui des serveurs principaux.
À l'invite de commande, tapez :

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
    search <expression>] [-refineSearch <string>][-comment <string>]
<!--NeedCopy-->
```

Exemple :


```
add rewrite action rewrite_act insert_http_header "User_location"
   CLIENT.IP.SRC.LOCATION
<!--NeedCopy-->
```

Add rewrite policy

Ajoutez une stratégie de réécriture pour déterminer si l'action de réécriture doit être exécutée. Dans ce cas, toutes les requêtes envoyées au serveur d'applications doivent comporter un en-tête HTTP personnalisé, de sorte que la règle peut être « true ».
À l'invite de commande, tapez :

```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <
   string>] [-logAction <string>]
<!--NeedCopy-->
```

Exemple :

```
add rewrite policy rewrite_pol true rewrite_act -logaction log_act
<!--NeedCopy-->
```

Lier la stratégie de réécriture à l'équilibrage de charge

Liez la stratégie de réécriture au serveur virtuel d'équilibrage de charge requis de type HTTP/SSL.
À l'invite de commande, tapez :

```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
   <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver http_vserver -policyName rewrite_pol -priority 100 -
   type REQUEST
<!--NeedCopy-->
```

Prise en charge de Syslog pour la journalisation des détails de géolocalisation (facultatif)

Si vous préférez consigner les détails de géolocalisation de l'utilisateur, vous devez spécifier l'action SYSLOG à exécuter lorsqu'une demande correspond à la stratégie. L'appliance stocke les détails sous forme de message de journal dans le fichier ns.log.

Pour plus d'informations sur l'audit SYSLOG et NSLOG, consultez la rubrique Journalisation des audits .

Sortie pour les détails de géolocalisation utilisateur

La sortie suivante est enregistrée dans l'appliance à l'aide du SYSLOG ou de l' `newnslog` action si vous essayez d'accéder à une application depuis l'emplacement Bangalore et si l'appliance utilise la fonction de géolocalisation, « CLIENT.IP.SRC.LOCATION'.

```
Asia.India.Karnataka.Banglore
<!--NeedCopy-->
```

Exemple de journal de sortie :

```
07/23/2018:19:03:54 GMT  Debug 0-PPE-0 : default REWRITE Message 22 0 :
     "Request Location: asia.in.karnataka.bangalore.\*.\*"
07/23/2018:19:23:55 GMT  Debug 0-PPE-0 : default RESPONDER Message 32 0
Done
<!--NeedCopy-->
```

Utiliser l'adresse IP source du client lors de la connexion au serveur

May 5, 2023

Vous pouvez configurer l'appliance NetScaler pour transférer les paquets du client vers le serveur sans modifier l'adresse IP source. Ceci est utile lorsque vous ne pouvez pas insérer l'adresse IP du client dans un en-tête, par exemple lorsque vous travaillez avec des services non HTTP.

Pour plus d'informations sur la configuration globale d'USIP, consultez Activation de l'utilisation du mode IP source.

Pour activer le mode USIP pour un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -usip (YES | NO)
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -usip YES
<!--NeedCopy-->
```


Pour activer le mode USIP pour un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis ouvrez un service.
2. Dans Paramètres avancés, dans la section Paramètres du service, sélectionnez **Utiliser l'adresse IP source**.

Utiliser l'adresse IP source du client pour la communication principale dans une configuration d'équilibrage de charge v4-v6

May 5, 2023

Dans une configuration d'équilibrage de charge v4 à v6, pour les services dont l'USIP est désactivé, l'appliance NetScaler communique avec les serveurs associés à partir de l'une des adresses SNIP IPv6 (SNIP6) configurées.

Pour les services pour lesquels l'USIP est activé, vous devez définir le paramètre de préfixe NAT USIP global pour que les serveurs associés connaissent l'adresse IP du client associée aux paquets de demande. Le préfixe NAT USIP est un préfixe IPv6 global de longueur 32/40/48/56/64/96 bits configuré sur l'appliance NetScaler.

Pour un service d'équilibrage de charge sur lequel l'USIP est activé, l'appliance traduit le paquet de demande IPv4 en paquet IPv6 et définit l'adresse IP source du paquet IPv6 traduit selon une concaténation de :

- le préfixe NAT USIP d'une longueur de 32/40/48/56/64/96 bits.
- zéros complétés si la longueur du préfixe USIP NAT est inférieure à 96 bits. Nombre de bits complétés par des zéros = longueur du préfixe NAT USIP 96. Par exemple, si la longueur du préfixe NAT USIP est 64, le nombre de bits rembourrés avec des zéros = 96-64 = 32.
- l'adresse source IPv4 [32 bits] qui a été reçue dans le paquet de requête. En d'autres termes, les 32 derniers bits de l'adresse IPv6 source sont définis sur l'adresse IPv4 du client.

À la réception d'un paquet de réponse IPv6 du serveur, l'appliance NetScaler traduit le paquet IPv6 en paquet IPv4 et définit l'adresse IP de destination du paquet IPv4 traduit sur les 32 derniers bits de l'adresse IP de destination du paquet IPv6.

> **Remarque** : Cette fonctionnalité n'est pas prise en charge pour la configuration de NetScaler Gateway et les configurations d'équilibrage de charge de commutation de contenu et de redirection du cache.

Étapes de configuration

La configuration de l'USIP pour une configuration d'équilibrage de charge v4 à v6 comprend les tâches suivantes :

- **Ajoutez le préfixe NAT USIP global**. Il s'agit d'un préfixe IPv6 global de longueur 32/40/48/56/64/96 bits à configurer sur l'appliance.
- **Activer le mode global USIP**. Pour plus d'informations, voir Activer l'utilisation du mode IP source.
- **Activez le mode USIP pour les services d'équilibrage**de charge. Pour plus d'informations, voir Utiliser l'adresse IP source du client lors de la connexion au serveur.

Pour ajouter un préfixe NAT global USIP à l'aide de l'interface de ligne de commande :

- `set ipv6 -usipnatprefix <prefix/prefix_length>`
- `show ipv6`

Pour ajouter un préfixe NAT USIP global à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, puis cliquez sur **Modifier les paramètres IPv6**.
2. Sur l'écran **Configurer la configuration pour IPV6**, définissez le paramètre de **préfixe NAT USIP** .

Exemple de configuration

```
> set ipv6 -usipnatprefix 2001:DB8:90::/64
Done

> enable ns mode USIP
Done

> add lb vserver LBVS-1 HTTP 203.0.113.90 80
Done

> add service SVC-1 2001:DB8:5001::30 HTTP 80 -usip yes
Done

> add service SVC-2 2001:DB8:5001::60 HTTP 80 -usip yes
Done

> bind lb vserver LBVS-1 SVC-1
Done

> bind lb vserver LBVS-1 SVC-2
Done

```



```
<!--NeedCopy-->
```

Configurer le port source pour les connexions côté serveur

May 5, 2023

Lorsque l'appliance NetScaler se connecte à un serveur physique, elle peut utiliser le port source issu de la demande du client ou un port proxy comme port source pour la connexion. Vous pouvez définir le paramètre Use Proxy Port sur YES pour gérer des situations telles que le scénario suivant :

- L'appliance NetScaler est configurée avec deux serveurs virtuels d'équilibrage de charge, LBVS1 et LBVS2.
- Les deux serveurs virtuels sont liés au même service, S-ANY.
- L'utilisation de l'adresse IP source (USIP) (du client) est activée sur le service.
- Le client C1 envoie deux demandes, Req1 et Req2, pour le même service.
- LBVS1 reçoit Req1 et LBVS2 reçoit Req2.
- LBVS1 et LBVS2 transmettent la demande à S-ANY, et lorsque S-ANY envoie la réponse, LBVS1 et LBVS2 transmettent la réponse au client.
- Considérez deux cas :
  - Utilisez le port client. Lorsque l'appliance utilise le port client, les serveurs virtuels utilisent l'adresse IP du client (car USIP est ON) et le port du client lors de la connexion au serveur. Par conséquent, lorsque le service envoie la réponse, l'appliance ne peut pas déterminer quel serveur virtuel doit recevoir la réponse.
  - Utilisez le port proxy. Lorsque l'appliance utilise un port proxy, les serveurs virtuels utilisent l'adresse IP du client (car USIP est ON), mais des ports différents lors de la connexion au serveur. Par conséquent, lorsque le service envoie la réponse, le numéro de port identifie le serveur virtuel qui doit recevoir la réponse.

Toutefois, si vous avez besoin d'une configuration totalement transparente, telle qu'une configuration de redirection de cache totalement transparente, vous devez désactiver le paramètre Utiliser le port proxy afin que l'appliance NetScaler puisse utiliser le port source à partir de la demande du client.

L'option Utiliser le port proxy devient pertinente si l'option Utiliser l'adresse IP source (USIP) est activée. Pour les types de services basés sur le protocole TCP, tels que TCP, HTTP et SSL, l'option est activée par défaut. Pour les types de service UDP, tels que UDP et DNS, y compris ANY, l'option est désactivée par défaut. Pour plus d'informations sur l'option USIP, reportez-vous à la section « Activation de l'utilisation du mode IP source ». «

Vous pouvez configurer le paramètre **Utiliser le port proxy** soit globalement, soit sur un service donné.

Configurer le paramètre d'utilisation du port proxy sur un service

Vous configurez le paramètre **Utiliser ProxyPort** sur le service si vous souhaitez remplacer le paramètre global.

Pour configurer le paramètre Utiliser le port proxy sur un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -useProxyPort (YES | NO)
<!--NeedCopy-->
```

Exemple :

```
set service svc1 -useproxyport YES
Done

show service svc1
svc1 (10.102.29.30:80) - HTTP
State: UP
. . .
Use Source IP: YES Use Proxy Port: YES
. . .
Done
<!--NeedCopy-->
```

Pour configurer le paramètre Utiliser le port proxy sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez Paramètres de trafic et sélectionnez **Utiliser le port proxy**.

Configurer le paramètre d'utilisation du port proxy de manière globale

Vous configurez le paramètre **Utiliser le port proxy** globalement si vous souhaitez appliquer le paramètre à tous les services de l'appliance NetScaler. Les paramètres **Use Proxy Port** spécifiques au service remplacent le paramètre global.

Pour configurer globalement le paramètre Utiliser le port proxy à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le paramètre **Utiliser le port proxy** globalement et vérifier la configuration :

```
set ns param -useproxyport ( ENABLED | DISABLED )`
show ns param`
<!--NeedCopy-->
```

Exemple :

```
set ns param -useproxyport ENABLED

Done

show ns param
Global configuration settings:
. . .
Use Proxy Port: ENABLED
Done
<!--NeedCopy-->
```

Pour configurer le paramètre Utiliser le port proxy globalement à l'aide de l'interface graphique

Accédez à **Système > Paramètres > Modifier les paramètres système globaux**, puis sélectionnez ou désactivez Utiliser le port proxy.

Définir une limite sur le nombre de connexions client

May 5, 2023

Vous pouvez spécifier un nombre maximum de connexions client que chaque serveur d'équilibrage de charge peut gérer. L'appliance NetScaler ouvre ensuite les connexions client à un serveur uniquement jusqu'à ce que cette limite soit atteinte. Lorsque le serveur équilibré de charge atteint sa limite, les sondes du moniteur sont ignorées et le serveur n'est pas utilisé pour l'équilibrage de charge tant qu'il n'a pas terminé le traitement des connexions existantes et libère de la capacité.

Pour plus d'informations sur le paramètre **Maximum Client**, reportez-vous à la section Services basés sur des noms de domaine d'équilibrage de charge.

Remarque : Les connexions en cours de fermeture ne sont pas prises en compte pour cette limite.

Pour définir une limite au nombre de connexions client à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -maxclient <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -maxClient 1000
<!--NeedCopy-->
```

Pour définir une limite au nombre de connexions client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**, puis sélectionnez **Maximum Clients**.

Définir une limite sur le nombre de requêtes par connexion au serveur

May 5, 2023

L'appliance NetScaler peut être configurée pour réutiliser les connexions afin d'améliorer les performances. Dans certains scénarios, cependant, les serveurs Web à charge équilibrée peuvent rencontrer des problèmes lorsque les connexions sont réutilisées pour un trop grand nombre de demandes. Pour les services HTTP ou SSL, utilisez l'option de requête max pour limiter le nombre de requêtes envoyées via une seule connexion à un serveur Web à charge équilibrée.

Remarque : Vous pouvez configurer l'option de demande maximale pour les services HTTP ou SSL uniquement.

Pour limiter le nombre de demandes client par connexion à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <ServiceName> -maxReq <Value>
<!--NeedCopy-->
```


Exemple :

```
set service Service-HTTP-1 -maxReq 100
<!--NeedCopy-->
```

Pour limiter le nombre de demandes client par connexion à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**, puis sélectionnez **Maximum Requêtes**.

Définir une valeur de seuil pour les moniteurs liés à un service

May 5, 2023

L'appliance NetScaler désigne un service comme étant actif uniquement lorsque la somme des poids de tous les moniteurs qui y sont liés et qui sont actifs est égale ou supérieure à la valeur seuil configurée sur le service. Le poids d'un moniteur indique dans quelle mesure ce moniteur contribue à désigner le service auquel il est lié comme étant UP.

Par défaut, le seuil du moniteur est défini sur 0 et les poids du moniteur sont définis sur 1. Tous les moniteurs ont alors le même poids et un service peut tomber en panne lorsque l'un des moniteurs tombe en panne.

Supposons par exemple que trois moniteurs, nommés respectivement Monitor-HTTP-1, Monitor-HTTP-2 et Monitor-HTTP-3, soient liés à Service-HTTP-1 et que le seuil configuré sur le service soit de trois. Supposons que les pondérations suivantes soient attribuées à chaque moniteur :

- Le poids de Monitor-HTTP-1 est de 1.
- Le poids de Monitor-HTTP-2 est de 3.
- Le poids de Monitor-HTTP-3 est de 1.

Le service est balisé uniquement lorsque l'une des conditions suivantes est vraie :

- Monitor-HTTP-2 est actif.
- Monitor-HTTP-2 et Monitor-HTTP-1 ou Monitor-HTTP-3 sont actifs
- Les trois écrans sont en marche.

Pour définir la valeur du seuil de surveillance sur un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
set service <name> -monThreshold <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -monThreshold 100
<!--NeedCopy-->
```

Pour définir la valeur du seuil de surveillance sur un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**, puis sélectionnez **Surveiller le seuil**.

Définir une valeur de délai d'attente pour les connexions client inactives

May 5, 2023

Vous pouvez configurer le service avec une valeur de délai d'expiration pour mettre fin à toute connexion client inactive une fois le délai configuré écoulé. Si le client est inactif pendant la durée configurée, l'appliance NetScaler ferme la connexion client.

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -cltTimeout <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -cltTimeout 100
<!--NeedCopy-->
```

Pour définir une valeur de délai d'expiration pour les connexions client inactives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.

2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**, puis sélectionnez **Délai d'attente d'inactivité du client**.

Définir une valeur de délai d'attente pour les connexions de serveur inactives

May 5, 2023

Vous pouvez configurer un service avec une valeur de délai d'expiration pour mettre fin à toute connexion au serveur inactive lorsque le délai configuré (en secondes) est écoulé. Si le serveur est inactif pendant la durée configurée, l'appliance NetScaler ferme la connexion au serveur.

Pour définir une valeur de délai d'expiration pour les connexions au serveur inactives à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -svrTimeout <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -svrTimeout 100
<!--NeedCopy-->
```

Pour définir une valeur de délai d'expiration pour les connexions au serveur inactives à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais**d'attente et sélectionnez **Délai d'inactivité du serveur**.

Définir une limite sur l'utilisation de la bande passante par les clients

May 5, 2023

Parfois, les serveurs peuvent avoir une bande passante limitée pour gérer les demandes des clients et peuvent être surchargés. Pour éviter la surcharge d'un serveur, vous pouvez spécifier une limite

maximale sur la bande passante, en Kbps, traitée par le serveur. L'appliance NetScaler transmet les demandes à un serveur d'équilibrage de charge uniquement jusqu'à ce que cette limite soit atteinte.

Pour définir une limite de bande passante maximale pour un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <name> -maxBandwidth <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-HTTP-1 -maxBandwidth 100
<!--NeedCopy-->
```

Pour définir une limite de bande passante maximale pour un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**et ouvrez un service.
2. Dans Paramètres avancés, sélectionnez **Seuils et délais d'attente**et sélectionnez **Bande passante maximale**.

Rediriger les requêtes client vers un cache

August 20, 2021

Vous pouvez configurer un service pour rediriger les demandes client vers un cache et transférer les demandes non mises en cache vers un service choisi par la méthode d'équilibrage de charge configurée.

Pour définir la redirection du cache sur un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set service <name> -cacheable <Value>
<!--NeedCopy-->
```

Exemple :


```
set service Service-HTTP-1 -cacheable YES
<!--NeedCopy-->
```

Pour définir la redirection du cache sur un service à l'aide de l'interface graphique graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**.
2. Ouvrez un service et définissez le type de cache.

Conserver l'identificateur VLAN pour la transparence VLAN

August 20, 2021

Vous pouvez configurer un serveur virtuel d'équilibrage de charge pour conserver l'identificateur VLAN du client dans les paquets à transférer aux serveurs. Le serveur virtuel doit être un serveur virtuel générique de type ANY et doit fonctionner en mode MAC.

Pour configurer un serveur virtuel d'équilibrage de charge afin de conserver l'ID VLAN client à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer un serveur virtuel d'équilibrage de charge afin de conserver l'ID VLAN client et vérifier la configuration :

```
set lb vserver <name> -m MAC -macmodeRetainvlan ENABLED

show lb vserver <name>
<!--NeedCopy-->
```

> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l' `-m MAC` option est activée, vous devez lier un moniteur non utilisateur.

Pour configurer un serveur virtuel d'équilibrage de charge afin de conserver l'ID VLAN client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**, puis **Conserver l'ID VLAN**.

Configurer la transition d'état automatique en fonction du pourcentage d'intégrité des services liés

May 5, 2023

Vous pouvez configurer un serveur virtuel d'équilibrage de charge pour passer automatiquement de l'état UP à l'état DOWN si le pourcentage de services actifs tombe en dessous d'un seuil configuré. Par exemple, si vous liez 10 services à un serveur virtuel d'équilibrage de charge et que vous configurez un seuil de 50 % pour ce serveur virtuel, il passe de UP à DOWN si six services ou plus sont INDISPONIBLES. Lorsque le pourcentage de santé dépasse la valeur seuil, le serveur virtuel revient à l'état UP.

Vous pouvez également activer une alarme SNMP appelée ENTITY-STATE si vous souhaitez que l'appliance NetScaler vous avertisse lorsque le pourcentage de santé des services liés entraîne un changement d'état d'un serveur virtuel.

Pour configurer la transition automatique d'état basée sur le pourcentage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une transition automatique d'état pour un serveur virtuel et vérifier la configuration :

```
set lb vserver <name> -healthThreshold <positive_integer>

show lb vserver <name>
<!--NeedCopy-->
```

Pour configurer la transition automatique d'état basée sur le pourcentage à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans Paramètres avancés, sélectionnez **Paramètres de trafic**et définissez un **seuil de santé**.

Pour activer l'alarme ENTITY-STATE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer l'alarme SNMP ENTITY-STATE et vérifier la configuration :

```
enable snmp alarm ENTITY-STATE

show snmp alarm
```



```
<!--NeedCopy-->
```

Pour activer l'alarme ENTITY-STATE à l'aide de l'interface graphique

1. Accédez à **Système > SNMP > Alarmes**.
2. Sélectionnez **ENTITY-STATE** et, dans la liste Action, sélectionnez **Activer**.

Proximité statique basée sur l'emplacement de NetScaler

June 20, 2023

> **Remarque**
>
> Le paramètre proximity from self est disponible à partir de la version 13.1 build 48.x.

Lorsque vous configurez la méthode d'équilibrage de charge de proximité statique, un serveur est choisi en fonction de l'adresse IP du client plutôt que de l'adresse IP de bouclage NetScaler. Par conséquent, le temps de réponse peut être plus long. Le paramètre proximity from self, lorsqu'il est activé, garantit que la demande est envoyée au serveur le plus proche de NetScaler à l'aide de l'adresse IP de bouclage NetScaler. La définition de ce paramètre sur OUI accélère le temps de réponse si les serveurs sont situés plus près du NetScaler que du client.

Conditions préalables

Sélectionnez la proximité statique comme méthode d'équilibrage de charge

Pour configurer le paramètre ProximityFromSelf à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le paramètre ProximityFromSelf et vérifier la configuration

```
set lbparameter -proximityFromSelf <NO/YES>
show lbparameter

<!--NeedCopy-->
```

Exemple :

```
set lbparameter -proximityFromSelf Yes
<!--NeedCopy-->
```


Pour configurer le paramètre Proximity from Self à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge**.
2. Sur la page Équilibrage de charge, sous la section **Paramètres**, cliquez sur **Modifier les paramètres d'équilibrage de charge**.
3. Sélectionnez **Proximity from Self**.
4. Cliquez sur **OK**.

Moniteurs intégrés

May 5, 2023

L'appliance NetScaler contient divers moniteurs intégrés que vous pouvez utiliser pour surveiller vos services. Ces moniteurs intégrés gèrent la plupart des protocoles courants. Ils offrent des options permettant de modifier certains paramètres, tels que l'intervalle, le délai de réponse pour répondre à vos besoins. Toutefois, vous ne pouvez pas modifier le nom et le protocole du moniteur. Pour plus d'informations, voir Modification des moniteurs. Vous pouvez également lier un moniteur intégré à un service et le dissocier du service.

> **Remarque**
>
> Vous pouvez créer un moniteur personnalisé basé sur un moniteur intégré. Pour savoir comment créer des moniteurs personnalisés, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des applications basée sur TCP

May 5, 2023

L'appliance NetScaler possède deux moniteurs intégrés qui surveillent les applications basées sur le protocole TCP : et. `tcp-default` `ping-default` Lorsque vous créez un service, le moniteur par défaut approprié lui est automatiquement lié, de sorte que le service peut être utilisé immédiatement s'il est UP. Le moniteur TCP par défaut est lié à tous les services TCP. Le moniteur Ping-Default est lié à tous les services autres que TCP.

Vous ne pouvez ni supprimer ni modifier les moniteurs par défaut. Lorsque vous liez un autre moniteur à un service TCP, le moniteur par défaut est indépendant du service. Le tableau suivant répertorie les types de moniteurs, ainsi que les paramètres et les processus de surveillance associés à chaque type.

Type de moniteur	Paramètres spécifiques	Processus
tcp	Non applicable	L'appliance NetScaler établit une liaison tridirectionnelle avec la destination du moniteur, puis ferme la connexion. Si l'appliance observe le trafic TCP vers la destination, elle n'envoie pas de demandes de surveillance TCP. Cela se produit si LRTM est désactivé. Par défaut, LRTM est désactivé sur ce moniteur.
http	httprequest ["HEAD/"] - Requête HTTP envoyée au service. respcode [200] - Un ensemble de codes de réponse HTTP est attendu du service.	L'appliance NetScaler établit une liaison tridirectionnelle avec la destination du moniteur. Une fois la connexion établie, l'appliance envoie des requêtes HTTP, puis compare le code de réponse avec l'ensemble de codes de réponse configuré.
tcp-ecv	send [""] : ce sont les données qui sont envoyées au service. La longueur maximale autorisée de la chaîne est de 512 octets. recv [""] - réponse attendue du service. La longueur maximale autorisée de la chaîne est de 128 octets. Le dernier caractère est une terminaison NULL.	L'appliance NetScaler établit une liaison tridirectionnelle avec la destination du moniteur. Lorsque la connexion est établie, l'appliance utilise le paramètre d'envoi pour envoyer des données spécifiques au service et attend une réponse spécifique via le paramètre de réception. Différents serveurs envoient des segments de tailles différentes. Toutefois, le motif doit se situer dans 16 segments TCP.

Type de moniteur	Paramètres spécifiques	Processus
http-ecv	send [””] - données HTTP envoyées au service ; recv [””] - les données de réponse HTTP attendues du service	L'appliance NetScaler établit une liaison tridirectionnelle avec la destination du moniteur. Lorsque la connexion est établie, l'appliance utilise le paramètre send pour envoyer les données HTTP au service et attend la réponse HTTP spécifiée par le paramètre de réception. (partie du corps HTTP sans inclure les en-têtes HTTP). Les données de réponse vides correspondent à n'importe quelle réponse. Les données attendues peuvent se trouver n'importe où dans les 24 000 premiers octets du corps HTTP de la réponse.
ping	Sans objet	L'appliance NetScaler envoie une demande d'écho ICMP à la destination du moniteur et attend une réponse d'écho ICMP.

Pour configurer des moniteurs intégrés pour des applications basées sur TCP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Pour configurer des moniteurs basés sur TCP à l'aide de CLI

Exécutez la commande suivante :

```
1 add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
     <string> -resptimeout <integer> [<units>] -retries <integer> -
     downTime <integer> [<units>] -action <action>
2 <!--NeedCopy-->
```


Exemple pour le type de moniteur TCP :

```
add lb monitor Exch2010-RPC-AddressBook TCP -LRTM ENABLED -interval 10
    -resptimeout 5 -destPort 59601
<!--NeedCopy-->
```

Exemple de type de moniteur HTTP :

```
add lb monitor Mon_S4B_FE_2 HTTP -respCode 200 -httpRequest "GET /
    Autodiscover/XFrame/XFrame.html" -LRTM ENABLED -retries 10 -secure
    YES
<!--NeedCopy-->
```

Exemple pour le type de moniteur HTTP-ECV :

```
add lb monitor STM_EXC2016_SSLBridge_MON HTTP-ECV -send "GET /owa/
    healthcheck.htm" -recv "200 OK" -LRTM ENABLED -destPort 443 -secure
    YES
<!--NeedCopy-->
```

Exemple de type de moniteur PING :

```
add lb monitor lbmon-localhost-ping PING -LRTM DISABLED -destIP
    127.0.0.1
<!--NeedCopy-->
```

Surveillance des services SSL

June 20, 2023

L'appliance NetScaler intègre des moniteurs sécurisés, un protocole TCPS et un protocole HTTPS. Vous pouvez utiliser les moniteurs sécurisés pour surveiller le trafic HTTP et non HTTP. Pour configurer un moniteur HTTP sécurisé, sélectionnez le type de moniteur HTTP et définissez l'indicateur de sécurité. Pour configurer un moniteur TCP sécurisé, sélectionnez le type de moniteur TCP et définissez l'indicateur de sécurité. Les moniteurs sécurisés fonctionnent comme suit :

- **Surveillance TCP sécurisée.** L'appliance NetScaler établit une connexion TCP. Une fois la connexion établie, l'appliance établit une liaison SSL avec le serveur. Une fois la poignée de main terminée, l'appliance ferme la connexion.
- **Surveillance HTTP sécurisée.** L'appliance NetScaler établit une connexion TCP. Une fois la connexion établie, l'appliance établit une liaison SSL avec le serveur. Lorsque la connexion SSL est établie, l'appliance envoie des requêtes HTTP via le canal crypté et vérifie les codes de réponse.

Le tableau suivant décrit les moniteurs intégrés disponibles pour surveiller les services SSL.

Type de moniteur	Sonde	Critères de réussite (condition directe)
TCP	Connexion TCP ; prise de contact SSL	Connexion TCP établie et prise de contact SSL réussie.
HTTP	Connexion TCP ; établissement de contact SSL ; requête HTTP cryptée	Une connexion TCP réussie est établie, une prise de contact SSL réussie est effectuée et le code de réponse HTTP attendu dans la réponse HTTP du serveur est crypté.
TCP-ECV	Connexion TCP. Poignée de contact SSL (Les données envoyées à un serveur sont chiffrées.)	Une connexion TCP réussie est établie, une liaison SSL réussie est effectuée et les données TCP attendues sont reçues du serveur.
HTTP-ECV	Connexion TCP ; prise de contact SSL (requête HTTP cryptée)	Une connexion TCP réussie est établie, une prise de contact SSL réussie est effectuée et les données HTTP attendues sont reçues du serveur.

Exemple de configuration pour le moniteur de vérification de l'état HTTP-ECV

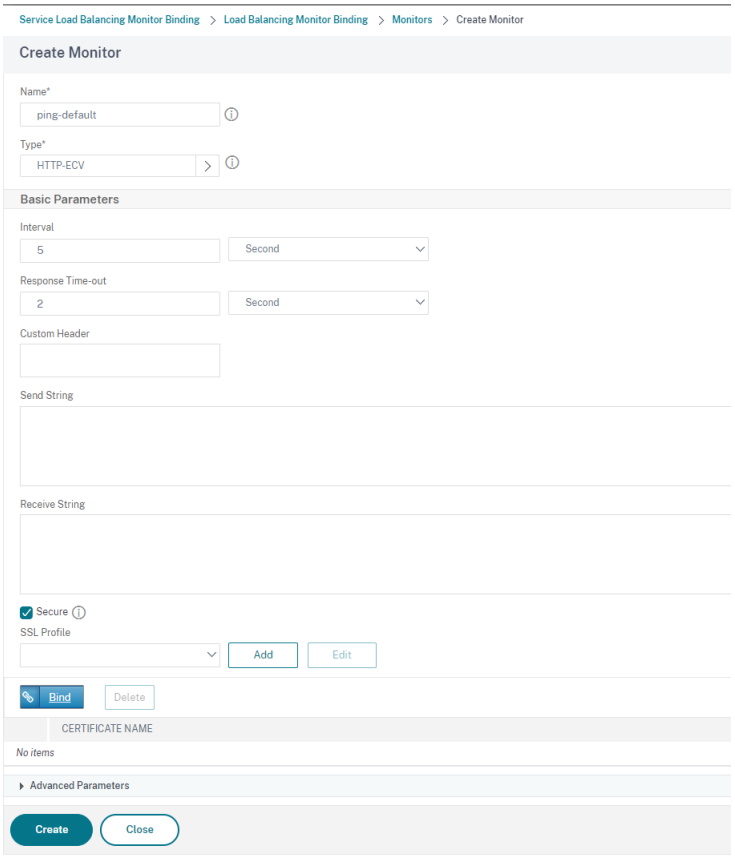
Les services HTTP disposent de moniteurs prédéfinis capables d'effectuer la vérification étendue du contenu (ECV).
Ces moniteurs sont utilisés lorsqu'une validation est requise au-delà d'une connexion TCP réussie. Ces moniteurs valident le service comme étant opérationnel, lorsque tous les critères suivants sont remplis :

- Une connexion TCP réussie.
- Un type de demande particulier doit être généré.
- Un message spécifique est attendu en réponse à partir de la **chaîne de réception**.

Pour ces moniteurs, une chaîne de demande est configurée avec une chaîne de réponse. Si la chaîne de réponse reçue par le moniteur NetScaler correspond à la chaîne configurée, le service est balisé.

Liez un moniteur à un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, créez un service et spécifiez le protocole **SSL**. Cliquez sur **OK**.
2. Cliquez dans le volet **Service to Load Balancing Monitor Binding**, puis cliquez sur **Ajouter une liaison**.
3. Choisissez le type de moniteur **HTTP-ECV** et cliquez sur **Modifier**.
4. Dans le volet **Configurer le moniteur**, sous l'onglet **Paramètres de base**, entrez les valeurs des paramètres suivants :
   - **Send String** — Chaîne que le moniteur doit envoyer au service.
   - **Chaîne de réception** : chaîne que le moniteur doit recevoir pour marquer le service comme étant actif.



5. Cliquez sur **OK** pour terminer la configuration du moniteur.
6. Cliquez sur **Sélectionner**.
7. Cliquez sur **Lier** pour lier le moniteur **HTTP-ECV** au service.
8. Cliquez sur **Fermer**.

Créer et lier un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb monitor <monitor-name> http-ecv
bind service <servicename> -monitorName <monitor-name>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor monitor-1 http-ecv
bind service services1 -monitorName monitor-1
<!--NeedCopy-->
```

Surveillance du service HTTP/2

May 5, 2023

L'appliance NetScaler prend en charge les moniteurs HTTP/2 pour surveiller l'état de santé des services HTTP/2.

Le moniteur HTTP/2 peut être configuré de deux manières différentes. Selon le type de trafic, vous pouvez configurer un moniteur HTTP/2.

- **HTTP/2 Direct.** Vous pouvez configurer HTTP/2 Direct pour surveiller les services HTTP/2 non sécurisés.
- **HTTP/2 SSL.** Vous pouvez configurer SSL HTTP/2 pour surveiller le trafic sécurisé via SSL. Activez le paramètre Secure Flag dans le HTTP/2 pour surveiller le trafic SSL.

Le http2direct et http2ssl sont les deux moniteurs intégrés différents pris en charge par le protocole HTTP/2.

Le tableau suivant répertorie les types de configuration et les processus de surveillance associés à chaque type.

Type de configuration	Sonde	Les critères de succès
HTTP/2 Direct	Connexion TCP ; préface de connexion HTTP2 et négociation des paramètres ; demande HTTP2	Le code d'état de réponse HTTP/2 doit correspondre au code de réponse configuré.

Type de configuration	Sonde	Les critères de succès
HTTP/2 SSL	Connexion TCP ; Handshake SSL ; préface de connexion HTTP2 & Négociation des paramètres ; demande HTTP2	Le serveur doit toujours sélectionner `ALPN` avec le protocole HTTP/2 et le code d'état de réponse HTTP/2 doit correspondre au code de réponse configuré.

Liez le moniteur HTTP/2 à un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `bind service <servicename> -monitorName <name>`
- `bind service <servicename> -monitorName <name>`

Exemple :

- `bind service s1 -monitorName http2direct`
- `bind service s2 -monitorName http2ssl`

Surveillance du service de protocole proxy

May 5, 2023

L'appliance NetScaler dotée d'un protocole proxy prend en charge la vérification du moniteur. La vérification du moniteur garantit que le serveur principal prend également en charge le protocole proxy. L'appliance NetScaler possède quatre types de moniteurs intégrés pour les services liés au HTTP ou au TCP : HTTP, HTTPS, HTTP-ECV et TCP-ECV.

Le tableau suivant répertorie les types de moniteurs, ainsi que les paramètres et les processus de surveillance associés à chaque type.

Type de configuration	Sonde	Les critères de succès
HTTP	`httprequest` [« HEAD/»] : requête HTTP envoyée au service. `respcode` [200] - Un ensemble de codes de réponse HTTP est attendu du service.	L'appliance NetScaler établit une liaison tridirectionnelle avec la destination du moniteur. Une fois la connexion établie, l'appliance envoie des requêtes HTTP, puis compare le code de réponse avec l'ensemble de codes de réponse configuré.
HTTPS	`httprequest` [« HEAD/»] : requête HTTPS envoyée au service. `respcode` [200] - Un ensemble de codes de réponse HTTPS est attendu du service.	L'appliance NetScaler établit une liaison tridirectionnelle avec la destination du moniteur. Une fois la connexion établie, l'appliance envoie des requêtes HTTPS, puis compare le code de réponse à l'ensemble de codes de réponse configuré.

Type de configuration	Sonde	Les critères de succès
HTTP-ECV	send [» »] : données HTTP envoyées au service. Reçu [» »] : les données de réponse HTTP attendues du service	L'appliance NetScaler établit une liaison tridirectionnelle avec la destination du moniteur. Lorsque la connexion est établie, l'appliance utilise le paramètre send pour envoyer les données HTTP au service et attend la réponse HTTP spécifiée par le paramètre de réception. (partie du corps HTTP sans inclure les en-têtes HTTP). Les données de réponse vides correspondent à n'importe quelle réponse. Les données attendues peuvent se trouver n'importe où dans les 24 000 premiers octets du corps HTTP de la réponse.
TCP-ECV	send [» »] - sont les données qui sont envoyées au service. La longueur maximale autorisée de la chaîne est de 512 K octets. reçu [» »] - la réponse attendue du service. La longueur maximale autorisée de la chaîne est de 128 K octets.	L'appliance NetScaler établit une liaison tridirectionnelle avec la destination du moniteur. Lorsque la connexion est établie, l'appliance utilise le paramètre d'envoi pour envoyer des données spécifiques au service et attend une réponse spécifique via le paramètre de réception. Différents serveurs envoient des segments de tailles différentes. Toutefois, le motif doit se situer dans 16 segments TCP.

Vous pouvez configurer le moniteur de protocole proxy à l'aide de `netprofile`.

Configuration du moniteur de protocole proxy à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

1. Ajouter un profil réseau avec le protocole proxy activé

   ```
   add netprofile <name> -proxyProtocol ( ENABLED | DISABLED )
   ```

Exemple :

```
1 add netprofile profile1 - proxyProtocol ENABLED
```

1. Liez le profil réseau à un service.

   ```
   set service <name> -netprofile <netprofile-name>
   ```

Exemple :

```
1 set service S1 - netprofile profile1
```

> **Remarque**
>
> Vous pouvez exécuter la commande précédente si vous souhaitez que le profil réseau soit lié à un service.

1. Liez le profil net à un moniteur.

   ```
   set lb monitor <monitor-name> <type> -netprofile <netprofile-name>
   ```

Exemple :

```
1 set lb monitor http1 HTTPS - netprofile profile1
```

> **Remarque**
>
> - Vous pouvez exécuter la commande précédente si vous souhaitez que le profil réseau soit lié à un moniteur.
> - Vous pouvez sélectionner le type de moniteur de votre choix. Il peut s'agir de HTTP, HTTPS, TCP-ECV ou HTTP-ECV.
>
> **Important**
>
> - Dans un cas général, le profil réseau (protocole proxy activé) lié à un service est pris en compte.

> - Si le profil réseau est lié à la fois au moniteur et au service, le profil net lié à la surveillance est pris en compte. Le profil réseau lié au service est ignoré.

Surveillance des services FTP

May 5, 2023

Pour surveiller les services FTP, l'appliance NetScaler ouvre deux connexions au serveur FTP. Il se connecte d'abord au port de contrôle, qui est utilisé pour transférer des commandes entre un client et un serveur FTP. Après avoir reçu la réponse attendue, il se connecte au port de données, qui est utilisé pour transférer des fichiers entre un client et un serveur FTP. Ce n'est que lorsque le serveur FTP répond comme prévu, sur les deux connexions, qu'il est marqué.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

L'appliance NetScaler possède deux moniteurs intégrés pour les services FTP : le moniteur FTP et le moniteur FTP-EXTENDED. Le moniteur FTP-EXTENDED est un moniteur scriptable. Il utilise le script nsftp.pl. Le script de surveillance FTP-EXTENDED est amélioré pour envoyer des sondes sécurisées aux services FTP. Vous pouvez créer un moniteur de type FTP-EXTENDED. Le script nsftp.pl est automatiquement extrait du répertoire par défaut.

Pour envoyer des sondes FTP sécurisées aux services FTP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add lb monitor <monitorName> <type> -username <string> -password <
     string> -filename <filename>
2 <!--NeedCopy-->
```

Exemple

```
1 add monitor mon1 FTP-EXTENDED -username root -password freebsd -
     filename fsdf
2 <!--NeedCopy-->
```

Pour envoyer des sondes FTP sécurisées à des services FTP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**.
2. Spécifiez le type de moniteur comme **FTP-EXTENDED**et définissez les paramètres.

3. Dans **Paramètres spéciaux**, spécifiez un nom de **fichier, un nomd'utilisateur**et un**mot de passe**.

Pour configurer des moniteurs intégrés afin de vérifier l'état des services FTP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance sécurisée des serveurs à l'aide de SFTP

May 5, 2023

Un script utilisateur « nssftp.pl » a été ajouté pour prendre en charge la surveillance du protocole SFTP (SSH File Transfer Protocol). Il est disponible dans la liste actuelle des moniteurs utilisateur NetScaler intégrés et se trouve dans le répertoire /netscaler/monitors. Le moniteur SFTP utilise le nom d'utilisateur et le mot de passe spécifiés pour vérifier si le fichier est présent sur le serveur.

Pour configurer la surveillance sécurisée à l'aide de SFTP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
   string> -secure ( YES | NO )
<!--NeedCopy-->
```

Exemple :

```
add monitor SFTP_MON USER -scriptname nssftp.pl -scriptargs "file=
   example.txt;user=sam;password=sam_passwd"
<!--NeedCopy-->
```

Pour configurer la surveillance sécurisée à l'aide du protocole SFTP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs** et, dans **Type**, spécifiez **UTILISATEUR**.
2. Dans **Paramètres spéciaux**, dans **Nom du script**, sélectionnez nssftp.pl.
3. Spécifiez les **arguments de script**.

Définir les paramètres SSL sur un moniteur sécurisé

August 20, 2021

> **Important**
>
> Cette fonctionnalité est prise en charge uniquement sur les nouveaux profils par défaut. Pour plus d'informations sur ces profils, consultez Présentation de l'infrastructure des profils SSL améliorés.

Un moniteur hérite des paramètres globaux ou du service auquel il est lié. Si un moniteur est lié à un service non SSL ou non SSL_TCP, tel que SSL_BRIDGE, vous ne pouvez pas le configurer avec des paramètres SSL tels que la version du protocole ou les chiffrements à utiliser. Par conséquent, si votre déploiement nécessite une surveillance SSL des serveurs back-end, la surveillance est inefficace.

Vous pouvez avoir plus de contrôle sur la surveillance basée sur SSL des serveurs back-end, en liant un profil SSL à un moniteur. Un profil SSL contient des paramètres SSL, des liaisons chiffrées et des liaisons ECC. Par exemple, vous pouvez définir l'authentification du serveur, les chiffrements et la version du protocole dans un profil SSL et lier le profil à un moniteur. Pour effectuer l'authentification du serveur, vous devez également lier un certificat d'autorité de certification à un moniteur. Pour effectuer l'authentification du client, vous devez lier un certificat client au moniteur. De nouveaux paramètres pour la commande « bind lb monitor » vous permettent de le faire.

> **Remarque**
>
> Les paramètres SSL ne prennent effet que si vous ajoutez un moniteur sécurisé. En outre, le type de profil SSL doit être **BackEnd**.

Types de surveillance prenant en charge les profils SSL

Les profils SSL peuvent être liés aux types de moniteurs suivants :

- HTTP
- HTTP-ECV
- TCP
- TCP-ECV
- HTTP-INLINE

Pour spécifier un profil SSL lors de l'ajout d'un moniteur à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
add lb monitor <monitorName> <type> -secure  YES   -sslprofile <string>
```



```
set lb monitor <monitorName> <type> -secure YES -sslprofile <string>
<!--NeedCopy-->
```

Exemple :

```
add ssl profile prof1 -sslProfileType  BackEnd

add lb monitor mon1 HTTP -secure  YES -sslprofile prof1
<!--NeedCopy-->
```

Pour lier une paire de clés de certificat à un moniteur à l'aide de la ligne de commande

À l'invite de commandes, tapez :

```
bind monitor  <monitor name> -certkeyName <string>  [(-CA  [-crlCheck (
    Mandatory | Optional ) | -ocspCheck ( Mandatory | Optional )]
<!--NeedCopy-->
```

Surveillance des services SIP

May 5, 2023

Un NetScaler possède deux moniteurs intégrés que vous pouvez utiliser pour surveiller les services SIP : les moniteursSIP-UDP et SIP-TCP**.** Un moniteur SIP vérifie périodiquement le service SIP auquel le moniteur SIP est lié, en envoyant des méthodes de demande SIP au service SIP. Si le service SIP répond par un code de réponse, le moniteur marque le service comme étant actif. Si le service SIP ne répond pas ou ne répond pas correctement, il est marqué comme étant en panne.

Paramètre	Spécifie
SiPuri	Schéma d'adressage SIP du serveur SIP.
`sipmethod`	Type de demande SIP utilisée pour sonder le service SIP. Spécifiez l'une des méthodes suivantes : INVITE, OPTION (valeur par défaut), REGISTER
`respcode`	Code de réponse SIP avec lequel le service SIP répond à la demande de sonde. Par défaut : 200.

Surveillance des services RADIUS

May 5, 2023

Le moniteur RADIUS de l'appliance NetScaler vérifie régulièrement l'état du service RADIUS auquel il est lié en envoyant une demande d'authentification au service. Le serveur RADIUS authentifie le moniteur RADIUS et envoie une réponse. Par défaut, le moniteur s'attend à recevoir un code de réponse de la valeur 2, la réponse d'acceptation d'accès par défaut, de la part du serveur RADIUS. Tant que le moniteur reçoit la réponse appropriée, il marque le service comme étant actif.

Remarque : Le moniteur RADIUS prend uniquement en charge l'authentification de type PAP.

- Si le client s'est authentifié avec succès, le serveur RADIUS envoie une réponse d'acceptation d'accès. Le code de réponse d'acceptation d'accès par défaut est 2, et il s'agit du code utilisé par l'appliance.
- Si le client ne parvient pas à s'authentifier correctement (par exemple en cas de non-concordance entre le nom d'utilisateur, le mot de passe ou la clé secrète), le serveur RADIUS envoie une réponse de rejet d'accès. Le code de réponse de rejet d'accès par défaut est 3, et il s'agit du code utilisé par l'appliance.

Paramètre	Spécifie
`userName`	Nom d'utilisateur sur le serveur RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3. Ce nom d'utilisateur est utilisé dans la sonde.
mot de passe	Mot de passe utilisé pour surveiller les serveurs RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP.
Clé RadKey	Valeur de clé secrète partagée que le serveur RADIUS utilise lors de l'authentification du client.
Radna Sid	NAS-ID qui est encapsulé dans la charge utile lorsqu'une demande d'accès est faite.
Rad Nasip	Adresse IP qui est encapsulée dans la charge utile lorsqu'une demande d'accès est faite. Lorsque RadNASip n'est pas configuré, l'appliance NetScaler envoie l'adresse IP mappée (MIP) au serveur RADIUS en tant qu'adresse IP du NAS.

Pour surveiller un service RADIUS, vous devez configurer le serveur RADIUS auquel il est lié comme suit :

1. Ajoutez le nom d'utilisateur et le mot de passe du client que le moniteur utilise pour l'authentification à la base de données d'authentification RADIUS.
2. Ajoutez l'adresse IP et la clé secrète du client à la base de données RADIUS appropriée.
3. Ajoutez les adresses IP utilisées par l'appliance pour envoyer des paquets RADIUS à la base de données RADIUS. Si l'appliance NetScaler possède plusieurs adresses IP mappées ou si une adresse IP de sous-réseau (SNIP) est utilisée, vous devez ajouter la même clé secrète pour toutes les adresses IP.

   Attention : Si l'adresse IP utilisée par l'appliance n'est pas ajoutée à la base de données RADIUS, le serveur RADIUS rejette tous les paquets.

Pour configurer des moniteurs intégrés afin de vérifier l'état du serveur RADIUS, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveiller la diffusion des informations comptables à partir d'un serveur RADIUS

May 5, 2023

Vous pouvez configurer un moniteur appelé moniteur de *comptabilité RADIUS* pour déterminer si le serveur RADIUS utilisé pour l'authentification, l'autorisation et la comptabilité (NetScaler AAA) fournit les informations de comptabilité comme prévu. Le moniteur est de type RADIUS_ACCOUNTING. La sonde est générée par un script Perl appelé nsbmradius.pl, qui se trouve dans le répertoire /nsconfig/monitors/. Le script envoie des sondes de demande de comptabilité successives au serveur RADIUS. La sonde est considérée comme réussie uniquement si le serveur de gestion RADIUS répond par un paquet dont le champ Code est défini sur 5, ce qui, selon la RFC 2866, indique un paquet de réponse comptable.

Lors de la configuration d'un moniteur de comptabilité RADIUS, vous devez spécifier une clé secrète. Vous pouvez spécifier des paramètres facultatifs, dont chacun représente un attribut RADIUS, tels que Acct-Status-Type et Framed-IP-Address. Pour plus d'informations sur ces attributs, consultez la RFC 2865, « Remote Authentication Dial In User Service (RADIUS) » et la RFC 2866, « RADIUS Accounting ». «

Pour configurer un moniteur de comptabilité RADIUS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur de comptabilité RADIUS et vérifier la configuration :

```
add lb monitor <monitorName> RADIUS_ACCOUNTING [-userName <string>] {
 -password  }
  {
 -radKey  }
  [-radNASip <ip_addr>] [-radAccountType <positive_integer>] [-
     radFramedIP <ip_addr>] [-radAPN <string>] [-radMSISDN <string>] [-
     radAccountSession <string>]

show lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple

```
add lb monitor radAccntMon RADIUS_ACCOUNTING -radKey "8d#>9jr4rV)L7%a2-
   zW13sM"
<!--NeedCopy-->
```

Surveillance des services DNS et DNS-TCP

May 5, 2023

L'appliance NetScaler possède deux moniteurs intégrés qui peuvent être utilisés pour surveiller les services DNS : DNS et DNS-TCP. Lorsqu'il est lié à un service, l'un ou l'autre des moniteurs vérifie régulièrement l'état de ce service DNS en lui envoyant une requête DNS. La requête renvoie à une adresse IPv4 ou IPv6. Cette adresse IP est ensuite comparée à la liste des adresses IP de test que vous configurez. La liste peut contenir jusqu'à cinq adresses IP. Si l'adresse IP résolue correspond à au moins une adresse IP de la liste, le service DNS est marqué comme actif. Si l'adresse IP résolue ne correspond à aucune adresse IP de la liste, le service DNS est marqué comme étant inactif.

Paramètre	Description
requête	Requête DNS (nom de domaine) envoyée au service DNS surveillé. Valeur par défaut : « \ 007 » Si la requête DNS réussit, le service est marqué comme UP. Sinon, il est marqué comme DOWN. Pour un moniteur inversé, si la requête DNS réussit, le service est marqué comme DOWN. Sinon, il est marqué comme UP. Si aucune réponse n'est reçue, le service est marqué comme étant DOWN.
Type de requête	Type de requête DNS qui est envoyée. Valeurs possibles : Adresse, Zone.
`IPAddress`	Liste des adresses IP vérifiées par rapport à la réponse à la sonde de surveillance DNS.
IPv6	Activez cette case à cocher si l'adresse IP utilise le format IPv6.

Pour configurer les moniteurs DNS ou DNS-TCP intégrés, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des services LDAP

May 5, 2023

L'appliance NetScaler possède un moniteur intégré qui peut être utilisé pour surveiller les services LDAP : le moniteur LDAP. Il vérifie régulièrement le service LDAP auquel il est lié en s'authentifiant et en lui envoyant une requête de recherche. Si la recherche aboutit, le service est balisé. Si le serveur LDAP ne trouve pas l'entrée, un message d'échec est envoyé au moniteur LDAP et le service est marqué comme DOWN.

Configurez le moniteur LDAP pour définir la recherche qu'il doit effectuer lors de l'envoi d'une requête. Vous pouvez utiliser le paramètre DN de base pour spécifier un emplacement dans la hiérarchie d'annuaires où le serveur LDAP doit démarrer la requête de test. Vous pouvez utiliser le paramètre Attribute pour spécifier un attribut de l'entité cible.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
Basé sur N	Nom de base du moniteur LDAP à partir duquel la recherche LDAP doit commencer. Si le serveur LDAP s'exécute localement, la valeur par défaut de base est dc=`netscaler`, dc=com.
bindDN	Nom BDN du moniteur LDAP.
filtre	Filtre pour le moniteur LDAP. Utilisez le paramètre de filtre dans une requête pour limiter le nombre de résultats. Si vous ne spécifiez pas ce paramètre dans la requête, le filtre s'applique à l'ensemble de la classe d'objets, ce qui peut s'avérer coûteux, comme une utilisation élevée du processeur.
mot de passe	Mot de passe utilisé pour la surveillance des serveurs LDAP.
attribut	Attribut du moniteur LDAP.

Pour configurer le moniteur LDAP intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des services MySQL

May 5, 2023

L'appliance NetScaler possède un moniteur intégré qui peut être utilisé pour surveiller les services MySQL : le moniteur MySQL. Il vérifie régulièrement le service MySQL auquel il est lié en lui envoyant une requête de recherche. Si la recherche aboutit, le service est balisé. Si le serveur MySQL ne répond pas ou si la recherche échoue, un message d'échec est envoyé au moniteur MySQL et le service est marqué comme étant inactif.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
base de données	Base de données utilisée pour le moniteur MySQL.
Requête SQL	Requête SQL utilisée pour le moniteur MySQL.

Pour configurer un moniteur MySQL intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Pour configurer des moniteurs MySQL à l'aide de la CLI

Exécutez la commande suivante :

```
add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
    string>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor mysql1 USER -scriptName nsmysql.pl -scriptArgs "database
    =cloud;user=cloud;password=password;query=show tables from cloud"
<!--NeedCopy-->
```

Surveillance des services SNMP

May 5, 2023

L'appliance NetScaler possède un moniteur intégré qui peut être utilisé pour surveiller les services SMNP : le moniteur SNMP. Il vérifie régulièrement l'agent SNMP sur le service auquel il est lié en envoyant une requête concernant l'ID d'identification d'entreprise (OID) que vous configurez pour la surveillance. Si la requête aboutit, le service est balisé. Si le service SNMP trouve l'OID que vous avez spécifié, la requête aboutit et le moniteur SNMP marque le service comme étant ouvert. S'il ne trouve pas l'OID, la requête échoue et le moniteur SNMP marque le service comme étant inactif.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
IDENTIFIANT SNMP	OID utilisé pour le moniteur SNMP.

Paramètre	Spécifie
Communauté SNMP	Communauté utilisée pour le moniteur SNMP.
Seuil SNMP	Seuil utilisé pour le moniteur SNMP.
Version SNMP	Version SNMP utilisée pour la surveillance de la charge. Valeurs possibles : V1, V2.

Pour configurer le moniteur SNMP intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des services NNTP

May 5, 2023

L'appliance NetScaler possède un moniteur intégré qui peut être utilisé pour surveiller les services NNTP : le moniteur NNTP. Il vérifie régulièrement le service NNTP auquel il est lié en se connectant au service et en vérifiant l'existence du groupe de discussion que vous spécifiez. Si le groupe de discussion existe, la recherche est réussie et le service est marqué. Si le service NNTP ne répond pas ou si la recherche échoue, le service est marqué comme étant inactif.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Le moniteur NNTP peut également être configuré pour publier un message de test dans le groupe de discussion.

Paramètre	Spécifie
`userName`	Nom d'utilisateur sur le serveur RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3. Ce nom d'utilisateur est utilisé dans la sonde.
mot de passe	Mot de passe utilisé pour surveiller les serveurs RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP.
groupe	Nom du groupe à interroger pour le moniteur NNTP.

Pour configurer le moniteur NNTP intégré, reportez-vous à la section Configuration des moniteurs

dans une configuration d'équilibrage de charge.

Surveillance des services POP3

May 5, 2023

L'appliance NetScaler possède un moniteur intégré qui peut être utilisé pour surveiller les services POP3 : le moniteur POP3. Il vérifie régulièrement le service POP3 auquel il est lié en ouvrant une connexion avec un serveur POP3. Si le serveur POP3 répond avec les bons codes de réponse dans le délai configuré, il marque le service comme étant ACTIF. Si le service POP3 ne répond pas ou ne répond pas correctement, il marque le service comme étant hors service.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
Nom d'utilisateur	Nom d'utilisateur du serveur POP3. Ce nom d'utilisateur est utilisé dans la sonde.
mot de passe	Mot de passe utilisé pour surveiller les serveurs POP3.
Nom du script	Le chemin et le nom du script à exécuter.
dispatcherIP	Adresse IP du répartiteur auquel la sonde est envoyée.
Port du répartiteur	Port du répartiteur vers lequel la sonde est envoyée.

Pour configurer le moniteur POP3 intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Pour configurer des moniteurs POP3 à l'aide de CLI

Exécutez la commande suivante :

```
add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
    string>
<!--NeedCopy-->
```

Exemple :


```
add lb monitor pop31 USER -scriptName nspop3.pl -scriptArgs "user=
    test@lbmon1.net;password=Freebsd123"

<!--NeedCopy-->
```

Surveillance des services SMTP

May 5, 2023

L'appliance NetScaler possède un moniteur intégré qui peut être utilisé pour surveiller les services SMTP : le moniteur SMTP. Le moniteur vérifie le service SMTP auquel il est lié en ouvrant une connexion avec lui et en effectuant une série de poignées de main pour s'assurer que le serveur fonctionne correctement. Si le service SMTP termine correctement les poignées de main, le moniteur marque le service UP. Sinon, si le service SMTP ne répond pas ou ne répond pas correctement, il marque le service DOWN.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP.

Paramètre	Spécifie
Nom du script	Le chemin et le nom du script à exécuter.
dispatcherIP	Adresse IP du répartiteur auquel la sonde est envoyée.
Port du répartiteur	Port du répartiteur vers lequel la sonde est envoyée.

Pour configurer le moniteur SMTP intégré, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des services RTSP

May 5, 2023

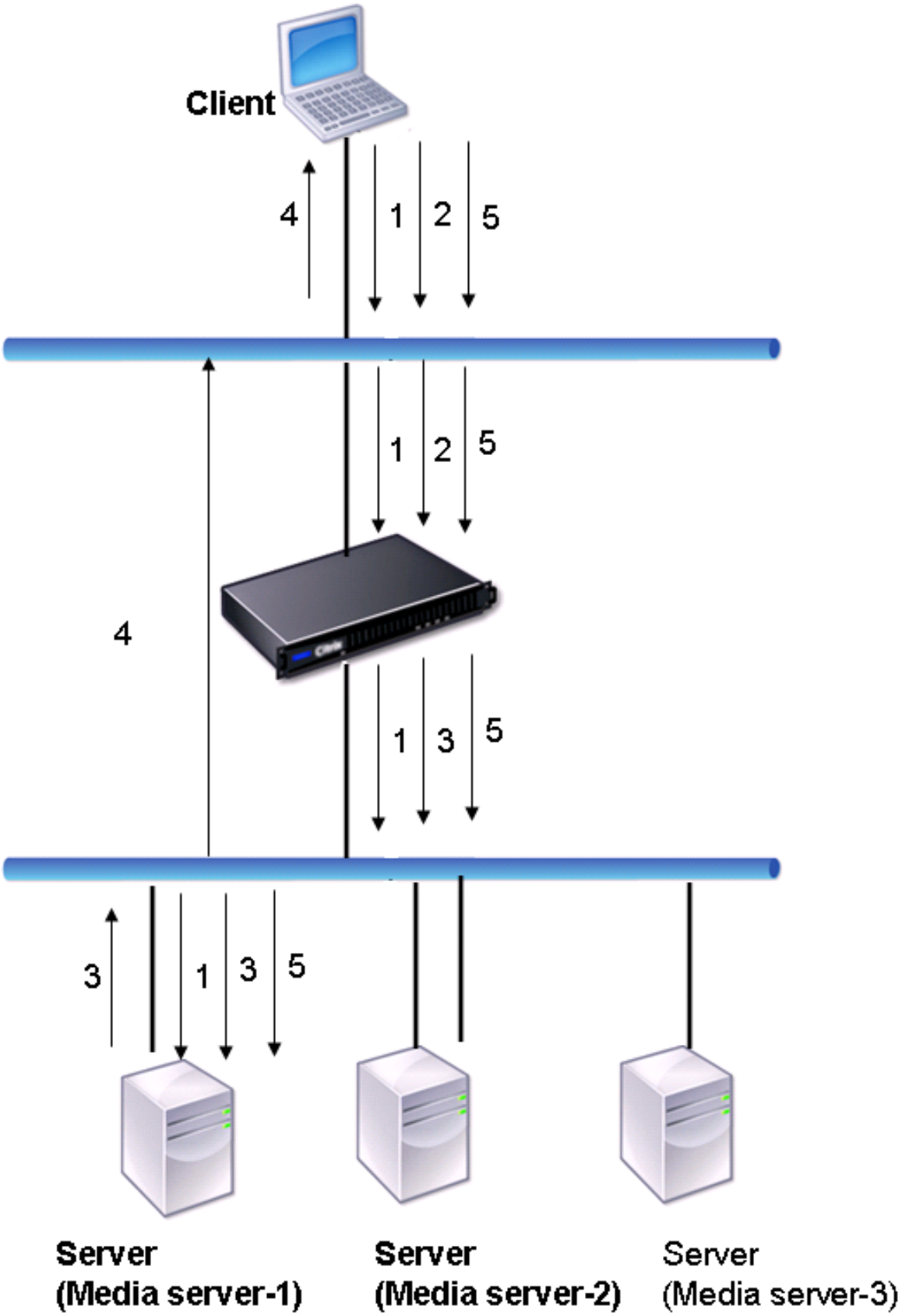
L'appliance NetScaler possède un moniteur intégré qui peut être utilisé pour surveiller les services RTSP : le moniteur RTSP. Il vérifie régulièrement le service RTSP auquel il est lié en ouvrant une connexion avec le serveur RTSP à charge équilibrée. Le type de connexion qu'il ouvre et la réponse qu'il attend varient en fonction de la configuration réseau. Si le service RTSP répond comme prévu dans

le délai configuré, il marque le service comme étant activé. Si le service ne répond pas ou ne répond pas correctement, il marque le service comme étant inactif.

L'appliance NetScaler peut être configurée pour équilibrer la charge des serveurs RTSP à l'aide de deux topologies : NAT-off et NAT-on. Les serveurs RTSP envoient leurs réponses directement au client, en contournant l'appliance. L'appliance doit être configurée pour surveiller les services RTSP différemment selon la topologie utilisée par votre réseau. L'appliance peut être déployée en mode en ligne ou non en mode NAT-off et NAT-on.

En mode NAT-off, l'appliance fonctionne comme un routeur : elle reçoit les requêtes RTSP du client et les achemine vers le service qu'elle sélectionne à l'aide de la méthode d'équilibrage de charge configurée. Si vos serveurs RTSP à équilibrage de charge se voient attribuer des FQDN accessibles au public dans le DNS, les serveurs d'équilibrage de charge envoient leurs réponses directement au client, en contournant l'appliance. La figure suivante montre cette configuration.

Figure 1. RTSP en mode NAT-off



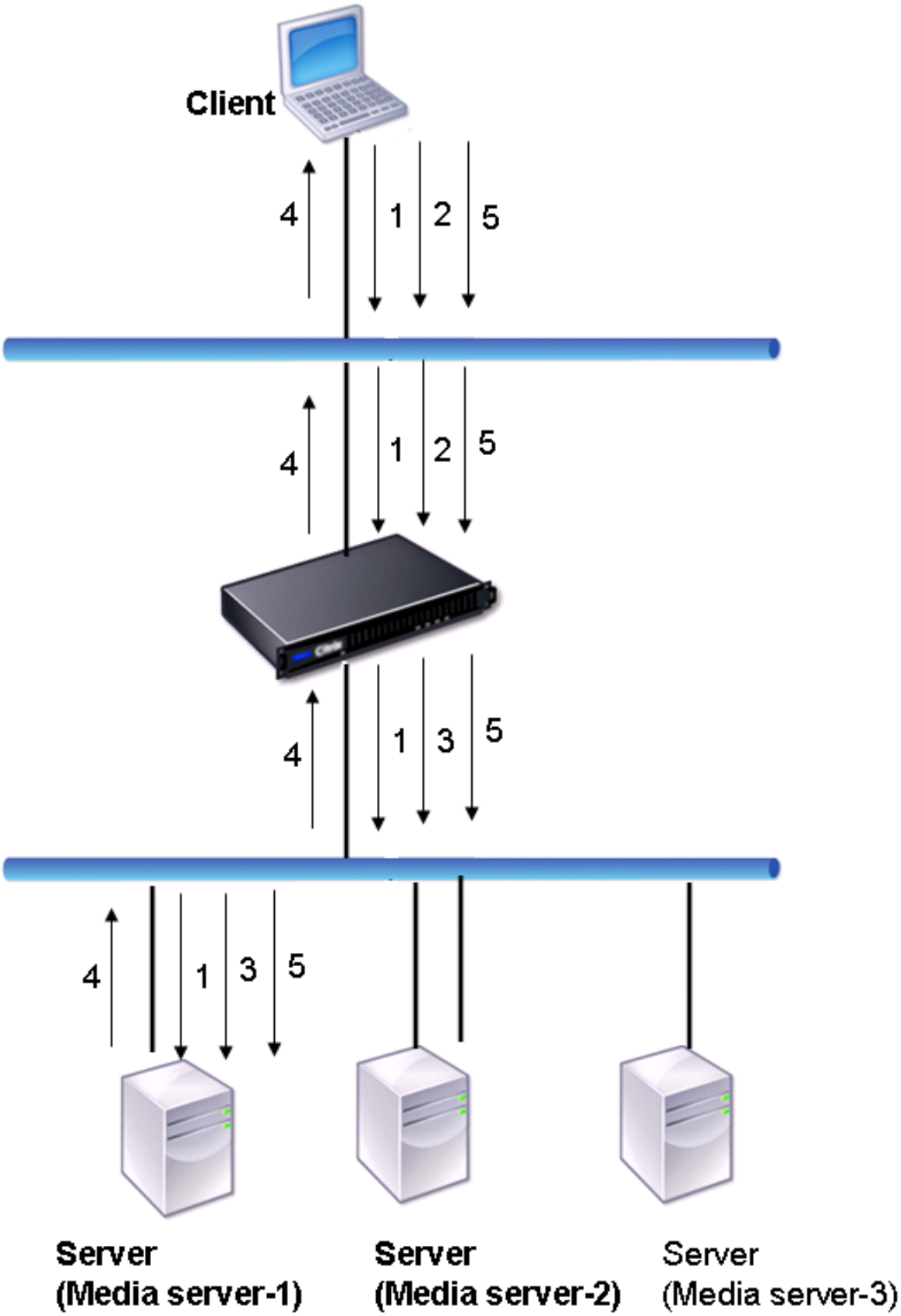
Le flux de demandes et de réponses dans ce scénario est le suivant :

1. Le client envoie une demande DESCRIBE à l'appliance. L'appliance utilise la méthode d'équilibrage de charge configurée pour choisir un service et achemine la demande vers Media Server-1.
2. Le client envoie une demande de configuration à l'appliance. Si l'ID de session RTSP est échangé dans la requête DESCRIBE, l'appliance, à l'aide de la persistance RTSPSID, achemine la demande vers Media Server-1. Si l'ID de session RTSP est échangé dans la demande SETUP, l'appliance effectue l'une des opérations suivantes :
   - Si la requête RTSP provient de la même connexion TCP, elle achemine la demande vers Media Server-1, préservant ainsi la persistance.
   - Si la demande arrive sur une connexion TCP différente, elle utilise la méthode d'équilibrage de charge configurée pour choisir un service et envoie la demande à ce service, sans maintenir la persistance. Cela signifie que la demande peut être envoyée à un autre service.
3. Media Server-1 reçoit la demande SETUP de l'appliance, alloue des ressources pour traiter la demande RTSP et envoie l'ID de session approprié au client.

   Remarque : L'appliance n'effectue pas de NAT pour identifier la connexion RTSP, car les connexions RTSP la contournent.
4. Pour les demandes suivantes, le client utilise ensuite l'ID de session pour identifier la session et envoyer des messages de contrôle au serveur multimédia. Media Server-1 exécute les actions demandées, telles que la lecture, le transfert ou le retour en arrière.

En mode NAT-on, l'appliance reçoit les demandes RTSP du client et achemine ces demandes vers le serveur multimédia approprié à l'aide de la méthode d'équilibrage de charge configurée. Le serveur multimédia envoie ensuite ses réponses au client via l'appliance, comme illustré dans le schéma suivant.

Figure 2. RTSP en mode NAT-on



Le flux de demandes et de réponses dans ce scénario est le suivant :

1. Le client envoie une demande DESCRIBE à l'appliance. L'appliance utilise la méthode d'équilibrage de charge configurée pour choisir un service et achemine la demande vers Media Server-1.
2. Le client envoie une demande de configuration à l'appliance. Si l'ID de session RTSP est échangé dans la requête DESCRIBE, l'appliance, à l'aide de la persistance RTSPSID, achemine la demande vers Media Server-1. Si l'ID de session RTSP est échangé dans la demande SETUP, l'appliance effectue l'une des opérations suivantes :
   - Si la requête RTSP provient de la même connexion TCP, elle achemine la demande vers Media Server-1, préservant ainsi la persistance.
   - Si la demande arrive sur une connexion TCP différente, elle utilise la méthode d'équilibrage de charge configurée pour choisir un service et envoie la demande à ce service, sans maintenir la persistance. Cela signifie que la demande peut être envoyée à un autre service.
3. Media Server-1 reçoit la demande SETUP de l'appliance, alloue des ressources pour traiter la demande RTSP et envoie l'ID de session approprié au client.
4. L'appliance exécute un protocole NAT pour identifier le client pour les connexions de données RTSP. Les connexions RTSP passent par l'appliance et sont routées vers le client approprié.
5. Pour les demandes suivantes, le client utilise ensuite l'ID de session pour identifier la session et envoyer des messages de contrôle à l'appliance. L'appliance utilise la persistance RTSPSID pour identifier le service approprié et achemine la demande vers Media Server-1. Media Server-1 exécute l'action demandée, telle que lire, transférer ou revenir en arrière.

Le moniteur RTSP utilise le protocole RTSP pour évaluer l'état des services RTSP. Le moniteur RTSP se connecte au serveur RTSP et exécute une série de contacts pour s'assurer que le serveur fonctionne correctement.

Paramètre	Spécifie
Requête RTSP	Chaîne de requête RTSP envoyée au serveur RTSP (par exemple, OPTIONS *). La valeur par défaut est 07. La longueur de la demande ne doit pas dépasser 163 caractères.
Code REP	Ensemble de codes de réponse attendus du service.

Pour obtenir des instructions sur la configuration d'un moniteur RTSP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance des requêtes ARP

May 5, 2023

L'appliance NetScaler possède un moniteur intégré qui peut être utilisé pour surveiller les demandes ARP : le moniteur ARP. Ce moniteur envoie régulièrement une demande ARP au service auquel il est lié et écoute la réponse attendue. S'il reçoit la réponse attendue, il marque le service comme étant actif. S'il ne reçoit aucune réponse ou s'il s'agit d'une mauvaise réponse, il marque le service comme étant inactif.

ARP localise une adresse matérielle pour un serveur à équilibrage de charge lorsque seule l'adresse de la couche réseau est connue. ARP est compatible avec IPv4 pour traduire les adresses IP en adresses MAC Ethernet. La surveillance ARP n'est pas pertinente pour les réseaux IPv6 et n'est donc pas prise en charge sur ces réseaux.

Il n'y a pas de paramètres spéciaux pour le moniteur ARP.

Pour obtenir des instructions sur la configuration d'un moniteur ARP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Surveillance du service Citrix Virtual Desktops Delivery Controller

May 5, 2023

Dans le cadre de la virtualisation des postes de travail, l'appliance NetScaler peut être utilisée pour équilibrer la charge des serveurs Citrix Virtual Desktops Delivery Controller déployés par l'environnement Citrix Virtual Desktops. L'appliance NetScaler fournit un moniteur intégré, un `CITRIX-XD-DDC` moniteur, qui surveille les serveurs Citrix Virtual Desktops Delivery Controller. Outre le contrôle de santé, vous pouvez également vérifier si la sonde est envoyée par un utilisateur valide du serveur Citrix Virtual Desktops Delivery Controller.

Le moniteur envoie une sonde au serveur Citrix Virtual Desktops Delivery Controller sous la forme d'un message XML. Si le serveur répond à la sonde en indiquant l'identité du parc de serveurs, la sonde est considérée comme réussie et l'état du serveur est marqué comme étant actif. Si la réponse HTTP ne comporte pas de code de réussite ou si l'identité de la batterie de serveurs n'est pas présente dans la réponse, la sonde est considérée comme un échec et l'état du serveur est marqué comme étant inactif.

L'option Valider les informations d'identification détermine la sonde à envoyer par le moniteur au serveur Citrix Virtual Desktops Delivery Controller, c'est-à-dire s'il convient de demander uniquement le nom du serveur ou de valider également les informations de connexion.

Remarque : Que les informations d'identification de l'utilisateur (nom d'utilisateur, mot de passe et domaine) soient spécifiées sur le moniteur
CITRIX-XD-DDC ou non, le serveur Citrix Virtual Desktops Delivery Controller ne valide les informations d'identification de l'utilisateur que si l'option de validation des informations d'identification est activée sur le moniteur.

Si vous utilisez l'assistant pour configurer l'équilibrage de charge des serveurs Citrix Virtual Desktops, le moniteur CITRIX-XD-DDC est automatiquement créé et lié aux services Citrix Virtual Desktops Delivery Controller.

Pour ajouter un moniteur XD-DDC avec l'option de validation des informations d'identification à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un moniteur XD-DDC et vérifier la configuration :

```
add lb monitor <monitorName> <monitorType> -userName <userName> -
    password <password> -domain <domain_name> -validateCred YES

show lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
 > add lb monitor xdddcmon Citrix-xd-ddc -userName Administrator -
    password E12Dc35450a1 -domain dhop -validateCred YES
 Done
> show lb monitor xdddcmon
1) Name......:xdddcmon Type......:CITRIX-XD-DDC State......: ENABLED

Standard parameters:
Interval......:..5 sec...Retries......:..3
Response timeout......:..2 sec...Down time......:..30 sec
Reverse......:..NO...Transparent......:..NO
Secure......:..NO...LRTM......:..ENABLED
Action......:..Not applicable...Deviation......:..0 sec
Destination IP......:..Bound service
Destination port......:..Bound service
Iptunnel......:..NO
TOS......:..NO...TOS ID......:..0
SNMP Alert Retries......:..0...Success Retries......:..1
Failure Retries......:..0

Special parameters:
```



```
User Name..........:"Administrator"
Password...........:*****
DDC Domain.........: "dhop"
Done
<!--NeedCopy-->
```

Pour spécifier l'option de validation des informations d'identification sur un moniteur XD-DDC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb monitor <monitorName> <monitorType> -userName -password -domain
   <domain_name> -validateCred YES
<!--NeedCopy-->
```

Exemple :

```
 set lb monitor XD_DDC_21.21.21.22_443_mn CITRIX-xd-ddc -userName
    Administrator -password D123S1R2A123 -domain dhop -validateCred YES
Done
<!--NeedCopy-->
```

Pour configurer un moniteur XD-DDC avec l'option de validation des informations d'identification à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**et créez un moniteur de type `Citrix-XD-DDC`.

Surveillance des magasins Citrix StoreFront

June 2, 2023

Vous pouvez configurer un moniteur utilisateur pour un magasin Citrix StoreFront. Le moniteur détermine l'état du magasin StoreFront en analysant successivement le service de compte, le service de découverte et le point de terminaison d'authentification (si le magasin Citrix StoreFront est un magasin authentifié). Si l'un de ces services ne répond pas à la sonde, la sonde du moniteur échoue et le magasin StoreFront est marqué comme étant DOWN. Le moniteur envoie des sondes à l'adresse IP et au port du service lié. Pour plus d'informations, consultez l' API Citrix StoreFront Store Services.

Remarque : Les sondes de surveillance proviennent de l'adresse NSIP. Toutefois, si le sous-réseau d'un serveur StoreFront est différent de celui de l'appliance, l'adresse IP du sous-réseau (SNIP) est utilisée.

À partir de la version 10.1 build 120.13, vous pouvez également lier un moniteur StoreFront à un groupe de services. Un moniteur est lié à chaque membre du groupe de services et des sondes sont envoyées à l'adresse IP et au port du membre lié (service). De plus, étant donné que chaque membre d'un groupe de services est désormais surveillé à l'aide de son adresse IP, vous pouvez désormais utiliser le moniteur StoreFront pour surveiller les nœuds de cluster StoreFront ajoutés en tant que membres du groupe de services.

Dans les versions antérieures, le moniteur StoreFront a essayé d'authentifier les magasins anonymes. Par conséquent, un service peut être marqué comme étant INACTIF et vous ne pouvez pas lancer Citrix Virtual Apps et Citrix Virtual Desktops à l'aide de l'URL du serveur virtuel d'équilibrage de charge.

À partir de la version 64.x, l'ordre de la sonde a changé. Le moniteur détermine maintenant l'état du magasin StoreFront en analysant successivement le service de compte, le document de découverte, puis le service d'authentification, et ignore l'authentification pour les magasins anonymes.

Le paramètre de nom d'hôte des moniteurs StoreFront est obsolète. Le paramètre secure est maintenant utilisé pour déterminer s'il faut utiliser HTTP (valeur par défaut) ou HTTPS pour envoyer des sondes de moniteur.

Pour utiliser le protocole HTTPS, définissez l'option sécurisée sur Oui.

Pour créer un moniteur StoreFront à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un moniteur StoreFront et vérifier la configuration :

```
1 add lb monitor <monitorName> STOREFRONT <string> -storeName <string> [-
     storefrontacctservice ( YES | NO )] -secure ( YES | NO )
2
3 show lb monitor <monitorName>
4 <!--NeedCopy-->
```

Exemple

```
1 add lb monitor storefront_ssl STOREFRONT -storename myStore -
     storefrontacctservice YES -secure YES
2 <!--NeedCopy-->
```

Pour créer un moniteur StoreFront à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**et créez un moniteur de type **STOREFRONT**.

> **Remarque**
>
> Pour plus d'informations sur les moniteurs StoreFront, consultez la documentation StoreFront.

Surveillance du service Oracle ECV

June 20, 2023

Le moniteur ECV (Extended Content Verification) d'un NetScaler peut être utilisé pour surveiller les bases de données Oracle. Pour suivre l'état de chaque serveur de base de données à charge équilibrée en temps réel, vous devez associer un moniteur Oracle ECV à chaque service. Le moniteur teste le service en envoyant des sondes périodiques au service sous la forme d'une requête SQL, parfois appelée « vérification de l'état ». Si le moniteur Oracle ECV reçoit une réponse rapide à ses sondes et que l'expression configurée est évaluée comme étant vraie, il marque le service comme étant actif. S'il ne reçoit pas de réponse en temps voulu au nombre de sondes indiqué ou si l'expression configurée est évaluée comme étant fausse, il marque le service comme étant hors service.
La solution de surveillance Netscaler Oracle ECV prend en charge toutes les versions d'Oracle jusqu'à la version 21c et tous les protocoles d'authentification par mot de passe.

Fonctionnalités de sécurité non prises en charge

Le moniteur NetScaler Oracle ECV prend uniquement en charge l'authentification par mot de passe. Il ne prend pas en charge toutes les fonctionnalités et capacités liées à la sécurité.

Les fonctionnalités de sécurité suivantes ne sont pas prises en charge :

- Chiffrement des données (SQLNET.ENCRYPTION_SERVER=Obligatoire)
- Intégrité des données (SQLNET.CRYPTO_CHECKSUM_SERVER=Obligatoire)
- Identifiants longs (O8L_LI)
- Authentification/chiffrement TLS
- Services d'authentification externes, tels que Kerberos et Radius
- Compression
- Portefeuille Oracle

Moniteurs personnalisés

May 5, 2023

En plus des moniteurs intégrés, vous pouvez utiliser des moniteurs personnalisés pour vérifier l'état de vos services. L'appliance NetScaler fournit plusieurs types de moniteurs personnalisés basés sur

des scripts inclus dans le système d'exploitation NetScaler. Les scripts peuvent être utilisés pour déterminer l'état des services en fonction de la charge sur le service ou le trafic réseau envoyé au service. Les moniteurs personnalisés sont les moniteurs en ligne, les moniteurs utilisateur et les moniteurs de charge.

Avec ces types de moniteurs, vous pouvez utiliser la fonctionnalité fournie ou créer vos propres scripts et utiliser ces scripts pour déterminer l'état du service auquel le moniteur est lié.

Configurer les moniteurs HTTP en ligne

May 5, 2023

Les moniteurs en ligne analysent et sondent les réponses des services auxquels ils sont liés uniquement lorsque ces services reçoivent des demandes client. Le moniteur en ligne est de type HTTP-INLINE et ne peut être configuré qu'avec les services HTTP et HTTPS. Un moniteur en ligne détermine que le service auquel il est lié est UP en vérifiant ses réponses aux demandes qui lui sont envoyées. Lorsqu'aucune demande client n'est envoyée au service, le moniteur intégré sonde le service à l'aide de l'URL configurée.

Remarque : Les moniteurs en ligne ne peuvent pas être liés à des services distants ou locaux HTTP ou HTTPS Global Server Load Balancing (GSLB), car ces services représentent des serveurs virtuels plutôt que de véritables serveurs Web à équilibrage de charge.

Les moniteurs en ligne ont une valeur de délai d'attente et un nombre de nouvelles tentatives en cas d'échec des sondes. Vous pouvez sélectionner l'un des types d'actions suivants que l'appliance NetScaler doit effectuer en cas de panne :

- **AUCUN.** Aucune action explicite n'est entreprise. Vous pouvez consulter le service et le moniteur, et le moniteur indique le nombre de réponses d'erreur contiguës actuelles et de réponses cumulées vérifiées.
- **JOURNAL.** Consigne l'événement dans ns/syslog et affiche les compteurs.
- **VERS LE BAS.** Marque le service vers le bas et ne dirige aucun trafic vers ce service. Ce paramètre interrompt toutes les connexions persistantes au service. Cette action enregistre également l'événement et affiche les compteurs.

Une fois le service arrêté, le service reste en panne pendant les temps d'arrêt configurés. Une fois le temps d'arrêt écoulé, le moniteur en ligne utilise l'URL configurée pour sonder le service afin de vérifier s'il est à nouveau disponible. Si la sonde réussit, l'état du service devient UP. Le trafic est dirigé vers le service, et la surveillance reprend comme avant.

Pour configurer des moniteurs en ligne, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Pour configurer des moniteurs HTTP en ligne à l'aide de l'interface de ligne de commande

Exécutez la commande suivante :

```
add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
    <string> -resptimeout <integer> [<units>] -retries <integer> -
    downTime <integer> [<units>] -action <action>
<!--NeedCopy-->
```

Exemple :

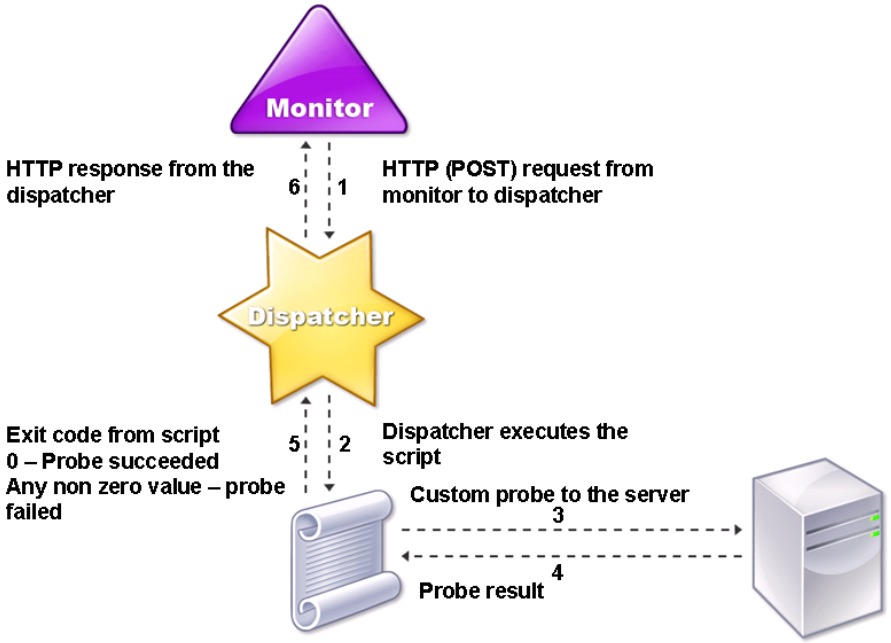
```
add lb monitor http_inline HTTP-INLINE -respCode 200 304 -httpRequest "
    HEAD /var/static/empty.htm" -resptimeout 4 -retries 1 -downTime 2 -
    action NONE
<!--NeedCopy-->
```

Comprendre les moniteurs utilisateur

May 5, 2023

Les moniteurs utilisateur étendent la portée des moniteurs personnalisés. Vous pouvez créer des moniteurs utilisateur pour suivre l'état des applications et des protocoles personnalisés que l'appliance NetScaler ne prend pas en charge. Le diagramme suivant illustre le fonctionnement d'un moniteur utilisateur.

Figure 1. Moniteurs utilisateur



Un moniteur utilisateur nécessite les composants suivants.

Dispatcher. Un processus, sur la solution matérielle-logicielle, qui écoute les demandes de surveillance. Un répartiteur peut se trouver sur l'adresse IP de bouclage (127.0.0.1) et sur le port 3013. Les répartiteurs sont également appelés répartiteurs internes. Un répartiteur peut également être un serveur Web prenant en charge l'interface CGI (Common Gateway Interface). Ces répartiteurs sont également connus sous le nom de répartiteurs externes. Ils sont utilisés pour les scripts personnalisés qui ne s'exécutent pas dans l'environnement FreeBSD, tels que les scripts .NET.

> Remarque :
>
> Vous pouvez configurer le moniteur et le répartiteur pour qu'ils utilisent HTTPS au lieu de HTTP en activant l'option « sécurisé » sur le moniteur et en le configurant en tant que répartiteur externe. Toutefois, un répartiteur interne ne comprend que le protocole HTTP et ne peut pas utiliser le protocole HTTPS.

Dans une configuration HA, le répartiteur s'exécute à la fois sur les appliances NetScaler principales et secondaires. Le répartiteur reste inactif sur la solution matérielle-logicielle secondaire.

script. Le script est un programme qui envoie des sondes personnalisées au serveur à charge équilibrée et renvoie le code de réponse au répartiteur. Le script peut renvoyer n'importe quelle valeur au répartiteur, mais si une sonde réussit, le script doit renvoyer la valeur zéro (0). Le répartiteur considère

toute autre valeur comme une défaillance de la sonde.

L'appliance NetScaler est fournie avec des exemples de scripts pour les protocoles couramment utilisés. Les scripts se trouvent dans le répertoire /nsconfig/moniteurs/. Si vous souhaitez ajouter un script, ajoutez-le ici. Pour personnaliser un script existant, créez une copie portant un nouveau nom et modifiez-la.

Important :

- À partir de NetScaler version 13.0 build 41.20, vous pouvez utiliser le `nsntlm-lwp.pl` script pour créer un moniteur afin de surveiller un serveur NTLM sécurisé.
- À partir de la version 10.1 122.17, les fichiers de script des moniteurs utilisateur se trouvent dans un nouvel emplacement.

  Si vous mettez à niveau un dispositif virtuel MPX ou VPX vers la version 10.1 build 122.17 ou ultérieure, les modifications sont les suivantes :

  - Un nouveau répertoire nommé conflicts est créé dans /nsconfig/monitors/ et tous les scripts intégrés des versions précédentes sont déplacés vers ce répertoire.
  - Tous les nouveaux scripts intégrés sont disponibles dans le répertoire /netscaler/monitors/. Tous les scripts personnalisés sont disponibles dans le répertoire /nsconfig/monitors/.
  - Enregistrez un nouveau script personnalisé dans le répertoire /nsconfig/monitors/.
  - Une fois la mise à niveau terminée, si un script personnalisé est créé et enregistré dans le répertoire /nsconfig/monitors/, avec le même nom que le script intégré, le script du répertoire /netscaler/monitors/ est prioritaire. Le script personnalisé n'est pas exécuté.

  Si vous provisionnez un dispositif virtuel avec la version 10.1 version 122.17 ou ultérieure, les modifications sont les suivantes :

  - Tous les scripts intégrés sont disponibles dans le répertoire /netscaler/monitors/.
  - Le répertoire /nsconfig/monitors/ est vide.
  - Si vous créez un script personnalisé, vous devez l'enregistrer dans le répertoire /nsconfig/monitors/.

Pour que les scripts fonctionnent correctement :

- Le nombre maximal de caractères dans le nom du script ne doit pas dépasser 63.
- Le nombre maximal d'arguments de script pouvant être fournis à un script ne doit pas dépasser 512.
- Le nombre maximal de caractères pouvant être fournis dans les arguments du script de paramètre ne doit pas dépasser 639.

Pour déboguer le script, vous devez l'exécuter à l'aide du script nsumon-debug.pl de l'interface de ligne de commande. Vous utilisez le nom du script (avec ses arguments), l'adresse IP et le port comme

arguments du script nsumon-debug.pl. Les utilisateurs doivent utiliser le nom du script, l'adresse IP, le port, le délai d'expiration et les arguments de script pour le script nsumon-debug.pl.

À l'interface de ligne de commande, tapez :

```
1 nsumon-debug.pl <scriptname> <IP> <port> <timeout> <partitionID> [
     scriptarguments][is_secure]
2 <!--NeedCopy-->
```

Important : à partir de la version 10.5 build 57.x et des fichiers de script 11.0 pour les moniteurs utilisateur prennent en charge les adresses IPv6 et incluent les modifications suivantes :

- Pour les protocoles suivants, de nouveaux protocoles `pm files` ont été inclus pour la prise en charge d'IPv6.
  - RADIUS
  - NNTP
  - POP3
  - SMTP
- Les exemples de scripts suivants dans /netscaler/monitors/ ont été mis à jour pour la prise en charge d'IPv6 :
  - nsbmradius.pl
  - nsldap.pl
  - nsnntp.pl
  - nspop3 nssf.pl
  - nssnmp.pl
  - nswi.pl
  - nstftp.pl
  - nssmtp.pl
  - nsrdp.pl
  - nsntlm-lwp.pl
  - nsftp.pl
  - nsappc.pl

  Après la mise à niveau vers la version 10.5 build 57.x ou 11.0, si vous souhaitez utiliser vos scripts personnalisés existants avec les services IPv6, assurez-vous de mettre à jour les scripts personnalisés existants avec les modifications fournies dans les exemples de scripts mis à jour dans /netscaler/monitors/.

Remarque : L'exemple de script nsmysql.pl ne prend pas en charge l'adresse IPv6. Si un service IPv6 est lié à un moniteur utilisateur qui utilise nsmysql.pl, la sonde échoue.

- Les types de moniteurs LB suivants ont été mis à jour pour prendre en charge les adresses IPv6 :
  - USER
  - SMTP
  - NNTP
  - LDAP
  - SNMP
  - POP3
  - FTP_EXTENDED
  - StoreFront
  - APPC
  - CITRIX_WI_EXTENDED

  Si vous créez un script personnalisé qui utilise l'un de ces types de moniteurs LB, veillez à inclure la prise en charge IPv6 dans le script personnalisé. Reportez-vous à l'exemple de script associé dans /netscaler/monitors/ pour connaître les modifications que vous devez apporter au script personnalisé pour la prise en charge d'IPv6.

Pour suivre l'état du serveur, le moniteur envoie une requête HTTP POST au répartiteur configuré. Cette demande POST contient l'adresse IP et le port du serveur, ainsi que le script à exécuter. Le répartiteur exécute le script en tant que processus enfant, avec des paramètres définis par l'utilisateur (le cas échéant). Ensuite, le script envoie une sonde au serveur. Le script envoie l'état de la sonde (code de réponse) au répartiteur. Le répartiteur convertit le code de réponse en réponse HTTP et l'envoie au moniteur. En fonction de la réponse HTTP, le moniteur marque le service comme étant en hausse ou en panne.

L'appliance NetScaler enregistre les messages d'erreur dans le fichier /var/nslog/nsumond.log lorsque les sondes du moniteur utilisateur échouent. Ces messages d'erreur détaillés sont affichés dans l'interface graphique et dans l'interface de ligne de commande pour les `show service`/ `service group` commandes.

Le tableau suivant répertorie les moniteurs utilisateur et les raisons possibles de l'échec.

Type de moniteur utilisateur	Raisons de défaillance
SMTP	Le moniteur ne parvient pas à établir une connexion au serveur.

Type de moniteur utilisateur	Raisons de défaillance
NNTP	Le moniteur ne parvient pas à établir une connexion au serveur.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	Le moniteur ne parvient pas à trouver le groupe NNTP.
LDAP	Le moniteur ne parvient pas à établir une connexion au serveur.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	Le moniteur ne parvient pas à se lier au serveur LDAP.
	Le moniteur ne parvient pas à localiser une entrée pour l'entité cible sur le serveur LDAP.
FTP	La connexion au serveur est dépassé.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	L'ouverture de session échoue.
	Le moniteur ne parvient pas à trouver le fichier sur le serveur.
POP3	Le moniteur ne parvient pas à établir une connexion à la base de données.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	L'ouverture de session échoue.

Type de moniteur utilisateur	Raisons de défaillance
POP3	Le moniteur ne parvient pas à établir une connexion à la base de données.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	L'ouverture de session échoue.
	La préparation de la requête SQL échoue.
	L'exécution de la requête SQL échoue.
SNMP	Le moniteur ne parvient pas à établir une connexion à la base de données.
	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	L'ouverture de session échoue.
	Le moniteur ne parvient pas à créer la session SNMP.
	Le moniteur ne parvient pas à trouver l'identifiant d'objet.
	Le paramètre de valeur de seuil du moniteur est supérieur ou égal au seuil réel du moniteur.
RDP (Windows Terminal Server)	Arguments de script manquants ou non valides, qui peuvent inclure un nombre d'arguments ou un format d'argument non valide.
	Le moniteur ne parvient pas à créer un socket.
	Les versions ne correspondent pas.
	Le moniteur n'arrive pas à confirmer la connexion.

Vous pouvez afficher le fichier journal à partir de l'interface de ligne de commande à l'aide des commandes suivantes, qui ouvrent un shell BSD, affichent le fichier journal à l'écran, puis ferment le shell

BSD et vous renvoient à l'interface de ligne de commande :

```
> shell
root@ns# cat /var/nslog/nsumond.log
root@ns# exit
>
<!--NeedCopy-->
```

Avant la version 13.0 build 52.X de NetScaler, la `show service/service group` commande affichait un message d'erreur générique indiquant que « la sonde a échoué » comme cause de l'échec de la sonde du moniteur utilisateur.

Exemple :

```
show service ftp

Monitor Name: mon2
State: UNKNOWN  Weight: 1   Passive: 0
Probes: 3    Failed [Total: 0 Current: 0]
Last response: Failure - Probe failed.
Response Time: 1071.838 millisec
<!--NeedCopy-->
```

À partir de la version 13.0 build 52.X de NetScaler, la `show service/service group` commande affiche la cause réelle de l'échec de la sonde du moniteur utilisateur.

Exemple :

```
show service ftp

Monitor Name: mon2
State: DOWN   Weight: 1   Passive: 0
Probes: 729   Failed [Total: 726 Current: 726]
Last response: Failure - Login failed.
Response Time: 8000.0 millisec
<!--NeedCopy-->
```

Les moniteurs utilisateur ont également une valeur de délai d'expiration et un nombre de relances pour les échecs de sonde. Vous pouvez utiliser des moniteurs utilisateur avec des moniteurs non utilisateurs. En cas d'utilisation élevée du processeur, un moniteur non utilisateur permet de détecter plus rapidement une panne de serveur.

Si la sonde du moniteur de l'utilisateur expire en cas d'utilisation élevée du processeur, l'état du service reste inchangé.

Example1:


```
add lb monitor <name> USER -scriptname <script-name> -resptimeout 5
    seconds
<!--NeedCopy-->
```

> Remarque
>
> Pour les moniteurs scriptables, le délai d'attente de réponse doit être configuré à une valeur égale au délai d'expiration attendu de 1 seconde. Par exemple, si vous vous attendez à ce que le délai d'attente soit de 4 secondes, configurez le délai d'attente de réponse sur 5 secondes.

Example2:

```
add lb monitor <name> USER -scriptname <script-name> -scriptargs <
    Arguments> -secureargs <Arguments>
<!--NeedCopy-->
```

> Remarque
>
> Citrix vous recommande d'utiliser le paramètre `secureargs` au lieu du paramètre `scriptargs` pour toutes les données sensibles liées aux scripts.

Comment utiliser un moniteur utilisateur pour vérifier les sites Web

May 5, 2023

Vous pouvez configurer un moniteur utilisateur pour vérifier les problèmes spécifiques de sites Web signalés par les serveurs HTTP à l'aide de codes HTTP spécifiques. Le tableau suivant répertorie les codes de réponse HTTP que ce moniteur utilisateur attend.

Code de réponse HTTP	Signification
200 - succès	Succès de la sonde.
503 - service non disponible	Défaillance de la sonde.
404 - introuvable	Script introuvable ou impossible à exécuter.
500 - Erreur interne du serveur	Erreur interne/contraintes de ressources dans le répartiteur (mémoire insuffisante, trop de connexions, erreur système inattendue ou trop de processus). Le service n'est pas marqué comme étant inactif.
400 - mauvaise demande	Erreur lors de l'analyse de la requête HTTP.

Code de réponse HTTP	Signification
502 - passerelle incorrecte	Erreur lors du décodage de la réponse du script.

Vous configurez le moniteur utilisateur pour HTTP à l'aide des paramètres suivants.

Paramètre	Spécifie
Nom du script	Le chemin et le nom du script à exécuter.
scriptArgs	Les chaînes qui sont ajoutées dans les données POST. Ils sont copiés textuellement sur la demande.
dispatcherIP	Adresse IP du répartiteur auquel la sonde est envoyée.
Port du répartiteur	Port du répartiteur vers lequel la sonde est envoyée.
Nom de fichier local	Le nom d'un fichier de script de surveillance sur le système local.
DestPath	Emplacement particulier de l'appliance NetScaler où le fichier local chargé est stocké.

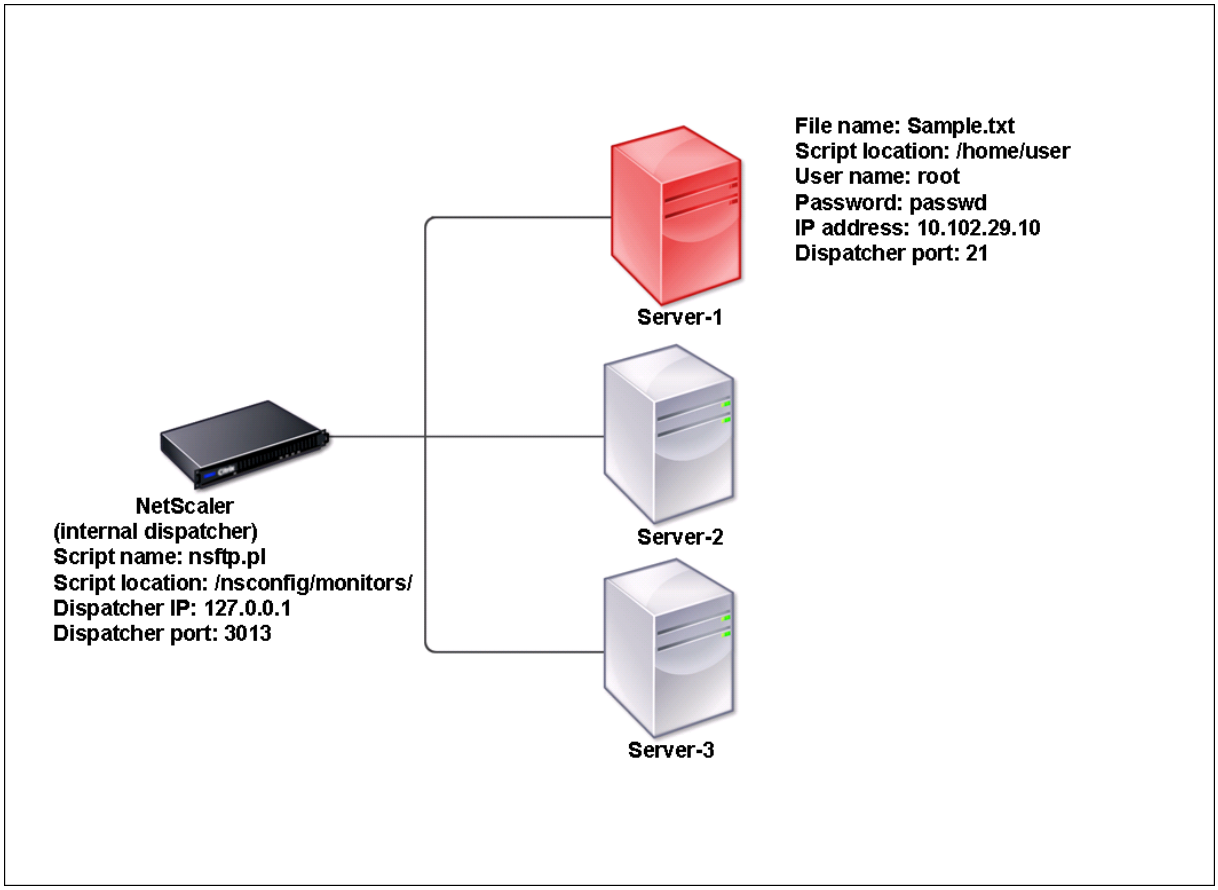
Pour créer un moniteur utilisateur pour surveiller HTTP, reportez-vous à la section Configuration des moniteurs dans une configuration d'équilibrage de charge.

Comprendre le répartiteur interne

May 5, 2023

Vous pouvez utiliser un moniteur utilisateur personnalisé avec le répartiteur interne. Imaginons le cas où vous devez suivre l'état d'un serveur en fonction de la présence d'un fichier sur le serveur. Le schéma suivant illustre ce scénario.

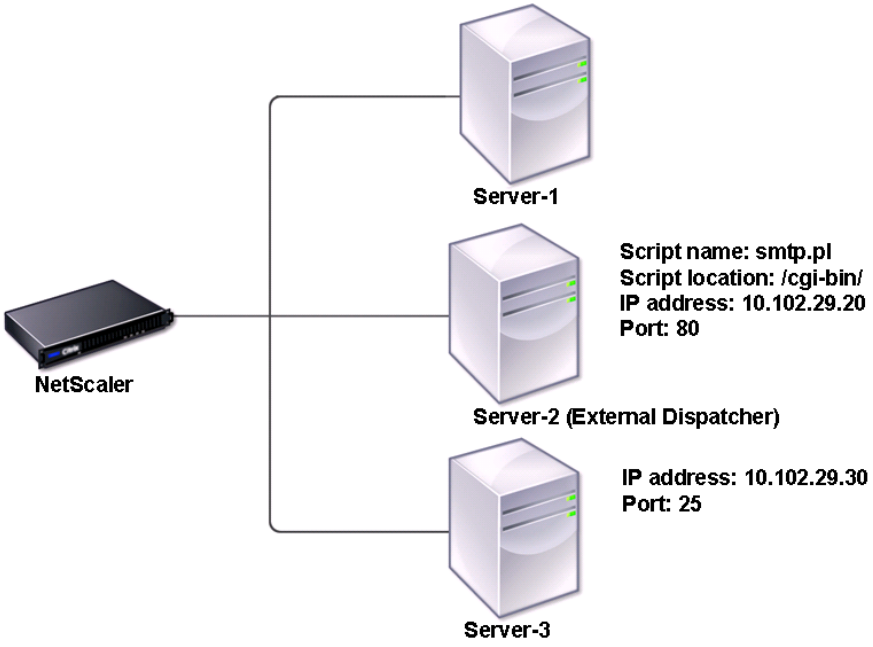
Figure 1. Utilisation d'un moniteur utilisateur avec le répartiteur interne



Une solution possible consiste à utiliser un script Perl qui initie une session FTP avec le serveur et vérifie la présence du fichier. Vous pouvez ensuite créer un moniteur utilisateur qui utilise le script Perl. L'appliance NetScaler inclut un tel script Perl (nsftp.pl) dans le répertoire /nsconfig/monitors/.

Vous pouvez utiliser un moniteur utilisateur avec un répartiteur externe. Imaginons le cas où vous devez suivre l'état d'un serveur en fonction de l'état d'un service SMTP sur un autre serveur. Ce scénario est illustré dans le schéma suivant.

Figure 2. Utilisation d'un moniteur utilisateur avec un répartiteur externe



Une solution possible serait de créer un script Perl qui vérifie l'état du service SMTP sur le serveur. Vous pouvez ensuite créer un moniteur utilisateur qui utilise le script Perl.

Configuration du moniteur utilisateur

May 5, 2023

Les moniteurs utilisateur suivent l'état des applications et des protocoles personnalisés qu'une appliance NetScaler ne prend pas en charge. Il s'agit d'une gamme étendue de moniteurs personnalisés. Pour configurer un moniteur utilisateur, vous devez effectuer les étapes suivantes :

- Écrivez un script qui peut surveiller les services qui lui sont liés.
- Téléchargez le script dans le `/nsconfig/monitors` répertoire de l'appliance NetScaler.
- Fournissez une autorisation exécutable sur le script.

Si le type de moniteur est un protocole que la solution matérielle-logicielle ne prend pas en charge, vous devez utiliser un moniteur de type **USER**. Les moniteurs utilisateur ne prennent en charge que les scripts de type Perl et Bash. Ils ne prennent pas en charge les scripts Python.

> **Remarque**
>
> Les sondes de surveillance proviennent de l'adresse NSIP. La `scriptargs` configuration pour le type de moniteur **USER** est affichée dans les fichiers de configuration et ns.conf en cours d'exécution.

Pour plus d'informations sur les moniteurs, voir Configurer les moniteurs.

Pour configurer un moniteur utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb monitor <monitorName> USER -scriptname <NameOfScript> -
    scriptargs <Arguments> -secureargs <Arguments>
<!--NeedCopy-->
```

Example1:

```
add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
    =/home/user/
sample.txt;user=root;password=passwd"
<!--NeedCopy-->
```

Example2:

```
add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
    =/home/user/
sample.txt -secureargs "user=root;password=passwd"
<!--NeedCopy-->
```

> Remarque
>
> Le `secureargs` paramètre stocke les arguments du script dans un format chiffré au lieu du format texte brut. Citrix vous recommande d'utiliser le `secureargs` paramètre au lieu du paramètre scriptargs pour toutes les données sensibles liées aux scripts, par exemple, le nom d'utilisateur et le mot de passe. Si vous choisissez d'utiliser les deux paramètres ensemble, le script spécifié dans `-scriptname` doit accepter les arguments dans l'ordre : `<scriptargs> <secureargs>`. Spécifiez les premiers arguments du `<scriptargs>` paramètre et le reste des arguments dans le `<secureargs>` paramètre. En d'autres termes, maintenez l'ordre défini pour les arguments. Les arguments sécurisés ne s'appliquent qu'au répartiteur interne. Si vous souhaitez utiliser un répartiteur externe, Citrix recommande de sécuriser les données vulnérables dans vos scripts.

Exemple 3 :

Supposons que vous ayez déjà configuré le `scriptargs` paramètre avec les arguments : « a=b ; c=d ; e=f ».

```
add monitor mon1 USER -scriptargs "a=b;c=d;e=f"
<!--NeedCopy-->
```

Si vous souhaitez utiliser le `secureargs` paramètre au lieu du `scriptargs` paramètre, procédez comme suit :

- Annule le `scriptargs` paramètre.
- Indiquez tous les arguments sous `secureargs` paramètre.

```
set monitor mon1 USER -scriptargs "" -secureargs "a=b;c=d;e=f"
<!--NeedCopy-->
```

Pour configurer un moniteur utilisateur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un moniteur**, procédez comme suit :
   - Sélectionnez le type de moniteur en tant qu' **UTILISATEUR**.
   - Choisissez le script dans le menu déroulant ou téléchargez votre propre script.
   - Entrez les valeurs appropriées pour les champs **Arguments de script** et **Arguments sécurisés** .
   - Cliquez sur **Create**.

   Un moniteur utilisateur est créé.

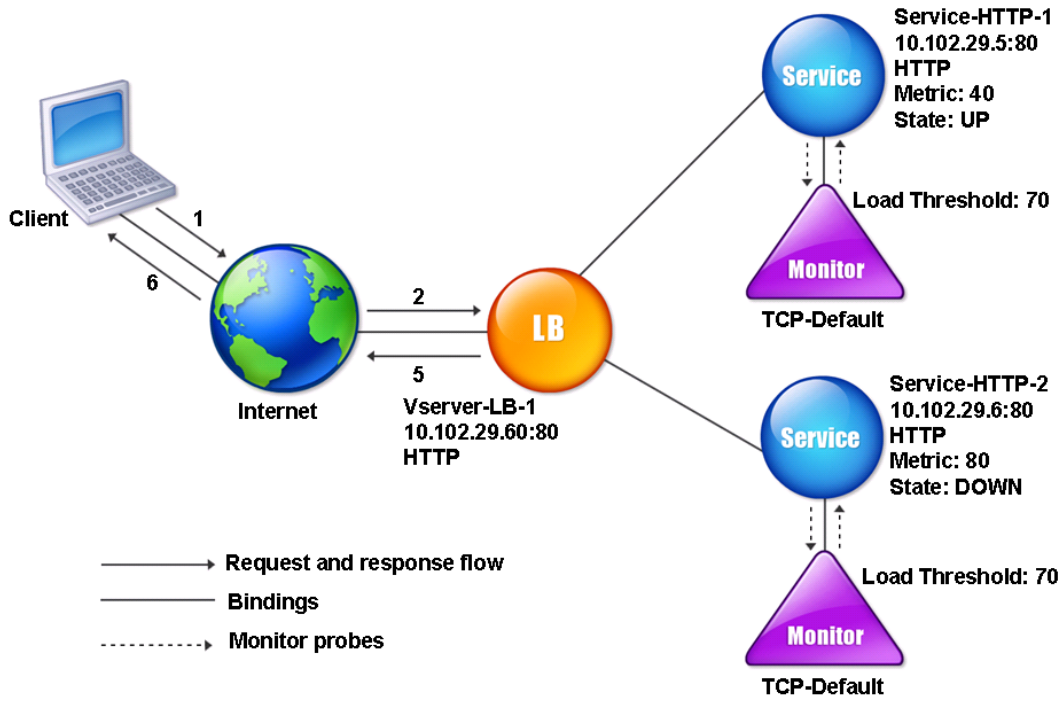
Comprendre le contrôle de charge

May 5, 2023

Les moniteurs de charge utilisent des OID interrogés par SNMP pour calculer la charge. Le moniteur de charge utilise l'adresse IP du service auquel il est lié (l'adresse IP de destination) pour les requêtes. Il envoie une requête SNMP au service, en spécifiant l'OID d'une métrique. Les métriques peuvent être le processeur, la mémoire ou le nombre de connexions au serveur. Le serveur répond à la requête par une valeur métrique. La valeur métrique de la réponse est comparée à la valeur seuil. L'appliance NetScaler prend en compte le service pour l'équilibrage de charge uniquement si la métrique est inférieure à la valeur seuil. Le service avec la valeur de charge la plus faible est considéré en premier.

Le diagramme suivant illustre un moniteur de charge configuré pour les services décrits dans la configuration d'équilibrage de charge de base discutée dans Configuration de l'équilibrage de charge de base.

Figure 1. Fonctionnement des moniteurs de charge



Remarque : le moniteur de charge ne détermine pas l'état du service. Cela permet uniquement à l'appliance de prendre en compte le service pour l'équilibrage de charge.

Après avoir configuré le moniteur de charge, vous devez configurer les mesures que le moniteur utilisera. Pour l'évaluation de la charge, le moniteur de charge prend en compte les paramètres du serveur appelés métriques, qui sont définis dans les tableaux de métriques de la configuration de l'appliance. Les tables métriques peuvent être de deux types :

- **Locaux.** Par défaut, cette table existe dans l'appliance. Il comprend quatre mesures : les connexions, les paquets, le temps de réponse et la bande passante. L'appliance spécifie ces mesures pour un service, et les requêtes SNMP ne sont pas émises pour ces services. Ces mesures ne peuvent pas être modifiées.
- **Personnalisé.** Un tableau défini par l'utilisateur. Chaque métrique est associée à un OID.

Par défaut, l'appliance génère les tables suivantes :

- NetScaler

- RADWARE
- CISCO-CSS
- LOCAL
- FONDERIE
- ALTÉON

Vous pouvez soit ajouter les tables de mesures générées par l'appliance, soit ajouter les tables de votre choix, comme indiqué dans le tableau suivant. Les valeurs du tableau de mesures ne sont fournies qu'à titre d'exemple. Dans un scénario réel, considérez les valeurs réelles des métriques.

Nom de la métrique	OID	Poids	Seuil
UC	1.2.3.4	2	70
Mémoire	4.5.6.7	3	80
Connexions	5.6.7.8	4	90

Pour calculer la charge d'une ou de plusieurs mesures, vous attribuez un poids à chaque mesure. Le poids par défaut est 1. Le poids représente la priorité accordée à chaque métrique. Si le poids est élevé, la priorité est élevée. L'appliance choisit un service en fonction de l'algorithme de hachage SOURCEIPDESTIP.

Vous pouvez également définir la valeur seuil pour chaque métrique. La valeur seuil permet à l'appliance de sélectionner un service pour l'équilibrage de charge si la valeur métrique du service est inférieure à la valeur seuil. La valeur de seuil détermine également la charge sur chaque service.

Configuration des moniteurs de charge

March 9, 2023

Pour configurer un moniteur de charge, créez d'abord le moniteur de charge. Pour obtenir des instructions sur la création d'un moniteur, voir Création de moniteurs. Ensuite, sélectionnez ou créez la table de mesures pour définir un ensemble de mesures qui déterminent l'état du serveur, et (si vous créez une table de mesures) liez chaque mesure à la table de mesures.

Pour créer une table de mesures à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
add lb metricTable <metricTableName>
```



```
bind lb metricTable <metricTableName> <metric> <SNMPOID>
<!--NeedCopy-->
```

Exemple :

```
add lb metricTable Table-Custom-1

bind lb metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5 11
<!--NeedCopy-->
```

Pour créer une table de mesures et y lier des métriques à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Tables de mesures** et créez une table de mesures.
2. Pour lier des mesures, cliquez sur **Lier et spécifiez une mesure et un OID** SNMP.

Dissocier les mesures d'une table de mesures

August 20, 2021

Vous pouvez dissocier les mesures d'une table de mesures si elles doivent être modifiées ou si vous souhaitez supprimer entièrement la table de mesures.

Pour dissocier les mesures d'une table de mesures à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind lb metricTable <metricTable> <metric>
<!--NeedCopy-->
```

Exemple :

```
unbind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5
<!--NeedCopy-->
```

Pour dissocier les mesures d'une table de mesures à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de la charge** > **Tables** de mesures.

2. Ouvrez une table de mesures, sélectionnez une mesure, puis cliquez sur **Supprimer**.

Vous pouvez afficher les détails de toutes les tables de mesures configurées, telles que le nom et le type, pour déterminer si la table de mesures est interne ou si elle est créée et configurée.

Configuration de la surveillance inverse pour un service

May 5, 2023

Un moniteur inversé marque un service comme étant en panne si les critères de la sonde sont satisfaits et en hausse s'ils ne le sont pas. Par exemple, si vous souhaitez qu'un service de sauvegarde reçoive du trafic uniquement lorsque le service principal est hors service, vous pouvez lier un moniteur inversé au service secondaire tout en le configurant pour sonder le service principal.

L'appliance NetScaler prend en charge les moniteurs inversés suivants :

- HTTP
- ICMP
- TCP (à partir de la version 11.1 build 49.x)

Configuration de la surveillance inverse HTTP pour un service

Le tableau suivant décrit les conditions de surveillance directe et inverse du protocole HTTP pour un service :

Condition	Directement	Inversé
Connexion non établie.	Échouer	Échouer
Le code de réponse HTTP correspond aux spécifications de la sonde.	Succès	Échouer
Le code de réponse HTTP ne correspond pas aux spécifications de la sonde.	Échouer	Succès
Le délai de la sonde a expiré.	Échouer	Échouer

Pour configurer la surveillance inverse HTTP pour un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add lb monitor <Monitor_Name> HTTP -respCode 200 -httpRequest "HEAD /"
    -destIP <Primary_Service_IP_Address> -destPort 80 -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

Configuration de la surveillance inverse ICMP pour un service

Le tableau suivant décrit les conditions de la surveillance directe et inverse par ICMP pour un service :

Condition	Directement	Inversé
La réponse d'écho ICMP est reçue.	Succès	Échouer
Le délai de la sonde a expiré.	Échouer	Succès

Pour configurer la surveillance inverse ICMP pour un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb monitor <Monitor_Name> PING -destIP <Primary_Service_IP_Address>
    -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

Configuration de la surveillance inverse TCP pour un service

Si un moniteur TCP direct reçoit une réinitialisation en réponse à une sonde de surveillance, le service est marqué comme étant inactif. Toutefois, si un moniteur TCP inversé reçoit une réponse RESET, la sonde est considérée comme réussie et le service est marqué comme étant activé.

Le tableau suivant décrit les conditions de la surveillance inverse TCP pour un service :

Condition	Directement	Inversé
La connexion TCP est établie.	Succès	Échouer
Le délai de la sonde a expiré.	Échouer	Échouer

Condition	Directement	Inversé
La réponse à la sonde est RÉINITIALISÉE.	Échouer	Succès

Pour configurer la surveillance inverse TCP pour un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb monitor <Monitor_Name> TCP -destip <Primary_Service_IP_Address>
    -destport <primary_service_port> -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

Pour configurer la surveillance inversée à l'aide de l'interface graphique

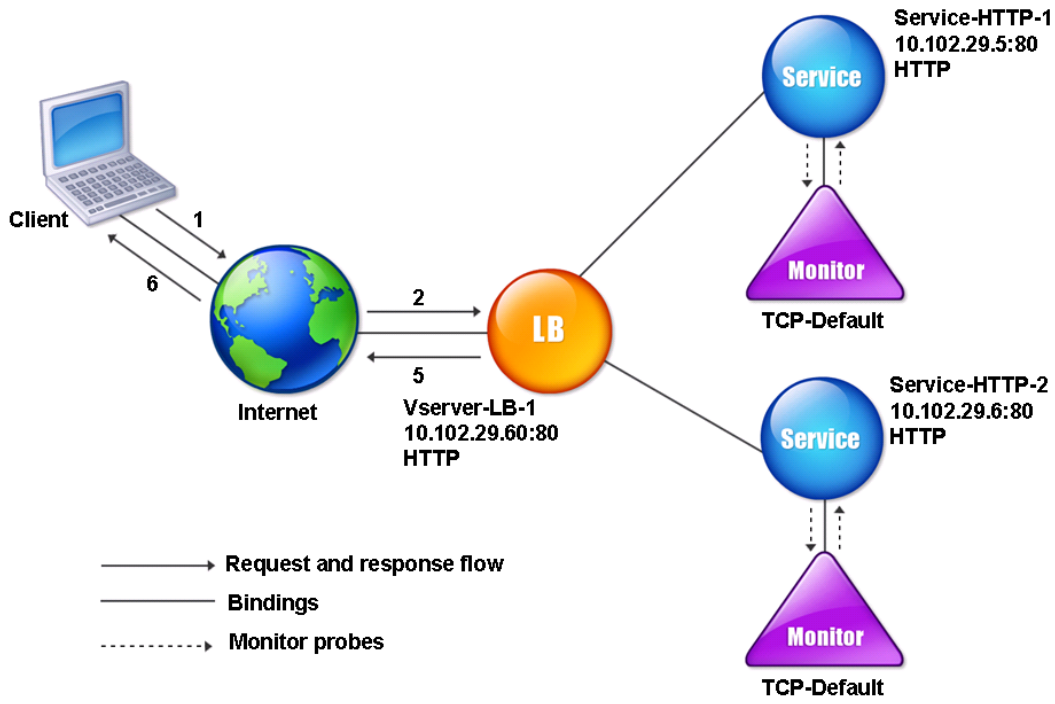
1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**.
2. Créez un moniteur HTTP, ICMP ou TCP et sélectionnez **Inverser**.

Configurer les moniteurs dans une configuration d'équilibrage de charge

August 20, 2021

Pour configurer des moniteurs sur un site Web, vous décidez d'abord d'utiliser un moniteur intégré ou de créer votre propre moniteur. Si vous créez un moniteur, vous pouvez choisir entre créer un moniteur basé sur un moniteur intégré ou créer un moniteur personnalisé utilisant un script que vous écrivez pour surveiller le service. Pour plus d'informations sur la création de moniteurs personnalisés, voir Moniteurs personnalisés. Une fois que vous avez choisi ou créé un moniteur, vous le liez ensuite au service approprié. Les noms de moniteur peuvent contenir jusqu'à 255 caractères. Le diagramme conceptuel suivant illustre une configuration d'équilibrage de charge de base avec des moniteurs.

Figure 1. Fonctionnement des moniteurs



Comme indiqué, chaque service est associé à un moniteur. Le moniteur sonde le serveur à équilibrage de charge via son service. Tant que le serveur à équilibrage de charge répond aux sondes, le moniteur le marque comme UP. Si le serveur à charge équilibrée ne répond pas au nombre de sondes désigné au cours de la période désignée, le moniteur le marque DOWN.

Cette section comprend les détails suivants :

- Création de moniteurs
- Configuration des paramètres de surveillance pour déterminer l'intégrité du service
- Liaison des moniteurs aux services
- Modification des moniteurs
- Activation et désactivation des moniteurs
- Moniteurs sans liaison
- Suppression de moniteurs
- Affichage des moniteurs
- Fermeture des connexions du moniteur
- Ignorer la limite supérieure des connexions client pour les sondes de moniteur

Créer des moniteurs

May 5, 2023

L'appliance NetScaler fournit un ensemble de moniteurs intégrés. Il vous permet également de créer des moniteurs personnalisés, soit sur la base des moniteurs intégrés, soit à partir de zéro.

Pour créer un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb monitor <monitorName> <monitorType> [<interval>]

add lb mon monitor-HTTP-1 HTTP

add lb mon monitor-HTTP-2 TCP 2
<!--NeedCopy-->
```

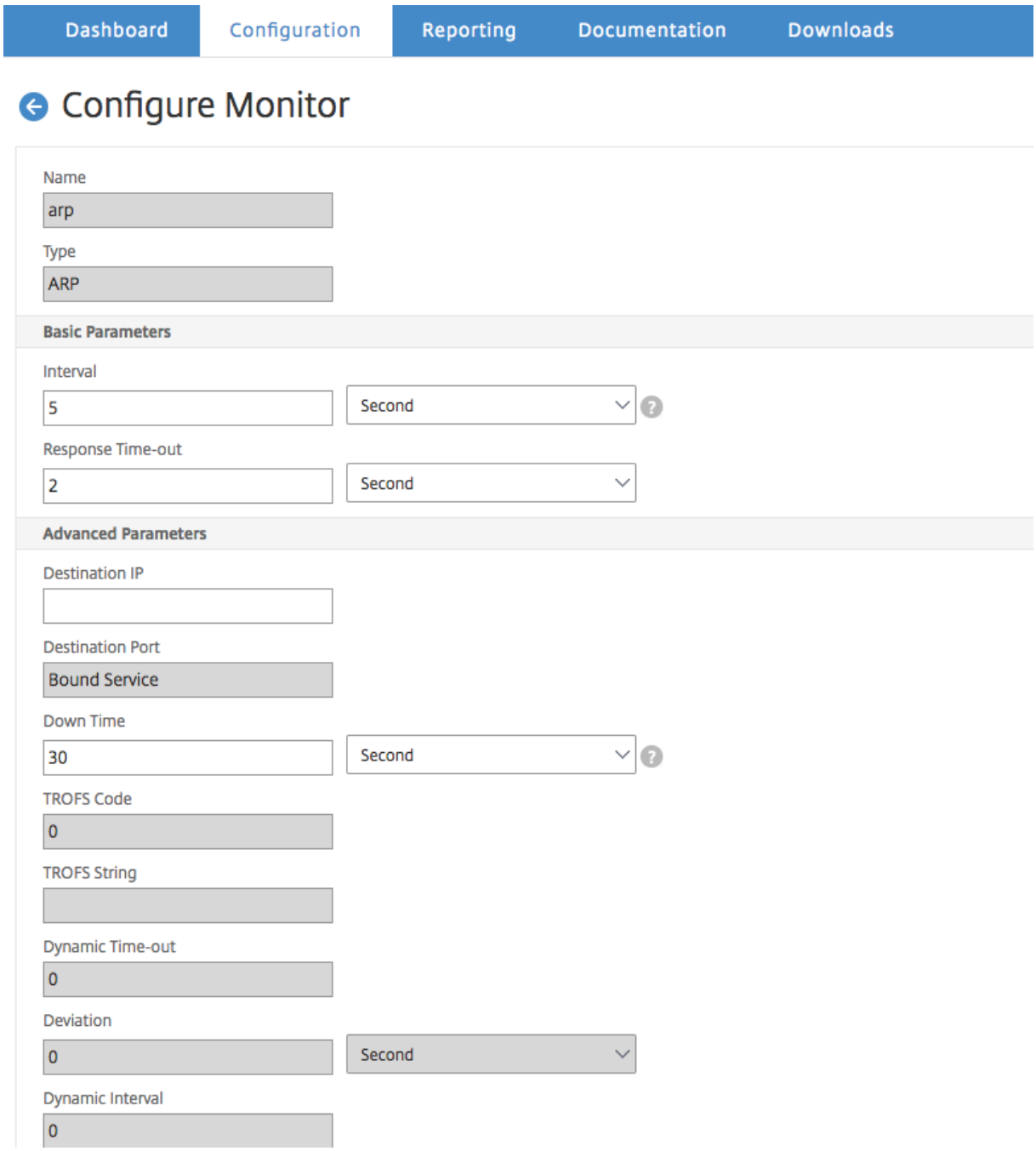
Pour créer un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**.
2. Cliquez sur **Ajouter** et créez un type de moniteur qui répond à vos besoins.

L'écran Créer un moniteur contient deux sections : **Paramètres de base** et **Paramètres avancés**.

Selon le type de moniteur, la section **Paramètres de base** contient les paramètres qui doivent être définis pour chaque moniteur. La section **Paramètres avancés** contient les paramètres qui peuvent être utilisés dans des cas d'utilisation avancés.

La figure suivante est un exemple de page Créer un moniteur du type de moniteur ARP.



Remarque

Avant NetScaler version 12.0 build 56.20, les paramètres de base et les paramètres avancés sont respectivement nommés paramètres standard et paramètres spéciaux.

Configurer les paramètres du moniteur pour déterminer l'intégrité du service

May 5, 2023

Vous pouvez configurer les paramètres de surveillance suivants pour marquer un service comme étant DOWN en fonction des sondes de surveillance.

Retries

Nombre maximum de sondes à envoyer pour établir l'état d'un service pour lequel une sonde de surveillance échoue.

Rétentatives en cas d'échec

Nombre de tentatives qui doivent échouer, hors du nombre spécifié pour le paramètre Retries, pour qu'un service soit marqué comme étant DOWN. Par exemple, si le paramètre Retries est défini sur 10 et que le paramètre Failure Retries est défini sur 6, sur les 10 sondes envoyées, au moins six sondes doivent échouer si le service doit être marqué comme DOWN.

alertRetries

Nombre d'échecs de sonde consécutifs après lesquels l'appliance génère une interruption SNMP appelée monProbeFailed.

Définition d'AlertEtries sur une valeur supérieure à la valeur Retries

Le paramètre AlertRetries, qui spécifie le nombre maximum de défaillances consécutives des sondes de surveillance après lesquelles l'appliance NetScaler génère un piège SNMP appelé MonProbeFailed, peut désormais être défini sur une valeur supérieure à la valeur Retries (qui spécifie le nombre maximum de sondes à envoyer pour établir l'état d'un service pour lequel une sonde de surveillance a échoué). Si la valeur AlertRetries est supérieure à la valeur Retries, le trap SNMP n'est envoyé que lorsque le service est hors service.

Par exemple, si vous définissez Retries sur 3, AlertRetries sur 12 et l'intervalle de temps sur 5 secondes, le service est marqué comme étant inactif au bout de 15 secondes (3*5), mais aucune alerte n'est générée. Si les sondes du moniteur échouent toujours au bout de 60 secondes (12*5), l'appliance NetScaler génère un piège MonProbeFailed. Si une sonde réussit entre 15 et 60 secondes, le service est marqué et aucune alerte n'est générée.

Le fait de définir la valeur AlertRetries sur une valeur supérieure à la valeur Retries permet de générer uniquement des alertes authentiques et d'éviter les faux positifs lors des redémarrages planifiés.

Pour définir la valeur du paramètre AlertRetries sur une valeur supérieure à la valeur Retries à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb monitor <monitorName> [-retries <integer>] [-alertRetries <
   integer>]
<!--NeedCopy-->
```

Exemple :

ajouter lb monitor monitor-HTTP-1 HTTP -retries 3 -AlertRetries 12

Pour définir la valeur du paramètre AlertRetries sur une valeur supérieure à la valeur Retries à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**.
2. Cliquez sur **Ajouter** pour ajouter un nouveau moniteur ou sélectionnez un moniteur existant et cliquez sur **Modifier**.
3. Dans la zone **Rétentatives**, tapez la valeur du paramètre Rétentatives.
4. Dans la zone **Rétentatives d'alerte SNMP**, tapez la valeur du paramètre. `alertRetries`

Liez les moniteurs aux services

May 5, 2023

Après avoir créé un moniteur, vous le liez à un service. Vous pouvez associer un ou plusieurs moniteurs à un service. Si vous liez un moniteur à un service, ce moniteur détermine si le service est marqué comme étant ACTIF ou NON.

Si vous liez plusieurs moniteurs à un service, l'appliance NetScaler vérifie l'état de tous les moniteurs puis décide de l'état du service. Vous pouvez configurer différents poids sur un moniteur. Le poids d'un moniteur indique dans quelle mesure ce moniteur contribue à désigner le service comme étant ACTIF ou INACTIF. Un moniteur dont le poids est plus élevé a une préférence plus élevée lorsqu'il s'agit de marquer le service VERS LE HAUT ou VERS LE BAS. Le poids par défaut est 1. Par conséquent, même si l'un des moniteurs échoue, le service est marqué comme DOWN. Pour plus d'informations, voir Définir une valeur de seuil pour les moniteurs liés à un service.

Remarque : L'adresse IP de destination d'une sonde de moniteur peut être différente de l'adresse IP du serveur et du port.

Pour lier un moniteur à un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind service <name> (-monitorName <string>)
<!--NeedCopy-->
```

Exemple :

```
bind service s1 -monitorName tcp
<!--NeedCopy-->
```

Pour lier un moniteur à un service à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Ouvrez le service et ajoutez un moniteur.

Modifier les moniteurs

August 20, 2021

Vous pouvez modifier les paramètres de n'importe quel moniteur que vous avez créé.

Remarque : Deux ensembles de paramètres s'appliquent aux moniteurs : ceux qui s'appliquent à tous les moniteurs, quel que soit leur type, et ceux qui sont spécifiques à un type de moniteur. Pour plus d'informations sur les paramètres d'un type de moniteur spécifique, consultez la description de ce type de moniteur.

Pour modifier un moniteur existant à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set lb monitor <monitorName> <type> -interval <interval> -resptimeout <
    resptimeout>
<!--NeedCopy-->
```

Exemple :


```
set mon monitor-HTTP-1 HTTP -interval 50 milli
-resptimeout 20 milli
<!--NeedCopy-->
```

Pour modifier un moniteur existant à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**, puis ouvrez un moniteur à modifier.

Activer et désactiver les moniteurs

August 20, 2021

Par défaut, les moniteurs liés aux services et aux groupes de services sont activés. Lorsque vous activez un moniteur, celui-ci commence à sonder les services auxquels il est lié. Si vous désactivez un moniteur lié à un service, l'état du service est déterminé à l'aide des autres moniteurs liés au service. Si le service est lié à un seul moniteur et si vous le désactivez, l'état du service est déterminé à l'aide du moniteur par défaut.

Pour activer un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
enable lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
enable lb mon monitor-HTTP-1
<!--NeedCopy-->
```

Pour activer un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Sélectionnez un moniteur et, dans la liste Action, sélectionnez Activer ou Désactiver.

Pour désactiver un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :


```
disable lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
disable lb mon monitor-HTTP-1
<!--NeedCopy-->
```

Dissocier les moniteurs

August 20, 2021

Vous pouvez dissocier les moniteurs d'un service et d'un groupe de services. Lorsque vous dissociez un moniteur du groupe de services, les moniteurs sont dissociés des services individuels qui constituent le groupe de services. Lorsque vous dissociez un moniteur d'un service ou d'un groupe de services, le moniteur ne sonde pas le service ou le groupe de services.

Remarque : Lorsque vous dissociez tous les moniteurs configurés par l'utilisateur d'un service ou d'un groupe de services, le moniteur par défaut est lié au service et au groupe de services. Les moniteurs par défaut sonde ensuite le service ou les groupes de services.

Pour dissocier un moniteur d'un service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
unbind lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
unbind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

Pour dissocier un moniteur d'un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service à modifier.
2. Cliquez dans la section Moniteurs, sélectionnez un moniteur, puis cliquez sur **Délier**.

Supprimer les moniteurs

May 5, 2023

Après avoir dissocié un moniteur que vous avez créé à partir de son service, vous pouvez le supprimer de la configuration NetScaler. (Si un moniteur est lié à un service, il ne peut pas être supprimé.)

Remarque : Lorsque vous supprimez des moniteurs liés à un service, le moniteur par défaut est lié au service. Vous ne pouvez pas supprimer les moniteurs par défaut.

Pour supprimer un moniteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm lb monitor <monitorName> <type>
<!--NeedCopy-->
```

Exemple :

```
rm lb monitor monitor-HTTP-1 HTTP
<!--NeedCopy-->
```

Pour supprimer un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Sélectionnez un moniteur, puis cliquez sur **Supprimer**.

Afficher les moniteurs

May 5, 2023

Vous pouvez afficher les services et les groupes de services liés à un moniteur. Vous pouvez vérifier les paramètres d'un moniteur pour résoudre les problèmes de configuration de NetScaler. La procédure suivante décrit les étapes pour afficher les liaisons d'un moniteur aux services et groupes de services.

Pour afficher les liaisons de moniteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show lb monbindings <MonitorName>
<!--NeedCopy-->
```


Exemple :

```
show lb monbindings monitor-HTTP-1
<!--NeedCopy-->
```

Pour afficher les liaisons de moniteurs à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Sélectionnez un moniteur, puis dans la liste Action, cliquez sur **Afficher les liaisons**.

Pour afficher des moniteurs à l'aide de la CLI

À l'invite de commande, tapez :

```
show lb monitor <monitorName>
<!--NeedCopy-->
```

Exemple :

```
show lb mon monitor-HTTP-1
<!--NeedCopy-->
```

Pour afficher des moniteurs à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**. Les détails des moniteurs disponibles apparaissent dans le volet Moniteurs.

Fermer les connexions du moni

May 5, 2023

L'appliance NetScaler envoie des sondes aux services via les moniteurs liés aux services. Par défaut, le moniteur de l'appliance et le serveur physique suivent la procédure de prise de main complète, même pour les sondes du moniteur. Toutefois, cette procédure ajoute des frais généraux au processus de surveillance et peut ne pas être toujours nécessaire.

Pour le moniteur de type TCP, vous pouvez configurer l'appliance pour fermer une connexion moniteur-sonde après avoir reçu SYN-ACK du service. Pour ce faire, définissez la valeur du paramètre MonitorConnectionClose sur RESET. Si vous souhaitez que la connexion moniteur-sonde suive la procédure complète, définissez la valeur sur FIN.

Remarque : Le paramètre MonitorConnectionClose s'applique uniquement aux moniteurs de type TCP et TCP par défaut.

Pour configurer la fermeture de la connexion du moniteur à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
set lb parameter -monitorConnectionClose <monitor_conn_close_option>
<!--NeedCopy-->
```

Exemple

```
set lb parameter -monitorConnectionClose RESET
<!--NeedCopy-->
```

Pour configurer la fermeture de la connexion du moniteur à l'aide de l'utilitaire de configuration :

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**.
2. Sélectionnez **FIN** ou **Reset**.

Fermeture des connexions du moniteur au niveau du service ou du groupe de services

Vous pouvez également configurer l'appliance pour fermer une connexion moniteur-sonde au niveau du service et du groupe de services en définissant le paramètre MonConnectionClose. Si ce paramètre n'est pas défini, la connexion du moniteur est fermée à l'aide de la valeur définie dans les paramètres d'équilibrage de charge globaux. Si ce paramètre est défini au niveau du service ou du groupe de services, la connexion du moniteur est fermée en envoyant un message de fin de connexion, avec le bit FIN ou RESET défini, au service ou au groupe de services.

Pour configurer la fermeture de la connexion du moniteur au niveau du service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <service_name> -monConnectionClose ( RESET | FIN )
<!--NeedCopy-->
```

Pour configurer la fermeture de la connexion du moniteur au niveau du groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
 set serviceGroup <service_name> -monConnectionClose ( RESET | FIN )
<!--NeedCopy-->
```

Pour configurer la fermeture de la connexion du moniteur au niveau du service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Ajoutez ou modifiez un service et, dans les **paramètres de base**, définissez le **bit de fermeture de la connexion de surveillance**.

Pour configurer la fermeture de la connexion du moniteur au niveau du groupe de services à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Ajoutez ou modifiez un groupe de services et, dans les **paramètres de base**, définissez le **bit de fermeture de la connexion de surveillance**.

> **Remarque :** Pour fermer une connexion moniteur-sonde à l'aide de paramètres d'équilibrage de charge globaux, vous pouvez configurer MonitorConnectionClose sur FIN ou RESET. Lorsque vous configurez le paramètre MonitorConnectionClose sur :
>
> - FIN : L'appliance effectue une prise de contact TCP complète.
> - RESET : l'appliance ferme la connexion après avoir reçu le SYN-ACK du service.
>
> Dans la version allégée de NetScaler CPX, la valeur du paramètre MonitorConnectionClose est définie sur RESET par défaut et ne peut pas être modifiée en FIN au niveau global. Vous pouvez toutefois modifier le paramètre MonitorConnectionClose en FIN au niveau du service.

Ignorer la limite supérieure des connexions client pour les sondes de moniteur

May 5, 2023

En fonction de considérations telles que la capacité d'un serveur physique, vous pouvez définir une limite au nombre maximum de connexions client établies à n'importe quel service. Si vous avez défini une telle limite pour un service, l'appliance NetScaler arrête d'envoyer des demandes au service lorsque le seuil est atteint et reprend l'envoi de connexions au service une fois que le nombre de connexions existantes se situe dans les limites. Vous pouvez configurer l'appliance pour ignorer cette vérification lorsqu'elle envoie des connexions moniteur-sonde à un service.

Remarque : Vous ne pouvez pas ignorer la vérification du nombre maximal de connexions clients pour un service individuel. Si vous spécifiez cette option, elle s'applique à tous les moniteurs liés à tous les services configurés sur l'appliance NetScaler.

Pour définir l'option Skip MaxClients for Monitor Connections à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb parameter -monitorSkipMaxClient (ENABLED|DISABLED)
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -monitorSkipMaxClient enabled
<!--NeedCopy-->
```

Pour définir l'option Skip MaxClients for Monitor Connections à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres d'équilibrage de charge**.
2. Sélectionnez **Ignorer MaxClients pour la surveillance des connexions**.

Gérez un déploiement à grande échelle

May 5, 2023

L'appliance NetScaler contient plusieurs fonctionnalités utiles lorsque vous configurez un déploiement d'équilibrage de charge de grande envergure. Au lieu de configurer des serveurs et des services virtuels individuellement, vous pouvez créer des groupes de serveurs et de services virtuels. Vous pouvez également créer une gamme de serveurs et de services virtuels, et vous pouvez traduire ou masquer les adresses IP des serveurs et des services virtuels.

Vous pouvez définir la persistance pour un groupe de serveurs virtuels. Vous pouvez lier des moniteurs à un groupe de services. La création d'une gamme de serveurs virtuels et de services de type identique vous permet de configurer et de configurer ces serveurs en une seule procédure. Cela réduit considérablement le temps nécessaire à la configuration de ces serveurs et services virtuels.

En traduisant ou en masquant des adresses IP, vous pouvez retirer des serveurs et des services virtuels. Vous pouvez ensuite apporter des modifications à votre infrastructure, sans reconfiguration étendue de votre service ni de définitions de serveurs virtuels.

Gammes de serveurs virtuels et de services

August 20, 2021

Lorsque vous configurez l'équilibrage de charge, vous pouvez créer des plages de serveurs et de services virtuels, éliminant ainsi la nécessité de configurer des serveurs et des services virtuels individuellement. Par exemple, vous pouvez utiliser une procédure unique pour créer trois serveurs virtuels avec trois adresses IP correspondantes. Lorsque plusieurs arguments utilisent une plage, les plages doivent être de même taille.

Voici les types de plages que vous pouvez spécifier lors de l'ajout de services et de serveurs virtuels à votre configuration :

- **Gammes numériques.** Au lieu de taper un seul nombre, vous pouvez spécifier une plage de nombres consécutifs.

  Par exemple, vous pouvez créer une plage de serveurs virtuels en spécifiant une adresse IP de départ, telle que 10.102.29.30, puis en tapant une valeur pour le dernier octet qui indique la plage, telle que 34. Dans cet exemple, cinq serveurs virtuels sont créés avec des adresses IP comprises entre 10.102.29.30 et 10.102.29.34.

  Remarque : Les adresses IP des serveurs et services virtuels doivent être consécutives.

- **Gammes alphabétiques.** Au lieu de saisir une lettre littérale, vous pouvez remplacer une plage par une lettre unique, par exemple [C-G]. Il en résulte que toutes les lettres de la fourchette sont incluses, dans ce cas C, D, E, F et G.

  Par exemple, si vous avez trois serveurs virtuels nommés et `Vserver-xVserver-yVserver-z`, au lieu de les configurer séparément, vous pouvez taper `vserver [x-z]` pour les configurer tous.

Création d'une gamme de serveurs virtuels

Pour créer une plage de serveurs virtuels à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
1 add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<
      port>]
2
```



```
add lb vserver <name>@[<rangeValue>]> <protocol> <IPAddress[<rangeValue
    >]> [<port>]
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
<!--NeedCopy-->
```

OU

```
add lb vserver vserver[P-R] http 10.102.29.[26-28] 80

vserver "vserverP" added

vserver "vserverQ" added

vserver "vserverR" added

Done
<!--NeedCopy-->
```

Pour créer une plage de serveurs virtuels à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

```
add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<
    port>]

add lb vserver <name>@\*\*[\*\*<rangeValue>\*\*]\*\*> <protocol> <
    IPAddress[<rangeValue>]> [<port>]
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
<!--NeedCopy-->
```

OU

```
add lb vserver vserver[P-R] http 10.102.29.[26-28] 80
vserver "vserverP" added
vserver "vserverQ" added
vserver "vserverR" added
```



```
Done
<!--NeedCopy-->
```

Pour créer une gamme de serveurs virtuels à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ajoutez un serveur virtuel et spécifiez une plage.

Création d'une gamme de services

Si vous spécifiez une plage pour le nom du service, spécifiez également une plage pour l'adresse IP.

Pour créer une gamme de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande :

```
add service <name>@ <IP>@ <protocol> <port>
<!--NeedCopy-->
```

Exemple :

```
> add service serv[1-3] 10.102.29.[102-104] http 80
service "serv1" added
service "serv2" added
service "serv3" added
 Done
<!--NeedCopy-->
```

Configuration des groupes de services

May 5, 2023

La configuration d'un groupe de services vous permet de gérer un groupe de services aussi facilement qu'un seul service. Par exemple, si vous activez ou désactivez une option quelconque, telle que la compression, la surveillance de l'état ou l'arrêt gracieux, pour un groupe de services, l'option est activée pour tous les membres du groupe de services.

Après avoir créé un groupe de services, vous pouvez le lier à un serveur virtuel et ajouter des services au groupe. Vous pouvez également lier des moniteurs à des groupes de services.

> **Remarque**
>
> Vous ne pouvez pas lier un service et un groupe de services ayant la même adresse IP et le même port au même serveur virtuel.

Les membres d'un groupe de services sont identifiés par une adresse IP ou un nom de serveur.

L'utilisation des membres du groupe DBS (Domain-Name Based Service) est avantageuse car il n'est pas nécessaire de reconfigurer le membre sur l'appliance NetScaler si l'adresse IP du membre change. L'appliance détecte automatiquement ces modifications via le serveur de noms configuré. Cette fonctionnalité est utile dans les scénarios cloud, où le fournisseur de services peut modifier un serveur physique ou modifier l'adresse IP d'un service. Si vous spécifiez un membre du groupe DBS, l'appliance apprend l'adresse IP de manière dynamique.

Vous pouvez lier des membres basés sur IP et des membres DBS au même groupe de services.

Remarque : Si vous utilisez des membres du groupe de services DBS, assurez-vous qu'un serveur de noms est spécifié ou qu'un serveur DNS est configuré sur l'appliance NetScaler. Un nom de domaine est résolu en adresse IP uniquement si l'enregistrement d'adresse correspondant est présent sur l'appliance ou le serveur de noms.

Créer des groupes de services

Vous pouvez configurer jusqu'à 8 192 groupes de services sur l'appliance NetScaler.

Pour créer un groupe de services à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
add servicegroup <ServiceGroupName> <Protocol>
<!--NeedCopy-->
```

Exemple :

```
add servicegroup Service-Group-1 HTTP
<!--NeedCopy-->
```

Pour créer un groupe de services à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**, puis ajoutez un groupe de services.

Lier un groupe de services à un serveur virtuel

Lorsque vous liez un groupe de services à un serveur virtuel, les services membres sont liés au serveur virtuel.

Pour lier un groupe de services à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb vserver <name>@ <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

Pour lier un groupe de services à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans les paramètres avancés, sélectionnez **Groupes de services**.

Lier un membre à un groupe de services

L'ajout de services à un groupe de services permet au groupe de services de gérer les serveurs. Vous pouvez ajouter les serveurs à un groupe de services en spécifiant les adresses IP ou les noms des serveurs.

Dans l'interface graphique, si vous souhaitez ajouter un membre du groupe de services basé sur un nom de domaine, sélectionnez **Serveur**.

Avec cette option, vous pouvez ajouter n'importe quel serveur auquel un nom a été attribué, qu'il s'agisse d'une adresse IP ou d'un nom attribué par l'utilisateur.

Pour ajouter des membres à un groupe de services à l'aide de l'interface de ligne de commande

Pour configurer un groupe de services, à l'invite de commande, tapez :

```
bind servicegroup <serviceGroupName> (<IP>@ | <serverName>) <port>
<!--NeedCopy-->
```


Exemples :

```
bind servicegroup Service-Group-1 10.102.29.30 80

bind servicegroup Service-Group-2 1000:0000:0000:0000:0005:0600:700a
   :888b 80

bind servicegroup CitrixEdu s1.citrite.net
<!--NeedCopy-->
```

Pour ajouter des membres à un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services** et ouvrez un groupe de services.
2. Cliquez dans la section Groupe de services et effectuez l'une des opérations suivantes :
   - Pour ajouter un membre de groupe de services IP, sélectionnez IP Based.
   - Pour ajouter un membre de groupe de services basé sur un nom de serveur, sélectionnez Basé sur le serveur.

   Si vous souhaitez ajouter un membre à un groupe de services basé sur un nom de domaine, sélectionnez **Basé sur un serveur**. Avec cette option, vous pouvez ajouter n'importe quel serveur auquel un nom a été attribué, qu'il s'agisse d'une adresse IP ou d'un nom attribué par l'utilisateur.
3. Si vous ajoutez un nouveau membre basé sur l'adresse IP, saisissez l'adresse IP dans la zone de texte Adresse IP. Si l'adresse IP utilise le format IPv6, cochez la case IPv6, puis entrez l'adresse dans la zone de texte Adresse IP

   Remarque : Vous pouvez ajouter une plage d'adresses IP. Les adresses IP de la plage doivent être consécutives. Spécifiez la plage en saisissant l'adresse IP de départ dans la zone de texte Adresse IP (par exemple, 10.102.29.30). Spécifiez l'octet final de la plage d'adresses IP dans la zone de texte située sous Plage (par exemple, 35). Dans la zone de texte Port, tapez le port (par exemple, 80), puis cliquez sur Ajouter.
4. Cliquez sur Create.

Lier un moniteur à un groupe de services

Lorsque vous créez un groupe de services, le moniteur par défaut du type approprié pour le groupe y est automatiquement lié. Les moniteurs analysent régulièrement les serveurs du groupe de services auquel ils sont liés et mettent à jour l'état des groupes de services.

Vous pouvez lier un moniteur différent de votre choix au groupe de services.

Pour lier un moniteur à un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind serviceGroup <serviceGroupName> -monitorName <string> -monState (
    ENABLED | DISABLED)
<!--NeedCopy-->
```

Exemple :

```
bind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
<!--NeedCopy-->
```

Vers un moniteur de liaison à un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Ouvrez un groupe de services et, dans les paramètres avancés, cliquez sur **Moniteurs**.

Conserver l'état d'origine d'un membre du groupe de services après avoir désactivé et activé un serveur virtuel

À partir de la version 64.x, une nouvelle option globale, —RetainDisableServer, vous permet de conserver l'état d'un membre d'un groupe de services lorsqu'un serveur est désactivé et réactivé.

Auparavant, l'état d'un membre passait de DISABLED à ENABLED dans les conditions suivantes :

- Deux applications sont déployées sur le même port d'un serveur virtuel.
- Deux groupes de services avec un membre commun sont liés à ce serveur virtuel, et le membre commun est activé dans un groupe et désactivé dans l'autre.
- Le serveur est désactivé puis réactivé.

Dans ces conditions, la désactivation du serveur désactive tous les membres du groupe de services et la réactivation du serveur active tous les membres, par défaut, quel que soit leur état antérieur. Pour ramener les membres à l'état d'origine, vous devez désactiver manuellement ces membres dans le groupe de services. C'est une tâche lourde et sujette aux erreurs.

Gérer les groupes de services

May 5, 2023

Vous pouvez modifier les paramètres des services d'un groupe de services et effectuer des tâches telles que l'activation, la désactivation et la suppression de groupes de services. Vous pouvez égale-

ment dissocier les membres d'un groupe de services. Pour plus d'informations sur les groupes de services, voir Configurer les groupes de services.

Modifier un groupe de services

Vous pouvez modifier les attributs des membres du groupe de services. Vous pouvez définir plusieurs attributs du groupe de services, tels que le nombre maximal de clients et la compression. Les attributs sont définis sur les serveurs individuels du groupe de services. Vous ne pouvez pas définir de paramètres sur le groupe de services tels que les informations de transport (adresse IP et port), le poids et l'ID du serveur.

Remarque : Un paramètre que vous définissez pour un groupe de services est appliqué aux serveurs membres du groupe, et non aux services individuels.

Pour modifier un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante avec un ou plusieurs des paramètres facultatifs :

```
set servicegroup <serviceGroupName> [-type <type>] [-maxClient <
    maxClient>] [-maxReq <maxReq>] [-cacheable (YES|NO)] [-cip (ENABLED|
    DISABLED)] [-cipHeader <cipHeader>] [-usip (YES|NO)] [-sc (ON|OFF)]
    [-sp (ON|OFF)] [-cltTimeout <cltTimeout>] [-svrTimeout <svrTimeout>]
     [-cka (YES|NO)] [-TCPB (YES|NO)] [-CMP (\*\*YES\*\*|\*\*NO\*\*)] [-
    maxBandwidth <maxBandwidth>] [-maxThreshold <maxThreshold>] [-state
    (ENABLED|DISABLED)] [-downStateFlush (ENABLED|DISABLED)
<!--NeedCopy-->
```

Exemple :

```
set servicegroup Service-Group-1 -type TRANSPARENT

set servicegroup Service-Group-1 -maxClient 4096

set servicegroup Service-Group-1 -maxReq 16384

set servicegroup Service-Group-1 -cacheable YES
<!--NeedCopy-->
```

Pour modifier un groupe de services à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**, puis ouvrez le groupe de services à modifier.

Supprimer un groupe de services

Lorsque vous supprimez un groupe de services, les serveurs liés au groupe conservent leurs paramètres individuels et continuent d'exister sur l'appliance NetScaler.

Pour supprimer un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
rm servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour supprimer un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services, puis cliquez sur **Supprimer**.

Délier un membre d'un groupe de services

Lorsque vous dissociez un membre du groupe de services, les attributs définis sur le groupe de services ne s'appliquent plus au membre que vous dissociez. Les services aux membres conservent toutefois leurs paramètres individuels et continuent d'exister sur l'appliance NetScaler.

Pour dissocier des membres d'un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
unbind servicegroup <serviceGroupName> <IP>@ [<port>]
<!--NeedCopy-->
```

Exemple :

```
unbind servicegroup Service-Group-1 10.102.29.30 80
<!--NeedCopy-->
```


Pour dissocier des membres d'un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Ouvrez un groupe de services et cliquez sur dans la section Membres du groupe de services.
3. Sélectionnez un membre du groupe de services, puis cliquez sur **Unbind (Délier)**.

Délier un groupe de services d'un serveur virtuel

Lorsque vous dissociez un groupe de services d'un serveur virtuel, les services membres sont dissociés du serveur virtuel et continuent d'exister sur l'appliance NetScaler.

Pour dissocier un groupe de services d'un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
unbind lb vserver <name>@ <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
unbind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

Pour dissocier un groupe de services d'un serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ouvrez le serveur virtuel et cliquez sur dans la section Groupe de services.
3. Sélectionnez le groupe de services, puis cliquez sur **Unbind (Délier)**.

Délier les moniteurs des groupes de services

Lorsque vous dissociez un moniteur d'un groupe de services, le moniteur que vous dissociez ne surveille plus les services individuels qui constituent le groupe.

Pour dissocier un moniteur d'un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
unbind serviceGroup <serviceGroupName> -monitorName <string>
<!--NeedCopy-->
```

Exemple :

```
unbind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
<!--NeedCopy-->
```

Pour dissocier un moniteur d'un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Ouvrez un groupe de services, puis cliquez sur dans la section Moniteurs.
3. Sélectionnez un moniteur, puis cliquez sur **Unbind (Délier)**.

Activer ou désactiver un groupe de services

Lorsque vous activez un groupe de services et les serveurs, les services appartenant au groupe de services sont activés. De même, lorsqu'un service appartenant à un groupe de services est activé, le groupe de services et le service sont activés. Par défaut, les groupes de services sont activés.

Après avoir désactivé un service activé, vous pouvez afficher le service à l'aide de l'utilitaire de configuration ou de la ligne de commande pour voir le temps restant avant que le service ne tombe en panne.

Pour désactiver un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
disable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
disable servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour désactiver un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services, puis dans la liste Action, cliquez sur **Désactiver**.

Pour activer un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
enable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
enable servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour activer un groupe de services à l'aide de l'utilitaire de configuration

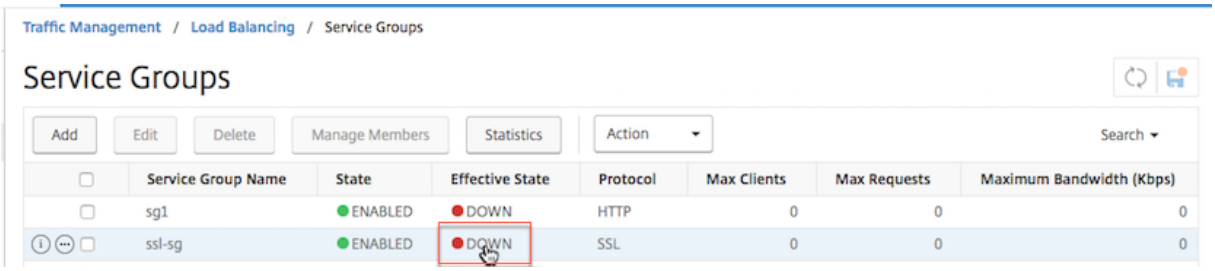
1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services, puis dans la liste Action, cliquez sur **Activer**.

Afficher le statut des membres des groupes de services

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.

Dans la page Groupes de services, la colonne **État effectif** affiche le statut des groupes de services. L'état HAUS/BAS dans la colonne **État effectif** est cliquable. Vous pouvez cliquer sur le statut et obtenir la liste des membres ainsi que leur statut dans la même vue. Sélectionnez un membre et cliquez sur le bouton **Surveiller les détails** pour afficher la raison de l'état en PANNE.

Remarque : Avant la version 12.0 de NetScaler version 56.20, l'état de la colonne **État effectif** n'était pas cliquable.



Affichage des propriétés d'un groupe de services

Vous pouvez afficher les paramètres suivants des groupes de services configurés :

- Nom
- Adresse IP
- State

- Protocole
- Connexions client maximales
- Nombre maximal de demandes par connexion
- Bande passante maximale
- Seuil de surveillance

L'affichage des détails de la configuration peut être utile pour résoudre les problèmes de votre configuration.

Pour afficher les propriétés d'un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour afficher les propriétés du groupe ou les propriétés et les membres du groupe :

```
show servicegroup <ServiceGroupName>

show servicegroup <ServiceGroupName> -includemembers
<!--NeedCopy-->
```

Exemple :

```
show servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour afficher les propriétés d'un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Cliquez sur la flèche en regard du groupe de services.

Affichage des statistiques des groupes de services

Vous pouvez afficher les données statistiques du groupe de services, telles que le taux de demandes, les réponses, les octets de demande et les octets de réponse. L'appliance NetScaler utilise les statistiques d'un groupe de services pour équilibrer la charge sur les services.

Pour afficher les statistiques d'un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
stat servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Exemple :

```
stat servicegroup Service-Group-1
<!--NeedCopy-->
```

Pour afficher les statistiques d'un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services, puis cliquez sur **Statistiques**.

Serveurs virtuels d'équilibrage de charge liés à un groupe de services

Dans les déploiements à grande échelle, le même groupe de services peut être lié à plusieurs serveurs virtuels d'équilibrage de charge. Dans ce cas, au lieu d'afficher chaque serveur virtuel pour voir le groupe de services auquel il est lié, vous pouvez afficher la liste de tous les serveurs virtuels d'équilibrage de charge liés à un groupe de services. Vous pouvez afficher les détails suivants de chaque serveur virtuel :

- Nom
- State
- Adresse IP
- Port

Pour afficher les serveurs virtuels liés à un groupe de services à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour afficher les serveurs virtuels liés à un groupe de services :

```
show servicegroupbindings <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
> show servicegroupbindings SVCGRPDTLS
SVCGRPDTLS - State :ENABLED
1) Test-pers (10.10.10.3:80) - State : DOWN
2) BRVSERV (10.10.1.1:80) - State : DOWN
3) OneMore (10.102.29.136:80) - State : DOWN
```



```
4) LBVIP1 (10.102.29.66:80) - State : UP
Done
>
<!--NeedCopy-->
```

Pour afficher les serveurs virtuels liés à un groupe de services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sélectionnez un groupe de services et, dans la liste Action, cliquez sur **Afficher les liaisons**.

Configurez un ensemble de membres de groupe de services souhaité pour un groupe de services dans un appel d'API NITRO

May 5, 2023

La prise en charge est ajoutée pour configurer un ensemble souhaité de membres de groupe de services pour un groupe de services dans un appel d'API NITRO. Une nouvelle API, l'API d'état souhaité, est ajoutée pour prendre en charge cette configuration. À l'aide de l'API État souhaité, vous pouvez :

- Fournissez une liste des membres du groupe de services dans une seule demande PUT sur la ressource « servicegroup_servicegroupmemberlist_binding ».
- Indiquez leur poids et leur état (facultatif) dans cette demande PUT.
- Synchronisez efficacement la configuration de l'appliance avec les modifications de déploiement autour des serveurs d'applications.

L'appliance NetScaler compare l'ensemble de membres souhaité demandé avec le jeu de membres configuré. Ensuite, il lie automatiquement les nouveaux membres et délie les membres qui ne sont pas présents dans la demande.

Remarque :

- Cette fonctionnalité est prise en charge uniquement pour les groupes de services de type `API`.
- Vous ne pouvez lier des services basés sur des adresses IP qu'à l'aide de l'API d'état souhaité, les services basés sur les noms de domaine ne sont
- Auparavant, un seul membre du groupe de services peut être lié dans un appel NITRO.

> **Important**
>
> L'API State souhaitée pour l'adhésion à ServiceGroup est prise en charge dans le déploiement du cluster NetScaler.

Cas d'utilisation : Synchroniser les modifications de déploiement sur l'appliance NetScaler dans le cadre de déploiements à grande échelle, tels que Kubernetes

Dans les déploiements à grande échelle et hautement dynamiques (par exemple Kubernetes), le défi consiste à maintenir la configuration de l'appliance à jour avec le taux de changement des déploiements afin de répondre avec précision au trafic applicatif. Dans de tels déploiements, les contrôleurs (Ingress ou E-W Controller) sont responsables de la mise à jour de la configuration de ADC. Chaque fois que des modifications sont apportées au déploiement, `kube-api server` envoie l'ensemble effectif de points de terminaison via l' « événement Endpoints » au contrôleur. Le Controller utilise l'approche Read-Delta-Modify où il effectue les opérations suivantes :

- Récupère l'ensemble de points de terminaison actuellement configuré (jeu de membres de groupe de services d'un groupe de services) pour le service à partir de l'appliance ADC.
- Compare l'ensemble de points de terminaison configuré avec celui de l'événement reçu.
- Lie les nouveaux points de terminaison (membres du groupe de services) ou dissocie les points de terminaison supprimés.

Étant donné que le taux de modification et la taille des services sont élevés dans cet environnement, cette méthode de configuration n'est pas efficace et peut retarder les mises à jour de configuration.

L'API d'état désiré résout le problème en acceptant le jeu de membres prévu pour un groupe de services dans une seule API, et met à jour efficacement la configuration.

Créer un groupe de services de type API à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>]
```

Exemple :

```
add serviceGroup svg1 HTTP -autoScale API
```

Vous pouvez configurer les paramètres `autoDisablegraceful`, `autoDisabledelay` et `autoScale` à l'aide de la commande add serviceGroup ou set serviceGroup.

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>] [-autoDisablegraceful ( YES | NO)] [-autoDisabledelay <
    secs>]

add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (API |
    CLOUD | DISABLED| DNS |POLICY)]

```



```
set serviceGroup <serviceGroupName [-autoDisablegraceful ( YES | NO)]
    [-autoDisabledelay <secs>]

set serviceGroup <serviceGroupName [-autoScale (API |CLOUD | DISABLED|
    DNS |POLICY)]
```

Exemple :

```
add serviceGroup svg1 HTTP autoDisablegraceful YES -autoDisabledelay
    100

add serviceGroup svg1 HTTP -autoScale API

set serviceGroup svg1 -autoDisablegraceful  YES -autoDisabledelay 100

set serviceGroup svg1 -autoScale API
```

Arguments

autoDisablegraceful

Indique l'arrêt normal du service. Si cette option est activée, l'appliance attend que toutes les connexions en suspens à ce service soient fermées avant de supprimer le service. Pour les clients qui ont déjà une session persistante sur le système, de nouvelles connexions ou demandes continuent d'être envoyées à ce service. Le membre du service est supprimé uniquement s'il n'y a aucune connexion en attente. Valeur par défaut : NON

autoDisabledelay

Indique le temps alloué (en secondes) pour un arrêt progressif. Au cours de cette période, de nouvelles connexions ou demandes continuent d'être envoyées à ce service pour les clients qui ont déjà une session persistante sur le système. Les connexions ou les demandes de nouveaux clients qui n'ont pas de session de persistance sur le système ne sont pas envoyées au service. Au lieu de cela, ils sont équilibrés en charge entre les autres services disponibles. Une fois le délai expiré, le membre du service est supprimé.

API Autoscale

L'argument API Autoscale permet d'utiliser l'API État souhaité pour lier le jeu de membres à un groupe de services prévu. Vous pouvez définir le groupe de services de type non-autoscale au type Autoscale de l'API d'état souhaité, si toutes les conditions fournies correspondent.

L'API d'état souhaité vérifie si l'adresse IP du membre du groupe de services est associée à un serveur existant. Si l'adresse IP correspond à un serveur existant, l'API réutilise l'adresse IP et le nom du serveur existant. Si l'adresse IP ne correspond à aucun serveur existant, l'API crée un serveur et attribue l'adresse IP elle-même comme nom de serveur.

Exemple :

Prenons l'exemple d'un serveur dont l'adresse IP est 2.2.2.2 et dont le nom est myserver et qui existe dans une appliance NetScaler. À l'aide de l'API d'état souhaitée, vous liez un ensemble de membres du groupe de services dont l'adresse IP est comprise entre 2.2.2.1 et 2.2.2.3.

Comme l'adresse IP 2.2.2.2 est associée à un serveur existant, l'API réutilise l'adresse IP et le nom (2.2.2.2 et monserveur). Comme il n'existe aucun serveur avec des adresses IP 2.2.2.1, 2.2.2.3, l'API crée des serveurs avec ces adresses IP. L'API attribue l'adresse IP elle-même comme nom du serveur.

Si l'adresse IP fournie dans la commande d'état souhaitée entre en conflit avec d'autres entités NetScaler telles que le serveur virtuel CS, un conflit se produit. Un message d'erreur contenant la raison de l'échec s'affiche. L'adresse IP du premier membre du groupe de services parmi la liste des membres ayant échoué est affichée dans le message d'erreur.

Exemple :

Prenons l'exemple d'un serveur dont l'adresse IP est 2.2.2.8 et qui est utilisé comme serveur LB. À l'aide de l'API d'état souhaitée, vous essayez de lier un ensemble de membres du groupe de services dont l'adresse IP est comprise entre 2.2.2.2 et 2.2.2.11.

Comme 2.2.2.8 est déjà utilisé pour le service LB, un conflit se produit. Le message d'erreur suivant s'affiche et contient la raison de l'échec et les liaisons de membres ayant échoué :

```
{
  "errorcode": 304, "message": "Address already in use", "severity": "
     ERROR", "servicegroup_servicegroupmemberlist_binding": {
  "servicegroupname": "sg1", "failedmembers": [ {
  "ip": "2.2.2.8", "port": 80  }
 , {
  "ip": "2.2.2.9", "port": 80  }
  ]  }
   }

<!--NeedCopy-->
```

Le code d'erreur 304 affiche le premier membre du groupe de services parmi la liste des membres défaillants, qui est 2.2.2.8.

La commande `set serviceGroup Autoscale` peut échouer si les liaisons de membres existantes répondent à l'une des conditions suivantes :

- Si le serveur lié au groupe de services est un serveur de noms ou un serveur basé sur un domaine.
- Si le nom du serveur de bouclage est autre que 127.0.0.1 ou 0000:0000:0000:0000:0000:0000:0000:0001.
- Si vous choisissez différents types de Autoscale (Cloud, API, DNS et stratégie) dans une commande set ServiceGroup et ajoutez la commande ServiceGroup.

Important :

- Les paramètres AutoDisableGraceful et AutoDisableDelay s'appliquent uniquement aux groupes de services de type Autoscale « API » et « CLOUD ».
- Si les paramètres AutoDisableGraceful ou AutoDisableDelay ne sont pas configurés, les membres du service sont immédiatement supprimés.

Dissocier un membre d'un groupe de services avec élégance

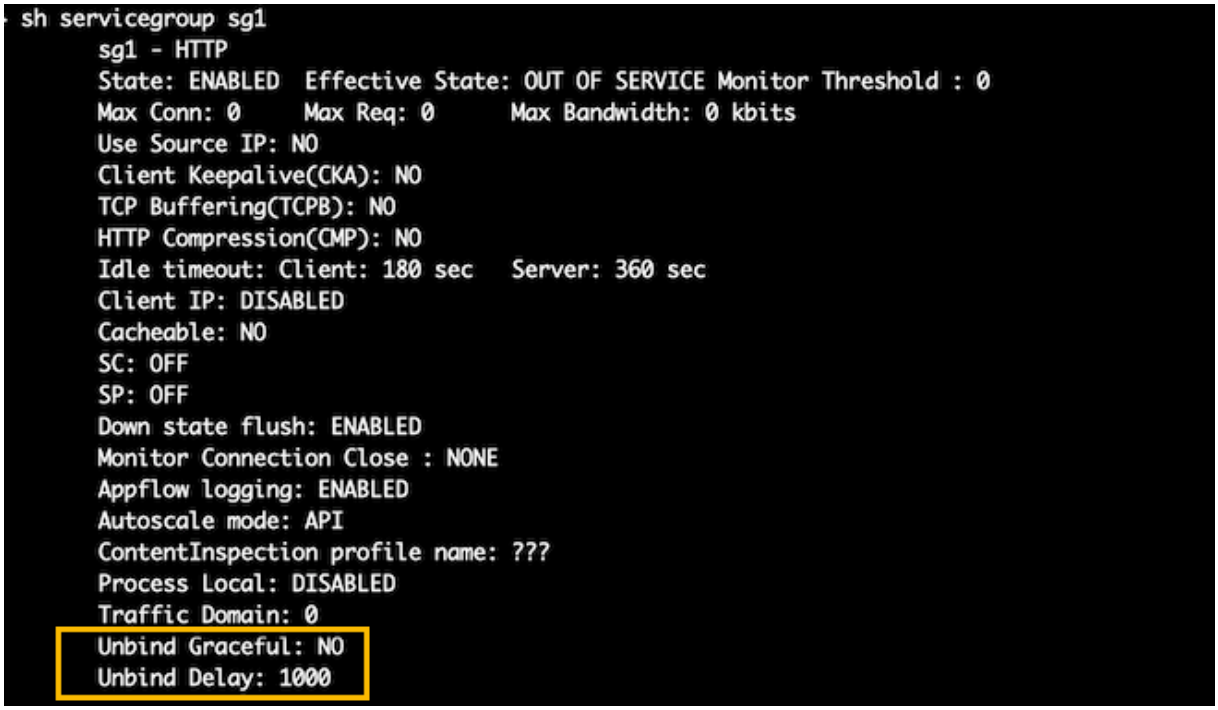
Si l'un des membres du groupe de services ne figure pas dans la liste des états souhaités, ces membres sont indépendants de manière gracieuse en fonction de la configuration du paramètre `autoDisablegraceful` ou `autoDisabledelay`.

- Si l'un de ces paramètres est défini, le membre du groupe de services n'est pas lié correctement.
- Si aucun de ces paramètres n'est défini, le membre du groupe de services est immédiatement indépendant.

Remarque :

- Les membres du groupe de services identifiés pour une déliaison gracieuse sont affichés uniquement lorsque la commande show service group est exécutée.
- Vous ne pouvez pas effectuer d'opération (définie, non définie, par exemple) sur le membre du groupe de services identifié pour la déliaison gracieuse.

La figure suivante montre un exemple de commande show service group.

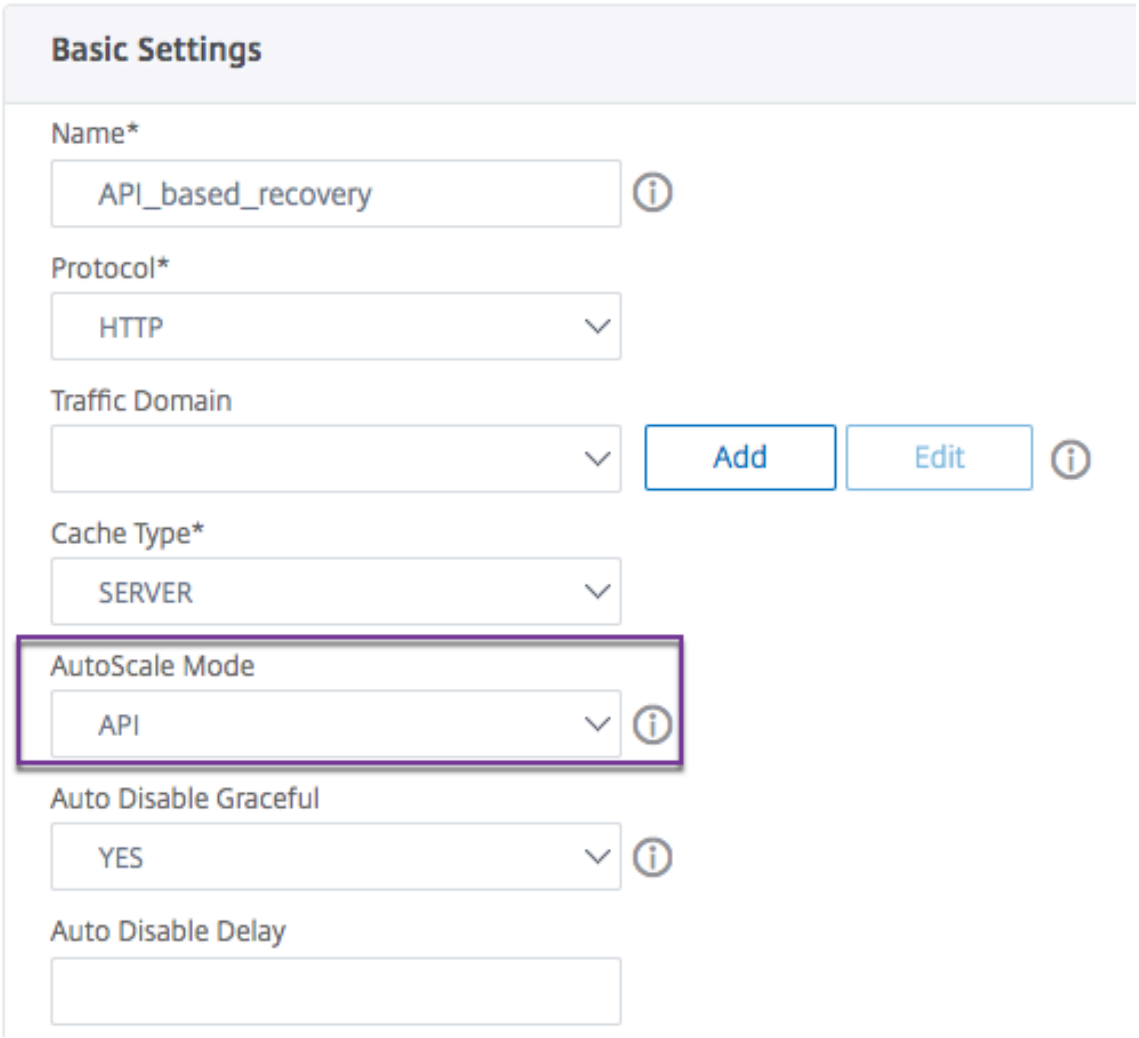


Créer un groupe de services de type API à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services**, puis cliquez sur **Ajouter**.
2. En **mode AutoScale**, sélectionnez **API**.

Configurer un arrêt progressif ou un délai pour un groupe de services de type API à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services**.



2. En **mode AutoScale**, sélectionnez **API**.
3. Dans **Auto Disable Graceful**, sélectionnez **OUI**.
4. Dans **Délai de désactivation automatique**, saisissez le temps d'attente pour un arrêt progressif.

Remarque : Les champs **Désactivation automatiqueou Délai d'affichage automatique**sont activés uniquement si vous sélectionnez**API**ou**CLOUD**en**mode AutoScale**.

Configurer le dimensionnement automatique des groupes de services basés sur le domaine

May 5, 2023

Un groupe de services basé sur un domaine se compose de membres dont les adresses IP sont

obtenues en résolvant les noms de domaine des serveurs liés au groupe de services. Les noms de domaine sont résolus par un serveur de noms dont vous configurez les détails sur l'appliance. Un groupe de services basé sur un domaine peut également inclure des membres basés sur l'adresse IP.

Le processus de résolution de noms pour un serveur basé sur un domaine peut renvoyer plusieurs adresses IP. Le nombre d'adresses IP dans la réponse DNS est déterminé par le nombre d'enregistrements d'adresse (A) configurés pour le nom de domaine, sur le serveur de noms. Même si le processus de résolution de noms renvoie plusieurs adresses IP, une seule adresse IP est liée au groupe de services. Pour augmenter ou réduire l'échelle d'un groupe de services, vous devez lier et dissocier manuellement d'autres serveurs basés sur un domaine vers et depuis le groupe de services, respectivement.

Toutefois, vous pouvez configurer un groupe de services basé sur un domaine pour qu'il soit mis à l'échelle automatiquement en fonction de l'ensemble complet des adresses IP renvoyées par un serveur de noms DNS pour un serveur basé sur un domaine. Pour configurer la mise à l'échelle automatique, lorsque vous liez un serveur basé sur un domaine à un groupe de services, activez l'option de dimensionnement automatique. Voici les étapes à suivre pour configurer un groupe de services basé sur un domaine qui se met à l'échelle automatiquement :

- Ajoutez un serveur de noms pour résoudre les noms de domaine. Pour plus d'informations sur la configuration d'un serveur de noms sur l'appliance, voir Ajout d'un serveur de noms.
- Ajoutez un serveur basé sur un domaine. Pour plus d'informations sur l'ajout d'un serveur basé sur un domaine, voir Configuration d'un objet serveur.
- Ajoutez un groupe de services et associez le serveur basé sur le domaine au groupe de services, l'option Mise à l'échelle automatique étant définie sur DNS. Pour plus d'informations sur l'ajout d'un groupe de services, reportez-vous à la section Configuration des groupes de services.

Lorsqu'un serveur basé sur un domaine est lié à un groupe de services et que l'option de mise à l'échelle automatique est définie sur la liaison, un moniteur UDP et un moniteur TCP sont automatiquement créés et liés au serveur basé sur le domaine. Les deux moniteurs fonctionnent comme des résolveurs. Le moniteur TCP est désactivé par défaut et l'appliance utilise le moniteur UDP pour envoyer des requêtes DNS au serveur de noms afin de résoudre le nom de domaine. Si la réponse DNS est tronquée (l'indicateur TC est défini sur 1), l'appliance revient au protocole TCP et utilise le moniteur TCP pour envoyer les requêtes DNS via TCP. Par la suite, l'appliance continue d'utiliser uniquement le moniteur TCP.

La réponse DNS du serveur de noms peut contenir plusieurs adresses IP pour le nom de domaine. Lorsque l'option de mise à l'échelle automatique est définie, l'appliance interroge chacune des adresses IP à l'aide du moniteur par défaut, puis inclut dans le groupe de services uniquement les adresses IP qui sont activées et disponibles. Après l'expiration des enregistrements d'adresse IP, tel que défini par leurs valeurs de durée de vie (TTL), le moniteur UDP (ou le moniteur TCP, si l'appliance est revenue à l'utilisation du moniteur TCP) interroge le serveur de noms pour la résolution de domaine et inclut toutes les nouvelles adresses IP du groupe de services. Si une adresse IP qui fait partie

du groupe de services n'est pas présente dans la réponse DNS, l'appliance supprime cette adresse du groupe de services après avoir fermé progressivement les connexions existantes au membre du groupe, processus au cours duquel elle n'autorise pas l'établissement de nouvelles connexions avec le membre. Si un nom de domaine qui a été résolu avec succès dans le passé entraîne une réponse NXDOMAIN, tous les membres du groupe de services associés à ce domaine sont supprimés.

Les membres statiques (basés sur l'adresse IP) et les membres basés sur le domaine à dimensionnement dynamique peuvent coexister dans un groupe de services. Vous pouvez également lier des membres ayant des noms de domaine différents à un groupe de services à l'aide du jeu d'options de dimensionnement automatique. Toutefois, chaque nom de domaine associé à un groupe de services doit être unique au sein du groupe de services. Vous devez activer l'option de dimensionnement automatique pour chaque serveur basé sur un domaine que vous souhaitez utiliser pour la mise à l'échelle automatique des groupes de services. Si une adresse IP est commune à un ou plusieurs domaines, l'adresse IP n'est ajoutée au groupe de services qu'une seule fois.

> **Important**
>
> - DNS Autoscale est pris en charge dans un déploiement de cluster.
> - La surveillance des chemins pour les groupes de services Autoscale n'est pas prise en charge dans le déploiement du cluster

Pour configurer un groupe de services pour qu'il évolue automatiquement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le groupe de services et vérifier la configuration :

```
add servicegroup <serviceGroupName> <serviceType> -autoscale DNS
<!--NeedCopy-->
```

Exemple

Dans l'exemple suivant, serveur1 est un serveur basé sur un domaine. La réponse DNS contient plusieurs adresses IP. Cinq adresses sont disponibles et sont ajoutées au groupe de services.

```
> add serviceGroup servGroup -autoScale YES
 Done
> sh servicegroup servGroup
       servGroup - HTTP
        State: ENABLED  Monitor Threshold : 0
              . . .
              . . .
```



```
        1)   192.0.2.31:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        2)   192.0.2.32:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        3)   192.0.2.36:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        4)   192.0.2.55:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        5)   192.0.2.80:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.
 Done
<!--NeedCopy-->
```

Pour configurer un groupe de services pour qu'il évolue automatiquement à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Créez un groupe de services et définissez le mode Autoscale sur DNS.

Remplacement des valeurs TTL

> **Remarque :**
>
> Cette option est prise en charge à partir de NetScaler 12.1 build 51.xx et versions ultérieures.

L'appliance NetScaler est configurée pour interroger régulièrement le serveur DNS pour toute mise à jour de l'enregistrement SRV associé à l'application lors du démarrage de l'application. Par défaut, la périodicité de cette requête dépend de la durée de vie publiée dans l'enregistrement SRV. Dans les applications du monde des microservices ou du cloud, les déploiements changent de manière plus dynamique. Par conséquent, les proxys doivent absorber plus rapidement les modifications apportées au déploiement des applications. Par conséquent, il est recommandé aux utilisateurs de définir explicitement le paramètre TTL du service basé sur le domaine sur une valeur inférieure à la durée de vie de l'enregistrement SRV et optimale pour votre déploiement. Vous pouvez remplacer la valeur TTL par deux méthodes :

- Lors de la liaison d'un membre au groupe de services
- Définition de la valeur TTL globalement à l'aide de la commande set lb parameter.

Si la valeur TTL est configurée à la fois lors de la liaison du membre du groupe de services et également globalement, la valeur TTL spécifiée lors de la liaison du membre du groupe de services est prioritaire. Si la valeur TTL n'est pas spécifiée lors de la liaison d'un membre d'un groupe de services ou au niveau global, l'intervalle de surveillance DBS est dérivé de la valeur TTL dans la réponse DNS.

Remplacement des valeurs TTL à l'aide de la CLI

- Pour remplacer la valeur TTL lors de la liaison, à l'invite de commandes, tapez :

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
    >])
<!--NeedCopy-->
```

Exemple :

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```

- Pour remplacer la valeur TTL globalement, à l'invite de commandes, tapez :

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -dbsTTL 15
<!--NeedCopy-->
```


Remplacement des valeurs TTL à l'aide de l'interface graphique

Pour remplacer la valeur TTL lors de la liaison :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage de charge**, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Modifier**.
5. Dans la zone Durée de **vie du service basé sur le domaine**, entrez la valeur TTL.

Pour remplacer la valeur TTL au niveau global :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Modifier les paramètres d'équilibrage de charge**.
2. Dans la zone Durée de **vie du service basé sur le domaine**, entrez la valeur TTL.

> **Remarque :**
>
> Si la valeur TTL du serveur basé sur le domaine est définie sur 0, la valeur TTL du paquet de données est utilisée.

Spécification de différents serveurs de noms pour les liaisons de groupes de services et de noms de domaine

> **Remarque :**
>
> Cette option est prise en charge à partir de NetScaler 12.1 build 51.xx et versions ultérieures.

Vous pouvez configurer différents serveurs de noms pour différents noms de domaine dans un groupe spécifique. La définition du paramètre NameServer est facultative lors de la liaison d'un serveur DBS au groupe de services. Lorsqu'aucun serveur de noms n'est spécifié lors de la liaison d'un membre au groupe de services, le serveur de noms configuré globalement est pris en compte.

Spécification de serveurs de noms lors de la liaison d'un serveur à des groupes de services à l'aide

À l'invite de commande, tapez :

```
bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
    ip_addr>] [-dbsTTL <secs>])
<!--NeedCopy-->
```


Exemple :

```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
    -dbsTTL 10
<!--NeedCopy-->
```

Spécification de serveurs de noms lors de la liaison d'un serveur à des groupes de services à l'aide

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage de charge**, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Modifier**.
5. Dans **Name Server**, spécifiez le nom du serveur de noms auquel la requête du domaine lié doit être envoyée.

TROFS à retard automatique

Vous pouvez configurer le déplacement progressif des membres d'un groupe de services vers l'état TROFS lorsque les adresses IP sont supprimées de la réponse DNS. Lorsque l'option TROFS à retard automatique est activée, NetScaler attend le délai de réponse le plus élevé sur tous les moniteurs connectés au groupe de services avant de faire passer les membres à l'état TROFS.

Cette option est utile lorsqu'un nouvel ensemble d'adresses IP remplace complètement les adresses existantes et que la connectivité doit être vérifiée avant d'ajouter les nouvelles adresses IP.

> **Remarque :**
>
> `-autoDelayedTrofs` Cette option est prise en charge à partir de NetScaler 13.1 build 37.xx et versions ultérieures.

Configurer TROFS à retard automatique à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>] [-autoDelayedTrofs ( YES | NO)]
<!--NeedCopy-->
```

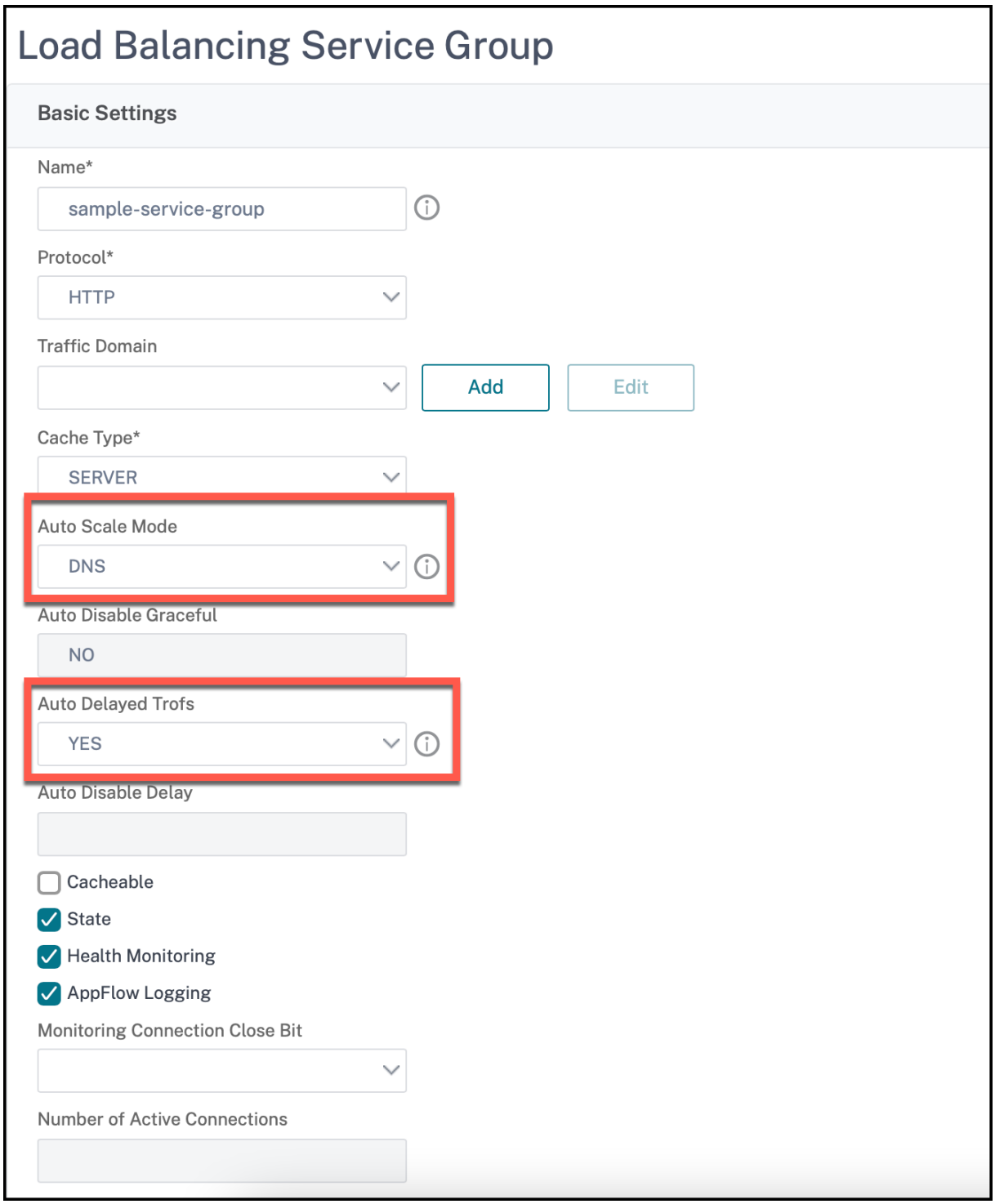

Exemple

```
> add serviceGroup sg1 HTTP -autoScale DNS -autoDelayedTrofs YES
<!--NeedCopy-->
```

Configuration de TROFS à temporisation automatique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services**.
2. En **mode Mise à l'échelle automatique**, sélectionnez **DNS**.
3. Dans **Auto Delayed Trofs**, sélectionnez **OUI**.

> **Remarque :**
>
> L'option Auto Delayed Trofs n'est activée que si vous sélectionnez DNS en mode AutoScale.



Découverte de services à l'aide d'enregistrements DNS SRV

May 5, 2023

Un enregistrement SRV (enregistrement de service) est une spécification des données du système de noms de domaine qui définit l'emplacement, c'est-à-dire le nom d'hôte et le numéro de port des serveurs pour des services spécifiés. L'enregistrement définit également le poids et la priorité de chaque serveur.

Exemple d'enregistrement SRV :

_http._tcp.example.com. 100 DANS SRV 10 60 5060 a.example.com.

Le tableau suivant décrit chaque élément d'un enregistrement SRV :

Service	Protocol	Name	TTL	Class	SRV	Priority	Weight	Port	Target
HTTP	TCP	example.com	100	IN	SRV	10	60	5060	a.example.com

Vous pouvez utiliser les enregistrements SRV DNS pour découvrir les points de terminaison du service. L'appliance NetScaler est configurée pour interroger régulièrement les serveurs DNS avec l'enregistrement SRV associé à un service. À la réception de l'enregistrement SRV, chacun des hôtes cibles publiés dans l'enregistrement SRV est lié à un groupe de services associé au service. Chacune des liaisons hérite du port, de la priorité et du poids de l'enregistrement SRV. Pour chaque déploiement de service, l'utilisateur doit configurer l'appliance NetScaler une seule fois lors de son lancement, ce qui en fait un déploiement d'une seule touche pour les applications.

Important : Le poids des membres du groupe de services appris dynamiquement ne peut pas être modifié à l'aide de l'interface de ligne de commande ou de l'interface graphique.

Cas d'utilisation : microservices d'équilibrage de charge

Les applications évoluent vers une architecture de microservices à partir d'architectures monolithiques. Le passage à l'architecture de microservices avec une solution d'échelle automatique du serveur back-end rend le déploiement d'applications plus dynamique. Pour prendre en charge un tel déploiement dynamique, les proxy ou ADC doivent être en mesure de détecter dynamiquement l'application ou les instances de service back-end et de les absorber dans la configuration du proxy.
La fonctionnalité de découverte de services à l'aide des enregistrements DNS SRV facilite la configuration de l'appliance NetScaler dans un tel scénario de déploiement dynamique. Les développeurs d'applications peuvent utiliser certaines des plates-formes d'orchestration pour déployer l'application. Les plates-formes d'orchestration lors de l'instanciation de conteneurs pendant le déploiement d'applications peuvent ne pas attribuer le port standard spécifique au protocole pour chacun de ces conteneurs. Dans de tels scénarios, la découverte des informations de port devient la clé de la configuration de l'appliance NetScaler. Les enregistrements SRV sont utiles dans un tel scénario. Les paramètres d'enregistrement SRV tels que la priorité et le poids peuvent être utilisés pour un meilleur équilibrage de charge des applications.

- Le paramètre Priority peut être utilisé pour dicter la priorité du pool de serveurs.

- Le paramètre de poids peut être utilisé pour dicter la capacité des instances du service principal et peut donc être utilisé pour l'équilibrage de charge pondéré.
- Chaque fois que le pool de serveurs principaux est modifié, par exemple qu'une instance principale est supprimée du pool, l'instance n'est supprimée gracieusement qu'une fois que toutes les connexions client existantes ont été honorées.

> **Remarque :**
>
> - Lors d'une découverte de service basée sur les enregistrements A/AAAA, toutes les adresses IP résolues ont le même poids car vous attribuez le poids au domaine en cours de résolution.
> - Si le poids de la réponse SRV est supérieur à 100, aucun service n'est créé.

Équilibrage de charge basé sur les priorités à l'aide d'enregistrements SRV

Vous pouvez utiliser les enregistrements SRV pour effectuer un équilibrage de charge basé sur les priorités. Le pool de serveurs basé sur les priorités peut être une alternative aux serveurs virtuels de sauvegarde. Le fichier ns.conf nécessite une configuration minimale par rapport aux serveurs virtuels de sauvegarde.

Dans l'équilibrage de charge basé sur la priorité à l'aide d'enregistrements SRV, un numéro de priorité est attribué à chaque pool de serveurs. Le nombre le plus faible a la priorité la plus élevée. L'un des serveurs du pool de priorité la plus élevée est sélectionné pour l'équilibrage de charge en fonction de l'intégrité et de la disponibilité du serveur. Si tous les serveurs du pool de serveurs ayant la priorité la plus élevée sont hors service, les serveurs ayant la priorité la plus élevée sont sélectionnés pour l'équilibrage de charge. Toutefois, si les serveurs du pool de serveurs de priorité la plus élevée sont de nouveau opérationnels, ils sont de nouveau sélectionnés dans le pool de priorité la plus élevée.

Le passage d'un pool de serveurs prioritaires à un autre pool de serveurs se fait facilement en effacant les transactions client existantes. Par conséquent, les clients actuels ne constatent aucune rupture dans l'accès à l'application.

Pour activer la recherche d'enregistrements SRV à l'aide de l'interface de ligne de commande

Effectuez les tâches suivantes pour activer la recherche d'enregistrements SRV :

1. Créez un serveur en spécifiant le paramètre de type de requête comme SRV.

   À l'invite de commande, tapez :

   ```
   add server <name> <domain> [-queryType <queryType>])
   <!--NeedCopy-->
   ```

   Exemple :


```
add server web_serv example.com -queryType SRV
<!--NeedCopy-->
```

Remarque :

- Par défaut, les requêtes IPv4 sont envoyées. Pour envoyer des requêtes IPv6, vous devez activer le domaine IPv6.
- Le nom de domaine cible SRV ne doit pas dépasser 127 caractères.

2. Créez un groupe de services avec le mode autoscale comme DNS.

   À l'invite de commande, tapez :

```
add serviceGroup <serviceGroupName> <serviceType> [-autoScale <
   autoScale>]
<!--NeedCopy-->
```

   Exemple :

```
add servicegroup svc_grp_1 http -autoscale dns
<!--NeedCopy-->
```

3. Liez le serveur créé à l'étape 1 au groupe de services en tant que membre.

   À l'invite de commande, tapez :

```
bind serviceGroup <serviceGroupName> <serverName>
<!--NeedCopy-->
```

   Exemple :

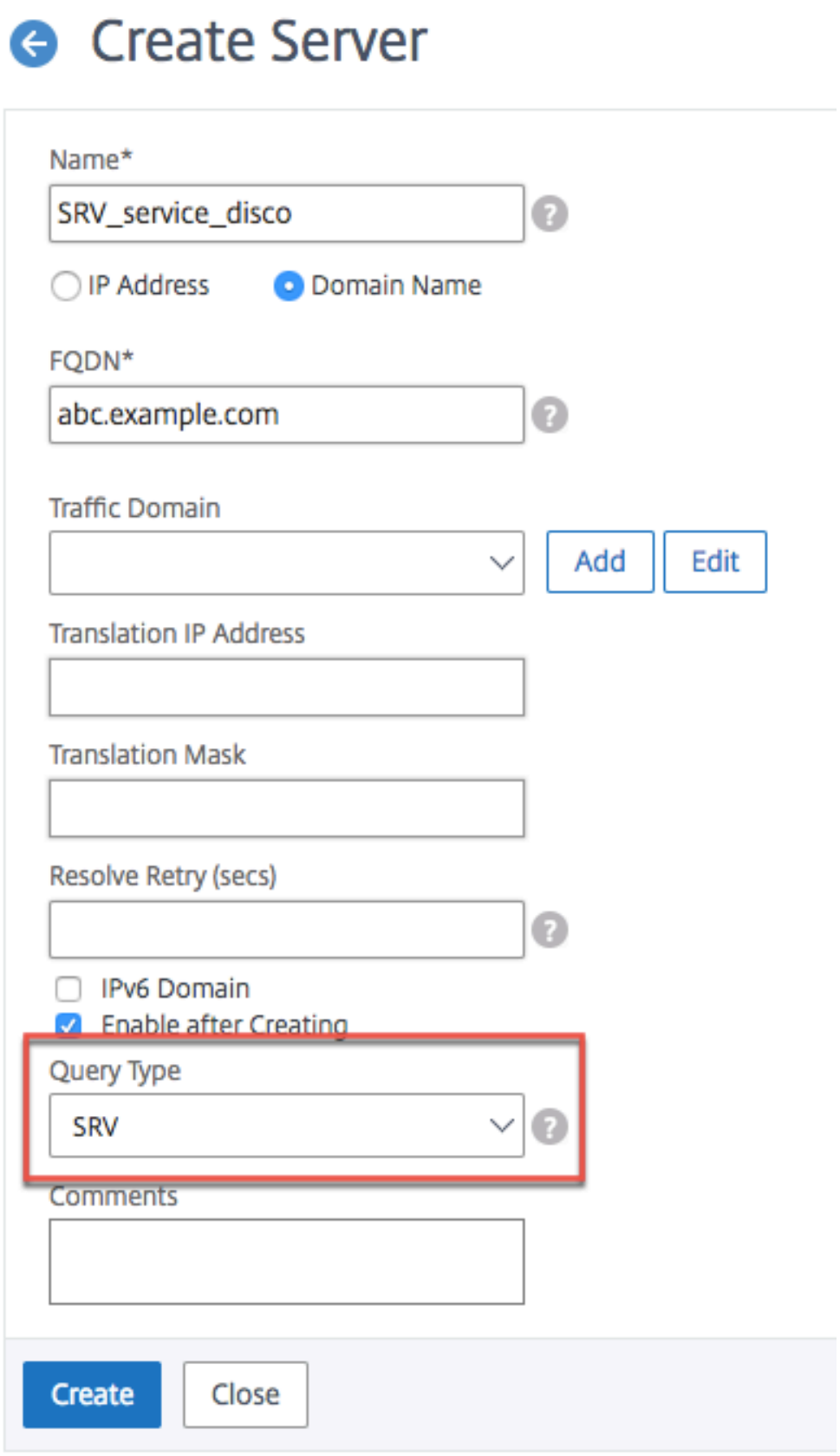
```
bind servicegroup svc_grp_1 web_serv
<!--NeedCopy-->
```

> **Remarque :**
>
> - Lorsque vous liez des serveurs à des membres du groupe de services, vous n'avez pas à saisir le numéro de port pour les types de serveurs SRV. Si vous spécifiez un numéro de port pour le type de serveur SRV, un message d'erreur s'affiche.
> - Vous pouvez éventuellement spécifier un serveur de noms et une valeur TTL lors de la liaison d'un serveur au groupe de services.

Pour activer la recherche d'enregistrements SRV à l'aide de l'interface graphique

Création d'un serveur

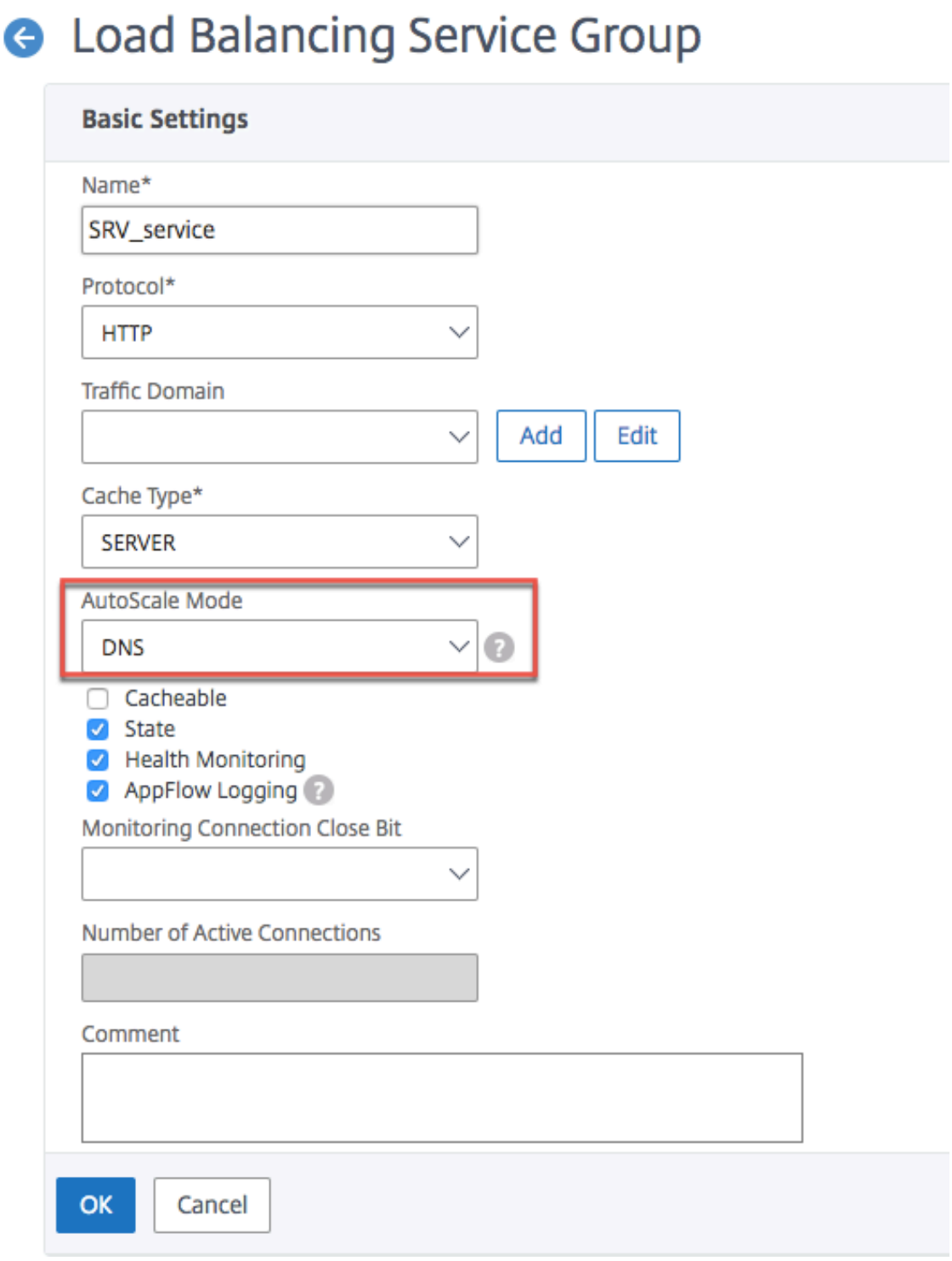
1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs**, puis cliquez sur **Ajouter** .



2. Dans la page **Créer un serveur**, sélectionnez nom de domaine.
3. Entrez les détails de tous les paramètres requis.
4. Dans **Type de requête**, sélectionnez **SRV**.
5. Cliquez sur **Create**.

Créez un groupe de services avec le mode autoscale comme DNS

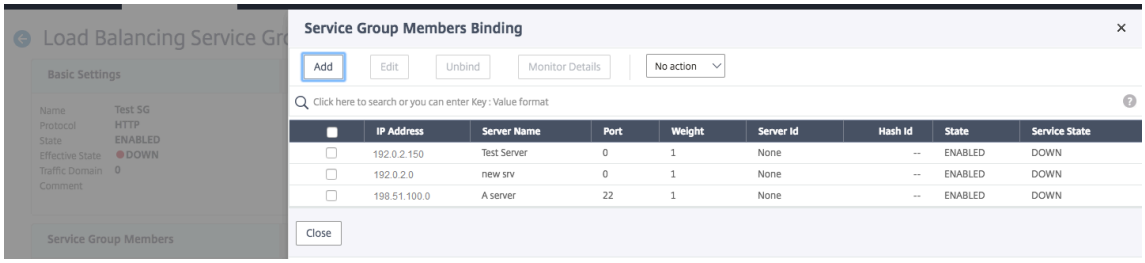
1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Sur la page **Load Balancing Service Group**, entrez les détails de tous les paramètres requis.
3. En **mode Mise à l'échelle automatique**, sélectionnez **DNS**.



4. Cliquez sur **OK**.

Lier le serveur au membre du groupe de services

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage de charge**, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Fermer** .



Remarque :

- Lors de la liaison, il n'est pas nécessaire de saisir le numéro de port pour les types de serveurs SRV. Si vous entrez un numéro de port pour le type de serveur SRV, un message d'erreur s'affiche.
- Vous pouvez éventuellement spécifier un serveur de noms et une valeur TTL lors de la liaison d'un serveur au groupe de services.

Remplacement des valeurs TTL

L'appliance NetScaler est configurée pour interroger régulièrement le serveur DNS pour toute mise à jour de l'enregistrement SRV associé à l'application lors du démarrage de l'application. Par défaut, la périodicité de cette requête dépend de la durée de vie publiée dans l'enregistrement SRV. Dans les applications du monde des microservices ou du cloud, les déploiements changent de manière plus dynamique. Par conséquent, les proxys doivent absorber plus rapidement les modifications apportées au déploiement des applications. Par conséquent, il est recommandé aux utilisateurs de définir explicitement le paramètre TTL du service basé sur le domaine sur une valeur inférieure à la durée de vie de l'enregistrement SRV et optimale pour votre déploiement. Vous pouvez remplacer la valeur TTL par deux méthodes :

- Lors de la liaison d'un membre au groupe de services
- Définition de la valeur TTL globalement à l'aide de la commande set lb parameter.

Si la valeur TTL est configurée à la fois lors de la liaison du membre du groupe de services et également globalement, la valeur TTL spécifiée lors de la liaison du membre du groupe de services est prioritaire. Si la valeur TTL n'est pas spécifiée lors de la liaison d'un membre d'un groupe de services ou au niveau global, l'intervalle de surveillance DBS est dérivé de la valeur TTL dans la réponse DNS.

Remplacement des valeurs TTL à l'aide de la CLI

- Pour remplacer la valeur TTL lors de la liaison, à l'invite de commandes, tapez :

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
    >])
<!--NeedCopy-->
```

Exemple :

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```

- Pour remplacer la valeur TTL globalement, à l'invite de commandes, tapez :

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Exemple :

```
set lb parameter -dbsTTL 15
<!--NeedCopy-->
```

Remplacement des valeurs TTL à l'aide de l'interface graphique

Pour remplacer la valeur TTL lors de la liaison :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage de charge**, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Modifier**.
5. Dans la zone Durée de **vie du service basé sur le domaine**, entrez la valeur TTL.

Pour remplacer la valeur TTL au niveau global :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Modifier les paramètres d'équilibrage de charge**.
2. Dans la zone Durée de **vie du service basé sur le domaine**, entrez la valeur TTL.

> **Remarque** : Si la valeur TTL du serveur basé sur un domaine est définie sur 0, la valeur TTL du paquet de données est utilisée.

Spécification de différents serveurs de noms pour les liaisons de groupes de services et de noms de domaine

Vous pouvez configurer différents serveurs de noms pour différents noms de domaine dans un groupe spécifique. La définition du paramètre NameServer est facultative lors de la liaison d'un serveur DBS au groupe de services. Lorsqu'aucun serveur de noms n'est spécifié lors de la liaison d'un membre au groupe de services, le serveur de noms configuré globalement est pris en compte.

Spécification de serveurs de noms lors de la liaison d'un serveur à des groupes de services à l'aide

À l'invite de commande, tapez :

```
bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
    ip_addr>] [-dbsTTL <secs>])
<!--NeedCopy-->
```

Exemple :

```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
    -dbsTTL 10
<!--NeedCopy-->
```

Spécification de serveurs de noms lors de la liaison d'un serveur à des groupes de services à l'aide

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Groupes de services**.
2. Dans la page **Groupes de services**, sélectionnez le groupe de services que vous avez créé et cliquez sur **Modifier**.
3. Dans la page **Groupes de services d'équilibrage de charge**, cliquez sur **Membres du groupe de services**.
4. Dans la page **Liaison de membres du groupe de services**, sélectionnez le serveur que vous avez créé et cliquez sur **Modifier**.
5. Dans **Name Server**, spécifiez le nom du serveur de noms auquel la requête du domaine lié doit être envoyée.

Traduire l'adresse IP d'un serveur de domaine

May 5, 2023

Pour simplifier la maintenance de l'appliance NetScaler et des serveurs basés sur des domaines qui y sont connectés, vous pouvez configurer des masques d'adresses IP et des adresses IP de traduction. Ces fonctions fonctionnent ensemble pour analyser les paquets DNS entrants et remplacer une nouvelle adresse IP par une adresse IP résolue par le DNS.

Lorsqu'elle est configurée pour un serveur basé sur un domaine, la traduction d'adresses IP permet à l'appliance de localiser une autre adresse IP de serveur lorsque vous arrêtez le serveur pour maintenance ou si vous effectuez d'autres modifications d'infrastructure affectant le serveur.

Lors de la configuration du masque, vous devez utiliser des valeurs de masque IP standard (une puissance de deux, moins un) et des zéros, par exemple, 255.255.0.0. Les valeurs différentes de zéro ne sont autorisées que dans les octets de départ.

Lorsque vous configurez une adresse IP de traduction pour un serveur, vous créez une correspondance 1:1 entre l'adresse IP d'un serveur et un autre serveur qui partage les octets de début ou de fin de son adresse IP. Le masque bloque certains octets de l'adresse IP du serveur d'origine. L'adresse IP résolue par DNS est transformée en une nouvelle adresse IP en appliquant l'adresse IP de traduction et le masque de traduction.

Par exemple, vous pouvez configurer une adresse IP de traduction 10.20.0.0 et un masque de traduction 255.255.0.0. Si l'adresse IP résolue par DNS pour un serveur est 40.50.27.3, cette adresse est transformée en 10.20.27.3. Dans ce cas, l'adresse IP de traduction fournit les deux premiers octets de la nouvelle adresse et le masque passe par les deux derniers octets de l'adresse IP d'origine. La référence à l'adresse IP d'origine, telle que résolue par le DNS, est perdue. Les surveillants de tous les services auxquels le serveur est lié signalent également l'adresse IP transformée.

Lorsque vous configurez une adresse IP de traduction pour un serveur basé sur un domaine, vous spécifiez un masque et une adresse IP vers lesquels l'adresse IP résolue par DNS doit être traduite.

Remarque : La traduction de l'adresse IP n'est possible que pour les serveurs basés sur un domaine. Vous ne pouvez pas utiliser cette fonctionnalité pour les serveurs IP. Le modèle d'adresse peut être basé uniquement sur les adresses IPv4.

Pour configurer une adresse IP de traduction pour un serveur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add server <name>@ <serverDomainName> -translationIp <
    translationIPAddress> -translationMask <netMask> -state <ENABLED|
    DISABLED>
<!--NeedCopy-->
```

Exemple :

```
add server myMaskedServer www.example.com -translationIp 10.10.10.10 -
    translationMask
255.255.0.0 -state ENABLED
<!--NeedCopy-->
```

Pour configurer une adresse IP de traduction pour un serveur à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs**, créez un serveur basé sur un domaine et spécifiez une adresse IP de traduction.

Masquer l'adresse IP d'un serveur virtuel

May 5, 2023

Vous pouvez configurer un masque et un modèle au lieu d'une adresse IP fixe pour un serveur virtuel. Cela permet de rediriger le trafic dirigé vers n'importe quelle adresse IP correspondant au masque et au modèle vers un serveur virtuel particulier. Par exemple, vous pouvez configurer un masque qui autorise la variable des trois premiers octets d'une adresse IP, de sorte que le trafic vers 111.11.11.198, 22.22.22.198 et 33.33.33.198 soit envoyé au même serveur virtuel.

En configurant un masque pour l'adresse IP d'un serveur virtuel, vous pouvez éviter la reconfiguration de vos serveurs virtuels en raison d'une modification du routage ou d'une autre modification de l'infrastructure. Le masque permet au trafic de continuer à circuler sans reconfiguration étendue de vos serveurs virtuels.

Le masque d'adresse IP d'un serveur virtuel fonctionne différemment d'une définition de modèle IP pour un serveur décrite dans la section Traduction de l'adresse IP d'un serveur de domaine. Pour un masque d'adresse IP de serveur virtuel, un masque non nul est interprété comme un octet considéré. Pour un service, la valeur non nulle est bloquée.

De plus, pour un masque d'adresse IP de serveur virtuel, les valeurs principales ou de fin peuvent être prises en compte. Si le masque d'adresse IP du serveur virtuel considère les valeurs de gauche de l'adresse IP, il s'agit d'un masque de transfert. Si le masque prend en compte les valeurs situées à droite de l'adresse, il s'agit d'un masque inversé.

Remarque : L'appliance NetScaler évalue tous les serveurs virtuels à masque direct avant d'évaluer les serveurs virtuels à masque inversé.

Lorsque vous masquez l'adresse IP d'un serveur virtuel, vous devez également créer un modèle d'adresse IP pour faire correspondre le trafic entrant avec le serveur virtuel approprié. Lorsque la solution matérielle-logicielle reçoit un paquet IP entrant, elle met en correspondance l'adresse IP de destination du paquet avec les bits pris en compte dans le modèle d'adresse IP, et après avoir trouvé une correspondance, elle applique le masque d'adresse IP pour construire l'adresse IP de destination finale.

Prenons l'exemple suivant :

- Adresse IP de destination dans le paquet entrant : 10.102.27.189
- Modèle d'adresse IP : 10.102.0.0
- Masque IP : 255.255.0.0
- Adresse IP de destination (finale) construite : 10.102.27.189.

Dans ce cas, les 16 premiers bits de l'adresse IP de destination d'origine correspondent au modèle d'adresse IP de ce serveur virtuel, de sorte que ce paquet entrant est routé vers ce serveur virtuel.

Si une adresse IP de destination correspond aux modèles IP de plusieurs serveurs virtuels, la correspondance la plus longue est prioritaire. Prenons l'exemple suivant :

- Serveur virtuel 1 : modèle IP 10.10.0.0, masque IP 255.255.0.0
- Serveur virtuel 2 : modèle IP 10.10.10.0, masque IP 255.255.255.0
- Adresse IP de destination dans le paquet : 10.10.10.45.
- Serveur virtuel sélectionné : Serveur virtuel 2.

Le modèle associé à Virtual Server 2 correspond à plus de bits que celui associé au serveur virtuel 1, de sorte que les adresses IP correspondantes sont envoyées à Virtual Server 2.

Remarque : Les ports sont également pris en compte si un disjoncteur est nécessaire.

Pour configurer un masque d'adresse IP de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <name>@ http -ipPattern <ipAddressPattern> -ipMask <
    ipMask> <listenPort>
<!--NeedCopy-->
```

Exemple :

Correspondance de motifs basée sur des octets de préfixe :


```
add lb vserver myLBVserver http -ippattern 10.102.0.0 -ipmask
   255.255.0.0 80
<!--NeedCopy-->
```

Correspondance de motifs basée sur les octets de fin :

```
add lb vserver myLBVserver1 http -ippattern 0.0.22.74 -ipmask
   0.0.255.255 80
<!--NeedCopy-->
```

Modifier un serveur virtuel basé sur des modèles :

```
set lb vserver myLBVserver1 -ippattern 0.0.22.74 -ipmask 0.0.255.255
<!--NeedCopy-->
```

Si vous configurez le serveur virtuel 1 comme suit :

```
add lb vserver vs1 HTTP -ippattern 100.1.1.0 -ipmask 255.255.255.0 80
<!--NeedCopy-->
```

L'appliance NetScaler ne répondra pas à une demande ARP sur toutes les adresses IP. Toutefois, il répond au trafic du serveur virtuel acheminé vers toutes les adresses IP de ce modèle.

Pour configurer un masque d'adresse IP de serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Dans la liste Type d'adresse, sélectionnez Modèle IP et spécifiez un modèle IP et un masque IP.

Configurer l'équilibrage de charge pour les protocoles couramment utilisés

May 5, 2023

Outre les sites Web et les applications Web, d'autres types d'applications déployées en réseau qui utilisent d'autres protocoles courants reçoivent souvent de grandes quantités de trafic et bénéficient donc de l'équilibrage de charge. Plusieurs de ces protocoles nécessitent des configurations spécifiques pour que l'équilibrage de charge fonctionne correctement. Parmi eux figurent FTP, DNS, SIP et RTSP.

Si vous configurez votre appliance NetScaler pour utiliser des noms de domaine pour vos serveurs plutôt que des adresses IP, vous devrez peut-être également configurer la traduction et le masquage IP pour ces serveurs.

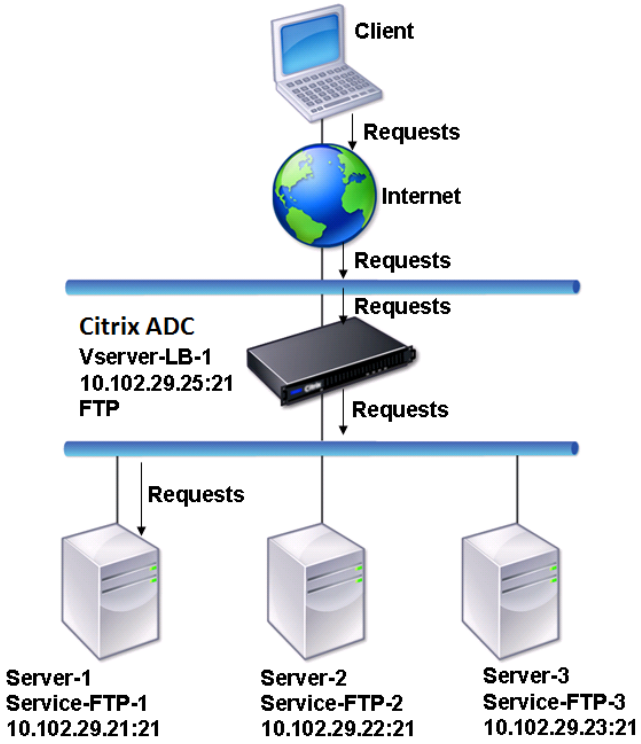
Équilibrage de charge d'un groupe de serveurs FTP

May 5, 2023

L'appliance NetScaler peut être utilisée pour équilibrer la charge des serveurs FTP. Le FTP exige que l'utilisateur établisse deux connexions sur deux ports différents vers le même serveur : la connexion de contrôle, par laquelle le client envoie des commandes au serveur, et la connexion de données, par laquelle le serveur envoie des données au client. Lorsque le client lance une session FTP en ouvrant une connexion de contrôle vers le serveur FTP, l'appliance utilise la méthode d'équilibrage de charge configurée pour sélectionner un service FTP et lui transmet la connexion de contrôle. Le serveur FTP à charge équilibrée ouvre ensuite une connexion de données avec le client pour l'échange d'informations.

Le schéma suivant décrit la topologie d'une configuration d'équilibrage de charge pour un groupe de serveurs FTP.

Figure 1. Topologie d'équilibrage de charge de base pour les serveurs FTP



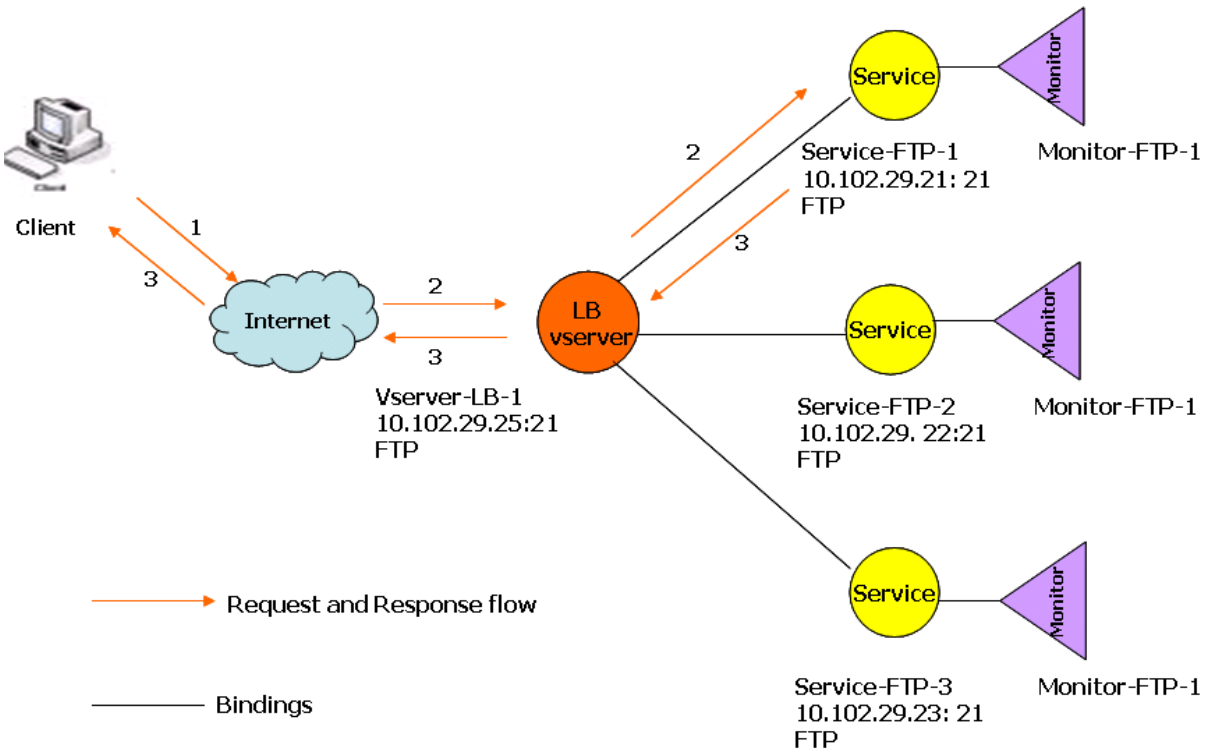
Dans le diagramme, les services Service-FTP-1, Service-FTP-2 et Service-FTP-3 sont liés au serveur virtuel vServer-LB-1. vServer-LB-1 transmet la demande de connexion du client à l'un des services en utilisant la méthode d'équilibrage de charge minimale de connexion. Les demandes suivantes sont transmises au service que l'appliance a initialement sélectionné pour l'équilibrage de charge.

Le tableau suivant répertorie les noms et les valeurs des entités de base configurées sur l'appliance.

Type d'entité	Nom	Adresse IP	Port	Protocole
Vserver	Vserver-LB-1	10.102.29.25	21	FTP
Services	Service-FTP-1	10.102.29.21	21	FTP
	Service-FTP-2	10.102.29.22	21	FTP
	Service-FTP-3	10.102.29.23	21	FTP
Moniteurs	FTP	Aucun	Aucun	Aucun

Le schéma suivant montre les entités d'équilibrage de charge et les valeurs des paramètres qui doivent être configurés sur l'appliance.

Figure 2. Modèle d'entité des serveurs FTP d'équilibrage de charge



L'appliance peut également fournir une option FTP passive permettant d'accéder aux serveurs FTP depuis l'extérieur d'un pare-feu. Lorsqu'un client utilise l'option FTP passive et établit une connexion de contrôle avec le serveur FTP, le serveur FTP initie également une connexion de contrôle avec le client. Il initie ensuite une connexion de données pour transférer un fichier via le pare-feu.

Pour créer des services et des serveurs virtuels de type FTP, reportez-vous à la section Configuration de l'équilibrage de charge de base. Nommez les entités et définissez les paramètres sur les valeurs décrites dans les colonnes de la table précédente. Lorsque vous configurez une configuration d'équilibrage de charge de base, un moniteur par défaut est lié aux services.

Ensuite, liez le moniteur FTP aux services en suivant la procédure décrite dans la section Liaison des moniteurs aux services.

Pour créer des moniteurs FTP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add lb monitor <MonitorName> FTP -interval <Interval> -userName <
     UserName> -password <Password>
2 <!--NeedCopy-->
```

Exemple :


```
add lb monitor monitor-FTP-1 FTP -interval 360 -userName User -password
    User
<!--NeedCopy-->
```

Pour créer des moniteurs FTP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Créez un moniteur de type FTP, et dans Paramètres spéciaux, spécifiez un nom d'utilisateur et un mot de passe.

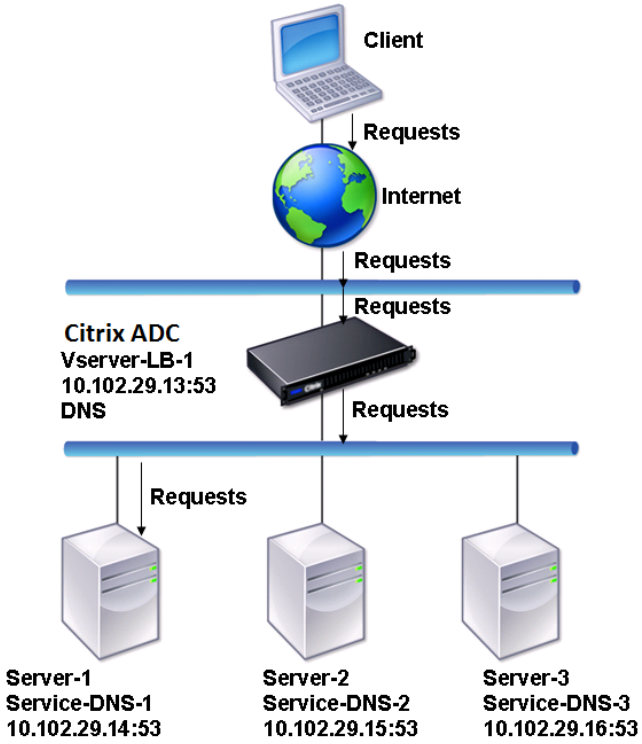
Serveurs DNS d'équilibrage de charge

May 5, 2023

Lorsque vous demandez la résolution DNS d'un nom de domaine, l'appliance NetScaler utilise la méthode d'équilibrage de charge configurée pour sélectionner un service DNS. Le serveur DNS auquel le service est lié résout ensuite le nom de domaine et renvoie l'adresse IP comme réponse. L'appliance peut également mettre en cache les réponses DNS et utiliser les informations mises en cache pour répondre aux futures demandes de résolution du même nom de domaine. Les serveurs DNS d'équilibrage de charge améliorent les temps de réponse DNS.

Le diagramme suivant décrit la topologie d'une configuration d'équilibrage de charge qui équilibre la charge d'un groupe de services DNS.

Figure 1. Topologie d'équilibrage de charge de base pour les serveurs DNS

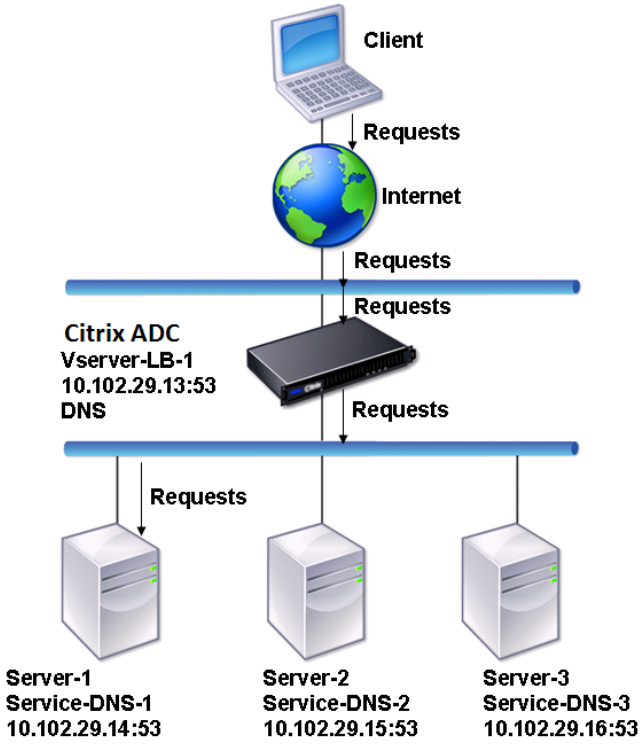


Dans le diagramme, les services Service-DNS-1, Service-DNS-2 et Service-DNS-3 sont liés au serveur virtuel vServer-LB-1. Le serveur virtuel vServer-LB-1 transmet les demandes des clients à un service en utilisant la méthode d'équilibrage de charge minimale de connexion. Le tableau suivant répertorie les noms et les valeurs des entités de base configurées sur l'appliance.

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.13	53	DNS
Services	Service-DNS-1	10.102.29.14	53	DNS
	Service-DNS-2	10.102.29.15	53	DNS
	Service-DNS-3	10.102.29.16	53	DNS
Moniteurs	monitor-DNS-1	Aucun	Aucun	Aucun

Le schéma suivant montre les entités d'équilibrage de charge et les valeurs des paramètres qui doivent être configurés sur l'appliance.

Figure 2. Modèle d'entité des serveurs DNS d'équilibrage de charge



Pour configurer une configuration d'équilibrage de charge DNS de base, reportez-vous à la section Configuration de l'équilibrage de charge de base. Suivez les procédures pour créer des services et des serveurs virtuels de type DNS, nommez les entités et définissez les paramètres à l'aide des valeurs décrites dans le tableau précédent. Lorsque vous configurez une configuration d'équilibrage de charge de base, le moniteur ping par défaut est lié aux services. Pour obtenir des instructions sur la liaison d'un moniteur DNS aux services DNS, vous pouvez également consulter la section Liaison des moniteurs aux services.

La procédure suivante décrit les étapes de création d'un moniteur qui mappe un nom de domaine à l'adresse IP en fonction d'une requête.

Pour configurer des moniteurs DNS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add lb monitor <monitorName> DNS -query <domainName> -queryType <
     Address|ZONE> -IPAddress <ipAddress>
2 <!--NeedCopy-->
```

Exemple :


```
add lb monitor monitor-DNS-1 DNS -query www.citrix.com -queryType
    Address -IPAddress 10.102.29.66

add lb monitor monitor-DNS-2 DNS -query www.citrix2.com -queryType
    Address -IPAddress
1000:0000:0000:0000:0005:0600:700a::888b-888d
<!--NeedCopy-->
```

Pour configurer des moniteurs DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Créez un moniteur de type DNS et, dans Paramètres spéciaux, spécifiez un type de requête et de requête.

Services d'équilibrage de charge basés sur les noms de domaine

May 5, 2023

Lorsque vous créez un service d'équilibrage de charge, vous pouvez fournir une adresse IP. Vous pouvez également créer un serveur à l'aide d'un nom de domaine. Le nom du serveur (nom de domaine) peut être résolu à l'aide d'un serveur de noms IPv4 ou IPv6, ou en ajoutant un enregistrement DNS faisant autorité (enregistrement A pour IPv4 ou enregistrement AAAA pour IPv6) à la configuration NetScaler.

Lorsque vous configurez des services avec des noms de domaine au lieu d'adresses IP, et si le serveur de noms résout le nom de domaine en une nouvelle adresse IP, le moniteur lié au service exécute une vérification de l'état de la nouvelle adresse IP et met à jour l'adresse IP du service uniquement lorsque l'adresse IP est jugée saine. Le moniteur peut être le moniteur par défaut lié au service ou vous pouvez lier n'importe quel autre moniteur pris en charge. Il sonde le service à intervalles réguliers définis dans les paramètres du moniteur. Si le nom de domaine correspond à une nouvelle adresse IP, le moniteur envoie une nouvelle sonde pour vérifier l'état du service. Toutes les sondes suivantes suivent l'intervalle prédéfini.

Remarque : Lorsque vous modifiez l'adresse IP d'un serveur, le service correspondant est sélectionné pour la première demande du client. Le serveur de noms convertit l'adresse IP du service en adresse IP modifiée pour la demande suivante, et le service est balisé.

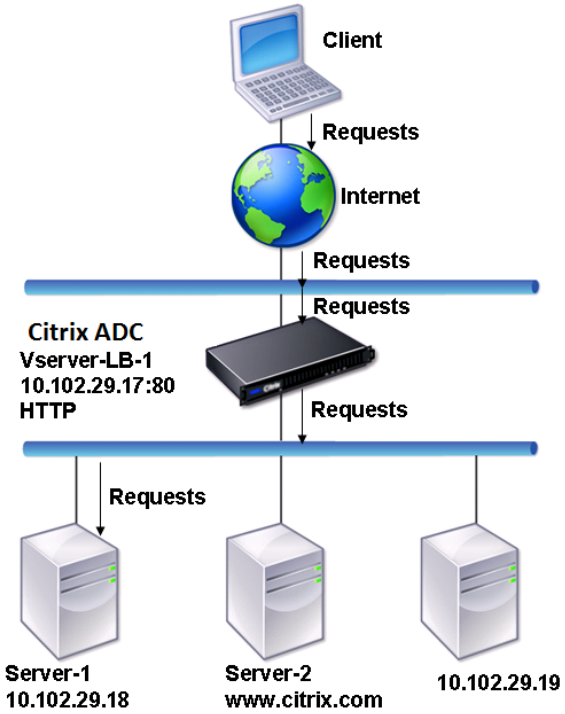
Les services basés sur des noms de domaine sont soumis aux restrictions suivantes :

- La longueur maximale d'un nom de domaine est de 255 caractères.

- Le paramètre Maximum Client est utilisé pour configurer un service qui représente le serveur basé sur le nom de domaine. Par exemple, un MaxClient de 1 000 est défini pour les services liés à un serveur virtuel. Lorsque le nombre de connexions sur le serveur virtuel atteint 2 000, le résolveur DNS modifie l'adresse IP des services. Toutefois, comme le compteur de connexions du service n'est pas réinitialisé, le serveur virtuel ne peut pas accepter de nouvelles connexions tant que toutes les anciennes connexions ne sont pas fermées.
- Lorsque l'adresse IP du service change, la persistance est difficile à maintenir.
- Si la résolution du nom de domaine échoue en raison d'un délai imparti, l'appliance utilise les anciennes informations (adresse IP).
- Lorsque la surveillance détecte qu'un service est hors service, l'appliance exécute une résolution DNS sur le service (représentant le serveur basé sur le nom de domaine) afin d'obtenir une nouvelle adresse IP.
- Les statistiques sont collectées sur un service et ne sont pas réinitialisées lorsque l'adresse IP change.
- Si une résolution DNS renvoie le code « erreur de nom » (3), l'appliance classe le service et remplace l'adresse IP par zéro.

Lorsque l'appliance reçoit une demande de service, elle sélectionne le service cible. De cette façon, l'appliance équilibre la charge sur vos services. Le diagramme suivant décrit la topologie d'une configuration d'équilibrage de charge qui équilibre la charge d'un groupe de serveurs basés sur des noms de domaine (DBS).

Figure 1. Topologie d'équilibrage de charge de base pour les serveurs DBS



Les services Service-HTTP-1, Service-HTTP-2 et Service-HTTP-3 sont liés au serveur virtuel vServer-LB-1. Le serveur virtuel vServer-LB-1 utilise la méthode d'équilibrage de charge la moins élevée pour choisir le service. L'adresse IP du service est résolue à l'aide du serveur de noms vServer-LB-2.

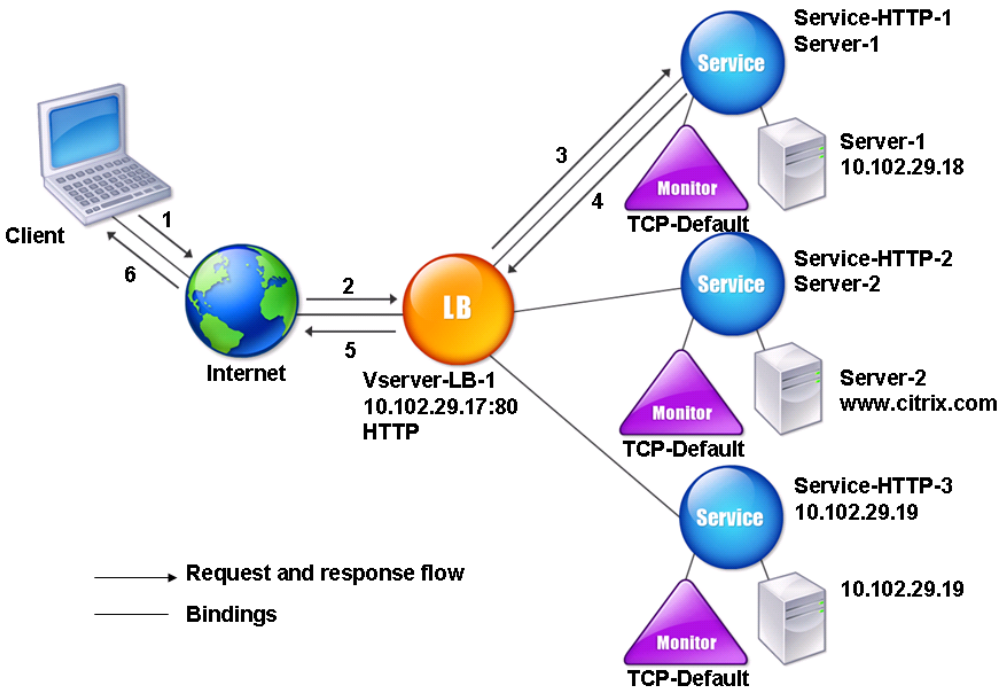
Le tableau suivant répertorie les noms et les valeurs des entités de base configurées sur l'appliance.

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.17	80	HTTP
	Vserver-LB-2	10.102.29.20	53	DNS
Serveurs	server-1	10.102.29.18	80	HTTP
	server-2	www.citrix.com	80	HTTP
Services	Service-HTTP-1	server-1	80	HTTP
	Service-HTTP-2	server-2	80	HTTP
	Service-HTTP-2	10.102.29.19	80	HTTP
Moniteurs	Valeur par défaut	Aucun	Aucun	Aucun

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur de noms	Aucun	10.102.29.19	Aucun	Aucun

Le schéma suivant montre les entités d'équilibrage de charge et les valeurs des paramètres qui doivent être configurés sur l'appliance.

Figure 2. Modèle d'entité des serveurs DBS d'équilibrage de charge



Pour configurer une configuration d'équilibrage de charge de base, reportez-vous à la section Configuration de l'équilibrage de charge de base. Créez les services et les serveurs virtuels de type HTTP, nommez les entités et définissez les paramètres à l'aide des valeurs décrites dans le tableau précédent.

Vous pouvez ajouter, supprimer, activer et désactiver des serveurs de noms externes. Vous pouvez créer un serveur de noms en spécifiant son adresse IP, ou vous pouvez configurer un serveur virtuel existant en tant que serveur de noms.

Pour ajouter un serveur de noms à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add dns nameServer <dnsVserverName>
<!--NeedCopy-->
```

Exemple :

```
add dns nameServer Vserver-LB-2
<!--NeedCopy-->
```

Pour ajouter un serveur de noms à l'aide de l'utilitaire de configuration

1. Accédez à **Gestiondu trafic**>**DNS**>**Serveurs**de**noms**.
2. Créez un serveur de noms DNS de type Serveur virtuel DNS et sélectionnez un serveur dans la liste des serveurs virtuels DNS.

Vous pouvez également ajouter un serveur de noms faisant autorité qui convertit le nom de domaine en adresse IP.

> **Remarque**
>
> Vous pouvez ajouter un serveur de noms de type TCP, UDP ou UDP_TCP aux sondes DBS du résolveur. Toutefois, si les serveurs de noms TCP et UDP coexistent et qu'un serveur de noms UDP reçoit une réponse avec le bit tronqué, cette réponse n'est pas retentée sur le serveur de noms TCP.

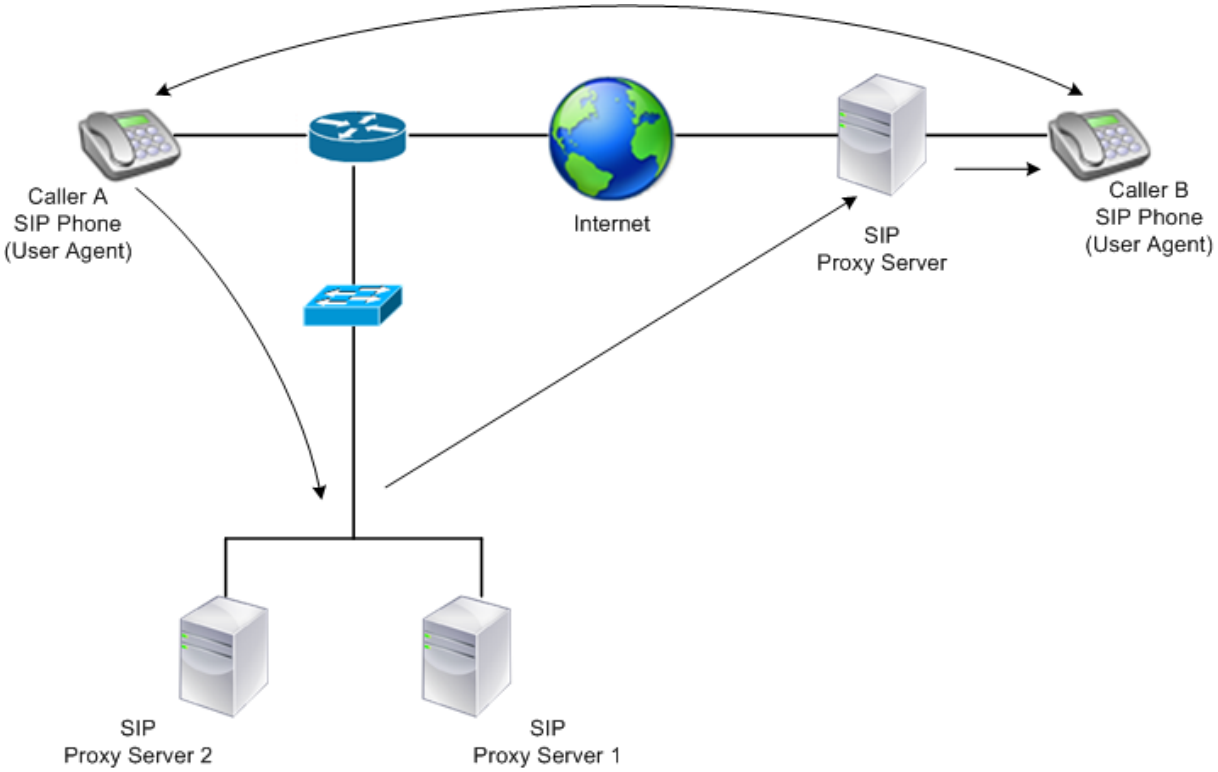
Équilibrage de charge d'un groupe de serveurs SIP

May 5, 2023

Le protocole SIP (Session Initiation Protocol) est conçu pour lancer, gérer et terminer des sessions de communication multimédia. Elle est devenue la norme pour la téléphonie Internet (VoIP). Les messages SIP peuvent être transmis via TCP ou UDP. Les messages SIP sont de deux types : les messages de demande et les messages de réponse.

Le trafic d'un système de communication basé sur SIP est acheminé via des appareils et des applications (entités) dédiés. Lors d'une session de communication multimédia, ces entités échangent des messages. La figure suivante montre un système de communication SIP de base :

Figure 1. Système de communication basé sur SIP



Un NetScaler vous permet d'équilibrer la charge des messages SIP via UDP ou TCP (y compris TLS). Vous pouvez configurer NetScaler pour équilibrer la charge des demandes SIP vers un groupe de serveurs proxy SIP. Pour ce faire, vous créez un serveur virtuel d'équilibrage de charge avec la méthode d'équilibrage de charge et le type de persistance définis selon l'une des combinaisons suivantes :

- Méthode d'équilibrage de la charge de hachage de l'ID d'appel sans paramètre de persistance
- Persistance basée sur l'identifiant d'appel avec le moins de connexions ou méthode d'équilibrage de charge circulaire
- Persistance basée sur des règles avec une méthode d'équilibrage de charge de connexion minimale ou d'arrondi

De plus, par défaut, NetScaler ajoute RPORT via l'en-tête de la demande SIP, de sorte que le serveur renvoie la réponse à l'adresse IP source et au port d'où provient la demande.

Remarque : Pour que l'équilibrage de charge fonctionne, vous devez configurer les proxys SIP afin qu'ils n'ajoutent pas d'adresses IP privées ou de domaines privés à l'en-tête/charge utile SIP. Les proxys SIP doivent ajouter à l'en-tête SIP un nom de domaine correspondant à l'adresse IP du serveur virtuel SIP. De plus, les proxys SIP doivent communiquer avec une base de données commune pour partager les informations d'enregistrement.

Trafic initié par le serveur

Pour le trafic sortant initié par le serveur SIP, configurez RNAT sur NetScaler afin que les adresses IP privées utilisées par les clients soient traduites en adresses IP publiques.

Si vous avez configuré des paramètres SIP qui incluent le port source ou de destination RNAT, l'appliance compare les valeurs des ports source et de destination des paquets de demande avec le port source RNAT et le port de destination RNAT. Si l'une des valeurs correspond, l'appliance met à jour l'en-tête VIA avec RPORT. La réponse SIP du client emprunte alors le même chemin que la demande.

Pour le trafic SSL initié par le serveur, NetScaler utilise une paire de clés de certificat intégrée. **Si vous souhaitez utiliser une paire de clés de certificat personnalisée, liez-la au service interne de NetScaler nommé nsrnatsip-127.0.0.1-5061.**

Prise en charge des stratégies et expressions

Le langage d'expressions par défaut de NetScaler contient plusieurs expressions qui fonctionnent sur les connexions SIP (Session Initiation Protocol). Ces expressions peuvent être liées uniquement aux serveurs virtuels SIP (sip_udp, sip_tcp ou sip_ssl) et aux points de liaison globaux. Vous pouvez utiliser ces expressions dans les politiques de changement de contenu, de limitation de débit, de réponse et de réécriture.

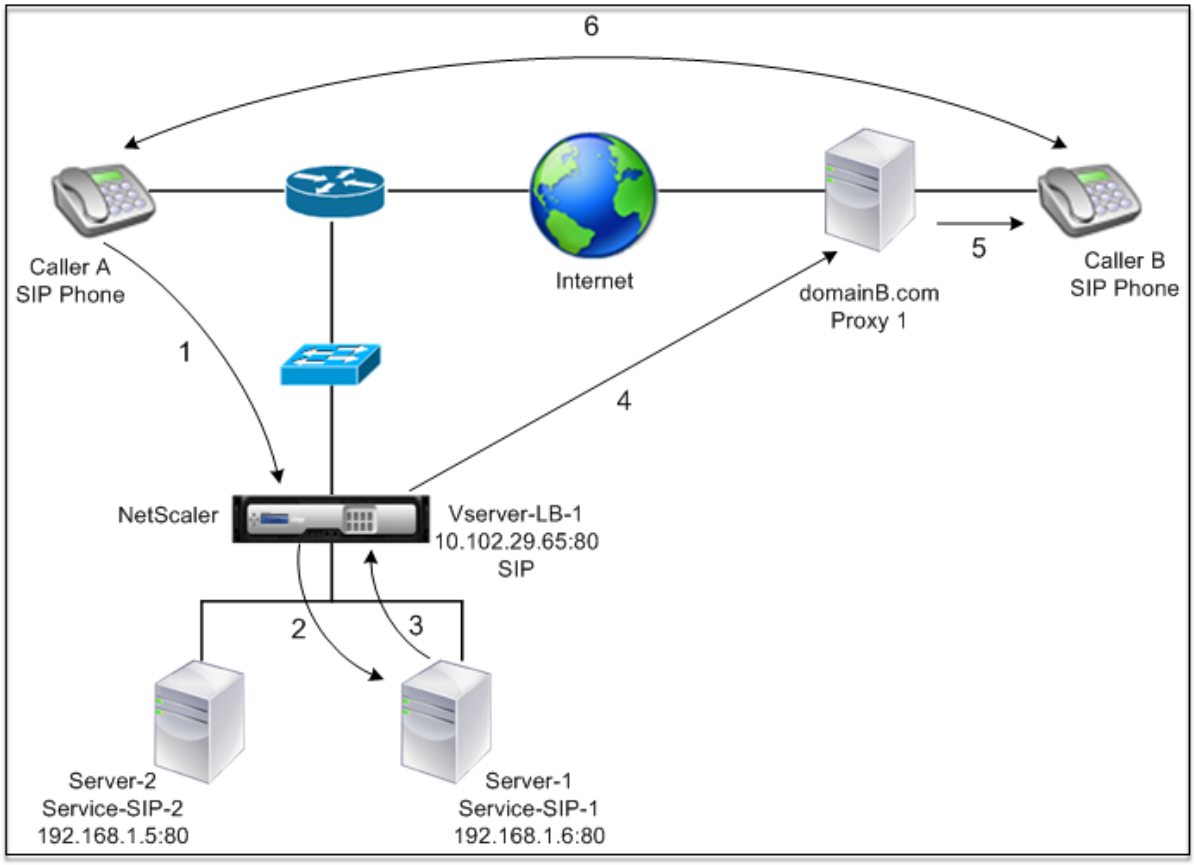
Configuration de l'équilibrage de charge pour le trafic de signalisation SIP via TCP ou UDP

Le NetScaler peut équilibrer la charge des serveurs SIP qui envoient des demandes via UDP ou TCP, y compris le trafic TCP sécurisé par TLS. L'ADC fournit les types de services suivants pour équilibrer la charge des serveurs SIP :

- SIP_UDP — Utilisé lorsque les serveurs SIP envoient des messages SIP via UDP.
- SIP_TCP — Utilisé lorsque les serveurs SIP envoient des messages SIP via TCP.
- SIP_SSL — Utilisé pour sécuriser le trafic de signalisation SIP via TCP à l'aide de SSL ou TLS. NetScaler prend en charge les modes suivants :
  - Connexion TLS de bout en bout entre le client, l'ADC et le serveur SIP.
  - Connexion TLS entre le client et l'ADC et connexion TCP entre l'ADC et le serveur SIP.
  - Connexion TCP entre le client et l'ADC et connexion TLS entre l'ADC et le serveur SIP.

La figure suivante montre la topologie d'une configuration configurée pour équilibrer la charge d'un groupe de serveurs SIP envoyant des messages SIP via TCP ou UDP.

Figure 2. Topologie d'équilibrage de charge SIP



Type d'entité	Nom	Adresse IP	Port	Type de service/Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.65	80	SIP_UDP/ SIP_TCP/ SIP_SSL
Services	Service-SIP-1	192.168.1.6	80	SIP_UDP/ SIP_TCP/ SIP_SSL
	Service-SIP-2	192.168.1.5	80	SIP_UDP/ SIP_TCP/ SIP_SSL
Moniteurs	Valeur par défaut	Aucun	80	SIP_UDP/ SIP_TCP/ SIP_SSL

Vous trouverez ci-dessous un aperçu de la configuration de l'équilibrage de charge de base pour le trafic SIP :

1. Configurez les services et configurez un serveur virtuel pour chaque type de trafic SIP pour lequel vous souhaitez équilibrer la charge :

   - **SIP_UDP** — Si vous équilibrez la charge du trafic SIP via UDP.
   - **SIP_TCP** — Si vous équilibrez la charge du trafic SIP via TCP.
   - **SIP_SSL** — Si vous équilibrez la charge et sécurisez le trafic SIP via TCP.

   Remarque : Si vous utilisez SIP_SSL, veillez à créer une paire de clés de certificat SSL. Pour plus d'informations, consultez la section Ajout d'une paire de clés de certificat.

2. Liez les services aux serveurs virtuels.
3. Si vous souhaitez surveiller l'état des services à l'aide d'un moniteur autre que celui par défaut (**tcp-default**), créez un moniteur personnalisé et liez-le aux services. NetScaler fournit deux types de moniteurs personnalisés, **SIP-UDP et SIP-TCP, pour la surveillance des services**SIP**.
4. Si vous utilisez un serveur virtuel SIP_SSL, liez une paire de clés de certificat SSL au serveur virtuel.
5. Si vous utilisez NetScaler comme passerelle pour les serveurs SIP dans votre déploiement, configurez RNAT.
6. Si vous souhaitez ajouter RPORT aux messages SIP initiés depuis le serveur SIP, configurez les paramètres SIP.

Pour configurer une configuration d'équilibrage de charge de base pour le trafic SIP à l'aide de l'interface de ligne de commande

Créez un ou plusieurs services. À l'invite de commande, tapez :

```
add service <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-SIP-UDP-1 192.0.2.5 SIP_UDP 80
<!--NeedCopy-->
```

Créez autant de serveurs virtuels que nécessaire pour gérer les services que vous avez créés. Le type de serveur virtuel doit correspondre au type de services que vous lui liez. À l'invite de commande, tapez :

```
add lb vserver <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```


Exemple :

```
add lb vserver Vserver-LB-1 SIP_UDP 10.102.29.60 80
<!--NeedCopy-->
```

Liez chaque service à un serveur virtuel. À l'invite de commande, tapez :

```
bind lb vserver <name> <serverName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-SIP-UDP-1
<!--NeedCopy-->
```

(Facultatif) Créez un moniteur personnalisé de type SIP-UDP ou SIP-TCP et liez-le au service. À l'invite de commande, tapez :

```
add lb monitor <monitorName> <monitorType> [<interval>]

bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor mon1 sip-UDP -sipMethod REGISTER -sipuRI sip:mon@test.
    com -sipregURI sip:mon@test.com -respcode 200

bind monitor mon1 Service-SIP-UDP-1
<!--NeedCopy-->
```

Si vous avez créé un serveur virtuel SIP_SSL, liez une paire de clés de certificat SSL au serveur virtuel. À l'invite de commandes, tapez : À l'invite de commandes, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -
    CA - skipCAName
<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1
<!--NeedCopy-->
```

Configurez le RNAT en fonction de la topologie de votre réseau. À l'invite de commandes, tapez l'une des commandes suivantes pour créer, respectivement, une entrée RNAT qui utilise une adresse réseau

comme condition et SNIP comme adresse IP NAT, une entrée RNAT qui utilise une adresse réseau comme condition et une adresse IP unique comme adresse IP NAT, une entrée RNAT qui utilise une ACL comme condition et un SNIP comme adresse IP NAT, ou une entrée RNAT qui utilise une ACL comme condition et adresse IP unique en tant qu'adresse IP NAT :

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ …

show rnat
<!--NeedCopy-->
```

Exemple :

```
add rnat RNAT-1 192.168.1.0 255.255.255.0

bind rnat RNAT-1 -natip 10.102.29.50
<!--NeedCopy-->
```

Si vous souhaitez utiliser une paire de clés de certificat personnalisée, liez-la au service interne de NetScaler nommé nsrnatsip-127.0.0.1-5061.

```
add ssl certKey <certkeyName> -cert <string> [-key <string>]

bind ssl service <serviceName> -certkeyName <string>
<!--NeedCopy-->
```

Exemple :

```
add ssl certKey c1 -cert cert.epm -key key.ky

bind ssl service nsrnatsip-127.0.0.1-5061 -certkeyName c1
<!--NeedCopy-->
```

Si vous souhaitez ajouter RPORT aux messages SIP initiés par le serveur SIP, tapez la commande suivante à l'invite de commandes :

```
set lb sipParameters -rnatSrcPort <rnatSrcPort> -rnatDstPort<
    rnatDstPort> -retryDur <integer> -addRportVip <addRportVip> -
    sip503RateThreshold <sip503_rate_threshold_value>
<!--NeedCopy-->
```

Exemple de configuration pour l'équilibrage de charge du trafic SIP via UDP


```
add service service-UDP-1 10.102.29.5 SIP_UDP 80

Done

add lb vserver vserver-LB-1 SIP_UDP 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-UDP-1

Done

add lb mon mon1 sip-udp -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-UDP-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
     -addRportVip ENABLED -sip503RateThreshold 1000

Done
<!--NeedCopy-->
```

Exemple de configuration pour l'équilibrage de charge du trafic SIP via TCP

```
add service service-TCP-1 10.102.29.5 SIP_TCP 80

Done

add lb vserver vserver-LB-1 SIP_TCP 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-TCP-1

```



```
Done

add lb mon mon1 sip-tcp -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-TCP-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
     -addRportVip ENABLED -sip503RateThreshold 1000

Done
<!--NeedCopy-->
```

Exemple de configuration pour l'équilibrage de charge et la sécurisation du trafic SIP sur TCP

```
add service service-SIP-SSL-1 10.102.29.5 SIP_SSL 80

Done

add lb vserver vserver-LB-1 SIP_SSL 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-SIP-SSL

Done

add lb mon mon1 sip-tCP -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-SIP-SSL

```



```
Done

bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
    -addRportVip ENABLED -sip503RateThreshold 1000

Done
<!--NeedCopy-->
```

Pour configurer une configuration d'équilibrage de charge de base pour le trafic SIP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ajoutez un serveur virtuel de type SIP_UDP, SIP_TCP ou SIP_SSL.
2. Cliquez sur la section **Service** et ajoutez un service de type SIP_UDP, SIP_TCP ou SIP_SSL.
3. **(Facultatif) Cliquez sur la section Moniteur et ajoutez un moniteur du type SIP-UDP ou SIP-TCP.**
4. Liez le moniteur au service et liez le service au serveur virtuel.
5. Si vous avez créé un serveur virtuel SIP_SSL, liez une paire de clés de certificat SSL au serveur virtuel. Cliquez sur la section Certificats et liez une paire de clés de certificat au serveur virtuel.
6. Configurez le RNAT en fonction de la topologie de votre réseau. Pour configurer RNAT :
   a) Accédez à **Système > Réseau > Routes**.
   b) Sur la page Routes, cliquez sur l'onglet **RNAT** .
   c) Dans le volet d'informations, cliquez sur **Configurer le RNAT**.
   d) Dans la boîte de dialogue Configurer RNAT, effectuez l'une des opérations suivantes :
      - Si vous souhaitez utiliser l'adresse réseau comme condition pour créer une entrée RNAT, cliquez sur **Réseau** et définissez les paramètres suivants :
        - Réseau
        - Masque réseau
      - Si vous souhaitez utiliser une ACL étendue comme condition pour créer une entrée RNAT, cliquez sur **ACL** et définissez les paramètres suivants :
        - Nom de l'ACL

- Port de redirection

e) Pour définir une adresse SNIP en tant qu'adresse IP NAT, passez à l'étape 7.

f) Pour définir une adresse IP unique comme IP NAT, dans la liste IP NAT disponible (s), sélectionnez l'adresse IP que vous souhaitez définir comme IP NAT, puis cliquez sur Ajouter. L'IP NAT que vous avez sélectionnée apparaît dans la liste IP NAT configurée.

g) Cliquez sur Créer, puis sur Fermer.

Si vous souhaitez utiliser une paire de clés de certificat personnalisée, liez-la au service interne de NetScaler nommé nsrnatsip-127.0.0.1-5061. Pour lier la paire :

a) Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis cliquez sur l'onglet Services internes.

b) **Sélectionnez nsrnatsip-127.0.0.1-5061 et cliquez sur Modifier.**

c) Cliquez sur la section **Certificats** et liez une paire de clés de certificat au service interne.

7. Si vous souhaitez ajouter RPORT aux messages SIP initiés par le serveur SIP, configurez les paramètres SIP. Accédez à **Gestion du trafic > Équilibrage de charge**, puis cliquez sur Modifier les paramètres SIP, définissez les différents paramètres SIP.

Exemple d'expression et de politique SIP : compression activée dans les demandes des clients

Un NetScaler ne peut pas traiter les demandes SIP client compressées, de sorte que la demande SIP du client échoue.

Vous pouvez configurer une politique de réponse qui intercepte le message SIP NEGOTIATE du client et recherche l'en-tête de compression. Si le message inclut un en-tête de compression, la politique répond par « 400 demandes erronées », de sorte que le client renvoie la demande sans la compresser.

À l'invite de commandes, tapez les commandes suivantes pour créer la stratégie de répondeur :

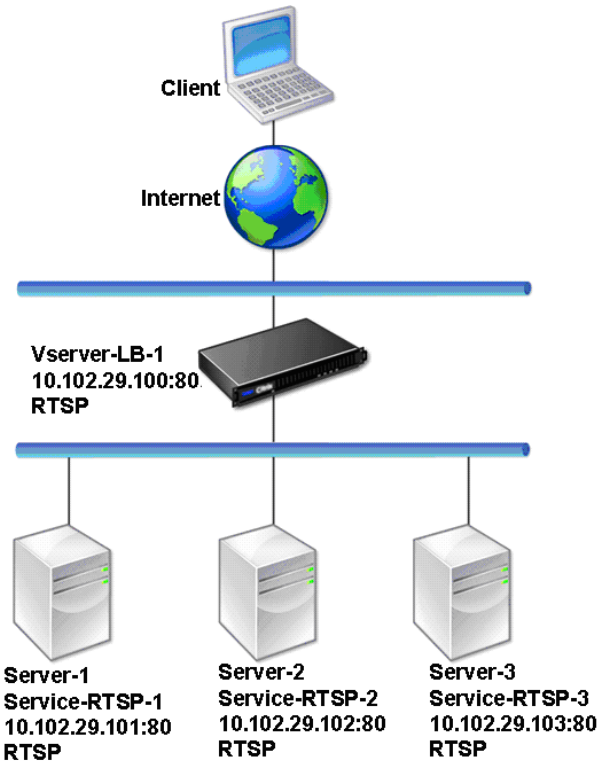
```
add responder action sipaction1 respondwith q{
 "SIP/2.0 400 Bad Requestrnrn" }


Done

add responder policy sippol1

add responder policy sippol1 "SIP.REQ.METHOD.EQ("NEGOTIATE")&&SIP.REQ.
   HEADER("Compression").EXISTS" sipaction1
<!--NeedCopy-->
```


Équilibrer la charge de serveurs RTSP

May 5, 2023

L'appliance NetScaler peut équilibrer la charge sur les serveurs RTSP afin d'améliorer les performances des flux audio et vidéo sur les réseaux. Le diagramme suivant décrit la topologie d'une configuration d'équilibrage de charge configurée pour équilibrer la charge d'un groupe de serveurs RTSP.

Figure 1. Topologie d'équilibrage de charge pour RTSP



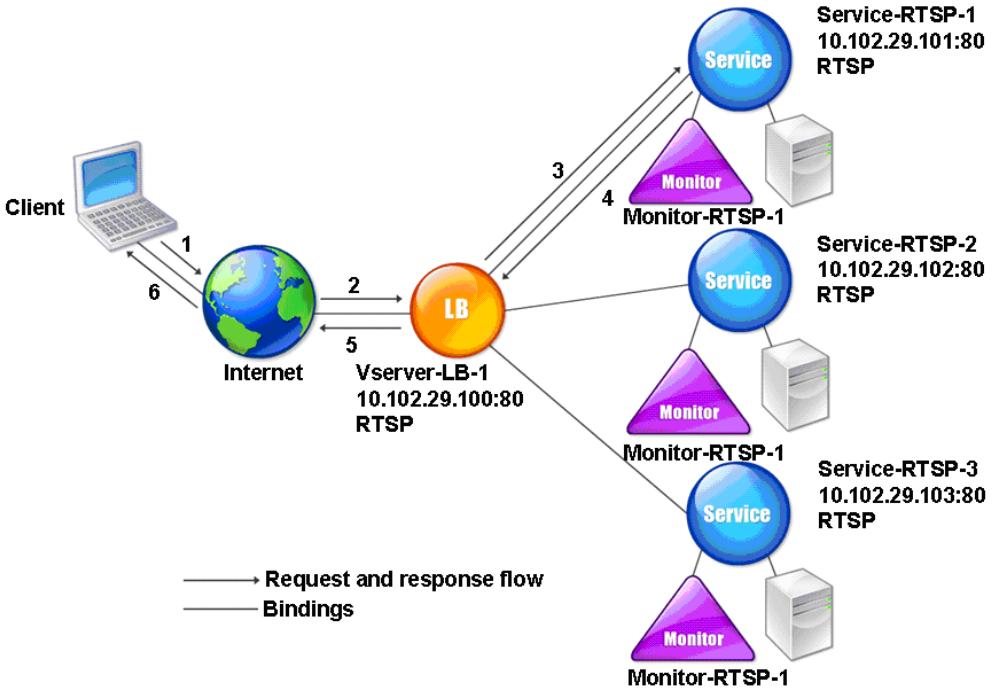
Dans l'exemple, les services Service-RTSP-1, Service-RTSP-2 et Service-RTSP-3 sont liés au serveur virtuel vServer-LB-1. Le tableau suivant répertorie les noms et les valeurs des exemples d'entités.

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.100	554	RTSP
Services	Service-RTSP-1	10.102.29.101	554	RTSP
	Service-RTSP-2	10.102.29.102	554	RTSP

Type d'entité	Nom	Adresse IP	Port	Protocole
	Service-RTSP-3	10.102.29.103	554	RTSP
Moniteurs	Monitor-RTSP-1	Aucun	554	RTSP

Le diagramme suivant montre les entités d'équilibrage de charge utilisées dans la configuration RTSP.

Figure 2. Modèle d'entité des serveurs RTSP d'équilibrage de charge



Pour configurer une configuration d'équilibrage de charge de base pour les serveurs RTSP, reportez-vous à la section Configuration de l'équilibrage de charge de base. Créez des services et des serveurs virtuels de type RTSP. Lorsque vous configurez une configuration d'équilibrage de charge de base, le moniteur par défaut TCP est lié aux services. Pour lier un moniteur RTSP à ces services, reportez-vous à la section Liaison des moniteurs aux services. La procédure suivante décrit comment créer un moniteur qui vérifie les serveurs RTSP.

Pour configurer des moniteurs RTSP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add lb monitor <monitorName> <type>
<!--NeedCopy-->
```

Exemple :

```
add lb monitor Monitor-RTSP-1 RTSP
<!--NeedCopy-->
```

Pour configurer des moniteurs RTSP à l'aide de l'interface graphique

Accédez à Gestion du trafic > Équilibrage de charge > Moniteurs et créez un moniteur de type RTSP.

Équilibrer la charge des serveurs de protocole Bureau à distance

May 5, 2023

Le protocole RDP (Remote Desktop Protocol) est un protocole compatible multicanal qui permet de disposer de canaux virtuels distincts pour transporter des données de présentation, des communications de périphérique série, des informations de licence, des données hautement cryptées (activité du clavier et de la souris), etc.

Le protocole RDP est utilisé pour fournir une interface graphique à un autre ordinateur du réseau. Le protocole RDP est utilisé avec les serveurs de terminaux Windows pour fournir un accès rapide avec une transmission quasi en temps réel des mouvements de la souris et des pressions de touches, même sur des connexions à faible bande passante.

Lorsque plusieurs serveurs de terminaux sont déployés pour fournir des services de bureau à distance, l'appliance NetScaler assure l'équilibrage de charge des serveurs de terminaux (Windows 2003 et 2008 Server Enterprise Editions). Parfois, un utilisateur qui accède à distance à une application peut souhaiter laisser l'application s'exécuter sur l'ordinateur distant tout en arrêtant l'ordinateur local. L'utilisateur ferme donc l'application locale sans se déconnecter de l'application distante. Une fois reconnecté à la machine distante, l'utilisateur doit pouvoir continuer avec l'application distante. Pour fournir cette fonctionnalité, l'implémentation de NetScaler RDP respecte le jeton de routage (cookie) défini par le répertoire de sessions ou le courtier des services Terminal afin que le client puisse se reconnecter au même serveur de terminal auquel il était connecté précédemment. Le répertoire de sessions, implémenté sur Windows 2003 Terminal Server, est appelé Broker sur Windows 2008 Terminal Server.

Lorsqu'une connexion TCP est établie entre le client et le serveur virtuel d'équilibrage de charge, NetScaler applique la méthode d'équilibrage de charge spécifiée et transmet la demande à l'un des

serveurs de terminaux. Le serveur terminal vérifie le répertoire des sessions pour déterminer si le client possède une session en cours d'exécution sur un autre serveur terminal du domaine.

S'il n'y a aucune session active sur un autre serveur de terminal, le serveur de terminaux répond en répondant à la demande du client et l'appliance NetScaler transmet la réponse au client.

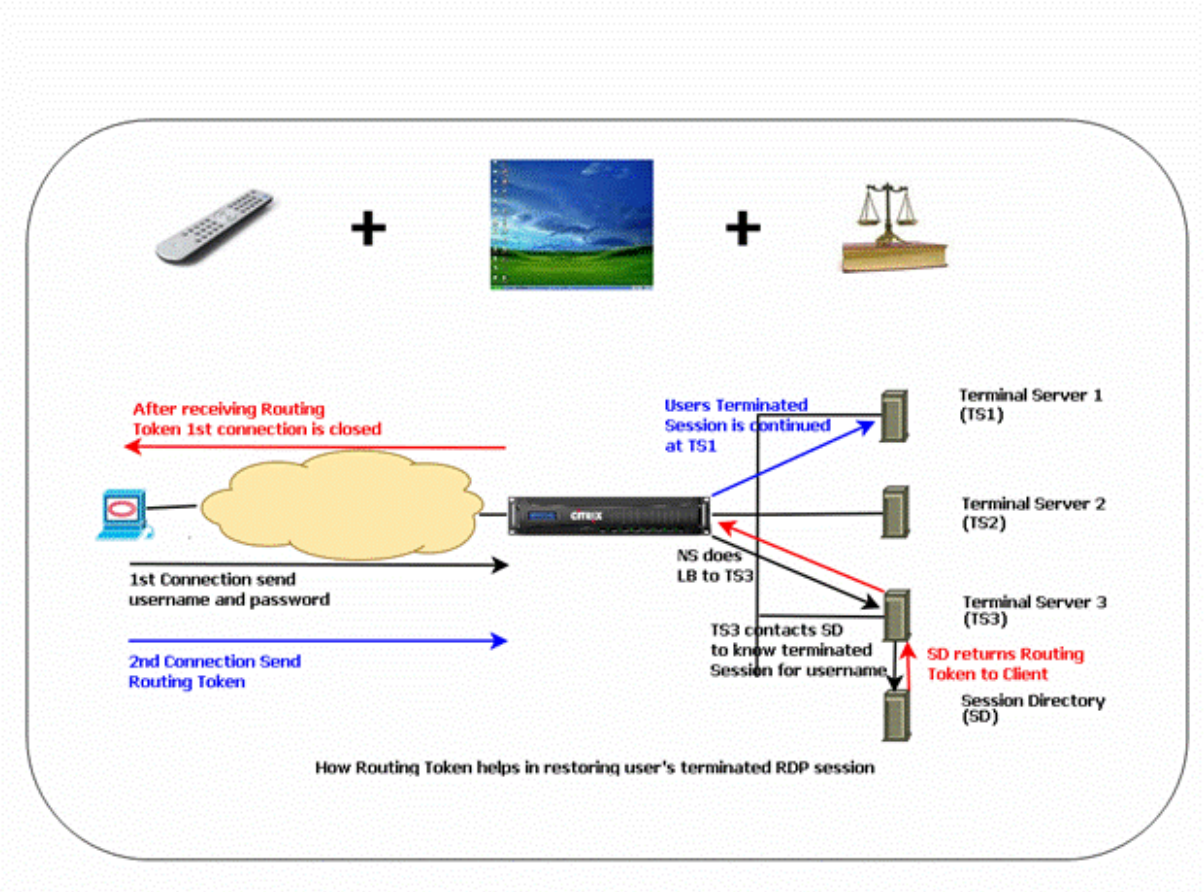
S'il existe une session active sur un autre serveur terminal, le serveur terminal qui reçoit la demande insère un cookie (appelé jeton de routage) contenant les détails de la session active et renvoie les paquets à l'appliance NetScaler, qui renvoie le paquet au client. Le serveur ferme la connexion avec le client. Lorsque le client essaie à nouveau de se connecter, NetScaler lit les informations du cookie et transmet le paquet au serveur terminal sur lequel le client a une session active.

Sur la machine cliente, l'utilisateur bénéficie d'une continuité du service et n'a aucune action spécifique à effectuer.

Remarque : La fonctionnalité Windows Session Directory nécessite le client Remote Desktop initialement publié avec Windows XP. Si une session avec un client Terminal Server Windows 2000 ou Windows NT 4.0 est déconnectée et que le client se reconnecte, le serveur avec lequel la connexion est établie est sélectionné par l'algorithme d'équilibrage de charge.

Le schéma suivant décrit l'équilibrage de charge RDP.

Figure 1. Topologie d'équilibrage de charge pour RDP



Remarque

- Lorsqu'un service RDP est configuré, la persistance est automatiquement maintenue à l'aide d'un jeton de routage. Il n'est pas nécessaire d'activer la persistance de manière explicite.
- L'appliance NetScaler prend uniquement en charge les cookies basés sur IP.
- Le script nsrdp.pl n'est pris en charge sur aucune version actuelle des serveurs Windows.

Assurez-vous que les sessions RDP déconnectées sont effacées sur les serveurs terminaux situés en arrière-plan afin d'éviter tout basculement entre deux serveurs terminal lorsqu'une session RDP est déconnectée sans déconnexion. Pour plus d'informations, consultez `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758177(v=ws.10)##BKMK_2`

Lorsque vous ajoutez un service RDP, NetScaler ajoute par défaut un moniteur de type TCP et le lie au service. Le moniteur par défaut est un simple moniteur TCP qui vérifie si un processus d'écoute existe sur le port 3389 du serveur spécifié pour le service RDP. S'il existe un processus d'écoute à 3389, NetScaler marque ce service comme étant ACTIF et s'il n'y a pas de processus d'écoute, il le marque comme étant HORS SERVICE.

Pour une surveillance plus efficace d'un service RDP, en plus du moniteur par défaut, vous pouvez

configurer un moniteur de script destiné au protocole RDP. Lorsque vous configurez le moniteur de script, NetScaler ouvre une connexion TCP vers le serveur spécifié et envoie un paquet RDP. Le moniteur marque le service comme étant actif uniquement s'il reçoit une confirmation de la connexion du serveur physique. Par conséquent, à partir du moniteur de script, NetScaler peut savoir si le service RDP est prêt à traiter une demande.

Le moniteur est un moniteur de type utilisateur et le script se trouve sur NetScaler à l'adresse /nsconfig/monitors/nsrdp.pl. Lorsque vous configurez le moniteur utilisateur, NetScaler exécute le script automatiquement. Pour configurer le moniteur de script, ajoutez-le et liez-le au service RDP.

Pour configurer l'équilibrage de charge RDP, créez des services de type RDP et liez-les à un serveur virtuel RDP.

Pour configurer les services d'équilibrage de charge RDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une configuration d'équilibrage de charge RDP et vérifier la configuration :

```
add service <name>@ <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Remarque : Répétez la commande précédente pour ajouter d'autres services.

Exemple

```
> add service ser1 10.102.27.182 RDP 3389
Done
> add service ser2 10.102.27.183 RDP 3389
Done
>show service ser1
ser1 (10.102. 27.182:3389) - RDP
        State: UP
…
            Server Name: 10.102.27.182
            Server ID : 0           Monitor Threshold : 0
        Down state flush: ENABLED
…
1)      Monitor Name: tcp-default
                State: UP       Weight: 1
…
                Response Time: 4.152 millisec
 Done
<!--NeedCopy-->
```


Pour configurer les services d'équilibrage de charge RDP à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis créez des services de type RDP.

Pour configurer un serveur virtuel d'équilibrage de charge RDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer un serveur virtuel d'équilibrage de charge RDP et vérifier la configuration :

```
add lb vserver <name>@ <serviceType> <ipAddress> <port>

bind lb vserver <name>@ <serviceName>

Bind all the RDP services to be load balanced to the virtual server.
<!--NeedCopy-->
```

Exemple :

Cet exemple comporte deux services RDP liés au serveur virtuel RDP.

```
add lb vs v1 rdP 10.102.27.186 3389
Done

bind lb vs v1 ser1
service "ser1" bound

bind lb vs v1 ser2
service "ser2" bound
Done

sh lb vs v1
v1 (10.102.27.186:3389) - RDP   Type: ADDRESS
State: UP
…
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION
  Current Method: Round Robin, Reason: A new service is bound
Mode: IP
Persistence: NONE
  L2Conn: OFF

1) ser1 (10.102.27.182: 3389) - RDPState: UP   Weight: 1
2) ser2 (10.102.27.183: 3389) - RDPState: UP   Weight: 1
```



```
24 Done
25 <!--NeedCopy-->
```

Pour configurer un serveur virtuel d'équilibrage de charge RDP à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, créez un serveur virtuel de type RDP et liez les services RDP à ce serveur virtuel.

Pour configurer un moniteur de script pour les services RDP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
1 add lb monitor <monitorName> USER -scriptName nsrdp.pl
2
3 bind lb monitor <monitorName> <rdpServiceName>
4 <!--NeedCopy-->
```

Exemple :

```
1 add service ser1 10.102.27.182 RDP 3389
2
3 add lb monitor RDP_MON USER -scriptName nsrdp.pl
4
5 bind lb monitor RDP_MON ser1
6
7 <!--NeedCopy-->
```

Pour configurer un moniteur de script pour les services RDP à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**, puis créez un moniteur de type USER.
2. Dans Paramètres spéciaux, dans la liste Nom du script, sélectionnez nsrdp.pl, puis liez ce moniteur à un service RDP.

Ordre de priorité pour les services d'équilibrage de charge

May 5, 2023

La fonction Ordre de priorité pour les services vous permet de hiérarchiser l'ordre des services ou des groupes de services en fonction des préférences de sélection de l'équilibrage de charge. Vous pouvez configurer l'ordre de priorité lorsque vous effectuez les opérations suivantes :

- Liez un service à un serveur virtuel d'équilibrage de charge.
- Liez un groupe de services à un serveur virtuel d'équilibrage de charge.
- Liez un membre du groupe de services au groupe de services d'équilibrage de charge.

Actuellement, vous pouvez configurer l'ordre de priorité des services à l'aide des approches suivantes. Toutefois, ces approches présentent les limites suivantes :

- Configuration d'une chaîne de serveurs virtuels de sauvegarde : le nombre de lignes de configuration est élevé et vous devez exécuter la commande `show` plusieurs fois pour connaître l'état de tous les services LB pour chaque serveur virtuel.
- Configuration de l'emplacement préféré : vous devez créer des entrées d'emplacement pour tous les points de terminaison de votre application.

La fonctionnalité Ordre de priorité pour les services résout les limitations précédentes avec moins de commandes de configuration et vous aide à effectuer la configuration de l'emplacement préféré sans avoir besoin de représentation de l'emplacement de toutes les adresses IP des services d'équilibrage de charge.

Configurer l'ordre de priorité des services d'équilibrage de charge

Pour configurer l'ordre de priorité des services d'équilibrage de charge, le paramètre `-order <number>` est ajouté aux commandes de liaison.

> **Remarque :**
>
> Le numéro de commande le plus bas a la priorité la plus élevée.

Commande :

```
bind lb vserver <vservername> <servicename/servicegroupname> -order <number>
```

Prenons l'exemple d'un ensemble de services liés à un serveur virtuel d'équilibrage de charge (vs1). À l'aide du paramètre
`- order <number>`, vous pouvez hiérarchiser l'ordre de sélection des services comme suit :

- Ensemble 1 (s1, s2) lié à vs1 — ordre 1
- Ensemble 2 (s3, s4) lié à vs1 — ordre 2
- Ensemble 3 (s5, s6) lié à vs1 — ordre 3

Après avoir lié les services à vs1 et lorsque vs1 reçoit le trafic client, l'ordre de sélection des services est le suivant :

- Le serveur virtuel (vs1) sélectionne d'abord les services de l'ensemble 1 (s1 et s2) portant le numéro d'ordre 1, car cet ensemble se voit attribuer le numéro d'ordre le plus bas. Par défaut, le numéro de commande le plus bas a la priorité la plus élevée.
- Si tous les services de l'ensemble 1 sont DOWN, vs1 sélectionne l'ensemble 2 (s3 et s4) avec le numéro d'ordre 2.
- Si tous les services des ensembles 1 et 2 sont hors service, vs1 sélectionne l'ensemble 3 (s5 et s6) avec le numéro d'ordre 3.

Configurer l'ordre de priorité pour les services d'équilibrage de charge à l'aide de

Pour configurer l'ordre de priorité des services d'équilibrage de charge, tapez les commandes suivantes à l'invite de commandes :

1. Ajoutez un serveur virtuel LB.

   ```
   add lb vserver vs1 HTTP 1.1.1.1 80
   ```

2. Ajoutez des services LB.

   ```
   add service s[1-6] 2.2.2.[1-6] HTTP 80
   ```

3. Définissez le numéro de commande et liez les services au serveur virtuel LB.

   ```
   bind lb vserver vs1 s1 -order 1
   bind lb vserver vs1 s2 -order 1
   bind lb vserver vs1 s3 -order 2
   bind lb vserver vs1 s4 -order 2
   bind lb vserver vs1 s5 -order 3
   bind lb vserver vs1 s6 -order 3
   ```

Configurer l'ordre de priorité pour les services d'équilibrage de charge à l'aide de

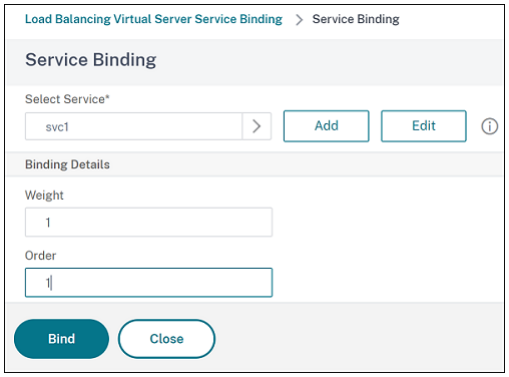
Pré-requis :

- Vous avez créé un serveur virtuel d'équilibrage de charge.
- Vous avez créé des services.

Pour configurer l'ordre de priorité des services d'équilibrage de charge et les lier au serveur virtuel, procédez comme suit :

1. Accédez à**Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis double-cliquez sur le serveur virtuel d'équilibrage de charge.
2. Dans **Serveur virtuel d'équilibrage de charge**, sous la section **Services et groupes de services**, cliquez sur **Liaison de service de serveur virtuel d'équilibrage de charge**.

3. Dans la boîte de dialogue**Liaison de service de serveur virtuel d'équilibrage de charge**, cliquez sur**Ajouter une liaison**.
4. Dans la boîte**de dialogue Liaison**de service, sélectionnez un service.
5. Saisissez un nombre dans le champ **Ordre**pour définir l'ordre de priorité du service.



6. Cliquez sur**Bind**.
7. Répétez les étapes 1 à 6 pour configurer un numéro d'ordre de priorité différent pour différents services.

Configurer l'ordre de priorité pour les services d'équilibrage de charge à l'aide de commandes

Par défaut, le numéro de commande le plus bas a la priorité la plus élevée. Toutefois, vous pouvez différer ce comportement par défaut à l'aide des nouvelles commandes d'action et de stratégie LB. Vous pouvez configurer l'ordre de sélection des services en fonction du trafic client entrant ou des données client.

Prenons l'exemple d'un ensemble de services liés à un serveur virtuel (vs1). À l'aide du paramètre `- order <number>`, vous avez configuré l'ordre de priorité des services comme suit :

- Ensemble 1 (s1, s2) lié à vs1 — ordre 1
- Ensemble 2 (s3, s4) lié à vs1 — ordre 2
- Ensemble 3 (s5, s6) lié à vs1 — ordre 3

Par défaut, le numéro de commande le plus bas a la priorité la plus élevée. Par conséquent, l'ordre de priorité par défaut est 1, 2 et 3 pour les services de l'ensemble 1, ensemble2 et ensemble3, respectivement. Toutefois, pour un trafic client spécifique, vous souhaitez modifier l'ordre de priorité sur 3, 1 et 2. Pour ce faire, vous pouvez ajouter une stratégie LB et la lier à vs1.

Une commande de stratégie LB se compose de deux éléments : une règle et une action. La règle est associée à une action, qui est exécutée si une demande correspond à la règle.

> **Remarque :**
>
> Les commandes de politique LB sont communes à la fois à la configuration LB et GSLB et s'appliquent aux demandes traitées par l'appliance NetScaler.

Action LB

Expression :

```
add lb action <name> <type> <string>
```

Exemple :

```
add lb action act1 -type SELECTIONORDER -value 3 2 1
```

Paramètres :

- `name`: nom de l'action.
- `type`: Type d'action.
- `string`: valeur de l'action spécifiée.

Politique LB

Expression :

```
add lb policy <name> <rule> <action> <undefaction>
```

Exemple :

```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
```

Paramètres :

- `name`: nom de la stratégie.
- `rule`: une règle se compose d'une ou plusieurs expressions. La règle est associée à une action, qui est exécutée si la demande correspond à la règle.
- `action`: DROP, NOLBACTION et RESET sont pris en charge.
- `undefaction`: l'appliance NetScaler génère un événement non défini (événement UNDEF) lorsqu'une demande ne correspond pas à une politique. Vous pouvez utiliser la `set lb param -undefAction <action>`commande pour définir l'action non définie. Vous pouvez attribuer ces actions à un événement non défini : DROP, NOLBACTION et RESET.

Prenons un exemple dans lequel vous ajoutez une action LB, une stratégie LB et liez la stratégie à un serveur virtuel d'équilibrage de charge (vs1) comme suit :

```
add lb action act1 -type SELECTIONORDER -value 3 1 2
```



```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1

bind lb vserver vs1 -policyName pol1 -priority 10
```

La règle sélectionne le trafic client correspondant à l'adresse IP et envoie ce trafic vers vs1. `8.8.8.8` Le type d'action LB (`SELECTIONORDER`) définit l'ordre de sélection du service. Après avoir lié la stratégie LB à vs1 et lorsque vs1 reçoit le trafic client de l'adresse IP`8.8.8.8`, les services sont sélectionnés dans l'ordre suivant :

1. Le serveur virtuel (vs1) sélectionne les services de l'ensemble 3 (s5 et s6) avec un ordre de priorité 3.
2. Si tous les services de l'ensemble 3 sont DOWN, vs1 sélectionne l'ensemble 1 (s1 et s2) avec un ordre de priorité 2.
3. Si tous les services de l'ensemble 3 et de l'ensemble 2 sont hors service, le vs1 sélectionne l'ensemble 1 (s1 et s2) avec l'ordre 1.

Configurer l'ordre de priorité pour les services d'équilibrage de charge avec les commandes de stratégie LB à l'aide de

Pour configurer l'ordre de priorité des services d'équilibrage de charge à l'aide des commandes de stratégie LB, tapez les commandes suivantes à l'invite de commandes :

1. Ajoutez une action LB.

   ```
   add lb action act1 -type SELECTIONORDER -value 3 1 2
   ```

2. Ajoutez une stratégie LB.

   ```
   add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
   ```

3. Ajoutez un serveur virtuel LB.

   ```
   add lb vserver vs1 HTTP 1.1.1.1 80
   ```

4. Liez la stratégie LB au serveur virtuel LB.

   ```
   bind lb vs vs1 -policyName pol1 -priority 10
   ```

5. Ajoutez des services LB.

   ```
   add service s[1-6] 2.2.2.[1-6] HTTP 80
   ```

6. Définissez l'ordre et liez les services au serveur virtuel LB.

   ```
   bind lb vserver vs1 s1 -order 1

   bind lb vserver vs1 s2 -order 1

   bind lb vserver vs1 s3 -order 2

   bind lb vserver vs1 s4 -order 2
   ```



```
bind lb vserver vs1 s5 -order 3

bind lb vserver vs1 s6 -order 3
```

Configurez l'ordre de priorité des services d'équilibrage de charge avec les commandes de stratégie LB à l'aide de l'interface

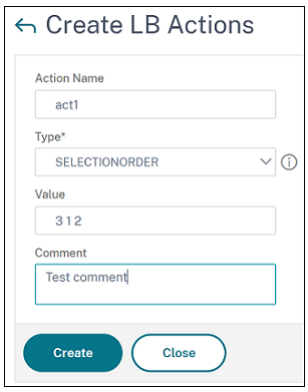
Pré-requis :

- Vous avez créé un serveur virtuel d'équilibrage de charge.
- Vous avez créé des services.

Étape 1 - Créer une action LB :

1. Accédez à **AppExpert > LB > Actions**.
2. Dans**Actions LB**, cliquez sur**Ajouter**.
3. Dans la boîte de dialogue**Créer des actions LB**, spécifiez des valeurs pour les paramètres suivants :
   - **Nom de l'action** : act1
   - **Type** : SELECTIONORDER
   - **Valeur** : 3 1 2

     > **Remarque :**
     >
     > Les chiffres du champ **Valeur**sont séparés par un espace.

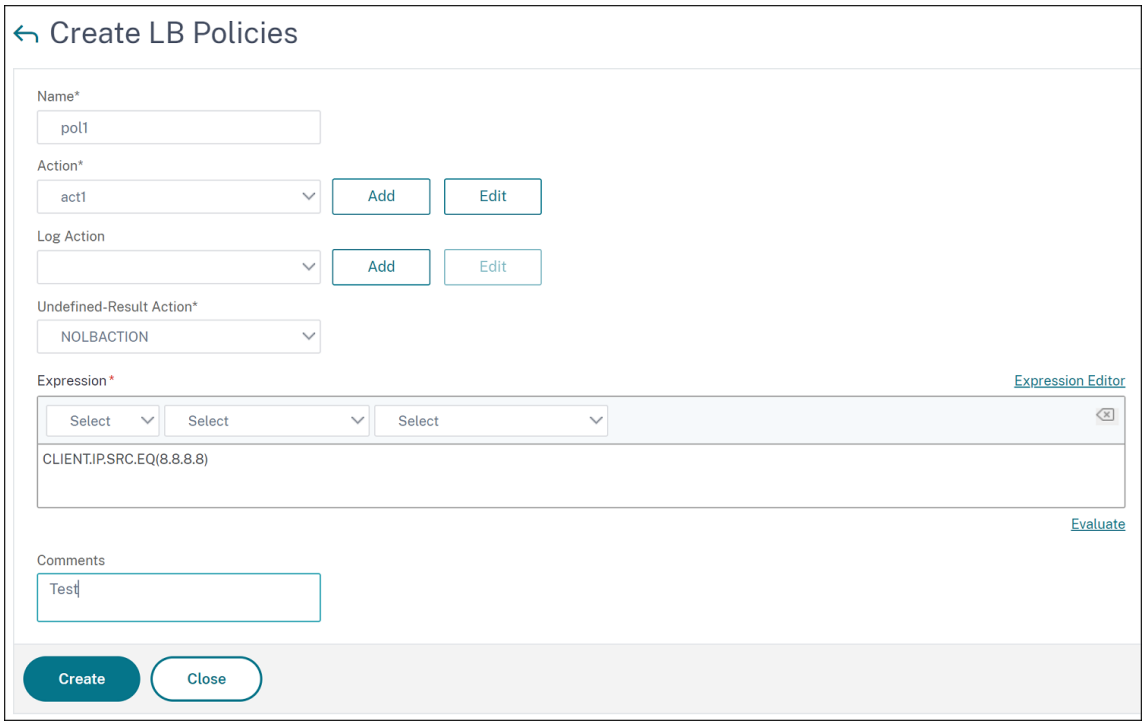


4. Cliquez sur **Create**.

Étape 2 - Créer une stratégie LB :

1. Accédez à **AppExpert > LB > Stratégies**.
2. Dans**Stratégies LB**, cliquez sur**Ajouter**.
3. Dans la boîte de dialogue**Créer des stratégies LB**, spécifiez des valeurs pour les paramètres suivants :

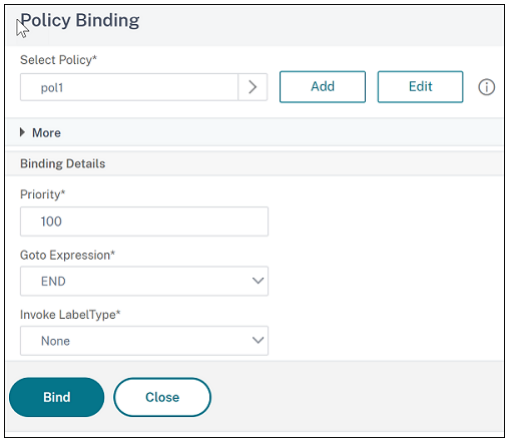
- **Nom** : pol1
- **Action** : acte 1
- **Action à résultat non défini** : NOLBACTION
- **Expression** : CLIENT.IP.SRC.EQ (8.8.8.8)



4. Cliquez sur**Créer**.

Étape 3 - Liez la stratégie LB au serveur virtuel LB :

1. Accédez à**Gestion du trafic > LB > Serveurs virtuels**et double-cliquez sur le serveur virtuel.
2. Dans**Paramètres avancés**, cliquez sur**Stratégies**.
3. Dans la section**Politiques**, cliquez sur l'icône plus (+).
4. Dans la boîte **de dialogue Choisir un type**, spécifiez des valeurs pour les paramètres suivants :
   - **Choisissez une stratégie** : LB
   - **Choisissez le type** : Demande
5. Cliquez sur **Ajouter une liaison**.
6. Dans la boîte de dialogue **Liaison de stratégie**, spécifiez des valeurs pour les paramètres suivants :
   - **Sélectionnez la stratégie** : pol 1
   - **Priorité** : 10
   - **Accédez à Expression** : FIN
   - **Invoke LabelType** : Aucun



7. Cliquez sur **Bind**.

Étape 4 - Configurez l'ordre de priorité pour les services d'équilibrage de charge :

Pour configurer l'ordre de priorité des services d'équilibrage de charge, consultez la procédure **Configurer l'ordre de priorité des services d'équilibrage de charge à l'aide de l'interface graphique** .

Paramètres de persistance pour les services

Si la persistance est configurée pour un service, la préférence est toujours donnée à la persistance, par défaut.

Prenons l'exemple d'un service dont la persistance est configurée et dont l'ordre de priorité est 1. Si un service d'ordre de priorité 0 est UP, la préférence est toujours donnée au service d'ordre de priorité 1.

Toutefois, vous pouvez remplacer ce comportement par défaut à l'aide de la commande CLI suivante :

```
set lb param -overridePersistencyforOrder <YES/NO>
```

Prenons l'exemple suivant :

Un ensemble de services est lié à un serveur virtuel (vs1) avec l'ordre de priorité suivant :

- Ensemble 1 (s1, s2) lié à vs1 — ordre 1
- Ensemble 2 (s3, s4) lié à vs1 — ordre 2

Tapez la commande suivante à l'invite de commandes pour remplacer la persistance :

```
set lb parameter -overridePersistencyforOrder YES
```

Si l'ensemble 1 (les services avec persistance sont configurés) est DOWN, les services de l'ensemble 2 traitent toutes les demandes jusqu'à ce que les services de l'ensemble 1 soient actifs. Une entrée de persistance pour la priorité 2 est créée.

Supposons qu'après un certain temps, les services de l'ensemble 1 soient actifs. Désormais, les services de l'ensemble 1 et de l'ensemble 2 sont prêts à traiter les demandes. Dans ce scénario, de nouvelles décisions d'équilibrage de charge sont prises lorsque les services d'ordre supérieur sont actifs. L'entrée de persistance est remplacée par une nouvelle entrée d'équilibrage de charge.

Bascule de priorité

Avec la fonctionnalité de basculement de priorité, vous pouvez basculer tout le trafic vers un service de faible priorité pendant la mise à niveau de version pour un service avec un ordre de priorité plus élevé. Vous pouvez utiliser les commandes suivantes pour basculer la priorité :

- `set lb vserver -toggleorder<Ascending/Descending>`
- `set lb vserver v1 -orderthreshold 80`

Par exemple, considérons qu'il existe deux services ayant les priorités suivantes :

- Service 1- order 0
- Service 2 — commande 1

Par défaut, le service 1 gère tout le trafic. Si le service 1 doit être mis à niveau, le trafic doit être redirigé vers le service 2.

À l'invite de commandes, tapez les commandes suivantes pour basculer la priorité :

```
set lb vserver -toggleorder Descending
```

Par défaut, 0 a une priorité supérieure. Cependant, après le basculement de priorité, 1 est considéré comme une priorité supérieure. Si une entrée de persistance est présente pour le service, le comportement de préférence de persistance est tel qu'expliqué dans la section **Paramètres de persistance pour les services**.

Cas d'utilisation 1 : Équilibrage de charge SMPP

May 5, 2023

Des millions de messages courts sont échangés quotidiennement entre des particuliers et des fournisseurs de services à valeur ajoutée, tels que des banques, des annonceurs et des services d'annuaire, à l'aide du protocole de message court pair à pair (SMPP). La livraison des messages est souvent retardée car les serveurs sont surchargés et le trafic n'est pas réparti de manière optimale entre les serveurs. NetScaler prend en charge l'équilibrage de charge SMPP et assure une distribution optimale des messages sur vos serveurs, évitant ainsi les mauvaises performances et les pannes.

NetScaler effectue un équilibrage de charge côté serveur lorsque des messages sont reçus de clients et côté client lorsque des messages sont reçus des serveurs.

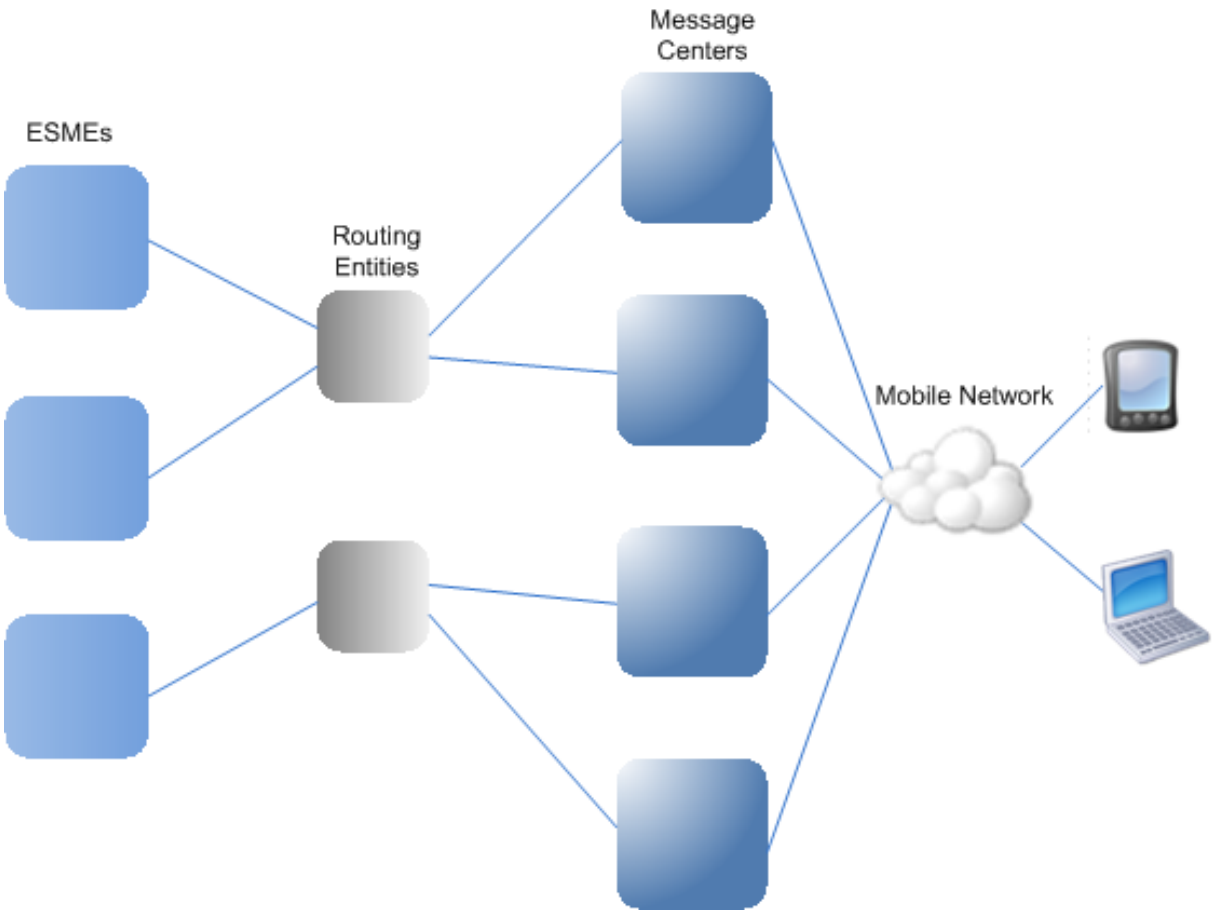
L'équilibrage de charge des messages SMPP par NetScaler offre les avantages suivants :

- Meilleure répartition de la charge sur les serveurs, ce qui se traduit par un temps de réponse plus rapide pour les utilisateurs finaux
- Surveillance de l'état du serveur et meilleures fonctionnalités de basculement
- Ajout rapide et facile de nouveaux serveurs (centres de messagerie) sans modifier la configuration du client
- Haute disponibilité

Introduction à SMPP

SMPP est un protocole de couche d'application pour le transfert de messages courts entre les entités de messages courts externes (ESME), les entités de routage (RE) et les centres de messages (MC) via des connexions TCP à longue durée de vie. Il est utilisé pour l'envoi de messages courts (SMS) entre amis, contacts et tiers tels que les banques (banque mobile), les annonceurs (commerce mobile) et les services d'annuaire. Les messages d'une ESME (entité non mobile) arrivent au MC, qui les distribue à des entités de messagerie courte (PME) telles que des téléphones portables. Le SMPP est également utilisé par les PME pour envoyer de courts messages à des tiers (par exemple, pour l'achat de produits, le paiement de factures et les transferts de fonds). Ces messages arrivent au MC et sont transmis au MC ou à l'ESME de destination.

Le diagramme suivant montre les différentes entités SMPP : ESME, RE et MCs, dans un réseau mobile.



Présentation de l'architecture des différentes entités SMPP dans un réseau mobile

Remarque : Les termes client et ESME sont utilisés de manière interchangeable dans tout le document.

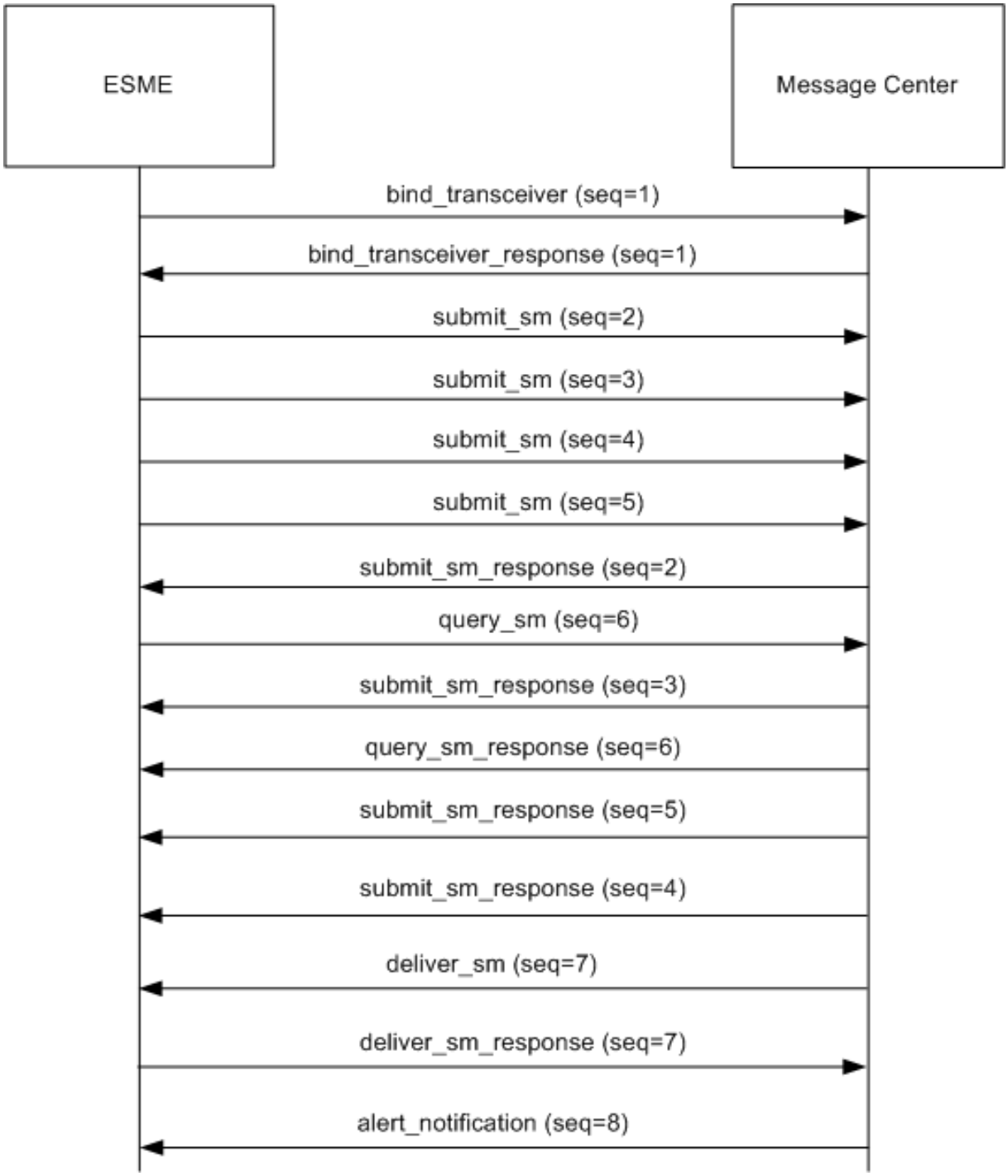
Un ESME (client) ouvre une connexion au MC dans l'un des trois modes suivants : émetteur, récepteur ou émetteur-récepteur. En tant qu'émetteur, il peut uniquement envoyer des messages pour livraison. En tant que récepteur, il ne peut recevoir que des messages. En tant qu'émetteur-récepteur, l'ESME peut à la fois envoyer et recevoir des messages. L'ESME envoie au MC l'un des trois messages (également appelés PDU) : bind_transmitter, bind_receiver ou bind_transceiver. Le MC répond par un bind_transmitter_resp, un bind_receiver_resp ou un bind_transceiver_resp, selon la requête.

Une fois la connexion établie, l'ESME peut, selon le mode dans lequel il est lié au MC, envoyer un message submit_sm ou data_sm, recevoir un message deliver_sm ou data_sm, ou envoyer et recevoir n'importe lequel de ces types de messages. L'ESME peut également envoyer des messages auxiliaires, tels que query_sm, replace_sm et cancel_sm, pour demander l'état d'une remise de message antérieure, remplacer un message antérieur par un nouveau message ou annuler un message non remis.

Si un message n'est pas remis parce qu'un ESME n'est pas disponible ou qu'un abonné mobile n'est pas en ligne, le message est mis en file d'attente. Plus tard, lorsque le MC détecte que l'abonné mobile est désormais joignable, il envoie une PDU alert_notification à l'ESME via une session de récepteur ou d'émetteur-récepteur, demandant la livraison de tous les messages en file d'attente.

Chaque PDU de demande possède un numéro de séquence unique. La PDU de réponse possède le même numéro de séquence que la demande d'origine. Comme l'échange de messages via SMPP peut se faire en mode asynchrone, un ESME ou un MC peut envoyer plusieurs demandes à la fois. Le numéro de séquence joue un rôle crucial dans le renvoi de la réponse au cours de la même session SMPP. En d'autres termes, le numéro de séquence permet la mise en correspondance des demandes et des réponses.

Le diagramme suivant montre comment le flux de trafic utilise les différentes PDU lorsque l'ESME se lie en tant qu'émetteur-récepteur.



Limitation :

L'appliance NetScaler ne prend pas en charge les opérations sortantes. En d'autres termes, un centre de messagerie ne peut pas lancer de session SMPP avec un ESME via l'appliance NetScaler.

Comment fonctionne l'équilibrage de charge SMPP sur NetScaler

Un ESME (client) envoie un message de liaison pour ouvrir une connexion à NetScaler. L'ADC authentifie chaque ESME et, en cas de succès, répond par un message approprié. NetScaler établit une connexion avec chaque centre de messagerie et équilibre la charge de tous les messages entre ces centres de messagerie. Lorsque l'ADC reçoit un message d'un client, il réutilise une connexion ouverte au centre de messagerie ou envoie une demande de liaison à un centre de messagerie si aucune connexion ouverte n'est disponible.

L'ADC peut équilibrer la charge des messages provenant des clients et des serveurs. Il peut surveiller l'état des centres de messagerie et gérer les messages concaténés. Il fournit également un support de commutation de contenu pour les centres de messagerie.

Messages en provenance des PME

Chaque ESME doit être ajouté en tant qu'utilisateur sur NetScaler pour l'authentification. Le client établit une connexion TCP avec un serveur virtuel SMPP configuré sur l'ADC en envoyant une demande de liaison. L'ADC authentifie le client et, en cas de succès, analyse le message de liaison. L'ADC envoie ensuite la demande au centre de messagerie sélectionné par la méthode d'équilibrage de charge configurée. Si aucune connexion au centre de messagerie n'est disponible pour être réutilisée, l'ADC ouvre une connexion TCP avec le centre de messagerie en envoyant une nouvelle demande de liaison au centre de messagerie.

Avant de transmettre la réponse (submit_sm_resp ou data_sm_resp) du centre de messagerie au client, l'ADC ajoute un ID de serveur personnalisé à l'ID du message afin d'identifier le centre de messagerie pour les opérations auxiliaires, telles que les requêtes, le remplacement ou l'annulation de demandes de message par le client. Les demandes provenant d'autres clients sont équilibrées de la même manière.

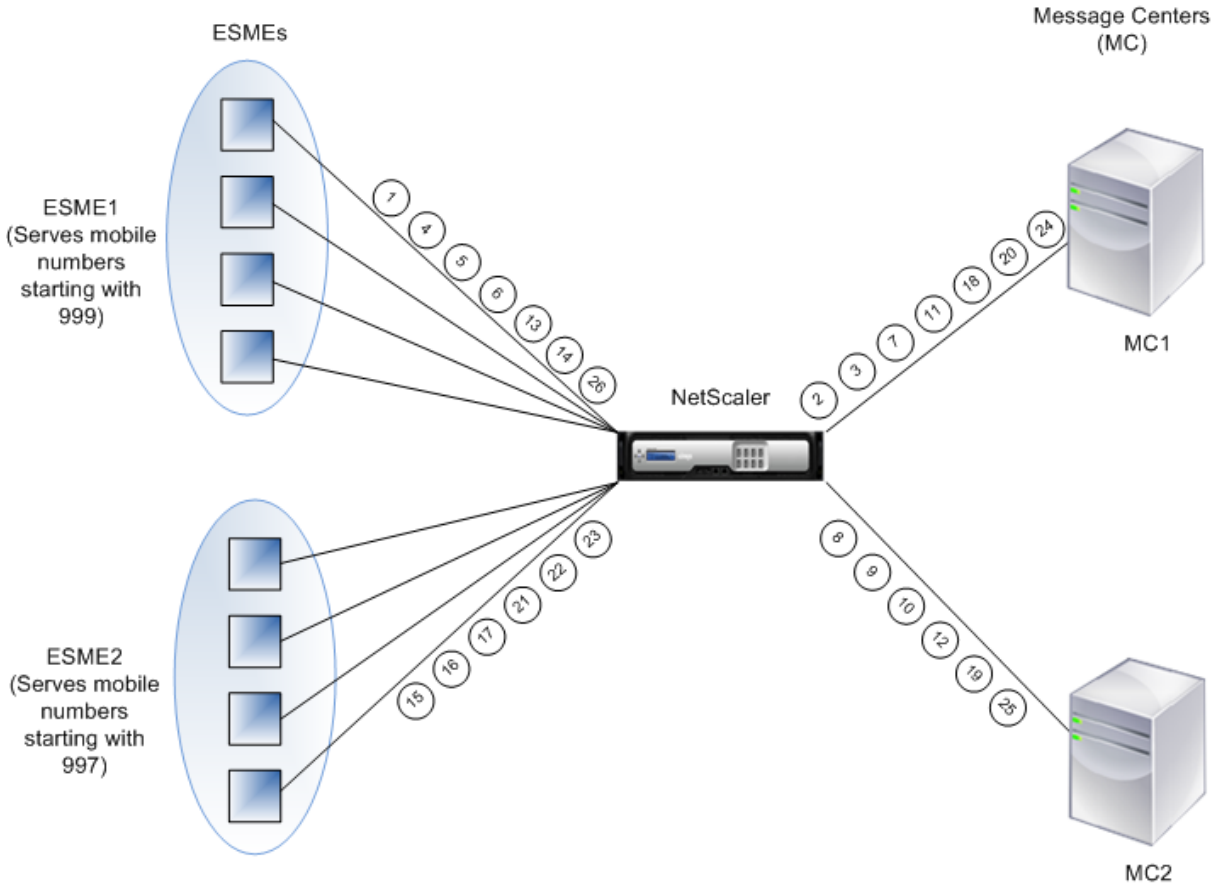
Dans la demande de liaison d'origine, un client spécifie la plage d'adresses qu'il peut servir. Cette plage est utilisée pour transférer les messages deliver_sm ou data_sm des centres de messagerie vers les clients.

Messages provenant d'un centre de messagerie

Les PME qui peuvent gérer une plage d'adresses spécifique sont regroupées dans un cluster. Tous les nœuds d'un cluster fournissent les mêmes informations d'identification. Au sein d'un cluster, seule la méthode du round robin est utilisée pour l'équilibrage de charge. Pour distribuer des messages d'origine mobile (MO), le centre de messagerie envoie un message deliver_sm à NetScaler. Si un cluster pouvant desservir la plage d'adresses de destination (par exemple, des nombres commençant par 998) est lié à l'ADC, il sélectionne ce cluster, puis équilibre la charge du message entre les nœuds ESME de ce cluster.

Si un ESME capable de servir des messages deliver_sm pour la plage d'adresses n'est pas lié à l'ADC et que la mise en file d'attente des messages est activée, le message est mis en file d'attente jusqu'à ce qu'un tel client se lie à l'ADC en mode récepteur ou émetteur-récepteur. Vous pouvez spécifier la taille de la file d'attente.

Le schéma suivant illustre le flux interne de PDU entre les ESME, NetScaler et les centres de messagerie. Par souci de simplicité, seuls deux ESME et deux centres de messages sont affichés.



Flux de messages (PDU) :

1. ESME1 envoie une demande de liaison à NetScaler
2. NetScaler envoie une demande de liaison à MC1
3. MC1 envoie une réponse de liaison à NetScaler
4. NetScaler envoie une réponse de liaison à ESME1
5. ESME1 envoie submit_sm (1) à NetScaler
6. ESME1 envoie submit_sm (2) à NetScaler
7. NetScaler transmet submit_sm (1) à MC1
8. NetScaler envoie une demande de liaison à MC2
9. MC2 envoie une réponse de liaison à NetScaler
10. NetScaler transmet submit_sm (2) à MC2
11. MC1 envoie submit_sm_resp (1) à NetScaler

12. MC2 envoie submit_sm_resp (2) à NetScaler
13. NetScaler transmet submit_sm_resp (1) à ESME1
14. NetScaler transmet submit_sm_resp (2) à ESME1
15. ESME2 envoie une demande de liaison à NetScaler
16. NetScaler envoie une réponse de liaison à ESME2
17. ESME2 envoie submit_sm (3) à NetScaler
18. NetScaler transmet submit_sm (3) à MC1
19. MC2 envoie deliver_sm à NetScaler (ESME2 sert la plage d'adresses spécifiée dans le message)
20. MC1 envoie submit_sm_resp (3) à NetScaler
21. NetScaler transmet submit_sm_resp (3) à ESME2
22. NetScaler transmet deliver_sm à ESME2
23. ESME2 envoie deliver_sm_resp à NetScaler
24. MC1 envoie alert_notification à NetScaler (ESME1 sert la plage d'adresses spécifiée dans le message)
25. NetScaler transmet deliver_sm_resp à MC2
26. NetScaler transmet l'alert_notification à ESME1

Surveillance de l'état de santé des centres de messagerie

Par défaut, un moniteur TCP_Default est lié à un service SMPP, mais vous pouvez lier un moniteur personnalisé de type SMPP. Le moniteur personnalisé ouvre une connexion TCP vers le centre de messagerie et envoie un paquet inquire_link. En fonction de la réussite ou de l'échec de la sonde, le service est marqué comme « UP » ou « NON ».

Basculement du contenu dans les centres de messagerie

Les centres de messagerie peuvent accepter plusieurs connexions (ou lier des demandes) provenant d'ESME. Vous pouvez configurer NetScaler pour qu'il bascule le contenu de ces requêtes en fonction des paramètres de liaison SMPP. Voici quelques expressions courantes pour configurer les méthodes de sélection d'un centre de messages :

- Sur la base de la plage d'adresses : dans l'exemple d'expression suivant, l'ADC sélectionne un centre de messagerie spécifique si la plage d'adresses commence à 988.

Exemple :

SMPP.BINDINFO.ADDRESS_RANGE.CONTAINS("^988")

- Sur la base de l'ID ESME : Dans l'exemple d'expression suivant, l'ADC sélectionne un centre de messagerie spécifique si l'ID ESME est égal à ESME1.

Exemple :

SMPP.BINDINFO.SYSTEM_ID.EQ (« ESME1 »)

- En fonction du type ESME : dans l'exemple d'expression suivant, l'ADC sélectionne un centre de messagerie spécifique si le type ESME est VMS. VMS est l'abréviation de Voice Mail System.

Exemple :

SMPP.BINDINFO.SYSTEM_TYPE.EQ (« MACHINES VIRTUELLES »)

- Sur la base du type de numéro (TON) de l'ESME : Dans l'exemple d'expression suivant, l'ADC sélectionne un centre de messagerie spécifique si TON est égal à 1 (1 représente un numéro international).

Exemple :

SMPP.BINDINFO.ADDR_TON.EQ (1)

- Sur la base de l'indicateur de plan de numérotation (NPI) de l'ESME : dans l'exemple d'expression suivant, l'ADC sélectionne un centre de messagerie spécifique si le NPI est égal à 0 (0 représente une connexion inconnue).

Exemple :

SMPP.BINDINFO.ADDR_NPI.EQ (0)

- En fonction du type de liaison : dans l'exemple d'expression suivant, l'ADC sélectionne un centre de messagerie spécifique si le type de liaison est TRANSCEIVER. (Un émetteur-récepteur peut envoyer et recevoir des messages.)

Exemple :

SMPP.BINDINFO.TYPE.EQ (ÉMETTEUR-RÉCEPTEUR)

Gestion des messages concaténés

Un SMS peut contenir au maximum 140 octets. Les messages plus longs doivent être divisés en parties plus petites. Si le mobile de destination est capable, les messages sont combinés et envoyés sous la forme d'un seul long SMS. NetScaler transmet les fragments d'un message au même centre de messagerie. Chaque message contient un numéro de référence, un numéro de séquence et le nombre total de fragments. Le numéro de référence est le même pour chaque fragment d'un long message. Le numéro de séquence indique la position du fragment particulier dans le message complet. Une fois que tous les fragments ont été reçus, l'ESME les combine en un seul long message et transmet le message à l'abonné mobile.

Si un client se déconnecte d'une connexion active, la connexion au centre de messagerie n'est pas fermée. Il est réutilisé pour les demandes d'autres clients.

Limitation

Les ID de message, provenant du centre de messagerie, supérieurs à 59 octets ne sont pas pris en charge. Si la longueur de l'ID de message renvoyé par le centre de messagerie est supérieure à 59 octets, les opérations auxiliaires échouent et NetScaler répond par un message d'erreur.

Configuration de l'équilibrage de charge SMPP sur NetScaler

Effectuez les tâches suivantes pour configurer l'équilibrage de charge SMPP sur l'ADC :

1. Ajoutez un utilisateur SMPP. L'ADC authentifie l'utilisateur avant d'accepter une demande de liaison de sa part. L'utilisateur est généralement un ESME.
2. Ajoutez un serveur virtuel d'équilibrage de charge, en spécifiant le protocole comme SMPP.
3. Ajoutez un service, en spécifiant le protocole SMPP, et un ID de serveur personnalisé unique pour chaque serveur. Liez le service au serveur virtuel d'équilibrage de charge créé précédemment.
4. Vous pouvez également créer un groupe de services et y ajouter des services.
5. Ajoutez éventuellement un moniteur de type SMPP-ECV et liez-le au service. Un moniteur TCP par défaut est lié par défaut.
6. Définissez les paramètres SMPP, tels que le mode client et la file de messages.

Pour configurer l'équilibrage de charge SMPP à l'aide de la ligne de commande

À l'invite de commande, tapez :

```
add smpp user <username> -password <password>
add service <name> <IP> SMPP <port>  - customserverID <customserverID>
add lb vserver <name> <IP> SMPP <port>
bind lb vserver <name> <service name>
set smpp param
<!--NeedCopy-->
```

Exemple

```
add smpp user smppclient1 -password c03ebb540695b6110eb31172f32245a1 -
    encrypted -encryptmethod ENCMTHD_2
add smpp user smppclient2 -password c03ebb540695b6110eb31172f32245a1 -
    encrypted -encryptmethod ENCMTHD_2
add service smmpsvc 10.102.84.140 SMPP 2775 -gslb NONE -maxClient 0 -
    maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
     180 -svrTimeout 360 -CustomServerID ab -CKA NO -TCPB NO -CMP NO
```



```
add service smmpsvc2 10.102.81.175 SMPP 2775 -gslb NONE -maxClient 0 -
    maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
     180 -svrTimeout 360 -CustomServerID xy -CKA NO -TCPB NO -CMP NO
add lb vserver smppvs SMPP 10.102.239.179 2775 -persistenceType NONE -
    cltTimeout 180
bind lb vserver smppvs smmpsvc2
bind lb vserver smppvs smmpsvc
set smpp param -addrrange "d*"
<!--NeedCopy-->
```

Pour configurer l'équilibrage de charge SMPP à l'aide de l'utilitaire de configuration

1. Accédez à **Système > Administration des utilisateurs > Utilisateurs SMPP**, puis ajoutez un utilisateur SMPP.
2. Accédez à **Gestion du trafic > Équilibrage de charge > Configurer les paramètres SMPP**et définissez les paramètres comme requis par votre déploiement.
3. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ajoutez un serveur virtuel de type SMPP.
4. Cliquez dans la section Service, ajoutez un service de type SMPP et spécifiez un ID de serveur.

Cas d'utilisation 2 : configurer la persistance basée sur des règles en fonction d'une paire nom-valeur dans un flux d'octets TCP

May 5, 2023

Certains protocoles transmettent des paires nom-valeur dans un flux d'octets TCP. Le protocole du flux d'octets TCP dans cet exemple est le protocole FIX (Financial Information eXchange). Dans une implémentation non XML, le protocole FIX permet à deux hôtes communiquant via un réseau d'échanger des informations commerciales ou liées au commerce sous forme de liste de paires nom-valeur (appelées « champs FIX »). Le format du champ est <tag>=<value><delimiter>. Ce format de valeur de balise traditionnel rend le protocole FIX idéal pour ce cas d'utilisation.

La balise dans un champ FIX est un identifiant numérique qui indique la signification du champ. Dans cet exemple ;

- La balise 35 indique le type de message.
- La valeur après le signe égal a une signification spécifique pour la balise donnée et est associée à un type de données. La valeur A pour la balise 35 indique que le message est un message d'ouverture de session.

- Le délimiteur est le caractère ASCII « Start of Header » (SOH) non imprimable (0x01), qui est le symbole de curseur (^).
- Un nom est également attribué à chaque champ. Le champ portant la balise 35 est le champ MsgType.

Voici un exemple de message d'ouverture de session.

8=FIX.4.1 9=61 35=A 49=INVMGR 56=BRKR 34=1 52= 20000426-12:05:06 98=0 108=30 10=157

Votre choix de type de persistance pour une liste de valeurs de balises telle que celle présentée ci-dessus est déterminé par les options qui s'offrent à vous pour extraire une chaîne particulière de la liste. Les méthodes de persistance basées sur des jetons nécessitent que vous spécifiez le décalage et la longueur du jeton que vous souhaitez extraire de la charge utile. Le protocole FIX ne vous permet pas de le faire, car le décalage d'un champ donné et la longueur de sa valeur peuvent varier d'un message à l'autre. Cette variation dépend du type de message, des champs précédents et de la longueur des valeurs précédentes. Il varie également en fonction de l'implémentation de l'un à l'autre, selon que des champs personnalisés ont été définis ou non. De telles variations rendent impossible de prédire le décalage exact d'un champ donné ou de spécifier la longueur de la valeur à extraire comme jeton. Dans ce cas, la persistance basée sur des règles est donc le type de persistance préféré.

Supposons qu'un serveur virtuel fixlb1 équilibrage la charge des connexions TCP à une batterie de serveurs hébergeant des instances d'une application compatible FIX. Vous souhaitez configurer la persistance des connexions sur la base de la valeur du champ SenderCompid, qui identifie l'entreprise qui envoie le message. La balise de ce champ FIX est 49 (illustrée dans l'exemple de message d'ouverture de session précédent).

Pour configurer la persistance basée sur des règles pour le serveur virtuel d'équilibrage de charge, définissez le type de persistance du serveur virtuel d'équilibrage de charge sur RULE et configurez le paramètre de règle avec une expression. L'expression doit extraire la partie de la charge utile TCP dans laquelle vous pensez trouver le champ SenderCompID, tape la chaîne résultante dans une liste nom-valeur basée sur les délimiteurs, puis extrait la valeur du champ SenderCompID (balise 49), comme suit :

```
set lb vserver fixlb1 -persistenceType RULE -rule "CLIENT.TCP.PAYLOAD(300).
TYPECAST_NVLIST_T('=','^').VALUE("\49\")"
```

Remarque : Des barres obliques inverses ont été utilisées dans l'expression car il s'agit d'une commande CLI. Si vous utilisez l'utilitaire de configuration, ne saisissez pas de barres obliques inverses.

Si le client envoie un message FIX contenant la liste nom-valeur de l'exemple de message d'ouverture de session précédent, l'expression extrait la valeur INVMGR et l'appliance NetScaler crée une session de persistance basée sur cette valeur.

L'argument de la fonction PAYLOAD () peut être aussi grand que vous le jugez nécessaire pour inclure le champ SenderCompid dans la chaîne extraite par la fonction. Vous pouvez également utiliser la

fonction SET_TEXT_MODE (IGNORECASE) si vous souhaitez que l'appliance ignore la casse lors de l'extraction de la valeur du champ, et que la fonction HASH crée une session de persistance basée sur un hachage de la valeur extraite. L'expression suivante utilise les fonctions SET_TEXT_MODE (IGNORECASE) et HASH :

```
CLIENT.TCP.PAYLOAD(500).TYPECAST_NVLIST_T('=','^').SET_TEXT_MODE(IGNORECASE
).VALUE("49").HASH
```

Vous trouverez ci-dessous d'autres exemples de règles que vous pouvez utiliser pour configurer la persistance des connexions FIX (à <tag> remplacer par la balise du champ dont vous souhaitez extraire la valeur) :

- Pour extraire la valeur d'un champ FIX dans les 300 premiers octets de la charge utile TCP, vous pouvez utiliser l'expression CLIENT.TCP.PAYLOAD (300) .BEFORE_STR (« ^ ») .AFTER_STR (» = »).<tag>
- Pour extraire une chaîne de 20 octets avec un décalage de 80, convertir la chaîne en une liste nom-valeur, puis extraire la valeur du champ souhaité, utilisez l'expression CLIENT.TCP.PAYLOAD (100) .SUBSTR (80,20) .TYPECAST_NVLIST_T ('=', '^') .VALUE (» «).<tag>
- Pour extraire les 100 premiers octets de la charge utile TCP, convertir la chaîne en une liste nom-valeur et extraire la valeur de la troisième occurrence du champ souhaité, utilisez l'expression CLIENT.TCP.PAYLOAD (100) .TYPECAST_NVLIST_T ('=', '^') .VALUE (» « ,2).<tag>
  Remarque : Si le deuxième argument transmis à la fonction
  VALUE () est
  n, l'appliance extrait la valeur de l'
  th instance
  (n+1) du champ car le décompte commence à zéro (
  0).

Vous trouverez ci-dessous d'autres exemples de règles que vous pouvez utiliser pour configurer la persistance. Seules les expressions basées sur la charge utile peuvent évaluer les données transmises via le protocole FIX. Les autres expressions sont des expressions plus générales permettant de configurer la persistance sur la base de protocoles réseau inférieurs.

- CLIENT.TCP.PAYLOAD (100)
- CLIENT.TCP.PAYLOAD (100) .HASH
- CLIENT.TCP.PAYLOAD (100) .SUBSTR (5,10)
- CLIENT.TCP.SRCPORT
- CLIENT.TCP.DSTPORT
- CLIENT.IP.SRC
- CLIENT.IP.DST
- CLIENT.IP.SRC.GET4
- CLIENT.IP.DST.GET4
- CLIENT.ETHER.SRCMAC.GET6

- CLIENT.ETHER.DSTMAC.GET5
- CLIENT.VLAN.ID

Cas d'utilisation 3 : configurer l'équilibrage de charge en mode de retour direct du serveur

May 5, 2023

L'équilibrage de charge en mode DSR (Direct Server Return) permet au serveur de répondre directement aux clients en utilisant un chemin de retour qui ne passe pas par l'appliance NetScaler. En mode DSR, toutefois, l'appliance peut continuer à effectuer des contrôles de santé sur les services. Dans un environnement à volume de données élevé, l'envoi du trafic du serveur directement au client en mode DSR augmente la capacité globale de traitement des paquets de l'appliance car les paquets ne transitent pas par l'appliance.

Le mode DSR présente les fonctionnalités et limites suivantes :

- Il prend en charge le mode à un bras et le mode intégré.
- L'appliance vieillit les sessions en fonction du délai d'inactivité.
- Étant donné que l'appliance ne fournit pas de proxy aux connexions TCP (c'est-à-dire qu'elle n'envoie pas SYN-ACK au client), elle n'arrête pas les attaques SYN. En utilisant le filtre de débit de paquets SYN, vous pouvez contrôler le taux de SYN sur le serveur. Pour contrôler le taux de SYNs, définissez un seuil pour le taux de SYNs. Pour vous protéger contre les attaques SYN, vous devez configurer l'appliance pour qu'elle utilise un proxy pour les connexions TCP. Toutefois, cela nécessite que le trafic inverse passe par l'appliance.
- Dans une configuration DSR, l'appliance NetScaler ne remplace pas l'adresse IP du serveur virtuel d'équilibrage de charge par l'adresse IP du serveur de destination. Au lieu de cela, il transfère les paquets à un service en utilisant l'adresse MAC du serveur. Le VIP doit être configuré sur le serveur et ARP doit être désactivé pour le VIP configuré sur le serveur. Cela empêche la demande du client de contourner l'appliance lorsqu'elle est configurée en mode à bras unique. Par exemple, un utilisateur doit configurer VIP dans l'interface de bouclage et désactiver l'ARP pour le même VIP.
- L'appliance obtient l'adresse MAC du serveur à partir du moniteur lié au service. Toutefois, les moniteurs utilisateur personnalisés (moniteurs de type USER), qui utilisent des scripts stockés sur l'appliance NetScaler, n'apprennent pas l'adresse MAC d'un serveur. Si vous utilisez uniquement des moniteurs personnalisés dans une configuration DSR, pour chaque demande reçue par le serveur virtuel, l'appliance tente de convertir l'adresse IP de destination en adresse MAC (en envoyant des requêtes ARP). Comme l'adresse IP de destination est une adresse IP virtuelle appartenant à l'appliance NetScaler, les requêtes ARP sont toujours résolues vers l'adresse MAC de l'interface NetScaler. Par conséquent, tout le trafic reçu par le serveur virtuel est renvoyé en

boucle vers l'appliance. Si vous utilisez des moniteurs utilisateur dans une configuration DSR, vous devez également configurer un autre moniteur d'un type différent (par exemple, un moniteur PING) pour les services, idéalement avec un intervalle plus long entre les sondes, afin que l'adresse MAC des serveurs puisse être apprise.

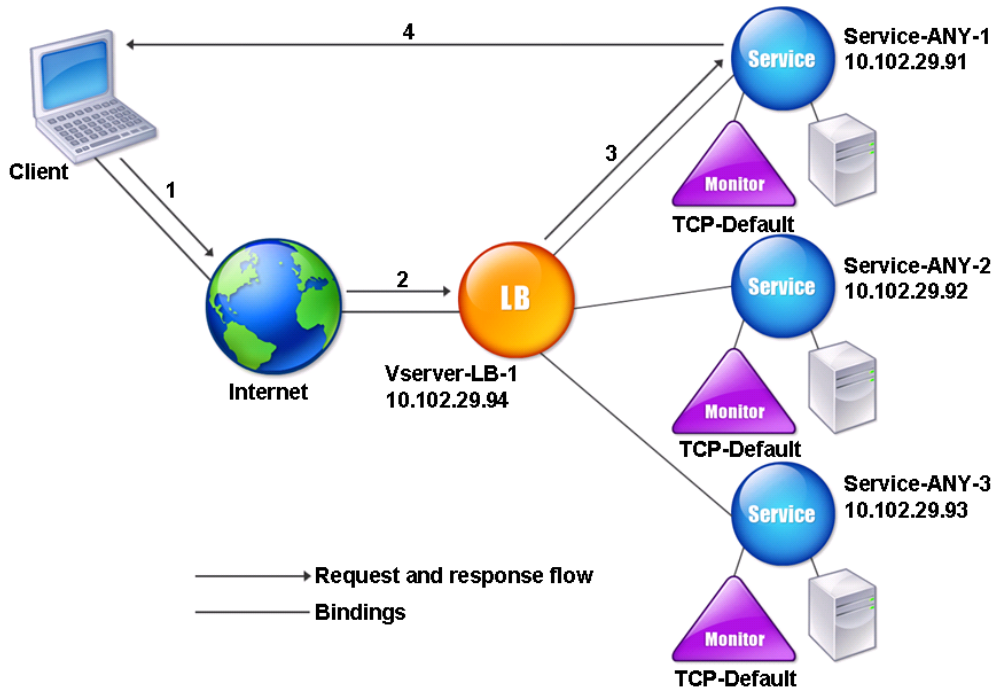
- L'appliance NetScaler apprend les paramètres L2 du serveur à partir du moniteur lié au service. Pour les moniteurs UDP-ECV, configurez une chaîne de réception pour permettre à l'appliance d'apprendre les paramètres L2 du serveur. Si la chaîne de réception n'est pas configurée et que le serveur ne répond pas, l'appliance n'apprend pas les paramètres L2 mais le service est configuré sur UP. Le trafic de ce service est bloqué.

Dans l'exemple de scénario, les services Service-ANY-1, Service-ANY-2 et Service-ANY-3 sont créés et liés au serveur virtuel Vserver-LB-1. Le serveur virtuel équilibre la charge de la demande du client vers un service, et le service répond directement aux clients, en contournant l'appliance NetScaler. Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance NetScaler en mode DSR.

Type d'entité	Nom	Adresse IP	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY
	Service-ANY-3	10.102.29.93	ANY
Moniteurs	TCP	Aucun	Aucun

Le schéma suivant montre les entités d'équilibrage de charge et les valeurs des paramètres à configurer sur l'appliance.

Figure 1. Modèle d'entité pour l'équilibrage de charge dans le modèle DSR



Pour que l'appliance fonctionne correctement en mode DSR, l'adresse IP de destination figurant dans la demande du client doit être inchangée. Au lieu de cela, l'appliance remplace le MAC de destination par celui du serveur sélectionné. Ce paramètre permet au serveur de déterminer l'adresse MAC du client pour transférer les demandes au client tout en contournant le serveur.

Ensuite, vous configurez une configuration d'équilibrage de charge de base comme décrit dans Configuration de l'équilibrage de chargede base, nommer les entités et définir les paramètres à l'aide des valeurs décrites dans le tableau précédent.

Après avoir configuré la configuration d'équilibrage de charge de base, vous devez la personnaliser pour le mode DSR. Pour ce faire, vous configurez une méthode d'équilibrage de charge prise en charge, telle que la méthode de hachage de l'adresse IP source avec un serveur virtuel sans session. Vous devez également définir le mode de redirection pour permettre au serveur de déterminer l'adresse MAC du client pour le transfert des réponses et de contourner l'appliance.

Après avoir configuré la méthode d'équilibrage de charge et le mode de redirection, vous devez activer le mode USIP sur chaque service. Le service utilise ensuite l'adresse IP source lors du transfert des réponses.

Pour configurer la méthode d'équilibrage de charge et le mode de redirection pour un serveur virtuel sans session à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
   RedirectionMode> -sessionless <Value>
<!--NeedCopy-->
```

Exemple

```
set lb vserver Vserver-LB-1 -lbMethod SourceIPHash -m MAC -sessionless
   enabled
<!--NeedCopy-->
```

> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l'option -m MAC est activée, vous devez lier un moniteur non utilisateur.

Pour configurer la méthode d'équilibrage de charge et le mode de redirection pour un serveur virtuel sans session à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel, sélectionnez le mode de redirection comme étant basé sur MAC et la méthode comme SOURCEIPHASH.
3. Dans Paramètres du trafic, sélectionnez Équilibrage de charge sans session.

Pour configurer un service afin qu'il utilise l'adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <ServiceName> -usip <Value>
<!--NeedCopy-->
```

Exemple :

```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```


Pour configurer un service afin qu'il utilise l'adresse IP source à l'aide de l'utilitaire de configuration

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Ouvrez un service, puis dans Paramètres de trafic, sélectionnez **Utiliser l'adresse IP source**.

Certaines étapes supplémentaires sont nécessaires dans certaines situations, décrites dans les sections suivantes.

Cas d'utilisation 4 : Configuration des serveurs LINUX en mode DSR

May 5, 2023

Le système d'exploitation LINUX nécessite que vous configuriez une interface de bouclage avec l'adresse IP virtuelle (VIP) de l'appliance NetScaler sur chaque serveur d'équilibrage de charge du cluster DSR.

Pour configurer le serveur LINUX en mode DSR

Pour créer une interface de boucle avec le VIP de l'appliance NetScaler sur chaque serveur d'équilibrage de charge, tapez les commandes suivantes à l'invite du système d'exploitation Linux :

```
ifconfig dummy0 up

ifconfig dummy0:0 inet <netscaler vip> netmask 255.255.255.255 up

echo 1 > /proc/sys/net/ipv4/conf/dummy0/arp_ignore

echo 2 > /proc/sys/net/ipv4/conf/dummy0/arp_announce
<!--NeedCopy-->
```

Ensuite, exécutez le logiciel qui remappe l'identifiant TOS en VIP.

Remarque : ajoutez les mappages corrects au logiciel avant de l'exécuter. Dans les commandes précédentes, le serveur LINUX utilise dummy0 pour se connecter au réseau. Lorsque vous utilisez cette commande, tapez le nom de l'interface utilisée par votre serveur LINUX pour se connecter au réseau.

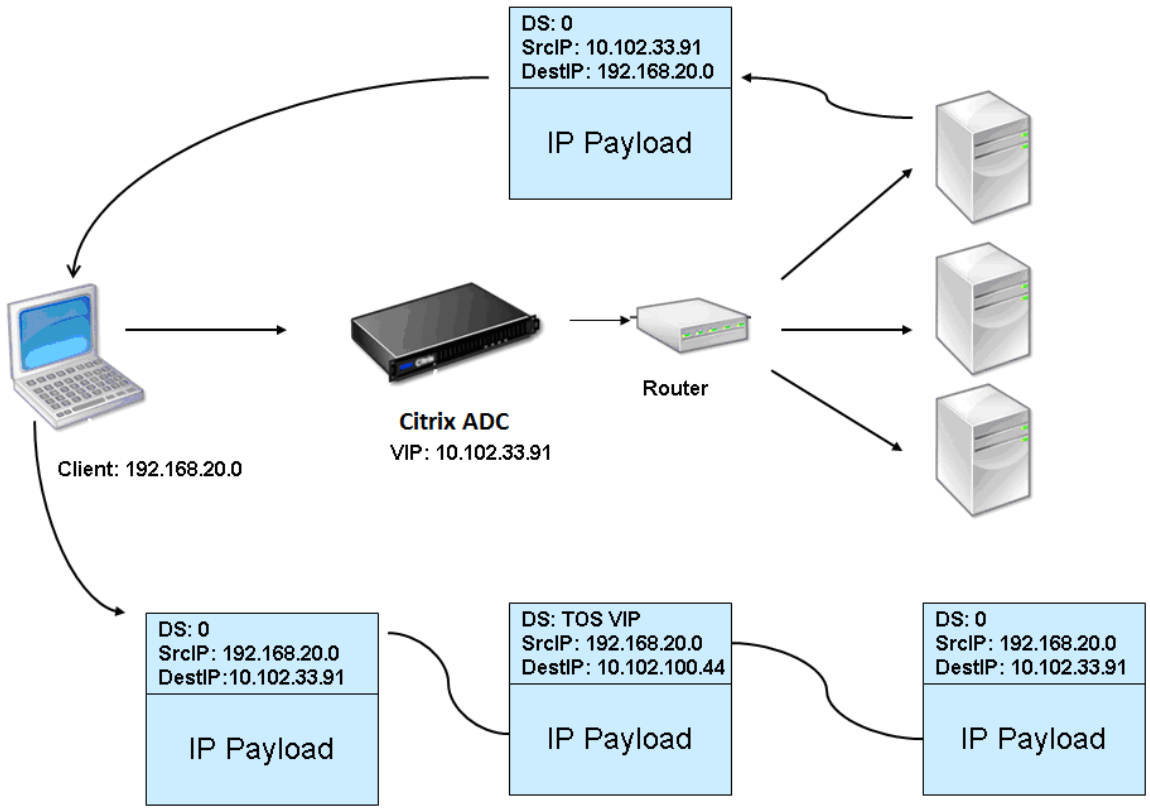
Cas d'utilisation 5 : configurer le mode DSR lors de l'utilisation de TOS

May 5, 2023

Les services différenciés (DS), également appelés TOS (Type de service), sont un champ qui fait partie de l'en-tête du paquet IPv4. Le champ équivalent dans l'en-tête IPv6 est Traffic Class. Le TOS est utilisé par les protocoles de couche supérieure pour optimiser le chemin d'un paquet. Les informations TOS codent l'adresse IP virtuelle (VIP) de l'appliance NetScaler, et les serveurs d'équilibrage de charge en extraient l'adresse VIP.

Dans le scénario suivant, l'appliance ajoute le VIP au champ **TOS** du paquet, puis transmet le paquet au serveur d'équilibrage de charge. Le serveur d'équilibrage de charge répond ensuite directement au client, en contournant l'appliance, comme illustré dans le schéma suivant.

Figure 1. L'appliance NetScaler en mode DSR avec TOS



La fonctionnalité TOS est personnalisée pour un environnement contrôlé comme suit :

- L'environnement ne doit comporter aucun périphérique dynamique, tel qu'un pare-feu dynamique et des passerelles TCP, sur le chemin entre l'appliance et les serveurs d'équilibrage de charge.
- Les routeurs situés à tous les points d'entrée du réseau doivent supprimer le champ TOS de tous les paquets entrants pour s'assurer que le serveur d'équilibrage de charge ne confond pas un autre champ TOS avec celui ajouté par l'appliance.
- Chaque serveur ne peut avoir que 63 VIP.

- Le routeur intermédiaire ne doit pas envoyer de messages d'erreur ICMP concernant la fragmentation. Le client ne comprend pas le message, car l'adresse IP source est l'adresse IP du serveur d'équilibrage de charge et non celle de NetScaler VIP.
- Le TOS est valide uniquement pour les services basés sur IP. Vous ne pouvez pas utiliser de services basés sur des noms de domaine avec TOS.

Dans l'exemple, Service-Any-1 est créé et lié au serveur virtuel vServer-LB-1. Le serveur virtuel équilibre la charge de la demande du client adressée au service, et le service répond directement aux clients, en contournant l'appliance. Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance en mode DSR.

Type d'entité	Nom	Adresse IP	Protocole
Serveur virtuel	Vserver-LB-1	10.102.33.91	ANY
Services	Service-ANY-1	10.102.100.44	ANY
Moniteurs	PING	Aucun	Aucun

DSR avec TOS nécessite que l'équilibrage de charge soit configuré sur la couche 3. Pour configurer une configuration d'équilibrage de charge de base pour la couche 3, reportez-vous à la section Configuration de l'équilibrage de charge de base. Nommez les entités et définissez les paramètres à l'aide des valeurs décrites dans le tableau précédent.

Après avoir configuré la configuration d'équilibrage de charge, vous devez personnaliser la configuration d'équilibrage de charge pour le mode DSR en configurant le mode de redirection pour permettre au serveur de désencapsuler le paquet de données, puis de répondre directement au client et de contourner l'appliance.

Après avoir spécifié le mode de redirection, vous pouvez éventuellement activer l'appliance pour qu'elle surveille le serveur de manière transparente. Cela permet à l'appliance de surveiller de manière transparente les serveurs à charge équilibrée.

Pour configurer le mode de redirection pour le serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <vServerName> -m <Value> -tosId <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -m TOS -tosId 3
```



```
<!--NeedCopy-->
```

Pour configurer le mode de redirection pour le serveur virtuel à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et, en mode redirection, sélectionnez TOS ID.

Pour configurer le moniteur transparent pour TOS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add monitor <MonitorName> <Type> -destip <DestinationIP> -tos <Value> -
   tosId <Value>
<!--NeedCopy-->
```

Exemple :

```
add monitor mon1 PING -destip 10.102.33.91 -tos Yes  -tosId 3
<!--NeedCopy-->
```

Pour créer le moniteur transparent pour TOS à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Créez un moniteur, sélectionnez TOS et tapez l'ID TOS que vous avez spécifié pour le serveur virtuel.

Moniteurs Wildcard TOS

Dans une configuration d'équilibrage de charge en mode DSR utilisant le champ TOS, la surveillance de ses services nécessite la création d'un moniteur TOS et lié à ces services. Un moniteur TOS distinct est requis pour chaque configuration d'équilibrage de charge en mode DSR à l'aide du champ TOS, car un moniteur TOS nécessite l'adresse VIP et l'ID TOS pour créer une valeur codée de l'adresse VIP. Le moniteur crée des paquets de sonde dans lesquels le champ **TOS** est défini sur la valeur codée de l'adresse VIP. Il envoie ensuite les paquets de sonde aux serveurs représentés par les services d'une configuration d'équilibrage de charge.

Avec de nombreuses configurations d'équilibrage de charge, la création d'un moniteur TOS personnalisé distinct pour chaque configuration est une tâche importante et fastidieuse. La gestion de ces moniteurs TOS est également une tâche importante. Vous pouvez désormais créer des moniteurs

TOS génériques. Créez un seul moniteur TOS générique pour toutes les configurations d'équilibrage de charge qui utilisent le même protocole (par exemple, TCP ou UDP).

Un moniteur TOS générique possède les paramètres obligatoires suivants :

- Type = <protocol>
- TOS = Oui

Les paramètres suivants peuvent être définis sur une valeur ou peuvent être laissés vides :

- IP destination
- Port de destination
- COUVERCLE DES JOUETS

Un moniteur TOS générique (avec IP de destination, port de destination et ID TOS non définis) lié à un service DSR apprend automatiquement l'ID TOS et l'adresse VIP du serveur virtuel d'équilibrage de charge. Le moniteur crée des paquets de sonde avec le champ TOS défini sur l'adresse VIP codée, puis envoie les paquets de sonde au serveur représenté par le service DSR.

Pour créer un moniteur de TOS générique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb monitor <monitorName> <Type> -tos YES

show lb monitor <monitorName>
<!--NeedCopy-->
```

Pour lier un moniteur TOS générique à un service à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb monitor <monitorName> <serviceName>

show lb monitor <monitorName>
<!--NeedCopy-->
```

Pour créer un moniteur TOS générique à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Moniteurs**.
2. Ajoutez un moniteur avec les paramètres suivants :
   - Type = <protocol>
   - TOS = OUI

Pour lier un moniteur TOS générique à un service à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Ouvrez un service et liez-y un moniteur TOS générique.

Dans l'exemple de configuration suivant, V1, V2 et V3 sont des serveurs virtuels d'équilibrage de charge de type ANY dont l'ID TOS est défini respectivement sur 1, 2 et 3. S1, S2, S3, S4 et S5 sont des services de type ANY. S1 et S2 sont liés à la fois à V1 et à V2. S3, S4 et S5 et lié à la fois à V1 et à V3. Le WLCD-TOS-MON est un moniteur TOS générique de type TCP lié à S1, S2, S3, S4 et S5.

WLCD-TOS-MON apprend automatiquement l'ID TOD et l'adresse VIP des serveurs virtuels liés à S1, S2, S3, S4 et S5.

Étant donné que S1 est lié à V1 et V2, WLCD-TOS-MON crée deux types de paquets de sonde pour S1, l'un avec le champ **TOS** défini sur l'adresse VIP codée (203.0.113.1) de V1 et l'autre avec l'adresse VIP (203.0.113.2) de V2. NetScaler envoie ensuite ces paquets de sonde au serveur représenté par S1. De même, WLCD-TOS-MON crée des paquets de sonde pour S2, S3, S4 et S5.

```
add lb monitor WLCD-TOS-MON  TCP -tos YES

Done

add lb vserver V1 ANY 203.0.113.1 * -m TOS  - tosID 1

Done

add lb vserver V2 ANY 203.0.113.2 * -m TOS  - tosID 2

Done

add lb vserver V3 ANY 203.0.113.3 * -m TOS  - tosID 3

Done

add service S1 198.51.100.1 ANY *

Done

add service S2 198.51.100.2 ANY *

Done

add service S3 198.51.100.3 ANY *

Done

```



```
add service S4 198.51.100.4 ANY *

Done

add service S5 198.51.100.5 ANY *

Done

bind lb monitor WLCD-TOS-MON S1

Done

bind lb monitor WLCD-TOS-MON S2

Done

bind lb monitor WLCD-TOS-MON S3

Done

bind lb monitor WLCD-TOS-MON S4

Done

bind lb monitor WLCD-TOS-MON S5

Done

bind lb vserver V1 S1, S2, S3, S4, S5

Done

bind lb vserver V2, S1, S2

Done

bind lb vserver V3 S3, S4, S5

Done
<!--NeedCopy-->
```


Cas d'utilisation 6 : configurer l'équilibrage de charge en mode DSR pour les réseaux IPv6 à l'aide du champ TOS

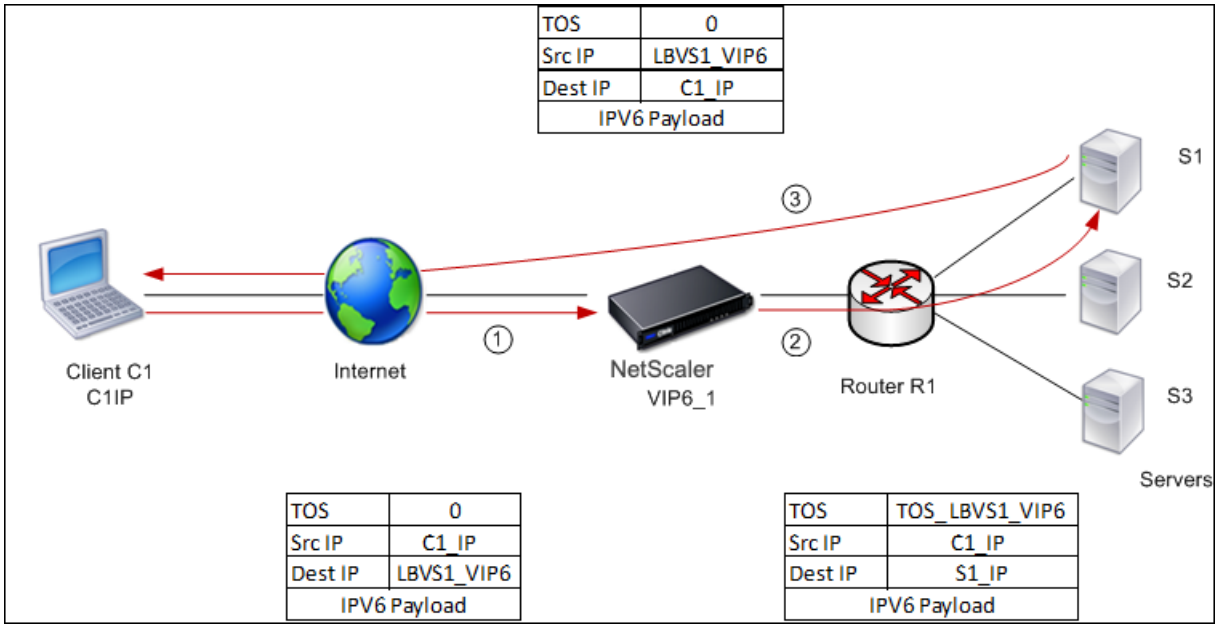
May 5, 2023

Vous pouvez configurer l'équilibrage de charge en mode Direct Server Return (DSR) pour les réseaux IPv6 à l'aide du champ Type de service (TOS) lorsque l'appliance NetScaler et les serveurs se trouvent sur des réseaux différents.

Remarque : Le champ TOS est également appelé champ Classe de trafic.

En mode DSR, lorsqu'un client envoie une demande à une adresse VIP6 sur une appliance NetScaler, l'appliance transmet cette demande au serveur en remplaçant l'adresse IPv6 de destination du paquet par l'adresse IPv6 du serveur et en définissant une valeur codée de l'adresse VIP6 dans le champ TOS (également appelé classe de trafic) de l'en-tête IPv6. Vous pouvez configurer le serveur pour qu'il utilise les informations du champ TOS afin de dériver l'adresse VIP6 à partir de la valeur codée, qui est ensuite utilisée comme adresse IP source dans les paquets de réponse. Le trafic de réponse est directement dirigé vers le client, en contournant l'appliance.

Prenons un exemple dans lequel un serveur virtuel d'équilibrage de charge LBVS1, configuré sur une appliance NetScaler NS1, est utilisé pour équilibrer la charge du trafic entre les serveurs S1, S2 et S3. L'appliance NetScaler NS1 et les serveurs S1, S2 et S3 se trouvent dans des réseaux différents. Le routeur R1 est donc déployé entre NS1 et les serveurs.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Entités	Nom
Adresse IPv6 du client C1	C1_IP (à titre de référence uniquement)
Serveur virtuel d'équilibrage de charge sur NS1	LBVS1
Adresse IPv6 de LBVS1	LBVS1_VIP6 (à titre de référence uniquement)
Valeur TOS	TOS_LBVS1_VIP6 (à titre de référence uniquement)
Service pour le serveur S1 sur NS1	SVC_S1
Adresse IPv6 pour le serveur S1	S1_IP (à des fins de référence uniquement)
Service pour le serveur S2 sur NS1	SVC_S2
Adresse IPv6 pour le serveur S1	S2_IP (à des fins de référence uniquement)
Service pour le serveur S3 sur NS1	SVC_S3
Adresse IPv6 pour le serveur S1	S3_IP (à des fins de référence uniquement)

Voici le flux de trafic dans l'exemple de scénario :

1. Le client C1 envoie une demande au serveur virtuel LBVS1.
2. L'algorithme d'équilibrage de charge de LBVS1 sélectionne le serveur S1 et l'appliance ouvre une connexion à S1. NS1 envoie la demande à S1 avec :
    - Le champ TOS est défini sur TOS_LBVS1_VIP6.
    - Adresse IP source sous la forme C1_IP.
3. À la réception de la demande, le serveur S1 utilise les informations du champ TOS pour dériver l'adresse LBVS1_VIP6, qui est l'adresse IP du serveur virtuel LBVS1 sur NS1. Le serveur envoie directement la réponse à C1, en contournant l'appliance, avec :
    - Adresse IP source définie sur l'adresse dérivée LBVS1_VIP6 afin que le client communique avec le serveur virtuel LBVS1 sur NS1 et non avec le serveur S1.

Pour configurer l'équilibrage de charge en mode DSR à l'aide de TOS, effectuez les étapes suivantes sur l'appliance

1. Activez le mode USIP globalement.
2. Ajoutez les serveurs en tant que services.
3. Configurez un serveur virtuel d'équilibrage de charge avec une valeur TOS.
4. Liez les services au serveur virtuel.

Pour configurer l'équilibrage de charge en mode DSR à l'aide de TOS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
enable ns mode USIP

add service <serviceName> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Répétez la commande précédente autant de fois que nécessaire pour ajouter chaque serveur en tant que service sur l'appliance NetScaler.

```
add lb vserver <name> <serviceType> <ip> <port> -m <redirectionMode> -
    tosId <positive_integer>

bind lb vserver <vserverName> <serviceName>
<!--NeedCopy-->
```

Pour activer le mode USIP à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres > Configurer les modes**, puis sélectionnez **Utiliser l'adresse IP source**.

Pour créer des services à l'aide de l'utilitaire de configuration

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis créez un service.

Pour créer un serveur virtuel d'équilibrage de charge et lier des services à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis créez un serveur virtuel.
2. Cliquez dans la section Service pour lier un service à ce serveur virtuel.

Cas d'utilisation 7 : Configurer l'équilibrage de charge en mode DSR à l'aide d'IP sur IP

May 5, 2023

Vous pouvez configurer une appliance NetScaler pour qu'elle utilise le mode DSR (Direct Server Return) sur les réseaux de couche 3 en utilisant le tunneling IP, également appelé configuration IP sur IP. Comme pour les configurations d'équilibrage de charge standard pour le mode DSR, cela permet aux serveurs de répondre directement aux clients au lieu d'utiliser un chemin de retour via l'appliance NetScaler. Cela améliore le temps de réponse et le débit. Comme pour le mode DSR standard, l'appliance NetScaler surveille les serveurs et effectue des contrôles de santé sur les ports de l'application.

Avec la configuration IP sur IP, l'appliance NetScaler et les serveurs n'ont pas besoin de se trouver sur le même sous-réseau de couche 2. Au lieu de cela, l'appliance NetScaler encapsule les paquets avant de les envoyer au serveur de destination. Une fois que le serveur de destination reçoit les paquets, il les décapsule, puis envoie ses réponses directement au client. C'est souvent ce que l'on appelle L3DSR.

Pour configurer le mode L3-DSR sur votre appliance NetScaler :

- Créez un serveur virtuel d'équilibragede charge. Définissez le mode sur IPTUNNEL et activez le suivi sans session.
- Créez des services. Créez un service pour chaque application principale et liez les services au serveur virtuel.
- Configurez pour la décapsulation. Configurez une appliance NetScaler ou un serveur principal pour qu'il fasse office de désencapsulateur.

  > Remarque :
  >
  > Lorsque vous utilisez une appliance NetScaler, la configuration de désencapsulation est un tunnel IP entre les appliances ADC, le back-end effectuant le L2DSR vers les serveurs réels.

Configurer un serveur virtuel d'équilibrage de charge

Configurez un serveur virtuel pour traiter les demandes adressées à vos applications. Attribuez le type de service correspondant au service ou utilisez un type de ANY pour plusieurs services.
Définissez la méthode de transfert sur IPTUNNEL et permettez au serveur virtuel de fonctionner en mode sans session. Configurez n'importe quelle méthode d'équilibrage de charge que vous souhaitez utiliser.

Pour créer et configurer un serveur virtuel d'équilibrage de charge pour DSR IP sur IP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour configurer un serveur virtuel d'équilibrage de charge pour DSR IP sur IP et vérifier la configuration :


```
add lb vserver <name> serviceType <serviceType> IPAddress <ip> Port <
    port> -lbMethod <method> -m <ipTunnelTag> -sessionless [ENABLED |
    DISABLED]

show lb vserver <name>
<!--NeedCopy-->
```

Exemple :

Dans l'exemple suivant, nous avons sélectionné la méthode d'équilibrage de charge en tant que SourceIphash et configuré l'équilibrage de charge sans session.

```
add lb vserver Vserver-LB-1 ANY 1.1.1.80 * -lbMethod SourceIPHash -m
    IPTUNNEL -sessionless ENABLED
<!--NeedCopy-->
```

Pour créer et configurer un serveur virtuel d'équilibrage de charge pour DSR IP sur IP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Créez un serveur virtuel et spécifiez le mode de redirection comme étant **basé sur le tunnel IP**.

Configurer les services pour le DSR IP sur IP

Après avoir créé votre serveur à charge équilibrée, configurez un service pour chacune de vos applications. Le service gère le trafic entre l'appliance NetScaler et ces applications et permet à l'appliance NetScaler de surveiller l'état de chaque application.

Affectez les services à utiliser le mode USIP et liez un moniteur de type IPTUNNEL au service pour une surveillance basée sur un tunnel.

Pour créer et configurer un service pour DSR IP sur IP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un service et éventuellement, créer un moniteur et le lier au service :

```
add service <serviceName> <serverName> <serviceType> <port> -usip <usip
    >

add monitor <monitorName> <monitorType> -destip <ip> -iptunnel <
    iptunnel>
```



```
4
5 bind service <serviceName> -monitorName <monitorName>
6 <!--NeedCopy-->
```

Exemple :

Dans l'exemple suivant, un moniteur de type IPTUNNEL est créé.

```
1 add monitor mon_DSR PING -destip 1.1.1.80 -iptunnel yes
2 add service svc_DSR01 2.2.2.100 ANY * -usip yes
3 bind service svc_DSR01 -monitorName mon_DSR
4 <!--NeedCopy-->
```

Une autre approche pour simplifier le routage au niveau du serveur et de l'appliance ADC consiste à configurer l'ADC et le serveur pour qu'ils utilisent une adresse IP provenant du même sous-réseau. Cela garantit que tout trafic ayant une destination d'un point de terminaison de tunnel est envoyé au-dessus du tunnel. Dans cet exemple, 10.0.1.0/30 est utilisé.

> **Remarque :**
>
> Le but du moniteur est de s'assurer que le tunnel est actif en atteignant le bouclage de chaque serveur via le tunnel IP. Si le service n'est pas en service, vérifiez si le routage IP externe entre ADC et le serveur est bon. Vérifiez également si les adresses IP internes sont accessibles via le tunnel IP. Des routes peuvent être requises sur le serveur, ou PBR est ajouté à ADC en fonction de l'implémentation choisie.

Exemple :

```
1 add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
2 add netProfile netProfile_DSR -srcIP 10.0.1.2
3 add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
     YES -netProfile netProfile_DSR
4 <!--NeedCopy-->
```

Pour configurer un moniteur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Créez un moniteur et sélectionnez **Tunnel IP**.

Pour créer et configurer un service pour DSR IP sur IP à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Créez un service et, dans l'onglet **Paramètres**, sélectionnez **Utiliser l'adresse IP source**.

Pour lier un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-DSR-1
<!--NeedCopy-->
```

Pour lier un service à un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et cliquez dans la section **Services** pour lier un service au serveur virtuel.

Utilisation de l'adresse IP du client dans l'en-tête externe des paquets de tunnel

NetScaler prend en charge l'utilisation de l'adresse IP client-source comme adresse IP source dans l'en-tête externe des paquets de tunnel liés au mode de retour direct du serveur à l'aide du tunneling IP. Cette fonctionnalité est prise en charge pour le DSR avec IPv4 et le DSR avec les modes de tunneling IPv6. Pour activer cette fonctionnalité, activez le paramètre **Utiliser l'adresse IP source du client** pour IPv4 ou IPv6. Ce paramètre est appliqué globalement à toutes les configurations DSR qui utilisent le tunneling IP.

Pour utiliser une adresse IP source client-source comme adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `set iptunnelparam -useclientsourceip [YES | NO]`
- `show iptunnelparam`

Pour utiliser l'adresse IP source du client comme adresse IP source à l'aide de l'interface graphique

1. Accédez à **Système > Réseau**.
2. Dans l'onglet **Paramètres**, cliquez sur **Paramètres globaux du tunnel IPv4**.

3. Dans la page **Configurer les paramètres globaux du tunnel IPv4**, activez la case à cocher **Utiliser l'adresse IP source du client** .
4. Cliquez sur **OK**.

Pour utiliser l'adresse IP source du client comme adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `set ip6tunnelparam -useclientsourceip [YES | NO]`
- `show ip6tunnelparam`

Pour utiliser l'adresse IP source du client comme adresse IP source à l'aide de l'interface graphique

1. Accédez à **Système > Réseau**.
2. Dans l'onglet **Paramètres**, cliquez sur **Paramètres globaux du tunnel IPv6**.
3. Dans la page **Configurer les paramètres globaux du tunnel IPv6**, activez la case à cocher **Utiliser l'adresse IP source du client** .
4. Cliquez sur **OK**.

Configuration de décapsulation

Vous pouvez configurer une appliance NetScaler ou un serveur principal en tant que désencapsulation.

Décapsulation de NetScaler

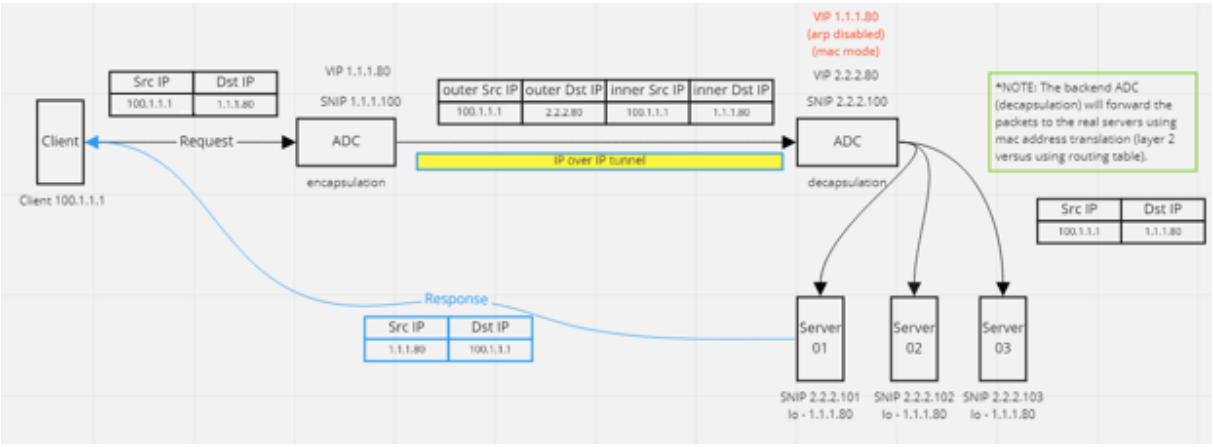
Lorsqu'une appliance NetScaler est utilisée comme désencapsulation, un tunnel IP doit être créé dans l'appliance NetScaler. Pour plus de détails, voir Configuration des tunnels IP.

La configuration de désencapsulation de NetScaler comprend les deux serveurs virtuels suivants :

- Le premier serveur virtuel reçoit le paquet encapsulé et supprime l'encapsulation IP externe.
- Le deuxième serveur virtuel dispose de l'adresse IP du service d'origine sur l'ADC frontal et utilise la traduction MAC pour transférer le paquet vers le serveur principal en utilisant l'adresse MAC des services liés. Cette configuration est généralement appelée L2DSR. Assurez-vous de désactiver ARP sur ce serveur virtuel.

Exemple de configuration :

L'illustration suivante montre une configuration de décapsulation à l'aide des appliances ADC.



La configuration complète requise pour la configuration est la suivante.

Configuration ADC frontale :

```
add service svc_DSR01 2.2.2.80 ANY * -usip YES -useproxyport NO
add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
    IPTUNNEL -sessionless ENABLED
bind lb vserver vip_DSR_ENCAP svc_DSR01
<!--NeedCopy-->
```

Configuration ADC back-end :

```
add ipTunnel DSR-IPIP 1.1.1.100 255.255.255.255 *

add service svc_DSR01_01 2.2.2.101 ANY * -usip YES -useproxyport NO
add service svc_DSR01_02 2.2.2.102 ANY * -usip YES -useproxyport NO
add service svc_DSR01_03 2.2.2.103 ANY * -usip YES -useproxyport NO

add lb vserver vs_DSR_DECAP ANY 2.2.2.80 * -lbMethod SOURCEIPHASH -m
    IPTUNNEL -sessionless ENABLED -netProfile netProf_DSR_MBF_noIP

add ns ip 1.1.1.80 255.255.255.255 -type VIP -arp DISABLED -snmp
    DISABLED
add lb vserver vs_DSR_Relay ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
    MAC -sessionless ENABLED

bind lb vserver vs_DSR_DECAP svc_DSR01_01
bind lb vserver vs_DSR_DECAP svc_DSR01_02
bind lb vserver vs_DSR_DECAP svc_DSR01_03

bind lb vserver vip_DSR_Relay svc_DSR01_01
bind lb vserver vip_DSR_Relay svc_DSR01_02
bind lb vserver vip_DSR_Relay svc_DSR01_03
```



```
19
20 add netProfile netProf_DSR_MBF_noIP -MBF ENABLED
21 add lb monitor mon_DSR_MAC PING -netProfile netProf_DSR_MBF_noIP
22 bind service svc_DSR01_01 -monitorName mon_DSR_MAC
23 bind service svc_DSR01_02 -monitorName mon_DSR_MAC
24 bind service svc_DSR01_03 -monitorName mon_DSR_MAC
25 <!--NeedCopy-->
```

L'exemple suivant montre une configuration de test utilisant Ubuntu et les serveurs Red Hat exécutant apache2. Ces commandes sont configurées sur chaque serveur principal.

```
1 sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
2 sudo sysctl net.ipv4.conf.all.arp_ignore=1
3 sudo sysctl net.ipv4.conf.all.arp_announce=2
4 sudo sysctl net.ipv4.conf.eth4.rp_filter=2 (The interface has the
     external IP with route towards the ADC)
5 sudo sysctl net.ipv4.conf.all.forwarding=1
6 sudo ip link set dev lo arp on
7 <!--NeedCopy-->
```

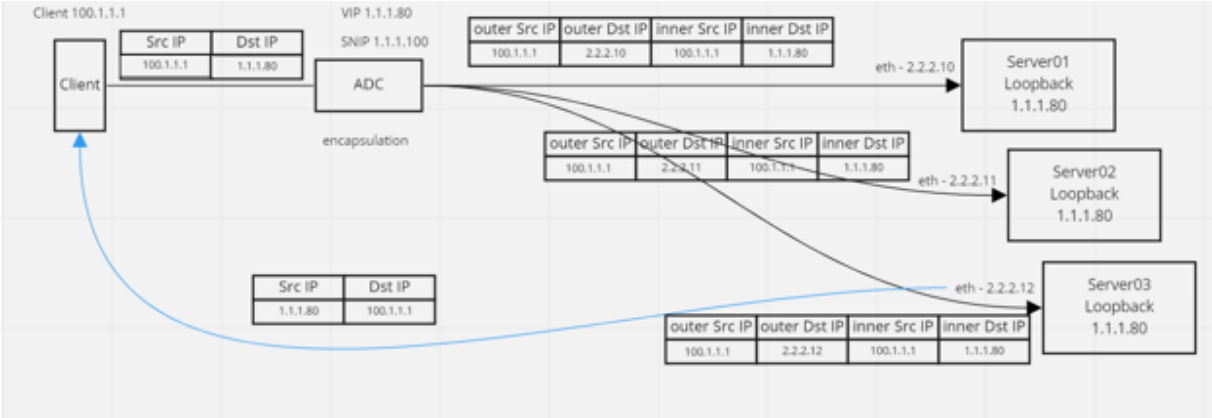
Décapsulation du serveur back-end

Lorsque vous utilisez les serveurs principaux comme décapsulation, la configuration principale varie en fonction du type de système d'exploitation du serveur. Vous pouvez configurer un serveur principal en tant que décapsulation en procédant comme suit :

1. Configurez une interface de boucle arrière avec IP pour IP de service.
2. Créez une interface de tunnel.
3. Ajouter un itinéraire via l'interface tunnel.
4. Configurez les paramètres d'interface nécessaires pour le trafic.

> Remarque :
>
> Les serveurs du système d'exploitation Windows ne peuvent pas effectuer de tunnels IP en mode natif. Les commandes sont donc fournies à titre d'exemple pour les systèmes Linux. Toutefois, les plug-ins tiers sont disponibles pour les serveurs Windows OS, ce qui ne relève pas du champ d'application de cet exemple.

L'illustration suivante montre une configuration de décapsulation à l'aide des serveurs principaux.



Exemple de configuration :

Dans cet exemple, 1.1.1.80 est l'adresse IP virtuelle (VIP) de NetScaler et 2.2.2.10-2.2.2.12 sont les adresses IP du serveur principal. L'adresse VIP est configurée dans l'interface de bouclage et un itinéraire est ajouté via l'interface du tunnel. Les moniteurs utilisent l'adresse IP du serveur et placent les paquets du moniteur sur le tunnel IP à l'aide des points de terminaison du tunnel.

La configuration complète requise pour la configuration est la suivante.

Configuration ADC frontale :

La configuration suivante crée un moniteur qui utilise le point de terminaison du tunnel comme source. Ensuite, envoyez des pings par tunnel à l'adresse IP du service.

```
1 add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
2 add netProfile netProfile_DSR -srcIP 10.0.1.2
3 add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
     YES -netProfile netProfile_DSR
4 <!--NeedCopy-->
```

La configuration suivante crée un service VIP pour service qui utilise l'adresse IP source d'origine. Ensuite, transfère le trafic via un tunnel IP vers les serveurs back-end.

```
1  add service svc_DSR01 2.2.2.10 ANY * -usip YES -useproxyport NO
2  bind service svc_DSR01 -monitorName mon_DSR
3
4  add service svc_DSR02 2.2.2.11 ANY * -usip YES -useproxyport NO
5  bind service svc_DSR02 -monitorName mon_DSR
6
7  add service svc_DSR03 2.2.2.12 ANY * -usip YES -useproxyport NO
8  bind service svc_DSR03 -monitorName mon_DSR
9
10 add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
     IPTUNNEL -sessionless ENABLED
11 bind lb vserver vip_DSR_ENCAP svc_DSR01
```



```
bind lb vserver vip_DSR_ENCAP svc_DSR02
bind lb vserver vip_DSR_ENCAP svc_DSR03
<!--NeedCopy-->
```

Configuration du serveur principal de chaque serveur :

Les commandes suivantes sont requises pour que le serveur principal reçoive le paquet IPIP, supprime l'encapsulation externe, puis réagisse depuis le bouclage à l'adresse IP du client d'origine. Cela garantit que les adresses IP du paquet reçu par le client correspondent aux adresses IP de la demande d'origine.

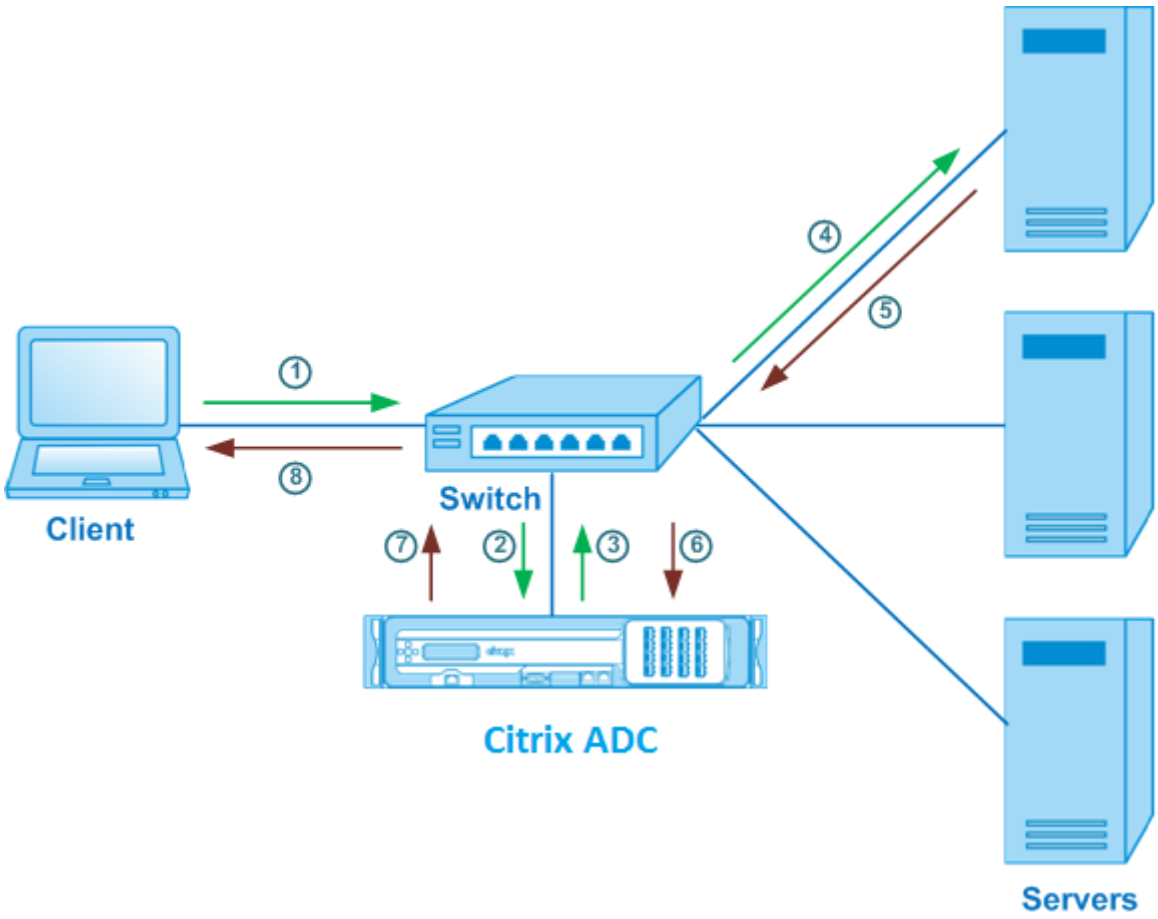
```
modprobe ipip
sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
nmcli connection add type ip-tunnel ip-tunnel.mode ipip con-name tun0
ifname tun0 remote 198.51.100.5 local 203.0.113.10
nmcli connection modify tun0 ipv4.addresses '10.0.1.1/30'
nmcli connection up tun0
sudo sysctl net.ipv4.conf.all.arp_ignore=1
sudo sysctl net.ipv4.conf.all.arp_announce=2
sudo sysctl net.ipv4.conf.tun0.rp_filter=2
sudo sysctl net.ipv4.conf.all.forwarding=1
sudo ip link set dev lo arp off
<!--NeedCopy-->
```

Cas d'utilisation 8 : Configurer l'équilibrage de charge en mode à un bras

May 5, 2023

Dans une configuration à bras unique, vous connectez l'appliance NetScaler au réseau via un seul VLAN. L'appliance reçoit la demande du client sur un seul VLAN et l'envoie au serveur sur le même VLAN. Il s'agit de l'un des scénarios de déploiement les plus simples, où le routeur, les serveurs et l'appliance sont tous connectés au même commutateur. Les demandes des clients au niveau du commutateur sont transférées à l'appliance, qui utilise la méthode d'équilibrage de charge configurée pour sélectionner le service.

Figure 1. Équilibrage de charge en mode à bras unique



Dans l'exemple de scénario, les services Service-ANY-1, Service-ANY-2 et Service-ANY-3 sont créés et liés au serveur virtuel Vserver-LB-1. Le serveur virtuel équilibre la charge de la demande du client vers un service. Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance en mode monobras.

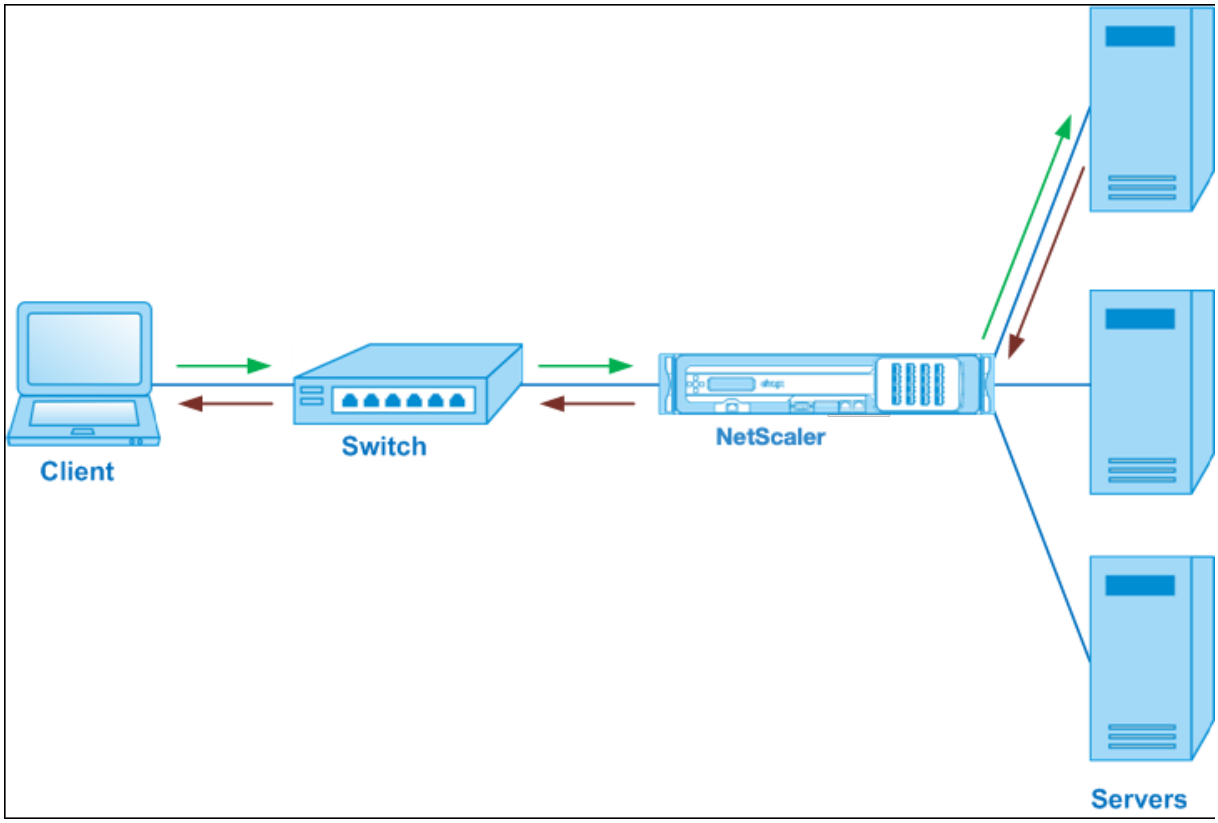
Type d'entité	Nom	Adresse IP	Protocole
Serveur virtuel	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY
	Service-ANY-3	10.102.29.93	ANY
Moniteurs	TCP	Aucun	Aucun

Pour configurer une configuration d'équilibrage de charge en mode à bras unique, reportez-vous à la section Configuration de l'équilibrage de charge de base.

Cas d'utilisation 9 : Configurer l'équilibrage de charge en mode en ligne

May 5, 2023

Dans une configuration en mode intégré (également appelé mode à deux bras), vous connectez l'appliance NetScaler au réseau via plusieurs VLAN. L'appliance reçoit la demande du client sur un VLAN et l'envoie au serveur sur un autre VLAN. Dans la configuration à deux bras, l'appliance est connectée entre les serveurs et le client. Les demandes des clients au niveau du commutateur sont transférées à l'appliance, qui utilise la méthode d'équilibrage de charge configurée pour sélectionner le service.



La configuration et le diagramme d'entités pour le mode en ligne sont les mêmes que ceux décrits dans Configuration de l'équilibrage de charge en mode à bras unique.

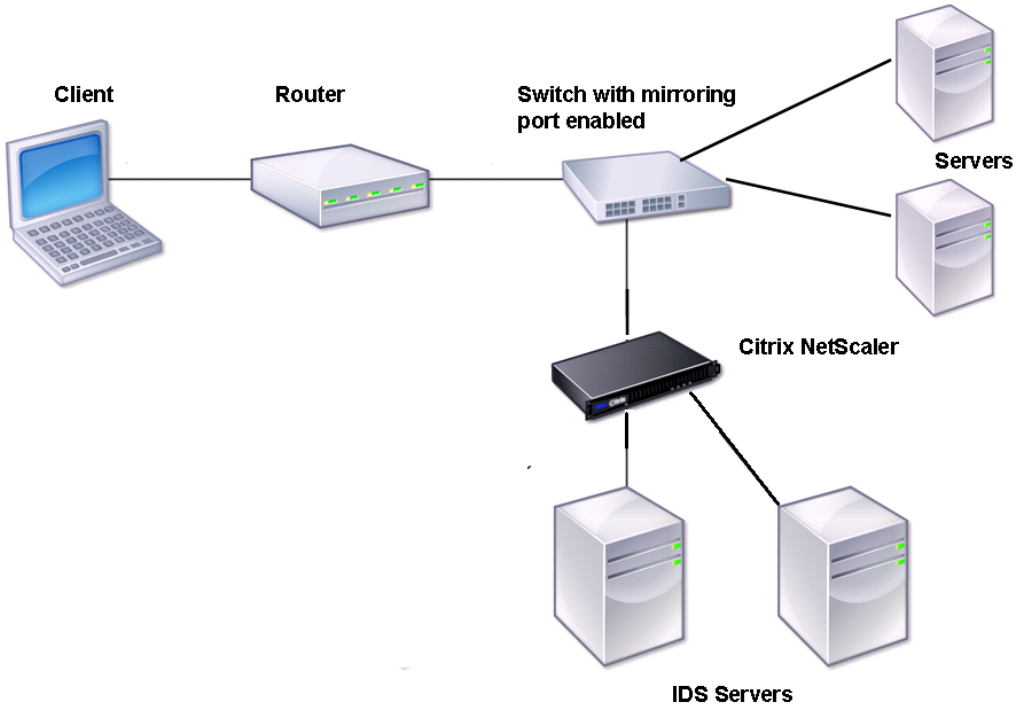
Cas d'utilisation 10 : Équilibrage de charge des serveurs de systèmes de détection d'intrusion

May 5, 2023

Pour permettre à l'appliance NetScaler de prendre en charge l'équilibrage de charge des serveurs du

système de détection des intrusions (IDS), les serveurs et les clients IDS doivent être connectés via un commutateur sur lequel la mise en miroir des ports est activée. Le client envoie une demande au serveur. La mise en miroir des ports étant activée sur le commutateur, les paquets de demande sont copiés ou envoyés vers le port du serveur virtuel de l'appliance NetScaler. L'appliance utilise ensuite la méthode d'équilibrage de charge configurée pour sélectionner un serveur IDS, comme indiqué dans le schéma suivant.

Figure 1. Topologie des serveurs IDS à charge équilibrée



Remarque : Actuellement, l'appliance prend en charge l'équilibrage de charge des périphériques IDS passifs uniquement.

Comme illustré dans le schéma précédent, la configuration de l'équilibrage de charge IDS fonctionne comme suit :

1. La demande du client est envoyée au serveur IDS et un commutateur doté d'un port miroir activé transmet ces paquets au serveur IDS. L'adresse IP source est l'adresse IP du client et l'adresse IP de destination est l'adresse IP du serveur. L'adresse MAC source est l'adresse MAC du routeur et l'adresse MAC de destination est l'adresse MAC du serveur.
2. Le trafic qui passe par le commutateur est reflété sur l'appliance. L'appliance utilise les informations de couche 3 (adresse IP source et adresse IP de destination) pour transférer le paquet

vers le serveur IDS sélectionné sans modifier l'adresse IP source ou l'adresse IP de destination. Il modifie l'adresse MAC source et l'adresse MAC de destination en fonction de l'adresse MAC du serveur IDS sélectionné.

Remarque : Lors de l'équilibrage de charge des serveurs IDS, vous pouvez configurer les méthodes d'équilibrage de charge SRCIPHASH, DESTIPHASH ou SRCIPDESTIPHASH. La méthode SRCIPDESTIPHASH est recommandée car les paquets provenant du client vers un service de l'appliance doivent être envoyés à un seul serveur IDS.

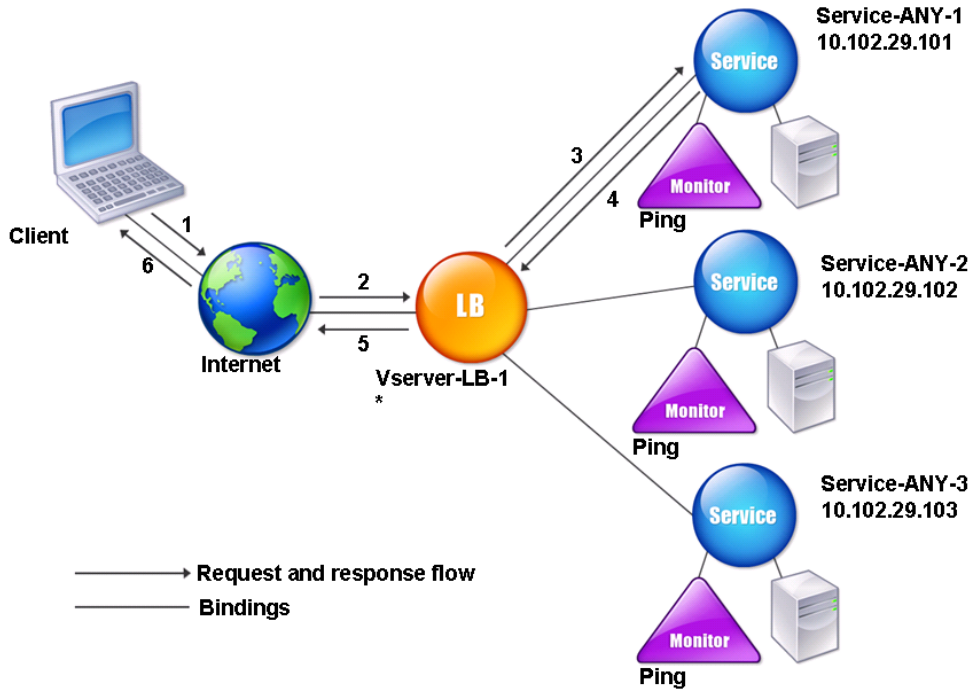
Supposons que Service-any-1, Service-any-2 et Service-any-3 soient créés et liés à vServer-LB-1. Le serveur virtuel équilibre la charge sur les services. Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance.

Type d'entité	Nom	Adresse IP	Port	Protocole
Serveur virtuel	Vserver-LB-1	*	*	ANY
Services	Service-ANY-1	10.102.29.101	*	ANY
	Service-ANY-2	10.102.29.102	*	ANY
	Service-ANY-3	10.102.29.103	*	ANY
Moniteurs	Ping	Aucun	Aucun	Aucun

Remarque : Vous pouvez utiliser le mode intégré ou le mode monobras pour une configuration d'équilibrage de charge IDS.

Le schéma suivant montre les entités d'équilibrage de charge et les valeurs des paramètres à configurer sur l'appliance.

Figure 2. Modèle d'entité pour les serveurs IDS d'équilibrage de charge



Pour configurer une configuration d'équilibrage de charge IDS, vous devez d'abord activer le transfert basé sur Mac. Désactivez également les modes de couche 2 et 3 sur l'appliance.

Pour activer le transfert basé sur Mac à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
enable ns mode <ConfigureMode>
<!--NeedCopy-->
```

Exemple :

```
enable ns mode MAC
<!--NeedCopy-->
```

Pour activer le transfert sur Mac à l'aide de l'utilitaire de configuration

Accédez à **Système > Paramètres > Configurer les modes**, puis sélectionnez **Transfert basé sur MAC**.

Ensuite, reportez-vous à la section « Configuration de l'équilibrage de chargede base » pour configurer une configuration d'équilibrage de charge de base.

Après avoir configuré la configuration d'équilibrage de charge de base, vous devez la personnaliser pour IDS en configurant une méthode d'équilibrage de charge prise en charge (telle que la méthode de hachage SRCIPDESTIP sur un serveur virtuel sans session) et en activant le mode MAC. L'appliance ne conserve pas l'état de la connexion et transmet uniquement les paquets aux serveurs IDS sans les traiter. L'adresse IP et le port de destination restent inchangés car le serveur virtuel est en mode MAC.

Pour configurer une méthode d'équilibrage de charge et un mode de redirection pour un serveur virtuel sans session à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
   RedirectionMode> -sessionless <Value>
<!--NeedCopy-->
```

Exemple :

```
set lb vserver Vserver-LB-1 -lbMethod SourceIPDestIPHash -m MAC -
   sessionless enabled
<!--NeedCopy-->
```

> **Remarque**
>
> Pour un service lié à un serveur virtuel sur lequel l'option -m MAC est activée, vous devez lier un moniteur non utilisateur.

Pour configurer une méthode d'équilibrage de charge et un mode de redirection pour un serveur virtuel sans session à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et, en mode de redirection, sélectionnez Basé sur MAC.
3. Dans Paramètres avancés, cliquez sur Méthodes, puis sélectionnez SRCIPDESTIPHASH. Cliquez sur Paramètres de trafic, puis sélectionnez Équilibrage de charge sans session.

Pour définir un service pour utiliser l'adresse IP source à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set service <ServiceName> -usip <Value>
```



```
<!--NeedCopy-->
```

Exemple :

```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```

Pour définir un service pour utiliser l'adresse IP source à l'aide de l'utilitaire de configuration

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
2. Ouvrez un service et, dans Paramètres, sélectionnez **Utiliser l'adresse IP source**.

Pour que USIP fonctionne correctement, vous devez le définir globalement. Pour plus d'informations sur la configuration globale d'USIP, consultez Addressage IP.

Cas d'utilisation 11 : Isolation du trafic réseau à l'aide de stratégies d'écoute

May 5, 2023

> **Remarque**
>
> La solution d'isolation du trafic utilisant des serveurs virtuels fictifs pour simuler l'isolation de plusieurs locataires n'est plus recommandée. Citrix vous recommande également d'utiliser la fonctionnalité NetScaler Admin Partitioning pour de tels déploiements. Pour plus d'informations, voir Partitionnement administrateur.

Une exigence de sécurité courante dans un centre de données consiste à maintenir l'isolement du chemin réseau entre le trafic de diverses applications ou locataires. Le trafic d'une application ou d'un locataire doit être isolé du trafic des autres applications ou locataires. Par exemple, une société de services financiers souhaiterait séparer le trafic des applications de son département des assurances de celui de ses applications de services financiers. Dans le passé, cela était facilement réalisable grâce à la séparation physique des dispositifs de service réseau tels que les pare-feux, les équilibreurs de charge et les IdP, ainsi qu'à la surveillance du réseau et à la séparation logique au sein de la structure de commutation.

À mesure que les architectures des centres de données évoluent vers des centres de données virtualisés multilocataires, les services réseau de la couche d'agrégation d'un centre de données sont consolidés. Cette évolution a fait de l'isolation des chemins réseau un élément essentiel pour les disposi-

tifs de service réseau et impose aux ADC de pouvoir isoler le trafic aux niveaux L4 à L7. En outre, tout le trafic d'un locataire particulier doit passer par un pare-feu avant d'atteindre la couche de service.

Pour répondre à l'exigence d'isolation des chemins réseau, une appliance NetScaler identifie les domaines du réseau et contrôle le trafic entre les domaines. La solution NetScaler comporte deux composants principaux : les politiques d'écoute et les serveurs virtuels fantômes.

Chaque chemin réseau à isoler se voit attribuer un serveur virtuel sur lequel une politique d'écoute est définie afin que le serveur virtuel écoute uniquement le trafic provenant d'un domaine réseau spécifié.

Pour isoler le trafic, les politiques d'écoute peuvent être basées sur plusieurs paramètres du client ou sur leurs combinaisons, et des priorités peuvent être attribuées aux politiques. Le tableau suivant répertorie les paramètres qui peuvent être utilisés dans les politiques d'écoute pour identifier le trafic.

Catégorie	Paramètres
Protocole Ethernet	Adresse MAC source, adresse MAC de destination
Interface réseau	ID réseau, débit de réception, débit d'envoi, débit de transmission
Protocole IP	Adresse IP source, adresse IP de destination
Protocole IPv6	Adresse IPv6 source, adresse IPv6 de destination
Protocole TCP	Port source, port de destination, taille maximale du segment, charge utile et autres options
Protocole UDP	Port source, port de destination
VLAN	ID

Tableau 1. Paramètres du client utilisés pour définir les politiques d'écoute

Sur l'appliance NetScaler, un serveur virtuel est configuré pour chaque domaine, avec une politique d'écoute spécifiant que le serveur virtuel doit écouter uniquement le trafic pour ce domaine. Un serveur virtuel d'équilibrage de charge parallèle, qui écoute le trafic destiné à n'importe quel domaine, est également configuré pour chaque domaine. Chacun des serveurs virtuels d'équilibrage de charge parallèle possède une adresse IP et un port génériques (*), et son type de service est défini sur ANY.

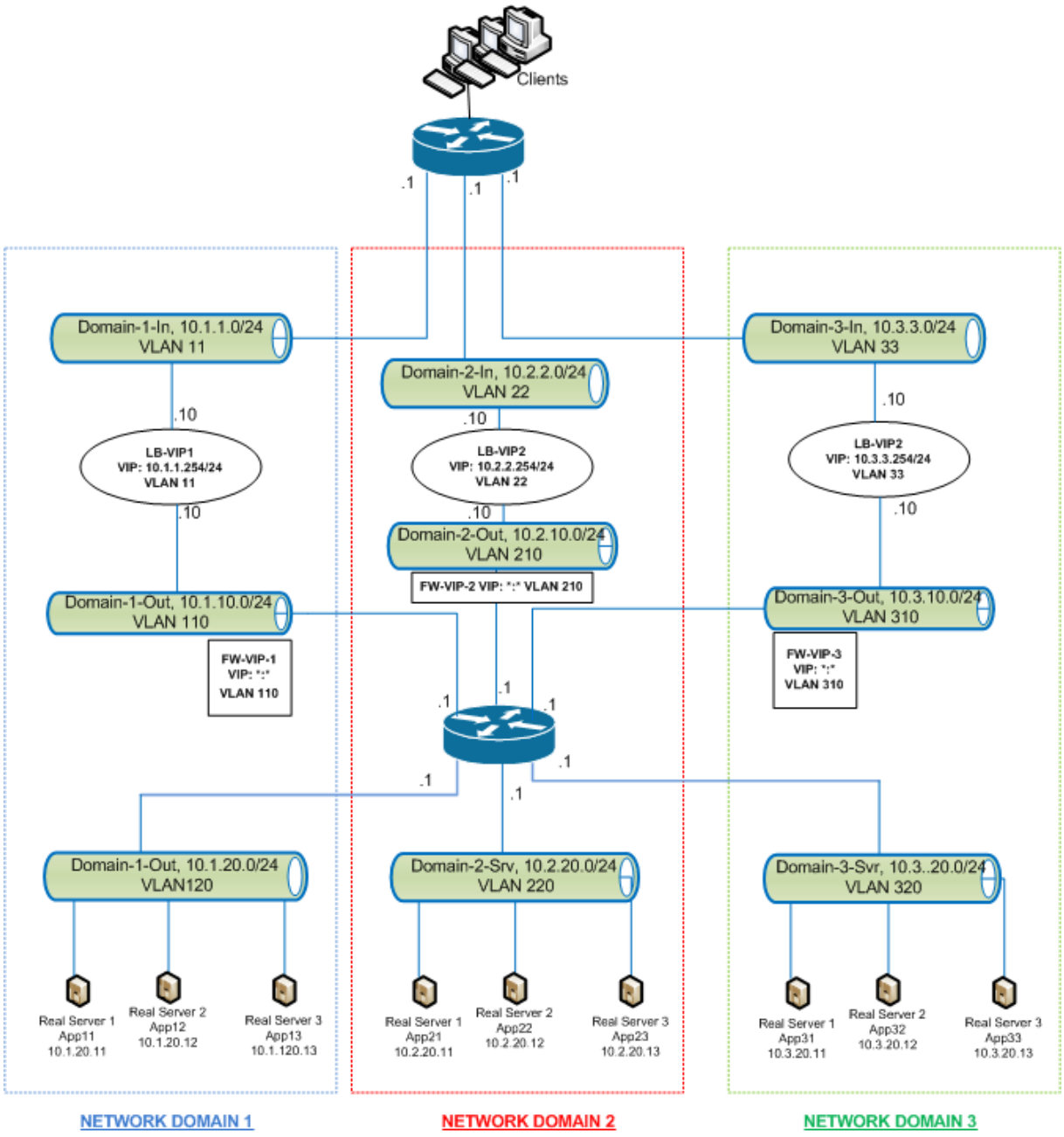
Dans chaque domaine, un pare-feu pour le domaine est lié en tant que service au serveur virtuel d'équilibrage de charge parallèle, qui transmet tout le trafic via le pare-feu. Le trafic local est trans-

féré vers sa destination et le trafic destiné à un autre domaine est transféré vers le pare-feu de ce domaine. Les serveurs virtuels d'équilibrage de charge parallèle sont configurés pour la redirection en mode MAC.

Comment les chemins réseau sont isolés

La figure suivante montre un flux de trafic typique entre les domaines. Examinez le flux de trafic au sein du domaine réseau 1 et entre le domaine réseau 1 et le domaine réseau 2.

Figure 1. Isolation du chemin réseau



Trafic au sein du domaine réseau 1

Le domaine réseau 1 possède trois VLAN : VLAN 11, VLAN110 et VLAN120. Les étapes suivantes décrivent le flux de trafic.

- Un client du VLAN 11 envoie une demande pour un service disponible à partir du pool de services du VLAN 120.
- Le serveur virtuel d'équilibrage de charge LB-VIP1, qui est configuré pour écouter le trafic provenant du VLAN 11, reçoit la demande et la transmet au VLAN 110. Le serveur virtuel du VLAN 110 transmet la demande au serveur virtuel d'équilibrage de charge parallèle FW-VIP-1.
- Le FW-VIP-1, qui est configuré pour écouter le trafic provenant du VLAN 110, reçoit la demande et la transmet au VLAN 120.
- Le serveur virtuel d'équilibrage de charge du VLAN 120 équilibre la charge de la demande vers l'un des serveurs physiques, App11, App12 ou App13.
- La réponse envoyée par le serveur physique est renvoyée par le même chemin vers le client dans le VLAN 11.

Cette configuration garantit que le trafic est toujours séparé au sein de NetScaler pour tout le trafic provenant d'un client.

Trafic entre le domaine réseau 1 et le domaine réseau 2

Le domaine réseau 1 possède trois VLAN : VLAN 11, VLAN110 et VLAN120. Le domaine réseau 2 possède également trois VLAN : VLAN 22, VLAN 210 et VLAN 220. Les étapes suivantes décrivent le flux de trafic entre le VALN 11 et le VLAN 22.

- Un client du VLAN 11, qui appartient au domaine réseau 1, envoie une demande pour un service disponible à partir du pool de services du VLAN 220, qui appartient au domaine réseau 2.
- Dans le domaine réseau 1, le serveur virtuel d'équilibrage de charge LB-VIP1, qui est configuré pour écouter le trafic provenant du VLAN 11, reçoit la demande et la transmet au VLAN 110.
- Le serveur virtuel d'équilibrage de charge parallèle FW-VIP-1, qui est configuré pour écouter le trafic VLAN 110 destiné à tout autre domaine, reçoit la demande et la transmet au serveur virtuel de pare-feu FW-VIP-2 car la demande est destinée à un serveur physique du domaine réseau 2.
- Dans le domaine réseau 2, FW-VIP-2 transmet la demande au VLAN 220.
- Le serveur virtuel d'équilibrage de charge du VLAN 220 équilibre la charge de la demande vers l'un des serveurs physiques, App21, App22 ou App23.
- La réponse envoyée par le serveur physique revient par le même chemin à travers le pare-feu du domaine réseau 2, puis au domaine réseau 1 pour atteindre le client dans le VLAN 11.

Étapes de configuration

Pour configurer l'isolation des chemins réseau à l'aide de politiques d'écoute, procédez comme suit :

- Ajoutez des expressions de politique d'écoute. Chaque expression spécifie un domaine auquel le trafic est destiné. Vous pouvez utiliser l'ID du VLAN ou d'autres paramètres pour identifier le trafic.
- Pour chaque domaine réseau, configurez deux serveurs virtuels comme suit :
  - Créez un serveur virtuel d'équilibrage de charge pour lequel vous spécifiez une stratégie d'écoute qui identifie le trafic destiné à ce domaine. Vous pouvez spécifier le nom d'une expression créée précédemment ou vous pouvez créer une expression lors de la création du serveur virtuel.
  - Créez un autre serveur virtuel d'équilibrage de charge, appelé serveur virtuel instantané, pour lequel vous spécifiez une expression de stratégie d'écoute qui s'applique au trafic destiné à n'importe quel domaine. Sur ce serveur virtuel, définissez le type de service sur ANY et l'adresse IP et le port sur un astérisque (*). Activez le transfert basé sur Mac sur ce serveur virtuel.
  - Activez l'option de connexion L2 sur les deux serveurs virtuels.
    Généralement, pour identifier une connexion, l'appliance NetScaler utilise les quatre tuples suivants : adresse IP du client, port client, adresse IP de destination et port de destination. Lorsque vous activez l'option Connexion L2, les paramètres de couche 2 de la connexion (numéro de canal, adresse MAC et ID VLAN) sont utilisés en plus du 4-tuple normal.
- Ajoutez des services représentant les pools de serveurs dans le domaine et liez-les au serveur virtuel.
- Configurez le pare-feu pour chaque domaine en tant que service et liez tous les services de pare-feu au serveur virtuel Shadow.

Pour isoler le trafic réseau à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
add policy expression <expressionName> <listenPolicyExpression>

add lb vserver <name> <serviceType> <ip> <port> -l2conn ON -
   listenPolicy <expressionName>
<!--NeedCopy-->
```

Ajoutez un serveur virtuel d'équilibrage de charge pour chaque domaine. Ce serveur virtuel est destiné au trafic du même domaine.

```
add lb vserver <name> ANY * * -l2conn ON -m MAC -listenPolicy <
   expressionName>
<!--NeedCopy-->
```


Ajoutez un serveur virtuel d'équilibrage de charge parallèle pour chaque domaine. Ce serveur virtuel est destiné au trafic d'autres domaines.

Exemple :

```
add policy expression e110 client.vlan.id==110
add policy expression e210 client.vlan.id==210
add policy expression e310 client.vlan.id==310
add policy expression e11 client.vlan.id==11
add policy expression e22 client.vlan.id==22
add policy expression e33 client.vlan.id==33

add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -persistenceType NONE -
    listenPolicy e11
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP2 HTTP 10.2.2.254 80 -persistenceType NONE -
    listenPolicy e22
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP3 HTTP 10.3.3.254 80 -persistenceType NONE -
    listenPolicy e33
-cltTimeout 180 -l2Conn ON


add lb vserver FW-VIP-1 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e110 -Listenpriority 1 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-2 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e210 -Listenpriority 2 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-3 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e310 -Listenpriority 3 -m MAC -cltTimeout
    120


add service RD-1 10.1.1.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO

add service RD-2 10.2.2.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
```



```
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO

add service RD-3 10.3.3.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO


bind lb vserver FW-VIP-1 RD-1

bind lb vserver FW-VIP-2 RD-2

bind lb vserver FW-VIP-3 RD-3
<!--NeedCopy-->
```

Pour isoler le trafic réseau à l'aide de l'utilitaire de configuration

1. Ajoutez des services représentant les serveurs, comme décrit dans la section Création d'un service.
2. Ajoutez chaque pare-feu en tant que service :
   a) Accédez à **Traffic Management > Load Balancing > Services**.
   b) Créez un service en spécifiant le protocole comme ANY, le serveur comme adresse IP du pare-feu et le port comme 80.
3. Configurez un serveur virtuel d'équilibrage de charge.
4. Configurez le serveur virtuel d'équilibrage de charge parallèle.
5. Pour chaque domaine du réseau, répétez les étapes 3 et 4.
6. Dans le volet Serveurs virtuels d'équilibrage de charge, ouvrez les serveurs virtuels que vous avez créés et vérifiez les paramètres.

Cas d'utilisation 12 : configurer Citrix Virtual Desktops pour l'équilibrage de charge

May 5, 2023

Pour améliorer les performances lors de la mise à disposition d'applications de bureau virtuel, vous pouvez intégrer l'appliance NetScaler à Citrix Virtual Desktops et utiliser la fonctionnalité d'équilibrage de charge de NetScaler pour répartir la charge sur les serveurs Desktop Delivery Controller (DDC).

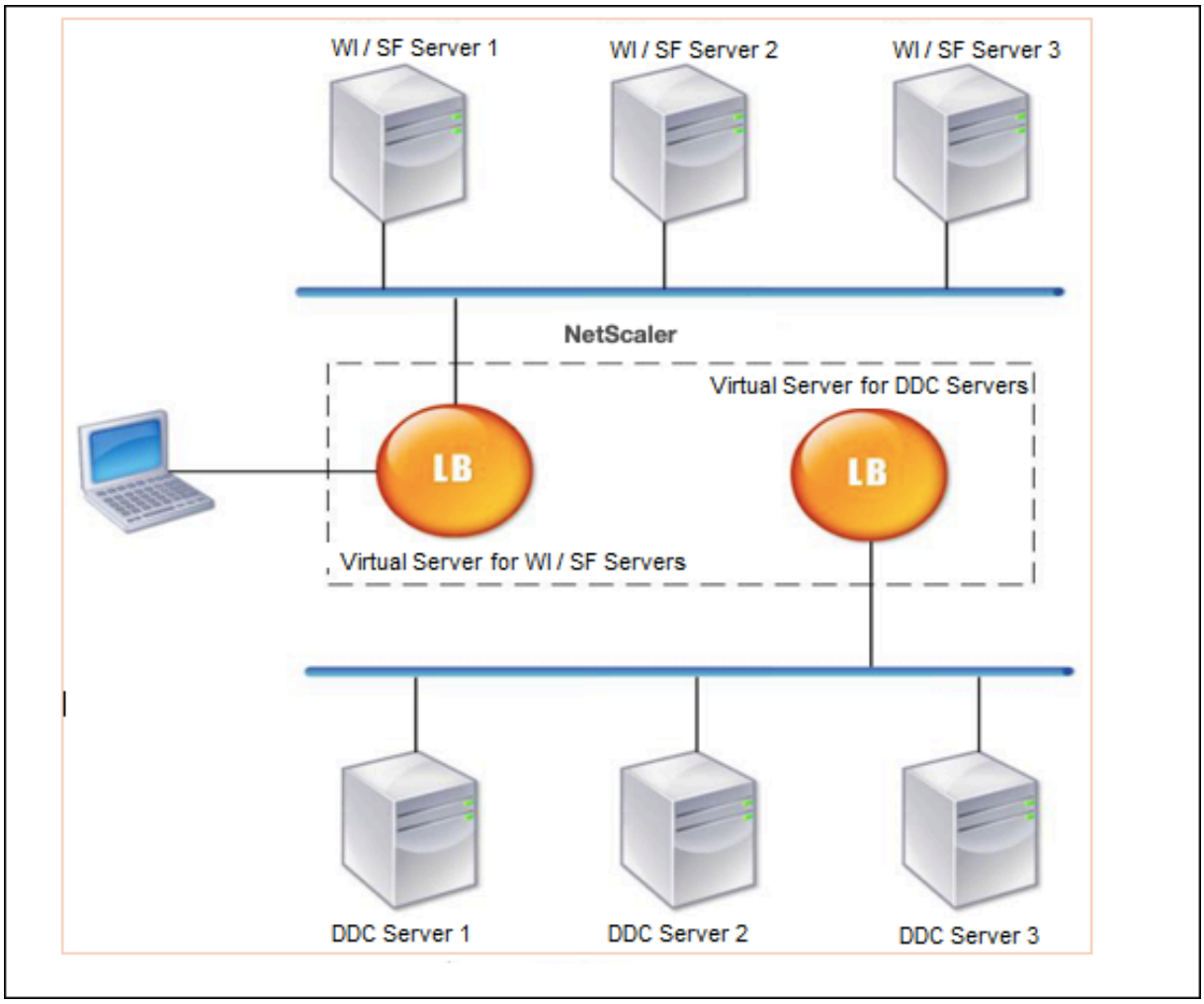
En général, vous utilisez Citrix Virtual Desktops dans les situations où les applications ne sont pas compatibles avec l'exécution sur un serveur de terminaux ou des applications virtuelles, ou si chaque bureau virtuel a des exigences uniques. Dans ce cas, vous avez besoin d'un hôte de bureau pour chaque utilisateur qui se connecte. Toutefois, les hôtes peuvent être regroupés afin que vous n'ayez besoin que d'un seul hôte pour chaque utilisateur actuellement connecté.

Le principal service d'application déployé pour Citrix Virtual Desktops est le Desktop Delivery Controller (DDC). Le DDC est installé sur un serveur et sa fonction principale consiste à enregistrer les hôtes de bureau et à négocier les connexions des clients avec eux.

Le DDC authentifie également les utilisateurs et gère l'assemblage des environnements de bureau virtuels des utilisateurs en contrôlant l'état des postes de travail, ainsi qu'en démarrant et en arrêtant les postes de travail.

En général, plusieurs DDC sont installés pour améliorer la disponibilité.

La figure suivante montre la topologie d'une appliance NetScaler fonctionnant avec Citrix Virtual Desktops.



> **Remarque :**
>
> Bien que vous puissiez utiliser le protocole HTTP, nous vous recommandons d'utiliser le protocole SSL pour la communication entre le client et l'appliance NetScaler. Vous pouvez utiliser le protocole HTTP pour communiquer entre NetScaler et les serveurs DDC même si vous utilisez le protocole SSL pour communiquer avec le client.

Pour configurer l'équilibrage de charge pour Citrix Virtual Desktops à l'aide de l'interface graphique

1. Créez un service.
   a) Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
   b) Créez un service en spécifiant un nom, une adresse IP, un port et un type de protocole, puis cliquez sur **OK**.
2. Créez un serveur virtuel d'équilibrage de charge.
   a) Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et cliquez sur **Ajouter**.
   b) Créez un serveur virtuel en spécifiant un nom, une adresse IP, un port et un type de protocole, puis cliquez sur **OK**.
3. Liez le service au serveur virtuel d'équilibrage de charge.
4. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et sélectionnez un serveur.
   a) Cliquez sur **Modifier**.
   b) Dans les **Services et groupes de services**, cliquez sur ** puis sur **Ajouter une liaison**.
   c) Sélectionnez le service que vous souhaitez lier et entrez la valeur de pondération.
   d) Cliquez sur **Bind**.

Pour configurer l'équilibrage de charge pour Citrix Virtual Desktops à l'aide de l'interface de ligne de commande

- Pour créer un service, à l'invite de commande, tapez :

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```


- Pour créer un serveur virtuel, à l'invite de commande, tapez :

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```

Exemple :

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80

- Pour lier un service à un serveur virtuel d'équilibrage de charge, à l'invite de commande, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

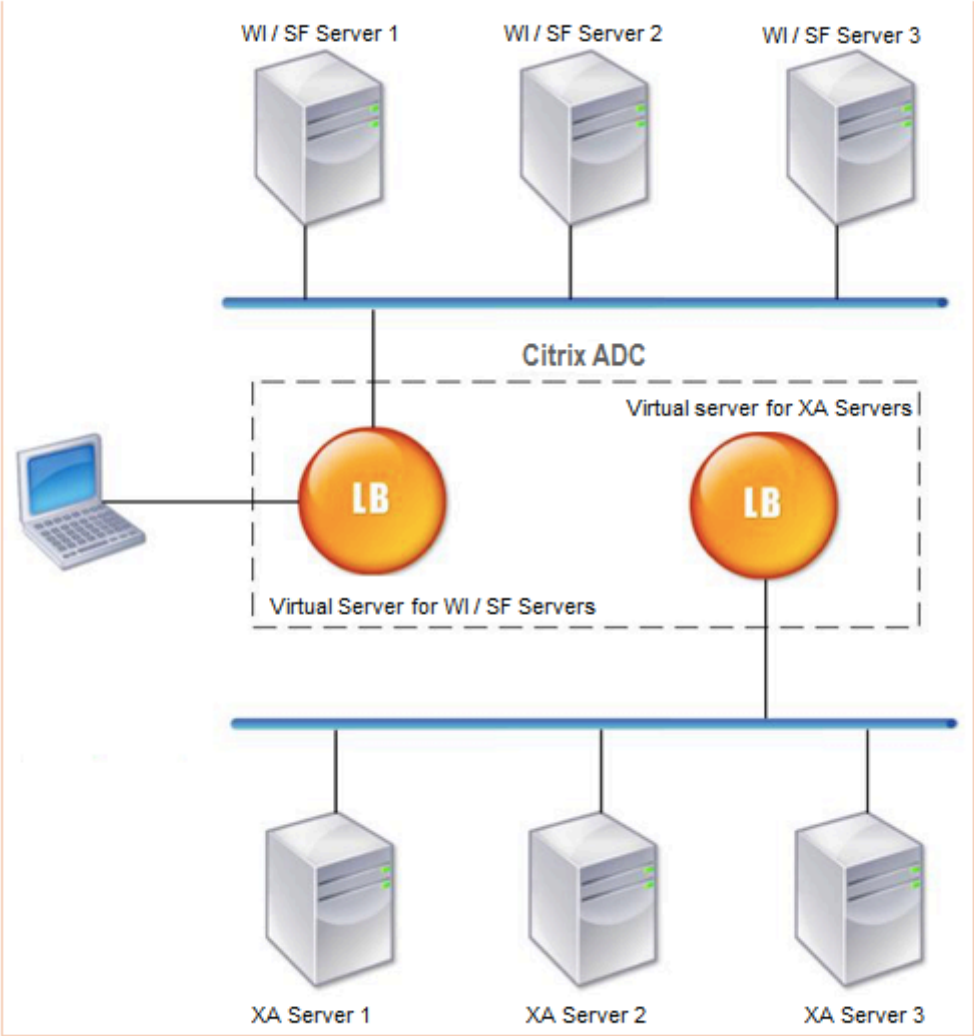
Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Cas d'utilisation 13 : Configuration de Citrix Virtual Apps pour l'équilibrage de charge

May 5, 2023

Pour une mise à disposition efficace des applications, vous pouvez intégrer l'appliance NetScaler à Citrix Virtual Apps et utiliser la fonctionnalité d'équilibrage de charge de NetScaler pour répartir la charge entre les batteries de serveurs Citrix Virtual Apps. La figure suivante est un diagramme topologique d'une telle configuration.



Les serveurs d'interface Web fournissent un accès sécurisé aux ressources de l'application Citrix Virtual Apps via le navigateur Web de l'utilisateur. Le client d'interface Web présente aux utilisateurs toutes les ressources, telles que les applications, le contenu et les bureaux, mises à disposition dans les batteries de serveurs Citrix Virtual Apps. Les utilisateurs peuvent accéder aux ressources publiées via un navigateur Web standard ou via le plug-in en ligne Citrix.

Le navigateur Web de l'appareil de l'utilisateur envoie des informations au serveur Web, qui communique avec les serveurs de la batterie de serveurs pour permettre à l'utilisateur d'accéder aux ressources.

L'interface Web et le broker XML sont des services complémentaires. L'interface Web permet aux utilisateurs d'accéder aux applications, et le broker XML évalue les autorisations de l'utilisateur afin de déterminer quelles applications apparaissent dans l'interface Web.

Le service XML est installé sur tous les serveurs de la batterie de serveurs. Le service XML spécifié dans l'interface Web fonctionne en tant que broker XML. Sur la base des informations d'identification de l'utilisateur transmises par le serveur d'interface Web, le serveur XML Broker envoie une liste d'applications accessibles à l'utilisateur.

Dans les grandes entreprises où plusieurs serveurs d'interface Web et serveurs XML Broker sont déployés, Citrix recommande d'équilibrer la charge de ces serveurs à l'aide de l'appliance NetScaler. Configurez un serveur virtuel pour équilibrer la charge des serveurs de l'interface Web et un autre pour les serveurs XML Broker. La méthode d'équilibrage de charge et d'autres fonctionnalités peuvent être configurées sur le serveur virtuel si nécessaire.

> **Remarque**
>
> Bien que vous puissiez utiliser le protocole HTTP, Citrix vous recommande d'utiliser le protocole SSL pour la communication entre le client et NetScaler. Vous pouvez utiliser le protocole HTTP pour la communication entre NetScaler et les serveurs WI même si vous utilisez le protocole SSL pour communiquer avec le client.

Pour configurer l'équilibrage de charge pour Citrix Virtual Apps à l'aide de l'interface graphique

1. Créez un service.
   a) Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
   b) Créez un service en spécifiant un nom, une adresse IP, un port et un type de protocole, puis cliquez sur **OK**.
2. Créez un serveur virtuel d'équilibrage de charge.
   a) Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et cliquez sur **Ajouter**.
   b) Créez un serveur virtuel en spécifiant un nom, une adresse IP, un port et un type de protocole, puis cliquez sur **OK**.
3. Liez le service au serveur virtuel d'équilibrage de charge.
4. Accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et sélectionnez un serveur.
   a) Cliquez sur **Modifier**.
   b) Dans les **Services et groupes de services**, cliquez sur **** puis sur **Ajouter une liaison**.
   c) Sélectionnez le service que vous souhaitez lier et entrez la valeur de pondération.
   d) Cliquez sur **Bind**.

Pour configurer l'équilibrage de charge pour Citrix Virtual Apps à l'aide de l'interface de ligne de commande

- Pour créer un service, à l'invite de commande, tapez :

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

- Pour créer un serveur virtuel, à l'invite de commande, tapez :

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

- Pour lier un service à un serveur virtuel d'équilibrage de charge, à l'invite de commande, tapez :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Cas d'utilisation 14 : Assistant ShareFile pour l'équilibrage de charge Citrix ShareFile

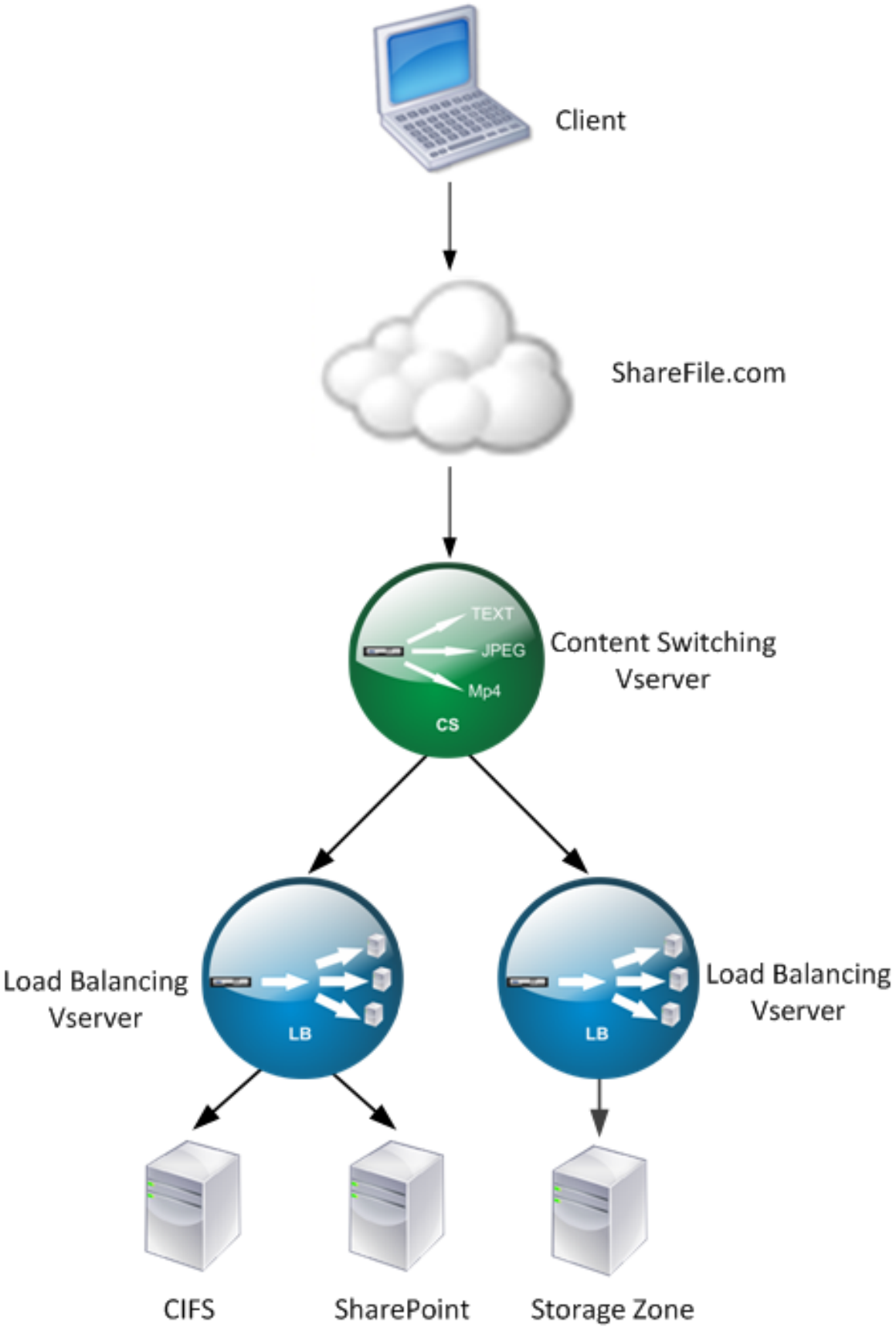
May 5, 2023

Vous pouvez configurer l'équilibrage de charge pour Citrix ShareFile à l'aide de l'assistant. L'assistant Citrix ShareFile aide à configurer la configuration d'équilibrage de charge pour le site ShareFile en fonction du type de contenu demandé. Le serveur de commutation de contenu dirige la demande selon qu'il s'agit d'une requête StorageZone, CIFS ou SharePoint. Le changement de contenu est basé

sur des politiques. L'assistant génère automatiquement les politiques permettant d'identifier si la demande concerne StorageZone, CIFS ou SharePoint. Le serveur virtuel de commutation de contenu utilise ces politiques pour diriger la demande vers le serveur d'équilibrage de charge approprié.

Un flux de données typique peut être décrit comme le montre le schéma suivant.

Figure 1. Équilibrage de la charge de données ShareFile

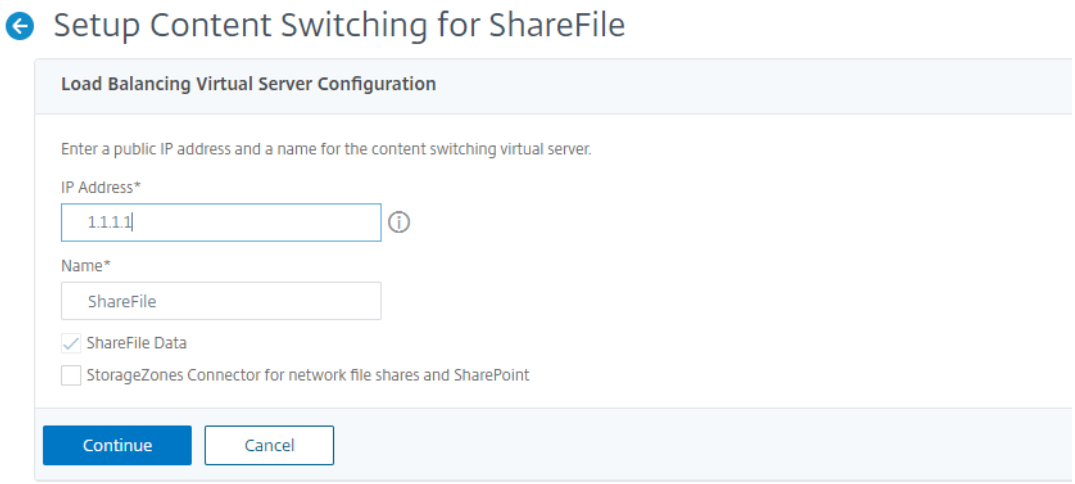


Vous pouvez consulter les serveurs virtuels d'équilibrage de charge créés par l'assistant ShareFile en accédant à **Gestion du trafic > Serveurs et services virtuels> Serveurs virtuels**. Vous ne pouvez pas supprimer manuellement les serveurs virtuels créés à l'aide de l'assistant ShareFile. Utilisez l'assistant pour supprimer les serveurs virtuels.

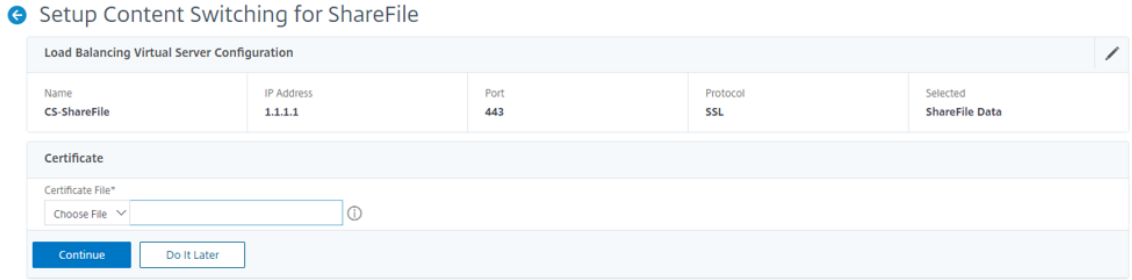
NetScaler utilise l'authentification LDAP pour SharePoint ou la requête CIFS. L'authentification par hachage est utilisée pour authentifier les demandes pour StorageZones.

Pour configurer une appliance NetScaler pour l'équilibrage de charge | Citrix ShareFile

1. Dans le volet de navigation, cliquez sur **Gestion du trafic**.
2. Dans la section **Citrix ShareFile**, cliquez sur **Configurer NetScaler**pour ShareFile.
3. Sur la page **Configuration du changement de contenu pour ShareFile**, fournissez les informations suivantes :
   - Adresse IP : adresse IP du serveur virtuel de commutation de contenu.
   - Nom : nom du serveur virtuel de commutation de contenu.
   - Si vous souhaitez configurer l'équilibrage de charge pour CIFS ou SharePoint, activez la case à cocher **StorageZone Connector for Network File Share/SharePoint**, puis cliquez sur **Continuer**. Par défaut, la case à cocher **ShareFile Data** est activée.

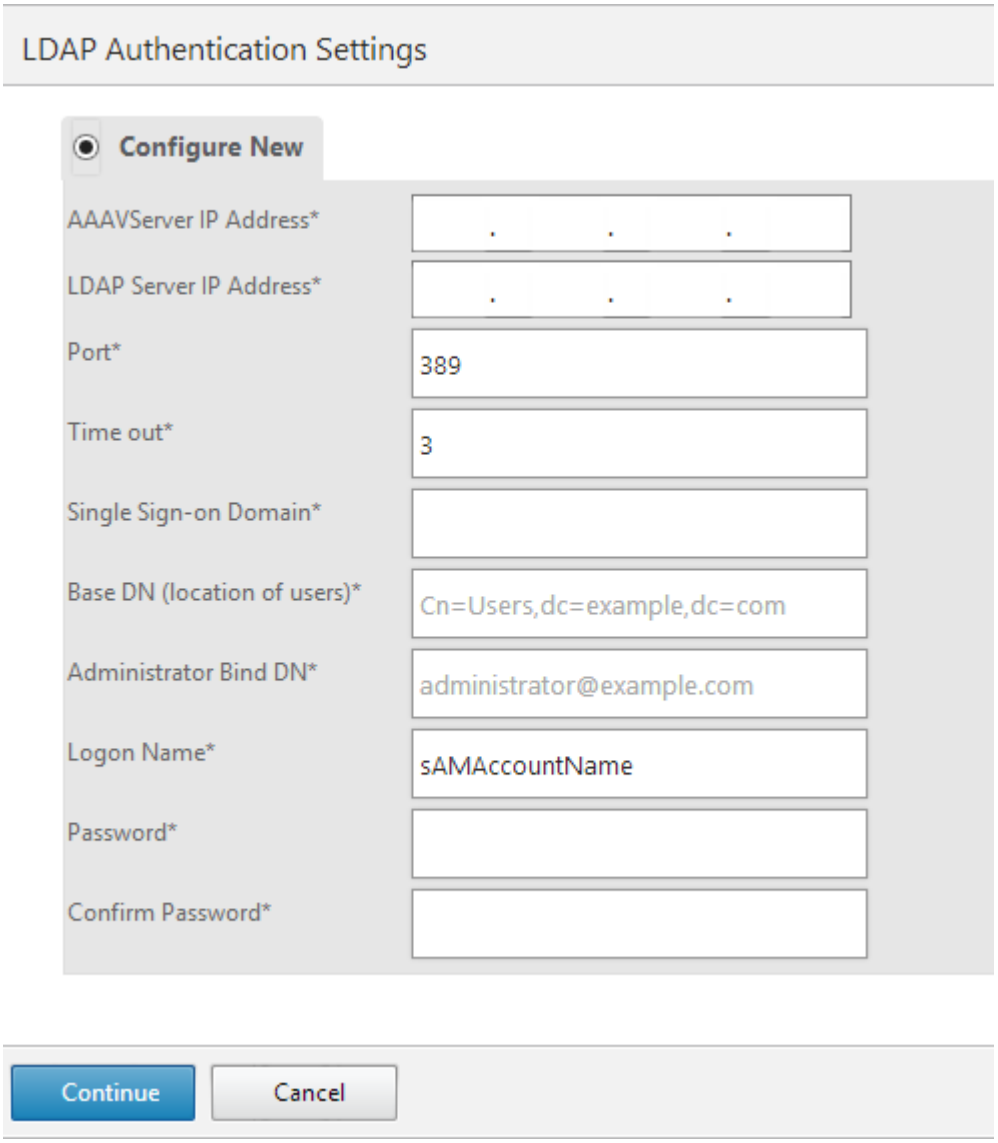


4. Fournissez un certificat valide. Si vous possédez un certificat, cliquez sur **Choisir un certificat** et sélectionnez le certificat dans la liste déroulante. Si vous devez installer un certificat, cliquez sur **Installer le certificat** et fournissez la paire de clés de certificat.



5. Cliquez sur **Continuer**.
6. Dans la boîte de dialogue **Ajouter un nouveau contrôleur StorageZone**, spécifiez les valeurs des paramètres suivants :
    - Adresse IP du StorageZone Controller : adresse IP
    - Port : numéro de port. La valeur par défaut est 443.
    - Protocole : sélectionnez la

7. Cliquez sur **Créer**, puis sur **Terminé**. L'assistant crée automatiquement un service et génère automatiquement le nom du service.
8. Si vous avez choisi l'équilibrage de charge pour CIFS ou SharePoint à l'étape 4.c, spécifiez les valeurs des paramètres d'authentification LDAP :
    - Adresse IP du serveur virtuel NetScaler AAA : adresse IP du serveur virtuel NetScaler AAA
    - Adresse IP du serveur LDAP : adresse IP du serveur LDAP
    - Port : numéro de port. La valeur par défaut est 389
    - Timeout : valeur du délai d'attente en minutes
    - Domaine d'authentification unique : nom de domaine d'authentification unique
    - DN de base : nom de domaine de base
    - Administrator Bind DN : nom du compte LDAP avec le nom de domaine, par exemple, administrator@domainname.com
    - Nom d'ouverture de session : le nom d'ouverture de session est le nom SamAccountName
    - Mot de passe et confirmation du mot de passe : entrez le mot de passe et confirmez



9. Cliquez sur **Continuer**, puis sur **Terminé**.

Pour supprimer la configuration d'équilibrage de charge pour ShareFile

1. Dans le volet de navigation, cliquez sur **Gestion du trafic**.
2. Dans la section **Citrix ShareFile**, cliquez sur **Supprimer la configuration ShareFile**.

Cas d'utilisation 15 : configurer l'équilibrage de charge de couche 4 sur l'appliance NetScaler

May 5, 2023

L'équilibreur de charge de couche 4 (ports TCP et UDP) utilise les informations fournies dans la couche de transport réseau pour acheminer les demandes des clients entre les groupes de serveurs.

Lorsqu'une connexion de couche 4 est établie entre un client et un serveur, elle dispose d'une vue par paquets du trafic échangé entre eux. L'équilibreur de charge de couche 4 prend ses décisions de routage en fonction des informations d'adresse extraites des premiers paquets du flux TCP, et n'inspecte pas le contenu des paquets. Par conséquent, l'équilibrage de charge de la couche 4 est également appelé équilibrage de charge basé sur la connexion.

L'équilibreur de charge de couche 4 surveille la santé d'un serveur. Le trafic n'est pas acheminé vers le serveur s'il est en panne.

L'équilibrage de charge de couche 4 est utile pour diverses applications utilisant des charges utiles TCP ou UDP. De tels protocoles échangent des données sous forme de charge utile TCP et n'ont pas de structure spécifique à suivre.

Pour configurer l'équilibrage de charge de la couche 4 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

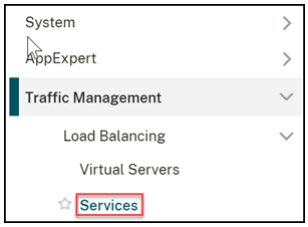
```
add service <name> <serverName> <serviceType> <port>
add lb vserver <name> <serviceType> <ip> <port>
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
add service TCPservice 192.0.2.3 TCP 1
add lb vserver TCPserver TCP 192.0.2.4 1
bind lb vserver TCPserver TCPservice
<!--NeedCopy-->
```

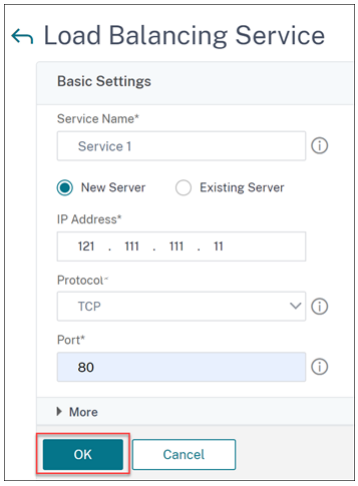
Pour configurer l'équilibrage de charge de la couche 4 à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**.



2. Cliquez sur **Ajouter** pour créer un service.

3. Spécifiez les détails requis dans **Nom du service** et **adresse IP**.
4. Sélectionnez **TCP** ou **UDP** dans **Protocol**.
5. Cliquez sur **OK**.



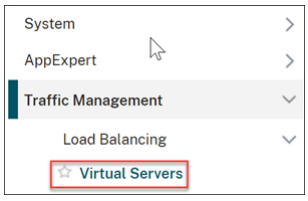
6. Cliquez sur **Terminé**.

   Un service est créé.

   Lorsque vous créez un service en utilisant UDP comme protocole de couche de transport, un moniteur ping (moniteur intégré) est automatiquement lié au service. Lorsque vous créez un service en utilisant TCP comme protocole de couche de transport, un moniteur **tcp_default** est automatiquement lié au service.

   Pour la configuration de l'équilibrage de charge, vous pouvez lier votre service à un autre type de moniteur ou à plusieurs moniteurs. Pour les exigences de surveillance avancée, vous pouvez utiliser le moniteur **tcp-ecv** et configurer les messages de demande et de réponse.

7. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

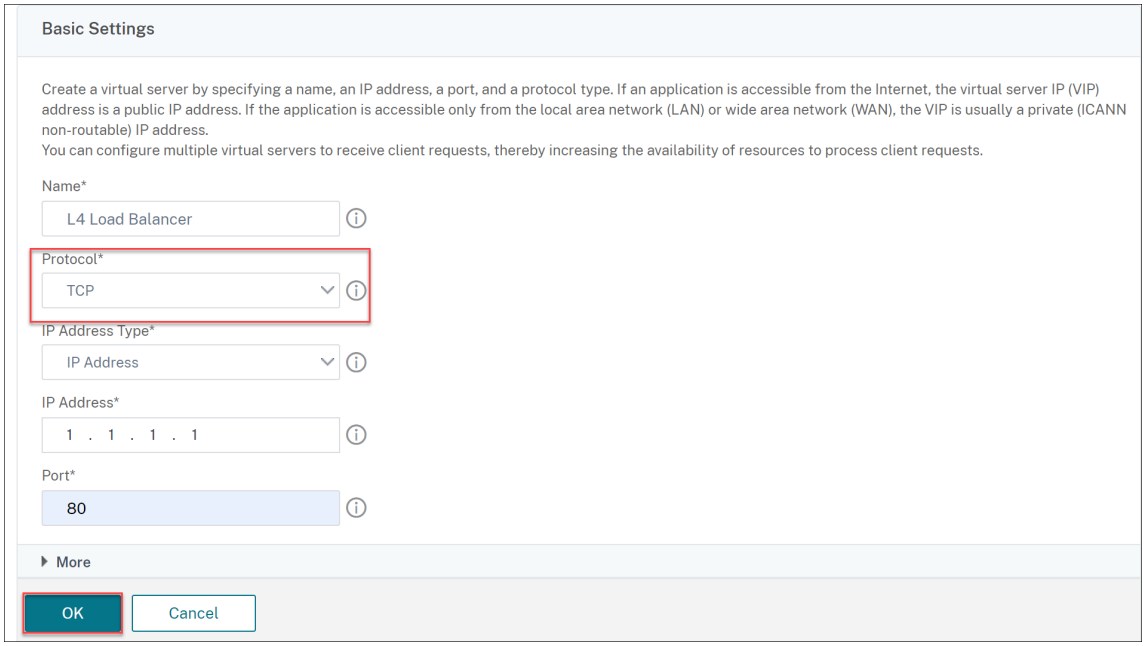


8. Cliquez sur **Ajouter** pour créer un nouveau serveur virtuel.

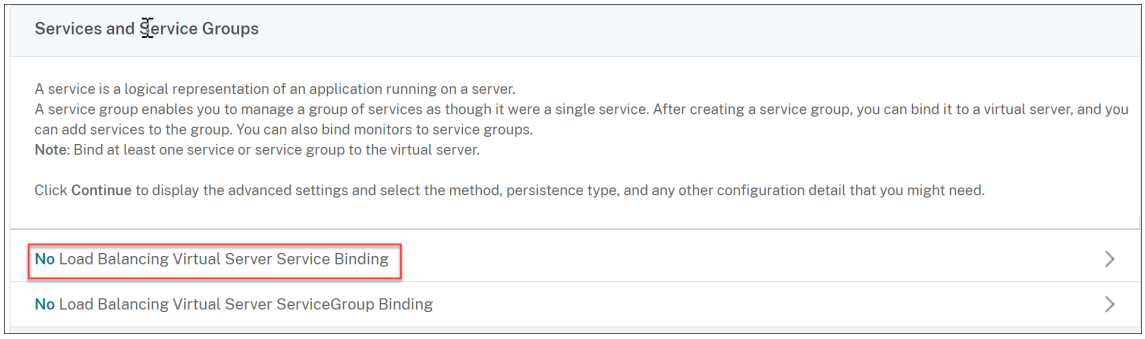
   Lorsque l'équilibrage de charge est configuré, vous pouvez vous connecter au site Web, à l'application ou au serveur à charge équilibrée via l'adresse IP ou le nom de domaine complet du serveur virtuel.

9. Spécifiez les détails requis dans **Nom**, **Type d'adresse IP**et **Adresse IP**.
10. Sélectionnez **TCP** ou **UDP** dans **Protocol**.

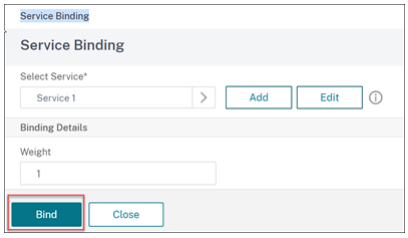
11. Tapez un numéro de port (de 0 à 1023 en fonction du type de service) dans **Port**.
12. Cliquez sur **OK**.



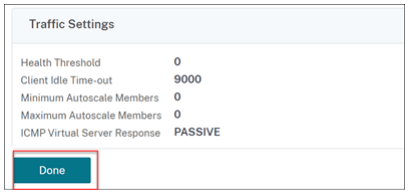
13. Cliquez **sur Liaison de service de serveur virtuel sans équilibrage** de charge dans **Services et groupes de services**.



14. Dans la page **Liaison de services**, sélectionnez **Cliquez pour sélectionner** dans **Sélectionner un service**.
15. Sélectionnez le service à lier, puis cliquez sur **Sélectionner**.
16. Cliquez sur **Liaison pour lier** le service au serveur virtuel.



17. Cliquez sur **Continuer**.
18. Cliquez sur **Terminé**.



La configuration du serveur virtuel d'équilibrage de charge de couche 4 est terminée.

Dépannage

May 5, 2023

Si l'équilibrage de charge ne fonctionne pas comme prévu après l'avoir configuré, vous pouvez utiliser certains outils courants pour accéder aux ressources NetScaler et diagnostiquer le problème.

Ressources pour résoudre les problèmes d'équilibrage de charge

Pour de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème de commutation de contenu sur une appliance NetScaler :

- Dernier fichier ns.conf
- `newnslog` Fichiers pertinents
- Traces de paquets éthéré enregistrées sur l'appliance et le client concerné, si possible
- Le fichier ns.log

Outre les ressources ci-dessus, les outils suivants accélèrent le dépannage :

- Un outil complémentaire de navigateur qui peut afficher les en-têtes HTTP. Cela peut être utilisé pour résoudre les problèmes liés à la persistance.
- L'application Wireshark personnalisée pour les fichiers de trace NetScaler.

Résolution des problèmes d'équilibrage de charge

- **Problème**

L'utilisation du processeur atteint 100 % lorsqu'un moniteur utilisateur est lié à un service lié à un serveur virtuel sur lequel l'option -m MAC est activée.

- **Résolution**

Liez un moniteur non utilisateur au service.

- **Problème**

  J'ai créé un script utilisateur pour la surveillance, mais il ne fonctionne pas.

  Résolution

  Vérifiez le nombre d'arguments dans le script. La limite est de 512. Un script comportant plus de 512 arguments peut ne pas fonctionner correctement. Utilisez le script nsumon-debug.pl de l'interface de ligne de commande pour déboguer le script.

- **Problème**

  Je vois beaucoup de sondes de moniteur, et ils semblent augmenter le trafic réseau inutilement. Existe-t-il un moyen de désactiver les sondes du moniteur ?

  Résolution

  Vous pouvez désactiver les connexions de la sonde du moniteur en désactivant le moniteur ou en définissant la valeur du paramètre HealthMonitor dans la commande set service sur NO. Avec l'option NO, l'appliance affiche le service comme UP à tout moment.

- **Problème**

  J'ai configuré des moniteurs pour les services, mais les connexions sont toujours dirigées vers des serveurs hors service.

  Résolution

  Vous devez probablement réduire les intervalles entre les sondes du moniteur. L'appliance NetScaler ne détecte pas l'état DOWN tant que le moniteur n'envoie pas de sonde.

- **Problème**

  Une métrique liée au moniteur est présente dans les tables de métriques locales et personnalisées.

  Résolution

  Ajoutez le préfixe local au nom de la métrique si la métrique est choisie dans la table de métriques locale. Toutefois, si la métrique est choisie dans le tableau personnalisé, vous n'avez pas besoin d'ajouter de préfixe.

- **Problème**

  Les sondes de surveillance d'un service n'atteignent pas le service.

  Résolution

  Vérifiez si vous avez défini une limite au nombre de connexions pour un service. Si oui, exemptez les connexions moniteur-sonde de cette limite en définissant le paramètre MonitorSkipMaxClient sur ENABLED.

- **Problème**

  Je suis en mesure d'envoyer un ping aux serveurs, mais l'état des services est toujours affiché comme étant en panne.

  Résolution

  Vérifiez le type de moniteur configuré. Par exemple, si un serveur n'est pas configuré pour SSL et que vous utilisez un moniteur HTTPS, l'état du service est marqué comme étant DOWN. Dans ce cas, l'utilisation d'un moniteur TCP doit changer l'état du service sur UP.

- **Problème**

  La définition d'un poids pour les dispositifs de surveillance de la charge ne permet pas de déterminer l'état du service.

  Résolution

  Les moniteurs de charge ne peuvent pas déterminer l'état du service. Par conséquent, il n'est pas approprié de définir un poids sur les moniteurs de charge.

- **Problème**

  Un service n'est pas stable.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez qu'un serveur correct est lié au service.
  - Vérifiez le type de moniteur lié au service.
  - Vérifiez les raisons des défaillances du moniteur. Vous pouvez ouvrir un service à partir de la page Services et vérifier les détails du nombre de sondes, de défaillances et de l'état de la dernière réponse du moniteur dans l'onglet Monitors de la boîte de dialogue Configurer le service. Pour afficher les détails, cliquez sur le moniteur configuré.
  - S'il s'agit d'un moniteur personnalisé, liez un moniteur TCP ou ping au service et vérifiez l'état du moniteur. Si cela permet de résoudre le problème, cela signifie qu'il existe un problème avec le moniteur personnalisé et que celui-ci doit faire l'objet d'une enquête plus approfondie.
  - Vous pouvez enregistrer des traces de paquets sur l'appliance NetScaler et vérifier les sondes du moniteur et la réponse du serveur pour une enquête plus approfondie.

- **Problème**

  L'adresse IP virtuelle (VIP) n'est pas stable ou son état est affiché comme DOWN.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez que la fonctionnalité d'équilibrage de charge est sous licence.

- Vérifiez que la fonctionnalité est activée.
- Vérifiez qu'un service approprié est lié au serveur virtuel.
- Si le statut de l'adresse VIP est affiché comme DOWN, vérifiez qu'un administrateur a activé le service. Si ce n'est pas le cas, le statut du service doit être hors service. Dans ce cas, vous devez activer le service et vérifier si le problème est résolu.
- Vérifiez le (s) service (s) lié (s) au serveur virtuel et suivez les étapes de dépannage mentionnées pour le problème de service non stable.
- Si l'adresse VIP n'est pas stable, tous les services liés au serveur virtuel doivent échouer. Par conséquent, vérifiez si tous les services échouent en même temps. Si tel est le cas, il existe un problème de réseau entre l'appliance NetScaler et les serveurs.

- **Problème**

  Le site présente un équilibrage de charge irrégulier.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez la méthode d'équilibrage de charge configurée sur l'appliance.
  - Vérifiez que les poids associés aux services sont comme prévu.
  - Si la méthode d'équilibrage de charge est autre que Round Robin, vérifiez le nombre de connexions au serveur connecté dans le `newnslog` fichier. Vous pouvez exécuter la commande suivante pour vérifier le numéro du `newnslog` fichier :

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

    Vérifiez les services du serveur virtuel spécifique et vérifiez le temps de réponse, les connexions ouvertes établies (OE), le nombre de demandes, les demandes persistantes et le taux persistant (P) pour résoudre davantage le problème.
  - Si la méthode d'équilibrage de charge est ronde, vérifiez les demandes persistantes comme mentionné à l'étape précédente. En outre, vérifiez si le service n'est pas stable. Si ce n'est pas le cas, suivez les étapes de dépannage mentionnées pour le problème d'instabilité du service
  - Vérifiez si la persistance est configurée sur l'appliance.
  - Vérifiez si un service n'est pas stable. Si oui, suivez les étapes de dépannage mentionnées pour le problème de service non stable.

- **Problème**

  L'état du service est affiché comme étant EN BAS.

  Résolution

  Envisagez de dépanner les composants suivants :

- Vérifiez si une adresse SNIP est configurée.
- Vérifiez que les moniteurs appropriés sont liés au service.
- Si des moniteurs personnalisés sont liés au service, liez un moniteur TCP ou ping au service et vérifiez l'état du moniteur. Si cela permet de résoudre le problème, cela signifie qu'il existe un problème avec le moniteur personnalisé et que celui-ci doit faire l'objet d'une enquête plus approfondie.
- Vérifiez si l'état du service est affiché comme DOWN pour le serveur qui se trouve dans un autre sous-réseau. Si oui, vérifiez si Use Subnet IP (USNIP) résout le problème car cela peut être dû au fait que l'adresse MIP ne peut pas communiquer avec le serveur.

- **Problème**

  Il y a un problème avec le temps de réponse.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez le temps de réponse du serveur à partir des statistiques du service en exécutant la commande suivante :

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

  - Vérifiez si le service n'est pas stable et si l'état du service s'affiche comme étant hors service.

- **Problème**

  L'un des serveurs traite plus de demandes que les autres serveurs à charge équilibrée.

  Résolution

  Envisagez de dépanner les composants suivants :

  - Vérifiez la méthode d'équilibrage de charge. Utilisez la méthode Round Robin pour répartir la demande du client de manière égale, quelle que soit la charge sur les serveurs.
  - Déterminez si la persistance est activée pour la configuration d'équilibrage de charge. Si la persistance est activée, un serveur donné peut supporter une charge plus lourde pour maintenir sa session, surtout si les sessions de persistance sont longues.
  - Vérifiez si des pondérations sont affectées à chaque service. L'attribution de poids appropriés contribue à une bonne répartition de la charge.

- **Problème**

  Les connexions à un serveur d'équilibrage de charge spécifique sont bloquées. Par exemple, toutes les connexions à un serveur Outlook peuvent être bloquées.

  Résolution

  Envisagez de dépanner les composants suivants :

- Vérifiez la méthode d'équilibrage de charge. S'il s'agit d'un système circulaire, envisagez de modifier la méthode en utilisant le moins de connexions.
- Envisagez de réduire le délai d'attente du moniteur. Un délai d'attente plus court permet de marquer un service comme étant DOWN plus tôt, ce qui aiderait à diriger le trafic vers le serveur qui est fonctionnel.
- Si les connexions sont bloquées pendant une longue période, une file d'attente de surtension peut s'accumuler. Envisagez de vider la file d'attente des surtensions pour éviter un pic soudain de charge sur le serveur.
- Si les serveurs fonctionnent à leur niveau maximal, envisagez d'ajouter un nouveau serveur pour de meilleures performances.

- **Problème**

  La majorité des connexions sont dirigées vers un serveur particulier, même lorsque la méthode de moindre connexion est configurée pour l'équilibrage de charge.

  Résolution

  Déterminez si la persistance est configurée et si elle est de type IP source. Si la persistance de l'adresse IP source est configurée même avec la méthode utilisant le moins de connexions, les demandes sont envoyées à un serveur spécifique. L'adresse IP du serveur est requise pour conserver les informations de session. Envisagez d'utiliser la persistance basée sur les cookies HTTP.

- **Conseils de dépannage**
  Pour d'autres problèmes, prenez en compte les conseils suivants pour résoudre un problème non répertorié ci-dessus :

  - Si plusieurs moniteurs de charge sont liés à un service, la charge sur le service est la somme de toutes les valeurs sur les moniteurs de charge qui lui sont liés. Pour que l'équilibrage de charge fonctionne correctement, vous devez lier le même ensemble de moniteurs à tous les services.
  - Si vous désactivez un moniteur de charge lié au service alors que le service est lié à un serveur virtuel, le serveur virtuel utilise la méthode circulaire pour l'équilibrage de charge.
  - Lorsque vous liez un service à un serveur virtuel où la méthode d'équilibrage de charge est CUSTOMLOAD et où l'état du service est UP, le serveur virtuel utilise la méthode Round Robin initiale pour l'équilibrage de charge. Il continue d'être en ronde ronde si le service ne dispose pas de moniteurs de charge personnalisés ou si l'état d'au moins un des moniteurs de charge personnalisés n'est pas UP.
  - Tous les services liés à un serveur virtuel où la méthode d'équilibrage de charge est CUSTOMLOAD, les services doivent avoir des moniteurs de charge liés à eux.
  - La méthode d'équilibrage de charge CUSTOMLOAD suit également la ronde de démarrage.
  - Si vous désactivez une liaison basée sur des mesures et qu'il s'agit de la dernière mesure active, le serveur virtuel spécifique utilise la méthode round robin pour l'équilibrage de

charge. Une métrique est désactivée en définissant le seuil de métrique sur zéro.
- Lorsqu'une métrique liée à un moniteur dépasse la valeur seuil, ce service en particulier n'est pas pris en compte pour l'équilibrage de charge. Si tous les services ont atteint le seuil, le serveur virtuel utilise la méthode circulaire pour l'équilibrage de charge et un message d'erreur « 5xx - erreur d'occupation du serveur » s'affiche.
- Un maximum de 10 mesures d'un tableau personnalisé peuvent être liées au moniteur.
- Les OID doivent être des variables scalaires.
- Pour un équilibrage de charge réussi, l'intervalle doit être aussi faible que possible. Si l'intervalle est élevé, le délai de récupération de la valeur de charge augmente. Par conséquent, l'équilibrage de charge s'effectue à l'aide de valeurs incorrectes.
- Un utilisateur ne peut pas modifier la table locale.

FAQ sur l'équilibrage de charge

May 5, 2023

Quelles sont les différentes politiques d'équilibrage de charge que je peux créer sur l'appliance NetScaler ?

Vous pouvez créer les types de politiques d'équilibrage de charge suivants sur l'appliance NetScaler :

- Connexions moindres
- Round Robin
- Temps de réponse le plus court
- Bande passante minimale
- Moins de paquets
- Hachage d'URL
- Hachage du nom de domaine
- Hachage de l'adresse IP source
- Hachage de l'adresse IP de destination
- IP source - Hachage IP de destination
- Jeton
- LRTM

Puis-je garantir la sécurité de la batterie de serveurs Web en mettant en œuvre un équilibrage de charge à l'aide de l'appliance NetScaler ?

Oui. Vous pouvez garantir la sécurité d'une ferme de serveurs Web en mettant en œuvre un équilibrage de charge à l'aide de l'appliance NetScaler. L'appliance NetScaler vous permet d'implémenter

les options suivantes de la fonctionnalité d'équilibrage de charge :

- Masquage des adresses IP : vous permet d'installer les serveurs réels sur un espace d'adresses IP privé pour des raisons de sécurité et de conservation des adresses IP. Ce processus est transparent pour l'utilisateur final car l'appliance NetScaler accepte les demandes au nom du serveur. En mode masquage d'adresses, l'appliance isole complètement les deux réseaux. Par conséquent, un client peut accéder à un service s'exécutant sur le sous-réseau privé, tel qu'un serveur FTP ou Telnet, via un autre VIP sur l'appliance pour ce service.
- Mappage des ports : permet d'héberger les services TCP réels sur des ports non standard pour des raisons de sécurité. Ce processus est transparent pour l'utilisateur final car l'appliance NetScaler accepte les demandes au nom du serveur sur l'adresse IP et le numéro de port standard annoncés.

Quels sont les différents appareils que je peux utiliser pour équilibrer la charge avec une appliance NetScaler ?

Vous pouvez équilibrer la charge des appareils suivants à l'aide d'une appliance NetScaler :

- Batteries de serveurs
- Caches ou proxies inverses
- Dispositifs de pare-feu
- Systèmes de détection d'intrusion
- Appareils de déchargement SSL
- Appareils de compression
- Serveurs d'inspection de contenu

Pourquoi dois-je implémenter la fonctionnalité d'équilibrage de charge pour le site Web ?

Vous pouvez implémenter la fonctionnalité d'équilibrage de charge pour le site Web afin de tirer les avantages suivants :

- Réduisez le temps de réponse : lorsque vous implémentez la fonctionnalité d'équilibrage de charge pour le site Web, l'un des principaux avantages est l'augmentation du temps de chargement auquel vous pouvez vous attendre. Comme deux serveurs ou plus se partagent la charge du trafic Web, chacun des serveurs gère moins de trafic qu'un seul serveur. Cela signifie que davantage de ressources sont disponibles pour répondre aux demandes des clients. Cela se traduit par un site Web plus rapide.
- Redondance : La mise en œuvre de la fonctionnalité d'équilibrage de charge introduit un peu de redondance. Par exemple, si le site est équilibré sur trois serveurs et que l'un d'eux ne répond pas du tout, les deux autres peuvent continuer à fonctionner et les visiteurs du site ne remar-

quent même pas de temps d'arrêt. Toute solution d'équilibrage de charge cesse immédiatement d'envoyer du trafic vers le serveur principal qui n'est pas disponible.

Pourquoi dois-je désactiver l'option MBF (Mac Based Forwarding) pour Link Load Balancing (LLB) ?

- Si vous activez l'option MBF, l'appliance NetScaler considère que le trafic entrant en provenance du client et le trafic sortant vers le même client transitent par le même routeur en amont. Toutefois, la fonctionnalité LLB nécessite le meilleur chemin d'accès pour le trafic retour.
- L'activation de l'option MBF rompt cette conception de topologie en envoyant le trafic sortant via le routeur qui a transféré le trafic client entrant.

Réseau

May 5, 2023

Les rubriques suivantes fournissent une référence conceptuelle et des instructions pour configurer les différents composants réseau sur l'appliance NetScaler.

Adressage IP	Découvrez les différents types d'adresses IP détenues par NetScaler et comment les créer, les personnaliser et les supprimer.
Interfaces	Configurez certaines des configurations réseau de base qui doivent être effectuées pour commencer.
Listes de contrôle d'accès (ACL)	Configurez les différents types de listes de contrôle d'accès et comment les créer, les personnaliser et les supprimer.
Routage IP	Découvrez et configurez les fonctionnalités de routage de l'appliance NetScaler, à la fois statique et dynamique.
Protocole Internet version 6 (IPv6)	Découvrez comment l'appliance NetScaler prend en charge le protocole IPv6.
Domaines de trafic	Découvrez et configurez les domaines de trafic afin de segmenter le trafic réseau pour différentes applications.

VXLAN	Apprenez et configurez les VXLAN pour répondre aux besoins d'évolutivité de votre centre de données.

Adressage IP

May 5, 2023

Avant de pouvoir configurer l'appliance NetScaler, vous devez attribuer l'adresse NSIP, également appelée adresse IP de gestion. Vous pouvez également créer d'autres adresses IP appartenant à NetScaler pour extraire des serveurs et établir des connexions avec les serveurs. Dans ce type de configuration, l'appliance fait office de proxy pour les serveurs abstraits. Vous pouvez également établir des connexions proxy à l'aide de traductions d'adresses réseau (INAT et RNAT). Lors de connexions par proxy, l'appliance peut se comporter comme un périphérique de pontage (couche 2) ou comme un périphérique de transfert de paquets (couche 3). Pour rendre le transfert de paquets plus efficace, vous pouvez configurer des entrées ARP statiques. Pour IPv6, vous pouvez configurer la découverte de voisins (ND).

Configuration des adresses IP appartenant à NetScaler

May 5, 2023

Les adresses IP appartenant à NetScaler (adresse NSIP, adresses IP virtuelles (VIP), adresses IP de sous-réseau (SNIP) et adresses IP du site d'équilibrage de charge globale des serveurs (GSLBIP) n'existent que sur l'appliance NetScaler. Le NSIP identifie de manière unique le NetScaler sur votre réseau et permet d'accéder à l'appliance. Une adresse VIP est une adresse IP publique à laquelle un client envoie des requêtes. NetScaler met fin à la connexion du client au niveau du VIP et établit une connexion avec un serveur. Cette nouvelle connexion utilise un SNIP ou un MIP comme adresse IP source pour les paquets transmis au serveur. Si vous avez plusieurs centres de données répartis géographiquement, chaque centre de données peut être identifié par un GSLBIP unique. Vous pouvez configurer certaines adresses IP appartenant à NetScaler pour fournir un accès aux applications de gestion.

Configuration de l'adresse NSIP

May 5, 2023

L'adresse NSIP est l'adresse IP à laquelle vous accédez à l'appliance NetScaler à des fins de gestion. L'appliance ne peut avoir qu'un seul NSIP, également appelé adresse IP de gestion. Vous devez ajouter cette adresse IP lorsque vous configurez NetScaler pour la première fois. Vous ne pouvez pas supprimer une adresse NSIP. Pour des raisons de sécurité, le NSIP doit être une adresse IP non routable sur le réseau local de votre organisation.

Si vous modifiez cette adresse, vous devez redémarrer l'appliance NetScaler. Si l'adresse de sous-réseau de la nouvelle adresse NSIP est différente de la précédente, vous devez ajouter une route par défaut pour ce sous-réseau afin que la nouvelle adresse NSIP soit accessible depuis d'autres réseaux du réseau local.

> **Important**
>
> La configuration de l'adresse NSIP est obligatoire.

La modification de l'adresse NSIP d'une appliance NetScaler comprend les tâches suivantes :

- Modifiez l'adresse NSIP.
- Ajoutez un itinéraire par défaut pour l'adresse de sous-réseau de l'adresse NSIP, s'il n'en existe pas.
- Enregistrez la configuration.
- Redémarrez l'appliance.

Procédures de ligne de commande

Pour modifier l'adresse NSIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ****définir ns config -ipAddress -netmask**** <ip_addr><netmask>
- **show ns config**

Pour ajouter un itinéraire par défaut à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter un itinéraire 0 0** <gateway IP address>
- **afficher l'itinéraire**

Pour enregistrer la configuration à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **enregistrer la configuration**

Pour redémarrer l'appliance NetScaler à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **reboot**

Procédures GUI

Pour configurer l'adresse NSIP à l'aide de l'interface graphique :

1. Cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit de la page de **configuration** .
2. Cliquez sur le volet d' **adresses NSIP** .
3. Sur la page d' **adresse NSIP**, définissez les paramètres suivants, puis cliquez sur **OK** :
    - Adresse NSIP
    - Masque réseau

Pour ajouter un itinéraire par défaut à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Itinéraires** et, dans l'onglet **Basic**, ajoutez un itinéraire par défaut avec les paramètres suivants, puis cliquez sur **Créer**.

- Réseau (réglé sur zéro)
- Masque réseau (réglé sur zéro)
- Passerelle (adresse IP de la passerelle)

Pour redémarrer NetScaler à l'aide de l'interface graphique :

1. Sur la page de l'onglet **Informations système** du nœud **Système**, cliquez sur **Redémarrer**.
2. Lorsque vous êtes invité à redémarrer, sélectionnez **Enregistrer la configuration** pour vous assurer de ne perdre aucune configuration.

Exemple de configuration

Dans l'exemple suivant, l'adresse NSIP d'un dispositif NetScaler est remplacée par 192.0.2.90, qui possède une adresse de sous-réseau (192.0.2.0/24) différente de celle de l'adresse NSIP précédente. Par conséquent, une route par défaut est ajoutée pour ce sous-réseau, de sorte que la nouvelle adresse NSIP devient accessible à partir d'autres réseaux.

```
1 > set nsconfig -ipAddress 192.0.2.90 -netmask 255.255.255.0
2
3  Warning: The configuration must be saved and the system rebooted for
      these settings to take effect
4 > add route 0 0 192.0.2.1
5
```



```
 Warning: The configuration must be saved and the system rebooted for
    these settings to take effect
> save config

 Done
> reboot
```

Configuration et gestion des adresses IP virtuelles (VIP)

May 5, 2023

La configuration d'une adresse IP de serveur virtuel (VIP) n'est pas obligatoire lors de la configuration initiale de NetScaler. Lorsque vous configurez l'équilibrage de charge, vous affectez des adresses VIP aux serveurs virtuels.

Pour plus d'informations sur la configuration d'une configuration d'équilibrage de charge, voir Équilibrage de charge.

Dans certains cas, vous devez personnaliser les attributs VIP ou activer ou désactiver une adresse VIP. Une adresse VIP est généralement associée à un serveur virtuel, et certains attributs VIP sont personnalisés pour répondre aux exigences du serveur virtuel. Vous pouvez héberger le même serveur virtuel sur plusieurs appliances NetScaler résidant sur le même domaine de diffusion, à l'aide des attributs ARP et ICMP. Une fois que vous avez ajouté un VIP (ou n'importe quelle adresse IP), l'appliance envoie des requêtes ARP, puis y répond. Les adresses IP VIP sont les seules adresses IP appartenant à NetScaler qui peuvent être désactivées. Lorsqu'une adresse VIP est désactivée, le serveur virtuel qui l'utilise tombe en panne et ne répond pas aux demandes de service ARP, ICMP ou L4. Au lieu de créer des adresses VIP une par une, vous pouvez spécifier une plage consécutive d'adresses VIP.

Pour créer une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter un type d'adresse <IPAddress><netmask>IP ns <type>
- Afficher notre adresse IP <IPAddress>

Exemple :

```
> add ns ip 10.102.29.59 255.255.255.0 -type VIP
 Done
<!--NeedCopy-->
```

Pour créer une plage d'adresses VIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter un type d'adresse <IPAddress><netmask>IP ns <type>
- Afficher notre adresse IP <IPAddress>

Exemple :

```
> add ns ip 10.102.29.[60-64] 255.255.255.0 -type VIP
ip "10.102.29.60" added
ip "10.102.29.61" added
ip "10.102.29.62" added
ip "10.102.29.63" added
ip "10.102.29.64" added
 Done
<!--NeedCopy-->
```

Pour activer ou désactiver une adresse VIP IPv4 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants pour activer ou désactiver un VIP et vérifier la configuration :

- activer ns ip <IPAddress>
- Afficher notre adresse IP <IPAddress>
- désactiver ns ip <IPAddress>
- Afficher notre adresse IP <IPAddress>

Exemple :

```
> enable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Enabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
          ssh: Disabled
          gui: Disabled
          snmp: Disabled
        Restrict access: Disabled
        dynamic routing: Disabled
        hostroute: Disabled
```



```
 Done
> disable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Disabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
          ssh: Disabled
          gui: Disabled
          snmp: Disabled
        Restrict access: Disabled
        dynamic routing: Disabled
        hostroute: Disabled

 Done
<!--NeedCopy-->
```

Pour configurer une adresse VIP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **IP** > **IPv4S, puis**ajoutez une nouvelle adresse IP ou modifiez une adresse existante.

Pour créer une plage d'adresses VIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP** > **IPv4S**.
2. Dans la liste des **actions**, sélectionnez **Ajouter une plage**.

Pour activer ou désactiver une adresse VIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP** > **IPv4S**.
2. Procédez comme suit :
   - Sélectionnez une adresse VIP.
   - Maintenez la touche **Ctrl** enfoncée et sélectionnez plusieurs entrées d'adresse de serveur.
   - Maintenez la touche **Shift enfoncée** et sélectionnez une série d'entrées d'adresses de serveur.
   - Sélectionnez toutes les adresses en cochant la case située sur le côté gauche de la ligne d'en-tête.
3. Dans la liste des **actions**, sélectionnez **Désactiver** ou **Activer**.

Détection d'une appliance NetScaler dans une configuration d'équilibrage de charge UDP via des mises à jour TTL

Le tableau suivant montre comment une appliance NetScaler gère la valeur TTL des paquets reçus dans différentes fonctionnalités.

Fonctionnalité	Valeur TTL
Serveur virtuel	Le TTL est défini sur 255 lors du transfert de la demande vers les serveurs principaux. Le TTL est décrémenté de 1 lors de la transmission de la réponse au client.
Mode L2	Le TTL n'est pas modifié.
Mode L3	TTL est réglé sur 255.
INAT	Le TTL est défini sur 255 lors du transfert de la demande vers le serveur principal. Le TTL est décrémenté de 1 lors de la transmission de la réponse au client.

Certaines entreprises/scénarios exécutant une application de surveillance nécessitent que l'appliance NetScaler d'une configuration d'équilibrage de charge soit détectée comme l'un des sauts d'un traceroute. Une appliance NetScaler dotée d'une configuration d'équilibrage de charge n'est pas détectée dans un traceroute car, par défaut, l'appliance définit la valeur TTL sur 255 au lieu de la décrémenter lors du transfert de la demande vers un serveur principal.

Pour répondre à cette exigence, le paramètre **Decrement TTL** d'une adresse VIP peut être utilisé. Ce paramètre s'applique à tous les serveurs virtuels UDP utilisant ce VIP.

Lorsque vous activez le paramètre **Decrement TTL** d'un VIP, l'appliance NetScaler décrémente la valeur TTL de 1 au lieu de la définir sur 255 lors du transfert des demandes, qui sont reçues sur les serveurs virtuels UDP qui utilisent ce VIP.

La surveillance des applications utilisant les données de traceroute peut désormais détecter la présence d'une appliance NetScaler ou d'une configuration d'équilibrage de charge UDP.

Avant de commencer

Avant de commencer à configurer une appliance NetScaler à détecter dans un traceroute d'une configuration d'équilibrage de charge, notez les points suivants :

- Le paramètre TTL de décrémentation est pris en charge uniquement pour les serveurs virtuels d'équilibrage de charge UDP.

- Le paramètre TTL de décrémentation est pris en charge pour les adresses VIP IPv4 ainsi que pour les adresses VIP IPv6 (VIP6).
- Le paramètre TTL de décrémentation est pris en charge pour les appliances NetScaler autonomes ainsi que pour les configurations de haute disponibilité (HA) et de clusters.

Étapes de configuration

La configuration d'une appliance NetScaler à détecter dans un traceroute d'une configuration d'équilibrage de charge UDP comprend les tâches suivantes :

- Création d'une configuration d'équilibrage de charge UDP
- Activez le paramètre Decrement TTL pour l'adresse VIP

Procédures CLI

Pour activer l'option de décrémentation TTL pour une adresse VIP à l'aide de l'interface de ligne de commande :

- Pour activer l'option de décrémentation TTL pour une adresse VIP lors de l'ajout de l'adresse VIP, à l'invite de commande, tapez :
  - **ajouter ns ip** <ip><mask>-**type VIP** -**DecrementTTL ACTIVÉ**
  - **Afficher notre adresse IP** <VIP address>
- Pour activer l'option de décrémentation TTL pour une adresse VIP existante, à l'invite de commande, tapez :
  - **set ns ip** <ip><mask>-**DecrementTTL ACTIVÉ**
  - **Afficher notre adresse IP** <VIP address>

Pour activer l'option de décrémentation TTL pour une adresse VIP6 à l'aide de l'interface de ligne de commande :

- Pour activer l'option de décrémentation TTL pour une adresse VIP6 lors de l'ajout de l'adresse VIP6, à l'invite de commande, tapez :
  - **ajouter ns ip6** <IP6/prefix> <mask>-**type VIP** -**DecrementTTL**ACTIVÉ
  - **Afficher notre IP66** <VIP6/prefix>
- Pour activer l'option de décrémentation TTL pour une adresse VIP6 existante, à l'invite de commande, tapez :
  - **set ns ip6** <ip6/prefix> <mask>-**DecrementTTL**ACTIVÉ
  - **Afficher notre IP66** <VIP6 address>

```
1    > add ns ip 203.0.113.30 -type VIP -decrementTTL ENABLED
2     Done
3
4    > add ns ip6  2001:DB8:5001::30 -type VIP -decrementTTL ENABLED
```



```
5       Done
6 <!--NeedCopy-->
```

Procédures GUI

Pour activer l'option de décrémentation TTL pour une adresse VIP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **IP** > **IPv4S**et activez le paramètre **Decrement TTL** lors de l'ajout d'une nouvelle adresse VIP ou de la modification d'une adresse existante.

Pour activer l'option de décrémentation TTL pour une adresse VIP6 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **IP** > **IPv6s** et activez le paramètre **Decrement TTL** tout en ajoutant une nouvelle adresse VIP6 ou en modifiant une adresse existante.

Configuration de la suppression des réponses ARP pour les adresses IP virtuelles (VIP)

May 5, 2023

Vous pouvez configurer l'appliance NetScaler pour qu'elle réponde ou non aux demandes ARP concernant une adresse IP virtuelle (VIP) en fonction de l'état des serveurs virtuels associés à cette adresse VIP.

Par exemple, si les serveurs virtuels V1, de type HTTP, et V2, de type HTTPS, partagent l'adresse VIP 10.102.29.45 sur une appliance NetScaler, vous pouvez configurer l'appliance pour qu'elle ne réponde à aucune demande ARP pour VIP 10.102.29.45 si les versions V1 et V2 sont toutes deux à l'état DOWN.

Les trois options suivantes sont disponibles pour configurer la suppression de la réponse ARP pour une adresse IP virtuelle.

- **NONE**. L'appliance NetScaler répond à toute demande ARP concernant l'adresse VIP, quel que soit l'état des serveurs virtuels associés à l'adresse.
- **UN VSERVER**. L'appliance NetScaler répond à toute demande ARP concernant l'adresse VIP si au moins l'un des serveurs virtuels associés est en état UP.
- **TOUS LES VSERVER**. L'appliance NetScaler répond à toute demande ARP concernant l'adresse VIP si tous les serveurs virtuels associés sont en état UP.

Le tableau suivant montre l'exemple de comportement de l'appliance NetScaler pour un VIP configuré avec deux serveurs virtuels :

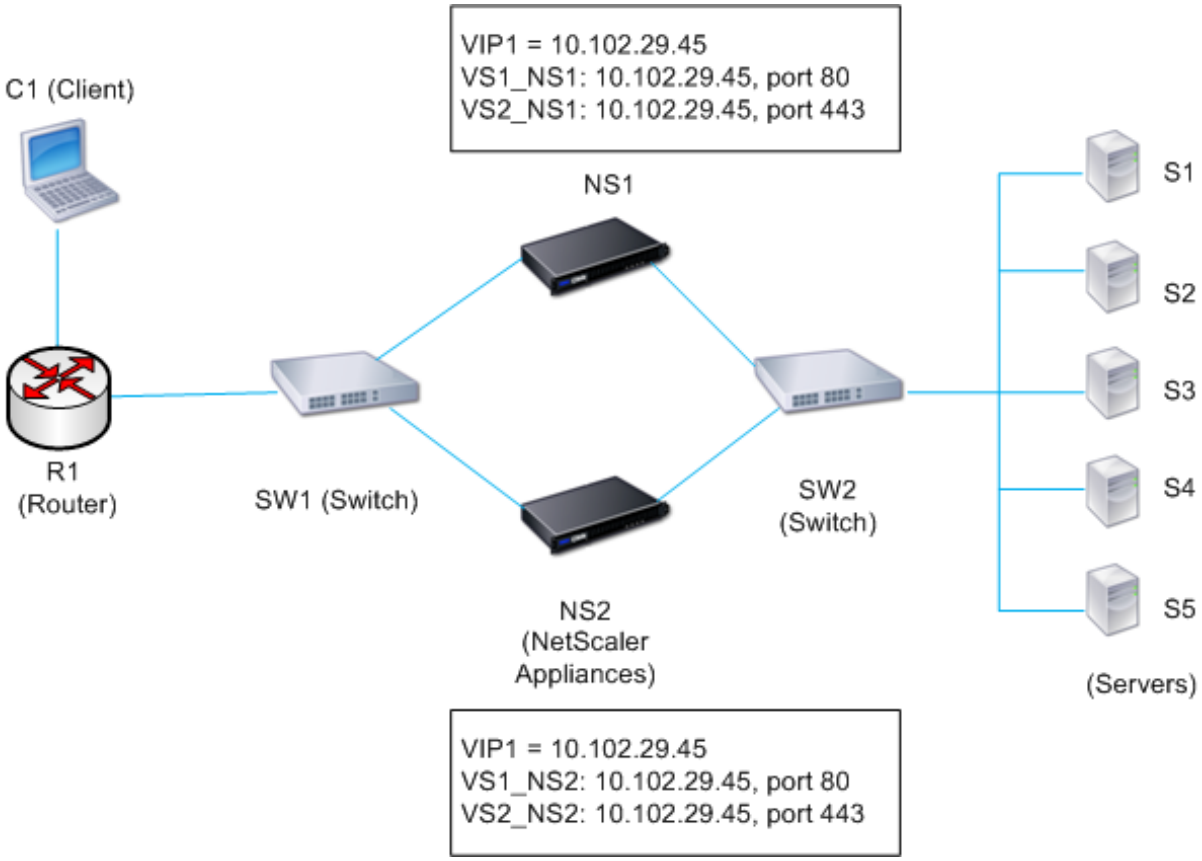
Serveurs virtuels associés pour un VIP	ÉTAT 1	ÉTAT 2	ÉTAT 3	ÉTAT 4
NONE				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Répondre à une demande d'ARP pour ce VIP ?	Oui	Oui	Oui	Oui
UN SERVEUR VIRTUEL				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Répondre à une demande d'ARP pour ce VIP ?	Oui	Oui	Oui	Non
TOUS LES SERVEURS VIRTUELS				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Répondre à une demande d'ARP pour ce VIP ?	Oui	Non	Non	Non

Prenons un exemple dans lequel vous souhaitez tester les performances de deux serveurs virtuels, V1 et V2, qui ont la même adresse VIP mais sont de types différents et sont chacun configuré sur les appliances NetScaler NS1 et NS2. Appelons l'adresse VIP partagée *VIP1*.

La V1 équilibre la charge des serveurs S1, S2 et S3. La version V2 équilibre la charge des serveurs S4 et S5.

Sur NS1 et NS2, pour VIP1, le paramètre de suppression ARP est défini sur ALL_VSERVER. Si vous souhaitez tester les performances des versions V1 et V2 sur NS1, vous devez désactiver manuellement les versions V1 et V2 sur NS2, afin que NS2 ne réponde à aucune demande ARP pour VIP1.

Figure 1.



Le flux d'exécution est le suivant :

1. Le client C1 envoie une demande à V1. La demande atteint R1.
2. R1 ne possède pas d'entrée APR pour l'adresse IP (VIP1) de V1. R1 diffuse donc une requête ARP pour VIP1.
3. NS1 répond avec l'adresse MAC source MAC1 et l'adresse IP source VIP1. NS2 ne répond pas à la demande ARP.
4. SW1 apprend le port pour VIP1 à partir de la réponse ARP et met à jour sa table de pont, tandis que R1 met à jour l'entrée ARP avec MAC1 et VIP1.
5. R1 transmet le paquet à l'adresse VIP1 sur NS1.
6. L'algorithme d'équilibrage de charge de NS1 sélectionne le serveur S2, et NS1 ouvre une connexion entre l'une de ses adresses SNIP et S2. Lorsque S2 envoie une réponse au client, la réponse est renvoyée par le même chemin.
7. Vous voulez maintenant tester les performances des versions V1 et V2 sur NS2. Vous devez donc activer les versions V1 et V2 sur NS2 et les désactiver sur NS1. NS2 diffuse désormais un message ARP pour VIP1. Dans le message, MAC2 est l'adresse MAC source et VIP1 est l'adresse IP source.
8. SW1 apprend le numéro de port permettant d'accéder à MAC2 à partir de la diffusion ARP et met à jour sa table de pont pour envoyer les demandes clients suivantes concernant VIP1 à NS2. R1 met à jour sa table ARP.
9. Supposons maintenant que l'entrée ARP pour VIP1 expire dans la table ARP de R1 et que le client

C1 envoie une demande pour V1. Comme R1 ne possède pas d'entrée APR pour VIP1, il diffuse une requête ARP pour VIP1.

10. NS2 répond avec une adresse MAC source et VIP1 comme adresse IP source. NS1 ne répond pas à la demande ARP.

Pour configurer la suppression de la réponse ARP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **[définir une adresse IP** <arpResponse>-**ARPResponse]**
- **sh ns ip** <IPAddress>

Exemple :

```
1 > set ns ip 10.102.29.96 -arpResponse ALL_VSERVERS
2  Done
3 <!--NeedCopy-->
```

Pour configurer la suppression de la réponse ARP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP** > **IPv4S**.
2. Ouvrez une entrée d'adresse IP et sélectionnez le type de réponse ARP.

Configuration des adresses IP de sous-réseau (SNIP)

May 5, 2023

Une adresse IP de sous-réseau (SNIP) est une adresse IP appartenant à NetScaler qui est utilisée par NetScaler pour communiquer avec les serveurs.

NetScaler utilise l'adresse IP du sous-réseau comme adresse IP source pour les connexions des clients aux serveurs par proxy. Il utilise également l'adresse IP du sous-réseau pour générer ses propres paquets, tels que des paquets liés aux protocoles de routage dynamique, ou pour envoyer des sondes de surveillance afin de vérifier l'état des serveurs. Selon la topologie de votre réseau, il se peut que vous deviez configurer un ou plusieurs SNIP pour différents scénarios.

Pour configurer une adresse SNIP sur un NetScaler, vous ajoutez l'adresse SNIP, puis vous activez le mode global Use Subnet IP (USNIP). Au lieu de créer des SNIP un par un, vous pouvez spécifier une plage consécutive de SNIP.

Pour configurer une adresse SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter ns ip <IPAddress><netmask>-type SNIP
- Afficher notre adresse IP <IPAddress>

Exemple :

```
> add ns ip 10.102.29.203 255.255.255.0 -type SNIP
 Done
<!--NeedCopy-->
```

Pour créer une plage d'adresses SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter ns ip <IPAddress><netmask>-type SNIP
- Afficher notre adresse IP <IPAddress>

Exemple :

```
> add ns ip 10.102.29.[205-209] 255.255.255.0 -type SNIP
ip "10.102.29.205" added
ip "10.102.29.206" added
ip "10.102.29.207" added
ip "10.102.29.208" added
ip "10.102.29.209" added
 Done
<!--NeedCopy-->
```

Pour activer ou désactiver le mode USNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- activer ns ModeUSnip
- désactiver ns ModeUsnip

Pour configurer une adresse SNIP à l'aide de l'interface graphique :

Accédez à Système > Réseau > IP > IPv4S, puis ajoutez une nouvelle adresse SNIP ou modifiez une adresse existante.

Pour créer une plage d'adresses SNIP à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > IP > IPv4S.
2. Dans la liste des actions, sélectionnez Ajouter une plage.

Pour activer ou désactiver le mode USNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- activer ns ModeUSnip
- désactiver ns ModeUsnip

Pour activer ou désactiver le mode USNIP à l'aide de l'interface graphique :

1. Accédez à Système > Paramètres, dans le groupe Modes et fonctionnalités, cliquez sur Modifier les modes.
2. Sélectionnez ou désactivez l'option Utiliser l'adresse IP du sous-réseau.

Utilisation de SNIP pour un sous-réseau de serveur directement connecté

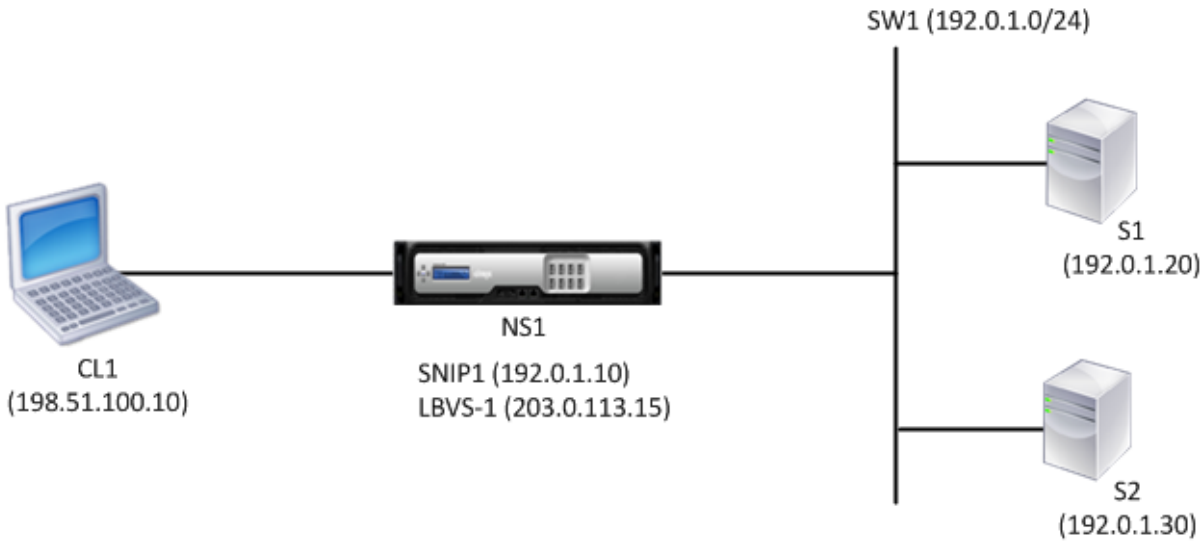
Pour activer la communication entre NetScaler et un serveur connecté directement à NetScaler ou connecté uniquement via un commutateur L2, vous devez configurer une adresse IP de sous-réseau appartenant au sous-réseau du serveur. Vous devez configurer au moins une adresse IP de sous-réseau pour chaque sous-réseau directement connecté, à l'exception du sous-réseau de gestion directement connecté via NSIP.

Prenons l'exemple d'une configuration d'équilibrage de charge dans laquelle le serveur virtuel d'équilibrage de charge LBVS1 sur NetScaler NS1 est utilisé pour équilibrer la charge des serveurs S1 et S2, qui sont connectés à NS1 via le commutateur L2 SW1. S1 et S2 appartiennent au même sous-réseau.

L'adresse SNIP SNIP1, qui appartient au même sous-réseau que S1 et S2, est configurée sur NS1. Dès que SNIP1 est configuré, NS1 diffuse des paquets ARP pour SNIP1.

Les services SVC-S1 et SVC-S2 sur NS1 représentent S1 et S2. Dès que ces services sont configurés, NS1 diffuse des requêtes ARP pour S1 et S2 afin de résoudre le mappage IP-Mac. Après que S1 et S2 répondent, NS1 leur envoie des sondes de surveillance à intervalles réguliers, à partir de l'adresse SNIP1, pour vérifier leur état de santé.

Pour plus d'informations sur la configuration de l'équilibrage de charge sur un NetScaler, consultez la section Équilibrage de charge.



Voici le flux de trafic dans cet exemple :

1. Le client C1 envoie un paquet de demande à LBVS-1. Le paquet de requête a :

- IP source = adresse IP du client (198.51.100.10)
- IP de destination = adresse IP de LBVS-1 (203.0.113.15)

2. LBVS1 de NS1 reçoit le paquet de requête.
3. L'algorithme d'équilibrage de charge de LBVS1 sélectionne le serveur S2.
4. Comme S2 est directement connecté à NS1 et que SNIP1 (192.0.1.10) est la seule adresse IP de NS1 qui appartient au même sous-réseau que S2, NS1 ouvre une connexion entre SNIP1 et S2.
5. NS1 envoie le paquet de demande à S2 depuis SNIP1. Le paquet de requête a :
   - IP source = SNIP1 (192.0.1.10)
   - IP de destination = adresse IP de S2 (192.0.1.30)
6. La réponse de S2 renvoie par le même chemin.

Utilisation de SNIP pour les sous-réseaux de serveurs connectés via un routeur

Pour permettre la communication entre NetScaler et les serveurs des sous-réseaux connectés via un routeur, vous devez configurer au moins une adresse IP de sous-réseau appartenant au sous-réseau de l'interface directement connectée au routeur. L'ADC utilise cette adresse IP de sous-réseau pour communiquer avec les serveurs des sous-réseaux accessibles via le routeur.

Prenons l'exemple d'une configuration d'équilibrage de charge dans laquelle le serveur virtuel d'équilibrage de charge LBVS1 sur NetScaler NS1 est utilisé pour équilibrer la charge des serveurs S1, S2, S3 et S4, qui sont connectés à NS1 via le routeur R1.

S1 et S2 appartiennent au même sous-réseau, 192.0.2.0/24, et sont connectés à R1 via le commutateur L2 SW1. S3 et S4 appartiennent à un sous-réseau différent, 192.0.3.0/24, et sont connectés à R1 via le commutateur L2 SW2.

NetScaler NS1 est connecté au routeur R1 via le sous-réseau 192.0.1.0/24. L'adresse SNIP SNIP1, qui appartient au même sous-réseau que l'interface directement connectée au routeur (192.0.1.0/24), est configurée sur NS1. NS1 utilise cette adresse pour communiquer avec les serveurs S1 et S2 et avec les serveurs S3 et S4.

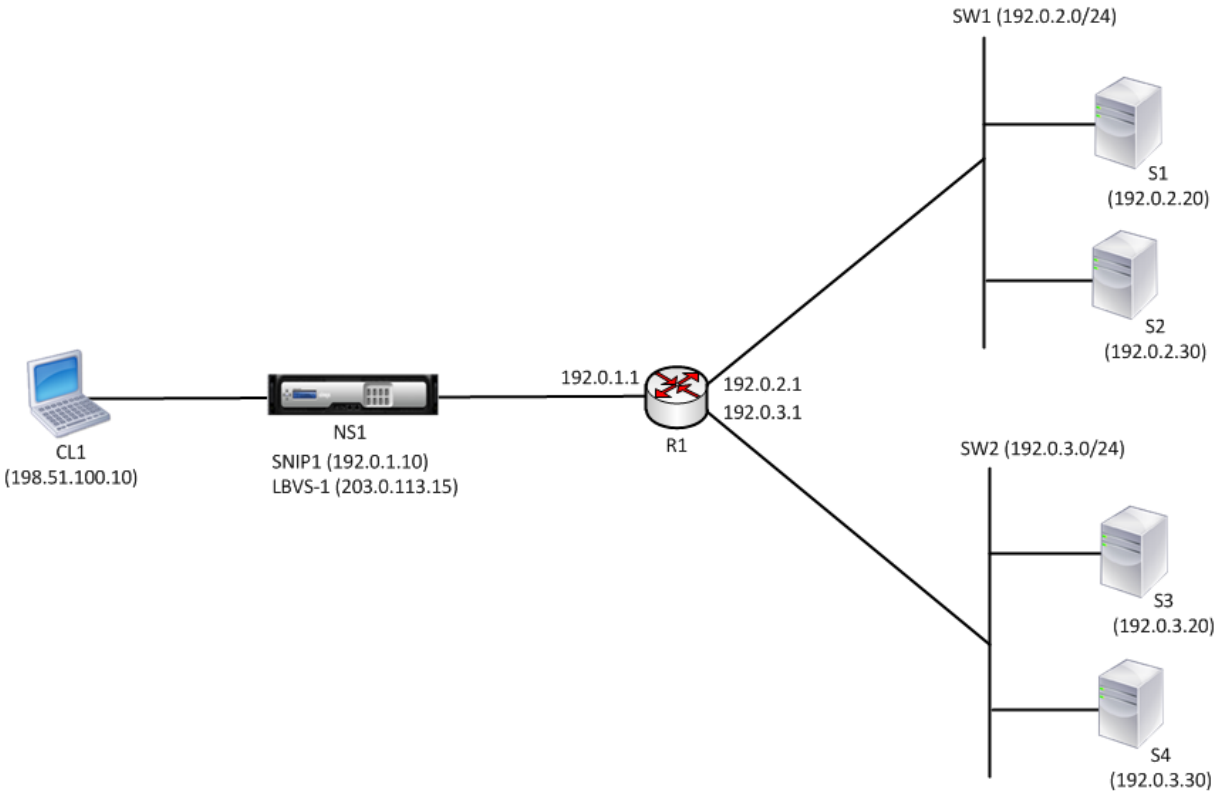
Pour plus d'informations sur la configuration de l'équilibrage de charge sur un NetScaler, consultez la section Équilibrage de charge.

Dès que l'adresse SNIP1 est configurée, NS1 diffuse les paquets d'annonce ARP pour SNIP1.

La table de routage de NS1 comprend les entrées de routage pour S1, S2, S3 et S4 à R1. Ces entrées de route sont soit des entrées de route statiques, soit annoncées par R1 à NS1, à l'aide de protocoles de routage dynamiques.

Les services SVC-S1, SVC-S2, SVC-S3 et SVC-S4 sur NS1 représentent les serveurs S1, S2, S3 et S4. NS1 constate, dans ses tables de routage, que ces serveurs sont accessibles via R1. NS1 leur envoie des sondes de surveillance à intervalles réguliers, à partir de l'adresse SNIP1, pour vérifier leur état de santé.

Pour plus d'informations sur le routage IP sur un NetScaler, consultez la section Routage IP.



Voici le flux de trafic dans cet exemple :

1. Le client C1 envoie un paquet de demande à LBVS-1. Le paquet de requête a :
   - IP source = adresse IP du client (198.51.100.10)
   - IP de destination = adresse IP de LBVS-1 (203.0.113.15)
2. LBVS1 de NS1 reçoit le paquet de requête.
3. L'algorithme d'équilibrage de charge de LBVS1 sélectionne le serveur S3.
4. NS1 vérifie sa table de routage et constate que S3 est accessible via R1. SNIP1 (192.0.1.10) est la seule adresse IP sur NS1 qui appartient au même sous-réseau que le routeur R1. NS1 ouvre une connexion entre SNIP1 et S3 via R1.
5. NS1 envoie le paquet de demande à R1 depuis SNIP1. Le paquet de requête a :
   - Adresse IP source = SNIP1 (192.0.1.10)
   - Adresse IP de destination = adresse IP de S3 (192.0.3.20)
6. La demande parvient à R1, qui vérifie sa table de routage et transmet le paquet de demande à S3.
7. La réponse de S3 renvoie par le même chemin.

Utilisation de SNIP pour plusieurs sous-réseaux de serveurs (VLAN) sur un commutateur L2

Lorsque vous disposez de plusieurs sous-réseaux de serveur (VLAN) sur un commutateur L2 connecté à un NetScaler, vous devez configurer au moins une adresse SNIP pour chacun des sous-réseaux de serveur, afin que NetScaler puisse communiquer avec ces sous-réseaux de serveur.

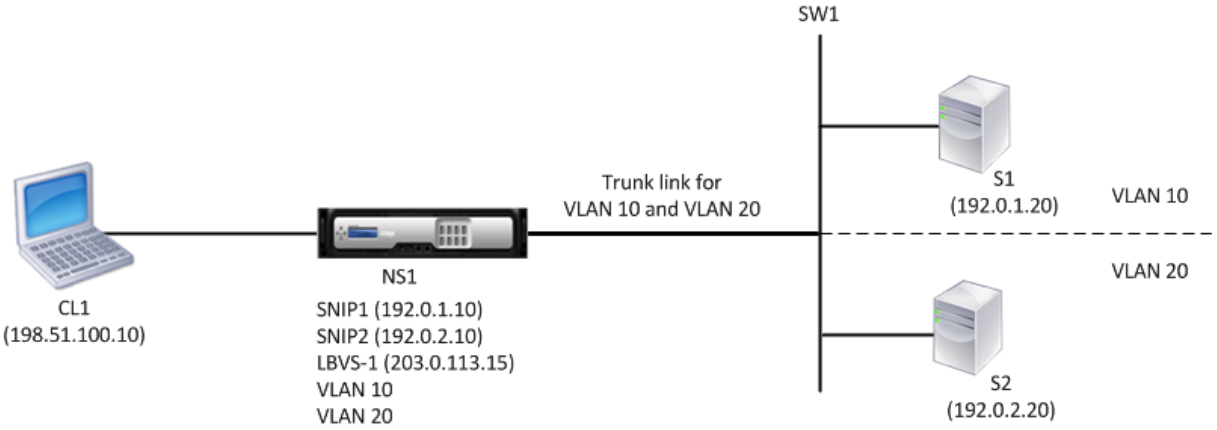
Prenons l'exemple d'une configuration d'équilibrage de charge dans laquelle le serveur virtuel d'équilibrage de charge LBVS1 sur NetScaler NS1 est utilisé pour équilibrer la charge des serveurs S1 et S2, qui sont connectés à NS1 via le commutateur L2 SW1. S1 et S2 appartiennent à des sous-réseaux différents et font partie du VLAN 10 et du VLAN20, respectivement. La liaison entre NS1 et SW1 est une liaison de jonction et est partagée par VLAN10 et VLAN20.

Pour plus d'informations sur la configuration de l'équilibrage de charge sur un NetScaler, consultez la section Équilibrage de charge.

Les adresses IP de sous-réseau SNIP1 (à des fins de référence uniquement) et SNIP2 (à des fins de référence uniquement) sont configurées sur NS1. NS1 utilise SNIP1 (sur le VLAN 10) pour communiquer avec le serveur S1 et SNIP2 (sur le VLAN 20) pour communiquer avec S2. Dès que SNIP1 et SNIP2 sont configurés, NS1 diffuse des paquets d'annonce ARP pour SNIP1 et SNIP2.

Pour plus d'informations sur la configuration des VLAN sur un NetScaler, consultez la section Configurationd'un VLAN.

Les services SVC-S1 et SVC-S2 sur NS1 représentent les serveurs S1 et S2. Dès que ces services sont configurés, NS1 diffuse les requêtes ARP les concernant. Une fois que S1 et S2 ont répondu, NS1 leur envoie des sondes de surveillance à intervalles réguliers pour vérifier leur état de santé. NS1 envoie des sondes de surveillance à S1 à partir de l'adresse SNIP1 et à S2 à partir de l'adresse SNIP2.



Voici le flux de trafic dans cet exemple :

1. Le client C1 envoie un paquet de demande à LBVS-1. Le paquet de requête a :
   - IP source = adresse IP du client (198.51.100.10)
   - IP de destination = adresse IP de LBVS-1 (203.0.113.15)

2. LBVS1 de NS1 reçoit le paquet de requête.
3. L'algorithme d'équilibrage de charge de LBVS1 sélectionne le serveur S2.
4. Comme S2 est directement connecté à NS1 et que SNIP2 (192.0.2.10) est la seule adresse IP de NS1 qui appartient au même sous-réseau que S2, NS1 ouvre une connexion entre SNIP2 et S2. Remarque : Si S1 est sélectionné, NS1 ouvre une connexion entre SNIP1 et S1.
5. NS1 envoie le paquet de demande à S2 depuis SNIP2. Le paquet de requête a :
   - IP source = SNIP1 (192.0.2.10)
   - IP de destination = adresse IP de S2 (192.0.2.20)
6. La réponse de S2 renvoie par le même chemin.

Configuration des adresses IP du site GSLB (GSLBIP)

May 5, 2023

Une adresse IP de site GSLB (GSLBIP) est une adresse IP associée à un site GSLB. Il n'est pas obligatoire de spécifier une adresse GSLBIP lors de la configuration initiale de l'appliance NetScaler. Une adresse GSLBIP n'est utilisée que lorsque vous créez un site GSLB.

Pour plus d'informations sur la création d'une adresse IP de site GSLB, consultez Global Server Load Balancing.

Supprimer une adresse IP appartenant à NetScaler

May 5, 2023

Vous pouvez supprimer n'importe quelle adresse IP à l'exception du NSIP. Le tableau suivant fournit des informations sur les processus que vous devez suivre pour supprimer les différents types d'adresses IP. Avant de supprimer un VIP, supprimez le serveur virtuel associé.

Type d'adresse IP	Implications
Adresse IP du sous-réseau (SNIP)	Si l'adresse IP supprimée est la dernière adresse IP du sous-réseau, la route associée est supprimée de la table de routage. Si l'adresse IP supprimée est la passerelle figurant dans l'entrée de route correspondante, la passerelle de cette route de sous-réseau est remplacée par une autre adresse IP appartenant à NetScaler.
Adresse IP du serveur virtuel (VIP)	Avant de supprimer un VIP, vous devez d'abord supprimer le serveur virtuel qui lui est associé. Pour plus d'informations sur la suppression du serveur virtuel, reportez-vous à la section Équilibrage de charge.
Adresse IP du site GSLB-Site-IP	Avant de supprimer une adresse IP de site GSLB, vous devez supprimer le site qui lui est associé. Pour plus d'informations sur la suppression du site, consultez Global Server Load Balancing.

Pour supprimer une adresse IP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

rm ns ip <IPaddress>

Exemple :

```
1 > rm ns ip 10.102.29.54
2 Done
3 <!--NeedCopy-->
```

Pour supprimer une adresse IP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **IP** > **IPv4S**, supprimez l'adresse IP.

Configuration des contrôles d'accès aux applications

May 5, 2023

Les contrôles d'accès aux applications, également appelés contrôles d'accès de gestion, constituent un mécanisme unifié pour gérer l'authentification des utilisateurs et mettre en œuvre des règles qui déterminent l'accès des utilisateurs aux applications et aux données. Vous pouvez configurer les SNIP pour fournir un accès aux applications de gestion. L'accès à la gestion pour le NSIP est activé par défaut et ne peut pas être désactivé. Vous pouvez toutefois le contrôler à l'aide des ACL.

Pour plus d'informations sur l'utilisation des ACL, consultez Listes de contrôle d'accès (ACL).

L'appliance NetScaler ne prend pas en charge l'accès de gestion aux VIP.

Le tableau suivant fournit un résumé de l'interaction entre l'accès à la gestion et les paramètres de service spécifiques pour Telnet.

Accès à la gestion	Telnet (état configuré sur NetScaler)	Telnet (État effectif au niveau IP)
Activer	Activer	Activer
Activer	Désactiver	Désactiver
Désactiver	Activer	Désactiver
Désactiver	Désactiver	Désactiver

Le tableau suivant fournit une vue d'ensemble des adresses IP utilisées comme adresses IP sources dans le trafic sortant.

Application/IP	NSIP	SNIP	VIP
ARP	Oui	Oui	Non
Trafic côté serveur	Non	Oui	Non
RNAT	Non	Oui	Oui
PING ICMP	Oui	Oui	Non
Routage dynamique	Oui	Oui	Oui

Le tableau suivant fournit une vue d'ensemble des applications disponibles sur ces adresses IP.

Application/IP	NSIP	SNIP	VIP
SNMP	Oui	Oui	Oui
Accès au système	Oui	Oui	Non

Vous pouvez accéder à NetScaler et le gérer à l'aide d'applications telles que Telnet, SSH, GUI et FTP.

Remarque : Telnet et FTP sont désactivés sur NetScaler pour des raisons de sécurité. Pour les activer, contactez le support client. Une fois les applications activées, vous pouvez appliquer les contrôles au niveau IP.

Pour configurer NetScaler afin qu'il réponde à ces applications, vous devez activer les applications de gestion spécifiques. Si vous désactivez l'accès à la gestion pour une adresse IP, les connexions existantes qui utilisent cette adresse IP ne sont pas interrompues, mais aucune nouvelle connexion ne peut être initiée.

De plus, les applications non liées à la gestion qui s'exécutent sur le système d'exploitation FreeBSD sous-jacent sont exposées aux attaques de protocole, et ces applications ne tirent pas parti des capacités de prévention des attaques de l'appliance NetScaler.

Vous pouvez bloquer l'accès à ces applications non liées à la gestion sur un SNIP ou un NSIP. Lorsque l'accès est bloqué, un utilisateur qui se connecte à un NetScaler à l'aide du SNIP ou du NSIP ne peut pas accéder aux applications non liées à la gestion exécutées sur le système d'exploitation sous-jacent.

Pour configurer l'accès à la gestion d'une adresse IP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

set ns ip <value**-MGMTAccesss -**telnet** -**ftp** -**gui** -**ssh** - snmp - RestrictAccess** (ACTIVÉ)**0 <value><value><value><value><value> | (**HANDICAPÉ**)

Exemple :

```
1  > set ns ip 10.102.29.54 -mgmtAccess enabled -restrictAccess ENABLED
2   Done
3 <!--NeedCopy-->
```

Pour activer l'accès de gestion à une adresse IP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP** > **IPv4S**.
2. Ouvrez une entrée d'adresse IP et sélectionnez l'option **Activer le contrôle d'accès à la gestion** pour prendre en charge les applications répertoriées.

Activez un accès sécurisé à l'interface graphique de NetScaler à l'aide d'une adresse IP de sous-réseau (SNIP)

L'accès sécurisé à l'interface graphique de NetScaler est activé par défaut pour NetScaler IP (NSIP). Vous pouvez également activer un accès sécurisé à l'appliance NetScaler à l'aide d'une adresse IP de sous-réseau de l'appliance.

Après avoir configuré une adresse SNIP pour un accès sécurisé à une paire haute disponibilité, l'accès sécurisé est disponible pour l'appliance principale, si vous accédez à l'adresse SNIP.

Procédure NetScaler CLI

Pour activer un accès sécurisé à l'interface graphique de NetScaler à l'aide d'une adresse IP de sous-réseau (SNIP) à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

set ns ip <SNIP_Address>**-type SNIP -gui SECUREONLY -MGMTaccess ACTIVÉ**

Exemple :

```
1   > set ns ip 203.0.113.99 -mgmtAccess enabled -restrictAccess ENABLED
2
3    Done
4  <!--NeedCopy-->
```

Comment NetScaler proxie les connexions

May 5, 2023

Lorsqu'un client établit une connexion, l'appliance NetScaler met fin à la connexion client, initie une connexion à un serveur approprié et envoie le paquet au serveur. L'appliance n'effectue pas cette action pour le type de service UDP ou ANY.

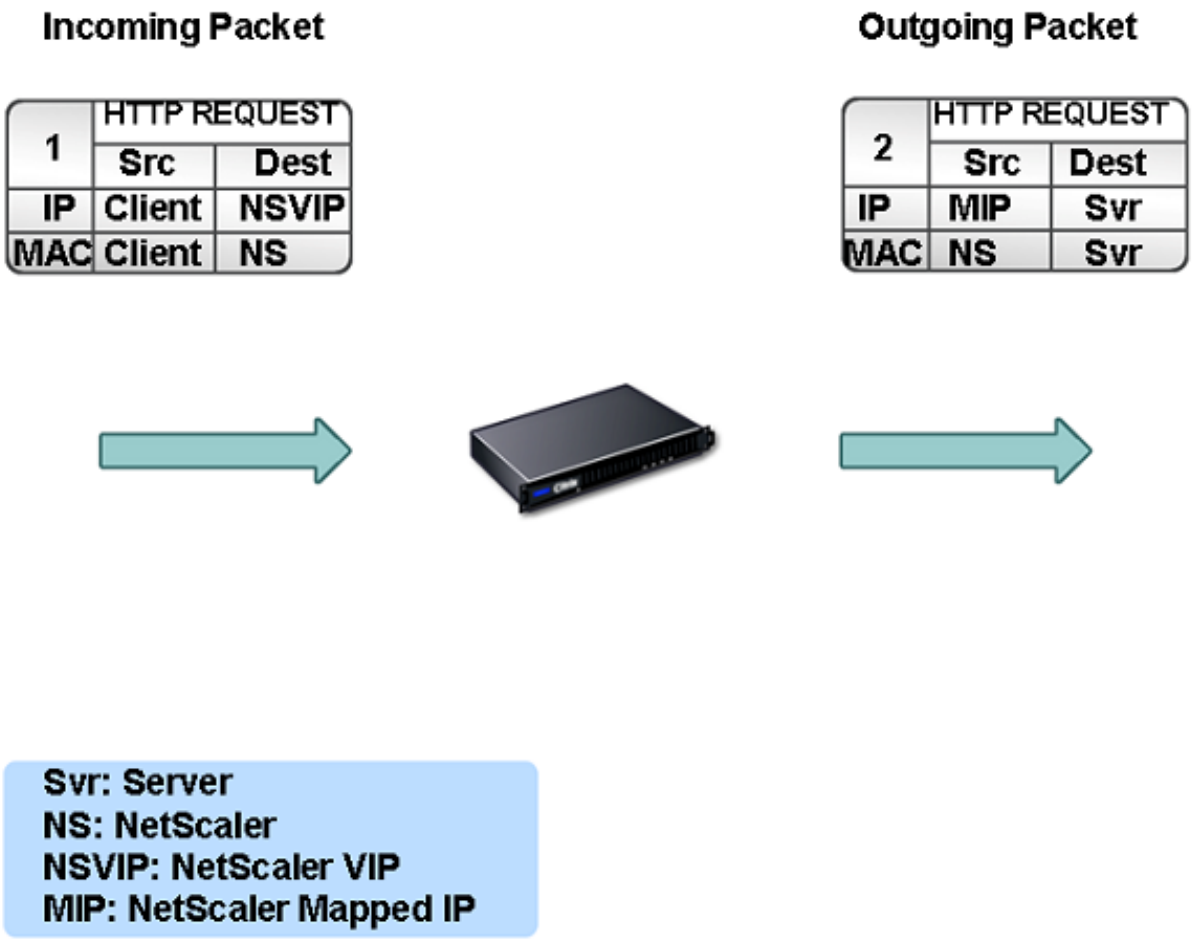
Pour plus d'informations sur les types de service, voir Équilibrage de charge.

Vous pouvez configurer NetScaler pour qu'il traite le paquet avant d'établir la connexion avec un serveur. Le comportement par défaut consiste à modifier les adresses IP source et destination d'un paquet avant de l'envoyer au serveur. Vous pouvez configurer NetScaler pour conserver l'adresse IP source des paquets en activant le mode Utiliser l'adresse IP source.

Comment l'adresse IP de destination est sélectionnée

Le trafic envoyé à l'appliance NetScaler peut être envoyé à un serveur virtuel ou à un service. L'appliance gère différemment le trafic vers les serveurs et services virtuels. NetScaler met fin au trafic reçu à l'adresse IP d'un serveur virtuel (VIP) et remplace l'adresse IP de destination par l'adresse IP du serveur avant de transférer le trafic vers le serveur, comme indiqué dans le schéma suivant.

Figure 1. Connexions proxy à des VIP



Les paquets destinés à un service sont envoyés directement au serveur approprié et NetScaler ne modifie pas les adresses IP de destination. Dans ce cas, NetScaler fonctionne comme un proxy.

Comment l'adresse IP source est sélectionnée

Lorsque l'appliance NetScaler communique avec les serveurs physiques ou les appareils homologues, elle n'utilise pas par défaut l'adresse IP du client. NetScaler gère un pool d'adresses IP de sous-réseau (SNIP) et sélectionne une adresse IP dans ce pool à utiliser comme adresse IP source d'une connexion au serveur physique. Selon le sous-réseau dans lequel le serveur physique est placé, NetScaler sélectionne une adresse SNIP spécifique.

Remarque : Si l'option Utiliser l'adresse IP source (USIP) est activée, l'appliance utilise l'adresse IP du client.

Activer le mode Utiliser l'adresse IP source

May 5, 2023

Lorsque l'appliance NetScaler communique avec les serveurs physiques ou les appareils homologues, elle utilise par défaut l'une de ses propres adresses IP comme adresse IP source. L'appliance gère un pool d'adresses IP de sous-réseau (SNIP) et sélectionne une adresse IP dans ce pool à utiliser comme adresse IP source pour une connexion au serveur physique. La décision de sélectionner une adresse SNIP dépend du sous-réseau dans lequel réside le serveur physique.

Si nécessaire, vous pouvez configurer l'appliance NetScaler pour utiliser l'adresse IP du client comme adresse IP source. Certaines applications ont besoin de l'adresse IP réelle du client. Les cas d'utilisation suivants en sont quelques exemples :

- L'adresse IP du client dans le journal d'accès Web est utilisée à des fins de facturation ou d'analyse de l'utilisation.
- L'adresse IP du client est utilisée pour déterminer le pays d'origine du client ou le fournisseur d'accès Internet d'origine du client. Par exemple, de nombreux moteurs de recherche tels que Google fournissent du contenu pertinent au lieu auquel appartient l'utilisateur.
- L'application doit connaître l'adresse IP du client pour vérifier que la demande provient d'une source fiable.
- Parfois, même si un serveur d'applications n'a pas besoin de l'adresse IP du client, un pare-feu placé entre le serveur d'applications et NetScaler peut avoir besoin de l'adresse IP du client pour filtrer le trafic.

Activez le mode USE Source IP (USIP) si vous souhaitez que NetScaler utilise l'adresse IP du client pour communiquer avec les serveurs.

La figure suivante montre comment l'appliance utilise les adresses IP en mode USIP.

Avant de commencer

Avant d'activer le mode USIP, notez les points suivants :

- Activez l'USIP dans les situations suivantes :
  - Équilibrage de charge des serveurs du système de détection d'intrusion (IDS)
  - Équilibrage de charge SMTP
  - Basculement de connexion sans état
  - Équilibrage de charge sans session
  - Si vous utilisez le mode Direct Server Return (DSR)
- Le paramètre global USIP s'applique uniquement aux services créés après la définition du paramètre global USIP. En d'autres termes, le paramètre global USIP ne s'applique pas aux services existants lorsque le paramètre global USIP est défini. Par exemple, la désactivation globale de l'USIP ne désactive pas l'USIP sur les services existants. Mais cela empêche l'activation automatique de l'USIP pour les services créés ultérieurement.

  Pour activer ou désactiver l'USIP sur un ensemble de services existants, vous devez activer ou désactiver l'USIP sur chacun de ces services.
- Lorsque l'USIP est activé, vous devez définir la passerelle du serveur sur l'une des adresses IP appartenant à NetScaler (de type Subnet IP (SNIP) afin que la réponse du serveur passe toujours par l'appliance NetScaler.
- Si vous activez l'USIP, définissez le délai d'inactivité pour les connexions au serveur à une valeur inférieure à la valeur par défaut, afin que les connexions inactives soient effacées rapidement côté serveur.
- Pour une redirection transparente du cache, si vous activez USIP, activez également L2CONN.
- Comme les connexions HTTP ne sont pas réutilisées lorsque l'USIP est activé, un grand nombre de connexions côté serveur peuvent s'accumuler. Les connexions au serveur inactives peuvent bloquer les connexions d'autres clients. Définissez donc des limites quant au nombre maximum de connexions à un service. Citrix recommande également de définir le délai d'expiration du serveur HTTP, pour un service sur lequel l'USIP est activé, à une valeur inférieure à la valeur par défaut, afin que les connexions inactives soient effacées rapidement côté serveur.
- Comme alternative au mode USIP, vous avez la possibilité d'insérer l'adresse IP du client (CIP) dans l'en-tête de demande de la connexion côté serveur pour un serveur d'applications qui a besoin de l'adresse IP du client.
- Dans les versions précédentes de NetScaler, le mode USIP offrait les options de port source suivantes pour les connexions côté serveur :
  - **Utilisez le port du client**. Avec cette option, les connexions ne peuvent pas être réutilisées. Pour chaque demande du client, une nouvelle connexion est établie avec le serveur physique.

- **Utilisez le port proxy**. Avec cette option, la réutilisation de la connexion est possible pour toutes les demandes provenant d'un même client.

Dans les versions ultérieures de NetScaler, si l'USIP est activé, la valeur par défaut est d'utiliser un port proxy pour les connexions côté serveur et de ne pas réutiliser les connexions. Le fait de ne pas réutiliser les connexions peut ne pas affecter la vitesse d'établissement des connexions.

Par défaut, l'option Utiliser le port proxy est activée si le mode USIP est activé.

Remarque : Si vous activez le mode USIP, il est recommandé d'activer l'option Utiliser le port proxy.

Pour plus d'informations sur l'option Utiliser le port proxy, voir Configurer le port source pour les connexions côté serveur.

Étapes de configuration

Activez le mode USE Source IP (USIP) si vous souhaitez que NetScaler utilise l'adresse IP du client pour communiquer avec les serveurs. Par défaut, le mode USIP est désactivé. Le mode USIP peut être activé globalement sur NetScaler ou sur un service spécifique. Si vous l'activez globalement, USIP est activé par défaut pour tous les services créés ultérieurement. Si vous activez l'USIP pour un service spécifique, l'adresse IP du client n'est utilisée que pour le trafic dirigé vers ce service.

Procédures CLI

Pour activer ou désactiver globalement le mode USIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **enable ns mode USIP**
- **disable ns mode USIP**

Pour activer le mode USIP pour un service à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

set service <name>@ -**usip** (**YES** | **NO**)

Exemple :

```
1 > set service Service-HTTP-1 -usip YES
2 Done
3 <!--NeedCopy-->
```


Procédures GUI

Pour activer globalement le mode USIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Modifier les modes**.
2. Sélectionnez l'option **Utiliser l'adresse IP source** .

Pour activer le mode USIP pour un service à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services** et modifiez un service.
2. Dans **Paramètres avancés**, sélectionnez **Paramètres du service**et sélectionnez **Utiliser l'adresse IP source**.

Configuration de la traduction d'adresses réseau

May 5, 2023

La traduction d'adresses réseau (NAT) implique la modification des adresses IP source et/ou de destination et/ou des numéros de port TCP/UDP des paquets IP qui transitent par l'appliance NetScaler. L'activation de la NAT sur l'appliance renforce la sécurité de votre réseau privé et le protège d'un réseau public tel qu'Internet, en modifiant les adresses IP sources de votre réseau lorsque les données transitent par NetScaler. De plus, à l'aide des entrées NAT, l'ensemble de votre réseau privé peut être représenté par quelques adresses IP publiques partagées. NetScaler prend en charge les types de traduction d'adresses réseau suivants :

- **NAT entrant (INAT).** NetScaler remplace l'adresse IP de destination dans les paquets générés par le client par l'adresse IP privée du serveur.
- **NAT inversé (RNAT).** NetScaler remplace l'adresse IP source dans les paquets générés par les serveurs par les adresses IP NAT publiques.

Traduction des adresses réseau entrantes

May 5, 2023

Lorsqu'un client envoie un paquet à une appliance NetScaler configurée pour la traduction d'adresses réseau entrantes (INAT), l'appliance traduit l'adresse IP de destination publique du paquet en une adresse IP de destination privée et transmet le paquet au serveur à cette adresse.

Les configurations suivantes sont prises en charge :

- Mappage**IPv4-IPv4 :**une adresse IPv4 publique sur l'appliance NetScaler écoute les demandes de connexion pour le compte d'un serveur IPv4 privé. L'appliance NetScaler traduit l'adresse IP de destination publique du paquet en adresse IP de destination du serveur. L'appliance transmet ensuite le paquet au serveur à cette adresse.
- Mappage**IPv4-IPv6** : une adresse IPv4 publique sur l'appliance NetScaler écoute les demandes de connexion pour le compte d'un serveur IPv6 privé. L'appliance NetScaler crée un paquet de requête IPv6 avec l'adresse IP du serveur IPv6 comme adresse IP de destination.
- Mappage**IPv6-IPv4 :**une adresse IPv6 publique sur l'appliance NetScaler écoute les demandes de connexion pour le compte d'un serveur IPv4 privé. L'appliance NetScaler crée un paquet de requête IPv4 avec l'adresse IP du serveur IPv4 comme adresse IP de destination.
- Mappage**IPv6-IPv6** : une adresse IPv6 publique sur l'appliance NetScaler écoute les demandes de connexion pour le compte d'un serveur IPv6 privé. L'appliance NetScaler traduit l'adresse IP de destination publique du paquet en adresse IP de destination du serveur. L'appliance transmet ensuite le paquet au serveur à cette adresse.

Lorsque l'appliance transmet un paquet à un serveur, l'adresse IP source attribuée au paquet est déterminée comme suit :

- Si le mode Utiliser l'adresse IP du sous-réseau (USNIP) est activé et que le mode Utiliser l'adresse IP source (USIP) est désactivé, l'appliance utilise une adresse IP de sous-réseau (SNIP) comme adresse IP source.
- Si le mode USIP est activé et que le mode USNIP est désactivé, l'appliance utilise l'adresse IP du client (CIP) comme adresse IP source.
- Si les modes USIP et USNIP sont activés, le mode USIP est prioritaire.
- Vous pouvez également configurer NetScaler pour qu'il utilise une adresse IP unique comme adresse IP source, en définissant le paramètre ProxyIP.
- Si aucun des modes ci-dessus n'est activé et qu'aucune adresse IP unique n'a été spécifiée, NetScaler tente d'utiliser un MIP comme adresse IP source.
- Si les modes USIP et USNIP sont activés et qu'une adresse IP unique a été spécifiée, l'ordre de priorité est le suivant : USIP-Unique IP-USNIP-MIP-Error.

Pour protéger NetScaler des attaques DoS, vous pouvez activer le proxy TCP. Toutefois, si d'autres mécanismes de protection sont utilisés sur votre réseau, vous pouvez les désactiver.

Configurer les règles INAT

Vous pouvez créer, modifier ou supprimer une entrée INAT.

Procédures CLI

Pour créer une entrée INAT à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une entrée INAT et vérifier sa configuration :

- **add inat** <name><publicIP><privateIP>[-**tcpproxy** (**ACTIVÉ** | **DÉSACTIVÉ**)] [-**ftp (ACTIVÉ | DÉSACTIVÉ)] [-**usip** (0 1 ACTIVÉ 2 | DÉSACTIVÉ 3)] [- 4 usnip 5 6 (7 ACTIVÉ 8 | 9 DÉSACTIVÉ 0)] [- 1 2 ProxyIP \ < 3 4 ip_addr > 5 6 ipv6_addr>] 7 8**********
- **afficher dans** <name>[\]

Exemple :

```
> add inat ip4-ip4 172.16.1.2 192.168.1.1 -proxyip 10.102.29.171
 Done
<!--NeedCopy-->
```

Pour modifier une entrée INAT à l'aide de l'interface de ligne de commande :

Pour modifier une entrée INAT, tapez la `set inat` commande, le nom de l'entrée et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour supprimer une configuration INAT à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **m. inat** <name>

Exemple :

```
> rm inat ip4-ip4
 Done
<!--NeedCopy-->
```

Procédures GUI

Pour configurer une entrée INAT à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Routes** > **INAT**, puis ajoutez une entrée INAT ou modifiez une entrée INAT existante.

Pour supprimer une configuration INAT à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Routes** > **INAT**, supprimez la configuration INAT.

Basculement de connexion pour les règles INAT

Le basculement des connexions ou la mise en miroir des connexions permettent au nœud principal de dupliquer les informations de connexion et de persistance avec le nœud secondaire dans le cadre

d'une haute disponibilité. Les informations d'état de la connexion sont partagées régulièrement avec le nœud secondaire lorsque la mise en miroir des connexions est activée.

L'activation du basculement de connexion offre une plus grande fiabilité, mais cela se fait au prix d'une perte de temps du système pour partager les informations d'état. Les données de connexion sont synchronisées avec l'unité de secours à chaque mise à jour de l'état du paquet ou du flux. Il ne doit donc être utilisé qu'aux endroits où la fiabilité du niveau de connexion est primordiale.

Les configurations de haute disponibilité de l'appliance NetScaler prennent en charge le basculement des connexions pour les connexions INAT. Le nœud principal envoie des mappages INAT et d'autres informations de connexion liées à l'INAT au nœud secondaire à intervalles réguliers. L'appliance secondaire utilise les informations de mappage et de connexion uniquement en cas de basculement.

Lorsqu'un basculement se produit, le nouveau nœud principal dispose d'informations sur les connexions INAT établies avant le basculement. Par conséquent, il continue à desservir ces connexions même après le basculement.

Du point de vue du client, le basculement est transparent. Pendant la période de transition, le client et le serveur peuvent rencontrer une brève interruption et retransmissions. Le basculement de connexion peut être activé conformément à la règle INAT.

Pour activer le basculement de connexion sur une règle INAT, vous activez le `connFailover` paramètre de cette règle RNAT spécifique à l'aide de l'interface de ligne de commande.

Procédure CLI

Pour activer le basculement de connexion pour une règle INAT à l'aide de l'interface de ligne de commande :

Pour activer le basculement de connexion lors de l'ajout d'une règle INAT, tapez à l'invite de commandes :

- **add inat[-**tcpproxy** (**ACTIVÉ** | **DÉSACTIVÉ**)] [-**ftp (ACTIVÉ | DÉSACTIVÉ)] [-**usip** (0 ACTIVÉ 1 | 2 DÉSACTIVÉ 3)] [- 4 usnip 5 (6 ACTIVÉ 7 | 8 DÉSACTIVÉ 9)] [- 0 1 ProxyIP \ 2 3 4 5 6 <ip_addr|ipv6_addr>] - connfailover (**<name><publicIP><privateIP**** ACTIVÉ | **DÉSACTIVÉ**) **********
- **montrer inat** <name>

Pour activer le basculement de connexion lors de la modification d'une règle INAT existante, à l'invite de commandes, tapez :

- **set inat -connfailover (ACTIVÉ | DÉSACTIVÉ**)**
- **montrer inat** <name>

Coexistence de l'INAT et des serveurs virtuels

May 5, 2023

Si INAT et RNAT sont configurés, la règle INAT est prioritaire sur la règle RNAT. Si le RNAT est configuré avec une adresse IP de traduction d'adresses réseau (IP NAT), l'adresse IP NAT est sélectionnée comme adresse IP source pour ce client RNAT.

L'adresse IP de destination publique par défaut dans une configuration INAT est l'adresse IP virtuelle (VIP) de l'appareil NetScaler. Les serveurs virtuels utilisent également des VIP. Lorsque l'INAT et un serveur virtuel utilisent la même adresse IP, la configuration Vserver remplace la configuration INAT.

Vous trouverez ci-dessous quelques exemples de scénarios de configuration et leurs effets.

Étui	Résultat
Vous avez configuré un serveur virtuel et un service pour envoyer directement au serveur tous les paquets de données reçus sur un port NetScaler spécifique. Vous avez également configuré INAT et activé TCP. En configurant INAT de cette manière, tous les paquets de données reçus via un moteur TCP sont envoyés avant de les envoyer au serveur.	Tous les paquets reçus sur NetScaler, à l'exception de ceux reçus sur le port spécifié, passent par le moteur TCP.
Vous avez configuré un serveur virtuel et un service pour envoyer tous les paquets de données de type de service TCP, reçus sur un port spécifique de NetScaler, au serveur après leur passage par le moteur TCP. Vous avez également configuré INAT et désactivé TCP. En configurant INAT de cette manière, les paquets de données reçus sont envoyés directement au serveur.	Seuls les paquets reçus sur le port spécifié transitent par le moteur TCP.
Vous avez configuré un serveur virtuel et un service pour envoyer tous les paquets de données reçus à l'un des deux serveurs. Vous essayez de configurer INAT pour envoyer tous les paquets de données reçus à un autre serveur.	La configuration INAT n'est pas autorisée.

Étui	Résultat
Vous avez configuré INAT pour envoyer tous les paquets de données reçus directement à un serveur. Vous essayez de configurer un serveur virtuel et un service pour envoyer tous les paquets de données reçus à deux serveurs différents.	La configuration du vserver n'est pas autorisée.

Apatride NAT46

May 5, 2023

La fonction Stateless NAT46 permet la communication entre les réseaux IPv4 et IPv6 via la traduction de paquets IPv4 vers IPv6, et vice versa, sans conserver aucune information de session sur l'appliance NetScaler.

Pour une configuration NAT46 sans état, l'appliance traduit un paquet IPv4 en IPv6 ou un paquet IPv6 en IPv4, comme défini dans les RFC 6145 et 2765.

Une configuration NAT46 sans état sur l'appliance NetScaler comporte les composants suivants :

- **Entrée INAT IPv4-IPv6.** Entrée INAT définissant une relation 1:1 entre une adresse IPv4 et une adresse IPv6. En d'autres termes, une adresse IPv4 de l'appliance écoute les demandes de connexion pour le compte d'un serveur IPv6. Un paquet de requête IPv4 pour cette adresse IPv4 est traduit en paquet IPv6, puis le paquet IPv6 est envoyé au serveur IPv6.

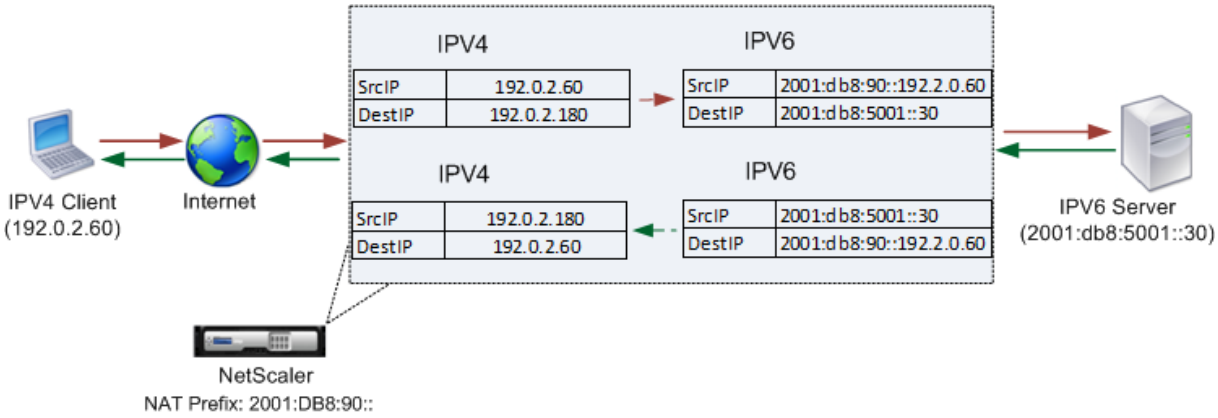
  L'appliance traduit un paquet de réponse IPv6 en un paquet de réponse IPv4 avec son champ d'adresse IP source défini comme l'adresse IPv4 spécifiée dans l'entrée INAT. Le paquet traduit est ensuite envoyé au client.

- **Préfixe IPv6 NAT46.** Préfixe IPv6 global de longueur 96 bits (128-32=96) configuré sur l'appliance. Lors de la traduction d'un paquet IPv4 vers un paquet IPv6, l'appliance définit l'adresse IP source du paquet IPv6 traduit selon une concaténation du préfixe IPv6 NAT46 [96 bits] et de l'adresse source IPv4 [32 bits] qui a été reçue dans le paquet de demande.

  Lors de la traduction de paquets IPv6 vers IPv4, l'appliance définit l'adresse IP de destination du paquet IPv4 traduit sur les 32 derniers bits de l'adresse IP de destination du paquet IPv6.

Prenons l'exemple d'une entreprise hébergeant le site www.example.com sur le serveur S1, qui possède une adresse IPv6. Pour permettre la communication entre les clients IPv4 et le serveur IPv6 S1, l'appliance NetScaler NS1 est déployée avec une configuration NAT46 sans état qui inclut une entrée

INAT IPv4-IPv6 pour le serveur S1 et un préfixe NAT46. L'entrée INAT inclut une adresse IPv4 à laquelle l'appliance écoute les demandes de connexion des clients IPv4 pour le compte du serveur IPv6 S1.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple :

Entités	Nom	Valeur
Adresse IP du client	Client_IPv4 (à titre de référence uniquement)	192.0.2.60
Adresse IPv6 du serveur	SEVR_IPv6 (à des fins de référence uniquement)	2001:DB8:5001::30
Adresse IPv4 définie dans l'entrée INAT pour le serveur IPv6 S1	MAP-SEVR-IPv4 (à titre de référence uniquement)	192.0.2.180
Préfixe IPv6 pour la traduction en NAT 46	NAT46_Prefix (à titre de référence uniquement)	2001:DB8:90::

Voici le flux de trafic dans cet exemple :

1. Le client IPv4 CL1 envoie un paquet de demande à l'adresse MAP-SEVR-IPv4 (192.0.2.180) sur l'appliance NetScaler.
2. L'appliance reçoit le paquet de demande et recherche dans les entrées INAT NAT46 l'adresse IPv6 mappée à l'adresse MAP-SEVR-IPv4 (192.0.2.180). Il trouve l'adresse SEVR-IPv6 (2001:DB 8:5001 : :30).
3. L'appliance crée un paquet de requête IPv6 traduit avec :
   - Champ d'adresse IP de destination = SEVR-IPv6 = 2001:DB 8:5001::30
   - Champ d'adresse IP source = Concaténation du préfixe NAT (96 premiers bits) et de Client_IPv4 (32 derniers bits) = 2001:DB 8:90 : :192.0.2.60
4. L'appliance envoie la demande IPv6 traduite à SEVR-IPv6.
5. Le serveur IPv6 S1 répond en envoyant un paquet IPv6 à l'appliance NetScaler avec :

- Champ d'adresse IP de destination = Concaténation du préfixe NAT (96 premiers bits) et de Client_IPv4 (32 derniers bits) = 2001:DB 8:90 : :192.0.2.60
- Champ d'adresse IP source = SEVR-IPv6 = 2001:DB 8:5001::30

6. L'appliance reçoit le paquet de réponse IPv6 et vérifie que son adresse IP de destination correspond au préfixe NAT46 configuré sur l'appliance. Comme l'adresse de destination correspond au préfixe NAT46, l'appliance recherche dans les entrées INAT NAT46 l'adresse IPv4 associée à l'adresse SEVR-IPv6 (2001:DB 8:5001 : :30). Il trouve l'adresse MAP-SEVR-IPv4 (192.0.2.180).
7. L'appliance crée un paquet de réponse IPv4 avec :
   - Champ d'adresse IP de destination = Le préfixe NAT46 supprimé de l'adresse de destination de la réponse IPv6 = Client_IPv4 (192.0.2.60)
   - Champ d'adresse IP source = adresse MAP-SEVR-IPv4 (192.0.2.180)
8. L'appliance envoie la réponse IPv4 traduite au client CL1.

Limites de Stateless NAT46

Les limitations suivantes s'appliquent aux personnes apatrides NAT46 :

- La traduction des options IPv4 n'est pas prise en charge.
- La traduction des en-têtes de routage IPv6 n'est pas prise en charge.
- La traduction des en-têtes d'extension saut par saut des paquets IPv6 n'est pas prise en charge.
- La traduction des en-têtes ESP et EH des paquets IPv4 n'est pas prise en charge.
- La traduction de paquets de multidiffusion n'est pas prise en charge.
- La traduction des en-têtes des options de destination et des en-têtes de routage source n'est pas prise en charge.
- La traduction de paquets UDP IPv4 fragmentés ne contenant pas de somme de contrôle UDP n'est pas prise en charge.

Configurer Stateless NAT46

La création des entités requises pour une configuration NAT46 statique sur l'appliance NetScaler implique les procédures suivantes :

1. Créez une entrée INAT de mappage IPv4-IPv6 avec le mode sans état activé.
2. Créez un préfixe IPv6 NAT46.

Procédures CLI

Pour configurer une entrée de mappage INAT à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter inat <name><publicIPv4><privateIPv6>-mode STATELESS

- montrer inat <name>

Pour créer un préfixe NAT46 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- définir le préfixe inatparam -NAT46v6 <ipv6_addr|*>
- montrer inatparam

Exemple :

```
 > add inat exmpl-com-stls-nat46 192.0.2.180
2001:DB8:5001::30 -mode stateless
Done

> set inatparam -nat46v6Prefix 2001:DB8:90::/96
Done
<!--NeedCopy-->
```

Procédures GUI

Pour créer une entrée de mappage INAT à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > Itinéraires > INAT.
2. Ajoutez une nouvelle entrée INAT ou modifiez une entrée INAT existante.
3. Définissez les paramètres suivants :
   - Nom*
   - Adresse IP publique*
   - Adresse IP privée* (Cochez la case IPv6 et entrez l'adresse au format IPv6.)
   - Mode (sélectionnez Stateless dans la liste déroulante.)

   * Un paramètre obligatoire

Pour créer un préfixe NAT46 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Configurer les paramètres INAT**et définissez le paramètre **Préfixe** .

Définition des paramètres globaux pour Stateless NAT46

L'appliance fournit certains paramètres globaux facultatifs pour les configurations NAT46 sans état.

Pour définir les paramètres globaux du NAT46 sans état à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set inatparam** <positive_integer>[-**Nat46Ignoretos** (**OUI** | **NON**)] [-**Nat46ZeroChecksum (ACTIVÉ | DÉSACTIVÉ)] [- Nat46v6MTU \] [-**Nat46FragHeader** (0 1 ACTIVÉ 2 | DÉSACTIVÉ 3)] 4 5 6 7 8 9 0 ********
- **montrer inatparam**

Exemple :

```
> set inatparam -nat46IgnoreTOS YES -nat46ZeroCheckSum DISABLED -
    nat46v6Mtu 1400 -nat46FragHeader DISABLED
 Done
<!--NeedCopy-->
```

Pour définir les paramètres globaux pour Stateless NAT46 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Configurer les paramètres INAT**.

DNS64

May 5, 2023

La fonctionnalité NetScaler DNS64 répond par un enregistrement DNS AAAA synthétisé à un client IPv6 qui envoie une requête AAAA pour un domaine IPv4 uniquement. La fonctionnalité DNS64 est utilisée avec la fonction NAT64 pour permettre une communication fluide entre les clients uniquement IPv6 et les serveurs uniquement IPv6. Le DNS64 permet la découverte du domaine IPV4 par les clients IPV6 uniquement, tandis que NAT64 permet la communication entre les clients et les serveurs.

Pour synthétiser un enregistrement AAAA, l'appliance NetScaler récupère un enregistrement DNS A à partir d'un serveur DNS. Le préfixe DNS64 est un préfixe IPv6 96 bits configuré sur l'appliance NetScaler. L'appliance NetScaler synthétise l'enregistrement AAAA par concaténation du préfixe DNS64 (96 bits) et de l'adresse IPv4 (32 bits).

Pour permettre la communication entre les clients IPv6 et les serveurs IPv4, une appliance NetScaler avec configuration DNS64 et NAT64 peut être déployée côté client IPv6 ou côté serveur IPv4. Dans les deux cas, la configuration DNS64 de l'appliance NetScaler est similaire et inclut un serveur virtuel d'équilibrage de charge faisant office de serveur proxy pour les serveurs DNS. Si l'appliance NetScaler est déployée côté client, le serveur virtuel d'équilibrage de charge doit être spécifié, sur le client IPv6, en tant que serveur de noms pour un domaine.

Prenons un exemple dans lequel une appliance NetScaler avec une configuration DNS64 et NAT64 est configurée côté IPv4. Dans cet exemple, une entreprise héberge le site www.example.com sur le serveur S1, qui possède une adresse IPv4. Pour permettre la communication entre les clients IPv6

et le serveur IPv4 S1, l'appliance NetScaler NS1 est déployée avec une configuration DNS64 et NAT64 dynamique.

La configuration DNS64 inclut le serveur virtuel d'équilibrage de charge DNS LBVS-DNS64-1, sur lequel l'option DNS64 est activée. Une politique DNS64 nommée DNS64-Policy-1 et une action DNS64 associée nommée DNS64-Action-1 sont également configurées sur NS1, et DNS64-Policy-1 est lié à LBVS-DNS64-1. LBVS-DNS64-1 agit comme un serveur proxy DNS pour les serveurs DNS DNS-1 et DNS-2.

Lorsque le trafic arrivant sur LBVS-DNS64-1 répond aux conditions spécifiées dans DNS64-Policy-1, le trafic est traité conformément aux paramètres de DNS64-Action-1. DNS64-Action-1 spécifie le préfixe DNS64 utilisé, avec l'enregistrement A reçu d'un serveur DNS, pour synthétiser un enregistrement AAAA.

Le paramètre DNS global cacherecords est activé sur l'appliance NetScaler, de sorte que l'appliance met en cache les enregistrements DNS. Ce paramètre est nécessaire pour que le DNS64 fonctionne correctement.

Le tableau suivant répertorie les paramètres utilisés dans l'exemple ci-dessus : exemples de paramètres DNS64.

Voici le flux de trafic dans cet exemple :

1. Le client IPv6 CL1 envoie une requête DNS AAAA pour l'adresse IPv6 du site www.example.com.
2. La demande est reçue par le serveur virtuel d'équilibrage de charge DNS LBVS-DNS64-1 sur l'appliance NetScaler NS1.
3. NS1 vérifie ses enregistrements de cache DNS pour l'enregistrement AAAA demandé et constate que cet enregistrement AAAA pour le site www.example.com n'existe pas dans le cache DNS.
4. L'algorithme d'équilibrage de charge de LBVS-DNS64-1 sélectionne le serveur DNS DNS-1 et lui transmet la requête AAAA.
5. Le site www.example.com étant hébergé sur un serveur IPv4, le serveur DNS DNS-1 ne possède aucun enregistrement AAAA pour le site www.example.com.
6. DNS-1 envoie soit une réponse DNS AAAA vide, soit un message d'erreur à LBVS-DNS64-1.
7. Étant donné que l'option DNS64 est activée sur LBVS-DNS64-1 et que la requête AAAA de CL1 correspond à la condition spécifiée dans DNS64-Policy-1, NS1 envoie une demande DNS A à DNS-1 pour l'adresse IPv4 de www.example.com.
8. DNS-1 répond en envoyant l'enregistrement DNS A pour www.example.com à LBVS-DNS64-1. L'enregistrement A inclut l'adresse IPv4 de www.example.com.
9. NS1 synthétise un enregistrement AAAA pour le site www.example.com avec :
    - Adresse IPv6 pour le site www.example.com = Concaténation du préfixe DNS64 (96 bits) spécifié dans le DNS64Action associé et de l'adresse IPv4 de l'enregistrement DNS A (32 bits) = 2001:DB 8:300 : :192.0.2.60
10. NS1 envoie l'enregistrement AAAA synthétisé au client IPv6 CL1. NS1 met également en cache l'enregistrement A dans sa mémoire. NS1 utilise l'enregistrement A mis en cache pour synthétiser les enregistrements AAAA pour les demandes AAAA suivantes.

Points à prendre en compte pour une configuration DNS64

Avant de configurer DNS64 sur une appliance NetScaler, tenez compte des points suivants :

- La fonctionnalité DNS64 de l'appliance NetScaler est conforme à la norme RFC 6174.
- La fonctionnalité DNS64 de l'appliance NetScaler ne prend pas en charge le protocole DNSSEC. L'appliance NetScaler ne synthétise pas un enregistrement AAAA à partir d'une réponse DNSSEC reçue d'un serveur DNS. Une réponse est classée comme une réponse DNSSEC uniquement si elle contient des enregistrements RRSIG.
- L'appliance NetScaler prend en charge le préfixe DNS64 d'une longueur de 96 bits seulement.
- Bien que la fonctionnalité DNS64 soit utilisée avec la fonctionnalité NAT64, les configurations DNS64 et NAT64 sont indépendantes de l'appliance NetScaler. Pour un flux particulier, vous devez spécifier la même valeur de préfixe IPv6 pour le préfixe DNS64 et les paramètres de préfixe NAT64, de sorte que les adresses IPv6 synthétisées reçues par le client soient routées vers la configuration NAT64 particulière. Pour plus d'informations sur la configuration de NAT64 sur une appliance NetScaler, consultez Stateful NAT64.
- Les différents cas de traitement DN64 par l'appliance NetScaler sont les suivants :
  - Si la réponse AAAA du serveur DNS inclut des enregistrements AAAA, chaque enregistrement de la réponse est vérifié pour l'ensemble de règles d'exclusion configuré sur l'appliance NetScaler pour la configuration DNS64 particulière. NetScaler supprime les adresses IPv6, dont le préfixe correspond à la règle d'exclusion, de la réponse. Si la réponse obtenue inclut au moins un enregistrement IPv6, l'appliance NetScaler transmet cette réponse au client. Sinon, l'appliance synthétise une réponse AAAA à partir de l'enregistrement A du domaine et l'envoie au client IPv6.
  - Si la réponse AAAA du serveur DNS est une réponse vide, l'appliance demande des enregistrements de ressource A portant le même nom de domaine ou recherche dans ses propres enregistrements si l'appliance est un serveur de noms de domaine authentique pour le domaine. Si la demande aboutit à une réponse vide ou à une erreur, celle-ci est transmise au client.
  - Si la réponse du serveur DNS inclut RCODE=1 (erreur de format), l'appliance NetScaler transmet la même information au client. S'il n'y a pas de réponse avant l'expiration du délai, l'appliance NetScaler envoie une réponse avec RCODE=2 (panne du serveur) au client.
  - Si la réponse du serveur DNS inclut un CNAME, la chaîne est suivie jusqu'à ce que l'enregistrement A ou AAAA final soit atteint. Si le CNAME ne possède aucun enregistrement de ressource AAAA, l'appliance NetScaler récupère l'enregistrement DNS A à utiliser pour synthétiser l'enregistrement AAAA. La chaîne CNAME est ajoutée à la section de réponse avec l'enregistrement AAAA synthétisé, puis envoyée au client.

- La fonctionnalité DNS64 de l'appliance NetScaler permet également de répondre aux demandes PTR. Lorsqu'une demande PTR pour un domaine d'une adresse IPv6 est reçue sur l'appliance et que l'adresse IPv6 correspond à l'un des préfixes DNS64 configurés, l'appliance crée un enregistrement CNAME mappant le domaine IP6-ARPA à l'IN-ADDR correspondant. Le domaine ARPA et le nouveau domaine IN-ADDR.ARPA sont utilisés pour la résolution. L'appliance recherche les enregistrements PTR locaux et, s'ils ne sont pas présents, elle envoie une demande PTR pour le domaine IN-ADDR.ARPA au serveur DNS. L'appliance NetScaler utilise la réponse du serveur DNS pour synthétiser la réponse à la demande PTR initiale.

Étapes de configuration

La création des entités requises pour une configuration NAT64 dynamique sur l'appliance NetScaler implique les procédures suivantes :

- **Ajoutez des services DNS.** Les services DNS sont une représentation logique des serveurs DNS pour lesquels l'appliance NetScaler fait office de serveur proxy DNS. Pour plus d'informations sur la définition des paramètres facultatifs d'un service, voir Équilibrage de charge.
- **Ajouter une action DNS64 et une stratégie DNS64, puis liez l'action DNS64 à la stratégie DNS64.** Une politique DNS64 spécifie les conditions à mettre en correspondance avec le trafic pour le traitement DNS64 conformément aux paramètres de l'action DNS64 associée. L'action DNS64 spécifie le préfixe DNS64 obligatoire et les paramètres facultatifs de la règle d'exclusion et des règles mappées.
- **Créez un serveur virtuel d'équilibrage de charge DNS et liez-y les services DNS et la politique DNS64.** Le serveur virtuel d'équilibrage de charge DNS agit comme un serveur proxy DNS pour les serveurs DNS représentés par les services DNS liés. Le trafic arrivant sur le serveur virtuel est mis en correspondance avec la stratégie DNS64 liée pour le traitement DNS64. Pour plus d'informations sur la définition des paramètres facultatifs d'un serveur virtuel d'équilibrage de charge, voir Équilibrage de charge.

  Remarque : l'interface de ligne de commande comporte des commandes distinctes pour ces deux tâches, mais l'interface graphique les combine dans une seule boîte de dialogue.

  Activez la mise en cache des enregistrements DNS. Activez le paramètre global pour que l'appliance NetScaler mette en cache les enregistrements DNS, qui sont obtenus via des opérations de proxy DNS. Pour plus d'informations sur l'activation de la mise en cache des enregistrements DNS, voir Système de noms de domaine.

Procédures CLI

Pour créer un service de type DNS à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter un service <name><IP><serviceType><port>…

Pour créer une action DNS64 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <expression><expression>ajouter le <actionName>préfixe DNS action64 <ipv6_addr|*> [-MappedRule \] [-ExcludeRule \]

Pour créer une stratégie DNS64 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <expression>ajouter une politique DNS 64 <name>-rule -action <string>

Pour créer un serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter lb vserver <name>DNS <IPAddress><port>-dns64 (ACTIVÉ | DÉSACTIVÉ) [-BypassAAA (OUI | NON)]…

Pour lier les services DNS et la stratégie DNS64 au serveur virtuel d'équilibrage de charge DNS à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <name><serviceName>lier lb vserver…
- <string><positive_integer>bind lb vserver <name>-PolicyName -priority…

Procédures GUI

Pour créer un service de type DNS à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Services, puis ajoutez un nouveau service.
2. Définissez les paramètres suivants :
   - Nom du service*
   - Serveur*
   - Protocole* (Sélectionnez DNS dans la liste déroulante.)
   - Port*

Pour créer une action DNS64 à l'aide de l'interface graphique :

Accédez à Gestion du trafic > DNS > Actions. Dans l'onglet DNS Actions64, ajoutez une nouvelle action DNS64.

Pour créer une politique DNS64 à l'aide de l'interface graphique :

Accédez à Gestion du trafic > DNS > Politiques. Dans l'onglet Politiques DNS 64, ajoutez une nouvelle politique DNS64.

Pour créer un serveur virtuel d'équilibrage de charge DNS et y lier les services DNS et la politique DNS64 à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels, puis ajoutez un nouveau serveur virtuel.
2. Définissez les paramètres suivants :
   - Nom*
   - Adresse IP*
   - Protocole* (Sélectionnez DNS dans la liste déroulante.)
   - Port*
3. Sélectionnez l'option Activer DNS64.
4. Dans le volet Services, liez le service au serveur virtuel.
5. Dans le volet Politiques, liez la politique au serveur virtuel.

Exemple de configuration

```
 > add service SVC-DNS-1 203.0.113.50 DNS 53
 Done

> add service SVC-DNS-2 203.0.113.60 DNS 53
 Done

> add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
 Done

> add dns Policy64 DNS64-Policy-1 -rule "CLIENT.IPv6.SRC.IN_SUBNET
   (2001:DB8:5001::/64)"
-action DNS64-Action-1
 Done

> add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
 Done

> bind lb vserver LBVS-DNS64-1 SVC-DNS-1
 Done

> bind lb vserver LBVS-DNS64-1 SVC-DNS-2
 Done

> bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
 Done

<!--NeedCopy-->
```


Traduction NAT64 avec état

May 9, 2023

La fonctionnalité dynamique NAT64 permet la communication entre les clients IPv6 et les serveurs IPv4 via la traduction de paquets IPv6 vers IPv4, et vice versa, tout en conservant les informations de session sur l'appliance NetScaler.

Une configuration NAT64 dynamique sur l'appliance NetScaler comporte les composants suivants :

- **Règle NAT64** : entrée composée d'une règle ACL6 et d'un netprofile, qui consiste en un pool d'adresses SNIP appartenant à NetScaler.
- Préfixe**IPv6 NAT64 : préfixe**IPv6 global d'une longueur de 96 bits (128-32=96) configuré sur l'appliance.
  Remarque : Actuellement, l'appliance NetScaler ne prend en charge qu'un seul préfixe à utiliser couramment avec toutes les règles NAT 64.

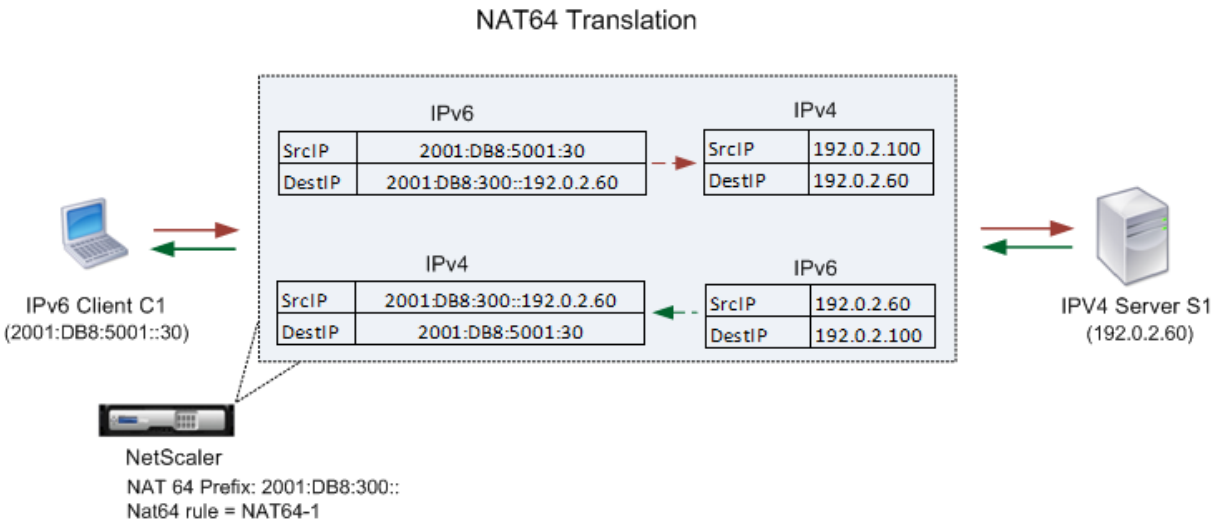
L'appliance NetScaler considère un paquet IPv6 entrant pour la traduction NAT64 lorsque toutes les conditions suivantes sont remplies :

- Le paquet IPv6 entrant correspond à la règle ACL6 liée à une règle NAT64.
- L'adresse IP de destination du paquet IPv6 correspond au préfixe IPv6 NAT64.

Lorsqu'un paquet de requête IPv6 reçu par l'appliance NetScaler correspond à un ACL6 défini dans une règle NAT64 et que l'adresse IP de destination du paquet correspond au préfixe IPv6 NAT64, l'appliance NetScaler considère le paquet IPv6 à traduire.

L'appliance traduit ce paquet IPv6 en un paquet IPv4 dont l'adresse IP source correspond à l'une des adresses IP liées au profil réseau défini dans la règle NAT64, et une adresse IP de destination composée des 32 derniers bits de l'adresse IPv6 de destination du paquet de requête IPv6. L'appliance NetScaler crée une session NAT64 pour ce flux particulier et transmet le paquet au serveur IPv4. Les réponses ultérieures du serveur IPv4 et les demandes du client IPv6 sont traduites en conséquence par l'appliance, sur la base des informations de la session NAT64 en question.

Prenons l'exemple d'une entreprise hébergeant le site www.example.com sur le serveur S1, qui possède une adresse IPv4. Pour permettre la communication entre les clients IPv6 et le serveur IPv4 S1, l'appliance NetScaler NS1 est déployée avec une configuration NAT64 dynamique qui inclut une règle NAT64 et un préfixe NAT64. Une adresse IPv6 mappée du serveur S1 est formée en concaténant le préfixe IPv6 NAT64 [96 bits] et l'adresse source IPv4 [32 bits]. Cette adresse IPv6 mappée est ensuite configurée manuellement dans les serveurs DNS. Les clients IPv6 obtiennent l'adresse IPv6 mappée à partir des serveurs DNS pour communiquer avec le serveur IPv4 S1.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple : exemples de paramètres de traduction NAT64 avec état.

Voici le flux de trafic dans cet exemple :

1. Le client IPv6 CL1 envoie un paquet de requête à l'adresse MAP-SEVR-IPv6 (2001:DB 8:300 : :192.0.2.60).
2. L'appliance NetScaler reçoit le paquet de demande. Si le paquet de demande correspond à l'ACL6 défini dans la règle NAT64 et que l'adresse IP de destination du paquet correspond au préfixe IPv6 NAT64, NetScaler considère le paquet IPv6 pour la traduction.
3. L'appliance crée un paquet de requête IPv4 traduit avec :
   - Champ d'adresse IP de destination contenant le préfixe NAT64 supprimé de l'adresse de destination de la requête IPv6 (SEVR_IPv4 = 192.0.2.60)
   - Champ d'adresse IP source contenant l'une des adresses IPv4 liées à Netprofile-1 (dans ce cas, 192.0.2.100)
4. L'appliance NetScaler crée une session NAT64 pour ce flux et envoie la demande IPv4 traduite au serveur S1.
5. Le serveur IPv64 S1 répond en envoyant un paquet IPv4 à l'appliance NetScaler avec :
   - Champ d'adresse IP de destination contenant 192.0.2.100
   - Champ d'adresse IP source contenant l'adresse du SEVR_IPv4 (192.0.2.60)
6. L'appliance reçoit le paquet de réponse IPv4, recherche toutes les entrées de session et constate que le paquet de réponse IPv6 correspond à l'entrée de session NAT64 créée à l'étape 4. L'appliance prend en compte le paquet IPv4 pour la traduction.
7. L'appliance crée un paquet de réponse IPv6 traduit avec :
   - Champ d'adresse IP de destination = Client_IPV6=2001:DB 8:5001 : :30

- Champ d'adresse IP source = Concaténation du préfixe NAT64 (96 premiers bits) et de SEVR_IPv4 (32 derniers bits) =2001:DB 8:300 : :192.0.2.60

8. L'appliance envoie la réponse IPv6 traduite au client CL1.

Limites de Statelful NAT64

Les limitations suivantes s'appliquent à Stateful NAT64 :

- La traduction des options IPv4 n'est pas prise en charge.
- La traduction des en-têtes de routage IPv6 n'est pas prise en charge.
- La traduction des en-têtes d'extension saut par saut des paquets IPv6 n'est pas prise en charge.
- La traduction des en-têtes ESP et EH des paquets IPv6 n'est pas prise en charge.
- La traduction de paquets de multidiffusion n'est pas prise en charge.
- Les paquets du protocole SCTP (Stream Control Transmission Protocol), du protocole DCCP (Datagram Congestion Control Protocol) et du protocole IPsec ne sont pas traduits.

Configuration de Stateful NAT64

La création des entités requises pour une configuration NAT64 dynamique sur l'appliance NetScaler implique les procédures suivantes :

1. Ajoutez une règle ACL6 avec l'action ALLOW.
2. Ajoutez un ipset qui lie plusieurs adresses IP.
3. Ajoutez un profil réseau et liez-y l'ipset. Si vous souhaitez lier une seule adresse IP, il n'est pas nécessaire de créer une entité ipset. Dans ce cas, liez l'adresse IP directement au profil réseau.
4. Ajoutez une règle NAT64, qui inclut la liaison de la règle ACL6 et du netprofile à la règle NAT 64.
5. Ajoutez un préfixe IPv6 NAT64.

Procédures CLI

Pour ajouter une règle ACL6 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- add ns acl6 <acl6name> <acl6action> …

Pour ajouter un ensemble d'adresses IP et y lier plusieurs adresses IP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- add ipset <name>
- bind ipset <name> <IPaddress …>

Pour ajouter un profil réseau à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- add netprofile <name> -srcIP <IPaddress ou IPset>

Pour ajouter une règle NAT64 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- add nat64 <name> <acl6name> -netProfile <string>

Pour ajouter un préfixe NAT64 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
set ipv6 -natprefix <ipv6_addr                    *>
```

-

Exemple :

```
 > add acl6 ACL6-1 ALLOW -srcIPv6 2001:DB8:5001::30
 Done

> apply acls6
 Done

> add ip 192.0.2.100 255.255.255.0  - type SNIP
 Done

> add ip 192.0.2.102 255.255.255.0   - type SNIP
 Done

> add ipset IPset-1
 Done

> bind ipset IPset-1 192.0.2.100 192.0.2.102
IPAddress "192.0.2.100" bound
IPAddress "192.0.2.102" bound
 Done

> add netprofile Netprofile-1 -srcIP IPset-1
 Done

> add nat64 NAT64-1 ACL6-1 -netprofile Netprofile-1
 Done

```



```
> set ipv6 -natprefix 2001:DB8:300::/96
 Done
<!--NeedCopy-->
```

Procédures GUI

Pour ajouter une règle NAT64 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Routes > NAT64 et accédez à une nouvelle règle NAT64, ou modifiez une règle existante.

Pour ajouter un préfixe NAT64 à l'aide de l'interface graphique :

Accédez à Système > Réseau, dans le groupe Paramètres, cliquez sur Configurer les paramètres INATet définissez le paramètre Préfixe.

RNAT

May 5, 2023

Dans Reverse Network Address Translation (RNAT), l'appliance NetScaler remplace les adresses IP source des paquets générés par les serveurs par des adresses IP NAT publiques. Par défaut, l'appliance utilise une adresse SNIP comme adresse IP NAT. Vous pouvez également configurer l'appliance pour qu'elle utilise une adresse IP NAT unique pour chaque sous-réseau. Vous pouvez également configurer RNAT à l'aide des listes de contrôle d'accès (ACL). Les modes Utiliser l'IP source (USIP), Utiliser l'adresse IP du sous-réseau (USNIP) et Link Load Balancing (LLB) affectent le fonctionnement de RNAT. Vous pouvez afficher des statistiques pour surveiller le RNAT.

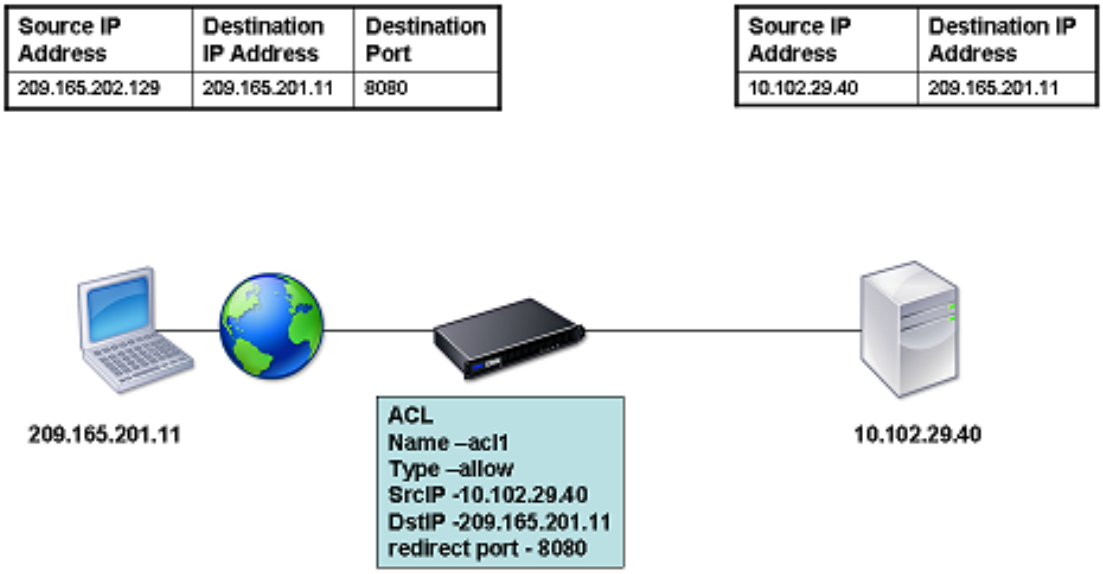
Remarque : La plage de ports éphémères pour RNAT sur l'appliance NetScaler est 1024-65535.

Vous pouvez utiliser une adresse réseau ou une ACL étendue comme condition pour une entrée RNAT :

- **À l'aide d'une adresse réseau.** Lorsque vous utilisez une adresse réseau, le traitement RNAT est effectué sur tous les paquets provenant du réseau spécifié.
- **Utilisation de listes de contrôle d'accès étendues.** Lorsque vous utilisez des ACL, le traitement RNAT est effectué sur tous les paquets qui correspondent aux ACL. Pour configurer l'appliance NetScaler afin qu'elle utilise une adresse IP unique pour le trafic correspondant à une ACL, vous devez effectuer les trois tâches suivantes :
  1. Configurez l'ACL.
  2. Configurez RNAT pour modifier l'adresse IP source et le port de destination.
  3. Appliquez l'ACL.

Le schéma suivant illustre le RNAT configuré avec une ACL.

Figure 1. RNAT avec ACL

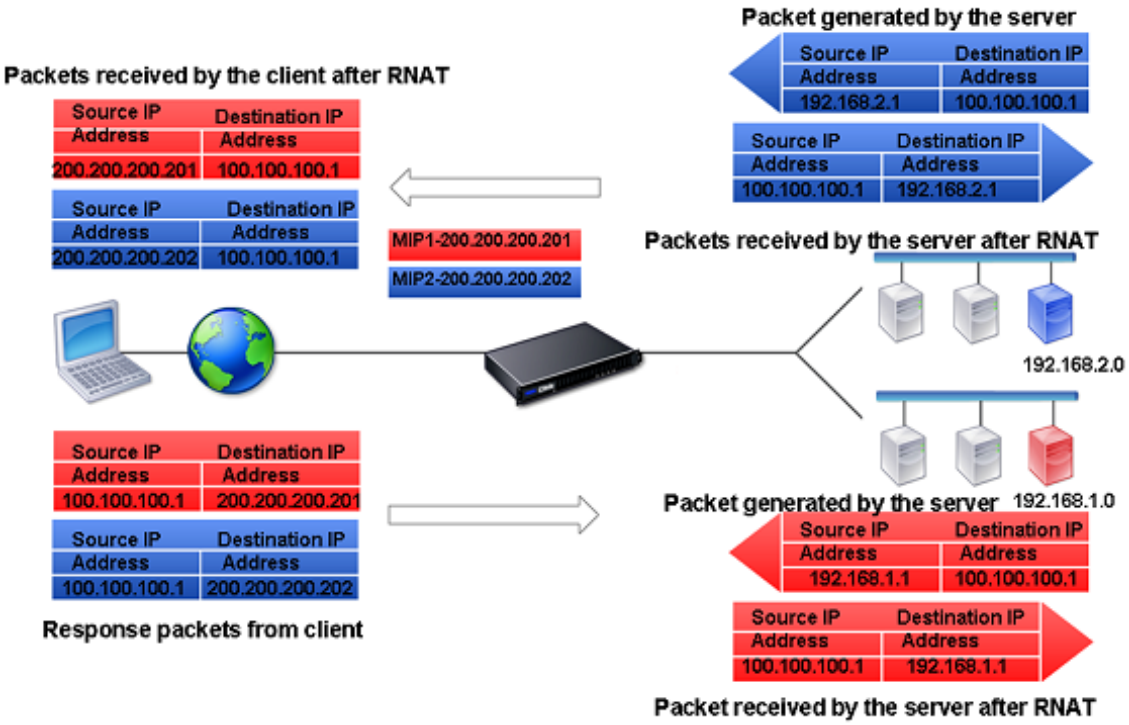


Les choix de base suivants s'offrent à vous pour le type d'adresse IP NAT :

- **Utilisation d'un SNIP comme adresse IP NAT.** Lorsque vous utilisez un SNIP comme adresse IP NAT, l'appliance NetScaler remplace les adresses IP source des paquets générés par le serveur par un SNIP. Par conséquent, l'adresse SNIP doit être une adresse IP publique. Si le mode Use Subnet IP (USNIP) est activé, NetScaler peut utiliser une adresse IP de sous-réseau (SNIP) comme adresse IP NAT.
- **Utilisation d'une adresse IP unique comme adresse IP NAT.** Lorsque vous utilisez une adresse IP unique comme adresse IP NAT, l'appliance NetScaler remplace les adresses IP source des paquets générés par le serveur par l'adresse IP unique spécifiée. L'adresse IP unique doit être une adresse IP publique appartenant à NetScaler. Si plusieurs adresses IP NAT sont configurées pour un sous-réseau, la sélection des adresses IP NAT utilise l'algorithme round robin.

  Cette configuration est illustrée dans le schéma suivant.

  Figure 2. Utilisation d'une adresse IP unique comme adresse IP NAT



Avant de commencer

Avant de configurer une règle RNAT, tenez compte des points suivants :

- Lorsque RNAT et Use Source IP (USIP) sont tous deux configurés sur l'appliance NetScaler, RNAT est prioritaire. En d'autres termes, l'adresse IP source des paquets, qui correspond à une règle RNAT, est remplacée conformément au paramètre de la règle RNAT.
- Dans une topologie où l'appliance NetScaler effectue à la fois un équilibrage de charge de liaison (LLB) et un RNAT pour le trafic provenant du serveur, l'appliance sélectionne l'adresse IP source en fonction du routeur. La configuration LLB détermine la sélection du routeur. Pour plus d'informations sur LLB, reportez-vous à la section Équilibrage de charge des liaisons.

Configurer RNAT

Les instructions suivantes fournissent des procédures de ligne de commande distinctes pour créer des entrées RNAT qui utilisent différentes conditions et différents types d'adresses IP NAT. Dans l'interface graphique, toutes les variantes peuvent être configurées dans la même boîte de dialogue. Il n'existe donc qu'une seule procédure pour les utilisateurs de l'interface graphique.

Procédures CLI

Pour créer une règle RNAT à l'aide de l'interface de ligne de commande :

À l'invite de commandes, pour créer la règle et vérifier la configuration, tapez :

- `add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))`
- `bind rnat <name> <natIP>@ …`
- `show rnat`

Pour modifier ou supprimer une règle RNAT à l'aide de l'interface de ligne de commande :

- Pour modifier une règle RNAT :

  `set rnat <name> (<aclname> [-redirectPort <port>])`

- Pour supprimer une règle RNAT, tapez la commande.

  `rm rnat <name>`

Utilisez la commande suivante pour vérifier la configuration :

- `show rnat`

Exemples :

```
A network address as the condition and a SNIP address as the NAT IP address:

> add rnat RNAT-1 192.168.1.0 255.255.255.0
Done

A network address as the condition and a unique IP address as the NAT IP address:

> add rnat RNAT-2 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-2 -natip 10.102.29.50
Done

If instead of a single NAT IP address you specify a range, RNAT entries are created with all the NetScaler-owned IP addresses, except the NSIP, that fall within the range specified:

> add rnat RNAT-3 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-3 -natip 10.102.29.[50-110]
Done


An ACL as the condition and a SNIP address as the NAT IP address:
```



```
24
25 > add rnat RNAT-4 acl1
26 Done
27
28 An ACL as a condition and a unique IP address as the NAT IP address:
29
30 > add rnat RNAT-4 acl1
31 Done
32
33 > bind rnat RNAT-4 -natip 10.102.29.50
34 Done
35
36 If instead of a single NAT IP address you specify a range, RNAT entries
       are created with all the NetScaler-owned IP addresses, except the
      NSIP, that fall within the range specified:
37
38 > add rnat RNAT-5 acl1
39 Done
40
41 > bind rnat RNAT-5 -natip 10.102.29.[50-70]
42 Done
43
44 <!--NeedCopy-->
```

Procédures GUI

Pour créer une entrée RNAT à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **NAT**, cliquez sur l'onglet **RNAT** et ajoutez une nouvelle règle RNAT ou modifiez une règle existante.

Moniteur RNAT

Vous pouvez afficher les statistiques RNAT pour résoudre les problèmes liés à la traduction des adresses IP.

Le tableau suivant décrit les statistiques associées à RNAT et à RNAT IP.

Statistique	Description
Octets reçus	Octets reçus pendant les sessions RNAT
Octets envoyés	Octets envoyés pendant les sessions RNAT
Paquets reçus	Paquets reçus pendant les sessions RNAT

Statistique	Description
Paquets envoyés	Paquets envoyés pendant les sessions RNAT
Synchronisation envoyée	Demandes de connexions envoyées pendant les sessions RNAT
Sessions en cours	Sessions RNAT actuellement actives

Pour afficher les statistiques RNAT à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **État rant**

Exemple :

```
1  > stat rnat
2
3  RNAT summary
4                                Rate (/s)            Total
5  Bytes Received                  0                    0
6  Bytes Sent                      0                    0
7  Packets Received                0                    0
8  Packets Sent                    0                    0
9  Syn Sent                        0                    0
10 Current RNAT sessions           --                   0
11  Done
12 >
13 <!--NeedCopy-->
```

Pour surveiller le RNAT à l'aide de l'interface graphique :

Accédez à Système**>**Réseau**>**NAT**, cliquez sur l'onglet**RNAT**, puis sur Statistiques.**

Configurer RNAT6

Les règles RNAT (Reverse Network Address Translation) pour les paquets IPv6 sont appelées RNAT6. Lorsqu'un paquet IPv6 généré par un serveur répond aux conditions spécifiées dans la règle RNAT6, l'appliance remplace l'adresse IPv6 source du paquet IPv6 par une adresse IPv6 NAT configurée avant de le transférer vers la destination. L'adresse IPv6 NAT est l'une des adresses SNIP6 ou VIP6 appartenant à NetScaler.

Lorsque vous configurez une règle RNAT6, vous pouvez spécifier un préfixe IPv6 ou un ACL6 comme condition :

- **À l'aide d'une adresse réseau IPv6**. Lorsque vous utilisez un préfixe IPv6, l'appliance effectue un traitement RNAT sur les paquets IPv6 dont l'adresse IPv6 correspond au préfixe.
- **Utilisation d'ACL6s**. Lorsque vous utilisez un ACL6, l'appliance effectue un traitement RNAT sur les paquets IPv6 qui répondent aux conditions spécifiées dans l'ACL6.

Vous disposez de l'une des options suivantes pour définir l'adresse IP NAT :

- Spécifiez un ensemble d'adresses SNIP6 et VIP6 appartenant à NetScaler pour une règle RNAT6. L'appliance NetScaler utilise l'une des adresses IPv6 de cet ensemble comme adresse IP NAT pour chaque session. La sélection est basée sur l'algorithme Round Robin et est effectuée pour chaque session.
- Ne spécifiez aucune adresse SNIP6 ou VIP6 appartenant à NetScaler pour une règle RNAT6. L'appliance NetScaler utilise n'importe laquelle des adresses SNIP6 ou VIP6 appartenant à NetScaler comme adresse IP NAT. La sélection est basée sur le réseau de saut suivant auquel est destiné un paquet IPv6 correspondant à la règle RNAT.

Procédures CLI

Pour créer une règle RNAT6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, pour créer la règle et vérifier la configuration, tapez :

- **ajouter rnat6** <port><name>(<network>| (<acl6name>[-**RedirectPort** \]))
- **bind rnat6** <name> <natIP6>@ …
- **afficher rnat6**

Pour modifier ou supprimer une règle RNAT6 à l'aide de l'interface de ligne de commande :

- **Pour modifier une règle RNAT6 dont la condition est ACL6, tapez la commande**set rnat6**, suivie d'une nouvelle valeur pour le paramètre RedirectPort.** <name>
- <name>Pour supprimer une règle RNAT6, tapez la commande **clear rnat6** .

Procédures GUI

Pour configurer une règle RNAT6 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **NAT**, cliquez sur l'onglet **RNAT6** et ajoutez une nouvelle règle RNAT6 ou modifiez une règle existante.

Moniteur RNAT6

Vous pouvez afficher les statistiques relatives à la fonctionnalité RNAT6 pour surveiller les performances ou pour résoudre les problèmes liés à la fonctionnalité RNAT6. Vous pouvez afficher un résumé des statistiques des règles RNAT6 ou d'une règle RNAT6 particulière. Les compteurs statistiques

reflètent les événements survenus depuis le dernier redémarrage de l'appliance NetScaler. Tous ces compteurs sont remis à 0 lorsque l'appliance NetScaler est redémarrée.

La liste suivante répertorie certains des compteurs de statistiques associés à la fonctionnalité RNAT6 :

- **Octets reçus** : nombre total d'octets reçus pendant les sessions RNAT6.
- **Octets envoyés** : nombre total d'octets envoyés pendant les sessions RNAT6.
- **Paquets reçus** : nombre total de paquets reçus pendant les sessions RNAT6.
- **Paquets envoyés** : nombre total de paquets envoyés pendant les sessions RNAT6.
- **Synchronisation envoyée** : nombre total de demandes de connexions envoyées pendant les sessions RNAT6
- **Sessions en cours - Sessions** RNAT6 actuellement actives

Pour afficher un résumé des statistiques de toutes les règles RNAT6 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **Stat Rnat6**

Pour afficher les statistiques d'une règle RNAT6 spécifiée à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **stat rnat6 [** <rnat6 rule name>]

Pour afficher les statistiques RNAT6 à l'aide de l'interface graphique :

Accédez à Système**>**Réseau**>**NAT**, cliquez sur l'onglet**RNAT6**, puis sur Statistiques.**

```
> stat rnat6

RNAT6 summary

                          Rate (/s)               Total

Bytes Received             178                20644

Bytes Sent                 178                20644

Packets Received            5                  401

Packets Sent                5                  401

Syn Sent                    0                    2

Current RNAT6 sessions      --                   1

Done
```



```
20
21 <!--NeedCopy-->
```

Heure de début du journal et raisons de fermeture de la connexion dans les entrées du journal RNAT

Pour diagnostiquer ou résoudre les problèmes liés au RNAT, l'appliance NetScaler enregistre les sessions RNAT chaque fois qu'elles sont fermées.

Un message de journal pour une session RNAT contient les informations suivantes :

- Adresse IP appartenant à NetScaler (adresse NSIP ou adresse SNIP) d'où provient le message du journal
- Horodatage de la création du journal
- Protocole de la session RNAT
- Adresse IP source
- Adresse IP RNAT
- Adresse IP de destination
- Heure de début de la session RNAT
- Heure de clôture de la session RNAT
- Nombre total d'octets envoyés par l'appliance NetScaler pour cette session RNAT
- Nombre total d'octets reçus par l'appliance NetScaler pour cette session RNAT
- Motif de clôture de la session du RNAT. L'appliance NetScaler enregistre le motif de fermeture des sessions TCP RNAT qui n'utilisent pas le proxy TCP (proxy TCP désactivé) de l'appliance. Les types de motifs de fermeture enregistrés pour les sessions TCP RNAT sont les suivants :
  - **FIN DU TCP**. La session RNAT a été fermée en raison d'un TCP FIN envoyé par le périphérique source ou de destination.
  - **TCP RST.** La session RNAT a été fermée en raison d'une réinitialisation TCP envoyée par le périphérique source ou de destination.
  - **DÉLAI D'EXPIRATION.** Le délai imparti pour la session RNAT a expiré.

Le tableau suivant présente quelques exemples d'entrées de journal pour les sessions RNAT.

Type d'entrée	Exemple d'entrée dans le journal
Exemple d'entrée de journal pour une session UDP RNAT	Dec 1 15:28:12 10.102.53.114 12/01/ 2015:15:28:12 GMT 0-PPE-0 : UDP par défaut NAT_OTHERCONN_DELINK 154 0 : Source 1.2.2. 5:23431 - Destination 192.168.123. 122:22 - NatiP 192.168.123. 1:4045 - Destination 192.168.123. 122:22 - Heure de début 12/01/2015:15:26:58 GMT - Heure Delink 12/01/ 2015:15:58 GMT - Heure Delink Time 12/01/ 2011/ 5:15:28:12 GMT - Total_Bytes_Send 2511 - Total_Bytes_Recv 3725
Exemple d'entrée de journal pour une session TCP RNAT. L'entrée du journal indique que la session s'est fermée à cause de la réinitialisation du protocole TCP	Dec 1 15:29:59 10.102.53.114 12/01/ 2015:15:27:59 GMT 0-PPE-0 : TCP par défaut NAT_OTHERCONN_DELINK 152 0 : Source 1.2.2. 5:33826 - Destination 192.168.123. 122:22 - NatiP 192.168.123. 1:2384 - Destination 192.168.123. 122:22 - Heure de début 12/01/2015:15:27:40 GMT - Heure Delink 12/01/ 2015:15:27:59 GMT - Total_Bytes_Send 2147 - Total_Bytes_recv 3257 - Motif de fermeture TCP RST
Exemple d'entrée de journal pour une session TCP RNAT. L'entrée du journal indique que le délai de la session a expiré	Dec 1 15:30:12 10.102.53.114 12/01/ 2015:15:30:12 GMT 0-PPE-0 : TCP par défaut NAT_OTHERCONN_DELINK 155 0 : Source 1.2.2. 5:64976 - Destination 192.168.123. 115:22 - NatiP 192.168.123. 1:19636 - Destination 192.168.123. 115:22 - Heure de début 12/01/2015 5:15:27:25 GMT - Heure Delink 12/01/ 2015:15:30:12 GMT - Total_Bytes_Send 0 - Total_Bytes_Recv 0 - Délai d'expiration du délai de fermeture

Basculement de connexion dynamique pour RNAT

Le basculement de connexion permet d'éviter toute interruption de l'accès aux applications déployées dans un environnement distribué. L'appliance NetScaler prend désormais en charge le basculement dynamique des connexions pour les connexions liées aux règles RNAT dans une configuration NetScaler High Availability (HA). Dans une configuration HA, le basculement de connexion

(ou mise en miroir des connexions) fait référence au processus qui consiste à maintenir active une connexion TCP ou UDP établie en cas de basculement.

L'appliance principale envoie des messages à l'appliance secondaire pour synchroniser les informations actuelles concernant les connexions RNAT. L'appliance secondaire utilise ces informations de connexion uniquement en cas de basculement. Lorsqu'un basculement se produit, le nouveau dispositif NetScaler principal dispose d'informations sur les connexions établies avant le basculement et continue donc à fournir ces connexions même après le basculement. Du point de vue du client, ce basculement est transparent. Pendant la période de transition, le client et le serveur peuvent subir une brève interruption et des retransmissions.

Le basculement de connexion peut être activé conformément à la règle RNAT. Pour activer le basculement de connexion sur une règle RNAT, vous activez le paramètre ConnFailover (Connection Failover) de cette règle RNAT spécifique à l'aide de l'interface de ligne de commande ou de l'interface graphique.

Pour activer le basculement de connexion pour une règle RNAT à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `set rnat <name> -connfailover (ENABLED | DISABLED)`
- `show rnat`

Pour activer le basculement de connexion pour une règle RNAT à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **NAT**, puis cliquez sur l'onglet **RNAT** .
2. Sélectionnez **Basculement de connexion** lors de l'ajout d'une nouvelle règle RNAT ou lors de la modification d'une règle existante.

Réservation du port source pour les connexions RNAT aux serveurs

Pour une requête atteignant une configuration RNAT qui possède une ou plusieurs adresses IP RNAT et dont le paramètre Utiliser le port proxy est désactivé, l'appliance NetScaler utilise l'une des adresses IP RNAT et le port source de la demande RNAT pour se connecter aux serveurs. Avant la version 13.0 47.x, la connexion RNAT (à l'aide du port source du client RNAT) au serveur échoue si le même port source est déjà utilisé dans d'autres connexions.

- **Port source inférieur à 1024**. Par défaut, l'appliance NetScaler réserve les 1024 premiers ports de toute adresse IP appartenant à NetScaler (y compris les adresses IP RNAT). Avant la version 13.0 47.x, la connexion RNAT (à l'aide du port source du client RNAT) au serveur échoue si le port source de la requête RNAT est inférieur ou égal à 1024. Avec la version 13.0 47.x, la connexion RNAT (à l'aide du port source du client RNAT) au serveur réussit même si le port source de la requête RNAT est inférieur ou égal à 1024.

- **Port source supérieur à 1024**. Avant la version 13.0 47.x, la connexion RNAT (à l'aide du port source du client RNAT) au serveur échoue si le même port source est déjà utilisé dans d'autres connexions. Avec la version 13.0 47.x, vous pouvez spécifier une plage de ports source client RNAT dans le paramètre `Retain Source Port range` (`retainsourceportrange`) dans le cadre d'une configuration RNAT. L'appliance NetScaler réserve ces ports source du client RNAT sur l'adresse IP RNAT à utiliser uniquement pour la connexion RNAT aux serveurs.

Suppression de sessions RNAT

Vous pouvez supprimer toutes les sessions RNAT indésirables ou inefficaces de l'appliance NetScaler. L'appliance libère immédiatement les ressources (telles que le port de l'adresse IP NAT et la mémoire) allouées à ces sessions, les rendant ainsi disponibles pour de nouvelles sessions. L'appliance supprime également tous les paquets suivants liés à ces sessions supprimées. Vous pouvez supprimer toutes les sessions RNAT ou certaines d'entre elles de l'appliance NetScaler.

Pour effacer toutes les sessions RNAT à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **séance de rinçage**

Pour effacer des sessions RNAT sélectives à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **flush rnatsession** <ip_addr**(**-réseau -**masque réseau****) | -**AntiP | - aclname**)** <ip_addr><netmask><strin

Pour effacer toutes les sessions RNAT ou certaines d'entre elles à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **NAT**, puis cliquez sur l'onglet **RNAT** .
2. Dans le menu **Actions**, cliquez sur **Flush RNAT Sessions pour supprimer toutes les sessions** RNAT ou certaines d'entre elles (par exemple, supprimer des sessions RNAT avec une adresse IP RNAT spécifique, ou appartenir à une règle RNAT spécifique basée sur un réseau ou une ACL).

Exemples de configurations :

```
1     Clear all RNAT sessions existing on a NetScaler appliance
2
3     > flush rnatsession
4
5     Done
6
7     Clear all RNAT sessions belonging to network based RNAT rules that
         has 203.0.113.0/24 network as the matching condition.
8
9     > flush rnatsession -network 203.0.113.0 -netmask 255.255.255.0
```



```
10
11      Done
12
13      Clear all RNAT sessions with RNAT IP 192.0.2.90.
14
15      > flush rnatsession -natIP 192.0.2.90
16
17      Done
18
19      Clear all RNAT sessions belonging to ACL based RNAT rules that has
            ACL-RNAT-1 as the matching condition.
20
21      > flush rnatsession -aclname ACL-RNAT-1
22
23      Done
24  <!--NeedCopy-->
```

Configuration de la traduction IPv6-IPv4 basée sur un préfixe

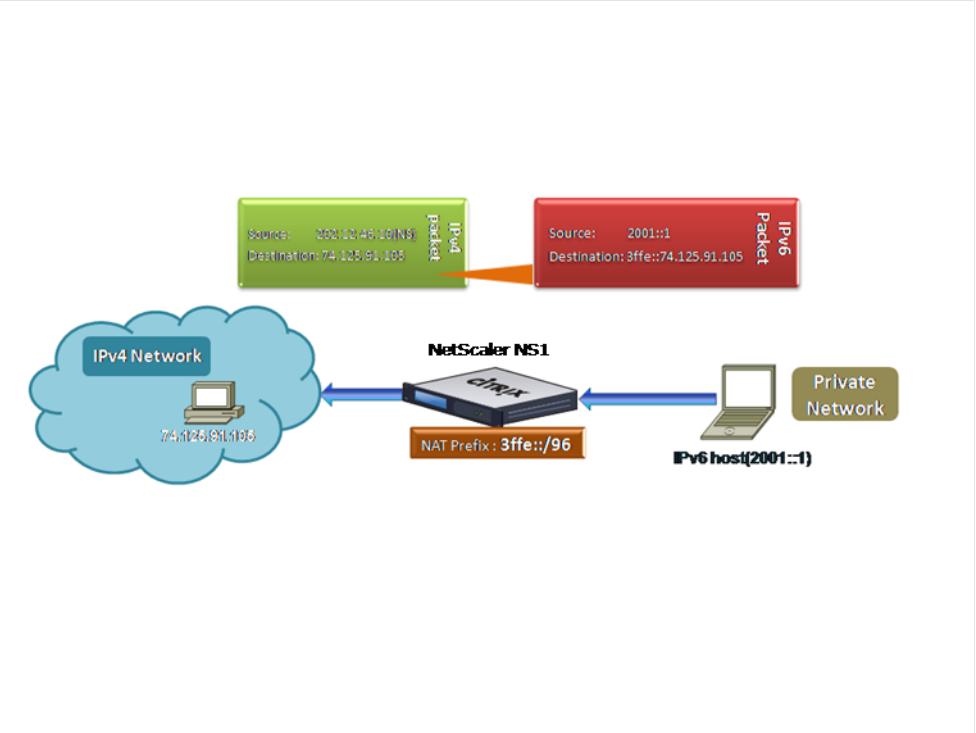
May 5, 2023

La traduction basée sur les préfixes est un processus qui consiste à traduire des paquets envoyés depuis des serveurs IPv6 privés en paquets IPv4, à l'aide d'un préfixe IPv6 configuré dans l'appliance NetScaler. Ce préfixe a une longueur de 96 bits (128-32=96). Les serveurs IPv6 incorporent l'adresse IP de destination des serveurs ou hôtes IPv4 dans les 32 derniers bits du champ d'adresse IP de destination des paquets IPv6. Les 96 premiers bits du champ d'adresse IP de destination sont définis comme le préfixe NAT IPv6.

L'appliance NetScaler compare les 96 premiers bits de l'adresse IP de destination de tous les paquets IPv6 entrants au préfixe configuré. En cas de correspondance, l'appliance NetScaler génère un paquet IPv4 et définit l'adresse IP de destination comme étant les 32 derniers bits de l'adresse IP de destination du paquet IPv6 correspondant. Les paquets IPv6 adressés à ce préfixe doivent être routés vers NetScaler afin que la traduction IPv6-IPv4 soit effectuée par NetScaler.

Dans le schéma suivant, 3ffe : :/96 est configuré en tant que préfixe NAT IPv6 sur NetScaler NS1. L'hôte IPv6 envoie un paquet IPv6 avec l'adresse IP de destination 3ffe : :74.125.91.105. NS1 compare les 96 premiers bits de l'adresse IP de destination de tous les paquets IPv6 entrants au préfixe configuré, et ils correspondent. NS1 génère ensuite un paquet IPv4 et définit l'adresse IP de destination comme 74.125.91.105.

Figure 1. Traduction basée sur un préfixe IPv6-IPv4



Pour configurer la traduction IPv6-IPv4 basée sur des préfixes à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- définir ipv6 [-natprefix \ <ipv6_addr| \ *>]
- show ipv6

Exemple :

```
> set ipv6 -natprefix 3ffe::/96
 Done
<!--NeedCopy-->
```

Pour configurer la traduction IPv6-IPv4 basée sur des préfixes à l'aide de l'interface graphique :

Accédez à Système > Réseau, dans le groupe Paramètres, cliquez sur Configurer les paramètres INATet définissez le paramètre Préfixe.

NAT préfixe IP

May 5, 2023

L'appliance NetScaler prend en charge la traduction d'une partie de l'adresse IP source au lieu de

l'adresse complète des paquets reçus sur l'appliance. Le préfixe IP NAT inclut la modification d'un ou plusieurs octets ou bits de l'adresse IP source.

L'appliance NetScaler prend en charge le préfixe IP NAT pour les configurations d'équilibrage de charge des types suivants : ANY, UDP, DNS, TCP et HTTP.

Cas d'utilisation : zonification des clients pour le déploiement d'une appliance NetScaler et d'un dispositif d'optimisation

Le préfixe IP NAT est très utile dans un déploiement qui inclut une appliance NetScaler et un périphérique d'optimisation (par exemple, Citrix ByteMobile). Ce type de déploiement comporte différents réseaux clients situés géographiquement, qui partagent la même adresse réseau. L'appliance NetScaler doit envoyer le trafic reçu de chacun des réseaux clients au périphérique d'optimisation avant de le transférer vers la destination.

L'appareil renvoie le trafic optimisé à l'appliance NetScaler. Les exigences d'optimisation étant différentes pour le trafic provenant de chaque réseau client, le dispositif d'optimisation doit reconnaître le réseau client de chaque paquet qu'il reçoit. La solution consiste à séparer le trafic de chaque réseau client vers une zone différente à l'aide de VLAN. Le préfixe IP NAT avec un paramètre différent est configuré pour chaque zone. L'appliance NetScaler traduit le dernier octet de l'adresse IP source de chaque paquet, et la valeur d'octet traduite est différente pour chaque zone.

Prenons l'exemple de deux zones, Z1 et Z2, partageant l'adresse réseau 192.0.2.0/24. Sur l'appliance NetScaler, les entités NAT à préfixe IP nommées natrule-1 et natrule-2 sont configurées pour ces deux zones. Avant que l'appliance ne transfère un paquet depuis Z1, natrule-1 traduit le dernier octet de l'adresse IP source du paquet en 100. De même, pour les paquets provenant de Z2, natrule-2 traduit le dernier octet de l'adresse IP source en 200. Pour deux clients, CL1-Z1 dans la zone Z1 et CL1-Z2 dans la zone Z2, chacun avec l'adresse IP 192.0.2.30, l'appliance NetScaler traduit l'adresse IP source des paquets de CL1-Z1 en 100.0.2.30 et des paquets de CL1-Z2 en 200.0.2.30. Le dispositif d'optimisation auquel l'appliance NetScaler envoie les paquets traduits est configuré pour utiliser l'adresse IP source d'un paquet afin de reconnaître la zone. Il applique donc l'optimisation appropriée configurée pour la zone d'où provient le paquet.

Étapes de configuration

La configuration du préfixe IP NAT comprend les étapes suivantes :

- **Créez un profil réseau et définissez le paramètre de règle NAT d'un profil réseau**. Une règle NAT spécifie deux adresses IP et un masque de réseau. La première adresse IP (spécifiée par le paramètre Adresse IP) est l'adresse IP source qui doit être traduite avec la seconde (spécifiée par le paramètre IP Rewrite). Le masque de réseau indique la partie de l'adresse IP source qui doit être traduite par la même partie de la seconde adresse IP.

- **Liez le profil réseau aux serveurs ou services virtuels d'équilibrage**de charge. Un profil réseau avec un paramètre de règle NAT peut être lié à un serveur virtuel ou à un service de type ANY, UDP, DNS, TCP et HTTP. Après avoir lié un profil réseau à un serveur ou à un service virtuel, l'appliance NetScaler fait correspondre l'adresse IP source des paquets entrants liés au serveur ou au service virtuel avec le paramètre de règle NAT. NetScaler exécute ensuite le préfixe IP NAT pour les paquets qui correspondent à la règle NAT.

Pour configurer la traduction NAT du préfixe IP à l'aide de la ligne de commande :

À l'invite de commande, tapez :

- **lier NetProfile** <ip_addr><netmask><rewriteIp><name>(-** NaturRule**)
- **afficher le profil réseau** <name>

Pour configurer le préfixe IP NAT à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **Profils réseau**.
2. Définissez les paramètres suivants sous Règles NAT lors de l'ajout ou de la modification de NetProfiles.
    - Adresse IP
    - Masque réseau
    - Réécrire l'adresse IP

Exemple de configuration

Dans l'exemple de configuration suivant, le profil réseau PARTIAL-NAT-1 possède des paramètres NAT de préfixe IP et est lié au serveur virtuel d'équilibrage de charge LBVS-1, de type ANY. Pour les paquets reçus sur LBVS-1 à partir de 192.0.0.0/8, l'appliance NetScaler traduit le dernier octet de l'adresse IP source du paquet en 100. Par exemple, s'il s'agit d'un paquet dont l'adresse IP source est 192.0.2.30 reçu sur LBVS-1, l'appliance NetScaler traduit l'adresse IP source en 100.0.2.30 avant de l'envoyer à l'un des serveurs liés.

```
1 > add netprofile PARTIAL-NAT-1
2 Done
3
4 > bind netprofile PARTIAL-NAT-1  - natrule 192.0.0.0 255.0.0.0 100.0.0.0
5 Done
6
7 > add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1
8 Done
9 <!--NeedCopy-->
```


ARP statique

May 5, 2023

Vous pouvez ajouter des entrées ARP statiques à la table ARP et en supprimer. Après avoir ajouté une entrée, vous devez vérifier la configuration. Si l'adresse IP, le port ou l'adresse MAC changent après la création d'une entrée ARP statique, vous devez supprimer ou ajuster manuellement l'entrée statique. Par conséquent, la création d'entrées ARP statiques n'est pas recommandée sauf si cela est nécessaire.

Pour ajouter une entrée ARP statique à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter une adresse IP IP arp** <ip_addr>-**mac**<mac_addr>-**ifnum** <interface_name>
- **show arp** <IPAddress>

Exemple :

```
1 > add arp -ip 10.102.29.6 -mac 00:24:e8:73:ca:ec -ifnum 1/1
2  Done
3 <!--NeedCopy-->
```

Pour supprimer une entrée ARP statique à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande **rm arp** et l'adresse IP.

Pour ajouter une entrée ARP statique à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Table ARP**et ajoutez une entrée ARP statique.

Spécifier un VLAN dans une entrée ARP statique

Dans une entrée ARP statique, vous pouvez spécifier le VLAN via lequel le périphérique de destination est accessible. Cette fonctionnalité est utile lorsque l'interface spécifiée dans l'entrée ARP statique fait partie de plusieurs VLAN balisés et que la destination est accessible via l'un des VLAN. L'appliance NetScaler inclut l'ID VLAN spécifié dans les paquets sortants correspondant à l'entrée ARP statique. Si vous ne spécifiez pas d'ID de VLAN dans une entrée ARP et que l'interface spécifiée fait partie de plusieurs VLAN balisés, l'appliance attribue le VLAN natif de l'interface à l'entrée ARP.

Par exemple, supposons que l'interface NetScaler 1/2 fasse partie du VLAN 2 natif et des VLAN 3 et 4 balisés, et que vous ajoutiez une entrée ARP statique pour le périphérique réseau A, qui fait partie du VLAN 3 et est accessible via l'interface 1/2. Vous devez spécifier le VLAN 3 dans l'entrée ARP du périphérique réseau A. L'appliance NetScaler inclut ensuite le VLAN 3 balisé dans tous les paquets destinés au périphérique réseau A et les envoie depuis l'interface 1/2.

Si vous ne spécifiez pas d'ID de VLAN, l'appliance NetScaler attribue le VLAN 2 natif à l'entrée ARP. Les paquets destinés au périphérique A sont supprimés dans le chemin réseau, car ils ne spécifient pas le VLAN 3 balisé, qui est le VLAN du périphérique A.

Pour spécifier un VLAN dans une entrée ARP statique à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter arp -adresse IP -mac** <ip_addr>**-ifnum** <mac_addr><interface_name><positive_integer>[-vlan \]**
- **show arp** <IPAddress>

Exemple :

```
> add arp -ip 198.51.100.91 -mac 36:db:4b:f6:12:15 -ifnum 1/2 -vlan 3
Done
<!--NeedCopy-->
```

Définir le délai d'expiration pour les entrées ARP dynamiques

August 20, 2021

Vous pouvez définir globalement un délai de vieillissement (valeur de délai d'attente) pour les entrées ARP apprises dynamiquement. La nouvelle valeur s'applique uniquement aux entrées ARP qui sont apprises dynamiquement après la définition de la nouvelle valeur. Les entrées ARP existantes expirent après la période de vieillissement configurée précédemment. Vous pouvez spécifier une valeur de délai ARP comprise entre 1 et 1 200 secondes.

Pour définir le délai d'expiration des entrées ARP dynamiques à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **set arpparam** -**timeout** <positive_integer>]
- **show arpparam**

Exemple :

```
> set arpparam -timeout 500
 Done
<!--NeedCopy-->
```

Pour définir le délai d'expiration des entrées ARP dynamiques sur sa valeur par défaut à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **unset arpparam**
- **show arpparam**

Exemple :

```
> unset arpparam
 Done
<!--NeedCopy-->
```

Pour définir le délai d'expiration des entrées ARP dynamiques à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Configurer les paramètres globaux ARP** et définissez le paramètre **Délai d'expiration d'entrée de table ARP**.

Neighbor Discovery

May 5, 2023

La découverte des voisins (ND) est l'un des protocoles les plus importants d'IPv6. Il s'agit d'un protocole basé sur les messages qui combine les fonctionnalités du protocole de résolution d'adresses (ARP), du protocole ICMP (Internet Control Message Protocol) et de la découverte de routeurs. ND permet aux nœuds de publier leurs adresses de couche de liens et d'obtenir les adresses MAC ou les adresses de couche de liens des nœuds voisins. Ce processus est effectué par le protocole Neighbor Discovery (ND6).

La découverte des voisins peut exécuter les fonctions suivantes :

- **Découverte des routeurs** : permet à un hôte de découvrir les routeurs locaux sur une liaison rattachée et de configurer automatiquement un routeur par défaut.
- **Découverte des préfixes** : permet à l'hôte de découvrir les préfixes réseau pour les destinations locales.

  Remarque : L'appliance NetScaler ne prend pas en charge la découverte des préfixes.
- **Découverte des paramètres** : permet à un hôte de découvrir des paramètres de fonctionnement supplémentaires, tels que le MTU et la limite de sauts par défaut pour le trafic sortant.
- **Configuration automatique des adresses** : permet aux hôtes de configurer automatiquement les adresses IP pour les interfaces avec et sans services de configuration d'adresses dynamiques tels que DHCPv6. NetScaler ne prend pas en charge la configuration automatique des adresses pour les adresses IPv6 globales.
- **Résolution d'adresse** : équivalente à l'ARP dans IPv4, permet à un nœud de convertir l'adresse IPv6 d'un nœud voisin en son adresse de couche de liaison.

- **Détection de l'inaccessibilité du voisin** : permet à un nœud de déterminer l'état d'accessibilité d'un voisin.
- **Détection d'adresses dupliquées** : permet à un nœud de déterminer si une adresse NSIP est déjà utilisée par un nœud voisin.
- **Redirection** : équivalent au message de redirection ICMP IPv4, permet à un routeur de rediriger l'hôte vers une meilleure adresse IPv6 de premier saut pour atteindre une destination.

Remarque : L'appliance NetScaler ne prend pas en charge la redirection IPv6.

Étapes de configuration

La configuration de la découverte des voisins comprend les tâches suivantes :

- Ajouter des voisins IPv6
- (Facultatif) Supprimer les voisins IPv6

Procédures CLI

Pour ajouter un voisin IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter nd6** <integer><neighbor><mac><ifnum>[-**vlan **]
- **sh nd6**

Exemple :

```
1  > add nd6 2001::1 00:04:23:be:3c:06 1/1  - vlan 1
2   Done
3
4  > show nd6
5     Neighbor                 MAC-Address(Vlan, Interface)       State
                TIME
6     --------                 ---------------------------       -----
              --------
7  1) ::1                      00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
          PERMANENT
8  2) fe80::2d0:68ff:fe0b:58da 00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
          PERMANENT
9  3) 2001::1                  00:04:23:be:3c:06(   1,   1/1)   REACHABLE
            STATIC
10  Done
11 <!--NeedCopy-->
```


Pour supprimer une entrée de découverte de voisins à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ****rm nd6 - vlan**** <Neighbor><VLANID>

Exemple :

```
1  rm nd6 3ffe:100:100::1 -vlan 1
2 <!--NeedCopy-->
```

Pour supprimer toutes les entrées de découverte de voisins à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **transparent nd6**

Procédures GUI

Pour ajouter un voisin IPv6 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Voisins IPv6**, puis ajoutez un nouveau voisin IPv6.

Pour supprimer une entrée de découverte de voisins à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Voisins IPv6**, supprimez le voisin IPv6.

Pour supprimer toutes les entrées de découverte de voisins à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Voisins IPv6**, puis cliquez sur **Effacer**.

Tunnels IP

May 5, 2023

Un tunnel IP est un canal de communication qui peut être créé à l'aide de technologies d'encapsulation entre deux réseaux dépourvus de chemin de routage. Chaque paquet IP partagé entre les deux réseaux est encapsulé dans un autre paquet puis envoyé via le tunnel.

L'appliance NetScaler implémente le tunneling IP de la manière suivante :

- **NetScaler en tant qu'encapsulateur (équilibrage de charge avec mode DSR)** : imaginez une organisation qui possède plusieurs centres de données dans différents pays, où le NetScaler peut se trouver au même endroit et les serveurs principaux dans un autre pays. En substance, NetScaler et les serveurs principaux se trouvent sur des réseaux différents et sont connectés via un routeur.

Lorsque vous configurez Direct Server Return (DSR) sur ce NetScaler, le paquet envoyé depuis le sous-réseau source est encapsulé par le NetScaler et envoyé via un routeur et un tunnel au serveur principal approprié. Le serveur principal désencapsule le paquet et répond directement au client, sans autoriser le paquet à passer via NetScaler.

- **NetScaler en tant que désencapsulateur :** imaginez une organisation possédant plusieurs centres de données dotés chacun de NetScaler et de serveurs principaux. Lorsqu'un paquet est envoyé du centre de données A au centre de données B, il est généralement envoyé via un intermédiaire, par exemple un routeur ou un autre NetScaler. NetScaler traite le paquet puis le transmet au serveur principal. Toutefois, si un paquet encapsulé est envoyé, NetScaler doit être en mesure de le désencapsuler avant de l'envoyer aux serveurs principaux. Pour permettre au NetScaler de fonctionner comme un désencapsulateur, un tunnel est ajouté entre le routeur et le NetScaler. Lorsque le paquet encapsulé, avec des informations d'en-tête supplémentaires, atteint NetScaler, le paquet de données est désencapsulé, c'est-à-dire que les informations d'en-tête supplémentaires sont supprimées, puis le paquet est transmis aux serveurs principaux appropriés.

  Le NetScaler peut également être utilisé comme désencapsuleur pour la fonctionnalité d'équilibrage de charge, en particulier dans les scénarios où le nombre de connexions sur un vserver dépasse une valeur seuil et où toutes les nouvelles connexions sont ensuite redirigées vers un vserver de sauvegarde.

La fonctionnalité IP Tunnel est disponible avec une licence NetScaler Premium Edition. Pour plus d'informations sur les licences de l'édition NetScaler et la matrice des fonctionnalités de NetScaler, consultez la fiche technique de NetScalerEditions.

Configuration des tunnels IP

La configuration de tunnels IP sur une appliance NetScaler consiste à créer des entités de tunnel IP. Une entité de tunnel IP spécifie les adresses IP des points de terminaison du tunnel local et distant et le protocole à utiliser pour le tunnel IP.

Remarque : lors de la configuration d'un tunnel IP dans une configuration de cluster, l'adresse IP locale doit être une adresse SNIP entrelacée.

Procédures CLI

Pour créer un tunnel IP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter iptunnel-**type** -**protocole** (**ipoverip** | GRE)**<name><remote><remoteSubnetMask><local>
- **show iptunnel**

Pour supprimer un tunnel IP à l'aide de l'interface de ligne de commande :

Pour supprimer un tunnel IP, tapez la commande **rm iptunnel** et le nom du tunnel.

Pour créer un tunnel IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **ajouter un tunnel IP6** <name><remoteIp><local>
- **afficher le tunnel IP6**

Pour supprimer un tunnel IPv6 à l'aide de l'interface de ligne de commande :

Pour supprimer un tunnel IPv6, tapez la commande **rm ip6tunnel** et le nom du tunnel.

Procédures GUI

Pour créer un tunnel IP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Tunnels IP**, puis ajoutez un nouveau tunnel IP.

Pour créer un tunnel IPv6 à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Tunnels IP** > **Tunnels IPv6**, puis ajoutez un nouveau tunnel IPv6.

Personnalisation des tunnels IP à l'échelle mondiale

En spécifiant globalement l'adresse IP source, vous pouvez attribuer une adresse IP source commune à tous les tunnels. De plus, étant donné que la fragmentation sollicite beaucoup le processeur, vous pouvez spécifier globalement que l'appliance NetScaler supprime tout paquet nécessitant une fragmentation. Sinon, si vous souhaitez fragmenter tous les paquets tant qu'une valeur seuil de processeur n'est pas atteinte, vous pouvez spécifier la valeur de seuil de processeur de manière globale.

Procédures CLI

Pour personnaliser globalement les tunnels IP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set IPTunnelParam**-**SrcIP - SrcIPRoundRobin (OUI | NON)**- DropFrag [OUI** | NON] - DropFragCpuThreshold**** <sourceIPAddress><Positive integer>
- **show ipTunnelParam**

Exemple :

```
1 > set iptunnelparam -srcIP 12.12.12.22 -dropFrag Yes -
     dropFragCpuThreshold 50
2  Done
```



```
3
4 > set iptunnelparam -srcIPRoundRobin YES -dropFrag Yes  -
     dropFragCpuThreshold 50
5  Done
6 <!--NeedCopy-->
```

Pour personnaliser globalement les tunnels IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set ip6tunnelparam**-srCip - srcipRoundRobin (OUI | NON)**- DropFrag [OUI** | NON] - DropFragCpuThreshold****** <IPv6Address><Positive integer>
- **afficher le paramètre ip6tunnelparam**

Procédures GUI

Pour personnaliser globalement les tunnels IP à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**, dans le groupe Paramètres, cliquez sur **Paramètres généraux du tunnel IPv4**.

1. Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Paramètres généraux du tunnel IPv6**.
2. Dans la boîte de dialogue **Configurer les paramètres globaux du tunnel IP**, définissez les paramètres.

Pour personnaliser globalement les tunnels IPv6 à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Paramètres généraux du tunnel IPv6**.
2. Dans la boîte de dialogue **Configurer les paramètres globaux du tunnel IP**, définissez les paramètres.

Options de charge utile GRE dans un tunnel IP GRE

Pour un tunnel IP GRE configuré, l'appliance NetScaler encapsule l'intégralité du paquet de couche 2, y compris l'en-tête Ethernet et l'en-tête VLAN (balise VLAN dot1q). Les tunnels IP GRE entre les appliances NetScaler et certains appareils tiers peuvent ne pas être stables, car ces appareils tiers ne sont pas programmés pour traiter certains en-têtes de paquets de couche 2. Pour configurer un tunnel GRE IP stable entre une appliance NetScaler et un appareil tiers, vous pouvez utiliser le paramètre de charge utile GRE du jeu de commandes du tunnel IP GRE. Le paramètre de charge utile GRE peut également être appliqué à un GRE avec tunnel IPSec.

Vous pouvez définir le paramètre de charge utile GRE pour effectuer l'une des opérations suivantes avant que le paquet ne soit envoyé via le tunnel GRE :

- **Ethernet avec DOT1Q**. Transportez l'en-tête Ethernet ainsi que l'en-tête VLAN. C'est le réglage par défaut. Pour un tunnel lié à un pont réseau, l'en-tête Ethernet interne et l'en-tête VLAN contiennent des informations provenant de l'ARP et de la table des ponts de l'appliance NetScaler. Pour un tunnel défini comme saut suivant vers une règle PBR, l'adresse MAC de destination Ethernet interne est définie sur zéro et l'en-tête du VLAN spécifie le VLAN par défaut. Le paquet encapsulé (GRE) envoyé depuis le point de terminaison du tunnel NetScaler a le format suivant :

Outer Ethernet Header	Outer IP Header	GRE Header	Inner Ethernet	Inner VLAN header	Inner IP/IPv6/ARP header	Inner TCP/UDP Header	Payload

- **Ethernet**. Transportez l'en-tête Ethernet mais supprimez l'en-tête VLAN. Étant donné que les paquets ne transportent aucune information VLAN dans le tunnel, pour un tunnel doté de ce paramètre et lié à un netbridge, vous devez lier un VLAN approprié au netbridge afin que, lors de la réception de paquets sur le tunnel, NetScaler puisse transférer ces paquets vers le VLAN spécifié. Si le tunnel est défini comme saut suivant dans une règle PBR, NetScaler achemine les paquets reçus sur le tunnel. Le paquet encapsulé (GRE) envoyé depuis le point de terminaison du tunnel NetScaler a le format suivant :

Outer Ethernet header	Outer IP header	GRE Header	Inner Ethernet header	Inner IP/IPv6/ARP header	Inner TCP/UDP header	Payload

- **IP**. Supprimez l'en-tête Ethernet ainsi que l'en-tête VLAN. Comme les tunnels dotés de ce paramètre ne comportent pas d'en-têtes de couche 2, ils ne peuvent pas être liés à un netbridge mais peuvent être définis comme saut suivant dans une règle PBR. Lors de la réception du paquet, le terminal du tunnel homologue le consomme ou l'achemine. Le paquet encapsulé (GRE) envoyé depuis le point de terminaison du tunnel NetScaler a le format suivant :

Outer Ethernet header	Outer IP header	GRE header	Inner IP/IPv6 header	Inner TCP/UDP header	Payload

Pour supprimer les en-têtes de couche 2 de paquets dans un tunnel IP GRE à l'aide de l'interface de ligne de commande :

- **ajouter IPTunnel** <grepayload><string><name><remote><remoteSubnetMask><local>[-**protocole** \ [- <GRE**vlan \]] [- <positive_integer**grepayload** \] [- IPsecProfileName** \]**
- **show iptunnel** <tunnelname>

Exemple :

```
> add iptunnel IPTUNNEL-1 203.0.113.133 255.255.255.0 198.51.100.15 -
    protocol GRE - grepayload Ethernet -ipsecProfileName IPTUNNEL-IPSEC
    -1
```



```
2 Done
3 <!--NeedCopy-->
```

Trafic IPv6 via les tunnels IPV4 GRE

L'appliance NetScaler prend en charge le transfert du trafic IPv6 via un tunnel GRE IPV4. Cette fonctionnalité peut être utilisée pour permettre la communication entre des réseaux IPv6 isolés sans mettre à niveau l'infrastructure IPv4 entre eux.

Pour configurer cette fonctionnalité, vous associez une règle PBR6 au tunnel GRE IPv4 configuré via lequel vous souhaitez que NetScaler envoie et reçoive du trafic IPv6. Les paramètres d'adresse IPv6 source et d'adresse IPv6 de destination de la règle PBR6 spécifient les réseaux IPv6 dont le trafic doit traverser le tunnel GRE IPv4.

Remarque : le protocole IPsec n'est pas pris en charge sur les tunnels IPv4 GRE configurés pour transférer des paquets IPv6.

Pour créer un tunnel IPv4 GRE à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter IPTunnel - protocole GRE<name><remote><remoteSubnetMask><local>
- **afficher IPTunnel** <name>

Pour associer une règle PBR6 à un tunnel IPv4 GRE à l'aide de l'interface de ligne de commande :

- **ajouter nds pbr6**ALLOW- **ScripV6** <pbrName><network-range**-DSTipv6** - IPTunnel** <network-range><tunnelName>
- **afficher le PBR**

Exemple de configuration

Dans l'exemple de configuration suivant, le tunnel IP GRE Tunnel-v6ONv4 est créé avec l'adresse IP du point de terminaison du tunnel distant 10.10.6.30 et l'adresse IP du point de terminaison du tunnel local 10.10.5.30. Le tunnel est ensuite lié à pbr6 PBR6-v6onv4. Le Srcipv6 spécifie le réseau IPv6 connecté au point de terminaison local et DestIPv6 spécifie le réseau IPv6 connecté au point de terminaison distant. Le trafic provenant de ces réseaux IPv6 est autorisé à traverser le tunnel IPv4 GRE.

```
1 > add ipTunnel TUNNEL-V6onV4 10.10.6.30 255.255.255.255 10.10.5.30 -
     protocol GRE
2 -ipsecProfileName None
3 Done
4 > add ns pbr6 PBR6-V6onV4 ALLOW -srcIPv6 = 2001:0db8:1::1-2001:0db8
     :1::255 -destIPv6 =
5 1-2001:0db8:4::255 -ipTunnel TUNNEL-V6onV4
```



```
<!--NeedCopy-->
```

Envoyer le trafic de réponse via un tunnel IP-IP

Vous pouvez configurer une appliance NetScaler pour envoyer le trafic de réponse via un tunnel IP-IP au lieu de le rediriger vers la source. Par défaut, lorsque l'appliance reçoit une demande d'un autre NetScaler ou d'un appareil tiers via un tunnel IP-IP, elle achemine le trafic de réponse au lieu de l'envoyer via le tunnel. Vous pouvez utiliser des routes basées sur des politiques (PBR) ou activer le transfert basé sur Mac (MBF) pour envoyer la réponse via le tunnel.

Dans une règle PBR, spécifiez les sous-réseaux aux deux extrémités dont le trafic doit traverser le tunnel. Définissez également le saut suivant comme nom du tunnel. Lorsque le trafic de réponse correspond à la règle PBR, l'appliance NetScaler envoie le trafic via le tunnel.

Vous pouvez également activer MBF pour répondre à cette exigence, mais la fonctionnalité est limitée au trafic pour lequel l'appliance NetScaler stocke les informations de session (par exemple, le trafic lié à l'équilibrage de charge ou aux configurations RNAT). L'appliance utilise les informations de session pour envoyer le trafic de réponse via le tunnel.

Procédures CLI

Pour créer une règle PBR et y associer le tunnel IP-IP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter ns pbr**ALLOW**** **<pbr_name><remote_subnet_range-srCip = - DEStip= - IPTunnel**** <local_subnet_range><tunnel_name>
- **apply ns pbrs**
- **afficher ns pbr** <pbr_name>

Pour activer le transfert basé sur Mac à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **activer le mode NS MBF**
- **show ns mode**

Procédures GUI

Pour créer une règle PBR et y associer le tunnel IP-IP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **PBR.** Dans l'onglet **PBR**, créez une règle **PBR** .
2. Lors de la création du PBR, définissez le **type de saut suivant** sur le **tunnel IP** et le **nom du tunnel IP sur le nom** du tunnel IP-IP configuré.

Pour activer le transfert basé sur Mac à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, puis dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.
2. Sur la page **Configurer les modes**, sélectionnez le **transfert basé sur Mac**.

Exemple de configuration

Prenons l'exemple d'un tunnel IPIP, NS1-NS2-IPIP, qui est configuré entre deux appliances NetScaler NS1 et NS2.

Par défaut, pour toute demande que NS2 reçoit via le tunnel, il achemine le trafic de réponse vers la source au lieu de l'envoyer (à NS1) via le tunnel.

Vous pouvez configurer des routes basées sur des politiques (PBR) ou activer le transfert basé sur MAC (MBF) sur NS2 pour lui permettre d'envoyer la réponse via le tunnel.

Dans l'exemple de configuration suivant sur NS2, NS1-NS2-IPIP est un tunnel IPIP et NS1-NS2-IPIP-PBR est une règle PBR. Pour les demandes (avec une adresse IP source interne comprise entre 10.102.147.0-10.102.147.255 et une adresse IP de destination interne comprise entre 10.102.147.0-10.102.147.255) reçues par NS2 via le tunnel, NS2 envoie la réponse correspondante via le tunnel (à NS1) au lieu de l'acheminer vers la source. La fonctionnalité est limitée au trafic correspondant à la règle PBR.

```
1  > add iptunnel NS1-NS2-IPIP 192.0.2.99 255.255.255.255 203.0.113.99 -
       protocol IPIP
2
3  Done
4  > add pbr NS1-NS2-IPIP-PBR -srcIP 10.102.147.0-10.102.147.255  - destIP
       10.20.1.0-10.20.1.255  - ipTunnel NS1-NS2-IPIP
5
6  Done
7  > apply pbrs
8
9  Done
10 <!--NeedCopy-->
```

Vous pouvez également activer MBF sur NS2. La fonctionnalité est limitée au trafic pour lequel NS2 stocke les informations de session (par exemple, le trafic lié à l'équilibrage de charge ou aux configurations RNAT).

```
1  > enable ns mode MBF
2
3  Done
4  <!--NeedCopy-->
```


Paquets IPv4 de classe E

May 5, 2023

Par défaut, l'appliance NetScaler supprime tous les paquets s'ils contiennent une adresse IPv4 de classe E dans les champs IP source ou IP de destination. Si votre configuration utilise des adresses IPv4 de classe E, vous pouvez configurer l'appliance NetScaler pour traiter les paquets IPv4 de classe E.

Avant de commencer

Avant de commencer à configurer une appliance NetScaler pour traiter les paquets IPv4 de classe E, notez les points suivants :

- Les appliances NetScaler ne prennent pas en charge la configuration d'adresses IPv4 appartenant à NetScaler (par exemple, SNIP et VIP) dans la plage de classe E. Les appliances NetScaler prennent uniquement en charge le traitement des paquets IPv4 de classe E.
- Une appliance NetScaler utilise en interne des adresses IPv4 de classe E pour la fonctionnalité IPv6. L'appliance NetScaler ne prend pas en charge les deux fonctionnalités (traitement des paquets IPv4 de classe E et prise en charge du protocole IPv6) fonctionnant simultanément. L'appliance NetScaler impose une restriction pour ne pas activer la fonctionnalité IPv6 lorsque le traitement des paquets IPv4 de classe E est activé, et vice versa.

Étapes de configuration

La configuration d'une appliance NetScaler pour traiter des paquets IPv4 de classe E consiste à activer le paramètre de couche 3 des **clients d'adresses IPv4 de classe E** (**AllowClasseIPv4**).

Procédures CLI

Pour configurer l'appliance NetScaler afin qu'elle traite les paquets IPv4 de classe E à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set l3param**-AllowClasseIPv4**(ACTIVÉ | DÉSACTIVÉ)****
- **afficher l3param**

Exemple de configuration :

```
1 > set l3param -allowClassEIPv4 ENABLED
2
3 Done
```



```
4
5  > sh l3param
6
7      Network L3 related Configuration Parameters
8
9      icmpgen_rate_threshold      : 100
10
11     srcnat                      : ENABLED
12
13     override_rnat               : DISABLED
14
15     drop_df_flag                : DISABLED
16
17     .
18
19     .
20
21     .
22
23     IPv6DynamicRouting          : DISABLED
24
25     allowClassEIPv4             : ENABLED
26
27 Done
28 <!--NeedCopy-->
```

Procédures GUI

Pour configurer l'appliance NetScaler afin qu'elle traite les paquets IPv4 de classe E à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, puis dans la section **Paramètres**, cliquez sur **Configurer les paramètres de la couche 3**.
2. Sélectionnez les **clients d'adresse IPv4 Classe E** et cliquez sur **OK** .

Surveillez les ports libres disponibles sur une appliance NetScaler pour une nouvelle connexion principale

May 5, 2023

Pour communiquer avec les serveurs physiques ou d'autres appareils homologues, l'appliance NetScaler utilise une adresse IP appartenant à Citrix comme adresse IP source. L'appliance NetScaler

gère un pool d'adresses IP et sélectionne dynamiquement une adresse IP lors de la connexion à un serveur. En fonction du sous-réseau dans lequel le serveur physique est placé, l'appliance décide de l'adresse IP à utiliser. Ce pool d'adresses est utilisé pour envoyer du trafic et surveiller les sondes.

Vous pouvez afficher le nombre total de ports libres disponibles sur les adresses IP détenues par NetScaler pour une nouvelle connexion principale. Ces informations vous aident à déterminer s'il est nécessaire de disposer d'un plus grand nombre d'adresses IP appartenant à NetScaler si les ports libres disponibles sont presque épuisés.

Vous pouvez fournir les informations suivantes à l'appliance NetScaler afin de calculer le nombre total de ports libres disponibles pour une nouvelle connexion principale :

- Adresse IP appartenant à Citrix (facultatif)
- Adresse IP de destination
- Port de destination
- Protocole TCP ou non TCP

Lorsque vous spécifiez toutes les informations, à l'exception de la spécification d'une adresse IP appartenant à Citrix :

- L'appliance NetScaler effectue une recherche d'itinéraire pour trouver toutes les adresses IP appartenant à NetScaler qui peuvent se connecter à l'adresse IP de destination. L'appliance trouve et affiche ensuite le nombre total de ports libres disponibles sur ces adresses IP appartenant à NetScaler pour la nouvelle connexion principale spécifiée.

  > **Remarque :**
  >
  > L'appliance NetScaler n'effectue pas de recherche ECMP, de chemin de recherche LLB ou de chemin de recherche PBR pour rechercher les adresses IP appartenant à NetScaler qui peuvent se connecter à l'adresse IP de destination.

Lorsque vous spécifiez toutes les informations, y compris la spécification d'une adresse IP appartenant à Citrix :

- L'appliance NetScaler affiche le nombre de ports libres disponibles sur l'adresse IP spécifiée pour la nouvelle connexion principale spécifiée.

Avant de commencer

Avant d'afficher le nombre total de ports libres disponibles pour une nouvelle connexion dorsale, notez les points suivants :

- L'appliance NetScaler n'effectue pas de recherche ECMP, de chemin de recherche LLB ou de chemin de recherche PBR pour rechercher les adresses IP appartenant à NetScaler qui peuvent se connecter à l'adresse IP de destination.

- L'appliance NetScaler ne prend pas en charge l'affichage des ports libres disponibles sur une adresse IP locale de lien.

Étapes à suivre pour afficher le nombre de ports libres disponibles sur une appliance NetScaler pour une nouvelle connexion principale

Pour afficher le nombre total de ports libres disponibles sur une appliance NetScaler pour une nouvelle connexion principale :

À l'invite de commandes, tapez :

- **show portallocation** [-**srcIP** \<ip_addr|ipv6_addr>] -**destIP** <ip_addr|ipv6_addr> -**destPort** <port> -**protocol** <1 for TCP, 0 for non-TCP protocol>

Exemple : nombre total de ports libres disponibles sur une appliance NetScaler autonome :

```
> show portallocation -destip 198.51.100.30 -destport 80 -protocol 1

        Freeports available : 64505
 Done


> show portallocation -srcip 192.0.2.30 -destip 198.51.100.30 -destport
    80 -protocol 1

        Freeports available for IPAddress 192.0.2.30 : 20505
 Done
<!--NeedCopy-->
```

Exemple : nombre total de ports libres disponibles sur une configuration de cluster :

L'exemple de sortie suivant affiche le nombre total de ports libres disponibles sur chaque nœud d'une configuration de cluster à deux nœuds.

```
> show portallocation -destip 198.51.100.30 -destport 80 -protocol 1

    Node Id: 1
    Freeports available : 32321

    Node Id: 0
    Freeports available : 32184

Done
<!--NeedCopy-->
```


Surveillez l'utilisation des ports sur une appliance NetScaler pour les connexions dorsales à l'aide du SNMP

Vous pouvez utiliser l'alarme PORT-ALLOC-EXCEED SNMP pour surveiller l'utilisation des ports sur une appliance NetScaler pour les connexions dorsales.

PORT-ALLOC-EXCEED L'alarme SNMP inclut les normal-threshold paramètres high-threshold et, qui spécifient le total des ports alloués aux adresses IP détenues par NetScaler sous forme de pourcentages. Par exemple, si le high-threshold paramètre est défini sur 90, l'appliance NetScaler génère et envoie des messages d'interruption lorsque l'événement suivant se produit :

- lorsque le pourcentage d'allocation de ports dépasse 90 % sur l'une des adresses IP appartenant à NetScaler pour les connexions dorsales

Les alertes SNMP vous aident à déterminer si vous avez besoin d'un plus grand nombre d'adresses IP appartenant à NetScaler si les ports libres disponibles sont presque épuisés.

Pour surveiller l'utilisation des ports sur une appliance NetScaler pour les connexions dorsales à l'aide du SNMP

À l'invite de commandes, tapez :

- **set snmp alarm PORT-ALLOC-EXCEED** -**logging** (ENABLED | DISABLED) -**severity** <severity> -**state** (ENABLED | DISABLED) -**thresholdValue** <positive_integer> [-**normalValue** \<positive_integer>] -**time** <secs>
- **sh snmp alarm PORT-ALLOC-EXCEED**

Exemple :

```
> set snmp alarm PORT-ALLOC-EXCEED -logging ENABLED  -severity Major -
    state ENABLED -thresholdValue 90 -time 1200
Done

> sh snmp alarm port-alloc-EXCEED

Alarm                   Alarm Threshold     Normal Threshold    Time
      State       Severity        Logging
-----                   ---------------     ----------------    ----
      --------    -------------   --------
1) PORT-ALLOC-EXCEED    80                  80                  7200
      ENABLED     Major           ENABLED
Done

<!--NeedCopy-->
```

Pour plus d'informations sur la configuration des alarmes SNMP et des écouteurs d'interruptions SNMP, consultez la section Configuration de NetScaler pour générerdes interruptions SNMP.

Interfaces

May 5, 2023

Avant de commencer à configurer les interfaces, déterminez si votre configuration peut utiliser le mode de transfert basé sur Mac et activez ou désactivez ce paramètre système en conséquence. Le nombre d'interfaces dans votre configuration est différent selon les différents modèles de l'appliance NetScaler. Outre la configuration d'interfaces individuelles, vous pouvez les regrouper de manière logique, en utilisant des VLAN pour restreindre le flux de données au sein d'un ensemble d'interfaces, et vous pouvez agréger des liens en canaux. Dans une configuration haute disponibilité, vous pouvez configurer une adresse MAC virtuelle si nécessaire. Si vous utilisez le mode L2, vous souhaiterez peut-être modifier le vieillissement de la table de pont.

Lorsque votre configuration est terminée, décidez si vous devez activer le paramètre système pour la découverte du chemin MTU. Les appliances NetScaler peuvent être déployées en mode actif-actif à l'aide de VRRP. Un déploiement actif-actif permet non seulement d'éviter les temps d'arrêt, mais aussi d'utiliser efficacement toutes les appliances NetScaler du déploiement. Vous pouvez utiliser l'outil Network Visualizer pour visualiser la configuration réseau d'un déploiement NetScaler et configurer des interfaces, des canaux, des VLAN et des groupes de ponts.

Configuration du transfert sur Mac

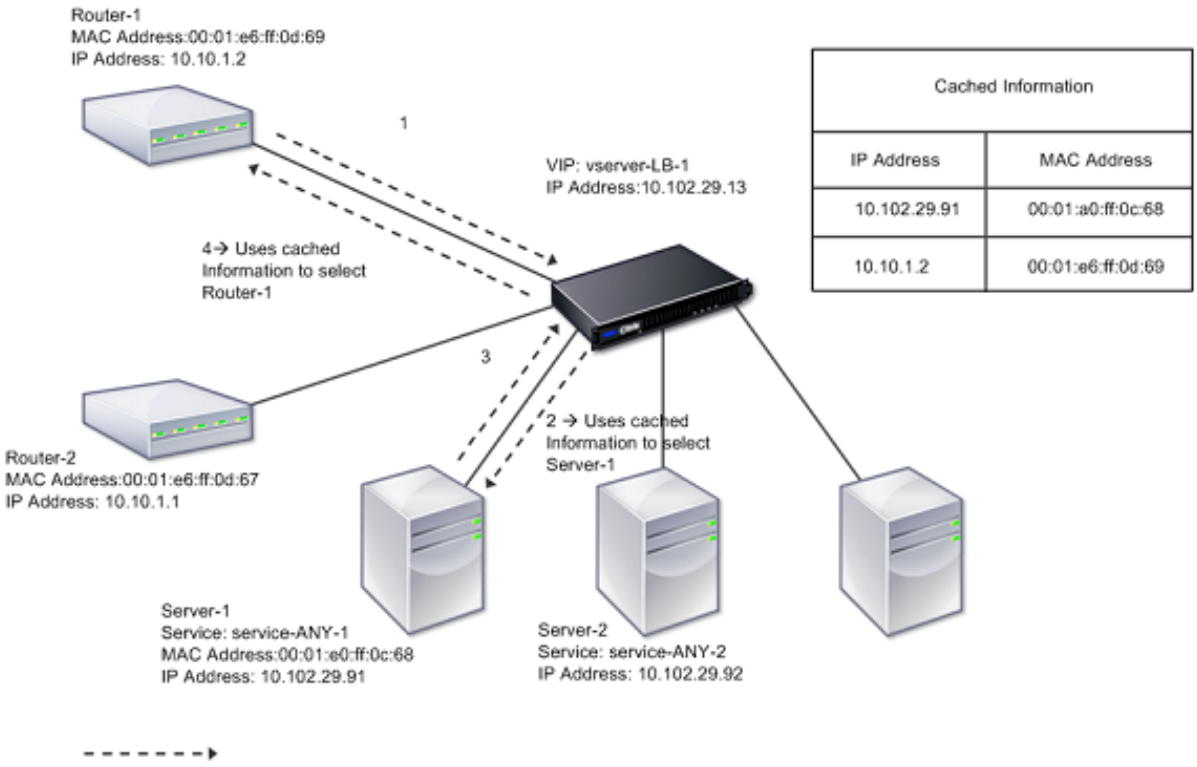
May 5, 2023

Lorsque le transfert basé sur Mac (MBF) est activé, lorsqu'une demande parvient à l'appliance NetScaler, celle-ci mémorise l'adresse MAC source de la trame et l'utilise comme adresse MAC de destination pour les réponses qui en résultent. Le transfert basé sur MAC peut être utilisé pour éviter les recherches sur plusieurs routes/ARP et pour éviter les flux de paquets asymétriques. Le transfert basé sur Mac peut être requis lorsque NetScaler est connecté à plusieurs appareils statiques, tels que des VPN ou des pare-feux, car il garantit que le trafic de retour est envoyé vers le même appareil que celui d'où provient le trafic initial.

Le transfert basé sur Mac est utile lorsque vous utilisez des appareils VPN, car il garantit que tout le trafic passant par un VPN repasse par le même périphérique VPN.

Le diagramme de topologie suivant illustre le processus de transfert basé sur Mac.

Figure 1. Mode de transfert basé sur Mac



Lorsque le transfert basé sur MAC (MBF) est activé, NetScaler met en cache l'adresse MAC de :

- La source (un périphérique de transmission tel qu'un routeur, un pare-feu ou un périphérique VPN) de la connexion entrante.
- Le serveur qui répond aux demandes.

Lorsqu'un serveur répond via l'appliance NetScaler, l'appliance définit l'adresse MAC de destination du paquet de réponse sur l'adresse mise en cache, garantissant ainsi que le trafic circule de manière symétrique, puis transmet la réponse au client. Le processus contourne les fonctions de recherche de table de routage et de recherche ARP. Toutefois, lorsque NetScaler initie une connexion, il utilise la route et les tables ARP pour la fonction de recherche. Dans une configuration de retour direct du serveur, vous devez activer le transfert basé sur Mac.

Pour plus d'informations sur les configurations de retour direct du serveur, voir Équilibrage de charge.

Certaines topologies de déploiement peuvent exiger que les chemins entrants et sortants passent par différents routeurs. Le transfert basé sur Mac romprait cette conception topologique.

MBF devrait être désactivé dans les situations suivantes :

- **Lorsqu' un serveur utilise l'association de cartes d'interface réseau (NIC) sans utiliser LACP (802.1ad Link Aggregation).** Pour activer le transfert basé sur Mac dans ce cas, vous devez utiliser un périphérique de couche 3 entre NetScaler et le serveur.
  Remarque : Le MBF peut être activé lorsque le serveur utilise l'association NIC et LACP, car l'interface virtuelle utilise une adresse MAC unique.

- **Lorsque le clustering de pare-feu est utilisé**. Le clustering du pare-feu suppose que l'ARP est utilisé pour résoudre l'adresse MAC du trafic entrant. Parfois, l'adresse MAC entrante peut être une adresse MAC non clusterisée et ne doit pas être utilisée pour le traitement des paquets entrants.

Lorsque le MBF est désactivé, l'appliance utilise la connectivité L2 ou L3 pour transmettre les réponses des serveurs aux clients. Selon la table de routage, les routeurs utilisés pour la connexion sortante et la connexion entrante peuvent être différents. En cas de trafic inverse (réponse du serveur) :

- Si la source et la destination se trouvent sur des sous-réseaux IP différents, l'appliance utilise la recherche d'itinéraire pour localiser la destination.
- Si la source se trouve sur le même sous-réseau que la destination, NetScaler consulte la table ARP pour localiser l'interface réseau et lui transmet le trafic. Si la table ARP n'existe pas, NetScaler demande les entrées ARP.

Pour activer ou désactiver le transfert basé sur Mac à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **activer le mode NS MBF**
- **désactiver le mode NS MBF**

Pour activer ou désactiver le transfert sur Mac à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.
2. Sélectionnez ou désactivez l'option de **transfert sur Mac** .

Transfert basé sur MAC pour une configuration d'équilibrage de charge

Certaines configurations d'équilibrage de charge nécessitent que l'appliance NetScaler contourne le MBF global (s'il est activé) pour ces configurations et utilise à la place les recherches Route/ARP pour envoyer des paquets vers la destination.

Le paramètre MBF d'un profil réseau est utilisé pour activer ou désactiver le MBF pour une configuration d'équilibrage de charge spécifique. Le MBF peut être défini pour le côté client ainsi que pour le côté serveur d'une configuration d'équilibrage de charge en liant les profils réseau (MBF activé ou désactivé) au serveur virtuel et aux services.

Par exemple, si un profil réseau avec MBF désactivé est lié au serveur virtuel d'une configuration d'équilibrage de charge, l'appliance NetScaler contourne le MBF global (s'il est activé) et utilise à la place les recherches Route/ARP pour envoyer des paquets de réponse aux clients.

Avant de commencer

Avant de commencer à configurer MBF pour une configuration d'équilibrage de charge, notez les points suivants :

- Dans une configuration d'équilibrage de charge, le côté client (serveur virtuel) et le côté serveur (service/groupes de services) peuvent avoir des paramètres MBF différents.
- Une configuration d'équilibrage de charge hérite du paramètre MBF global si le MBF n'est pas défini explicitement dans les profils réseau liés au serveur virtuel et aux services.
- Dans une configuration d'équilibrage de charge, le côté serveur (service) hérite du paramètre MBF côté client du profil réseau lié au serveur virtuel si aucun profil réseau n'est lié au service.
- Dans une configuration d'équilibrage de charge avec mode retour direct au serveur, le côté client hérite du paramètre MBF du profil réseau lié au service.
- Dans une configuration de commutation de contenu, le côté client prend le paramètre MBF du profil réseau lié au serveur virtuel de commutation de contenu plutôt que du serveur virtuel d'équilibrage de charge cible.

Limitations

Avant de commencer à configurer MBF pour une configuration d'équilibrage de charge, notez les limites suivantes :

- Le paramètre MBF pour les configurations d'équilibrage de charge n'est pas pris en charge dans une configuration de cluster.
- Pour un serveur virtuel d'équilibrage de charge avec mode MAC ou paramètres L2Conn, le MBF est activé quel que soit le paramètre MBF dans le profil réseau lié au serveur virtuel.
- L'appliance NetScaler ne prend pas en charge la configuration du MBF pour les moniteurs d'équilibrage de charge utilisant le profil réseau. En d'autres termes, le paramètre MBF d'un profil réseau n'est pas appliqué aux écrans auxquels le profil réseau est lié. Le paramètre MBF global est appliqué aux moniteurs quel que soit le paramètre MBF du profil net lié.

Configurer MBF pour la configuration de l'équilibrage de charge

La configuration de MBF pour une configuration d'équilibrage de charge comprend les tâches suivantes :

- Activez le paramètre MBF dans un profil réseau.
- Liez le profil réseau à un serveur virtuel ou à des services d'équilibrage de charge.

Pour activer MBF dans un profil réseau à l'aide de l'interface de ligne de commande :

- Pour activer MBF lors de l'ajout d'un profil réseau, à l'invite de commande, tapez :
  - **ajouter NetProfile-**MBF** (**ACTIVÉ | DÉSACTIVÉ**)** <name>

  - **afficher le profil réseau** <name>
- Pour activer MBF dans un profil réseau existant, à l'invite de commande, tapez :
  - **définir NetProfile-**MBF** (**ACTIVÉ | DÉSACTIVÉ**)** <name>
  - **afficher le profil réseau** <name>

Pour activer MBF dans un profil réseau à l'aide de l'interface graphique**

1. Accédez à **Système** > **Réseau** > **Profils réseau**.
2. Activez le paramètre **MBF** lors de l'ajout ou de la modification d'un profil réseau.

Dans l'exemple de configuration suivant, le profil réseau NETPROFILE-MBF-LBVS a activé MBF et est lié au serveur virtuel d'équilibrage de charge LBVS-1. En outre, le profil net NETPROFILE-MBF-SVC a activé MBF et est lié à un service d'équilibrage de charge SVC-1.

```
> add netprofile NETPROFILE-MBF-LBVS -MBF ENABLED

Done

> add netprofile NETPROFILE-MBF-SVC -MBF ENABLED

Done

> set lb vserver LBVS-1 -netprofile NETPROFILE-MBF-LBVS

Done

> set service SVC-1 -netprofile NETPROFILE-MBF-SVC

Done

<!--NeedCopy-->
```

Configuration des interfaces réseau

May 5, 2023

Les interfaces réseau de l'appliance NetScaler sont numérotées en `<slot><port>` notation. Après avoir configuré vos interfaces, affichez les interfaces et leurs paramètres pour vérifier la configuration. Vous pouvez également afficher ces informations pour résoudre un problème de configuration.

Pour gérer les interfaces réseau, vous pouvez procéder comme suit :

- Activez certaines interfaces et désactivez-en d'autres.
- Réinitialisez une interface pour renégocier ses paramètres.

- Efface les statistiques accumulées pour une interface.

Pour vérifier la configuration, vous pouvez afficher les paramètres de l'interface. Vous pouvez afficher les statistiques d'une interface afin d'évaluer son état.

Définissez les paramètres de l'interface réseau

La configuration de l'interface réseau n'est ni synchronisée ni propagée. Pour une paire HA, vous devez effectuer la configuration sur chaque unité indépendamment.

Pour définir les paramètres de l'interface réseau à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
1 -  set interface <id> [-speed <speed>] [-duplex <duplex>] [-flowControl
      <flowControl>] [-autoneg ( DISABLED | ENABLED )] [-haMonitor ( ON |
      OFF )] [ ( ON | OFF )] [-tagall ( ON | OFF )] [-lacpMode <lacpMode
     >] [-lacpKey<positive_integer>] [-lacpPriority <positive_integer>]
     [-lacpTimeout (LONG | SHORT )] [-ifAlias <string>] [-throughput <
     positive_integer>][-bandwidthHigh <positive_integer> [-
     bandwidthNormal <positive_integer>]]
2 -  show interface [<id>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > set interface 1/8 -duplex full
2  Done
3 <!--NeedCopy-->
```

Pour définir les paramètres de l'interface réseau à l'aide de l'interface graphique :

Accédez à **Système > Réseau > Interfaces**, sélectionnez l'interface réseau que vous souhaitez modifier (par exemple, 1/8), cliquez sur **Modifier**, puis définissez les paramètres.

Configuration de la taille et du type de sonnerie de réception pour une interface

Vous pouvez augmenter la taille et le type de sonnerie de réception pour les interfaces IX, F1X, F2X ou F4X sur les plateformes NetScaler MPX et SDX.

L'augmentation de la taille de l'anneau permet de mieux gérer les pics de trafic, mais cela peut avoir un impact sur les performances. Une taille de sonnerie allant jusqu'à 8192 est prise en charge pour les interfaces IX. Une taille d'anneau allant jusqu'à 4 096 est prise en charge pour les interfaces F1X, F2X et F4X. La taille de bague par défaut reste 2048.

Les types d'anneaux d'interface sont élastiques par défaut. Leur taille augmente ou diminue en fonction du taux d'arrivée des paquets. Vous pouvez configurer le type de sonnerie comme « fixe », auquel cas la taille de la sonnerie ne change pas en fonction du débit de trafic.

Remarque : Cette fonctionnalité est prise en charge à partir de la version 13.0 build 41.x et est prise en charge sur les plates-formes dotées d'interfaces IX, F1X, F2X ou F4X.

Utilisez la `show hardware` commande pour identifier si votre appliance possède des interfaces IX, F1X, F2X ou F4X.

Exemples :

Le modèle suivant possède 16 interfaces F1X (10G) et 4 interfaces F4X (40G).

```
> sh hardware
        Platform: NSMPX-25000-40G 20\*CPU+16\*F1X+4\*F4X+2\*E1K+2*CVM
            N3 250040
        Manufactured on: 12/16/2016
        CPU: 2800MHZ
        Host Id: 234913926
        Serial no: N43RJCRV3X
        Encoded serial no: N43RJCRV3X
        Netscaler UUID: 336a32d6-2cfa-11e8-bf01-00e0ed5dd23c
        BMC Revision: 4.08
 Done
<!--NeedCopy-->
```

Le modèle suivant possède 2 interfaces 1X (10G).

```
> sh hardware
        Platform: NSMPX-10500 8\*CPU+2\*E1K+8\*E1K+2\*IX+8*CVM 1620
            760100
        Manufactured on: 12/27/2010
        CPU: 2832MHZ
        Host Id: 1707114630
        Serial no: 7VZZV1ZXJ4
        Encoded serial no: 7VZZV1ZXJ4
        Netscaler UUID: eb1bfd72-5176-11e7-ba18-00e0ed1b0d12
 Done
<!--NeedCopy-->
```

Pour configurer la taille et le type de sonnerie à l'aide de l'interface de ligne de commande sur la ligne de commande, tapez :

```
set interface <id> -ringsize <positive_integer> -ringtype ( Elastic |
    Fixed )
<!--NeedCopy-->
```


Paramètres :

`ringsize`:

Taille de la sonnerie de réception de l'interface. Un nombre plus élevé fournit davantage de mémoires tampon pour gérer le trafic entrant.

Valeur par défaut : 2048 Valeur
minimale : 512 Valeur
maximale : 16384

`ringtype`:

Type d'anneau de réception de l'interface. Un type d'anneau fixe préalloue le nombre configuré de mémoires tampon quel que soit le débit de trafic. En revanche, un anneau élastique se dilate et se rétrécit en fonction du débit du trafic entrant.

Valeurs possibles : élastique, fixe

Valeur par défaut : Elastic

Exemple :

```
> set interface 40/2 -ringsize 4096 -ringtype Fixed
 Done
> show interface 40/2

1)      Interface 40/2 (40G Ethernet, CR4, 40 Gbit) #21  flags=0xc020 <
    ENABLED, UP, UP, autoneg, HAMON, HEARTBEAT, 802.1q> MTU=1500, native
     vlan=10, MAC=00:e0:ed:75:14:2a, uptime 119h26m32s
        Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
           throughput 0
        Actual: media UTP, speed 40000, duplex FULL, fctl OFF,
           throughput 40000
        LLDP Mode: NONE, LR Priority: 1024
        RX: Pkts(1443972660032) Bytes(1457207315336105) Errs(0) Drops
           (53319) Stalls(0)
        TX: Pkts(1452311431262) Bytes(1458534011197761) Errs(0) Drops
           (788) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
        Rx Ring: Configured size=4096, Actual size=4096, Type: Fixed
 Done
<!--NeedCopy-->
```

La dernière ligne indique la taille de bague configurée et réelle, ainsi que le type de bague.

Pour configurer la taille et le type de bague à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > Interfaces**.
2. Sélectionnez votre interface et cliquez sur **Modifier**.
3. Dans **Taille de la bague**, spécifiez l'une des options suivantes :
   - **Interfaces IX :** 512, 1024, 2048, 4096 ou 8192.
   - **Interfaces F1X, F2X ou F4X :** 512, 1024, 2048 ou 4096.
4. Dans **Type de bague**, sélectionnez Elastique ou Fixe.
5. Cliquez sur **OK**.

Activer et désactiver les interfaces réseau

Par défaut, les interfaces réseau sont activées. Désactivez toute interface réseau qui n'est pas connectée au réseau afin qu'elle ne puisse ni envoyer ni recevoir de paquets. La désactivation d'une interface réseau connectée au réseau dans une configuration haute disponibilité peut provoquer un basculement.

Pour plus d'informations sur la haute disponibilité, voir Haute disponibilité.

Pour activer ou désactiver une interface réseau à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
1 -  enable interface <interface_num>
2 -  show interface <interface_num>
3 -  disable interface <interface_num>
4 -  show interface <interface_num>
5 <!--NeedCopy-->
```

Exemple :

```
1  > enable interface 1/8
2   Done
3  > show interface 1/8
4          Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
5          flags=0x4004000 <ENABLED, DOWN, BOUND to LA/1, down, autoneg,
               802.1q>
6          MTU=1514, MAC=00:d0:68:15:fd:3d, downtime 906h58m40s
7          Requested: media UTP, speed AUTO, duplex FULL, fctl OFF,
               throughput 0
8          RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
9          TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
10         NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
```



```
        Bandwidth thresholds are not set.
Done
<!--NeedCopy-->
```

Pour activer ou désactiver une interface réseau à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > Interfaces**.
2. Sélectionnez l'interface réseau et, dans la liste des **actions**, sélectionnez Activer ou Désactiver.

Réinitialisation des interfaces réseau

Les paramètres de l'interface réseau contrôlent des propriétés telles que le duplex et la vitesse. Pour renégocier les paramètres d'une interface réseau, vous devez la réinitialiser.

Pour réinitialiser une interface réseau à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
-  reset interface <interface_num>
-  show interface <interface_num>
<!--NeedCopy-->
```

Exemple :

```
> reset interface 1/8
 Done
<!--NeedCopy-->
```

Pour réinitialiser une interface réseau à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > Interfaces**.
2. Sélectionnez l'interface réseau et, dans la liste des **actions**, sélectionnez **Réinitialiser l'interface**.

Surveiller une interface réseau

Vous pouvez afficher les statistiques de l'interface réseau pour contrôler les paramètres et utiliser les informations pour vérifier l'état de l'interface réseau. Vous pouvez surveiller des paramètres tels que les paquets envoyés et reçus, le débit, les unités de données du protocole LACP (Link Aggregate Control Protocol) et les erreurs. Vous pouvez effacer les statistiques d'une interface réseau pour contrôler ses statistiques à partir du moment où elles sont effacées.

Pour afficher les statistiques des interfaces réseau à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :


```
-  stat interface <interface_num>
<!--NeedCopy-->
```

Exemple :

```
> stat interface 1/8
 Done
<!--NeedCopy-->
```

Pour effacer les statistiques d'une interface réseau à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
-  clear interface <interface_num>
<!--NeedCopy-->
```

Exemple :

```
> clear interface 1/8
 Done
<!--NeedCopy-->
```

Pour afficher les statistiques d'une interface à l'aide de l'interface graphique :

Accédez à **Système > Réseau > Interfaces**, sélectionnez l'interface réseau et cliquez sur **Statistiques d'interface**.

Pour effacer les statistiques d'une interface réseau à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > Interfaces**.
2. Sélectionnez l'interface réseau et, dans la liste des **actions**, sélectionnez **Effacer les statistiques**.

Configuration des règles de session de transfert

May 5, 2023

Par défaut, l'appliance NetScaler ne crée pas d'entrées de session pour le trafic qu'elle transfère uniquement (mode L3). Dans le cas où une demande d'un client demandant à l'appliance de transférer vers un serveur entraîne une réponse qui doit être renvoyée par le même chemin, vous pouvez créer une règle de session de transfert. Une règle de session de transfert crée des entrées de session de transfert pour le trafic qui provient ou est destiné à un réseau particulier et qui est

transféré par NetScaler. Vous pouvez créer des règles de session de transfert pour le trafic IPv4 ainsi que pour le trafic IPv6.

Lorsque vous configurez une règle de session de transfert IPv4, vous pouvez spécifier une adresse réseau IPv4 ou une ACL étendue comme condition d'identification du trafic IPv4 pour lequel créer une entrée de session de transfert :

- **Adresse réseau**. Lorsque vous spécifiez une adresse réseau IPv4, l'appliance crée des sessions de transfert pour le trafic IPv4 dont la source ou la destination correspond à l'adresse réseau.
- **Règle ACL étendue**. Lorsque vous spécifiez une règle ACL étendue, l'appliance crée des sessions de transfert pour le trafic IPv4 qui répondent aux conditions spécifiées dans la règle ACL étendue.

Lorsque vous configurez une règle de session de transfert IPv6, vous pouvez spécifier un préfixe IPv6 ou un ACL6 comme condition d'identification du trafic IPv6 pour lequel créer une entrée de session de transfert :

- **Préfixe IPv6**. Lorsque vous spécifiez un préfixe IPv6, l'appliance crée des sessions de transfert pour le trafic IPv6 dont la source ou la destination correspond au préfixe IPv6.
- **Règle ACL6.** Lorsque vous spécifiez une règle ACL6, l'appliance crée des sessions de transfert pour le trafic IPv6 qui répondent aux conditions spécifiées dans la règle ACL6.

Pour créer une règle de session de transfert IPv4 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une règle de session de transfert et vérifier la configuration :

- ajouter ForwardingSession <name>[\ <network>\<netmask>] | [-aclname \<string>] -connfailover (ACTIVÉ | DÉSACTIVÉ)
- show forwardingSession

Exemple :

```
A network address as the condition:

> add forwardingSession fs-nw-1 10.102.105.51 255.255.255.255
 Done

An ACL as the condition:

> add forwardingSession fs-acl-1 acl1
 Done
<!--NeedCopy-->
```

Pour configurer une règle de session de transfert IPv4 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Sessions de transfert, ajoutez une nouvelle session de transfert IPv4 ou modifiez une session de transfert existante.

Pour créer une règle de session de transfert IPv6 à l'aide de l'interface de ligne de commande :

- À l'invite de commandes, tapez les commandes suivantes pour créer une règle de session de transfert et vérifier la configuration :
  - <string>ajouter une session de transfert <name>[\<IPv6 prefix>] | [-acl6name \]
  - show forwardingSession

  Exemple :

```
    An IPv6 prefix as the condition:

    > add forwardingSession fsv6-pfx-1 3ffe::/64
     Done

    An ACL6 rule as the condition:

    > add forwardingSession fsv6-acl6-1  - acl6name ACL6-FS
     Done
<!--NeedCopy-->
```

Pour configurer une règle de session de transfert IPv6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Sessions de transfert, ajoutez une nouvelle session de transfert IPv6 ou modifiez une session de transfert existante.

Affectation d'une règle ACL à une règle de session de transfert existante

Vous pouvez attribuer une règle ACL à une règle de session de transfert basée sur une adresse réseau/un préfixe IPv6, auquel cas elle devient une règle de session de transfert basée sur une ACL. Vous pouvez également remplacer une règle ACL existante par une autre règle ACL dans une règle de session de transfert basée sur une ACL. Une fois que les entrées de session de transfert associées existantes (le cas échéant) ont expiré, les règles commencent à utiliser l'ACL nouvellement attribuée pour identifier le trafic IPv4/IPv6 pour lequel créer une entrée de session de transfert.

Pour attribuer une règle ACL étendue à une règle de session de transfert IPv4 existante à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- `set forwardingSession <name> [-aclname <string>]`
- `show forwardingSession <name>`

Pour attribuer une règle ACL6 à une règle de session de transfert IPv6 existante à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- `set forwardingSession <name> [-acl6name <string>]`
- `show forwardingSession <name>`

Exemple :

```
1 > add forwardingSession FS-1 -aclname ACL-9
2 Done
3
4 > add forwardingSession FS6-1  - acl6name ACL6-9
5 Done
```

Désactivation de la direction pour le transfert de sessions sur une configuration de cluster

Le comportement par défaut d'un cluster NetScaler est que le nœud qui reçoit le trafic (récepteur de flux) dirige le trafic vers un autre nœud (processeur de flux), qui traite le trafic. La direction du trafic du récepteur de flux vers le processeur de flux s'effectue via le panneau arrière du cluster et est appelée direction.

Le pilotage peut représenter une surcharge pour le traitement en temps réel ou lorsque la configuration inclut des liaisons à latence élevée.

Le pilotage des sessions de transfert peut désormais être désactivé afin que le traitement devienne local pour le récepteur de flux. C'est-à-dire que le récepteur de débit devient le processeur de débit.

Avant de commencer

Prenez note des points suivants avant de configurer les règles de session de transfert dans une configuration de cluster :

- Vous devez configurer les ensembles de liens à utiliser pour le transfert de sessions.
- Vous devez activer le transfert basé sur MAC (MBF) dans la configuration du cluster.

Configuration des règles de session de transfert dans une configuration de cluster

La désactivation du pilotage pour le transfert des règles de session dans une configuration de cluster peut être effectuée aux deux niveaux suivants :

- **Niveau de règle de session de transfert spécifique**. Activez le paramètre Process Local lors de l'ajout d'une nouvelle règle de session de transfert ou de la modification d'une règle de session de transfert existante.
- **Au niveau mondial**. Activez le paramètre Process Local lors de l'ajout d'une nouvelle instance de cluster ou de la modification d'une instance de cluster existante. Le paramètre global est prioritaire sur le paramètre de règle de la session de transfert.

Procédures CLI

Pour désactiver le pilotage d'une règle de session de transfert sur une configuration de cluster à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des jeux de commandes suivants :

- Si vous ajoutez une nouvelle règle de session de transfert :
  - **ajouter une session de transfert**(([\]) | -acl6name | - aclname) - **ProcessLocal ACTIVÉ**<name><network><netmask><string><string>
  - **show forwardingSession** <name>
- Si vous reconfigurez une règle de session de transfert existante :
  - **définir ForwardingSession- ProcessLocal ACTIVÉ**<name>
  - **show forwardingSession** <name>

Pour désactiver le pilotage de toutes les règles de session de transfert (au niveau global) sur une configuration de cluster à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des jeux de commandes suivants :

- Si vous ajoutez une nouvelle instance de cluster :
  - **ajouter une instance de cluster** <clid>-**ProcessLocal activé**
  - **afficher l'instance du cluster** <clid>
- Si vous reconfigurez une instance de cluster existante :
  - **définir l'instance du cluster** <clid>-**ProcessLocal activé**
  - **afficher l'instance du cluster** <clid>

Exemple de configuration :

Vous trouverez ci-dessous deux exemples de désactivation du pilotage au niveau des règles de session de transfert et un exemple de désactivation du pilotage au niveau global.

```
An IPv4 forwarding session rule:

> add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV4-1 10.102.105.51
    255.255.255.255 -processLocal Enabled
```



```
Done

An IPv6 forwarding session rule:

> add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV6-1  -acl6name ACL6-
   FWD-SESSN-1 -processLocal Enabled
Done

A cluster setup, with an instance ID 10, has steering disabled at
   global level:

> set cluster instance 10 -processLocal Enabled
Done
<!--NeedCopy-->
```

Procédures GUI

Pour désactiver le pilotage d'une règle de session de transfert sur une configuration de cluster à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Sessions de transfert**, sélectionnez **Process Local** tout en ajoutant une nouvelle règle de session de transfert ou en modifiant une règle de session de transfert existante.

Pour désactiver le pilotage de toutes les règles de session de transfert (au niveau global) sur une configuration de cluster à l'aide de l'interface graphique :

Accédez à **Système** > **Cluster**et sélectionnez **Process Local** lors de l'ajout d'une configuration de cluster ou de la modification d'une configuration de cluster existante.

Comprendre les VLAN

May 5, 2023

Une appliance NetScaler prend en charge le port de couche 2 et les VLAN marqués IEEE 802.1q. Les configurations VLAN sont utiles lorsque vous devez restreindre le trafic à certains groupes de stations. Vous pouvez configurer une interface réseau dans le cadre de plusieurs VLAN à l'aide du balisage IEEE 802.1q.

Vous pouvez configurer des VLAN et les lier à des sous-réseaux IP. Le NetScaler effectue ensuite le transfert IP entre ces VLAN (s'il est configuré comme routeur par défaut pour les hôtes de ces sous-réseaux).

NetScaler prend en charge les types de VLAN suivants :

- **VLAN basés sur les ports.** L'appartenance à un VLAN basé sur des ports est définie par un ensemble d'interfaces réseau qui partagent un domaine de diffusion de couche 2 commun et exclusif. Vous pouvez configurer plusieurs VLAN basés sur des ports. Par défaut, toutes les interfaces réseau du NetScaler sont membres du VLAN 1.

  Si vous appliquez le balisage 802.1q au port, l'interface réseau appartient à un VLAN basé sur le port. Le trafic de couche 2 est ponté au sein d'un VLAN basé sur un port, et les diffusions de couche 2 sont envoyées à tous les membres du VLAN si le mode de couche 2 est activé. Lorsque vous ajoutez une interface réseau non balisée en tant que membre d'un nouveau VLAN, elle est supprimée de son VLAN actuel.

- **VLAN par défaut.** Par défaut, les interfaces réseau de NetScaler sont incluses dans un seul VLAN basé sur les ports en tant qu'interfaces réseau non balisées. Ce VLAN est le VLAN par défaut. Il possède un ID VLAN (VID) de 1. Ce VLAN existe en permanence. Il ne peut pas être supprimé et son VID ne peut pas être modifié.

  Lorsque vous ajoutez une interface réseau à un autre VLAN en tant que membre non balisé, l'interface réseau est automatiquement supprimée du VLAN par défaut. Si vous dissociez une interface réseau de son VLAN basé sur les ports actuel, elle est de nouveau ajoutée au VLAN par défaut.

- **VLAN balisés.** Le balisage 802.1q (défini dans la norme IEEE 802.1q) permet à un périphérique réseau (tel que NetScaler) d'ajouter des informations à une trame au niveau de la couche 2 afin d'identifier l'appartenance au VLAN de la trame. Le balisage permet aux environnements réseau de disposer de réseaux VLAN couvrant plusieurs appareils. Un périphérique qui reçoit le paquet lit l'étiquette et reconnaît le VLAN auquel appartient la trame. Certains appareils réseau ne prennent pas en charge la réception de paquets balisés et non balisés sur la même interface réseau, en particulier les commutateurs Force10. Dans ce cas, vous devez contacter le service client pour obtenir de l'aide.

  L'interface réseau peut être un membre étiqueté ou non d'un VLAN. Chaque interface réseau est un membre non balisé d'un seul VLAN (son VLAN natif). Cette interface réseau transmet les trames du VLAN natif sous forme de trames non balisées. Une interface réseau peut faire partie de plusieurs VLAN si les autres VLAN sont balisés.

  Lorsque vous configurez le balisage, veillez à ce qu'il corresponde à la configuration du VLAN aux deux extrémités du lien. Le port auquel NetScaler se connecte doit se trouver sur le même VLAN que l'interface réseau NetScaler.

  Remarque : Cette configuration VLAN n'est ni synchronisée ni propagée. Vous devez donc effectuer la configuration sur chaque unité d'une paire HA indépendamment.

Application de règles pour classer les cadres

Les VLAN ont deux types de règles pour classer les trames :

- **Règles d'entrée.** Les règles d'entrée classent chaque trame comme appartenant uniquement à un seul VLAN. Lorsqu'une trame est reçue sur une interface réseau, les règles suivantes sont appliquées pour classer la trame :
  - Si la trame n'est pas balisée ou si sa valeur de balise est égale à 0, le VID de la trame est défini sur le port VID (PVID) de l'interface de réception, qui est classé comme appartenant au VLAN natif. (Les PVID sont définis dans la norme IEEE 802.1q.)
  - Si le cadre possède une valeur de balise égale à FFF, le cadre est supprimé.
  - Si le VID de la trame indique un VLAN dont l'interface réseau réceptrice n'est pas membre, la trame est supprimée. Par exemple, si un paquet est envoyé depuis un sous-réseau associé à l'ID VLAN 12 vers un sous-réseau associé à l'ID VLAN 10, le paquet est abandonné. Si un paquet non balisé avec VID 9 est envoyé depuis le sous-réseau associé à l'ID VLAN 10 vers une interface réseau PVID 9, le paquet est supprimé.
- **Règles de sortie.** Les règles de sortie suivantes sont appliquées :
  - Si le VID de la trame indique un VLAN dont l'interface réseau de transmission n'est pas membre, la trame est supprimée.
  - Au cours du processus d'apprentissage (défini par la norme IEEE 802.1q), le Src MAC et le VID sont utilisés pour mettre à jour la table de recherche de pont du NetScaler.
  - Une trame est supprimée si son VID indique un VLAN qui ne possède aucun membre. (Vous définissez les membres en liant les interfaces réseau à un VLAN.)

VLAN et transfert de paquets sur NetScaler

Le processus de transfert sur l'appliance NetScaler est similaire à celui de n'importe quel commutateur standard. Toutefois, NetScaler effectue le transfert uniquement lorsque le mode de couche 2 est activé. Les principales caractéristiques du processus de transfert sont les suivantes :

- Les restrictions de topologie sont appliquées. L'application implique la sélection de chaque interface réseau du VLAN en tant que port de transmission (en fonction de l'état de l'interface réseau), des restrictions de pontage (ne pas transférer sur l'interface réseau réceptrice) et des restrictions MTU.
- Les trames sont filtrées sur la base des informations figurant dans la table de la table de transfert de la base de données de transfert (FDB) de NetScaler. La recherche dans la table de pont est basée sur le MAC de destination et le VID. Les paquets adressés à l'adresse MAC du NetScaler sont traités au niveau des couches supérieures.
- Toutes les trames de diffusion et de multidiffusion sont transférées vers chaque interface réseau membre du VLAN, mais le transfert n'a lieu que si le mode L2 est activé. Si le mode L2 est désac-

tivé, les paquets de diffusion et de multidiffusion sont supprimés. Cela est également vrai pour les adresses MAC qui ne figurent pas actuellement dans la table de transition.
- Une entrée VLAN possède une liste d'interfaces réseau membres qui font partie de son ensemble de membres non balisés. Lors du transfert de trames vers ces interfaces réseau, aucune balise n'est insérée dans la trame.
- Si l'interface réseau est un membre étiqueté de ce VLAN, le tag est inséré dans le cadre lorsque le cadre est transféré.

Lorsqu'un utilisateur envoie des paquets de diffusion ou de multidiffusion sans que le VLAN ne soit identifié, c'est-à-dire lors de la détection d'adresses dupliquées (DAD) pour NSIP ou ND6 pour le saut suivant de la route, le paquet est envoyé sur toutes les interfaces réseau, avec un balisage approprié basé sur les règles d'entrée et de sortie. Le ND6 identifie généralement un VLAN, et un paquet de données est envoyé uniquement sur ce VLAN. Les VLAN basés sur les ports sont communs à IPv4 et IPv6. Pour IPv6, NetScaler prend en charge les VLAN basés sur des préfixes.

Configuration d'un VLAN

May 5, 2023

Vous pouvez implémenter des VLAN dans les environnements suivants :

- Sous-réseau unique
- Sous-réseaux multiples
- Réseau local unique
- VLAN (pas de balisage)
- VLAN (balisage 802.1q)

Si vous configurez des VLAN dont les membres sont uniquement des interfaces réseau non balisées, le nombre total de VLAN possibles est limité au nombre d'interfaces réseau disponibles dans NetScaler. Si davantage de sous-réseaux IP sont requis avec une configuration VLAN, le balisage 802.1q doit être utilisé.

Lorsque vous liez une interface réseau à un VLAN, l'interface réseau est supprimée du VLAN par défaut. Si les interfaces réseau doivent faire partie de plusieurs VLAN, vous pouvez les lier aux VLAN en tant que membres balisés.

Vous pouvez configurer NetScaler pour transférer le trafic entre les VLAN au niveau de la couche 3. Dans ce cas, un VLAN est associé à un seul sous-réseau IP. Les hôtes d'un VLAN qui appartiennent à un seul sous-réseau utilisent le même masque de sous-réseau et une ou plusieurs passerelles par défaut connectées à ce sous-réseau. La configuration de la couche 3 pour un VLAN est facultative. La couche 3 est utilisée pour le transfert IP (routage inter-VLAN). Chaque VLAN possède une adresse IP

et un masque de sous-réseau uniques qui définissent un sous-réseau IP pour le VLAN. Dans une configuration HA, cette adresse IP est partagée avec les autres appliances NetScaler. NetScaler transfère les paquets entre les sous-réseaux IP (VLAN) configurés.

Lorsque vous configurez NetScaler, vous ne devez pas créer de sous-réseaux IP qui se chevauchent. Cela nuit à la fonctionnalité de la couche 3.

Chaque VLAN est un domaine de diffusion de couche 2 unique. Deux VLAN, chacun lié à des sous-réseaux IP distincts, ne peuvent pas être combinés en un seul domaine de diffusion. Le transfert du trafic entre deux VLAN nécessite un périphérique de transfert (routage) de couche 3, tel que l'appliance NetScaler.

Configuration de VLAN dans une configuration HA

La configuration VLAN pour une configuration à haute disponibilité nécessite que les appliances NetScaler aient la même configuration matérielle et que les VLAN configurés sur celles-ci doivent être des images miroir.

La configuration VLAN correcte est mise en œuvre automatiquement lorsque la configuration est synchronisée entre les appliances NetScaler. Il en résulte des actions identiques sur tous les appareils. Par exemple, l'ajout de l'interface réseau 0/1 au VLAN2 ajoute cette interface réseau au VLAN 2 sur toutes les appliances participant à la configuration de haute disponibilité.

Remarque : Si vous utilisez des commandes spécifiques à l'interface réseau dans une configuration HA, les configurations que vous créez ne sont pas propagées vers l'autre appliance NetScaler. Vous devez exécuter ces commandes sur chaque appliance d'une paire HA pour vous assurer que la configuration des deux appliances de la paire HA reste synchronisée.

Création ou modification d'un VLAN

Pour configurer un VLAN, vous créez une entité VLAN, puis vous liez des interfaces réseau et des adresses IP au VLAN. Si vous supprimez un VLAN, ses interfaces membres sont ajoutées au VLAN par défaut.

Procédures CLI

Pour créer un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `add vlan <id> [-aliasName <string>] [-ipv6DynamicRouting (ENABLED|DISABLED)]`
- `sh vlan <id>`

Exemple :

```
1    > add vlan 2  -aliasName "Network A"   Done
2 <!--NeedCopy-->
```

Pour lier une interface à un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `bind vlan <id> -ifnum <slot/port>`
- `sh vlan <id>`

Exemple :

```
1    > bind vlan 2 -ifnum 1/8   Done
2 <!--NeedCopy-->
```

Pour lier une adresse IP à un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `bind vlan <id> -IPAddress <IPAddress> <netMask>`
- `sh vlan <id>`

Exemple :

```
1    > bind vlan 2 -IPAddress 10.102.29.54 255.255.255.0   Done
2 <!--NeedCopy-->
```

Pour supprimer un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `rm vlan <id>`

Procédures GUI

Pour configurer un VLAN à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > VLAN, ajoutez un nouveau VLAN ou modifiez un VLAN existant.
2. Pour lier une adresse IP à un VLAN, sous Liaisons IP, sélectionnez l'option Active correspondant à l'adresse IP que vous souhaitez lier au VLAN (par exemple, 10.102.29.54). La colonne Type affiche le type d'adresse IP (tel qu'une adresse IP mappée, une adresse IP virtuelle ou une adresse IP de sous-réseau) pour chaque adresse IP de la colonne Adresse IP.
3. Pour lier une interface réseau à un VLAN, sous Liaisons d'interface, sélectionnez l'option Active correspondant à l'interface que vous souhaitez lier au VLAN.

Surveillance des réseaux locaux virtuels

Vous pouvez afficher les statistiques du VLAN telles que les paquets reçus, les octets reçus, les paquets envoyés et les octets envoyés, et utiliser ces informations pour identifier les anomalies et/ou déboguer un VLAN.

Pour afficher les statistiques d'un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `stat vlan <vlanID>`

Exemple :

```
  stat vlan 2
<!--NeedCopy-->
```

Pour afficher les statistiques d'un VLAN à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > VLAN.
2. Sélectionnez le VLAN, puis cliquez sur Statistiques.

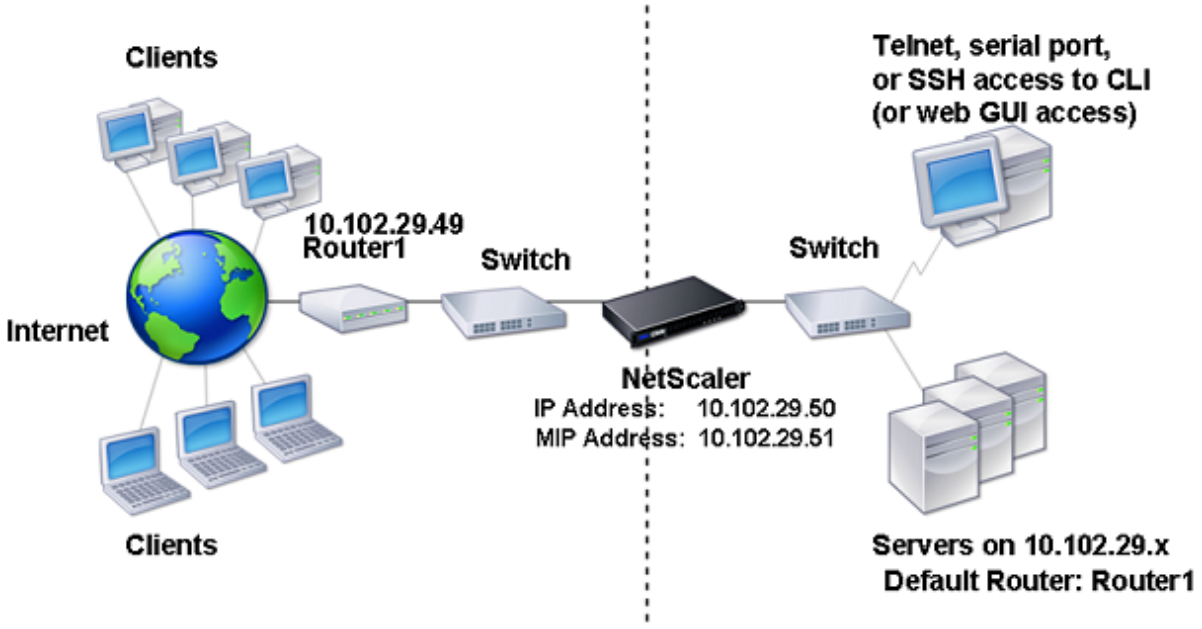
Configuration de VLAN sur un seul sous-réseau

May 5, 2023

Avant de configurer un VLAN sur un seul sous-réseau, assurez-vous que le mode couche 2 est activé.

La figure suivante montre un environnement de sous-réseau unique

Figure 1. VLAN sur un seul sous-réseau



Dans la figure ci-dessus :

1. Le routeur par défaut pour NetScaler et les serveurs est le routeur 1.
2. Le mode de couche 2 doit être activé sur NetScaler pour que NetScaler ait un accès direct aux serveurs.
3. Pour ce sous-réseau, un serveur virtuel peut être configuré pour l'équilibrage de charge sur l'appliance NetScaler.

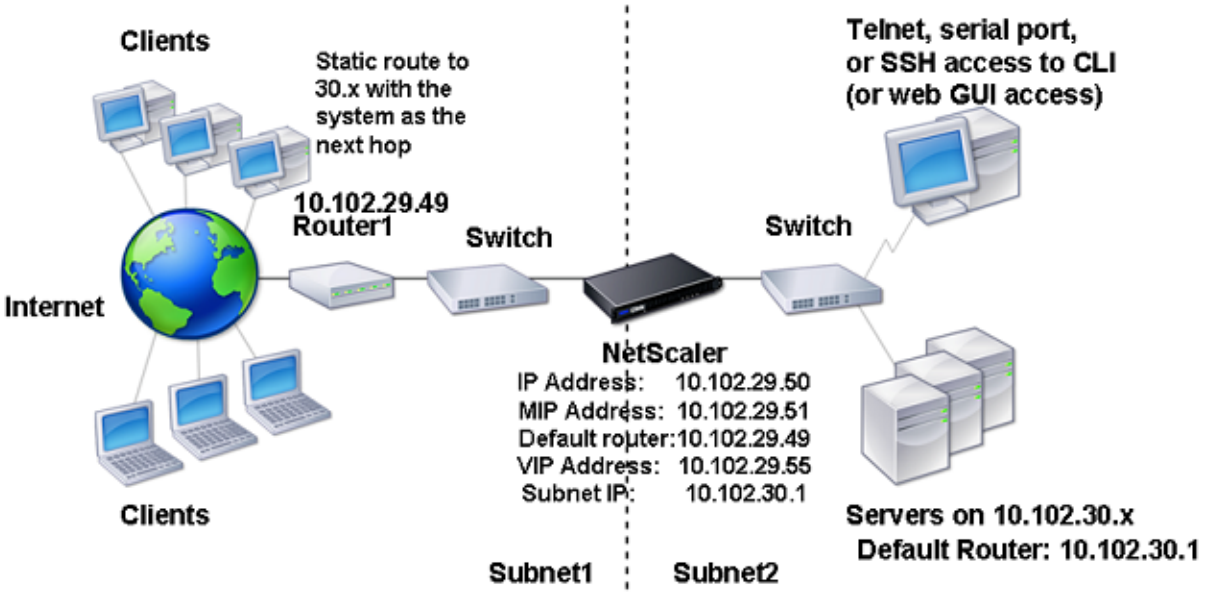
Pour configurer un VLAN sur un seul sous-réseau, suivez les procédures décrites dans Configuration d'un VLAN.

Configuration de VLAN sur plusieurs sous-réseaux

August 20, 2021

Pour configurer un seul VLAN sur plusieurs sous-réseaux, vous devez ajouter un VIP pour le VLAN et configurer le routage de manière appropriée. La figure suivante montre un seul VLAN configuré sur plusieurs sous-réseaux.

Figure 1. Plusieurs sous-réseaux dans un seul VLAN



Pour configurer un seul VLAN sur plusieurs sous-réseaux, effectuez les tâches suivantes :

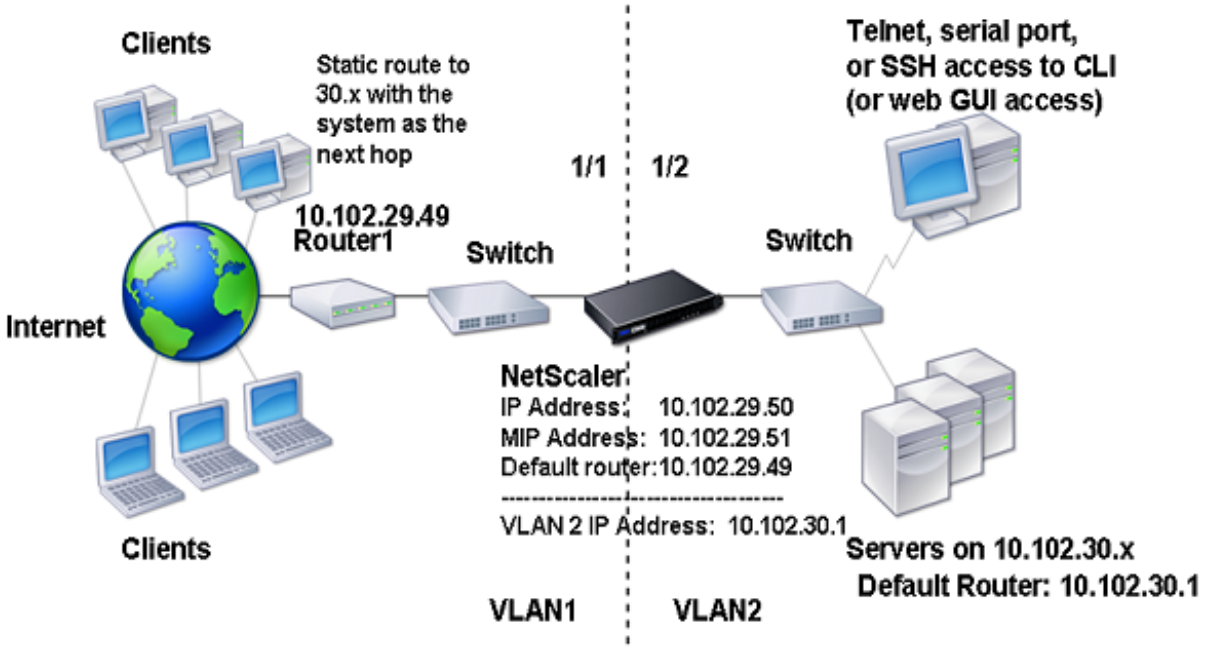
1. Désactivez le mode Couche 2. Pour connaître la procédure de désactivation du mode couche 2, reportez-vous à Modes de transfert de paquets.
2. Ajoutez une adresse VIP. Pour connaître la procédure d'ajout d'une adresse VIP, reportez-vous à la section Configuration et gestion des adresses IP virtuelles (VIP).
3. Configurez la règle RNAT. Pour connaître la procédure de configuration de l'ID RNAT, reportez-vous à la section Configuration de RNAT.

Configuration de plusieurs VLAN non balisés sur plusieurs sous-réseaux

May 5, 2023

Dans les environnements comportant plusieurs VLAN non balisés répartis sur plusieurs sous-réseaux, un VLAN est configuré pour chaque sous-réseau IP. Une interface réseau est liée à un seul VLAN. La figure suivante montre cette configuration.

Figure 1. Sous-réseaux multiples avec VLAN - Pas de balisage



Pour implémenter la configuration présentée dans la figure ci-dessus, effectuez les tâches suivantes :

1. Ajoutez le VLAN 2.
2. Liez l'interface réseau 1/2 du NetScaler au VLAN 2 en tant qu'interface réseau non balisée.
3. Liez l'adresse IP et le masque de sous-réseau au VLAN 2.

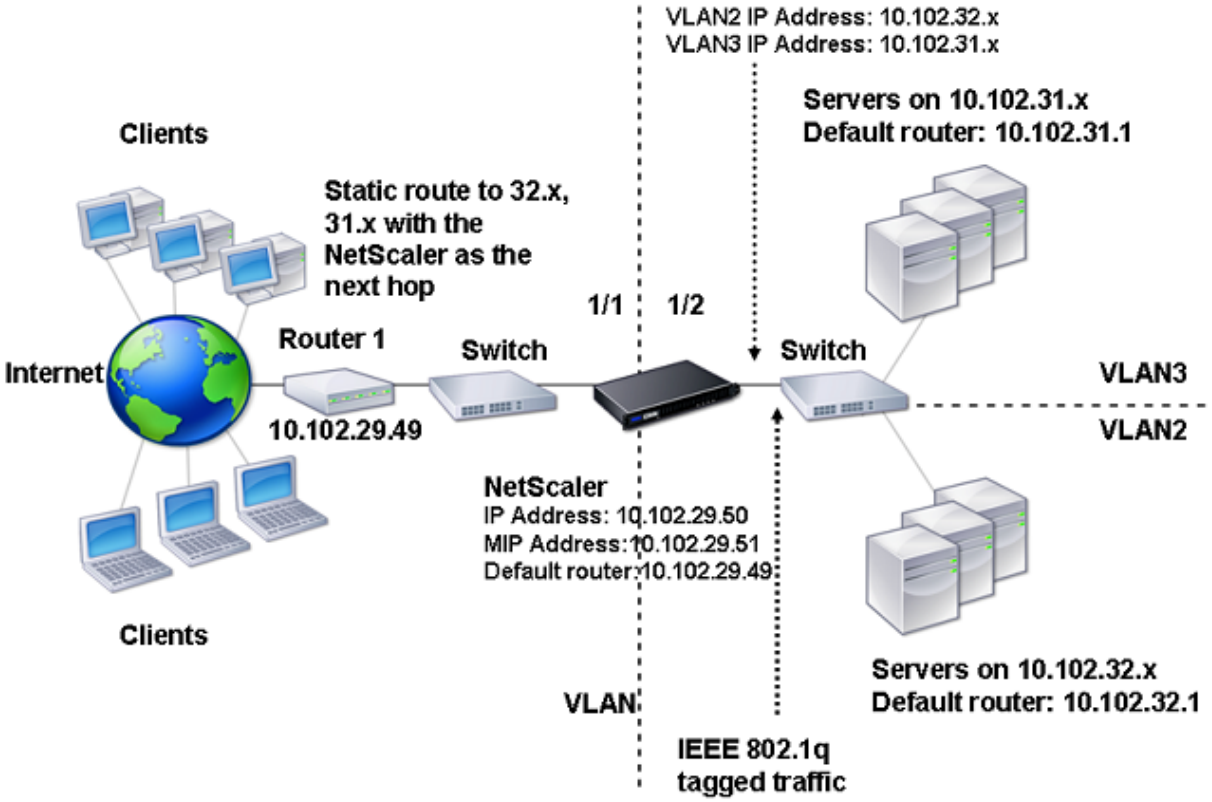
Pour connaître les procédures relatives à ces tâches, reportez-vous à la section Configuration d'un VLAN.

Configuration de plusieurs VLAN avec le balisage 802.1q

May 5, 2023

Pour plusieurs VLAN avec balisage 802.1q, chaque VLAN est configuré avec un sous-réseau IP différent. Chaque interface réseau se trouve dans un VLAN. L'un des VLAN est configuré comme balisé. La figure suivante montre cette configuration.

Figure 1. Plusieurs VLAN avec balisage IEEE 802.1q



Pour implémenter la configuration présentée dans la figure ci-dessus, effectuez les tâches suivantes :

1. Ajoutez le VLAN 2.
2. Liez l'interface réseau 1/2 du NetScaler au VLAN 2 en tant qu'interface réseau non balisée.
3. Liez l'adresse IP et le masque de réseau au VLAN 2.
4. Ajoutez le VLAN 3.
5. Liez l'interface réseau 1/2 du NetScaler au VLAN 3 en tant qu'interface réseau balisée.
6. Liez l'adresse IP et le masque de réseau au VLAN 3.

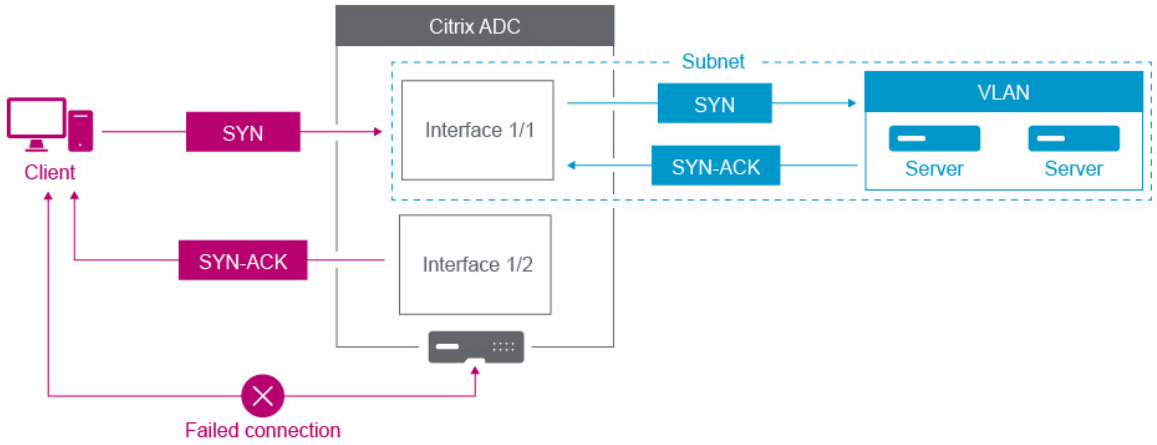
Pour connaître les procédures relatives à ces tâches, reportez-vous à la section Configuration d'un VLAN.

Associer un sous-réseau IP à une interface NetScaler à l'aide de VLAN

May 5, 2023

Par défaut, une appliance NetScaler ne permet aucune différenciation entre les interfaces réseau. L'appliance fonctionne davantage comme un concentrateur réseau qu'un commutateur. Cela peut conduire à des boucles réseau de couche 3 dans lesquelles le trafic dupliqué est transmis sur plusieurs interfaces.

Dans de tels scénarios, selon la conception du réseau, il est possible qu'une demande soit transmise sur une interface et que la réponse correspondante soit reçue sur une interface différente.



Par exemple, un paquet SYN envoyé sur une interface et la réponse SYN-ACK reçue sur une autre interface peuvent entraîner l'échec de la connexion, car l'appliance s'attend à recevoir le SYN-ACK sur la même interface qui a envoyé le paquet SYN d'origine.

Pour résoudre ces problèmes, l'appliance peut utiliser des VLAN internes ou externes pour associer des sous-réseaux spécifiques à des interfaces.

Avant de commencer

Avant de commencer à associer un sous-réseau IP à une interface NetScaler à l'aide de VLAN, notez les points suivants :

- La connectivité réseau peut être perdue accidentellement lors de l'association d'un VLAN au sous-réseau ou à l'interface actuellement utilisée pour accéder à l'interface graphique ou à l'interface de ligne de commande de NetScaler. Par conséquent, dans de tels scénarios, il est fortement recommandé d'effectuer la modification en accédant à l'interface de ligne de commande via la console série d'un dispositif NetScaler physique ou via la console série virtuelle d'un NetScaler VPX.
- Les interfaces de gestion NetScaler ne disposent pas de certaines fonctionnalités d'optimisation matérielle, ce qui les rend moins souhaitables pour le trafic de données de production. Il est donc recommandé de configurer NetScaler pour n'utiliser que les interfaces de gestion du trafic (NSIP). Dans la configuration par défaut, il n'existe aucune différenciation logique entre les interfaces de gestion et les interfaces de données sur un NetScaler matériel. Pour atteindre cet objectif, il est recommandé que le NSIP se trouve sur un VLAN distinct du trafic de données, ce qui permet au trafic de gestion de se trouver sur une interface distincte.

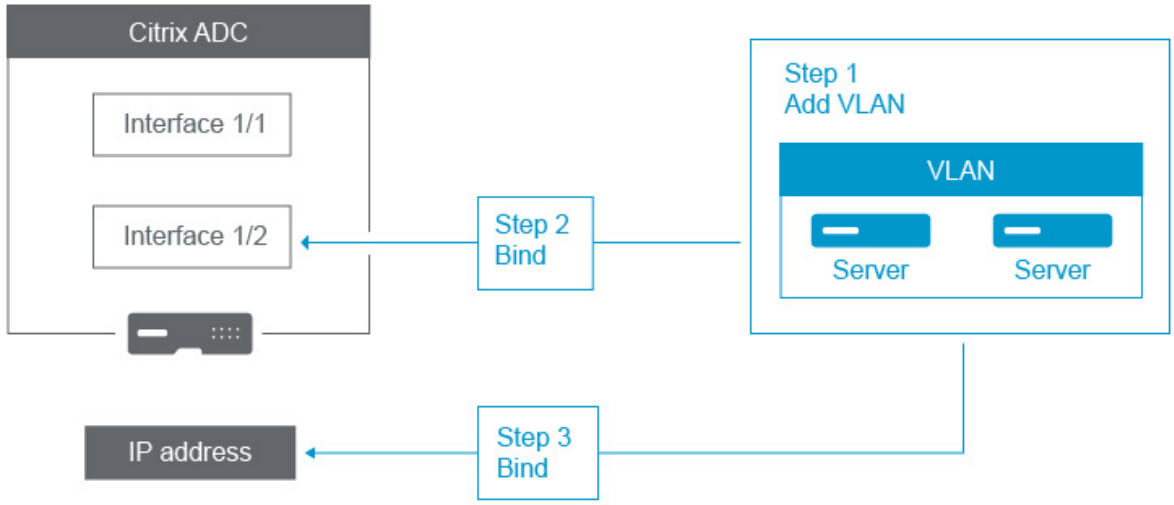
  Bien que le concept soit le même, pour modifier les associations VLAN du sous-réseau qui contient l'adresse NSIP, vous devez configurer le NSVLAN au lieu de suivre les instructions

ci-dessous. Ces modifications nécessiteront également un redémarrage de NetScaler pour entrer en vigueur. Pour plus d'informations, voir Configuration de NSVLAN.

- Sur NetScaler SDX, il est fortement recommandé que le NSIP de chaque instance se trouve sur le même sous-réseau et le même VLAN que la SVM (interface graphique du service de gestion) et XenServer du SDX. La SVM communique avec les instances via le réseau. Si la SVM, XenServer et les instances ne se trouvent pas sur le même VLAN et le même sous-réseau, le trafic de gestion doit circuler en dehors du SDX. Dans ce cas, des problèmes de réseau peuvent faire apparaître l'état de l'instance en jaune ou en rouge et empêcher les modifications de gestion et de configuration des instances NetScaler.

Étapes de configuration

L'association d'un sous-réseau IP à une interface NetScaler comprend les tâches suivantes :



Ajoutez un VLAN. Lors de l'ajout d'un VLAN, si vous balisez le VLAN, vous devez sélectionner un numéro de VLAN défini dans le commutateur réseau pour le port de commutateur associé. Si le VLAN n'est pas balisé et est interne à l'appliance, il est recommandé de sélectionner le numéro de VLAN disponible dans la configuration du commutateur pour en faciliter la consultation.

Liez une interface au VLAN. Lors de la liaison, si vous utilisez l'agrégation de liens, associez le VLAN au canal LA (par exemple, LA/1) plutôt qu'à l'interface physique. Le VLAN doit être associé à une seule interface réseau.

Si vous souhaitez baliser le trafic sur l'interface, utilisez l'option tagué (Tag). Dans le cas contraire, le trafic quitte l'appliance sans étiquette et est associé au VLAN natif du port du commutateur.

Liez une adresse IP au VLAN. Lors de la liaison, si vous liez plusieurs adresses IP du même sous-réseau, une erreur se produit. Lorsqu'une adresse IP est associée à un VLAN, toutes les adresses IP de ce sous-réseau sont automatiquement associées au VLAN.

> **Remarque :**
>
> dans une configuration haute disponibilité (HA), ces configurations VLAN sont ajoutées automatiquement du nœud principal au nœud secondaire lors de la synchronisation HA. Pour plus d'informations sur les configurations haute disponibilité, voir Haute disponibilité.

Procédures CLI

Pour ajouter un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add vlan** <id>
- **vlan sh** <id>

Pour lier une interface à un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **bind vlan** <id> -**ifnum** <slot/port>
- **vlan sh** <id>

Pour lier une adresse IP à un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **bind vlan - Adresse** <id**IP** <IPAddress><netMask>
- **vlan sh** <id>

Exemple :

```
> add vlan 100

> bind vlan 100 -ifnum 1/1

> bind vlan 100 -ipAddress 10.0.1.0 255.255.255.0
<!--NeedCopy-->
```

Procédures GUI

Pour configurer un VLAN à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VLAN**, ajoutez un nouveau VLAN.
2. Pour lier une interface réseau à un VLAN, sous **Liaisons d'interface**, sélectionnez l'option **Active** correspondant à l'interface que vous souhaitez lier au VLAN.

3. Pour lier une adresse IP à un VLAN, sous **Liaisons IP,**sélectionnez l'option **Active** correspondant à l'adresse IP que vous souhaitez lier au VLAN (par exemple, 10.102.29.54). La colonne **Type** affiche le type d'adresse IP de chaque adresse IP dans la colonne **Adresse IP** .

Bonnes pratiques en matière de mise en réseau et de VLAN des appliances NetScaler

May 5, 2023

Une appliance NetScaler utilise des VLAN pour déterminer quelle interface doit être utilisée pour quel trafic. De plus, l'appliance NetScaler ne participe pas à Spanning Tree. Sans une configuration VLAN appropriée, l'appliance NetScaler n'est pas en mesure de déterminer l'interface à utiliser et peut fonctionner davantage comme un HUB que comme un commutateur ou un routeur. En d'autres termes, l'appliance NetScaler peut utiliser toutes les interfaces pour chaque conversation.

Symptômes d'une mauvaise configuration du VLAN

Les problèmes de configuration d'un VLAN peuvent se manifester sous de nombreuses formes, notamment des problèmes de performances, l'impossibilité d'établir des connexions, des sessions déconnectées de manière aléatoire et, dans des situations graves, des perturbations du réseau apparemment sans rapport avec l'appliance NetScaler elle-même. L'appliance NetScaler peut également signaler des déplacements MAC, des interfaces muettes et/ou des dépassements de mémoire tampon émis ou reçus par l'interface de gestion, en fonction de la nature exacte de l'interaction avec votre réseau.

MAC Moves (counter nic_tot_bdg_mac_moved) : ce problème indique que l'appliance NetScaler utilise plusieurs interfaces pour communiquer avec le même appareil (adresse MAC), car elle n'a pas pu déterminer correctement quelle interface utiliser.

Interfaces désactivées (counter nic_err_bdg_muted) : ce problème indique que l'appliance NetScaler a détecté qu'elle créait une boucle de routage en raison de problèmes de configuration du VLAN et qu'elle a donc arrêté une ou plusieurs des interfaces problématiques afin d'éviter une panne réseau.

Dépassements de mémoire tampon d'interface, qui font généralement référence aux interfaces de gestion (counter nic_err_tx_overflow) : Ce problème peut survenirsi trop de trafic est transmis via une interface de gestion. Les interfaces de gestion de l'appliance NetScaler ne sont pas conçues pour gérer de gros volumes de trafic, ce qui peut résulter d'erreurs de configuration du réseau et du VLAN incitant l'appliance NetScaler à utiliser une interface de gestion pour le trafic de données de production. Cela se produit souvent parce que l'appliance NetScaler n'a aucun moyen de différencier

le trafic sur le VLAN/sous-réseau du NSIP (NSVLAN) du trafic de production normal. Il est fortement recommandé que le NSIP se trouve sur un VLAN et un sous-réseau distincts de tous les appareils de production tels que les postes de travail et les serveurs.

ACK orphelins (counter tcp_err_orphan_ack) : ce problème indique que l'appliance NetScaler a reçu un paquet ACK auquel elle ne s'attendait pas, généralement sur une interface différente de celle d'où provenait le trafic ACK. Cette situation peut être due à des erreurs de configuration du VLAN dans lesquelles l'appliance NetScaler transmet via une interface différente de celle que la machine cible utilise habituellement pour communiquer avec l'appliance NetScaler (souvent associée à des déplacements de MAC)

Taux élevés de retransmissions ou d'abandons de retransmission (compteurs : tcp_err_retransmit_giveups, tcp_err_7th_retransmit, divers autres compteurs de retransmission) : l'appliance NetScaler tente de retransmettre un paquet TCP au total 7 fois avant qu'il n'abandonne et ne mette fin à la connexion. Bien que cette situation puisse être due à des problèmes de réseau, elle est souvent le résultat d'une mauvaise configuration du VLAN et de l'interface.

Cerveau divisé en haute disponibilité : lecerveau divisé est une condition dans laquelle les deux nœuds de haute disponibilité pensent qu'ils sont principaux, ce qui entraîne la duplication des adresses IP et la perte des fonctionnalités de l'appliance NetScaler. Cela se produit lorsque les deux nœuds de haute disponibilité ne peuvent pas communiquer entre eux à l'aide de Heartbeats à haute disponibilité sur le port UDP 3003 à l'aide du NSIP, sur n'importe quelle interface. Cela est généralement dû à des erreurs de configuration du VLAN, dans lesquelles le VLAN natif sur les interfaces de l'appliance NetScaler n'est pas connecté entre les appliances NetScaler.

Meilleures pratiques pour les configurations VLAN et réseau

1. Chaque sous-réseau doit être associé à un VLAN.
2. Plusieurs sous-réseaux peuvent être associés au même VLAN (selon la conception de votre réseau).
3. Chaque VLAN doit être associé à une seule interface (aux fins de cette discussion, un canal LA compte comme une interface unique).
4. Si vous avez besoin que plusieurs sous-réseaux soient associés à une interface, les sous-réseaux doivent être balisés.
5. Contrairement à la croyance populaire, la fonctionnalité de transfert basé sur Mac (MBF) de l'appliance NetScaler n'est pas conçue pour atténuer ce type de problème. Le MBF est principalement conçu pour le mode DSR (Direct Server Return) de l'appliance NetScaler, qui est rarement utilisé dans la plupart des environnements (il est conçu pour permettre au trafic de contourner délibérément l'appliance NetScaler sur le chemin de retour depuis les serveurs principaux). Le MBF peut masquer des problèmes de VLAN dans certains cas, mais il ne faut pas s'y

fier pour résoudre ce type de problème.

6. Chaque interface de l'appliance NetScaler nécessite un VLAN natif (contrairement à Cisco, où les VLAN natifs sont facultatifs), bien que le paramètre TagAll d'une interface puisse être utilisé de manière à ce qu'aucun trafic non balisé ne quitte l'interface en question.
7. Le VLAN natif peut être balisé si nécessaire pour la conception de votre réseau (il s'agit de l'option TagAll pour l'interface).
8. Le VLAN du sous-réseau du NSIP de votre appliance NetScaler constitue un cas particulier. C'est ce qu'on appelle le NSVLAN. Les concepts sont les mêmes mais les commandes permettant de le configurer sont différentes et les modifications apportées au NSVLAN nécessitent un redémarrage de l'appliance NetScaler pour prendre effet. Si vous tentez de lier un VLAN à un SNIP qui partage le même sous-réseau que le NSIP, le message « Opération non autorisée » s'affiche. Cela est dû au fait que vous devez utiliser les commandes NSVLAN à la place. De plus, sur certaines versions du microprogramme, vous ne pouvez pas définir un NSVLAN si ce numéro de VLAN existe à l'aide de la commande. `add VLAN` Supprimez simplement le VLAN, puis reconfigurez le NSVLAN.
9. Les Heartbeats à haute disponibilité utilisent toujours le VLAN natif de l'interface correspondante (éventuellement étiqueté si l'option TagAll est définie sur l'interface).
10. Il doit y avoir une communication entre au moins un ensemble de VLAN natifs sur les deux nœuds d'une paire haute disponibilité (cela peut être direct ou via un routeur). Les VLAN natifs sont utilisés pour les pulsations cardiaques à haute disponibilité. Si les appliances NetScaler ne peuvent pas communiquer entre les VLAN natifs sur n'importe quelle interface, cela peut entraîner des basculements en haute disponibilité et éventuellement une situation de division du cerveau dans laquelle les deux appliances NetScaler pensent qu'elles sont les principales (ce qui entraîne des adresses IP dupliquées, entre autres choses).
11. L'appliance NetScaler ne participe pas à Spanning Tree. Il n'est donc pas possible d'utiliser Spanning Tree pour fournir une redondance d'interface lors de l'utilisation d'une appliance NetScaler. Utilisez plutôt une forme d'agrégation de liens (LACP ou LAG manuel) à cette fin.

    Remarque : Si vous souhaitez disposer d'une agrégation de liens entre plusieurs commutateurs physiques, vous devez configurer les commutateurs en tant que commutateurs virtuels, à l'aide d'une fonctionnalité telle que Switch Stack de Cisco.
12. La synchronisation à haute disponibilité et la propagation des commandes utilisent par défaut le NSIP/NSVLAN. Pour les séparer dans un autre VLAN, vous pouvez utiliser l'option SyncVLAN de la commande. `set HA node`
13. Rien n'est intégré à la configuration par défaut de l'appliance NetScaler qui indique qu'une interface de gestion (0/1 ou 0/2) est limitée au trafic de gestion uniquement. Cette restriction doit être appliquée par l'utilisateur final via la configuration du VLAN. Les interfaces de gestion

ne sont pas conçues pour gérer le trafic de données. La conception de votre réseau doit donc tenir compte de ce point. Les interfaces de gestion, contenues sur la carte mère de l'appliance NetScaler, ne disposent pas de diverses fonctionnalités de déchargement, telles que le déchargement CRC, des tampons de paquets plus importants et d'autres optimisations, ce qui les rend beaucoup moins efficaces pour gérer de gros volumes de trafic. Pour séparer les données de production du trafic de gestion, le NSIP ne doit pas se trouver sur le même sous-réseau/VLAN que votre trafic de données.

14. Si vous souhaitez utiliser une interface de gestion pour transporter le trafic de gestion, il est préférable que l'itinéraire par défaut se trouve sur un sous-réseau autre que le sous-réseau du NSIP (NSVLAN).

    Dans de nombreuses configurations, la route par défaut est utilisée pour les communications entre postes de travail (dans un scénario Internet). Si l'itinéraire par défaut se trouve sur le même sous-réseau que le NSIP, l'appliance ADC peut utiliser l'interface de gestion pour envoyer et recevoir du trafic de données. Cette utilisation du trafic de données peut surcharger l'interface de gestion.

15. De plus, un SDX, la SVM, XenServer et tous les NSIP d'instance NetScaler doivent se trouver sur le même VLAN et le même sous-réseau. L'appliance SDX ne **contient aucun panneau arrière** permettant la communication entre les instances SVM/XEN/. S'ils ne se trouvent pas sur le même VLAN/sous-net/interface, le trafic entre eux doit quitter le matériel physique, être acheminé sur votre réseau et revenir.

    Cette configuration peut entraîner des problèmes de connectivité évidents entre les instances et la SVM et n'est donc pas recommandée. Cela se manifeste souvent par un indicateur jaune de l'état de l'instance dans la SVM pour l'instance VPX en question et par l'impossibilité d'utiliser la SVM pour reconfigurer une instance VPX.

16. Si certains VLAN sont liés à des sous-réseaux et d'autres non, lors d'un basculement en haute disponibilité, les paquets GARP ne sont envoyés pour aucune adresse IP sur les sous-réseaux qui ne sont pas liés à un VLAN. Cette configuration peut entraîner des interruptions de connexion et des problèmes de connectivité lors de basculements en haute disponibilité. Ce problème est dû au fait que l'appliance NetScaler ne peut pas notifier la modification des adresses IP de propriété MAC du réseau sur les appliances NetScaler non configurées par VMAC.

    Cela se traduit par le fait que pendant ou après un basculement en haute disponibilité, le compteur ip_tot_floating_ip_err s'incrémente sur l'ancienne appliance NetScaler principale pendant plus de quelques secondes, ce qui indique que le réseau n'a pas reçu ni traité de paquets GARP et que le réseau continue de transmettre des données à la nouvelle appliance NetScaler secondaire.

Configuration de NSVLAN

May 5, 2023

Le NSVLAN est un VLAN auquel est lié le sous-réseau de l'adresse IP de gestion NetScaler (NSIP). Le sous-réseau NSIP est disponible uniquement sur les interfaces associées au NSVLAN. Par défaut, NSVLAN est VLAN 1, mais vous pouvez désigner un VLAN différent comme NSVLAN. Dans ce cas, vous devez redémarrer l'appliance NetScaler pour que la modification soit prise en compte. Après le redémarrage, le trafic du sous-réseau NSIP est limité au nouveau NSVLAN.

Le trafic provenant du sous-réseau IP NetScaler peut être balisé (802.1q) avec l'ID VLAN spécifié pour NSVLAN. Vous devez configurer l'interface de commutateur connectée pour baliser et autoriser ce même ID de VLAN sur l'interface connectée. Si vous supprimez votre configuration NSVLAN, le sous-réseau NSIP est automatiquement lié au VLAN 1, ce qui restaure le NSVLAN par défaut.

Pour configurer NSVLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set ns config -nsvlan** <positive_integer> -**ifnum** <interface_name> … [-**tagged** (YES|NO)]
- **show ns config**

> **Remarque :**
>
> La configuration prend effet après le redémarrage de l'appliance NetScaler.

Exemple :

```
> set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged YES
 Done

> save config
 Done
<!--NeedCopy-->
```

Pour restaurer la configuration NSVLAN par défaut à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **unset ns config** -**nsvlan**
- **show ns config**

Exemple :

```
> unset ns config -nsvlan
 Done
<!--NeedCopy-->
```


Pour configurer NSVLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Paramètres**, dans le groupe **Paramètres**, cliquez sur **Modifier les paramètres NSVLAN**.

Définition du MTU sur le NSVLAN

Par défaut, la MTU du NSVLAN est définie sur 1 500 octets. Vous pouvez modifier ce paramètre pour optimiser le débit et les performances du réseau. Par exemple, vous pouvez configurer le NSVLAN pour traiter les trames jumbo.

Pour définir la MTU du NSVLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set vlan** <id> **-mtu** <positive_integer>
- **show vlan** <id>

Pour définir la MTU du NSVLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **VLAN**, ouvrez le NSVLAN et définissez le paramètre **Maximum Transmission Unit** .

Exemple de configuration :

Dans l'exemple de configuration suivant, VLAN 100 est le NSVLAN.

```
> set ns config -nsvlan 100 -ifnum 1/1 -tagged no

  Warning: The configuration must be saved and the system rebooted for
     these settings to take effect

> set vlan 100 -mtu 1600

  Done

> sh vlan

  1)  VLAN ID: 1

      Link-local IPv6 addr:
    fe80::947b:52ff:fead:12d5/64

      Interfaces : 1/2 LO/1

  2)  VLAN ID: 100    VLAN Alias Name:

      MTU: 1600
```



```
21
22       Interfaces : 1/1
23
24       IPs :
25
26           10.102.53.114     Mask: 255.255.255.0
27
28   Done
29
30 > save config
31
32   Done
33 <!--NeedCopy-->
```

Configuration de la liste des VLAN autorisés

May 9, 2023

NetScaler accepte et envoie les paquets balisés d'un VLAN sur une interface si le VLAN est explicitement configuré sur l'appliance NetScaler et que l'interface est liée au VLAN. Certains déploiements (par exemple, Bump in the wire) nécessitent que l'appliance NetScaler fonctionne comme un périphérique transparent pour accepter et transférer des paquets balisés liés à un grand nombre de VLAN. Pour répondre à cette exigence, la configuration et la gestion d'un grand nombre de VLAN ne constituent pas une solution réalisable.

La liste des VLAN autorisés sur une interface spécifie une liste de VLAN. L'interface accepte et envoie de manière transparente les paquets balisés liés aux VLAN spécifiés sans qu'il soit nécessaire de configurer explicitement ces VLAN sur l'appliance.

Points à prendre en compte avant de configurer la liste des VLAN autorisés

Tenez compte des points suivants avant de configurer la liste des VLAN autorisés

- Dans une configuration à haute disponibilité, la liste des VLAN autorisés n'est ni propagée ni synchronisée. Par conséquent, vous devez configurer la liste des VLAN autorisés sur les deux nœuds.
- Le trafic d'un VLAN natif peut fuir vers les interfaces non membres qui spécifient le VLAN natif dans sa liste de VLAN autorisés.
- Un maximum de 60 plages de VLAN peuvent être spécifiées dans le cadre de la liste de VLAN autorisés pour une interface.

- L'appliance NetScaler ne prend pas en charge la liste des VLAN autorisés sur les interfaces faisant partie de canaux d'agrégation de liens ou d'ensembles d'interfaces redondants. Pour plus d'informations sur le jeu d'interfaces redondantes, voir Ensemble d' interfaces redondantes.
- La liste des VLAN autorisés n'est pas prise en charge sur une configuration de cluster NetScaler.
- L'appliance NetScaler ne prend pas en charge la liste des VLAN autorisés pour les groupes Bridge.
- L'appliance NetScaler ne prend pas en charge la liste des VLAN autorisés pour les VXLAN.

Configuration de la liste des VLAN autorisés

Pour configurer la liste des VLAN autorisés à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set interface** <id> **-trunkmode** (ON|OFF) **-trunkAllowedVlan** <int[-int]> …
- **show interface** <id>

Pour configurer la liste des VLAN autorisés à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Interfaces**, sélectionnez une interface réseau, cliquez sur **Modifier**, puis définissez les paramètres suivants :

- Mode tronc
- VLAN autorisé par jonction

Exemple de configuration :

Dans l'exemple de configuration suivant, les VLAN des plages 100-120, 190-200 et 300-330 sont spécifiés dans la liste des VLAN autorisés pour l'interface 1/2.

```
> set int 1/2 -trunkmode on -trunkallowedVlan 100-120 190-200 300-330

Done

> sh int 1/2

1)      Interface 1/2 (Gig Ethernet 10/100/1000 MBits) #6
        flags=0xc020

        <ENABLED, UP, UP, AUTONEG OFF, HEARTBEAT, 802.1q, trunkmode>

        Trunk Allowed Vlans:  100-120 190-200 300-330

Done

```



```
<!--NeedCopy-->
```

Configuration des groupes de ponts

May 5, 2023

Généralement, lorsque vous souhaitez fusionner deux ou plusieurs VLAN en un seul domaine, vous modifiez la configuration du VLAN sur tous les appareils des domaines distincts. Cette tâche peut s'avérer fastidieuse. Pour fusionner plus facilement plusieurs VLAN en un seul domaine de diffusion, vous pouvez utiliser des groupes de ponts.

La fonctionnalité des groupes de ponts fonctionne de la même manière qu'un VLAN. Plusieurs VLAN peuvent être liés à un seul groupe de ponts, et tous les VLAN liés au même groupe de ponts forment un seul domaine de diffusion. Vous ne pouvez lier que des VLAN de couche 2 à un groupe de ponts. Pour les fonctionnalités de couche 3, vous devez attribuer une adresse IP à un groupe de ponts.

En mode couche 2, un paquet de diffusion reçu sur une interface appartenant à un VLAN particulier est ponté vers d'autres VLAN appartenant au même groupe de ponts. Dans le cas d'un paquet monodiffusion, l'appliance NetScaler recherche dans sa table de pont les adresses MAC apprises de tous les VLAN appartenant au même groupe de ponts.

En mode de transfert de couche 3, un sous-réseau IP est lié à un groupe de ponts. Le NetScaler accepte les paquets entrants appartenant au sous-réseau lié et transfère les paquets uniquement sur les VLAN liés au groupe de ponts.

Le routage IPv6 peut être activé sur un groupe de ponts configuré.

> **Remarque**
>
> La fonction Bridge Group et le mode Bridge BPDU ne peuvent pas fonctionner ensemble.

Étapes de configuration

Procédez comme suit pour configurer un groupe de ponts :

- Activer le mode couche 2
- Ajouter un groupe de ponts et lier des VLAN au groupe de ponts

Procédures CLI

Pour activer le mode couche 2 à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

- **enable ns mode l2**
- **show ns mode**

Pour ajouter un groupe de ponts et lier des VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter un groupe de ponts** <id>[- Routage**dynamique IPv6 (ACTIVÉ | DÉSACTIVÉ)**] ****
- **bind bridgegroup** <id> -**vlan** <positive_integer>
- **Afficher le groupe de pont** <id>

Exemple :

```
> add bridgegroup 12
 Done
<!--NeedCopy-->
```

Pour supprimer un groupe de ponts à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **groupe de pont RM** <id>

Exemple :

```
 rm bridgegroup 12
<!--NeedCopy-->
```

Procédures GUI

Pour configurer un groupe de ponts à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Groupes** de ponts, ajoutez un nouveau groupe de ponts et liez des VLAN au groupe de ponts, ou modifiez un groupe de ponts existant.

Configuration de MAC virtuels

August 20, 2021

Les nœuds principaux et secondaires d'une configuration haute disponibilité (HA) partagent l'entité flottante d'adresse MAC virtuelle. Le nœud principal possède les adresses IP flottantes (telles que MIP, SNIP et VIP) et répond aux demandes ARP de ces adresses IP avec sa propre adresse MAC. Par conséquent, la table ARP d'un périphérique externe, tel qu'un routeur en amont, est mise à jour avec l'adresse IP flottante et l'adresse MAC du nœud principal.

Lorsqu'un basculement se produit, le nœud secondaire prend la relève en tant que nouveau nœud principal. L'ancien nœud secondaire utilise Gratuitous ARP (GARP) pour annoncer les adresses IP flottantes qu'il avait apprises de l'ancien nœud principal. L'adresse MAC que le nouveau nœud principal annonce est l'adresse MAC de sa propre interface réseau. Certains périphériques (quelques routeurs) n'acceptent pas ces messages GARP. Par conséquent, ces périphériques externes conservent le mappage d'adresse IP vers Mac que l'ancien nœud principal avait annoncé. Cela peut entraîner la chute d'un site GSLB.

Par conséquent, vous devez configurer un MAC virtuel sur les deux nœuds d'une paire HA. Cela signifie que les deux nœuds ont des adresses MAC identiques. Lorsqu'un basculement se produit, l'adresse MAC du nœud secondaire reste inchangée et les tables ARP sur les périphériques externes n'ont pas besoin d'être mises à jour.

Pour connaître les procédures de configuration d'un MAC virtuel, reportez-vous à la section Configuration des adresses MAC virtuelles.

Configuration de l'agrégation de liens

May 5, 2023

L'agrégation de liens combine les données provenant de plusieurs ports en une seule liaison haut débit. La configuration de l'agrégation de liens augmente la capacité et la disponibilité du canal de communication entre l'appliance NetScaler et les autres appareils connectés. Un lien agrégé est également appelé « canal ». Vous pouvez configurer les canaux manuellement ou utiliser le protocole LACP (Link Aggregation Control Protocol). Vous ne pouvez pas appliquer LACP à un canal configuré manuellement, ni configurer manuellement un canal créé par LACP.

Lorsqu'une interface réseau est liée à un canal, les paramètres de canal ont priorité sur les paramètres d'interface réseau. (En d'autres termes, les paramètres de l'interface réseau sont ignorés.) Une interface réseau ne peut être liée qu'à un seul canal.

Lorsqu'une interface réseau est liée à un canal, elle abandonne sa configuration VLAN. Lorsque les interfaces réseau sont liées à un canal, manuellement ou par LACP, elles sont supprimées des VLAN auxquels elles appartenaient à l'origine et ajoutées au VLAN par défaut. Toutefois, vous pouvez lier le canal à l'ancien VLAN ou à un nouveau. Par exemple, si vous liez les interfaces réseau 1/2 et 1/3 à un VLAN portant l'ID 2, puis que vous les liez à un canal LA/1, les interfaces réseau sont déplacées vers le VLAN par défaut, mais vous pouvez les lier à nouveau au VLAN 2.

Configuration manuelle de l'agrégation de liens

Lorsque vous créez un canal d'agrégation de liens, son état est DOWN jusqu'à ce que vous y liez une interface active. Vous pouvez modifier une chaîne à tout moment. Vous pouvez supprimer des chaînes

ou les activer/désactiver.

Procédures CLI

Pour créer un canal d'agrégation de liens à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <interfaceName>ajouter un canal <id>[-ifnum \…] <positive_integer><positive_integer><positive_integer>[-state (ACTIVÉ | DÉSACTIVÉ)] [-speed \] [<speed>-FlowControl \] <glowControl>[-Moniteur HA (ACTIVÉ | DÉSACTIVÉ) [-IFAlias][-tagall (ON | OFF)] \] [<string>-débit \] [-BandwidthHigh \ [-BandwidthNormal \]]
- show channel

Exemple :

```
> add channel LA/1 -ifnum 1/8
Done
<!--NeedCopy-->
```

Pour lier une interface à un canal d'agrégation de liens existant ou en dissocier une à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- canal de liaison <id><interfaceName>
- canal de dissociation <id><interfaceName>

Exemple :

```
bind channel LA/1 1/8
<!--NeedCopy-->
```

Pour modifier un canal d'agrégation de liens à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez la commande
set channel, l'ID du canal et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour supprimer un canal d'agrégation de liens à l'aide de l'interface de ligne de commande :

Important : lorsqu'un canal est supprimé, les interfaces réseau qui y sont liées induisent des boucles réseau qui diminuent les performances du réseau. Vous devez désactiver les interfaces réseau avant de supprimer le canal.

À l'invite de commande, tapez :

- canal rm <id>

Exemple :


```
> rm channel LA/1
 Done
<!--NeedCopy-->
```

Procédures GUI

Pour configurer un canal d'agrégation de liens à l'aide de l'interface graphique :

Accédez à Système > Réseau > Canaux, ajoutez un nouveau canal ou modifiez un canal existant.

Pour supprimer un canal d'agrégation de liens à l'aide de l'interface graphique :

> **Important :**
>
> Lorsqu'un canal est supprimé, les interfaces réseau qui y sont liées induisent des boucles réseau qui diminuent les performances du réseau. Vous devez désactiver les interfaces réseau avant de supprimer le canal.

Accédez à Système > Réseau > Canaux, sélectionnez le canal que vous souhaitez supprimer et cliquez sur Supprimer.

Configuration de l'agrégation de liens à l'aide du protocole de contrôle d'agrégation de liens

Le protocole LACP (Link Aggregation Control Protocol) permet aux périphériques réseau d'échanger des informations d'agrégation de liens en échangeant des unités de données LACP (LACPDU). Par conséquent, vous ne pouvez pas activer le LACP sur les interfaces réseau membres d'un canal que vous avez créé manuellement.

Lorsque vous utilisez le LACP pour configurer l'agrégation de liens, vous utilisez des commandes et des paramètres différents pour modifier les canaux d'agrégation de liens et pour créer des canaux d'agrégation de liens. Pour supprimer un canal, vous devez désactiver le LACP sur toutes les interfaces qui font partie du canal.

Remarque : Dans une configuration haute disponibilité, les configurations LACP ne sont ni propagées ni synchronisées.

Configuration de la priorité du système LACP

La priorité du système LACP détermine quel dispositif homologue d'un canal LACP LA peut contrôler le canal LA. Ce numéro est appliqué globalement à tous les canaux LACP de l'appliance. Plus la valeur est basse, plus la priorité est élevée.

Pour configurer la priorité du système LACP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour définir la priorité d'une appliance autonome et vérifier la configuration :

- définir lacp -SysPriority <positive_integer>
- afficher lacp

Exemple :

```
set lacp -sysPriority 50
<!--NeedCopy-->
```

Pour définir la priorité d'un nœud de cluster spécifique, connectez-vous à l'adresse IP du cluster et, à l'invite de commandes, tapez les commandes suivantes :

- <positive_integer>définir lacp -SysPriority -OwnerNode <positive_integer>
- afficher lacp

Exemple :

```
set lacp -sysPriority 50 -ownerNode 2
<!--NeedCopy-->
```

Pour configurer la priorité du système LACP à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > Interfaces et, dans la liste des actions, sélectionnez Définir le LACP.
2. Spécifiez la priorité du système et le nœud propriétaire (applicable uniquement pour une configuration de cluster).

Création de canaux d'agrégation de liens

Pour créer un canal d'agrégation de liens à l'aide du protocole LACP, vous devez activer le protocole LACP et spécifier la même clé LACP sur chaque interface que vous souhaitez intégrer au canal. Par exemple, si vous activez le protocole LACP et définissez la clé LACP sur 3 sur les interfaces 1/1 et 1/2, un canal d'agrégation de liens LA/3 est créé et les interfaces 1/1 et 1/2 y sont automatiquement liées.

Remarque :

- Lorsque vous activez le LACP sur une interface réseau, vous devez spécifier la clé LACP.
- Par défaut, le LACP est désactivé sur toutes les interfaces réseau.

Pour créer un canal LACP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <positive_integer>définir l'interface <id>[-LacpMode \<lacpMode>] [-LacpKey \] [<positive_integer>-LacpPriority \] [-LACPTimeout (LONG | COURT)]

- afficher l'interface [\<id>]

Pour créer un canal LACP à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces, ouvrez l'interface réseau et définissez les paramètres.

Modification des canaux d'agrégation de liens

Après avoir créé un canal LACP en spécifiant des interfaces, vous pouvez modifier les propriétés du canal.

Pour modifier un canal LACP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <interfaceName>définir le canal <id>[-ifnum \…] <positive_integer><positive_integer>[-state (ACTIVÉ | DÉSACTIVÉ)] [-speed \] [<speed>-FlowControl \] [<glowControl>-HAMonitor (ACTIVÉ | DÉSACTIVÉ)] [-IFAlias \] [<string>-débit \] [<positive_integer>-tagall (ACTIVÉ | DÉSACTIVÉ)] [-BandwidthHigh \ [-BandwidthNormal \]]
- show channel

Exemple :

```
> set channel LA/3 -state ENABLED -speed 10000
 Done
<!--NeedCopy-->
```

Pour modifier un canal LACP à l'aide de l'interface graphique :

Accédez à Système > Réseau > Canaux et modifiez un canal LACP existant.

Supprimer un canal d'agrégation de liens

Pour supprimer un canal d'agrégation de liens créé à l'aide du protocole LACP, vous devez désactiver le protocole LACP sur toutes les interfaces qui font partie du canal.

Pour supprimer un canal LACP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- définir l'interface <id>-LACPMode Désactiver
- afficher l'interface [\<id>]

Pour supprimer un canal LACP à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces, ouvrez l'interface réseau et désactivez l'option Activer le LACP.

Redondance des liens à l'aide des canaux LACP

La redondance des liens à l'aide des canaux LACP permet à NetScaler de diviser un canal LACP en sous-canaux logiques, un sous-canal étant actif et les autres en mode veille. Si le sous-canal actif ne parvient pas à atteindre un seuil de débit minimum, l'un des sous-canaux de secours devient actif et prend le relais.

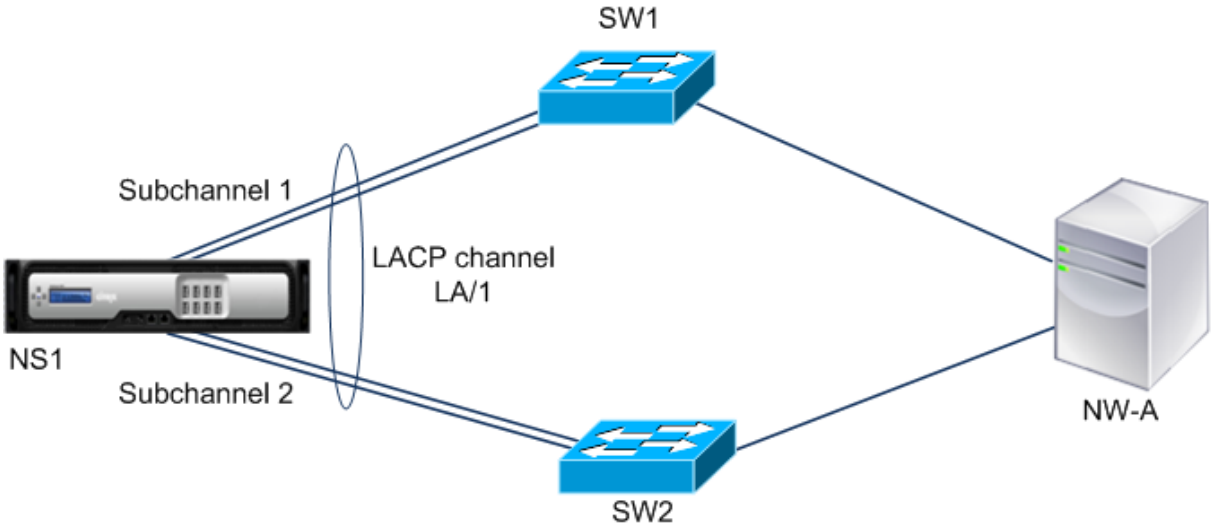
Un sous-canal est créé à partir de liens qui font partie du canal LACP et qui sont connectés à un périphérique particulier. Par exemple, pour un canal LACP avec quatre interfaces sur un NetScaler, dont deux des interfaces sont connectées au périphérique A et les deux autres connectées au périphérique B, l'ADC crée deux sous-canaux logiques, un sous-canal avec deux liens vers le périphérique A et un autre sous-canal avec deux liens vers le périphérique B.

Pour configurer la redondance des liens pour un canal LACP, définissez le paramètre LRMinThroughput, qui spécifie le seuil de débit minimum (en Mbit/s) à atteindre par le sous-canal actif. La définition de ce paramètre crée automatiquement les sous-canaux. Lorsque le débit maximal pris en charge par le canal actif tombe en dessous de la valeur LRMinThroughput, un basculement de liaison se produit et un sous-canal de secours devient actif.

Si vous désactivez le paramètre LrMinThroughput d'un canal LACP ou si vous définissez la valeur sur zéro, la redondance des liens pour ce canal est désactivée, ce qui est le paramètre par défaut.

Exemple

Prenons un exemple de redondance des liens configurée entre NetScaler NS1 et les commutateurs SW1 et SW2.



NS1 est connecté au périphérique réseau NW-A via SW1 et SW2.
Sur NS1, le canal LACP LA/1 est créé à partir des interfaces 1/1, 1/2, 1/3 et 1/4. Les interfaces 1/1 et 1/2 de NS1 sont connectées à SW1, et les interfaces 1/3 et 1/4 sont connectées à SW2. Chacune des

quatre liaisons prend en charge un débit maximal de 1000 Mbit/s.
Lorsque le paramètre LrMinThroughput est défini sur une certaine valeur (disons 2000), NS1 crée deux sous-canaux logiques à partir de LA/1, un sous-canal (disons le sous-canal 1) utilisant les interfaces 1/1 et 1/2 (connecté à SW1), et l'autre sous-canal (sous-canal 2) à l'aide des interfaces 1/3 et 1/4 (connecté à SW2).

NS1 applique un algorithme pour activer un sous-canal (disons le sous-canal 1) et mettre l'autre en veille. NS1 et le périphérique réseau NW-A sont accessibles l'un à l'autre uniquement via le sous-canal actif.

Supposons que le sous-canal 1 soit actif et que son débit maximal pris en charge soit inférieur à la valeur LRMinThroughput (par exemple, l'une de ses liaisons échoue et le débit maximal pris en charge tombe à 1 000 Mbit/s). Le sous-canal 2 devient actif et prend le relais.

Redondance des liens à l'aide de canaux LACP dans une configuration de haute disponibilité

Dans une configuration haute disponibilité (HA), si vous souhaitez configurer le basculement HA basé sur le débit (paramètre de débit) et la redondance des liens (paramètre LRMinThroughput) sur un canal LACP, vous devez définir le paramètre de débit sur une valeur inférieure ou égale à celle du paramètre LrMinThroughput.

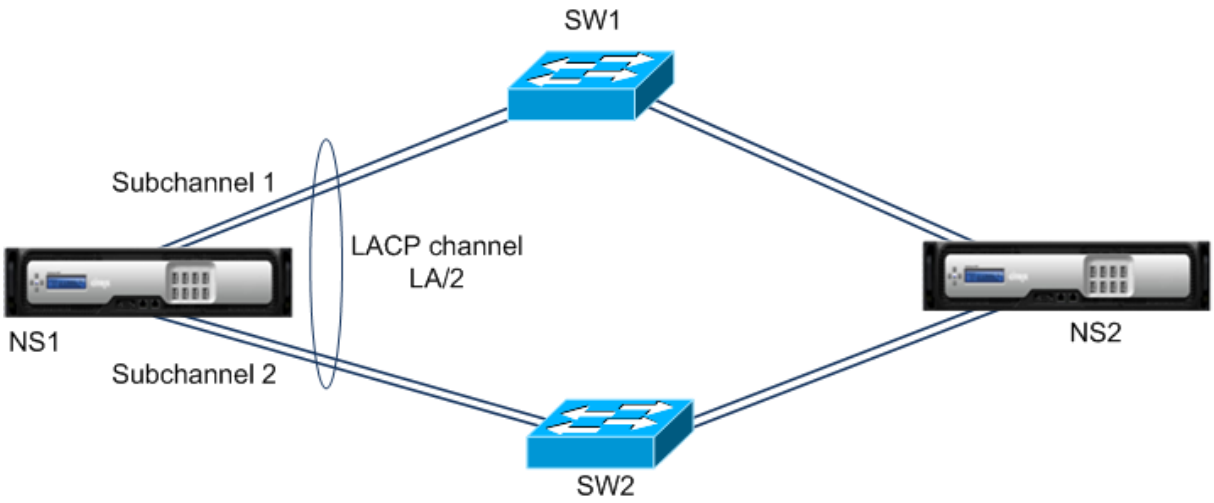
Le débit maximal pris en charge d'un canal LACP est calculé comme le débit maximal pris en charge du sous-canal actif.

Si la valeur du paramètre de débit est égale ou inférieure à la valeur du paramètre lrminthroughput, le basculement HA se produit lorsque les deux conditions suivantes existent simultanément :

- Aucun des débits maximaux pris en charge par les sous-canaux ne correspond à la valeur du paramètre LRMinThroughput.
- Le débit maximal pris en charge par le canal LACP ne correspond pas à la valeur du paramètre de débit

Prenons l'exemple d'une configuration HA dotée de NetScalers NS1 et NS2, avec des commutateurs SW1 et SW2. NS1 est connecté à NS2 via SW1 et SW2.

Sur NS1, le canal LACP LA/1 est créé à partir des interfaces 1/1, 1/2, 1/3 et 1/4. Les interfaces 1/1 et 1/2 de NS1 sont connectées à SW1, et les interfaces 1/3 et 1/4 sont connectées à SW2. Chacune des quatre liaisons prend en charge un débit maximal de 1000 Mbit/s.



Les paramètres LACP de cet exemple sont les suivants :

Paramètre	Valeur
Débit	2000
débit lrmin	2000

NS1 forme deux sous-canaux à partir de LA/1, un sous-canal (disons le sous-canal 1) à l'aide des interfaces 1/1 et 1/2 (connecté à SW1), et l'autre sous-canal (sous-canal 2) à l'aide des interfaces 1/3 et 1/4 (connecté à SW2). Chacun des deux sous-canaux prend en charge un débit maximal de 2 000 Mbit/s. En appliquant un algorithme, NS1 active un sous-canal (disons le sous-canal 1) et active l'autre en veille.

Supposons que le sous-canal 1 soit actif et que son débit maximal pris en charge soit inférieur à la valeur LRMinThroughput (par exemple, l'une de ses liaisons échoue et le débit maximal pris en charge tombe à 1 000 Mbit/s). Le sous-canal 2 devient actif et prend le relais. Le basculement HA ne se produit pas, car le débit maximal pris en charge par le canal LACP n'est pas inférieur à la valeur du paramètre de débit :

Débit maximal pris en charge du canal LACP = Débit maximal pris en charge du canal actif = Débit maximal pris en charge du sous-canal 2 = 2 000 Mbit/s

Si le débit maximal pris en charge par le sous-canal 2 tombe également en dessous de la valeur lrminthroughput (par exemple, si l'une de ses liaisons échoue et que le débit maximal pris en charge tombe à 1 000 Mbit/s), un basculement HA se produit, car le débit maximal pris en charge du canal LACP est alors inférieur à la valeur du paramètre de débit :

Configurer la redondance des liens à l'aide des canaux LACP

Pour configurer la redondance des liens pour un canal LACP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer le canal et vérifier la configuration :

- **définir le canal -LRMinThroughput** <id><positive_integer>
- **show channel**

Exemple :

```
1 > set channel la/1 - lrMinThroughput 2000
2 Done
3 > set channel la/2 - throughput 2000 - lrMinThroughput 2000
4 Done
5 <!--NeedCopy-->
```

Pour configurer la redondance des liens pour un canal LACP à l'aide de l'interface graphique

1. Accédez à Système > Réseau > Canaux.
2. Dans le volet de détails, sélectionnez un canal LACP pour lequel vous souhaitez configurer la redondance des liens, puis cliquez sur Modifier.
3. Dans la boîte de dialogue Configurer le canal LACP, définissez le paramètre LrMinThroughput.
4. Cliquez sur Fermer.

Jeu d'interfaces redondantes

June 2, 2023

> **Remarque**
>
> La configuration de redondance des liens n'est pas prise en charge sur une instance NetScaler VPX hébergée sur une appliance NetScaler SDX.

Un ensemble d'interfaces redondantes est un ensemble d'interfaces dont l'une est active et les autres sont en veille. En cas de défaillance de l'interface active, l'une des interfaces de secours prend le relais et devient active.

Les principaux avantages de l'utilisation de jeux d'interfaces redondants sont les suivants :

- Un ensemble d'interfaces redondantes garantit la fiabilité de la connexion entre l'appliance NetScaler et un appareil homologue en fournissant des liens de sauvegarde entre eux.

- Contrairement à la redondance de liens utilisant le protocole LACP, aucune configuration n'est requise sur le périphérique homologue pour un ensemble d'interfaces redondantes. Pour le périphérique homologue, l'ensemble d'interfaces redondantes apparaît comme des interfaces individuelles et non comme un ensemble ou une collection.
- Dans une configuration haute disponibilité (HA), les ensembles d'interfaces redondants peuvent minimiser le nombre de basculements en mode HA.

> **Remarque**
>
> L'ensemble d'interfaces redondantes était auparavant connu sous le nom de « regroupement de cartes réseau » lorsqu'il a été introduit pour la première fois dans la version 10.5.

Fonctionnement d'un ensemble d'interfaces redondantes

Pour un jeu d'interfaces redondant, l'appliance NetScaler dérive une adresse MAC sur la base d'un algorithme interne et l'attribue à l'ensemble d'interfaces redondantes. Cette adresse MAC est partagée par toutes les interfaces membres et n'est utilisée que par l'interface active à la fois. L'interface active diffuse des messages GARP, qui contiennent l'adresse MAC attribuée au jeu d'interfaces redondant et non l'adresse MAC physique de l'interface. Lorsque l'interface active actuelle échoue et est reprise par une autre interface, la nouvelle interface active envoie des messages GARP. Le dispositif homologue met à jour sa table de transfert avec les nouvelles informations d'interface actives. Les interfaces de secours n'envoient aucun message GARP. Les interfaces de secours n'envoient aucun paquet et abandonnent tous les paquets qu'elles reçoivent.

Dans un ensemble d'interfaces redondantes, la sélection de l'interface membre comme active est basée sur l'un des facteurs suivants :

- **Priorité d'interface redondante**. Il s'agit d'un paramètre d'une interface qui définit la priorité de l'interface dans un ensemble d'interfaces redondantes pour la sélection des membres actifs. Ce paramètre spécifie un entier positif. Réduisez la valeur au-dessus de la priorité de la sélection des membres actifs. L'interface membre ayant la priorité la plus élevée (valeur la plus faible) est sélectionnée comme interface active de l'ensemble d'interfaces redondantes.
- **Ordre contraignant des interfaces membres**. Si toutes les interfaces membres ont la même priorité d'interface redondante, l'interface membre qui a été liée en premier au jeu d'interfaces redondantes est sélectionnée comme interface active du jeu d'interfaces redondantes.

Dans un ensemble d'interfaces redondantes, la sélection active de l'interface est déclenchée lors de l'un des événements suivants :

- Lorsque l'interface active actuelle échoue ou que vous la désactivez.
- Lorsque vous définissez la priorité d'une interface de secours sur une valeur inférieure à celle de l'interface active actuelle. L'interface de secours prend le relais en tant qu'interface active.
- Lorsque vous liez une interface dont la priorité est inférieure à celle de l'interface active actuelle. L'interface nouvellement liée prend le relais en tant qu'interface active.

Points à prendre en compte pour configurer des ensembles d'interfaces redondants

Tenez compte des points suivants avant de configurer un ensemble d'interfaces redondantes :

- Dans une appliance autonome ou dans une configuration haute disponibilité, un ensemble de liens redondants est spécifié en notation LR/X, où X peut être compris entre 1 et 4. Par exemple, LR/1.
- Dans une configuration à haute disponibilité, les configurations d'ensembles d'interfaces redondants ne se propagent pas et ne se synchronisent pas avec le nœud secondaire.
- Vous pouvez configurer un maximum de quatre ensembles d'interfaces redondants sur une appliance NetScaler.
- Vous pouvez lier un maximum de 16 interfaces à un ensemble d'interfaces redondantes.
- Les interfaces membres d'un jeu d'interfaces redondant ne peuvent pas être liées à un autre jeu d'interfaces redondant.
- Les interfaces membres d'un ensemble d'interfaces redondantes ne peuvent pas être liées à un canal LA (Link Aggregate).
- Les canaux LA ne peuvent pas être liés à un ensemble d'interfaces redondant.
- Les ensembles d'interfaces redondants ne peuvent pas être liés à un canal LA.
- Dans une configuration de cluster :
  - Les ensembles d'interfaces redondants ne peuvent pas être liés à une agrégation de liens de cluster.
  - Un ensemble de liens redondants est spécifié en notation N/LR/X (par exemple, 1/LR/3). Où :
    N est l'ID du nœud du cluster sur lequel l'ensemble d'interfaces redondantes doit être créé.
    X est un identifiant d'ensemble redondant par liens sur un nœud de cluster. X peut être compris entre 1 et 4.
  - Une agrégation de liens de cluster ne peut pas être liée à un ensemble d'interfaces redondantes.
  - Un jeu d'interfaces redondantes ne peut inclure que les interfaces du nœud auquel appartient le jeu d'interfaces redondant.
  - Une configuration d'ensemble de redondance eLink existante sur une appliance autonome passe automatiquement à la notation de cluster (N/LR/X) une fois que l'appliance est ajoutée à une configuration de cluster.

Étapes de configuration

La configuration d'un ensemble d'interfaces redondantes sur une appliance NetScaler comprend les tâches suivantes :

- **Créez un ensemble d'interfaces redondantes**. Utilisez l'opération de commande channel pour créer un ensemble d'interfaces redondant.

Dans une appliance autonome ou dans une configuration haute disponibilité, un ensemble de liens redondants est spécifié en notation LR/X, où X peut être compris entre 1 et 4. Par exemple, LR/1.

Dans une configuration de cluster, un ensemble de liens redondants est spécifié dans N/LR/X (par exemple, 1/LR/3), où : N est l'ID du nœud de cluster sur lequel le jeu d'interfaces redondantes doit être créé ; X est l'identifiant du jeu de liens redondants sur un nœud de cluster. X peut être compris entre 1 et 4.

- **Liez les interfaces à l'ensemble d'interfaces redondantes**. Associez les interfaces souhaitées au jeu d'interfaces redondantes. Une interface ne peut pas faire partie de plusieurs ensembles d'interfaces redondants.
- **(Facultatif) Définissez une priorité d'interface redondante sur l'interface membre**. Utilisez l'opération de commande d'interface pour définir la priorité de l'interface redondante sur une interface membre souhaitée d'un ensemble d'interfaces redondantes.

Pour créer un ensemble d'interfaces redondantes à l'aide de l'interface de ligne de commande :

À l'invite de commandes :

- add channel <ID>
- show channel <ID>

Pour lier des interfaces à un ensemble d'interfaces redondantes à l'aide de l'interface de ligne de commande :

À l'invite de commandes :

- bind channel <ID> <ifnum>
- show channel <ID>

Pour définir la priorité d'interface redondante d'une interface à l'aide de l'interface de ligne de commande :

À l'invite de commandes :

- set interface <ID> -lrsetpriority <positive_integer>
- show interface <ID>

Exemple de configuration 1 :

Dans l'exemple suivant, un ensemble d'interfaces redondant LR/1 est créé et les interfaces 1/1, 1/2, 1/3 et 1/4 sont liées à LR/1. La priorité de l'interface redondante est définie sur une valeur par défaut de 1024 pour toutes ces interfaces membres. La sortie de la commande show channel indique que l'interface 1/1 est l'interface active actuelle pour l'ensemble d'interfaces redondantes lr/1.

```
1 > add channel lr/1
2  Done
```



```
> bind channel lr/1 1/1 1/2 1/3 1/4
 Done
> show channel
1)    Interface LR/1 (Link Redundant) #23
        flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
        LLDP Mode: NONE,
        RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
        TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
                1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Active Member
                1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
Done
<!--NeedCopy-->
```

Exemple de configuration 2 :

Dans l'exemple suivant, une priorité d'interface redondante de l'interface membre 1/4 est fixée à 100, ce qui est inférieur à la priorité d'interface redondante définie pour toutes les autres interfaces membres de LR/1.

La sortie de la commande show channel indique que l'interface 1/4 est l'interface active actuelle pour l'ensemble d'interfaces redondantes LR/1.

```
> set interface 1/4 -lrsetPriority 100
Done
> show channel
1)      Interface LR/1 (Link Redundant) #23
        flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
        LLDP Mode: NONE,
        RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
        TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
```



```
13          NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
14          Bandwidth thresholds are not set.
15                  1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                        Inactive Member
16                  1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                        Inactive Member
17                  1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                        Inactive Member
18                  1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                        Active Member
19  Done
20  <!--NeedCopy-->
```

Exemple de configuration 3 :

Envisagez une configuration en cluster de quatre nœuds N1, N2, N3 et N4. Dans cet exemple, le jeu d'interfaces redondantes 1/LR/3 est créé sur le nœud N1 et les interfaces 1/1/1, 1/1/2 et 1/1/3 y sont liées. La priorité de l'interface redondante est définie sur une valeur par défaut de 1024 pour toutes ces interfaces membres. La sortie de la commande show channel indique que l'interface 1/1/1 est l'interface active actuelle pour l'ensemble d'interfaces redondantes 1/LR/3.

```
1       > add channel 1/LR/3
2
3       Done
4       > bind channel 1/LR/3 1/1/1 1/1/2 1/1/3
5
6       Done
7       > show channel
8       1)    Interface 1/LR/3 (Link Redundant) #14
9               flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON,
                   802.1q>
10              MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0
                   h00m00s
11              Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
12              throughput 0
13              Actual: throughput 1000
14              LLDP Mode: NONE,
15              RX: Pkts(66) Bytes(4406) Errs(0) Drops(82) Stalls(0)
16              TX: Pkts(55) Bytes(2626) Errs(0) Drops(145) Stalls(0)
17              NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted
                   (0)
18              Bandwidth thresholds are not set.
19
20              1/1/1: UTP-1000-FULL-OFF UP  0h14m06s LR Active Member
21              1/1/2: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member
```



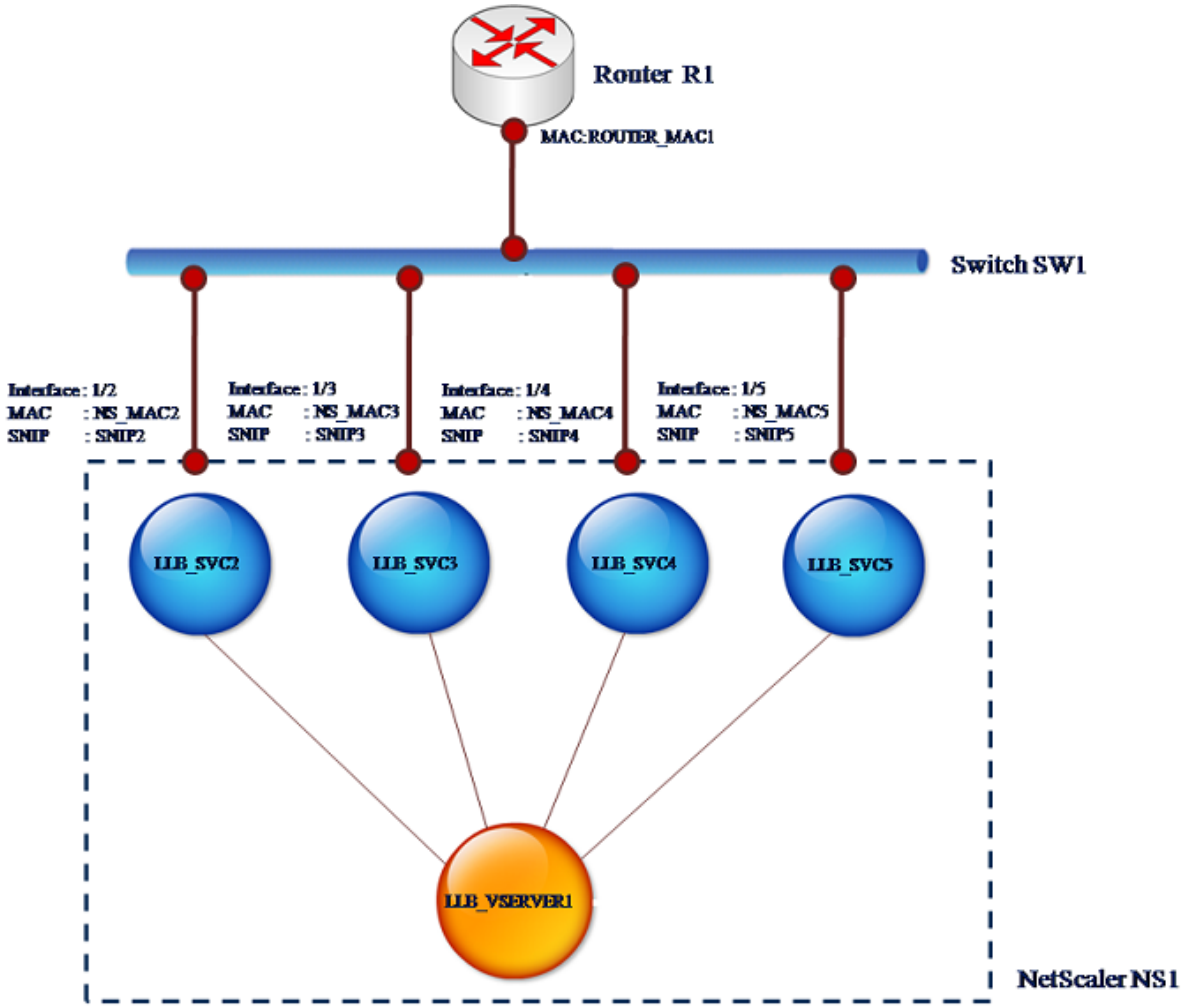
```
22              1/1/3: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member
23
24      Done
25  <!--NeedCopy-->
```

Liaison d’une adresse SNIP à une interface

May 5, 2023

Vous pouvez désormais lier une adresse SNIP appartenant à NetScaler à une interface sans utiliser de VLAN de couche 3. Tous les paquets liés à l’adresse SNIP passeront uniquement par l’interface liée.

Cette fonctionnalité peut être utile dans un scénario où le commutateur en amont ne prend pas en charge les canaux d’agrégation de liens et où vous souhaitez que l’appliance NetScaler équilibre la charge du trafic, provenant d’un serveur, sur les quatre liens menant au commutateur en amont, comme indiqué dans l’illustration suivante.



Les tableaux suivants décrivent les exemples de paramètres du scénario :

Entité	Nom	Valeur
Adresses SNIP sur NS1	SNIP2 (à titre de référence uniquement)	10.10.10.2
	SNIP3 (à titre de référence uniquement)	10.10.10.3
	SNIP4 (à titre de référence uniquement)	10.10.10.4
	SNIP5 (à titre de référence uniquement)	10.10.10.5
Serveur virtuel LLB sur NS1	LLB_VSERVER1	-
Moniteur transparent sur NS1	TRANS_MON	-

Entité	Nom	Valeur
Services LLB sur NS1	LLB_SVC2	10.10.10.240
	LLB_SVC3	10.10.10.120
	LLB_SVC4	10.10.10.60
	LLB_SVC5	10.10.10.30
Adresse MAC de l'interface 1/2 sur NS1	NS_MAC_2 (à titre de référence uniquement)	00:e0:ed:0f:bc:e0
Adresse MAC de l'interface 1/3 sur NS1	NS_MAC_3 (à titre de référence uniquement)	00:e0:ed:0f:bc:df
Adresse MAC de l'interface 1/4 sur NS1	NS_MAC_4 (à titre de référence uniquement)	00:e0:ed:0f:bc:de
Adresse MAC de l'interface 1/5 sur NS1	NS_MAC_5 (à titre de référence uniquement)	00:e0:ed:1c:89:53
Adresse IP du routeur R1	Router_IP (à titre de référence uniquement)	10.10.10.1
Adresse MAC de l'interface de R1	ROUTER_MAC1 (à titre de référence uniquement)	00:21:a1:2d:db:cc

Pour configurer les paramètres de l'exemple, procédez comme suit :

1. Ajoutez quatre SNIP différents dans différentes plages de sous-réseaux. Ceci est pour ARP à résoudre sur quatre liens différents. Pour plus d'informations sur la création d'une adresse SNIP, consultez Configuration des adresses IP de sous-réseau (SNIP).

   Exemple CLI :

   ```
   > add ns ip 10.10.10.2 255.255.255.0 -type SNIP
    Done
   > add ns ip 10.10.10.3 255.255.255.128 - type SNIP
   Done
   > add ns ip 10.10.10.4 255.255.255.192 - type SNIP
   Done
   > add ns ip 10.10.10.5 255.255.255.224 - type SNIP
   Done
   <!--NeedCopy-->
   ```

2. Ajoutez quatre services fictifs différents dans les sous-réseaux SNIP ajoutés. Ceci permet de s'assurer que le trafic est envoyé avec l'adresse IP source comme l'un des quatre SNIP con-

figurés. Pour plus d'informations sur la création d'un service, voir Configurer l'équilibrage de charge de base.

Exemple CLI :

```
> add service LLB_SVC2 10.10.10.240 any *
 Done
> add service LLB_SVC3 10.10.10.120 any *
 Done
> add service LLB_SVC4 10.10.10.60 any *
 Done
> add service LLB_SVC5 10.10.10.30 any *
 Done
<!--NeedCopy-->
```

3. Ajoutez un moniteur de ping transparent pour surveiller la passerelle. Liez le moniteur à chacun des services fictifs configurés. Ceci est de rendre l'état des services comme UP. Pour plus d'informations sur la création d'un moniteur transparent, voir Configurer les moniteurs dans une configuration d'équilibrage de charge.

   Exemple CLI :

```
> add monitor TRANS_MON ping -destIP 10.10.10.1 -transparent YES
 Done
> bind monitor TRANS_MON LLB_SVC2
 Done
> bind monitor TRANS_MON LLB_SVC3
 Done
> bind monitor TRANS_MON LLB_SVC4
 Done
> bind monitor TRANS_MON LLB_SVC5
 Done
<!--NeedCopy-->
```

4. Ajoutez un serveur virtuel d'équilibrage de charge de liaison (LLB) et liez les services factices à celui-ci. Pour plus d'informations sur la création d'un serveur virtuel LLB, voir Configuration d'un programme d'installation LLB de base.

   Exemple CLI :

```
> add lb vserver LLB_VSERVER1 any
 Done
> set lb vserver LLB_VSERVER1 -lbmethod ROUNDROBIN
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
```



```
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
<!--NeedCopy-->
```

5. Ajoutez le serveur virtuel LLB comme itinéraire LLB par défaut. Pour plus d'informations sur la création d'une route LLB, consultez Configuration d'une configuration LLB de base.

   Exemple CLI :

```
> add lb route 0.0.0.0 0.0.0.0  LLB_VSERVER1
 Done
<!--NeedCopy-->
```

6. Ajoutez une entrée ARP pour chacun des services fictifs avec l'adresse MAC de la passerelle. De cette façon, la Gateway est accessible via ces services factices. Pour plus d'informations sur l'ajout d'une entrée ARP, voir Configuration de l'ARP statique.

   Exemple CLI :

```
> add arp -ipaddress 10.10.10.240 -mac 00:21:a1:2d:db:cc -ifnum
   1/2
 Done
> add arp -ipaddress 10.10.10.120 -mac 00:21:a1:2d:db:cc -ifnum
   1/3
 Done
> add arp -ipaddress 10.10.10.60 -mac 00:21:a1:2d:db:cc -ifnum 1/4
 Done
> add arp -ipaddress 10.10.10.30 -mac 00:21:a1:2d:db:cc -ifnum 1/5
 Done
<!--NeedCopy-->
```

7. Liez une interface spécifique à un SNIP en ajoutant une entrée ARP pour chacun de ces SNIP. Ceci permet de s'assurer que le trafic de réponse atteindra la même interface à travers laquelle la requête est sortie. Pour plus d'informations sur l'ajout d'une entrée ARP, voir Configuration de l'ARP statique.

   Exemple CLI :

```
> add arp -ipAddress 10.10.10.2 -mac 00:e0:ed:0f:bc:e0 -ifnum 1/2
 Done
> add arp -ipAddress 10.10.10.3 -mac 00:e0:ed:0f:bc:df -ifnum 1/3
 Done
```



```
> add arp -ipAddress 10.10.10.4 -mac 00:e0:ed:0f:bc:de -ifnum 1/4
 Done
> add arp -ipAddress 10.10.10.5 -mac 00:e0:ed:1c:89:53 -ifnum 1/5
 Done
<!--NeedCopy-->
```

Surveillez la table de bridge et modifiez le temps de vieillissement

May 5, 2023

L'appliance NetScaler relie les trames sur la base de la recherche dans la table de pont de l'adresse MAC de destination et de l'ID du VLAN. Toutefois, l'appliance effectue le transfert uniquement lorsque le mode de couche 2 est activé.

La table de pont est générée dynamiquement, mais vous pouvez l'afficher, modifier la durée de vieillissement de la table de pont et consulter les statistiques de pontage. Toutes les entrées MAC de la table de pont sont mises à jour en fonction du temps de vieillissement.

Pour définir la durée de vieillissement des entrées de la table de pont à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **définir l2param- bridgeagetimeout** <positive_integer>
- **afficher l2param**

Exemple :

```
> set l2param -bridgeagetimeout 90
 Done
<!--NeedCopy-->
```

Pour afficher les statistiques d'une table de pont à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **pont de l'État**

Pour définir la durée de vieillissement des entrées de la table de pont à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**. Sur la page **Réseau**, dans la section **Paramètres**, cliquez sur **Configurer les paramètres de la couche 2** et définissez la **valeur du délai d'expiration pour le paramètre Bridge Table Entries (secondes).**

Pour afficher les statistiques d'une table de pont à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Bridge Table**, sélectionnez l'adresse MAC et cliquez sur **Statistiques**.

Appliances NetScaler en mode actif-actif à l'aide de VRRP

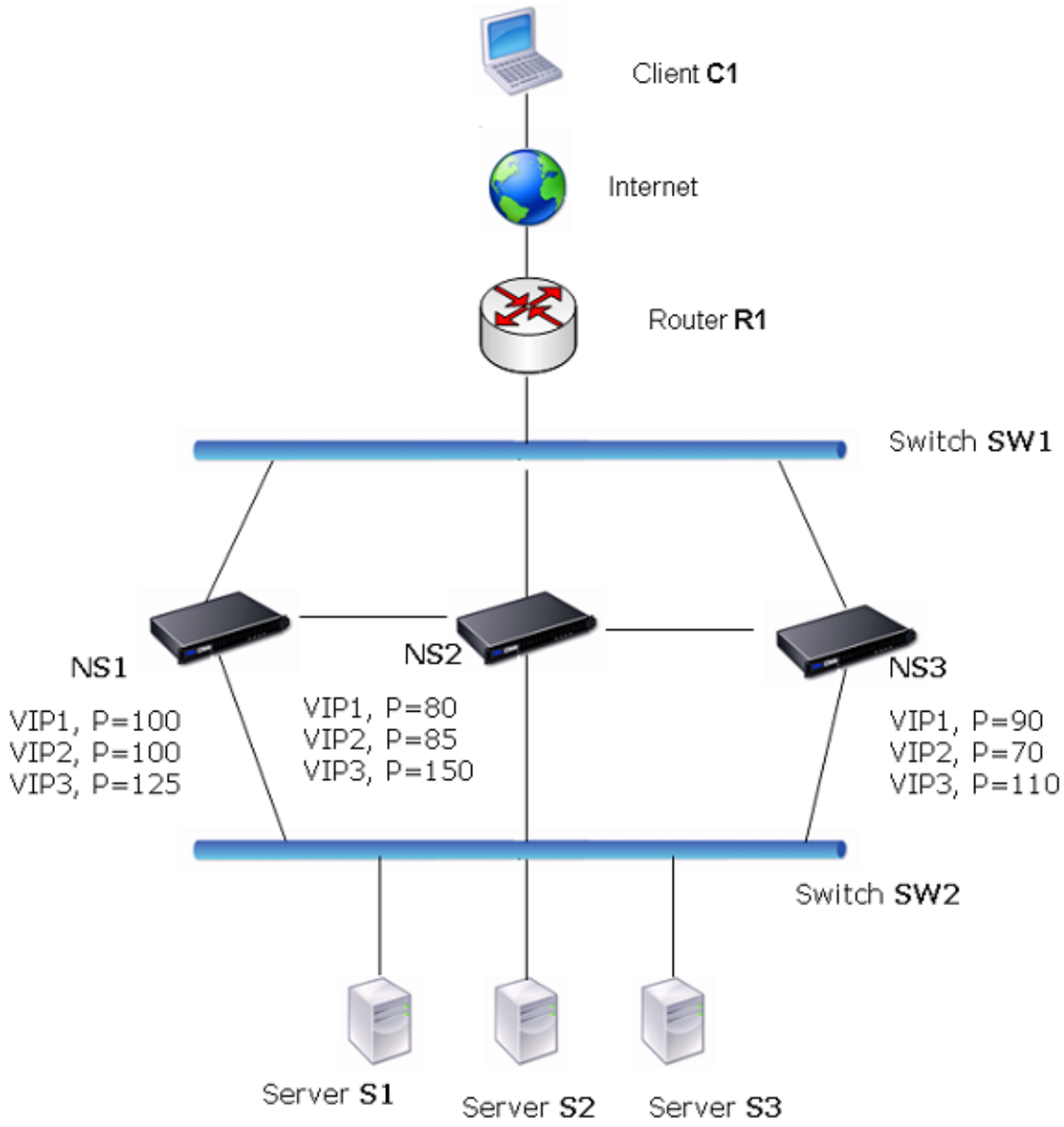
May 5, 2023

Un déploiement actif-actif permet non seulement d'éviter les temps d'arrêt, mais aussi d'utiliser efficacement toutes les appliances NetScaler du déploiement. En mode de déploiement actif-actif, les mêmes VIP sont configurés sur toutes les appliances NetScaler de la configuration, mais avec des priorités différentes, de sorte qu'un VIP donné ne peut être actif que sur une appliance à la fois.

Le VIP actif est appelé VIP principal, et les VIP correspondants sur les autres appliances NetScaler sont appelés VIP de sauvegarde. En cas de défaillance d'un VIP principal, le VIP de secours ayant la priorité la plus élevée prend le relais et devient le VIP principal. Toutes les appliances NetScaler participant à un déploiement actif-actif utilisent le protocole VRRP (Virtual Router Redundancy Protocol) pour annoncer leurs VIP et les priorités correspondantes à intervalles réguliers.

Les appliances NetScaler en mode actif-actif peuvent être configurées de telle sorte qu'aucun NetScaler ne soit inactif. Dans cette configuration, différents ensembles de VIP sont actifs sur chaque NetScaler. Par exemple, dans le schéma suivant, VIP1, VIP2, VIP3 et VIP4 sont configurés sur les appliances NS1, NS2 et NS3. En raison de leurs priorités, VIP1 et VIP 2 sont actifs sur NS1, VIP3 est actif sur NS2 et VIP 4 est actif sur NS3. Si, par exemple, NS1 échoue, VIP1 sur NS3 et VIP2 sur NS2 deviennent actifs.

Figure 1. Une configuration active-active



Les appliances NetScaler présentées dans le schéma ci-dessus traitent le trafic comme suit :

1. Le client C1 envoie une demande à VIP1. La demande atteint R1.
2. R1 ne possède pas d'entrée ARP pour VIP1, il diffuse donc une requête ARP pour VIP1.
3. VIP1 étant actif dans NS1, NS1 répond avec une adresse MAC source en tant que MAC virtuel (par exemple MAC1 virtuel) associée à VIP1, et VIP1 en tant qu'adresse IP source.
4. SW1 apprend le port pour VIP1 à partir de la réponse ARP et met à jour sa table de pont.
5. R1 met à jour l'entrée ARP avec les entrées MAC1 et VIP1 virtuels.

6. R1 transmet le paquet au VIP1 sur NS1.
7. L'algorithme d'équilibrage de charge de NS1 sélectionne le serveur S2, et NS1 ouvre une connexion entre l'une de ses adresses SNIP et S2.
8. S2 répond au SNIP sur NetScaler.
9. NS1 envoie la réponse de S2 au client. Dans la réponse, NS1 insère l'adresse MAC de l'interface physique comme adresse MAC source et VIP1 comme adresse IP source.
10. En cas de défaillance de NS1, les appliances NetScaler utilisent le protocole VRRP pour sélectionner le VIP1 ayant la priorité la plus élevée. Dans ce cas, VIP1 sur NS3 devient actif et les deux étapes suivantes mettent à jour la configuration active-active.
11. NS3 diffuse un message GARP pour VIP1. Dans le message, le MAC1 virtuel est l'adresse MAC source et VIP1 est l'adresse IP source.
12. SW1 découvre le nouveau port pour le MAC1 virtuel à partir de la diffusion GARP et met à jour sa table de pont pour envoyer les demandes clients suivantes pour VIP1 à NS3. R1 met à jour sa table ARP.

La priorité d'un VIP peut être modifiée par le suivi de l'état de santé. Si vous activez le suivi de l'état de santé, vous devez vous assurer que la préemption est également activée, afin qu'un VIP dont la priorité est réduite puisse être devancé par un autre VIP.

Dans certains cas, le trafic peut atteindre un VIP de secours. Pour éviter de supprimer ce trafic, vous pouvez activer le partage, nœud par nœud, lors de la création d'une configuration active-active. Vous pouvez également activer l'option d'envoi global vers le serveur principal. Sur un nœud sur lequel le partage est activé, il est prioritaire par rapport à l'envoi vers le serveur principal.

Suivi de la santé

La priorité de base (BP-range 1-255) détermine généralement quel VIP est le VIP principal, mais la priorité effective (EP) peut également affecter la détermination.

Par exemple, si un VIP sur NS1 a une priorité de 101 et que le même VIP sur NS2 a une priorité de 99, le VIP sur NS1 est actif. Toutefois, si deux serveurs virtuels utilisent le VIP sur NS1 et que l'un d'entre eux tombe en panne, le suivi de l'état de santé peut réduire l'EP du VIP sur NS1. VRRP fait ensuite du VIP sur NS2 le VIP actif.

Les options de suivi de l'état de santé permettant de modifier l'EP sont les suivantes :

- **AUCUN.** Pas de suivi. EP = BP
- **ALL.** Si tous les serveurs virtuels sont actifs, alors EP = BP. Dans le cas contraire, EP = 0.
- **UN.** Si au moins un serveur virtuel est actif, alors EP = BP. Dans le cas contraire, EP = 0.
- **PROGRESSIF.** Si TOUS les serveurs virtuels fonctionnent, alors EP = BP. Si TOUS les serveurs virtuels sont hors service, EP = 0. Sinon EP = BP (1 - K/N), où N est le nombre total de serveurs virtuels associés au VIP et k est le nombre de serveurs virtuels inactifs.

Remarque : Si vous spécifiez une valeur autre que NONE, la préemption doit être activée, de sorte que le VIP de sauvegarde ayant la priorité la plus élevée soit actif si la priorité du VIP principal est abaissée.

Préemption

La préemption d'un VIP actif par un autre VIP qui atteint une priorité plus élevée est activée par défaut et devrait normalement être activée. Dans certains cas, toutefois, vous souhaiterez peut-être le désactiver. La préemption est un paramètre par nœud pour chaque VIP.

La préemption peut se produire dans les situations suivantes :

- Un VIP actif tombe en panne et un VIP avec une priorité inférieure prend sa place. Si le VIP ayant la priorité la plus élevée revient en ligne, il devance le VIP actuellement actif.
- Le suivi de l'état de santé fait en sorte que la priorité d'un VIP de sauvegarde soit supérieure à celle du VIP actif. Le VIP de sauvegarde préempte ensuite le VIP actif.

Partage

Si le trafic atteint un VIP de sauvegarde, le trafic est interrompu à moins que l'option de partage ne soit activée sur le VIP de sauvegarde. Ce comportement est un paramètre par nœud pour chaque VIP et est désactivé par défaut.

Dans la figure **Une configuration active-active** VIP1 sur NS1 est active et les VIP VIP1 sur NS2 et NS3 sont des sauvegardes. Dans certaines circonstances, le trafic peut atteindre VIP1 sur NS2. Si le partage est activé sur NS2, ce trafic est traité au lieu d'être supprimé.

Configuration du mode actif-actif

May 5, 2023

Sur chaque appliance NetScaler que vous souhaitez déployer en mode actif-actif, vous devez ajouter un MAC virtuel et lier le MAC virtuel à un VIP. Le MAC virtuel d'un VIP donné doit être identique sur chaque appliance. Par exemple, si VIP 10.102.29.5 est créé sur les appliances, un ID de routeur virtuel (VRID) doit être créé sur chaque NetScaler et lié à VIP 10.102.29.5 sur chaque NetScaler. Lorsque vous liez un MAC virtuel à un VIP, l'appliance envoie des publicités VRRP à chaque VLAN lié à ce VIP. Le MAC virtuel peut être partagé par différents VIP configurés sur le même NetScaler.

Configuration du mode actif-actif IPv4

Effectuez les tâches suivantes sur chacune des appliances NetScaler à inclure dans la configuration active-active :

- **Ajoutez une adresse MAC virtuelle**. Ajoutez une adresse MAC virtuelle en ajoutant un VRID. Vous pouvez également spécifier une priorité et activer ou désactiver la préemption et le partage sur cette adresse VRID.
- **Ajoutez une adresse VIP et associez le VRID du MAC virtuel**. Ajoutez une adresse VIP et définissez le paramètre VRID sur le VRID nouvellement créé. Les attributs du VRID (par exemple, priorité et préemption) sont liés à cette adresse VIP.
  Remarque : La même adresse VIP doit être ajoutée à toutes les autres appliances NetScaler.

Pour ajouter une adresse MAC virtuelle à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- **ajouter vRID** <tracking><id>[-**priorité** \<positive_integer>] [-**préemption** (**ACTIVÉ** |DÉSACTIVÉ**))][-**sharing** (**ENABLED**|**DISABLED**)] [-**suivi \]**
- **show vrid**

Pour ajouter une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter ns ip** <IPv4Address>-type VIP -vrid <value>
- **show ns ip**

Pour configurer un MAC virtuel à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC**, dans l'onglet **VMAC**, ajoutez un nouveau MAC virtuel ou modifiez un MAC virtuel existant.
2. Définissez les paramètres suivants :
   - ID du routeur virtuel
   - Priority
   - Suivi
   - Préemption
   - Partage

Pour configurer une adresse VIP et y associer le VRID à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP**, dans l'onglet **IPv4S**, ajoutez une adresse IP de type VIP.
2. Lors de l'ajout de l'adresse IP, sélectionnez l'ID du routeur virtuel dans la liste déroulante **Virtual Router Id** .

Exemple de configuration :

L'exemple de configuration suivant concerne le déploiement des appliances NetScaler NS1 et NS2 en mode actif-actif IPv4. L'adresse VIP 203.0.113.10 est configurée à la fois sur NS1 et NS2, avec une

valeur de priorité différente sur chaque appliance. Sur chaque appliance, cette adresse VIP est liée à une adresse MAC virtuelle. 203.0.113.10 est maître sur NS2, car sa priorité (200) sur NS2 est supérieure à celle sur NS1 (100).

```
    Settings on NS1

    > add vrid 10 -Priority 100 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

    Done

    Settings on NS2

    > add vrid 10 -Priority 200 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

    Done
<!--NeedCopy-->
```

Configuration du mode actif-actif d'IPv6

Effectuez les tâches suivantes sur chacune des appliances NetScaler à inclure dans la configuration active-active :

- **Ajoutez une adresse MAC6 virtuelle**. Ajoutez une adresse MAC6 virtuelle en ajoutant un VRID6. Vous pouvez également spécifier une priorité et activer ou désactiver la préemption et le partage sur cette adresse VRID6.
- **Ajoutez une adresse VIP6**. Ajoutez une adresse VIP6. Définissez le paramètre VRID6 sur le VRID6 du MAC virtuel nouvellement créé. Les attributs du MAC6 virtuel (par exemple, priorité et préemption) sont liés à cette adresse VIP6.
  Remarque : La même adresse VIP6 doit être ajoutée à toutes les autres appliances NetScaler.

Pour ajouter une adresse MAC6 virtuelle à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter vRID6** <id>[-**priorité** \<positive_integer>] [-**préemption** (**ACTIVÉE** | **DÉSACTIVÉE**)] [-**partage 0 (1 ACTIVÉ | DÉSACTIVÉ 2)] 3 4****

- **show vrID6**

Pour ajouter une adresse VIP6 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajoute-nous ip6**-type** VIP - vrid** <IPv6Address><value>
- **show ns ip6**

Pour configurer un MAC6 virtuel à l'aide de l'interface graphique :

1. **Accédez à**Système**>**Réseau**>**VMAC**, dans l'onglet**VMAC6**, ajoutez un nouveau MAC6 virtuel ou modifiez un VMAC6 existant.**
2. Définissez les paramètres suivants :
   - ID du routeur virtuel
   - Priority
   - Préemption
   - Partage

Pour configurer une adresse VIP6 et y associer le VRID à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP**. Dans l'onglet **IPv6 s**, ajoutez une adresse IPv6 de type VIP.
2. Lors de l'ajout de l'adresse VIP6, sélectionnez le VRID6 dans la liste déroulante **Virtual Router Id** .

Exemple de configuration :

L'exemple de configuration suivant concerne le déploiement des appliances NetScaler NS1 et NS2 en mode actif-actif IPv6. L'adresse VIP6 2001:db8 : :5001 est configurée à la fois sur NS1 et NS2, avec une valeur de priorité différente sur chaque appliance. Sur chaque appliance, cette adresse VIP6 est liée à une adresse MAC6 virtuelle. 2001:db8 : :5001 est maître sur NS2, car sa priorité (200) sur NS2 est supérieure à celle sur NS1 (100).

```
    Settings on NS1
    > add vrid6 10 - Priority 100 - Preemption Enable - sharing Enable

    Done
    > add ns ip6 2001:db8::5001 - type VIP - vrid6 10

    Done
    Settings on NS2
    > add vrid6 10 - Priority 200 - Preemption Enable - sharing Enable

    Done
    > add ns ip6 2001:db8::5001 - type VIP - vrid6 10

    Done
<!--NeedCopy-->
```

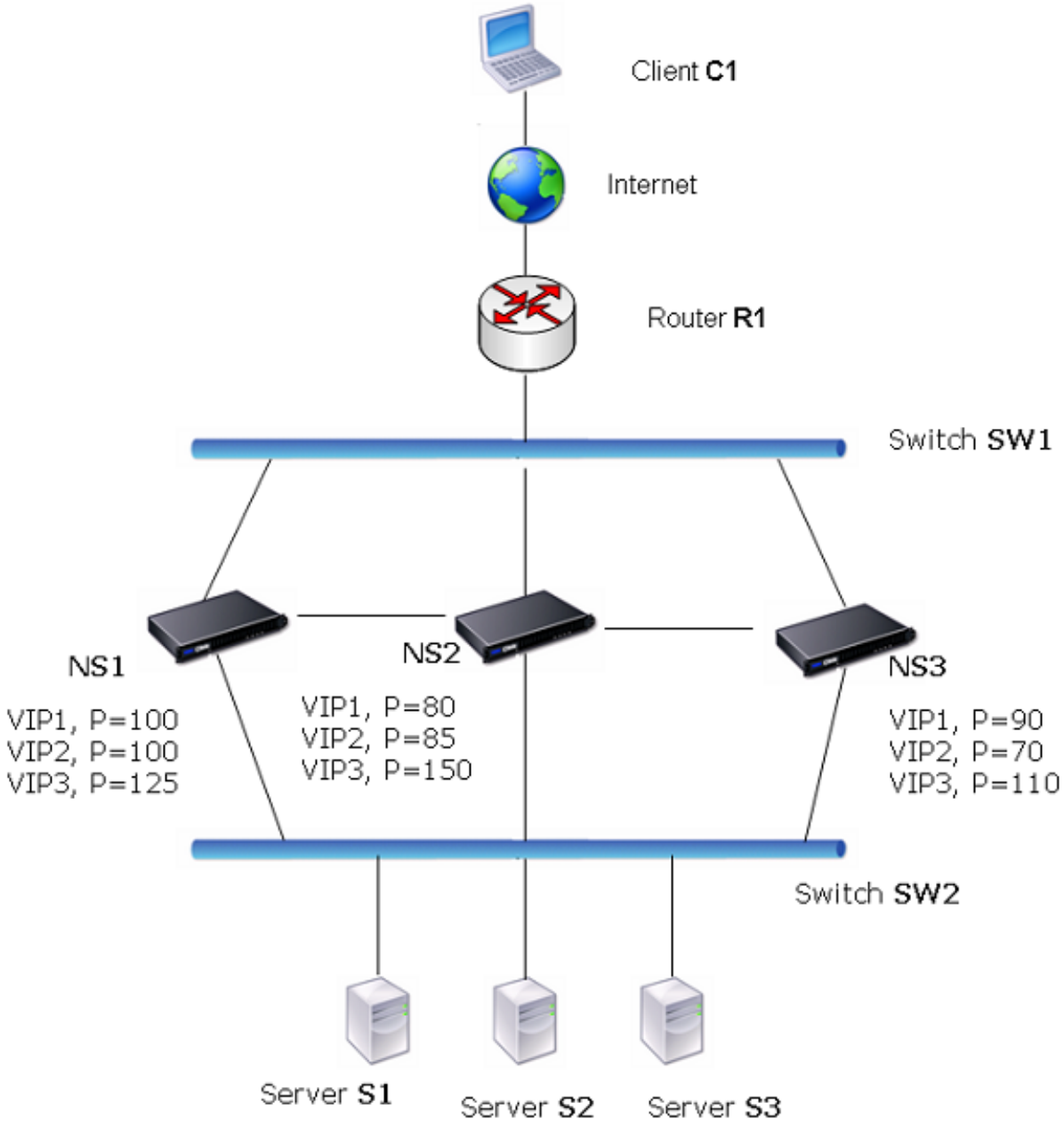

Configuration de l’envoi vers le maître

May 5, 2023

Habituellement, le trafic destiné à un VIP atteint l’appliance NetScaler sur laquelle le VIP est actif, car une demande ARP avec le VIP et un MAC virtuel sur cette appliance a atteint le routeur en amont. Mais dans certains cas, tels que des itinéraires statiques configurés sur le routeur en amont pour le sous-réseau VIP ou une topologie bloquant cet itinéraire, le trafic peut atteindre une appliance NetScaler sur laquelle le VIP est en état de sauvegarde. Si vous souhaitez que cette appliance transfère les paquets de données à l’appliance sur laquelle le VIP est actif, vous devez activer l’option d’envoi vers le maître. Ce comportement est un paramètre par nœud et est désactivé par défaut.

Par exemple, dans le schéma suivant, VIP1 est configuré sur NS1, NS2 et NS3 et est actif sur NS1. Dans certaines circonstances, le trafic destiné à VIP1 (actif sur NS1) peut atteindre VIP1 sur NS3. Lorsque l’option d’envoi vers le maître est activée sur NS3, NS3 transfère le trafic vers NS1 via NS2 en utilisant les entrées de route pour NS1.

Figure 1. Une configuration active-active avec l’option Envoyer vers le maître activée



Pour activer l'envoi vers le maître à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

définir VRIDParam- SendToMaster (ACTIVÉ)****	(**HANDICAPÉ**)

Exemple :


```
> set vrIDParam -sendToMaster ENABLED
 Done
<!--NeedCopy-->
```

Pour activer l'envoi vers le maître à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Paramètres du routeur virtuel**.
2. Sélectionnez l'option **Envoyer au maître** .

Configuration des intervalles de communication VRRP

May 5, 2023

Dans un déploiement actif-actif, tous les nœuds NetScaler utilisent le protocole VRRP (Virtual Router Redundancy Protocol) pour publier leurs adresses VIP principales et les priorités correspondantes dans des paquets publicitaires VRRP (messages d'accueil) à intervalles réguliers.

Le VRRP utilise les intervalles de communication suivants :

- **Hello Interval**. Intervalle entre les messages d'accueil VRRP qu'un nœud d'une adresse VIP principale envoie à ses nœuds homologues.
- **Dead Interval**. Délai au bout duquel le nœud d'une adresse VIP de secours considère que l'état de l'adresse VIP principale est DOWN si aucun message d'bonjour VRRP n'est reçu du nœud de l'adresse VIP principale. Après l'intervalle mort, l'adresse VIP de sauvegarde prend le relais et devient l'adresse VIP principale.

Vous pouvez modifier ces intervalles à la valeur souhaitée. Ces deux intervalles de communication sont définis par nœud pour toutes les adresses VIP de ce nœud.

Pour configurer les intervalles de communication VRRP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **définissez vridParam** <secs>[-**HelloInterval** \<msecs>] [- DeadInterval \]**
- **sh vrIDParam**

Exemple :

```
> set vrIDParam -helloInterval 500 -deadInterval 2
 Done
<!--NeedCopy-->
```

Pour configurer les intervalles de communication VRRP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau**, dans le groupe **Paramètres**, cliquez sur **Paramètres du routeur virtuel**.
2. Dans **Configurer le paramètre du routeur virtuel**, définissez les paramètres **Hello Interval** et **Dead Interval** .
3. Cliquez sur **OK**.

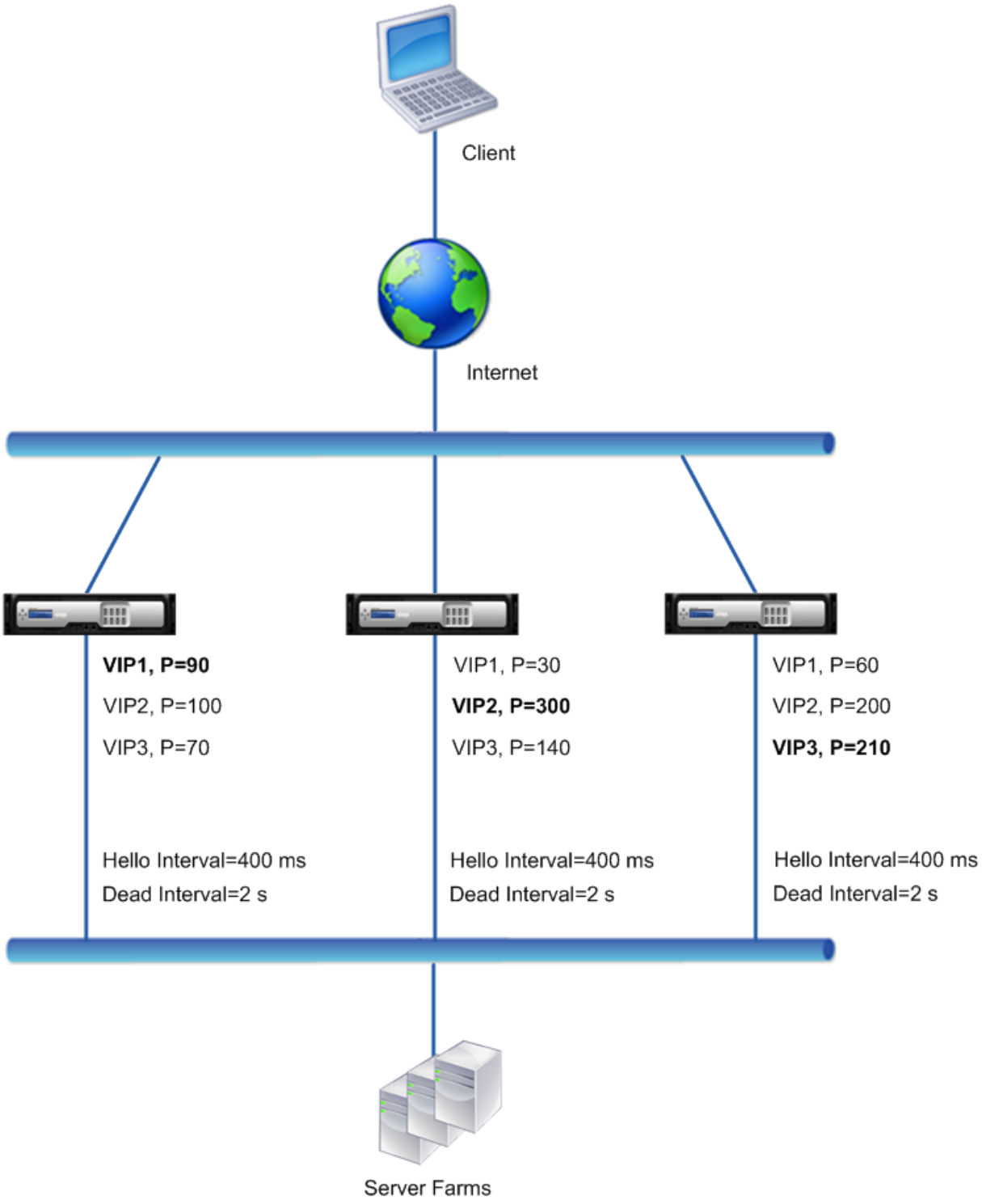
Exemple 1 : Nœuds avec les mêmes intervalles morts VRRP

Envisagez un déploiement actif-actif composé de NetScalers NS1, NS2 et NS3. Les adresses IP virtuelles VIP1, VIP2, VIP3 sont configurées sur chacun de ces ADC. En raison de leurs priorités, VIP1 est actif sur NS1, VIP2 est actif sur NS2 et VIP3 est actif sur NS3.

Comme indiqué dans le tableau ci-dessous, l'intervalle mort est défini sur la même valeur (2 secondes) sur les trois nœuds. Les intervalles de communication VRRP (intervalle bonjour et intervalle mort) d'un nœud s'appliquent à tous les VRID configurés sur le nœud et, à leur tour, à toutes les adresses VIP associées aux VRID du nœud.

Sur chaque nœud, les adresses VIP actives (master) sur ce nœud utilisent l'intervalle hello, et l'intervalle mort est utilisé par les adresses VIP inactives (sauvegarde) sur ce nœud. La préemption est désactivée pour les adresses VIP des trois nœuds.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple : paramètres de l'exemple 1 de l'intervalle VRRP.



Le flux d'exécution est le suivant :

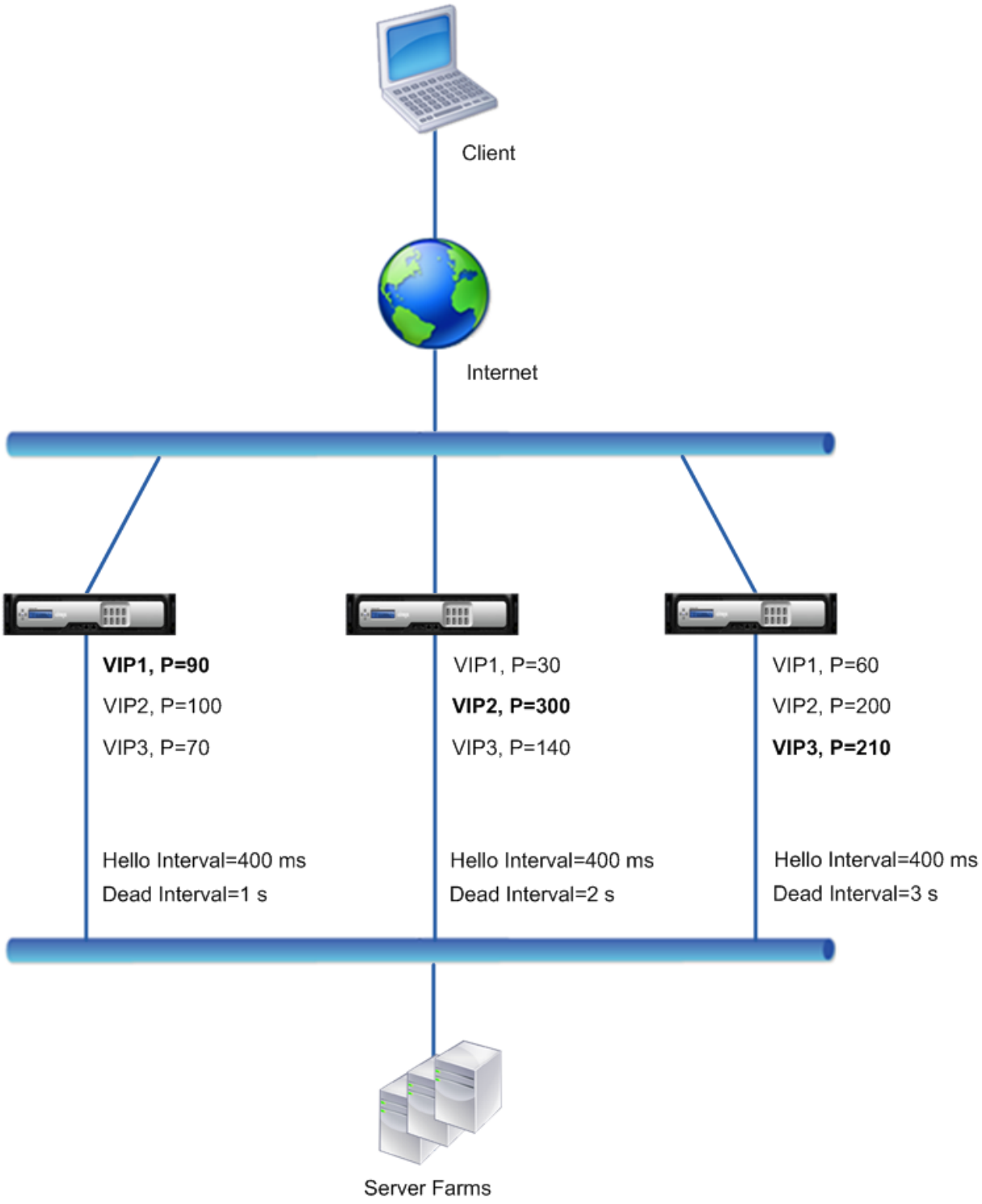
1. NS1 envoie des messages bonjour à un intervalle défini de 400 ms à NS2 et NS3 pour l'adresse VIP1, car VIP1 est actif (le maître) sur NS1. De même, NS2 envoie des messages d'bonjour pour VIP2 et NS3 envoie des messages d'bonjour pour VIP3.

2. Sur NS1, l'intervalle mort défini s'applique à VIP2 et VIP3, car ils sont inactifs (sauvegardes) sur NS1. De même, sur NS2, l'intervalle mort défini s'applique à VIP1 et VIP3, et sur NS3, l'intervalle mort défini s'applique à VIP1 et VIP2.
3. Si NS1 tombe en panne, NS2 et NS3 considèrent que NS1 est hors service s'ils ne reçoivent aucun message d'accueil de NS1 pendant 2 secondes (intervalle d'inactivité). VIP1 sur NS3 prend le relais et devient actif (master) car sa priorité VRID (60) est supérieure à celle de VIP1 sur NS2 (30).

Exemple 2 : Nœuds avec différents intervalles morts VRRP

Envisagez un déploiement VRRP similaire au déploiement décrit dans l'exemple 1, mais avec un intervalle mort différent sur chaque nœud (NS1, NS2 et NS3). La préemption est désactivée pour les adresses VIP des trois nœuds.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple : paramètres de l'exemple 2 de l'intervalle VRRP.



Le flux d'exécution est le suivant lorsque NS1 tombe en panne :

1. NS2 considère que NS1 est hors service après n'avoir reçu aucun message d'accueil de NS1 pendant 2 secondes (intervalle mort de NS2).
2. VIP1 sur NS2 prend le relais et devient actif (master). NS2 commence maintenant à envoyer des

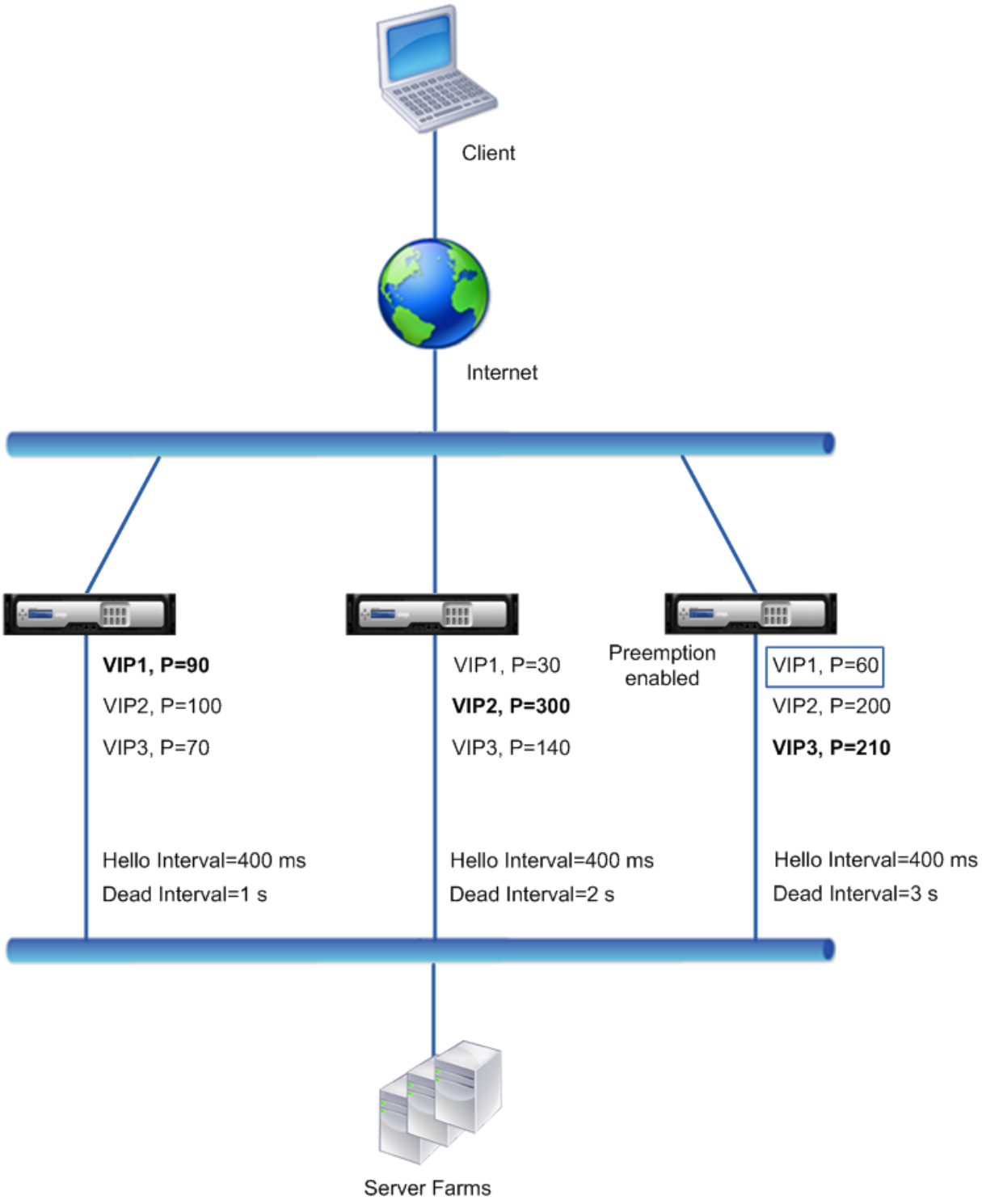
messages de bonjour pour VIP1.

Même si VIP1 sur NS3 a une priorité VRIP plus élevée (60) que VIP1 sur NS2 (30), l'intervalle mort plus long de NS3 (3 secondes, contre 2 secondes pour NS2) empêche VIP1 sur NS3 de prendre le relais avant que VIP 1 sur NS2 ne l'ait déjà fait.

Exemple 3 : Nœuds avec différents intervalles morts et la préemption activée

Considérez un déploiement VRRP similaire au déploiement décrit dans l'Example1, mais avec des intervalles morts différents sur les trois nœuds, NS1, NS2 et NS3, et avec la préemption activée pour l'adresse VIP1 sur NS3.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple : paramètres de l'exemple 3 de l'intervalle VRRP.



Le flux d'exécution est le suivant lorsque NS1 tombe en panne :

1. NS2 considère que NS1 est hors service après n'avoir reçu aucun message d'accueil de NS1 pendant 2 secondes (intervalle mort défini par NS2). À ce stade, NS3, avec un intervalle mort de 3 secondes, ne considère pas que NS1 est en panne.

2. VIP1 sur NS2 prend le relais et devient actif (master). NS2 commence maintenant à envoyer des messages de bonjour pour VIP1.
3. Lors de la réception de messages bonjour de NS2 pour VIP1, NS3 préempte NS2 pour VIP1 car la préemption est activée pour VIP1 de NS3 et la priorité VRID (60) de VIP1 de NS3 est supérieure à celle (30) de VIP1 de NS2.
4. VIP1 sur NS3 prend le relais et devient actif (master). NS3 commence maintenant à envoyer des messages de bonjour pour VIP1.

Configuration du suivi de l'intégrité en fonction de l'état de l'interface

May 5, 2023

Pour garantir qu'une adresse VIP de secours prenne le relais en tant que VIP principale avant que le nœud de l'adresse VIP principale actuelle ne tombe complètement en panne, vous pouvez configurer un nœud pour modifier la priorité d'une adresse VIP lorsque l'état d'une interface sur le nœud change. Par exemple, le nœud réduit la priorité d'une adresse VIP lorsque l'état d'une interface passe à DOWN, et augmente la priorité lorsque l'état de l'interface passe à UP. Cette fonctionnalité est une configuration par nœud pour chaque adresse VIP.

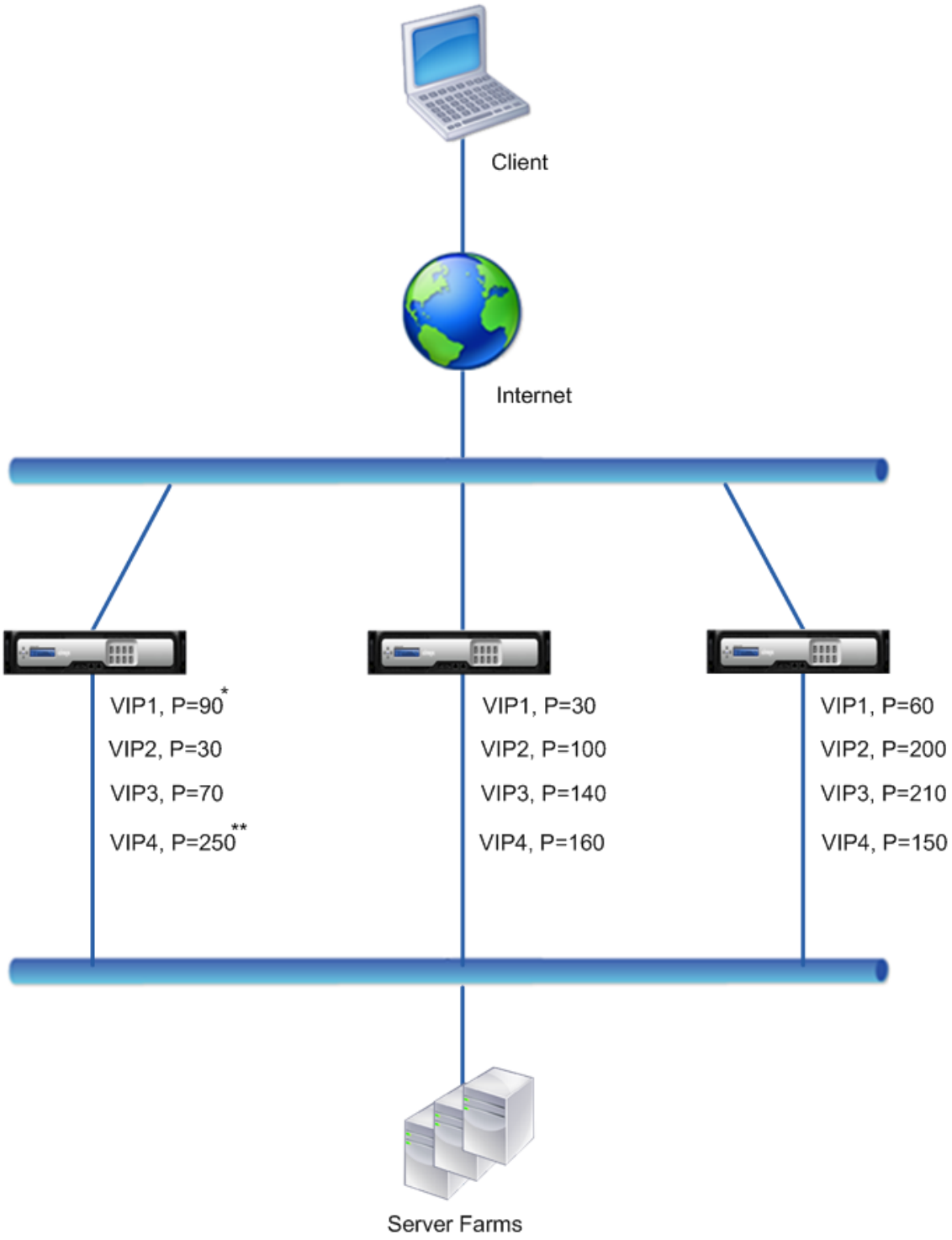
Exemple

Envisagez un déploiement actif-actif composé de NetScalers NS1, NS2 et NS3. Les adresses IP virtuelles VIP1, VIP2, VIP3 et VIP4 sont configurées sur chacun de ces ADC. En raison de leurs priorités, VIP1 et VIP4 sont actifs sur NS1, VIP2 est actif sur NS2 et VIP3 est actif sur NS3.

Pour garantir que les adresses VIP actives sur NS1 sont reprises par NS2 ou NS3 avant que NS1 ne tombe complètement en panne, le suivi de l'état basé sur l'interface est configuré pour les adresses VIP1 et VIP4 sur NS1. La configuration du suivi de santé basé sur l'interface pour une adresse VIP consiste à associer les interfaces souhaitées et à définir le paramètre de priorité réduite (TrackIfNumPriority) pour le VRID associé à l'adresse VIP. Par exemple, sur NS1, les interfaces 1/2, 1/3 et 1/5 sont associées au VRID de VIP1, et la priorité réduite est définie sur 20.

La préemption est activée pour ces adresses VIP dans les trois nœuds.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple : exemples de paramètres de suivi de l'état de santé.



* Packet Interfaces = 1/2, 1/3, 1/5
Reduced Priority = 20

** Packet Interfaces = 1/5, 1/7
Reduced Priority = 55

Le flux d'exécution est le suivant sur NS1 lorsque plusieurs interfaces tombent en panne sur NS1 :

1. Si l'interface 1/3 tombe en panne, la priorité de l'adresse VIP1 est réduite de 20 (valeur de priorité réduite de VIP1), car l'interface 1/3 est associée à VIP1 :
   - Priorité effective du VIP1 = (Priorité actuelle - priorité réduite) = (90-20) = 70
2. De même, si l'interface 1/5 tombe en panne, la priorité de l'adresse VIP1 est encore réduite :
   - Priorité effective de VIP1 = (Priorité actuelle - priorité réduite) = (70-20) = 50
3. À ce stade, la priorité effective de VIP1 sur NS1 est inférieure à la priorité de VIP1 sur NS3. NS3 préempte NS1 pour VIP1. VIP1 sur NS3 prend le relais et devient actif (master).
4. De plus, étant donné que l'interface 1/5 est également associée à VIP4, la priorité de VIP4 est réduite de la valeur de priorité réduite du VIP4 (55).
   - Priorité effective du VIP4 = (250 - 55) = 195
5. Si l'interface 1/7 tombe en panne, la priorité de VIP4 est encore réduite :
   - Priorité effective du VIP4 = (Priorité actuelle - priorité réduite) = (195-55) = 145
6. À ce stade, la priorité effective de VIP4 sur NS1 est inférieure à la priorité de VIP4 sur NS2. NS2 préempte NS1 pour VIP4. VIP4 sur NS3 prend le relais et devient actif (master). Cette configuration garantit qu'aucune des quatre adresses VIP n'est active sur NS1 avant qu'elle ne tombe complètement en panne.

Étapes de configuration pour le mode actif-actif IPv4

Pour configurer cette fonctionnalité sur un nœud pour une adresse VIP, vous définissez le paramètre de priorité réduite (TrackIfNumPriority), puis vous associez les interfaces dont l'état doit être suivi pour modifier la priorité de l'adresse VIP. Lorsque l'état de l'interface associée passe à DOWN ou UP, le nœud réduit ou augmente la priorité de l'adresse VIP selon la valeur de priorité réduite configurée (TrackIfNumPriority).

Pour définir une priorité réduite et lier les interfaces à l'ID du routeur virtuel à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **définir vRid [-**** <id><positive_integer>TrackIfNumPriority \]
- **bind vrID** <id> -**trackifNum** <interface_name>
- **afficher le vRId** <id>

Exemple :

```
    > set vrID 125 -trackifNumPriority 10
    Done

    > bind vrID 125 -trackifNum 1/4 1/5
    Done
<!--NeedCopy-->
```


Pour définir une priorité réduite et lier les interfaces à l'ID du routeur virtuel à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC**.
2. **Dans l'onglet**VMacs**, sélectionnez un ID de routeur virtuel, puis cliquez sur Modifier.**
3. Sous **Configurer le MAC virtuel**, définissez le paramètre **Priorité réduite** .
4. Sélectionnez les **interfaces suivies pour l'option VRID** et, sous **Interfaces associées**, ajoutez des interfaces à l'ID du routeur virtuel.

Étapes de configuration pour le mode actif-actif d'IPv6

Pour configurer cette fonctionnalité sur un nœud pour une adresse VIP6, vous définissez le paramètre de priorité réduite (TrackIfNumPriority), puis vous associez les interfaces dont l'état doit être suivi pour modifier la priorité de l'adresse VIP6. Lorsque l'état de l'interface associée passe à DOWN ou UP, le nœud réduit ou augmente la priorité de l'adresse VIP6 selon la valeur de priorité réduite configurée (TrackIfNumPriority).

Pour modifier automatiquement la priorité d'une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

- Si vous ajoutez un nouveau MAC6 virtuel :
  - **ajouter vRID6** <positive_integer><id>[-** TrackIfNumPriority \]
  - **lier vRID6** <id- **TrackIfNum** <interface_name>
  - **afficher vRID6** <id>
- Si vous reconfigurez un MAC6 virtuel existant :
  - **définir vRID6** <positive_integer><id>[-** TrackIfNumPriority \]
  - **lier vRID6** <id- **TrackIfNum** <interface_name>
  - **afficher vRID6** <id>

Exemple :

```
    > set vrID6 130 -trackifNumPriority 10
    Done

    > bind vrID6 130 -trackifNum 1/4 1/5
    Done
<!--NeedCopy-->
```


Retarder la préemption

May 5, 2023

Par défaut, une adresse VIP de secours préempte l'adresse VIP principale immédiatement lorsque sa priorité devient supérieure à celle du VIP principal. Lorsque vous configurez une adresse VIP de sauvegarde, vous pouvez spécifier la durée pendant laquelle vous souhaitez retarder la préemption. Le délai de préemption est un paramètre par nœud pour chaque adresse VIP de sauvegarde.

Le paramètre de délai de préemption pour un VIP de sauvegarde ne s'applique pas dans les conditions suivantes :

- Le nœud du VIP principal tombe en panne. Dans ce cas, le VIP de sauvegarde prend le relais en tant que VIP principal après l'intervalle mort défini sur le nœud du VIP de sauvegarde.
- La priorité du VIP principal est fixée à zéro. Le VIP de sauvegarde prend le relais en tant que VIP principal après l'intervalle d'inactivité défini sur le nœud du VIP de sauvegarde.

Exemple : report de la préemption

Envisagez un déploiement actif-actif composé d'appliances NetScaler NS1 et NS2. L'adresse IP virtuelle VIP1 est configurée sur chacune de ces appliances. En raison de leurs priorités, VIP1 est maître sur NS2. La préemption est activée et le délai de préemption est défini pour VIP1 sur ces deux nœuds.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Entité et paramètres	Paramètres sur NS1	Paramètres sur NS2
VIP1 (à titre de référence uniquement)	**Adresse IP :192.0.1.10, **VRID : 10, Priorité :100, Préemption :**activée,**Délai de préemption :**1000 secondes**	**Adresse IP :192.0.1.10, **VRID : 10, Priorité :200, Préemption :**activée,**Délai de préemption :**2000 secondes**
Intervalle mort	1 secondes	2 secondes

Voici quelques exemples de comportements de préemption possibles dans cette configuration :

- Si la priorité de VIP1 sur NS1 est définie sur une valeur (par exemple, 210) supérieure à celle de VIP1 sur NS2, VIP1 sur NS1 prend le relais en tant que maître après le délai de préemption défini (1 000 secondes).
- Si un troisième nœud NS3 avec les paramètres VRRP suivants est ajouté à ce déploiement, VIP1 sur NS3 devient maître après le délai de préemption défini (3 000 secondes).

    - VIP1
        * GRILLE : 30
        * Adresse IP :
        * Priorité = 300
        * Délai de préemption = 3000 secondes
- Si NS2 tombe en panne, VIP1 sur NS1 prend le relais en tant que maître au bout d'une seconde (définissez un intervalle mort sur NS1). Le délai de préemption pour VIP1 sur NS1 ne s'applique pas dans ce cas.
- Si NS2 tombe en panne et que NS1 redémarre, VIP1 sur NS1 devient maître 1 seconde (définir un intervalle mort sur NS1) après le démarrage de NS1. Le délai de préemption pour VIP1 sur NS1 ne s'applique pas dans ce cas.
- Si la priorité de VIP1 sur NS2 est définie sur zéro, VIP1 passe en mode veille. VIP1 sur NS1 prend le relais en tant que maître au bout d'une seconde (définissez un intervalle mort sur NS1). Le délai de préemption pour VIP1 sur NS1 ne s'applique pas dans ce cas.

Configuration de la préemption des délais pour le mode actif-actif IPv4

Pour configurer le délai de préemption pour une adresse VIP, vous devez définir le paramètre du délai de préemption de l'adresse MAC virtuelle associée. Vous pouvez définir ce paramètre lorsque vous ajoutez l'adresse, ou vous pouvez modifier une adresse MAC virtuelle existante.

Pour configurer le délai de préemption à l'aide de l'interface de ligne de commande :

- Pour définir le délai de préemption lors de l'ajout d'un MAC virtuel, à l'invite de commande, tapez :
    - ****ajouter un vRID - preemptiondelaytimer**** <id><secs>
    - **afficher le vRId**
- Pour définir le délai de préemption lors de la modification d'un MAC virtuel, à l'invite de commandes, tapez :
    - ****définir vRId - preemptiondelaytimer**** <id><secs>
    - **afficher le vRId**

Pour configurer le délai de préemption à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC**.
2. Dans l'onglet **VMAC** . Lors de l'ajout d'un nouveau MAC virtuel ou de la modification d'un MAC virtuel existant, définissez le paramètre **Preemption Delay Timer** .

Exemple de configuration :

La configuration suivante utilise les paramètres répertoriés dans le tableau de la section Exemple : Retarder la préemption.

```
1     Settings on NS1
```



```
2
3       > set vrid param  - deadInterval 1
4
5       Done
6
7       > add ns ip 192.0.1.10 255.255.255.255  - type VIP
8
9       Done
10
11      > add vrid 10  - Priority 100  - Preemption Enable  -
           preemptiondelaytimer 1000
12
13      Done
14
15      > bind ns ip 192.0.1.10 255.255.255.255  - vrid 10
16
17      Done
18
19      Settings on NS2
20
21      > set vrid param  - deadInterval 2
22
23      Done
24
25      > add ns ip 192.0.1.10 255.255.255.255  - type VIP
26
27      Done
28
29      > add vrid 20  - Priority 200  - Preemption Enable  -
           preemptiondelaytimer 2000
30
31      Done
32
33      > set ns ip 192.0.1.10 255.255.255.255  - vrid 10
34
35      Done
36  <!--NeedCopy-->
```

Configuration de la préemption des délais pour le mode actif-actif d'IPv6

Pour configurer le délai de préemption pour une adresse VIP6, vous devez définir le paramètre du temporisateur de préemption de l'adresse MAC6 virtuelle associée. Vous pouvez définir ce paramètre lorsque vous ajoutez l'adresse MAC6 virtuelle, ou vous pouvez modifier une adresse MAC6 virtuelle

existante.

Pour configurer le délai de préemption à l'aide de l'interface de ligne de commande :

- Pour définir le délai de préemption lors de l'ajout d'un MAC6 virtuel, à l'invite de commande, tapez :
  - **ajouter vRid6** <id- **PreemptionDelaytimer** <secs>
  - **show vrID6**
- Pour définir le délai de préemption lors de la modification d'un MAC6 virtuel, à l'invite de commande, tapez :
  - **set vRID6** <id- **temporisateur de préemption** <secs>
  - **show vrID6**

Pour configurer le délai de préemption à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC**.
2. Dans l'onglet **VMAC6** . Lors de l'ajout d'une adresse MAC6 virtuelle ou de la modification d'une adresse MAC6 virtuelle existante, définissez le paramètre **Preemption Delay Timer** .

Conserver une adresse VIP dans l'état de sauvegarde

January 21, 2021

Vous pouvez forcer une adresse VIP à rester toujours en état de sauvegarde. Cette opération est utile pour la maintenance ou le test d'un déploiement VRRP.

Lorsqu'une adresse VIP est forcée de rester en état de sauvegarde, elle ne participe pas aux transitions d'état VRRP. En outre, il ne peut pas devenir maître même si tous les autres nœuds tombent en panne.

Pour forcer une adresse VIP à rester en état de sauvegarde, définissez la priorité de l'adresse MAC virtuelle associée sur zéro. Pour s'assurer qu'aucune des adresses VIP d'un nœud ne gère le trafic au cours d'un processus de maintenance sur le nœud, définissez toutes les priorités sur zéro.

Vous pouvez définir la priorité d'une adresse MAC virtuelle lors de l'ajout ou de la modification de l'adresse.

Pour forcer une adresse VIP à rester dans l'état de sauvegarde à l'aide de l'interface de ligne de commande :

- Pour définir la priorité lors de l'ajout d'un MAC virtuel, à l'invite de commandes, tapez :
  - **add vrID** <id> -**priority** 0
  - **show vrID**
- Pour définir la priorité lors de la modification d'un MAC virtuel, à l'invite de commandes, tapez :

- **set vrID** <id> -**priority** 0
- **show vrID**

Pour forcer une adresse VIP à rester en état de sauvegarde à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **VMAC**.
2. Sous l'onglet **VMAC**, tout en ajoutant un nouveau MAC virtuel ou en modifiant un MAC virtuel existant, définissez le paramètre **Priority** sur zéro.

Visualiseur de réseau

May 5, 2023

Le visualiseur réseau affiche une vue graphique de toutes les interfaces, canaux, VLAN, adresses IP et liaisons aux VLAN d'une appliance NetScaler. Une interface ou un canal activé est marqué d'une étiquette noire. Une interface ou un canal désactivé est marqué en rouge.

Cette vue complète des connexions réseau de l'appliance peut être utile pour détecter les failles dans la conception du réseau et pour optimiser le réseau. Cela peut également aider un nouvel administrateur à comprendre facilement la configuration réseau de l'appliance.

Pour ouvrir le visualiseur de réseau :

Accédez à **Système** > **Réseau**. Dans **Moniteur des connexions**, cliquez sur **Visualiseur réseau**.

Configuration du protocole Link Layer Discovery Protocol

May 5, 2023

Le NetScaler prend en charge le protocole LLDP (Link Layer Discovery Protocol), une norme industrielle (IEEE 802.1AB). Le protocole LLDP est un protocole de couche 2 qui permet à NetScaler de faire connaître son identité et ses fonctionnalités aux appareils directement connectés, ainsi que de connaître l'identité et les fonctionnalités de ces appareils voisins.

> **Remarque :**
> Le protocole LLDP (Link Layer Discovery Protocol) est uniquement pris en charge sur les plateformes NetScaler MPX.

À l'aide de LLDP, NetScaler transmet et reçoit des informations sous la forme de messages LLDP appelés unités de données par paquets LLDP (LLDPU). Un LLDPU est une séquence d'éléments d'information de type, de longueur et de valeur (TLV). Chaque TLV contient un type spécifique d'informations sur le dispositif qui transmet le LLDPDU. Le NetScaler envoie les TLV suivants dans chaque LLDPU :

- ID du châssis
- ID de port
- Valeur en termes de durée de vie
- Nom du système
- Description du système
- Description du port
- Capacités du système
- Adresse de gestion
- ID du port VLAN
- Agrégation de liens

Remarque : Vous ne pouvez pas spécifier les TLV à envoyer dans les messages LLDP.

Les interfaces NetScaler prennent en charge les modes LLDP suivants :

- **NONE**. L'interface ne reçoit ni ne transmet de messages LLDP à l'appareil directement connecté.
- **ÉMETTEUR**. L'interface transmet des messages LLDP au périphérique directement connecté mais ne reçoit pas de messages LLDP du périphérique directement connecté.
- **RÉCEPTEUR**. L'interface reçoit des messages LLDP du périphérique directement connecté mais ne transmet pas de messages LLDP au périphérique directement connecté.
- **ÉMETTEUR-RÉCEPTEUR.** L'interface transmet des messages LLDP vers et reçoit des messages LLDP de l'appareil directement connecté.

Le mode LLDP d'une interface dépend du mode LLDP configuré aux niveaux global et de l'interface. Le tableau suivant présente les modes résultant des combinaisons disponibles de paramètres au niveau global et de l' interface : modes Interface et LLDP de niveau global.

Notez les points suivants relatifs aux messages LLDP transmis ou reçus par NetScaler :

- **Transmission de messages LLDP.** Le NetScaler transmet les LLDPU à partir d'interfaces qui fonctionnent en mode TRANSMITTER ou TRANSCEIVER LLDP.

  Les paramètres de transmission LLDP globaux sur NetScaler sont les suivants :

  - **Minuteur** Intervalle, en secondes, entre les LLDPU que NetScaler envoie à un appareil directement connecté.
  - **Multiplicateur Holdtime.** Un multiplicateur pour calculer la durée pendant laquelle le dispositif récepteur stocke les informations LLDP dans sa base de données avant de les supprimer ou de les supprimer. La durée est calculée comme la valeur du paramètre **Holdtime Multiplier** multipliée par la valeur du paramètre Timer.

- **Réception de messages LLDP.** NetScaler stocke les informations LLDPDU dans sa base d'informations de gestion (MIB). Les informations LLDP stockées sont classées ou regroupées sous l'ID de l'interface qui a reçu le LLDPDU. NetScaler conserve ces informations LLDP pendant la durée spécifiée dans le LLDPU reçu.

Si l'ADC reçoit un autre LLDPDU sur une interface avant que les informations LLDP stockées pour cette interface ne soient supprimées, l'ADC remplace les informations LLDP stockées pour cette interface par des informations contenues dans le nouveau LLDPDU.

Étapes de configuration

La configuration de LLDP sur une appliance NetScaler comprend les tâches suivantes :

1. **Définissez les paramètres LLDP au niveau global.** Dans cette tâche, vous définissez les paramètres LLDP globaux tels que le temporisateur LLDP, le multiplicateur de temps d'attente et le mode LLDP.
2. **Définissez les paramètres LLDP au niveau de l'interface.** Dans cette tâche, vous allez définir le mode LLDP pour une interface.
3. **(Facultatif) Afficher les informations relatives à l'appareil voisin.** Vous pouvez afficher les informations LLDP du périphérique voisin collectées sur toutes les interfaces de NetScaler, ou simplement les informations LLDP collectées sur des interfaces spécifiques. Si vous ne spécifiez pas d'interface, les informations s'affichent pour toutes les interfaces.

Les conditions préalables à la configuration de LLDP sur un NetScaler sont les suivantes :

1. Assurez-vous de bien comprendre le protocole LLDP standard (IEEE 802.1AB).
2. Vérifiez que vous avez configuré LLDP sur les appareils directement connectés souhaités.

Procédures CLI

Pour définir les paramètres LLDP au niveau global à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <positive_integer><Mode>définir le paramètre lldp [- [-HoldTimeTxMult [-Mode \][-timer <positive_integer>]]
- show lldp param

Pour configurer une interface pour LLDP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- définir l'interface <id>-lldpmode <lldpmode>
- show interface <id>

Pour afficher les informations sur les appareils voisins à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- Afficher les voisins LLDP
- Afficher les voisins LLDP <ifnum>

Procédures GUI

Pour définir les paramètres LLDP au niveau global à l'aide de l'interface graphique :

1. Accédez à Système > Réseau, puis cliquez sur Configurer les paramètres LLDP.
2. Définissez les paramètres suivants :
   - Multiplicateur de temporisation
   - Minuteur
   - Mode

Pour configurer une interface pour LLDP à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces, ouvrez l'interface et définissez le paramètre du mode LLDP.

Pour afficher les informations sur les appareils voisins à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces et, dans la liste des actions, sélectionnez Afficher les voisins LLDP.

Support LLDP dans une configuration de cluster

Dans une configuration de cluster, l'interface graphique et l'interface de ligne de commande affichent la configuration voisine LLDP de tous les nœuds du cluster ou de certains d'entre eux lorsque l'on accède à l'interface graphique ou à la CLI via l'adresse IP du cluster (CLIP). Toute modification apportée au mode LLDP au niveau global est appliquée au mode LLDP au niveau global sur chacun des nœuds du cluster.

Prenons l'exemple d'une configuration de cluster à trois nœuds, NS1, NS2 et NS3. Chacun de ces nœuds est connecté aux deux routeurs Router-1 et Router-2. Le résultat suivant s'affiche lorsque l'opération **show lldp neighbor -summary** est exécutée sur l'interface de ligne de commande du cluster accessible via l'adresse IP du cluster (CLIP) de la configuration du cluster. La sortie affiche les informations de voisinage LLDP de tous ces nœuds.

```
1  > show lldp neighbor -summary
2
3  Node Id: 1
4  ------------------------------------------------------------
5      Interface    ChassisId           PortId     System name
6  ------------------------------------------------------------
7  1     1/1/1      fe:c7:3b:13:bd:11    1/1         Router-1
8
9  2     1/1/2      12:68:7b:9e:4c:11    1/1         Router-2
10
11 Node Id: 2
12 ------------------------------------------------------------
```



```
    Interface    ChassisId           PortId     System name
-------------------------------------------------------------
1     2/1/1      fe:c7:3b:13:bd:12    1/2        Router-1

2     2/1/2      12:68:7b:9e:4c:12    1/2        Router-2

Node Id: 3
-------------------------------------------------------------
    Interface    ChassisId            PortId     System name
-------------------------------------------------------------

1     3/1/1       fe:c7:3b:13:bd:13    1/3        Router-1

2     3/1/2       12:68:7b:9e:4c:13    1/3        Router-2

Done
<!--NeedCopy-->
```

Trames Jumbo

May 5, 2023

Les appliances NetScaler prennent en charge la réception et la transmission de trames jumbo contenant jusqu'à 9 216 octets de données IP. Les trames Jumbo peuvent transférer des fichiers volumineux plus efficacement qu'il n'est possible avec la taille MTU IP standard de 1 500 octets.

Une appliance NetScaler peut utiliser des trames jumbo dans les scénarios de déploiement suivants :

- De Jumbo à Jumbo. L'appliance reçoit les données sous forme de trames Jumbo et les envoie sous forme de trames Jumbo.
- Non-Jumbo vers Jumbo. L'appliance reçoit les données sous forme de trames normales et les envoie sous forme de trames jumbo.
- Jumbo à Non-Jumbo. L'appliance reçoit les données sous forme de trames jumbo et les envoie en tant que trames régulières.

L'appliance NetScaler prend en charge les trames jumbo dans une configuration d'équilibrage de charge pour les protocoles suivants :

- TCP
- N'importe quel protocole via TCP (par exemple, HTTP)
- SIP
- RADIUS

Configuration de la prise en charge des Jumbo Frames sur une appliance NetScaler

May 5, 2023

Pour permettre à l'appliance NetScaler de prendre en charge les trames Jumbo, vous devez définir le MTU sur plus de 1 500 sur les interfaces ou les canaux LA, ainsi que sur les VLAN sur lesquels vous souhaitez que l'appliance NetScaler prenne en charge les Jumbo Frames.

Points à prendre en compte avant de définir le MTU des interfaces, des canaux LA ou des VLAN sur une appliance NetScaler

1. Lorsque vous créez un canal LA, le canal prend le MTU de la première interface liée si aucun MTU n'est spécifié pour le canal.
2. Le MTU d'un canal est propagé à toutes les interfaces liées.
3. Lorsqu'une interface est liée au canal dont le MTU est différent du MTU de l'interface, l'interface est ajoutée à la liste des inactifs.
4. Lorsque vous modifiez le MTU d'une interface membre, l'interface est ajoutée à la liste des utilisateurs inactifs.
5. Lorsqu'une interface est indépendante du canal, l'interface conserve la valeur MTU du canal.
6. Vous pouvez définir le MTU d'une interface, d'un canal ou d'un VLAN sur une valeur comprise entre 1500 et 9216.
7. Vous ne pouvez pas définir le MTU sur le VLAN par défaut. L'appliance NetScaler utilise le MTU de l'interface via laquelle elle reçoit ou envoie des données depuis ou vers le VLAN par défaut.
8. Pour le trafic basé sur TCP sur une configuration d'équilibrage de charge sur une appliance NetScaler, les MSS sont définis en conséquence à chaque point de terminaison pour la prise en charge des trames jumbo :
    - Pour une connexion entre un client et un serveur virtuel d'équilibrage de charge sur l'appliance NetScaler, le MSS de l'appliance NetScaler est défini dans un profil TCP, qui est ensuite lié au serveur virtuel d'équilibrage de charge.
    - Pour une connexion entre l'appliance NetScaler et un serveur, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié au service représentant le serveur sur l'appliance NetScaler.
    - Par défaut, un profil TCP nstcp_default_profile est lié à tous les serveurs et services d'équilibrage de charge basés sur TCP sur l'appliance NetScaler.
    - Pour prendre en charge les trames jumbo, vous pouvez soit modifier la valeur MSS du profil TCP nstcp_default_profile, soit créer un profil TCP personnalisé et définir son MSS en con-

séquence, puis lier le profil TCP personnalisé aux serveurs et services virtuels d'équilibrage de charge souhaités.

- La valeur MSS par défaut de tout profil TCP est 1460.

Procédures CLI

Pour définir le MTU d'une interface à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- définir l'interface <id>-mtu <positive_integer>
- show interface <id>

Exemple :

```
1 > set interface 10/1 -mtu 9000
2 Done
3 <!--NeedCopy-->
```

Pour définir le MTU d'un canal à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- définir le canal <id>-mtu <positive_integer>
- chaîne d'émission <id>

Exemple :

```
1 > set channel LA/1 -mtu 9000
2 Done
3 <!--NeedCopy-->
```

Pour définir le MTU d'un VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <id>ajouter vlan -mtu <positive_integer>
- show vlan <id>

Exemple :

```
1 > set vlan 20 -mtu 9000
2 Done
3 <!--NeedCopy-->
```


Procédures GUI

Pour définir le MTU d'une interface à l'aide de l'interface graphique :

Accédez à Système > Réseau > Interfaces, ouvrez l'interface et définissez le paramètre Unité de transmission maximale.

Pour définir le MTU d'un canal à l'aide de l'interface graphique :

Accédez à Système > Réseau > Canaux, ouvrez le canal et définissez le paramètre Unité de transmission maximale.

Pour définir le MTU d'un VLAN à l'aide de l'interface graphique :

Accédez à Système > Réseau > VLAN, ouvrez le VLAN et définissez le paramètre Unité de transmission maximale.

Cas d'utilisation 1 — Configuration Jumbo vers Jumbo

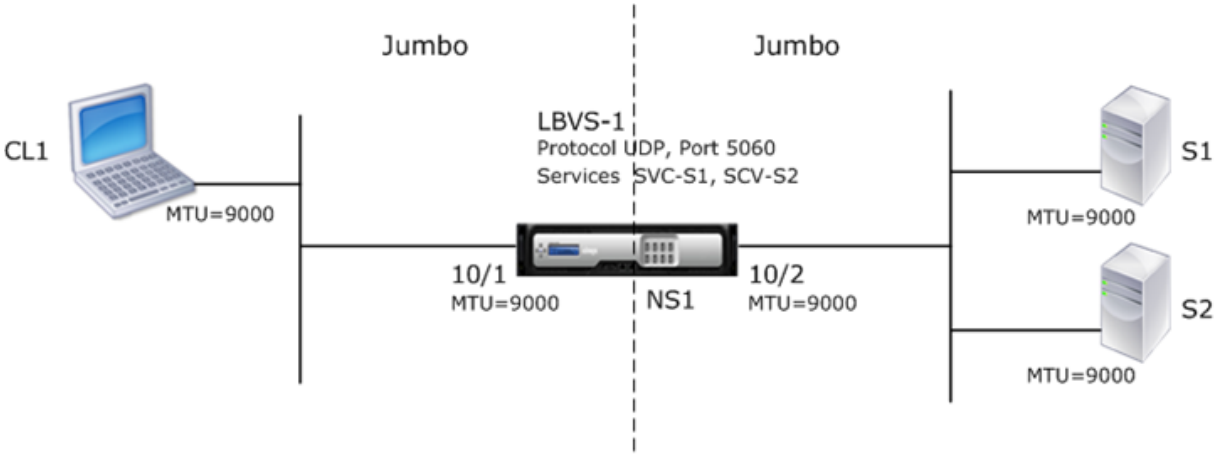
May 5, 2023

Prenons l'exemple d'une configuration jumbo to jumbo dans laquelle le serveur virtuel d'équilibrage de charge SIP LBVS-1, configuré sur l'appliance NetScaler NS1, est utilisé pour équilibrer la charge du trafic SIP sur les serveurs S1 et S2. La connexion entre le client CL1 et NS1 et la connexion entre NS1 et les serveurs prennent en charge les trames étendues.

L'interface 10/1 de NS1 reçoit ou envoie du trafic depuis ou vers le client CL1. L'interface 10/2 de NS1 reçoit ou envoie du trafic depuis ou vers le serveur S1 ou S2. Les interfaces 10/1 et 10/2 de NS1 font partie du VLAN 10 et du VLAN 20, respectivement.

Pour prendre en charge les trames jumbo, le MTU est défini sur 9216, sur NS1, pour les interfaces 10/1, 10/2 et les VLAN VLAN 10, VLAN 20.

Tous les autres périphériques réseau, y compris CL1, S1, S2, dans cet exemple de configuration, sont également configurés pour prendre en charge les trames Jumbo.



Le tableau suivant répertorie les paramètres utilisés dans l'exemple.

Entité	Nom	Détails
Adresse IP du client CL1	-	192.0.2.10
Adresse IP des serveurs	S1	198.51.100.19
	S2	198.51.100.20
Adresse SNIP sur NS1		198.51.100.18
MTU spécifiée pour les interfaces et les VLAN sur NS1	10/1	9000
	10/2	9000
	VLAN 10	9000
	VLAN 20	9000
Services sur NS1 représentant des serveurs	SVC-S1	**Adresse IP :198.51.100.19, **Protocole : SIP, Port : 5060****
	SVC-S2	**Adresse IP :198.51.100.20, **Protocole : SIP, Port : 5060****
Serveur virtuel d'équilibrage de charge sur le VLAN 10	LBVS-1	**Adresse IP :203.0.113.15, **Protocole : SIP, Port :5060, Services liés : SVC-S1**, SVC-S2**

Voici le flux de trafic de la demande de CL1 à NS1 :

1. CL1 crée une demande SIP de 20 000 octets à envoyer à LBVS-1 de NS1.
2. CL1 envoie les données de demande sous forme de fragments IP à LBVS-1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) définie sur l'interface à partir de laquelle CL1 envoie ces fragments à NS1.
    - Taille du premier fragment IP = [en-tête IP+en-tête UDP+segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième fragment IP = [en-tête IP+segment de données SIP] = [20+ 8980] = 9000
    - Taille du dernier fragment IP = [en-tête IP+segment de données SIP] = [20+ 2048] = 2068
3. NS1 reçoit les fragments IP de la requête à l'interface 10/1. NS1 accepte ces fragments, car la taille de chacun de ces fragments est inférieure ou égale à la MTU (9000) de l'interface 10/1.
4. NS1 réassemble ces fragments IP pour former la requête SIP de 20 000 octets. NS1 traite cette demande.
5. L'algorithme d'équilibrage de charge de LBVS-1 sélectionne le serveur S1.
6. NS1 envoie les données de demande sous forme de fragments IP à S1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) de l'interface 10/2, à partir de laquelle NS1 envoie ces fragments à S1. Les paquets IP proviennent d'une adresse SNIP NS1.
    - Taille du premier fragment IP = [en-tête IP+en-tête UDP+segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième fragment IP = [en-tête IP+segment de données SIP] = [20+ 8980] = 9000
    - Taille du dernier fragment IP = [en-tête IP+segment de données SIP] = [20+ 2048] = 2068

Voici le flux de trafic de la réponse de S1 à CL1 dans cet exemple :

1. Le serveur S1 crée une réponse SIP de 30 000 octets à envoyer à l'adresse SNIP de NS1.
2. S1 envoie les données de réponse sous forme de fragments IP à l'adresse SNIP de NS1. La taille de chaque fragment IP est égale ou inférieure au MTU (9000) défini sur l'interface à partir de laquelle S1 envoie ces fragments à NS1.
    - Taille du premier fragment IP = [en-tête IP+en-tête UDP+segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième et du troisième fragment IP = [en-tête IP+segment de données SIP] = [20 + 8980] = 9000
    - Taille du dernier fragment IP = [en-tête IP+segment de données SIP] = [20 + 3068] = 3088
3. NS1 reçoit les fragments IP de réponse à l'interface 10/2. NS1 accepte ces fragments, car la taille de chaque fragment est inférieure ou égale à la MTU (9000) de l'interface 10/2.
4. NS1 réassemble ces fragments IP pour former la réponse SIP de 30 000 octets. NS1 traite cette réponse.

5. NS1 envoie les données de réponse sous forme de fragments IP à CL1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) de l'interface 10/1, à partir de laquelle NS1 envoie ces fragments à CL1. Les fragments IP proviennent de l'adresse IP de LBVS-1.
    - Taille du premier fragment IP = [en-tête IP+en-tête UDP+segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième et du troisième fragment IP = [en-tête IP+segment de données SIP] = [20 + 8980] = 9000
    - Taille du dernier fragment IP = [en-tête IP+segment de données SIP] = [20 + 3068] = 3088

Tâches de configuration

Le tableau suivant répertorie les tâches, les commandes NetScaler et des exemples permettant de créer la configuration requise sur l'appliance NetScaler.

Tâche	Syntaxe de commande NetScaler	Exemple
Définissez le MTU des interfaces souhaitées pour la prise en charge des trames jumbo	définir l'interface <id>-mtu<positive_integer>, afficher l'interface <id>	set int 10/1 -mtu 9000 set int 10/2 -mtu 9000
Créez des VLAN et définissez la MTU des VLAN souhaités pour la prise en charge des trames jumbo	<positive_integer>ajouter vlan <id>-mtu, afficher le vlan <id>	ajouter le vlan 10 -mtu 9000 ajouter le vlan 20 -mtu 9000
Lier des interfaces à des VLAN	<interface_name>lier le vlan <id>-ifnum, afficher le vlan <id>	lier vlan 10 -ifnum 10/1 lier vlan 20 -ifnum 10/2
Ajouter une adresse SNIP	ajouter ns ip <IPAddress><netmask>-type SNIP, afficher ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Création de services représentant des serveurs SIP	<port>ajouter le service <serviceName><ip>SIP_UDP, afficher le service <name>	ajouter le service SVC-S1 198.51.100.19 SIP_UDP 5060 ajouter le service SVC-S2 198.51.100.20 SIP_UDP 5060
Créer des serveurs virtuels d'équilibrage de charge SIP et y lier les services	<vserverName><serviceName>ajouter lb vserver <name>SIP_UDP <ip><port>bind lb vserver, afficher lb vserver <name>	ajouter lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060 lien lb vserver LBVS-1 SVC-S1 lien lb vserver LBVS-1 SVC-S2

Tâche	Syntaxe de commande NetScaler	Exemple
Enregistrez la configuration	enregistrer la configuration ns, afficher la configuration ns	

Cas d'utilisation 2 — Configuration non-Jumbo vers Jumbo

May 5, 2023

Prenons l'exemple d'une configuration standard à Jumbo dans laquelle le serveur virtuel d'équilibrage de charge LBVS-1, configuré sur une appliance NetScaler NS1, est utilisé pour équilibrer la charge du trafic entre les serveurs S1 et S2. La connexion entre le client CL1 et NS1 prend en charge les trames normales, tandis que la connexion entre NS1 et les serveurs prend en charge les trames jumbo.

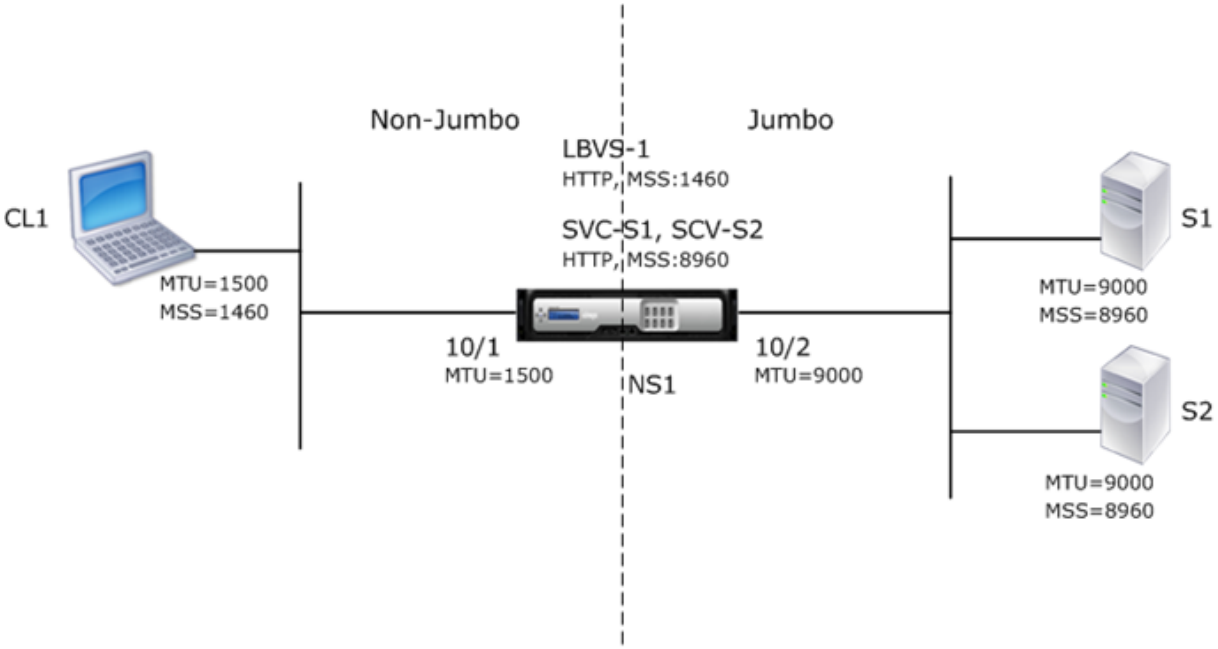
L'interface 10/1 de NS1 reçoit ou envoie du trafic depuis ou vers le client CL1. L'interface 10/2 de NS1 reçoit ou envoie du trafic depuis ou vers le serveur S1 ou S2.

Les interfaces 10/1 et 10/2 de NS1 font partie du VLAN 10 et du VLAN 20, respectivement. Pour ne prendre en charge que les trames normales entre CL1 et NS1, le MTU est défini sur la valeur par défaut de 1500 pour l'interface 10/1 et le VLAN 10

Pour la prise en charge des trames Jumbo entre NS1 et les serveurs, le MTU est défini sur 9000 pour l'interface 10/2 et le VLAN 20. Les serveurs et tous les autres périphériques réseau entre NS1 et les serveurs sont également configurés pour prendre en charge les trames Jumbo.

Le trafic HTTP étant basé sur TCP, les MSS sont définis en conséquence à chaque point d'extrémité pour la prise en charge des trames Jumbo.

- Pour prendre en charge les trames jumbo pour la connexion entre une adresse SNIP de NS1 et S1 ou S2, le MSS sur NS1 est défini en conséquence dans un profil TCP personnalisé, qui est lié aux services (SVC-S1 et SVC-S1) représentant S1 et S2 sur NS1.
- Pour ne prendre en charge que les trames normales pour la connexion entre CL1 et le serveur virtuel LBVS-1 de NS1, le profil TCP par défaut nstcp_default_profile est utilisé. Il est lié par défaut à LBVS-1 et dont le MSS est défini sur la valeur par défaut de 1460.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Entité	Nom	Détails
Adresse IP du client CL1		192.0.2.10
Adresse IP des serveurs	S1	198.51.100.19
	S2	198.51.100.20
Adresse SNIP sur NS1		198.51.100.18
MTU spécifiée pour les interfaces et les VLAN sur NS1	10/1	1500
	10/2	9000
	VLAN 10	1500
	VLAN 20	9000
Default TCP profile	nstcp_default_profile	MASSE : 1460
Profil TCP personnalisé	NS1-SERVERS-JUMBO	MASSE : 8960
Services sur NS1 représentant des serveurs	SVC-S1	Adresse IP : 198.51.100.19, Protocole : HTTP, Port : 80, profil TCP : NS1-SERVERS-JUMBO (MSS : 8960)

Entité	Nom	Détails
	SVC-S2	Adresse IP : 198.51.100.20, Protocole : HTTP, Port : 80, profil TCP : NS1-SERVERS-JUMBO (MSS : 8960)
Serveur virtuel d'équilibrage de charge sur le VLAN 10	LBVS-1	Adresse IP = 203.0.113.15, protocole : HTTP, port : 80, services liés : SVC-S1, SVC-S2, profil TCP : nstcp_default_profile (MSS:1460)

Voici le flux de trafic de la demande de CL1 à S1 dans cet exemple :

1. Le client CL1 crée une demande HTTP de 200 octets à envoyer au serveur virtuel LBVS-1 de NS1.
2. CL1 ouvre une connexion à LBVS-1 de NS1. CL1 et NS1 échangent leurs valeurs MSS TCP respectives lors de l'établissement de la connexion.
3. Étant donné que le MSS de NS1 est plus grand que la requête HTTP, CL1 envoie les données de la demande dans un seul paquet IP à NS1.

   Taille du paquet de requête = [En-tête IP+ En-tête TCP + Requête TCP] = [20 + 20 + 200] = 240
4. NS1 reçoit le paquet de requête à l'interface 10/1, puis traite les données de requête HTTP dans le paquet.
5. L'algorithme d'équilibrage de charge de LBVS-1 sélectionne le serveur S1 et NS1 ouvre une connexion entre l'une de ses adresses SNIP et S1. NS1 et CL1 échangent leurs valeurs MSS TCP respectives lors de l'établissement de la connexion.
6. Étant donné que le MSS de S1 est plus grand que la requête HTTP, NS1 envoie les données de la demande dans un seul paquet IP à S1.

   Taille du paquet de demande = [En-tête IP+en-tête TCP + [Demande TCP] = [20 + 20 + 200] = 240

Voici le flux de trafic de la réponse de S1 à CL1 dans cet exemple :

1. Le serveur S1 crée une réponse HTTP de 18 000 octets à envoyer à l'adresse SNIP de NS1.
2. S1 segmente les données de réponse en multiples du MSS de NS1 et envoie ces segments dans des paquets IP à NS1. Ces paquets IP proviennent de l'adresse IP de S1 et sont destinés à l'adresse SNIP de NS1.

- Taille des deux premiers paquets = [En-tête IP+en-tête TCP + (segment TCP = taille MSS de NS1)] = [20 + 20+ 8960] = 9000
- Taille du dernier paquet = [En-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20 + 2080] = 2120

3. NS1 reçoit les paquets de réponse à l'interface 10/2.
4. À partir de ces paquets IP, NS1 assemble tous les segments TCP pour former les données de réponse HTTP de 18 000 octets. NS1 traite cette réponse.
5. NS1 segmente les données de réponse en multiples du MSS de CL1 et envoie ces segments en paquets IP, de l'interface 10/1 à CL1. Ces paquets IP proviennent de l'adresse IP de LBVS-1 et sont destinés à l'adresse IP de CL1.
    - Taille de tous les paquets sauf le dernier = [En-tête IP + En-tête TCP + (charge utile TCP = taille MSS du CL1)] = [20 + 20 + 1460] = 1500
    - Taille du dernier paquet = [En-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20+480] = 520

Tâches de configuration

Le tableau suivant répertorie les tâches, les commandes NetScaler et des exemples permettant de créer la configuration requise sur l'appliance NetScaler.

Tâches	Syntaxe CLI	Exemples
Définissez le MTU des interfaces souhaitées pour la prise en charge des trames jumbo	définir l'interface <id>-mtu<positive_integer>, afficher l'interface <id>	set int 10/1 -mtu 1500 set int 10/2 -mtu 9000
Créez des VLAN et définissez la MTU des VLAN souhaités pour la prise en charge des trames jumbo	<positive_integer>ajouter vlan <id>-mtu, afficher le vlan <id>	ajouter le vlan 10 -mtu 1500 ajouter le vlan 20 -mtu 9000
Lier des interfaces à des VLAN	<interface_name>lier le vlan <id>-ifnum, afficher le vlan <id>	lier vlan 10 -ifnum 10/1 lier vlan 20 -ifnum 10/2
Ajouter une adresse SNIP	ajouter ns ip <IPAddress><netmask>-type SNIP, afficher ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP

Tâches	Syntaxe CLI	Exemples
Créer des services représentant des serveurs HTTP	ajouter un service <serviceName><ip>HTTP<port> afficher le service <name>	ajouter le service SVC-S1 198.51.100.19 http 80, ajouter le service SVC-S2 198.51.100.20 http 80
Créer des serveurs virtuels d'équilibrage de charge HTTP et y lier les services	ajouter lb vserver <name>HTTP <ip><port>, lier lb vserver <vserverName><serviceName>, afficher lb vserver <name>	ajouter lb vserver LBVS-1 http 203.0.113.15 80, lier lb vserver LBVS-1 SVC-S1, lier lb vserver LBVS-1 SVC-S2
Créez un profil TCP personnalisé et définissez son MSS pour la prise en charge des trames jumbo	<positive_integer>ajouter le profil TCP <name>-mss, afficher le profil TCP <name>	add tcpprofile NS1-SERVERS-JUMBO -mss 8960
Liez le profil TCP personnalisé aux services souhaités	<string>définir le service <Name>-TCPProfileName, afficher le service <name>	définir le service SVC-S1 -TCPProfileName NS1-SERVERS-JUMBO, définir le service SVC-S2 -TCPProfileName NS1-SERVERS-JUMBO
Enregistrez la configuration	enregistrer la configuration ns, afficher la configuration ns	

Cas d'utilisation 3 — Coexistence de flux Jumbo et non-Jumbo sur le même ensemble d'interfaces

May 5, 2023

Prenons un exemple dans lequel les serveurs virtuels d'équilibrage de charge LBVS-1 et LBVS-2 sont configurés sur l'appliance NetScaler NS1. LBVS-1 est utilisé pour équilibrer la charge du trafic HTTP entre les serveurs S1 et S2, et LBVS-2 est utilisé pour équilibrer la charge du trafic entre les serveurs S3 et S4.

CL1 se trouve sur le VLAN 10, S1 et S2 sont sur VLAN20, CL2 est sur le VLAN 30, et S3 et S4 sont sur le VLAN 40. Les VLAN 10 et VLAN 20 prennent en charge les trames jumbo, tandis que les VLAN 30 et VLAN 40 ne prennent en charge que les trames normales.

En d'autres termes, la connexion entre CL1 et NS1 et la connexion entre NS1 et le serveur S1 ou S2 prennent en charge les trames Jumbo. La connexion entre CL2 et NS1 et la connexion entre NS1 et le serveur S3 ou S4 ne prennent en charge que les trames normales.

L'interface 10/1 de NS1 reçoit ou envoie du trafic depuis ou vers des clients. L'interface 10/2 de NS1 reçoit ou envoie du trafic depuis ou vers les serveurs.

L'interface 10/1 est liée à la fois au VLAN 10 et au VLAN 30 en tant qu'interface balisée, et l'interface 10/2 est liée à la fois au VLAN 20 et au VLAN 40 en tant qu'interface balisée.

Pour la prise en charge des trames Jumbo, le MTU est réglé sur 9216 pour les interfaces 10/1 et 10/2.

Sur NS1, le MTU est défini sur 9000 pour le VLAN 10 et le VLAN 20 pour la prise en charge des trames jumbo, et le MTU est défini sur la valeur par défaut de 1500 pour le VLAN 30 et le VLAN 40 pour la prise en charge uniquement des trames normales.

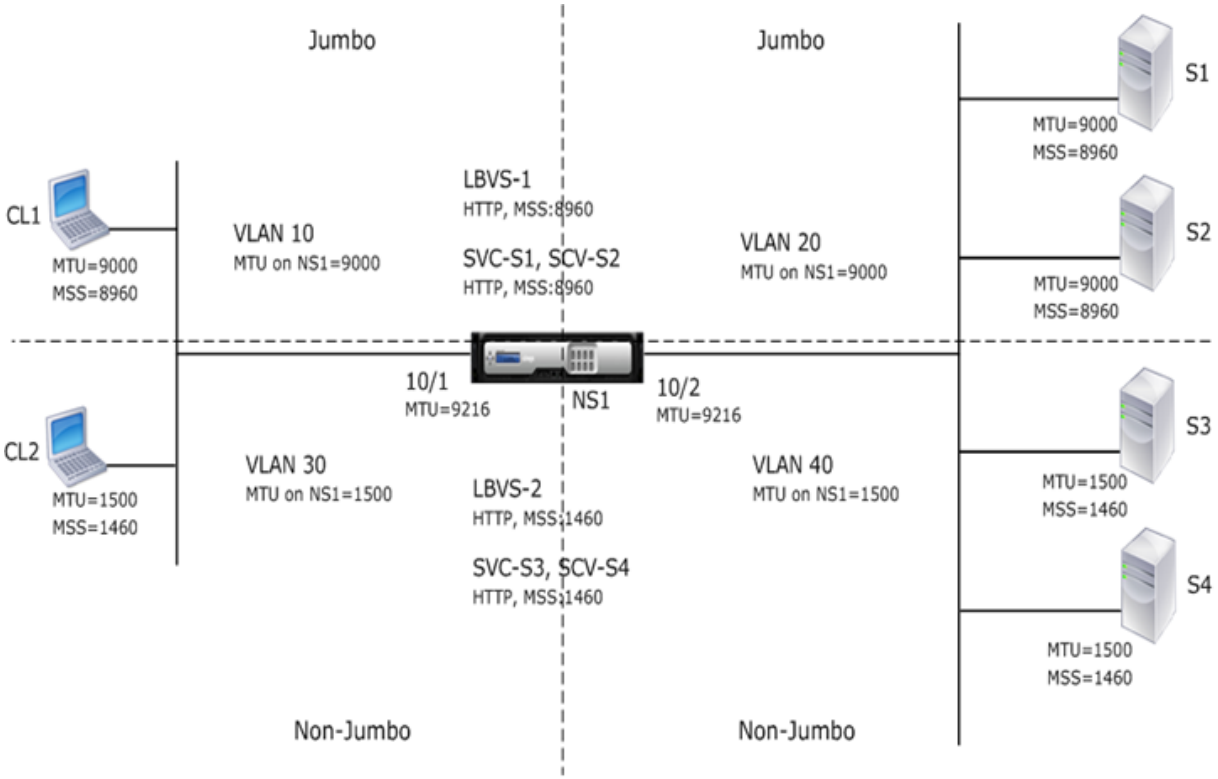
Le MTU effectif sur une interface NetScaler pour les paquets balisés VLAN est le MTU de l'interface ou le MTU du VLAN, la valeur la plus faible étant retenue. Par exemple :

- Le MTU de l'interface 10/1 est 9216. Le MTU du VLAN 10 est 9000. Sur l'interface 10/1, le MTU des paquets balisés VLAN 10 est 9000.
- Le MTU de l'interface 10/2 est 9216. Le MTU du VLAN 20 est 9000. Sur l'interface 10/2, le MTU des paquets balisés VLAN 20 est 9000.
- Le MTU de l'interface 10/1 est 9216. Le MTU du VLAN 30 est de 1500. Sur l'interface 10/1, le MTU des paquets balisés VLAN 30 est de 1500.
- Le MTU de l'interface 10/2 est 9216. Le MTU du VLAN 40 est de 1500. Sur l'interface 10/2, le MTU des paquets balisés VLAN 40 est de 9000.

CL1, S1, S2 et tous les périphériques réseau entre CL1 et S1 ou S2 sont configurés pour des trames Jumbo.

Le trafic HTTP étant basé sur TCP, les MSS sont définis en conséquence à chaque point d'extrémité pour la prise en charge des trames Jumbo.

- Pour la connexion entre CL1 et le serveur virtuel LBVS-1 de NS1, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié à LBVS-1.
- Pour la connexion entre une adresse SNIP NS1 et S1, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié au service (SVC-S1) représentant S1 sur NS1.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple : les cadres Jumbo utilisent des exemples de paramètres de cas 3.

Voici le flux de trafic de la demande de CL1 à S1 :

1. Le client CL1 crée une demande HTTP de 20 000 octets à envoyer au serveur virtuel LBVS-1 de NS1.
2. CL1 ouvre une connexion à LBVS-1 de NS1. CL1 et NS1 échangent leurs valeurs MSS TCP lors de l'établissement de la connexion.
3. Étant donné que la valeur MSS de NS1 est inférieure à la requête HTTP, CL1 segmente les données de la demande en multiples de MSS de NS1 et envoie ces segments dans des paquets IP marqués VLAN 10 à NS1.
    - Taille des deux premiers paquets = [En-tête IP+en-tête TCP + (segment TCP = NS1 MSS)] = [20 + 20+ 8960] = 9000
    - Taille du dernier paquet = [En-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20 + 2080] = 2120
4. NS1 reçoit ces paquets à l'interface 10/1. NS1 accepte ces paquets car la taille de ces paquets est égale ou inférieure au MTU effectif (9000) de l'interface 10/1 pour les paquets balisés VLAN 10.
5. À partir des paquets IP, NS1 assemble tous les segments TCP pour former la demande HTTP de 20 000 octets. NS1 traite cette demande.
6. L'algorithme d'équilibrage de charge de LBVS-1 sélectionne le serveur S1 et NS1 ouvre une con-

nexion entre l'une de ses adresses SNIP et S1. NS1 et CL1 échangent leurs valeurs MSS TCP respectives lors de l'établissement de la connexion.

7. NS1 segmente les données de demande en multiples de MSS de S1 et envoie ces segments dans des paquets IP marqués VLAN 20 vers S1.
    - Taille des deux premiers paquets = [En-tête IP+en-tête TCP + (Charge utile TCP = S1 MSS)] = [20 + 20+ 8960] = 9000
    - Taille du dernier paquet = [En-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20 + 2080] = 2120

Voici le flux de trafic de la réponse de S1 à CL1 :

1. Le serveur S1 crée une réponse HTTP de 30 000 octets à envoyer à l'adresse SNIP de NS1.
2. S1 segmente les données de réponse en multiples du MSS de NS1 et envoie ces segments dans des paquets IP marqués VLAN 20 vers NS1. Ces paquets IP proviennent de l'adresse IP de S1 et sont destinés à l'adresse SNIP de NS1.
    - Taille des trois premiers paquets = [En-tête IP+en-tête TCP + (segment TCP = taille MSS de NS1)] = [20 + 20+ 8960] = 9000
    - Taille du dernier paquet = [En-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20+ 3120] = 3160
3. NS1 reçoit les paquets de réponse à l'interface 10/2. NS1 accepte ces paquets, car leur taille est inférieure ou égale à la valeur MTU effective (9000) de l'interface 10/2 pour les paquets balisés VLAN 20.
4. À partir de ces paquets IP, NS1 assemble tous les segments TCP pour former la réponse HTTP de 30 000 octets. NS1 traite cette réponse.
5. NS1 segmente les données de réponse en multiples du MSS de CL1 et envoie ces segments dans des paquets IP étiquetés VLAN 10, de l'interface 10/1 à CL1. Ces paquets IP proviennent de l'adresse IP de LBVS et sont destinés à l'adresse IP de CL1.
    - Taille des trois premiers paquets = [En-tête IP+en-tête TCP + [(charge utile TCP = taille MSS de CL1)] = [20 + 20+ 8960] = 9000
    - Taille du dernier paquet = [En-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20+ 3120] = 3160

Tâches de configuration

Le tableau suivant répertorie les tâches, les commandes et les exemples permettant de créer la configuration requise sur l'appliance NetScaler : Les cadres Jumbo utilisent les tâches de configuration du cas 3.

Support NetScaler pour le déploiement de Microsoft Direct Access

May 5, 2023

Microsoft Direct Access est une technologie qui permet aux utilisateurs distants de se connecter de manière fluide et sécurisée aux réseaux internes de l'entreprise, sans avoir à établir une connexion VPN distincte. Contrairement aux connexions VPN, qui nécessitent l'intervention de l'utilisateur pour ouvrir et fermer des connexions, un client compatible Direct Access se connecte automatiquement aux réseaux internes de l'entreprise chaque fois que le client se connecte à Internet.

Manage-Out est une fonctionnalité de Microsoft Direct Access qui permet aux administrateurs du réseau d'entreprise de se connecter à des clients Direct Access extérieurs au réseau et de les gérer (par exemple, en effectuant des tâches d'administration, telles que la planification des mises à jour des services et la fourniture d'une assistance à distance).

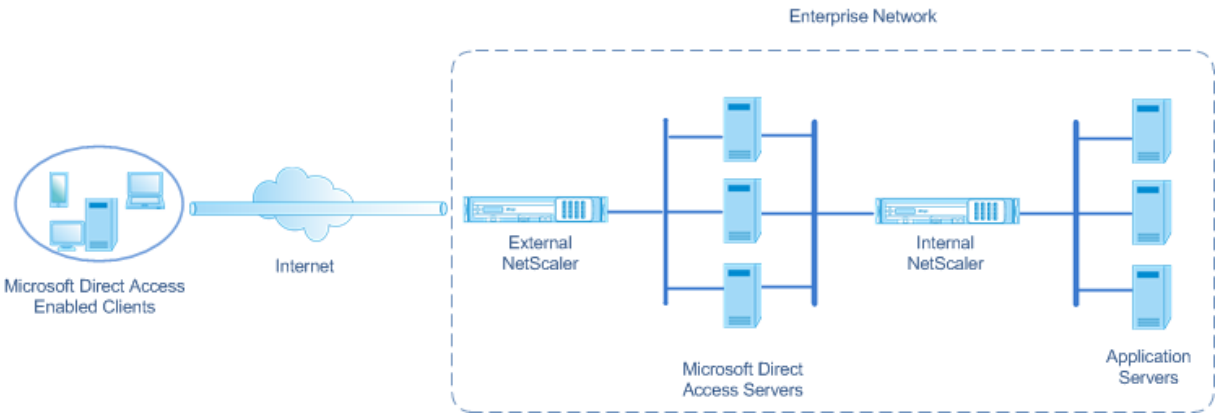
Dans un déploiement à accès direct, les appliances NetScaler offrent une haute disponibilité, une évolutivité, des performances et une sécurité élevées. La fonctionnalité d'équilibrage de charge de NetScaler envoie le trafic client via le serveur le plus approprié. Les appliances peuvent également transférer le trafic Manage-Out via le bon chemin pour atteindre le client.

Architecture

L'architecture d'un déploiement Microsoft Direct Access se compose de clients compatibles Direct Access, de serveurs Direct Access, de serveurs d'applications et d'appliances NetScaler internes et externes. Les clients se connectent à un serveur d'applications via un serveur d'accès direct. Une appliance NetScaler externe équilibre la charge du trafic client vers un serveur Direct Access, tandis qu'une appliance NetScaler interne transmet le trafic client du serveur Direct Access au serveur d'applications de destination. L'accès direct est utilisé pour tunnaliser le trafic IPv6 du client sur le réseau IPv4. Un serveur virtuel d'équilibrage de charge IPv4 sur l'appliance NetScaler externe équilibre la charge du trafic tunnelé du client vers l'un des serveurs Direct Access. Le serveur d'accès direct extrait les paquets IPv6 des paquets IPv4 du client reçu et les envoie au serveur d'applications de destination via l'appliance NetScaler interne. L'appliance NetScaler interne dispose de règles de session de transfert avec l'option de cache de route source activée pour stocker les informations de connexion de couche 2 et de couche 3 concernant le trafic du client depuis le serveur Direct Access. L'appliance NetScaler stocke les informations de couche 2 et de couche 3 suivantes dans une table appelée table de cache d'itinéraires source :

- Adresse IP source du paquet reçu
- Adresse MAC du serveur d'accès direct qui a envoyé le paquet
- ID VLAN de l'appliance NetScaler qui a reçu le paquet
- ID d'interface de l'appliance NetScaler qui a reçu le paquet

L'appliance NetScaler utilise les informations de la table de cache d'itinéraires source pour transmettre une réponse au même serveur Direct Access, car elle possède les informations de tunneling nécessaires pour atteindre le client. En outre, l'appliance interne utilise la table de cache de routage source pour transférer le trafic de gestion du serveur d'applications vers le serveur d'accès direct approprié afin d'atteindre un client particulier.



Configuration de l'appliance NetScaler interne dans un déploiement Microsoft Direct Access

Pour configurer l'appliance NetScaler interne afin de transférer la réponse d'un serveur d'applications et de gérer le trafic vers la Access Gateway direct appropriée, configurez les règles de session de transfert. Dans chaque règle, définissez le paramètre sourceroutecache sur ENABLED.

Pour créer une règle de session de transfert à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter une session de transfert** <string>**(([\]) | **-acl6name | -aclname) -sourceroutecache** (ACTIVÉ | **DÉSACTIVÉ**]** <name><network>0 <string>
- **show forwardingsession** <name>

Exemple de configuration :

Dans l'exemple suivant, la règle de session de transfert MS-DA-FW-1 est créée sur l'appliance NetScaler interne. La session de transfert stocke les informations de couche 2 et de couche 3 pour tous les paquets IPv6 entrants à partir d'un serveur d'accès direct qui correspond au préfixe IPv6 source 2001:DB8 : :/96.

```
1 > add forwardingSession MS-DA-FW-1 2001:DB8::/96 -sourceroutecache -
    ENABLED
2  Done
```


Affichage de la table du cache de routage source

Vous pouvez afficher la table du cache d'itinéraires source pour surveiller ou détecter les connexions indésirables entre les serveurs d'accès direct et les serveurs d'applications.

Pour afficher la table de cache d'itinéraires source à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **afficher la sourceroutecachable**

Exemple :

```
1 > show sourceroutecachetable
2 SOURCEIP            MAC                 VLAN    INTERFACE
3 2001:DB8:5001:10    56:53:24:3d:02:eb    30        1/2
4 2001:DB8:5003:30    60:54:35:3e:04:bd    60        1/3
5 Done
```

Effacement de la table de cache de l'itinéraire source

Vous pouvez effacer toutes les entrées de la table de cache d'itinéraires source sur une appliance NetScaler.

Pour effacer la table de cache d'itinéraires source à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **flush ns sourceroutecachable**

Listes de contrôle d'accès

May 5, 2023

Les listes de contrôle d'accès (ACL) filtrent le trafic IP et protègent votre réseau contre tout accès non autorisé. Une ACL est un ensemble de conditions que NetScaler évalue pour déterminer s'il convient d'autoriser l'accès. Par exemple, le service financier ne souhaite probablement pas autoriser l'accès à ses ressources par d'autres services, tels que les ressources humaines et la documentation, et ces services souhaitent restreindre l'accès à leurs données.

Lorsque NetScaler reçoit un paquet de données, il compare les informations qu'il contient avec les conditions spécifiées dans l'ACL et autorise ou refuse l'accès. L'administrateur de l'organisation peut configurer les ACL pour qu'elles fonctionnent dans les modes de traitement suivants :

- Autoriser : traite le paquet.

- Pont : reliez le paquet à la destination sans le traiter. Le paquet est directement envoyé par transfert de couche 2 et de couche 3.
- Refuser : déposez le paquet.

Les règles ACL constituent le premier niveau de défense de NetScaler.

NetScaler prend en charge les types d'ACL suivants :

- **Les listes ACL simples** filtrent les paquets en fonction de leur adresse IP source et, éventuellement, de leur protocole, de leur port de destination ou de leur domaine de trafic. Tout paquet ayant les caractéristiques spécifiées dans la liste ACL est supprimé.
- **Les listes ACL étendues filtrent les** paquets de données en fonction de divers paramètres, tels que l'adresse IP source, le port source, l'action et le protocole. Une ACL étendue définit les conditions qu'un paquet doit remplir pour que NetScaler puisse le traiter, le relier ou le supprimer.

Nomenclature

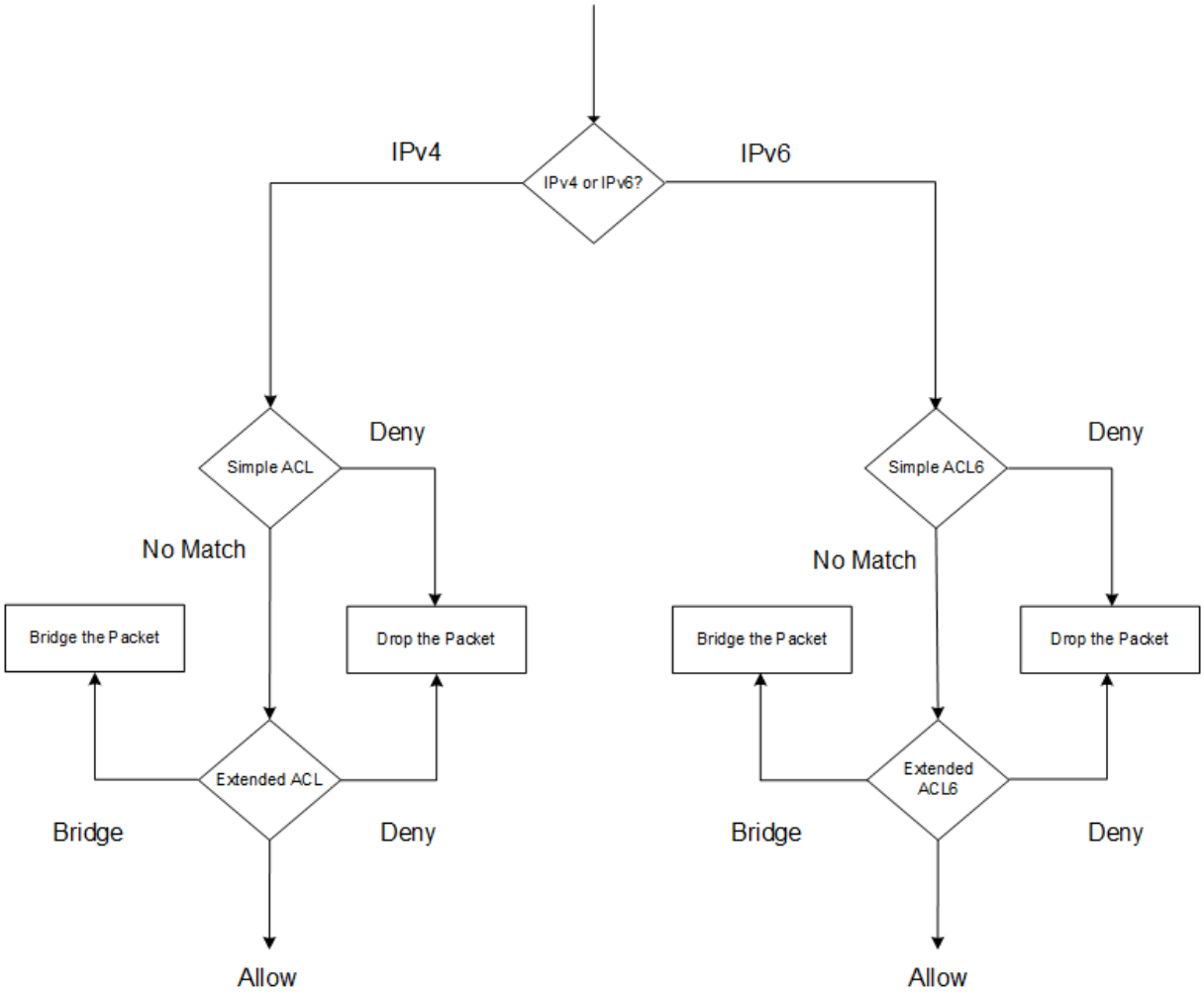
Dans les interfaces utilisateur de NetScaler, les termes ACL simple et ACL étendu font référence aux ACL qui traitent les paquets IPv4. Une ACL qui traite des paquets IPv6 est appelée ACL6 simple et/ou ACL6 étendue. Lorsque vous discutez des deux types, cette documentation les désigne parfois comme des ACL simples ou des ACL étendues.

Priorité ACL

Si des ACL simples et étendues sont configurées, les paquets entrants sont d'abord comparés aux ACL simples.

NetScaler détermine d'abord si le paquet entrant est un paquet IPv4 ou IPv6, puis compare les caractéristiques du paquet aux ACL simples ou aux ACL6 simples. Si une correspondance est trouvée, le paquet est supprimé. Si aucune correspondance n'est trouvée, le paquet est comparé aux ACL étendues ou aux ACL6 étendues. Si cette comparaison aboutit à une correspondance, le paquet est traité comme spécifié dans l'ACL. Le paquet peut être ponté, supprimé ou autorisé. Si aucune correspondance n'est trouvée, le paquet est autorisé.

Figure 1. Séquence de flux ACL simple et étendue



ACL simples et ACL6 simples

May 5, 2023

Une ACL simple ou un ACL6 simple utilise peu de paramètres et peut être configuré uniquement pour supprimer les paquets IP. Les paquets peuvent être supprimés en fonction de leur adresse IP source et, éventuellement, de leur protocole, de leur port de destination ou de leur domaine de trafic.

Lors de la création d'une ACL simple ou d'une ACL6 simple, vous pouvez spécifier un temps de vie (TTL), en secondes, après quoi l'ACL expire. Les ACL avec TTL ne sont pas enregistrées lorsque vous enregistrez la configuration. Vous pouvez afficher des ACL simples et des ACL6 simples pour vérifier leur configuration, et vous pouvez afficher leurs statistiques.

Configuration des ACL simples et des ACL6 simples

La configuration d'une ACL simple ou d'une ACL6 simple sur un NetScaler peut inclure les tâches suivantes.

- **Créez des ACL simples ou des ACL6**simples. Créer des ACL simples ou des ACL6 simples pour supprimer (refuser) les paquets en fonction de leur adresse IP source et, éventuellement, de leur protocole, de leur port de destination ou de leur domaine de trafic.
- **Supprimez les ACL simples ou les ACL6**simples. Ces ACL ne peuvent pas être modifiées une fois créées. Si vous devez modifier une liste ACL simple ou un ACL6 simple, vous devez la supprimer et en créer une.

Procédures CLI

Pour créer une ACL simple à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
1 - ns simpleacl <aclname> DENY -srcIP <ip_addr> [-destPort <port> -
    protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 - show ns simpleacl [<aclname>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > add simpleacl rule1 DENY -srcIP 10.102.29.5 -TTL 600
2 Done
3 <!--NeedCopy-->
```

Pour créer un ACL6 simple à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
1 - add ns simpleacl6 <aclname> DENY - srcIPv6 <ipv6_addr|null> [-
    destPort <port> -protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 - show ns simpleacl6 [<aclname>]
3 <!--NeedCopy-->
```

Exemple :

```
1 > add ns simpleacl6 rule1 DENY - srcIPv6 3ffe:192:168:215::82 -
    destPort 80 -Protocol TCP -TTL 9000
2  Done
3 <!--NeedCopy-->
```

Pour supprimer une seule ACL simple à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **rm ns simplecal** <aclname>
- **show ns simpleacl**

Pour supprimer un seul ACL6 simple à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **rm ns simpleacl6**<aclname>
- **show ns simpleacl6**

Pour supprimer toutes les ACL simples à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **clear ns simpleacl**
- **show ns simpleacl**

Pour supprimer tous les ACL6 simples à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **effacer ns simpleacl6**
- **show ns simpleacl6**

Procédures GUI

Pour créer une ACL simple à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL simples**, ajoutez une nouvelle ACL simple.

Pour créer un ACL6 simple à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **Simple ACL6s**, ajoutez un nouvel ACL6 simple.

Pour supprimer une seule ACL simple à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL simples**, supprimez la liste ACL simple.

Pour supprimer un seul ACL6 simple à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL6s simples**, supprimez l'ACL6 simple.

Pour supprimer toutes les ACL simples à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL**.
2. Dans l'onglet **ACLs simples**, dans la liste des **actions**, cliquez sur **Effacer**.

Pour supprimer tous les ACL6 simples à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL**.
2. **Dans l'onglet**Simple ACL6s**, dans la liste des**actions**, cliquez sur Effacer.**

Affichage des statistiques ACL simples et ACL6 simples

Vous pouvez afficher les statistiques ACL simples (ou ACL6 simples), qui incluent le nombre de correspondances, le nombre d'erreurs et le nombre de listes ACL simples configurées.

Le tableau suivant décrit les statistiques que vous pouvez afficher pour les listes ACL simples et les ACL6 simples.

Statistiques	Indique
Match ACL	Paquets correspondant à une ACL
ACL misses	Paquets ne correspondant à aucune ACL
Nombre d'ACL	Nombre d'ACL configurées

Procédures CLI

Pour afficher des statistiques ACL simples à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **démarrer avec simpleacl**

Exemple :

```
1  > stat ns simpleacl
2
3  SimpleACL Statistics
4
5                                                Rate (/s)
                                                    Total
6  SimpleACL hits                                       0
                         0
7  SimpleACL misses                                     0
       51872
8  SimpleACLs count                                    --
                         2
9  Done
10 <!--NeedCopy-->
```

Pour afficher des statistiques ACL6 simples à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **démarrer : simpleacl6**

Procédures GUI

Pour afficher des statistiques ACL simples à l'aide de l'interface graphique :

Accédez à Système**>**Réseau**>**ACL**et, dans l'onglet**ACL simples**, sélectionnez l'ACL et cliquez sur Statistiques.**

Pour afficher des statistiques ACL6 simples à l'aide de l'interface graphique :

Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL6s simples**, sélectionnez l'ACL6 simple et cliquez sur **Statistiques**.

Fin des connexions établies

Pour une ACL simple ou une ACL6 simple, NetScaler bloque toutes les nouvelles connexions qui répondent aux conditions spécifiées dans l'ACL. Les paquets liés aux connexions existantes qui ont été établies avant la création de l'ACL ne sont pas bloqués. Pour mettre fin à des connexions précédemment établies qui correspondent à une ACL existante, vous pouvez exécuter une opération de purge à partir de l'interface de ligne de commande ou de l'interface graphique.

Flush peut être utile dans les cas suivants :

- Vous recevez une liste d'adresses IP sur liste noire et vous souhaitez empêcher complètement ces adresses IP d'accéder à NetScaler. Dans ce cas, vous créez des ACL simples ou des ACL6 simples pour bloquer toute nouvelle connexion à partir de ces adresses IP, puis vider toutes les connexions existantes associées à ces adresses.
- Vous souhaitez mettre fin à de nombreuses connexions à partir d'un réseau particulier sans prendre le temps de les arrêter une par une.

Avant de commencer

- Lorsque vous exécutez flush, NetScaler parcourt toutes ses connexions établies et met fin aux connexions qui répondent aux conditions spécifiées dans l'une des ACL simples configurées sur l'ADC.
- Si vous envisagez de créer plusieurs ACL simples et de vider les connexions existantes qui correspondent à l'une d'entre elles, vous pouvez minimiser l'effet sur les performances en créant d'abord toutes les listes ACL simples, puis en exécutant le vidage une seule fois.

Procédures CLI

Pour mettre fin à toutes les connexions IPv4 établies qui correspondent à l'une de vos ACL simples configurées à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **flush simplecal -setSessions**

Pour mettre fin à toutes les connexions IPv6 établies qui correspondent à l'un de vos ACL6 simples configurés à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **flush simpleACL6 - EST Sessions**

Procédures GUI

Pour mettre fin à toutes les connexions IPv4 établies qui correspondent à l'une des ACL simples que vous avez configurées à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL**.
2. Dans l'onglet **ACLs simples**, dans la liste des **actions**, cliquez sur **Flush**.

Pour mettre fin à toutes les connexions IPv6 établies qui correspondent à l'un de vos ACL6 simples configurés à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL**.
2. **Dans l'onglet**Simple ACL6s**, dans la liste des**actions**, cliquez sur Flush.**

ACL étendues et ACL6 étendues

May 5, 2023

Les ACL étendues et les ACL6 étendues fournissent des paramètres et des actions qui ne sont pas disponibles avec les ACL simples. Vous pouvez filtrer les données en fonction de paramètres tels que l'adresse IP source, le port source, l'action et le protocole. Vous pouvez spécifier des tâches pour autoriser un paquet, refuser un paquet ou pont un paquet.

Les ACL étendues et les ACL6 peuvent être modifiées après leur création, et vous pouvez renuméroter leurs priorités pour spécifier l'ordre dans lequel elles sont évaluées.

Remarque : Si vous configurez des ACL simples et étendues, les ACL simples sont prioritaires sur les ACL étendues.

Les actions suivantes peuvent être effectuées sur les ACL étendues et les ACL6 : Modifier, Appliquer, Désactiver, Activer, Supprimer et Renuméroter (priorité). Vous pouvez afficher les listes de contrôle d'accès étendues et les ACL6 pour vérifier leur configuration, et vous pouvez afficher leurs statistiques.

Vous pouvez configurer NetScaler pour qu'il enregistre les détails des paquets qui correspondent à une ACL étendue.

Application des ACL étendues et des ACL6 étendues : Contrairement aux ACL et ACL6 simples, les ACL et ACL6 étendues créées sur NetScaler ne fonctionnent pas tant qu'elles ne sont pas appliquées. De plus, si vous apportez des modifications à une ACL étendue ou à une ACL6, telles que la désactivation des ACL, la modification d'une priorité ou la suppression des ACL, vous devez réappliquer les listes ACL ou ACL6 étendues. Vous devez les réappliquer après avoir activé la journalisation. La procédure d'application des ACL étendues ou des ACL6 les réapplique toutes. Par exemple, si vous avez appliqué les règles ACL étendues 1 à 10, puis que vous créez et appliquez la règle 11, les 10 premières règles sont appliquées à nouveau.

Si une session est associée à une liste de contrôle d'accès REFUSÉE, cette session est interrompue lorsque vous appliquez les listes de contrôle d'accès.

Les ACL étendues et les ACL6 sont activées par défaut. Lorsqu'ils sont appliqués, NetScaler commence à comparer les paquets entrants avec eux. Toutefois, si vous les désactivez, ils ne sont pas utilisés tant que vous ne les avez pas réactivés, même s'ils sont réappliqués.

Renumérotation des priorités des ACL étendues et des ACL6 étendues : les numéros de priorité déterminent l'ordre dans lequel les ACL étendues ou ACL6 sont comparées à un paquet. Une liste de contrôle d'accès dont le numéro de priorité est inférieur a une priorité plus élevée. Il est évalué avant les ACL avec des numéros de priorité plus élevés (priorités inférieures), et la première ACL correspondant au paquet détermine l'action appliquée au paquet.

Lorsque vous créez une ACL étendue ou une ACL6, NetScaler lui attribue automatiquement un numéro de priorité multiple de 10, sauf indication contraire de votre part. Par exemple, si deux ACL étendues ont des priorités de 20 et 30, respectivement, et que vous souhaitez qu'une troisième ACL ait une valeur comprise entre ces nombres, vous pouvez lui attribuer une valeur de 25. Si vous souhaitez par la suite conserver l'ordre dans lequel les ACL sont évaluées, mais rétablir leur numérotation à des multiples de 10, vous pouvez utiliser la procédure de renumérotation.

Configuration des ACL étendues et des ACL6 étendues

La configuration d'une ACL étendue ou d'une ACL6 sur un NetScaler comprend les tâches suivantes.

- **Créez une ACL étendue ou une ACL6.** Créez une ACL étendue ou une ACL6 pour autoriser, refuser ou relier un paquet. Vous pouvez spécifier une adresse IP ou une plage d'adresses IP à mettre en correspondance avec les adresses IP source ou de destination des paquets. Vous pouvez spécifier un protocole à mettre en correspondance avec le protocole des paquets entrants.
- (Facultatif) **Modifiez une ACL étendue ou une ACL6**. Vous pouvez modifier les ACL étendues ou les ACL6 que vous avez précédemment créées. Ou, si vous souhaitez temporairement en mettre un hors d'usage, vous pouvez le désactiver, puis le réactiver ultérieurement.
- **Appliquez des ACL étendues ou des ACL6**. Après avoir créé, modifié, désactivé ou réactivé, ou supprimé une ACL étendue ou une ACL6, vous devez appliquer les ACL ou ACL6 étendues pour les activer.

- (Facultatif) **Renuméroter les priorités des ACL étendues ou des ACL6**. Si vous avez configuré des listes de contrôle d'accès avec des priorités qui ne sont pas des multiples de 10 et que vous souhaitez rétablir la numérotation en multiples de 10, utilisez la procédure de renumérotation.

Procédures CLI

Pour créer une liste de contrôle d'accès étendue à l'aide de l'interface de lignede commande :

À l'invite de commande, tapez :

- **add ns acl** <aclname> <aclaction> [-**srcIP** [\<operator>] <srcIPVal>] [-**srcPort** [\<operator>] <srcPortVal>] [-**destIP** [\<operator>] <destIPVal>] [-**destPort** [\<operator>] <destPortVal>] [-**TTL** \<positive_integer>] [-**srcMac** \<mac_addr>] [(-**protocol** \<protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** \<positive_integer>] [-**interface** \<interface_name>] [-**icmpType** \<positive_integer> [-**icmpCode** \<positive_integer>]] [-**priority** \<positive_integer>] [-**state** (ENABLED | DISABLED)] [-**logstate** (ENABLED | DISABLED) [-**ratelimit** \<positive_integer>]]
- **show ns acl** [\<aclName>]

Pour créer un ACL6 étendu à l'aide de l'interface de lignede commande :

À l'invite de commande, tapez :

- **add ns acl6** <acl6name> <acl6action> [-**srcIPv6** [\<operator>] <srcIPv6Val>] [-**srcPort** [\<operator>] <srcPortVal>] [-**destIPv6** [\<operator>] <destIPv6Val>] [-**destPort** [\<operator>] <destPortVal>] [-**TTL** \<positive_integer>] [-**srcMac** \<mac_addr>] [(-**protocol** \<protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** \<positive_integer>] [-**interface** \<interface_name>] [-**icmpType** \<positive_integer> [-**icmpCode** \<positive_integer>]] [-**priority** \<positive_integer>] [-**state** (ENABLED | DISABLED)]
- **show ns acl6** [\<aclName>]

Pour modifier une liste de contrôle d'accès étendue à l'aide de l'interface de lignede commande :

Pour modifier une liste de contrôle d'accès étendue, tapez la commande **set ns acl**, le nom de l'ACL étendue et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour modifier un ACL6 étendu à l'aide de l'interface de ligne de commande :

Pour modifier un ACL6 étendu, tapez la commande **set ns acl6**, le nom de l'ACL6 étendu et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour désactiver ou activer une liste de contrôle d'accès étendue à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **disable ns acl** <aclname>
- **enable ns acl** <aclname>

Pour désactiver ou activer un ACL6 étendu à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **disable ns acl6** <aclname>
- **enable ns acl6** <aclname>

Pour appliquer des ACL étendues à l'aide de l'interface de lignede commande

À l'invite de commande, tapez :

- **apply ns acls**

Pour appliquer des ACL6 étendus à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **apply ns acls6**

Pour renuméroter les priorités des ACL étendues à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **renumber ns acls**

Pour renuméroter les priorités des ACL6 étendus à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **renumber ns acls6**

Procédures GUI

Pour configurer une liste de contrôle d'accès étendue à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL étendues**, ajoutez une nouvelle ACL étendue ou modifiez une ACL étendue existante. Pour activer ou désactiver une liste de contrôle d'accès étendue existante, sélectionnez-la, puis sélectionnez **Activer** ou **désactiver** dans la liste **Action** .

Pour configurer un ACL6 étendu à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACLs** et, sous l'onglet **ACL6 étendu**, ajoutez un nouvel ACL6 étendu ou modifiez un ACL6 étendu existant. Pour activer ou désactiver un ACL6 étendu existant, sélectionnez-le, puis sélectionnez **Activer** ou **Désactiver** dans la liste **Action** .

Pour appliquer des listes de contrôle d'accès étendues à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL étendues**, dans la liste **Action**, cliquez sur **Appliquer**.

Pour appliquer des ACL6 étendues à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL6 étendu**, dans la liste **Action**, cliquez sur **Appliquer**.

Pour renuméroter les priorités des listes de contrôle d'accès étendues à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL étendues**, dans la liste **Action**, cliquez sur **Renuméroter la ou les priorités**.

Pour renuméroter les priorités des ACL6 étendues à l'aide de l'interface graphique :

- Accédez à **Système** > **Réseau** > **ACL** et, sous l'onglet **ACL6 étendu**, dans la liste **Action**, cliquez sur **Renuméroter la ou les priorités**.

Exemples de configurations

Le tableau suivant présente des exemples de configuration de règles ACL étendues via l'interface de ligne de commande : exemples de configurations ACL.

Journalisation des listes ACL étendues

Vous pouvez configurer NetScaler pour qu'il enregistre les détails des paquets qui correspondent à des ACL étendues.

En plus du nom ACL, les détails consignés incluent des informations spécifiques au paquet, telles que les adresses IP source et de destination. Les informations sont stockées soit dans le fichier syslog, soit dans le fichier `nslog`, en fonction du type de journalisation globale (`syslog or nslog`) activé.

La journalisation doit être activée au niveau global et au niveau ACL. Le paramètre global est prioritaire.

Pour optimiser la journalisation, lorsque plusieurs paquets du même flux correspondent à une ACL, seuls les détails du premier paquet sont consignés et le compteur est incrémenté pour chaque paquet appartenant au même flux. Un flux est défini comme un ensemble de paquets ayant les mêmes valeurs pour l'adresse IP source, l'adresse IP de destination, le port source, le port de destination et les paramètres de protocole. Pour éviter une surcharge de messages de journal, NetScaler applique une limitation de débit interne afin que les paquets appartenant au même flux ne soient pas enregistrés à plusieurs reprises. Le nombre total de flux différents pouvant être enregistrés à un moment donné est limité à 10 000.

Remarque : Vous devez appliquer les listes de contrôle d'accès après avoir activé la journalisation.

Procédures CLI

Pour configurer la journalisation ACL étendue à l'aide de l'interface de lignede commande :

À l'invite de commandes, tapez les commandes suivantes pour configurer la journalisation et vérifier la configuration :

- **set ns acl** <aclName> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** \<positive_integer>]
- **apply acls**
- **show ns acl** [\<aclName>]

Procédures GUI

Pour configurer la journalisation ACL étendue à l'aide de l'interface graphique :

1. Accédez à **Système > Réseau > ACL** et, sous l'onglet **ACL étendues**, ouvrez l'ACL étendue.
2. Définissez les paramètres suivants :
   - **État du journal** : activez ou désactivez la journalisation des événements liés à la règle ACL étendue. Les messages de journal sont stockés sur le `syslog or auditlog` serveur configuré.
   - **Limite du nombre de journaux** : nombre maximal de messages de journal à générer par seconde. Si vous définissez ce paramètre, vous devez activer le paramètre Log State .

Exemple de configuration

```
> set ns acl restrict -logstate ENABLED -ratelimit 120
Warning: ACL modified, apply ACLs to activate change

> apply ns acls
Done
<!--NeedCopy-->
```

Journalisation des ACL6 étendues

Vous pouvez configurer l'appliance NetScaler pour qu'elle enregistre les détails des paquets qui correspondent à une règle ACL6 étendue. En plus du nom ACL6, les détails consignés incluent des informations spécifiques au paquet, telles que les adresses IP source et de destination. Les informations sont stockées dans un syslog ou dans un `nslog` fichier, selon le type de journalisation (`syslog or nslog`) que vous avez configuré dans l'appliance NetScaler.

Pour optimiser la journalisation, lorsque plusieurs paquets du même flux correspondent à un ACL6, seuls les détails du premier paquet sont consignés. Le compteur est incrémenté pour tous les autres

paquets appartenant au même flux. Un flux est défini comme un ensemble de paquets qui ont les mêmes valeurs pour les paramètres suivants :

- IP source
- IP destination
- Port source
- Port de destination
- Protocole (TCP ou UDP)

Si un paquet entrant ne provient pas du même flux, un nouveau flux est créé. Le nombre total de flux différents pouvant être enregistrés à un moment donné est limité à 10 000.

Procédures CLI

Pour configurer la journalisation d'une règle ACl6 étendue à l'aide de l'interface de lignede commande :

- Pour configurer la journalisation lors de l'ajout de la règle ACL6 étendue, à l'invite de commandes, tapez :
  - **add acl6** <acl6Name> <acl6action> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** \<positive_integer>]
  - **apply acls6**
  - **show acl6** [\<acl6Name>]
- Pour configurer la journalisation d'une règle ACL6 étendue existante, à l'invite de commandes, tapez :
  - **set acl6** <acl6Name> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** \<positive_integer>]
  - **show acl6** [\<acl6Name>]
  - **apply acls6**

Procédures GUI

Pour configurer la journalisation ACL6 étendue à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **ACL**, puis cliquez sur l'onglet **ACL6 étendu** .
2. Définissez les paramètres suivants lors de l'ajout ou de la modification d'une règle ACL6 étendue existante.
   - **État du journal** : activez ou désactivez la journalisation des événements liés à la règle ACL6 étendue. Les messages de journal sont stockés dans le Syslog ou le `auditlog` serveur configuré.
   - **Limite du nombre de journaux** : nombre maximal de messages de journal à générer par seconde. Si vous définissez ce paramètre, vous devez activer le paramètre **Log State** .

Exemple de configuration

```
> set acl6 ACL6-1 -logstate ENABLED -ratelimit 120
Done

> apply acls6
Done
<!--NeedCopy-->
```

Affichage des listes de contrôle d'accès étendues et des statistiques ACL6 étendues

Vous pouvez afficher des statistiques sur les listes de contrôle d'accès étendues et les ACL6.

Le tableau suivant répertorie les statistiques associées aux listes ACL étendues et aux ACL6, ainsi que leurs descriptions.

Statistique	Spécifie
Allow ACL matches	Paquets correspondant aux ACL avec le mode de traitement défini sur Autoriser. NetScaler traite ces paquets.
Matchs NAT ACL	Paquets correspondant à une ACL NAT, entraînant une session NAT.
Deny ACL matches	Les paquets ont été supprimés parce qu'ils correspondent aux ACL avec le mode de traitement défini sur DENY.
Matchs ACL Bridge	Paquets correspondant à une liste ACL de pont, qui, en mode transparent, contourne le traitement du service.
ACL matches	Paquets correspondant à une liste ACL.
ACL misses	Paquets ne correspondant à aucune liste de contrôle d'accès.
ACL Count	Nombre total de règles ACL configurées par les utilisateurs.

Statistique	Spécifie
Effective ACL Count	Nombre total d'ACL effectifs configurés en interne. Pour une ACL étendue avec une plage d'adresses IP, l'appliance NetScaler crée en interne une ACL étendue pour chaque adresse IP. Par exemple, pour une ACL étendue comportant 1 000 adresses IPv4 (plage ou ensemble de données), NetScaler crée en interne 1 000 ACL étendues.

Procédures CLI

Pour afficher les statistiques de toutes les listes de contrôle d'accès étendues à l'aide de l'interface de lignede commande :

À l'invite de commande, tapez :

- **stat ns acl**

Pour afficher les statistiques de tous les ACL6 étendus à l'aide de l'interface de lignede commande :

À l'invite de commande, tapez :

- **stat ns acl6**

Procédures GUI

Pour afficher les statistiques d'une liste de contrôle d'accès étendue à l'aide de l'interface graphique :

- Accédez à **Système > Réseau > ACL**, sous l'onglet **ACL étendues**, sélectionnez l'ACL étendue, puis cliquez sur **Statistiques**.

Pour afficher les statistiques d'un ACL6 étendu à l'aide de l'interface graphique :

- Accédez à **Système > Réseau > ACL**, sous l'onglet **ACL6s étendus**, sélectionnez l'ACL étendue, puis cliquez sur **Statistiques**.

ACL avec état

Une règle ACL dynamique crée une session lorsqu'une demande correspond à la règle et autorise les réponses qui en résultent même si ces réponses correspondent à une règle de refus d'ACL dans

l'appliance NetScaler. Une ACL avec état décharge le travail de création de règles ACL et de règles de session de transfert supplémentaires pour autoriser ces réponses spécifiques.

Il est préférable d'utiliser les ACL Stateful dans le cadre du déploiement d'un pare-feu Edge d'une appliance NetScaler répondant aux exigences suivantes :

- L'appliance NetScaler doit autoriser les demandes émanant de clients internes et les réponses associées provenant d'Internet.
- L'appliance doit supprimer les paquets d'Internet qui ne sont liés à aucune connexion client.

Avant de commencer

Avant de configurer des règles ACL avec état, notez les points suivants :

- L'appliance NetScaler prend en charge les règles ACL dynamique et les règles ACL6 statiques.
- Dans une configuration haute disponibilité, les sessions d'une règle ACL avec état ne sont pas synchronisées avec le nœud secondaire.
- Vous ne pouvez pas configurer une règle ACL en tant que règle statique si la règle est liée à une configuration NetScaler NAT. Voici quelques exemples de configurations NetScaler NAT :
  - RNAT
  - NAT à grande échelle (NAT44 à grande échelle, DS-Lite, NAT64 à grande échelle)
  - NAT64
  - Session de transfert
- Vous ne pouvez pas configurer une règle ACL en tant qu'état si les paramètres TTL et Établi sont définis pour cette règle ACL.
- Les sessions créées pour une règle ACL avec état continuent d'exister jusqu'à l'exode, quelles que soient les opérations ACL suivantes :
  - Supprimer ACL
  - Désactiver l'ACL
  - Effacer l'ACL
- Les listes de contrôle d'accès avec état ne sont pas prises en charge pour les protocoles suivants :
  - FTP actif
  - TFTP

Configurer les règles ACL IPv4 avec état

La configuration d'une règle ACL avec état consiste à activer le paramètre avec état d'une règle ACL.

Pour activer le paramètre avec état d'une règle ACL à l'aide de l'interface de lignede commande :

- Pour activer le paramètre stateful lors de l'ajout d'une règle ACL, à l'invite de commandes, tapez :
  - **add acl** <lname> ALLOW -**stateful** (ENABLED | DISABLED)

- **apply acls**
- **show acl** <name>

- Pour activer le paramètre stateful d'une règle ACL existante, à l'invite de commandes, tapez :
  - **set acl** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls**
  - **show acl** <name>

Pour activer le paramètre avec état d'une règle ACL à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **ACL** et, dans l'onglet **ACL étendues** .
2. Activez le paramètre **Stateful** lors de l'ajout ou de la modification d'une règle ACL existante.

Exemple de configuration

```
> add acl ACL-1 allow -srciP 1.1.1.1 -stateful Yes

Done

> apply acls

Done

> show acl

1)         Name: ACL-1

    Action: ALLOW                          Hits: 0

    srcIP = 1.1.1.1

    destIP

    srcMac:

    Protocol:

    Vlan:                                 Interface:

    Active Status: ENABLED                 Applied Status: NOTAPPLIED

    Priority: 10                           NAT: NO

    TTL:
```



```
30
31      Log Status: DISABLED
32
33      Forward Session: NO
34
35      Stateful: YES
36  <!--NeedCopy-->
```

Configurer les règles ACL6 avec état

La configuration d'une règle ACL6 avec état consiste à activer le paramètre avec état d'une règle ACL6.

Pour activer le paramètre avec état d'une règle ACL6 à l'aide de l'interface de lignede commande :

- Pour activer le paramètre stateful lors de l'ajout d'une règle ACL6, à l'invite de commandes, tapez :
  - **add acl6** <name> ALLOW -stateful (ENABLED | DISABLD)
  - **apply acls6**
  - **show acl6** <name>
- Pour activer le paramètre stateful d'une règle ACL6 existante, à l'invite de commandes, tapez :
  - **set acl6** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls6**
  - **show acl6** <name>

Pour activer le paramètre avec état d'une règle ACL6 à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **ACLs** et, dans l'onglet **Extended ACL6s** .
2. Activez le paramètre **Stateful** lors de l'ajout ou de la modification d'une règle ACL6 existante.

Exemple de configuration

```
1  >  add acl6 ACL6-1 allow -srcipv6 1000::1  - stateful Yes
2
3  Done
4
5  >  apply acls6
6
7  Done
8
9  > show acl6
10
```



```
1)    Name: ACL6-1

    Action: ALLOW                          Hits: 0

    srcIPv6 = 1000::1

    destIPv6

    srcMac:

    Protocol:

    Vlan:                                 Interface:

    Active Status: ENABLED                 Applied Status: NOTAPPLIED

    Priority: 10                           NAT: NO

    TTL:

    Forward Session: NO

    Stateful: YES
<!--NeedCopy-->
```

ACL étendues basées sur un jeu de données

De nombreuses ACL sont nécessaires dans une entreprise. La configuration et la gestion de nombreuses listes de contrôle d'accès sont difficiles et fastidieuses lorsqu'elles nécessitent des modifications fréquentes.

Une appliance NetScaler prend en charge les ensembles de données dans des ACL étendues. Le jeu de données est une fonctionnalité existante d'une appliance NetScaler. Un jeu de données est un tableau de modèles indexés de types : nombre (entier), adresse IPv4 ou adresse IPv6.

La prise en charge des jeux de données dans les listes ACL étendues est utile pour créer plusieurs règles ACL, qui nécessitent des paramètres ACL communs.

Lors de la création d'une règle ACL, au lieu de spécifier les paramètres communs, vous pouvez spécifier un jeu de données, qui inclut ces paramètres communs.

Toutes les modifications apportées au jeu de données sont automatiquement reflétées dans les règles ACL qui utilisent ce jeu de données. Les listes de contrôle d'accès avec jeux de données sont plus faciles à configurer et à gérer. Ils sont également plus petits et plus faciles à lire que les ACL classiques.

Actuellement, l'appliance NetScaler prend uniquement en charge les types de jeux de données suivants pour les ACL étendues :

- Adresse IPv4 (pour spécifier l'adresse IP source ou l'adresse IP de destination ou les deux pour une règle ACL)
- number (pour spécifier le port source ou le port de destination ou les deux pour une règle ACL)

Avant de commencer

Avant de configurer des règles ACL étendues basées sur des jeux de données, notez les points suivants :

- Assurez-vous de bien connaître la fonctionnalité d'ensemble de données d'une appliance NetScaler. Pour plus d'informations sur les jeux de données, voir Jeux de modèles et jeux de données.
- L'appliance NetScaler prend en charge les ensembles de données uniquement pour les ACL étendues IPv4.
- L'appliance NetScaler prend uniquement en charge les types de jeux de données suivants pour les ACL étendues :
  - Adresse IPv4
  - nombre
- L'appliance NetScaler prend en charge les ACL étendues basées sur des ensembles de données pour toutes les configurations NetScaler : autonome, haute disponibilité et cluster.
- Pour une ACL étendue avec des ensembles de données contenant des plages, l'appliance NetScaler crée en interne une ACL étendue pour chaque combinaison des valeurs du jeu de données.
  - **Exemple 1** : pour une ACL étendue basée sur un jeu de données IPv4 avec 1 000 adresses IPv4 liées à l'ensemble de données et dont l'ensemble de données est défini sur le paramètre IP source, l'appliance NetScaler crée en interne 1 000 ACL étendues.
  - **Exemple 2** : liste de contrôle d'accès étendue basée sur un jeu de données avec les paramètres suivants définis :
    * L'adresse IP source est définie sur un ensemble de données contenant 5 adresses IP.
    * L'adresse IP de destination est définie sur un ensemble de données contenant 5 adresses IP.
    * Le port source est défini sur un jeu de données contenant 5 ports.
    * Le port de destination est défini sur un jeu de données contenant 5 ports.

    L'appliance NetScaler crée en interne 625 ACL étendues. Chacune de ces listes de contrôle d'accès internes contient une combinaison unique des quatre valeurs de paramètres mentionnées ci-dessus.

- L'appliance NetScaler prend en charge un maximum de 10 000 ACL étendues. Pour une ACL étendue basée sur un jeu de données IPv4 avec une plage d'adresses IP liée au jeu de données, l'appliance NetScaler arrête de créer des ACL internes une fois que le nombre total d'ACL étendues atteint la limite maximale.
- Les compteurs suivants sont présents dans le cadre des statistiques ACL étendues :
  * **Nombre d'ACL**. Nombre total de règles ACL configurées par les utilisateurs.
  * Nombre de**LCA effectif**. Nombre total de règles ACL effectives que l'appliance NetScaler configure en interne.

  Pour plus d'informations, reportez-vous à la section Affichage des statistiques ACL étendues et ACL6sétendues.

- L'appliance NetScaler ne prend pas en charge les `unset` opérations `set` d'association/de dissociation de jeux de données avec les paramètres d'une ACL étendue. Vous pouvez définir les paramètres ACL sur un jeu de données uniquement pendant l'opération `add`.

Configuration des listes ACL étendues basées sur les jeux de données

La configuration d'une règle ACL étendue basée sur un jeu de données comprend les tâches suivantes :

- **Ajoutez un jeu de données**. Un jeu de données est un tableau de modèles indexés de types : nombre (entier), adresse IPv4 ou adresse IPv6. Dans cette tâche, vous créez un type de jeu de données, par exemple un jeu de données de type IPv4.
- **Liez des valeurs au jeu de données**. Spécifiez une valeur ou une plage de valeurs dans le jeu de données. Les valeurs spécifiées doivent être du même type que le type de jeu de données. Par exemple, vous pouvez spécifier une adresse IPv4, une plage d'adresses IPv4 ou une plage d'adresses IPv4 en notation CIDR à un ensemble de données IPv4.
- **Ajoutez une liste d'accès étendue et définissez des paramètres ACL au jeu de données**. Ajoutez une liste de contrôle d'accès étendue et définissez les paramètres ACL requis dans le jeu de données. Ce paramètre entraîne la définition des paramètres sur les valeurs spécifiées dans le jeu de données.
- **Appliquez des listes ACL étendues**. Appliquez les ACL pour activer toutes les listes ACL étendues nouvelles ou modifiées.

Pour ajouter un jeu de données de stratégie à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add policy dataset** <name> <type>
- **show policy dataset**

Pour lier un motif à l'ensemble de données à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **bind policy dataset** <name> <value> [-endRange \<string>]
- **show policy dataset**

Pour ajouter une ACL étendue et définir les paramètres ACL sur le jeu de données à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add ns acl** <aclname> <aclaction> [-**srcIP** [\<operator>] <srcIPVal>] [-**srcPort** [\<operator>] <srcPortVal>] [-**destIP** [\<operator>] <destIPVal>] [-**destPort** [\<operator>] <destPortVal>] …
- **show acls**

Pour appliquer des ACL étendues à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **apply acls**

Exemple de configuration

Dans l'exemple de configuration suivant d'une liste de contrôle d'accès étendue basée sur un jeu de données, deux jeux `DATASET_IP_ACL_1` de données IPv4 `DATASET_IP_ACL_2` sont créés. Deux jeux de données de ports `DATASET_PORT_ACL_1` et `DATASET_PORT_ACL_1` sont créés.

Deux adresses IPv4 : 192.0.2.30 et 192.0.2.60 sont liées à `DATASET_IP_ACL_1`. Deux plages d'adresses IPv4 : (198.51.100.15 - 45) et (203.0.113.60-90) sont liées à `DATASET_IP_ACL_2`. `DATASET_IP_ACL_1` est ensuite spécifié pour le paramètre `srcIP` et `DATASET_IP_ACL_1` pour le paramètre `destIP` de la liste de contrôle d'accès étendue `ACL-1`.

Deux numéros de port, 2001 et 2004, sont liés à `DATASET_PORT_ACL_1`. Deux plages de ports : (5001 - 5040) et (8001 - 8040) sont liées à `DATASET-PORT-ACL-2`. `DATASET_IP_ACL_1` est ensuite spécifié pour le paramètre `srcIP` et `DATASET_IP_ACL_1` pour le paramètre `destIP` de la liste de contrôle d'accès étendue `ACL-1`.

```
add policy dataset DATASET_IP_ACL_1 IPV4
add policy dataset DATASET_IP_ACL_2 IPV4

add policy dataset DATASET_PORT_ACL_1 NUM
add policy dataset DATASET_PORT_ACL_2 NUM

bind dataset DATASET_IP_ACL_1 192.0.2.30
bind dataset DATASET_IP_ACL_1 192.0.2.60
bind dataset DATASET_IP_ACL_2 198.51.100.15 -endrange 198.51.100.45
bind dataset DATASET_IP_ACL_2 203.0.113.1/24
```



```
11
12 bind dataset DATASET_PORT_ACL_1 2001
13 bind dataset DATASET_PORT_ACL_1 2004
14 bind dataset DATASET_PORT_ACL_2 5001 -endrange 5040
15 bind dataset DATASET_PORT_ACL_2 8001 -endrange 8040
16
17 add ns acl ACL-1 ALLOW -srcIP DATASET_IP_ACL_1 -destIP DATASET_IP_ACL_2
18 -srcPort DATASET_PORT_ACL_1 -destPort DATASET_PORT_ACL_2  - protocol TCP
19 <!--NeedCopy-->
```

Masque générique d'adresse MAC pour les ACL

August 20, 2021

Un paramètre de masque générique a été introduit pour les ACL étendues et les ACL6 et est utilisé avec le paramètre d'adresse MAC source pour définir une plage d'adresses MAC à correspondre à l'adresse MAC source des paquets entrants.

Les masques génériques spécifient quels chiffres hexadécimaux de l'adresse MAC sont utilisés et quels chiffres hexadécimaux sont ignorés. Le paramètre de masque générique spécifie une série de 1 et de zéros et a une longueur de 12 chiffres. Chaque chiffre est un masque pour le chiffre hexadécimal correspondant de l'adresse MAC. Un chiffre zéro dans le masque générique indique que le chiffre hexadécimal correspondant de l'adresse MAC doit être pris en compte et un chiffre indique que le chiffre hexadécimal correspondant doit être ignoré.

Le masque générique doit répondre aux conditions suivantes :

- A seulement une série de zéros
- A seulement une série de uns
- Commencer par une série de zéros

Voici quelques exemples de masques génériques valides :

- 000000111111
- 000000011111
- 000011111111

Voici quelques exemples de masques génériques non valides :

- 000000111100
- 111110000000
- 010101010101

Pour une ACL, un masque générique 000000111111 pour l'adresse MAC 96:fa: 95:1d:67:4 a définit la plage d'adresses MAC 96:FA:95:00:00:00 - 96:FA:95:FF:FF. Cette plage d'adresses MAC est mise en correspondance avec l'adresse MAC source des paquets entrants.

Pour spécifier une plage d'adresses MAC source dans une règle ACL à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 -  add ns acl <name> <action> -srcMac <mac_addr> -srcMacMask <string>
2 -  show ns acl <aclname>
3 <!--NeedCopy-->
```

Exemple :

```
1 add ns acl ACL-1 ALLOW  - protocol TCP  - srcport 2000-3000 -srcMac 96:fa
     :95:1d:67:4a
2   - srcMacMask 000000111111
3 Done
4 <!--NeedCopy-->
```

Pour spécifier une plage d'adresses MAC source dans une règle ACL6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
1 -  add ns acl6 <name> <action> -srcMac <mac_addr> -srcMacMask <string>
2 -  show ns acl6 <acl6name>
3 <!--NeedCopy-->
```

Exemple :

```
1 > add ns acl6 ACL6-1 ALLOW -destIPv6 2001::45 -srcMac 96:fa:90:1d:67:4a
2  - srcMacMask 000000001111
3 Done
4 <!--NeedCopy-->
```

Blocage du trafic sur les ports internes

May 5, 2023

Par défaut, une appliance NetScaler ne bloque aucun type de trafic interne, même à l'aide de règles ACL.

Le tableau suivant répertorie les types de trafic interne qu'une appliance NetScaler ne bloque pas, même à l'aide de règles ACL :

Configuration de NetScaler	Protocole	Port de destination	Adresse IP de destination
Tous	TCP	3008–3011	NSIP ou SNIP
Tous	TCP	179	NSIP ou SNIP
Tous	UDP	520	NSIP ou SNIP
Haute disponibilité	UDP	3003	NSIP
Haute disponibilité	TCP	22	NSIP
Cluster :	UDP	7000	NSIP

Cette fonctionnalité qui consiste à ne pas bloquer les types de trafic mentionnés précédemment est spécifiée par le paramètre par défaut du paramètre global Layer-3 `Implicit ACL Allow` (`implicitACLAllow`).

Vous pouvez désactiver ce paramètre si vous souhaitez bloquer les types de trafic mentionnés précédemment à l'aide des règles ACL. Une appliance dans une configuration haute disponibilité fait une exception pour son nœud partenaire (principal ou secondaire). Il ne bloque pas le trafic en provenance de ce nœud.

Pour désactiver ou activer ce paramètre à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set l3param** -**implicitACLAllow** [ENABLED|DISABLED]
- **sh l3param**

Remarque : Le paramètre ImplicitAclAllow est activé par défaut.

Exemple :

```
> set l3param -implicitACLAllow DISABLED
Done
<!--NeedCopy-->
```

Routage IP

May 5, 2023

Les appliances NetScaler prennent en charge le routage dynamique et statique. Le routage simple n'étant pas le rôle principal d'un NetScaler, l'objectif principal de l'exécution de protocoles de routage dynamique est de permettre l'injection d'intégrité des routes (RHI), afin qu'un routeur en amont puisse choisir le meilleur parmi plusieurs itinéraires vers un serveur virtuel distribué topographiquement.

La plupart des implémentations de NetScaler utilisent des routes statiques pour réduire les frais de routage. Vous pouvez créer des itinéraires statiques de sauvegarde et surveiller les itinéraires pour activer le basculement automatique en cas de panne d'un itinéraire statique. Vous pouvez également attribuer des poids pour faciliter l'équilibrage de charge entre les routes statiques, créer des routes nulles pour empêcher les boucles de routage et configurer des routes statiques IPv6. Vous pouvez configurer des itinéraires basés sur des politiques (PBR), pour lesquels les décisions de routage sont basées sur des critères que vous spécifiez.

Configuration des itinéraires dynamiques

May 5, 2023

Lorsqu'un protocole de routage dynamique est activé, le processus de routage correspondant surveille les mises à jour des itinéraires et annonce les itinéraires. Les protocoles de routage permettent à un routeur en amont d'utiliser la technique ECMP (Equal Cost Multipath) pour équilibrer la charge du trafic vers des serveurs virtuels identiques hébergés sur deux appliances NetScaler autonomes. Le routage dynamique sur une appliance NetScaler utilise trois tables de routage. Dans une configuration haute disponibilité, les tables de routage de l'appliance secondaire reflètent celles de la solution principale.

Pour connaître les guides de référence des commandes et les commandes non prises en charge sur le protocole de routage dynamique, consultez Guides de référence des commandes du protocole de routage dynamique et commandes non prises en charge.

NetScaler prend en charge les protocoles suivants :

- Protocole d'information de routage (RIP) version 2
- Ouvrez d'abord le chemin le plus court (OSPF) version 2
- Protocole Border Gateway (BGP)
- Protocole d'information de routage de nouvelle génération (RIPng) pour IPv6
- Open Shortest Path First (OSPF) version 3 pour IPv6
- Protocole ISIS

Vous pouvez activer plusieurs protocoles simultanément.

Tables de routage dans NetScaler

Dans une appliance NetScaler, la table de routage du noyau NetScaler, la table de routage du noyau FreeBSD et la table de routage NSM FIB contiennent chacune un ensemble différent de routes et ont un objectif différent. Ils communiquent entre eux à l'aide de sockets de routage UNIX. Les mises à jour d'itinéraires ne sont pas automatiquement propagées d'une table de routage à une autre. Vous devez configurer la propagation des mises à jour d'itinéraires pour chaque table de routage.

Table de routage du noyau NS

La table de routage du noyau NS contient les routes de sous-réseau correspondant au NSIP et à chaque SNIP et MIP. En général, aucune route correspondant aux VIP n'est présente dans la table de routage du noyau NS. L'exception est un VIP ajouté à l'aide de la commande add ns ip et configuré avec un masque de sous-réseau autre que 255.255.255.255. Si plusieurs adresses IP appartiennent au même sous-réseau, elles sont extraites sous la forme d'une route de sous-réseau unique. En outre, cette table contient une route vers le réseau de bouclage (127.0.0.0) et toutes les routes statiques ajoutées via la CLI (CLI). Les entrées de ce tableau sont utilisées par NetScaler pour le transfert de paquets. À partir de l'interface de ligne de commande, ils peuvent être inspectés à l'aide de la commande show route.

Table de routage FreeBSD

Le seul but de la table de routage FreeBSD est de faciliter l'initiation et la fin du trafic de gestion (telnet, ssh, etc.). Dans une appliance NetScaler, ces applications sont étroitement liées à FreeBSD, et il est impératif que FreeBSD dispose des informations nécessaires pour gérer le trafic en provenance et à destination de ces applications. Cette table de routage contient une route vers le sous-réseau NSIP et une route par défaut. De plus, FreeBSD ajoute des routes de type WAScloned (W) lorsque NetScaler établit des connexions avec des hôtes sur des réseaux locaux. En raison de l'utilité hautement spécialisée des entrées de cette table de routage, toutes les autres mises à jour de routage provenant du noyau NS et des tables de routage NSM FIB contournent la table de routage FreeBSD. Ne le modifiez pas à l'aide de la commande route. La table de routage FreeBSD peut être inspectée à l'aide de la commande netstat depuis n'importe quel shell UNIX.

Module de services réseau (NSM) FIB

La table de routage NSM FIB contient les itinéraires publicitaires qui sont distribués par les protocoles de routage dynamique à leurs homologues du réseau. Il peut contenir :

- **Itinéraires connectés**. Sous-réseaux IP directement accessibles depuis NetScaler. Généralement, les routes correspondant au sous-réseau NSIP et aux sous-réseaux sur lesquels les protocoles de routage sont activés sont présentes dans NSM FIB en tant que routes connectées.

- **Routes du noyau**. Toutes les adresses VIP sur lesquelles l'option -hostRoute est activée sont présentes dans NSM FIB en tant que routes du noyau si elles répondent aux niveaux RHI requis. En outre, NSM FIB contient toutes les routes statiques configurées sur l'interface de ligne de commande pour lesquelles l'option - advertise est activée. Sinon, si NetScaler fonctionne en mode Static Route Advertising (SRADV), toutes les routes statiques configurées sur la CLI sont présentes dans NSM FIB. Ces routes statiques sont marquées comme routes du noyau dans NSM FIB, car elles appartiennent en fait à la table de routage du noyau NS.
- **Routes statiques**. Normalement, toute route statique configurée dans VTYSH est présente dans NSM FIB. Si les distances administratives des protocoles sont modifiées, ce n'est pas toujours le cas. Il est important de noter que ces routes ne peuvent jamais entrer dans la table de routage du noyau NS.
- **Itinéraires appris**. Si NetScaler est configuré pour apprendre les itinéraires de manière dynamique, le NSM FIB contient les itinéraires appris par les différents protocoles de routage dynamique. Les itinéraires appris par l'OSPF nécessitent toutefois un traitement spécial. Ils sont téléchargés sur FIB uniquement si l'option fib-install est activée pour le processus OSPF. Cela peut être fait à partir de la vue router-config dans VTYSH.

Routage dynamique dans une configuration à haute disponibilité

Dans une configuration à haute disponibilité, le nœud principal exécute le processus de routage et propage les mises à jour de la table de routage vers le nœud secondaire. La table de routage du nœud secondaire reflète la table de routage du nœud principal.

Expédition continue

Après le basculement, le nœud secondaire met un certain temps à démarrer le protocole, à connaître les itinéraires et à mettre à jour sa table de routage. Mais cela n'affecte pas le routage, car la table de routage du nœud secondaire est identique à la table de routage du nœud principal. Ce mode de fonctionnement est connu sous le nom de transfert continu.

Mécanisme d'évitement des trous noirs

Après le basculement, le nouveau nœud principal injecte toutes ses routes VIP dans le routeur en amont. Toutefois, ce routeur conserve les routes de l'ancien nœud principal pendant 180 secondes. Comme le routeur n'est pas au courant du basculement, il tente d'équilibrer la charge du trafic entre les deux nœuds. Pendant les 180 secondes qui précèdent l'expiration des anciennes routes, le routeur envoie la moitié du trafic à l'ancien nœud principal inactif, qui est en fait un trou noir.

Pour éviter cela, le nouveau nœud principal, lorsqu'il injecte une route, lui attribue une métrique légèrement inférieure à celle spécifiée par l'ancien nœud principal.

Interfaces pour la configuration du routage dynamique

Pour configurer le routage dynamique, vous pouvez utiliser l'interface graphique ou une interface de ligne de commande. NetScaler prend en charge deux interfaces de ligne de commande indépendantes : la CLI et le Virtual Teletype Shell (VTYSH). La CLI est l'interpréteur de commandes natif de l'appliance. Le VTYSH est exposé par ZebOS. La suite de routage NetScaler est basée sur ZebOS, la version commerciale de GNU Zebra.

> **Remarque :**
>
> Citrix vous recommande d'utiliser VTYSH pour toutes les commandes, à l'exception de celles qui ne peuvent être configurées que sur l'interface de ligne de commande. L'utilisation de la CLI doit généralement être limitée aux commandes permettant d'activer les protocoles de routage, de configurer la publicité des itinéraires hôtes et d'ajouter des itinéraires statiques pour le transfert de paquets.

Guides de référence des commandes du protocole de routage dynamique et commandes non prises en charge

Le tableau suivant répertorie les liens du guide de référence des commandes, pour différents protocoles de routage dynamique et les commandes non prises en charge sur l'appliance NetScaler : guides de référence du protocole de routage dynamique etcommandes non prises en charge.

Configuration du RIP

May 5, 2023

Le protocole RIP (Routing Information Protocol) est un protocole à vecteur de distance. NetScaler prend en charge le protocole RIP tel que défini dans les RFC 1058 et RFC 2453. RIP peut s'exécuter sur n'importe quel sous-réseau.

Après avoir activé RIP, vous devez configurer la publicité des itinéraires RIP. Pour résoudre les problèmes, vous pouvez limiter la propagation du RIP. Vous pouvez afficher les paramètres RIP pour vérifier la configuration.

Activation et désactivation du RIP

Utilisez l'une des procédures suivantes pour activer ou désactiver RIP. Une fois que vous avez activé RIP, l'appliance NetScaler lance le processus RIP. Une fois que vous avez désactivé RIP, l'appliance arrête le processus RIP.

Pour activer ou désactiver le routage RIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, entrez l'une des commandes suivantes pour activer ou désactiver RIP :

- **activer la fonctionnalité ns RIP**
- **désactiver la fonctionnalité NS RIP**

Pour activer ou désactiver le routage RIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Modifier les fonctionnalités avancées**.
2. Sélectionnez ou désactivez l'option de **routage RIP** .

Itinéraires publicitaires

Le RIP permet à un routeur en amont d'équilibrer la charge du trafic entre deux serveurs virtuels identiques hébergés sur deux appliances NetScaler autonomes. La publicité d'itinéraire permet à un routeur en amont de suivre les entités du réseau situées derrière le NetScaler.

Pour configurer RIP afin de publier des itinéraires à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
routeur rip	Démarrez le processus de routage RIP et entrez en mode de configuration pour le processus de routage.
redistribute static	Redistribuez les routes statiques.
redistribute kernel	Redistribuez les routes du noyau.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```


Limiter les propagations RIP

Si vous devez résoudre des problèmes de configuration, vous pouvez configurer le mode écoute uniquement sur n'importe quelle interface.

Pour limiter la propagation du RIP à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
routeur rip	Démarrez le processus de routage RIP et entrez en mode de configuration pour le processus de routage.
passive-interface < vlan_name>	Supprime les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router rip
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Vérification de la configuration RIP

Vous pouvez afficher la table de routage et d'autres paramètres RIP.

Pour afficher les paramètres RIP à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes dans l'ordre suivant :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
voyage aux cendres	Afficher la table de routage RIP mise à jour.
interface SSH Rip <vlan_name>	Affiche les informations RIP pour le VLAN spécifié.

Exemple :

```
NS# VTYSH
NS# sh rip
NS# sh rip interface VLAN0
<!--NeedCopy-->
```

Configuration d'OSPF

May 5, 2023

NetScaler prend en charge la version 2 d'Open Shortest Path First (OSPF) (RFC 2328). Les fonctionnalités d'OSPF sur NetScaler sont les suivantes :

- Si un vserver est actif, les routes de l'hôte vers le vserver peuvent être injectées dans les protocoles de routage.
- L'OSPF peut s'exécuter sur n'importe quel sous-réseau.
- L'apprentissage des itinéraires annoncé par les routeurs OSPF voisins peut être désactivé sur NetScaler.
- NetScaler peut publier des métriques externes de type 1 ou de type 2 pour tous les itinéraires.
- NetScaler peut publier les paramètres de métrique spécifiés par l'utilisateur pour les itinéraires VIP. Par exemple, vous pouvez configurer une mesure par VIP sans carte d'itinéraire spéciale.
- Vous pouvez spécifier l'ID de zone OSPF pour NetScaler.
- NetScaler prend en charge les zones pas si tronquées (NSSA). Une NSSA est similaire à une zone tampon OSPF mais permet l'injection de voies externes de manière limitée dans la zone tronquée. Pour prendre en charge les NSSA, un nouveau bit d'option (le bit N) et un nouveau type (type 7) de zone d'annonce d'état de liaison (LSA) ont été définis. Les LSA de type 7 prennent en charge les informations de routage externes dans un NSSA. Un routeur de bordure de zone (ABR) NSSA convertit un LSA de type 7 en un LSA de type 5 qui est propagé dans le domaine OSPF. La spécification OSPF définit uniquement les classes générales de configuration de zone suivantes :
  - LSA de type 5 : Les routeurs internes à la zone sont inondés dans le domaine par des routeurs de frontière AS (ASBR).
  - Stub : Ne permet à aucun LSA de type 5 d'être propagé dans/dans toute la zone et dépend plutôt du routage par défaut vers des destinations externes.

Après avoir activé l'OSPF, vous devez configurer la publication des routes OSPF. Pour le dépannage, vous pouvez limiter la propagation OSPF. Vous pouvez afficher les paramètres OSPF pour vérifier la configuration.

Activation et désactivation de l'OSPF

Pour activer ou désactiver l'OSPF, vous devez utiliser l'interface de ligne de commande ou l'interface graphique. Lorsque l'OSPF est activé, NetScaler lance le processus OSPF. Lorsque l'OSPF est désactivé, NetScaler arrête le processus de routage OSPF.

Pour activer ou désactiver le routage OSPF à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

1. **enable ns feature OSPF**
2. **disable ns feature OSPF**

Pour activer ou désactiver le routage OSPF à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Modifier les fonctionnalités avancées**.
2. Sélectionnez ou désactivez l'option **Routage OSPF** .

Routes publicitaires OSPF

L'OSPF permet à un routeur en amont d'équilibrer la charge du trafic entre deux serveurs virtuels identiques hébergés sur deux appliances NetScaler autonomes. La publicité par itinéraire permet à un routeur en amont de suivre les entités du réseau situées derrière le NetScaler.

Pour configurer OSPF afin de publier des itinéraires à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entre en mode de configuration globale.
router OSPF	Démarrez le processus de routage OSPF et passez en mode de configuration pour le processus de routage.
network A.B.C.D/M area <0-4294967295>	Activez le routage sur un réseau IP.
redistribute static	Redistribuez les routes statiques.
redistribute kernel	Redistribuez les routes du noyau.

Exemple :

```
1 >VTYSH
```



```
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# network 10.102.29.0/24 area 0
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Limitation des propagations OSPF

Si vous devez dépanner votre configuration, vous pouvez configurer le mode d'écoute uniquement sur n'importe quel VLAN donné.

Pour limiter la propagation OSPF à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router OSPF	Démarrez le processus de routage OSPF et passe en mode de configuration pour le processus de routage.
passive-interface < vlan_name>	Supprime les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Vérification de la configuration OSPF

Vous pouvez afficher les voisins OSPF actuels et les itinéraires OSPF.

Pour afficher les paramètres OSPF à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
sh OSPF neighbor	Affiche les voisins actuels.
sh OSPF route	Affiche les itinéraires OSPF.

Exemple :

```
>VTYSH
NS# sh ip OSPF neighbor
NS# sh ip OSPF route
<!--NeedCopy-->
```

Configuration du redémarrage progressif pour OSPF

Dans une configuration haute disponibilité (HA) non INC dans laquelle un protocole de routage est configuré, après un basculement, les protocoles de routage convergent et les routes entre le nouveau nœud principal et les routeurs voisins adjacents sont apprises. L'apprentissage par voie prend un certain temps. Pendant ce temps, le transfert des paquets est retardé, les performances du réseau peuvent être perturbées et les paquets peuvent être abandonnés.

Le redémarrage progressif permet à une configuration HA lors d'un basculement d'ordonner à ses routeurs adjacents de ne pas supprimer les routes apprises de l'ancien nœud principal de leurs bases de données de routage. En utilisant les informations de routage de l'ancien nœud principal, le nouveau nœud principal et les routeurs adjacents commencent immédiatement à transférer des paquets, sans perturber les performances du réseau.

> **Remarque :**
>
> Le redémarrage progressif n'est pas pris en charge pour les configurations haute disponibilité en mode INC.

Pour configurer le redémarrage progressif pour OSPF à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
VTYSH	VTYSH	Saisit l'invite de commande VTYSH.
configure terminal	NS# configure terminal	Entre en mode de configuration globale.

Commande	Exemple	Description de la commande
router-id <id>	NS(config)# router-id 1.1.1.1	Définit un identifiant de routeur pour l'appliance NetScaler. Cet identifiant est défini pour tous les protocoles de routage dynamique. Le même ID doit être spécifié dans l'autre nœud dans une configuration haute disponibilité configurée pour que le redémarrage progressif fonctionne correctement dans la configuration HA.
ospf restart grace-period <1-1800>	NS(config)# ospf restart grace-period 170	Spécifie la période de grâce, en secondes, pendant laquelle les itinéraires doivent être conservés dans les dispositifs d'assistance. Valeur par défaut : 120 secondes.
ospf restart helper max-grace-period <1-1800>	NS(config)# ospf restart helper max-grace-period 180	Il s'agit d'une commande facultative visant à limiter la période de grâce maximale pendant laquelle l'appliance NetScaler sera en mode assistant. Si l'appliance NetScaler reçoit un LSA opaque dont la période de grâce est supérieure à la période de grâce maximale définie pour l'assistant, le LSA est supprimé et NetScaler n'est pas placé en mode auxiliaire.

Commande	Exemple	Description de la commande
router ospf	NS(config)# router ospf	Lance le processus de routage OSPF et passe en mode de configuration pour le processus de routage.
network A.B.C.D/M area <0-4294967295>	NS (config-router) # réseau 192.0.2.0/24 zone 0	Enables routing on an IP network.
capability restart graceful	NS(config-router)# capability restart graceful	Permet un redémarrage progressif du processus de routage OSPF.
redistribute kernel	NS(config-router)# redistribute kernel	Redistribue les routes du noyau.

Configuration de BGP

May 5, 2023

L'appliance NetScaler prend en charge le protocole BGP (RFC 4271). Les fonctionnalités de BGP sur NetScaler sont les suivantes :

- NetScaler annonce les itinéraires à ses homologues BGP.
- Le NetScaler injecte des routes hôtes vers des adresses IP virtuelles (VIP), en fonction de l'état des serveurs virtuels sous-jacents.
- NetScaler génère des fichiers de configuration pour exécuter BGP sur le nœud secondaire après un basculement dans une configuration HA.
- Ce protocole prend en charge les échanges de routes IPv6.
- As-Override Support in Border Gateway Protocol

Après avoir activé le BGP, vous devez configurer la publication des routes BGP. Pour le dépannage, vous pouvez limiter la propagation BGP. Vous pouvez afficher les paramètres BGP pour vérifier la configuration.

Activation et désactivation du BGP

Pour activer ou désactiver le BGP, vous devez utiliser l'interface de ligne de commande ou l'interface graphique. Lorsque le BGP est activé, l'appliance NetScaler lance le processus BGP. Lorsque le BGP est désactivé, l'appliance arrête le processus BGP.

Pour activer ou désactiver le routage BGP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- enable ns feature BGP
- disable ns feature BGP

Pour activer ou désactiver le routage BGP à l'aide de l'interface graphique :

1. Accédez à Système > Paramètres, dans le groupe Modes et fonctionnalités, cliquez sur Modifier les fonctionnalités avancées.
2. Sélectionnez ou désactivez l'option Routage BGP.

Routes IPv4 publicitaires

Vous pouvez configurer l'appliance NetScaler pour annoncer les itinéraires hôtes aux VIP et pour annoncer les itinéraires vers les réseaux en aval.

Pour configurer BGP afin d'annoncer des routes IPv4 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire. Valeurs possibles : 1 à 4 294 967 295.
Neighbor < IPv4 address> remote-as < as-number>	Mettez à jour la table de voisins BGP IPv4 avec l'adresse IPv4 locale du lien du voisin dans le système autonome spécifié.
Address-family ipv4	Passez en mode de configuration de famille d'adresses.
Neighbor < IPv4 address> activate	Préfixes Exchange pour la famille de routeurs IPv4 entre le pair et le nœud local à l'aide de l'adresse locale du lien.
redistribute kernel	Redistribuez les routes du noyau.
redistribute static	Redistribuez les routes statiques.

Exemple :


```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor 10.102.29.170 remote-as 100
NS(config-router)# Address-family ipv4
NS(config-router-af)# Neighbor 10.102.29.170 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
<!--NeedCopy-->
```

Annonces des routes IPv6 BGP

Le protocole BGP (Border Gateway Protocol) permet à un routeur en amont d'équilibrer la charge du trafic entre deux serveurs virtuels identiques hébergés sur deux appliances NetScaler autonomes. La publicité par itinéraire permet à un routeur en amont de suivre les entités du réseau situées derrière le NetScaler.

Prérequis pour IPv6 BGP

Avant de commencer à configurer le protocole BGP IPv6, procédez comme suit :

- Assurez-vous de bien comprendre le protocole BGP IPv6.
- Activez la fonctionnalité IPv6.

Étapes de configuration

Pour configurer BGP afin de publier des routes IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire. Valeurs possibles : 1 à 4 294 967 295.
Neighbor < IPv6 address> remote-as < as-number>	Mettez à jour la table de voisins BGP IPv6 avec l'adresse IPv6 locale du lien du voisin dans le système autonome spécifié.

Commande	Spécifie
Address-family ipv6	Passez en mode de configuration de famille d'adresses.
Neighbor < IPv6 address> activate	Préfixes Exchange pour la famille de routeurs IPv6 entre le pair et le nœud local à l'aide de l'adresse locale du lien.
redistribute kernel	Redistribuez les routes du noyau.
redistribute static	Redistribuez les routes statiques.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor a1bc::102 remote-as 100
NS(config-router)# Address-family ipv6
NS(config-router-af)# Neighbor a1bc::102 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
<!--NeedCopy-->
```

Vérification de la configuration BGP

Vous pouvez utiliser VTYSH pour afficher les paramètres BGP.

Pour afficher les paramètres BGP à l'aide de la ligne de commande VTYSH

À l'invite de commande, tapez :

```
VTYSH
You are now in the VTYSH command prompt. An output similar to the
   following appears:
NS170#
At the VTYSH command prompt, type:
NS170# sh ip BGP
NS170# sh BGP
NS170# sh ip BGP neighbors
NS170# sh ip BGP summary
NS170# sh ip BGP route-map <map-tag>
<!--NeedCopy-->
```


As-Override Support in Border Gateway Protocol

Dans le cadre de la fonctionnalité de prévention de boucle BGP, si un routeur reçoit un paquet BGP contenant le numéro de système autonome (ASN) du routeur dans le chemin des systèmes autonomes (AS), le routeur supprime le paquet. L'hypothèse est que le paquet provient du routeur et a atteint l'endroit d'où il provient.

Si une entreprise possède plusieurs sites avec un même ASN, la prévention des boucles BGP empêche les sites ayant un ASN identique d'être liés par un autre ASN. Les mises à jour de routage (paquets BGP) sont supprimées lorsqu'un autre site les reçoit.

Pour résoudre ce problème, la fonctionnalité BGP AS-Override a été ajoutée au module de routage ZebOS BGP de NetScaler.

Lorsque l'AS-Override est activé pour un appareil homologue, lorsque l'appliance NetScaler reçoit un paquet BGP à transférer vers l'homologue et que l'ASN du paquet correspond à celui de l'homologue, l'appliance remplace l'ASN du paquet BGP par son propre numéro ASN avant de transférer le paquet.

Vous pouvez activer AS-Override pour un voisin spécifique ou un groupe de voisins (groupe de pairs) à l'aide de la ligne de commande VTYSH.

Pour configurer BGP AS-Override pour un voisin IPv4 à l'aide de la ligne de commande VTYSH :

Commande	Spécifie
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire.
Neighbor < IPv4 address> remote-as < as-number>	Mettez à jour la table de voisins BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.
Neighbor <IPv4 address> as-override	Activez BGP en tant que remplacement pour le voisin spécifié.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# Neighbor 192.0.2.100 remote-as 100
4      NS(config-router)# Neighbor 10.102.29.100 as-override
5  <!--NeedCopy-->
```

Pour configurer BGP AS-Override pour un groupe de pairs BGP IPv4 à l'aide de la ligne de commande VTYSH :

Commande	Spécifie
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire.
Neighbor <peer group name> **peer-group**	Créez un groupe de pairs BGP.
Neighbot <IPv4 address> **peer-group** <peer group name>	Associez des voisins au groupe de pairs spécifié.
Neighbor <peer group name> remote-as < as-number>	Mettez à jour la table de voisins BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.
Neighbor <peer group name> as-override	Activez BGP en tant que remplacement pour tous les voisins associés au groupe de pairs spécifié.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# neighbor external-peers-1 peer-group
4      NS(config-router)# neighbor 192.0.2.101 peer-group external-peers-1
5      NS(config-router)# neighbor 192.0.2.102 peer-group external-peers-1
6      NS(config-router)# neighbor 192.0.2.103 peer-group external-peers-1
7      NS(config-router)# Neighbor external-peers-1 remote-as 100
8      NS(config-router)# Neighbor external-peers-1 as-override
9  <!--NeedCopy-->
```

Pour configurer BGP AS-Override pour un voisin IPv6 à l'aide de la ligne de commande VTYSH :

Commande	Spécifie
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire.
Neighbor < IPv6 address> remote-as < as-number>	Mettez à jour la table de voisins BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.
Neighbor <IPv6 address> as-override	Activez BGP en tant que remplacement pour le voisin spécifié.

Commande	Spécifie
Address-family ipv6	Passez en mode de configuration de famille d'adresses.
Neighbor < IPv6 address> activate	Échangez les préfixes de la famille de routeurs IPv6 entre le voisin spécifié et NetScaler à l'aide de l'adresse locale du lien.
Neighbor <IPv6 address> as-override	Activez BGP en tant que remplacement pour le voisin spécifié.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# Neighbor a1bc::102 remote-as 100
4      NS(config-router)# Neighbor a1bc::102 as-override
5      NS(config-router)# Address-family ipv6
6      NS(config-router-af)# Neighbor a1bc::102 activate
7      NS(config-router)# Neighbor a1bc::102 as-override
8  <!--NeedCopy-->
```

Pour configurer BGP AS-Override pour un groupe de pairs IPv6 à l'aide de la ligne de commande VTYSH :

Commande	Spécifie
configure terminal	Entrer en mode de configuration globale.
router BGP < ASnumber>	Système autonome BGP. < ASnumber> est un paramètre obligatoire.
Neighbor <peer group name> **peer-group**	Créez un groupe de pairs BGP.
Neighbor <IPv6 address> **peer-group** <peer group name>	Associez un voisin au groupe de pairs spécifié.
Neighbor <peer group name> remote-as < as-number>	Mettez à jour la table de voisins BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.
Neighbor <peer group name> as-override	Activez BGP en tant que remplacement pour tous les voisins associés au groupe de pairs spécifié.
Address-family ipv6	Passez en mode de configuration de famille d'adresses.

Commande	Spécifie
Neighbor <peer group name> activate	Échangez les préfixes de la famille de routeurs IPv6 entre les voisins du groupe d'homologues spécifié et NetScaler à l'aide de l'adresse locale du lien.
Neighbor <peer group name> as-override	Activez BGP en tant que remplacement pour tous les voisins associés au groupe de pairs spécifié.

```
    > VTYSH NS# configure terminal
    NS(config)# router BGP 200
    NS(config-router)# neighbor external-peers-2 peer-group
    NS(config-router)# neighbor 2001::1 peer-group external-peers-2
    NS(config-router)# neighbor 2001::2 peer-group external-peers-2
    NS(config-router)# Neighbor external-peers-2 remote-as 100
    NS(config-router)# Neighbor external-peers-2 as-override
    NS(config-router)# Address-family ipv6
    NS(config-router-af)# Neighbor external-peers-2 activate
    NS(config-router)# Neighbor external-peers-2 as-override
<!--NeedCopy-->
```

Redémarrage gracieux

Dans une configuration haute disponibilité (HA) non INC dans laquelle un protocole de routage est configuré, après un basculement, les protocoles de routage convergent et les routes entre le nouveau nœud principal et les routeurs voisins adjacents sont apprises. L'apprentissage par voie prend un certain temps. Pendant ce temps, le transfert des paquets est retardé, les performances du réseau peuvent être perturbées et les paquets peuvent être abandonnés.

Le redémarrage progressif permet à une configuration HA lors d'un basculement d'ordonner à ses routeurs adjacents de ne pas supprimer les routes apprises de l'ancien nœud principal de leurs bases de données de routage. En utilisant les informations de routage de l'ancien nœud principal, le nouveau nœud principal et les routeurs adjacents commencent immédiatement à transférer des paquets, sans perturber les performances du réseau.

> **Remarque :**
>
> Le redémarrage progressif n'est pas pris en charge pour les configurations haute disponibilité en mode INC.

Configuration du redémarrage progressif pour BGP

Pour configurer le redémarrage progressif pour BGP à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
VTYSH	VTYSH	Saisit l'invite de commande VTYSH.
configure terminal	NS# configure terminal	Entre en mode de configuration globale.
router-id <ID>	NS(config)# router-id 1.1.1.1	Un identifiant de routeur pour l'appliance NetScaler. Cet identifiant est défini pour tous les protocoles de routage dynamique. Le même identifiant doit être spécifié sur l'autre nœud dans une configuration haute disponibilité pour que le redémarrage progressif fonctionne correctement.
router bgp <AS-number>	NS(config)# router bgp 5	Passe en mode de configuration BGP.
bgp graceful-restart	NS(config)# bgp graceful-restart	Permet un redémarrage progressif du processus de routage BGP.
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Spécifie la période de grâce, en secondes, pendant laquelle les routeurs d'assistance attendent une connexion TCP à partir du nouveau nœud principal après un basculement. Pendant ce temps, les routeurs d'assistance conservent les itinéraires.

Commande	Exemple	Description de la commande
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Spécifie la durée, en secondes, pendant laquelle l'appliance NetScaler en mode assistant conserve les itinéraires obsolètes pour le redémarrage des routeurs voisins. La valeur par défaut est 360 secondes.
neighbor <IPv4 address of the peer router> remote-as <AS-number>	NS(config-router)# neighbor 192.0.2.30 remote-as 2	Établit l'appairage BGP avec le routeur voisin spécifié.
neighbor <IPv4 address of the peer router> capability graceful-restart	NS(config-router)# neighbor 192.0.2.30 capability graceful-restart	Permet un redémarrage progressif avec le voisin spécifié.
redistribute kernel	NS(config-router)# redistribute kernel	Redistribue les routes du noyau.

Configuration du redémarrage progressif pour IPv6 BGP

Pour configurer le redémarrage progressif pour IPv6 BGP à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
VTYSH	VTYSH	Saisit l'invite de commande VTYSH.
configure terminal	NS# configure terminal	Entre en mode de configuration globale.

Commande	Exemple	Description de la commande
router-id <id>	NS(config)# router-id 1.1.1.1	Définit un identifiant de routeur pour l'appliance NetScaler. Cet identifiant est défini pour tous les protocoles de routage dynamique. Le même ID doit être spécifié dans l'autre nœud dans une configuration haute disponibilité pour que le redémarrage progressif fonctionne correctement.
router bgp <AS-number>	NS(config)# router bgp 5	Passe en mode de configuration pour le protocole BGP.
bgp graceful-restart	NS(config)# bgp graceful-restart	Permet un redémarrage progressif du processus de routage BGP.
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Spécifie la période de grâce, en secondes, pendant laquelle les routeurs d'assistance attendent une connexion TCP à partir du nouveau nœud principal après un basculement. Pendant ce temps, les routeurs d'assistance conservent les itinéraires. La valeur par défaut est 360 secondes.

Commande	Exemple	Description de la commande
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Spécifie la durée, en secondes, pendant laquelle l'appliance NetScaler en mode assistant conserve les itinéraires obsolètes pour le redémarrage des routeurs voisins. La valeur par défaut est 360 secondes.
neighbor <IPv6 address> remote-as <AS-number>	NS(config-router)# neighbor 2001:db8::10 remote-as 2	Établit l'appairage BGP avec le routeur voisin spécifié.
address-family ipv6	NS(config-router)#address-family ipv6	Entre en mode de configuration de famille d'adresses.
neighbor <IPv6 address of the neighbor> activate	NS(config-router-af)#neighbor 2001:db8::10 activate	Permet l'échange d'itinéraires de famille d'adresses avec le périphérique routeur voisin spécifié.
neighbor <IPv6 address of the neighbor> capability graceful-restart	NS(config-router-af)#neighbor 2001:db8::10 capability graceful-restart	Permet un redémarrage progressif avec le routeur voisin spécifié.
redistribute kernel	NS(config-router-af)#redistribute kernel	Redistribue les routes du noyau.
exit-address-family	NS(config-router-af)#exit-address-family	Quitte le mode de configuration de la famille d'adresses

Configuration de l'authentification MD5 pour IPv4 BGP

L'appliance NetScaler prend en charge l'authentification MD5 pour le protocole BGP (Border Gateway Protocol). Lorsque l'authentification est activée, tout segment TCP appartenant au BGP échangé entre l'appliance NetScaler et son appareil homologue est vérifié et accepté uniquement si l'authentification est réussie. Pour que l'authentification soit réussie, les deux homologues doivent être configurés avec le même mot de passe MD5. Si l'authentification échoue, la relation de voisinage BGP n'est pas établie. La prise en charge de l'authentification MD5 pour BGP dans l'appliance NetScaler est conforme à la RFC 2385.

Avant de commencer

Avant de commencer à configurer l'authentification BGP MD5, tenez compte des points suivants :

- Assurez-vous de bien comprendre les différents composants de l'authentification BGP MD5, décrits dans la RFC 2385.
- L'authentification BGP MD5 n'est pas prise en charge pour les partitions d'administration NetScaler.
- L'authentification BGP MD5 n'est pas prise en charge pour les configurations BGP IPv6.
- L'authentification BGP MD5 est prise en charge pour les configurations de clusters NetScaler ainsi que pour les configurations de haute disponibilité.
- En raison du problème suivant dans FreeBSD, Citrix recommande de définir des valeurs de durée de vie et de maintien faibles (par exemple, 5 et 15) et de configurer un redémarrage progressif pour une session BGP dans une configuration haute disponibilité de couche 2. Sinon, lorsque l'authentification MD5 est activée, BGP peut prendre plus de temps pour rétablir une connexion avec le voisin après un basculement.
  - Le dernier ACK de FreeBSD ne contient pas de condensé md5 :
    * https://forums.freebsd.org/threads/11170/
    * http://support.pfsense.narkive.com/povrH5HI/bgp-md5-weird-behavior-when-connection-closes

Étapes de configuration

Pour configurer l'authentification MD5 pour IPv4 BGP à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
vtysh	Affiche l'invite de commande VTYSH.
configure terminal	Entre en mode de configuration globale.
router bgp <AS-number>	Passe en mode de configuration pour le protocole BGP. <AS-number>est un numéro de système autonome BGP et est un paramètre obligatoire.
Voisin <neighbour IPv4 address>à distance < AS-number >	Met à jour la table BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.

Commande	Spécifie
mot de < neighbour IPv4 address > passe voisin < password in double quotes>	Configure l'authentification MD5 pour le voisin spécifié avec le mot de passe MD5 spécifié. Pour que l'authentification MD5 réussisse, vous devez configurer le même mot de passe MD5 sur l'appliance NetScaler et sur l'appliance voisine.

```
> vtysh

ns# configure terminal

ns(config)#router bgp 5

ns(config-router)#neighbor 20.20.20.138 remote-as 1

ns(config-router)#neighbor 20.20.20.138 password  “secret”

ns(config-router)#redistribute kernel

ns(config-router)#exit

<!--NeedCopy-->
```

Configuration des ASN BGP 4 octets aux formats asplain et asdot

L'appliance NetScaler prend en charge la configuration et l'affichage de numéros de système autonomes (ASN) BGP à 4 octets au format asplain ou asdot, comme défini dans la RFC 5396.

- **asplain**. Notation de valeur décimale dans laquelle les ASN de 2 et 4 octets sont représentés en valeur décimale. Par exemple, 65527 est un ASN de 2 octets et 234567 est un ASN de 4 octets.
- **asdot** Notation par points du système autonome où les ASN de 2 octets sont représentés en valeur décimale (comme dans asplain) et les ASN de 4 octets sont représentés par une notation à points. Par exemple, 65527 est un ASN de 2 octets et 3,37959 est un ASN de 4 octets. (3,37959 est un format asdot pour le nombre décimal 234567).

Exemples de configuration BGP ASN aux formats asplain et asdot

Par défaut, l'appliance NetScaler affiche les ASN BGP au format asplain, mais vous pouvez configurer pour qu'ils s'affichent au format asdot. Vous pouvez configurer des ASN BGP locaux et distants au

format asplain ou asdot.

Voici quelques exemples de configuration BGP ASN aux formats asplain et asdot :

- Affiche le numéro AS BGP dans un format simple. Par défaut, l'appliance NetScaler affiche le numéro BGP AS dans un format simple.

```
ns#conf t
ns(config)# router bgp 196908
ns(config-router)# end
ns#
ns# sh run router bgp
!
router bgp 196908
!
<!--NeedCopy-->
```

- Affiche le numéro AS BGP au format asdot. Exécutez la `asnotation-dot` commande bgp pour afficher le numéro AS BGP au format asdot.

```
ns#conf t
ns(config)#router bgp 196908
ns(config-router)#bgp asnotation-dot
ns(config-router)#end
ns#
ns#sh run router bgp
!
router bgp 3.300
bgp asnotation-dot
!
<!--NeedCopy-->
```

- Configurez et affichez le numéro AS BGP au format asdot. Exécutez la `bgp asnotation-dot` commande pour afficher le numéro AS BGP au format asdot.

```
ns# conf t
ns(config)# router bgp 3.300
ns(config-router)# bgp asnotation-dot
ns#
ns# sh run router bgp
!
router bgp 3.300
bgp asnotation-dot
!
<!--NeedCopy-->
```


- Afficher le numéro AS BGP au format asplain à partir du format asdot. Exécutez la `no asnotation-dot` commande bgp pour afficher le numéro AS BGP au format asplain.

```
ns#conf t
ns(config)#router bgp 3.300
ns(config-router)#no bgp asnotation-dot
ns(config-router)#end
ns#

ns#sh run router bgp
!
router bgp 196908
!
<!--NeedCopy-->
```

- Configurez et affichez le numéro as-number distant au format asdot. Exécutez la commande `bgp asnotation-dot`. Dans l'exemple de configuration, le numéro d'appel distant 80000 est configuré au format asdot 1.14464.

```
ns# conf t
ns(config)# router bgp 3.300
ns(config-router)# bgp asnotation-dot
ns(config-router)# neighbor 192.168.1.2 remote-as 1.14464
ns(config-router)#end
ns#
ns#
ns#sh run router bgp
!
router bgp 3.300
bgp asnotation-dot
neighbor 192.168.1.2 remote-as 1.14464
!
ns#
<!--NeedCopy-->
```

- Afficher les numéros AS locaux et distants BGP au format asplain à partir du format asdot. Exécutez la commande `no asnotation-dot` bgp.

```
ns#conf t
ns(config)#router bgp 3.300
ns(config-router)#no bgp asnotation-dot
ns(config-router)#end
ns#

ns#sh run router bgp
```



```
!
router bgp 196908
neighbor 192.168.1.2 remote-as 80000
!
ns#
<!--NeedCopy-->
```

> **Remarque :**
>
> Au lieu de configurer pour des voisins BGP individuels, la même configuration asplain ou asdot peut également être utilisée pour les groupes de pairs BGP.

Configuration du RIP IPv6

May 5, 2023

Le protocole RIP (IPv6 Routing Information Protocol) ou RIPng est un protocole à vecteur de distance. Ce protocole est une extension du RIP pour prendre en charge le protocole IPv6. Après avoir activé IPv6 RIP, vous devez configurer la publicité des routes RIP IPv6. Pour résoudre les problèmes, vous pouvez limiter la propagation du protocole RIP IPv6. Vous pouvez afficher les paramètres RIP IPv6 pour vérifier la configuration.

Prérequis pour IPv6 RIP

Avant de commencer à configurer IPv6 RIP, procédez comme suit :

- Assurez-vous de bien comprendre le protocole IPv6 RIP.
- Installez la licence IPv6 sur l'appliance NetScaler.
- Activez la fonctionnalité IPv6.

Itinéraires RIP IPv6 publicitaires

Le RIP IPv6 permet à un routeur en amont d'équilibrer la charge du trafic entre deux serveurs virtuels identiques hébergés sur deux appareils NetScaler autonomes. La publicité d'itinéraire permet à un routeur en amont de suivre les entités du réseau situées derrière le NetScaler.

Pour configurer IPv6 RIP afin de publier des itinéraires IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
routeur ipv6 rip	Démarrez le processus de routage IPv6 RIP et entrez en mode de configuration pour le processus de routage.
redistribute static	Redistribuez les routes statiques.
redistribute kernel	Redistribuez les routes du noyau.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Limiter les propagations RIP IPv6

Si vous devez résoudre des problèmes de configuration, vous pouvez configurer le mode écoute uniquement sur n'importe quelle interface.

Pour limiter la propagation du RIP IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
routeur ipv6 rip	Démarrez le processus de routage IPv6 RIP et entrez en mode de configuration pour le processus de routage.
passive-interface < vlan_name>	Supprime les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Vérification de la configuration RIP IPv6

Vous pouvez utiliser VTYSH pour afficher la table de routage IPv6 RIP et les informations RIP IPv6 pour un VLAN spécifié.

Pour afficher les paramètres RIP IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commandes	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
Rip IPv6 SSH	Afficher la table de routage RIP IPv6 mise à jour.
interface Rip sh IPv6 <vlan_name>	Afficher les informations RIP IPv6 pour le VLAN spécifié.

Exemple :

```
NS# VTYSH
NS# sh ipv6 rip
NS# sh ipv6 rip interface VLAN0
<!--NeedCopy-->
```

Configuration de l'OSPF IPv6

May 5, 2023

IPv6 OSPF ou OSPF version 3 (OSPF v3) est un protocole d'état de liaison utilisé pour échanger des informations de routage IPv6. Après avoir activé l'OSPF IPv6, vous devez configurer la publication des routes OSPF IPv6. Pour le dépannage, vous pouvez limiter la propagation OSPF IPv6. Vous pouvez afficher les paramètres OSPF IPv6 pour vérifier la configuration.

Prérequis pour IPv6 OSPF

Avant de commencer à configurer IPv6 OSPF, procédez comme suit :

- Assurez-vous de bien comprendre le protocole OSPF IPv6.
- Installez la licence IPv6 sur l'appliance NetScaler.
- Activez la fonctionnalité IPv6.

Routes IPv6 publicitaires

L'IPv6 OSPF permet à un routeur en amont d'équilibrer la charge du trafic entre deux serveurs virtuels identiques hébergés sur deux appareils NetScaler autonomes. La publicité par itinéraire permet à un routeur en amont de suivre les entités du réseau situées derrière le NetScaler.

Pour configurer IPv6 OSPF afin de publier des routes IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commandes	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
routeur IPv6 OSPF	Démarrez le processus de routage OSPF IPv6 et passez en mode de configuration pour le processus de routage.
redistribute static	Redistribuez les routes statiques.
redistribute kernel	Redistribuez les routes du noyau.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Limitation des propagations OSPF IPv6

Si vous devez dépanner votre configuration, vous utilisez VTYSH pour configurer le mode d'écoute uniquement sur un VLAN donné.

Pour limiter la propagation OSPF IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commandes	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
routeur IPv6 OSPF	Démarrez le processus de routage OSPF IPv6 et passez en mode de configuration pour le processus de routage.
interface passive < vlan_name >	Supprime les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Vérification de la configuration OSPF IPv6

Vous utilisez VTYSH pour afficher les voisins actuels OSPF IPv6 et les routes OSPF IPv6.

Pour afficher les paramètres OSPF IPv6 à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
Voisin OSPF sh ipv6	Affiche les voisins actuels.
route OSPF sh ipv6	Affiche les routes OSPF IPv6.

Exemple :

```
>VTYSH
NS# sh ipv6 OSPF neighbor
NS# sh ipv6 OSPF route
```



```
<!--NeedCopy-->
```

Authentification OSPFv3

Pour garantir l'intégrité, l'authentification de l'origine des données et la confidentialité des données des paquets OSPFv3, l'authentification OSPFv3 doit être configurée sur des homologues OSPFv3.

L'appliance NetScaler prend en charge l'authentification OSPFv3 et est partiellement conforme à la RFC 4552. L'authentification OSPFv3 est basée sur les deux protocoles IPsec : Authentication Header (AH) et Encapsulating Security Payload (ESP). L'appliance NetScaler prend uniquement en charge le protocole AH pour l'authentification OSPFv3.

L'authentification OSPFv3 utilise des associations de sécurité (SA) IPsec définies manuellement entre les pairs OSPFv3 et ne repose pas sur le protocole IKE pour former des associations de sécurité dynamiques. Les associations de sécurité manuelles définissent les valeurs d'index des paramètres de sécurité (SPI), les algorithmes et les clés à utiliser entre les pairs. Les associations de sécurité manuelles ne nécessitent aucune négociation entre les pairs ; par conséquent, la même association de sécurité doit être définie sur les deux pairs.

Vous pouvez configurer l'authentification OSPFv3 sur un VLAN ou pour une zone OSPFv3. Lorsque vous configurez pour un VLAN, les paramètres sont appliqués à toutes les interfaces qui sont membres du VLAN. Lorsque vous configurez l'authentification OSPFv3 pour une zone OSPF, les paramètres sont appliqués à tous les VLAN de cette zone. Les paramètres sont à leur tour appliqués à toutes les interfaces membres de ces VLAN. Ces paramètres ne s'appliquent pas aux VLAN membres sur lesquels vous avez configuré directement l'authentification OSPFv3.

Tenez compte des points et limites suivants avant de configurer l'authentification OSPFv3 sur une appliance NetScaler :

- Assurez-vous de bien comprendre les différents composants de l'authentification OSPFv3, décrits dans la RFC 4552.
- Seul le protocole Authentication Header est pris en charge pour l'authentification OSPFv3. L'encapsulation de la charge utile de sécurité (ESP) n'est pas prise en charge.
- Vous devez définir une association de sécurité avec le même paramètre sur l'interface homologue.
- La nouvelle saisie des touches manuelles n'est pas prise en charge.

Pour configurer l'authentification OSPFv3 sur un VLAN à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué : commandes VLAN d'authentification OSPFv3.

Exemple :

```
> VTYSH NS# configure terminal
```



```
NS(config)# interface vlan2
NS(config-if)# ipv6 ospf authentication ipsec spi 256 md5 123456789
    ABCDEF0123456789ABCDEF0
<!--NeedCopy-->
```

Pour configurer l'authentification OSPFv3 sur une zone OSPF à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué : Authentification OSPFv3 OSPF Area commandes.

Exemple :

```
> VTYSH NS# configure terminal
ns(config)#router ipv6 ospf 30
ns(config-router)# area 1 authentication ipsec spi 256
    md5123456789ABCDEF0123456789ABCDEF0
<!--NeedCopy-->
```

Configuration du redémarrage progressif pour IPv6 OSPF

Dans une configuration haute disponibilité (HA) non INC dans laquelle un protocole de routage est configuré, après un basculement, les protocoles de routage convergent et les routes entre le nouveau nœud principal et les routeurs voisins adjacents sont apprises. L'apprentissage par voie prend un certain temps. Pendant ce temps, le transfert des paquets est retardé, les performances du réseau peuvent être perturbées et les paquets peuvent être abandonnés.

Le redémarrage progressif permet à une configuration HA lors d'un basculement d'ordonner à ses routeurs adjacents de ne pas supprimer les routes apprises de l'ancien nœud principal de leurs bases de données de routage. En utilisant les informations de routage de l'ancien nœud principal, le nouveau nœud principal et les routeurs adjacents commencent immédiatement à transférer des paquets, sans perturber les performances du réseau.

> **Remarque :**
>
> Le redémarrage progressif n'est pas pris en charge pour les configurations haute disponibilité en mode INC.

Pour configurer le redémarrage progressif pour IPv6 OSPF à l'aide de la ligne de commande VTYSH, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
VTYSH	> VTYSH	Saisit l'invite de commande VTYSH.

Commande	Exemple	Description de la commande
configure terminal	NS# configure terminal	Entre en mode de configuration globale.
router-id id>	NS(config)#router-id 1.1.1.1	Définit un identifiant de routeur pour l'appliance NetScaler. Cet identifiant est défini pour tous les protocoles de routage dynamique. Le même ID doit être spécifié dans l'autre nœud dans une configuration haute disponibilité configurée pour que le redémarrage progressif fonctionne correctement dans la configuration HA.
IPv6ospf restart grace-period <1-1800>	NS(config)# IPv6ospf restart grace-period 170	Spécifie la période de grâce, en secondes, pendant laquelle les itinéraires doivent être conservés dans les dispositifs d'assistance. Valeur par défaut : 120 secondes.
IPv6 ospf restart helper max-grace-period <1-1800>	NS(config)# IPv6 ospf restart helper max-grace-period 180	Il s'agit d'une commande facultative visant à limiter la période de grâce maximale pendant laquelle l'appliance NetScaler sera en mode assistant. Si l'appliance NetScaler reçoit un LSA opaque dont la période de grâce est supérieure à la période de grâce maximale définie pour l'assistant, le LSA est supprimé et NetScaler n'est pas placé en mode auxiliaire.

Commande	Exemple	Description de la commande
interface <VLANID>	NS(config)#interface vlan3	Passe en mode de configuration VLAN.
ipv6 router ospf area <area_id> tag <tag_id>	NS(config-if)#ipv6 router ospf area 0 tag 1	Démarre le processus de routage OSPF IPv6 sur un VLAN.
exit	NS(config-if)#exit	Quitte le mode de configuration VLAN.
router ipv6 ospf	NS(config)# router ipv6 ospf 1	Démarre le processus de routage OSPF IPv6 et passe en mode de configuration pour le processus de routage.
capability restart graceful	NS(config-router)#capability restart graceful	Permet un redémarrage progressif du processus de routage OSPF IPv6.
redistribute kernel	NS(config-router)# redistribute kernel	Redistribue les routes du noyau.

Configuration d'ISIS

May 5, 2023

L'appliance NetScaler prend en charge le protocole de routage dynamique de système à système intermédiaire (IS-IS ou ISIS). Ce protocole prend en charge les échanges de routes IPv4 et IPv6. L'IS-IS est un protocole d'état de liaison et est donc moins sujet aux boucles de routage. Avec les avantages d'une convergence plus rapide et de sa capacité à prendre en charge des réseaux plus étendus, ISIS peut s'avérer très utile dans les réseaux de fournisseurs d'accès à Internet (ISP).

Conditions préalables à la configuration d'ISIS

Avant de commencer à configurer ISIS, procédez comme suit :

- Assurez-vous de bien comprendre le protocole ISIS.
- Pour les itinéraires IPV6, activez :
  - Fonctionnalité de traduction du protocole IPv6.
  - Option de routage dynamique IPv6 sur les VLAN sur lesquels vous souhaitez exécuter le protocole ISIS.

Permettre à ISIS

Utilisez l'une des procédures suivantes pour activer la fonctionnalité de routage ISIS sur l'appliance NetScaler.

Pour activer le routage ISIS à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

activer la fonctionnalité NS ISIS

Pour activer le routage ISIS à l'aide de l'interface graphique :

1. Accédez à Système > Paramètres, dans le groupe Modes et fonctionnalités, cliquez sur Modifier les fonctionnalités avancées.
2. Sélectionnez ou désactivez l'option de routage ISIS.

Création d'un processus de routage ISIS et démarrage de celui-ci sur un VLAN

Pour créer un processus de routage ISIS, vous devez utiliser la ligne de commande VTYSH.

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Description
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entre dans le mode de configuration global.
routeur ISIS [tag]	Crée un processus de routage ISIS et un mode de configuration pour le processus de routage.
prochain XX… XXXX.YYYYY.YYYYY.YYYYY.00	**Spécifie une valeur NET pour le processus de routage, où :** · XX… .XXXX**est l'adresse de zone (peut être comprise entre 1 et 13 octets),** · YYYY.YYYYY est l'ID système (6 octets), · 00**est le sélecteur N (1 octet).**
is-type (niveau 1|niveau 1-2 | niveau 2 uniquement)	Définit le processus de routage ISIS au niveau de routage spécifié. Par défaut : niveau 1-2.
Routage IPv6 ns	Démarre le démon de routage dynamique IPv6.
interface <vlan_name>	Passe en mode de configuration VLAN.
routeur IP ISIS	Active le processus de routage ISIS sur le VLAN pour les échanges de routes IPv4.
routeur IPv6 ISIS	Active le processus de routage ISIS sur le VLAN pour les échanges de routes IPv6.

Exemple :

```
> VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# net 15.aabb.ccdd.0097.00
NS(config-router)# is-type level-1
NS(config-router)# exit
NS(config)# ns IPv6-routing
NS(config)# interface vlan0
NS(config-if)#  ip router isis 11
NS(config-if)# ipv6 router isis 11
<!--NeedCopy-->
```

Itinéraires publicitaires

La publicité des itinéraires permet à un routeur en amont de suivre les entités du réseau situées derrière l'appliance NetScaler.

Pour configurer ISIS afin de publier des itinéraires à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Description
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entre dans le mode de configuration global.
routeur ISIS [tag]	Démarre l'instance de routage ISIS et passe en mode de configuration pour le processus de routage.
redistribuer connecté (niveau 1 ou niveau 1-2 ou niveau 2)	**Redistribue les itinéraires connectés, où :**niveau 1 : redistribue les itinéraires connectés au niveau 1**, niveau**1-2 : redistribue les itinéraires connectés au niveau 1 et au niveau 2, niveau 2**: redistribue les itinéraires connectés au niveau 2.**
redistribuer le noyau (niveau 1 ou niveau 1-2 ou niveau 2)	**Redistribue les routes du noyau, où :**niveau 1 : redistribue les routes du noyau au niveau 1**, niveau**1-2 : Redistribue les routes du noyau au niveau 1 et au niveau 2, niveau 2**: redistribue les routes du noyau au niveau 2.**

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# redistribute connected level-1
NS(config-router)# redistribute kernel level-1
<!--NeedCopy-->
```

Limiter la propagation de l'EIIS

Si vous devez résoudre des problèmes de configuration, vous pouvez configurer le mode d'écoute uniquement sur n'importe quel VLAN donné.

Pour limiter la propagation d'ISIS à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Description
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entre dans le mode de configuration global.
router isis [tag]	Passe en mode de configuration pour le processus de routage.
interface passive <vlan_name>	Supprime les mises à jour de routage sur les interfaces liées au VLAN spécifié.

Exemple :

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Vérification de la configuration ISIS

Vous pouvez utiliser VTYSH pour afficher la table de routage ISIS et les informations ISIS pour un VLAN spécifié.

Pour afficher les paramètres ISIS à l'aide de la ligne de commande VTYSH :

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commandes	Description
VTYSH	Affiche l'invite de commande VTYSH.
Afficher son itinéraire	Affiche la table de routage ISIS IPv4 mise à jour.
afficher l'itinéraire IPv6 ISIS	Affiche la table de routage ISIS IPv6 mise à jour.
interface sh isis <vlan_name>	Affiche les informations ISIS IPv6 pour le VLAN spécifié.

Exemple :

```
NS# VTYSH
NS#  show ip isis route
NS#  show ipv6 isis route
NS# sh isis interface VLAN0
<!--NeedCopy-->
```

Installer des routes vers la table de routage NetScaler

May 5, 2023

L'appliance NetScaler peut utiliser des routes apprises par différents protocoles de routage une fois que vous les avez installées dans la table de routage de l'appliance.

Pour installer différentes routes vers la table de routage interne à l'aide de la ligne de commande VTYSH :

Dans l'interface de ligne de commande, tapez les commandes suivantes en fonction des routes que vous souhaitez installer :

Commandes	Spécifie
VTYSH	Affiche l'invite de commande VTYSH.
configure terminal	Entrer en mode de configuration globale.
ns route-install (par défaut)	Installez les routes IPv4 par défaut vers la table de routage interne.
DNS route-install RIP	Installez des routes spécifiques au RIP IPv4 vers la table de routage interne.

Commandes	Spécifie
BGP ns route-install	Installez les routes spécifiques IPv4 BGP vers la table de routage interne.
ns route-install OSPF	Installez des routes spécifiques IPv4 OSPF vers la table de routage interne.
ns route-install IPv6 (par défaut)	Installez les routes IPv6 par défaut vers la table de routage interne.
ns route-install IPv6 RIP	Installez des routes spécifiques au RIP IPv6 vers la table de routage interne.
ns route-install IPv6 BGP	Installez des routes BGP IPv6 spécifiques vers la table de routage interne.
ns route-install IPv6 OSPF	Installez des routes spécifiques IPv6 OSPF vers la table de routage interne.

Exemple :

```
>VTYSH
NS# configure terminal
NS# ns route-install Default
NS(config)# ns route-install RIP
NS(config)# ns route-install BGP
NS(config)# ns route-install OSPF
NS# ns route-install IPv6 Default
NS(config)# ns route-install IPv6 RIP
NS(config)# ns route-install IPv6 BGP
NS(config)# ns route-install IPv6 OSPF
<!--NeedCopy-->
```

Nombre maximum de routes ECMP prises en charge dans une appliance NetScaler

Dans une appliance NetScaler, jusqu'à 32 itinéraires ECMP (Equal Cost Multiple Path) sont pris en charge. La sélection de l'itinéraire est basée sur cinq tuples. Pour plus d'informations, voir Sélection d'itinéraires basée sur cinq tuples.

Publication des itinéraires SNIP et VIP vers des zones sélectives

January 21, 2021

Pour annoncer certaines adresses SNIP dans des zones sélectives, l'activation du mode DRADV ou la redistribution des opérations ZebOSS de connexion ne peut pas être utilisée. En effet, ces opérations envoient toutes les routes connectées à ZebOS. En outre, ajouter des routes statiques factices dans ZebOS pour les sous-réseaux requis, ou ajouter des ACL dans ZebOS pour filtrer les routes connectées non désirées, est une tâche lourde et fastidieuse.

Les options Route réseau et Balise permettent de résoudre ce problème. Vous pouvez activer l'option Route réseau pour une seule adresse SNIP par sous-réseau. L'itinéraire connecté pour cette adresse SNIP est envoyé en tant que route du noyau vers ZebOSS.

Pour les adresses VIP et SNIP, Tag, peut recevoir un entier compris entre 1 et 4294967295. Ce paramètre peut être défini uniquement lorsque l'option Route hôte ou Route réseau est activée pour les adresses VIP ou SNIP. La valeur de balise associée aux adresses VIP et SNIP est également envoyée avec leurs itinéraires vers ZebOS. Les balises avec différentes valeurs peuvent être définies pour les routes VIP et SNIP. Ces valeurs de balise peuvent ensuite être appariées dans les cartes de route dans les ZebOS et annoncées dans des zones sélectives.

Publicité des itinéraires SNIP vers des zones sélectives

Pour configurer les paramètres de routage réseau et de balise d'une adresse SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- Si vous ajoutez une nouvelle adresse SNIP :
  - **add ns ip** <IPAddress>@ <netmask> -**type SNIP** -**networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **montrer ns ip** <IPAddress>
- Si vous reconfigurez une adresse SNIP existante :
  - **set ns ip** <IPAddress>@ <netmask> -**type SNIP** - **networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **montrer ns ip** <IPAddress>

Pour configurer les paramètres de routage réseau et de balise d'une adresse SNIP à l'aide de l'interface graphique :

1. Accédez à **Système**> **Réseau**> **IP**> **IPv4**.
2. Définissez les paramètres **Route réseau** et **Balise** lors de l'ajout d'une adresse IP de sous-réseau (SNIP) ou de la modification d'une adresse IP de sous-réseau existante.

Annoncer des itinéraires VIP vers des zones sélectives

Pour configurer les paramètres d'itinéraire hôte et de balise d'une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

- Si vous ajoutez une nouvelle adresse VIP :
  - **add ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **montrer ns ip** <IPAddress>
- Si vous reconfigurez une adresse VIP existante :
  - **set ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **montrer ns ip** <IPAddress>

Pour configurer les paramètres d'itinéraire réseau et de balise d'une adresse VIP à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IPs> IPv4**.
2. Définissez les paramètres **Route de l'hôte** et **Tag** lors de l'ajout d'une adresse VIP ou de la modification d'une adresse VIP existante.

Configuration de la détection de transfert bidirectionnel

May 5, 2023

Le protocole de détection bidirectionnelle du transfert (BFD) est un mécanisme permettant de détecter rapidement les défaillances des chemins de transfert. Le BFD détecte les défaillances de chemin en quelques millisecondes. Le BFD est utilisé avec des protocoles de routage dynamique.

En mode BFD, les homologues de routage échangent des paquets BFD à un intervalle négocié. Si aucun paquet n'est reçu d'un homologue dans l'intervalle négocié plus l'intervalle de grâce, l'homologue est considéré comme mort et une notification sera envoyée à l'ensemble des protocoles de routage enregistrés. À leur tour, les protocoles de routage recalculent le meilleur chemin et reprogramment la table de routage. Le BFD prend en charge des intervalles de temps plus courts par rapport aux temporisateurs fournis par les protocoles de routage, ce qui permet une détection plus rapide des défaillances.

L'appliance NetScaler prend en charge le BFD pour les protocoles de routage suivants : BGP (IPv4 et IPv6), OSPFv2 (IPv4) et OSPFv3 (IPv6). La prise en charge du BFD dans l'appliance NetScaler est conforme aux RFC 5880, 5881 et 5883.

Points à prendre en compte pour configurer la détection du transfert bidirectionnel

Avant de commencer à configurer BFD, tenez compte des points suivants :

- Assurez-vous de bien comprendre les différents composants du BFD, décrits dans les RFC 5880, 5881 et 5883.
- Le BFD sur une appliance NetScaler est pris en charge pour les protocoles de routage suivants :
  - BGP (IPv4 et IPv6)
  - OSPFv2 (IPv4)
  - OSPFv3 (IPv6)
- Le BFD sur une appliance NetScaler n'est pas pris en charge pour les protocoles de routage suivants :
  - ISIS
  - RIP (IPv4)
  - RIPNG (IPv6)
- Les fonctionnalités BFD suivantes ne sont pas prises en charge sur une appliance NetScaler :
  - Mode Echo BFD
  - Authentification BFD
  - Mode asynchrone BFD Demand
- Les valeurs minimales pour l'intervalle BFD et les temporisateurs BFD Rx sont de 100 millisecondes.
- Lorsque le BFD est utilisé dans une topologie avec des adresses IP partagées (par exemple, une configuration de haute disponibilité de couche 2 avec des adresses SNIP ou une configuration de cluster avec des adresses IP réparties par bandes), le BFD arrête les sessions actives lors d'un basculement car le temps de détection des défaillances du BFD (de l'ordre des millisecondes) est inférieur à l'intervalle de détection du basculement HA (3 à 4 secondes). Citrix recommande donc d'utiliser le redémarrage progressif dans les topologies HA de couche 2, car les itinéraires sont conservés pendant le processus de basculement.

Étapes de configuration

La configuration de BFD sur une appliance NetScaler comprend les tâches suivantes :

- Configurer les paramètres BFD
- Configurer le support BFD pour les protocoles de routage dynamique

Configurer les paramètres BFD

L'appliance NetScaler fournit des paramètres de session BFD distincts pour les sessions à saut unique, les sessions à sauts multiples IPv4 et les sessions à sauts multiples IPv6. Si vous ne configurez pas les paramètres BFD pour un type de session, les valeurs par défaut sont appliquées à cette session.

La valeur par défaut de chaque paramètre BFD est la même pour les sessions à saut unique, les sessions IPv4 à sauts multiples et les sessions IPv6 à sauts multiples. Le tableau suivant affiche la valeur par défaut de chaque paramètre BFD.

Nom du paramètre BFD	Valeur par défaut
Intervalle	750 millisecondes
Rx minimum	500 millisecondes
Multipliateur	3

> **IMPORTANT :**
>
> Les cartes réseau Mellanox d'une appliance NetScaler ADC mettent environ 1 500 ms à s'initialiser. Vous devez régler les temporisateurs BFD sur plus de 1 500 ms pour une appliance NetScaler dotée de cartes réseau Mellanox. Citrix recommande de régler les temporisateurs BFD sur 3 000 ms :
>
> - Intervalle Tx = 600 ms
> - Rx minimum = 600 ms
> - Multiplicateur = 5

Configuration des paramètres BFD pour une session à saut unique

Pour configurer les paramètres BFD pour une session à saut unique à l'aide de la VTYSH ligne de commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de VTYSH commande.
`configure terminal`	Entrer en mode de configuration globale.
`interface` `vlan ID>`	Entrez dans le mode de configuration de l'interface.
`bfd singlehop-peer interval <num> minrx <num> multiplier <num>`	Configurez les paramètres BFD sur l'interface spécifiée.

Exemple de configuration :

```
1 > vtysh
2
3 ns# configure terminal
```



```
4
5  ns(config)# interface vlan3
6
7  ns(config-if)# bfd singlehop-peer interval 200 minrx 200 multiplier 5
8
9  ns(config-if)# exit
10 <!--NeedCopy-->
```

Configuration des paramètres BFD pour les sessions IPv4 à sauts multiples

Pour configurer les paramètres BFD pour les sessions IPv4 à sauts multiples à l' `VTYSH` aide de la ligne de commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de `VTYSH` commande.
`configure terminal`	Entrer en mode de configuration globale.
`bfd multihop-peer <ipv4addr> interval <num> minrx <num> multiplier <num>`	Configurez les paramètres BFD pour les sessions IPv4 à sauts multiples.

Exemple de configuration :

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)# bfd multihop-peer 20.20.20.138 interval 300 minrx 300
           multiplier 5
6
7      ns(config)# exit
8  <!--NeedCopy-->
```

Configuration des paramètres BFD pour les sessions IPv6 à sauts multiples

Pour configurer les paramètres BFD pour les sessions IPv6 à sauts multiples à l' `VTYSH` aide de la ligne de commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de `VTYSH` commande.
`configure terminal`	Entrer en mode de configuration globale.
`bfd multihop-peer ipv6 <ipv6addr> interval <num> minrx <num> multiplier <num>`	Configurez les paramètres BFD pour les sessions IPv6 à sauts multiples.

Exemple de configuration :

```
1      > vtysh
2
3      ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx
           500 multiplier 5
4
5      ns(config)# exit
6  <!--NeedCopy-->
```

Configurer le support BFD pour les protocoles de routage dynamique

Vous pouvez activer BFD pour un protocole de routage dynamique pour un type de session avec un homologue. Par exemple, saut unique et sauts multiples. L'appliance NetScaler applique les paramètres BFD pertinents à la session.

Configuration de BFD pour une session à saut unique BGP IPv4

Pour configurer BFD pour une session BGP à saut unique IPv4 à l'aide de la ligne de `VTYSH` commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de `VTYSH` commande.
`configure terminal`	Entrer en mode de configuration globale.
`router bgp <asnumber>`	Système autonome BGP. `asnumber` est un paramètre obligatoire.
`neighbor <ipv4addr> remote-as <num>`	Mettez à jour la table BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.

Commande	Spécifie
`neighbor <ipv4addr> fall-over bfd`	Activez BFD pour le voisin spécifié.

Exemple de configuration :

```
    > vtysh

    ns# configure terminal

    ns(config)#router bgp 1

    ns(config-router)#neighbor 20.20.20.138 remote-as 1

    ns(config-router)#neighbor 20.20.20.138 fall-over bfd

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
<!--NeedCopy-->
```

Configuration de BFD pour une session BGP à sauts multiples IPv4

Pour configurer BFD pour une session BGP à sauts multiples IPv4 à l'aide de la ligne de `VTYSH` commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de `VTYSH` commande.
`configure terminal`	Entrer en mode de configuration globale.
`router bgp <asnumber>`	Système autonome BGP. `asnumber` est un paramètre obligatoire.
`neighbor <ipv4addr> remote-as <num>`	Mettez à jour la table BGP IPv4 avec l'adresse IPv4 du voisin dans le système autonome spécifié.
`neighbor <ipv4addr> fall-over bfd multihop`	Activez BFD pour le voisin spécifié.

Exemple de configuration :


```
    > vtysh

    ns# configure terminal

    ns(config)#router bgp 1

    ns(config-router)#neighbor 20.20.20.138 remote-as 1

    ns(config-router)#neighbor 20.20.20.138 fall-over bfd multihop

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
<!--NeedCopy-->
```

Configuration du BFD pour une session IPv6 BGP à saut unique

Pour configurer BFD pour une session IPv6 BGP à saut unique à l'aide de la ligne de `VTYSH` commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de `VTYSH` commande.
`configure terminal`	Entrer en mode de configuration globale.
`router bgp <asnumber>`	Système autonome BGP. `asnumber` est un paramètre obligatoire.
`neighbor <ipv6addr> remote-as <num>`	Mettez à jour la table BGP IPv6 avec l'adresse IPv6 locale du lien du voisin dans le système autonome spécifié.
`neighbor <ipv6addr> fall-over bfd`	Activez BFD pour le voisin spécifié.
`address-family ipv6`	Passez en mode de configuration de famille d'adresses.
`neighbor <ipv6addr> activate`	Préfixes Exchange pour la famille de routeurs IPv6 entre le pair et le nœud local à l'aide de l'adresse locale du lien.

Exemple de configuration :

```
> vtysh
```



```
2
3  ns# configure terminal ns(config)#router bgp 1
4
5  ns(config-router)#neighbor 30fe:123::124 remote-as 1
6
7  ns(config-router)#neighbor 30fe:123::124 fall-over bfd
8
9  ns(config-router)#address-family ipv6
10
11 ns(config-router-af)#neighbor 30fe:123::124 activate
12
13 ns(config-router-af)#redistribute kernel
14
15 ns(config-router-af)#exit
16
17 <!--NeedCopy-->
```

Configuration du BFD pour une session IPv6 BGP à sauts multiples

Pour configurer BFD pour une session IPv6 BGP à sauts multiples à l'aide de la ligne de VTYSH commande, à l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de VTYSH commande.
`configure terminal`	Entrer en mode de configuration globale.
`router bgp <asnumber>`	Système autonome BGP. `asnumber` est un paramètre obligatoire.
`neighbor <ipv6addr> remote-as <num>`	Mettez à jour la table BGP IPv6 avec l'adresse IPv6 locale du lien du voisin dans le système autonome spécifié.
`neighbor <ipv6addr> fall-over bfd multihop`	Activez BFD pour le voisin spécifié.
`address-family ipv6`	Passez en mode de configuration de famille d'adresses.
`neighbor <ipv6addr> activate`	Échangez les préfixes de la famille de routeurs IPv6 entre le pair et le nœud local à l'aide de l'adresse lien-local.

Exemple de configuration :

```
> vtysh

ns# configure terminal

ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx 500
    multiplier 5

ns(config)#router bgp 1

ns(config-router)#neighbor 20fe:125::138 remote-as 1

ns(config-router)#neighbor 20fe:125::138 fall-over bfd multihop

ns(config-router)#address-family ipv6

ns(config-router-af)#neighbor 20fe:125::138 activate

ns(config-router-af)#redistribute kernel

ns(config-router-af)#end

<!--NeedCopy-->
```

Configuration de BFD pour OSPFv2 (IPv4) sur les interfaces

Vous pouvez activer le BFD sur toutes les interfaces ou sur une interface spécifique qui utilise le protocole OSPFv2.

Pour configurer BFD pour OSPFv2 sur toutes les interfaces à l'aide de la ligne de commande : VTYSH

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de `VTYSH` commande.
`configure terminal`	Entrer en mode de configuration globale.
`router ospf <process tag>`	Entrez en mode de configuration OSPFv2.
`bfd all-interfaces`	Activez BFD sur toutes les interfaces qui utilisent OSPFv2.

Exemple de configuration :

```
    > vtysh

    ns# configure terminal

    ns(config)#router ospf 1

    ns(config-router)#bfd all-interfaces

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
<!--NeedCopy-->
```

Pour configurer BFD pour OSPFv2 sur une interface spécifique à l'aide de la ligne de commande :

VTYSH

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de `VTYSH` commande.
`configure terminal`	Entrer en mode de configuration globale.
`interface` `<vlan ID>`	Entrez dans le mode de configuration de l'interface.
`ip ospf bfd`	Activez BFD sur l'interface spécifiée qui utilise OSPFv2.

Exemple de configuration :

```
    > vtysh

    ns# configure terminal

    ns(config)# interface vlan5

    ns(config-if)# ip ospf bfd

    ns(config-if)# exit
<!--NeedCopy-->
```


Configuration de BFD pour OSPFv3 (IPv6) sur les interfaces

Vous pouvez activer le BFD sur toutes les interfaces ou sur une interface spécifique qui utilise le protocole OSPFv3.

Pour configurer BFD pour OSPFv3 sur toutes les interfaces à l'aide de la ligne de commande : VTYSH

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de `VTYSH` commande.
`configure terminal`	Entrer en mode de configuration globale.
`router ipv6 ospf <process tag>`	Entrez en mode de configuration OSPFv3.
`bfd all-interfaces`	Activez BFD sur toutes les interfaces qui utilisent OSPFv3.

Exemple de configuration :

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)#router ipv6 ospf 10
6
7      ns(config-router)#bfd all-interfaces
8
9      ns(config-router)#redistribute kernel
10
11     ns(config-router)#exit
12 <!--NeedCopy-->
```

Pour configurer BFD pour OSPFv3 sur une interface spécifique à l'aide de la ligne de commande : VTYSH

À l'invite de commandes, tapez les commandes suivantes, dans l'ordre indiqué :

Commande	Spécifie
`vtysh`	Afficher l'invite de `VTYSH` commande.
`configure terminal`	Entrer en mode de configuration globale.

Commande	Spécifie
interface <vlan ID>	Entrez dans le mode de configuration de l'interface.
ipv6 ospf bfd	Activez BFD sur l'interface spécifiée qui utilise OSPFv3.

Exemple de configuration :

```
    > vtysh

    ns# configure terminal

    ns(config)# interface vlan15

    ns(config-if)# ipv6 ospf bfd

    ns(config-if)# exit
<!--NeedCopy-->
```

Configuration des itinéraires statiques

May 5, 2023

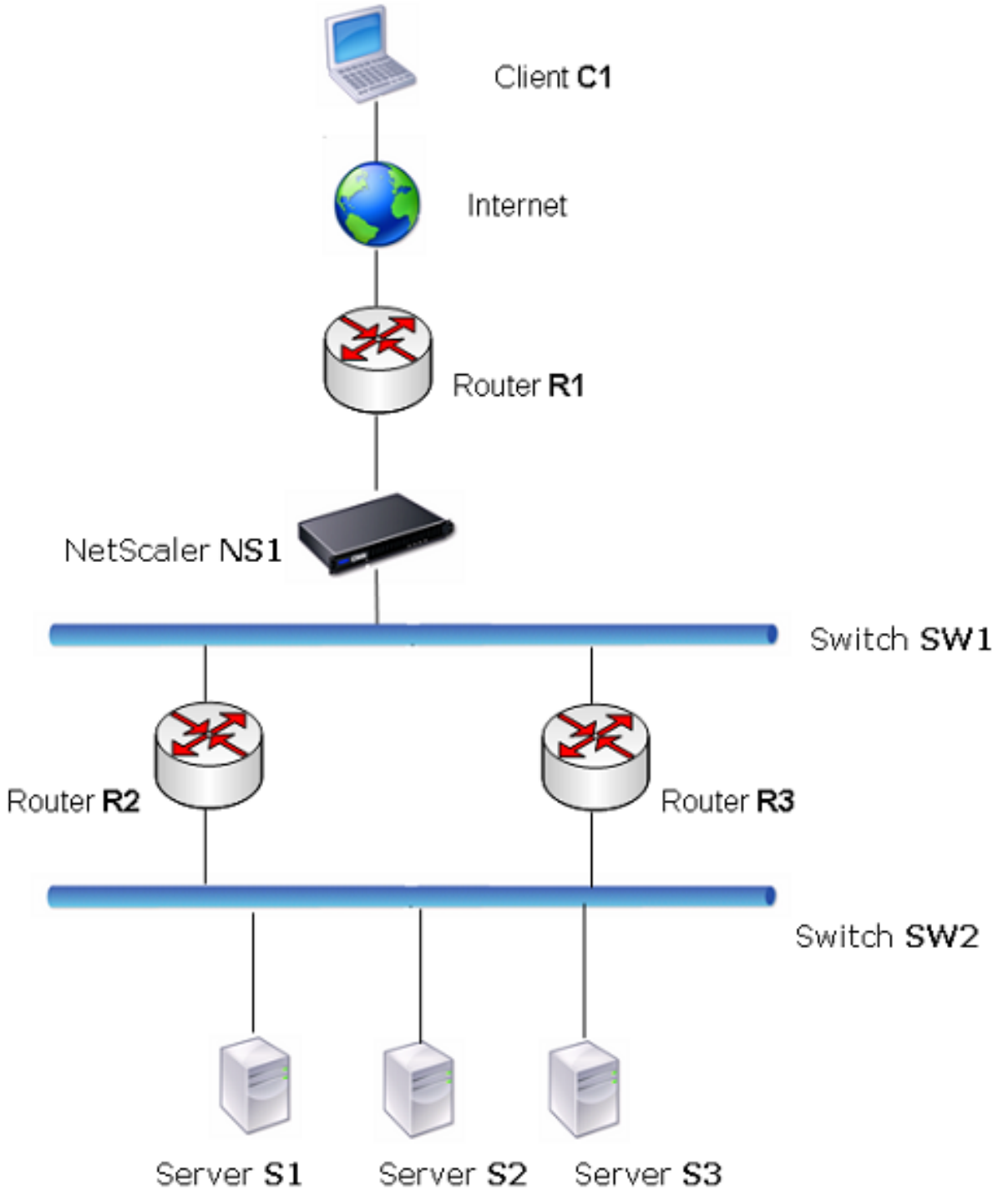
Les routes statiques sont créées manuellement pour améliorer les performances de votre réseau. Vous pouvez surveiller les itinéraires statiques pour éviter les interruptions de service. Vous pouvez également attribuer des poids aux itinéraires ECMP et créer des itinéraires nuls pour empêcher les boucles de routage.

Routes statiques surveillées. Si un itinéraire créé manuellement (statique) tombe en panne, aucun itinéraire de secours n'est automatiquement activé. Vous devez supprimer manuellement l'itinéraire statique principal inactif. Toutefois, si vous configurez l'itinéraire statique en tant que route surveillée, l'appliance NetScaler peut activer automatiquement un itinéraire de sauvegarde.

La surveillance statique des itinéraires peut également être basée sur l'accessibilité du sous-réseau. Un sous-réseau est généralement connecté à une interface unique, mais il est logiquement accessible via d'autres interfaces. Les sous-réseaux liés à un VLAN ne sont accessibles que si le VLAN est actif. Les VLAN sont des interfaces logiques via lesquelles les paquets sont transmis et reçus par NetScaler. Une route statique est marquée comme étant en panne si le saut suivant se trouve sur un sous-réseau inaccessible.

Remarque : Dans une configuration haute disponibilité (HA), la valeur par défaut pour les routes d'état surveillées (MSR) sur le nœud secondaire est UP. La valeur est définie pour éviter un intervalle de transition d'état lors du basculement, qui pourrait entraîner la suppression de paquets sur ces routes.

Examinez la topologie simple suivante, dans laquelle un NetScaler répartit la charge du trafic vers un site sur plusieurs serveurs.



Le routeur R1 déplace le trafic entre le client et l'appliance NetScaler. L'appliance peut accéder aux serveurs S1 et S2 via les routeurs R2 ou R3. Il dispose de deux routes statiques permettant d'accéder

au sous-réseau des serveurs, l'une avec R2 comme passerelle et l'autre avec R3 comme passerelle. La surveillance est activée sur ces deux itinéraires. La distance administrative de la route statique avec la passerelle R2 est inférieure à celle de la route statique avec la passerelle R3. Par conséquent, R2 est préférable à R3 pour transférer le trafic vers les serveurs. De plus, l'itinéraire par défaut sur NetScaler pointe vers R1 afin que tout le trafic Internet quitte correctement.

Si R2 échoue alors que la surveillance est activée sur la route statique, qui utilise R2 comme passerelle, NetScaler la marque comme étant hors service. NetScaler utilise désormais la route statique avec R3 comme passerelle et transfère le trafic vers les serveurs via R3.

NetScaler prend en charge la surveillance des routes statiques IPv4 et IPv6. Vous pouvez configurer NetScaler pour surveiller un itinéraire statique IPv4 en créant un nouveau moniteur ARP ou PING ou en utilisant des moniteurs ARP ou PING existants. Vous pouvez configurer NetScaler pour surveiller un itinéraire statique IPv6 soit en créant un nouveau moniteur Neighbor Discovery pour IPv6 (ND6) ou PING, soit en utilisant les moniteurs ND6 ou PING existants.

Itinéraires statiques pondérés. Lorsque l'appliance NetScaler prend des décisions de routage impliquant des itinéraires de même distance et de même coût, c'est-à-dire des itinéraires ECMP (Equal Cost Multi-Path), elle équilibre la charge entre ces itinéraires à l'aide d'un mécanisme de hachage basé sur les adresses IP source et destination. Pour un itinéraire ECMP, vous pouvez toutefois configurer une valeur de poids. Le NetScaler utilise ensuite à la fois le poids et la valeur hachée pour équilibrer la charge.

Itinéraires nuls. Si l'itinéraire choisi dans une décision de routage est inactif, l'appliance NetScaler choisit un itinéraire de secours. Si toutes les routes de sauvegarde deviennent inaccessibles, l'appliance peut rediriger le paquet vers l'expéditeur, ce qui peut entraîner une boucle de routage entraînant une congestion du réseau. Pour éviter cette situation, vous pouvez créer une route nulle, qui ajoute une interface nulle en tant que passerelle. La route nulle n'est jamais la route préférée, car sa distance administrative est supérieure à celle des autres routes statiques. Mais elle est sélectionnée si les autres routes statiques deviennent inaccessibles. Dans ce cas, l'appliance supprime le paquet et empêche une boucle de routage.

Configuration d'itinéraires statiques IPv4

Vous pouvez ajouter un itinéraire statique simple ou un itinéraire nul en définissant quelques paramètres, ou vous pouvez définir des paramètres supplémentaires pour configurer un itinéraire statique surveillé ou surveillé et pondéré. Vous pouvez modifier les paramètres d'un itinéraire statique. Par exemple, vous pouvez attribuer un poids à un itinéraire non pondéré ou désactiver la surveillance sur un itinéraire surveillé.

Procédures CLI

Pour créer un itinéraire statique à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter un itinéraire <network><netmask><gateway>[-cost \<positive_integer>] [-advertise (DÉSACTIVÉ | ACTIVÉ)]
- afficher l'itinéraire [\ <network>\ <netmask>[\<gateway>]] [\<routeType>] [-detail]

Exemple :

```
1 > add route 10.102.29.0 255.255.255.0 10.102.29.2 -cost 2 -advertise
     ENABLED
2  Done
3 <!--NeedCopy-->
```

Pour créer un itinéraire statique surveillé à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une route statique surveillée et vérifier la configuration :

- <positive_integer>ajouter un itinéraire <network><netmask><gateway>[-distance \<positive_integer>] [-poids][-msr (ENABLED | DISABLED) [-monitor <string>]]
- afficher l'itinéraire [\ <network>\ <netmask>[\<gateway>]] [\<routeType>] [-detail]

Exemple :

```
1 > add route 10.102.29.0 255.255.255.0 10.102.29.3 -distance 5 -weight 6
      -msr ENBLED -monitor PING
2  Done
3 <!--NeedCopy-->
```

Pour créer un itinéraire nul à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- ajouter une route <network><netmask>nulle
- afficher l'itinéraire <network><netmask>

Exemple :

```
1 > add route 10.102.29.0 255.255.255.0 null
2  Done
3 <!--NeedCopy-->
```

Pour supprimer un itinéraire statique à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

itinéraire RM <network><netmask><gateway>

Exemple :


```
> rm route 10.102.29.0 255.255.255.0 10.102.29.3
 Done
<!--NeedCopy-->
```

Procédures GUI

Pour configurer un itinéraire statique à l'aide de l'interface graphique :

Accédez à Système > Réseau > Itinéraires et, dans l'onglet Basic, ajoutez un nouvel itinéraire statique ou modifiez un itinéraire statique existant.

Pour supprimer un itinéraire à l'aide de l'interface graphique :

Accédez à Système > Réseau > Itinéraires et, dans l'onglet Basic, supprimez l'itinéraire statique.

Configuration d'itinéraires statiques IPv6

Vous pouvez configurer un maximum de six routes statiques IPv6 par défaut. Les routes IPv6 sont sélectionnées en fonction de l'accessibilité de l'adresse MAC du périphérique de destination. Cela peut être déterminé à l'aide de la fonctionnalité IPv6 Neighbor Discovery. Les routes sont équilibrées en termes de charge et seuls les mécanismes de hachage basés sur la source/la destination sont utilisés. Par conséquent, les mécanismes de sélection d'itinéraires tels que le round robin ne sont pas pris en charge. Il n'est pas nécessaire que l'adresse du saut suivant de l'itinéraire par défaut appartienne au sous-réseau NSIP.

Procédures CLI

Pour créer un itinéraire IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une route IPv6 et vérifier la configuration :

- <positive_integer>ajouter route6 <network><gateway>[-vlan \]
- <gateway>Afficher l'itinéraire 6 [\ <network>[\]

Exemple :

```
> add route6 ::/0 FE80::67 -vlan 5
 Done
<!--NeedCopy-->
```

Pour créer un itinéraire statique IPv6 surveillé à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour créer une route statique IPv6 surveillée et vérifier la configuration :

- <string>ajouter route6 <network><gateway>[-msr (ACTIVÉ | DÉSACTIVÉ) [-monitor \]
- <gateway>Afficher l'itinéraire 6 [\ <network>[\]

Exemple :

```
1 > add route6 ::/0 2004::1 -msr ENABLED -monitor PING
2  Done
3 <!--NeedCopy-->
```

Pour supprimer une route IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

RM route6 <network><gateway>

Exemple :

```
1 > rm route6 ::/0 FE80::67
2  Done
3 <!--NeedCopy-->
```

Procédures GUI

Pour configurer un itinéraire IPv6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Itinéraires et, dans l'onglet IPV6, ajoutez un nouvel itinéraire IPv6 ou modifiez un itinéraire IPv6 existant.

Pour supprimer une route IPv6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > Itinéraires et, sous l'onglet IPV6, supprimez l'itinéraire IPv6.

Injection d'intégrité de routage en fonction des paramètres du serveur

May 5, 2023

L'option et le paramètre suivants sont introduits pour contrôler la fonctionnalité RHI (Route Health Injection) de l'appliance NetScaler pour annoncer l'itinéraire d'une adresse VIP.

- **VSVR_CNTRLD**. Il s'agit d'une option pour le paramètre (niveau RHI du serveur virtuel) d'une adresse VIP. Lorsque cette option est définie sur le paramètre Vserver RHI Level, le comportement de RHI en matière de publicité de l'itinéraire de l'adresse VIP dépend du paramètre RHI STATE défini sur tous les serveurs virtuels associés à l'adresse VIP, ainsi que de leurs états.
- **ÉTAT DE RHI**. Il s'agit d'un paramètre de serveur virtuel. Vous pouvez définir le paramètre RHI STATE sur PASSIVE ou ACTIVE. Par défaut, le paramètre RHI STATE est défini sur PASSIVE.

Pour une adresse VIP, lorsque le paramètre RHI (niveau RHI du serveur Vserver) est défini sur VSVR_CNTRLD, les comportements RHI suivants pour l'adresse VIP sont les suivants sur la base des paramètres RHI STATE des serveurs virtuels associés à l'adresse VIP :

- Si vous définissez RHI STATE sur PASSIVE sur tous les serveurs virtuels, NetScaler annonce toujours l'itinéraire de l'adresse VIP.
- Si vous définissez RHI STATE sur ACTIVE sur tous les serveurs virtuels, NetScaler annonce l'itinéraire pour l'adresse VIP si au moins l'un des serveurs virtuels associés est en état UP.
- Si vous définissez RHI STATE sur ACTIVE sur certains et PASSIVE sur d'autres, NetScaler annonce l'itinéraire pour l'adresse VIP si au moins l'un des serveurs virtuels associés, dont l'ÉTAT RHI est défini sur ACTIVE, est à l'état UP.

Le tableau suivant présente l'exemple de comportement RHI pour une adresse VIP sur la base des paramètres RHI STATE sur les serveurs virtuels associés à l'adresse VIP. L'appliance NetScaler possède deux serveurs virtuels V1 et V2 associés à l'adresse VIP :

Serveurs virtuels associés pour un VIP	État 1	État 2	État 3	État 4
État RHI défini sur PASSIVE sur tous les serveurs virtuels				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Annoncez l'itinéraire pour cette adresse VIP ?	Oui	Oui	Oui	Oui
État RHI défini sur ACTIVE sur tous les serveurs virtuels				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN

Serveurs virtuels associés pour un VIP	État 1	État 2	État 3	État 4
Annoncez l'itinéraire pour cette adresse VIP ?	Oui	Oui	Oui	Non
État RHI défini sur ACTIVE sur un serveur virtuel et PASSIF sur l'autre				
V1 (État RHI = ACTIF)	UP	UP	DOWN	DOWN
V2 (État RHI = PASSIF)	UP	DOWN	UP	DOWN
Annoncez l'itinéraire pour cette adresse VIP ?	Oui	Oui	Non	Non

Pour configurer RHI pour une adresse VIP, en fonction du réglage des paramètres RHI (RHI State) des serveurs virtuels associés, effectuez les étapes suivantes :

- Définissez le paramètre RHI (Vserver RHI Level) sur VSVR_CNTRLD pour l'adresse VIP.
- Définissez le paramètre RHI State pour chaque serveur virtuel associé à l'adresse VIP.

Pour définir le niveau RHI du vServer pour une adresse VIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **définir ns ip** <vserverRHILevel><IPAddress>[-** vServerRhiLevel \]

Pour définir le paramètre RHI State d'un serveur virtuel à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set lb vserver** <name>[-**RhisState** (**PASSIF** | **ACTIF)]**

Pour définir le niveau RHI vServer pour une adresse VIP à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **IP**.
2. Sélectionnez une adresse VIP, puis cliquez sur **Modifier**.
3. **Définissez le paramètre**Vserver RHI Level**sur**VSVR_CNTRLD**, puis cliquez sur OK.**

Pour définir le paramètre RHI State d'un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sélectionnez un serveur virtuel d'équilibrage de charge, puis cliquez sur **Modifier**.
3. Définissez le paramètre **RHI State**, puis cliquez sur **OK.**

Configuration des itinéraires basés sur des stratégies

May 5, 2023

Le routage basé sur des règles base les décisions de routage sur des critères que vous spécifiez. Une route basée sur des règles (PBR) spécifie les critères de sélection des paquets et, généralement, le saut suivant auquel envoyer les paquets sélectionnés. Par exemple, vous pouvez configurer l'appliance NetScaler pour acheminer les paquets sortants d'une adresse ou d'une plage IP spécifique vers un routeur de saut suivant particulier. Chaque paquet est mis en correspondance avec chaque PBR configuré, dans l'ordre déterminé par les priorités spécifiées, jusqu'à ce qu'une correspondance soit trouvée. Si aucune correspondance n'est trouvée ou si le PBR correspondant spécifie une action DENY, NetScaler applique la table de routage pour un routage normal basé sur la destination.

Un PBR base les décisions de routage pour les paquets de données sur des paramètres tels que l'adresse IP source, le port source, l'adresse IP de destination, le port de destination, le protocole et l'adresse MAC source. Un PBR définit les conditions qu'un paquet doit remplir pour que NetScaler l'achemine. Ces actions sont appelées « modes de traitement ». « Les modes de traitement sont les suivants :

- **AUTORISER.** L'appliance envoie le paquet au routeur de saut suivant désigné.
- **NIER.** NetScaler applique la table de routage pour le routage normal basé sur la destination.

Vous pouvez créer des PBR pour le trafic IPv4 et IPv6 sortant.

De nombreux utilisateurs commencent par créer des PBR, puis les modifient. Pour activer un nouveau PBR, vous devez l'appliquer. Pour désactiver un PBR, vous pouvez le supprimer ou le désactiver. Vous pouvez modifier le numéro de priorité d'un PBR pour lui donner une priorité supérieure ou inférieure.

Routes basées sur des règles (PBR) pour le trafic IPv4

May 5, 2023

La configuration des PBR implique les tâches suivantes :

- Créez un PBR.
- Appliquez des PBR.
- (Facultatif) Désactivez ou activez un PBR.
- (Facultatif) Renuméroter la priorité du PBR.

Création ou modification d'un PBR

Vous ne pouvez pas créer deux PBR avec les mêmes paramètres. Si vous tentez de créer un doublon, un message d'erreur s'affiche.

Vous pouvez configurer la priorité d'un PBR. La priorité (une valeur entière) définit l'ordre dans lequel l'appliance NetScaler évalue les PBR. Lorsque vous créez un PBR sans spécifier de priorité, NetScaler attribue automatiquement une priorité multiple de 10.

Si un paquet correspond à la condition définie par le PBR, NetScaler exécute une action. Si le paquet ne correspond pas à la condition définie par le PBR, NetScaler compare le paquet avec le PBR ayant la priorité la plus élevée.

Au lieu d'envoyer les paquets sélectionnés à un routeur à saut suivant, vous pouvez configurer le PBR pour qu'il les envoie à un serveur virtuel d'équilibrage de charge de liaison auquel vous avez lié plusieurs sauts suivants. Cette configuration peut fournir une sauvegarde en cas d'échec d'un lien de saut suivant.

Prenons l'exemple suivant. Deux PBR, p1 et p2, sont configurés sur NetScaler et les priorités 20 et 30 leur sont automatiquement attribuées. Vous devez ajouter un troisième PBR, p3, à évaluer immédiatement après le premier PBR, p1. Le nouveau PBR, p3, doit avoir une priorité comprise entre 20 et 30. Dans ce cas, vous pouvez définir la priorité sur 25.

Procédures CLI

Pour créer un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <interface_name><positive_integer><string>add ns pbr <name><action>[-SrcIP [\]] [<operator><srcIPVal>-SrcPort [\]] [<operator><srcPortVal><operator><destIPVal>-DestIP [\]] [-DestPort [\]] [<operator><interface_name>0 -NextHop \] [<interface_name>1 -SrcMac \] [-protocole \ <interface_name>2 <interface_name>3 |-Numéro de protocole \] [<positive_integer>-vlan \] [<positive_integer>-interface \] [-priorité \] [-msr (ACTIVÉ | DÉSACTIVÉ) [-moniteur \]] [-state (ACTIVÉ | DÉSACTIVÉ)]
- show ns pbr

Exemple :


```
> add ns pbr pbr1  allow -srcip 10.102.37.252 -destip 10.10.10.2 -
   nexthop 10.102.29.77
 Done
<!--NeedCopy-->
```

Pour modifier la priorité d'un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour modifier la priorité et vérifier la configuration :

- <interface_name><positive_integer><string>set ns pbr <name>[-action (AUTORISER | REFUSER)] [-SrcIP [\]] [-SrcPort [\<operator>]<srcIPVal>] [<operator><srcPortVal><operator><destIPVal>-DestIP [\]] [-DestPort [\]] [<operator><destPortVal>-NextHop \] [<interface_name>0 -SrcMac \] [-protocole \ | <interface_name>1 <interface_name>2 -Numéro de protocole \] [<positive_integer>-vlan \] [<positive_integer>-interface \] [-priorité \] [-msr (ACTIVÉ | DÉSACTIVÉ) [-monitor \]] [-state (ACTIVÉ | DÉSACTIVÉ)]
- <name>Afficher le fichier pbr [\]

Exemple :

```
> set ns pbr pbr1 -priority 23
 Done
<!--NeedCopy-->
```

Pour supprimer un ou tous les PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- rm ns pbr <name>
- Clear NS PBRS

Exemple :

```
> rm ns pbr pbr1
 Done

> clear ns PBRs
 Done
<!--NeedCopy-->
```

Procédures GUI

Pour créer un PBR à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, dans l'onglet PBR, ajoutez un nouveau PBR ou modifiez un PBR existant.

Pour supprimer un ou tous les PBR à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, dans l'onglet PBR, supprimez le PBR.

Appliquer un PBR

Vous devez appliquer un PBR pour l'activer. La procédure suivante réapplique tous les PBR que vous n'avez pas désactivés. Les PBR constituent un arbre de mémoire (table de recherche). Par exemple, si vous créez 10 PBR (p1 - p10), puis que vous créez un autre PBR (p11) et que vous l'appliquez, tous les PBR (p1 - p11) sont récemment appliqués et une nouvelle table de recherche est créée. Si un PBR DENY est associé à une session, la session est détruite.

Vous devez appliquer cette procédure après chaque modification apportée à un PBR. Par exemple, vous devez suivre cette procédure après avoir désactivé un PBR.

Remarque : Les PBR créés sur l'appliance NetScaler ne fonctionnent pas tant qu'ils ne sont pas appliqués.

Pour appliquer un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

appliquer ns PBR

Pour appliquer un PBR à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > PBR.
2. Dans l'onglet PBR, sélectionnez le PBR, dans la liste Actions, sélectionnez Appliquer.

Activation ou désactivation des PBR

Par défaut, les PBR sont activés. Cela signifie que lorsque des PBR sont appliqués, l'appliance NetScaler compare automatiquement les paquets entrants aux PBR configurés. Si aucun PBR n'est requis dans la table de recherche, mais qu'il doit être conservé dans la configuration, il doit être désactivé avant que les PBR ne soient appliqués. Une fois les PBR appliqués, NetScaler ne compare pas les paquets entrants aux PBR désactivés.

Pour activer ou désactiver un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- activer ns pbr <name>
- disable ns pbr <name>

Exemple :

```
1 > enable ns PBR pbr1
2  Done
```



```
> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                           Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                                 Protocol:
        Vlan:                                   Interface:
        Active Status: ENABLED                  Applied Status: APPLIED
        Priority: 10
        NextHop: 10.102.29.77

 Done

> disable ns PBR pbr1
Warning: PBR modified, use 'apply pbrs' to commit this operation

> apply pbrs
 Done

> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                           Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                                 Protocol:
        Vlan:                                   Interface:
        Active Status: DISABLED                 Applied Status:
           NOTAPPLIED
        Priority: 10
        NextHop: 10.102.29.77
Done
<!--NeedCopy-->
```

Pour activer ou désactiver un PBR à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > PBR.
2. Dans l'onglet PBR, sélectionnez le PBR, dans la liste des actions, sélectionnez Activer ou Désactiver.

Renumérotation des PBR

Vous pouvez renuméroter automatiquement les PBR pour définir leurs priorités sur des multiples de 10.

Pour renuméroter les PBR à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- renuméroter ns pbrs

Pour renuméroter les PBR à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, sous l'onglet PBR, dans la liste des actions, sélectionnez Renuméroter les priorités.

Cas d'utilisation : PBR avec sauts multiples

Imaginons un scénario dans lequel deux PBR, PBR1 et PBR2, sont configurés sur l'appliance NetScaler NS1. PBR1 achemine tous les paquets sortants, avec l'adresse IP source 10.102.29.30, vers le routeur de saut suivant R1. PBR2 achemine tous les paquets sortants, avec l'adresse IP source 10.102.29.90, vers le routeur R2 du saut suivant. R3 est un autre routeur à saut suivant connecté à NS1.

Si le routeur R1 tombe en panne, tous les paquets sortants correspondant à PBR1 sont supprimés. Pour éviter cette situation, vous pouvez spécifier un serveur virtuel d'équilibrage de charge de liaison (LLB) dans le champ du saut suivant lors de la création ou de la modification d'un PBR. Les multiples sauts suivants sont liés au serveur virtuel LLB en tant que services (par exemple R1, R2 et R3). Désormais, si R1 échoue, tous les paquets qui correspondent à PBR1 sont routés vers R2 ou R3 selon la méthode LB configurée sur le serveur virtuel LLB.

L'appliance NetScaler génère une erreur si vous tentez de créer un PBR avec un serveur virtuel LLB comme saut suivant dans les cas suivants :

- Ajouter un autre PBR avec le même serveur virtuel LLB.
- Spécification d'un serveur virtuel LLB inexistant.
- Spécifier un serveur virtuel LLB pour lequel les services liés ne sont pas les sauts suivants.
- Spécification d'un serveur virtuel LLB pour lequel la méthode LB n'est pas définie sur l'une des options suivantes :
  - ROUNDROBIN
  - DESTINATIONIPHASH
  - SOURCEIPHASH
  - SRCIPDESTIPHASH
  - LEASTPACKETS
  - LEASTBANDWIDTH
  - LTRM
  - CALLIDHASH
  - CUSTOM LOAD
- Spécification d'un serveur virtuel LLB pour lequel le type de persistance LB n'est pas défini sur l'un des suivants :
  - DESTIP
  - SOURCEIP

- SRCDSTIP

Le tableau suivant répertorie les noms et les valeurs des entités configurées sur l'appliance NetScaler :

Type d'entité	Nom	Adresse IP
Serveur virtuel d'équilibrage de charge des liens	LLB1	SO
Services (prochains arrêts)	Router1	1.1.1.254
	Router2	2.2.2.254
	Router3	3.3.3.254
PBR	PBR1	SO
	PBR2	SO

Tableau 1. Exemples de valeurs pour la création d'entités

Pour implémenter la configuration décrite ci-dessus, vous devez :

1. Créez les services Router1, Router2 et Router3 qui représentent les routeurs à saut suivant R1, R2 et R3.
2. Créez le serveur virtuel d'équilibrage de charge des liens LLB1 et liez-y les services Router1, Router2 et Router3.
3. Créez les PBR PBR1 et PBR2, avec les champs du saut suivant définis respectivement comme LLB1 et 2.2.2.254 (adresse IP du routeur R2).

Pour créer un service à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter un service <name><IP><serviceType><port>
- show service <name>

Exemple :

```
> add service Router1 1.1.1.254 ANY *
 Done
> add service Router2 2.2.2.254 ANY *
 Done
> add service Router3 3.3.3.254 ANY *
 Done
<!--NeedCopy-->
```

Pour créer un service à l'aide de l'interface graphique :

Accédez à Gestion du trafic > Équilibrage de charge > Services, puis créez un service.

Pour créer un serveur virtuel d'équilibrage de charge des liens et lier un service à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter lb vserver <name><serviceType>
- serveur vserver bind lb < name> <serviceName>
- afficher lb vserver < name>

Exemple :

```
> add lb vserver LLB1 ANY
 Done
> bind lb vserver LLB1 Router1 Router2 Router3
 Done
<!--NeedCopy-->
```

Pour créer un serveur virtuel d'équilibrage de charge des liens et lier un service à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels, puis créez un serveur virtuel pour l'équilibrage de charge des liens. Spécifiez **ANY** dans le champ **Protocole** .
   Remarque : Assurez-vous que la case
   Directly Addressable n'est pas cochée.
2. Sous l'onglet **Services**, dans la colonne **Actif**, cochez la case correspondant au service que vous souhaitez lier au serveur virtuel.

Pour créer un PBR à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- <nextHopVal>ajouter ns pbr <name><action>[-SrCip [\]] [-NextHop \ <operator><srcIPVal>]
- show ns pbr

Exemple :

```
> add pbr PBR1 ALLOW -srcIP 10.102.29.30 -nextHop LLB1
 Done
> add pbr PBR2 ALLOW -srcIP 10.102.29.90 -nextHop 2.2.2.254
 Done
<!--NeedCopy-->
```

Pour créer un PBR à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, sous l'onglet PBR, ajoutez un nouveau PBR.

Routes basées sur des règles (PBR6) pour le trafic IPv6

May 5, 2023

La configuration du PBR6s implique les tâches suivantes :

- Créez un PBR6.
- Appliquez PBR6s.
- (Facultatif) Désactivez ou activez un PBR6.
- (Facultatif) Renuméroter la priorité du PBR6.

Création ou modification d'un PBR6

Vous ne pouvez pas créer deux PBR6 avec les mêmes paramètres. Si vous tentez de créer un doublon, un message d'erreur s'affiche.

Vous pouvez configurer la priorité d'un PBR6. La priorité (une valeur entière) définit l'ordre dans lequel l'appliance NetScaler évalue les PBR6. Lorsque vous créez un PBR6 sans spécifier de priorité, NetScaler attribue automatiquement une priorité multiple de 10.

Si un paquet correspond à la condition définie par le PBR6, NetScaler exécute une action. Si le paquet ne correspond pas à la condition définie par le PBR6, NetScaler compare le paquet au PBR6 ayant la priorité la plus élevée.

Procédures CLI

Pour créer un PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add ns pbr6** <string><nextHopVal><name><action>[-SrciPv6 [\]] [<operator><srcIPv6Val>-SrcPort [\]] [<operator><srcPortVal><operator><destIPv6Val>-DestIPv6 [\]] [-DestPort [\]] [<operator>0 -SrcMac \] [-protocole \ 1 2 |-Numéro de protocole \] [-vlan \] [3 3 -interface \] [4 -priority \] [-state (ACTIVÉ | DÉSACTIVÉ)] [-msr (ACTIVÉ | DÉSACTIVÉ)] [-msr (ACTIVÉ | DÉSACTIVÉ) [moniteur \]] [-NextHop \] [-NextHop VLAN \ 3 <positive_integer >]
- show ns pbr

Pour modifier ou supprimer un PBR6 à l'aide de l'interface de ligne de commande :

Pour modifier un PBR6, tapez la <name>commande **set pbr6** et les paramètres à modifier, avec leurs nouvelles valeurs.

Pour supprimer un ou tous les PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **rm ns pbr6** <name>
- **clear ns pbr6**

Procédures GUI

Pour créer ou modifier un PBR6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR et, dans l'onglet PBR6s, ajoutez un nouveau PBR6 ou modifiez un PBR6 existant.

Pour supprimer un ou tous les PBR6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR et, dans l'onglet PBR6s, supprimez le PBR6.

Appliquer les PBR6s

Vous devez appliquer un PBR6 pour l'activer. La procédure suivante réapplique tous les PBR6 que vous n'avez pas désactivés. Les PBR6 constituent un arbre de mémoire (table de consultation). Par exemple, si vous créez 10 PBR6 (p6_1 - p6_10), puis que vous créez un autre PBR6 (p6_11) et que vous l'appliquez, tous les PBR6 (p6_1 - p6_11) sont récemment appliqués et une nouvelle table de recherche est créée. Si un DENY PBR6 est associé à une session, la session est détruite.

Vous devez appliquer cette procédure après chaque modification apportée à un PBR6. Par exemple, vous devez suivre cette procédure après avoir désactivé un PBR6.

Remarque : Les PBR6 créés sur l'appliance NetScaler ne fonctionnent pas tant qu'ils ne sont pas appliqués.

Pour appliquer PBR6s à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **appliquer en PBR6**

Pour appliquer PBR6s à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > PBR.
2. Dans l'onglet PBR6s, sélectionnez le PBR6, dans la liste Actions, sélectionnez Appliquer.

Activation ou désactivation d'un PBR6

Par défaut, les PBR6 sont activés. Cela signifie que lorsque des PBR6 sont appliqués, l'appliance NetScaler compare automatiquement les paquets IPv6 sortants aux PBR6 configurés. Si aucun PBR6 n'est requis dans la table de recherche, mais qu'il doit être conservé dans la configuration, il doit être désactivé avant que les PBR6 ne soient appliqués. Une fois les PBR6 appliqués, NetScaler ne compare pas les paquets entrants aux PBR6 désactivés.

Pour activer ou désactiver un PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- **activer ns pbr** <name>
- **disable ns pbr** <name>

Pour activer ou désactiver un PBR6 à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > PBR.
2. Dans l'onglet PBR6s, sélectionnez le PBR6, dans la liste des actions, sélectionnez Activer ou Désactiver.

Renumérotation des PBR6

Vous pouvez renuméroter automatiquement les PBR6 pour définir leurs priorités sur des multiples de 10.

Pour renuméroter les PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **renuméroter ns pbr6**

Pour renuméroter les PBR6 à l'aide de l'interface graphique :

Accédez à Système > Réseau > PBR, sous l'onglet PBR6s, dans la liste Action, sélectionnez Renuméroter les priorités.

Masque générique d'adresse MAC pour PBR

August 20, 2021

Un paramètre de masque générique a été introduit pour les PBR étendus et PBR6 et est utilisé avec le paramètre d'adresse MAC source pour définir une plage d'adresses MAC à comparer avec l'adresse MAC source des paquets sortants.

Les masques génériques spécifient quels chiffres hexadécimaux de l'adresse MAC sont utilisés et quels chiffres hexadécimaux sont ignorés. Le paramètre de masque générique spécifie une série de 1 et de zéros et a une longueur de 12 chiffres. Chaque chiffre est un masque pour le chiffre hexadécimal correspondant de l'adresse MAC. Un chiffre zéro dans le masque générique indique que le chiffre hexadécimal correspondant de l'adresse MAC doit être pris en compte et un chiffre indique que le chiffre hexadécimal correspondant doit être ignoré.

Le masque générique doit répondre aux conditions suivantes :

- A seulement une série de zéros

- A seulement une série de uns
- Commencer par une série de zéros

Voici quelques exemples de masques génériques valides :

- 000000111111
- 000000011111
- 000011111111

Voici quelques exemples de masques génériques non valides :

- 000000111100
- 111110000000
- 010101010101

Pour une règle PBR, un masque générique 000000111111 pour l'adresse MAC 96:fa : 95:1 d : 67:4 a définit la plage d'adresses MAC 96:FA : 95:00:00:00 - 96:FA:95:FF:FF. Cette plage d'adresses MAC est mise en correspondance avec l'adresse MAC source des paquets sortants.

Pour spécifier une plage d'adresses MAC source dans une règle PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns pbr** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>
- **show ns pbr** <pbrname>

Exemple :

```
1 > add ns pbr PBR-1 ALLOW -srcip 192.0.2.34 -srcMac 96:fa:95:1d:67:4a
      - srcMacMask 000000111111 -nexthop 198.51.100.1
2
3  Done
```

Pour spécifier une plage d'adresses MAC source dans une règle PBR6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns pbr6** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>
- **show pbr6** <pbr6name>

Exemple :

```
1 > add ns pbr6 PBR6-1 ALLOW  - srcipv6 2001:db8:0::7 -srcMac 96:fa:95:1d
     :67:4a   - srcMacMask 000000001111 -nexthop 2001:db8:0::1
2  Done
```


Utilisation de routes basées sur une stratégie NULL pour supprimer les paquets sortants

May 5, 2023

Certaines situations peuvent nécessiter que l'appliance NetScaler supprime des paquets sortants spécifiques au lieu de les acheminer, par exemple lors de tests et lors de la migration du déploiement.

Les routes basées sur une politique NULL peuvent être utilisées pour supprimer des paquets sortants spécifiques. Un PBR NULL est un type de PBR dont le paramètre nexthop est défini sur NULL. L'appliance NetScaler supprime les paquets sortants qui correspondent à un PBR NULL.

Configuration de PBR NULL pour les paquets IPv4

Pour créer un PBR NULL à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add ns pbr ALLOW** <name><mac_addr><string><protocol>[**-td** \<positive_integer>] [-**SrcIP [\]]** [- <operator><srcIPVal**SrcPort [\]] [- <operator><srcPortVal><operator>0**DestIP** [\]] [-**DestPort** [\]] <operator1 0 (- 2 NextHop NULL) 1 [2 SrcMac \ [- SrcMacMask \]] [- protocole 3 \ | - 4 5 6 7**ProtocolNumber** \<positive_integer>] [-**vlan** \ <positive_integer>| -**vxlan** \<positive_integer>] [-**interface \] [- <interface_name**priorité** 0 \<positive_integer>] [- 1 msr 2 (3 ACTIVÉ 4 | 5 DÉSACTIVÉ 6) [7 -monitor 8 \<string>]] [- 9 state 0 (ACTIVÉ | DÉSACTIVÉ) [- 1 2 3 4**<string>Groupe de propriétaires \]** </g********** **
- **apply ns pbrs**
- **afficher ns pbr**<id>

Pour configurer un PBR NULL à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau**> **PBR, dans**l'onglet **PBR, ajoutez un nouveau PBRNULL ou modifiez un PBR NULL**existant.

Exemple de configuration

Dans l'exemple de configuration suivant, NULL PBR6 PBR6-NULL-EXAMPLE-1 est configuré pour supprimer tous les paquets IPv6 sortants de l'interface 1/5.

```
> add ns pbr PBR6-NULL-EXAMPLE-1 ALLOW  - nextHop NULL -interface 1/5
 Done

> apply ns pbr6
 Done
```


Répartition du trafic sur plusieurs itinéraires basée sur les informations de cinq tuples

May 5, 2023

Dans une configuration d'équilibrage de charge, une appliance NetScaler peut disposer de plusieurs itinéraires pour envoyer un paquet vers sa destination. Par exemple : vers un serveur et vers un client.

Une appliance NetScaler utilise un algorithme de hachage pour sélectionner un itinéraire pour envoyer le paquet vers sa destination.

L'algorithme de hachage utilise les deux tuples suivants d'un paquet pour calculer un hachage, sur la base duquel l'appliance NetScaler sélectionne un itinéraire pour le paquet.

- Adresse IP source
- Adresse IP de destination

La sélection d'itinéraires sur la base des informations de deux tuples peut entraîner une répartition inégale du trafic sur les itinéraires disponibles. Cette répartition inégale du trafic entraîne une surcharge du trafic sur certains itinéraires.

Pour résoudre ce problème, à partir de la version 13.0 71.x, l'appliance NetScaler utilise les cinq informations tuples suivantes relatives à un paquet dans l'algorithme de hachage afin de sélectionner un itinéraire pour le paquet :

- Adresse IP source (IP du client)
- Port source (port client)
- Adresse IP de destination (IP du service)
- Port de destination (port de service)
- Numéro de protocole

La sélection des itinéraires basée sur les informations de cinq tuples garantit une répartition uniforme du trafic sur les itinéraires disponibles. Cette répartition uniforme du trafic évite la surcharge du trafic sur un itinéraire.

Prenons un exemple de configuration d'équilibrage de charge dans laquelle un client envoie une demande à l'adresse VIP. L'appliance NetScaler utilise les cinq tuples d'informations suivants pour sélectionner un itinéraire pour envoyer le paquet de demande au serveur d'équilibrage de charge :

- Adresse IP source (adresse IP du client)
- Port source (port client)
- Adresse IP de destination (adresse IP du service)
- Port de destination (numéro de port de service)
- Numéro de protocole

Si le mode Use Source IP (USIP) est activé, les cinq tuples sont considérés comme des entrées de hachage pour sélectionner une route. Si le mode Utiliser l'adresse IP du sous-réseau (USNIP) est activé, le SNIP et le port source ne sont pas considérés comme des entrées car ils sont sélectionnés après la sélection de l'itinéraire. Pour plus d'informations sur la configuration des modes USIP et USNIP, voir Activer l'utilisation du mode IP source et Configuration des adresses IP de sous-réseau (SNIP).

> **Remarque :**
>
> À partir de la version 13.1 30.x, l'appliance NetScaler utilise l'algorithme de hachage à cinq tuples au lieu de l'algorithme de hachage à deux tuples pour sélectionner un itinéraire pour les sondes du moniteur d'équilibrage de charge.

Priorité par rapport aux autres fonctionnalités NetScaler basées sur la sélection d'itinéraires

Cette section décrit la priorité de la sélection d'itinéraires sur la base de la fonctionnalité à cinq tuples et d'autres fonctionnalités liées à la sélection d'itinéraires dans une appliance NetScaler.

- **Routes basées sur des stratégies (PBR)**. Les règles PBR ont toujours préséance sur la sélection d'itinéraires basée sur cinq tuples.
- **Transfert basé sur Mac (MBF)**. Dans une configuration d'équilibrage de charge, le MBF ou la sélection de route basée sur cinq tuples est prioritaire dans les cas suivants :
  - Pour le trafic initié par un client vers l'adresse VIP de la configuration d'équilibrage de charge dans l'appliance NetScaler :
    - Trafic de demande destiné à un serveur à charge équilibrée. La sélection d'itinéraire basée sur cinq tuples a la préférence sur MBF.
    - Trafic de réponse destiné au client. MBF a la préférence sur la sélection d'itinéraires basée sur cinq tuples.
  - Pour le trafic initié par un serveur vers l'adresse SNIP de l'appliance NetScaler :
    - Trafic de réponse destiné au client. La sélection d'itinéraire basée sur cinq tuples a la préférence sur MBF.
    - Trafic de demande destiné à un serveur à charge équilibrée. MBF a la préférence sur la sélection d'itinéraires basée sur cinq tuples.

Dépannage des problèmes de routage

May 5, 2023

Pour rendre votre processus de dépannage aussi efficace que possible, commencez par collecter des informations sur votre réseau. Vous devez obtenir les informations suivantes concernant l'appliance

NetScaler et les autres systèmes du réseau :

- Schéma topologique complet, y compris la connectivité de l'interface et les détails du commutateur intermédiaire.
- Configuration en cours d'exécution. Vous pouvez utiliser la commande show running pour obtenir la configuration en cours pour ns.conf et Zebos.conf.
- Résultat de la commande History, pour déterminer si des modifications de configuration ont été apportées lorsque le problème est survenu.
- Sortie des commandes Top et ps -ax, pour déterminer si un démon de routage utilise trop le processeur ou se comporte mal.
- Tous les fichiers principaux liés au routage dans /var/core - nsm, bgpr, ospfd ou ripd. Vérifiez l'horodatage pour voir s'ils sont pertinents.
- Fichiers dr_error.log et dr_info.log depuis /var/log.
- Sortie de la commande de date et des détails de l'heure pour tous les systèmes concernés. Imprimez les dates sur tous les appareils les unes après les autres, afin que les heures figurant dans les messages du journal puissent être corrélées à divers événements.
- Fichiers ns.log, newnslog pertinents.
- Fichiers de configuration, fichiers journaux et détails de l'historique des commandes des routeurs en amont et en aval.

FAQ sur le routage générique

January 21, 2021

Les utilisateurs ont généralement les questions suivantes sur la façon de résoudre les problèmes de routage génériques :

- Comment enregistrer les fichiers de configuration ?

  La commande write de VTYSH enregistre uniquement ZebOSs.conf. Exécutez la commande save ns config à partir de la CLI pour enregistrer les fichiers ns.conf et ZebOSs.conf.

- Si j'ai configuré à la fois un itinéraire statique par défaut et un itinéraire par défaut appris dynamiquement, quelle est la route par défaut préférée ?

  L'itinéraire appris dynamiquement est l'itinéraire par défaut préféré. Ce comportement est unique aux itinéraires par défaut. Toutefois, dans le cas du Network Services Module (NSM), à moins que les distances administratives ne soient modifiées, un itinéraire configuré statiquement dans le RIB est préféré à un itinéraire dynamique. L'itinéraire qui est téléchargé dans la FIB NSM est l'itinéraire statique.

- Comment bloquer la publicité des itinéraires par défaut ?

La route par défaut n'est pas injectée dans ZebOS.

- Comment afficher la sortie de débogage des démons réseau ?

  Vous pouvez écrire une sortie de débogage à partir de démons réseau dans un fichier en entrant la commande de fichier journal suivante à partir de la vue de configuration globale dans VTYSH :

```
ns(config)# log file /var/ZebOS.log
<!--NeedCopy-->
```

  Vous pouvez diriger la sortie de débogage vers la console en entrant la commande Terminal Monitor à partir de la vue utilisateur VTYSH :

```
ns# terminal monitor
<!--NeedCopy-->
```

- Comment collecter les cœurs de démons en cours d'exécution ?

  Vous pouvez utiliser l'utilitaire gcore pour collecter les cœurs de démons en cours d'exécution pour traitement par gdb. Cela peut être utile pour déboguer des démons qui se comportent mal sans mettre l'ensemble de l'opération de routage à l'arrêt.

```
gcore [-s] [-c core] [executable] pid
<!--NeedCopy-->
```

  L'option -s arrête temporairement le démon lors de la collecte de l'image principale. Il s'agit d'une option recommandée, car elle garantit que l'image résultante affiche le noyau dans un état cohérent.

```
root@ns#gcore -s -c nsm.core /netscaler/nsm 342
<!--NeedCopy-->
```

- Comment exécuter un lot de commandes ZebOSS ?

  Vous pouvez exécuter un lot de commandes ZebOSS à partir d'un fichier en entrant la commande VTYSH -f <file-name>. Cela ne remplace pas la configuration en cours d'exécution, mais y ajoute. Toutefois, en incluant des commandes pour supprimer la configuration existante dans le fichier de commandes, puis en ajoutant celles pour la nouvelle configuration souhaitée, vous pouvez utiliser ce mécanisme pour remplacer une configuration spécifique :

```
!
router bgp 234
network 1.1.1.1 255.255.255.0
!
route-map bgp-out2 permit 10
 set metric 9900
```



```
 set community 8602:300
!
<!--NeedCopy-->
```

Résolution des problèmes spécifiques à OSPF

May 5, 2023

Avant de commencer à résoudre un problème spécifique à l'OSPF, vous devez collecter des informations auprès de l'appliance NetScaler et de tous les systèmes du réseau local concerné, y compris les routeurs en amont et en aval. Pour commencer, entrez les commandes suivantes :

1. Afficher l'interface depuis nscli et VTYSH
2. afficher l'interface ospf
3. Afficher les détails du voisin OSPF
4. afficher l'itinéraire IP
5. afficher l'itinéraire OSPF
6. afficher le résumé de la base de données OSPF
    - Si la base de données ne contient que quelques LSA, entrez show ip ospf database router, show ip ospf database A. network, show ip ospf database external et d'autres commandes pour obtenir tous les détails des LSA.
    - Si la base de données contient un grand nombre de LSA, entrez la commande show ip ospf database self-originated.
7. afficher ospf
8. montre-nous une adresse IP. Cela garantit que les détails de tous les VIP qui vous intéressent sont inclus.
9. Obtenez les journaux des périphériques d'appairage et exécutez la commande suivante :

    ```
    gcore -s -c xyz.core /netscaler/ospfd <pid>
    ```

    Remarque : La commande gcore n'est pas perturbatrice.

Collectez des informations supplémentaires à partir de NetScaler comme suit :

1. Activez la journalisation des messages d'erreur en saisissant la commande suivante dans la vue de configuration globale de VTYSH :


```
ns(config)# log file /var/ospf.log
<!--NeedCopy-->
```

2. Activez le débogage des événements OSPF et enregistrez-les à l'aide de la commande suivante :

```
ns(config) #log file /var/ospf.log
<!--NeedCopy-->
```

Activer le paquet debug ospf lsa uniquement si le nombre de LSA dans la base de données est relativement faible (< 500).

Protocole Internet version 6 (IPv6)

May 5, 2023

Une appliance NetScaler prend en charge le protocole IPv6 côté serveur et côté client et peut donc fonctionner comme un nœud IPv6. Il peut accepter des connexions provenant de nœuds IPv6 (hôtes et routeurs) et de nœuds IPv4, et peut effectuer une traduction de protocole (RFC 2765) avant d'envoyer du trafic vers les services.

Le tableau suivant répertorie certaines des fonctionnalités IPv6 prises en charge par l'appliance NetScaler.

Tableau 1. Certaines fonctionnalités IPv6 prises en charge

Fonctionnalités IPv6
Adresses IPv6 pour les SNIP (NSIP6, VIP6 et SNIP6)
Découverte de voisins (résolution d'adresses, détection d'adresses dupliquées, détection d'inaccessibilité des voisins, découverte de routeurs)
Applications de gestion (ping6, telnet6, ssh6)
Routage statique et routage dynamique (OSPF, BGP, RIPng et ISIS)
VLAN basés sur les ports
Listes de contrôle d'accès pour les adresses IPv6 (ACL6)
Protocoles IPv6 (TCP6, UDP6, ICMP6)
Support côté serveur (adresses IPv6 pour les serveurs virtuels, les services)
USIP (Utiliser l'adresse IP source) et DSR (Direct Server Return) pour IPv6
SNMP et CVPN pour IPv6

Fonctionnalités IPv6
HA avec adresse de nœud IPv6 native
Adresses IPv6 pour MIP
Découverte du Path-MTU pour IPv6

Mise en œuvre du support IPv6

Vous devez activer la fonctionnalité IPv6 sur une appliance NetScaler avant de pouvoir l'utiliser ou la configurer. Si IPv6 est désactivé, NetScaler ne traite pas les paquets IPv6. Il affiche l'avertissement suivant lorsque vous exécutez une commande non prise en charge :

```
"Warning: Feature(s) not enabled [IPv6PT]"
<!--NeedCopy-->
```

Utilisez l'une des procédures suivantes pour activer ou désactiver IPv6.

Procédures CLI

Pour activer ou désactiver IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

- activer la fonctionnalité ns ipv6pt
- désactiver la fonctionnalité ns ipv6pt

Procédures GUI

Pour activer ou désactiver IPv6 à l'aide de l'interface graphique :

1. Accédez à **Système** > **Paramètres**, dans le groupe **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.
2. Sélectionnez ou désactivez l'option **Traduction du protocole IPv6** .

Prise en charge de VLAN

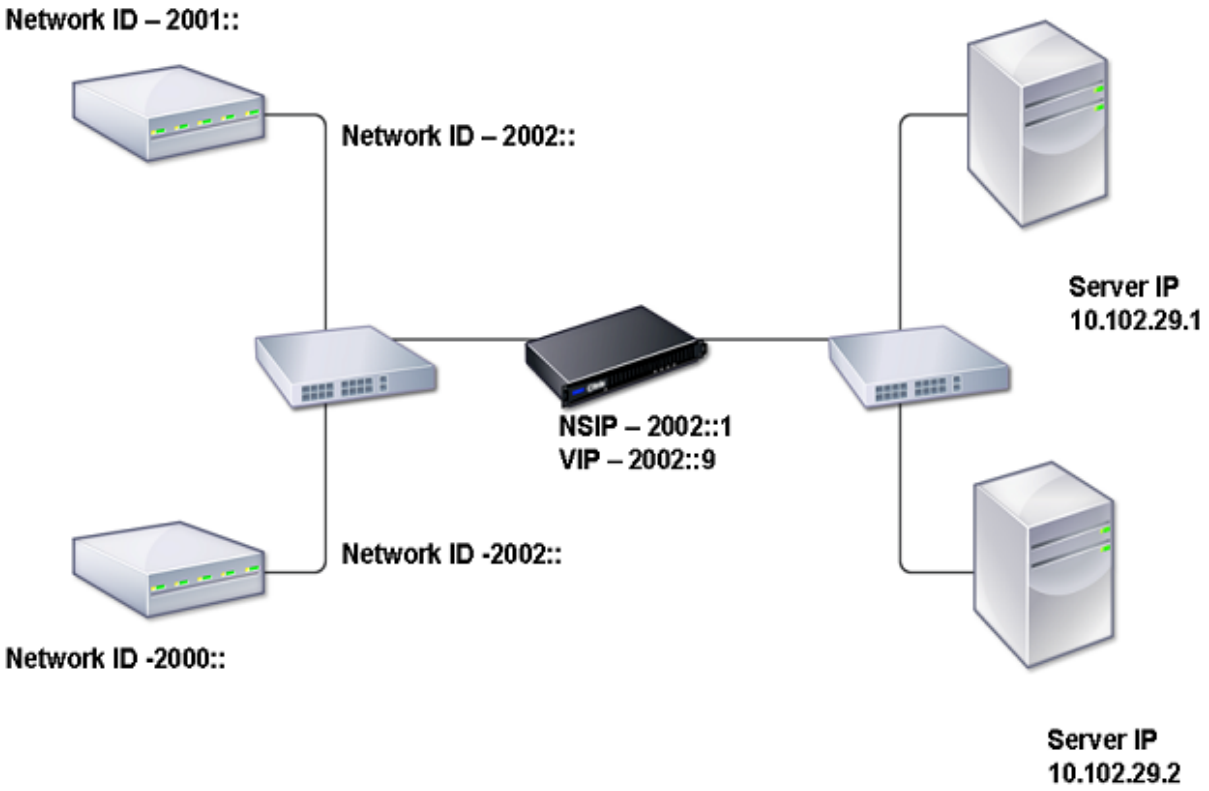
Si vous devez envoyer des paquets de diffusion ou de multidiffusion sans identifier le VLAN (par exemple, pendant DAD pour NSIP ou ND6 pour le saut suivant de l'itinéraire), vous pouvez configurer l'appliance NetScaler pour qu'elle envoie le paquet sur toutes les interfaces avec le balisage approprié. Le VLAN est identifié par ND6 et un paquet de données est envoyé uniquement sur le VLAN. Pour plus d'informations sur ND6 et les VLAN, voir Configuration de la découverte de voisins.

Les VLAN basés sur les ports sont courants pour IPv4 et IPv6. Les VLAN basés sur des préfixes sont pris en charge pour IPv6.

Scénario de déploiement simple

Vous trouverez ci-dessous un exemple de configuration d'équilibrage de charge simple composée d'un serveur virtuel IPv6 et de services IPv4, comme illustré dans le diagramme de topologie suivant.

Figure 1. Exemple de topologie IPv6



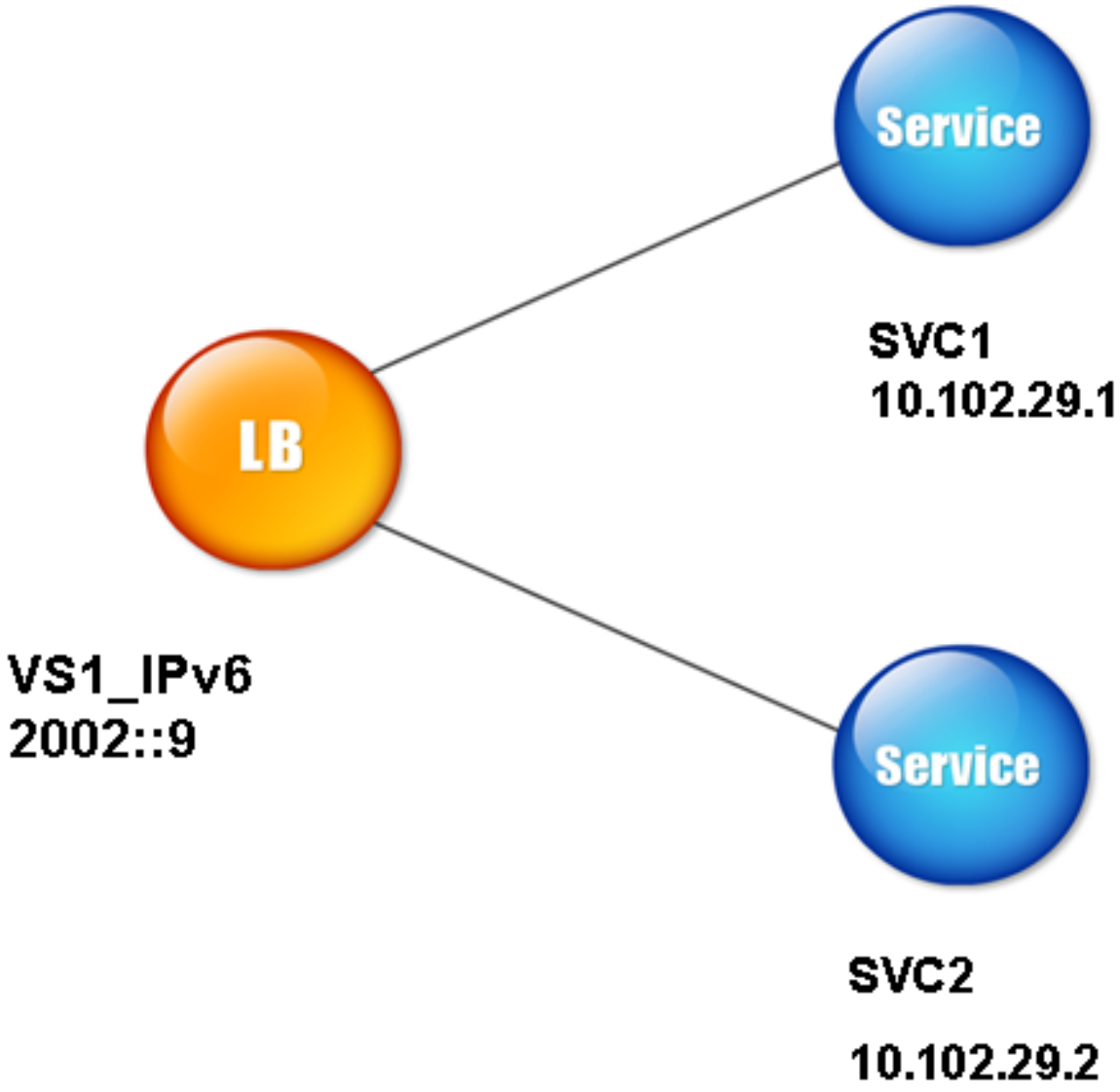
Le tableau suivant résume les noms et les valeurs des entités qui doivent être configurées sur NetScaler.

Tableau 2 Exemples de valeurs pour la création d'entités

Type d'entité	Nom	Valeur
Serveur virtuel LB	VS1_IPv6	2002::9
Services	SVC1	10.102.29.1
	SVC2	10.102.29.2

La figure suivante montre les entités et les valeurs des paramètres à configurer sur NetScaler.

Figure 2. Diagramme d'entité IPv6



Pour configurer ce scénario de déploiement, vous devez procéder comme suit :

1. Créez un service IPv6.
2. Créez un vserver LB IPv6.
3. Liez les services au vserver.

Procédures CLI

Pour créer des services IPv4 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter un service** <Name><IPAddress><Protocol><Port>
- **service sh** <Name>

Exemple :

```
1 > add service SVC1 10.102.29.1 HTTP 80
2 Done
3
4 >add service SVC2 10.102.29.2 HTTP 80
5 Done
6 <!--NeedCopy-->
```

Pour créer un serveur virtuel IPv6 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **ajouter lb vserver** <Name><IPAddress><Protocol><Port>
- **Serveur virtuel sh lab** <Name>

Exemple :

```
1 > add lb vserver VS1_IPv6 2002::9 HTTP 80
2 Done
3 <!--NeedCopy-->
```

Pour lier un service à un serveur virtuel LB à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **serveur vserver bind lb** <name><service>
- **Serveur virtuel sh lab** <name>

Exemple :

```
1 > bind lb vserver VS1_IPv6 SVC1
2 Done
3 <!--NeedCopy-->
```

Procédures GUI

Pour créer des services IPv4 à l'aide de l'interface graphique :

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, cliquez sur **Ajouter**, puis définissez les paramètres suivants :

- Service Name
- Adresse IP
- Protocole
- Port

Pour créer un serveur virtuel IPv6 à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, cliquez sur **Ajouter**et cochez la case **IPv6** .
2. Définissez les paramètres suivants :
    - Nom
    - Protocole
    - Type d'adresse IP
    - Adresse IP
    - Port

Pour lier un service à un serveur virtuel LB à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Sur la page **Serveurs virtuels d'équilibrage de charge**, sélectionnez le serveur virtuel auquel vous souhaitez lier le service (par exemple, VS1_IPv6).
3. Cliquez sur **Ouvrir**.
4. Dans la boîte de dialogue **Configurer le serveur virtuel (équilibrage de charge)**, sous l'onglet **Services**, cochez la case **Active** correspondant au service que vous souhaitez lier au vserver (par exemple, SVC1).
5. Cliquez sur **OK**.
6. Répétez les étapes 1 à 4 pour lier le service (par exemple, SVC2 au vserver).

Modification de l'en-tête de l'hôte

Lorsqu'une requête HTTP contient une adresse IPv6 dans l'en-tête de l'hôte et que le serveur ne comprend pas l'adresse IPv6, vous devez mapper l'adresse IPv6 à une adresse IPv4. L'adresse IPv4 est ensuite utilisée dans l'en-tête hôte de la requête HTTP envoyée au vserver.

Procédures CLI

Pour remplacer l'adresse IPv6 dans l'en-tête de l'hôte par une adresse IPv4 à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set ns ip6- carte** <IPv6Address><IPAddress>
- **sh ns ip6** <IPv6Address>

Exemple :

```
> set ns ip6 2002::9 -map 200.200.200.200
Done
<!--NeedCopy-->
```

Procédures GUI

Pour remplacer l'adresse IPv6 dans l'en-tête de l'hôte par une adresse IPv4 à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **IP** et, dans l'onglet **IPv6**, sélectionnez l'adresse IP pour laquelle vous souhaitez configurer une adresse IP mappée, par exemple 2002:0:0:0:0:0:9, puis cliquez sur Modifier.
2. Dans la zone de texte **IP mappée**, tapez l'adresse IP mappée que vous souhaitez configurer, par exemple 200.200.200.200.

Insertion VIP

Si une adresse IPv6 est envoyée à un serveur IPv4, le serveur risque de ne pas comprendre l'adresse IP figurant dans l'en-tête HTTP et de générer une erreur. Pour éviter cela, vous pouvez mapper une adresse IPv4 au VIP IPv6. Vous pouvez ensuite activer l'insertion VIP pour permettre l'insertion de l'adresse VIP IPv4 et du numéro de port dans les requêtes HTTP envoyées aux serveurs.

Procédures CLI

Pour configurer une adresse IPv6 cartographique à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

set ns ip6- carte <IPv6Address><IPAddress>

Exemple :

```
> set ns ip6 2002::9 -map 200.200.200.200
 Done
<!--NeedCopy-->
```

Pour activer l'insertion VIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ****set lb vserver - InsertVServerIPPort**** <name><Value>
- **Serveur virtuel sh lab** <name>

Exemple :

```
> set lb vserver VS1_IPv6 -insertVserverIPPort ON
 Done

<!--NeedCopy-->
```

Procédures GUI

Pour configurer une adresse IPv6 cartographique à l'aide de l'interface graphique :

1. **Accédez à**Système**>**Réseau**>**IP**, dans l'onglet**IPv6**, sélectionnez l'adresse IP pour laquelle vous souhaitez configurer une adresse IP cartographique, par exemple 2002:0:0:0:0:0:9, puis cliquez sur Modifier.**
2. Dans la zone de texte **IP mappée**, tapez l'adresse IP cartographique que vous souhaitez configurer, par exemple 200.200.200.200.

Pour activer l'insertion VIP à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez le serveur virtuel pour lequel vous souhaitez activer l'insertion de ports, puis cliquez sur **Modifier**.
2. Dans l'onglet **Avancé**, sous **Paramètres du trafic**, dans la liste déroulante **Insertion du port IP du serveur virtuel**, sélectionnez **VIPADDR**.
3. Dans la zone de texte **Insertion du port IP du serveur virtuel**, tapez l'en-tête vip.

Domaines de trafic

May 5, 2023

> **Avertissement**
>
> Citrix vous recommande d'utiliser les partitions d'administration au lieu d'utiliser les domaines de trafic. Pour plus d'informations, consultez la page Partitionnement administrateur .

Les domaines de trafic sont un moyen de segmenter le trafic réseau pour différentes applications. Vous pouvez utiliser des domaines de trafic pour créer plusieurs environnements isolés au sein d'une appliance NetScaler. Une application appartenant à un domaine de trafic spécifique communique avec les entités et traite le trafic au sein de ce domaine. Le trafic appartenant à un domaine de trafic ne peut pas franchir la limite d'un autre domaine de trafic.

Avantages de l'utilisation de Traffic Domains

Les principaux avantages de l'utilisation de domaines de trafic sur une appliance NetScaler sont les suivants :

- **Utilisation d'adresses IP dupliquées dans un réseau**. Les domaines de trafic vous permettent d'utiliser une adresse IP en double sur le réseau. Vous pouvez attribuer la même adresse IP ou la même adresse réseau à plusieurs appareils d'un réseau, ou à plusieurs entités d'une appliance NetScaler, à condition que chacune des adresses dupliquées appartient à un domaine de trafic différent.
- **Utilisation d'entités dupliquées sur l'appliance NetScaler.** Les domaines de trafic vous permettent également d'utiliser des entités de fonctionnalités NetScaler dupliquées sur l'appliance. Vous pouvez créer des entités avec les mêmes paramètres tant que chaque entité est affectée à un domaine de trafic distinct.
  Remarque : les entités dupliquées portant le même nom ne sont pas prises en charge.
- **Multilocation**. À l'aide des domaines de trafic, vous pouvez fournir des services d'hébergement à plusieurs clients en isolant le type de trafic applicatif de chaque client dans un espace d'adressage défini sur le réseau.

Un domaine de trafic est identifié de manière unique par un identifiant, qui est une valeur entière. Chaque domaine de trafic nécessite un VLAN ou un ensemble de VLAN. La fonctionnalité d'isolation du domaine de trafic dépend des VLAN liés au domaine de trafic. Plusieurs VLAN peuvent être liés à un domaine de trafic, mais le même VLAN ne peut pas faire partie de plusieurs domaines de trafic. Par conséquent, le nombre maximal de domaines de trafic pouvant être créés dépend du nombre de VLAN configurés sur l'appliance.

Domaine de trafic par défaut

Une appliance NetScaler possède un domaine de trafic préconfiguré, appelé domaine de *trafic par défaut*, dont l'ID est 0. Tous les paramètres et configurations d'usine font partie du domaine de trafic par défaut. Vous pouvez créer d'autres domaines de trafic, puis segmenter le trafic entre le domaine de trafic par défaut et chacun des autres domaines de trafic. Vous ne pouvez pas supprimer le domaine de trafic par défaut de l'appliance NetScaler. Toute entité d'entité que vous créez sans définir l'ID du domaine de trafic est automatiquement associée au domaine de trafic par défaut.

Remarque : Certaines fonctionnalités et configurations sont prises en charge uniquement dans le domaine de trafic par défaut. Ils ne fonctionnent pas dans les domaines de trafic autres que ceux par défaut. Pour obtenir la liste des fonctionnalités prises en charge dans tous les domaines de trafic, consultez la section Fonctionnalités NetScaler prises en charge dans les domaines de trafic.

Fonctionnement des domaines de trafic

À titre d'illustration des domaines de trafic, prenons un exemple dans lequel deux domaines de trafic, avec les ID 1 et 2, sont configurés sur l'appliance NetScaler NS1.

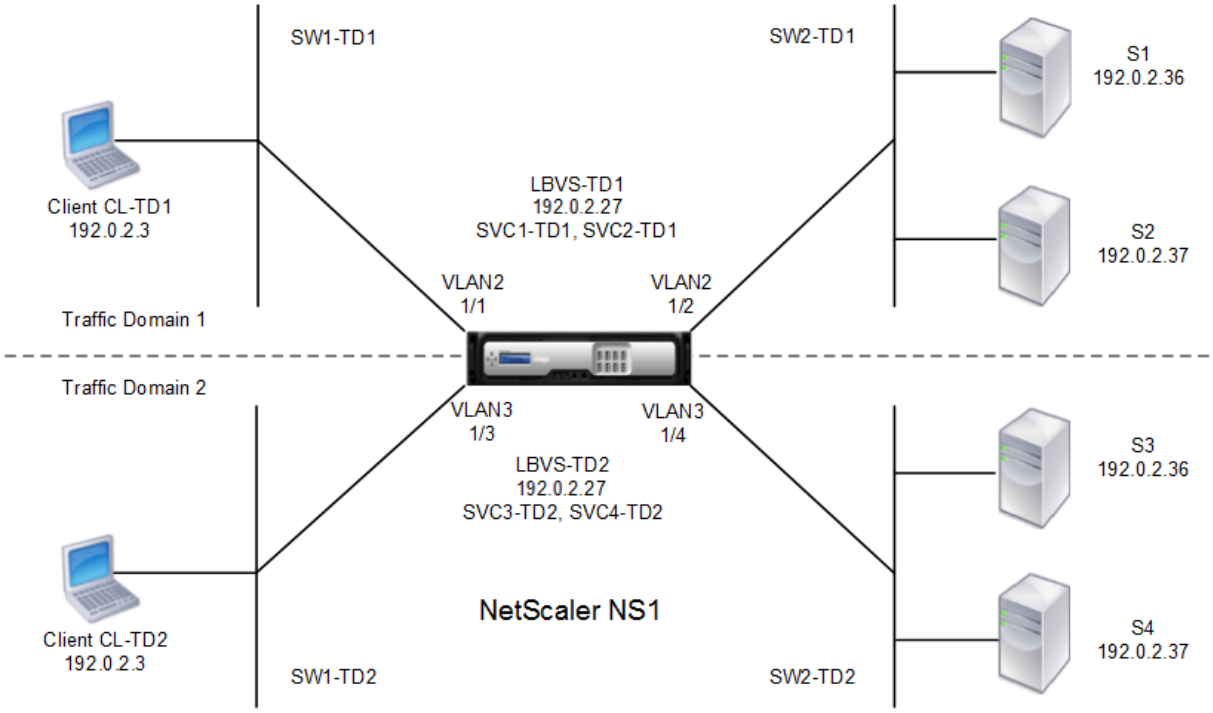
Dans le domaine de trafic 1, le serveur virtuel d'équilibrage de charge LBVS-TD1 est configuré pour équilibrer la charge du trafic entre les serveurs S1 et S2. Sur l'appliance NetScaler, les serveurs S1 et S2 sont représentés par les services SVC1-TD1 et SVC2-TD1, respectivement. Les serveurs S1 et S2 sont connectés à NS1 via le commutateur L2 SW2-TD1. Le client CL-TD1 se trouve sur un réseau privé connecté à NS1 via le commutateur L2 SW1-TD1. SW1-TD1 et SW2-TD1 sont connectés au VLAN 2 de NS1. Le VLAN 2 est lié au domaine de trafic 1, ce qui signifie que le client CL-TD1 et les serveurs S1 et S2 font partie du domaine de trafic 1.

De même, dans le domaine de trafic 2, le serveur virtuel d'équilibrage de charge LBVS-TD2 est configuré pour équilibrer la charge du trafic entre S3 et S4. Sur l'appliance NetScaler, les serveurs S3 et S4 sont représentés par les services SVC3-TD2 et SVC4-TD2, respectivement. Les serveurs S3 et S4 sont connectés à NS1 via le commutateur L2 SW2-TD2. Le client CL-TD2 se trouve sur un réseau privé connecté à NS1 via le commutateur L2 SW1-TD2. SW1-TD2 et SW2-TD2 sont connectés au VLAN 3 de NS1. Le VLAN 3 est lié au domaine de trafic 2, ce qui signifie que le client CL-TD2 et les serveurs S3 et S4 font partie du domaine de trafic 2.

Sur l'appliance NetScaler, les entités LBVS-TD1 et LBVS-TD2 partagent les mêmes paramètres, y compris l'adresse IP. Il en va de même pour SVC1-TD1 et SVC3-TD2, ainsi que pour SVC2-TD1 et SVC4-TD2. Cela est possible car ces entités se trouvent dans des domaines de trafic différents.

De même, les serveurs S1 et S3, S2 et S4 partagent la même adresse IP, et les clients CL-TD1 et CL-TD2 ont chacun la même adresse IP.

Figure 1. Fonctionnement des domaines de trafic



Le tableau suivant répertorie les paramètres utilisés dans l'exemple.

Entité	Nom	Détails
Paramètres du domaine de trafic 1		
VLAN liés au domaine de trafic 1	VLAN 2	ID VLAN : 2 interfaces liées : 1/1, 1/2
Client connecté à TD1	CL-TD1 (à titre de référence uniquement)	Adresse IP : 192.0.2.3
Serveur virtuel d'équilibrage de charge dans TD1	LBVS-TD1	Adresse IP : 192.0.2.27
Service lié au serveur virtuel LBVS-TD1	SVC1-TD1	Adresse IP : 192.0.2.36
Service lié au serveur virtuel LBVS-TD1	SVC2-TD1	Adresse IP : 192.0.2.37
SNIP	SNIP-TD1 (à des fins de référence uniquement)	Adresse IP : 192.0.2.27
Paramètres du domaine de trafic 2		

Entité	Nom	Détails
VLAN lié au domaine de trafic 2	VLAN 3	ID VLAN : 3 interfaces liées : 1/3, 1/4
Client connecté à TD2	CL-TD2 (à titre de référence uniquement)	Adresse IP : 192.0.2.3
Serveur virtuel d'équilibrage de charge dans TD2	LBVS-TD2	Adresse IP : 192.0.2.27
Service lié au serveur virtuel LBVS-TD2	SVC3-TD2	Adresse IP : 192.0.2.36
Service lié au serveur virtuel LBVS-TD2	SVC4-TD2	Adresse IP : 192.0.2.37
SNIP dans TD2	SNIP-TD2 (à des fins de référence uniquement)	Adresse IP : 192.0.2.29

Voici le flux de trafic dans le domaine de trafic 1 :

1. Le client CL-TD1 diffuse une demande ARP pour l'adresse IP 192.0.2.27 via le commutateur L2 SW1-TD1.
2. La demande ARP atteint NS1 sur l'interface 1/1, qui est liée au VLAN 2. Étant donné que le VLAN 2 est lié au domaine de trafic 1, NS1 met à jour la table ARP du domaine de trafic 1 pour l'adresse IP du client CL-TD1.
3. Étant donné que la demande ARP est reçue sur le domaine de trafic 1, NS1 recherche une entité configurée sur le domaine de trafic 1 dont l'adresse IP est 192.0.2.27. NS1 détecte qu'un serveur virtuel d'équilibrage de charge LBVS-TD1 est configuré sur le domaine de trafic 1 et possède l'adresse IP 192.0.2.27.
4. NS1 envoie une réponse ARP avec l'adresse MAC de l'interface 1/1.
5. La réponse ARP atteint CL-TD1. CL-TD1 met à jour sa table ARP pour l'adresse IP de LBVS-TD1 avec l'adresse MAC de l'interface 1/1 de NS1.
6. Le client CL-TD1 envoie une demande à 192.0.2.27. La demande est reçue par LBVS-TD1 sur le port 1/1 de NS1.
7. L'algorithme d'équilibrage de charge de LBVS-TD1 sélectionne le serveur S2, et NS1 ouvre une connexion entre un SNIP dans le domaine de trafic 1 (192.0.2.27) et S2.
8. S2 répond à SNIP 192.0.2.27 sur NS1.
9. NS1 envoie la réponse de S2 au client CL-TD1.

Voici le flux de trafic dans le domaine de trafic 2 :

1. Le client CL-TD2 diffuse une demande ARP pour l'adresse IP 192.0.2.27 via le commutateur L2 SW1-TD2.

2. La demande ARP atteint NS1 sur l'interface 1/3, qui est liée au VLAN 3. Étant donné que le VLAN 3 est lié au domaine de trafic 2, NS1 met à jour l'entrée de la table ARP du domaine de trafic 2 pour l'adresse IP du client CL-TD2, même si une entrée ARP pour la même adresse IP (CL-TD1) est déjà présente dans la table ARP du domaine de trafic 1.
3. Étant donné que la demande ARP est reçue dans le domaine de trafic 2, NS1 recherche dans le domaine de trafic 2 une entité dont l'adresse IP est 192.0.2.27. NS1 constate que le serveur virtuel d'équilibrage de charge LBVS-TD2 est configuré dans le domaine de trafic 2 et possède l'adresse IP 192.0.2.27. NS1 ignore LBVS-TD1 dans le domaine de trafic 1, même s'il possède la même adresse IP que LBVS-TD2.
4. NS1 envoie une réponse ARP avec l'adresse MAC de l'interface 1/3.
5. La réponse ARP atteint CL-TD2. CL-TD2 met à jour son entrée de table ARP pour l'adresse IP de LBVS-TD2 avec l'adresse MAC de l'interface 1/3 de NS1.
6. Le client CL-TD2 envoie une demande à 192.0.2.27. La demande est reçue par LBVS-TD2 sur l'interface 1/3 de NS1.
7. L'algorithme d'équilibrage de charge de LBVS-TD2 sélectionne le serveur S3, et NS1 ouvre une connexion entre un SNIP dans le domaine de trafic 2 (192.0.2.29) et S3.
8. S2 répond à SNIP 192.0.2.29 sur NS1.
9. NS1 envoie la réponse de S2 au client CL-TD2.

Fonctionnalités NetScaler prises en charge dans les domaines de trafic

Les fonctionnalités de NetScaler répertoriées dans la liste suivante sont prises en charge dans tous les domaines de trafic.

> **Important**
>
> Toute fonctionnalité NetScaler non répertoriée ci-dessous est prise en charge uniquement dans le domaine de trafic par défaut.

- Table ARP
- Tableau ND6
- Table Bridge
- Tous les types d'adresses IPv4 et IPv6
- Routes IPv4 et IPv6
- ACL et ACL6
- PBR & PBR6
- INAT
- RNAT
- RNAT6
- MSR
- MSR6
- Profils de réseau

- MIB SNMP
- Fragmentation
- Moniteurs (les moniteurs scriptables ne sont pas pris en charge)
- Commutation de contenu
- Redirection de cache
- Persistance (les groupes de persistance ne sont pas pris en charge)
- Service (les services basés sur le domaine ne sont pas pris en charge)
- Groupe de services (les groupes de services basés sur un domaine ne sont pas pris en charge)
- Politiques (*)
- PING
- TRACEROUTE
- PMTU
- Haute disponibilité (la mise en miroir des connexions n'est pas prise en charge)
- Cluster (pris en charge sur les clusters L2. Non pris en charge sur les clusters L3)
- Persistance des cookies
- MSS
- Journalisation (Syslog n'est pas pris en charge)
- Protection contre les surtensions
- Équilibrage de charge (Les types suivants ne sont pas pris en charge :)
  - TFTP
  - RTSP
  - Diameter
  - SIP
  - SMPP
- NAT46
- NAT64
- DNS64
- Règles de transfert de session
- SNMP

Remarque

- * Les stratégies n'ont pas de points de liaison globaux pour les domaines de trafic. Toutefois, les stratégies peuvent être liées à un serveur virtuel d'équilibrage de charge spécifique d'un domaine de trafic.
- Les fonctionnalités GSLB (Global Server Loading Balancing) et ADNS de NetScaler ne prennent pas en compte les domaines de trafic. Si la configuration GSLB doit être partagée entre tous les domaines de trafic, les méthodes GSLB Static Proximity et Round Trip Time (RTT) ne fonctionnent pas. Pour contourner ce scénario, vous pouvez utiliser des méthodes GSLB autres que RTT et Static Proximity. Pour plus d'informations, veuillez consulter

> http://support.citrix.com/article/CTX202277.

Configuration des domaines de trafic

La configuration d'un domaine de trafic sur l'appliance NetScaler comprend les tâches suivantes :

- **Ajoutez des VLAN.** Créez des VLAN et liez-leur des interfaces spécifiées.
- **Créez une entité de domaine de trafic et liez-y des VLAN.** Il s'agit des deux tâches suivantes :
  - Créez une entité de domaine de trafic identifiée de manière unique par un ID, qui est une valeur entière.
  - Liez les VLAN spécifiés à l'entité du domaine de trafic. Toutes les interfaces liées aux VLAN spécifiés sont associées au domaine de trafic. Plusieurs VLAN peuvent être liés à un domaine de trafic, mais un VLAN ne peut pas faire partie de plusieurs domaines de trafic.
- **Créez des entités d'entités sur le domaine de trafic**. Créez les entités d'entités requises dans le domaine de trafic. Les commandes CLI et les boîtes de dialogue de configuration de toutes les fonctionnalités prises en charge dans un domaine de trafic autre que celui par défaut incluent un paramètre appelé *identificateur de domaine de trafic* (td). Lors de la configuration d'une entité d'entités, si vous souhaitez que l'entité soit associée à un domaine de trafic particulier, vous devez spécifier le td. Toute entité d'entité que vous créez sans définir le td est automatiquement associée au domaine de trafic par défaut.

Pour vous donner une idée de la façon dont les entités d'entités sont associées à un domaine de trafic, cette rubrique couvre les procédures de configuration de toutes les entités mentionnées dans la figure intitulée How Traffic Domains Work.

L'interface de ligne de commande comporte deux commandes pour ces deux tâches, mais l'interface graphique les combine dans une seule boîte de dialogue.

Procédures CLI

Pour créer un VLAN et y lier des interfaces à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add vlan** <id>
- **bind vlan** <id> -**ifnum** <slot/port>
- **show vlan** <id>

Pour créer une entité de domaine de trafic et y lier des VLAN à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add ns trafficdomain** <td>
- **bind ns trafficdomain** <td> -**vlan** <id>

- **show ns trafficdomain** <td>

Pour créer un service à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add service** <name> <IP> <serviceType> <port> -**td** <id>
- **show service** <name>

Pour créer un serveur virtuel d'équilibrage de charge et y associer des services à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add lb vserver** <name> <serviceType> <IPAddress> <port> -**td** <id>
- **bind lb vserver** <name> <serviceName>
- **show lb vserver** <name>

Procédures GUI

Pour créer un VLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **VLAN**, cliquez sur **Ajouter**et définissez les paramètres.

Pour créer une entité de domaine de trafic à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Domaines de trafic**, cliquez sur **Ajouter**, puis dans la boîte de dialogue **Créer un domaine de trafic**, définissez les paramètres.

Pour créer un service à l'aide de l'interface graphique :

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, cliquez sur **Ajouter**et définissez les paramètres.

Pour créer un serveur virtuel d'équilibrage de charge à l'aide de l'interface graphique :

Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, cliquez sur **Ajouter**et définissez les paramètres.

Liaisons d'entités de domaine Inter Traffic

May 5, 2023

Vous pouvez lier les services d'un domaine de trafic à un serveur virtuel d'un autre domaine de trafic. Tous les services devant être liés à un serveur virtuel dans un domaine de trafic différent doivent résider dans le même domaine de trafic.

Vous configurez cette prise en charge à l'aide de la commande bind lb vserver existante ou de la procédure GUI associée.

Cette fonctionnalité peut faciliter l'interaction entre différents domaines de trafic. Dans une entreprise, les serveurs peuvent être regroupés selon différents domaines de trafic. Les serveurs virtuels sont créés dans un domaine de trafic faisant face à Internet. Un serveur virtuel de ce domaine de trafic peut être configuré pour équilibrer la charge des serveurs d'un autre domaine de trafic. Ce serveur virtuel reçoit des demandes de connexion provenant d'Internet à transmettre aux serveurs liés.

Lorsqu'un NetScaler est utilisé dans une infrastructure cloud, chaque locataire peut se voir attribuer un domaine de trafic distinct et toutes les ressources (y compris les serveurs) d'un locataire peuvent être regroupées dans le domaine de trafic du locataire. Pour chaque locataire, un serveur virtuel est créé pour les serveurs d'équilibrage de charge dans son domaine de trafic. Tous ces serveurs virtuels sont regroupés dans un seul domaine de trafic faisant face à Internet.

Prenons un exemple dans lequel le fournisseur de services cloud Example-Cloud-A possède trois domaines de trafic, avec les ID 10, 20 et 30, configurés sur l'appliance NetScaler NS1.

Example-Org-A et Example-Org-B sont des locataires d'Example-Cloud-A. Le domaine de trafic 20 est attribué au locataire A et le domaine 30 au locataire B. Les serveurs S1 et S2 résident dans le domaine de trafic 20 et les serveurs S3 et S4 résident dans le domaine de trafic 30.

Le domaine de trafic 10 fait face à Internet. Les serveurs virtuels LBVS-1 et LBVS-2 sont créés dans le domaine de trafic 10. LBVS-1, dans le domaine de trafic 10, est configuré pour équilibrer la charge des serveurs S1 et S2, qui se trouvent dans le domaine de trafic 20. LBVS-2, dans le domaine de trafic 10, est configuré pour équilibrer la charge des serveurs S3 et S4, qui se trouvent dans le domaine de trafic 30.

Par conséquent, ces serveurs virtuels acceptent les demandes de connexion Internet pour les serveurs qui se trouvent dans un domaine de trafic différent de celui des serveurs virtuels.

Domaines de trafic virtuels basés sur MAC

May 5, 2023

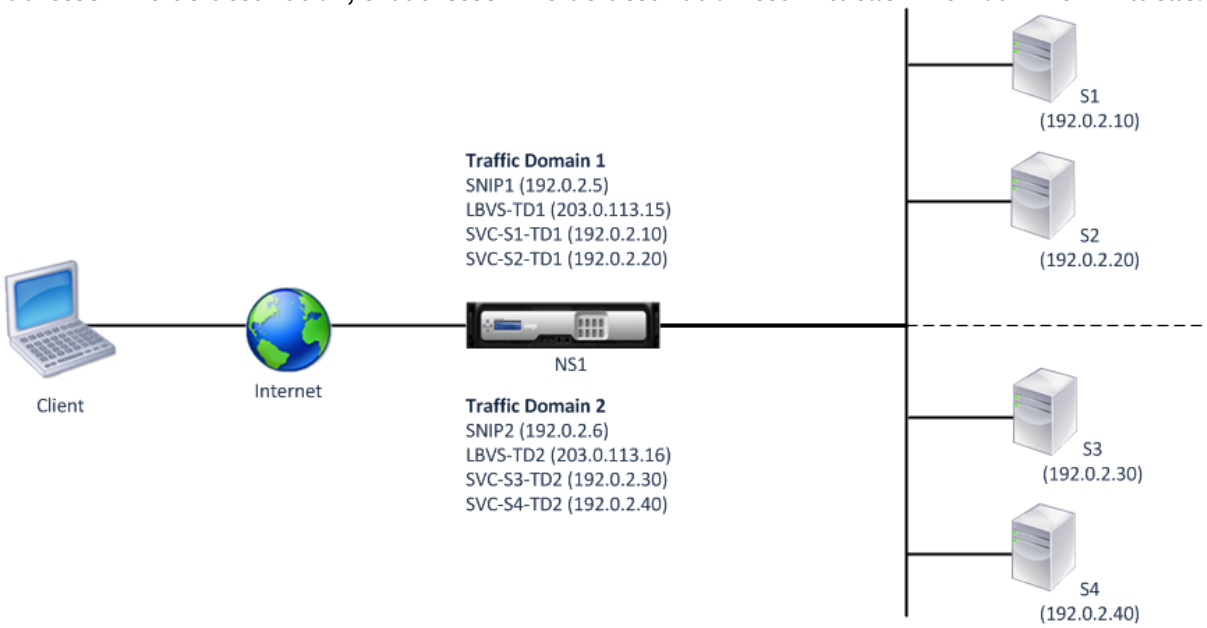
Vous pouvez associer un domaine de trafic à une adresse MAC virtuelle plutôt qu'à des VLAN. NetScaler envoie ensuite l'adresse MAC virtuelle du domaine de trafic dans toutes les réponses aux requêtes ARP pour les entités réseau de ce domaine. Par conséquent, l'ADC peut séparer le trafic entrant suivant pour différents domaines de trafic sur la base de l'adresse MAC de destination, car l'adresse MAC de destination est l'adresse MAC virtuelle d'un domaine de trafic. Après avoir créé des entités sur un domaine de trafic, vous pouvez facilement les gérer et les surveiller en effectuant des opérations au niveau du domaine de trafic.

Prenons un exemple dans lequel deux domaines de trafic, avec les ID 1 et 2, sont configurés sur l'appliance NetScaler NS1. NetScaler crée une adresse MAC virtuelle MAC1 et l'associe au domaine de trafic 1. De même, NetScaler a créé une autre adresse MAC virtuelle (virtuelle MAC2) et l'a associée au domaine de trafic 2.

Dans le domaine de trafic 1, le serveur virtuel d'équilibrage de charge LBVS-TD1 est configuré pour équilibrer la charge du trafic entre les serveurs S1 et S2. Sur l'appliance NetScaler, les serveurs S1 et S2 sont représentés par les services SVC1-TD1 et SVC2-TD1, respectivement. Une adresse IP de sous-réseau (SNIP) SNIP1 est configurée pour permettre à NetScaler de communiquer avec S1 et S2. Étant donné que le MAC1 virtuel est associé au domaine de trafic 1, l'appliance envoie le MAC1 virtuel en tant qu'adresse MAC dans toutes les annonces ARP et les réponses ARP pour LBVS-TD1 et SNIP1.

De même, dans le domaine de trafic 2, le serveur virtuel d'équilibrage de charge LBVS-TD2 est configuré pour équilibrer la charge du trafic entre S3 et S4. Sur l'appliance NetScaler, les serveurs S3 et S4 sont représentés par les services SVC3-TD2 et SVC4-TD2, respectivement. Une adresse SNIP SNIP2 est configurée pour permettre à NetScaler de communiquer avec S3 et S4. Étant donné que le MAC2 virtuel est associé au domaine de trafic 2, l'appliance envoie MAC2 virtuel en tant qu'adresse MAC dans toutes les annonces ARP et réponses ARP pour LBVS-TD2 et SNIP2.

NetScaler sépare le trafic entrant suivant pour les domaines de trafic 1 ou 2 sur la base de l'adresse MAC de destination, si l'adresse MAC de destination est virtuelle MAC1 ou MAC2 virtuelle.



Le tableau suivant répertorie les paramètres utilisés dans l'exemple : exemples de paramètres de domaine de trafic basé sur MAC virtuel.

Avant de commencer

Voici les points à prendre en compte avant de configurer un domaine de trafic virtuel basé sur un MAC :

1. les domaines de trafic virtuels basés sur MAC constituent le moyen le plus simple de séparer le trafic réseau.
2. Étant donné que les domaines de trafic basés sur des adresses MAC virtuelles séparent le trafic réseau en fonction des adresses MAC virtuelles et non des VLAN, vous ne pouvez pas créer d'adresses IP dupliquées sur différents domaines de trafic basés sur des MAC virtuels sur un NetScaler.
3. les domaines de trafic virtuels basés sur MAC ne fonctionnent pas lorsque NetScaler est déployé uniquement en mode L2.
4. Les domaines de trafic basés sur un VLAN et un MAC virtuel peuvent coexister sur un NetScaler. Les domaines de trafic basés sur un MAC virtuel s'exécutent en fait sur tous les VLAN qui ne sont liés à aucun domaine de trafic basé sur un VLAN.

Étapes de configuration

La configuration d'un domaine de trafic virtuel basé sur un MAC sur une appliance NetScaler comprend les tâches suivantes :

- Créez une entité de domaine de trafic et activez l'option MAC virtuel. Créez une entité de domaine de trafic identifiée de manière unique par un ID, qui est une valeur entière, puis activez l'option MAC virtuel. Après avoir créé l'entité de domaine de trafic, NetScaler crée une adresse MAC virtuelle puis l'associe à l'entité de domaine de trafic.
- Créez des entités d'entités sur le domaine de trafic. Créez les entités fonctionnelles requises dans le domaine de trafic en spécifiant l'identifiant du domaine de trafic (td) lors de la configuration de ces entités de fonctionnalité. Les entités réseau appartenant à NetScaler créées dans un domaine de trafic basé sur un MAC virtuel sont associées à l'adresse MAC virtuelle, qui est associée au domaine de trafic. NetScaler envoie ensuite l'adresse MAC virtuelle du domaine de trafic dans les annonces ARP et les réponses ARP pour ces entités réseau.

Procédures CLI

Pour créer un domaine de trafic virtuel basé sur un MAC à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- add ns trafficDomain <td> [-vmac (ACTIVÉ | DÉSACTIVÉ)]
- show ns trafficdomain <td>

Pour configurer une adresse SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ajouter ns ip <IPAddress><netmask>-type SNIP —td <id>
- montrez-nous l'adresse IP <IPAddress>-td <id>

Pour créer un service à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- add service <name> <IP> <serviceType> <port> -td <id>
- afficher le service <name>-td <id>

Pour créer un serveur virtuel d'équilibrage de charge et y associer des services à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- add lb vserver <name> <serviceType> <IPAddress> <port> -td <id>
- bind lb vserver <name> <serviceName>
- <name>afficher lb vserver -td <id>

Exemple :

```
> add ns trafficDomain 1 -vmac ENABLED
 Done
> add ns trafficDomain 2 -vmac ENABLED
 Done

> add ns ip 192.0.2.5 255.255.255.0 -type -SNIP -td 1
 Done
> add service  SVC-S1-TD1  192.0.2.10 HTTP 80 -td 1
 Done
> add service  SVC-S2-TD1  192.0.2.20 HTTP 80 -td 1
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.15 80 -td 1
 Done
> bind lb vserver  LBVS-TD1 SVC-S1-TD1
 Done
> bind lb vserver  LBVS-TD1 SVC-S2-TD1
 Done

> add ns ip 192.0.2.6 255.255.255.0 -type -SNIP -td 2
 Done
> add service  SVC-S3-TD2  192.0.2.30 HTTP 80 -td 2
 Done
> add service  SVC-S4-TD2  192.0.2.40 HTTP 80 -td 2
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.16 80 -td 1
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
```



```
30   Done
31 <!--NeedCopy-->
```

Procédures GUI

Pour créer un domaine de trafic virtuel basé sur un MAC à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > Interfaces.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Sur la page Créer un domaine de trafic, définissez les paramètres suivants :
   - ID de domaine de trafic*
   - Activer Mac
4. Cliquez sur Create.

Pour configurer une adresse SNIP à l'aide de l'interface graphique :

1. Accédez à Système > Réseau > IP > IPv4
2. Accédez à Réseau > IP > IPv4
3. Dans le volet de détails, cliquez sur Ajouter
4. Sur la page Créer une adresse IP, définissez les paramètres suivants. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
   - Adresse IP
   - Masque réseau
   - Type d'adresse IP
   - ID de domaine de trafic
5. Cliquez sur Create.

Pour créer un service à l'aide de l'interface graphique :

1. Accédez à Traffic Management > Load Balancing > Services.
2. Dans le volet de détails, cliquez sur Ajouter.
3. Sur la page Paramètres de base, définissez les paramètres suivants. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
   - Service Name
   - Serveur
   - Protocole
   - Port
   - ID de domaine de trafic
4. Cliquez sur Continuer, puis sur Terminé.
5. Répétez les étapes 2 à 4 pour créer un autre service.
6. Cliquez sur Fermer.

Pour créer un serveur virtuel d'équilibrage de charge et y lier des services à l'aide de l'interface graphique :

1. Accédez à Gestion du trafic > Équilibrage de charge > Serveurs virtuels.
2. Dans le volet Serveurs virtuels d'équilibrage de charge, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer des serveurs virtuels (équilibrage de charge), définissez les paramètres suivants. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
    - Nom
    - Adresse IP
    - Protocole
    - Port
    - ID de domaine de trafic
4. Cliquez sur Continuer. Dans le volet Service, cliquez sur >.
5. Sur la page Service, cliquez sur Insérer, puis cochez la case correspondant aux services que vous souhaitez lier au serveur virtuel.
6. Cliquez sur Continuer, puis sur Terminé.
7. Répétez les étapes 2 à 5 pour créer un autre serveur virtuel

VXLAN

May 9, 2023

Les appliances NetScaler prennent en charge les réseaux locaux virtuels extensibles (VXLAN). Un VXLAN superpose des réseaux de couche 2 à une infrastructure de couche 3 en encapsulant des trames de couche 2 dans des paquets UDP. Chaque réseau superposé est connu sous le nom de segment VXLAN et est identifié par un identifiant 24 bits unique appelé identifiant de réseau VXLAN (VNI). Seuls les périphériques réseau au sein du même VXLAN peuvent communiquer entre eux.

Les VXLAN fournissent les mêmes services réseau Ethernet de couche 2 que les VLAN, mais avec une extensibilité et une flexibilité accrues. Les deux principaux avantages de l'utilisation de VXLAN sont les suivants :

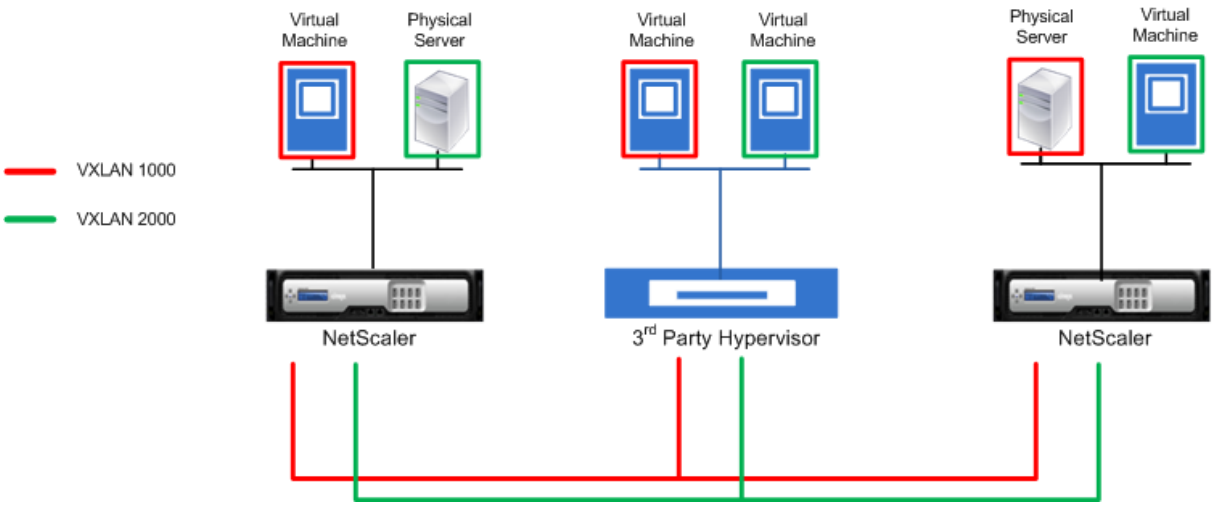
- **Évolutivité accrue.** La virtualisation des serveurs et les architectures de cloud computing ont considérablement augmenté la demande de réseaux de couche 2 isolés dans un centre de données. La spécification VLAN utilise un ID VLAN 12 bits pour identifier un réseau de couche 2. Vous ne pouvez donc pas aller au-delà de 4 094 VLAN. Ce nombre peut s'avérer insuffisant lorsque l'on a besoin de milliers de réseaux de couche 2 isolés. Le VNI 24 bits prend en charge jusqu'à 16 millions de segments VXLAN dans le même domaine administratif.
- **Flexibilité accrue.** Étant donné que le VXLAN transporte des trames de données de couche 2 sur des paquets de couche 3, les VXLAN étendent les réseaux L2 à différentes parties d'un

centre de données et à des centres de données géographiquement séparés. Les applications qui sont hébergées dans différentes parties d'un centre de données et dans différents centres de données mais qui font partie du même VXLAN apparaissent comme un seul réseau contigu.

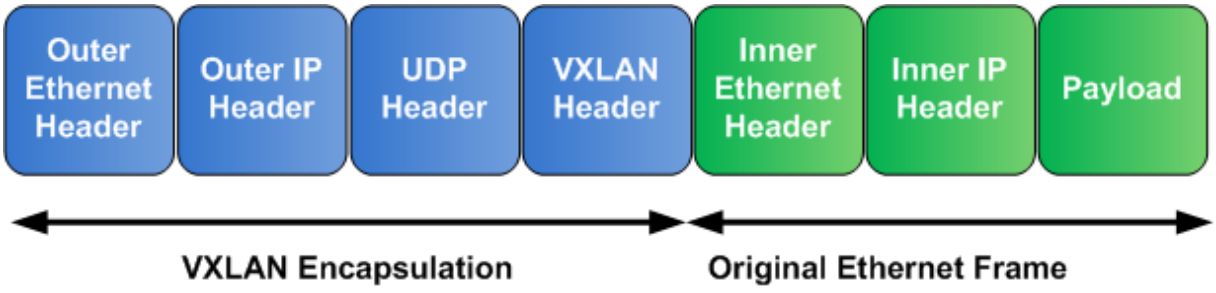
Comment fonctionnent les VXLAN

Les segments VXLAN sont créés entre les points de terminaison du tunnel VXLAN (VTEP). Les VTEP prennent en charge le protocole VXLAN et effectuent l'encapsulation et la désencapsulation du VXLAN. Vous pouvez considérer un segment VXLAN comme un tunnel entre deux VTEP, dans lequel un VTEP encapsule une trame de couche 2 avec un en-tête UDP et un en-tête IP et l'envoie via le tunnel. L'autre VTEP reçoit et désencapsule le paquet pour obtenir la trame de couche 2. Un NetScaler est un exemple de VTEP. D'autres exemples sont les hyperviseurs tiers, les machines virtuelles compatibles VXLAN et les commutateurs compatibles VXLAN.

L'illustration suivante montre des machines virtuelles et des serveurs physiques connectés via des tunnels VXLAN.



L'illustration suivante montre le format d'un paquet VXLAN.



Les VXLAN d'un NetScaler utilisent un mécanisme de couche 2 pour envoyer des trames de diffusion, de multidiffusion et de monodiffusion inconnues. Un VXLAN prend en charge les modes suivants pour envoyer ces trames L2.

- Mode**Unicast : dans ce mode**, vous spécifiez les adresses IP des VTEP lors de la configuration d'un VXLAN sur un NetScaler. Le NetScaler envoie des trames de diffusion, de multidiffusion et de monodiffusion inconnues via la couche 3 à tous les VTEP de ce VXLAN.
- Mode**multidiffusion : Dans ce mode**, vous spécifiez l'adresse IP d'un groupe de multidiffusion lors de la configuration d'un VXLAN sur un NetScaler. NetScalers ne prend pas en charge le protocole IGMP (Internet Group Management Protocol). Les NetScalers s'appuient sur le routeur en amont pour rejoindre un groupe de multidiffusion, qui partage une adresse IP de groupe de multidiffusion commune. Le NetScaler envoie des trames de diffusion, de multidiffusion et de diffusion unique inconnues via la couche 3 à l'adresse IP du groupe de multidiffusion de ce VXLAN.

À l'instar d'une table de pont de couche 2, NetScalers gère les tables de mappage VXLAN en fonction de l'en-tête interne et externe des paquets VXLAN reçus. Ce tableau met en correspondance les adresses MAC des hôtes distants et les adresses IP VTEP pour un VXLAN particulier. NetScaler utilise la table de mappage VXLAN pour rechercher l'adresse MAC de destination d'une trame de couche 2. Si une entrée pour cette adresse MAC est présente dans la table VXLAN, NetScaler envoie la trame de couche 2 sur la couche 3, à l'aide du protocole VXLAN, à l'adresse IP VTEP mappée spécifiée dans l'entrée de mappage pour un VXLAN.

Étant donné que les VXLAN fonctionnent de la même manière que les VLAN, la plupart des fonctionnalités NetScaler qui prennent en charge le VLAN en tant que paramètre de classification prennent en charge le VXLAN. Ces fonctionnalités incluent un paramètre VXLAN facultatif, qui spécifie le VNI VXLAN.

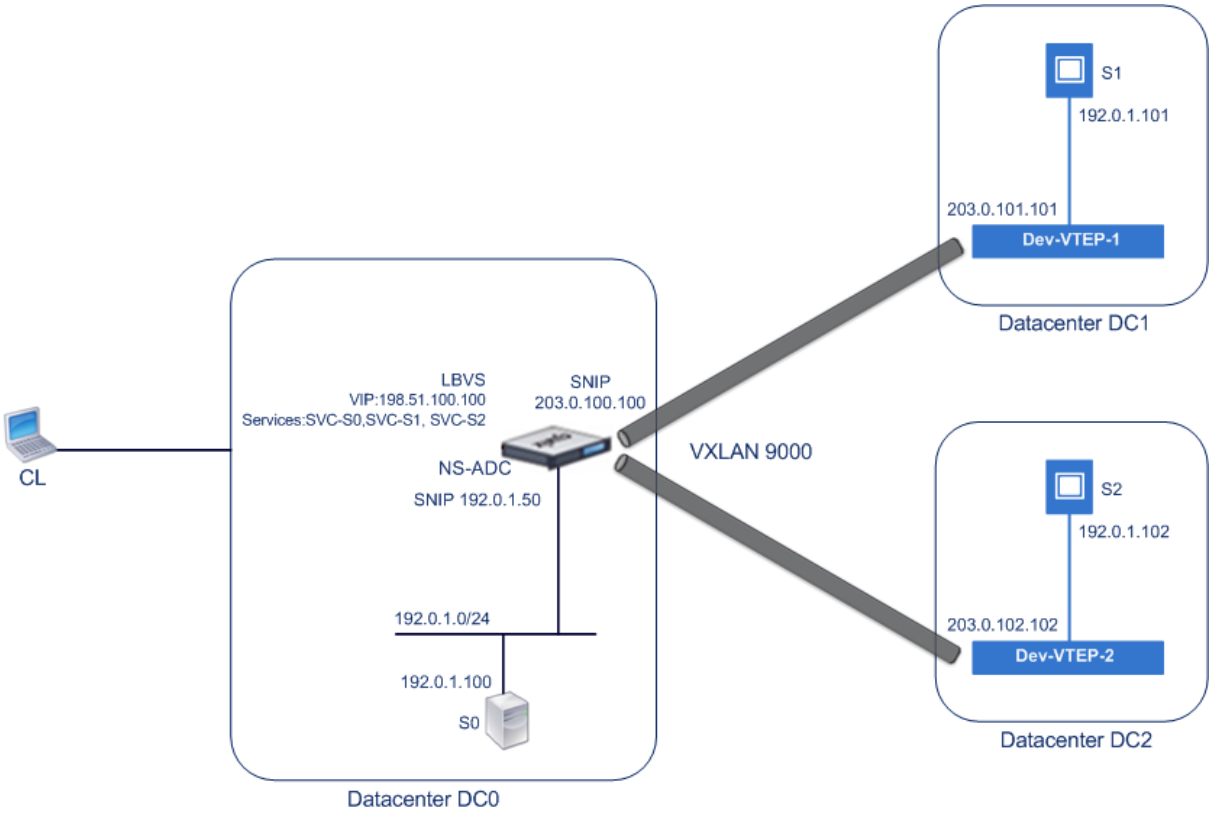
Dans une configuration haute disponibilité (HA), la configuration VXLAN est propagée ou synchronisée avec le nœud secondaire.

Cas d'utilisation du VXLAN : équilibrage de charge entre les centres de données

Pour comprendre les fonctionnalités VXLAN d'un NetScaler, prenons un exemple dans lequel Example Corp héberge un site à l'adresse www.example.com. Pour garantir la disponibilité des applications, le site est hébergé sur trois serveurs, S0, S1 et S2. Un serveur virtuel d'équilibrage de charge, LBVS, sur NetScaler NS-ADC est utilisé pour équilibrer la charge de ces serveurs. S0, S1 et S2 résident dans les centres de données DC0, DC1 et DC2, respectivement. Dans DC0, le serveur S0 est connecté à NS-ADC.

S0 est un serveur physique, tandis que S1 et S2 sont des machines virtuelles (VM). S1 s'exécute sur le périphérique hôte de virtualisation Dev-VTEP-1 dans le centre de données DC1 et S2 s'exécute sur le périphérique hôte Dev-VTEP-2 dans DC2. NS-ADC, Dev-VTEP-1 et Dev-VTEP-2 prennent en charge le protocole VXLAN.

S0, S1 et S2 font partie du même sous-réseau privé, 192.0.1.0/24. Si S0, S1 et S2 font partie d'un domaine de diffusion commun, le VXLAN 9000 est configuré sur NS-ADC, Dev-VTEP-1 et Dev-VTEP-2. Les serveurs S1 et S2 font partie du VXLAN9000 sur Dev-VTEP-1 et Dev-VTEP-2, respectivement.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple :
paramètres VXLAN.

Les services SVC-S0, SVC-S1 et SVC-S2 sur NS-ADC représentent S0, S1 et S2. Dès que ces services sont configurés, NS-ADC diffuse des requêtes ARP pour S0, S1 et S2 afin de résoudre le mappage IP-Mac. Ces requêtes ARP sont également envoyées via VXLAN 9000 à Dev-VTEP-1 et Dev-VTEP-2.

Le flux de trafic permettant de résoudre la demande ARP pour S2 est le suivant :

1. Le NS-ADC diffuse une requête ARP pour S2 afin de résoudre le mappage IP-Mac. Ce paquet contient :
   - Adresse IP source = Adresse IP du sous-réseau SNIP-for-Servers (192.0.1.50)
   - Adresse MAC source = adresse MAC de l'interface du NS-ADC à partir de laquelle le paquet est envoyé = NS-MAC-1
2. NS-ADC prépare le paquet ARP à envoyer via le VXLAN 9000 en encapsulant le paquet avec les en-têtes suivants :
   - En-tête VXLAN avec un ID (VNI) de 9000
   - En-tête UDP standard, somme de contrôle UDP définie sur 0 × 0000 et port de destination défini sur 4789.
3. NS-ADC envoie le paquet encapsulé résultant à Dev-VTEP-1 et Dev-VTEP-2 sur VXLAN-9000. Le paquet encapsulé contient :
   - Adresse IP source = SNIP-VTEP-0 (203.0.100.100).

4. Dev-VTEP-2 reçoit le paquet UDP et décapsule l'en-tête UDP, à partir duquel Dev-VTEP-2 apprend que le paquet est un paquet lié au VXLAN. Dev-VTEP-2 décapsule ensuite l'en-tête VXLAN et apprend l'ID VXLAN du paquet. Le paquet résultant est le paquet de requête ARP pour S2, identique à celui de l'étape 1.
5. À partir de l'en-tête interne et externe du paquet VXLAN, Dev-VTEP-2 crée une entrée dans sa table de mappage VXLAN qui montre le mappage de l'adresse MAC (NS-MAC-1) et du SNIP-VTEP-0 (203.0.100.100) pour VXLAN9000.
6. Dev-VTEP-2 envoie le paquet ARP à S2. Le paquet de réponse de S2 atteint Dev-VTEP-2. Dev-VTEP-2 effectue une recherche dans sa table de mappage VXLAN et obtient une correspondance pour l'adresse MAC de destination NS-MAC-1. Le Dev-VTEP-2 sait désormais que le NS-MAC-1 est accessible via SNIP-VTEP-0 (203.0.100.100) via VXLAN 9000.
7. S2 répond avec son adresse MAC (MAC-S2). Le paquet de réponse ARP contient :
    - Adresse IP de destination = Adresse IP du sous-réseau SNIP-for-Servers (192.0.1.50)
    - Adresse MAC de destination = NS-MAC-1
8. Le paquet de réponse de S2 atteint Dev-VTEP-2. Dev-VTEP-2 effectue une recherche dans sa table de mappage VXLAN et obtient une correspondance pour l'adresse MAC de destination NS-MAC-1. Le Dev-VTEP-2 sait désormais que le NS-MAC-1 est accessible via SNIP-VTEP-0 (203.0.100.100) via VXLAN 9000. Dev-VTEP-2 encapsule la réponse ARP avec des en-têtes VXLAN et UDP, et envoie le paquet résultant à SNIP-VTEP-0 (203.0.100.100) de NS-ADC.
9. À la réception du paquet, NS-ADC désencapsule le paquet en supprimant les en-têtes VXLAN et UDP. Le paquet résultant est la réponse ARP de S2. NS-ADC met à jour sa table de mappage VXLAN pour l'adresse MAC de S2 (MAC-S2) avec l'adresse IP de Dev-VTEP-2 (203.0.102.102) pour VXLAN 9000. NS-ADC met également à jour sa table ARP pour l'adresse IP de S2 (192.0.1.102) avec l'adresse MAC de S2 (MAC-S2).

Voici le flux de trafic pour le serveur virtuel d'équilibrage de charge LBVS dans cet exemple :

1. Le client CL envoie un paquet de demande au LBVS de NS-ADC. Le paquet de requête a :
    - Adresse IP source = adresse IP du client CL (198.51.100.90)
    - Adresse IP de destination = adresse IP (VIP) de LBVS = 198.51.110.100
2. Le LBVS de NS-ADC reçoit le paquet de requête et son algorithme d'équilibrage de charge sélectionne le serveur S2 du centre de données DC2.
3. NS-ADC traite le paquet de requête en remplaçant son adresse IP de destination par l'adresse IP de S2 et son adresse IP source par l'une des adresses IP de sous-réseau (SNIP) configurées sur NS-ADC. Le paquet de requête a :
    - Adresse IP source = Adresse IP du sous-réseau sur NS-ADC = SNIP-for-Servers (192.0.1.50)
    - Adresse IP de destination = adresse IP de S2 (192.0.1.102)
4. Le NS-ADC trouve une entrée de mappage VXLAN pour S2 dans sa table de pont. Cette entrée indique que S2 est accessible via Dev-VTEP-2 via VXLAN 9000.
5. NS-ADC prépare le paquet à envoyer via le VXLAN 9000 en encapsulant le paquet avec les entêtes suivants :

- En-tête VXLAN avec un ID (VNI) de 9000
- En-tête UDP standard, somme de contrôle UDP définie sur 0 × 0000 et port de destination défini sur 4789.

6. NS-ADC envoie le paquet encapsulé obtenu à Dev-VTEP-2. Le paquet de requête a :
   - Adresse IP source = adresse SNIP = SNIP-VTEP-0 (203.0.100.100)
   - Adresse IP de destination = adresse IP de Dev-VTEP-2 (203.0.102.102)
7. Dev-VTEP-2 reçoit le paquet UDP et décapsule l'en-tête UDP, à partir duquel Dev-VTEP-2 apprend que le paquet est un paquet lié au VXLAN. Dev-VTEP-2 décapsule ensuite l'en-tête VXLAN et apprend l'ID VXLAN du paquet. Le paquet résultant est le même que celui de l'étape 3.
8. Dev-VTEP-2 transmet ensuite le paquet à S2.
9. S2 traite le paquet de demande et envoie la réponse à l'adresse SNIP de NS-ADC. Le paquet de réponse contient :
   - Adresse IP source = adresse IP de S2 (192.0.1.102)
   - Adresse IP de destination = Adresse IP du sous-réseau sur NS-ADC = SNIP-for-Servers (192.0.1.50)
10. Dev-VTEP-2 encapsule le paquet de réponse de la même manière que NS-ADC a encapsulé le paquet de demande aux étapes 4 et 5. Dev-VTEP-2 envoie ensuite le paquet UDP encapsulé à l'adresse SNIP SNIP-for-Servers (192.0.1.50) de NS-ADC.
11. Lors de la réception du paquet UDP encapsulé, NS-ADC désencapsule le paquet en supprimant les en-têtes UDP et VXLAN de la même manière que Dev-VTEP-2 a désencapsulé le paquet à l'étape 7. Le paquet résultant est le même paquet de réponse qu'à l'étape 9.
12. NS-ADC utilise ensuite la table de session pour équilibrer la charge du serveur virtuel LBVS et transmet le paquet de réponse au client CL. Le paquet de réponse contient :
    - Adresse IP source = adresse IP du client CL (198.51.100.90)
    - Adresse IP de destination = adresse IP (VIP) de LBVS (198.51.110.100)

Points à prendre en compte lors de la configuration de VXLAN

Tenez compte des points suivants avant de configurer des VXLAN sur un NetScaler :

- Un maximum de 2048 VXLAN peuvent être configurés sur un NetScaler.
- Les VXLAN ne sont pas pris en charge dans un cluster.
- Les adresses IPv6 locales liées au lien ne peuvent pas être configurées pour chaque VXLAN.
- NetScalers ne prend pas en charge le protocole IGMP (Internet Group Management Protocol) pour former un groupe de multidiffusion. NetScalers s'appuie sur le protocole IGMP de son routeur en amont pour rejoindre un groupe de multidiffusion, qui partage une adresse IP de groupe de multidiffusion commune. Vous pouvez spécifier l'adresse IP d'un groupe de multidiffusion lors de la création d'entrées de table de pont VXLAN, mais le groupe de multidiffusion doit être configuré sur le routeur en amont. Le NetScaler envoie des trames de diffusion, de multidiffu-

sion et de diffusion unique inconnues via la couche 3 à l'adresse IP du groupe de multidiffusion de ce VXLAN. Le routeur en amont transmet ensuite le paquet à tous les VTEP qui font partie du groupe de multidiffusion.

- L'encapsulation VXLAN ajoute une surcharge de 50 octets à chaque paquet :

  En-tête Ethernet externe (14) + en-tête UDP (8) + en-tête IP (20) + en-tête VXLAN (8) = 50 octets

  Pour éviter la fragmentation et la dégradation des performances, vous devez ajuster les paramètres MTU de tous les périphériques réseau d'un chemin VXLAN, y compris les périphériques VXLAN VTEP, afin de gérer les 50 octets de surcharge contenus dans les paquets VXLAN.

  Important : les trames Jumbo ne sont pas prises en charge sur les appliances virtuelles NetScaler VPX, les appliances NetScaler SDX et les appliances NetScaler MPX 15000/17000. Ces appliances prennent en charge une taille MTU de seulement 1 500 octets et ne peuvent pas être ajustées pour gérer la surcharge de 50 octets des paquets VXLAN. Le trafic VXLAN peut être fragmenté ou subir une dégradation des performances si l'un de ces dispositifs se trouve sur le chemin VXLAN ou agit comme un périphérique VTEP VXLAN.
- Sur les appliances NetScaler SDX, le filtrage VLAN ne fonctionne pas pour les paquets VXLAN.
- Vous ne pouvez pas définir de valeur MTU sur un VXLAN.
- Vous ne pouvez pas lier des interfaces à un VXLAN.

Étapes de configuration

La configuration d'un VXLAN sur une appliance NetScaler comprend les tâches suivantes.

- **Ajoutez une entité VXLAN**. Créez une entité VXLAN identifiée de manière unique par un entier positif, également appelé identifiant réseau VXLAN (VNI). Au cours de cette étape, vous pouvez également spécifier le port UDP de destination du VTEP distant sur lequel le protocole VXLAN s'exécute. Par défaut, le paramètre du port UDP de destination est défini sur 4789 pour l'entité VXLAN. Ce paramètre de port UDP doit correspondre aux paramètres de tous les VTEP distants pour ce VXLAN. Vous pouvez également lier des VLAN à ce VXLAN. Le trafic (qui inclut les diffusions, les multidiffusions, les monodiffusions inconnues) de tous les VLAN liés est autorisé sur ce VXLAN. Si aucun VLAN n'est lié au VXLAN, NetScaler autorise le trafic de tous les VLAN, sur ce VXLAN, qui ne font partie d'aucun autre VXLAN.
- **Liez l'adresse IP VTEP locale à l'entité VXLAN**. Liez l'une des adresses SNIP configurées au VXLAN pour générer les paquets VXLAN sortants.
- **Ajoutez une entrée bridgetable.** Ajoutez une entrée bridgetable spécifiant l'ID VXLAN et l'adresse IP VTEP distante pour le VXLAN à créer.
- **(Facultatif) Liez différentes entités de fonctionnalités au VXLAN configuré**. Les VXLAN fonctionnent de la même manière que les VLAN. La plupart des fonctionnalités de NetScaler qui

prennent en charge le VLAN en tant que paramètre de classification prennent également en charge le VXLAN. Ces fonctionnalités incluent un paramètre VXLAN facultatif, qui spécifie le VNI VXLAN.

- **(Facultatif) Affichez la table de mappage VXLAN**. Affichez le tableau de mappage VXLAN, qui inclut les entrées de mappage entre l'adresse MAC de l'hôte distant et l'adresse IP VTEP d'un VXLAN particulier. En d'autres termes, un mappage VXLAN indique qu'un hôte est accessible via le VTEP sur un VXLAN particulier. NetScaler apprend les mappages VXLAN et met à jour sa table de mappage à partir des paquets VXLAN qu'il reçoit. NetScaler utilise la table de mappage VXLAN pour rechercher l'adresse MAC de destination d'une trame de couche 2. Si une entrée pour cette adresse MAC est présente dans la table VXLAN, NetScaler envoie la trame de couche 2 sur la couche 3, à l'aide du protocole VXLAN, à l'adresse IP VTEP mappée spécifiée dans l'entrée de mappage pour un VXLAN.

Procédures CLI

Pour ajouter une entité VXLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- **ajouter un vxlan** <id>
- **afficher vxlan**<id>

Pour lier l'adresse IP VTEP locale au VXLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- **lier vxlan** <id**- SRCip** <IPaddress>
- **afficher vxlan**<id>

Pour ajouter un bridgetable à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez

- **ajouter bridgetable** <ID**-**mac - vxlan**-**vtep** <macaddress><IPaddress>
- **afficher Bridgetable**

Pour afficher la table de transfert VXLAN à l'aide de la ligne de commande :

À l'invite de commande, tapez :

- **afficher Bridgetable**

Procédures GUI

Pour ajouter une entité VXLAN et lier une adresse IP VTEP locale à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **VXLAN, puis**ajoutez une nouvelle entité VXLAN ou modifiez une entité VXLAN existante.

Pour ajouter un bridgetable à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Table de pont**, définissez les paramètres suivants lors de l'ajout ou de la modification d'une entrée de table de pont VXLAN :

- MAC
- VTEP
- IDENTIFIANT VXLAN

Pour afficher la table de transfert VXLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **Table de pont**.

```
Example
> add vxlan 9000
Done
> bind vxlan 9000 -srcIP 203.0.100.100

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
   203.0.101.101

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
   203.0.102.102

Done
```

Prise en charge des protocoles de routage dynamique IPv6 sur les VXLAN

L'appliance NetScaler prend en charge les protocoles de routage dynamique IPv6 pour les VXLAN. Vous pouvez configurer différents protocoles de routage dynamique IPv6 (par exemple, OSPFv3, RIPng, BGP) sur des réseaux VXLAN à partir de la ligne de commande VTYSH. Une option IPv6 Dynamic Routing Protocol a été ajoutée au jeu de commandes VXLAN pour activer ou désactiver les protocoles de routage dynamique IPv6 sur un VXLAN. Après avoir activé les protocoles de routage dynamique IPv6 sur un VXLAN, les processus liés aux protocoles de routage dynamique IPv6 doivent être démarrés sur le VXLAN à l'aide de la ligne de commande VTYSH.

Pour activer les protocoles de routage dynamique IPv6 sur un VXLAN à l'aide de l'interface de ligne de commande :

- **ajouter vxlan** <ID>[- Routage**dynamique IPv6 (ACTIVÉ | DÉSACTIVÉ)**] ****
- **show vxlan**


```
In the following sample configuration, VXLAN-9000 is created and has
    IPv6 dynamic routing protocols enabled on it. Then, using the VTYSH
    command line, process for the IPv6 OSPF protocol is started on the
    VXLAN.

> add vxlan 9000 -ipv6DynamicRouting ENABLED

Done
> bind vxlan 9000 -srcIP 203.0.100.100

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
    203.0.101.101

Done
> VTYSH
NS# configure terminal
NS(config)# ns IPv6-routing
NS(config)# interface VXLAN-9000
NS(config-if)# ipv6 router OSPF area 3
```

Extension de VLAN de plusieurs entreprises vers un cloud à l'aide de cartes VXLAN-VLAN

Les tunnels CloudBridge Connector sont utilisés pour étendre le VLAN d'une entreprise vers un cloud. Les VLAN étendus par plusieurs entreprises peuvent avoir des identifiants de VLAN qui se chevauchent. Vous pouvez isoler les VLAN de chaque entreprise en les mappant à un VXLAN unique dans le cloud. Sur une appliance NetScaler, qui est le point de terminaison du connecteur CloudBridge dans le cloud, vous pouvez configurer une carte VXLAN-VLAN qui relie les VLAN d'une entreprise à un VXLAN unique dans le cloud. Les VXLAN prennent en charge le balisage VLAN pour étendre plusieurs VLAN d'une entreprise depuis CloudBridge Connector vers le même VXLAN.

Effectuez les tâches suivantes pour étendre les VLAN de plusieurs entreprises vers un cloud :

1. Créez une carte VXLAN-VLAN.
2. Liez la carte VXLAN-VLAN à une configuration de tunnel CloudBridge Connector basée sur un pont réseau ou sur PBR sur l'appliance NetScaler sur le cloud.
3. (Facultatif) Activez le balisage VLAN dans une configuration VXLAN.

Procédures CLI

Pour ajouter une carte VXLAN-VLAN à l'aide de l'interface de ligne de commande :

- **add vxlanVlanMap** <name>
- **show vxlanVlanMap** <name>

Pour lier un VXLAN et un VLAN à une carte VXLAN-VLAN à l'aide de l'interface de ligne de commande :

- **bind vxlanVlanMap** <name> [-**vxlan** <positive_integer> -**vlan** <int[-int]> …]
- **show vxlanVlanMap** <name>

Pour lier une carte VXLAN-VLAN à un tunnel CloudBridge Connector basé sur un pont réseau à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

si vous ajoutez un nouveau pont réseau :

- **add netbridge** <name> [-**vxlanVlanMap** <string>]
- **show netbridge** <name>

en cas de reconfiguration d'un pont réseau existant :

- **set netbridge** <name> [-**vxlanVlanMap** <string>]
- **show netbridge** <name>

Pour lier une carte VXLAN-VLAN à un tunnel CloudBridge Connector basé sur PBR à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

si vous ajoutez un nouveau PBR :

- **add pbr** <name> **ALLOW** (-**ipTunnel** <ipTunnelName> [-**vxlanVlanMap** <name>])
- **show pbr** <name>

si vous reconfigurez un PBR existant :

- **set pbr** <name> **ALLOW** (-**ipTunnel** <ipTunnelName> [-**vxlanVlanMap** <name>])
- **show pbr** <name>

Pour inclure des balises VLAN dans des paquets liés à un VXLAN à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez l'un des ensembles de commandes suivants.

si vous ajoutez un nouveau VXLAN :

- **add vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)
- **show vxlan** <vnid>

si vous reconfigurez un VXLAN existant :

- **set vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)
- **show vxlan** <vnid>

Procédures GUI

Pour ajouter une carte VXLAN-VLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > Carte VLAN **VXLAN, ajoutez une carte VLAN**VXLAN.

Pour lier une carte VXLAN-VLAN à un tunnel CloudBridge Connector basé sur Netbridge à l'aide de l'interface graphique :

Accédez à **Système** > **CloudBridge Connector** > Pont **réseau, sélectionnez une carte VXLAN-VLAN dans la liste déroulante des VLAN**VXLAN**tout en ajoutant un nouveau pont** réseau ou en reconfigurant un pont réseau existant.

Pour lier une carte VXLAN-VLAN à un tunnel CloudBridge Connector basé sur PBR à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau >**PBR****. Dans l'onglet Routage basé sur des politiques (PBR), sélectionnez une carte **VXLAN-VLAN dans la liste déroulante des VLAN VXLAN tout** en ajoutant un nouveau **PBR ou en reconfigurant** un PBR existant.

Pour inclure des balises VLAN dans des paquets liés à un VXLAN à l'aide de l'interface graphique :

Accédez à **Système** > **Réseau** > **VXLAN**, activez le **balisage VLAN interne** tout en ajoutant un nouveau VXLAN ou en reconfigurant un VXLAN existant.

```
> add vxlanVlanMap VXLANVLAN-DC1

Done

> bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3000 -vlan 3

Done

> bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3500 -vlan 4

Done

>add vxlanVlanMap VXLANVLAN-DC2

Done

> bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 8000 -vlan 3 4

Done

> set pbr PBR-CBC-DC-1-CLOUD ALLOW  -ipTunnel  CBC-DC-1-CLOUD -
    vxlanVlanMap VXLANVLAN-DC1

```



```
Done

> set pbr PBR-CBC-DC-2-CLOUD ALLOW  -ipTunnel  CBC-DC-2-CLOUD -
    vxlanVlanMap VXLANVLAN-DC2

Done
```

Tunnels Geneve

May 5, 2023

Une appliance NetScaler prend en charge le protocole Geneve (Generic Network Virtualization Encapsulation) tel que défini dans la RFC 8926.
La virtualisation des serveurs et l'architecture du cloud computing ont augmenté la demande de réseaux isolés de couche 2 dans un centre de données.

La limite VLAN de 4094 s'est révélée inadéquate et des protocoles d'encapsulation tels que VXLAN et NVGRE ont été introduits pour surmonter cette limite. Ces protocoles diffèrent principalement dans la mise en œuvre du plan de contrôle. Le protocole Geneve ne définit pas de spécifications pour le plan de contrôle. Le protocole laisse à l'implémentation le soin de définir les spécifications du plan de contrôle.

Le protocole Geneve est une technologie d'encapsulation qui vise à créer des réseaux superposés de couche 2 sur une infrastructure de couche 3 en encapsulant des trames de couche 2 dans des paquets UDP.

Un identifiant unique 24 bits appelé VNID identifie chaque VLAN. Seul le même ID de segment (VNID) peut communiquer entre eux. Une appliance NetScaler prend en charge l'encapsulation Geneve sur le port UDP 6081.

Il existe deux types de tunnels Geneve qui peuvent être créés :

- Les tunnels peuvent étendre un VLAN existant en mode L2 ou L3. En mode L2, le pontage se produit entre le VLAN et le tunnel et les entrées sont mises à jour dans la table des ponts.

  En mode L3, le proxy ARP entre en vigueur pour apprendre l'adresse MAC et les informations de tunnel de l'adresse client/serveur. La table ARP inclut les informations MAC et tunnel correspondantes.

- Le tunnel Geneve peut fonctionner avec différents VLAN en mode L3 en utilisant des routes basées sur des stratégies (PBR).
  Lorsqu'un paquet doit être envoyé à un hôte accessible sur un segment du tunnel de Genève, l'appliance NetScaler encapsule le paquet dans un en-tête du tunnel de Genève et l'envoie au point de terminaison du tunnel.

NetScaler peut également servir de point de terminaison de tunnel. Un point d'extrémité de tunnel part et termine les tunnels Geneve. Lorsque le mode de couche 2 est activé, l'appliance NetScaler fait office de point de terminaison du tunnel et relie les paquets entre les VLAN et les tunnels de Genève. NetScaler apprend le VNID et le point de terminaison du tunnel sur lesquels une adresse MAC est accessible. Il stocke ensuite ces informations dans la table de pontage.

Le tunnel Geneve est pris en charge dans les partitions d'administration NetScaler, les configurations haute disponibilité de NetScaler et les configurations de clusters NetScaler.

Dans une configuration haute disponibilité, une configuration de tunnel Geneve est propagée ou synchronisée vers le nœud secondaire. Dans une configuration de cluster, la configuration du tunnel Geneve (entrelacé) est identique et présente sur tous les nœuds de cluster.

Configuration des tunnels Geneve

La configuration d'un tunnel Geneve sur une appliance NetScaler comprend les tâches suivantes :

- Ajout d'un tunnel IP avec protocole
- Ajouter un pont en filet
- relier le tunnel Geneve au pont du réseau

Pour ajouter un tunnel IP avec le protocole Geneve à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add iptunnel** <name> <remote> <remoteSubnetMask> <local> -**protocol** <Geneve> -**destPort** <port> -**tosInherit** (**ENABLED** | **DISABLED**) -**vlanTagging** (**ENABLED** | **DISABLED**) -**vnid**
- **show iptunnel**

Pour ajouter un pont réseau à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add netbridge** <name>
- **show netbridge**

Pour lier le tunnel Geneve au Netbridge à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **bind netbridge** <name> -**vlan** <Vlan ID> -**tunnel** <tunnel name>
- **show netbridge**

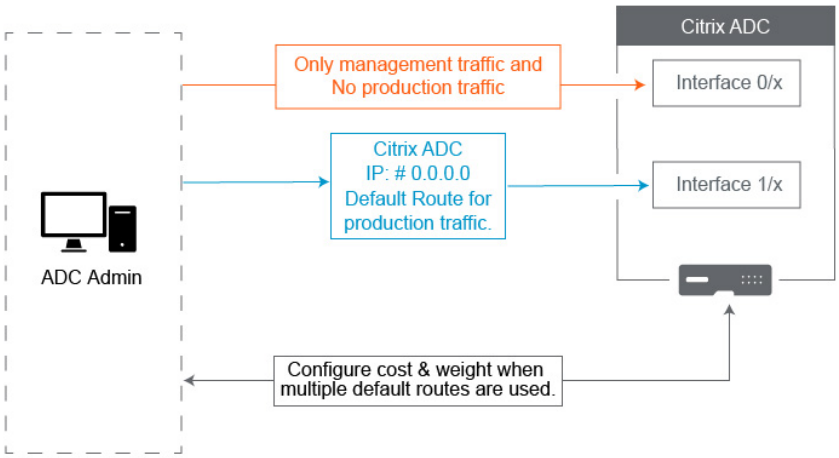
Meilleures pratiques pour les configurations réseau

May 5, 2023

Les sections suivantes décrivent certaines des meilleures pratiques pour configurer les fonctionnalités réseau sur une appliance NetScaler.

Routage et itinéraires par défaut

Voici quelques bonnes pratiques pour configurer les fonctionnalités de couche 3 sur une appliance NetScaler.



- **L'interface `0/x` d'une appliance NetScaler ou d'une appliance NetScaler SDX ne doit pas être utilisée**pour le trafic de production. Sur un MPX ou un SDX, les interfaces nommées `0/x` font référence aux interfaces de gestion. Cela ne signifie pas que vous devez utiliser ces interfaces pour la gestion. Cela signifie que ces interfaces ne sont PAS conçues pour le trafic de production. Ils ne disposent pas des mémoires tampon matérielles ni de l'optimisation nécessaires pour atteindre un débit soutenu de 1 Gbit/s. Par conséquent, si votre route par défaut se trouve dans le même sous-réseau que votre NSIP, vous devez soit modifier la route par défaut, soit utiliser une `1/x` interface pour votre réseau de gestion, car les `1/x` interfaces sont entièrement optimisées pour le trafic de production de 1 Gbit/s.

  > **Remarque** :
  >
  > Cela ne s'applique pas à une appliance NetScaler VPX.

  - **Option 1** Ne pas connecter aux interfaces `0/x` — Déconnectez le câble de l'interface `0/1`. NetScaler écoute le NSIP sur les autres interfaces. (REMARQUE : ce n'est pas une option pour SDX, car la SVM et XenServer ne peuvent communiquer qu'avec des interfaces) `0/x`
  - **Option 2**. Modifiez l'itinéraire par défaut vers une autre interface, comme indiqué dans la section suivante.

- **La passerelle par défaut (route 0.0.0.0) doit se trouver sur un réseau de production et non sur une interface quelconque `0/x`**. Lors de la première configuration d'un NetScaler, il vous

demande le NSIP, le masque de sous-réseau et l'adresse de la passerelle. Le problème que cela crée pour les administrateurs est qu'ils ont simplement configuré leur route par défaut pour qu'elle se trouve sur leur réseau de gestion à l'aide de l'interface 0/1.

- Pour vérifier quels sont vos itinéraires, exécutez l'interface de ligne de commande `show route` et votre passerelle par défaut est l'adresse IP de la ligne où le réseau et le masque de réseau sont 0.0.0.0. Voici un exemple où la passerelle se trouve sur la ligne 1 :

```
1  > sh route
2          Network          Netmask          Gateway/OwnedIP
               State   Traffic Domain  Type
3          -------          -------          ---------------
               -----   --------------  ----
4  1)      0.0.0.0          0.0.0.0          10.25.213.65     UP
            0               STATIC
5  2)      127.0.0.0        255.0.0.0        127.0.0.1        UP
            0               PERMANENT
6  3)      10.25.213.64     255.255.255.192  10.25.213.68     UP
            0               DIRECT
7  4)      172.16.0.0       255.255.255.0    172.16.0.1       UP
            0               DIRECT
8
9  <!--NeedCopy-->
```

- Pour vérifier l'interface et le VLAN utilisés pour votre passerelle par défaut, consultez le tableau ARP à l'aide de l'interface de ligne `sh arp` de commande. Vous pouvez également rechercher l'adresse IP spécifique à l'aide de `show arp | grep 10.25.213.65`. Voici un exemple dans lequel vous voyez que la passerelle 10.25.213.65 utilise l'interface 1/1 et le VLAN 1 :

```
1  > sh arp
2          IP               MAC                Iface VLAN
               Origin     TTL     Traffic Domain
3          --               ---                ----- ----
               ------     ---     --------------
4  1)      127.0.0.1        02:00:18:a4:00:1e  LO/1  1
       PERMANENT  N/A    0
5  2)      10.25.213.70     02:00:0f:46:00:28  1/1   1
       DYNAMIC    967    0
6  3)      10.25.213.68     02:00:18:a4:00:1e  LO/1  1
       PERMANENT  N/A    0
7  4)      10.25.213.67     02:00:0f:46:00:28  1/1   1
       DYNAMIC    641    0
8  5)      10.25.213.65     00:08:e3:ff:fd:90  1/1   1
       DYNAMIC    483    0
```



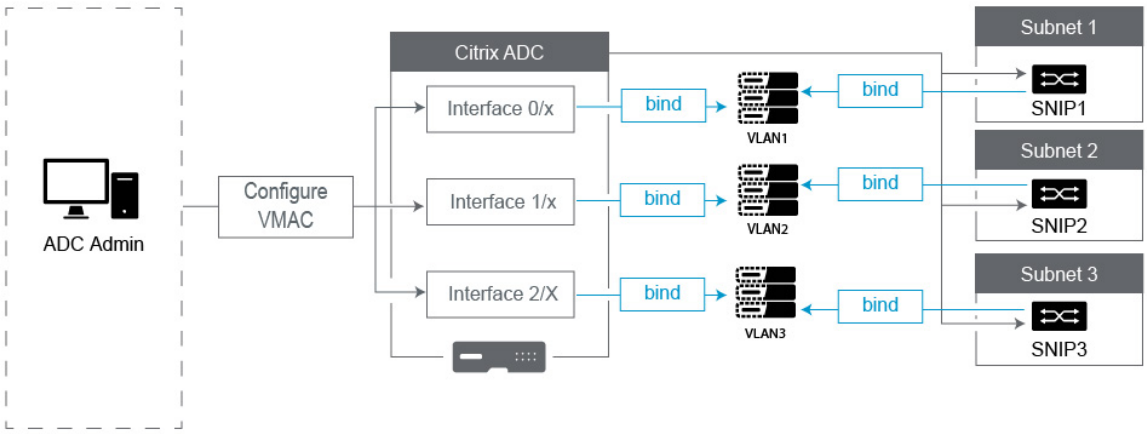
```
9   <!--NeedCopy-->
```

- Modifiez l'itinéraire par défaut pour utiliser une passerelle sur votre sous-réseau et votre interface de production. Supposons que votre réseau de gestion est 10.0.0.0/24 avec la passerelle 10.0.0.1 et que le réseau de production est 10.1.1.0/24 avec la passerelle 10.1.1.1. Configurez votre configuration comme suit :
  * SNIP : (Accès à la gestion désactivé) 10.1.1.2
  * NSIP : (Accès à la gestion activé) 10.0.0.2
  * Itinéraire par défaut : 0.0.0.0 0.0.0.0 10.1.1.1 (Système > Réseau > Itinéraires). Cela utilise un routeur sur le réseau SNIP au lieu du réseau NSIP.

    > **Remarque** :
    >
    > La modification de la passerelle par défaut peut interrompre le trafic de gestion, sauf si vous configurez des itinéraires statiques, un itinéraire basé sur des politiques ou si vous activez le transfert basé sur MAC.

Interfaces, canaux et VLAN

Voici quelques bonnes pratiques pour configurer les fonctionnalités de couche 2 sur une appliance NetScaler.



- **Ne connectez pas plusieurs interfaces/canaux au même VLAN, y compris le VLAN 1** :
  - Si vous ne configurez pas correctement vos VLAN, cela peut provoquer un routage de paquets inattendu sur votre réseau et une mise en boucle de couche 2 chaque fois que plusieurs interfaces actives sont associées au même VLAN (natif ou balisé).

- Par défaut, toutes les interfaces et tous les canaux se trouvent sur le VLAN natif 1. Cela peut créer deux problèmes :
  - NetScaler pense que tout le trafic reçu se trouve sur le même réseau. Il utilise donc n'importe quelle interface pour envoyer le trafic. Si vous avez un VLAN natif différent sur l'interface sur laquelle il a envoyé les données, le trafic ne sera pas acheminé comme prévu.
  - Si NetScaler reçoit des paquets de diffusion sur un port, il peut les retransmettre sur un autre port. Si les deux ports de commutation se trouvent sur le même VLAN, vous venez de créer une boucle de couche 2.
- Pour supprimer une interface/un canal du VLAN 1 :
  - Si vous n'utilisez pas de VLAN natifs sur l'interface de votre commutateur/canal de port. Remplacez le VLAN natif sur l'interface/le canal NetScaler par un numéro de VLAN inutilisé tel que 999. Vous ne devez pas utiliser le même numéro de VLAN inutilisé pour plusieurs canaux ou interfaces, car cela crée une boucle de couche 2.
  - Si vous utilisez des VLAN natifs sur l'interface de votre commutateur/canal de port. Modifiez le VLAN natif sur l'interface/le canal NetScaler en conséquence. Veillez toutefois à ne pas avoir plusieurs interfaces ou canaux actifs sur le même VLAN, car cela créerait des boucles de couche 2.
  - Vous ne pouvez pas supprimer le VLAN natif. Au lieu de cela, vous pouvez le modifier ou définir TagAll pour l'interface ou le canal. Si le port du commutateur n'est pas configuré avec un VLAN natif non balisé, activez tagall sur l'interface afin que les paquets de pulsations de haute disponibilité soient balisés.
- Pour afficher le VLAN natif sur une interface, exécutez l'interface de ligne `sh interface` de commande. Cela vous indiquera également si l'interface utilise l'option TAGALL.

- **Liez une interface à votre VLAN** : NetScaler, par défaut, n'attache pas de nouveau VLAN à une interface. Cela signifie que le VLAN ne sera pas utilisé tant que vous ne l'aurez pas lié à une interface. Lorsque le nouveau VLAN n'est pas lié à une interface et que ce VLAN est balisé, NetScaler supprime tout le trafic entrant depuis ce VLAN. De même, ne liez pas le même VLAN à plusieurs interfaces.
  - Liez des sous-réseaux à vos VLAN. Le NetScaler ne fonctionne pas comme un routeur classique. La plupart des routeurs relient des adresses IP à des interfaces. Sur un NetScaler, les adresses IP flottent sur n'importe quelle interface, sauf configuration contraire. Par conséquent, pour tout sous-réseau que vous souhaitez garantir que NetScaler envoie via un VLAN spécifique, en particulier lorsque NetScaler initie ce trafic, vous devez lier un SNIP au sein de ce sous-réseau au VLAN.
  - Un argument courant que nous entendons contre cela est que cela fonctionnait correcte-

ment par le passé et qu'il ne fonctionne plus maintenant sans lier le sous-réseau au VLAN. Cela se produit souvent parce que NetScaler apprend à quel VLAN envoyer le trafic, mais cela peut prendre du temps lorsqu'il construit ses tables ARP. Après un redémarrage ou une mise à niveau du microprogramme, lorsqu'il recommence à créer les tables ARP, il se peut qu'il apprenne initialement et qu'il utilise donc un chemin différent de celui que vous souhaitez, tel que votre itinéraire par défaut. Il est préférable de lui indiquer le chemin à emprunter en liant le SNIP au VLAN. Une fois qu'un SNIP est lié à un VLAN, l'ensemble du sous-réseau de ce SNIP est lié au VLAN.

  - Assurez-vous que chaque SNIP est lié à un VLAN (sauf dans les cas où vous avez plusieurs SNIP dans un sous-réseau, vous ne devez en lier qu'un seul) et que le VLAN, à son tour, est lié à une seule interface ou à un seul canal. Il est également souvent préférable d'avoir un SNIP dans chaque sous-réseau, mais cela n'est pas obligatoire car l'itinéraire le plus spécifique sera utilisé pour tout sous-réseau de destination qui ne possède pas de SNIP.

- Pour identifier le VLAN et l'interface utilisés par un sous-réseau :

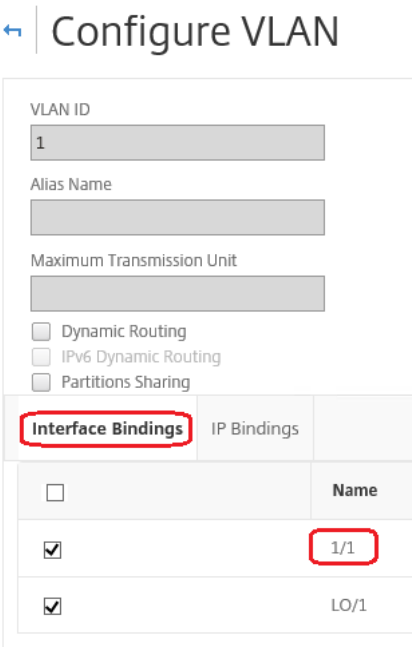
  1. Accédez à **Système > Réseau > VLAN**.
  2. Modifiez chaque VLAN configuré, à tour de rôle, jusqu'à ce que vous trouviez l'adresse IP correcte, comme expliqué à l'étape suivante.
  3. Cliquez sur l'onglet Liaisons IP pour voir quelle adresse IP, et donc quel sous-réseau, est lié et utilise donc ce VLAN.
  4. Une fois que vous avez identifié le VLAN auquel est liée une adresse IP, lorsque cette adresse IP se trouve dans le sous-réseau de l'itinéraire par défaut, cliquez sur les liaisons d'interface. Chaque interface ou canal lié à ce VLAN sera utilisé.

Exemple

Supposons que l'itinéraire par défaut est `0.0.0.0 0.0.0.0 10.1.1.1`.

Supposons que vous ayez deux SNIP 10.0.0.5 et 10.1.1.69. Étant donné que 10.1.1.69 se trouve dans le sous-réseau de l'itinéraire par défaut, c'est celui que vous souhaitez rechercher. Dans les captures d'écran ci-dessous, nous examinons le VLAN 1 et nous voyons que l'adresse IP 10.1.1.69 est liée à ce VLAN. Nous savons donc que nous recherchons le bon VLAN.

Cliquez maintenant sur Interface Bindings. Dans les liaisons de l'interface VLAN, nous voyons que l'interface `1/1` est utilisée pour ce sous-réseau et est donc utilisée pour la route par défaut.



> **REMARQUE** :
>
> Si aucune adresse IP n'est liée à vos VLAN, elle sera envoyée par défaut au VLAN 1. Dans ce cas, regardez quelles interfaces sont liées au VLAN 1. Cela signifie également que NetScaler n'utilisera pas vos VLAN configurés pour le trafic qu'il initie à moins que vous ne liez une adresse IP au nouveau VLAN.

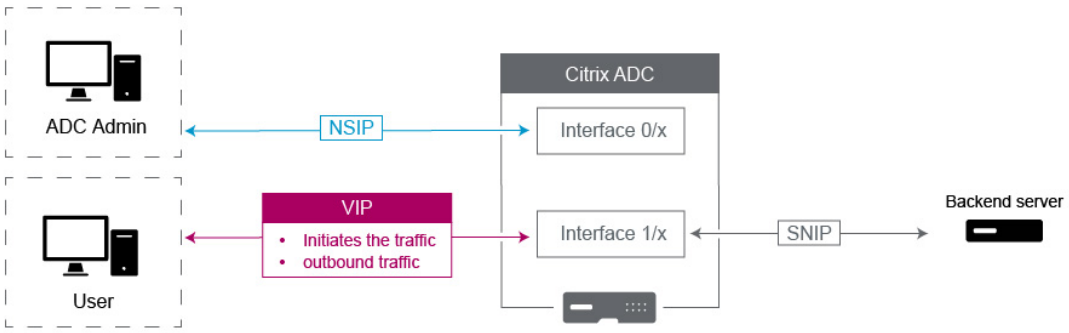
ARP gratuit

Si GARP ne fonctionne pas, utilisez VMAC - Par défaut, NetScaler utilise GARP pour annoncer ses liaisons d'adresses IP à MAC à d'autres périphériques réseau. Cela fonctionne généralement sans problème. Toutefois, à mesure que vous créez de nouveaux services dans NetScaler, vous pouvez rencontrer des problèmes lors du basculement sur une paire HA. Le problème le plus courant est que les services restent indisponibles dans le NetScaler auquel vous avez basculé parce que certains périphériques réseau n'ont pas mis à jour leurs tables ARP avec la nouvelle adresse MAC. Vous pouvez facilement le vérifier en consultant leurs tables ARP pour voir si les adresses MAC correspondent à celles du NetScaler désormais principal. Dans ce cas, il est fort probable que certains de vos appareils réseau limitent le nombre de publicités GARP qu'ils diffusent. Dans ce cas, il est nécessaire de configurer le VMAC sur toutes vos interfaces et/ou canaux actifs. Si vous prévoyez d'avoir une configuration importante sur votre NetScaler, il peut être préférable de configurer VMAC pour toutes les interfaces et tous les canaux lors du déploiement initial.

> **REMARQUE** : N'
>
> oubliez pas de configurer le VMAC pour l'interface ou le canal utilisé par votre itinéraire par défaut.

Adresses IP détenues par NetScaler

Cette section décrit les meilleures pratiques pour configurer les adresses IP appartenant à NetScaler :



- **IP NetScaler (NSIP)** : cette adresse IP est généralement utilisée pour la gestion car il s'agit de la seule adresse IP unique à un NetScaler individuel dans un environnement HA ou de cluster. Il est également important de noter que le trafic LDAP, RADIUS et User scripted Monitor (tel que le moniteur LDAP et le moniteur StoreFront) provient du NSIP et est donc acheminé via le VLAN et l'interface auxquels le NSIP est lié (VLAN natif par défaut 1). Si vous avez besoin du trafic LDAP et RADIUS pour provenir du SNIP, créez un serveur virtuel LB pour vos serveurs principaux.
- **IP du sous-réseau (SNIP)** : cette adresse IP est utilisée pour initier la communication avec les serveurs principaux et est toujours à l'origine du trafic. Cela dit, il peut être la destination du trafic dans les cas suivants :
  - Elle peut être utilisée comme adresse de passerelle sur d'autres appareils lors du routage de couche 3 sur NetScaler.
  - Il peut, lorsqu'il est activé, accepter des services de gestion, tels que l'accès à l'interface graphique, au SSH et au SNMP.
- **IP virtuelle (VIP)** : Le VIP est unique en ce sens qu'il ne sera jamais utilisé pour initier du trafic sortant. Il est destiné à recevoir du trafic uniquement. Une fois qu'il reçoit du trafic, il répond et renvoie le trafic sortant au client. En d'autres termes, l'adresse VIP ne déclenche pas le trafic sortant.

Notez que cela signifie également qu'il n'est pas utilisé comme source pour communiquer avec les serveurs back-end utilisés dans, par exemple, un serveur virtuel LB.

Configuration pour générer le trafic de données NetScaler FreeBSD à partir d'une adresse SNIP

May 9, 2023

Certaines fonctionnalités de données NetScaler s'exécutent sur le système d'exploitation FreeBSD sous-jacent plutôt que sur le système d'exploitation NetScaler. Pour cette raison, ces fonctionnalités envoient du trafic provenant de l'adresse IP NetScaler (NSIP) plutôt que d'une adresse SNIP. L'approvisionnement du trafic de données à partir de l'adresse NSIP n'est pas souhaitable si votre configuration comporte des configurations permettant de séparer l'ensemble du trafic de gestion et du trafic de données.

Les fonctionnalités de données NetScaler suivantes s'exécutent sur le système d'exploitation FreeBSD sous-jacent et envoient du trafic provenant de l'adresse IP NetScaler (NSIP) :

- Moniteurs scriptables d'équilibrage de charge
- Synchronisation automatique GSLB

Pour résoudre ce problème, vous pouvez utiliser le paramètre global Layer-2 :. `useNetprofileBSDtraffic` Lorsque vous activez ce paramètre, les fonctionnalités NetScaler envoient du trafic provenant de l'une des adresses SNIP d'un profil réseau associé à la fonctionnalité.

Avant de commencer

Avant de configurer l'appliance NetScaler pour générer le trafic associé aux fonctionnalités NetScaler à partir d'une adresse SNIP, notez les points suivants :

- Actuellement, le paramètre global de couche 2 n' `useNetprofileBSDtraffic` est pris en charge que pour les moniteurs scriptables d'équilibrage de charge.

  Pour configurer l'appliance NetScaler afin de générer le trafic de synchronisation automatique GSLB à partir d'une adresse SNIP, vous pouvez utiliser des règles ACL étendues et des règles RNAT comme solution de contournement.

- La `useNetprofileBSDtraffic` prise en charge des moniteurs scriptables d'équilibrage de charge s'applique uniquement aux profils réseau liés aux services associés. Le `useNetprofileBSDtraffic` support n'est pas applicable aux profils réseau liés aux groupes de services associés.

  En d'autres termes, l'appliance NetScaler n'utilise aucune adresse SNIP provenant des profils réseau liés aux groupes de services pour l'approvisionnement du trafic des moniteurs scriptables d'équilibrage de charge.

- La `useNetprofileBSDtraffic` prise en charge ne s'applique pas aux services SSL.

En d'autres termes, l'appliance NetScaler n'utilise aucune adresse SNIP provenant des profils réseau liés aux services SSL pour l'approvisionnement du trafic des moniteurs scriptables d'équilibrage de charge.

Configurer l'appliance NetScaler pour qu'elle source le trafic des moniteurs scriptables à partir d'une adresse SNIP

La configuration de l'appliance NetScaler pour qu'elle source le trafic des moniteurs scriptables à partir d'une adresse SNIP comprend les tâches suivantes :

- Activez le paramètre global Layer-2. `useNetprofileBSDtraffic`
- Créez un profil réseau et liez-y au moins une adresse SNIP.
- Liez le profil réseau aux services d'équilibrage de charge qui utilisent des moniteurs scriptables.

Pour activer le paramètre Layer-2 UsenetProfileBSDTraffic à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **set l2param**-UsenetProfileBSDTraffic**(ACTIVÉ/DÉSACTIVÉ)****
- **afficher l2param**

Pour créer un profil réseau et y lier des adresses SNIP à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- ****ajouter NetProfile - SRCip**** <name><string>
- **afficher NetProfile**

Pour lier un profil réseau à un service d'équilibrage de charge à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **définir le service** <name>-**NetProfile** <string>
- **show service** <name>

Exemple de configuration

L'exemple de configuration suivant permet à une appliance NetScaler d'approvisionner le trafic de moniteurs scriptables provenant d'une adresse SNIP. Un profil réseau NETPROFILE-1 est configuré avec l'adresse SNIP 198.51.100.20 liée à celui-ci. Un moniteur utilisateur/scriptable USER-MONITOR-1 est créé et est lié à un service d'équilibrage de charge SERVICE-1. NETPROFILE-1 est lié à SERVICE-1. L'appliance NetScaler fournit tous les paquets de surveillance scriptables de USER-MONITOR-1 à partir de l'adresse SNIP 198.51.100.20.


```
set l2param -useNetprofileBSDtraffic ENABLED

set netprofile NETPROFILE-1 -srcip 198.51.100.20

add lb monitor USER-MONITOR-1 USER -scriptName nsftp.pl -scriptArgs "
    file=Index.png;user=nsroot;password=nsroot" -dispatcherIP 127.0.0.1
    -dispatcherPort 3013 -destIP 203.0.113.90 -destPort 21

bind service SERVICE-1 -monitorName USER-MONITOR-1

set service SERVICE-1 -netProfile NETPROFILE-1

<!--NeedCopy-->
```

Configurer l'appliance NetScaler pour qu'elle génère le trafic de synchronisation automatique GSLB à partir d'une adresse SNIP

La configuration de l'appliance NetScaler pour qu'elle génère le trafic de synchronisation automatique GSLB à partir d'une adresse SNIP comprend les tâches de contournement suivantes :

- **Créez une règle ACL étendue**. Une règle ACL étendue identifie les paquets de synchronisation automatique GSLB. Cette identification est basée sur l'adresse IP source et l'adresse IP de destination.
- **Appliquez des ACL.** L'application des ACL active la règle ACL nouvellement créée.
- **Créez une règle RNAT basée sur une ACL**. Une règle RNAT modifie l'adresse IP source de ces paquets de l'adresse NSIP à une adresse SNIP.

> **Remarque :**
>
> Dans une configuration de haute disponibilité ou de cluster, vous devez ajouter des règles ACL et RNAT pour toutes les adresses NSIP de la configuration.

Pour créer une ACL étendue à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add acl** <aclname> **ALLOW** -**srcIP** = <NSIP address> -**destIP** = <destination IP address of the packets>
- **show acl** <aclName>

Pour appliquer des ACL étendues à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **apply acls**

Pour créer une règle RNAT basée sur une ACL à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- **add rnat** <name> <aclname>
- **bind rnat** <name> -**natIP** <SNIP address - source IP address for the packets>
- **show rnat** <name>

Exemple de configuration

L'exemple de configuration suivant permet à une appliance NetScaler de générer du trafic de synchronisation automatique GSLB à partir d'une adresse SNIP. L'ACL-2 identifie les paquets de synchronisation automatique GSLB, qui proviennent de l'adresse NSIP 192.0.1.20 et destinés à l'adresse IP du site GSLB 203.0.113.20. RNAT-2 change l'adresse IP source en adresse SNIP 198.51.100.20 pour ces paquets identifiés.

```
add acl ACL-2 ALLOW -srcIP = 192.0.1.20  -destIP = 203.0.113.20

apply acls

add rnat RNAT-2 ACL-2

bind rnat RNAT-2 -natIP 198.51.100.20
<!--NeedCopy-->
```

Observabilité

July 7, 2023

En raison de la complexité croissante des applications modernes, la surveillance et le dépannage des applications constituent de plus en plus de défis pour les équipes informatiques. Il est également plus important pour les équipes de développement de logiciels de gagner en visibilité sur le comportement de l'infrastructure et des applications. L'observabilité comble cette lacune en fournissant des informations plus approfondies sur l'ensemble de l'infrastructure. Les outils d'observabilité peuvent collecter des données télémétriques sur les performances des applications ou des systèmes en continu en s'intégrant à divers composants de l'infrastructure informatique et en fournissant une visibilité globale de votre infrastructure informatique.

Certains des avantages de l'observabilité peuvent être résumés comme suit :

- Dépannage plus rapide : les informations détaillées obtenues grâce aux outils d'observabilité vous aident à diagnostiquer et à résoudre les problèmes du système plus rapidement.

- Amélioration des performances des applications : la surveillance des indicateurs clés et l'identification des problèmes aident les développeurs à prendre des décisions fondées sur les données afin d'améliorer les performances des applications.
- Fiabilité et expérience utilisateur améliorées : les données d'observabilité permettent aux développeurs de résoudre de manière proactive les défaillances du système susceptibles de perturber l'expérience utilisateur.

Qu'est-ce que l'observabilité

L'observabilité est la capacité de comprendre l'état interne d'un système en analysant les données qu'il produit, telles que les journaux, les métriques, les traces et les événements. L'observabilité vous permet de comprendre et de répondre à des questions spécifiques sur le comportement de votre système en cas de panne. Grâce à une connaissance approfondie de vos systèmes, vous pouvez être mieux préparé aux inconnues.
Par exemple, vous pouvez suivre la lenteur ou la rapidité, les défaillances et les mesures à prendre pour améliorer les performances du système.

Les métriques, les journaux et les traces sont les principaux piliers de l'observabilité.

- Métriques : Les mesures sont une représentation numérique de données mesurées sur une certaine période. Les données métriques sont utiles pour suivre l'état de santé d'un système au fil du temps. Ces mesures numériques incluent l'utilisation du processeur, l'utilisation de la mémoire et les taux d'erreur.
- Journaux : les journaux sont des messages ou des enregistrements qui décrivent des événements survenus à un moment donné. Ces messages ou enregistrements sont généralement générés par une application ou un système.
- Traces : les traces représentent le parcours d'une demande au fur et à mesure qu'elle traverse les différentes parties d'un système distribué. Les traces documentent la manière dont une demande est traitée et le temps nécessaire pour la traiter. Ces données peuvent aider à identifier les goulots d'étranglement et autres problèmes de latence.

Surveillance et observabilité

La surveillance est un ensemble d'outils ou de solutions pour vous informer en cas de problème. Grâce à l'observabilité, vous pouvez identifier ce qui se passe et identifier rapidement la racine des problèmes pour savoir pourquoi ils se sont produits. Il intègre les faits et les données générés par la surveillance pour vous offrir une vue complète des performances et de l'état de santé de votre système. Grâce à l'observabilité, vous pouvez analyser automatiquement vos données et améliorer l'expérience utilisateur sur la base d'une saisie rapide et précise.

Observabilité avec NetScaler

Lorsque NetScaler est déployé en tant que proxy pour les déploiements d'applications, NetScaler inspecte chaque demande ou réponse utilisateur pour le routage global et le routage du centre de données local. Les milliers de journaux et de compteurs fournis par NetScaler vous permettent de disposer d'informations détaillées sur les paquets HTTP, TCP, SSL et DNS. Vous pouvez tirer parti de ces données et informations riches provenant de NetScaler pour résoudre et identifier les problèmes. Vous pouvez exporter les données de NetScaler vers vos points de terminaison d'observabilité préférés pour créer des visualisations et obtenir des informations détaillées sur les applications en temps réel.

NetScaler fournit des intégrations avec des outils d'observabilité populaires tels que Prometheus, Splunk, ElasticSerach et Kafka.
L'intégration directe de NetScaler est disponible avec Prometheus. Grâce à l'intégration directe, il n'est pas nécessaire de déployer un agent ou un nœud supplémentaire pour exporter les données et créer des tableaux de bord personnalisés répondant à vos besoins. Prometheus se concentre sur la surveillance des données chronologiques qui collectent des mesures numériques auprès de toutes les entités.

NetScaler ADM possède plusieurs fonctionnalités d'observabilité intégrées, telles que les informations SSL, les informations sur les transactions Web et les informations sur les API.

NetScaler peut fournir trois types d'informations dans le cadre de l'observabilité :

- Informations sur les applications et les API : les informations sur l'état des applications aident à résoudre les problèmes liés aux sites Web d'applications présentant une latence élevée, un nombre élevé d'erreurs ou des performances médiocres. Il inclut également des mesures de surveillance des erreurs, du trafic, de la latence et de la saturation. Ensemble, ces signaux sont considérés comme les signaux d'or pour surveiller l'état des applications.
- Informations sur la sécurité des applications et des API : les informations sur la sécurité des applications incluent les violations WAF détectées ou évitées par rapport au trafic global, les principales applications touchées par les violations WAF ou BOT, et les CVE, les classifications BOT entre les bons et les mauvais robots, et fournissent des informations sur les attaquants.
- Informations sur l'infrastructure réseau : les informations sur l'infrastructure NetScaler incluent des informations sur NetScaler, telles que l'utilisation du processeur, de la mémoire et des disques, et la télémétrie de l'interface réseau. Vous pouvez également obtenir des informations spécifiques au niveau des fonctionnalités telles que SSL, GSLB, Multipath TCP (MPTCP) et des informations sur la surveillance du SSL TLS, telles que les détails d'expiration des certificats, le protocole utilisé et la force du chiffrement.

Pour des informations détaillées sur l'exportation directe de métriques vers Prometheus depuis NetScaler, consultez la section Surveillance de NetScaler, des applications et de la sécurité des applications à l'aide de Prometheus.

Équilibrage de la charge

May 5, 2023

La fonction d'équilibrage de charge prioritaire vous permet d'attribuer un numéro de priorité à chacun des services ou groupes de services liés à un serveur virtuel d'équilibrage de charge prioritaire. Un service ou un groupe de services dont le numéro est le plus bas a la priorité la plus élevée. Le trafic de l'application est distribué uniquement à ce service ou à un groupe de services tant que ce service ou ce groupe de services est actif. Le service ou le groupe de services auquel est attribué le numéro de priorité suivant ne devient opérationnel que lorsque tous les services ou membres du groupe de services ayant la priorité la plus élevée sont hors service. Toutefois, lorsque l'un des services ou un membre du groupe de services ayant la priorité la plus élevée redevient disponible, le trafic est redirigé vers ce service ou ce groupe de services.

Par exemple, considérez les groupes de services SVG1, SVG2 et SVG3 liés à un serveur virtuel d'équilibrage de charge prioritaire. Le nombre maximum de groupes de priorité est fixé à trois. Vous attribuez la priorité à chaque groupe comme suit :

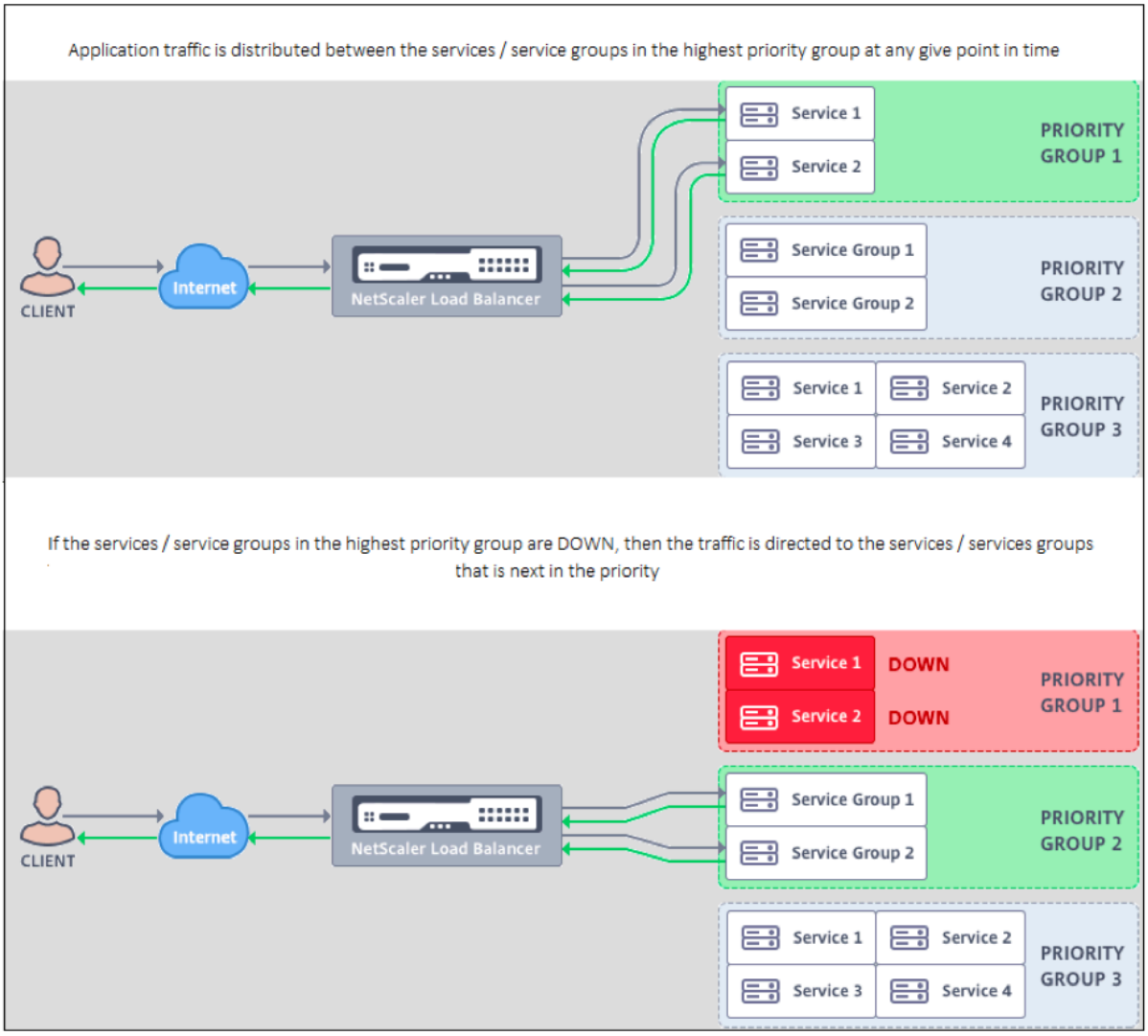
- SVG1 — priorité 1
- SVG2 — priorité 2
- SVG3 — priorité 3

Dans ce scénario, le trafic de l'application est dirigé vers le groupe de services SVG1 car ce groupe se voit attribuer le numéro de priorité le plus bas. Si tous les membres du SVG1 sont hors service, le trafic est distribué au groupe de services SVG2 car ce groupe se voit attribuer le numéro de priorité inférieur suivant. Si tous les membres de SVG2 sont également hors service, le trafic est distribué vers SVG3. Toutefois, lorsque l'un des membres de SVG1 est actif, le trafic est redirigé vers SVG1 car le numéro le plus bas et la priorité la plus élevée sont attribués à SVG1.

Vous pouvez attribuer une priorité à un service ou à un groupe de services pour mettre à niveau le service ou le groupe de services spécifique ayant la priorité la plus élevée, chaque fois que cela est nécessaire avec un impact minimal ou nul sur le trafic de production.

De plus, si la mise à niveau échoue, vous pouvez basculer en toute sécurité vers le service ou le groupe de services suivant dans la priorité, avec un impact minimal ou nul sur le trafic de production.

La figure suivante illustre la fonctionnalité d'équilibrage de charge prioritaire.



Configurer l'équilibrage de charge prioritaire

> **Remarque**
>
> La configuration d'équilibrage de charge prioritaire de NetScaler est prise en charge uniquement via l'interface graphique. Vous ne pouvez pas configurer l'équilibrage de charge prioritaire à l'aide de l'interface de ligne de commande.

1. Accédez à **Gestion du trafic** > **Équilibrage de charge prioritaire**> **Virtual *Servers** et spécifiez le protocole du serveur virtuel, l'adresse IP et le numéro de port du serveur virtuel.
2. Dans la zone **Groupes de priorité maximale**, entrez le nombre de services prioritaires ou les groupes de services qui peuvent être liés à ce serveur virtuel. La valeur par défaut est 2 et la priorité maximale pouvant être définie est 10. Ce paramètre n'est pas modifiable une fois configuré.

Remarque :

Après avoir spécifié le nombre maximum de groupes de priorités et cliqué sur **OK**, un serveur virtuel de commutation de contenu et un nombre « n » de serveurs virtuels d'équilibrage de charge de sauvegarde sont créés. L'alphabet « n » représente le nombre maximum de groupes prioritaires.

Par exemple, si vous avez saisi le nom du serveur virtuel sous la forme vs1 et que vous avez défini le groupe de priorité maximum sur 5, un serveur virtuel de commutation de contenu portant le nom `_Pri.LB##vs1##MaxPri=5` et les 5 serveurs virtuels d'équilibrage de charge suivants sont créés.

- `_Pri.LB##vs1##MaxPri=5_LB1`
- `_Pri.LB##vs1##MaxPri=5_LB2`
- `_Pri.LB##vs1##MaxPri=5_LB3`
- `_Pri.LB##vs1##MaxPri=5_LB4`
- `_Pri.LB##vs1##MaxPri=5_LB5`

3. Après avoir spécifié le nombre maximum de groupes de priorité et cliqué sur **OK**, vous êtes invité à choisir les services ou les groupes de services qui doivent être liés à ce serveur virtuel de commutation de contenu.

   - Pour lier des services au serveur virtuel, cliquez sur **Insérer** dans la section Services. Ensuite, sélectionnez un service existant ou créez-en un et définissez la priorité de ce service. Définissez également le numéro de priorité auquel ce service doit être lié.
   - Pour lier des groupes de services au serveur virtuel, cliquez sur **Insérer** dans la section Groupes de services. Ensuite, sélectionnez un groupe de services existant ou créez-en un et définissez la priorité de ce groupe de services. Définissez également le numéro de priorité auquel ce groupe de services doit être lié.

   Répétez l'étape 3 en fonction du nombre maximum de groupes de priorité que vous avez saisi.

   Remarque :

   - Le service ou le groupe de services ayant la priorité la plus élevée est lié au serveur virtuel d'équilibrage de charge qui représente la priorité la plus élevée.

   Par exemple, si vous avez attribué les priorités 1 et 2 à des groupes de services `SG_App1 and SG_App2` respectivement, elle `SG_App1` est liée à `virtual server _Pri.LB##vs1##MaxPri=5_LB1 and SG_App2` est lié à `virtual server _Pri.LB##vs1##MaxPri=5_LB2` créé à l'étape 2.

   - Pour modifier la priorité du groupe de services ou du service, cliquez sur l'icône Modifier sur la page Serveur virtuel d'équilibrage de charge prioritaire et modifiez la priorité selon vos besoins.

- Vous ne pouvez pas définir explicitement les méthodes d'équilibrage de charge et la persistance pour chaque serveur virtuel, car la configuration de tous les serveurs virtuels d'équilibrage de charge est identique.

4. Dans les sections Paramètres avancés, effectuez l'autre configuration qui répond à vos besoins.

> **Important :**
>
> Les entités créées lors de la configuration de l'équilibrage de charge prioritaire ne doivent pas être modifiées à partir d'autres onglets de l'interface graphique ni à partir de l'interface de ligne de commande. Il est recommandé de modifier les entités d'équilibrage de charge prioritaires à partir de l'onglet Équilibrage de charge prioritaire uniquement.

Extensions NetScaler

May 5, 2023

Les extensions NetScaler peuvent être utilisées pour personnaliser une appliance NetScaler en écrivant du code d'extension. Actuellement, les extensions de politique et de protocole sont prises en charge. Les extensions de stratégie peuvent être utilisées pour étendre le langage de la politique. Les extensions de protocole peuvent être utilisées pour ajouter la prise en charge de protocoles personnalisés sur une appliance NetScaler.

Les extensions NetScaler sont également prises en charge sur NetScaler CPX.

Ce document contient les informations suivantes :

- NetScaler Extensions - Présentation du langage
- NetScaler Extensions - Référence de bibliothèque
- Référence de l'API NetScaler Extensions
- Extensions de protocole
- Extensions de stratégie

Extensions NetScaler : présentation du langage

May 5, 2023

Le langage d'extension est basé sur le langage de programmation Lua 5.2. Lua fournit un moteur d'exécution compact offrant de bonnes performances, conçu pour être intégré à des programmes C, tels que le logiciel NetScaler.

Le langage d'extension est typé dynamiquement, ce qui signifie que chaque objet contient ses propres informations de type. Toute variable peut contenir n'importe quel type à tout moment pendant l'exécution. Les types de variables ne sont donc pas déclarés.

Le langage est également de forme libre, où les espaces blancs entre les jetons sont ignorés. Les déclarations peuvent être séparées par des points-virgules, mais cela n'est pas obligatoire et cela n'est généralement pas fait. Les blocs d'instructions sont généralement terminés à la fin. Il n'y a pas de crochets autour de blocs tels que {et} en C ou Java.

Les identificateurs sont des séquences de lettres (a à z et A à Z), de chiffres (0 à 9) et de traits de soulignement (_) qui ne commencent pas par un chiffre. Les identificateurs font la distinction entre majuscules et minuscules, de sorte que var, VAR et Var sont tous des identifiants différents.

Les commentaires commencent par –. Tout ce qui suit – est ignoré jusqu'à la fin de la ligne. Exemple :

```
-- This is a comment.
```

Types simples

May 5, 2023

Le langage autorise les valeurs des types simples suivants :

- Nombres
- Cordes
- Booléen
- Néant
- Autres types

Nombres

Tous les nombres (nombres entiers pairs) sont représentés par des valeurs à virgule flottante IEEE 754. Les nombres entiers jusqu'à 2^54 ont des représentations exactes. Les valeurs numériques peuvent être représentées par :

- Entiers décimaux signés et non signés (exemples : 10, -5)
- Nombres réels avec virgules décimales (10,5, 3,14159)
- Nombres réels avec exposants (1.0e+10)
- Hexadécimaux (0xffff0000)

Les expressions de politique NetScaler sont de trois types numériques :

- Entiers 32 bits (num_at)
- Entiers 64 bits (unsigned_long_at)

- Virgule flottante 64 bits (double_at)

Tous ces éléments sont convertis en type numérique lorsqu'ils sont transmis à une fonction d'extension, et les nombres sont convertis dans le type numérique de politique attendu lorsqu'ils sont renvoyés.

Cordes

Les chaînes sont des séquences d'octets de n'importe quelle longueur. Ils correspondent au type **text_at** de la politique. Les chaînes peuvent contenir des octets nuls (0x00). Les données binaires arbitraires peuvent être contenues dans des chaînes, y compris n'importe quelle représentation de code de caractère (par exemple UTF-8 et Unicode complet). Toutefois, les fonctions de chaîne telles que **string.upper ()** supposent un ASCII 8 bits.

Les chaînes sont automatiquement allouées lorsqu'elles sont utilisées. Il n'est pas nécessaire (ni même moyen) d'allouer explicitement des tampons pour les chaînes. Les chaînes sont également automatiquement désallouées par la collecte des déchets lorsqu'elles ne sont plus utilisées. Il n'est pas nécessaire (ni même moyen) de libérer des chaînes de caractères de manière explicite. Cette allocation et cette désallocation automatiques permettent d'éviter certains problèmes courants dans des langages tels que le C, tels que les fuites de mémoire et les pointeurs qui pendent.

Les littéraux de chaîne sont des chaînes de caractères entre guillemets doubles ou simples. Il n'y a aucune différence entre les deux types de guillemets : « une chaîne littérale » est identique à « une chaîne littérale ». La barre oblique inverse habituelle est disponible : \s (bell), \b (backspace), \f (feed de formulaire), \n (saut de ligne), \t (onglet horizontal), \\ (barre oblique inverse), \" (guillemet double) et \' (guillemet simple). Les valeurs décimales peuvent être saisies à l'aide d'une barre oblique inverse et d'un à trois chiffres (\ d, \ dd, \ ddd). Les valeurs d'octets hexadécimales peuvent être saisies par une barre oblique inverse, un x et deux chiffres hexadécimaux (\ xhh)

Une syntaxe spéciale appelée notation entre crochets longs peut être utilisée pour les chaînes littérales longues et multilignes. Cette notation place la chaîne entre crochets doubles avec zéro ou plusieurs signes égaux entre les crochets. L'idée est de trouver une combinaison de crochets et d'égaux qui ne figure pas dans la chaîne. Aucune séquence d'échappement n'est respectée dans la chaîne. Exemples :

[[Il s'agit d'une chaîne multiligne utilisant la notation entre crochets longs.]]

[= [Il s'agit d'une chaîne multiligne utilisant une notation longue avec [[et]] et un caractère non échappé dedans.] =]

La notation de crochets longs peut être utilisée pour faire un commentaire multi-ligne. Exemple :

– [[
Il s'agit d'un commentaire multiligne.
–]]

Booléen

Les valeurs booléennes vraies et fausses habituelles sont fournies. Notez que les valeurs booléennes sont différentes des valeurs numériques, contrairement à C où zéro est supposé faux et toute valeur différente de zéro est vraie.

Néant

nil est une valeur spéciale qui signifie « aucune valeur ». Il s'agit de son propre type et n'est équivalent à aucune autre valeur, contrairement à C où NULL est défini comme étant égal à zéro.

Autres types

Il existe deux autres types, les données utilisateur et les fils de discussion. Ce sont des sujets avancés qui ne sont pas abordés ici.

Variables

January 21, 2021

Les variables contiennent des valeurs qui peuvent changer lors de l'exécution de l'extension. En raison du typage dynamique, toute variable peut contenir des valeurs de n'importe quel type. Il n'y a pas de déclaration de type pour les variables. Au lieu de cela, le type d'une variable est déterminé au moment de l'exécution. En fait, le type de valeur d'une variable peut changer pendant l'exécution, bien que ce ne soit pas une pratique recommandée. Une variable a initialement la valeur nil.

Les noms de variables sont des identificateurs, de même que les chaînes de lettres, de chiffres et de traits de soulignement qui ne commencent pas par un chiffre. Exemples : en-têtes, en-têtes combined_headers.

Variables globales

Dans Lua, les variables qui ne sont pas déclarées autrement sont globales au sein du programme. Cependant, les variables globales ne sont pas autorisées dans les fonctions d'extension de stratégie, car il existe plusieurs moteurs de paquets dans lesquels une fonction peut être exécutée, et chaque moteur de paquets a sa propre mémoire.

Si vous utilisez une variable globale dans votre extension, vous obtiendrez une erreur d'exécution : essayez de mettre à jour ou de créer un rapport global dans **/var/log/ns.log**.

Les fautes de frappe dans les noms de variables sont un problème potentiel, car la variable avec la faute de frappe sera interprétée comme une autre variable globale et ne provoquera pas d'erreur de

syntaxe comme dans un langage comme C ou Java. Comme indiqué ci-dessus, vous obtiendrez une erreur d'exécution à la place.

Variables locales

Une variable peut être déclarée locale à un bloc d'instructions, comme une fonction. Ceci est fait par nom variable local. La variable sera portée au bloc, c'est-à-dire qu'elle n'existera que dans le bloc. La déclaration locale peut éventuellement affecter une valeur à la variable.

Exemples :

```
local headers = {}
local combined_headers = {}
```

Expressions

January 21, 2021

Les expressions calculent les valeurs à partir de valeurs variables et littérales.

- Opérations arithmétiques
- Opérations relationnelles
- Opérations logiques
- Concaténation
- Longueur
- Priorité

Opérations arithmétiques

Les opérations arithmétiques sont effectuées sur les valeurs numériques. Si une valeur de chaîne est utilisée dans une opération arithmétique, elle est convertie en nombre — si cela échoue, une erreur est renvoyée.

a + b	ajouter a et b
a - b	soustraire b de a
a * b	multiplier a et b
a/b	diviser a par b
a% b	modulo = a - math.floor(a/b)*b

a ^ b	élever a à la puissance b ; b peut être n'importe quel nombre
-a	annule a

Opérations relationnelles

Les opérations relationnelles comparent deux valeurs et retournent true si la relation est satisfaite et false si ce n'est pas le cas. Des opérations relationnelles peuvent être effectuées entre des valeurs de n'importe quel type. Si les valeurs ne sont pas du même type, false est renvoyé. Les nombres sont comparés de la manière habituelle. Les chaînes sont comparées à l'aide de la séquence de classement pour les paramètres régionaux actuels.

a == b	a est égal à b
a ~= b	a n'est pas égal à b
a < b	a est inférieur à b
a > b	a est supérieur à b
a <= b	a est inférieur ou égal à b
a >= b	a est supérieur ou égal à b

Opérations logiques

Les opérations logiques sont traditionnellement effectuées sur des valeurs booléennes, mais dans ce langage, elles peuvent être effectuées sur deux valeurs. nil et false est considéré comme faux et toute autre valeur est considérée comme vrai. Les opérations logiques utilisent l'évaluation raccourci, où si la première valeur détermine le résultat de l'opération, la deuxième valeur n'est pas évaluée.

a and b	si a est faux ou nul alors retournez un autre retour b
a or b	si a n'est pas faux et pas nul alors retournez un autre retour b

not a	si un n'est pas faux ou nul retourne faux sinon retourne vrai

Les opérations et et ou peuvent être utilisées pour l'évaluation conditionnelle dans une expression :

a or b	peut être utilisé pour fournir une valeur par défaut b si a est non initialisé (nil). Ceci est utile pour les paramètres optionnels dans les fonctions.
a and b or c	peut être utilisé pour choisir non néant b ou c en fonction de la condition a. Si a est vrai, alors a et b renvoie b, et b ou c renvoie b. Si a est faux, alors a et b renvoie false et false ou c renvoie c. Cela équivaut à a ? b: c dans le langage de programmation C.

Concaténation

La concaténation de chaîne est s1.. s2. Cela crée une nouvelle chaîne assez grande pour contenir le contenu de s1 et s2 et copie le contenu dans la nouvelle chaîne. Une erreur se produit si s1 ou s2 ne sont pas des chaînes. Notez que la concaténation répétée peut avoir des frais de copie considérables. Si vous construisez une chaîne de n octets en concaténant un octet à la fois, cela copiera n* (n+1) /2 octets. Pour de meilleures performances, vous pouvez mettre des morceaux d'une chaîne à concaténer dans une table (discuté plus loin), puis utiliser la fonction table.concat (). Un exemple de ceci est illustré dans l'exemple COMBINE_HEADERS ().

Longueur

La longueur d'une chaîne s est renvoyée par #s. L'opérateur # est également utilisé avec les tables de tableau, comme discuté plus loin.

Priorité

La priorité de l'opérateur détermine l'ordre dans lequel les opérations sont exécutées dans une expression, avec des opérations de priorité supérieure effectuées avant celles de priorité inférieure. L'ordre

de priorité peut, comme d'habitude, être remplacé par des parenthèses. Par exemple, dans`a + b \* c`, * a une priorité supérieure à +, de sorte que l'expression est évaluée comme`a + (b \* c)`.

highest	^
-	not # - (unary)
-	* / %
-	..
-	= ~= < > <= >=
-	and
lowest	ou

Les opérations avec la même priorité sont exécutées de gauche à droite (associative gauche), sauf ^ et.. qui sont exécutées de droite à gauche (associative droite). Donc a^b^c est évalué comme a^(b^c).

Attribution

January 21, 2021

L'instruction affectation évalue une expression et affecte la valeur résultante à une variable.

```
variable = expression
```

Comme indiqué précédemment, les valeurs de n'importe quel type peuvent être affectées à n'importe quelle variable, de sorte que ce qui suit est autorisé :

```
local v1 = "a string literal"
v1 = 10
```

Une instruction d'affectation peut réellement définir plusieurs variables, en utilisant le formulaire

variable1, variable2, … = expression1, expression2, …

S'il y a plus de variables que d'expressions, les variables supplémentaires sont affectées à zéro. S'il y a plus d'expressions que de variables, les valeurs d'expression supplémentaires sont ignorées. Les expressions sont toutes évaluées avant les affectations, de sorte que cela peut être utilisé pour échanger succinctement les valeurs de deux variables :

v1, v2 = v2, v1

équivaut à

tmp = v1
v2 = v1
v1 = tmp

Tables

August 20, 2021

Les tables sont des collections d'entrées avec des clés et des valeurs. Il s'agit de la seule structure de données agrégées fournie. Toutes les autres structures de données (tableaux, listes, ensembles, etc.) sont construites à partir de tables. Les clés et les valeurs de table peuvent être n'importe quel type, y compris d'autres tables. Les clés et les valeurs d'une même table peuvent mélanger les types.

- Constructeurs de table
- Utilisation de la table
- Tables en tant que tableaux
- Tables en tant qu'enregistrements

Constructeurs de table

Les constructeurs de table vous permettent de spécifier une table avec des clés et des valeurs associées. La syntaxe est :

{[key1] = value1, [key2] = value2, …}

où les clés et les valeurs sont des expressions. Si les clés sont des chaînes qui ne sont pas des mots réservés, les crochets et les guillemets autour des clés peuvent être omis. Exemple :

{key1 = "value1", key2 = "value2", key3 = "value3"}

Une table vide est spécifiée simplement par {}.

Un constructeur de table peut être utilisé dans une affectation pour définir une variable pour faire référence à une table. Exemples :

local t1 = {} – set t1 to an empty table
local t2 = {key1 = "value1", key2 = "value2", key3 = "value3"}

Notez que les tables elles-mêmes sont anonymes. Plusieurs variables peuvent faire référence à la même table. Poursuivant l'exemple ci-dessus :

t3 local = t2 - t2 et t3 se réfèrent à la même table

Utilisation de la table

Comme vous vous y attendiez, vous pouvez utiliser des clés pour trouver des valeurs dans une table. La syntaxe est la[clé]de table, où table est une référence de table (généralement une variable assignée à une table), et key est une expression fournissant la clé. Si cela est utilisé dans une expression et que la clé existe dans la table, cela renvoie la valeur associée à la clé. Si la clé n'est pas dans la table, cela renvoie nil. Si elle est utilisée comme variable dans une affectation et que la clé n'existe pas dans la table, elle crée une nouvelle entrée pour la clé et la valeur. Si la clé existe déjà dans la table, elle remplace la valeur de la clé par la nouvelle valeur. Exemples :

local t = {} — définit t sur une table vide
t[« k1"] = « v1" — crée une entrée pour la clé « k1" et la valeur « v1"
v1 = t[« k1"] — définit v1 à la valeur de la clé « k1" = « v1"
t[« k1"] = « nouveau_v1" — définit la valeur de la clé « k1 » sur « new_v1"

Tableau en tant que tableaux

Le tableau traditionnel peut être implémenté en utilisant une table avec des clés entières comme indices. Un tableau peut avoir des indices, y compris négatifs, mais la convention est de démarrer des tableaux à l'index 1 (pas 0 comme c'est le cas avec des langages comme C et Java). Il existe un constructeur de table à usage spécial pour de tels tableaux :

{value1, value2, value3, … }

Les références de tableaux sont alors des[index de]tableaux.

L'opérateur de longueur # renvoie le nombre d'éléments dans un tableau avec des indices consécutifs commençant à 1. Exemple :

local a = {"value1", "value2", "value3"}
local length = #a – sets length to the length of array a = 3

Les tableaux peuvent être clairsemés, où seuls les éléments définis sont alloués. Mais # ne peut pas être utilisé sur un tableau clairsemé avec des indices non consécutifs. Exemple :

local sparse_array = {} — configurer un tableau vide
sparse_array[1] = « value1" — ajouter un élément à l'index 1
sparse_array[99] = « value99 » — ajouter un élément à l'index 99

Les tableaux multidimensionnels peuvent être configurés en tant que tables de tables. Par exemple, une matrice 3x3 peut être configurée par :

local m = {{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}
local v22 = m[2][2] — définit v22 à 5

Tables en tant qu'enregistrements

Les enregistrements avec des champs peuvent être implémentés sous forme de tables avec des clés de nom de champ. Le formulaire de référence table.field peut être utilisé pour la table[« field »]. Exemples :

local person = {name = "John Smith", phone = "777-777-7777"}
local name = person.name – sets name to "John Smith"

Un tableau de tables peut être utilisé pour une séquence d'enregistrements. Exemple :

local people = {
{name = "John Smith", phone = "777-777-7777"},
{name = "Jane Doe", phone = "888-888-8888"}
…
}

name = people[2].name — définit le nom sur « Jane Doe »

Structures de contrôle

May 5, 2023

Le langage des fonctions d'extension fournit les instructions habituelles pour contrôler l'exécution du programme.

- Si alors sinon
- Tout en faisant et en répétant jusqu'à
- Pour numérique
- Pause
- Goto

Si alors sinon

Si les instructions sélectionnent des blocs d'instructions à exécuter en fonction d'une ou de plusieurs conditions. Il existe trois formes :

Si c'est le cas, formulaire

```
if expression then
     statements to execute if expression is not false or nil
end
<!--NeedCopy-->
```


Si c'est le cas, sinon, formulaire

```
if expression then
     statements to execute if expression is not false or nil
else
     statements to execute if expression is false or nil
end
<!--NeedCopy-->
```

Si alors sinon sinon Formulaire

```
if expression1 then
     statements to execute if expression1 is not false or nil
     elseif expression2 then
          statements to execute if expression2 is not false or nil
. . .
else
     statements to execute if all expressions are false or nil
end
<!--NeedCopy-->
```

Exemple :

```
if headers[name] then

     local next_value_index = #(headers[name]) + 1
     headers[name][next_value_index] = value

else

     headers[name] = {
 name .. ":" .. value }


end
<!--NeedCopy-->
```

Remarque :

- L'expression n'est pas entre parenthèses comme c'est le cas en C et Java.
- Il n'existe pas d'équivalent à l'instruction de commutation C/Java. Vous devez utiliser une série d'instructions if elseif pour obtenir l'équivalent.

Tout en faisant et en répétant jusqu'à

Les instructions **while** et **repeat** fournissent des boucles contrôlées par une expression.

```
while expression do
     statements to execute while expression is not false or nil
end

repeat

     statements to execute until expression is not false or nil

until expression
<!--NeedCopy-->
```

Exemple pour tandis que :

```
local a = {
 1, 2, 3, 4 }

local sum, i = 0, 1 -- multiple assignment initializing sum and i
while i <= #a do -- check if at the end of the array
     sum = sum + a[i] -- add array element with index i to sum
     i = i + 1 -- move to the next element
end
<!--NeedCopy-->
```

Exemple de répétition :

```
sum, i = 0, 1 -- multiple assignment initializing sum and i
repeat
     sum = sum + a[i] -- add array element with index i to sum
     i = i + 1 -- move to the next element
until i > #a -- check if past the end of the array
<!--NeedCopy-->
```

Bien entendu, il est possible d'écrire une boucle qui ne se termine pas, par exemple, si vous omettez l'instruction i = i + 1 dans l'un ou l'autre de ces exemples. Lorsqu'une telle fonction est exécutée, NetScaler détecte que la fonction ne s'est pas terminée dans un délai raisonnable et la supprime avec une erreur d'exécution :

```
Cpu limit reached. Terminating extension execution in [[string "function
extension function..."]]: line line-number.
```

sera indiqué dans /var/log/ns.log.

Pour numérique

Il existe deux types de boucles. Le premier est le for numérique, qui est similaire à l'utilisation habituelle de l'instruction for en C et Java. L'instruction numeric for initialise une variable, teste si la variable a dépassé une valeur finale et, dans le cas contraire, exécute un bloc d'instructions, incrémente la variable et répète. La syntaxe de la boucle numérique for est la suivante :

```
for variable = initial, final, increment do

     statements in the loop body

end
<!--NeedCopy-->
```

où initial, final et incrément sont toutes des expressions qui produisent (ou peuvent être converties en) nombres. La variable est considérée comme locale par rapport au bloc d'instructions for loop ; elle ne peut pas être utilisée en dehors de la boucle. L'incrément peut être omis ; la valeur par défaut est 1. Les expressions sont évaluées une seule fois au début de la boucle. La condition finale est variable > finale si l'incrément est positif et variable < finale si l'incrément est négatif. La boucle se termine immédiatement si l'incrément est égal à 0.

Exemple (équivalent aux boucles while et repeat de la section précédente) :

```
sum = 0
for i = 1, #a do -- increment defaults to 1
     sum = sum + a[i]
end
<!--NeedCopy-->
```

Le second type de boucle for est le for générique, qui peut être utilisé pour des types de boucles plus flexibles. Cela implique l'utilisation de fonctions, nous en parlerons donc plus tard après l'introduction des fonctions.

Pause

L'instruction break est utilisée à l'intérieur d'une boucle while, repeat ou for. Il mettra fin à la boucle et reprendra l'exécution à la première instruction suivant la boucle. Exemple (également équivalent aux précédents while, repeat et pour les boucles) :

```
sum, i = 0, 1
while true do
     if i > #a then
          break
     end
```



```
6       sum = sum + a[i]
7       i = i + 1
8   end
9   <!--NeedCopy-->
```

Goto

L'instruction goto peut être utilisée pour accéder à une étiquette en avant ou en arrière. L'étiquette est un identifiant et sa syntaxe est ::label : :. L'instruction goto est goto label. Exemple (encore une fois équivalent aux boucles précédentes) :

```
1   sum, i = 0, 1
2   ::start_loop::
3       if i > #a then
4           goto end_loop -- forward jump
5       end
6       sum = sum + a[i]
7       i = i + 1
8       goto start_loop -- backwards jump
9   ::end_loop::
10  . . .
11  <!--NeedCopy-->
```

L'utilisation de gotos dans la programmation fait l'objet d'une longue controverse. En général, vous devez essayer d'utiliser les autres structures de contrôle pour rendre vos fonctions plus lisibles et plus fiables. Mais une utilisation judicieuse et occasionnelle de gotos peut conduire à de meilleurs programmes. Les gotos peuvent notamment être utiles pour gérer les erreurs.

Fonctions

May 5, 2023

Les fonctions sont un élément de base de la programmation. Elles constituent un moyen pratique et puissant de regrouper des instructions exécutant une tâche. Ils constituent l'interface entre l'appliance NetScaler et le code d'extension. Pour les stratégies, vous définissez des fonctions d'extension de stratégie. Pour les protocoles, vous implémentez des fonctions de rappel pour les comportements de protocole. Les fonctions sont constituées de définitions de fonctions qui spécifient quelles valeurs sont passées dans et hors de la fonction et quelles instructions sont exécutées pour la fonction, et d'appels de fonction, qui exécutent des fonctions avec des données d'entrée spécifiques et obtiennent des résultats de la fonction.

Fonctions de rappel du comportement du protocole

Le comportement du client TCP consiste en une fonction de rappel (on_data) qui traite les événements de flux de données du client TCP. Pour implémenter l'équilibrage de charge basé sur les messages (MBLB) pour un protocole TCP, vous pouvez ajouter du code pour cette fonction de rappel afin de traiter le flux de données TCP provenant du client et d'analyser le flux d'octets en messages de protocole.

Les fonctions de rappel d'un comportement sont appelées avec un contexte, qui correspond à l'état du module de traitement. Le contexte est l'instance du module de traitement. Par exemple, les rappels du comportement du client TCP sont appelés avec différents contextes pour différentes connexions TCP clientes.

En plus du contexte, les fonctions de rappel de comportement peuvent comporter d'autres arguments. Habituellement, le reste des arguments est passé en tant que charge utile, qui est la collection de tous les arguments. Ainsi, les instances du module de traitement programmable peuvent être considérées comme une combinaison de fonctions d'état d'instance et de rappel d'événement, c'est-à-dire le contexte et le comportement. Et le trafic circule à travers le pipeline comme charge utile d'événement.

Prototype de la fonction de rappel client TCP :

```
1
2                 Function                client on_data (ctxt, payload)
3
4                                                 //.code
5
6                 end
7
8
9 <!--NeedCopy-->
```

Où,

- ctxt - Contexte de traitement du client TCP
- payload — charge utile d'événement
  - payload.data : données TCP reçues, disponibles sous forme de flux d'octets

Fonctions d'extension de stratégie

Étant donné que le langage d'expression de stratégie NetScaler est tapé, la définition d'une fonction d'extension doit spécifier les types de ses entrées et sa valeur de retour. La définition **de la fonction Lua** a été étendue pour inclure ces types :


```
function self-type: function-name(parameter1: parameter1-type, and so
   on): return-type
     statements
end

<!--NeedCopy-->
```

Où,

Les types sont NSTEXT, NSNUM, NSBOOL ou NSDOUBLE.

Self-type est le type de l'auto-paramètre implicite qui est passé à la fonction. Lorsque la fonction d'extension est utilisée dans une expression de politique NetScaler, il s'agit de la valeur générée par l'expression située à gauche de la fonction. Une autre façon de voir cela est que la fonction étend ce type dans le langage de politique NetScaler.

Les types de paramètres sont les types de chaque paramètre spécifié dans l'appel de fonction d'extension dans l'expression de stratégie. Une fonction d'extension peut avoir zéro paramètre ou plus.

Type de retour est le type de la valeur renvoyée par l'appel de la fonction d'extension. Il s'agit de l'entrée de la partie de l'expression de stratégie, le cas échéant, à droite de la fonction, ou bien de la valeur du résultat de l'expression.

Exemple :

```
function NSTEXT:COMBINE_HEADERS(): NSTEXT
```

Utilisation de la fonction d'extension dans une expression de stratégie :

```
HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1\r\n").COMBINE_HEADERS()
```

Ici, l'auto-paramètre est le résultat de `HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1\r\n")`, qui est une valeur de texte. Le résultat de l'appel COMBINE_HEADERS () est du texte, et comme il n'y a rien à droite de cet appel, le résultat de l'expression entière est du texte.

Définition de la fonction locale

Outre les fonctions d'extension, aucune fonction globale ne peut être définie dans un fichier d'extension. Mais les fonctions locales peuvent être définies dans les fonctions d'extension à l'aide de l'instruction normale de la fonction Lua. Cela déclare le nom de la fonction et les noms de ses paramètres (également appelés arguments), et comme toutes les déclarations de Lua, ne spécifie aucun type. La syntaxe est la suivante :

```
local function function-name(parameter1-name, parameter2-name, and so
   on)
     statements
```



```
end

<!--NeedCopy-->
```

Les noms des fonctions et des paramètres sont tous des identificateurs. (Le nom de la fonction est en fait une variable et l'instruction de fonction est un raccourci pour nom-fonction locale = fonction (paramètre1, etc.), mais vous n'avez pas besoin de comprendre cette subtilité pour utiliser des fonctions.)

Notez que, et ainsi de suite, est utilisé ici pour la continuation du modèle des noms de paramètres au lieu de l'habituel…. C'est parce que… lui-même signifie en fait une liste de paramètres variables, qui ne sera pas discutée ici.

Corps de fonction et retour

Le bloc d'instructions entre la fonction et les instructions de fin est le corps de la fonction. Dans le corps de la fonction, les paramètres de la fonction agissent comme des variables locales, avec des valeurs fournies par les appels de fonction, comme décrit précédemment.

L'instruction return fournit les valeurs à renvoyer à l'appelant de la fonction. Il doit apparaître à la fin d'un bloc (dans une fonction, si c'est le cas, pour la boucle, etc.). Il peut être dans son propre bloc do return… end). Il ne spécifie aucune, une ou plusieurs valeurs de retour :

```
return -- returns nil
return expression -- one return value
return expression1, expression2, ... -- multiple return values

<!--NeedCopy-->
```

Exemples :

```
local function fsum(a)
     local sum = 0
     for i = 1, #a do
          sum = sum + a[i]
     end
     return sum
end

Local function fsum_and_average(a)
     local sum = 0
     for i = 1, #a do
          sum = sum + a[i]
     end
```



```
14       return sum, sum/#a
15  end
16
17  <!--NeedCopy-->
```

Les appels de fonctions

Un appel de fonction exécute le corps d'une fonction, fournit des valeurs pour ses paramètres et reçoit des résultats. La syntaxe d'un appel de fonction est nom-fonction (expression1, expression2, etc.), où les paramètres de la fonction sont définis sur les expressions correspondantes. Le nombre d'expressions et de paramètres ne doit pas nécessairement être le même. S'il y a moins d'expressions que de paramètres, les paramètres restants sont définis sur zéro. Vous pouvez donc rendre un ou plusieurs paramètres facultatifs à la fin de l'appel, et votre fonction peut vérifier s'ils sont spécifiés en vérifiant s'ils ne sont pas nuls. Une méthode courante consiste à utiliser l'opération OR :

```
1  function f(p1, p2) -- p2 is optional
2       p2 = p2 or 0 -- if p2 is nil, set to a default of 0
3       . . .
4  end
5
6  <!--NeedCopy-->
```

S'il y a plus d'expressions que de paramètres, les valeurs d'expression restantes sont ignorées.

Comme indiqué précédemment, les fonctions peuvent renvoyer plusieurs valeurs. Ces retours peuvent être utilisés dans une instruction d'affectation multiple. Exemple :

```
1  local my_array = {
2   1, 2, 3, 4 }
3
4  local my_sum, my_ave = sum_and_average(my_array)
5
6  <!--NeedCopy-->
```

Fonctions d'itérateur et boucles génériques for

Maintenant que nous avons introduit des fonctions, nous pouvons parler de boucles for génériques. La syntaxe de la boucle for générique (avec une variable) est la suivante :

```
1  for variable in iterator(parameter1, parameter2, and so on) do
2       statements in the for loop body
3  end
4
```



```
<!--NeedCopy-->
```

Où iterator () est une fonction avec zéro ou plusieurs paramètres qui fournissent une valeur pour une variable à chaque itération du corps de la boucle. La fonction itérateur garde une trace de son emplacement dans l'itération à l'aide d'une technique appelée closure, dont vous n'avez pas à vous soucier ici. Il signale la fin de l'itération en renvoyant zéro. Les fonctions d'itérateur peuvent renvoyer plus d'une valeur, pour une utilisation dans plusieurs affectations.

L'écriture d'une fonction itérateur dépasse le cadre de cet article, mais il existe peu d'itérateurs intégrés utiles qui illustrent le concept. L'un est l'itérateur pairs (), qui parcourt les entrées d'une table et renvoie deux valeurs, la clé et la valeur de l'entrée suivante.

Exemple :

```
local t = {
 k1 = "v1", k2 = "v2", k3 = "v3" }

local a = {
  }
  -- array to accumulate key-value pairs
local n = 0 -- number of key-value pairs
for key, value in pairs(t) do
     n = n + 1
     a[n] = key.. " = ".. Value -- add key-value pair to the array
end
local s = table.concat(a, ";") -- concatenate all key-value pairs into
   one string

<!--NeedCopy-->
```

Un autre itérateur utile est la `string.gmatch()` fonction, utilisée dans l'`COMBINE_HEADERS()` exemple suivant.

Extensions NetScaler - référence de bibliothèque

May 5, 2023

La liste des bibliothèques prises en charge dans les extensions de politique.

- Bibliothèque de base
- Bibliothèque de chaînes
- Modèles d'expressions régulières - Classes de caractères
- Modèles d'expressions régulières - Éléments du modèle

- Bibliothèque de tables
- Bibliothèque de mathématiques
- Bibliothèque Bitwise
- Bibliothèque du système d'exploitation
- Bibliothèque NetScaler

Bibliothèque de base

affirmer (v [, message])	Emet une erreur, avec un message facultatif, lorsque v est faux.
erreur (message)	Met fin à une fonction et signale le message d'erreur.
altérations (a)	Itérateur pour un tableau a. Renvoie un indice et une valeur pour chaque itération.
paires (t)	Itérateur pour une table t. Renvoie une clé et une valeur pour chaque itération.
pour numéroter (e [, base])	Convertit e en nombre, avec une base facultative.
tostring (v)	Convertit v en chaîne
type (v)	Renvoie le type de v : nombre, chaîne, booléen, table, etc.
getmetatable (objet)	Renvoie la valeur nil si l'objet ne possède pas de métable. Sinon, si la métatable de l'objet comporte un champ « __metatable », renvoie la valeur associée. Dans le cas contraire, renvoie la métatable de l'objet donné.
setmetatable (table, metatable)	Définit la métatable pour la table donnée. (Vous ne pouvez pas modifier la métatable d'autres types à partir de Lua, uniquement à partir de C.) Si la valeur métatable est nulle, supprime la métatable de la table donnée. Si la métatable d'origine comporte un champ « __metatable », génère une erreur.

sélectionner (index, ···)	Renvoie tous les arguments après l'indice du numéro d'argument. Si index est chaîne "#", alors il retourne le nombre total d'arguments supplémentaires qu'il a reçus.
pcall (f [, arg1, ··])	Appelle la fonction f avec les arguments donnés en mode protégé. Il renvoie le code d'état comme premier résultat qui indique si l'appel a réussi ou non. Si l'appel a réussi, avec le code d'état, il renvoie également tous les résultats de l'appel, sinon renvoie un message d'erreur.
xpcall (f, msh [, arg1, ···])	Cette fonction est similaire à pcall, sauf qu'elle prend également un argument pour la gestion des erreurs.
_VERSION	Renvoie la version actuelle de l'interpréteur.

Bibliothèque de chaînes

chaîne.octet (s [, i [, j]])	Renvoie les valeurs d'octets pour s [i] à s [j]. Par défaut i = 1 et j = i
chaîne.char (…)	Renvoie une chaîne construite à partir des paramètres entiers.
string.find (s, pattern [, init [, plain])	Recherche la première correspondance d'un motif d'expression régulière dans s. Renvoie le premier et le dernier index de match ou nul. init est l'index de départ, par défaut 1. plain = true signifie que le pattern n'est pas une regex.
string.format (formulaire,…)	Renvoie une version formatée des paramètres.
chaîne.gmatch (s, modèle)	Itérateur pour rechercher s avec le modèle regex. Renvoie les valeurs correspondantes.
chaîne.gsub (s, pattern, repl [, n])	Renvoie une copie de s dans laquelle toutes (ou n) occurrences du modèle ont été remplacées par repl.

string.len (s)	Renvoie la longueur de la chaîne.
chaîne.lower (s)	Renvoie une copie de la chaîne convertie en minuscules.
string.match (s, pattern [, init])	Recherche la première correspondance du motif regex dans s et renvoie les captures ou le motif entier. init est l'index à démarrer, par défaut 1.
string.rep (s, n [, sep])	Retourne une chaîne qui est n copies de s, avec le séparateur sep, par défaut aucun séparateur
chaîne.reverse (s)	Renvoie une chaîne qui est s inversée.
chaîne.sub (s, i [, j])	Renvoie la sous-chaîne de s de s [i] à s [j], j par défaut étant la fin de la chaîne.
chaîne.upper (s)	Renvoie une copie de la chaîne convertie en majuscules.
string.dump (fonction)	Renvoie une chaîne contenant une représentation binaire de la fonction donnée.

Modèles d'expressions régulières - classes de caractères

x	le caractère x, sauf pour les caractères magiques ^$ () %. [] *+- ?)
.	n'importe quel personnage
%a	n'importe quelle lettre
%c	n'importe quel caractère de contrôle
%d	n'importe quel chiffre
%g	n'importe quel caractère imprimable à l'exception de l'espace
%l	n'importe quelle lettre minuscule
%p	n'importe quel caractère de ponctuation
%s	n'importe quel caractère d'espace blanc
%u	n'importe quelle lettre majuscule

%w	n’importe quelle lettre alphanumérique
%x	un personnage magique x échappé (par exemple%%)
[ensemble]	un ensemble de caractères : séquence de caractères individuels, plages x-y et classes %
[^set]	personnages ne figurant pas dans le set.

Modèles d’expression régulière - éléments du modèle

X	une classe de caractères
X*	0 ou plusieurs répétitions les plus longues de caractères dans X
X+	1 ou plusieurs répétitions de caractères en X
X-	0 ou plusieurs répétitions les plus courtes de caractères dans X
X ?	0 ou 1 caractère en X
%n	n=1 à 9 ; correspond à la nième chaîne capturée
%bxy	correspond à une sous-chaîne entre deux caractères équilibrés x et y. L’exemple %b () fait correspondre la sous-chaîne entre deux parenthèses équilibrées.
%f [définir]	correspond à une chaîne vide à n’importe quelle position de telle sorte que le caractère suivant appartient à set et que le caractère précédent n’appartient pas à set.

Une matrice est une séquence d’éléments de la matrice. ^pattern correspond au début d’une chaîne et pattern$ correspond à la fin de la chaîne.

Les sous-chaînes correspondantes peuvent être capturées à l’aide de (pattern). Les parenthèses sans motif () capturent la position actuelle de la chaîne (un nombre).

Bibliothèque de tables

table.concat (liste [, sep [, i [, j]]])	Renvoie une liste de chaînes [i].. sep.. list [i+1].. sep. list [j]. Par défaut, sep est la chaîne vide. Par défaut i est 1, j est #list.
table.insert (liste, [pos,] valeur)	Insère une valeur dans la liste à l'index pos. La valeur par défaut pour pos est #list (fin de la liste).
pack de tables (…)	Retourne un tableau contenant les paramètres commençant à l'index 1, et une clé n avec le nombre total de paramètres.
table.remove (list [, pos])	Supprime de la liste l'élément à la position pos, déplaçant les éléments pour remplir la position. Renvoie l'élément supprimé. Par défaut pour posis #list (fin de la liste.)
table.sort (list [, comp])	Trier les éléments de la liste en place. comp est la fonction de comparaison à utiliser. La valeur par défaut pour comp est <.
table.unpack (list [, i [, j]])	Renvoie la liste [i] à la liste [j]. La valeur par défaut pour i est 1 et j est #list <c/ode>.

Bibliothèque de mathématiques

Diverses fonctions trigonométriques et logarithmiques ne sont pas représentées.

math.abs (x)	Renvoie la valeur absolue de x.
math.ceil (x)	Renvoie le plus petit entier >= x.
sol mathématique (x)	Renvoie le plus grand entier <= x.
math.fmod (x, y)	Renvoie le reste de x/y en arrondissant le quotient vers zéro.
maths. énorme	Une valeur >= n'importe quel autre nombre.
math.max (x,…)	Renvoie l'argument maximum.
math.min (x,…)	Renvoie l'argument minimum.

math.modf (x)	Renvoie les parties intégrales et fractionnaires de x.
math.random ()	Renvoie un nombre pseudo-aléatoire compris entre 0 et 1.
math.random (m)	Renvoie un entier pseudo-aléatoire compris entre 1 et m.
math.random (m, n)	Renvoie un entier pseudo-aléatoire compris entre m et n.
math.randomseed (x)	Définit x pour le générateur de nombres pseudo-aléatoires.
math.sqrt (x)	Renvoie la racine carrée de x (x^0,5)
math.acos (x)	Renvoie l'arc-cosinus de x (en radians).
math.asin (x)	Renvoie l'arc-sinus de x (en radians).
math.atan (x)	Renvoie l'arc-tangent de x (en radians).
math.atan2 (y, x)	Renvoie l'arc-tangent de y/x (en radians).
math.cos (x)	Renvoie le cosinus de x.
math.cosh (x)	Renvoie le cosinus hyperbolique de x.
math.sin (x)	Renvoie le sinus de x.
math.sinh (x)	Renvoie le sinus hyperbolique de x.
math.tan (x)	Renvoie la tangente de x.
math.tanh (x)	Renvoie la tangente hyperbolique de x.
math.deg (x)	Renvoie l'angle x (exprimé en radians) en degrés.
math.exp (x)	Renvoie la valeur e^x.
math.frexp (x)	Renvoie m et e tels que x = m2e, e est un entier et la valeur absolue de m se situe dans la plage [0,5, 1).
math.ldexp (m, e)	Retourne m2e (e devrait être un entier).
math.log (x [, base])	Renvoie le logarithme de x dans la base donnée. La valeur par défaut pour base est e.
math.pow (x, y)	Renvoie x^y.

math.rad (x)	Renvoie l'angle x (exprimé en degrés) en radians.
math.pi	La valeur de π.

Bibliothèque Bitwise

Sauf indication contraire :

- Toutes les fonctions acceptent des arguments numériques dans la plage (-2^51, +2^51).
- Chaque argument est normalisé par rapport au reste de sa division par 2^32 et tronqué en un entier (d'une manière non spécifiée), de sorte que sa valeur finale se situe dans la plage [0,2^32 - 1].
- Tous les résultats se situent dans la plage [0,2^32 - 1].

bit32.arshift (x, disp)	Renvoie x bits de disp décalés arithmétiquement vers la droite (+disp) ou vers la gauche (-disp).
bit32.band (…)	Renvoie la valeur bit par bit des arguments.
bit32.bnot (x)	Renvoie la négation bit par bit de x.
bit32.bor (…)	Renvoie la valeur bit par bit ou des arguments.
bit32.btest(…)	Renvoie la valeur true si le nombre de bits par bit des arguments n'est pas nul.
bit32.bxor (…)	Renvoie le bit exclusif ou des arguments.
bit32.extract (n, champ [, largeur])	Retourne les bits en n du champ au champ + largeur - 1 (nombre de bits du plus au moins significatif). La valeur par défaut pour la largeur est 1.
bit32.replace (n, v, champ [, largeur])	Renvoie une copie de n avec les bits d'un champ à l'autre, plus la largeur -1 est remplacée par v. La largeur par défaut est 1.
bit32.lrotate (x, disp)	Renvoie x bits de disp pivotés vers la gauche (+disp) ou vers la droite (-disp).
bit32.lshift (x, disp)	Renvoie x bits de disp décalés vers la gauche (+disp) ou vers la droite (-disp).

bit32.rrotate (x, disp)	Renvoie x bits de disp pivotés vers la droite (+disp) ou vers la gauche (-disp).
bit32.rshift (x, disp)	Renvoie x bits de disp décalés vers la droite (+disp) ou vers la gauche (-disp).

Bibliothèque du système d'exploitation

horloge du système d'exploitation ()	Renvoie une approximation de la quantité en secondes de temps CPU.
os.date ([format [, heure]])	Renvoie une chaîne ou un tableau contenant la date et l'heure, formaté selon le format de chaîne donné.
os.time ([table])	Renvoie l'heure actuelle lorsqu'elle est appelée sans arguments, ou une heure représentant la date et l'heure spécifiées par la table donnée.
os.difftime (t2, t1)	Renvoie le nombre de secondes entre l'instant t1 et l'instant t2.

Bibliothèque NetScaler

ns.logger:level (message)	Pour enregistrer les messages dont le niveau est « urgence », « alerte », « critique », « erreur », « avertissement », « notice », « information » ou « débogage ». Les paramètres sont les mêmes que ceux de la fonction C printf () : une chaîne de format et un nombre variable d'arguments pour fournir des valeurs pour les spécificateurs % dans la chaîne de format.

Référence de l'API des extensions NetScaler

May 5, 2023

Les comportements sont une formalisation de modèles programmables courants disponibles sur une appliance NetScaler. Par exemple, un serveur virtuel TCP prend en charge un comportement de client TCP et un comportement de serveur TCP. Un comportement est un ensemble prédéfini de fonctions de rappel. Vous pouvez implémenter des comportements en fournissant des fonctions de rappel. Par exemple, le comportement d'un client TCP peut consister en la fonction on_data, qui traite le flux de données TCP.

Comportement du client TCP

on_data - fonction de rappel pour les événements de données du client TCP. Le callback prend deux arguments :

- **ctxt - Contexte** de traitement du client TCP
- **charge utile : charge utile** de l'événement
  - **payload.data - Données** TCP reçues, disponibles sous forme de flux d'octets

Comportement du serveur TCP

on_data - fonction de rappel pour les événements de données du serveur TCP, le rappel prend deux arguments :

- **ctxt - Contexte** de traitement du serveur TCP
- **charge utile : charge utile** de l'événement
  - **payload.data - données** TCP reçues, disponibles sous forme de flux d'octets

Contexte du client TCP

Le contexte qui est transmis aux rappels d'événements du client TCP :

- **ctxt.output** - Le contexte de traitement suivant dans le pipeline. Les gestionnaires de rappel d'extensions peuvent envoyer des données de type ns.tcp.stream à ctxt.output à l'aide des événements DATA, qui signifie un message partiel ou EOM, qui signifie un message de fin de protocole. L'événement EOM peut contenir ou non des données TCP. Un événement EOM avec des données TCP peut être envoyé sans événement DATA préalable pour envoyer des données de message de protocole complètes et marquer la fin du message. La décision d'équilibrage de charge est prise, en aval par le serveur virtuel d'équilibrage de charge, sur les premières données reçues. Une nouvelle décision d'équilibrage de charge est prise après la réception du message EOM. Ainsi, pour diffuser les données des messages de protocole, envoyez plusieurs

événements DATA avec le dernier événement comme EOM. Tous les événements DATA contigus et les événements EOM suivants sont envoyés à la même connexion serveur sélectionnée par la décision d'équilibrage de charge sur le premier événement DATA de la séquence.

- **ctxt.input** - Le contexte de traitement précédent dans le pipeline d'où proviennent les données du flux TCP.
- **ctxt:hold (data)** - Fonction permettant de stocker les données pour un traitement ultérieur. Lors d'un appel en attente avec des données, les données sont stockées dans le contexte. Plus tard, lorsque d'autres données sont reçues dans le même contexte, les données nouvellement reçues sont ajoutées aux données précédemment stockées et le flux de données combiné est ensuite transmis à la fonction de rappel on_data. Après l'appel d'une mise en attente, la référence de données n'est plus utilisable et génère des erreurs à chaque utilisation.
- **ctxt.vserver - Le contexte du serveur** virtuel.
- **ctxt.client** : contexte de traitement de la connexion client. Ce contexte de traitement peut être utilisé pour envoyer des données au client et pour récupérer certaines informations relatives à la connexion, telles que l'adresse IP, les ports source et de destination.
- **ctxt:close ()** — Ferme la connexion client en envoyant FIN au client Après avoir appelé cette API, le contexte de traitement du client n'est plus utilisable et génère des erreurs à chaque utilisation.

Contexte du serveur TCP

Le contexte qui est transmis aux rappels d'événements du serveur TCP :

- **ctxt.output** — Le contexte de traitement suivant dans le pipeline. Les gestionnaires de rappel d'extensions peuvent envoyer des données de type ns.tcp.stream à ctxt.output à l'aide des événements DATA, qui signifie un message partiel ou EOM, qui signifie un message de fin de protocole.
- **ctxt.input** - Le contexte de traitement précédent dans le pipeline d'où proviennent les données du flux TCP.
- **ctxt:hold (data)** - Fonction permettant de stocker les données pour un traitement ultérieur. Lors d'un appel en attente avec des données, les données sont stockées dans le contexte. Plus tard, lorsque d'autres données sont reçues dans le même contexte, les données nouvellement reçues sont ajoutées aux données précédemment stockées et le flux de données combiné est ensuite transmis à la fonction de rappel on_data. Après l'appel d'une mise en attente, la référence de données n'est plus utilisable et génère des erreurs à chaque utilisation.
- **ctxt.vserver - Le contexte du serveur** virtuel.
- **ctxt.server** - Contexte de traitement de la connexion au serveur. Ce contexte de traitement peut être utilisé pour envoyer des données au serveur et pour récupérer certaines informations relatives à la connexion, telles que l'adresse IP, les ports source et de destination.

- **ctxt:reuse_server_connection ()** - Cette API est utilisée pour permettre la réutilisation de la connexion au serveur pour d'autres connexions client dans le contexte du serveur uniquement. Cette API ne peut être utilisée que si un événement EOM est utilisé (dans l'API ns.send ()) pour envoyer les données dans le contexte client. Dans le cas contraire, l'appliance ADC renvoie une erreur.

  Pour permettre à une connexion serveur d'être réutilisée par d'autres clients, cette API doit être appelée à la fin de chaque message de réponse. Après avoir appelé cette API, si d'autres données sont reçues sur cette connexion au serveur, cela est considéré comme une erreur et la connexion au serveur est fermée. Si cette API n'est pas utilisée, la connexion au serveur ne peut être utilisée que pour le client pour lequel elle a été ouverte. De même, si le même serveur est sélectionné pour une autre décision d'équilibrage de charge pour ce client, la même connexion au serveur est utilisée pour envoyer les données du client. Après avoir utilisé cette API, la connexion au serveur cesse d'être liée à la connexion client pour laquelle elle a été ouverte et peut être réutilisée pour une nouvelle décision d'équilibrage de charge pour toute autre connexion client. Après avoir appelé cette API, le contexte du serveur n'est plus utilisable et génère une erreur à chaque utilisation.

  Remarque : Cette API est disponible dans NetScaler 12.1 build 49.xx et versions ultérieures.

- **ctxt:close ()** — Ferme la connexion au serveur en envoyant FIN au serveur Après avoir appelé cette API, le contexte de traitement du client n'est plus utilisable et affiche une erreur à chaque utilisation.

  Remarque : Cette API est disponible dans NetScaler 12.1 build 50.xx et versions ultérieures.

Contexte du serveur virtuel

Le contexte du serveur virtuel utilisateur disponible via les contextes transmis aux rappels :

- **vserver:counter_increment (counter_name)** - Incrémente la valeur d'un compteur de serveur virtuel passé en argument. Les compteurs intégrés suivants sont actuellement pris en charge.
  - **- invalid_messages** — Nombre de demandes/réponses non valides sur ce serveur virtuel.
  - **- invalid_messages_dropped** — Nombre de demandes/réponses non valides supprimées par ce serveur virtuel.
- **vserver.params** : paramètres configurés pour le serveur virtuel utilisateur. Les paramètres permettent de configurer les extensions. Le code d'extension peut accéder aux paramètres spécifiés dans la CLI pour ajouter un serveur virtuel utilisateur.

Contexte de connexion du client

Contexte de traitement de la connexion client pour obtenir des informations relatives à la connexion.

- **client.ssl — Contexte SSL**
- **client.tcp — contexte TCP**
- **client.is_ssl** — Vrai si la connexion client est basée sur SSL

Contexte de connexion au serveur

Contexte de traitement de la connexion au serveur pour obtenir des informations relatives à la connexion.

- **server.ssl — Contexte SSL**
- **server.tcp — Contexte TCP**
- **server.is_ssl** — Vrai si la connexion au serveur est basée sur SSL

Contexte TCP

Le contexte TCP fonctionne selon le protocole TCP.

- **tcp.srcport — Port** source sous forme de numéro
- **tcp.dstport - Port de** destination sous forme de numéro

Contexte IP

Le contexte IP fonctionne sur les données du protocole IP ou IPv6.

- **ip.src** - Contexte de l'adresse IP source.
- **ip.dst - Contexte** de l'adresse IP de destination.

Remarque : Cette API est disponible dans NetScaler 12.1 build 51.xx et versions ultérieures.

Contexte de l'adresse IP

Le contexte d'adresse IP fonctionne sur les données d'adresse IP ou IPv6.

- **<address>.to_s** - La chaîne d'adresse dans la notation ASCII appropriée.
- **<address>.to_n** - La valeur numérique de l'adresse sous forme de chaîne d'octets dans l'ordre du réseau (4 octets pour IPv4 et 16 octets pour IPv6).
- **<address>.version** - Renvoie 4 pour IPv4 et 6 pour IPv6.
- **<address>:subnet(<prefix value>)** - Renvoie la chaîne d'adresse du sous-réseau après application du numéro de préfixe.
  - Pour l'adresse IPv4, la valeur doit être comprise entre 0 et 32
  - Pour l'adresse IPv6, la valeur doit être comprise entre 0 et 128.

- **<address>:apply_mask(<mask string>)** - Renvoie la chaîne d'adresse après l'application de la chaîne de masque. L'API valide la version de l'argument et vérifie les erreurs de manière appropriée.
- **address>:eq(<address string>)** - Renvoie vrai ou faux selon que l'argument est équivalent à l'objet d'adresse. L'API valide la version des arguments.

Remarque : Cette API est disponible dans NetScaler 12.1 build 51.xx et versions ultérieures.

Contexte SSL

Le contexte SSL fournit des informations relatives à la connexion SSL frontale.

- **ssl.cert : contexte du** certificat SSL. Pour la connexion client, il fournit le contexte du certificat client et pour la connexion au serveur, il fournit le contexte du certificat serveur.
- **ssl.version** : nombre qui représente la version du protocole SSL de la transaction en cours, comme suit :

  - - 0: The transaction is not SSL-based
  - - 0x002: The transaction is SSLv2
  - - 0x300: The transaction is SSLv3
  - - 0x301: The transaction is TLSv1
  - - 0x302: The transaction is TLSv1.1
  - - 0x303: The transaction is TLSv1.2

- **ssl.cipher_name - Le nom du** chiffrement SSL sous forme de chaîne s'il est appelé depuis une connexion SSL, sinon donne une chaîne NULL.
- **ssl.cipher_bits — Nombre de bits** dans la clé cryptographique.

Contexte du certificat SSL

- **cert.version** — Numéro de version du certificat. Si la connexion n'est pas basée sur SSL, renvoie 0.
- **cert.VALID_NOT_BEFORE — Date au format chaîne avant** laquelle le certificat n'est pas valide.
- **cert.VALID_NOT_AFTER — Date au format chaîne après** laquelle le certificat n'est plus valide.
- **cert.days_to_expire** — Nombre de jours avant lesquels le certificat est valide. Renvoie -1 pour un certificat expiré.
- **cert.to_PEM** — Certificat au format binaire.
- **cert.issuer** - Nom distinctif (DN) de l'émetteur dans le certificat sous forme de liste nom-valeur. Le signe égal (« = ») est le délimiteur du nom et de la valeur, et la barre oblique («/») est le délimiteur qui sépare les paires nom-valeur.

Voici un exemple du DN renvoyé :
/C =US/O=MyCompany/OU=www.mycompany.com/CN=www.mycompany.com/EmailAddress=myuserid@mycompany.com

- **cert.auth_keyid** — Contexte de l'extension Authority Key Identifier du certificat X.509 V3.
  - **auth_keyid.exists** : VRAI si le certificat contient une extension Authority Key Identifier.
  - **auth_keyid.issuer_name - Nom** distinctif de l'émetteur dans le certificat sous forme de liste nom-valeur.
    Le signe égal (« = ») est le délimiteur du nom et de la valeur, et la barre oblique («/») est le délimiteur qui sépare les paires nom-valeur.

  Voici un exemple :
  /C =us/o=MyCompany/ou=www.mycompany.com/cn=www.mycompany.com/EmailAddress=myuserid@mycompany.com
  - **auth_keyid.keyid - Champ keyIdentifier de l'identifiant** de clé d'autorité en tant que blob
  - **auth_keyid.cert_serialnumber : champ SerialNumber** de l'identifiant de clé d'autorité en tant que blob.
- **cert.pk_algorithm** : nom de l'algorithme à clé publique utilisé par le certificat.
- **cert.pk_size - Taille** de la clé publique utilisée dans le certificat.
- **cert.serialnumber - Numéro de** série du certificat client. S'il s'agit d'une transaction non SSL ou s'il y a une erreur dans le certificat, cela donne une chaîne vide.
- **cert.signature_algorithm : nom de l'algorithme** cryptographique utilisé par l'autorité de certification pour signer ce certificat.
- **cert.subject_keyid : ID** de clé d'objet du certificat client. S'il n'y a pas de Subject KeyID, cela donne un objet de texte de longueur nulle.
- **cert.subject** - Nom distinctif du sujet en tant que valeur-nom. Un signe égal (« = ») sépare les noms des valeurs et une barre oblique («/») délimite les paires nom-valeur.

Voici un exemple :
/C =us/o=MyCompany/ou=www.mycompany.com/cn=www.mycompany.com/EmailAddress=myuserid@mycompany.com

Bibliothèques NetScaler

- **ns.tcp.stream** - Bibliothèque de type chaîne pour gérer les données TCP sous forme de flux d'octets. La taille maximale des données de flux TCP sur lesquelles ces API peuvent fonctionner est de 128 Ko. Les fonctions de la bibliothèque ns.tcp.stream peuvent également être appelées

dans le style d'appel habituel orienté objet d'extension. Par exemple, data:len () est identique à ns.tcp.stream.len (data)

- **ns.tcp.stream.len (data) - Renvoie la longueur des données** en octets, similaire à la chaîne .len de Lua
- **ns.tcp.stream.find (data, pattern [, init])** - Fonction similaire à la chaîne string.find de Lua. En outre, il effectue également une correspondance partielle à la fin des données. En cas de correspondance partielle, l'indice de départ est renvoyé et l'indice de fin devient nul.
- **ns.tcp.stream.split (data, length)** - Divise les données en deux segments, le premier étant de la longueur spécifiée. Après un fractionnement réussi, les données d'origine ne sont plus utilisables en tant que flux de données TCP. Toute tentative de l'utiliser de cette manière entraîne une erreur.
- **ns.tcp.stream.byte (data [, i [, j]]) - Fonction similaire à string.byte** de Lua. Renvoie les codes numériques internes des caractères data [i], data [i+1],..., data [j].
- n**s.tcp.stream.sub (data, i [, j])** - Fonction similaire à la chaîne string.sub de Lua. Renvoie la sous-chaîne de s qui commence à i et continue jusqu'à j.
- **ns.tcp.stream.match (data, pattern, [, init])** - Fonction similaire à la fonction string.match de Lua. Recherche la première *correspondance* du modèle dans la chaîne s.

- **ns.send (processing_ctxt, event_name, event_data)** - Fonction générique permettant d'envoyer des événements vers un contexte de traitement. Les données d'événements sont une table Lua qui peut contenir n'importe quel contenu. Le contenu dépend de l'événement. Une fois l'API ns.send () appelée, la référence de données n'est plus utilisable. Toute tentative d'utilisation entraîne une erreur.
- **ns.pipe (src_ctxt, dest_ctxt) - À l'aide d'un appel à l'API pipe ()**, le code d'extension peut connecter le contexte source à un contexte de destination. Après un appel à pipe, tous les événements envoyés du contexte source au module suivant du pipeline vont directement au contexte de destination. Cette API est généralement utilisée par le module qui fait l'appel pipe () pour se retirer du pipeline.
- **ns.inet** — Bibliothèque d'adresses Internet.
  - **ns.inet.apply_mask (address_str, mask_str) - renvoie** la chaîne d'adresse après l'application de la chaîne de masque.
  - **ns.inet.aton (address_str)** - Renvoie la valeur numérique de l'adresse sous forme de chaîne d'octets dans l'ordre du réseau (4 octets pour IPv4 et 16 pour IPv6).
  - **ns.inet.ntoa (byte_str) - Convertit une** valeur d'octet numérique en chaîne d'octets en chaîne d'adresse.
  - **ns.inet.ntohs (number)** - Convertit l'ordre des octets du réseau donné en ordre des octets de l'hôte. Si l'entrée est supérieure à 2^16 - 1, renvoie une erreur.
  - **ns.inet.htons (number)** - Convertit l'ordre des octets de l'hôte donné en ordre des octets

du réseau. Si l'entrée est supérieure à 2^16 - 1, renvoie une erreur.
- **ns.inet.ntohl (number)** : convertit l'ordre des octets du réseau donné en ordre des octets de l'hôte. Si l'entrée est supérieure à 2^32 - 1, renvoie une erreur.
- **ns.inet.htonl (number)** : convertit l'ordre des octets de l'hôte donné en ordre des octets du réseau. Si l'entrée est supérieure à 2^32 - 1, renvoie une erreur.
- **ns.inet.subnet (address_str, subnet_value) — Renvoie la chaîne d'adresse du sous-réseau après** l'application du sous-réseau donné.

Extensions de protocole

May 5, 2023

Les appliances NetScaler prennent en charge nativement des protocoles tels que HTTP. En outre, vous pouvez utiliser des extensions de protocole pour ajouter la prise en charge de protocoles personnalisés. Actuellement, seuls les protocoles personnalisés basés sur le protocole TCP sont pris en charge, par exemple le protocole MQTT (Message Queuing Telemetry Transport). Pour les transactions sécurisées, le protocole TCP sur SSL est également pris en charge.

Les extensions de protocole de l'appliance NetScaler font partie de l'infrastructure de script de haut niveau disponible sur l'appliance NetScaler. Le langage de script est basé sur le langage de programmation Lua 5.2. Pour ajouter un protocole personnalisé à une appliance NetScaler, l'utilisateur doit écrire un code d'extension pour implémenter les comportements applicables. Par exemple, les comportements ns.tcp.client et ns.tcp.server sont applicables aux protocoles basés sur TCP. Pour implémenter un comportement, implémentez uniquement les rappels que vous souhaitez personnaliser. Si le rappel n'est pas implémenté, sa valeur par défaut prend effet. Pour plus d'informations sur le langage de script, consultez NetScaler Extensions -Présentation du langage. Pour plus d'informations sur les comportements, consultez la section Référence de l' API NetScaler Extensions.

Les extensions du protocole NetScaler peuvent être utilisées aux fins suivantes :

- Ajoutez la prise en charge de nouveaux protocoles sur l'appliance NetScaler par programmation, à l'aide d'extensions.
- Analysez le trafic du protocole et effectuez un équilibrage de charge basé sur les messages (MBLB) spécifique au protocole.
- Configurer la persistance d'équilibrage de charge définie par l'utilisateur.

Extensions de protocole - architecture

May 5, 2023

Pour obtenir une extensibilité au niveau du trafic, le traitement du trafic sur une appliance NetScaler est présenté sous la forme d'un pipeline de modules de traitement distincts. Le trafic les traverse au fur et à mesure qu'il le traite de l'entrée à la sortie. Ces modules du pipeline suivent un modèle de partage nul. La transmission de messages est utilisée pour envoyer les données de trafic d'un module du pipeline au module suivant.

Certains points du pipeline de traitement du trafic sont étendus afin que vous puissiez ajouter du code pour personnaliser le comportement de NetScaler.

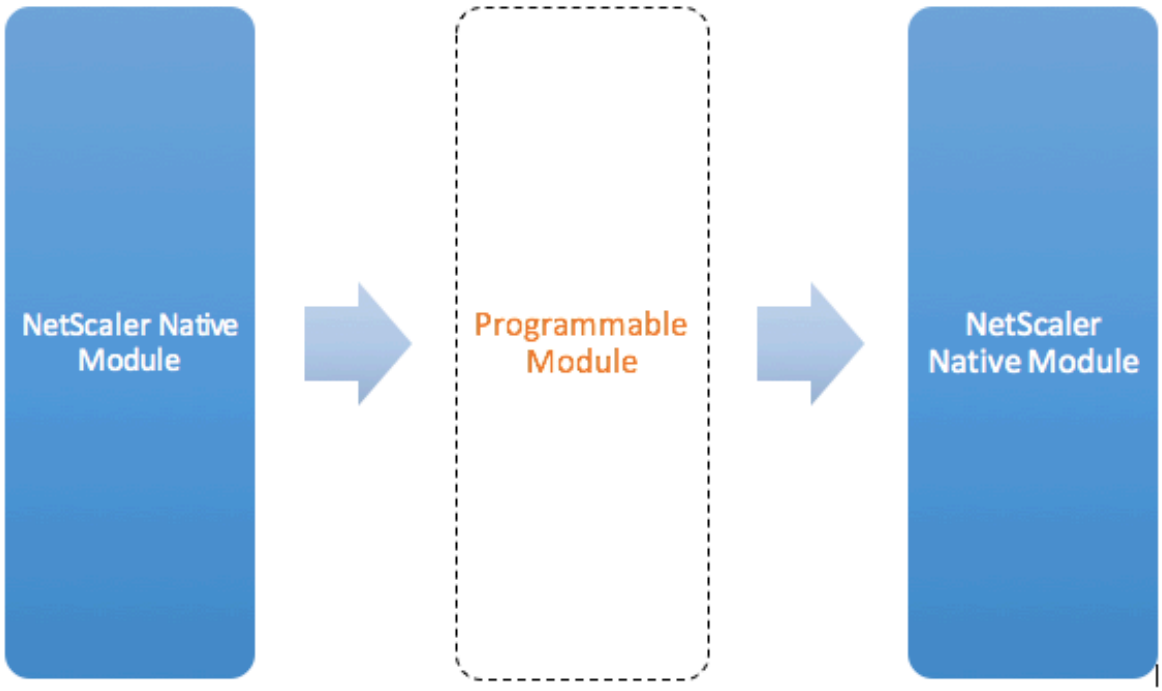


Figure: A Programmable Module In the Traffic Pipeline

Par défaut, le trafic contourne un module programmable auquel vous n'ajoutez aucun code.

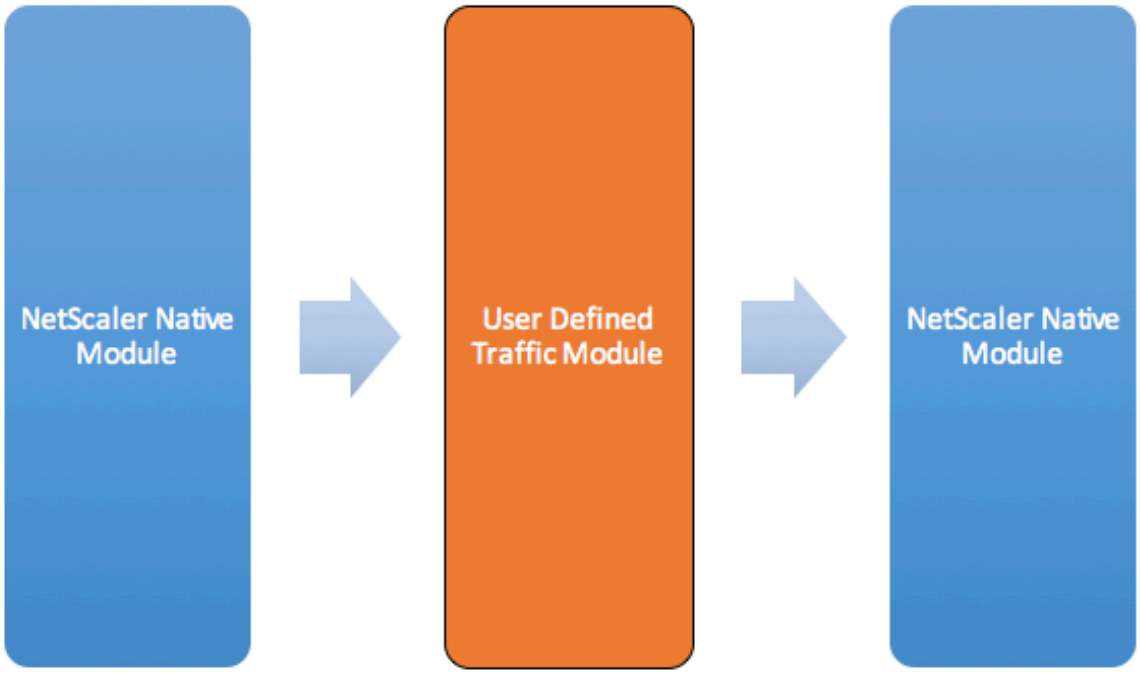


Figure: User Defined Traffic Module

Comportements

Les interfaces programmables permettant de personnaliser la gestion du trafic sont appelées comportements. Les comportements sont essentiellement une formalisation de modèles programmables courants disponibles sur une appliance NetScaler. Les comportements consistent en un ensemble prédéfini de fonctions de rappel d'événements. Vous pouvez implémenter un comportement en fournissant des fonctions de rappel conformes au comportement.

Par exemple, le comportement du client TCP consiste en une fonction de rappel (on_data) qui traite les événements du flux de données du client TCP. Pour implémenter l'équilibrage de charge basé sur les messages (MBLB) pour un protocole TCP, vous pouvez ajouter du code pour cette fonction de rappel afin de traiter le flux de données TCP provenant du client et d'analyser le flux d'octets en messages de protocole.

Contexte :

Les fonctions de rappel d'un comportement sont appelées avec un contexte, qui correspond à l'état du module de traitement. Le contexte est l'instance du module de traitement. Par exemple, les rappels du comportement du client TCP sont appelés avec différents contextes pour différentes connexions TCP clientes.

Charge utile :

En plus du contexte, les fonctions de rappel de comportement peuvent comporter d'autres arguments. Habituellement, le reste des arguments est passé en tant que charge utile, qui est la collection de tous les arguments.

Ainsi, les instances du module de traitement programmable peuvent être considérées comme une combinaison de fonctions d'état d'instance et de rappel d'événement, c'est-à-dire le contexte et le comportement. Et le trafic circule à travers le pipeline comme charge utile d'événement.

Pour les extensions de l'API NetScaler, consultez la référence de l'API de l'extension NetScaler.

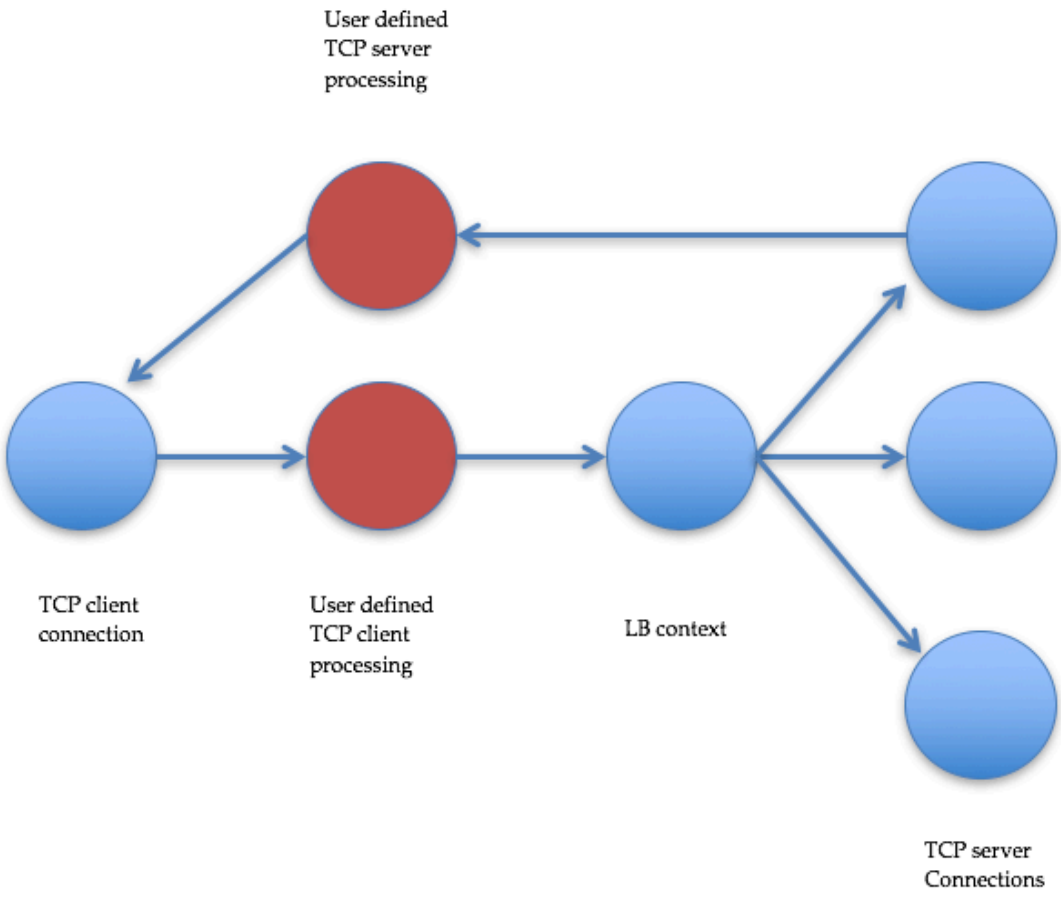
L'extrait de code suivant montre une fonction définie par l'utilisateur pour gérer les événements de flux de données client TCP. Le contexte et la charge utile sont transmis à la fonction par le code NetScaler. Ce code transmet simplement les données TCP reçues lors de chaque appel au contexte du module de traitement suivant du pipeline. Dans ce cas, le module suivant est le contexte d'équilibrage de charge (LB), qui est un module natif NetScaler.

```
function client.on_data(ctxt, payload)
    ns.send(ctxt.output, "DATA", {
 data = payload.data }
 )
end
<!--NeedCopy-->
```

Extensions de protocole : pipeline de trafic pour les comportements client et serveur TCP définis par l'utilisateur

May 5, 2023

La figure suivante illustre l'exemple d'extension de protocole : pipeline de trafic pour les comportements des clients et des serveurs TCP définis par l'utilisateur.



Traffic Pipeline For User Defined TCP Client And Server Behaviors

Ajouter un protocole personnalisé à l'aide d'extensions de protocole

Les commandes de l'interface de ligne de commande (CLI) pour le protocole personnalisé utilisent le mot clé « user » pour indiquer la nature définie par l'utilisateur des entités de configuration sous-jacentes. À l'aide du code d'extension, vous pouvez ajouter un nouveau protocole utilisateur au système et ajouter des serveurs virtuels utilisateur pour les protocoles définis par l'utilisateur. Les serveurs virtuels utilisateur sont à leur tour configurables en définissant des paramètres. Les valeurs configurées pour les paramètres du serveur virtuel sont disponibles dans le code d'extension.

L'exemple suivant illustre le flux utilisateur permettant d'ajouter la prise en charge d'un nouveau protocole. L'exemple ajoute la prise en charge du protocole MQTT au système. Le MQTT est un protocole de connectivité « Internet des objets » de machine à machine. Il s'agit d'un moyen de transport léger de messagerie de publication/d'abonnement. Utile pour les connexions avec des sites distants, ce protocole utilise des outils client et courtier pour publier des messages à l'intention des abonnés.

1. Importez le fichier d'implémentation de l'extension du protocole MQTT dans le système NetScaler. La liste des codes pour mqtt.lua est présentée ci-dessous. L'exemple ci-dessous importe le fichier d'extension MQTT hébergé sur un serveur Web.

   ```
   import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
   ```

2. Ajoutez un nouveau protocole utilisateur basé sur TCP au système à l'aide de l'extension.

   ```
   add user protocol MQTT -transport TCP -extension mqtt_code
   ```

3. Ajoutez un serveur virtuel d'équilibrage de charge utilisateur et liez-y les services principaux.

   ```
   add service mqtt_svr1 10.217.24.48 USER_TCP 1501
   add service mqtt_svr2 10.217.24.48 USER_TCP 1502
   add lb vserver mqtt_lb USER_TCP  - lbmethod USER_TOKEN
   bind lb vserver mqtt_lb mqtt_svr1
   bind lb vserver mqtt_lb mqtt_svr2
   <!--NeedCopy-->
   ```

4. Ajoutez un serveur utilisateur pour le protocole nouvellement ajouté. Définissez le paramètre defaultlb sur le serveur virtuel LB configuré ci-dessus.

   ```
   add user vserver mqtt_vs MQTT 10.217.24.28 8765 -defaultLb mqtt_lb
   ```

5. Le cas échéant, activez la persistance de session MQTT en fonction de l'ID client, définissez le type de persistance sur USERSESSION.

   ```
   set lb vserver mqtt_lb -persistenceType USERSESSION
   ```

Extensions de protocole - cas d'utilisation

May 5, 2023

Les extensions de protocole peuvent être utilisées pour les cas d'utilisation suivants.

- Équilibrage de charge basé sur les messages (MBLB)
- Streaming
- Équilibrage de charge basé sur des jetons
- Persistance de l'équilibrage de charge
- Équilibrage de charge basé sur la connexion TCP
- Équilibrage de charge basé sur le contenu
- SSL
- Modifier le trafic
- Générer du trafic vers le client ou le serveur
- Données de traitement relatives à l'établissement de la connexion

Équilibrage de charge basé sur les messages

Les extensions de protocole prennent en charge l'équilibrage de charge basé sur les messages (MBLB), qui permet d'analyser n'importe quel protocole sur une appliance NetScaler et d'équilibrer la charge des messages de protocole arrivant sur une connexion client, c'est-à-dire de distribuer les messages sur plusieurs connexions serveur. Le MBLB est obtenu par un code utilisateur qui analyse le flux de données TCP du client.

Le flux de données TCP est transmis aux rappels on_data pour les comportements du client et du serveur. Le flux de données TCP est accessible aux fonctions d'extension via une interface de type chaîne Lua. Vous pouvez utiliser une API similaire à l'API de chaîne Lua pour analyser le flux de données TCP.

Les API utiles incluent :

```
data:len()
```

```
data:find()
```

```
data:byte()
```

```
data:sub()
```

```
data:split()
```

Une fois que le flux de données TCP a été analysé en un message de protocole, le code utilisateur équilibre la charge en envoyant simplement le message de protocole au prochain contexte disponible à partir du contexte transmis au rappel on_data pour le client.

L'API ns.send () est utilisée pour envoyer des messages à d'autres modules de traitement. Outre le contexte de destination, l'API d'envoi prend le nom de l'événement et la charge utile facultative comme arguments. Il existe une correspondance biunivoque entre le nom de l'événement et les noms des fonctions de rappel pour les comportements. <event_name>Les rappels pour les événements sont appelés on_. Les noms de rappel utilisent uniquement des minuscules.

Par exemple, les rappels on_data du client et du serveur TCP sont des gestionnaires définis par l'utilisateur pour les événements nommés « DATA ». Pour envoyer l'intégralité du message de protocole en un seul appel d'envoi, l'événement EOM est utilisé. EOM, qui signifie fin de message, signifie la fin du message de protocole envoyé au contexte LB en aval. Une nouvelle décision d'équilibrage de charge est donc prise pour les données qui suivent ce message.

Le code d'extension peut parfois ne pas recevoir l'intégralité du message de protocole lors de l'événement on_data. Dans ce cas, les données peuvent être conservées à l'aide de l'API ctxt:hold (). L'API hold est disponible à la fois pour les contextes TCP client et serveur de rappel. Lorsque l'option « Conserver les données » est appelée, les données sont stockées dans le contexte. Lorsque d'autres données sont reçues dans le même contexte, les données nouvellement reçues sont ajoutées aux données précédemment stockées et la fonction de rappel on_data est appelée à nouveau avec les données combinées.

Remarque : La méthode d'équilibrage de charge utilisée dépend de la configuration du serveur virtuel d'équilibrage de charge correspondant au contexte d'équilibrage de charge.

L'extrait de code suivant montre l'utilisation de l'API d'envoi pour envoyer le message de protocole analysé.

Exemple :

```
    function client.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to lb
        ns.send(ctxt.output, "EOM", {
 data = message }
 )
    end -- client.on_data

    function server.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to client
        ns.send(ctxt.output, "EOM", {
 data = message }
 )

    end -- server.on_data
<!--NeedCopy-->
```

Streaming

Dans certains scénarios, il peut ne pas être nécessaire de suspendre le flux de données TCP jusqu'à ce que l'intégralité du message de protocole soit collectée. En fait, ce n'est pas conseillé à moins que cela ne soit nécessaire. La conservation des données augmente l'utilisation de la mémoire sur l'appliance NetScaler et peut rendre l'appliance vulnérable aux attaques DDoS en épuisant la mémoire de l'appliance NetScaler avec des messages de protocole incomplets sur de nombreuses connexions.

Les utilisateurs peuvent diffuser des données TCP dans les gestionnaires de rappel des extensions à l'aide de l'API d'envoi. Au lieu de conserver les données jusqu'à ce que l'ensemble du message soit collecté, les données peuvent être envoyées par morceaux. L'envoi de données à ctxt.output à l'aide de l'événement DATA envoie un message de protocole partiel. Elle peut être suivie d'autres événements DATA. Un événement EOM doit être envoyé pour marquer la fin du message de protocole. Le contexte d'équilibrage de charge en aval prend la décision d'équilibrage de charge sur la base des pre-

mières données reçues. Une nouvelle décision d'équilibrage de charge est prise après la réception du message EOM.

Pour diffuser les données des messages de protocole, envoyez plusieurs événements DATA suivis d'un événement EOM. Les événements DATA contigus et l'événement EOM suivant sont envoyés à la même connexion serveur sélectionnée par décision d'équilibrage de charge pour le premier événement DATA de la séquence.

Dans le cas d'un contexte d'envoi vers un client, les événements EOM et DATA sont en fait identiques, car le contexte client ne gère pas spécialement les événements EOM en aval.

Équilibrage de charge basé sur des jetons

Pour les protocoles pris en charge nativement, une appliance NetScaler prend en charge une méthode d'équilibrage de charge basée sur des jetons qui utilise des expressions PI pour créer le jeton. Pour les extensions, le protocole n'étant pas connu à l'avance, les expressions PI ne peuvent pas être utilisées. Pour l'équilibrage de charge basé sur des jetons, vous devez définir le serveur virtuel d'équilibrage de charge par défaut pour qu'il utilise la méthode d'équilibrage de charge USER_TOKEN et fournir la valeur du jeton à partir du code d'extension en appelant l'API d'envoi avec un champ user_token. Si la valeur du jeton est envoyée depuis l'API d'envoi et que la méthode d'équilibrage de charge USER_TOKEN est configurée sur le serveur virtuel d'équilibrage de charge par défaut, la décision d'équilibrage de charge est prise en calculant un hachage basé sur la valeur du jeton. La longueur maximale de la valeur du jeton est de 64 octets.

```
add lb vserver v\\_mqttlb USER\\_TCP -lbMethod USER\\_TOKEN
```

L'extrait de code de l'exemple suivant utilise une API d'envoi pour envoyer la valeur d'un jeton LB.

Exemple :

```
        -- send the message to lb




        -- user_token is set to do LB based on clientID




        ns.send(ctxt.output, "EOM", {
data = message,

                                user_token = token_info }
)
```



```
<!--NeedCopy-->
```

Persistance de l'équilibrage de charge

La persistance de l'équilibrage de charge est étroitement liée à l'équilibrage de charge basé sur des jetons. Les utilisateurs doivent être en mesure de calculer par programmation la valeur de la session de persistance et de l'utiliser pour équilibrer la charge de persistance. L'API d'envoi est utilisée pour envoyer des paramètres de persistance. Pour utiliser la persistance de l'équilibrage de charge, vous devez définir le type de persistance USERSESSION sur le serveur virtuel d'équilibrage de charge par défaut et fournir un paramètre de persistance à partir du code d'extension en appelant l'API d'envoi avec un champ user_session. La longueur maximale de la valeur du paramètre de persistance est de 64 octets.

Si vous avez besoin de plusieurs types de persistance pour un protocole personnalisé, vous devez définir les types de persistance utilisateur et les configurer. Les noms des paramètres utilisés pour configurer les serveurs virtuels sont déterminés par l'implémenteur du protocole. La valeur configurée d'un paramètre est également disponible pour le code d'extension.

L'interface de ligne de commande et l'extrait de code suivants montrent l'utilisation d'une API d'envoi pour prendre en charge la persistance de l'équilibrage de charge. La liste de codes dans la section Liste de codes pour mqtt.lua illustre également l'utilisation du champ user_session.

Pour la persistance, vous devez spécifier le type de persistance USERSESSION sur le serveur virtuel d'équilibrage de charge et transmettre la valeur user_session à partir de l'API ns.send.

```
add lb vserver v\\_mqttlb USER\\_TCP -persistencetype USERSESSION
```

Envoyez le message MQTT à l'équilibreur de charge, en définissant le champ user_session sur ClientID dans la charge utile.

Exemple :

```
-- send the data so far to lb

-- user_session is set to clientID as well (it will be used to persist
   session)

ns.send(ctxt.output,  "DATA" , {
 data = data, user_session = clientID }
 )
<!--NeedCopy-->
```


Équilibrage de charge basé sur la connexion TCP

Pour certains protocoles, le MBLB peut ne pas être nécessaire. Au lieu de cela, vous aurez peut-être besoin d'un équilibrage de charge basé sur une connexion TCP. Par exemple, le protocole MQTT doit analyser la partie initiale du flux TCP pour déterminer le jeton pour l'équilibrage de charge. De plus, tous les messages MQTT de la même connexion TCP doivent être envoyés à la même connexion au serveur.

L'équilibrage de charge basé sur une connexion TCP peut être réalisé en utilisant l'API d'envoi avec uniquement des événements DATA et en n'envoyant aucun EOM. Ainsi, le contexte d'équilibrage de charge en aval base la décision d'équilibrage de charge sur les données reçues en premier et envoie toutes les données suivantes à la même connexion serveur sélectionnée par la décision d'équilibrage de charge.

En outre, certains cas d'utilisation peuvent nécessiter la possibilité de contourner la gestion des extensions une fois que la décision d'équilibrage de charge a été prise. Le contournement des appels d'extension permet d'améliorer les performances, car le trafic est traité uniquement par du code natif. Le contournement peut être effectué à l'aide de l'API ns.pipe (). Un appel au code d'extension de l'API pipe () peut connecter le contexte d'entrée à un contexte de sortie. Après l'appel à pipe (), tous les événements provenant du contexte d'entrée vont directement au contexte de sortie. En fait, le module à partir duquel l'appel pipe () est effectué est supprimé du pipeline.

L'extrait de code suivant montre la diffusion en continu et l'utilisation de l'API pipe() pour contourner un module. La liste de codes de la section Liste de codes pour mqtt.lua illustre également comment effectuer le streaming et l'utilisation de l'API pipe () pour contourner le module pour le reste du trafic sur la connexion.

Exemple :

```
        -- send the data so far to lb
        ns.send(ctxt.output, "DATA", {
 data = data,
                                    user_token = clientID }
 )
        -- pipe the subsequent traffic to the lb - to bypass the client
            on_data handler
        ns.pipe(ctxt.input, ctxt.output)
<!--NeedCopy-->
```

Équilibrage de charge basé sur le contenu

Pour les protocoles natifs, la fonctionnalité similaire à la commutation de contenu pour les extensions de protocole est prise en charge. Grâce à cette fonctionnalité, au lieu d'envoyer les données à

l'équilibrage de charge par défaut, vous pouvez envoyer les données à l'équilibreur de charge sélectionné.

La fonctionnalité de commutation de contenu pour les extensions de protocole est réalisée à l'aide de l'API ctxt:lb_connect ().<lbname> Cette API est disponible dans le contexte du client TCP. À l'aide de cette API, le code d'extension peut obtenir un contexte d'équilibrage de charge correspondant à un serveur virtuel d'équilibrage de charge déjà configuré. Vous pouvez ensuite utiliser l'API d'envoi avec le contexte d'équilibrage de charge ainsi obtenu.

Le contexte lb peut parfois être NULL :

- Le serveur virtuel n'existe pas
- Le serveur virtuel n'est pas du type de protocole utilisateur
- L'état du serveur virtuel n'est pas actif
- Le serveur virtuel est un serveur virtuel utilisateur, et non un serveur virtuel d'équilibrage de charge

Si vous supprimez le serveur virtuel d'équilibrage de charge cible lorsqu'il est utilisé, toutes les connexions associées à ce serveur virtuel d'équilibrage de charge sont réinitialisées.

L'extrait de code suivant montre l'utilisation de l'API lb_connect (). Le code mappe l'ID client aux noms de serveurs virtuels d'équilibrage de charge (lbname) à l'aide de la table Lua lb_map, puis obtient le contexte LB pour lbname à l'aide de lb_connect (). Enfin, envoie vers le contexte LB à l'aide de l'API d'envoi.

```
1     local lb_map = {
2
3        ["client1*"] = "lb_1",
4        ["client2*"] = "lb_2",
5        ["client3*"] = "lb_3",
6        ["client4*"] = "lb_4"
7      }
8
9
10    -- map the clientID to the corresponding LB vserver and connect to
         it
11    for client_pattern, lbname in pairs(lb_map) do
12       local match_idx = string.find(clientID, client_pattern)
13       if (match_idx == 1) then
14      lb_ctxt = ctxt:lb_connect(lbname)
15      if (lb_ctxt == nil) then
16         error("Failed to connect to LB vserver: " .. lbname)
17      end
18      break
19       end
20    end
```



```
21     if (lb_ctxt == nil) then
22     -- If lb context is NULL, the user can raise an error or send data
          to default LB
23        error("Failed to map LB vserver for client: " .. clientID)
24     end
25 -- send the data so far to lb
26 ns.send(lb_ctxt, "DATA", {
27  data = data }
28
29 <!--NeedCopy-->
```

SSL

Le protocole SSL pour les protocoles utilisant des extensions est pris en charge de la même manière que le protocole SSL pour les protocoles natifs. En utilisant le même code d'analyse pour créer des protocoles personnalisés, vous pouvez créer une instance de protocole via TCP ou SSL qui peut ensuite être utilisée pour configurer les serveurs virtuels. De même, vous pouvez ajouter des services utilisateur via TCP ou SSL.

Pour plus d'informations, consultez Configuration du déchargement SSL pour MQTT et Configuration du déchargement SSL pour MQTT avec chiffrement de bout en bout.

Multiplexage de connexion serveur

Parfois, le client envoie une demande à la fois et envoie la demande suivante uniquement après réception de la réponse du serveur à la première demande. Dans ce cas, la connexion au serveur peut être réutilisée pour d'autres connexions client et pour le message suivant sur la même connexion, une fois la réponse envoyée au client. Pour autoriser la réutilisation de la connexion au serveur par d'autres connexions client, vous devez utiliser l'API ctxt : reuse_server_connection () dans le contexte côté serveur.

Remarque : Cette API est disponible dans NetScaler 12.1 build 49.xx et versions ultérieures.

Modifier le trafic

Pour modifier les données de la demande ou de la réponse, vous devez utiliser la fonctionnalité de réécriture native qui utilise une expression PI de politique avancée. Étant donné que vous ne pouvez pas utiliser d'expressions PI dans les extensions, vous pouvez utiliser les API suivantes pour modifier les données d'un flux TCP.

```
1 data:replace(offset, length, new_string)
2 data:insert(offset, new_string)
```



```
data:delete(offset, length)
data:gsub(pattern, replace [,n]))
```

L'extrait de code suivant montre l'utilisation de l'API replace().

```
-- Get the offset of the pattern, we want to replace
   local old_pattern =  "pattern to repalace"
local old_pattern_length = old_pattern:len()
   local pat_off, pat_end = data:find(old_pattern)
   -- pattern is not present
if (not pat_off) then
    goto send_data
   end
  -- If the data we want to modify is not completely present, then
  -- wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
     goto done
  end
data:replace(pat_off, old_pattern_length,  "new pattern" )
::send_data::
ns.send(ctxt.output,  "EOM" , {
 data = data }
 )
::done::
```

L'extrait de code suivant montre l'utilisation de l'API insert().

```
data:insert(5,  "pattern to insert" )
```

L'extrait de code suivant montre l'utilisation de l'API insert (), lorsque nous voulons insérer après ou avant un motif :

```
-- Get the offset of the pattern, after or before which we want to
   insert
   local pattern =  "pattern after/before which we need to insert"
local pattern_length = pattern:len()
   local pat_off, pat_end = data:find(pattern)
-- pattern is not present
   if (not pat_off) then
    goto send_data
   end
  -- If the pattern after which we want to insert is not
  -- completely present, then wait for more data
```



```
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
     goto done
  end
-- Insert after the pattern
data:insert(pat_end + 1,  “pattern to insert” )
   -- Insert before the pattern
data:insert(pat_off,  “pattern to insert” )
::send_data::
    ns.send(ctxt.output,  “EOM” , {
 data = data }
 )
::done::
```

L’extrait de code suivant montre l’utilisation de l’API delete ().

```
-- Get the offset of the pattern, we want to delete
   local delete_pattern =  “pattern to delete”
local delete_pattern_length = delete_pattern:len()
   local pat_off, pat_end = data:find(old_pattern)
   -- pattern is not present
if (not pat_off) then
          goto send_data
   end
  -- If the data we want to delete is not completely present,
  -- then wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
    goto done
  end
data:delete(pat_off, delete_pattern_length)
::send_data::
ns.send(ctxt.output,  “EOM” , {
 data = data }
 )
::done::
```

L’extrait de code suivant montre l’utilisation de l’API gsub().

```
    -- Replace all the instances of the pattern with the new string
data:gsub( “old pattern” ,  “new string” )
-- Replace only 2 instances of  “old pattern”
data:gsub( “old pattern” ,  “new string” , 2)
```



```
-- Insert new_string before all instances of  “http”
data:gsub( “input data” ,  “(http)” ,  “new_string%1” )
-- Insert new_string after all instances of  “http”
data:gsub( “input data” ,  “(http)” ,  “%1new_string” )
-- Insert new_string before only 2 instances of  “http”
data:gsub( “input data” ,  “(http)” ,  “new_string%1” , 2)
```

Remarque : Cette API est disponible dans NetScaler 12.1 build 50.xx et versions ultérieures.

Générer du trafic vers le client ou le serveur

Vous pouvez utiliser l’API ns.send () pour envoyer des données provenant du code d’extension à un client et à un serveur principal. Pour envoyer ou recevoir une réponse directement avec un client, à partir du contexte du client, vous devez utiliser ctxt.client comme cible. Pour envoyer ou recevoir une réponse directement avec un serveur principal à partir du contexte du serveur, vous devez utiliser ctxt.server comme cible. Les données de la charge utile peuvent être des données de flux TCP ou une chaîne Lua.

Pour arrêter le traitement du trafic sur une connexion, vous pouvez utiliser l’API ctxt:close () depuis le contexte client ou serveur. Cette API ferme la connexion côté client ou toute connexion serveur qui y est liée.

Lorsque vous appelez l’API ctxt:close (), le code d’extension envoie le paquet TCP FIN aux connexions client et serveur et si des données supplémentaires sont reçues du client ou du serveur sur cette connexion, l’appliance réinitialise la connexion.

L’extrait de code suivant montre l’utilisation des API ctxt.client et ctxt:close().

```
    -- If the input packet is not MQTT CONNECT type, then
-- send some error response to the client.
function client.on_data(ctxt, payload)
    local data = payload.data
    local offset = 1
    local msg_type = 0
    local error_response =  “Missing MQTT Connect packet.”
    byte = data:byte(offset)
msg_type = bit32.rshift(byte, 4)
if (msg_type ~= 1) then
-- Send the error response
   ns.send(ctxt.client,  “DATA” , {
 data = error_response }
 )
-- Since error response has been sent, so now close the connection
    ctxt:close()
end
```


L'extrait de code suivant montre l'exemple lorsque l'utilisateur peut injecter les données dans le flux de trafic normal.

```
-- After sending request, send some log message to the server.
function client.on_data(ctxt, payload)
local data = payload.data
local log_message =  "client id :  "..data:sub(3, 7)..."  user name :  "
    data:sub(9, 15)
-- Send the request we get from the client to backend server
ns.send(ctxt.output,  "DATA" , {
 data = data }
 )
After sending the request, also send the log message
ns.send(ctxt.output,  "DATA" , {
 data = log_message"  }
 )
end
```

L'extrait de code suivant montre l'utilisation de l'API ctxt.to_server.

```
-- If the HTTP response status message is  "Not Found" ,
-- then send another request to the server.
function server.on_data(ctxt, payload)
    local data = payload.data
    local request  "GET /default.html HTTP/1.1\r\n\r\n" ss
    local start, end = data:find( "Not Found" )
    if (start) then
    -- Send the another request to server
        ns.send(ctxt.server,  "DATA" , {
 data = request }
 )
end
```

Remarque : Cette API est disponible dans NetScaler 12.1 build 50.xx et versions ultérieures.

Traitement des données sur l'établissement de connexion

Il se peut que vous souhaitiez envoyer certaines données à l'établissement de la connexion (lorsque l'ACK final est reçu). Par exemple, dans le protocole proxy, vous souhaiterez peut-être envoyer les adresses IP et les ports source et destination du client au serveur principal de l'établissement de connexion. Dans ce cas, vous pouvez utiliser le gestionnaire de rappel client.init () pour envoyer les données relatives à l'établissement de la connexion.

L'extrait de code suivant montre l'utilisation du callback client.init() :


```
-- Send a request to the next processing context
-- on the connection establishment.
function client.init(ctxt)
   local request  “PROXY TCP4”  + ctxt.client.ip.src.to_s +  “  “ +
      ctxt.client.ip.dst.to_s +  “  “ + ctxt.client.tcp.srcport +  “  “
       +     ctxt.client.tcp.dstport
-- Send the another request to server
   ns.send(ctxt.output,  “DATA” , {
 data = request }
 )
  end
```

Remarque : Cette API est disponible dans NetScaler 13.0 build xx.xx et versions ultérieures.

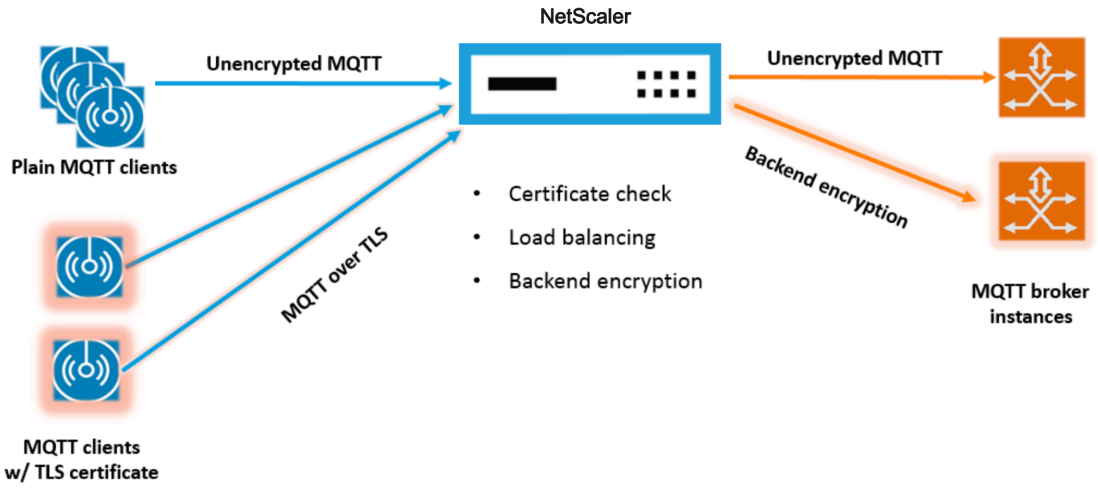
Tutoriel — Ajouter le protocole MQTT à l’appliance NetScaler à l’aide d’extensions de protocole

May 5, 2023

Les commandes de l’interface de ligne de commande (CLI) pour le protocole personnalisé utilisent le mot clé « user » pour indiquer la nature définie par l’utilisateur des entités de configuration sous-jacentes. À l’aide du code d’extension, vous pouvez ajouter un nouveau protocole utilisateur au système et ajouter des serveurs virtuels utilisateur pour les protocoles définis par l’utilisateur. Les serveurs virtuels utilisateur sont à leur tour configurables en définissant des paramètres. Les valeurs configurées pour les paramètres du serveur virtuel sont disponibles dans le code d’extension.

Le protocole MQTT est utilisé à des fins d’illustration.

Le schéma suivant illustre une appliance NetScaler et des outils client et courtier MQTT.



Liste de codes pour mqtt.lua

May 5, 2023

La liste de codes ci-dessous, mqtt.lua, fournit le code permettant d'implémenter le protocole MQTT sur NetScaler à l'aide d'extensions de protocole. Seule la fonction de rappel des données du client TCP est définie dans le code, à savoir client.on_data (). Pour les données du serveur, il n'ajoute pas de fonction de rappel et le chemin natif rapide entre le serveur et le client emprunte le chemin natif rapide. Pour les données client, le code analyse le message du protocole CONNECT MQTT et extrait le ClientID. Il utilise ensuite la valeur ClientID pour user_token, qui est utilisée pour équilibrer la charge de tout le trafic client pour la connexion en fonction du ClientID en définissant la méthode LB pour le serveur virtuel LB comme USER_TOKEN. Il utilise également le ClientID pour la valeur user_session, qui peut être utilisée pour la persistance LB en définissant le type de persistance pour le serveur LB vserver comme USERSESSION. Le code utilise le ns.send () pour effectuer LB et envoyer les données initiales. Il utilise l'API ns.pipe () pour envoyer le reste du trafic client directement à la connexion au serveur, en contournant les appels au gestionnaire de rappel d'extension.

```
--[[

  MQTT event handler for TCP client data

    ctxt - TCP client side App processing context.

    data - TCP Data stream received.

    - parse the client ID from the connect message - the first message
       should be connect
```



```
10
11      - send the data to LB with ClientID as user token and session
12
13      - pipe the subsequent data to LB directly. This way the subsequent
            MQTT traffic will
14
15        bypass the tcp client on_data handler
16
17      - if a parse error is seen, throw an error so the connection is
            reset
18
19  --]]
20
21  function client.on_data(ctxt, payload)
22
23      local data = payload.data
24
25      local data_len = data:len()
26
27      local offset = 1
28
29      local byte = nil
30
31      local utf8_str_len = 0
32
33      local msg_type = 0
34
35      local multiplier = 1
36
37      local max_multiplier = 128 * 128 * 128
38
39      local rem_length = 0
40
41      local clientID = nil
42
43      -- check if MQTT fixed header is present (fixed header length is
            atleast 2 bytes)
44
45      if (data_len < 2) then
46
47          goto need_more_data
48
49      end
50
51      byte = data:byte(offset)
```



```
52
53      offset = offset + 1
54
55         -- check for connect packet - type value 1
56
57      msg_type = bit32.rshift(byte, 4)
58
59      if (msg_type ~= 1) then
60
61          error("Missing MQTT Connect packet.")
62
63      end
64
65      -- parse the remaining length
66
67      repeat
68
69          if (multiplier > max_multiplier) then
70
71             error("MQTT CONNECT packet parse error - invalid Remaining
                  Length.")
72
73         end
74
75         if (data_len < offset) then
76
77            goto need_more_data
78
79         end
80
81         byte = data:byte(offset)
82
83         offset = offset + 1
84
85         rem_length = rem_length + (bit32.band(byte, 0x7F) * multiplier)
86
87         multiplier = multiplier * 128
88
89      until (bit32.band(byte, 0x80) == 0)
90
91      -- protocol name
92
93      -- check if protocol name length is present
94
95      if (data_len < offset + 1) then
```



```
96
97          goto need_more_data
98
99       end
100
101      -- protocol name length MSB
102
103      byte = data:byte(offset)
104
105      offset = offset + 1
106
107      utf8_str_len = byte * 256
108
109      -- length LSB
110
111      byte = data:byte(offset)
112
113      offset = offset + 1
114
115      utf8_str_len = utf8_str_len + byte
116
117         -- skip the variable header for connect message
118
119      -- the four required fields (protocol name, protocol level, connect
             flags, keep alive)
120
121      offset = offset + utf8_str_len + 4
122
123      -- parse the client ID
124
125      --
126
127      -- check if client ID len is present
128
129      if (data_len < offset + 1) then
130
131         goto need_more_data
132
133      end
134
135         -- client ID length MSB
136
137      byte = data:byte(offset)
138
139      offset = offset + 1
```



```
140
141     utf8_str_len = byte * 256
142
143     -- length LSB
144
145     byte = data:byte(offset)
146
147     offset = offset + 1
148
149     utf8_str_len = utf8_str_len + byte
150
151     if (data_len < (offset + utf8_str_len - 1)) then
152
153         goto need_more_data
154
155     end
156
157     clientID = data:sub(offset, offset + utf8_str_len - 1)
158
159     -- send the data so far to lb, user_token is set to do LB based on
           clientID
160
161     -- user_session is set to clientID as well (it will be used to
           persist session)
162
163     ns.send(ctxt.output, "DATA", {
164 data = data,
165
166                                 user_token = clientID,
167
168                                 user_session = clientID }
169 )
170
171        -- pipe the subsequent traffic to the lb - to bypass the
              extension handler
172
173     ns.pipe(ctxt.input, ctxt.output)
174
175     goto parse_done
176
177     ::need_more_data::
178
179     ctxt:hold(data)
180
181     ::parse_done::
```



```
182
183     return
184
185 end
186 <!--NeedCopy-->
```

Configurez MQTT à l'aide d'extensions de protocole

May 5, 2023

Les étapes suivantes ajoutent un protocole MQTT à l'appliance NetScaler.

Importez le fichier d'extension dans l'appliance NetScaler, à partir d'un serveur Web (via HTTP) ou de votre poste de travail local. Pour plus d'informations sur l'importation du fichier d'extension, voir Importer des extensions.

```
import ns extension local:mqtt_generic_fs.lua mqtt_code
```

Ajoutez un nouveau protocole TCP utilisateur au système à l'aide de l'extension.

```
add user protocol MQTT -transport TCP -extension mqtt_code
```

Ajoutez un service de type USER_TCP pour indiquer qu'il s'agit d'un protocole défini par l'utilisateur.

```
add service s1 10.102.90.112 USER_TCP 80
```

Ajoutez un serveur virtuel d'équilibrage de charge utilisateur et liez-y les services principaux.

```
add lb vs mysv USER_TCP
```

```
bind lb vs mysv s1
```

Ajoutez un serveur virtuel utilisateur pour le protocole nouvellement ajouté et faites du serveur virtuel d'équilibrage de charge configuré à l'étape précédente l'équilibreur de charge par défaut.

```
add user vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv
```

Le cas échéant, activez la persistance de session MQTT en fonction de l'ID client, définissez le type de persistance sur USERSESSION.

```
set lb vserver mqtt_lb -persistenceType USERSESSION
```

Configuration du déchargement SSL pour MQTT

May 5, 2023

Vous pouvez implémenter le déchargement SSL pour les protocoles utilisateur en ajoutant une instance SSL pour le protocole. L'exemple ci-dessous montre comment effectuer le déchargement SSL pour un protocole utilisateur. Le trafic vers les services principaux n'est pas chiffré avec cette configuration.

Remarque : Cet exemple ne fournit pas de détails relatifs à l'ajout ou à la mise à jour d'une paire de clés certificat-clé et à la lier à un serveur virtuel. Pour plus de détails, voir Certificats SSL.

Les commandes suivantes ajoutent le protocole MQTT_SSL en incluant mqtt.lua avec la valeur de transport « SSL ».

```
import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
add user protocol MQTT_SSL -transport SSL -extension mqtt_code
<!--NeedCopy-->
```

Les commandes suivantes ajoutent un serveur virtuel d'équilibrage de charge utilisateur et y lient les services principaux.

```
add service mqtt_svr1 10.217.24.48 USER_TCP 1501
add service mqtt_svr2 10.217.24.48 USER_TCP 1502
add lb vserver mqtt_lb USER_TCP  - lbMethod ROUNDROBIN
bind lb vserver mqtt_lb mqtt_svr1
bind lb vserver mqtt_lb mqtt_svr2
<!--NeedCopy-->
```

La commande suivante ajoute un serveur virtuel utilisateur pour le protocole MQTT_SSL récemment ajouté. L'utilisation de MQTT_SSL signifie que l'appliance NetScaler effectuera le déchargement SSL, car MQTT_SSL a été configuré avec le transport SSL. La commande définit également le paramètre defaultlb sur le serveur virtuel d'équilibrage de charge configuré à l'étape précédente.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Pour le déchargement SSL, vous devez également activer la fonctionnalité SSL et lier une clé de certification au serveur virtuel de l'utilisateur. Pour plus d'informations, consultez les rubriques suivantes :

Ajouter ou mettre à jour une paire de clés de certificat

Lier la paire de clés de certificat au serveur virtuel SSL

Exemple :

```
enable ns feature SSL

add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
```



```
<!--NeedCopy-->
```

Configuration du déchargement SSL avec un chiffrement de bout en bout pour MQTT

May 5, 2023

L'exemple suivant montre comment effectuer un déchargement SSL pour MQTT avec un chiffrement de bout en bout.

Remarque : Cet exemple ne fournit pas de détails relatifs à l'ajout ou à la mise à jour d'une paire de clés certificat-clé et à la lier à un serveur virtuel. Pour plus de détails, voir Certificats SSL.

Les commandes suivantes importent le fichier d'extension et ajoutent le protocole MQTT_SSL avec le transport SSL.

```
import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
add user protocol MQTT_SSL -transport SSL -extension mqtt_code
<!--NeedCopy-->
```

Les commandes suivantes ajoutent un serveur virtuel d'équilibrage de charge utilisateur et y lient les services principaux. Le serveur virtuel d'équilibrage de charge et les services sont configurés pour le type de service USER_SSL_TCP.

```
add service mqtt_svr1 10.217.24.48 USER_SSL_TCP 1501
add service mqtt_svr2 10.217.24.48 USER_SSL_TCP 1502
add lb vserver mqtt_lb USER_SSL_TCP  - lbmethod RR
bind lb vserver mqtt_lb mqtt_svr1
bind lb vserver mqtt_lb mqtt_svr2
<!--NeedCopy-->
```

La commande suivante ajoute un serveur virtuel utilisateur pour le protocole MQTT_SSL récemment ajouté. L'utilisation de MQTT_SSL signifie que l'appliance NetScaler effectuera le déchargement SSL, car MQTT_SSL a été configuré avec le transport SSL. La commande fait également du serveur virtuel d'équilibrage de charge, configuré à l'étape précédente, l'équilibreur de charge par défaut.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Pour le chiffrement de bout en bout, vous devez également activer la fonctionnalité SSL et lier une clé de certification à l'utilisateur et aux serveurs virtuels d'équilibrage de charge par défaut. Pour plus d'informations, consultez les rubriques suivantes :

Ajouter ou mettre à jour une paire de clés de certificat

Lier la paire de clés de certificat au serveur virtuel SSL

```
enable ns feature SSL

add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_lb  -certkeyName mqtt_svr_cert_key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
<!--NeedCopy-->
```

Tutoriel : équilibrage de charge des messages Syslog à l'aide d'extensions de protocole

May 5, 2023

Le protocole Syslog disponible sur l'appliance NetScaler fonctionne uniquement pour les messages générés sur l'appliance NetScaler. Il n'équilibre pas la charge des messages provenant de nœuds externes. Pour équilibrer la charge de ces messages, vous devez utiliser la fonctionnalité d'extensions de protocole et écrire la logique d'analyse des messages Syslog à l'aide du langage de programmation Lua 5.2.

Code pour analyser un message Syslog

Seule la fonction de rappel des données du client TCP est définie dans le code, à savoir client.on_data (). Pour les données du serveur, il n'ajoute pas de fonction de rappel et le chemin natif rapide entre le serveur et le client emprunte le chemin natif rapide. Le code identifie la limite du message en fonction du caractère final. Si le paquet TCP contient plusieurs messages Syslog, nous divisons le paquet en fonction du caractère final et nous équilibrons la charge de chaque message.

```
--[[

  Syslog event handler for TCP client data

    ctxt - TCP client side App processing context.

    data - TCP Data stream received.

--]]

function client.on_data(ctxt, payload)
```



```
12
13                  local message = nil
14
15                  local data_len
16
17                  local data = payload.data
18
19                  local trailing_character = "\n"
20
21                  ::split_message::
22
23                                      -- Get the offset of trailing
                                           character
24
25                                      local new_line_character_offset =
                                           data:find(trailing_character)
26
27                                      -- If trailing character is not
                                           found, then wait for more data.
28
29                                      if (not new_line_character_offset)
                                           then
30
31                                                          goto
                                                               need_more_data
32
33                                      end
34
35                                      -- Get the length of the current
                                           message
36
37                                      data_len = data:len()
38
39                                      -- Check whether we have more than
                                           one message
40
41                                      -- by comparing trailing character
                                           offset and
42
43                                      -- current data length
44
45                                      if (data_len >
                                           new_line_character_offset) then
46
47                                                          -- If we have
```



```
                                                                more than one
                                                                message, then
                                                                split
48
49                                                          -- the data into
                                                                two parts such
                                                                 that first
                                                                part
50
51                                                          -- will contain
                                                                message upto
                                                                trailing
                                                                character
52
53                                                          -- offset and
                                                                second part
                                                                will contain
54
55                                                          -- remaining
                                                                message.
56
57                                                          message, data =
                                                                data:split(
                                                                new_line_character_offse
                                                                )
58
59                                      else
60
61                                                          message = data
62
63                                                          data = nil
64
65                                      end
66
67  -- Send the data to the backend server.
68
69                                      ns.send(ctxt.output, "EOM", {
70   data = message }
71   )
72
73                                      goto done
74
75                                      ::need_more_data::
76
77                                                          -- Wait for more
```



```
                                                                    data
78
79                                                                  ctxt:hold(data)
80
81                                                                  data = nil
82
83                                                                  goto done
84
85                                                  ::done::
86
87                                                                  -- If we have
                                                                       more data to
                                                                       parse,
88
89                                                                  -- then do
                                                                       parsing again.
90
91                                                                  if (data) then
92
93                                                                                  goto
                                                                                       split_
94
95                                                                  end
96
97  end
98  <!--NeedCopy-->
```

Configuration du protocole Syslog à l'aide d'extensions de protocole

May 5, 2023

Les étapes suivantes ajoutent un protocole SYSLOG utilisateur à l'appliance NetScaler.

Importez le fichier d'extension dans l'appliance NetScaler, à partir d'un serveur Web (via HTTP) ou de votre poste de travail local. Pour plus d'informations sur l'importation du fichier d'extension, reportez-vous à la section Importation d'extensions.

```
import ns extension local:syslog_parser.lua syslog_parser_code
```

Ajoutez un nouveau protocole TCP utilisateur au système à l'aide de l'extension.

```
add user protocol USER_SYSLOG -transport TCP -extension syslog_parser_code
```


Ajoutez un service de type USER_TCP pour indiquer qu'il s'agit d'un protocole défini par l'utilisateur.

```
add service s1 10.102.90.112 USER_TCP 80
```

Ajoutez un serveur virtuel d'équilibrage de charge utilisateur et liez-y les services principaux.

```
1 add lb vs mysv USER_TCP
2
3 bind lb vs mysv s1
4 <!--NeedCopy-->
```

Ajoutez un serveur virtuel utilisateur pour le protocole nouvellement ajouté et faites du serveur virtuel d'équilibrage de charge configuré à l'étape précédente l'équilibreur de charge par défaut.

```
add user vs v_syslog USER_SYSLOG 10.217.24.28 80 -defaultlb mysv
```

Référence de la commande Protocol extensions

May 8, 2023

Le tableau suivant répertorie toutes les nouvelles commandes ajoutées pour les protocoles personnalisés, ainsi que les commandes existantes qui ont été modifiées pour les protocoles personnalisés.

```
show lb persistentSessions [<vserv-name>]
```

- **Commande CLI :**

  ```
  add user protocol <name> -transport ( TCP | SSL )-extension <string> -comment <string>]>
  ```

- **Description :**

  Ajoute un nouveau protocole utilisateur à l'appliance NetScaler à l'aide d'extensions. Actuellement, seuls les protocoles utilisateur avec une valeur de transport TCP ou SSL sont pris en charge.

  > **Exemple :**
  >
  > ajout du protocole utilisateur MQTT -transport TCP -extension mqtt_code

- **Commande CLI :**

  ```
  rm user protocol <name>
  ```

- **Description :**

  Supprime un protocole utilisateur précédemment ajouté à l'appliance NetScaler.

> **Exemple :**
>
> protocole utilisateur rm mqtt

- **Commande CLI :**

```
set user protocol <name> -comment <string>
```

- **Description :**

  Modifie les paramètres d'un protocole utilisateur précédemment ajouté à l'appliance NetScaler.

> **Exemple :**
>
> définir le protocole utilisateur mqtt -comment « Implémentation du protocole MQTT »

- **Commande CLI :**

```
unset user protocol <name> -comment
```

- **Description :**

  Supprime les paramètres d'un protocole utilisateur précédemment ajouté à l'appliance NetScaler.

> **Exemple :**
>
> protocole utilisateur non défini mqtt -comment « Implémentation du protocole MQTT »

- **Commande CLI :**

```
update ns extension <extension name>
```

- **Description :**

  Met à jour l'implémentation d'un protocole utilisateur précédemment ajouté à l'aide d'extensions.

  Vous pouvez mettre à jour l'implémentation du protocole uniquement si le protocole n'est utilisé par aucun serveur virtuel utilisateur.

> **Exemple :**
>
> mise à jour de l'extension ns my-extension

- **Commande CLI :**

```
add lb vserver <name> [USER_TCP | USER_SSL_TCP] [-lbmethod USER_TOKEN]
[-persistencetype USERSESSION] [-timeout <value>]
```

- **Description :**

  Ajoute un serveur virtuel d'équilibrage de charge à l'appliance NetScaler. Il s'agit d'une commande CLI existante.

Pour les serveurs virtuels utilisateur d'équilibrage de charge, le type de service à utiliser est USER_TCP ou USER_SSL_TCP. L'adresse IP et le port ne sont pas autorisés sur les serveurs virtuels d'équilibrage de charge utilisateur.

Pour les serveurs virtuels d'équilibrage de charge utilisateur, seule la méthode d'équilibrage de charge ROUNDROBIN est autorisée et la valeur du jeton est fournie par le code d'extension. De même, seule la persistance USERSESSION est autorisée et le paramètre de persistance est fourni par le code de l'extension.

> **Exemple :**
>
> ajouter lb vserver mysv USER_TCP —lbmethod ROUNDROBIN

- **Commande CLI :**

```
add user vserver <name> <userProtocol> <IPAddress> <port> -defaultLB <
string> [-params <string>] [-comment <string>]
```

- **Description :**

Ajoute un serveur virtuel pour un protocole utilisateur à l'aide d'extensions. Le serveur virtuel d'équilibrage de charge utilisateur par défaut configuré est disponible pour le gestionnaire d'extension de données du client TCP sous la forme ctxt.output. Pour un serveur virtuel, les paramètres d'extension peuvent être définis à l'aide de l'option -params avec un nom et une paire de valeurs. La valeur de paramètre correspondante est disponible pour les gestionnaires d'extensions sous la forme ctxt.vserver.params. \ <paramName>.

> **Exemple :**
>
> ajout d'un utilisateur vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv

- **Commande CLI :**

```
rm user vserver <name>
```

- **Description :**

Supprime un serveur virtuel utilisateur précédemment ajouté à l'appliance NetScaler.

> **Exemple :**
>
> rm user vserver v_mqtt

- **Commande CLI :**

```
set user vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-defaultLB
<string>] [-params <string>] [-comment <string>]
```

- **Description :**

Modifie les paramètres d'un serveur virtuel utilisateur précédemment ajouté à l'appliance NetScaler. Lorsqu'une nouvelle valeur est attribuée à un paramètre d'extension par l'option -params, l'ancienne valeur est remplacée.

> **Exemple :**
>
> set user vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment « Implémentation du protocole MQTT »

- **Commande CLI :**

```
unset user vserver <name> [-params] [-comment]
```

- **Description :**

Supprime les paramètres d'un serveur virtuel utilisateur précédemment ajouté à l'appliance NetScaler. Si vous utilisez l'option —params pour annuler la définition d'un paramètre d'extension, la valeur de paramètre correspondante disponible pour les gestionnaires d'extensions est remplacée par nil.

> **Exemple :**
>
> utilisateur non défini vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment « Implémentation du protocole MQTT »

- **Commande CLI :**

```
show user protocol [<name>]
```

- **Description :**

Affiche des informations sur un protocole utilisateur, telles que l'extension et les rappels.

> **Exemple :**
>
> afficher le protocole utilisateur mqtt

- **Commande CLI :**

```
show user vserver [<name>]
```

- **Description :**

Affiche des informations sur un serveur virtuel utilisateur.

> **Exemple :**
>
> afficher l'utilisateur vserver vs_mqtt

- **Commande CLI :**

```
stat user vserver [<name>]
```


- **Description :**

  Affiche les statistiques relatives à un serveur virtuel utilisateur.

  > **Exemple :**
  >
  > utilisateur stat vserver vs_mqtt

- **Commande CLI :**

```
show lb persistentSessions [<vserv-name>]
```

- **Description :**

  Affiche des informations sur les sessions persistantes. Il s'agit d'une CLI existante. Pour les protocoles utilisateur, le type de persistance est affiché sous la forme USERSESSION.

- **Commande CLI :**

```
rm lb vserver <name>
```

- **Description :**

  Supprime un serveur LB vserver utilisateur précédemment ajouté à l'appliance NetScaler.

  > **Exemple :**
  >
  > rm lb vserver mysv

- **Commande CLI :**

```
add service <name> <IPAddr> (USER_TCP | USER_SSL_TCP)<Port>
```

- **Description :**

  Ajoute un service principal à utiliser pour un protocole utilisateur. Il s'agit d'une commande CLI existante avec les nouveaux types de service USER_TCP et USER_SSL_TCP.

  > **Exemple :**
  >
  > add service mqtt_svr1 10.217.24.48 USER_TCP 1501
  >
  > **Remarque** : Les commandes « set service and unset service » existantes peuvent être utilisées pour supprimer ou modifier les paramètres d'un service précédemment ajouté pour un protocole utilisateur.

- **Commande CLI :**

```
bind lb vserver <name> <serviceName>
```

- **Description :**

  Lie un service à un serveur LB vserver utilisateur. Le type de service doit être USER_TCP/USER_SSL_TCP pour la liaison à un vserver LB avec le type USER_TCP/USER_SSL_TCP.

> **Exemple :**
>
> bind lb vserver mysv mqtt_svr1

- **Commande CLI :**

  ```
  unbind lb vserver <name> <serviceName>
  ```

- **Description :**

  Supporte un service précédemment lié à un serveur LB vserver utilisateur.

  > **Exemple : dissocier**
  >
  > lb vserver mysv mqtt_svr1

- **Commande CLI :**

  ```
  rm service <name>
  ```

- **Description :**

  Supprime un service précédemment ajouté pour un protocole utilisateur.

  > **Exemple :**
  >
  > rm service mqtt_svr1

Résolution des problèmes liés aux extensions de

May 5, 2023

Si votre fonction d'extension ne se comporte pas comme prévu, vous pouvez utiliser la fonctionnalité de suivi des extensions pour vérifier le comportement de votre fonction d'extension. Vous pouvez également ajouter la journalisation à votre fonction d'extension à l'aide de la fonctionnalité de journalisation personnalisée, qui vous permet de définir le niveau de journalisation à capturer sur l'appliance NetScaler.

Journalisation personnalisée

Vous pouvez également ajouter votre propre journalisation à votre fonction d'extension. Pour ce faire, utilisez la fonction intégrée ns.logger:level (), où le niveau est urgent, alerte, critique, erreur, avertissement, notification, information ou débogage. Les paramètres sont les mêmes que ceux de la fonction C printf () : une chaîne de format et un nombre variable d'arguments pour fournir des valeurs pour le % spécifié dans la chaîne de format. Par exemple, vous pouvez ajouter ce qui suit à la fonction COMBINE_HEADERS pour enregistrer le résultat d'un appel :


```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"

ns.logger:info("Result: %s", result_str)

return result_str
<!--NeedCopy-->
```

La fonction ci-dessus enregistrerait le message suivant to/var/log/ns.log pour l'exemple d'entrée indiqué dans les exemples de messages de journal abrégés de la section Suivi des extensions ci-dessus.

```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: \*/\*^M H2: h2val1, h2val2,
h2val3^M ^M"
```

Extensions de stratégie

May 5, 2023

La fonctionnalité d'extension de stratégie vous permet d'écrire des fonctions d'extension pour des types de politiques intégrés. Les extensions peuvent être utilisées dans des expressions de politique, tout comme les fonctions intégrées. Elles sont exécutées lorsque les expressions de politique correspondantes sont évaluées. Cette fonctionnalité est utile pour :

- Ajouter des fonctions personnalisées aux politiques existantes.
- Mettre en œuvre des constructions logiques pour répondre aux exigences complexes des clients.

La fonctionnalité d'extension des politiques permet de remédier à ces limitations en permettant aux utilisateurs d'écrire des fonctions d'extension pour les types de politiques intégrés. Les extensions peuvent ensuite être utilisées dans les expressions de politique, tout comme les fonctions intégrées. Elles sont exécutées lorsque les expressions de politique correspondantes sont évaluées.

Le tableau suivant répertorie les types de politiques qui peuvent être utilisés lors de l'écriture d'une extension, ainsi que leurs mappages associés.

Type de stratégie	Type de politique mappé	Résultat
TEXT_T	NSTEXT	Chaîne
BOOL_AT	NSBOOL	Booléen

Type de stratégie	Type de politique mappé	Résultat
NUM_AT	NSNUM	Nombre (virgule flottante à double précision)
DOUBLE_AT	NSDOUBLE	Nombre (virgule flottante à double précision)

Conditions préalables à l'utilisation des extensions de politique

Les fonctions importées doivent être conformes aux normes de politique existantes. Par conséquent :

- Le nom de la fonction doit commencer par une lettre et peut contenir des chiffres ou des traits de soulignement.
- Le nom de la fonction ne fait pas la distinction entre majuscules et minuscules selon les politiques de NetScaler.
- La fonction doit renvoyer une seule valeur même si le langage d'extension renvoie plusieurs valeurs.
- Les fonctions comportant un nombre variable d'arguments ne sont pas prises en charge.

Comment fonctionnent les extensions de politique ?

Les politiques existantes sur une appliance NetScaler utilisent un interpréteur pour évaluer les fonctions, qui sont importées dans un fichier d'extension de politique. Lorsqu'un utilisateur importe une nouvelle fonction dans un fichier d'extension de politique :

1. La syntaxe et d'autres conditions du fichier d'extension sont validées.
2. Si la validation échoue, l'erreur est signalée à l'utilisateur.
3. Si la validation aboutit, le fichier d'extension est importé dans l'appliance NetScaler et son contenu peut être utilisé dans des expressions de politique, comme n'importe quelle fonction de stratégie intégrée
    a) Si l'évaluation de l'expression de politique renvoie une erreur pendant l'exécution, elle est signalée sous la forme d'un événement undef et le compteur d'erreurs associé est incrémenté.

    Remarque : Si un événement de sous-définition de stratégie se produit et que la règle de stratégie contient une ou plusieurs fonctions d'extension de stratégie, la `show ns extension <name>` commande affiche les résultats undef lorsqu'elle est appliquée à ces extensions de stratégie. Si la fonction d'extension est abandonnée, la valeur du compteur d'abandon est incrémentée.
    b) Si l'évaluation de l'expression de politique aboutit, l'évaluation de l'expression reprend jusqu'à ce que l'expression soit entièrement évaluée ou jusqu'à ce qu'elle soit abandonnée

en raison d'une erreur.

Si l'exécution de la fonction d'extension prend trop de temps, elle est abandonnée et le compteur d'erreurs relatif à cette fonction d'extension est incrémenté. La fonction d'extension est sandboxée, ce qui empêche :

- Utilisation excessive du processeur sur l'appliance NetScaler.
- Utilisation excessive de la mémoire sur l'appliance NetScaler.
- Utilisation de bibliothèques intégrées nuisibles ou de bibliothèques ou de fichiers binaires tiers.
- Scripts de longue durée susceptibles de provoquer le redémarrage de l'appliance NetScaler.

Configuration des extensions de politique

May 5, 2023

Lorsque votre fichier d'extension de politique est prêt, importez-le dans l'appliance NetScaler. Le processus d'importation copie le fichier d'extension dans un répertoire de l'appliance NetScaler et vérifie l'absence d'erreurs de syntaxe.

Après l'importation, vous devez rendre le fichier d'extension disponible pour une utilisation dans les expressions de stratégie.

Remarque : La commande d'importation est utilisée pour télécharger le contenu du fichier depuis une source \<src\>externe ou interne vers le système de fichiers NetScaler. Pour charger ce contenu de fichier dans un ou plusieurs moteurs de paquets pour la première fois, utilisez la commande add. En cas de mise à jour du contenu du fichier, le contenu mis à jour peut être téléchargé sur le système de fichiers NetScaler en exécutant la commande d'importation avec l'argument overwrite. La commande met à jour le contenu du système de fichiers. Pour charger le contenu mis à jour sur un ou plusieurs moteurs de paquets, utilisez la commande update.

Configurer les extensions de stratégie à l'aide de la CLI

1. Importez le fichier d'extension de politique dans l'appliance NetScaler, à partir d'un serveur Web (via HTTP) ou de votre poste de travail local.

   a) Importation HTTP

   Si un serveur Web est disponible, vous pouvez stocker le fichier d'extension dans le répertoire du serveur Web et l'importer dans l'appliance NetScaler.

```
1 import ns extension <src> <name> [-comment<string>] [-
     overwrite]
2 <!--NeedCopy-->
```


Exemple :

```
import ns extension http://myhost/path/to/extension
   myextension -comment  “Custom crc calculation
<!--NeedCopy-->
```

b) Importation locale

Vous pouvez utiliser le client SSH pour copier le fichier d’extension depuis votre poste de travail vers le répertoire /var/tmp de l’appliance NetScaler

```
scp extension-file-name <ns-userid@ns-ip-addr>:/var/tmp
<!--NeedCopy-->
```

où

- `extension-file-name` est le nom du fichier d’extension sur votre machine cliente.
- `ns-userid` est l’utilisateur de l’appliance NetScaler autorisé à écrire dans /var/tmp.
- `ns-ip-addr` est l’adresse IP de NetScaler.

Après avoir copié le fichier sur l’appliance NetScaler, exécutez la commande d’importation sur l’appliance NetScaler.

```
import ns extension local:<extension-file-name extension-name>
<!--NeedCopy-->
```

Remarque : L’interface de ligne de commande doit être utilisée pour importer un fichier d’extension local, en exécutant la commande
import .

2. Ajoutez l’extension de stratégie au moteur de paquets pour évaluation.

```
add ns extension <name> [-comment <string>]
<!--NeedCopy-->
```

Exemple :

```
add ns extension myextension
<!--NeedCopy-->
```

Après l’importation d’un fichier d’extension, vous pouvez le mettre à jour, si vous avez inclus le paramètre -overwrite dans la commande d’importation, ou le supprimer. Vous pouvez également afficher les détails d’un fichier d’extension importé.

Mettre à jour un fichier d’extension sur l’appliance NetScaler à partir de la source

À l’invite de commande, tapez :


```
update ns extension <name>
<!--NeedCopy-->
```

Remarque : Vous pouvez mettre à jour le fichier d'extension uniquement après avoir importé le fichier d'extension spécifié dans l'appliance NetScaler à l'aide du paramètre -overwrite.

Exemple :

```
update ns extension myextension
<!--NeedCopy-->
```

Supprimer un fichier d'extension de l'appliance NetScaler

À l'invite de commandes, tapez :

```
rm ns extension <name>
<!--NeedCopy-->
```

Exemple :

```
rm ns extension myextension
<!--NeedCopy-->
```

Afficher les détails de la fonction d'extension spécifiée sur l'appliance NetScaler

À l'invite de commande, tapez :

```
show ns extension <name>
<!--NeedCopy-->
```

Exemple :

```
show ns extension myextension
<!--NeedCopy-->
```

Configurer les extensions de politique à l'aide de l'interface graphique

1. Importez le fichier d'extension de politique dans l'appliance NetScaler, à partir d'un serveur Web (via HTTP) ou de votre poste de travail local.
    a) Accédez à **AppExpert** > **Extensions** de **stratégie, cliquez sur Extensionde stratégie, dans la liste déroulante Importer** de, sélectionnez l'URL correspondant à l'emplacement du fichier d'extension à importer.

b) Accédez à **AppExpert** > **Extensions de stratégie**, **Extension de stratégie** et importez le fichier d'extension en sélectionnant Fichier dans la liste déroulante **Importer** depuis.

2. Ajoutez l'extension de stratégie au moteur de paquets pour évaluation.

   Accédez à **AppExpert** > **Extensions de stratégie** et, dans l'onglet**Extensions de stratégie**, ajoutez le fichier d'extension.

Mettre à jour un fichier d'extension sur l'appliance NetScaler à partir de la source

Accédez à **AppExpert** > **Extensions de stratégie** et, dans l'onglet **Extensions de stratégie**, mettez à jour le fichier d'extension.

Supprimer un fichier d'extension de l'appliance NetScaler

Accédez à **AppExpert** > **Extensions de stratégie** et, onglet **Extensions de stratégie**, supprimez le fichier d'extension.

Afficher les détails de la fonction d'extension spécifiée sur l'appliance NetScaler

Accédez à **AppExpert** > **Extensions de stratégie** et, sous l'onglet **Fonctions des extensions de stratégie**, cliquez sur la flèche de liste déroulante de la fonction d'extension dont vous souhaitez voir les détails.

Extensions de stratégie - cas d'utilisation

May 5, 2023

Certaines applications client présentent des exigences qui ne peuvent pas être satisfaites par les politiques et expressions existantes. La fonctionnalité d'extension des politiques permet aux clients d'ajouter des fonctions personnalisées à leurs applications pour répondre à leurs besoins.

Les cas d'utilisation suivants illustrent l'ajout de nouvelles fonctions à l'aide de la fonctionnalité d'extension de politique de l'appliance NetScaler.

- Cas 1 : hachage personnalisé
- Cas 2 : réduire les barres obliques doubles dans les URL
- Cas 3 : Combiner les en-têtes

Cas 1 : hachage personnalisé

La fonction CUSTOM_HASH fournit un mécanisme permettant d'insérer n'importe quel type de valeur de hachage dans les réponses envoyées au client. Dans ce cas d'utilisation, la fonction de hachage est utilisée pour calculer le hachage de la chaîne de requête pour une demande HTTP de réécriture et pour insérer un en-tête HTTP nommé CUSTOM_HASH avec la valeur calculée. La fonction CUSTOM_HASH implémente l'algorithme de hachage DJB2.

Exemple d'utilisation de CUSTOM_HASH :

```
> add rewrite action test_custom_hash insert_http_header "CUSTOM_HASH"
   "HTTP.REQ.URL.QUERY.CUSTOM_HASH"
<!--NeedCopy-->
```

Exemple de définition de CUSTOM_HASH () :

```
    -- Extension function to compute custom hash on the text

    -- Uses the djb2 string hash algorithm
    function NSTEXT:CUSTOM_HASH() : NSTEXT

        local hash = 5381

        local len = string.len(self)

        for i = 1, len do

             hash = bit32.bxor((hash * 33), string.byte(self, i))

        end

        return tostring(hash)

    end
<!--NeedCopy-->
```

Description ligne par ligne de l'exemple ci-dessus :

```
function NSTEXT:CUSTOM_HASH() : NSTEXT

Defines the CUSTOM_HASH() function, with text input and a text return
   value.

local hash = 5381
local len = string.len(self)

```



```
Declares two local variables:

 - hash. Accumulates the compute hash value and is seeded with the
    number 5381

 - len. Sets to the length of the self input text string, using the
    built-in string.len() function.

for i = 1, len do
      hash = bit32.bxor((hash * 33), string.byte(self, i))
end

Iterates through each byte of the input string and adds the byte to the
    hash. It uses the built-in string.byte() function to get the byte
   and the built-in bit32.bxor() function to compute the XOR of the
   existing hash value (multiplied by 33) and the byte.

return tostring(hash)

Calls the built-in tostring() function to convert the numeric hash
   value to a string and returns the string as the value of the
   function.
<!--NeedCopy-->
```

Cas 2 : réduire les barres obliques doubles dans les URL

La réduction des barres obliques doubles dans les URL améliore le temps d'affichage du site Web, car les navigateurs analysent les URL à barre oblique unique de manière plus efficace. Les URL à barre oblique unique permettent également de maintenir la compatibilité avec les applications qui n'acceptent pas les barres obliques doubles. La fonctionnalité d'extension de la politique permet aux clients d'ajouter une fonction qui remplace les barres obliques doubles par des barres obliques simples dans les URL. L'exemple suivant illustre l'ajout d'une fonction d'extension de politique qui réduit les barres obliques doubles dans les URL.

Exemple de définition de COLLAPSE_DOUBLE_SLASHES () :

```
    -- Collapse double slashes in URL to a single slash and return the
       result
    function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT

        local result = string.gsub(self, "//", "/")

        return result

```



```
    end
<!--NeedCopy-->
```

Description ligne par ligne de l'exemple ci-dessus :

```
function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT

Declares the COLLAPSE_DOUBLE_SLASHES() function with text input and
   return.

local result = string.gsub(self, "//", "/")

Declares a local variable named result and uses the built-in string.
   gsub() function to replace all double slashes with single slashes in
    the self input text.

The second parameter of string.gsub() is actually a regular expression
   pattern, although here a simple string is used for the pattern.

return result

Returns the resulting string.
<!--NeedCopy-->
```

Cas 3 : Combiner les en-têtes

Certaines applications client ne peuvent pas gérer plusieurs en-têtes dans une demande. De plus, l'analyse d'en-têtes dupliqués avec les mêmes valeurs d'en-tête, ou de plusieurs en-têtes portant le même nom mais des valeurs différentes dans une requête, consomme du temps et des ressources réseau. La fonctionnalité d'extension des politiques permet aux clients d'ajouter une fonction permettant de combiner ces en-têtes en en-têtes uniques avec une valeur combinant les valeurs d'origine. Par exemple, en combinant les valeurs des en-têtes H1 et H2.

Demande initiale :

```
GET /combine_headers HTTP/1.1
User-Agent: amigo unit test
Host: myhost
H2: h2val1
H1: abcd
Accept: \*/\*
H2: h2val2
Content-Length: 0
H2: h2val3
```



```
10 H1: 1234
11 <!--NeedCopy-->
```

Demande modifiée :

```
1 GET /combine_headers HTTP/1.1
2 User-Agent: amigo unit test
3 Host: myhost
4 H2: h2val1, h2val2, h2val3
5 H1: abcd, 1234
6 Accept: \*/\*
7 Content-Length: 0
8 <!--NeedCopy-->
```

En général, ce type de modification de demande est effectué à l'aide de la fonctionnalité de réécriture, qui utilise des expressions de politique pour délimiter la partie de la demande à modifier (la cible) et la modification à effectuer (l'expression du générateur de chaînes). Toutefois, les expressions de politique n'ont pas la capacité d'itérer sur un nombre arbitraire d'en-têtes.

La solution à ce problème nécessite une extension de la fonctionnalité de politique. Pour ce faire, nous allons définir une fonction d'extension, appelée COMBINE_HEADERS. Avec cette fonction, nous pouvons configurer l'action de réécriture suivante :

```
> add rewrite action combine_headers_act replace 'HTTP.REQ.FULL_HEADER
.AFTER_STR("HTTP/1.1rn")''HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1rn").
COMBINE_HEADERS'
```

Ici, la cible de réécriture est HTTP.REQ.FULL_HEADER.AFTER_STR (« HTTP/1.1Rn »). Le AFTER_STR (« HTTP/1.1rn ») est obligatoire car FULL_HEADER inclut la première ligne de la requête HTTP (par exemple GET /combine_headers HTTP/1.1).

L'expression du générateur de chaînes est HTTP.REQ.FULL_HEADER.AFTER_STR (« http/1.1rn ») .COMBINE_HEADERS, où les en-têtes (moins la première ligne) sont introduits dans la fonction d'extension COMBINE_HEADERS, qui combine et renvoie les valeurs des en-têtes.

Exemple de définition de COMBINE_HEADERS () :

```
1     -- Extension function to combine multiple headers of the same name
         into one header.
2
3
4
5     function NSTEXT:COMBINE_HEADERS(): NSTEXT
6
7         local headers = {
8   }
```



```
 -- headers

      local combined_headers = {
}
-- headers with final combined values
      -- Iterate over each header (format "name:valuer\r\n")

      -- and build a list of values for each unique header name.

      for name, value in string.gmatch(self, "([^:]+):([^\r\n]*)\r\n"
         ) do

          if headers[name] then

              local next_value_index = #(headers[name]) + 1

              headers[name][next_value_index] = value

          else

              headers[name] = {
name .. ":" .. value }


          end

      end



      -- iterate over the headers and concat the values with
         separator ","

      for name, values in pairs(headers) do

          local next_header_index = #combined_headers + 1

          combined_headers[next_header_index] = table.concat(values,
             ",")

      end



      -- Construct the result headers using table.concat()
```



```
51
52          local result_str = table.concat(combined_headers, "\r\n") .. "\
                r\n\r\n"
53
54          return result_str
55
56      end
57  <!--NeedCopy-->
```

Description ligne par ligne de l'exemple ci-dessus :

```
1  function NSTEXT:COMBINE_HEADERS(): NSTEXT
2
3  Defines the COMBINE_HEADERS extension function, with the text input
       into the function from the policy expression and a text return type
       to the policy expression.
4
5  local headers = {
6    }
7    -- headers
8  local combined_headers = {
9    }
10   -- headers with final combined values
11
12 Declares local variables headers and combined_headers and initialize
       these variables to empty tables. headers will be a table of arrays
       of strings, where each array holds one or more values for a header.
       combined_headers will be an array of strings, where each array
       element is a header with its combined values.
13
14 for name, value in string.gmatch(self, "([^:]+):([^\r\n]*)\r\n") do
15 . . .
16 end
17 <!--NeedCopy-->
```

Ce générique for loop analyse chaque en-tête de l'entrée. L'itérateur est la fonction intégrée string.gmatch (). Cette fonction prend deux paramètres : une chaîne à rechercher et un modèle à utiliser pour faire correspondre des parties de la chaîne. La chaîne à rechercher est fournie par le paramètre implicite self, qui est le texte des en-têtes saisis dans la fonction.

Le modèle est exprimé à l'aide d'une expression régulière (regex en abrégé). Cette expression régulière correspond au nom et à la valeur de chaque en-tête, que la norme HTTP définit comme ***nom* :*value* \ r \ n.** *Les parenthèses de la regex indiquent les parties correspondantes à extraire. Le schéma de la regex est donc* ***(*match-name) :(match-value*) \ r \ n.*** Le modèle de ***nom de correspondance*** doit

correspondre à tous les caractères sauf les deux-points. C'est écrit `[^:]+`. `[^:]` est n'importe quel caractère à l'exception de `:` et `+` représente une ou plusieurs répétitions. De même, le modèle de *valeur de correspondance* doit correspondre à tous les caractères sauf le `\r\n`, il est donc écrit. `[^\r\n]*[^\r\n]` correspond à n'importe quel caractère sauf `\r\n` et et `*` correspond à zéro ou plusieurs répétitions. Cela rend la regex `([^:]+):([^\r\n]*)\r\n`complète.

L'instruction for utilise une attribution multiple pour définir le nom et la valeur des deux correspondances renvoyées par l'itérateur string.gmatch (). Elles sont implicitement déclarées en tant que variables locales dans le corps de la boucle for.

```
if headers[name] then
     local next_value_index = #(headers[name]) + 1
     headers[name][next_value_index] = value
else
     headers[name] = {
 name .. ":" .. value }

end
<!--NeedCopy-->
```

Ces instructions dans la boucle for placent les noms et les valeurs d'en-tête dans la table des en-têtes. La première fois qu'un nom d'en-tête est analysé (disons H2 : h2val1 dans l'exemple d'entrée), il n'y a aucune entrée d'en-tête pour le nom et les en-têtes [nom] sont nuls.

Puisque nil est traité comme false, la clause else est exécutée. Cela définit l'entrée des en-têtes pour name à un tableau avec une valeur de chaîne *name* :*value.*

Remarque : Le constructeur du tableau dans la boucle else est équivalent à {[1] = name.. « : ».. value}, qui définit le premier élément du tableau.) Pour le premier en-tête H2, il définit les en-têtes [“H2”] = {“ H2:H2val1”}.

Sur les instances suivantes d'un en-tête (disons, H2 : h2val2 dans l'exemple d'entrée). headers [name] n'est pas nul, donc la clause then est exécutée. Cela détermine le prochain index disponible dans la valeur du tableau pour les en-têtes [nom] et place la valeur de l'en-tête dans cet index. Pour le deuxième en-tête H2, il définit les en-têtes [“H2”] = {“ H2:H2val1”, « h2val2”}.

```
for name, values in pairs(headers) do
    local next_header_index = #combined_headers + 1
    combined_headers[next_header_index] = table.concat(values, ",")
end
<!--NeedCopy-->
```

Une fois que les en-têtes d'origine ont été analysés et que la table des en-têtes a été remplie, cette boucle crée le tableau combined_headers. Elle utilise la fonction pairs () comme itérateur de boucle for.

Chaque appel à pairs () renvoie le nom et la valeur de l'entrée suivante dans la table des en-têtes.

La ligne suivante détermine le prochain index disponible dans le tableau combined_headers, et la ligne suivante définit cet élément du tableau comme l'en-tête combiné. Elle utilise la fonction intégrée table.concat (), qui prend comme arguments un tableau de chaînes et une chaîne à utiliser comme séparateur, et renvoie une chaîne qui est la concaténation des chaînes du tableau, séparées par le séparateur.

Par exemple, pour les valeurs = {"H2:H2val1", « h2val2"}, cela produit « H2:H2val1, h2val2 »

```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"
<!--NeedCopy-->
```

Une fois le tableau combined_headers créé, il concatène les éléments en une seule chaîne et ajoute un double \ r \ n qui met fin aux en-têtes HTTP.

```
return result_str
<!--NeedCopy-->
```

Renvoie une chaîne comme résultat de la fonction d'extension COMBINE_HEADERS.

Résolution des problèmes liés aux extensions de stratégie

May 5, 2023

Si votre fonction d'extension ne se comporte pas comme prévu, vous pouvez utiliser la fonctionnalité de suivi des extensions pour vérifier le comportement de votre fonction d'extension. Vous pouvez également ajouter la journalisation à votre fonction d'extension à l'aide de la fonctionnalité de journalisation personnalisée, qui vous permet de définir le niveau de journalisation à capturer sur l'appliance NetScaler.

Cette rubrique fournit des informations sur :

- Traçage des extensions
- Journalisation personnalisée

Traçage des extensions

Pour montrer ce que fait votre fonction d'extension, la fonctionnalité de suivi des extensions enregistre l'exécution de la fonction dans le journal système NetScaler (/var/log/ns.log). La journalisation des traces utilise le niveau de journal DEBUG, qui n'est normalement pas activé. Par conséquent, vous devez activer TOUS les niveaux de journalisation. Vous pouvez ensuite activer le suivi en définissant l'option -trace de la commande d'extension set ns. Les paramètres disponibles sont les suivants :

- désactiver désactiver le traçage (équivalent à unset ns extension -trace).
- les appels tracent les appels de fonction avec des arguments et la fonction renvoie la première valeur de retour.
- les lignes tracent les numéros de ligne ci-dessus et les numéros de ligne des lignes exécutées.
- tous tracent ce qui précède ainsi que les variables locales modifiées par les lignes exécutées.

Exemple :

```
set audit syslogParams -loglevel ALL

set ns extension combine_headers -trace all
<!--NeedCopy-->
```

Chaque message de suivi a le format

```
log-header : default NSEXTENSION Message message-number 0 : "TRACE function
-name CALL call-number: event"
```

Où,

- log-header fournit les horodatages, l'adresse IP NetScaler et l'ID du moteur de paquets.
- le numéro de message est un numéro séquentiel identifiant le message du journal.
- function-name est le nom de la fonction d'extension.
- call-number est un numéro séquentiel pour chaque appel de fonction d'extension. Il peut être utilisé pour regrouper tous les messages de suivi pour un appel de fonction d'extension.
- l'événement est l'un des suivants :
  - CALL nom-fonction ; les valeurs des paramètres indiquent que la fonction a été appelée avec les paramètres spécifiés.
  - RETURN FROM nom-fonction ; return = value indique qu'une fonction a renvoyé la (première) valeur spécifiée. (Aucune valeur de retour supplémentaire n'est signalée.)
  - Numéro de ligne LIGNE ; valeurs variables indiquent qu'une ligne a été exécutée et répertorie toutes les variables dont les valeurs ont été modifiées.

Où,

- la valeur ou les valeurs sont
  - un nombre, avec ou sans virgule décimale,
  - une chaîne, entre guillemets doubles et contenant des caractères échappés comme décrit précédemment,
  - un booléen vrai ou faux,
  - néant
  - un constructeur de table, au format {[key1] =value1, [key2] =value2,…}.
- parameter-values est parameter1 = value1 ; parameter2 = value2 , …
- les valeurs variables sont variable1 = valeur1 ; variable2 = valeur2,…

Voici un exemple de messages de journal abrégés :

```
>shell tail -f /var/log/ns.log | grep TRACE | more

... NSEXTENSION Message 3035 0 : "TRACE combine_headers CALL 30 : CALL
   COMBINE_HEADERS; self = "User-Agent: curl/7.24.0 (amd64-portbld-
   freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nHost:
   10.217.24.7\r\nAccept: \*/\*\r\nH2: h2val1\r\nH1: abcd\r\nH2: h2val2
   \r\nH2: h2val3\r\n\r\n""

... NSEXTENSION Message 3036 0 : "TRACE combine_headers CALL 30 : LINE
   4; headers = {
  }
 "

... NSEXTENSION Message 3037 0 : "TRACE combine_headers CALL 30 : LINE
   5; combined_headers = {
  }
 "

... NSEXTENSION Message 3038 0 : "TRACE combine_headers CALL 30 : CALL
   gmatch"

... NSEXTENSION Message 3039 0 : "TRACE combine_headers CALL 30 :
   RETURN FROM gmatch; return = function 0x2bee5a80"

... NSEXTENSION Message 3040 0 : "TRACE combine_headers CALL 30 : CALL
   for iterator"

... NSEXTENSION Message 3041 0 : "TRACE combine_headers CALL 30 :
   RETURN FROM for iterator; return = " curl/7.24.0 (amd64-portbld-
   freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""

... NSEXTENSION Message 3042 0 : "TRACE combine_headers CALL 30 : LINE
   9; name = "User-Agent"; value = " curl/7.24.0 (amd64-portbld-
   freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""

... NSEXTENSION Message 3043 0 : "TRACE combine_headers CALL 30 : LINE
   10"

... NSEXTENSION Message 3044 0 : "TRACE combine_headers CALL 30 : LINE
   14; headers = {
 ["User-Agent"]={
 [1]="User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0
     OpenSSL/0.9.8y zlib/1.2.3" }
```



```
28    }
29   "
30
31  . . .
32
33  ... NSEXTENSION Message 3117 0 : "TRACE combine_headers CALL 30 : CALL
       for iterator"
34
35  ... NSEXTENSION Message 3118 0 : "TRACE combine_headers CALL 30 :
       RETURN FROM for iterator; return = nil"
36
37  ... NSEXTENSION Message 3119 0 : "TRACE combine_headers CALL 30 : LINE
       19"
38
39  ... NSEXTENSION Message 3120 0 : "TRACE combine_headers CALL 30 : CALL
       concat"
40
41  ... NSEXTENSION Message 3121 0 : "TRACE combine_headers CALL 30 :
       RETURN FROM concat; return = "User-Agent: curl/7.24.0 (amd64-portbld
       -freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\
       nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3""
       ... NSEXTENSION Message 3122 0 : "TRACE combine_headers CALL 30 :
       LINE 25; result_str = "User-Agent: curl/7.24.0 (amd64-portbld-
       freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\
       nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3\r\
       n\r\n""
42
43  ... NSEXTENSION Message 3123 0 : "TRACE combine_headers CALL 30 :
       RETURN FROM COMBINE_HEADERS; return = "User-Agent: curl/7.24.0 (
       amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r
       \nH1: abcd\r\nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1,
       h2val2, h2val3\r\n\r\n""
44  <!--NeedCopy-->
```

Journalisation personnalisée

Vous pouvez également ajouter votre propre journalisation à votre fonction d'extension. Pour ce faire, utilisez la fonction intégrée ns.logger :*level*(), où le *niveau est urgent*, alerte, critique, erreur, avertissement, notification, information ou débogage. Les paramètres sont les mêmes que ceux de la fonction C printf () : une chaîne de format et un nombre variable d'arguments pour fournir des valeurs pour le % spécifié dans la chaîne de format. Par exemple, vous pouvez ajouter ce qui suit à la fonction COMBINE_HEADERS pour enregistrer le résultat d'un appel :


```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"

ns.logger:info("Result: %s", result_str)

return result_str
<!--NeedCopy-->
```

La fonction ci-dessus enregistrerait le message suivant to/var/log/ns.log pour l'exemple d'entrée indiqué dans les exemples de messages de journal abrégés de la section Suivi des extensions ci-dessus.

```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: */*^M H2: h2val1, h2val2,
h2val3^M ^M"
```

Optimisation

May 5, 2023

Les fonctionnalités d'optimisation de NetScaler réduisent les temps de transaction entre les clients et les serveurs et réduisent la consommation de bande passante. Ils améliorent également les performances du serveur en déchargeant certaines tâches et en rendant d'autres plus efficaces.

Fonctionnalité	Description
Keep-Alive du client	Gère plusieurs demandes sur une seule connexion client. Le client n'a pas besoin de négocier une nouvelle connexion pour chaque demande envoyée au serveur.
Compression HTTP	Compresse les réponses HTTP envoyées depuis les serveurs vers des navigateurs compatibles avec la compression. Les réponses plus petites réduisent le temps de téléchargement et économisent de la bande passante.
Mise en cache intégrée	Stocke les réponses aux demandes des clients. Les demandes suivantes pour le même contenu sont traitées à partir du cache NetScaler au lieu d'être transférées vers le serveur d'origine.

Fonctionnalité	Description
Optimisation frontale	Réduit le temps de chargement et de rendu des pages Web en simplifiant et en optimisant le contenu diffusé dans le navigateur client. **Remarque** : prise en charge à partir de NetScaler 10.5.

Le client reste en vie

May 5, 2023

La fonction de maintien en vie du client permet d'envoyer des demandes de plusieurs clients sur une seule connexion. Cette fonctionnalité bénéficie de la gestion des transactions. Lorsque le mode Keep-Alive du client est activé sur une appliance et que la réponse du serveur à la demande du client contient la connexion : fermez l'en-tête HTTP et exécute les tâches suivantes :

- Renomme le nom d'en-tête Connection existant en mélangeant les caractères du nom de l'en-tête.
- Ajoute un nouvel en-tête Connection : avec Keep-Alive comme valeur de l'en-tête.

Le mode Client Keep-Alive permet à l'appliance NetScaler de traiter plusieurs demandes et réponses à l'aide de la même connexion socket. La fonctionnalité maintient la connexion entre le client et l'appliance (connexion côté client) ouverte même après la fermeture de la connexion avec l'appliance par le serveur. Cela permet à plusieurs clients de demander à l'aide d'une seule connexion et enregistre les allers-retours associés à l'ouverture et à la fermeture d'une connexion. Le maintien en vie du client est particulièrement utile dans les sessions SSL.

Client keep-alive est utile pour les scénarios suivants :

- Si le serveur ne prend pas en charge le client, maintenez-le en vie.
- Si le serveur le prend en charge mais qu'une application du serveur ne le prend pas en charge, le client reste actif.

> **Remarque :**
> La fonction Keep-Alive du client s'applique au trafic HTTP et SSL. Client-keep alive peut être configuré globalement pour gérer l'ensemble du trafic. Vous pouvez également l'activer sur des services spécifiques.

Dans l'environnement Keep-Alive du client, les services configurés interceptent le trafic client et la demande du client est dirigée vers le serveur d'origine. Le serveur envoie la réponse et ferme la connexion entre le serveur et l'appliance. Si un en-tête « Connection : Close » figure dans la réponse

du serveur, l'appliance altère cet en-tête dans la réponse côté client et la connexion côté client reste ouverte. Par conséquent, le client n'a pas besoin d'ouvrir une nouvelle connexion pour la demande suivante. Au lieu de cela, la connexion au serveur est rouverte.

> **Remarque :**
> Si un serveur renvoie deux en-têtes « Connection : Close », un seul est modifié. Cela entraîne des retards importants dans le rendu de l'objet par le client, car le client ne suppose pas que l'objet a été complètement livré tant que la connexion n'est pas fermée.

Configurer le maintien en vie du client

Le maintien en vie du client, par défaut, est désactivé sur NetScaler, à la fois globalement et au niveau du service. Par conséquent, vous devez activer la fonctionnalité dans l'étendue requise.

> **Remarque :**
> Si vous activez le maintien de la vie du client globalement, il est activé pour tous les services, que vous l'activiez ou non au niveau du service. Vous devez également configurer certains paramètres HTTP pour spécifier les éléments suivants :
>
> - le nombre maximum de connexions HTTP conservées dans le pool de réutilisation des connexions.
> - activer le multiplexage des connexions et activer la persistance `Etag`.
>
> **Remarque :**
> Lorsque la fonctionnalité Persistent `ETag` est activée, l' `ETag` en-tête inclut des informations sur le serveur qui a diffusé le contenu. Cela garantit que les demandes conditionnelles de validation du cache ou les demandes du navigateur, pour ce contenu, parviennent toujours au même serveur.

Configurer le maintien en vie du client à l'aide de l'interface de commande NetScaler

À l'invite de commandes, procédez comme suit :

1. Activez le maintien en vie du client sur NetScaler.
   - Au niveau mondial - `enable ns mode cka`
   - Au niveau du service - `set service <name> -CKA YES`

   > **Remarque :**
   >
   > Le maintien en vie du client ne peut être activé que pour les services HTTP et SSL.

2. Configurez les paramètres HTTP sur le profil HTTP lié à un ou plusieurs services.

```
set ns httpProfile <name> -maxReusePool <value> -conMultiplex
    ENABLED -persistentETag ENABLED
```



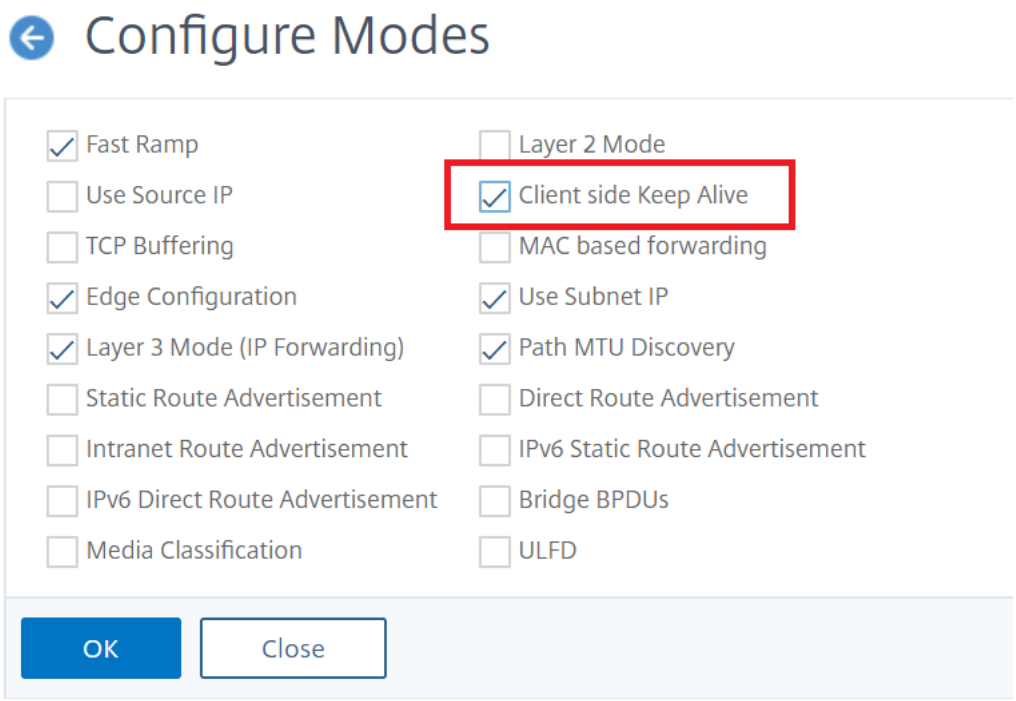
```
<!--NeedCopy-->
```

> **Remarque :**
>
> Configurez ces paramètres sur le `nshttp_default _profile HTTP` profil pour les rendre disponibles dans le monde entier.

Configuration de la fonction Keep-Alive du client à l'aide de l'interface graphique NetScaler

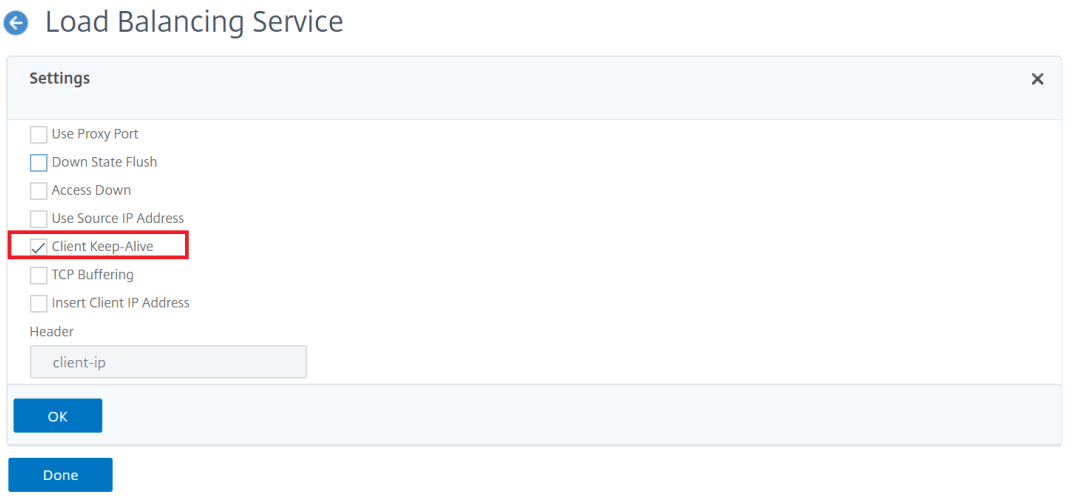
1. Activez le maintien en vie du client sur NetScaler.
   - Au niveau mondial

     Accédez à **Système** > **Paramètres**, cliquez sur **Configurer les modes** et sélectionnez **Keep Alive côté client**.

   - Au niveau du service

     Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis sélectionnez le service requis. Dans la section **Paramètres**, cochez la case **Client Keep-Alive.**



2. Configurez les paramètres HTTP requis sur le profil HTTP lié à un ou plusieurs services.
3. Accédez à **Système** > **Profils**, puis dans l'onglet **Profils HTTP**, sélectionnez le profil requis et mettez à jour les paramètres HTTP requis.

Compression HTTP

May 5, 2023

Pour les sites Web dont le contenu est compressible, la fonctionnalité de compression HTTP implémente une compression sans perte pour réduire la latence, les longs temps de téléchargement et d'autres problèmes de performances réseau en compressant les réponses HTTP envoyées depuis les serveurs vers les navigateurs sensibles à la compression. Vous pouvez améliorer les performances des serveurs en déchargeant les tâches de compression gourmandes en calculs de vos serveurs vers l'appliance NetScaler.

Le tableau suivant décrit les fonctionnalités de la fonction de compression HTTP :

Fonctionnalité	Description
Taux de compression	Le taux de compression dépend des types de fichiers contenus dans les réponses, mais il est toujours important, ce qui réduit sensiblement la quantité de données transmises sur le réseau.

Fonctionnalité	Description
Connaissance du navigateur	NetScaler diffuse les données compressées uniquement aux navigateurs compatibles avec la compression, ce qui réduit le temps de transaction entre le client et le serveur. La plupart des navigateurs Web modernes prennent en charge la compression HTTP.
blocage de la compression	Vous pouvez définir des filtres de contenu pour bloquer sélectivement la compression en appliquant des actions intégrées.
Mise en cache de compression	Lorsque la fonction de mise en cache intégrée est activée, les demandes suivantes pour le même contenu sont envoyées à partir du cache local, ce qui réduit le nombre d'allers-retours vers le serveur et améliore les temps de transaction.
Prise en charge HTTPS	La compression est utile sur les connexions SSL, car elle réduit la quantité de contenu qui doit être chiffré, soit sur le serveur, soit par l'appliance NetScaler, puis déchiffré par le client.
Filtrage intelligent des réponses	Le moteur de compression NetScaler filtre intelligemment les réponses du serveur en fonction de paramètres de compression définis. Par exemple, le moteur de compression détecte les réponses de longueur nulle et les réponses compressées et ne les compresse pas. La détection des réponses compressées permet aux sites d'origine d'utiliser la compression basée sur le serveur avec la fonctionnalité de compression NetScaler.

Fonctionnalité	Description
Commutation des	L'appliance NetScaler dirige de manière transparente les demandes des clients sensibles à la compression vers des serveurs capables de la compression, de sorte que les réponses à ces clients soient compressées et que les réponses aux autres clients ne soient pas retardées par le traitement de compression.

Fonctionnement de la compression HTTP

Un NetScaler peut compresser à la fois les données statiques et générées dynamiquement. Il applique l'algorithme de compression GZIP ou DEFLATE pour supprimer les informations superflues et répétitives des réponses du serveur et représenter les informations d'origine dans un format plus compact et efficace. Ces données compressées sont envoyées au navigateur du client et décompressées selon les algorithmes pris en charge par le navigateur (GZIP ou DEFLATE).

La compression NetScaler traite différemment le contenu statique et dynamique.

- Les fichiers statiques ne sont compressés qu'une seule fois et une copie compressée est stockée dans la mémoire locale. Les demandes ultérieures des clients concernant les fichiers mis en cache sont traitées à partir de cette mémoire.
- Les pages dynamiques sont créées dynamiquement chaque fois qu'un client en fait la demande.

Lorsqu'un client envoie une demande au serveur :

1. La demande du client parvient à NetScaler. L'ADC examine les en-têtes et stocke des informations sur le type de compression pris en charge par le navigateur, le cas échéant.
2. L'ADC transmet la demande au serveur et reçoit la réponse.
3. Le moteur de compression NetScaler examine la compressibilité de la réponse du serveur en la comparant aux politiques.
4. Si la réponse correspond à une politique associée à une action de compression et que le navigateur client prend en charge un algorithme de compression spécifié par l'action, NetScaler applique l'algorithme et envoie la réponse compressée au navigateur client.
5. Le client applique l'algorithme de compression pris en charge pour décompresser la réponse.

Configurer la compression HTTP

Par défaut, la compression est désactivée sur NetScaler. Vous devez activer la fonctionnalité avant de la configurer. Si la fonctionnalité est activée, l'ADC compresse les demandes de serveur spécifiées par

les stratégies de compression.

Pour activer la compression HTTP à l'aide de l'interface de ligne de commande

La compression ne peut être activée que pour les services HTTP et SSL. Vous pouvez l'activer globalement, de sorte qu'il s'applique à tous les services HTTP et SSL, ou vous pouvez l'activer uniquement pour des services spécifiques.

À l'invite de commandes, saisissez l'une des commandes suivantes pour activer la compression globalement ou pour un service spécifique :

- `enable ns feature cmp`
  OU
- `set service \<name\> -CMP YES`

Pour configurer la compression à l'aide de l'interface graphique

Procédez comme suit :

Pour activer la compression globalement, accédez à Système > Paramètres, cliquez sur **Configurer les fonctionnalités de base**, puis sélectionnez Compression HTTP.

Pour activer la compression pour un service spécifique, accédez à **Gestion du trafic > Équilibrage de charge > Services**, sélectionnez le service, puis cliquez sur Modifier. Dans le groupe Paramètres, cliquez sur l'icône en forme de crayon et activez Compression.

Configuration d'une action de compression

Une action de compression spécifie l'action à effectuer lorsqu'une demande ou une réponse correspond à la règle (expression) de la stratégie à laquelle l'action est associée. Par exemple, vous pouvez configurer une stratégie de compression qui identifie les demandes qui seront envoyées à un serveur particulier et associer la stratégie à une action qui compresse la réponse du serveur.

Il existe quatre actions de compression intégrées :

- COMPRESSER : utilise l'algorithme GZIP pour compresser les données des navigateurs qui prennent en charge GZIP ou GZIP et DEFLATE. Utilise l'algorithme DEFLATE pour compresser les données des navigateurs qui prennent uniquement en charge l'algorithme DEFLATE. Si le navigateur ne prend pas en charge l'un ou l'autre algorithme, la réponse du navigateur n'est pas compressée.
- NOCOMPRESS : ne compresse pas les données.
- GZIP : utilise l'algorithme GZIP pour compresser les données des navigateurs qui prennent en charge la compression GZIP. Si le navigateur ne prend pas en charge l'algorithme GZIP, la réponse du navigateur n'est pas compressée.
- DEFLATE : utilise l'algorithme DEFLATE pour compresser les données des navigateurs qui prennent en charge l'algorithme DEFLATE. Si le navigateur ne prend pas en charge l'algorithme

DEFLATE, la réponse du navigateur n'est pas compressée. Après avoir créé une action, vous l'associez à une ou plusieurs politiques de compression.

À l'invite de commandes, saisissez la commande suivante pour créer une action de compression :

```
add cmp action <name> <cmpType> [-addVaryHeader <addVaryHeader> -varyHeaderValue
<string>]
```

Pour configurer une stratégie de compression à l'aide de l'interface de ligne de commande

Une politique de compression contient une règle, qui est une expression logique qui permet à l'appliance NetScaler d'identifier le trafic qui doit être compressé.

Lorsque NetScaler reçoit une réponse HTTP d'un serveur, il évalue les politiques de compression intégrées et toutes les politiques de compression personnalisées afin de déterminer s'il convient de compresser la réponse et, le cas échéant, le type de compression à appliquer. Les priorités attribuées aux stratégies déterminent l'ordre dans lequel les stratégies sont mises en correspondance avec les demandes.

À l'invite de commandes, saisissez la commande suivante pour créer une stratégie de compression :

```
add cmp policy <name> -rule <expression> -resAction <string>
```

Pour créer une action de compression à l'aide de l'interface graphique

Accédez à **Optimisation** > **Compression HTTP** > **Actions**, cliquez sur **Ajouter** et créez une action de compression pour spécifier le type de compression à effectuer sur la réponse HTTP.

Configuration d'une stratégie de compression

Une politique de compression contient une règle, qui est une expression logique qui permet à l'appliance NetScaler d'identifier le trafic qui doit être compressé.

Lorsque NetScaler reçoit une réponse HTTP d'un serveur, il évalue les politiques de compression intégrées et toutes les politiques de compression personnalisées afin de déterminer s'il convient de compresser la réponse et, le cas échéant, le type de compression à appliquer. Les priorités attribuées aux stratégies déterminent l'ordre dans lequel les stratégies sont mises en correspondance avec les demandes.

Le tableau suivant répertorie les stratégies de compression HTTP intégrées. Ces stratégies sont activées globalement lorsque vous activez la compression.

Stratégie classique ou avancée intégrée	Description
ns_nocmp_mozilla_47, ns_adv_nocmp_mozilla_47	Empêche la compression des fichiers CSS lorsqu'une requête est envoyée depuis un navigateur Mozilla 4.7.
ns_cmp_mscss, ns_adv_cmp_mscss	Compresse les fichiers CSS lorsque la demande est envoyée depuis un navigateur Microsoft Internet Explorer.
ns_cmp_msapp, ns_adv_cmp_msapp	Compresse les fichiers générés par les applications suivantes : Microsoft Office Word, Microsoft Office Excel, Microsoft Office PowerPoint.
ns_cmp_content_type, ns_adv_cmp_content_type	Compresse les données lorsque la réponse contient un en-tête Content-type et contient du texte.
ns_nocmp_xml_fr, ns_adv_nocmp_xml_fr	Empêche la compression lorsqu'une demande est envoyée à partir d'un navigateur Microsoft Internet Explorer et que la réponse contient un en-tête Content-Type et contient du texte ou du XML.

Liaison d'une stratégie de compression

Pour mettre en œuvre une politique de compression, vous devez la lier soit globalement, afin qu'elle s'applique à tout le trafic qui passe par NetScaler, soit à un serveur virtuel spécifique, de sorte que la politique s'applique uniquement aux demandes dont la destination est l'adresse VIP de ce serveur virtuel.

Lorsque vous liez une stratégie, vous lui attribuez une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées. Vous pouvez définir la priorité sur n'importe quel nombre entier positif.

Pour lier une stratégie de compression à l'aide de l'interface de ligne de commande

À l'invite de commandes, saisissez l'une des commandes suivantes pour lier une stratégie de compression globalement ou à un serveur virtuel spécifique :

- `bind cmp global <policyName> [-priority <positive_integer>] [-state (ENABLED|DISABLED)]...`
- `bind lb vserver <vserverName> -policyName <policyName> -type (Request|Response)-priority <positive_integer> )`

Répétez cette commande pour chaque serveur virtuel auquel vous souhaitez lier la stratégie de compression.

Pour lier une stratégie de compression à l'aide de l'interface graphique

Procédez comme suit :

Au niveau global, accédez à **Optimisation** > **Compression HTTP** > **Stratégies**, cliquez sur **Gestionnaire de stratégies** et liez les stratégies requises en spécifiant le point de liaison et le type de connexion appropriés (demande/réponse).

Au niveau du serveur virtuel

Pour le serveur virtuel d'équilibrage de charge, accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez le serveur virtuel requis, cliquez sur **Stratégies**et liez la stratégie correspondante.

Pour le serveur virtuel de commutation de contenu, accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez le serveur virtuel requis, cliquez sur **Stratégies**et liez la stratégie correspondante.

Définissez les paramètres de compression globaux pour des performances optimales

De nombreux utilisateurs acceptent les valeurs par défaut des paramètres de compression globaux, mais vous pouvez peut-être fournir une compression plus efficace en personnalisant ces paramètres.

> **Remarque**
> Après avoir configuré les paramètres de compression globaux, il n'est pas nécessaire de redémarrer votre solution matérielle-logicielle. Ils sont immédiatement appliqués aux nouveaux flux.

Le tableau suivant décrit les paramètres de compression que vous pouvez définir sur NetScaler.

Paramètres de compression	Description
Taille Quantum	Taille, en Ko, de la mémoire tampon conservée pour l'accumulation des réponses du serveur. Les réponses sont compressées lorsque la taille de la mémoire tampon dépasse cette valeur. Par exemple, si vous définissez la taille quantique à 50 Ko, NetScaler compresse le contenu de la mémoire tampon lorsque sa taille dépasse 50 Ko. Valeur minimale : 1. Valeur maximale : 63488. Par défaut : 57344.
Niveau de compression	Niveau de compression à appliquer aux réponses du serveur. Valeurs possibles : meilleure vitesse, meilleure compression, optimale.

Paramètres de compression	Description
Taille de réponse HTTP minimale	Taille minimale, en octets, d'une réponse HTTP compressée. Les réponses inférieures à la valeur spécifiée par ce paramètre sont envoyées sans être compressées.
Contournement de la compression sur l'utilisation du processeur	Utilisation du processeur NetScaler, en pourcentage, à partir de laquelle aucune compression n'est effectuée. Par défaut : 100.
Type de politique*	Type de stratégies utilisées pour la compression. Valeurs possibles : stratégie classique, avancée. Par défaut : Classic.
Autoriser la compression côté serveur	Autorisez les serveurs à envoyer des données compressées à NetScaler.
Compresser le paquet push	À la réception d'un paquet avec un drapeau TCP PUSH, compressez immédiatement les paquets accumulés, sans attendre que le tampon quantique soit rempli.
Cache externe	Émettez une directive de réponse privée indiquant que le message de réponse est destiné à un seul utilisateur et ne doit pas être mis en cache par un cache partagé ou proxy.

Pour configurer la compression HTTP à l'aide de l'interface graphique

Procédez comme suit :

- Pour activer la compression globale, accédez à **Système** > **Paramètres**, cliquez sur **Configurer les fonctionnalités de base**, puis sélectionnez **Compression HTTP**.
- Pour activer la compression pour un service spécifique, accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, sélectionnez le service et cliquez sur **Modifier**.
- Dans le groupe **Paramètres**, cliquez sur l'icône en forme de crayon et activez **la compression**.

Pour créer une action de compression à l'aide de l'interface graphique

Accédez à **Optimisation** > **Compression HTTP** > **Actions**, cliquez sur **Ajouter** et créez une action de compression pour spécifier le type de compression à effectuer sur la réponse HTTP

Pour créer une stratégie de compression à l'aide de l'interface graphique

Accédez à **Optimisation** > **Compression HTTP** > **Politiques**, cliquez sur **Ajouter**et créez une politique de compression en spécifiant la condition et l'action correspondante à exécuter.

Évaluation de la configuration de compression

Vous pouvez afficher les statistiques de compression dans l'utilitaire de tableau de bord ou dans un moniteur SNMP. L'utilitaire de tableau de bord affiche des statistiques récapitulatives et détaillées sous forme de tableau et de graphique.

Vous pouvez également afficher les statistiques d'une stratégie de compression, y compris le nombre de demandes incrémentées par le compteur de stratégie pendant la compression basée sur la stratégie.

> **Remarque**
>
> - Pour plus d'informations sur les statistiques et les graphiques, consultez l'aide du tableau de bord sur l'appliance NetScaler.
> - Pour plus d'informations sur le protocole SNMP, consultez la rubrique SNMP .

Pour afficher les statistiques de compression à l'aide de l'interface de ligne de commande

À l'invite de commandes, saisissez les commandes suivantes pour afficher les statistiques de compression :

1. Pour afficher le résumé des statistiques de compression.

```
stat cmp
```

> **Remarque**
> La commande stat cmp policy affiche les statistiques pour les stratégies de compression de stratégie avancée uniquement.

2. Pour afficher les résultats et les détails de la politique de compression

```
show cmp policy \<name\>
```

3. Pour afficher des statistiques de compression détaillées

```
stat cmp -detail
```

Pour afficher les statistiques de compression à l'aide du tableau de bord :

Dans l'utilitaire Tableau de bord, vous pouvez afficher les types de statistiques de compression suivants :

- Sélectionnez Compression pour afficher un résumé des statistiques de compression.
- Pour afficher des statistiques de compression détaillées par type de protocole, cliquez sur le bouton Détails
- Pour afficher le taux de demandes traitées par la fonction de compression, cliquez sur l'onglet Affichage graphique.

Pour afficher les statistiques de compression à l'aide du protocole SNMP

Vous pouvez afficher les statistiques de compression suivantes à l'aide de l'application de gestion de réseau SNMP.

- Nombre de demandes de compression (OID : 1.3.6.1.4.1.5951.4.1.1.50.1)
- Nombre d'octets compressés transmis (OID : 1.3.6.1.4.1.5951.4.1.1.50.2)
- Nombre d'octets compressibles reçus (OID : 1.3.6.1.4.1.5951.4.1.1.50.3)
- Nombre de paquets compressibles transmis (OID : 1.3.6.1.4.1.5951.4.1.1.50.4)
- Nombre de paquets compressibles reçus (OID : 1.3.6.1.4.1.5951.4.1.1.50.5)
- Rapport des données compressibles reçues et des données compressées transmises (OID : 1.3.6.1.4.1.5951.4.1.1.50.6)
- Rapport entre le total des données reçues et le total des données transmises (OID : 1.3.6.1.4.1.5951.4.1.1.50.7)

Pour afficher plus de statistiques de compression à l'aide de l'interface graphique

1. Pour afficher les statistiques de compression HTTP :

Accédez à **Optimisation** > **Compression HTTP** et cliquez sur **Statistiques**.

1. Pour afficher les statistiques d'une stratégie de compression.

Accédez à **Optimisation** > **Compression HTTP** > **Politiques** > sélectionnez la politique, puis cliquez sur **Statistiques**.

1. Pour afficher les statistiques d'une étiquette de stratégie de compression
2. Accédez à **Optimisation** > **Compression HTTP** > **Politiques** > sélectionnez un libellé de politique, puis cliquez sur **Statistiques**.

Déchargement de la compression HTTP

La compression sur un serveur peut affecter les performances du serveur. Un NetScaler placé devant vos serveurs Web et configuré pour la compression HTTP décharge la compression du contenu statique et dynamique, économisant ainsi des cycles de processeur et des ressources du serveur.

Vous pouvez décharger la compression des serveurs Web de l'une des deux manières suivantes :

Désactivez la compression sur les serveurs Web, activez la fonctionnalité de compression NetScaler au niveau global et configurez les services pour la compression.

Laissez la fonctionnalité de compression activée sur les serveurs Web et configurez l'appliance NetScaler pour supprimer l'en-tête « Accept Encoding » de toutes les demandes des clients HTTP. Les serveurs envoient ensuite des réponses non compressées. NetScaler compresse les réponses du serveur avant de les envoyer aux clients.

> **Remarque**
> La deuxième option ne fonctionne pas si les serveurs compressent automatiquement toutes les réponses. NetScaler ne tente pas de compresser une réponse déjà compressée.

Le paramètre Servercmp permet à l'appliance NetScaler de gérer la compression HTTP de déchargement. Par défaut, ce paramètre est défini sur ON pour que le serveur envoie des données compressées

à l'appliance NetScaler. Pour décharger la compression HTTP, vous devez définir le paramètre servercmp sur OFF. À l'invite de commandes, saisissez les commandes suivantes :

```
set service <service name> -CMP YES
```

Répétez cette commande pour chaque service pour lequel vous souhaitez activer la compression.

```
show service <service name>
```

Répétez cette commande pour chaque service afin de vérifier que la compression est activée.

```
Save config
```

```
set cmp parameter -serverCmp OFF
```

> **Remarque :**
>
> Lorsque le `Servercmp` paramètre est activé et que la solution matérielle-logicielle reçoit une réponse compressée du serveur, la solution matérielle-logicielle ne compresse plus les données. Au lieu de cela, il transmet la réponse compressée au client.

Mise en cache intégrée

May 5, 2023

Le cache intégré fournit un stockage en mémoire sur l'appliance NetScaler et diffuse du contenu Web aux utilisateurs sans qu'il soit nécessaire d'aller et retour vers un serveur d'origine. Pour le contenu statique, le cache intégré nécessite peu de configuration initiale. Une fois que vous avez activé la fonctionnalité de cache intégrée et effectué la configuration de base (par exemple, en déterminant la quantité de mémoire de l'appliance NetScaler que le cache est autorisé à utiliser), le cache intégré utilise des politiques intégrées pour stocker et diffuser des types spécifiques de contenu statique, notamment de simples pages Web et des fichiers image. Vous pouvez également configurer le cache intégré pour stocker et diffuser du contenu dynamique marqué comme non mis en cache par les serveurs Web et d'applications (par exemple, les enregistrements de base de données et les cotations boursières).

> **Remarque :**
>
> Le terme Cache intégré peut être utilisé de façon interchangeable avec AppCache ; notez que d'un point de vue fonctionnel, les deux termes signifient la même chose.

Lorsqu'une demande ou une réponse correspond à la règle (expression logique) spécifiée dans une stratégie intégrée ou une stratégie que vous avez créée. L'appliance NetScaler exécute l'action associée à la politique. Par défaut, toutes les stratégies stockent les objets mis en cache et les récupèrent depuis le groupe de contenus par défaut. Vous pouvez créer vos propres groupes de contenus pour différents types de contenu.

Pour permettre à l'appliance de rechercher des objets mis en cache dans un groupe de contenus, vous pouvez configurer des sélecteurs. Les sélecteurs font correspondre les objets mis en cache aux expressions, ou vous pouvez spécifier des paramètres pour rechercher des objets dans le groupe de contenus. Si vous utilisez des sélecteurs comme recommandé par Citrix, configurez-les d'abord afin de pouvoir spécifier des sélecteurs lorsque vous configurez des groupes de contenu. Configurez ensuite les groupes de contenu que vous souhaitez ajouter, afin qu'ils soient disponibles lorsque vous configurez les stratégies. Pour terminer la configuration initiale, créez des banques de stratégies en liant chaque stratégie à un point de liaison global ou à un serveur virtuel. Vous pouvez également lier une étiquette pouvant être appelée depuis d'autres banques de stratégies.

La mise en cache intégrée peut être améliorée à l'aide de la méthode de préchargement des objets mis en cache avant leur expiration planifiée. Pour gérer la gestion des données mises en cache, vous pouvez configurer des en-têtes relatifs à la mise en cache insérés dans les réponses. Le cache intégré peut également servir de proxy de transfert pour d'autres serveurs de cache.

> **Remarque :**
>
> La mise en cache intégrée nécessite une certaine connaissance des requêtes et des réponses HTTP. Pour plus d'informations sur la structure des données HTTP, consultez les *en-têtes HTTP dynamiques* à l'adresse `"<http://livehttpheaders.mozdev.org/>."`

Fonctionnement du cache d'intégration

Le cache intégré surveille les requêtes HTTP et SQL qui transitent par l'appliance NetScaler et compare les demandes aux politiques stockées. En fonction du résultat, la fonction de cache intégrée recherche la réponse dans le cache ou transmet la demande au serveur d'origine. Pour les requêtes HTTP, la mise en cache intégrée sert de contenu partiel provenant du cache en réponse à des demandes de plage d'octets unique et de plage d'octets en plusieurs parties.

Les données mises en cache sont compressées si le client accepte le contenu compressé. Vous pouvez configurer les délais d'expiration pour un groupe de contenus et vous pouvez faire expirer de manière sélective les entrées d'un groupe de contenus.

Les données fournies par le cache intégré sont considérées comme un succès, tandis que les données fournies depuis l'origine sont perdues dans le cache, comme décrit dans le tableau suivant.

Type de transaction	Spécifications
Accès au cache	Les réponses que l'appliance NetScaler fournit à partir du cache, notamment : des objets statiques, par exemple, des fichiers image et des pages Web statiques, 200 pages OK, 203 pages de réponses non autorisées, 300 pages à choix multiples, 301 pages déplacées définitivement, 302 pages trouvées, 304 pages non modifiées. Ces réponses sont appelées réponses positives. L'appliance NetScaler met également en cache les réponses négatives suivantes : 307 pages de redirection temporaires, 403 pages interdites, 404 pages introuvables, 410 pages disparues. Pour améliorer encore les performances, vous pouvez configurer l'appliance NetScaler pour mettre en cache davantage de types de contenu.
Echec du cache stockable	En cas d'échec du cache stockable, l'appliance NetScaler récupère la réponse auprès du serveur d'origine et stocke la réponse dans le cache avant de la transmettre au client.
Echec du cache non stockable	Une erreur de cache non stockable n'est pas appropriée pour la mise en cache. Par défaut, toute réponse contenant les codes d'état suivants est une erreur de cache non stockable : codes d'état 201, 202, 204, 205, 206, tous les codes 4xx, à l'exception des codes d'état 403, 404 et 410, 5xx

> **Remarque :**
>
> Pour intégrer la mise en cache dynamique à votre infrastructure d'applications, utilisez l'API NITRO pour émettre des commandes de cache à distance. Par exemple, vous pouvez configurer des déclencheurs qui font expirer les réponses mises en cache lorsqu'une table de base de données est mise à jour.

Pour garantir la synchronisation des réponses mises en cache avec les données du serveur d'origine, vous devez configurer des méthodes d'expiration. Lorsque l'appliance NetScaler reçoit une demande

qui correspond à une réponse expirée, elle actualise la réponse depuis le serveur d'origine.

> **Remarque :**
>
> Citrix vous recommande de synchroniser les heures sur l'appliance NetScaler et sur un ou plusieurs serveurs principaux.

Fonctionnement du cache dynamique

La mise en cache dynamique évalue les demandes et les réponses HTTP en fonction de paires paramètre-valeur, de chaînes, de modèles de chaînes ou d'autres données. Supposons, par exemple, qu'un utilisateur recherche le bogue 31231 dans une application de signalement de bogues. Le navigateur envoie la demande suivante au nom de l'utilisateur :

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
          Template=view&TableId=1000
2
3     Host: mycompany.net
4
5     User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
          Gecko/2008052906 Firefox/3.0
6
7     Accept: text/html,application/xhtml+xml,application/xml;q
          =0.9,\*/\*;q=0.8
8
9     Accept-Language: en-us,en;q=0.5
10 <!--NeedCopy-->
```

Dans cet exemple, les requêtes GET pour cette application de signalement de bogues contiennent toujours les paramètres suivants :

- IssuePage
- RecordID
- Modèle
- TableId

Les requêtes GET ne mettent pas à jour ni ne modifient les données. Vous pouvez donc configurer ces paramètres dans les stratégies de mise en cache et les sélecteurs, comme suit :

- Vous configurez une stratégie de mise en cache qui recherche la chaîne mybugreportingsystem et la méthode GET dans les requêtes HTTP. Cette stratégie dirige les demandes de correspondance vers un groupe de contenus en cas de bogues.
- Dans le groupe de contenu pour les bogues, vous configurez un sélecteur `hit` qui correspond à différentes paires paramètre-valeur, notamment IssuePage, RecordID, etc.

> **Remarque**
>
> Un navigateur peut envoyer plusieurs requêtes GET en fonction d'une action de l'utilisateur. Voici une série de trois requêtes GET distinctes qu'un navigateur émet lorsqu'un utilisateur recherche un bogue basé sur un identifiant de bogue.

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
          Template=view&TableId=1000
2
3     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
          viewbtns&RecordId=31231&TableId=1000
4
5     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
          viewbody&RecordId=31231&tableid=1000
6 <!--NeedCopy-->
```

Pour répondre à ces demandes, plusieurs réponses sont envoyées au navigateur de l'utilisateur, et la page Web que l'utilisateur voit est un ensemble de réponses.

Si un utilisateur met à jour un rapport de bogue, les réponses correspondantes dans le cache doivent être actualisées avec les données du serveur d'origine. L'application de signalement de bogues émet des requêtes HTTP POST lorsqu'un utilisateur met à jour un rapport de bogue. Dans cet exemple, vous configurez les éléments suivants pour vous assurer que les requêtes POST déclenchent une invalidation dans le cache :

- Une stratégie d'invalidation au moment de la demande qui recherche la chaîne mybugreportingsystem et la méthode de requête HTTP POST, et qui dirige les demandes correspondantes vers le groupe de contenus pour les rapports de bogues.
- Un sélecteur d'invalidation pour le groupe de contenus pour les rapports de bogues qui fait expirer le contenu mis en cache en fonction du paramètre RecordID. Ce paramètre apparaît dans toutes les réponses, de sorte que le sélecteur d'invalidation peut faire expirer tous les éléments pertinents du cache.

L'extrait suivant montre une demande POST qui met à jour l'exemple de rapport de bogue.

```
1     POST /mybugreportingsystem/mybugreport.dll?TransitionForm HTTP/1.1\
          r\n
2
3     User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
          Opera 7.23 [en]\r\n
4
5     Host: mybugreportingsystem\r\n
6
7     Cookie:ttSearch.134=%23options%3Afalse%23active%23owner%3Afalse%23
          unowned%3Afalse%23submitter%3Afalse%23incsub%3Atrue;
```



```
8
9       Cookie2: $Version=1\r\n
10
11      . . .
12
13      \r\n
14
15      ProjectId=2&RecordId=31231&TableId=1000&TransitionId=1&Action=
           Update&CopyProjectId=0&ReloadForm=0&State=&RecordLockId=49873+
           issues+in+HTTP&F43. . .
16  <!--NeedCopy-->
```

Lorsque l'appliance NetScaler reçoit cette demande, elle effectue les opérations suivantes :

- Associe la demande à une stratégie d'invalidation.
- Trouve le groupe de contenus nommé dans la stratégie.
- Applique le sélecteur d'invalidation pour ce groupe de contenus et fait expirer toutes les réponses qui correspondent à RecordID=31231.

Lorsqu'un utilisateur émet une nouvelle demande pour ce rapport de bogue, l'appliance NetScaler accède au serveur d'origine pour obtenir des copies mises à jour de toutes les réponses associées à l'instance du rapport. Il stocke les réponses dans le groupe de contenus et les transmet au navigateur de l'utilisateur, qui réassemble le rapport et l'affiche.

Configuration du cache intégré

Pour utiliser le cache intégré, vous devez installer la licence et activer la fonctionnalité. Une fois que vous avez activé le cache intégré, l'appliance NetScaler® met automatiquement en cache les objets statiques conformément aux politiques intégrées et génère des statistiques sur le comportement du cache. (Les stratégies intégrées comportent un trait de soulignement à la position initiale du nom de la stratégie.)

Même si les stratégies intégrées sont adaptées à votre situation, vous souhaiterez peut-être modifier les attributs globaux. Par exemple, vous souhaiterez peut-être modifier la quantité de mémoire de l'appliance NetScaler allouée au cache intégré.

Si vous souhaitez observer le fonctionnement du cache avant de modifier les paramètres, reportez-vous à la section « Affichage des objets mis en cache et des statistiques de cache ».

> **Remarque :**
>
> Le cache NetScaler est un stockage en mémoire qui est purgé lorsque vous redémarrez l'appliance.

Pour installer une licence de cache intégrée

- Une licence de cache intégrée est requise.
- Obtenez un code de licence auprès de Citrix, accédez à l'interface de ligne de commande et connectez-vous.

Sur l'interface de ligne de commande, copiez le fichier de licence dans le dossier `/nsconfig/license`.

- Redémarrez l'appliance NetScaler à l'aide de la commande suivante :

```
reboot
```

Pour activer la mise en cache intégrée :
lorsque vous activez la mise en cache intégrée, l'appliance NetScaler commence à mettre en cache les réponses du serveur. Si vous n'avez configuré aucune stratégie ou aucun groupe de contenu, les stratégies intégrées stockent les objets mis en cache dans le groupe de contenu par défaut.

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver la mise en cache intégrée :

```
enable ns feature IC
```

Configurer les attributs globaux pour la mise en cache

Les attributs globaux s'appliquent à toutes les données mises en cache. Vous pouvez spécifier la quantité de mémoire NetScaler allouée au cache intégré, via l'insertion d'un en-tête. Critère permettant de vérifier qu'un objet mis en cache doit être diffusé. La longueur maximale d'un corps POST autorisé dans le cache, indique s'il faut contourner l'évaluation des stratégies pour les requêtes HTTP GET et action à entreprendre lorsqu'une stratégie ne peut pas être évaluée.

La capacité de la mémoire cache est limitée uniquement par la mémoire de l'appliance matérielle. De plus, tout moteur de paquets (hub de distribution central de toutes les demandes TCP entrantes) de l'appliance nCore NetScaler connaît les objets mis en cache par d'autres moteurs de paquets de l'appliance nCore NetScaler.

> **Remarque :**
>
> Lorsque la limite de mémoire globale par défaut est définie sur 0 et que la fonctionnalité de mise en cache intégrée (IC) est activée, l'appliance ne met en cache aucun objet. Pour la mise en cache, vous devez configurer explicitement la limite de mémoire globale. Toutefois, si vous activez l'option « définir le paramètre d'authentification, d'autorisation et d'audit EnableStaticPageCaching », une partie de la mémoire par défaut sera configurée dans l'appliance. Cette mémoire est insuffisante pour la mise en cache d'objets volumineux et il est donc nécessaire d'attribuer une limite de mémoire plus élevée au circuit intégré. Pour ce faire, configurez la commande « set cache parameter –memLimit ». Le nouveau paramètre n'est appliqué qu'après avoir enregistré la configuration et redémarré l'appliance.

Vous pouvez modifier la limite de mémoire globale configurée pour la mise en cache des objets. Toutefois, lorsque vous mettez à jour la limite de mémoire globale à une valeur inférieure à la valeur existante (par exemple, de 10 Go à 4 Go), l'appliance continue d'utiliser la limite de mémoire.

Cela signifie que même si la limite de mise en cache intégrée est configurée à une certaine valeur, la limite réelle utilisée peut être plus élevée. Cette mémoire excessive est toutefois libérée lorsque les objets sont retirés du cache.

La sortie de la commande show cache parameter indique la valeur configurée (limite d'utilisation de la mémoire) et la valeur réelle utilisée (limite d'utilisation de la mémoire (valeur active)).

À l'invite de commande, tapez :

```
1     set cache parameter [-memLimit <MBytes>] [-via <string>] [-
          verifyUsing <criterion>] [-maxPostLen <positiveInteger>] [-
          prefetchMaxPending <positiveInteger>] [-enableBypass(YES|NO)] [-
          undefAction (NOCACHE|RESET)]
2 <!--NeedCopy-->
```

Activer la mise en cache intégrée via l'interface graphique NetScaler

Accédez à **Système** > **Paramètres**, cliquez sur **Configurer les fonctionnalités de base**, puis sélectionnez **Mise en cache intégrée**.

Configurer les paramètres globaux pour la mise en cache à l'aide de l'interface graphique NetScaler

Accédez à **Optimisation** > **Mise en cache intégrée**, cliquez sur **Modifier les paramètres du cache** et configurez les paramètres globaux pour la mise en cache.

Configurer un groupe de contenu intégré, un jeu de modèles et des stratégies pour le cache intégré

L'appliance NetScaler inclut une configuration de mise en cache intégrée que vous pouvez utiliser pour la mise en cache du contenu. La configuration se compose d'un groupe de contenus appelé ctx_cg_poc, d'un ensemble de modèles appelé ctx_file_extensions et d'un ensemble de stratégies de cache intégrées. Dans le groupe de contenus ctx_cg_poc, seuls les objets de 500 Ko ou moins sont mis en cache. Le contenu est mis en cache pendant 86 000 secondes et la limite de mémoire pour le groupe de contenus est de 512 Mo. L'ensemble de modèles est un tableau indexé d'extensions courantes pour la mise en correspondance des types de fichiers.

Le tableau suivant répertorie les stratégies de mise en cache intégrées. Par défaut, les stratégies ne sont liées à aucun point de liaison. Vous devez lier les politiques à un point de liaison si vous souhaitez

que l'appliance NetScaler évalue le trafic par rapport aux politiques. Les stratégies mettent en cache les objets du groupe de contenu ctx_cg_poc.

Nom de la stratégie de mise en cache intégrée	Règle de stratégie
_cacheVPNStaticObjects	HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS_IN
_cacheTCPVPNStaticObjects	HTTP.REQ.URL.ENDSWITH(".css")
_cacheOCVPNStaticObjects	HTTP.REQ.URL.ENDSWITH(".pdf")
_cacheWFStaticObjects	HTTP.REQ.URL.ENDSWITH(".js")
_mayNoCacheReq	HTTP.RES.HEADER("Content-Type").CONTAINS("application/x-javascript")
_noCacheRest	TRUE

Vider la configuration du cache

Vous pouvez vider un groupe de cache, des groupes de cache ou un localisateur d'objets de cache. Les commandes suivantes permettent de vider les objets du cache.

À l'invite de commande, tapez :

```
flush cache contentgroup all
```

Exemple

```
1          0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hello
2          0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hi
3
4          Flush cache contentGroup all
5          done
6
7  `flush cache contentgroup <content group name>`
8  <!--NeedCopy-->
```

Exemple :

```
1          0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hello
2          0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hi
```



```
3
4         Flush cache ob -| 0x00000089bae000000004
5         done
6
7 `flush cache object (-locator <positive_integer> | (-url <URL> (-host <
     string> [-port <port>] [-groupName <string>] [-httpMethod ( GET |
     POST )]))))`
8 <!--NeedCopy-->
```

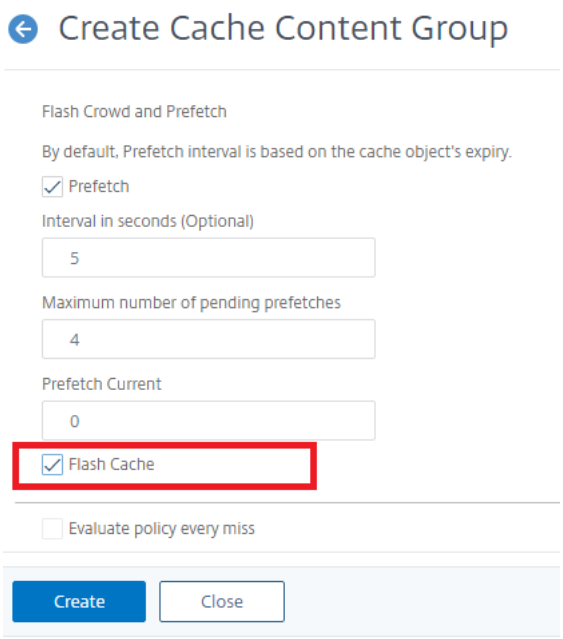
Exemple :

```
1         0x00000089bae000000006 DEFAULT GET //1.1.1.1:80/html/index.html
2
3         flush cache ob -URL /html/index.html -host 1.1.1.1 -groupName
             DEFAULT
4         done
5 <!--NeedCopy-->
```

Configuration du cache vide à l'aide de l'interface graphique NetScaler

Suivez les étapes pour configurer le vidage du cache à l'aide de l'interface graphique NetScaler

1. Accédez à **Optimisation** > **Groupes de contenu**.
2. Dans le volet détaillé **des groupes de contenus**, cliquez sur **Ajouter**.
3. Sur la page **Créer des groupes de contenu en cache**, définissez le paramètre suivant sous l'onglet **Autres** :
   a) Videz le cache. Cochez la case pour vider l'objet du cache.
4. Cliquez sur **Créer** et **Fermer**.



Configuration de la mise en cache intégrée pour différents scénarios

La section suivante décrit la configuration de la mise en cache intégrée sur l'appliance NetScaler pour différents scénarios.

À partir de la version 9.2 de NetScaler, la mise en cache intégrée dispose de plus de mémoire pour la mise en cache. La mémoire de mise en cache intégrée n'est limitée que par la mémoire disponible sur l'appliance matérielle. Vous pouvez allouer jusqu'à 50 % de la mémoire disponible à la fonction de mise en cache intégrée.

Pour définir l'allocation de mémoire pour le cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cache parameter -memlimit <value>
```

> **Remarque :**
>
> La limite de mémoire globale par défaut pour la mise en cache intégrée est nulle. Par conséquent, même si vous activez la fonctionnalité de mise en cache intégrée, l'appliance NetScaler ne met aucun objet en cache tant que la limite de mémoire globale n'est pas explicitement définie.

La section suivante vous indique de configurer la mise en cache intégrée sur différents scénarios.

> **Remarque :**
>
> La limite de mémoire de l'appliance NetScaler est identifiée au démarrage de l'appliance. Par

> conséquent, toute modification de la limite de mémoire nécessite le redémarrage de l'appliance pour que les modifications soient applicables à tous les moteurs de paquets.

La mise en cache intégrée est activée et la limite de mémoire cache est définie sur une valeur différente de zéro

Imaginez un scénario dans lequel vous démarrez l'appliance, la fonction de mise en cache intégrée est activée et la limite de mémoire globale est définie sur un nombre positif. La mémoire que vous avez définie précédemment est allouée à la fonction de mise en cache intégrée lors du processus de démarrage. Vous souhaiterez peut-être modifier la limite de mémoire à une autre valeur en fonction de la mémoire disponible sur l'appliance.

Configuration à l'aide de l'interface de ligne de commande

1. Afficher le paramètre cache

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 MBytes
4                  Memory usage limit (active value): 500 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

1. Définir une limite de mémoire non nulle

```
set cache parameter -memlimit 600
```

> **Remarque :**
>
> La commande précédente affiche le message d'avertissement suivant : **Avertissement : Pour utiliser une nouvelle limite de mémoire cache intégrée, enregistrez la configuration et redémarrez l'appliance NetScaler.**

1. Enregistrez la configuration

```
save config
```

1. À partir de l'invite shell, exécutez la commande suivante pour vérifier dans le fichier de configuration.


```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Redémarrer l'appliance

```
root@ns## reboot
```

1. Vérifier la nouvelle valeur de la limite de mémoire

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 600 MBytes
4                  Memory usage limit (active value): 600 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

Une fois tous les moteurs de paquets démarrés avec succès, la fonction de mise en cache intégrée négocie la mémoire que vous aviez configurée. Si l'appliance ne peut pas utiliser la mémoire configurée, celle-ci est allouée en conséquence. Si la mémoire disponible est inférieure à celle que vous avez allouée, l'appliance recommande un nombre inférieur. La fonctionnalité de mise en cache intégrée utilise la même valeur que la valeur active.

La mise en cache intégrée est désactivée et la limite de mémoire cache est définie sur une valeur différente de zéro

Dans ce scénario, lorsque vous démarrez l'appliance, la fonctionnalité de mise en cache intégrée est désactivée et la limite de mémoire globale est définie sur un nombre positif. Par conséquent, aucune mémoire n'est allouée à la mise en cache intégrée pendant le processus de démarrage.

Configuration à l'aide de l'interface de ligne de commande

1. Afficher le paramètre cache

```
1          > show cache parameter
2                  Integrated cache global configuration:
```



```
3                   Memory usage limit: 600 MBytes
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12  <!--NeedCopy-->
```

1. Définir une nouvelle limite de mémoire

```
set cache parameter -memlimit 500
```

> **Remarque :**
>
> La commande précédente affiche le message d'avertissement suivant : **Avertissement : fonctionnalité non activée [IC]**.

1. Enregistrez la configuration

```
save config
```

1. À partir de l'invite shell, exécutez la commande suivante pour vérifier dans le fichier de configuration

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Vérifier la nouvelle valeur de la limite de mémoire

```
1           > show cache parameter
2                   Integrated cache global configuration:
3                   Memory usage limit: 500 MBytes
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12  <!--NeedCopy-->
```


1. Activer la fonctionnalité de mise en cache intégrée

```
enable ns feature IC
```

1. Vérifier la nouvelle valeur de la limite de mémoire

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 Mbytes
4                  Memory usage limit (active value): 500 Mbytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

> **Remarque :**
>
> 500 Mo de mémoire sont alloués à la fonction de mise en cache intégrée.

1. Enregistrez la configuration pour vous assurer que la mémoire est automatiquement allouée à la fonctionnalité lors du redémarrage de l'appliance.

La mise en cache intégrée est activée et la mémoire cache est définie sur zéro

Dans ce scénario, lorsque vous démarrez l'appliance, la fonctionnalité de mise en cache intégrée est activée et la limite de mémoire globale est définie sur zéro. Par conséquent, aucune mémoire n'est allouée à la mise en cache intégrée pendant le processus de démarrage.

Configuration à l'aide de l'interface de ligne de commande

1. Vérifiez les limites de mémoire définies dans le fichier ns.conf à partir de l'invite shell

```
root@ns## cat ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Vérifier la valeur de la limite de mémoire

```
1          > show cache parameter
```



```
2                   Integrated cache global configuration:
3                   Memory usage limit: 0 Mbytes
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12  <!--NeedCopy-->
```

> **Remarque :**
>
> La limite de mémoire est définie sur 0 Mo et aucune mémoire n'est allouée à la fonction de mise en cache intégrée.

1. Définissez les limites de mémoire pour garantir que la fonction de mise en cache intégrée met en cache les objets

```
set cache parameter -memLimit 600
```

Une fois la commande précédente exécutée, l'appliance négocie la mémoire pour la fonction de mise en cache intégrée et la mémoire disponible est affectée à la fonction. Cela permet à l'appliance de mettre en cache des objets sans redémarrer l'appliance.

1. Vérifier la valeur de la limite de mémoire

```
1           > show cache parameter
2                   Integrated cache global configuration:
3                   Memory usage limit: 600 Mbytes
4                   Memory usage limit (active value): 600 Mbytes
5                   Maximum value for Memory usage limit: 843 MBytes
6                   Via header: NS-CACHE-9.3:
7                   Verify cached object using: HOSTNAME_AND_IP
8                   Max POST body size to accumulate: 0 bytes
9                   Current outstanding prefetches: 0
10                  Max outstanding prefetches: 4294967295
11                  Treat NOCACHE policies as BYPASS policies: YES
12                  Global Undef Action: NOCACHE
13  <!--NeedCopy-->
```

> **Remarque :**
>
> 600 Mo de mémoire sont alloués à la fonction de mise en cache intégrée.

1. Enregistrez la configuration. Assurez-vous que la mémoire est automatiquement allouée à la fonctionnalité lors du redémarrage de l'appliance.
2. Vérifiez les limites de mémoire définies dans le fichier ns.conf à partir de l'invite shell

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

La mise en cache intégrée est désactivée et la mémoire cache est définie sur zéro

Dans ce scénario, lorsque vous démarrez l'appliance, la fonctionnalité de mise en cache intégrée est désactivée et la limite de mémoire globale est définie à zéro. Par conséquent, aucune mémoire n'est allouée à la mise en cache intégrée pendant le processus de démarrage.

Configuration à l'aide de l'interface de ligne de commande

1. Vérifiez les limites de mémoire définies dans le fichier ns.conf à partir de l'invite shell

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Vérifier la valeur de la limite de mémoire

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 0 Mbytes
4                  Maximum value for Memory usage limit: 843 MBytes
5                  Via header: NS-CACHE-9.3: 18
6                  Verify cached object using: HOSTNAME_AND_IP
7                  Max POST body size to accumulate: 0 bytes
8                  Current outstanding prefetches: 0
9                  Max outstanding prefetches: 4294967295
10                 Treat NOCACHE policies as BYPASS policies: YES
11                 Global Undef Action: NOCACHE
12 <!--NeedCopy-->
```

> **Remarque :**
>
> La limite de mémoire est définie sur 0 Mo et aucune mémoire n'est allouée à la fonction de mise

> en cache intégrée. De plus, lorsque vous exécutez une commande de configuration du cache, le message d'avertissement suivant s'affiche **: Avertissement : fonctionnalité non activée [IC]**.

1. Activer la fonctionnalité de mise en cache intégrée

```
enable ns feature IC
```

> **Remarque :**
>
> À ce stade, lorsque vous activez la fonctionnalité de mise en cache intégrée, l'appliance n'alloue pas de mémoire à la fonction. Par conséquent, aucun objet n'est mis en cache dans la mémoire. En outre, lorsque vous exécutez une commande de configuration du cache, le message d'avertissement suivant s'affiche : **Aucune mémoire n'est configurée pour le circuit intégré. Utilisez la commande set cache parameter pour définir la limite de mémoire.**

1. Définissez les limites de mémoire pour garantir que la fonction de mise en cache intégrée met en cache les objets

```
set cache parameter -memLimit 500
```

Une fois la commande précédente exécutée, l'appliance négocie la mémoire pour la fonction de mise en cache intégrée et la mémoire disponible est affectée à la fonction. L'appliance met en cache les objets sans redémarrer l'appliance.

> **Remarque :**
>
> L'ordre dans lequel vous activez la fonction et définissez les limites de mémoire est important. Si vous définissez les limites de mémoire avant d'activer la fonctionnalité, le message d'avertissement suivant s'affiche : **Avertissement : fonctionnalité non activée [IC]**.

1. Vérifier la valeur de la limite de mémoire

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 Mbytes
4                  Memory usage limit (active value): 500 Mbytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3:
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```


> **Remarque :**
>
> 500 Mo de mémoire sont alloués à la fonction de mise en cache intégrée.

1. Enregistrez la configuration

```
save config
```

1. Vérifiez les limites de mémoire définies dans le fichier ns.conf à partir de l'invite shell

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Modifier la limite de mémoire

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

Configuration des sélecteurs et des groupes de contenu de base

May 5, 2023

Vous pouvez configurer des sélecteurs et les appliquer à des groupes de contenus. Lorsque vous ajoutez un sélecteur à un ou plusieurs groupes de contenus, vous spécifiez si le sélecteur doit être utilisé pour identifier les demandes de cache ou pour identifier les objets mis en cache devant être invalidés (expirés). Les sélecteurs sont facultatifs. Vous pouvez également configurer des groupes de contenus pour utiliser des `hit` paramètres et des paramètres d'invalidation. Citrix vous recommande toutefois de configurer des sélecteurs.

Après avoir configuré des sélecteurs ou décidé d'utiliser des paramètres à la place, vous êtes prêt à configurer un groupe de contenus de base. Après avoir créé le groupe de contenu de base, vous devez décider comment les objets doivent expirer du cache et configurer l'expiration du cache. Vous pouvez modifier davantage le cache comme décrit dans Amélioration des performances du cache et Configuration des cookies, des en-têtes et des interrogations, mais vous pouvez tout d'abord configurer des stratégies de mise en cache.

> **Remarque**
>
> Les paramètres et les sélecteurs des groupes de contenus ne sont utilisés qu'au moment de la demande, et vous les associez généralement à des politiques qui utilisent les actions MAY_CACHE ou MAY_NOCACHE.

Avantages des sélecteurs

Un sélecteur est un filtre qui localise des objets particuliers dans un groupe de contenus. Si vous ne configurez pas de sélecteur, l'appliance Citrix® ADC recherche une correspondance exacte dans

le groupe de contenus. Cela peut entraîner la présence de plusieurs copies du même objet dans un groupe de contenus. Par exemple, un groupe de contenus qui ne possède pas de sélecteur peut avoir besoin de stocker les URL pour host1.domain.com \ mypage.htm, host2.domain.com \ mypage.htm et host3.domain.com \ mypage.htm. En revanche, un sélecteur peut faire correspondre uniquement l'URL (mypage.html, en utilisant l'expression http.req.url) et le domaine (.com, en utilisant l'expression http.req.hostname.domain), ce qui permet de satisfaire les demandes par la même URL.

Les expressions de sélection peuvent effectuer une simple mise en correspondance de paramètres (par exemple, pour rechercher des objets qui correspondent à quelques paramètres de chaîne de requête et à leurs valeurs). Une expression de sélection peut utiliser une logique booléenne, des opérations arithmétiques et des combinaisons d'attributs pour identifier des objets (par exemple, des segments d'un radical d'URL, une chaîne de requête, une chaîne dans le corps d'une requête POST, une chaîne dans un en-tête HTTP, un cookie). Les sélecteurs peuvent également exécuter des fonctions de programmation pour analyser les informations contenues dans une demande. Par exemple, un sélecteur peut extraire du texte dans un corps POST, convertir le texte en liste et extraire un élément spécifique de la liste.

Pour plus d'informations sur les expressions et sur ce que vous pouvez spécifier dans une expression, voir Stratégies et expressions.

Utiliser les paramètres au lieu de sélecteurs

Bien que Citrix recommande d'utiliser des sélecteurs avec un groupe de contenus, vous pouvez à la place configurer des `hit` paramètres et des paramètres d'invalidation. Supposons, par exemple, que vous configuriez trois `hit` paramètres dans un groupe de contenus pour les rapports de bogues : BugID, Issuer et Assignee. Si une demande contient BuGID=456, avec Issuer=RohiTV et Assignee=Robert, l'appliance NetScaler peut fournir des réponses qui correspondent à ces paires paramètre-valeur.

Les paramètres d'invalidation d'un groupe de contenus font expirer les entrées mises en cache. Supposons, par exemple, que BugID soit un paramètre d'invalidation et qu'un utilisateur envoie une requête POST pour mettre à jour un rapport de bogue. Une politique d'invalidation dirige la demande vers ce groupe de contenus, et le paramètre d'invalidation du groupe de contenus fait expirer toutes les réponses mises en cache qui correspondent à la valeur BugID. (La prochaine fois qu'un utilisateur enverra une requête GET pour ce rapport, une politique de mise en cache peut permettre à l'appliance NetScaler d'actualiser l'entrée mise en cache du rapport à partir du serveur d'origine.)

Notez que le même paramètre peut être utilisé comme `hit` paramètre ou comme paramètre d'invalidation.

Les groupes de contenus extraient les paramètres de demande dans l'ordre suivant :

- Requête d'URL

- Carrosserie POST
- En-tête du cookie

Après la première occurrence d'un paramètre, quel que soit son emplacement dans la requête, toutes ses occurrences suivantes sont ignorées. Par exemple, si un paramètre existe à la fois dans la requête URL et dans le corps POST, seul celui de la requête URL est pris en compte.

Si vous décidez d'utiliser des paramètres d'accès et d'invalidation pour un groupe de contenus, configurez les paramètres lors de la configuration du groupe de contenus.

Remarque : Citrix vous recommande d'utiliser des sélecteurs plutôt que des groupes de contenus paramétrés, car les sélecteurs sont plus flexibles et peuvent être adaptés à un plus grand nombre de types de données.

Configurer un sélecteur

Un groupe de contenus peut utiliser un sélecteur d'accès pour récupérer les accès du cache ou un sélecteur d'invalidation pour les objets mis en cache qui ont expiré et en récupérer de nouveaux sur le serveur d'origine.

Un sélecteur contient un nom et une expression logique, appelée *expression avancée*.

Pour plus d'informations sur les expressions avancées, voir Stratégies et expressions.

Pour configurer un sélecteur, vous lui attribuez un nom et entrez une ou plusieurs expressions. La meilleure pratique consiste à inclure le radical et l'hôte de l'URL dans une expression de sélection, sauf s'il existe une bonne raison de les omettre.

Pour configurer un sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add cache selector \<selectorName\> ( \<rule\> ... )
```

Pour plus d'informations sur la configuration de l'expression ou des expressions, reportez-vous à la section Pour configurer une expression de sélecteur à l'aide de l'interface de ligne de commande.

```
1 >add cache selector product_selector "http.req.url.query.value("
     ProductId")" "http.req.url.query.value("BatchNum")" "http.req.url.
     query.value("depotLocation")"
2
3 > add cache selector batch_selector "http.req.url.query.value("
     ProductId")" "http.req.url.query.value("BatchId")" "http.req.url.
     query.value("depotLocation")"
4
5 > add cache selector product_id_selector "http.req.url.query.value("
     ProductId")"
6
```



```
> add cache selector batchnum_selector "http.req.url.query.value("
    BatchNum")" "http.req.url.query.value("depotLocation")"

> add cache selector batchid_selector "http.req.url.query.value("
    depotLocation")" "http.req.url.query.value("BatchId")"

<!--NeedCopy-->
```

Pour configurer un sélecteur à l'aide de l'interface graphique

Accédez à **Optimisation > Mise en cache intégrée > Sélecteurs de cache, puis ajoutez le sélecteur**de cache.

Groupes de contenus

Un groupe de contenus est un conteneur pour les objets mis en cache qui peuvent être servis dans une réponse. Lorsque vous activez le cache intégré pour la première fois, les objets pouvant être mis en cache sont stockés dans un groupe de contenus nommé Default. Vous pouvez créer des groupes de contenus dotés de propriétés uniques. Par exemple, vous pouvez définir des groupes de contenus distincts pour les données d'image, les rapports de bogues et les cotations boursières, et vous pouvez configurer le groupe de contenus de cotation pour qu'il soit actualisé plus souvent que les autres groupes.

Vous pouvez configurer l'expiration de l'intégralité d'un groupe de contenus ou de certaines entrées d'un groupe de contenus.

Les données d'un groupe de contenus peuvent être statiques ou dynamiques, comme suit :

- **Groupes de contenus statiques**. Trouve une correspondance exacte entre le radical d'URL et le nom d'hôte de la demande et le radical d'URL et le nom d'hôte de la réponse.
- **Groupes de contenus dynamiques**. Recherche les objets qui contiennent des paires paramètre-valeur particulières, des chaînes arbitraires ou des modèles de chaîne particuliers. Les groupes de contenus dynamiques sont utiles pour mettre en cache des données fréquemment mises à jour (par exemple, un rapport de bogue ou une cotation boursière).

Répondre à une demande provenant d'un groupe de contenus

1. Un utilisateur saisit des critères de recherche pour un élément, tel qu'un rapport de bogue, puis clique sur le bouton Rechercher dans un formulaire HTML.
2. Le navigateur émet une ou plusieurs requêtes HTTP GET. Ces requêtes contiennent des paramètres (par exemple, le propriétaire du bogue, l'ID du bogue, etc.).
3. Lorsque l'appliance NetScaler reçoit les demandes, elle recherche une politique correspondante et, si elle trouve une politique de mise en cache qui correspond à ces demandes, elle dirige les demandes vers un groupe de contenus.

4. Le groupe de contenus recherche les objets appropriés dans le groupe de contenus, en fonction de critères que vous configurez dans un sélecteur.

Par exemple, le groupe de contenus peut récupérer les réponses qui correspondent `NameField=username and BugID=ID`.

1. Si elle trouve des objets correspondants, l'appliance NetScaler peut les transmettre au navigateur de l'utilisateur, où ils sont regroupés en une réponse complète (par exemple, un rapport de bogue).

Invalider un objet dans un groupe de contenus

1. Un utilisateur modifie des données (par exemple, l'utilisateur modifie le rapport de bogue et clique sur le bouton Soumettre).
2. Le navigateur envoie ces données sous la forme d'une ou de plusieurs requêtes HTTP. Par exemple, il peut envoyer un rapport de bogue sous la forme de plusieurs requêtes HTTP POST contenant des informations sur le propriétaire du bogue et l'identifiant du bogue.
3. L'appliance NetScaler compare les demandes aux politiques d'invalidation. Généralement, ces politiques sont configurées pour détecter la méthode HTTP POST.
4. Si la demande correspond à une politique d'invalidation, l'appliance NetScaler recherche le groupe de contenus associé à cette politique et fait expirer les réponses qui correspondent aux critères d'invalidation configurés.

Par exemple, un sélecteur d'invalidation peut trouver des réponses qui correspondent. `NameField=username and BugID=ID`

1. La prochaine fois que l'appliance NetScaler reçoit une requête GET pour ces réponses, elle récupère les versions actualisées depuis le serveur d'origine, met en cache les réponses actualisées et transmet ces réponses au navigateur de l'utilisateur, où elles sont rassemblées dans un rapport de bogue complet.

Configuration d'un groupe de contenus de base

Par défaut, toutes les données mises en cache sont stockées dans le groupe de contenus par défaut. Vous pouvez configurer d'autres groupes de contenus et spécifier ces groupes de contenus dans une ou plusieurs politiques.

Vous pouvez configurer des groupes de contenus pour du contenu statique et vous devez configurer des groupes de contenus pour du contenu dynamique. Vous pouvez modifier la configuration de n'importe quel groupe de contenus, y compris le groupe par défaut.

Pour configurer un groupe de contenus de base à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
add cache contentgroup <name> (-hitSelector <hitSelectorName> -invalSelector
 <invalidationSelectorName> | -hitParams <hitParamName> -invalParams<
invalidationParamName>)-type <type> [-relExpiry <sec> | -relExpiryMilliSec
<msec>] [-heurExpiryParam <positiveInteger>]

add cache contentgroup Products_Details -hitSelector product_selector -
invalSelector id_selector

add cache contentgroup bugrep -hitParams IssuePage RecordID Template
TableId -invalParams RecordID -relExpiry 864000
```

Pour configurer un groupe de contenus de base à l'aide de l'interface graphique

Accédez à **Optimisation > Mise en cache intégrée > Groupes de contenus**, puis créez le groupe de contenu.

Faire expirer ou vider les objets mis en cache

Si une réponse ne comporte pas d'en-tête Expires ou d'en-tête Cache-Control avec un délai d'expiration (Max-Age ou Smax-Age), vous devez faire expirer les objets d'un groupe de contenus en utilisant l'une des méthodes suivantes :

- Configurez les paramètres d'expiration du groupe de contenus pour déterminer si l'objet doit être conservé et pendant combien de temps.
- Configurez une stratégie d'invalidation et une action pour le groupe de contenus. Pour plus d'informations, voir Configuration des stratégies pour la mise en cache et l'invalidation.
- Expire manuellement le groupe de contenu ou les objets qu'il contient.

Après l'expiration d'une réponse mise en cache, l'appliance NetScaler l'actualise la prochaine fois que le client émet une demande de réponse. Par défaut, lorsque le cache est plein, l'appliance NetScaler remplace d'abord la réponse la moins récemment utilisée.

La liste suivante décrit les méthodes permettant d'expirer les réponses mises en cache à l'aide des paramètres d'un groupe de contenus. Généralement, ces méthodes sont spécifiées en pourcentage ou en secondes :

- **Manuel**. Invalidez manuellement toutes les réponses d'un groupe de contenus ou toutes les réponses du cache.
- Basé sur**les réponses.** Intervalles d'expiration spécifiques pour les réponses positives et négatives. L'expiration basée sur la réponse n'est prise en compte que si l'en-tête Last-Modified est absent de la réponse.
- **Expiration heuristique**. Pour les réponses comportant un en-tête Last-Modified, l'expiration heuristique indique le temps écoulé depuis la modification de la réponse (calculé comme l'heure actuelle moins l'heure de la dernière modification, multipliée par la valeur d'expiration heuristique). Par exemple, si un en-tête Last-Modified indique qu'une réponse a été mise à jour

il y a 2 heures et que le paramètre d'expiration heuristique est de 10 %, les objets mis en cache expirent après 0,2 heure. Cette méthode suppose que les réponses fréquemment mises à jour doivent expirer plus souvent.

- **Absolu ou relatif**. Spécifiez l'heure exacte (absolue) à laquelle la réponse expire chaque jour, au format HH:MM, heure locale ou GMT. L'heure locale peut ne pas fonctionner dans tous les fuseaux horaires.

L'expiration relative indique quelques secondes ou millisecondes entre le moment où un échec du cache entraîne un transfert vers le serveur d'origine et l'expiration de la réponse. Si vous spécifiez l'expiration relative en millisecondes, entrez un multiple de 10. Cette forme d'expiration fonctionne pour toutes les réponses positives. Les en-têtes Last-Modified, Expires et Cache-Control de la réponse sont ignorés.

L'expiration absolue et relative remplace toutes les informations d'expiration figurant dans la réponse elle-même.

- **En téléchargement**. L'option Expire après réception d'une réponse complète fait expirer une réponse lorsqu'elle est téléchargée. Cela est utile pour les réponses fréquemment mises à jour, par exemple les cotations boursières. Par défaut, cette option est désactivée.

L'activation de Flash Cache et l'option Expire après réception d'une réponse complète accélèrent les performances des applications dynamiques. Lorsque vous activez les deux options, l'appliance NetScaler ne récupère qu'une seule réponse pour un bloc de demandes simultanées.

- **Épinglé.** Par défaut, lorsque le cache est plein, l'appliance NetScaler remplace d'abord la réponse la moins récemment utilisée. L'appliance NetScaler n'applique pas ce comportement aux groupes de contenus marqués comme épinglés.

Si vous ne configurez pas les paramètres d'expiration pour un groupe de contenus, voici d'autres options pour faire expirer les objets du groupe :

- Configurez une politique avec une action INVAL qui s'applique au groupe de contenus.
- Entrez les noms des groupes de contenus lors de la configuration d'une politique qui utilise une action INVAL.

Comment les méthodes d'expiration sont appliquées

L'expiration fonctionne différemment pour les réponses positives et négatives. Les réponses positives et négatives sont décrites dans le tableau ci-dessous *intitulé Expiration des réponses positives et négatives* .

Les règles générales suivantes permettent de comprendre la méthode d'expiration appliquée à un groupe de contenus :

- Vous pouvez contrôler si l'appliance NetScaler évalue les en-têtes de réponse lorsqu'elle décide de faire expirer ou non un objet.

- L'expiration absolue et relative amène l'appliance NetScaler à ignorer les en-têtes de réponse (ils remplacent toutes les informations d'expiration contenues dans la réponse).
- Les paramètres d'expiration heuristiques et l'expiration « Faible positive » et « Faible négative » (étiquetés comme valeurs **par défaut** dans l'utilitaire de configuration) obligent l'appliance NetScaler à examiner les en-têtes de réponse. Ces paramètres fonctionnent ensemble comme suit :
  - La valeur d'un en-tête Expires ou Cache-Control remplace ces paramètres de groupe de contenus.
  - Pour les réponses positives dépourvues d'en-tête Expires ou Cache-Control mais comportant un en-tête Last-Modified, l'appliance NetScaler compare les paramètres d'expiration heuristiques à la valeur de l'en-tête.
  - Pour les réponses positives dépourvues d'en-tête Expires, Cache-Control ou Last-Modified, l'appliance NetScaler utilise la valeur « faible positive ».
  - Pour les réponses négatives dépourvues d'en-tête Expires ou Cache-Control, l'appliance NetScaler utilise la valeur « faible négative ».

Le tableau suivant décrit la manière dont ces méthodes sont appliquées.

Type de réponse	Type d'en-tête d'expiration	Paramètre du groupe de contenus	Période pendant laquelle l'objet reste dans le cache
Positif	N'importe quel en-tête	Faire expirer le contenu après (relExpiry) sans autres paramètres	Utilisez la valeur du paramètre **Expire le contenu après** .
Positif	N'importe quel en-tête	Expire le contenu à (absExpiration) sans autre paramètre	Soustrayez la date actuelle de la valeur du paramètre **Expire le contenu à** .
Positif	N'importe quel en-tête	Faire expirer le contenu après (relExpiry) et faire expirer le contenu à (absExpiry)	Utilisez la plus petite des deux valeurs pour les paramètres du groupe de contenus. Consultez les lignes précédentes de ce tableau.

Type de réponse	Type d'en-tête d'expiration	Paramètre du groupe de contenus	Période pendant laquelle l'objet reste dans le cache
Positif	Dernière modification (avec tout autre en-tête)	Heuristique (HeureExpiry Param) avec tout autre paramètre	Soustrayez la date de dernière modification de la date actuelle, multipliez le résultat par la valeur du paramètre d'expiration heuristique, puis divisez par 100.
Positif	Dernière modification (avec tout autre en-tête)	Valeur par défaut (positive) (WeakPosrel Expiration) et aucun autre paramètre	Utilisez la valeur du paramètre d'expiration par défaut (positif).
Positif	Expires ou Cache-Control : l'en-tête Max-Age est présent	L'en-tête Last-Modified est absent, heuristique (paramètre HeureExpiry), Default (positif) (WeakPosRel Expiration), ou les deux	Soustrayez la date actuelle de la date d'expiration ou de la `Cache-Control: Max-Age` date.
Positif	pas d'en-têtes de mise en cache	Valeur par défaut (positive) (WeakPosrel Expiration) et tout autre paramètre d'expiration	Utilisez la valeur du paramètre Par défaut (positif).

Type de réponse	Type d'en-tête d'expiration	Paramètre du groupe de contenus	Période pendant laquelle l'objet reste dans le cache
Positif	pas d'en-têtes de mise en cache	L'heuristique (paramètre HeureExpiry) est présente, le paramètre par défaut (positif) (WeakPosRel Expiration) est absent.	Si l'en-tête Last-Modified est absent, la réponse n'est pas mise en cache ou elle est mise en cache avec le statut Déjà expiré. Si l'en-tête Last-Modified est présent, utilisez la valeur d'expiration heuristique.
Négatif	Expire ou `Cache-Control:Max-Age`	Expire le contenu après (relExpiry), Expire le contenu à (absExpiry) ou les deux paramètres	Soustrayez la date actuelle de la valeur de l'en-tête Expires ou utilisez la valeur de l'en-tête Cache-Control:Max-Age.
Négatif	Les en-têtes Expire ou Cache-Control sont absents	Expire le contenu après (relExpiry), Expire le contenu à (absExpiry) ou les deux paramètres	La réponse n'est pas mise en cache ou est mise en cache avec le statut Déjà expiré.
Négatif	Expire ou `Cache-Control:Max-Age`	N'importe quel réglage	Soustrayez la date actuelle de la `Cache-Control:Max-Age` date d'expiration.
Négatif	Les en-têtes Expires et Cache-Control:Max-Age sont absents	Par défaut (négatif) (expiration de WeakNegrel)	Utilisez la valeur du paramètre Par défaut (négatif).
Négatif	Les en-têtes Expires et Cache-Control:Max-Age sont absents	Tout paramètre autre que celui par défaut (négatif) (expiration de WeakNegrel)	L'objet n'est pas mis en cache ou est mis en cache avec le statut Déjà expiré.

Faire expirer un groupe de contenus par une méthode manuelle

Vous pouvez faire expirer manuellement toutes les entrées d'un groupe de contenus.

Pour faire expirer manuellement toutes les réponses d'un groupe de contenus à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
expire cache contentGroup <name>
```

Pour faire expirer manuellement toutes les réponses d'un groupe de contenus à l'aide de l'interface graphique

Accédez à **Optimisation > Mise en cache intégrée > Groupes de contenus**, sélectionnez le groupe de contenus et cliquez sur Invalider pour faire expirer toutes les réponses d'un groupe de contenus.

Pour faire expirer manuellement toutes les réponses du cache à l'aide de l'interface graphique

Accédez à **Optimisation > Mise en cache intégrée > Groupes de contenus**, puis cliquez sur Tout annuler pour faire expirer toutes les réponses du cache.

Configurer l'expiration périodique d'un groupe de contenus

Vous pouvez configurer un groupe de contenus pour qu'il exécute une expiration sélective ou complète de ses entrées. L'intervalle d'expiration peut être fixe ou relatif.

Pour configurer l'expiration d'un groupe de contenus à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cache contentgroup \<name> (-relExpiry|-relExpiryMilliSec|-absExpiry
|-absExpiryGMT| -heurExpiryParam|-weakPosRelExpiry|-weakNegRelExpiry| -
expireAtLastBye)\<expirationValue>
```

Pour configurer l'expiration d'un groupe de contenus à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenus**, sélectionnez le groupe de contenus et spécifiez la méthode d'expiration.

Faire expirer les réponses individuelles

L'expiration d'une réponse force l'appliance NetScaler à récupérer une copie actualisée depuis le serveur d'origine. Les réponses qui ne possèdent pas de validateur, par exemple, `ETag` ou d'en-têtes Last-Modified, ne peuvent pas être revalidées. Par conséquent, le fait de supprimer ces réponses a le même effet que de les faire expirer.

Pour faire expirer une réponse mise en cache dans un groupe de contenus pour des données statiques, vous pouvez spécifier une URL qui doit correspondre à l'URL stockée. Si la réponse mise en cache fait

partie d'un groupe de contenu paramétré, vous devez spécifier le nom du groupe et la racine d'URL exacte. Le nom d'hôte et le numéro de port doivent être identiques à ceux figurant dans l'en-tête de requête HTTP de l'hôte de la réponse mise en cache. Si le port n'est pas spécifié, le port 80 est supposé.

Pour faire expirer les réponses individuelles d'un groupe de contenus à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
expire cache object -url <URL> -host <hostName> [-port <port>] [-groupName<
contentGroupName>] [-httpMethod GET|POST]
```

Pour faire expirer les réponses individuelles d'un groupe de contenus à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
expire cache object -locator <positiveInteger>
```

Pour faire expirer une réponse mise en cache à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets en cache**, sélectionnez la réponse mise en cache et expirez.

Pour faire expirer une réponse à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets en cache**, cliquez sur **Rechercher** et définissez les critères de recherche pour trouver la réponse mise en cache requise et expirer.

Effacement des réponses dans un groupe de contenus

Vous pouvez supprimer ou vider toutes les réponses d'un groupe de contenus, certaines réponses d'un groupe ou toutes les réponses du cache. L'effacement d'une réponse mise en cache libère de la mémoire pour les nouvelles réponses mises en cache.

> **Remarque :**
>
> Pour vider les réponses de plusieurs objets à la fois, utilisez la méthode de l'utilitaire de configuration. L'interface de ligne de commande ne propose pas cette option.

Pour vider les réponses d'un groupe de contenus à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
flush cache contentGroup <name> [-query <queryString> | [-selectorValue <
selectorExpressionIDList> -host <hostName>]]
```

Pour effacer les réponses d'un groupe de contenus à l'aide de l'interface graphique

1. Accédez à **Optimisation** > Mise en **cache intégrée** > **Groupes de contenus**.

2. Dans le volet de détails, videz les réponses comme suit :
    - Pour vider toutes les réponses de tous les groupes de contenus, cliquez sur Tout annuler et videz toutes les réponses.
    - Pour effacer les réponses d'un groupe de contenus particulier, sélectionnez le groupe de contenus, cliquez sur **Invalider**et videz toutes les réponses.

> **Remarque** :
> Si ce groupe de contenus utilise un sélecteur, vous pouvez effacer les réponses de manière sélective en saisissant une chaîne dans la zone de texte Valeur du sélecteur et en saisissant un nom d'hôte dans la zone de texte Hôte. Cliquez ensuite sur **Flush et OK**. La valeur du sélecteur peut être une chaîne de requête de 2 319 caractères maximum utilisée pour l'invalidation paramétrée.

Si le groupe de contenus utilise un paramètre d'invalidation, vous pouvez effacer les réponses de manière sélective en saisissant une chaîne dans le champ **Requête** .

Si le groupe de contenus utilise un paramètre d'invalidation et que des objets d'invalidation appartenant à l'hôte cible sont configurés, entrez des chaînes dans les champs **Requête et Hôte** .

Pour vider une réponse mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
flush cache object -locator <positiveInteger> | -url <URL> -host <hostName>
 [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET|POST]
```

Pour vider une réponse mise en cache à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets en cache**, sélectionnez l'objet en cache et videz.

Supprimer un groupe de contenus

Vous pouvez supprimer un groupe de contenus s'il n'est utilisé par aucune politique stockant les réponses dans le cache. Si le groupe de contenus est lié à une politique, vous devez d'abord supprimer cette politique. La suppression du groupe de contenus entraîne la suppression de toutes les réponses stockées dans ce groupe.

Vous ne pouvez pas supprimer le groupe Default, BASEFILE ou Deltas. Le groupe par défaut stocke les réponses mises en cache qui n'appartiennent à aucun autre groupe de contenus.

Pour supprimer un groupe de contenus à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm cache contentgroup <name>
```

Pour supprimer un groupe de contenus à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu,** sélectionnez le groupe de contenu et supprimez.

Configuration des stratégies de mise en cache et d'invalidation

May 5, 2023

Les politiques permettent au cache intégré de déterminer s'il convient d'essayer de fournir une réponse à partir du cache ou de l'origine. L'appliance NetScaler fournit des politiques intégrées pour la mise en cache intégrée, et vous pouvez configurer d'autres politiques. Lorsque vous configurez une politique, vous l'associez à une action. Une action met en cache les objets auxquels la politique s'applique ou invalide (fait expirer) les objets. En général, vous basez les politiques de mise en cache sur les informations contenues dans les requêtes GET et POST. Vous basez généralement les politiques d'invalidation sur la présence de la méthode POST dans les demandes, ainsi que sur d'autres informations. Vous pouvez utiliser n'importe quelle information contenue dans une requête GET ou POST dans une politique de mise en cache ou d'invalidation.

Vous pouvez consulter certaines des politiques intégrées dans le nœud Politiques du cache intégré dans l'utilitaire de configuration. Les noms des politiques intégrés commencent par un trait de soulignement (_).

Les actions déterminent ce que fait l'appliance NetScaler lorsque le trafic correspond à une politique. Les actions suivantes sont disponibles :

- **Actions de mise en cache**. Les politiques que vous associez à l'action CACHE stockent les réponses dans le cache et les diffusent à partir du cache.
- **Actions d'invalidation**. Les politiques que vous associez à l'action INVAL font immédiatement expirer les réponses mises en cache et les actualisent depuis le serveur d'origine. Pour les applications Web, les politiques d'invalidation évaluent souvent les requêtes POST.
- **Actions « Ne pas mettre en cache »**. Les politiques que vous associez à une action NOCACHE ne stockent jamais d'objets dans le cache.
- Les**actions sont mises en cache provisoirement**. Les stratégies que vous associez à une action MAYCACHE ou MAYNOCACHE dépendent du résultat de plusieurs évaluations de stratégies.

Bien que le cache intégré ne stocke pas les objets spécifiés par la méthode LOCK, vous pouvez invalider les objets mis en cache à la réception d'une `LOCK` demande. Pour les stratégies d'invalidation uniquement, vous pouvez spécifier `LOCK` en tant que méthode à l'aide de l'expression `http.req.method.eq( "lock" )`. Contrairement aux stratégies `GET` et aux `POST` requêtes, vous devez mettre la méthode LOCK entre guillemets car l'appliance NetScaler reconnaît ce nom de méthode comme une chaîne uniquement.

Après avoir créé une stratégie, vous la liez à un point particulier dans le traitement global des demandes et des réponses. Bien que vous créez une stratégie avant de la lier, vous devez comprendre comment les points de liaison affectent l'ordre de traitement avant de créer vos stratégies.

Les polices liées à un point de liaison particulier constituent une banque de polices. Vous pouvez utiliser les expressions goto pour modifier l'ordre d'exécution dans une banque de règles. Vous pouvez également invoquer des stratégies dans d'autres banques de stratégies. En outre, vous pouvez créer des étiquettes et y lier des politiques. Une telle étiquette n'est pas associée à un point de traitement, mais les politiques qui y sont liées peuvent être invoquées à partir d'autres banques de politiques.

Actions à associer aux politiques de mise en cache intégrées

Le tableau suivant décrit les actions relatives aux politiques de mise en cache intégrées.

Action	Spécifications
CACHE	Sert une réponse à partir du cache si la réponse n'a pas expiré. Si la réponse doit être récupérée depuis le serveur d'origine, l'appliance NetScaler la met en cache avant de la diffuser. Même les données fréquemment mises à jour et consultées peuvent être mises en cache. Par exemple, les cours boursiers sont fréquemment mis à jour, mais ils peuvent être mis en cache afin de pouvoir être rapidement diffusés à plusieurs utilisateurs. Si nécessaire, les données mises en cache peuvent être actualisées immédiatement après leur téléchargement. Une action CACHE peut être remplacée par des politiques intégrées.
PAS DE CACHE	Récupère toujours la réponse depuis le serveur d'origine et marque la réponse comme non stockable. Vous configurez généralement les politiques NOCACHE pour les données sensibles ou personnalisées.

Action	Spécifications
MAY_CACHE	Utilisé dans une politique de temps de demande, ce paramètre permet provisoirement de stocker une réponse dans un groupe de contenus, en attendant l'évaluation des politiques de temps de réponse. Les options suivantes sont possibles : 1. Si une politique de temps de réponse correspondante comporte une action CACHE mais ne spécifie pas de groupe de contenus, la réponse est stockée dans le groupe par défaut à moins que les politiques intégrées ne remplacent cette politique. 2. Si une politique de temps de réponse correspondante comporte une action CACHE et spécifie le même groupe de contenus que celui indiqué dans la politique de temps de demande, la réponse est stockée dans le groupe de contenus nommé à moins que les politiques intégrées ne remplacent cette politique. 3. Si une politique de temps de réponse correspondante comporte une action CACHE mais spécifie un groupe de contenu différent de celui indiqué dans la politique de temps de demande, une action NOCACHE est appliquée. 4. Si une politique de temps de réponse correspondante comporte une action NOCACHE, effectuez une action NOCACHE. 5. S'il n'existe pas de politique de temps de réponse correspondante, une action CACHE est appliquée, à moins qu'une politique intégrée ne remplace cette politique.

Action	Spécifications
PEUT_NOCACHE	Dans le cas d'une politique de délai de demande, ce paramètre empêche provisoirement la mise en cache de la réponse. Au moment de la réponse, l'une des actions suivantes est prise : - Si aucune politique de temps de réponse ne correspond à la demande, l'action finale est NOCACHE. - Si une politique de temps de réponse correspondante contient une action CACHE, l'action finale est CACHE, sauf si les politiques intégrées remplacent cette politique. - Si une politique de temps de réponse correspondante contient une action NOCACHE, l'action finale est NOCACHE. -Si une politique de temps de réponse correspondante comporte une action CACHE mais ne spécifie pas de groupe de contenus, la dernière action consiste à mettre en cache la réponse dans le groupe de contenus par défaut, à moins que les politiques intégrées ne remplacent cette politique.
INVAL	Expire les réponses mises en cache. Selon la façon dont la politique et le groupe de contenus sont configurés, toutes les réponses d'un ou de plusieurs groupes de contenus ont expiré ou les objets sélectionnés dans le groupe de contenus ont expiré. Remarque : Vous pouvez spécifier les actions INVAL uniquement dans les politiques relatives au temps de demande.

Points d'ancrage d'une politique

Vous pouvez lier la politique à l'un des points de liaison suivants :

- **Une banque de politiques mondiales**. Il s'agit des banques de stratégies par défaut, de remplacement de l'heure de demande, de temps de réponse par défaut et de remplacement du temps de réponse, comme décrit dans « Ordre d'évaluation des stratégies ». «

- **Un serveur virtuel**. Les stratégies que vous liez à un serveur virtuel sont traitées après les stratégies globales de remplacement et avant les stratégies globales par défaut, comme décrit dans « Ordre d'évaluation des stratégies ». « Lorsque vous liez une stratégie à un serveur virtuel, vous la liez au traitement de la demande ou du temps de réponse.
- **Une étiquette de politique ad hoc**. Une étiquette de stratégie est un nom attribué à une banque de stratégies. Outre les étiquettes globales, le cache intégré comporte deux étiquettes de politique personnalisées intégrées :
  - _reqBuiltInDefaults. Par défaut, cette étiquette de stratégie est invoquée à partir de la banque de stratégies par défaut au moment de la demande.
  - _resBuiltInDefaults. Cette étiquette de stratégie, par défaut, est invoquée à partir de la banque de stratégies par défaut en matière de temps de réponse.

Vous pouvez également définir de nouvelles étiquettes de politique. Les politiques liées à une étiquette de politique définie par l'utilisateur doivent être appelées depuis une banque de stratégies pour l'un des points de liaison intégrés.

> **Important :**
> Vous devez lier une politique comportant une action INVAL à un point de liaison de dérogation au moment de la demande ou au moment de la réponse. Pour supprimer une politique, vous devez d'abord la dissocier.

Ordre d'évaluation des politiques

Pour qu'une politique avancée entre en vigueur, vous devez vous assurer qu'elle est invoquée à un moment donné pendant le traitement du trafic par l'appliance NetScaler. Pour spécifier l'heure d'appel, vous associez la politique à un point de liaison. Les points de fixation sont les suivants, classés par ordre d'évaluation :

- **Dépassement de l'heure de la demande**. Si une demande correspond à une politique de dérogation au moment de la demande, par défaut, l'évaluation de la politique au moment de la demande prend fin et l'appliance NetScaler enregistre l'action associée à la politique correspondante.
- **Serveur virtuel d'équilibrage de charge au moment de**la demande. Si l'évaluation des politiques ne peut pas être terminée une fois que toutes les politiques de remplacement du temps de demande ont été évaluées, l'appliance NetScaler traite les politiques de délai de demande qui sont liées aux serveurs virtuels d'équilibrage de charge. Si la demande correspond à l'une de ces politiques, l'évaluation prend fin et l'appliance NetScaler enregistre l'action associée à la politique correspondante.
- **Serveur virtuel de commutation de contenu au moment**de la demande. Les politiques liées à ce point de liaison sont évaluées après les politiques de temps de demande liées aux serveurs virtuels d'équilibrage de charge.

- **Heure de demande par défaut.** Si l'évaluation des politiques ne peut pas être terminée après tout le temps de demande, les politiques spécifiques au serveur virtuel sont évaluées, l'appliance NetScaler traite les politiques par défaut au moment de la demande. Si la demande correspond à une politique par défaut au moment de la demande, l'évaluation de la politique au moment de la demande prend fin par défaut et l'appliance NetScaler enregistre l'action associée à la politique correspondante.
- **Dérobage du temps de réponse**. Similaire à l'évaluation de la politique de dérogation au moment de la demande.
- Serveur**virtuel d'équilibrage de charge en temps de réponse**. Similaire à l'évaluation de la politique de serveur virtuel au moment de la demande.
- Serveur**virtuel de commutation de contenu en temps de réponse**. Similaire à l'évaluation de la politique de serveur virtuel au moment de la demande.
- **Temps de réponse par défaut.** Similaire à l'évaluation de la politique par défaut au moment de la demande.

Vous pouvez associer plusieurs politiques à chaque point de liaison. Pour contrôler l'ordre d'évaluation des politiques associées au point de liaison, vous devez configurer un niveau de priorité. En l'absence de toute autre information sur le contrôle des flux, les stratégies sont évaluées en fonction du niveau de priorité, en commençant par la valeur de priorité numérique la plus faible.

> **Remarque :**
> les politiques de temps de demande pour les données POST ou les en-têtes de cookie doivent être invoquées lors de l'évaluation du remplacement du moment de la demande, car les stratégies de temps de demande intégrées dans le cache intégré renvoient une `NOCACHE` action pour les demandes POST et une `MAY_NOCACHE` action pour les demandes contenant des cookies. Vous devez associer `MAY_CACHE` ou `MAY_NOCACHE` effectuer des actions à une stratégie de temps de demande pointant vers un groupe de contenu paramétré. La stratégie de temps de réponse détermine si la transaction est stockée dans le cache.

Configurer une stratégie de mise en cache intégrée

Vous configurez de nouvelles stratégies pour gérer les données que les stratégies intégrées ne peuvent pas traiter. Vous configurez des politiques distinctes pour la mise en cache, pour empêcher la mise en cache et pour invalider les données mises en cache. Les principaux éléments d'une politique de mise en cache intégrée sont les suivants :

- Règle : expression logique qui évalue une requête ou une réponse HTTP.
- Action : vous associez une politique à une action afin de déterminer ce qu'il convient de faire avec une demande ou une réponse qui correspond à la règle de politique.

Groupes de contenus : vous associez la politique à un ou plusieurs groupes de contenus pour identifier l'endroit où l'action doit être exécutée.

Pour configurer une politique de mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add cache policy <policyName> -rule <expression> -actionCACHE|MAY_CACHE
|NOCACHE|MAY_NOCACHE [-storeInGroup <contentGroupName>] [-undefAction
NOCACHE|RESET]
> add cache policy image_cache -rule "http.req.url.contains(\"jpg\")|| http
.req.url.contains(\"jpeg\")"-action CACHE -storeingroup myImages_group -
undefaction NOCACHE

> add cache policy bugReportPolicy -rule "http.req.url.query.contains(\"
IssuePage\")"-action CACHE -storeInGroup bugReportGroup

> add cache policy my_form_policy -rule "http.req.header(\"Host\")contains
(\"my.company.com\")&& http.req.method.eq(\"GET\")&& http.req.url.query.
contains(\"v=7\")"-action CACHE -storeInGroup my_form_event

> add cache policy viewproducts_policy -rule "http.req.url.contains(\"
viewproducts.aspx\")"-action CACHE -storeInGroup Product_Details
```

Pour configurer une politique d'invalidation à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add cache policy <policyName> -rule <expression> -action INVAL [-
    invalObjects "<contentGroupName1>[,<selectorName1>"]. . .]] | [-
    invalGroup <contentGroupName1>[, <contentGroupName2>. . .]] [-
    undefAction NOCACHE|RESET]
<!--NeedCopy-->
```

```
> add cache policy invalidation_events_policy -rule "http.req.header("
    Host")contains("my.company.com") && http.req.method.eq("GET") &&
    http.req.url.query.contains("v=8") -action INVAL -invalObjects
    my_form_event -undefaction NOCACHE
<!--NeedCopy-->
```

```
> add cache policy inval_all -rule "http.req.method.eq("POST") && http.
    req.url.contains("jpeg")" -action INVAL -invalGroups myImages_group
    myApps_group PDF_group
<!--NeedCopy-->
```

```
> add cache policy bugReportInvalidationPolicy -rule "http.req.url.
    query.contains("TransitionForm")" -action INVAL -invalObjects
    bugReport`
```



```
`> add cache policy editproducts_policy -rule "http.req.url.contains("
   editproducts.aspx")" -action INVAL -invalObjects "Product_Details,
   batchnum_sel" "Products_In_Depots,batchid_sel"
<!--NeedCopy-->
```

Pour configurer une politique de mise en cache ou d'invalidation à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Politiques**, puis créez la nouvelle politique.

Politique de mise en cache intégrée contraignante à l'échelle mondiale

Lorsque vous liez globalement une stratégie, elle est disponible pour tous les serveurs virtuels de l'appliance NetScaler.

Pour lier une stratégie de mise en cache intégrée globalement à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
bind cache global <policy> -priority <positiveInteger> [-
   typeREQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT] [-
   gotoPriorityExpression <expression>] [-invoke <labelType> <labelName
   >]
<!--NeedCopy-->
```

```
> bind cache global myCachePolicy -priority 100 -type req_default
<!--NeedCopy-->
```

> **Remarque :**
>
> L'argument type est facultatif pour les stratégies liées globalement, afin de maintenir une compatibilité descendante avec les stratégies que vous avez définies à l'aide de versions antérieures de l'appliance NetScaler. Si vous omettez le type, la politique est liée à REQ_DEFAULT ou RES_DEFAULT, selon que la règle de politique est une expression de temps de réponse ou de demande. Si la règle contient à la fois des paramètres de temps de demande et de temps de réponse, elle est liée à RES_DEFAULT. Voici un exemple de liaison qui omet le type

Vous trouverez ci-dessous un exemple de liaison qui omet le type.

```
> bind cache global myCache Policy 200
```

Pour lier une politique de mise en cache intégrée de manière globale à l'aide de l'utilitaire de configuration

Accédez à **Optimisation** > Mise en **cache intégrée**, cliquez sur **Gestionnaire de politiques de cache** et liez les politiques en spécifiant le point de liaison et le type de connexion pertinents (demande/réponse).

Liez une politique de mise en cache intégrée à un serveur virtuel

Lorsque vous liez une stratégie à un serveur virtuel, elle est disponible uniquement pour les demandes et réponses qui correspondent à la stratégie et qui passent par le serveur virtuel concerné.

Lorsque vous utilisez l'interface graphique, vous pouvez lier la stratégie à l'aide de la boîte de dialogue de configuration du serveur virtuel. Cela vous permet de visualiser toutes les politiques de tous les modules NetScaler liés à ce serveur virtuel. Vous pouvez également utiliser la boîte de dialogue de **configuration de Policy Manager** pour le cache intégré. Cela vous permet d'afficher uniquement les stratégies de mise en cache intégrées qui sont liées au serveur virtuel.

Pour lier une stratégie de mise en cache intégrée à un serveur virtuel à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
bind lb vserver <name>@ -policyName <policyName> -priority <
   positiveInteger> -type(REQUEST|RESPONSE)
<!--NeedCopy-->
```

```
bind cs vserver <name>@ -policyName <policyName> -priority <
   positiveInteger> -type(REQUEST|RESPONSE)
<!--NeedCopy-->
```

Pour lier une politique de mise en cache intégrée à un serveur virtuel à l'aide de l'utilitaire de configuration (méthode du serveur virtuel)

- Serveur virtuel CS : accédez à **Gestion du trafic > Commutation de contenu > Serveurs virtuels**, sélectionnez le serveur virtuel et liez les politiques de cache pertinentes.
- LB Virtual Server - Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, sélectionnez le serveur virtuel et liez les stratégies de cache pertinentes.

Pour lier une stratégie de mise en cache intégrée à un serveur virtuel à l'aide de l'interface graphique (méthode Policy Manager).

Accédez à **Optimisation** > **Mise en cache intégrée, cliquez sur Gestionnaire de stratégies** de cache et liez les stratégies de cache en spécifiant le point de liaison et le type de connexion appropriés.

> **Remarque :**
> Vous pouvez lier des stratégies de cache à la fois au serveur virtuel d'équilibrage de charge et au serveur virtuel de commutation de contenu en sélectionnant le point de liaison approprié.

Comment mettre en cache les versions compressées et non compressées d'un fichier

Par défaut, un client capable de gérer la compression peut recevoir des réponses non compressées ou des réponses compressées au format gzip, deflate, compress et pack200-gzip. Si le client gère la

compression, un en-tête de `Accept-Encoding:compression` format est envoyé dans la demande. Le type de compression accepté par le client doit correspondre au type de compression de l'objet mis en cache. Par exemple, un `cached.gzip` fichier ne peut pas être diffusé en réponse à une demande comportant un `Accept-Encoding:deflate` en-tête.

Un client qui ne peut pas gérer la compression se voit attribuer un échec de cache si la réponse mise en cache est compressée.

Pour la mise en cache dynamique, vous devez configurer deux groupes de contenu, l'un pour les données compressées et l'autre pour les versions non compressées des mêmes données. Voici un exemple de configuration des sélecteurs, des groupes de contenu et des stratégies pour la distribution de fichiers non compressés du cache à des clients qui ne peuvent pas gérer la compression et de servir des versions compressées des mêmes fichiers au client capable de gérer la compression.

```
add cache selector uncompressed_response_selector http.req.url "http.req.
header(\"Host\")"

add cache contentGroup uncompressed_group -hitSelector uncompressed_responst_selector
 -invalSelector uncomp_resp_sel

add cache policy cache_uncompressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\")&&
 !HTTP.REQ.HEADER(\"Accept-Encoding\").EXISTS"-action CACHE -storeInGroup
uncompressed_group

bind cache global cache_uncompressed -priority 100 -gotoPriorityExpression
END -type REQ_OVERRIDE

add cache selector compressed_response_selector HTTP.REQ.URL "HTTP.REQ.
HEADER(\"Host\")""HTTP.REQ.HEADER(\"Accept-Encoding\")"

add cache contentGroup compressed_group -hitSelector compressed_response_selector


add cache policy cache_compressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\")&&
 HTTP.REQ.HEADER(\"Accept-Encoding\").EXISTS"-action CACHE -storeInGroup
compressed_group

bind cache global cache_compressed -priority 200 -gotoPriorityExpression
END -type REQ_OVERRIDE
```

Configurer une banque de stratégies pour la mise en cache

Toutes les politiques associées à un point de référence particulier sont regroupées sous le nom de banque de stratégies. Outre la configuration des niveaux de priorité pour les politiques d'une banque, vous pouvez modifier l'ordre d'évaluation dans une banque en configurant des expressions Goto. Vous pouvez modifier davantage l'ordre d'évaluation en appelant une banque de stratégies externe depuis

la banque de stratégies actuelle. Vous pouvez également configurer de nouvelles banques de politiques auxquelles vous attribuez vos propres étiquettes. Comme ces banques de politiques ne sont liées à aucun point du cycle de traitement, elles ne peuvent être invoquées qu'à partir d'autres banques de politiques. Pour plus de commodité, les banques de stratégies dont les étiquettes ne correspondent pas à un point de liaison intégré sont appelées étiquettes de stratégie.

En plus de contrôler l'ordre d'évaluation des stratégies en liant la stratégie et en attribuant un niveau de priorité, comme décrit dans « Politiques de liaison », vous pouvez établir le flux au sein d'une banque de stratégies en configurant une expression Goto. Une expression Goto remplace le flux déterminé par les niveaux de priorité. Vous pouvez également contrôler le flux d'évaluation en appelant une banque de règles externe après avoir évalué une entrée dans la banque actuelle. L'évaluation revient toujours à la banque actuelle une fois l'évaluation terminée.

Le tableau suivant récapitule les entrées permettant de contrôler l'évaluation dans une banque de politiques.

Attribut	Spécifie
Nom	Le nom d'une politique ou, pour appeler une autre banque de stratégies sans évaluer la politique, le mot clé NOPOLICY. Vous pouvez spécifier NOPOLICY plusieurs fois dans une banque de stratégies, mais vous ne pouvez spécifier une politique nommée qu'une seule fois.
Priority	Un entier. Plus le nombre entier est faible, plus la priorité est élevée.

Attribut	Spécifie
Aller à Expression	Détermine la politique ou la banque de stratégies suivante à évaluer. Vous pouvez fournir l'une des valeurs suivantes : 1. SUIVANT : Accédez à la politique dont la priorité est immédiatement supérieure. 2. FIN : Arrête l'évaluation. 3. USE_INVOCATION_RESULT : Applicable si cette entrée fait appel à une autre banque de politiques. Si le dernier Goto de la banque invoquée a la valeur END, l'évaluation s'arrête. Si le Goto final est autre que END, la banque de politiques actuelle exécute une commande NEXT. 4. Nombre positif : numéro de priorité de la prochaine politique à évaluer. 5. Expression numérique : expression qui produit le numéro de priorité de la prochaine politique à évaluer. Le Goto ne peut aller de l'avant que dans une banque de polices. Omettre l'expression Goto revient à spécifier END.
Type d'appel	Désigne un type de banque de politiques. La valeur peut être l'une des suivantes : 1. Demander un serveur virtuel : invoque les politiques de temps de demande associées à un serveur virtuel. 2. Serveur virtuel de réponse : invoque les politiques de temps de réponse associées à un serveur virtuel. 3. Libellé de stratégie : appelle une autre banque de stratégies, identifiée par l'étiquette de stratégie de la banque.
Nom de l'invocation	Nom d'un serveur virtuel ou étiquette de politique, selon la valeur que vous avez spécifiée pour le type d'appel.

Le cache intégré comporte deux étiquettes de stratégie intégrées et vous pouvez configurer d'autres étiquettes de stratégie :

`_reqBuiltInDefaults`: cette étiquette de stratégie est appelée à partir du point de liaison par dé-

faut de l'heure de la demande.
_resBuiltInDefaults: cette étiquette de stratégie est appelée à partir du point de liaison par défaut du temps de réponse.

Pour appeler une étiquette de stratégie dans une banque de stratégies de mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind cache policylabel <labelName> -policname<policyName> -priority<
    priority> [-gotoPriorityExpression <gotoprioritыExpression>] [-
    invoke <labelType> <labelName>]
<!--NeedCopy-->
```

Pour appeler une étiquette de stratégie dans une banque de stratégies de mise en cache à l'aide de l'interface graphique :

1. Accédez à **Optimisation** > **Mise en cache intégrée, cliquez sur Gestionnaire de stratégies** de cache, puis spécifiez le point de liaison approprié (Remplacer Global ou Global par défaut) et le type de connexion pour afficher la liste des stratégies liées à ce point de liaison.
2. Si vous souhaitez invoquer une étiquette de stratégie sans évaluer une politique, cliquez sur **NOPOLICY**.

> **Remarque :**
>
> Pour appeler une banque de stratégies externe, cliquez sur le champ de la colonne Type d'appel, puis sélectionnez le type de banque de stratégies que vous souhaitez appeler à ce stade dans la banque de stratégies. Il peut s'agir d'un label global ou d'une banque de serveurs virtuels. Dans le champ Nom d'appel, entrez l'étiquette ou le nom du serveur virtuel.

Pour invoquer une étiquette de politique de mise en cache dans une banque de règles de serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind lb vserver <name>@ -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```

```
bind cs vserver <name> -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```


Pour invoquer une étiquette de politique de mise en cache dans une banque de règles de serveur virtuel à l'aide de l'interface graphique

1. **Accédez à**Gestion du trafic**> Équilibrage de**charge/Commutation de contenu**>**Serveurs virtuels**, sélectionnez le serveur virtuel et cliquez sur Politiques.**
2. Si vous configurez une entrée existante dans cette banque, ignorez cette étape. Si vous ajoutez une nouvelle stratégie à cette banque de stratégies ou si vous souhaitez utiliser l'entrée NOPOLICY « factice », cliquez sur **Ajouter** et effectuez l'une des opérations suivantes :
   - Pour configurer une nouvelle stratégie, cliquez sur Cache et configurez la nouvelle stratégie comme décrit dans Configuration d'une stratégie dans le cache intégré.
   - Pour appeler une banque de stratégies sans traiter de règle de stratégie, sélectionnez l'`NOPOLICY-CACHE` option.

> **Remarque :**
>
> Pour appeler une banque de stratégies externe, cliquez sur le champ de la colonne Type d'appel, puis sélectionnez le type de banque de stratégies que vous souhaitez appeler à ce stade dans la banque de stratégies. Il peut s'agir d'un label global ou d'une banque de serveurs virtuels. Dans le champ Nom d'appel, entrez l'étiquette ou le nom du serveur virtuel.

Configuration d'une étiquette de politique dans un cache intégré

Outre la configuration des stratégies dans une banque de stratégies pour l'un des points de liaison intégrés ou un serveur virtuel, vous pouvez créer des étiquettes de stratégie de mise en cache et configurer des banques de stratégies pour ces nouvelles étiquettes.

Une étiquette de stratégie pour le cache intégré ne peut être appelée qu'à partir de l'un des points de liaison que vous pouvez afficher dans le Gestionnaire de stratégies dans le volet de détails de la mise en **cache intégrée** (remplacement de la requête, requête par défaut, remplacement de réponse ou par défaut) ou les étiquettes de stratégie intégrées `\\_reqBuiltinDefaults` et `\\_resBuiltinDefaults`. Vous pouvez appeler une étiquette de stratégie n'importe quel nombre de fois, contrairement à une stratégie, qui ne peut être invoquée qu'une seule fois.

L'interface graphique de NetScaler fournit une option permettant de renommer une étiquette de politique. Le fait de renommer une étiquette de politique n'affecte pas le processus d'évaluation des politiques liées à l'étiquette.

> **Remarque** :
>
> Vous pouvez utiliser la stratégie `NOPOLICY` « factice » pour invoquer n'importe quelle étiquette de stratégie provenant d'une autre banque de stratégies. L'`NOPOLICY` entrée est un espace réservé qui ne traite pas de règle.

Pour configurer une étiquette de stratégie pour la mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour créer une étiquette de politique et vérifier la configuration :

- `add cache policylabel <labelName> -evaluates (REQ|RES)`
- `show cache policylabel <labelName>`

Invoquez cette étiquette de stratégie à partir d'une banque de stratégies.

Pour configurer une étiquette de stratégie pour la mise en cache à l'aide de l'interface graphique :

Accédez à **Optimisation** > **Mise en cache intégrée** > **Étiquettes** de stratégie, ajoutez une étiquette de stratégie et liez les stratégies mises en cache.

> **Remarque :**
> Pour vous assurer que NetScaler traite l'étiquette de politique au bon moment, configurez l'invocation de cette étiquette dans l'une des banques de politiques associées aux points de liaison intégrés.

Pour renommer une étiquette de stratégie à l'aide de l'interface graphique :

Accédez à **Optimisation** > **Mise en cache intégrée** > **Étiquettes** de stratégie, sélectionnez l'étiquette de stratégie et renommez.

Dissocier et supprimer une politique de mise en cache intégrée et une étiquette de politique

Vous pouvez dissocier une politique d'une banque de stratégies et la supprimer. Pour supprimer la politique, vous devez d'abord la dissocier. Vous pouvez également supprimer l'invocation d'une étiquette de stratégie et supprimer une étiquette de stratégie. Pour supprimer l'étiquette de politique, vous devez d'abord supprimer toutes les invocations que vous avez configurées pour l'étiquette.

Vous ne pouvez pas dissocier ni supprimer les étiquettes des points de liaison intégrés (demande par défaut, remplacement de demande, réponse par défaut et remplacement de réponse).

Pour dissocier une politique de mise en cache globale à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
unbind cache global <policy>
```

Pour dissocier une politique de mise en cache spécifique à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
(unbind lb vserver|unbind cs vserver)<vserverName> -policyName <policyName>
 -type(REQUEST|RESPONSE)
```

Pour supprimer une politique de mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm cache policy <policyName>
```

Pour dissocier une stratégie de mise en cache à l'aide de l'interface graphique :

Accédez à **Optimisation** > **Mise en cache intégrée, cliquez sur Gestionnaire de stratégies** de cache et dissociez les stratégies en spécifiant le point de liaison et le type de connexion appropriés (Request/Response).

Pour supprimer un appel d'étiquette de stratégie à l'aide de l'interface graphique :

1. Accédez à **Optimisation** > Mise en **cache intégrée**, cliquez sur **Gestionnaire de stratégies de cache**et spécifiez le point de liaison approprié (serveur virtuel d'équilibrage de charge ou serveur virtuel de commutation de contenu) et le type de connexion pour afficher la liste des stratégies de cache liées à ce serveur virtuel.
2. Dans la colonne Invoke de stratégie, désactivez l'entrée.

Prise en charge des protocoles de base de données

May 5, 2023

La fonction de cache intégrée surveille et met en cache les demandes de base de données conformément aux politiques de cache. Les utilisateurs doivent configurer les politiques de cache pour les protocoles MYSQL et MSSQL car l'appliance NetScaler ne fournit aucune politique par défaut. Lorsque vous configurez les protocoles par défaut, n'oubliez pas que les politiques basées sur les demandes ne prennent en charge que les actions CACHE et INVAL, tandis que les politiques basées sur les réponses ne prennent en charge que les actions « NOCACHE ». Après avoir configuré les politiques, vous devez les lier à des serveurs virtuels. Les politiques MYSQL et MSSQL, qu'il s'agisse de demande ou de réponse, sont liées uniquement aux serveurs virtuels.

Avant de créer une politique de cache, vous devez créer un groupe de contenu de cache de type MYSQL ou MSSQL. Lorsque vous créez un groupe de contenu de cache, associez au moins un sélecteur de sélection à celui-ci. Reportez-vous à la section Configuration d'un groupe de contenu de base pour configurer un groupe de contenu de cache.

L'exemple suivant explique comment configurer et vérifier la prise en charge du cache pour les protocoles SQL.

```
1 > enable feature IC
2 > set cache parameter -memlimit 100
3 > add cache selector sel1 mssql.req.query.text
4
5 > add cache contentgroup cg1  -type "MSSQL" -hitselector "sel1" -
     invalselector "inval_sel" -relExpiry "500" -maxResSize
```



```
 "100"
> add cache policy cp1  -rule "mssql.req.query.command.contains("select")" -action "CACHE" -storeInGroup "cg1"
> add cache policy cp2  -invalObjects "cg1" -rule "mssql.req.query.text.contains("insert")" -action "INVAL"
> add db user user1  -password "Pass1"
> add service svc_sql_1 10.102.147.70 mssql 64834 -healthMonitor "NO" -downstateflush "ENABLED"
> add lb vserver lb_mssql1 mssql 10.102.147.77 1433  -lbmethod "roundrobin"
> bind lb vserver lb_mssql1 svc_sql_1
> bind lb vserver lb_mssql1 -policyName cp1  -type "REQUEST" -priority "2"
> bind lb vserver lb_mssql1 -policyName cp2  -type "REQUEST" -priority "1"

> show cache selector sel1
     Name:sel1
                    Expressions:
                    1)mssql.req.query.text
> show cache policy cp1
                    Name:cp1
     Rule:mssql.req.query.command.contains("select")
                    CacheAction:CACHE
                    Stored in group: cg1
                    UndefAction:Use Global
                Hits:2
                    Undef Hits:0
                    Policy is bound to following entities
                    1) Bound to:
                                REQ VSERVER lb_mssql1
                                Priority:2
                                GotoPriorityExpression: END
<!--NeedCopy-->
```

Remarque :

Les méthodes de réduction des foules flash, comme expliqué dans Réduction des foules Flash, ne sont pas prises en charge pour les protocoles MYSQL et MSSQL.

Configuration des expressions pour la mise en cache des stratégies et des sélecteurs

May 5, 2023

Une expression de temps de demande examine les données de la transaction de temps de demande, et une expression de temps de réponse examine les données d'une transaction de temps de réponse. Dans une politique de mise en cache, si une expression correspond aux données d'une demande ou d'une réponse, l'appliance NetScaler prend l'action associée à la politique. Dans un sélecteur, les expressions de temps de demande sont utilisées pour trouver des réponses correspondantes qui sont stockées dans un groupe de contenus.

Avant de configurer des stratégies et des sélecteurs pour le cache intégré, vous devez connaître, au minimum, les noms d'hôte, les chemins et les adresses IP qui apparaissent dans les URL de requête et de réponse HTTP. Et vous devez probablement connaître le format des requêtes et réponses HTTP entières. Des programmes tels que les en-têtes HTTP en direct `http://livehttpheaders.mozdev.org/)or HTTPFox https://addons.mozilla.org/en-US/firefox/addon/6647` peuvent vous aider à étudier la structure des données HTTP avec lesquelles votre organisation travaille.

Voici un exemple de demande HTTP GET pour un programme de cotation boursière :

```
GET /quote.dll?page=dynamic&mode=data&mode=stock&symbol=CTXS&page=multi
    &selected=CTXS&random=0.00792039478975548 HTTP/1.1

Host: quotes.mystockquotes.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
    Gecko/2008052906 Firefox/3.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q
    =0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate,compress,pack200-gzip

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

Referer: http://quotes.mystockquotes.com/quote.dll?mode=stock&symbol=
```



```
      CTXS&page=multi&selected=CTXS
20
21 Cookie: __qca=1210021679-72161677-10297606
22 <!--NeedCopy-->
```

Lorsque vous configurez une expression, notez les limitations suivantes :

Type d'expression	Restrictions
Demander	Ne configurez pas les expressions de temps de demande dans une stratégie avec une action CACHE ou NOCACHE. Utilisez plutôt MAY_CACHE ou MAY_NOCACHE.
Réponse	Configurez les expressions de temps de réponse dans les stratégies de mise en cache uniquement. Les sélecteurs peuvent utiliser uniquement des expressions de temps de demande. Ne configurez pas les expressions de temps de réponse dans une stratégie avec une action INVAL. Remarque : Ne configurez pas les expressions de temps de réponse dans une stratégie avec une action CACHE et un groupe de contenus paramétré. Utilisez l'action MAY_CACHE.

> **Remarque :**
> Pour obtenir une présentation complète des expressions avancées, reportez-vous à la section Stratégies et expressions.

Syntaxe d'expression

Voici les composants de base de la syntaxe :

- Séparez les mots-clés par des points (.), comme suit :

```
http.req.url
```

- Enclenchez les valeurs de chaîne entre parenthèses et guillemets, comme suit :

```
http.req.url.query.contains("this")
```

- Lorsque vous configurez une expression à partir de la ligne de commande, vous devez échapper les guillemets internes (les guillemets qui délimitent les valeurs de l'expression, par opposition

aux guillemets qui délimitent l'expression). Une méthode consiste à utiliser une barre oblique, comme suit :

```
\"abc\"
```

Les expressions de sélecteur sont évaluées par ordre d'apparition, et plusieurs expressions d'une définition de sélecteur sont jointes par un AND logique. Contrairement aux expressions de sélection, vous pouvez spécifier des opérateurs booléens et modifier la priorité d'une expression avancée pour une règle de stratégie.

Configurer une expression dans une stratégie de mise en cache ou un sélecteur

> **Remarque :**
> La syntaxe d'une expression de stratégie est différente de celle d'une expression de sélection. Pour obtenir une présentation complète des expressions avancées, reportez-vous à la section « Stratégies et expressions. «

Pour configurer une expression de stratégie à l'aide de l'interface de ligne de commande

1. Commencez la définition de stratégie comme décrit dans la section « Liaison globale d'une stratégie de mise en cache intégrée ». «
2. Pour configurer la règle de stratégie, délimiter la règle entière entre guillemets et délimiter les valeurs de chaîne au sein de la règle par des guillemets d'échappement.

Voici un exemple :

« http.req.url.contains (« jpg ») »

1. Pour ajouter des valeurs booléennes, insérez &&, || ou ! opérateurs.

Voici quelques exemples :

```
"http.req.url.contains(\"jpg\")|| http.req.url.contains(\"jpeg\")"
```

```
"http.req.url.query.contains(\"IssuePage\")"
```

```
"http.req.header(\"Host\")contains(\"my.company.com\")&& http.req.method.eq
(\"GET\")&& http.req.url.query.contains(\"v=7\")"
```

1. Pour configurer un ordre d'évaluation pour les parties constitutives d'un composé

```
"http.req.url.contains(\"jpg\")|| (http.req.url.contains(\"jpeg\")&& http.
req.method.eq(\"GET\"))"
```

Pour configurer une expression de sélecteur à l'aide de l'interface de ligne de commande :

1. Démarrez la définition du sélecteur comme décrit dans « A propos des groupes de contenu ».
2. Pour configurer l'expression du sélecteur, délimiter la règle entière entre guillemets et délimiter les valeurs de chaîne dans la règle par des guillemets d'échappement.

Voici un exemple :

```
"http.req.url.contains(\"jpg\")"
```

1. Vous ne pouvez pas ajouter de valeurs booléennes, insérer &&, || ou ! opérateurs. Entrez chaque élément d'expression délimité entre guillemets. Les expressions multiples de la définition sont traitées comme une expression composée jointe par des ANDs logiques.

Voici quelques exemples :

```
1 "http.req.url.query.value("ProductId")" "http.req.url.query.value("
     BatchNum")" "http.req.url.query.value("depotLocation")"
2 <!--NeedCopy-->
```

Pour configurer une stratégie ou une expression de sélecteur à l'aide de l'interface graphique

1. Démarrez la définition de la stratégie ou du sélecteur comme décrit dans « Pour configurer une stratégie pour la mise en cache ou l'invalidation à l'aide de l'utilitaire de configuration » ou « Pour configurer un sélecteur à l'aide de l'utilitaire de configuration. «
2. Dans le champ **Expression**, vous pouvez soit taper manuellement la stratégie avancée en cliquant sur Basculer vers la syntaxe classique, soit créer une expression à l'aide de l' **éditeur d'expression**.
3. Pour insérer un opérateur entre deux parties d'une expression composée, cliquez sur le bouton Opérateurs et sélectionnez le type d'opérateur. Voici un exemple d'expression configurée avec un OR booléen (signalé par des barres verticales doubles, ||) :
4. Cliquez sur la liste déroulante **Expressions fréquemment utilisées** pour insérer les expressions couramment utilisées.
5. Pour tester l'expression, cliquez sur le bouton **Evaluer**. Dans la boîte de dialogue **Expression Evaluator**, sélectionnez le type de flux correspondant à l'expression. Dans le champ de données, collez la demande ou la réponse HTTP que vous souhaitez analyser à l'aide de l'expression, puis cliquez sur **Evaluer**.

Afficher les objets mis en cache et les statistiques de cache

Vous pouvez afficher des objets mis en cache particuliers et afficher des statistiques récapitulatives sur les demandes de cache, les échecs et l'utilisation de la mémoire. Les statistiques fournissent des informations sur la quantité de données qui sont servies à partir du cache, les éléments responsables du plus grand avantage de performances et les éléments que vous pouvez régler pour améliorer les performances du cache.

Cette section comprend les détails suivants :

- Affichage des objets mis en cache
- Recherche de réponses mises en cache particulières
- Affichage des statistiques de cache

Afficher les objets mis en cache

Après avoir activé la mise en cache, vous pouvez afficher les détails des objets mis en cache. Par exemple, vous pouvez afficher les éléments suivants :

- Tailles de réponse et tailles d'en-tête
- Codes d'état
- Groupes de contenus
- ETagen-têtes, Last-Modified et Cache-Control
- URL de demande
- Paramètres de l'accès
- Adresses IP de destination
- Délais de demande et de réponse

Pour afficher la liste des objets mis en cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show cache object
```

Propriétés	Description
Taille de la réponse (octets)	Taille de l'en-tête et du corps de la réponse.
Taille de l'en-tête de réponse (octets)	Taille de la partie en-tête de la réponse.
Code d'état de la réponse	Le code d'état envoyé avec la réponse.
ETag	En-tête ETag inséré dans la réponse. En général, cet en-tête indique si la réponse a récemment été modifiée.
Dernière modification	L'en-tête Last-Modified inséré dans la réponse. Cet en-tête indique la date à laquelle la réponse a été modifiée pour la dernière fois.
Contrôle du cache	L'en-tête Cache-Control inséré dans la réponse.
Date	En-tête Date qui indique quand la réponse a été envoyée.
Groupe de contenu	Le groupe de contenus dans lequel la réponse est stockée.
Match complexe	Si cet objet a été mis en cache en fonction de valeurs paramétrées, la valeur de ce champ est OUI.
Hôte	L'hôte spécifié dans l'URL qui a demandé cette réponse.

Propriétés	Description
Port hôte	Port d'écoute de l'hôte spécifié dans l'URL qui a demandé cette réponse
URL	URL émise pour la réponse stockée.
IP destination	Adresse IP du serveur à partir duquel cette réponse a été récupérée.
Port de destination	Port d'écoute du serveur de destination.
Paramètres de l'accès	Si le groupe de contenu qui stocke la réponse utilise des paramètres d'accès, ils sont répertoriés dans ce champ.
Sélecteur de succès	Si ce groupe de contenus utilise un sélecteur d'accès, il est répertorié dans ce champ.
Sélecteur Inval	Si ce groupe de contenus utilise un sélecteur d'invalidation, il est répertorié dans ce champ.
Expressions du sélecteur	Si ce groupe de contenus utilise un sélecteur, ce champ affiche l'expression qui définit la règle de sélection.
Request time	Durée en millisecondes écoulée depuis l'émission de la demande.
Temps de réponse	Durée en millisecondes écoulée depuis que le cache a commencé à recevoir la réponse.
Âge	Durée pendant laquelle l'objet est resté dans le cache.
Expiration	Durée après laquelle l'objet est marqué comme expiré.
Rinçage	Indique si la réponse a été vigée après son expiration.
Prefetch	Si Prefetch a été configuré pour ce groupe de contenus, délai avant expiration pendant lequel l'objet est récupéré depuis l'origine. La prélecture ne s'applique pas aux objets négatifs (par exemple, réponses 404 « objet introuvable »).

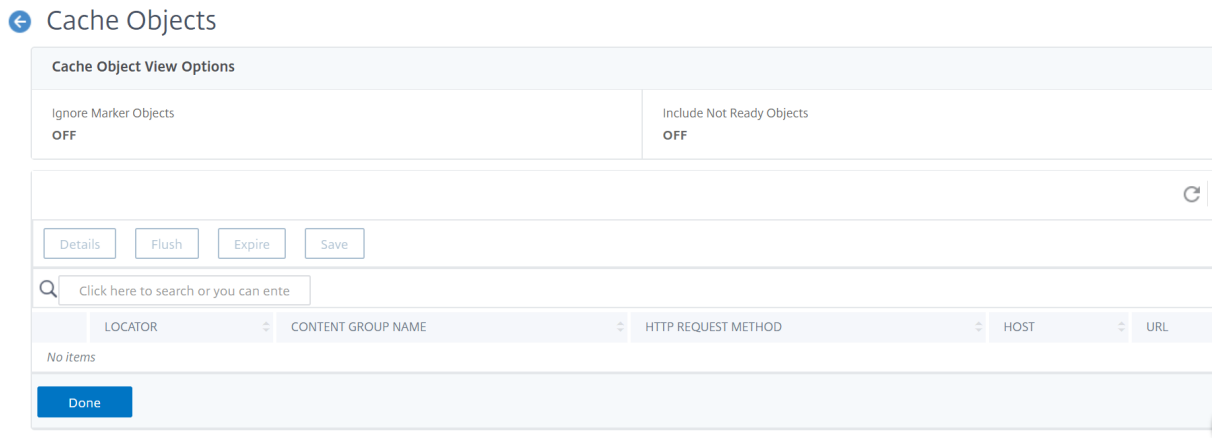
Propriétés	Description
Lecteurs actuels	Approximativement le nombre actuel de demandes traitées. Lorsqu'une réponse avec un objet d'en-tête Content-Length est en cours de téléchargement, les valeurs manques actuelles et les valeurs des lecteurs actuels sont généralement égales à 1. Lorsqu'un objet de réponse en morceaux est téléchargé, la valeur actuelle des échecs est généralement de 1, mais la valeur des lecteurs actuels est généralement égale à 0, car la réponse en morceaux qui est fournie au client ne provient pas des tampons de mise en cache intégrés.
Les manques actuelles	Nombre actuel de requêtes ayant entraîné une absence de cache et une récupération à partir du serveur d'origine. Cette valeur est généralement égale à 0 ou 1. Si Poll Every Time est activé pour un groupe de contenus, le nombre peut être supérieur à 1.
Accès	Nombre d'accès au cache pour cet objet.
Misses	Le nombre de mises en cache manquant pour cet objet
Format de compression	Type de compression appliqué à cet objet. Les formats de compression incluent gzip, deflate, compress et pack200-gzip.
Version HTTP en réponse	Version du protocole HTTP utilisée pour envoyer la réponse.
Etag faible présent en réponse	Les en-têtes d'étiquette forts changent si les bits d'une entité changent. Les en-têtes forts sont basés sur les valeurs d'octet d'un objet. Les en-têtes d'étiquette faibles changent si la signification d'une entité change. Les valeurs etag faibles sont basées sur l'identité sémantique. Les valeurs d'etags faibles commencent par un « W ».

Propriétés	Description
Cellule marqueur négative	Un objet marqueur peut être mis en cache, mais il ne répond pas encore à tous les critères de mise en cache. Par exemple, l'objet peut dépasser la taille de réponse maximale pour le groupe de contenus. Une cellule de marqueur est créée pour les objets de ce type. La prochaine fois qu'un utilisateur envoie une demande pour cet objet, un échec de cache est envoyé.
Marqueur Reason créé	La raison pour laquelle une cellule de marqueur a été créée (par exemple, « En attente de minhit », « Les données de réponse de longueur de contenu ne sont pas dans la limite de taille du groupe »).
Sondage automatique à chaque fois	Si le cache intégré reçoit une réponse 200 OK déjà expirée avec des validateurs (en-têtes de réponse Last-Modified ou ETag), il stocke la réponse et la marque comme auto-PET (interrogation automatique à chaque fois).
NetScaler Etag inséré en réponse	Une variante de l'en-tête ETag généré par l'appliance NetScaler. La valeur YES apparaît si NetScaler insère un Etag dans la réponse.
Réponse complète présente dans le cache	Indique s'il s'agit d'une réponse complète.
IP de destination vérifiée par DNS	Indique si la résolution DNS a été effectuée lors du stockage de l'objet.
Objet stocké via un proxy de transfert de cache	Indique si cette réponse a été stockée en raison d'un proxy de transfert configuré dans le cache intégré.
Object est un fichier de base Delta	Réponse compressée en delta.
En attente de minhits	Indique si ce groupe de contenus nécessite un nombre minimum de serveurs d'origine avant de mettre en cache une réponse.

Propriétés	Description
Comptage de Minhit	Si ce groupe de contenus nécessite un nombre minimum de demandes de serveur d'origine avant de mettre en cache un objet, ce champ affiche le nombre de demandes reçues jusqu'à présent.
Méthode de requête HTTP	La méthode, GET ou POST, utilisée dans la requête qui a obtenu cet objet.
Stocké par stratégie	Nom de la stratégie de mise en cache qui a provoqué le stockage de cet objet. La valeur NOT AVAILABLE indique que la stratégie a été désactivée ou supprimée. La valeur NONE indique que l'objet ne correspond pas à une stratégie visible, mais qu'il a été stocké selon des critères internes de mise en cache.
Les métadonnées du pare-feu d'application existent	Ce paramètre est utilisé lorsque le pare-feu d'application et le cache intégré sont tous deux activés. Le pare-feu d'application analyse le contenu d'une page de réponse, stocke ses métadonnées (par exemple, les URL et les formulaires contenus dans la page) et exporte les métadonnées avec la réponse vers le cache. Le cache stocke la page et les métadonnées, et lorsque le cache sert la page, il renvoie les métadonnées à la session de la demande.
objet de légende HTTP, nom, type, réponse	Ces cellules indiquent si ces données ont été stockées à la suite d'une expression de légende HTTP et fournissent des informations sur divers aspects de la légende et de la réponse correspondante. Pour plus d'informations sur les légendes HTTP, consultez « Légendes HTTP ».

Pour afficher les objets mis en cache à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets de cache**. Vous pouvez afficher tous les objets mis en cache et les trier en conséquence selon vos besoins.



Rechercher des réponses en cache particulières

Vous pouvez trouver des éléments individuels dans le cache en fonction de critères de recherche. Il existe différentes méthodes pour rechercher des éléments mis en cache, selon que le groupe de contenus contenant les données utilise des sélecteurs d'accès et d'invalidation, comme suit :

- Si le groupe de contenus utilise des sélecteurs, vous ne pouvez effectuer la recherche qu'à l'aide de l'ID de localisateur de l'élément mis en cache.
- Si le groupe de contenus n'utilise pas de sélecteurs, vous effectuez la recherche à l'aide de critères tels que l'URL, l'hôte et le nom du groupe de contenus.

Lorsque vous recherchez une réponse mise en cache, vous pouvez localiser certains éléments par URL et par hôte. Si la réponse se trouve dans un groupe de contenus qui utilise un sélecteur, vous ne pouvez la trouver qu'en utilisant un numéro de localisateur (par exemple, 0x00000000ad7af00000050). Pour enregistrer un numéro de localisateur en vue d'une utilisation ultérieure, cliquez avec le bouton droit de la souris sur l'entrée et sélectionnez **Copier**. Pour plus d'informations sur les sélecteurs, voir « Configuration des sélecteurs et des groupes de contenu de base ». «

Pour afficher les réponses mises en cache dans des groupes de contenu ne disposant pas d'un sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus <positive integer>] | -group <contentGroupName> |
 -ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

Pour afficher les réponses mises en cache dans des groupes de contenus dotés d'un sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

Pour afficher les réponses mises en cache dans des groupes de contenus qui ne possèdent pas de sélecteur à l'aide de l'utilitaire de configuration

Accédez à **Optimisation > Mise en cache intégrée > Objets de cache**, cliquez sur Rechercher et définissez les critères de recherche pour afficher la réponse mise en cache requise.

Si vous n'avez pas encore configuré de groupe de contenu, tous les objets se trouvent dans le groupe Par défaut.

Afficher les statistiques du cache

Le tableau suivant récapitule les statistiques de cache détaillées que vous pouvez consulter.

Comptoir	Description
—	—
Accès	Réponses trouvées et servies à partir du cache intégré. Inclut des objets statiques tels que des fichiers image, des pages avec des codes d'état 200, 203, 300, 301, 302, 304, 307, 403, 404, 410, et des réponses qui correspondent à une stratégie définie par l'utilisateur avec une action CACHE.
Misses	Demandes HTTP interceptées pour lesquelles la réponse a finalement été récupérée depuis le serveur d'origine.
Demandes	Nombre total de demandes de cache plus le nombre total d'échecs de cache.
Hits non-304	Si l'utilisateur demande un élément plusieurs fois et que l'élément du cache n'a pas changé depuis la dernière fois que l'appliance NetScaler l'a servi, l'appliance NetScaler fournit une réponse 304 au lieu de l'objet mis en cache.
Cette statistique indique le nombre d'éléments que l'appliance NetScaler a servis à partir du cache, à l'exclusion des 304 réponses.
304 visites	Nombre de 304 réponses (objet non modifié) que l'appliance NetScaler a servies à partir du cache.
Taux de réussite de 304 (%)	Pourcentage de 304 réponses traitées par l'appliance NetScaler, par rapport aux autres réponses.
Taux de succès (%)	Pourcentage de réponses que l'appliance NetScaler a envoyées depuis le cache (demandes de cache) par rapport aux réponses qui n'ont pas pu être servies depuis le cache.
Bande passante d'origine économisée (%)	Estimation de la capacité de traitement que l'appliance NetScaler a économisée sur le serveur d'origine en diffusant des réponses depuis le cache.
Octets servis par NetScaler	Nombre total d'octets que l'appliance NetScaler a servis depuis le serveur d'origine et le cache.
Octets servis par le cache	Nombre total d'octets que l'appliance NetScaler a servis à partir du cache.
Taux de succès en octets (%)	Pourcentage de données que l'appliance NetScaler a diffusées à partir

du cache, par rapport à toutes les données figurant dans toutes les réponses envoyées. |
Octets compressés à partir du cache	Quantité de données, en octets, que l'appliance NetScaler a servies sous forme compressée.
Manques stockables	Si l'appliance NetScaler ne trouve pas l'objet demandé dans le cache, elle récupère l'objet depuis le serveur d'origine. Ceci connu sous le nom de « cache miss » (échec d'accès au cache). Une mémoire cache manquante peut être stockée dans le cache.
Non stockables manquant	Un cache non stockable ne peut pas être stocké dans le cache.
Misses	Tous les fichiers cache manquaient.
Revalidations	Le paramètre Max-Age dans un en-tête Cache-Control détermine, en quelques secondes, quand un cache intermédiaire doit revalider le contenu avec le cache intégré avant de le diffuser à l'utilisateur.
Pour plus d'informations, reportez-vous à la section « Insertion d'un en-tête Cache-Control ». «
Revalidations réussies	Nombre de revalidations qui ont été effectuées.
Pour plus d'informations, reportez-vous à la section « Insertion d'un en-tête Cache-Control ». «
Conversions en requêtes conditionnelles	Une demande d'agent utilisateur pour un objet PET mis en cache est toujours convertie en demande conditionnelle et envoyée au serveur d'origine.
Pour plus d'informations, reportez-vous à la section « Interrogation du serveur Origin chaque fois qu'une demande est reçue. «
Taux d'échec stockable (%)	Le cache stockable manque en pourcentage des échecs de cache non stockables.
Taux de réévaluation réussie (%)	Les revalidations réussies en pourcentage de toutes les tentatives de revalidation.
Pour plus d'informations, reportez-vous à la section « Insertion d'un en-tête Cache-Control ». «
Expire au dernier octet	Nombre de fois que le contenu du cache a expiré immédiatement après avoir reçu le dernier octet du corps. S'applique uniquement aux réponses positives, comme décrit dans le tableau « Cache Hits and Misses ». «
Pour plus d'informations, reportez-vous à la section « Exemple d'optimisation des performances. «
`Flashcache` Misses	Si vous activez Flash Cache, le cache n'autorise qu'une seule requête à atteindre le serveur, ce qui élimine les foules Flash. Cette statistique indique le nombre de demandes Flash Cache qui ont été manquantes dans le cache.
Pour plus d'informations, consultez la section « Mise en file d'attente des demandes dans le cache. «
Accès Flashcache	Nombre de demandes Flash Cache qui ont été des accès au cache.
Pour plus d'informations, voir « Mettre les demandes en file d'attente dans le cache ». «
Requêtes d'invalidation paramétrées	Requêtes correspondant à une politique comportant une action d'invalidation (INVAL) et à un groupe de contenus utilisant un sélecteur ou des paramètres d'invalidation pour faire expirer de manière sélective les objets mis en cache du groupe.
Demandes d'annulation complètes	Demandes qui correspondent à une politique d'invalidation dans laquelle le paramètre InvalGroups est configuré et fait expirer un ou plusieurs groupes de contenus.

Demandes invales	Demandes qui correspondent à une politique d'invalidation et entraînent l'expiration de réponses spécifiques mises en cache ou de groupes de contenus entiers.
Demandes paramétrées	Nombre de demandes de cache traitées à l'aide d'une politique avec un groupe de contenus paramétré.
Nombre d'accès paramétrés autres que 304	Nombre de demandes de cache traitées à l'aide d'une politique avec un groupe de contenus paramétré, pour lesquelles une réponse complète en cache a été trouvée et la réponse n'était pas une réponse 304 (objet non mis à jour).
304 accès paramétrés	Nombre de demandes de cache traitées à l'aide d'une politique avec un groupe de contenus paramétré, dans lequel l'objet mis en cache a été trouvé et l'objet était une réponse 304 (objet non mis à jour).
Nombre total de visites paramétrées	Nombre de demandes de cache traitées à l'aide d'une politique avec un groupe de contenus paramétré, dans lequel l'objet mis en cache a été trouvé.
Taux de succès paramétré de 304 (%)	Pourcentage de 304 réponses (objet non mis à jour) trouvées à l'aide d'une politique paramétrée, par rapport à tous les accès au cache.
Effectuer un sondage à chaque demande	Si l'option Examiner à chaque fois est activée, l'appliance NetScaler consulte toujours le serveur d'origine avant de servir un objet stocké.
Pour plus d'informations, reportez-vous à la section « Interrogation du serveur Origin chaque fois qu'une demande est reçue. «
Interrogez chaque fois qu'un accès au cache a été trouvé à l'aide de la méthode Poll Every Time.
Pour plus d'informations, reportez-vous à la section « Interrogation du serveur Origin chaque fois qu'une demande est reçue. «
Poll every time hit ratio (%)	Pourcentage d'accès au cache à l'aide de la méthode Poll Every Time, par rapport à toutes les recherches d'objets mis en cache à l'aide de Poll Every Time. Pour plus d'informations, voir « Interrogation du serveur d'origine à chaque réception d'une demande ». «
Mémoire maximale (Ko)	Quantité maximale de mémoire dans l'appliance NetScaler allouée au cache. Pour plus d'informations, reportez-vous à la section « Configuration des attributs globaux pour la mise en cache ». «
Valeur maximale de la mémoire active (Ko)	Quantité maximale de mémoire (valeur active) qui sera définie une fois la mémoire allouée au cache. Pour plus d'informations, consultez « Comment configurer la fonctionnalité de mise en cache intégrée d'un dispositif NetScaler pour différents scénarios ». «
Mémoire utilisée (Ko)	Quantité de mémoire réellement utilisée.
Échecs d'allocation de mémoire	Nombre de tentatives infructueuses d'utilisation de la mémoire dans le but de stocker une réponse dans le cache.
Plus grande réponse à ce jour	Plus grande réponse en octets trouvée dans le cache ou sur le serveur d'origine et envoyée au client.
Objets en cache	Nombre d'objets dans le cache, y compris les réponses qui n'ont pas encore été complètement téléchargées et les réponses qui ont expiré mais qui n'ont pas encore été vidées.
Objets marqueurs	Les objets marqueurs sont créés lorsqu'une réponse dépasse la taille de réponse

maximale ou minimale pour le groupe de contenus, ou n'a pas encore reçu le nombre minimum de réponses pour le groupe de contenus. |
|Nombre de connexions en cours de servage|Nombre de connexions qui ont été diffusées depuis le cache. |
|Manque de traitement|Réponses qui ont été récupérées depuis le serveur d'origine, stockées dans le cache, puis diffusées. Devrait se rapprocher du nombre d'erreurs pouvant être stockées. N'inclut pas les erreurs non stockables. |

Pour afficher les statistiques du cache récapitulatif à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
stat cache
```

Pour afficher des statistiques de cache spécifiques à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
stat cache -detail
```

```
> stat cache -detail

Integrated Cache Statistics - Detail
Integrated Cache Statistics - Summary
                                          Rate (/s)
                                             Total


Hits                                             0
                        0

Misses                                           0
                        0

Requests                                         0
                        0

Hit ratio(%)                                    --
                        0

Origin bandwidth saved(%)                       --
                        0
Cached objects                                  --
                        0

Marker objects                                  --
                        0
```



```
                                                Rate (/s)
                                                   Total

Requests                                                0
                        0

Hit Statistics

                                                Rate (/s)
                                                   Total


Non-304 hits                                            0
                        0

304 hits                                                0
                        0


Sql hits                                                0
                        0


Hits                                                    0
                        0

304 hit ratio(%)                                       --
                        0

Hit ratio(%)                                           --
                        0

Origin bandwidth saved(%)                              --
                        0
Byte Statistics
                                                Rate (/s)
                                                   Total


Bytes served by NetScaler                             648
    55379204

Bytes served by cache                                   0
                        0
```



```
Byte hit ratio(%)                                   --
                        0
Compressed bytes from cache                          0
                        0

Miss Statistics

                                                Rate (/s)
                                                   Total

Storable misses                                      0
                        0

Non-storable misses                                  0
                        0

Misses                                               0
                        0

Revalidations                                        0
                        0

Successful revalidations                             0
                        0

Conversions to conditional req                       0
                        0


Storable miss ratio(%)                              --
                        0
Successful reval ratio(%)                           --
                        0

Flashcache Statistics
                                                Rate (/s)
                                                   Total


Expire at last byte                                  0
                        0

Flashcache misses                                    0
                        0
```



```
Flashcache hits                                    0
                        0

Invalidation Statistics

                                                Rate (/s)
                                                   Total

Parameterized inval requests                       0
                        0


Full inval requests                                0
                        0


Inval requests                                     0
                        0

Parameterized Caching Statistics

                                                Rate (/s)
                                                   Total


Parameterized requests                             0
                        0

Parameterized non-304 hits                         0
                        0

Parameterized 304 hits                             0
                        0


Total parameterized hits                           0
                        0

Parameterized 304 hit ratio(%)                    --
                        0

Poll Every Time (PET) Statistics

                                                Rate (/s)
```



```
                                                    Total
117
118
119 Poll every time requests                              0
                         0
120
121 Poll every time hits                                  0
                         0
122
123 Poll every time hit ratio(%)                        --
                         0
124
125 Memory Usage Statistics
126                                                  Total
127
128 Maximum memory(KB)                                   0
129
130 Maximum memory active value(KB)                      0
131
132 Utilized memory(KB)                                  0
133
134 Memory allocation failures                           0
135
136 Largest response so far(B)                           0
137
138 Cached objects                                       0
139
140 Marker objects                                       0
141
142 Hits being served                                    0
143 Misses being handled                                 0
144  Done
145 <!--NeedCopy-->
```

Pour afficher les statistiques du cache récapitulatif à l'aide de l'interface graphique

1. Cliquez sur l'onglet Tableau de **bord** en haut de la page.
2. Faites défiler l'écran jusqu'à la section **Mise en cache intégrée** de la fenêtre.
3. Pour afficher des statistiques détaillées, cliquez sur le lien Plus… en bas du tableau.

Pour afficher des statistiques de cache spécifiques à l'aide de l'interface graphique

1. Cliquez sur l'onglet **Rapports** en haut de la page.
2. Sous Rapports **intégrés, développez le cache intégré**, puis cliquez sur le rapport contenant les statistiques que vous souhaitez afficher.

3. Pour enregistrer le rapport en tant que modèle, cliquez sur **Enregistrer sous** et nommez le rapport. Le rapport enregistré apparaît sous Rapports **personnalisés** .

Afficher les objets mis en cache et les statistiques de cache

May 5, 2023

Vous pouvez consulter des objets spécifiques mis en cache et consulter des statistiques récapitulatives sur les accès et les échecs du cache et sur l'utilisation de la mémoire. Les statistiques fournissent des informations sur la quantité de données qui sont servies à partir du cache, les éléments responsables du plus grand avantage de performances et les éléments que vous pouvez régler pour améliorer les performances du cache.

Cette section comprend les détails suivants :

- Affichage des objets mis en cache
- Recherche de réponses mises en cache particulières
- Affichage des statistiques de cache

Afficher les objets mis en cache

Après avoir activé la mise en cache, vous pouvez afficher les détails des objets mis en cache. Par exemple, vous pouvez afficher les éléments suivants :

- Tailles de réponse et tailles d'en-tête
- Codes d'état
- Groupes de contenus
- ETagen-têtes, Last-Modified et Cache-Control
- URL de demande
- Paramètres de l'accès
- Adresses IP de destination
- Délais de demande et de réponse

Pour afficher la liste des objets mis en cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show cache object
```

Propriétés	Spécifications
Taille de la réponse (octets)	Taille de l'en-tête et du corps de la réponse.
Taille de l'en-tête de réponse (octets)	Taille de la partie en-tête de la réponse.

Propriétés	Spécifications
Code d'état de la réponse	Le code d'état envoyé avec la réponse.
ETag	L' ETag en-tête inséré dans la réponse. En général, cet en-tête indique si la réponse a récemment été modifiée.
Dernière modification	L'en-tête Last-Modified inséré dans la réponse. Cet en-tête indique la date à laquelle la réponse a été modifiée pour la dernière fois.
Cache-Control	L'en-tête Cache-Control inséré dans la réponse.
Date	En-tête Date qui indique quand la réponse a été envoyée.
Contentgroup	Le groupe de contenus dans lequel la réponse est stockée.
Match complexe	Si cet objet a été mis en cache en fonction de valeurs paramétrées, la valeur de ce champ est OUI.
Hôte	L'hôte spécifié dans l'URL qui a demandé cette réponse.
Port hôte	Port d'écoute de l'hôte spécifié dans l'URL qui a demandé cette réponse
URL	URL émise pour la réponse stockée.
IP destination	Adresse IP du serveur à partir duquel cette réponse a été récupérée.
Port de destination	Port d'écoute du serveur de destination.
Paramètres de l'accès	Si le groupe de contenu qui stocke la réponse utilise des paramètres d'accès, ils sont répertoriés dans ce champ.
Sélecteur de succès	Si ce groupe de contenus utilise un sélecteur d'accès, il est répertorié dans ce champ.
Sélecteur Inval	Si ce groupe de contenus utilise un sélecteur d'invalidation, il est répertorié dans ce champ.
Expressions du sélecteur	Si ce groupe de contenus utilise un sélecteur, ce champ affiche l'expression qui définit la règle de sélection.

Propriétés	Spécifications
Request time	Durée en millisecondes écoulée depuis l'émission de la demande.
Temps de réponse	Durée en millisecondes écoulée depuis que le cache a commencé à recevoir la réponse.
Âge	Durée pendant laquelle l'objet est resté dans le cache.
Expiration	Durée après laquelle l'objet est marqué comme expiré.
Rinçage	Indique si la réponse a été vigée après son expiration.
Prefetch	Si Prefetch a été configuré pour ce groupe de contenus, délai avant expiration pendant lequel l'objet est récupéré depuis l'origine. La prélecture ne s'applique pas aux objets négatifs (par exemple, réponses 404 « objet introuvable »).
Lecteurs actuels	Environ le nombre de visites actuellement diffusées. Lorsqu'une réponse avec un objet d'en-tête Content-Length est en cours de téléchargement, les valeurs manques actuelles et les valeurs des lecteurs actuels sont généralement égales à 1. Lorsqu'un objet de réponse en morceaux est téléchargé, la valeur actuelle des échecs est généralement de 1, mais la valeur des lecteurs actuels est généralement égale à 0, car la réponse en morceaux qui est fournie au client ne provient pas des tampons de mise en cache intégrés.
Les manques actuelles	Nombre actuel de requêtes ayant entraîné une absence de cache et une récupération à partir du serveur d'origine. Cette valeur est généralement égale à 0 ou 1. Si Poll Every Time est activé pour un groupe de contenus, le nombre peut être supérieur à 1.
Accès	Nombre d'accès au cache pour cet objet.

Propriétés	Spécifications
Misses	Nombre d'erreurs de cache pour cet objet.
Format de compression	Type de compression appliqué à cet objet. Les formats de compression incluent gzip, deflate, compress et pack200-gzip.
Version HTTP en réponse	Version du protocole HTTP utilisée pour envoyer la réponse.
Faible `etag` présence en réponse	`etag` Les en-têtes forts changent si les bits d'une entité changent. Les en-têtes forts sont basés sur les valeurs d'octet d'un objet. `etag` Les en-têtes faibles changent si la signification d'une entité change. Les `etag` valeurs faibles sont basées sur l'identité sémantique. `etags` Les valeurs faibles commencent par un « W ».
Cellule marqueur négative	Un objet marqueur peut être mis en cache, mais il ne répond pas encore à tous les critères de mise en cache. Par exemple, l'objet peut dépasser la taille de réponse maximale pour le groupe de contenus. Une cellule de marqueur est créée pour les objets de ce type. La prochaine fois qu'un utilisateur envoie une demande pour cet objet, un échec de cache est envoyé.
Marqueur Reason créé	La raison pour laquelle une cellule de marqueur a été créée (par exemple, « En attente de minhit », « Les données de réponse de longueur de contenu ne sont pas dans la limite de taille du groupe »).
Sondage automatique à chaque fois	Si le cache intégré reçoit une réponse 200 OK déjà expirée avec des validateurs (soit les en-têtes Last-Modified, soit les en-têtes de `ETag` réponse), il stocke la réponse et la marque comme Auto-PET (interrogation automatique à chaque fois).
NetScaler Etag inséré en réponse	Une variante de l' `ETag` en-tête généré par l'appliance NetScaler. La valeur YES apparaît si NetScaler insère un `Etag` dans la réponse.

Propriétés	Spécifications
Réponse complète présente dans le cache	Indique s'il s'agit d'une réponse complète.
IP de destination vérifiée par DNS	Indique si la résolution DNS a été effectuée lors du stockage de l'objet.
Objet stocké via un proxy de transfert de cache	Indique si cette réponse a été stockée en raison d'un proxy de transfert configuré dans le cache intégré.
Object est un fichier de base Delta	Réponse compressée en delta.
En attente de minhits	Indique si ce groupe de contenus nécessite un nombre minimum de serveurs d'origine avant de mettre en cache une réponse.
Comptage de Minhit	Si ce groupe de contenus nécessite un nombre minimum d'accès aux serveurs d'origine avant la mise en cache d'un objet, ce champ affiche le nombre d'accès reçus jusqu'à présent.
Méthode de requête HTTP	La méthode, GET ou POST, utilisée dans la requête qui a obtenu cet objet.
Stocké par stratégie	Nom de la stratégie de mise en cache qui a provoqué le stockage de cet objet. La valeur NOT AVAILABLE indique que la stratégie a été désactivée ou supprimée. La valeur NONE indique que l'objet ne correspond pas à une stratégie visible, mais qu'il a été stocké selon des critères internes de mise en cache.
Les métadonnées du pare-feu d'application existent	Ce paramètre est utilisé lorsque le pare-feu d'application et le cache intégré sont tous deux activés. Le pare-feu d'application analyse le contenu d'une page de réponse, stocke ses métadonnées (par exemple, les URL et les formulaires contenus dans la page) et exporte les métadonnées avec la réponse vers le cache. Le cache stocke la page et les métadonnées, et lorsque le cache sert la page, il renvoie les métadonnées à la session de la demande.

Propriétés	Spécifications
objet de légende HTTP, nom, type, réponse	Ces cellules indiquent si ces données ont été stockées à la suite d'une expression de légende HTTP et fournissent des informations sur divers aspects de la légende et de la réponse correspondante. Pour plus d'informations sur les légendes HTTP, consultez « Légendes HTTP ».

Rechercher des réponses en cache particulières

Vous pouvez trouver des éléments individuels dans le cache en fonction de critères de recherche. Il existe différentes méthodes pour rechercher des éléments mis en cache, selon que le groupe de contenus contenant les données utilise des sélecteurs d'accès et d'invalidation, comme suit :

Si le groupe de contenus utilise des sélecteurs, vous ne pouvez effectuer la recherche qu'à l'aide de l'ID de localisateur de l'élément mis en cache.

Si le groupe de contenus n'utilise pas de sélecteurs, vous effectuez la recherche à l'aide de critères tels que l'URL, l'hôte et le nom du groupe de contenus.

Lorsque vous recherchez une réponse mise en cache, vous pouvez localiser certains éléments par URL et par hôte. Si la réponse se trouve dans un groupe de contenus qui utilise un sélecteur, vous ne pouvez la trouver qu'en utilisant un numéro de localisateur (par exemple, 0x00000000ad7af00000050). Pour enregistrer un numéro de localisateur en vue d'une utilisation ultérieure, cliquez avec le bouton droit de la souris sur l'entrée et sélectionnez Copier. Pour plus d'informations sur les sélecteurs, voir « Configuration des sélecteurs et des groupes de contenu de base ». «

Pour afficher les réponses mises en cache dans des groupes de contenu ne disposant pas d'un sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus<positive integer>] | -group <contentGroupName> |
-ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

Pour afficher les réponses mises en cache dans des groupes de contenus dotés d'un sélecteur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

Pour afficher les réponses mises en cache dans des groupes de contenus dépourvus de sélecteur à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets de cache**, cliquez sur **Rechercher**et définissez les critères de recherche pour afficher la réponse mise en cache requise.

Si vous n'avez pas encore configuré de groupe de contenu, tous les objets se trouvent dans le groupe Par défaut.

Pour afficher les réponses mises en cache dans les groupes de contenus dotés d'un sélecteur à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Objets de cache**, cliquez sur **Rechercher**et définissez les critères de recherche du sélecteur pour afficher la réponse mise en cache requise.

Afficher les statistiques du cache

Le tableau suivant résume les statistiques du cache.

Comptoir

Spécifications

Affichage des statistiques du cache

Mise à jour : 28/10/2013

Le tableau suivant récapitule les statistiques de cache détaillées que vous pouvez consulter.

Comptoir	Spécifie
Accès	Réponses trouvées et servies à partir du cache intégré. Inclut des objets statiques tels que des fichiers image, des pages avec les codes d'état 200, 203, 300, 301, 302, 304, 307, 403, 404, 410 et des réponses qui correspondent à une politique définie par l'utilisateur avec une action CACHE.
Misses	Demandes HTTP interceptées pour lesquelles la réponse a finalement été récupérée depuis le serveur d'origine.

Comptoir	Spécifie
Demandes	Nombre total d'accès au cache et nombre total d'erreurs de cache.
Hits non-304	Si l'utilisateur demande un élément plusieurs fois et que l'élément du cache n'a pas changé depuis la dernière fois que l'appliance NetScaler l'a servi, l'appliance NetScaler fournit une réponse 304 au lieu de l'objet mis en cache. Cette statistique indique le nombre d'éléments que l'appliance NetScaler a servis à partir du cache, à l'exclusion des 304 réponses.
vue 304 fois	Nombre de 304 réponses (objet non modifié) que l'appliance NetScaler a envoyées à partir du cache.
Ratio de succès 304 (%)	Pourcentage de 304 réponses traitées par l'appliance NetScaler, par rapport aux autres réponses.
Taux de réussite (%)	Pourcentage de réponses que l'appliance NetScaler a envoyées à partir du cache (accès au cache) par rapport aux réponses qui n'ont pas pu être transmises à partir du cache.
Bande passante d'origine économisée (%)	Estimation de la capacité de traitement que l'appliance NetScaler a enregistrée sur le serveur d'origine en diffusant les réponses depuis le cache.
Octets desservis par NetScaler	Nombre total d'octets que l'appliance NetScaler a servis à partir du serveur d'origine et du cache.
Octets servis par le cache	Nombre total d'octets que l'appliance NetScaler a servis à partir du cache.
Taux de succès en octets (%)	Pourcentage de données que l'appliance NetScaler a diffusées à partir du cache, par rapport à l'ensemble des données figurant dans toutes les réponses envoyées.

Comptoir	Spécifie
Octets compressés depuis le cache	Quantité de données, en octets, que l'appliance NetScaler a servie sous forme compressée.
Manques mémorisables	Si l'appliance NetScaler ne trouve pas l'objet demandé dans le cache, elle le récupère sur le serveur d'origine. Ceci connu sous le nom de « cache miss » (échec d'accès au cache). Une erreur de mémoire cache stockable peut être enregistrée dans la mémoire cache.
Manques non mémorisables	Un échec du cache non stockable ne peut pas être stocké dans le cache.
Misses	Tous les caches sont absents.
Revalidations	Le paramètre Max-Age dans un en-tête Cache-Control détermine, en quelques secondes, à quel moment un cache intermédiaire doit revalider le contenu avec le cache intégré avant de le diffuser à l'utilisateur. Pour plus d'informations, voir « Insertion d'un en-tête Cache-Control ». «
Revalidations réussies	Nombre de revalidations effectuées. Pour plus d'informations, voir « Insertion d'un en-tête Cache-Control ». «
Conversions en exigences conditionnelles	Une demande d'agent utilisateur pour un objet PET mis en cache est toujours convertie en demande conditionnelle et envoyée au serveur d'origine. Pour plus d'informations, voir « Interrogation du serveur d'origine à chaque réception d'une demande ». «
Taux d'échec enregistrable (%)	Pourcentage d'erreurs de cache stockable par rapport aux erreurs de cache non stockables.
Taux de révélations réussies (%)	Pourcentage de revalidations réussies par rapport à toutes les tentatives de revalidation. Pour plus d'informations, voir « Insertion d'un en-tête Cache-Control ». «

Comptoir	Spécifie
Expire au dernier octet	Nombre de fois où le contenu du cache a expiré immédiatement après avoir reçu le dernier octet du corps. Applicable uniquement aux réponses positives, comme décrit dans le tableau « Cache Hits and Misses ». « Pour plus d'informations, voir « Exemple d'optimisation des performances ». «
Le cache Flash est absent	Si vous activez Flash Cache, le cache ne permet qu'à une seule requête d'atteindre le serveur, ce qui élimine les problèmes de mémoire flash. Cette statistique indique le nombre de demandes Flash Cache qui ont été manquantes dans le cache. Pour plus d'informations, consultez « Mettre les demandes en file d'attente dans le cache. «
`Flashcache` hits	Nombre de requêtes Flash Cache ayant atteint le cache. Pour plus d'informations, voir « Mettre les demandes en file d'attente dans le cache ». «
Demandes d'invalisation paramétrées	Demandes correspondant à une politique comportant une action d'invalidation (INVAL) et à un groupe de contenus utilisant un sélecteur ou des paramètres d'invalidation pour faire expirer de manière sélective les objets mis en cache du groupe.
Demandes invaliales complètes	Demandes qui correspondent à une politique d'invalidation dans laquelle le paramètre InvalGroups est configuré et fait expirer un ou plusieurs groupes de contenus.
Demandes invaliales	Demandes qui correspondent à une politique d'invalidation et entraînent l'expiration de réponses mises en cache spécifiques ou de groupes de contenus entiers.
Demandes paramétrées	Nombre de demandes de cache traitées à l'aide d'une politique avec un groupe de contenus paramétré.

Comptoir	Spécifie
Résultats paramétrés autres que 304	Nombre de demandes de cache qui ont été traitées à l'aide d'une politique avec un groupe de contenus paramétré, pour lesquelles une réponse complète a été trouvée et pour lesquelles la réponse n'était pas une réponse 304 (objet non mis à jour).
304 visites paramétrées	Nombre de demandes de cache traitées à l'aide d'une politique avec un groupe de contenus paramétré, dans lesquelles l'objet mis en cache a été trouvé et l'objet était une réponse 304 (objet non mis à jour).
Nombre total de visites paramétrées	Nombre de demandes de cache traitées à l'aide d'une politique avec un groupe de contenus paramétré, dans lequel l'objet mis en cache a été trouvé.
Taux de réussite paramétré de 304 (%)	Pourcentage de 304 réponses (objet non mis à jour) trouvées à l'aide d'une politique paramétrée, par rapport à tous les accès au cache.
Sondage à chaque fois que vous le demandez	Si l'option Poll Every Time est activée, l'appliance NetScaler consulte toujours le serveur d'origine avant de diffuser un objet stocké. Pour plus d'informations, voir « Interrogation du serveur d'origine à chaque réception d'une demande ». «
Sondage à chaque fois que vous recevez	Nombre de fois qu'un accès au cache a été détecté à l'aide de la méthode Poll Every Time. Pour plus d'informations, voir « Interrogation du serveur d'origine à chaque réception d'une demande ». «

Comptoir	Spécifie
Taux de réponse à chaque sondage (%)	Pourcentage d'accès au cache à l'aide de la méthode Poll Every Time, par rapport à toutes les recherches d'objets mis en cache à l'aide de la méthode Poll Every Time. Pour plus d'informations, voir « Interrogation du serveur d'origine à chaque réception d'une demande ». «
Mémoire maximale (Ko)	Quantité maximale de mémoire allouée au cache dans l'appliance NetScaler. Pour plus d'informations, consultez la section « Configuration des attributs globaux pour la mise en cache ».
Valeur maximale de la mémoire active (Ko)	Quantité maximale de mémoire (valeur active) qui sera définie une fois la mémoire réellement allouée au cache. Pour plus d'informations, consultez « Comment configurer la fonctionnalité de mise en cache intégrée d'un dispositif NetScaler pour différents scénarios ». «
Mémoire utilisée (Ko)	Quantité de mémoire réellement utilisée.
Défaillances d'allocation de mémoire	Nombre de tentatives infructueuses d'utilisation de la mémoire dans le but de stocker une réponse dans le cache.
Plus grande réponse à ce jour	Réponse la plus élevée en octets trouvée dans le cache ou sur le serveur d'origine et envoyée au client.
Objets mis en cache	Nombre d'objets dans le cache, y compris les réponses qui n'ont pas encore été complètement téléchargées et les réponses qui ont expiré mais qui n'ont pas encore été vidées.
Objets marqueurs	Les objets marqueurs sont créés lorsqu'une réponse dépasse la taille de réponse maximale ou minimale pour le groupe de contenus, ou n'a pas encore reçu le nombre minimum de réponses pour le groupe de contenus.

Comptoir	Spécifie
Hits en cours de service	Nombre d'accès qui ont été servis depuis le cache.
Manques en cours de traitement	Réponses qui ont été extraites du serveur d'origine, stockées dans le cache, puis diffusées. Devrait se rapprocher du nombre d'erreurs pouvant être stockées. N'inclut pas les erreurs non mémorisables.

Pour afficher les statistiques du cache récapitulatif à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
stat cache
```

Pour afficher des statistiques de cache spécifiques à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1  stat cache -detail
2
3      > stat cache -detail
4      Integrated Cache Statistics - Detail
5      Integrated Cache Statistics - Summary
6                                                  Rate (/s)
                                                      Total
7      Hits                                              0
                            0
8      Misses                                            0
                            0
9      Requests                                          0
                            0
10     Hit ratio(%)                                     --
                            0
11     Origin bandwidth saved(%)                        --
                            0
12     Cached objects                                   --
                            0
13     Marker objects                                   --
                            0
14                                                 Rate (/s)
                                                      Total
15     Requests                                          0
                            0
```



```
16      Hit Statistics
17                                                  Rate (/s)
                                                       Total
18      Non-304 hits                                        0
                            0
19      304 hits                                            0
                            0
20      Sql hits                                            0
                            0
21      Hits                                                0
                            0
22      304 hit ratio(%)                                   --
                            0
23      Hit ratio(%)                                       --
                            0
24      Origin bandwidth saved(%)                          --
                            0
25
26      Byte Statistics
27                                                  Rate (/s)
                                                       Total
28      Bytes served by NetScaler                         648
           55379204
29      Bytes served by cache                               0
                            0
30      Byte hit ratio(%)                                  --
                            0
31      Compressed bytes from cache                         0
                            0
32      Miss Statistics
33                                                  Rate (/s)
                                                       Total
34      Storable misses                                     0
                            0
35      Non-storable misses                                 0
                            0
36      Misses                                              0
                            0
37      Revalidations                                       0
                            0
38      Successful revalidations                            0
                            0
39      Conversions to conditional req                      0
                            0
40      Storable miss ratio(%)                             --
```



```
                              0
41      Successful reval ratio(%)                          --
                              0
42      Flashcache Statistics
43                                                  Rate (/s)
                                                       Total
44      Expire at last byte                                 0
                              0
45      Flashcache misses                                   0
                              0
46      Flashcache hits                                     0
                              0
47
48      Invalidation Statistics
49                                                  Rate (/s)
                                                       Total
50      Parameterized inval requests                        0
                              0
51      Full inval requests                                 0
                              0
52      Inval requests                                      0
                              0
53
54      Parameterized Caching Statistics
55                                                  Rate (/s)
                                                       Total
56      Parameterized requests                              0
                              0
57      Parameterized non-304 hits                          0
                              0
58      Parameterized 304 hits                              0
                              0
59      Total parameterized hits                            0
                              0
60      Parameterized 304 hit ratio(%)                     --
                              0
61
62      Poll Every Time (PET) Statistics
63                                                  Rate (/s)
                                                       Total
64      Poll every time requests                            0
                              0
65      Poll every time hits                                0
                              0
66      Poll every time hit ratio(%)                       --
```



```
                                0
67      Memory Usage Statistics
68                                                      Total
69      Maximum memory(KB)                                   0
70      Maximum memory active value(KB)                      0
71      Utilized memory(KB)                                  0
72      Memory allocation failures                           0
73      Largest response so far(B)                           0
74      Cached objects                                       0
75      Marker objects                                       0
76      Hits being served                                    0
77      Misses being handled                                 0
78       Done
79  <!--NeedCopy-->
```

Pour afficher les statistiques du cache récapitulatif à l'aide de l'interface graphique

1. Cliquez sur l'onglet Tableau de **bord** en haut de la page.
2. Faites défiler l'écran jusqu'à la section Mise en cache intégrée de la fenêtre.
3. Pour afficher des statistiques détaillées, cliquez sur le lien Plus… en bas du tableau.

Pour afficher des statistiques de cache spécifiques à l'aide de l'interface graphique

1. Cliquez sur l'onglet Rapports en haut de la page.
2. Sous Rapports intégrés, développez le cache intégré, puis cliquez sur le rapport contenant les statistiques que vous souhaitez afficher.
3. Pour enregistrer le rapport en tant que modèle, cliquez sur Enregistrer sous et nommez le rapport. Le rapport enregistré apparaît sous Rapports personnalisés .

Améliorer les performances du cache

May 5, 2023

Vous pouvez améliorer les performances du cache intégré, notamment en gérant les demandes simultanées pour les mêmes données mises en cache, en évitant les retards liés à l'actualisation des réponses mises en cache depuis le serveur d'origine et en veillant à ce qu'une réponse soit demandée suffisamment souvent pour valoir la peine d'être mise en cache.

Réduisez les embouteillages

Les « Flash Crowds » se produisent lorsque de nombreux utilisateurs demandent simultanément les mêmes données. Les requêtes provenant d'une foule Flash peuvent devenir des erreurs de cache si

vous avez configuré le cache de manière à ne traiter les accès qu'après le téléchargement de l'objet dans son intégralité.

Les techniques suivantes peuvent réduire ou éliminer les foules soudaines :

- **PREFETCH** : Actualise une réponse positive avant son expiration pour s'assurer qu'elle ne devienne jamais obsolète ou inactive. Pour plus d'informations, consultez la section « Actualisation d'une réponse avant son expiration ».
- Mise en**mémoire tampon du cache** : commence à envoyer une réponse à plusieurs clients lorsqu'il reçoit l'en-tête de réponse du serveur d'origine, plutôt que d'attendre que la réponse complète soit téléchargée. La seule limite au nombre de clients pouvant télécharger une réponse simultanément est celle des ressources système disponibles. L'appliance NetScaler télécharge et fournit des réponses même si le client à l'origine du téléchargement s'arrête avant la fin du téléchargement. Si la réponse dépasse la taille du cache ou si la réponse est fragmentée, le cache arrête de stocker la réponse, mais le service aux clients n'est pas interrompu.
- **Flash Cache :** Flash Cache met en file d'attente les requêtes vers le cache et n'autorise qu'une seule demande à atteindre le serveur à la fois.

Pour plus d'informations, consultez la section « Mettre les demandes en file d'attente dans le cache ».

Actualiser une réponse avant son expiration

Pour garantir qu'une réponse mise en cache est actualisée chaque fois que cela est nécessaire, l'option PREFETCH actualise une réponse avant son délai d'expiration calculé. L'intervalle de prélecture est calculé après réception de la première demande du client. À partir de ce moment, l'appliance NetScaler actualise la réponse mise en cache à un intervalle de temps que vous configurez dans le paramètre PREFETCH.

Ce paramètre est utile pour les données qui sont fréquemment mises à jour entre les demandes. Cela ne s'applique pas aux réponses négatives (par exemple, 404 messages).

Pour configurer le préchargement pour un groupe de contenus à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cache contentgroup <name> -prefetch YES [-prefetchPeriod <seconds> | -
prefetchPeriodMilliSec <milliseconds>] [-prefetchMaxPending <positiveInteger
>]
```

*Pour configurer le préchargement pour un groupe de contenus à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenus**, puis sélectionnez le **groupe de contenus**.

Dans l'onglet **Autres**, dans le groupe Flash Crowd et Prefetch, sélectionnez l'option **Prefetch et spécifiez les valeurs dans les zones de texte Intervalle et Nombre maximum de préchargements** en attente.

Mettre les demandes en file d'attente dans le cache

L'option Flash Cache met en file d'attente les demandes qui arrivent simultanément (une foule flash), récupère la réponse et la distribue à tous les clients dont les demandes se trouvent dans la file d'attente. Si, au cours de ce processus, la réponse ne peut plus être mise en cache, l'appliance NetScaler cesse de diffuser la réponse depuis le cache et transmet à la place la réponse du serveur d'origine aux clients en file d'attente. Si la réponse n'est pas disponible, les clients reçoivent un message d'erreur.

Flash Cache est désactivé par défaut. Vous ne pouvez pas activer Poll Every Time (PET) et Flash Cache sur le même groupe de contenus.

L'un des inconvénients de Flash Cache est que si le serveur répond par une erreur (par exemple, une erreur 404 qui est rapidement corrigée), l'erreur est transmise aux clients en attente.

> **Remarque** :
> Si Flash Cache est activé, dans certains cas, l'appliance NetScaler ne parvient pas à faire correspondre correctement l'en-tête Accept-Encoding de la demande du client à l'en-tête Content-Encoding de la réponse. L'appliance NetScaler peut supposer que ces en-têtes correspondent et générer un accès par erreur. Pour contourner ce problème, vous pouvez configurer des politiques de mise en cache intégrée afin d'interdire la diffusion des accès aux clients qui ne disposent pas d'un en-tête Accept-Encoding approprié.

Pour activer Flash Cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cache contentgroup <contentGroupName> -flashcache yes
```

Pour activer Flash Cache à l'aide de l'interface graphique

Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenus**, puis sélectionnez le groupe de contenus.

Dans l'onglet **Autres**, dans le groupe Flash Crowd et Prefetch, sélectionnez l'option **Prefetch** .

Mettre en cache une réponse lorsqu'un client arrête un téléchargement

Vous pouvez définir le paramètre Quick Abort pour continuer à mettre en cache une réponse, même si le client interrompt une demande avant que la réponse ne soit dans le cache.

Si la taille de la réponse téléchargée est inférieure ou égale à la taille de Quick Abort, l'appliance NetScaler arrête de télécharger la réponse. Si vous définissez le paramètre Quick Abort sur 0, tous les téléchargements sont interrompus.

Pour configurer la taille d'un abandon rapide à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cache contentgroup <name> -quickAbortSize <integerInKBytes>
```

Pour configurer la taille d'un abandon rapide à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenus**, puis sélectionnez le groupe de contenus.
2. Dans l'onglet **Mémoire**, définissez la valeur appropriée dans Quick Abort : Poursuivre la mise en cache s'il s'agit d'une zone de texte.

Exiger un nombre minimum d'accès au serveur avant la mise en cache

Vous pouvez configurer le nombre minimum de fois qu'une réponse doit être trouvée sur le serveur d'origine avant de pouvoir être mise en cache. Vous devez envisager d'augmenter le nombre minimum d'accès si la mémoire cache se remplit rapidement et présente un taux de succès inférieur aux prévisions.

La valeur par défaut pour le nombre minimum de résultats est 0. Cette valeur met en cache la réponse après la première demande.

Pour configurer le nombre minimum d'accès requis avant la mise en cache à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cache contentgroup <name> -minhits <positiveInteger>
```

Pour configurer le nombre minimum d'accès requis avant la mise en cache à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenus**, puis sélectionnez le groupe de contenus.
2. Dans l'onglet **Mémoire**, définissez la valeur appropriée dans Ne pas mettre en cache, si le nombre de résultats est inférieur à la zone de texte.

Exemple d'optimisation des performances

Dans cet exemple, un client accède à une cotation boursière. Les cours boursiers sont très dynamiques. Vous configurez le cache intégré pour fournir la même cotation boursière à des clients simultanés sans envoyer plusieurs demandes au serveur d'origine. La cotation boursière expire

après avoir été téléchargée vers les clients et la demande suivante est récupérée depuis le serveur d'origine. Cela garantit que le devis est toujours à jour.

L'aperçu des tâches suivant décrit les étapes de configuration du cache pour l'application de cotation boursière.

Configuration de la mise en cache pour une application de cotation boursière

Création d'un groupe de contenus pour les cotations boursières

Pour plus d'informations, voir « À propos des groupes de contenus ». «

Configurez les éléments suivants pour ce groupe de contenus :

1. Dans l'onglet **Méthode d'expiration**, cochez la case Expire après réception d'une réponse complète.
2. Dans l'onglet **Autres**, cochez la case **Flash Cache**, puis cliquez sur **Créer**.
3. Ajoutez une politique de cache pour mettre en cache les cotations boursières.

Pour plus d'informations, reportez-vous à la section « Configuration d'une stratégie dans le cache intégré. »

Configurez les éléments suivants pour la politique

1. Dans les **listes Action et Stocker dans le groupe**, sélectionnez **CACHE** et sélectionnez le groupe que vous avez défini à l'étape précédente.
2. Cliquez sur **Ajouter**et, dans la boîte de dialogue **Ajouter une expression**, configurez une expression qui identifie les demandes de cotation boursière, par exemple : http.req.url.contains (« cgi-bin/stock-quote.pl »)
3. Activez la politique.

Pour plus d'informations, consultez « Lier globalement une politique de mise en cache intégrée ». « Dans cet exemple, vous liez cette stratégie au traitement de remplacement au moment de la requête et définissez la priorité sur une valeur faible.

Configuration des cookies, des en-têtes et des sondages

May 5, 2023

Cette rubrique explique comment configurer le cache pour gérer les cookies, les en-têtes HTTP et le sondage du serveur d'origine. Cela inclut la modification du comportement par défaut qui entraîne une divergence du cache par rapport aux normes documentées, le remplacement des en-têtes HTTP susceptibles d'entraîner l'absence de stockage du contenu pouvant être mis en cache dans le cache et la configuration du cache pour toujours interroger l'origine du contenu mis à jour.

Divergence du comportement du cache par rapport aux normes

Par défaut, le cache intégré respecte les normes RFC suivantes :

- RFC 2616, « HTTP HTTP/1.1 »
- Les comportements de mise en cache décrits dans la RFC 2617, « Authentification HTTP : authentification d'accès basique et condensée »
- Le comportement de mise en cache décrit dans la RFC 2965, « Mécanisme de gestion de l'état HTTP »

Les stratégies intégrées et les attributs de groupe de contenu par défaut garantissent la conformité à la plupart de ces normes.

Le comportement du cache intégré par défaut diffère de la spécification comme suit :

- La prise en charge de l'en-tête Vary est limitée. Par défaut, toute réponse contenant un en-tête Vary est considérée comme ne pouvant pas être mise en cache, sauf si elle est compressée. Une réponse compressée contient un encodage de contenu : gzip, un encodage de contenu : deflate ou un encodage de contenu : pack200-gzip et peut être mise en cache même si elle contient l'en-tête Vary : Accept-encoding.
- Le cache intégré ignore les valeurs des en-têtes cache-control : no-cache et cache-control : private. Par exemple, une réponse qui contient cache-control: no-cache="set-cookie" est traitée comme si la réponse contenait Cache-Control: no-cache. Par défaut, la réponse n'est pas mise en cache.
- Une image (type de contenu = image/*) est toujours considérée comme pouvant être mise en cache, même si une réponse d'image contient des en-têtes set-cookie ou set-cookie2, ou si une demande d'image contient un en-tête de cookie. Le cache intégré supprime les en-têtes set-cookie et set-cookie2 d'une réponse avant de la mettre en cache. Cela diffère de la RFC 2965. Vous pouvez configurer le comportement compatible RFC comme suit :

```
1 add cache policy rfc_compliant_images_policy -rule "http.res.header.set
     -cookie2.exists || http.res.header.set-cookie.exists" -action
     NOCACHE
2
3
4 bind cache global rfc_compliant_images_policy -priority 100 -type
     REQ_OVERRIDE
5 <!--NeedCopy-->
```

- Les en-têtes de contrôle de cache suivants dans une demande obligent un cache compatible RFC à recharger une réponse mise en cache à partir du serveur d'origine :

```
Cache-control: max-age=0
```

```
Cache-control: no-cache
```


Pour se prémunir contre les attaques par déni de service, ce comportement n'est pas celui par défaut.

- Par défaut, le module de mise en cache considère qu'une réponse peut être mise en cache, sauf indication contraire d'un état d'en-tête de réponse. Pour rendre ce comportement conforme à la RFC 2616, définissez `-weakPosRelExpiry` et `-weakNegResExpiry` sur 0 pour tous les groupes de contenu.

Supprimer les cookies d'une réponse

Les cookies sont souvent personnalisés pour un utilisateur et ne doivent généralement pas être mis en cache. Le paramètre `Remove Response Cookies` supprime les en-têtes `Set-Cookie and Set-Cookie2` avant de mettre en cache une réponse. Par défaut, l'option `Remove Response Cookies` pour un groupe de contenu empêche la mise en cache des réponses avec des en-têtes `Set-Cookie` ou `Set-Cookie2`.

> **Remarque :**
> Lorsque les images sont mises en cache, le comportement intégré consiste à supprimer les en-têtes `Set-Cookie` et `Set-Cookie2` avant la mise en cache, quelle que soit la manière dont le groupe de contenu est configuré.
>
> Citrix vous recommande d'accepter la valeur par défaut `Remove Response Cookies` pour chaque groupe de contenu qui stocke des réponses intégrées, par exemple des images.

Pour configurer `Remove Response Cookies` pour un groupe de contenu à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
set cache contentgroup <name> -removeCookies YES
```

Configurer la suppression des cookies de réponse pour un groupe de contenus à l'aide de l'interface graphique NetScaler

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenus**, puis sélectionnez le groupe de contenus.
2. Dans l'onglet **Autres**, dans le groupe **Paramètres**, sélectionnez l'option Supprimer les cookies de réponse.

Insérer des en-têtes HTTP au moment de réponse

Le cache intégré peut insérer des en-têtes HTTP dans les réponses qui résultent de demandes de cache. L'appliance NetScaler ne modifie pas les en-têtes des réponses résultant d'erreurs de cache.

Le tableau suivant décrit les en-têtes que vous pouvez insérer dans une réponse.

En-tête	Spécifications
Âge	Fournit l'âge de la réponse en secondes, calculé à partir du moment où la réponse a été générée sur le serveur d'origine. Par défaut, le cache insère un en-tête Age pour chaque réponse diffusée à partir du cache.
via	Répertorie les protocoles et les destinataires entre les points de début et d'arrivée d'une demande ou d'une réponse. L'appliance NetScaler insère un en-tête Via dans chaque réponse qu'elle envoie depuis le cache. La valeur par défaut de l'en-tête inséré est `NS-CACHE-10.0` : dernier octet de l'adresse IP NetScaler. » Pour plus d'informations, consultez la section « Configuration des attributs globaux pour la mise en cache ».

En-tête	Spécifications
Tag	Le cache prend en charge la validation des réponses à l'aide de Last-Modified et des en-têtes Tag pour déterminer si une réponse est obsolète. Le cache insère un Tag dans une réponse uniquement s'il met en cache la réponse et si le serveur d'origine n'a pas inséré son propre en-tête Tag. La valeur Tag est un nombre unique arbitraire. La valeur Tag d'une réponse change si elle est actualisée à partir du serveur d'origine, mais elle reste la même si le serveur envoie une réponse 304 (objet non mis à jour). Les serveurs d'origine ne génèrent généralement pas de validateurs pour le contenu dynamique car le contenu dynamique est considéré comme ne pouvant pas être mis en cache. Vous pouvez remplacer ce comportement. Avec l'insertion de l'en-tête Tag, le cache est autorisé à ne pas fournir de réponses complètes. Au lieu de cela, l'agent utilisateur est tenu de mettre en cache la réponse dynamique envoyée par le cache intégré pour la première fois. Pour forcer un agent utilisateur à mettre en cache une réponse, vous configurez le cache intégré pour insérer un en-tête Tag et remplacer l'en-tête Cache-Control fourni par l'origine.

En-tête	Spécifications
Contrôle du cache	L'appliance NetScaler ne modifie généralement pas les en-têtes de mise en cache des réponses envoyées par le serveur d'origine. Si le serveur d'origine envoie une réponse étiquetée comme ne pouvant pas être mise en cache, le client traite la réponse comme ne pouvant pas être mise en cache même si l'appliance NetScaler met la réponse en cache. Pour mettre en cache les réponses dynamiques dans un agent utilisateur, vous pouvez remplacer les en-têtes Cache-Control du serveur d'origine. Cela s'applique uniquement aux agents utilisateurs et aux autres caches intermédiaires. Ils n'affectent pas le cache intégré.

En-tête	Spécifications
Âge	Fournit l'âge de la réponse en secondes, calculé à partir du moment où la réponse a été générée sur le serveur d'origine. Par défaut, le cache insère un en-tête Age pour chaque réponse diffusée à partir du cache.
via	Répertorie les protocoles et les destinataires entre les points de début et d'arrivée d'une demande ou d'une réponse. L'appliance NetScaler insère un en-tête Via dans chaque réponse qu'elle envoie depuis le cache. La valeur par défaut de l'en-tête inséré est « NS-CACHE-9.2 : dernier octet de l'adresse IP NetScaler ». Pour plus d'informations, consultez la section « Configuration des attributs globaux pour la mise en cache ».

En-tête	Spécifications
Tag	Le cache prend en charge la validation des réponses à l'aide des en-têtes Last-Modified et Tag pour déterminer si une réponse est obsolète. Le cache insère un Tag dans une réponse uniquement s'il met en cache la réponse et si le serveur d'origine n'a pas inséré son propre en-tête Tag. La valeur Tag est un nombre unique arbitraire. La valeur Tag d'une réponse change si elle est actualisée à partir du serveur d'origine, mais elle reste la même si le serveur envoie une réponse 304 (objet non mis à jour). Les serveurs d'origine ne génèrent généralement pas de validateurs pour le contenu dynamique car le contenu dynamique est considéré comme ne pouvant pas être mis en cache. Vous pouvez remplacer ce comportement. Avec l'insertion de l'en-tête Tag, le cache est autorisé à ne pas fournir de réponses complètes. Au lieu de cela, l'agent utilisateur est tenu de mettre en cache la réponse dynamique envoyée par le cache intégré pour la première fois. Pour forcer un agent utilisateur à mettre en cache une réponse, vous configurez le cache intégré pour insérer un en-tête Tag et remplacer l'en-tête Cache-Control fourni par l'origine.

En-tête	Spécifications
Contrôle du cache	L'appliance NetScaler ne modifie généralement pas les en-têtes de mise en cache des réponses envoyées par le serveur d'origine. Si le serveur d'origine envoie une réponse étiquetée comme ne pouvant pas être mise en cache, le client traite la réponse comme ne pouvant pas être mise en cache même si l'appliance NetScaler met la réponse en cache. Pour mettre en cache les réponses dynamiques dans un agent utilisateur, vous pouvez remplacer les en-têtes Cache-Control du serveur d'origine. Cela s'applique uniquement aux agents utilisateurs et aux autres caches intermédiaires. Ils n'affectent pas le cache intégré.

Insérer un en-tête age, via ou Tag

Les procédures suivantes décrivent comment insérer des en-têtes Age, Via et ETag.

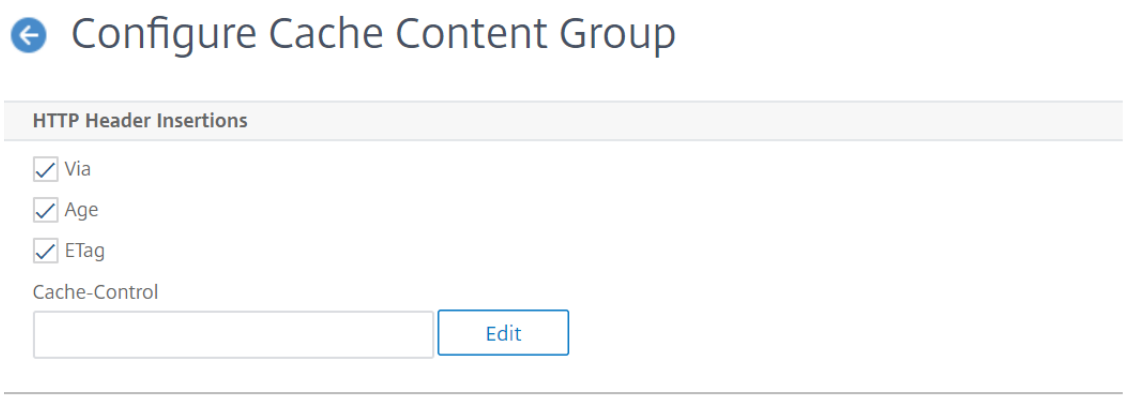
Insérez un en-tête Age, Via ou Etag à l'aide de l'interface de commande NetScaler :

À l'invite de commande, tapez :

```
set cache contentgroup <name> -insertVia YES -insertAge YES -insertETag YES
```

Configurez l'en-tête Age, Via ou Etag à l'aide de l'interface graphique NetScaler

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu,** puis sélectionnez le **groupe de contenu**.
2. Dans l'onglet **Autres**, dans le groupe Insertions d'en-tête HTTP, sélectionnez les options **Via**, **Age**ou **ETag**, selon le cas.
3. Les valeurs des autres types d'en-tête sont calculées automatiquement. Vous configurez la valeur Via dans les principaux paramètres du cache.



Insérer un en-tête de contrôle de cache

Lorsque le cache intégré remplace un en-tête Cache-Control inséré par le serveur d'origine, il remplace également l'en-tête Expires. Le nouvel en-tête Expires contient une date d'expiration antérieure. Cela garantit que les clients et les caches HTTP/1.0 (qui ne comprennent pas l'en-tête Cache-Control) ne mettent pas en cache le contenu.

Insérer un en-tête de contrôle du cache à l'aide de l'interface de commande NetScaler

À l'invite de commande, tapez :

```
set cache contentgroup <name> -cacheControl <value>
```

Insérer un en-tête de contrôle du cache à l'aide de l'interface graphique NetScaler

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenu**et
   a) Cliquez sur l'onglet **Méthode d'expiration**, désactivez les paramètres heuristiques et d'expiration par défaut et définissez la valeur appropriée dans la zone de texte Expire le contenu après.
   b) Cliquez sur l'onglet **Autres** et saisissez l'en-tête que vous souhaitez insérer dans la zone de texte Contrôle du cache. Vous pouvez également cliquer sur Configurer pour définir les directives Cache-Control dans les réponses mises en cache.

Ignorer les en-têtes de contrôle de cache et pragma dans les requêtes

Par défaut, le module de mise en cache traite les en-têtes Cache-Control et Pragma. Les jetons suivants dans les en-têtes Cache-Control sont traités comme décrit dans la RFC 2616.

- âge max
- Max-rassis
- seulement-si mis en cache

- pas de cache

Un en-tête Pragma : no-cache dans une requête est traité de la même manière qu'un en-tête Cache-Control : no-cache.

Si vous configurez le module de mise en cache pour ignorer les en-têtes Cache-Control et Pragma, une requête contenant un en-tête Cache-Control : No-Cache amène l'appliance NetScaler à récupérer la réponse du serveur d'origine, mais la réponse mise en cache n'est pas mise à jour. Si le module de mise en cache traite les en-têtes Cache-Control et Pragma, la réponse mise en cache est actualisée.

Le tableau suivant récapitule les implications de divers paramètres pour ces en-têtes et le paramètre Ignorer la demande de rechargement du navigateur.

Paramètre pour les en-têtes Ignorer Cache-Control et Pragma	Paramètre pour Ignorer la demande de rechargement du navigateur	Résultat
Oui	Oui ou Non	Ignorez les en-têtes Cache-Control et Pragma du client, y compris la directive Cache-Control : no-cache.
Non	Oui	L'en-tête Cache-Control : no-cache produit un échec de cache, mais une réponse déjà présente dans le cache n'est pas actualisée.
Non	Non	Une demande qui contient un en-tête Cache-Control : no-cache provoque un échec de cache et la réponse stockée est actualisée.

Pour ignorer les en-têtes Cache-Control et Pragma dans une requête à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set cache contentgroup <name> -ignoreReqCachingHdrs YES
```

Pour ignorer les demandes de rechargement du navigateur à l'aide de l'interface de ligne de commande

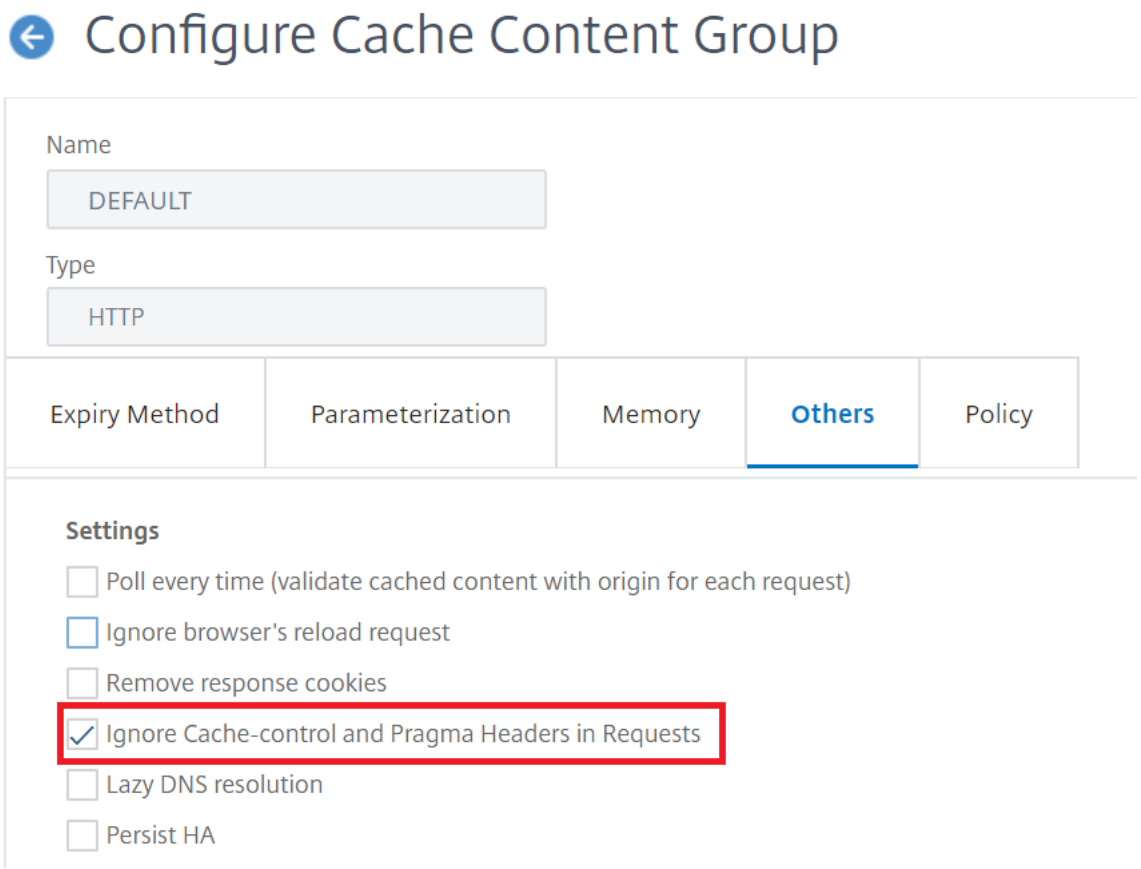
À l'invite de commande, tapez :

```
set cache contentgroup <name> -ignoreReloadReq NO
```


> **Remarque :**
> Par défaut, le paramètre -IgnoreLoadReq est défini sur OUI.

Ignorer les en-têtes Cache-Control et Pragma dans une requête à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenus**, puis sélectionnez le groupe de contenus.
2. Dans l'onglet **Autres**, dans le groupe **Paramètres**, sélectionnez **Ignorer le contrôle du cache et les en-têtes Pragma** dans l'option **Demandes** .



Exemple de stratégie pour ignorer les en-têtes Cache-Control :

Dans l'exemple suivant, vous configurez une stratégie de remplacement au moment de la demande pour mettre en cache les réponses qui contiennent le type de contenu : image/* quel que soit l'en-tête Cache-Control dans la réponse.

Pour configurer une stratégie de remplacement au moment de la demande afin de mettre en cache toutes les réponses avec image/*

Videz le cache à l'aide de l'option Tout invalider.

Configurez une nouvelle stratégie de cache et dirigez la stratégie vers un groupe de contenu particulier. Pour plus d'informations, reportez-vous à la section « Configuration d'une stratégie dans le cache intégré. »

Assurez-vous que le groupe de contenu utilisé par la stratégie est configuré pour ignorer les en-têtes Cache-Control, comme décrit dans la section « Ignorer les en-têtes Cache-Control et Pragma dans les demandes ».

Liez la stratégie à la banque de stratégies de remplacement au moment de la requête.

Pour plus d'informations, consultez la rubrique Liaison globale d'une stratégie de mise en cache intégrée .

Serveur d'origine du sondage chaque fois qu'une demande est reçue

Vous pouvez configurer l'appliance NetScaler pour qu'elle consulte toujours le serveur d'origine avant de fournir une réponse stockée. C'est ce que l'on appelle Poll Every Time (PET). Lorsque l'appliance NetScaler consulte le serveur d'origine et que la réponse PET n'a pas expiré, une réponse complète du serveur d'origine ne remplace pas le contenu mis en cache. Cette propriété est utile lors de la diffusion de contenu spécifique au client.

Après l'expiration d'une réponse PET, l'appliance NetScaler l'actualise lorsque la première réponse complète arrive du serveur d'origine.

La fonction Poll Every Time (PET) fonctionne comme suit :

Pour une réponse mise en cache qui possède des validateurs sous la forme d'un en-tête Tag ou Last-Modified, si la réponse expire, elle est automatiquement marquée PET et mise en cache.

Vous pouvez configurer la TEP pour un groupe de contenu.

Si vous configurez un groupe de contenu en tant que PET, chaque réponse du groupe de contenu est marquée PET. Le groupe de contenu PET peut stocker des réponses qui n'ont pas de validateurs. Les réponses qui sont automatiquement marquées TEP sont toujours expirées. Les réponses qui appartiennent à un groupe de contenu PET peuvent expirer après un certain délai, selon la façon dont vous configurez le groupe de contenu.

Deux types de demandes sont concernés par le sondage :

- Demandes conditionnelles : un client émet une demande conditionnelle pour s'assurer que la réponse qu'il a reçue est la copie la plus récente. Une demande d'agent utilisateur pour une réponse PET mise en cache est toujours convertie en demande conditionnelle et envoyée au serveur d'origine. Une demande conditionnelle comporte des validateurs dans les `If-None-Match` en-têtes `If-Modified-Since` ou. L' `If-Modified-Since` en-tête contient le temps écoulé depuis l' `Last-Modified` en-tête. Un en-tête If-None-Match contient la valeur de l'en-tête Tag de la réponse. Si la copie de la réponse du client est récente, le serveur d'origine répond

par 304 Non modifié. Si la copie est périmée, une réponse conditionnelle génère un 200 OK qui contient la réponse complète.

- Demandes non conditionnelles : Une demande non conditionnelle ne peut générer qu'un 200 OK contenant la réponse complète.

Réponse du serveur Origin	Action
Envoyer la réponse complète	Le serveur d'origine envoie la réponse telle quelle au client. Si la réponse mise en cache a expiré, elle est actualisée.
304 Non modifié	Les valeurs d'en-tête suivantes de la réponse 304 sont fusionnées avec la réponse mise en cache et la réponse mise en cache est servie au client : Date, Expire, Age, en-tête Cache-Control Max-Age et jetons S-Maxage
401 non autorisé ; 400 demandes incorrectes ; 405 méthode non autorisée ; 406 non acceptable ; 407 authentification proxy requise	La réponse de l'origine est servie telle quelle au client. La réponse mise en cache n'est pas modifiée.
Toute autre réponse d'erreur, par exemple, 404 Not Found	La réponse de l'origine est servie telle quelle au client. La réponse mise en cache est supprimée.

> **Remarque :**
> Le paramètre Poll Every Time traite les réponses affectées comme non stockables.

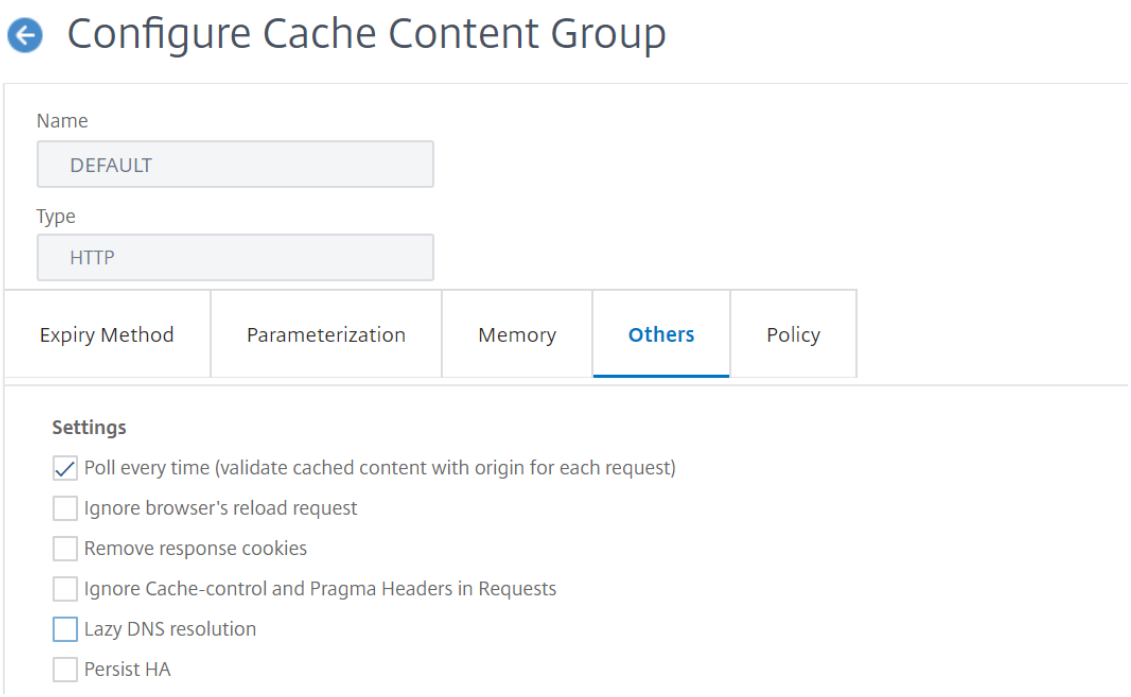
Pour configurer le sondage à chaque fois à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add cache contentgroup <contentGroupName> -pollEveryTime YES
```

Sondage en utilisant l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > **Groupes de contenus**, puis sélectionnez le groupe de contenus.
2. Dans l'onglet **Autres**, dans le groupe Paramètres, sélectionnez l'option Sonder à chaque fois (valider le contenu mis en cache avec l'origine pour chaque demande).



Contenu PET et spécifique au client

La fonction PET peut garantir que le contenu est personnalisé pour un client. Par exemple, un site Web qui propose du contenu dans plusieurs langues examine l'en-tête de demande Accept-Language pour sélectionner la langue du contenu qu'il diffuse. Pour un site Web multilingue où l'anglais est la langue prédominante, tout le contenu en langue anglaise peut être mis en cache dans un groupe de contenu PET. Cela garantit que chaque demande est envoyée au serveur d'origine pour déterminer la langue de la réponse. Si la réponse est en anglais et que le contenu n'a pas changé, le serveur d'origine peut diffuser un 304 non modifié dans le cache.

L'exemple suivant montre les commandes permettant de mettre en cache les réponses en anglais dans un groupe de contenu PET, de configurer une expression nommée qui identifie les réponses en anglais dans le cache et de configurer une stratégie qui utilise ce groupe de contenu et cette expression nommée. Le gras est utilisé pour mettre l'accent :

```
1 add cache contentgroup EnglishLanguageGroup -pollEveryTime YES
2 add expression containsENExpression  - rule "http.res.header(\\"Content-
     Language\\").contains(\\"en\\")"
3 add cache policy englishPolicy -rule containsENExpression -action CACHE
      -storeInGroup englishLanguageGroup
4 bind cache policy englishPolicy -priority 100 -precedeDefRules NO
5 <!--NeedCopy-->
```


TEP et authentification, autorisation et audit

Outlook Web Access (OWA) est un bon exemple de contenu généré dynamiquement qui bénéficie de la TEP. Toutes les réponses aux e-mails (objets *.EML) possèdent un `ETag` validateur qui permet de les stocker en tant que réponses TEP.

Chaque demande de réponse par e-mail est acheminée vers le serveur d'origine, même si la réponse est mise en cache. Le serveur d'origine détermine si le demandeur est authentifié et autorisé. Il vérifie également que la réponse existe sur le serveur d'origine. Si tous les résultats sont positifs, le serveur d'origine envoie une réponse 304 Non modifiée.

Configurer le cache intégré en tant que proxy de transfert

May 5, 2023

Le cache intégré peut servir de périphérique proxy de transfert qui transmet les demandes à d'autres appliances NetScaler ou à d'autres types de serveurs de cache. Vous configurez le cache intégré en tant que proxy de transfert en identifiant les adresses IP du ou des serveurs de cache. Après avoir configuré le proxy de transfert, l'appliance NetScaler envoie des demandes contenant l'adresse IP configurée au serveur de cache au lieu d'impliquer le cache intégré.

Pour configurer NetScaler en tant que proxy de cache direct à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add cache forwardProxy <IPAddress> <port>
```

Pour configurer NetScaler en tant que proxy de cache direct à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Mise en cache intégrée** > Proxy de **transfert**, puis ajoutez un proxy de transfert en spécifiant l'adresse IP et le numéro de port.

Paramètres par défaut pour le cache intégré

May 5, 2023

La fonctionnalité de cache intégré de NetScaler fournit des politiques intégrées avec des paramètres par défaut et des paramètres initiaux pour le groupe de contenus par défaut. Les informations de cette section définissent les paramètres des politiques intégrées et du groupe de contenus par défaut.

Politiques de mise en cache par défaut

Le cache intégré comporte des politiques intégrées. L'appliance NetScaler évalue les politiques dans un ordre particulier, comme indiqué dans les sections suivantes.

Vous pouvez remplacer ces politiques intégrées par une politique définie par l'utilisateur qui est liée à une banque de règles de remplacement au moment de la demande ou au temps de réponse.

> **Remarque**
> Si vous avez configuré des stratégies avant la version 9.0 et que vous avez spécifié le paramètre -precedeDefRules lors de la liaison des stratégies, elles sont automatiquement affectées aux points de liaison de dépassement pendant la migration.

Afficher les politiques par défaut

Les noms des politiques intégrés commencent par un trait de soulignement (_). Vous pouvez consulter les politiques intégrées à partir de la ligne de commande et de la console d'administration à l'aide de la commande show cache policy.

Politiques de demande par défaut

Vous pouvez remplacer les politiques de délai de requête intégrées suivantes en configurant de nouvelles politiques et en les liant au point de traitement de la dérogation au moment de la demande. Dans les politiques suivantes, notez que l'action MAY_NOCACHE stipule que la transaction est mise en cache uniquement lorsqu'il existe une directive CACHE configurée par l'utilisateur ou intégrée au moment de la réponse.

Les politiques suivantes sont liées à l'étiquette de politique _reqBuiltInDefaults. Ils sont classés par ordre de priorité.

Ne mettez pas en cache une réponse pour une requête utilisant une méthode autre que GET.

Le nom de la politique est _NongeTreq. Ce qui suit est la règle de stratégie :

```
!HTTP.REQ.METHOD.eq(GET)
```

Définissez une action NOCACHE pour une requête dont la valeur d'en-tête contient If-Match ou If-Unmodified-Since.

Le nom de la politique est _AdvancedConditionalReq. Ce qui suit est la règle de stratégie :

```
HTTP.REQ.HEADER("If-Match").EXISTS || HTTP.REQ.HEADER("If-Unmodified-Since"
).EXISTS
```

Définissez une action MAY_NOCACHE pour une demande avec les valeurs d'en-tête suivantes : Cookie, Authorization, Proxy-Authorization ou une demande contenant l'en-tête NTLM ou Negotiate.

Le nom de la politique est _PersonalizedReq. Ce qui suit est la règle de stratégie :

```
HTTP.REQ.HEADER("Cookie").EXISTS || HTTP.REQ.HEADER("Authorization").EXISTS
 || HTTP.REQ.HEADER("Proxy-Authorization").EXISTS || HTTP.REQ.IS_NTLM_OR_NEGOTIATE
```

Politiques de réponse par défaut

Vous pouvez remplacer les politiques de temps de réponse par défaut suivantes en configurant de nouvelles politiques et en les liant au point de traitement de remplacement du temps de réponse.

Les politiques suivantes sont liées à l'étiquette de politique **_resBuiltInDefaults** et sont évaluées dans l'ordre dans lequel elles sont répertoriées :

1. Ne mettez pas en cache les réponses HTTP sauf si elles sont de type 200, 304, 307, 203 ou si les types sont compris entre 400 et 499 ou entre 300 et 302.

   Le nom de la politique est **_UncacheableStatusRes**. Ce qui suit est la règle de stratégie :

   ```
   !((HTTP.RES.STATUS.EQ(200))|| (HTTP.RES.STATUS.EQ(304))|| (HTTP.RES.
   STATUS.BETWEEN(400,499))|| (HTTP.RES.STATUS.BETWEEN(300, 302))|| (HTTP.
   RES.STATUS.EQ(307))|| (HTTP.RES.STATUS.EQ(203)))
   ```

2. Ne mettez pas en cache une réponse HTTP si elle possède un en-tête Vary dont la valeur est autre que Accept-Encoding.

   Le module de compression insère l'en-tête Vary : Accept_Encoding. Le nom de cette expression est **_UncacheableVaryRes**. Ce qui suit est la règle de stratégie :

   ```
   ((HTTP.RES.HEADER("Vary").EXISTS)&& ((HTTP.RES.HEADER("Vary").INSTANCE
   (1).LENGTH > 0)|| (!HTTP.RES.HEADER("Vary").STRIP_END\\_WS.SET_TEXT_MODE
   (IGNORECASE).eq("Accept-Encoding"))))
   ```

3. Ne mettez pas en cache une réponse si la valeur de son en-tête Cache-Control est No-Cache, No-Store ou Private, ou si l'en-tête Cache-Control n'est pas valide.

   Le nom de la politique est **_UncacheableCacheControlRes**. Ce qui suit est la règle de stratégie :

   ```
   ((HTTP.RES.CACHE\\_CONTROL.IS\\_PRIVATE)|| (HTTP.RES.CACHE\\_CONTROL.IS
   \\_NO\\_CACHE)|| (HTTP.RES.CACHE\\_CONTROL.IS\\_NO\\_STORE)|| (HTTP.RES
   .CACHE\\_CONTROL.IS\\_INVALID))
   ```

4. Mache les réponses si l'en-tête Cache-Control possède l'une des valeurs suivantes : Public, Must-Revalidate, Proxy-Revalidate, Max-Age, S-Maxage.

   Le nom de la politique est **_CacheableCacheControlRes**. Ce qui suit est la règle de stratégie :


```
((HTTP.RES.CACHE_CONTROL.IS_PUBLIC)|| (HTTP.RES.CACHE_CONTROL.IS_MAX_AGE
)|| (HTTP.RES.CACHE_CONTROL.IS_MUST_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL
.IS_PROXY_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL.IS_S_MAXAGE))
```

5. Ne mettez pas en cache les réponses qui contiennent un en-tête Pragma.

   Le nom de la politique est **_UncacheablePragmares**. Ce qui suit est la règle de stratégie :

   ```
   HTTP.RES.HEADER("Pragma").EXISTS
   ```

6. Mettez en cache les réponses qui contiennent un en-tête Expires.

   Le nom de la politique est **_CacheableExpiryRes**. Ce qui suit est la règle de stratégie :

   ```
   HTTP.RES.HEADER("Expires").EXISTS
   ```

7. Si la réponse contient un en-tête Content-Type dont la valeur est Image, supprimez tous les cookies de l'en-tête et mettez-le en cache.

   Le nom de la politique est **_ImageRes**. Ce qui suit est la règle de stratégie :

   ```
   HTTP.RES.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).STARTSWITH("
   image/")
   ```

   Vous pouvez configurer le groupe de contenu suivant pour qu'il fonctionne avec cette politique :

   ```
   add cache contentgroup nocookie -group -removeCookies YES
   ```

8. Ne mettez pas en cache une réponse contenant un en-tête Set-Cookie.

   Le nom de la politique est **_ PersonalizedRes**. Ce qui suit est la règle de stratégie :

HTTP.RES.HEADER (« Définir le cookie ») .EXISTS	HTTP.RES.HEADER("Set-Cookie2").EXISTS

Restrictions relatives aux politiques par défaut

Vous ne pouvez pas remplacer les politiques de temps de demande intégrées suivantes par des politiques définies par l'utilisateur.

Ces politiques sont répertoriées par ordre de priorité.

1. Ne mettez aucune réponse en cache si la requête HTTP correspondante ne possède pas de méthode GET ou POST.
2. Ne mettez pas en cache les réponses à une demande si la longueur de l'URL de la requête HTTP plus le nom d'hôte dépassent 1744 octets.
3. Ne mettez pas en cache une réponse à une demande contenant un en-tête If-Match.
4. Ne mettez pas en cache une requête contenant un en-tête If-Unmodified-Since.

> **Remarque**
> Ceci est différent de l'en-tête If-Modified-Since.

1. Ne mettez pas en cache une réponse si le serveur ne définit pas d'en-tête d'expiration.

Vous ne pouvez pas remplacer les règles de temps de réponse intégrées suivantes. Ces politiques sont évaluées dans l'ordre dans lequel elles sont répertoriées :

1. Ne mettez pas en cache les réponses dont le code d'état de réponse HTTP est 201, 202, 204, 205 ou 206.
2. Ne mettez pas en cache les réponses dont le code d'état de réponse HTTP est 4xx, à l'exception des codes d'état 403, 404 et 410.
3. Ne mettez pas en cache les réponses si le type de réponse est terminé par FIN ou si la réponse ne possède pas l'un des attributs suivants : longueur du contenu ou encodage de transfert : fragmenté.
4. Ne mettez pas la réponse en cache si le module de mise en cache ne parvient pas à analyser son en-tête Cache-Control.

Paramètres initiaux du groupe de contenus par défaut

Lorsque vous activez la mise en cache intégrée pour la première fois, l'appliance NetScaler fournit un groupe de contenu prédéfini nommé groupe de contenu par défaut. Pour plus d'informations, consultez le tableau des paramètres par défaut du groupe de contenu .

Dépannage

May 5, 2023

Si la fonctionnalité de cache intégrée ne fonctionne pas comme prévu après l'avoir configurée, vous pouvez utiliser certains outils courants pour accéder aux ressources NetScaler et diagnostiquer le problème.

Ressources pour le dépannage

Pour plus d'informations sur les ressources disponibles pour le dépannage et les exemples de configurations, voir le fichier PDF Resource for troubleshooting.

Optimisation frontale

May 5, 2023

> **Remarque :** L'optimisation du front end est disponible si vous possédez une licence NetScaler Advanced ou Premium et que vous exécutez NetScaler version 10.5 ou ultérieure.

Les protocoles HTTP qui sous-tendent les applications Web ont été développés à l'origine pour prendre en charge la transmission et le rendu de pages Web simples. Les nouvelles technologies telles que JavaScript et les feuilles de style en cascade (CSS), ainsi que les nouveaux types de médias tels que les vidéos Flash et les images riches en graphiques, imposent de lourdes exigences sur les performances front-end, c'est-à-dire sur les performances au niveau du navigateur.

La fonctionnalité d'optimisation du front end (FEO) de NetScaler résout ces problèmes et réduit le temps de chargement et le temps de rendu des pages Web en :

- Réduire le nombre de demandes.
- Obligatoire pour le rendu de chaque page.
- Réduction du nombre d'octets dans les réponses aux pages.

Simplification et optimisation du contenu diffusé vers le navigateur client.

Vous pouvez personnaliser votre configuration FEO pour fournir les meilleurs résultats à vos utilisateurs. NetScalers prend en charge de nombreuses optimisations de contenu Web pour les utilisateurs de bureau et mobiles. Les tableaux suivants décrivent les optimisations du front-end fournies par la fonctionnalité FEO et les opérations effectuées sur différents types de fichiers.

Optimisations effectuées par la fonction FEO

Optimisation du Web	Problème	À quoi sert la fonctionnalité NetScaler FEO	Avantages
Doublure	Les navigateurs clients envoient souvent plusieurs demandes aux serveurs pour charger des CSS externes, des images et du JavaScript associés à la page Web.	CSS en ligne, JavaScript en ligne, CSS combiner	Le chargement du CSS externe, des images et du JavaScript en ligne avec les fichiers HTML améliore le temps de rendu des pages. Cette optimisation est utile pour le contenu qui n'est visualisé qu'une seule fois et pour les appareils mobiles dont la taille de cache est limitée.
Minification	Les données extraites des serveurs incluent des caractères non essentiels tels que des espaces blancs, des commentaires et des caractères de saut de ligne. Le temps que les navigateurs passent à traiter ces données crée de la latence sur le site Web.	Minification CSS, minification JavaScript, suppression des commentaires HTML	Les fichiers minifiés consomment moins de bande passante et évitent la latence causée par un traitement spécial.

Optimisation du Web	Problème	À quoi sert la fonctionnalité NetScaler FEO	Avantages
Optimisation de l'image	Les navigateurs mobiles ont souvent des vitesses de connexion lentes et une mémoire cache limitée. Le téléchargement des images sur des clients mobiles consomme plus de bande passante, de temps de traitement et d'espace cache, ce qui entraîne une latence du site Web.	Optimisation JPEG, insertion d'image CSS, Attributs de **réduction d'image**, conversion GIF en PNG, Insertion d'image HTML, conversion d'image WebP, JPEG, GIF, conversion d'image PNG en JPEG-XR	Réduit l'image à la taille indiquée dans la balise d'image par NetScaler, ce qui permet aux navigateurs clients de charger les images plus rapidement.
Repositionnement	Le traitement inefficace du CSS externe, des images et du code JavaScript augmente le temps de chargement des pages.	Chargement paresseux de l'image, déplacement CSS vers la tête, déplacement JavaScript vers la fin	Repositionne les éléments HTML pour réduire le temps de rendu des pages Web et permettre aux navigateurs clients de charger les objets plus rapidement.

Optimisation du Web	Problème	À quoi sert la fonctionnalité NetScaler FEO	Avantages
Gestion des connexions	De nombreux navigateurs limitent le nombre de connexions simultanées pouvant être établies avec un seul domaine. Cela peut amener les navigateurs à télécharger les ressources des pages Web une par une, ce qui entraîne un temps de navigation plus long.	Partage de domaines	Surmonte la limitation de connexion, ce qui améliore le temps d'affichage des pages en permettant aux navigateurs clients de télécharger davantage de ressources en parallèle.

Optimisations Web sur différents types de fichiers :

NetScaler peut effectuer des optimisations Web sur le CSS, les images, le Javascript et le HTML. Pour plus d'informations, reportez-vous à la section Web Optimisations PDF.

> **Remarque :**
> La fonction d'optimisation frontale prend uniquement en charge les caractères ASCII. Il ne prend pas en charge le jeu de caractères Unicode.

Comment fonctionne l'optimisation du front end

Une fois que NetScaler a reçu la réponse du serveur :

1. Analyse le contenu de la page, crée une entrée dans le cache (le cas échéant) et applique la politique FEO.

   Par exemple, un NetScaler peut appliquer les règles d'optimisation suivantes :

   - Supprimez les espaces blancs ou les commentaires présents dans un CSS ou JavaScript.
   - Combinez un ou plusieurs fichiers CSS en un seul fichier.
   - Convertissez le format d'image GIF au format PNG.

2. Réécrit les objets incorporés et enregistre le contenu optimisé dans le cache, avec une signature différente de celle utilisée pour l'entrée initiale du cache.
3. Pour les demandes suivantes, extrait les objets optimisés depuis le cache, et non depuis le serveur, et transmet les réponses au client.

**

Supprimez les informations superflues telles que les espaces blancs et les commentaires.

Période pendant laquelle le navigateur peut utiliser la ressource mise en cache sans vérifier si du nouveau contenu est disponible sur le serveur.

Configurer l'optimisation du front end

Vous pouvez éventuellement modifier les valeurs des paramètres globaux d'optimisation du front end. Sinon, commencez par créer des actions qui spécifient les règles d'optimisation à appliquer aux objets incorporés.

Après avoir configuré les actions, créez des politiques, chacune avec une règle spécifiant un type de demande pour lequel optimiser la réponse, et associez les actions aux politiques.

> **Remarque :** NetScaler évalue les politiques d'optimisation du front end uniquement au moment de la demande, et non au moment de la réponse.

Pour mettre en œuvre les politiques, liez-les à des points de liaison. Vous pouvez lier une politique de manière globale, afin qu'elle s'applique à tout le trafic qui passe par NetScaler, ou vous pouvez lier la politique à un serveur virtuel d'équilibrage de charge ou de commutation de contenu de type HTTP ou SSL. Lorsque vous liez une politique, attribuez-lui une priorité. Un numéro de priorité inférieur indique une valeur plus élevée. NetScaler applique les politiques dans l'ordre de leurs priorités.

Composants requis

L'optimisation du front end nécessite l'activation de la fonctionnalité de mise en cache intégrée de NetScaler. Vous devez également effectuer les configurations de mise en cache intégrées suivantes :

- Allouez de la mémoire cache.
- Définissez la taille maximale de réponse et la limite de mémoire pour un groupe de contenu de cache par défaut.

Pour plus d'informations sur la configuration de la mise en cache intégrée, consultez la section Mise en cache intégrée.

Remarque : Le terme Cache intégré peut être utilisé de façon interchangeable avec AppCache ; notez que d'un point de vue fonctionnel, les deux termes signifient la même chose.

Configurer l'optimisation du front end à l'aide de l'interface de commande NetScaler

À l'invite de commandes, procédez comme suit :

1. Activez la fonctionnalité d'optimisation du front end.

```
enable ns feature FEO
```

1. Créez une ou plusieurs actions d'optimisation du front-end.

```
add feo action <name> [-imgShrinkToAttrib] [-imgGifToPng] ...
```

Exemple : Pour ajouter une action d'optimisation frontale pour convertir des images au format GIF au format PNG et prolonger la période d'expiration du cache :

```
add feo action allact -imgGifToPng -pageExtendCache
```

1. [Facultatif] Spécifiez des valeurs autres que celles par défaut pour les paramètres globaux d'optimisation du front end.

```
set feo parameter [-cacheMaxage <integer>] [-JpegQualityPercent <integer>]
[-cssInlineThresSize <integer>] [-inlineJsThresSize <integer> [-inlineImgThresSize
 <integer>]
```

Exemple : Pour spécifier la période d'expiration maximale du cache :

```
set feo parameter -cacheMaxage 10
```

1. Créez une ou plusieurs stratégies d'optimisation frontale.

```
add feo policy <name> <rule> <action>
```

Exemple : Pour ajouter une stratégie d'optimisation frontale et l'associer à l'action allact spécifiée ci-dessus :

```
1 >add feo policy pol1 TRUE all act
2 >add feo policy pol1 "(HTTP.REQ.URL.CONTAINS("testsite"))" allact1
3 <!--NeedCopy-->
```

1. Liez la politique à un serveur virtuel d'équilibrage de charge ou de commutation de contenu, ou liez-la globalement.

```
bind lb vserver <name> -policyName <string> -priority <num>
```

```
bind cs vserver <name> -policyName <string> -priority <num>
```

```
bind feo global <policyName> <priority> -type <type> <gotoPriorityExpression
>
```

Exemple : Pour appliquer la politique d'optimisation du front end à un serveur virtuel nommé « abc » :

```
> bind lb vserver abc -policyName pol1 -priority 1 -type NONE
```


Exemple : Pour appliquer la politique d'optimisation du front end à l'ensemble du trafic atteignant l'ADC :

```
> bind feo global pol1 100 -type REQ_DEFAULT
```

1. Enregistrez la configuration. save ns config

Configurer l'optimisation frontale à l'aide de l'interface graphique

1. Accédez à **Optimisation** > **Optimisation frontale** > **Actions**, puis cliquez sur **Ajouter** et créez une action d'optimisation frontale en spécifiant les détails pertinents.
2. [Facultatif] Spécifiez les paramètres globaux d'optimisation du front end.
3. Accédez à **Optimisation > Optimisationdu front end**, puis dans le volet droit, sous Paramètres, cliquez sur**Modifier les paramètres d'optimisation du front end** et spécifiez les paramètres globaux d'optimisation du front end.
4. Créez une stratégie d'optimisation frontale.
5. Accédez à **Optimisation > Optimisationdu front end**>**Politiques**, cliquez sur**Ajouter** et créez une politique d'optimisation du front end en spécifiant les détails pertinents.
6. Liez la stratégie à un serveur virtuel d'équilibrage de charge ou de commutation de contenu.
   a) Accédez à **Optimisation** > **Optimisation frontale** > **Stratégies**.
   b) Sélectionnez une stratégie d'optimisation frontale et cliquez sur **Gestionnaire de stratégies**.
   c) Sous **Front End Optimization Policy Manager**, liez la stratégie d'optimisation frontale à un serveur virtuel d'équilibrage de charge ou de commutation de contenu.

Vérifier la configuration de l'optimisation frontale

L'utilitaire de tableau de bord affiche un résumé et des statistiques détaillées sous forme de tableaux et de graphiques. Vous pouvez consulter les statistiques FEO pour évaluer votre configuration FEO.

En option, vous pouvez également afficher les statistiques d'une politique FEO, notamment le nombre de sélections incrémentées par le compteur de politique au cours de la FEO basée sur une politique.

> **Remarque :**
> Pour plus d'informations sur les statistiques et les graphiques, consultez l'aide du tableau de bord sur l'appliance NetScaler.

Afficher les statistiques FEO à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour afficher un résumé des statistiques FEO, la sélection et les détails de la stratégie FEO, ainsi que les statistiques FEO détaillées, respectivement :

- `stat feo` Remarque : La commande stat feo policy affiche des statistiques uniquement pour les stratégies FEO avancées.
- `show feo policy name`
- `stat feo -detail`

Afficher les statistiques FEO sur le tableau de bord NetScaler

Dans l'interface graphique du tableau de bord, vous pouvez :

- Sélectionnez Optimisation du front end pour afficher un résumé des `FEO` statistiques.
- Cliquez sur l'onglet **Affichage graphique** pour afficher le taux de demandes traitées par la fonction FEO.

Optimisation des échantillons :

Reportez-vous à l' exemple de PDF pour obtenir des exemples d'actions d'optimisation du contenu appliquées au contenu HTML et aux objets incorporés dans le contenu HTML.

Classification des médias

May 5, 2023

Comprendre le type de trafic sur le réseau aide les administrateurs réseau à gérer la consommation de bande passante afin d'optimiser les performances du réseau. Le mode de classification des médias surveille et affiche les statistiques du trafic multimédia passant par l'appliance NetScaler.

Lorsque ce mode est activé, un administrateur réseau peut collecter des statistiques indiquant la quantité de données consultées et les types d'appareils à partir desquels les fichiers multimédia ont été consultés. L'appliance NetScaler prend également en charge les demandes de plage d'octets dans ce mode.

Actuellement, l'appliance NetScaler peut surveiller et afficher des statistiques pour les types de fichiers multimédia suivants :

Média	Type de fichier
Microsoft Smooth Streaming	Vidéo
Diffusion en direct avec Apple	Vidéo
Flux de transport de données audio (ADTS)	Audio
Codage audio avancé (AAC)	Audio
Vidéo Flash (FLV)	Audio et vidéo

Média	Type de fichier
3GP	Audio et vidéo

L'appliance peut afficher les statistiques des appareils suivants :

Plate-forme de l'appareil	Type d'appareil
iOS	iPad et iPod
Android	Mobiles et tablettes
Ordinateur portable ou de bureau	Ordinateurs portables et de bureau Windows
Autres	Autres appareils mobiles (mobiles et tablettes)

Les administrateurs réseau peuvent consulter les compteurs de statistiques suivants pour connaître la quantité de données accessibles via l'appliance NetScaler pour différents types de trafic multimédia.

Nom du fichier multimédia	Compteur de statistiques
Microsoft Smooth Streaming	`mcmssmthstrmvid`—Ce compteur enregistre le nombre total de vidéos Microsoft Smooth Streaming diffusées par l'appliance NetScaler ;`Mcmssmthstrvidpl`—Ce compteur enregistre le nombre total de listes de lecture vidéo Microsoft Smooth Streaming diffusées par l'appliance NetScaler ;`Mcmssmthstrmvidbytes`—Ce compteur enregistre le nombre total d'octets de données servis pour le trafic multimédia Microsoft Smooth Streaming sur l'appliance NetScaler ;`Mcmssmthstrmplvidbytespl`—Ce compteur enregistre le nombre total d'octets de playlist Microsoft Smooth Streaming servis par l'appliance NetScaler.

Nom du fichier multimédia	Compteur de statistiques
Diffusion en direct avec Apple	mccaplelivestrmngvid—Ce compteur enregistre le nombre total de vidéos Apple Live Streaming diffusées par l'appliance NetScaler. Mccapplelivestrmngvidpl : ce compteur enregistre le nombre total de playlists vidéo Apple Live Streaming diffusées par l'appliance NetScaler.Mcapplelivestreamingvidbytes—Ce compteur enregistre le nombre total d'octets de données diffusés pour le trafic multimédia Apple Live Streaming sur l'appliance NetScaler.Mcapplelivestreamingplaylistvidbytespl—Ce compteur enregistre le nombre total d'octets d'Apple Live Playlist servis par l'appliance NetScaler.
Flux de transport de données audio (ADTS)	mcadtsaudio—Ce compteur enregistre le nombre total de clips audio ADTS diffusés par l'appliance NetScaler.Mcadtsaudiobytes—Ce compteur enregistre le nombre total d'octets de données servis pour le trafic multimédia ADTS sur l'appliance NetScaler.
Codage audio avancé (AAC)	Mcaacaudio—Ce compteur enregistre le nombre total de clips audio AAC diffusés par l'appliance NetScaler.Mcaacaudiobytes—Ce compteur enregistre le nombre total d'octets de données servis pour le trafic multimédia AAC sur l'appliance NetScaler.
Vidéo Flash (FLV)	Mcflvvid—Ce compteur enregistre le nombre total de vidéos Flash diffusées par l'appliance NetScaler.Mcflvvidbytes—Ce compteur enregistre le nombre total d'octets de données diffusés pour les vidéos Flash sur l'appliance NetScaler.

Nom du fichier multimédia	Compteur de statistiques
3GP	`mc3gpvidbytes`—Ce compteur enregistre le nombre total d'octets de données servis pour le trafic multimédia 3GP sur l'appliance NetScaler.

L'appliance NetScaler détecte les types de fichiers multimédia en fonction de leurs signatures dans les *premiers octets du corps* des réponses. Par exemple, les octets initiaux du corps d'un fichier mp4 portent la signature suivante dans la réponse :

```
**....ftypmp42** ....isommp42....moov...lmvhd.....c.\!.c.\!..
```

L'appliance NetScaler détecte le type d'appareil client à l'aide de la *chaîne d'agent utilisateur* que l'appareil client inclut dans la requête HTTP GET. Par exemple, un Window Phone utilisant un navigateur UC contient la chaîne d'agent utilisateur suivante dans la requête HTTP GET :

```
User-Agent: **UCWEB**/2.0 (**Windows**; U; wds 8.10; en-US; HTC; 8X by HTC)
U2/1.0.0
```

Activer la classification des médias

Par défaut, la classification des médias est désactivée sur l'appliance NetScaler. Vous devez activer le mode avant de l'utiliser.

Pour activer la classification des médias à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
enable ns mode Mediaclassification
```

Pour activer la classification des médias à l'aide de l'interface graphique

Activer la classification des médias sur l'appliance NetScaler

Accédez à **Système** > **Paramètres** > **Configurer les modes** et sélectionnez **Classification des supports**.

Pour afficher les statistiques du trafic multimédia sur l'appliance NetScaler

Accédez à **Optimisation** et cliquez sur **Classification des médias** pour afficher les statistiques du trafic multimédia.

Vérifiez les statistiques de classification des médias

Vous pouvez consulter les statistiques du trafic multimédia dans l'utilitaire du tableau de bord ou à l'aide de l'interface de ligne de commande. L'utilitaire de tableau de bord affiche des statistiques

récapitulatives et détaillées sous forme de tableau et de graphique.

> **Remarque**
> Pour plus d'informations sur les statistiques et les graphiques, consultez l'aide du tableau de bord sur votre appliance NetScaler.

Pour afficher les statistiques de classification des médias à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour afficher un résumé des statistiques de classification des médias, afficher des statistiques détaillées ou effacer l'affichage :

```
stat Mediaclassification
```

```
stat Mediaclassification -detail
```

```
stat Mediaclassification -clearstats
```

Pour afficher les statistiques de classification des médias sur le tableau de bord

Dans l'utilitaire **Dashboard**, vous pouvez afficher les types suivants de statistiques de classification des médias :

1. Sélectionnez **Classification des médias** pour afficher un résumé des statistiques relatives au trafic multimédia.
2. Pour afficher des statistiques détaillées sur le trafic multimédia, cliquez sur **Détails**.
3. Pour effacer les statistiques du trafic multimédia, cliquez sur **Effacer**.

Réputation

May 5, 2023

NetScaler propose une sécurité basée sur la réputation. À l'aide de l'évaluation de la réputation pour déterminer le risque lié au traitement des demandes, vous pouvez prendre des mesures telles que bloquer ou abandonner certaines demandes afin d'améliorer les performances de votre application.

La fonctionnalité de réputation IP de NetScaler utilise des contrôles de réputation IP pour empêcher les attaques Zero Day et fournir une protection contre les sources malveillantes associées aux attaques Web, aux activités de phishing ou à l'analyse Web.

Pour plus de détails, voir Réputation IP.

Réputation IP

May 5, 2023

La réputation IP est un outil qui identifie les adresses IP qui envoient des demandes indésirables. À l'aide de la liste de réputation IP, vous pouvez rejeter les demandes provenant d'une adresse IP de mauvaise réputation. Optimisez les performances du pare-feu des applications Web en filtrant les demandes que vous ne souhaitez pas traiter. Réinitialisez, abandonnez une demande ou même configurez une stratégie de répondeur pour qu'elle entreprenne une action de répondeur spécifique.

Voici quelques attaques que vous pouvez prévenir en utilisant la réputation IP :

- **Ordinateurs personnels infectés par un virus**. (PC personnels) sont la principale source de spam sur Internet. La réputation IP peut identifier l'adresse IP qui envoie des demandes indésirables. La réputation IP peut être particulièrement utile pour bloquer les attaques DDoS, DoS ou inondation SYN anormale à grande échelle provenant de sources infectées connues.
- **Botnet géré et automatisé de manière centralisée**. Les attaquants ont gagné en popularité pour le vol de mots de passe, car il ne faut pas longtemps lorsque des centaines d'ordinateurs travaillent ensemble pour déchiffrer votre mot de passe. Il est facile de lancer des attaques de botnets pour trouver des mots de passe qui utilisent des mots de passe couramment utilisés dans le dictionnaire.
- **Serveur Web compromis**. Les attaques ne sont pas aussi fréquentes car la sensibilisation et la sécurité des serveurs ont augmenté, de sorte que les pirates et les spammeurs recherchent des cibles plus faciles. Il existe encore des serveurs Web et des formulaires en ligne que les pirates informatiques peuvent compromettre et utiliser pour envoyer des spams (tels que des virus et de la pornographie). Une telle activité est plus facile à détecter et à arrêter rapidement, ou à bloquer avec une liste de réputation telle que SpamRATS.
- **Exploits Windows**. (telles que les adresses IP actives proposant ou distribuant des logiciels malveillants, du code shell, des rootkits, des vers ou des virus).
- **Spammeurs et hackers connus**.
- **Campagnes de marketing par e-mail de masse**
- **Proxys d'hameçonnage** (adresses IP hébergeant des sites d'hameçonnage et autres fraudes telles que la fraude par clic publicitaire ou la fraude aux jeux).
- **Proxys anonymes** (IP fournissant des services de proxy et d'anonymisation, y compris The Onion Router alias TOR).

Une appliance NetScaler utilise **Webroot** comme fournisseur de services pour une base de données IP malveillante générée dynamiquement et les métadonnées de ces adresses IP. Les métadonnées peuvent inclure des détails de géolocalisation, une catégorie de menace, un nombre de menaces, etc. Le moteur Webroot Threat Intelligence reçoit des données en temps réel de millions de capteurs. Il capture, analyse, analyse et note automatiquement et en continu les données, à l'aide d'un apprentissage automatique avancé et d'une analyse comportementale. Les renseignements concernant une menace sont continuellement mis à jour.

L'appliance NetScaler valide une demande entrante pour détecter sa mauvaise réputation à l'aide de la base de données de réputation IP Uses de Webroot. La base de données contient une vaste collec-

tion de catégories de menaces IP classées par adresse IP. Vous trouverez ci-dessous les catégories de menaces IP et leur description.

- Sources de spam. Les sources de spam incluent le tunneling des messages de spam via un proxy, des activités SMTP anormales, des activités de spam sur le forum.
- Exploits Windows. La catégorie d'exploits Windows comprend l'adresse IP active offrant ou distribuant des logiciels malveillants, du code shell, des rootkits, des vers ou des virus
- Attaques Web. La catégorie des attaques Web comprend les scripts intersites, l'injection iFrame, l'injection SQL, l'injection interdomaines ou l'attaque par force brute par mot de passe de domaine
- Les botnets. La catégorie Botnet comprend les canaux C&C de botnet et la machine zombie infectée contrôlée par Bot Master
- Scanners. La catégorie Scanners comprend toutes les reconnaissances telles que les sondes, l'analyse de l'hôte, l'analyse de domaine et l'attaque par force brute
- Déni de service. La catégorie de déni de services comprend DOS, DDOS, inondation de synchronisation anormale, détection de trafic anormal
- Réputation. Refuser l'accès depuis les adresses IP actuellement connues pour être infectées par des logiciels malveillants. Cette catégorie comprend également les adresses IP dont le score moyen de l'indice de réputation Webroot est faible. L'activation de cette catégorie empêchera l'accès depuis les sources identifiées pour contacter les points de distribution de logiciels malveillants
- Hameçonnage La catégorie hameçonnage comprend les adresses IP hébergeant des sites de phishing, d'autres types d'activités frauduleuses telles que la fraude au clic publicitaire ou la fraude
- Proxy. La catégorie Proxy comprend les adresses IP fournissant des services proxy et def.
- Menaces mobiles. La catégorie Menace mobile comprend les adresses IP des applications mobiles malveillantes et indésirables. Cette catégorie exploite les données de l'équipe de recherche sur les menaces mobiles de Webroot.
- Proxy Tor. La catégorie de proxy Tor comprend les adresses IP agissant en tant que nœuds de sortie pour le réseau Tor. Les nœuds de sortie sont le dernier point de la chaîne de proxy et établissent une connexion directe avec la destination prévue de l'initiateur.

Lorsqu'une menace est détectée n'importe où sur le réseau, l'adresse IP est signalée comme malveillante et toutes les appliances connectées au réseau sont immédiatement protégées. Les modifications dynamiques des adresses IP sont traitées avec une vitesse et une précision élevées grâce à l'apprentissage automatique avancé.

Comme indiqué dans la fiche technique de Webroot, le réseau de capteurs de Webroot identifie de nombreux types de menaces IP clés, notamment les sources de spam, les exploits Windows, les botnets, les scanners, etc. (Voir le diagramme de flux sur la fiche technique.)

L'appliance NetScaler utilise un processus `iprep` client pour obtenir la base de données depuis We-

broot. Le `iprep` client utilise la méthode HTTP GET pour obtenir la liste des adresses IP absolues de Webroot pour la première fois. Plus tard, il vérifie les changements de delta une fois toutes les 5 minutes.

> **Important :**
>
> - Assurez-vous que l'appliance NetScaler dispose d'un accès Internet et que le DNS est configuré avant d'utiliser la fonctionnalité de réputation IP.
> - **Pour accéder à la base de données Webroot, l'appliance NetScaler doit pouvoir se connecter à**api.bcti.brightcloud.com**sur le port 443.** Chaque nœud du déploiement HA ou de cluster obtient la base de données de Webroot et doit pouvoir accéder à ce nom de domaine complet (FQDN).
> - Webroot héberge actuellement sa base de données de réputation dans AWS. NetScaler doit donc être en mesure de résoudre les domaines AWS pour le téléchargement de la base de données de réputation. En outre, le pare-feu doit être ouvert pour les domaines AWS.
>
> **Remarque :**
>
> Chaque moteur de paquets nécessite au moins 4 Go pour fonctionner correctement lorsque la fonctionnalité de réputation IP est activée.

Expressions de stratégie avancées. Configurez la fonctionnalité de réputation IP à l'aide d'expressions de stratégie avancées (expressions de stratégie avancées) dans les stratégies liées aux modules pris en charge, tels que le pare-feu d'application Web et le répondeur. Voici deux exemples d'expressions qui peuvent être utilisées pour détecter si l'adresse IP du client est malveillante.

1. **CLIENT.IP.SRC.IPREP_IS_MALICIOUS** : Cette expression renvoie la valeur TRUE si le client est inclus dans la liste des adresses IP malveillantes.
2. **CLIENT.IP.SRC.IPREP_THREAT_CATEGORY (CATEGORY)** : Cette expression renvoie la valeur TRUE si l'adresse IP du client est une adresse IP malveillante et se trouve dans la catégorie de menace spécifiée.
3. **CLIENT.IPV6.SRC.IPREP_IS_MALICIOUS and CLIENT.IPV6.SRC.IPREP_THREAT_CATEGORY** : Cette expression est évaluée à TRUE si l'IP du client est de type IPv6 et qu'il s'agit d'une adresse IP malveillante dans une catégorie de menace spécifiée.

Voici les valeurs possibles pour la catégorie de menace :

SPAM_SOURCES, WINDOWS_EXPLOITS, WEB_ATTACKS, BOTNETS, SCANNERS, DOS, REPUTATION, PHISHING, PROXY, NETWORK, CLOUD_PROVIDERS, MOBILE_THREATS, TOR_PROXY.

> **Remarque :**
>
> La fonctionnalité de réputation IP vérifie les adresses IP source et de destination. Il détecte les adresses IP malveillantes dans l'en-tête. Si l'expression PI d'une stratégie peut identifier l'adresse IP, la vérification de réputation IP détermine si elle est malveillante.

Message du journal iPrep. Le fichier `/var/log/iprep.log` contient des messages utiles qui capturent des informations sur la communication avec la base de données Webroot. Les informations peuvent porter sur les informations d'identification utilisées lors de la communication Webroot, l'échec de la connexion à Webroot, les informations incluses dans une mise à jour (telles que le nombre d'adresses IP dans la base de données).

Création d'une liste de blocage ou d'une liste d'adresses IP autorisées à l'aide d'un ensemble de données de stratégie. Vous pouvez maintenir une liste d'autorisation pour autoriser l'accès à des adresses IP spécifiques qui sont bloquées dans la base de données Webroot. Vous pouvez également créer une liste de blocage personnalisée d'adresses IP pour compléter le contrôle de réputation Webroot. Ces listes peuvent être créées à l'aide d'un **jeu de données de**stratégie. Un ensemble de données est une forme spécialisée de jeu de modèles parfaitement adapté à la correspondance d'adresses IPv4 ou IPv6. Pour utiliser des ensembles de données, commencez par créer l'ensemble de données et liez les adresses IPv4 ou IPv6 à celui-ci. Lorsque vous configurez une stratégie de comparaison d'une chaîne dans un paquet, utilisez un opérateur approprié et transmettez le nom du jeu de motifs ou du jeu de données en tant qu'argument.

Pour créer une liste d'adresses autorisées à traiter comme des exceptions lors de l'évaluation de la réputation IP, procédez comme suit :

- Configurez la stratégie de sorte que l'expression PI donne la valeur False même si une adresse de la liste d'autorisation est répertoriée comme malveillante par Webroot (ou tout autre fournisseur de services).

Activation ou désactivation de la réputation IP. La réputation IP fait partie de la fonctionnalité de réputation générale, qui est basée sur la licence. Lorsque vous activez ou désactivez la fonctionnalité de réputation, elle active ou désactive la réputation IP.

Procédure générale. Le déploiement de la réputation IP implique les tâches suivantes :

- Vérifiez que la licence installée sur l'appliance NetScaler prend en charge la réputation IP. Les licences de pare-feu d'application Premium et autonome prennent en charge la fonctionnalité de réputation IP.
- Activez les fonctionnalités de réputation IP et de pare-feu d'application.
- Ajoutez un profil de pare-feu d'application.
- Ajoutez une stratégie de pare-feu d'application à l'aide des expressions PI pour identifier les adresses IP malveillantes dans la base de données de réputation IP.
- Liez la stratégie de pare-feu d'application à un point de liaison approprié.
- Vérifiez que toute demande reçue d'une adresse malveillante est consignée dans le fichier `ns.log` pour montrer que la demande a été traitée comme indiqué dans le profil.

Configurez la fonctionnalité de réputation IP à l'aide de la CLI

À l'invite de commande, tapez :

- `enable feature reputation`
- `disable feature reputation`

Les exemples suivants montrent comment ajouter une stratégie de pare-feu d'application à l'aide de l'expression PI pour identifier les adresses malveillantes. Vous pouvez utiliser les profils intégrés, ajouter un profil ou configurer un profil existant pour appeler l'action souhaitée lorsqu'une demande correspond à une correspondance de stratégie.

Les exemples 3 et 4 montrent comment créer un jeu de données de stratégie pour générer une liste de blocage ou une liste d'adresses IP autorisées.

Exemple 1 :

La commande suivante crée une stratégie qui identifie les adresses IP malveillantes et bloque la demande en cas de déclenchement d'une correspondance :

```
add appfw policy pol1 CLIENT.IP.SRC.IPREP_IS_MALICIOUS APPFW_BLOCK
add appfw policy pol1 CLIENT.IPv6.SRC.IPREP_IS_MALICIOUS APPFW_BLOCK
add appfw policy pol1 "HTTP.REQ.HEADER(\"X-Forwarded-For\").TYPECAST_IPv6_ADDRESS_AT
.IPREP_IS_MALICIOUS"APPFW_RESET
```

Exemple 2 :

La commande suivante crée une stratégie qui utilise le service de réputation pour vérifier l'adresse IP du client dans l'en-tête `X-Forwarded-For` et réinitialiser la connexion si une correspondance est déclenchée.

```
> add appfw policy pol1 "HTTP.REQ.HEADER(\"X-Forwarded-For\").TYPECAST_IP_ADDRESS_AT
.IPREP_IS_MALICIOUS"APPFW_RESET**
```

Exemple 3 :

L'exemple suivant montre comment ajouter une liste pour ajouter des exceptions autorisant des adresses IP spécifiées :

```
> add policy dataset Allow_list1 ipv4

> bind policy dataset Allow_list1 10.217.25.17 -index 1

> bind policy dataset Allow_list1 10.217.25.18 -index 2
```

L'exemple suivant montre comment ajouter une liste pour ajouter des exceptions qui autorisent les adresses IPv6 spécifiées :

```
1 add policy dataset Allow_list_ipv6 ipv6
2 bind policy dataset Allow_list_ipv6 fe80::98c7:d8ff:fe3a:b562 -index 1
3 bind policy dataset Allow_list_ipv6 fe80::98c7:d8ff:fe3a:b563  -index 2
4
5 <!--NeedCopy-->
```


Exemple 4 :

L'exemple suivant montre comment ajouter la liste personnalisée pour signaler les adresses IP spécifiées comme malveillantes :

```
> add policy dataset Block_list1 ipv4

> bind policy dataset Block_list1 10.217.31.48 -index 1

> bind policy dataset Block_list1 10.217.25.19 -index 2
```

L'exemple suivant montre comment ajouter la liste personnalisée pour signaler les adresses IPv6 spécifiées comme malveillantes.

```
1 add policy dataset Block_list_ipv6 ipv6
2 bind policy dataset Block_list_ipv6 fe80::98c7:d8ff:ff3b:b562 -index 1
3 bind policy dataset Block_list_ipv6 fe80::ffc7:d8ff:fe3a:b562 -index 2
4 <!--NeedCopy-->
```

Exemple 5 :

L'exemple suivant illustre une expression de stratégie pour bloquer l'adresse IP du client dans les conditions suivantes :

- Il correspond à une adresse IP configurée dans le block_list1 personnalisé (exemple 4)
- Il correspond à une adresse IP répertoriée dans la base de données Webroot, sauf si elle est assouplie par inclusion dans la liste Allow_List1 (exemple 3).

```
1 > add appfw policy "Ip_Rep_Policy" "((CLIENT.IP.SRC.IPREP_IS_MALICIOUS
     || CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("Block_list1")) && ! (
     CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("Allow_list1")))"
     APPFW_BLOCK
2 <!--NeedCopy-->
```

L'exemple suivant montre une expression de stratégie pour bloquer l'IPv6 client dans les conditions suivantes :

1. Il correspond à une adresse IPv6 configurée dans le block_list_ipv6 personnalisé (exemple 4)
2. Il correspond à une adresse Ipv6 répertoriée dans la base de données Webroot, sauf si elle est assouplie par inclusion dans Allow_list_IPv6 (exemple 3).

```
1 add appfw policy "Ip_Rep_v6_Policy" "((CLIENT.IPV6.SRC.
     IPREP_IS_MALICIOUS || CLIENT.IPV6.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("
     Block_list_ipv6")) && ! (CLIENT.IPV6.SRC.TYPECAST_TEXT_T.
     CONTAINS_ANY("Allow_list_ipv6")))" APPFW_BLOCK
2 <!--NeedCopy-->
```

Utilisation du serveur proxy :

Si l'appliance NetScaler ne dispose pas d'un accès direct à Internet et est connectée à un proxy, configurez le client IP Reputation pour qu'il envoie des demandes au proxy.

Configurez un nom d'utilisateur et un mot de passe proxy sur le serveur proxy pour renforcer la sécurité de votre appliance.

À l'invite de commande, tapez :

```
set reputation settings -proxyServer <proxy server ip> -proxyPort <proxy
server port> -proxyUsername <username> -proxyPassword <password>
```

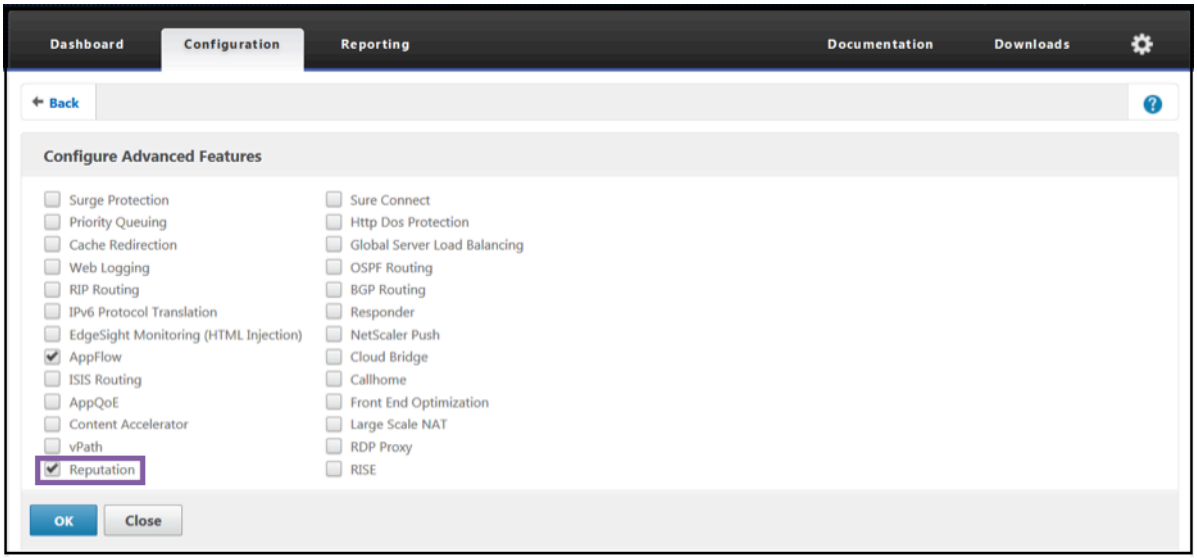
Exemple :

```
> set reputation settings proxyServer 10.102.30.112 proxyPort 3128 -proxyUsername
 defaultusername -proxyPassword defaultpassword

> set reputation settings -proxyServer testproxy.citrite.net -proxyPort 3128
 -proxyUsername defaultusername -proxyPassword defaultpassword

> unset reputation settings -proxyserver -proxyport -proxyUsername -proxyPassword


> sh reputation settings
```

> **Remarque :**
>
> L'adresse IP du serveur proxy peut être une adresse IP ou un nom de domaine complet (FQDN).

Configuration de la réputation IP à l'aide de l'interface graphique NetScaler

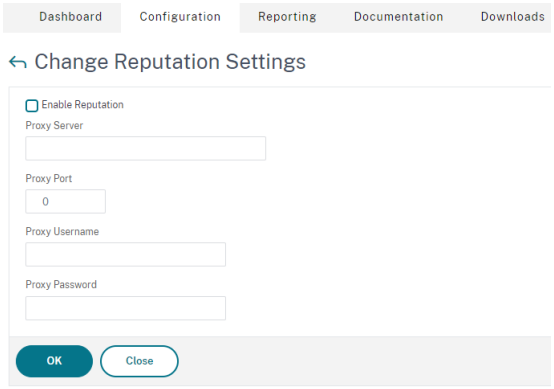
1. Accédez au **système > aux paramètres**. Dans la section **Modes et fonctionnalités**, cliquez sur le lien pour accéder au volet **Configurer les fonctionnalités avancées** et activez la case à cocher **Réputation** .
2. Cliquez sur **OK**.



Pour configurer un serveur proxy à l'aide de l'interface graphique NetScaler

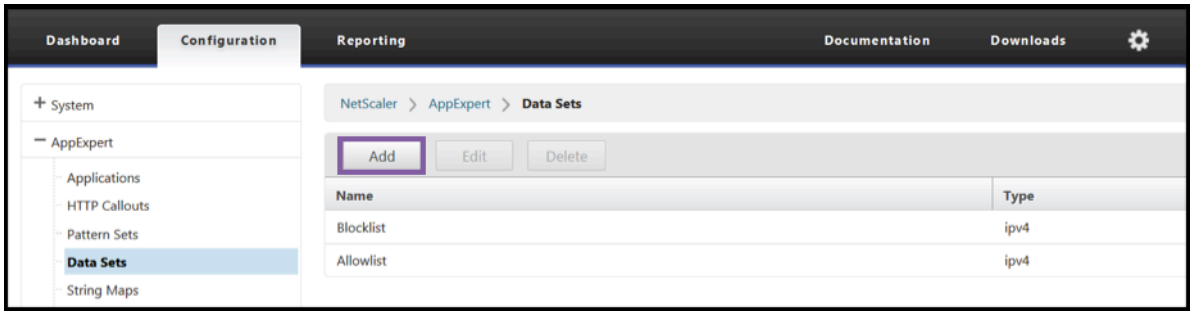
1. Dans l'onglet **Configuration**, accédez à **Sécurité > Réputation**.
2. Sous **Paramètres**, cliquez sur **Modifier les paramètres de réputation** pour configurer un serveur proxy.
3. Activez ou désactivez la fonctionnalité de réputation.
4. Entrez les informations suivantes pour configurer le serveur proxy :
   a) **Serveur proxy** : il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).
   b) **Port proxy** : il accepte des valeurs comprises entre [1 et 65535].
   c) **Nom d'utilisateur du proxy** : fournissez un nom d'utilisateur pour l'authentification du serveur proxy.
   d) **Mot de passe du proxy** : fournissez un mot de passe pour l'authentification du serveur proxy.

   > **Remarque :**
   > Les champs ProxyUserName et ProxyPassword sont activés si les champs Proxy-Server et ProxyPort sont configurés.

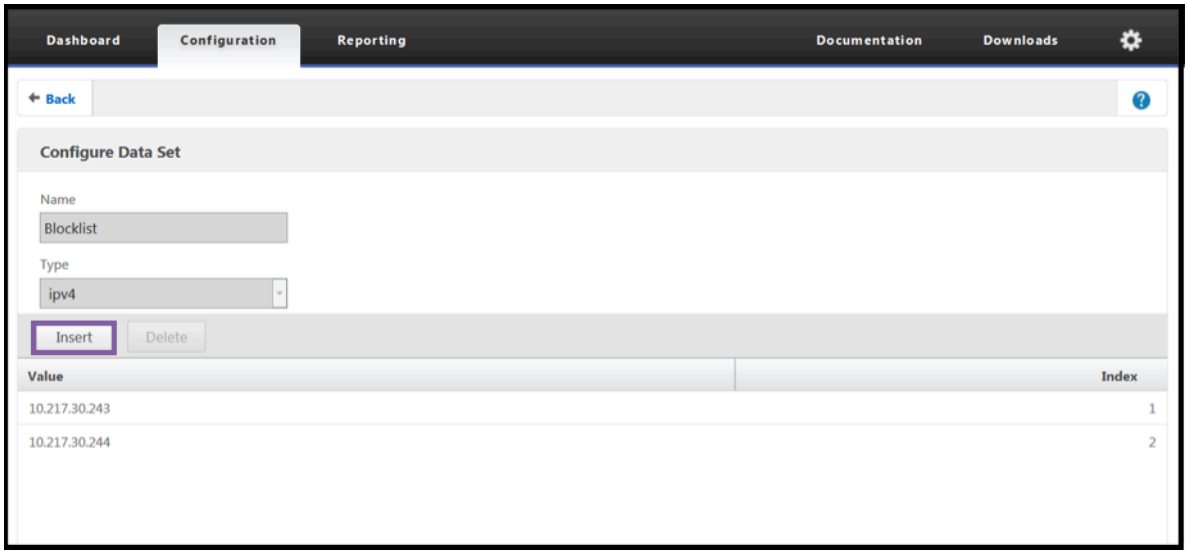


Créer une liste d'autorisation et une liste de blocage des adresses IP des clients à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, accédez à **AppExpert > Jeux de données**.
2. Cliquez sur **Ajouter**.



- Dans le volet **Créer un ensemble de données** (ou **Configurer un ensemble de données**), indiquez un nom significatif pour la liste des adresses IP. Le nom doit refléter l'objectif de la liste.
- Sélectionnez **Type** en tant qu' **IPv4** ou **IPv6**.
- Cliquez sur **Insérer** pour ajouter une entrée.



- Dans le volet de **liaison Configurer le jeu de données de stratégie**, ajoutez une adresse IP au format IPv4 ou IPv6 dans la zone de saisie Valeur.
- Fournissez un index.
- Ajoutez un commentaire qui explique l'objectif de la liste. Cette étape est facultative, mais elle est recommandée car un commentaire descriptif est utile pour gérer la liste.

De même, vous pouvez créer une liste de blocage et ajouter les adresses IP qui doivent être considérées comme malveillantes.

Reportez-vous également à la section Jeux de modèles et jeux de données pour plus de détails sur l'utilisation des jeux de données et la configuration des expressions de stratégie avancées.

Configuration d'une politique de pare-feu d'application à l'aide de l'interface graphique NetScaler

1. Dans l'onglet **Configuration**, accédez à **Sécurité > Pare-feu d'application > Stratégies > Pare-feu**. Cliquez sur **Ajouter** pour ajouter une stratégie à l'aide des expressions PI afin d'utiliser la réputation IP.

Vous pouvez également utiliser l'éditeur d'expressions pour créer votre propre expression de stratégie. La liste présente les options préconfigurées qui sont utiles pour configurer une expression à l'aide des catégories de menaces.

Résumé

- Bloque rapidement et précisément le mauvais trafic à la périphérie du réseau provenant d'adresses IP malveillantes connues qui posent différents types de menaces. Vous pouvez bloquer la demande sans analyser le corps.
- Configurez dynamiquement la fonctionnalité de réputation IP pour plusieurs applications.
- Sécurisez votre réseau contre les violations de données sans nuire aux performances, et consolidez les protections sur une structure de services unique grâce à des déploiements rapides et faciles.
- Vous pouvez effectuer des vérifications de réputation IP sur les adresses IP source et de destination.
- Vous pouvez également inspecter les en-têtes pour détecter les adresses IP malveillantes.
- La vérification de la réputation IP est prise en charge dans les déploiements de proxy direct et de proxy inverse.
- Le processus de réputation IP se connecte à Webroot et met à jour la base de données toutes les 5 minutes.
- Chaque nœud du déploiement High Availability (HA) ou Cluster obtient la base de données de Webroot.
- Les données de réputation IP sont partagées entre toutes les partitions des déploiements de partition d'admin-partition.
- Vous pouvez utiliser un ensemble de données AppExpert pour créer des listes d'adresses IP afin d'ajouter des exceptions pour les adresses IP bloquées dans la base de données Webroot. Vous pouvez également créer votre propre liste de blocage personnalisée pour désigner des adresses IP spécifiques comme malveillantes.
- Le fichier iprep.db est créé dans le dossier `/var/nslog/iprep`. Une fois créé, il n'est pas supprimé même si la fonctionnalité est désactivée.
- Lorsque la fonctionnalité de réputation est activée, la base de données NetScaler Webroot est téléchargée. Après cela, il est mis à jour toutes les 5 minutes.
- La version majeure de la base de données Webroot est la version : 1.
- La version mineure est mise à jour tous les jours. La version de mise à jour est incrémentée toutes les 5 minutes et est réinitialisée à 1 lorsque la version mineure est incrémentée.

- Les expressions PI vous permettent d'utiliser la réputation IP avec d'autres fonctionnalités, telles que le répondeur et la réécriture.
- Les adresses IP de la base de données sont en notation décimale.

Conseils de débogage

- Si vous ne pouvez pas voir la fonctionnalité de réputation dans l'interface graphique, vérifiez que vous disposez de la bonne licence.
- Surveillez les messages entrants `var/log/iprep.log` pour le débogage.
- **Connectivité Webroot** : si le `ns iprep: Not able to connect/resolve WebRoot` message s'affiche, assurez-vous que l'appliance dispose d'un accès Internet et que le DNS est configuré.
- **Serveur proxy** : si le `ns iprep: iprep_curl_download: 88 curl_easy_perform failed. Error code: 5 Err msg:couldnt resolve proxy name` message s'affiche, assurez-vous que la configuration du serveur proxy est correcte.
- La**fonctionnalité de réputation IP ne fonctionne pas** : le processus de réputation IP prend environ cinq minutes pour démarrer une fois que vous avez activé la fonctionnalité de réputation. La fonctionnalité de réputation IP risque de ne pas fonctionner pendant cette durée.
- **Téléchargement de la base**de données : si le téléchargement des données de la base de données IP échoue après l'activation de la fonctionnalité de réputation IP, l'erreur suivante apparaît dans les journaux.

```
iprep: iprep_curl_download:86 curl_easy_perform failed. Error code:7 Err
msg:Couldn't connect to server
```

Solution : autorisez le trafic sortant vers les URL suivantes ou configurez un proxy pour résoudre le problème.

```
1 localdb-ip-daily.brightcloud.com:443
2 localdb-ip-rtu.brightcloud.com:443
3 api.bcti.brightcloud.com:443
4 <!--NeedCopy-->
```

Déchargement et accélération SSL

May 5, 2023

Une appliance NetScaler configurée pour l'accélération SSL accélère de manière transparente les transactions SSL en déchargeant le traitement SSL du serveur. Pour configurer le déchargement SSL, vous configurez un serveur virtuel pour intercepter et traiter les transactions SSL, puis envoyer le

trafic déchiffré au serveur (sauf si vous configurez le chiffrement de bout en bout, auquel cas le trafic est rechiffré). À la réception de la réponse du serveur, l'appliance termine la transaction sécurisée avec le client. Du point de vue du client, la transaction semble se faire directement avec le serveur. Un NetScaler configuré pour l'accélération SSL exécute également d'autres fonctions configurées, telles que l'équilibrage de charge.

La configuration du déchargement SSL nécessite un certificat SSL et une paire de clés, que vous devez obtenir si vous ne possédez pas encore de certificat SSL. Parmi les autres tâches liées au SSL que vous devrez peut-être effectuer, citons la gestion des certificats, la gestion des listes de révocation de certificats, la configuration de l'authentification des clients et la gestion des actions et des politiques SSL.

Une appliance NetScaler non FIPS stocke la clé privée du serveur sur le disque dur. Sur un appareil FIPS, la clé est stockée dans un module cryptographique appelé module de sécurité matériel (HSM).

Toutes les appliances NetScaler qui ne prennent pas en charge les cartes FIPS (y compris les appliances virtuelles) prennent en charge les HSM externes Thales nShield® Connect et SafeNet. (Les appliances MPX 9700/10500/12500/15500 ne prennent pas en charge un HSM externe.)

Remarque : Les options liées à la norme FIPS pour certaines des procédures de configuration SSL décrites dans ce document sont spécifiques à une appliance NetScaler compatible FIPS.

Configuration de déchargement SSL

May 5, 2023

Pour configurer le déchargement SSL, vous devez activer le traitement SSL sur l'appliance NetScaler et configurer un serveur virtuel basé sur SSL. Le serveur virtuel interceptera le trafic SSL, le décryptera et le transmettra à un service lié au serveur virtuel. Pour sécuriser le trafic urgent, tel que le streaming multimédia, vous pouvez configurer un serveur virtuel DTLS. Pour activer le déchargement SSL, vous devez importer un certificat et une clé valides et lier la paire au serveur virtuel.

> **Remarque**
>
> À partir de la version 13.1 build 17.x, les protocoles inférieurs à TLSv1.2 sont désactivés sur les services internes SSL. Si le profil par défaut (amélioré) est activé, le profil `ns_default_ssl_profile_internal_frontend_service` est lié aux services internes SSL et les protocoles SSLv3, TLSv1.0 et TLSv1.1 sont désactivés dans le profil.

Activer le protocole SSL

Pour traiter le trafic SSL, vous devez activer le traitement SSL. Vous pouvez configurer des entités basées sur SSL, telles que des serveurs et des services virtuels, sans activer le traitement SSL. Cepen-

dant, ils ne fonctionnent pas tant que le traitement SSL n'est pas activé.

Activer le traitement SSL à l'aide de la CLI

À l'invite de commande, tapez :

```
enable ns feature ssl

show ns feature
<!--NeedCopy-->
```

Exemple :

```
enable ns feature SSL
 Done
show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 9)     SSL Offloading                  SSL                 ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

Activer le traitement SSL à l'aide de l'interface graphique

Accédez à **Système > Paramètres** et, dans le groupe **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités de base**, puis sur **Déchargement SSL**.

Configurer les services

Sur l'appliance NetScaler, un service représente un serveur physique ou une application sur un serveur physique. Une fois configurés, les services sont désactivés jusqu'à ce que l'appliance puisse atteindre le serveur physique sur le réseau et surveiller son état.

Ajouter un service à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour ajouter un service et vérifier la configuration :

```
add service <name> (<IP> | <serverName>) <serviceType> <port>
show service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
add service sslsvc 198.51.100.225 SSL 443

Done

sh ssl service sslsvc

            Advanced SSL configuration for Back-end SSL Service sslsvc:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Server Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: ???
            DHE Key Exchange With PSK: ???
            Tickets Per Authentication Context: ???

            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT_BACKEND
            Description: Default cipher list for Backend SSL session
     Done
<!--NeedCopy-->
```


Modifier ou supprimer un service à l'aide de la CLI

Pour modifier un service, utilisez la commande set service, qui est similaire à la commande add service, sauf que vous entrez le nom d'un service existant.

Pour supprimer un service, utilisez la commande rm service, qui accepte uniquement l'argument <name>.

```
rm service <servicename>
<!--NeedCopy-->
```

Exemple :

```
rm service sslsvc
<!--NeedCopy-->
```

Pour modifier un service, utilisez la commande set service, sélectionnez n'importe quel paramètre et modifiez son paramètre.

```
set service <name> (<IP> | <serverName>) <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
set service sslsvc 198.51.100.225 SSL 443
<!--NeedCopy-->
```

Configurer un service à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Services**, créez un service et spécifiez le protocole SSL.

Configuration du serveur virtuel SSL

Les sessions sécurisées nécessitent l'établissement d'une connexion entre le client et un serveur virtuel SSL sur l'appliance NetScaler. Le serveur virtuel SSL intercepte le trafic SSL, le déchiffre et le traite avant de l'envoyer aux services liés au serveur virtuel.

Remarque : Le serveur virtuel SSL est marqué comme étant hors service sur l'appliance NetScaler jusqu'à ce qu'une paire certificat/clé valide et au moins un service y soient liés. Un serveur virtuel basé sur SSL est un serveur virtuel d'équilibrage de charge de type de protocole SSL ou SSL_TCP. La fonctionnalité d'équilibrage de charge doit être activée sur l'appliance NetScaler.

Ajouter un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un serveur virtuel SSL et vérifier la configuration :

```
add lb vserver <name> (serviceType) <IPAddress> <port>
show ssl vserver <name>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver sslvs SSL 192.0.2.240 443
Done

sh ssl vserver sslvs

            Advanced SSL configuration for VServer sslvs:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: ENABLED          Refresh Count: 0
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Push Encryption Trigger: Always
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: DISABLED
            DHE Key Exchange With PSK: NO
            Tickets Per Authentication Context: 1
            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT
            Description: Default cipher list with encryption strength
                >= 128bit
```



```
32       Done
33 <!--NeedCopy-->
```

Modifier ou supprimer un serveur virtuel basé sur SSL à l'aide de l'interface de ligne de commande

Pour modifier les propriétés d'équilibrage de charge d'un serveur virtuel SSL, utilisez la commande `set lb vserver`. La commande set est similaire à la commande `add lb vserver`, sauf que vous entrez le nom d'un serveur virtuel existant. Pour modifier les propriétés **SSL** d'un serveur virtuel basé sur SSL, utilisez la commande `set ssl vserver`. Pour plus d'informations, consultez la section « Paramètres du serveur virtuel SSL » plus loin dans cette page.

Pour supprimer un serveur virtuel SSL, utilisez la commande `rm lb vserver`, qui n'accepte que l'argument `<name>`.

Configurer un serveur virtuel basé sur SSL à l'aide de l'interface graphique

Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, créez un serveur virtuel et spécifiez le protocole SSL.

Liez les services au serveur virtuel SSL

L'appliance ADC transmet les données SSL décryptées aux serveurs du réseau. Pour transférer des données, les services représentant ces serveurs physiques doivent être liés au serveur virtuel qui reçoit les données SSL.

En règle générale, la liaison entre l'appliance ADC et le serveur physique est sécurisée. Par conséquent, le transfert de données entre l'appliance et le serveur physique n'a pas besoin d'être crypté. Toutefois, vous pouvez fournir un chiffrement de bout en bout en chiffrant le transfert de données entre l'appliance et le serveur. Pour plus de détails, consultez la section Configurer le déchargement SSL avec un chiffrement de bout en bout.

Remarque : Activez la fonctionnalité d'équilibrage de charge sur l'appliance ADC avant de lier les services au serveur virtuel SSL.

Lier un service à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier le service au serveur virtuel et vérifier la configuration :

```
1 bind lb vserver <name> <serviceName>
2 show lb vserver <name>
```



```
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver sslvs sslsvc
     Done

sh lb vserver sslvs

            sslvs (192.0.2.240:443) - SSL       Type: ADDRESS
            State: DOWN[Certkey not bound]
            Last state change was at Wed May  2 11:43:04 2018
            Time since last state change: 0 days, 00:13:21.150
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Appflow logging: ENABLED
            No. of Bound Services :  1 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION      BackupMethod:
               ROUNDROBIN
            Mode: IP
            Persistence: NONE
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none
            L2Conn: OFF
            Skip Persistency: None
            Listen Policy: NONE
            IcmpResponse: PASSIVE
            RHIstate: PASSIVE
            New Service Startup Request Rate: 0 PER_SECOND, Increment
               Interval: 0
            Mac mode Retain Vlan: DISABLED
            DBS_LB: DISABLED
            Process Local: DISABLE
            Traffic Domain: 0
            TROFS Persistence honored: ENABLED
            Retain Connections on Cluster: NO
    1) sslsvc (198.51.100.225: 443) - SSL State: DOWN       Weight: 1
     Done
<!--NeedCopy-->
```


Dissocier un service d'un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
unbind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
unbind lb vserver sslvs sslsvc
     Done
<!--NeedCopy-->
```

Liaison d'un service à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel et cliquez sur la vignette **Liaisons de service de serveur virtuel d'équilibrage de charge** sous la section **Services et groupes de services** .
3. Dans la page **Liaison de service de serveur virtuel d'équilibrage de charge**, cliquez sur l'onglet **Ajouter des liaisons**, **cliquez sur Cliquez pour sélectionnersous Sélectionner un service**, puis activez la case à cocher en regard du service à lier.
4. Cliquez sur **Sélectionner**, puis sur **Lier**.

Configurer un serveur virtuel d'indication de nom de serveur (SNI) pour un hébergement sécurisé de plusieurs sites

L'hébergement virtuel est utilisé par les serveurs Web pour héberger plusieurs noms de domaine avec la même adresse IP. L'appliance prend en charge l'hébergement de plusieurs domaines sécurisés en déchargeant le traitement SSL des serveurs Web à l'aide de services SSL transparents ou d'un déchargement SSL basé sur un serveur virtuel. Toutefois, lorsque plusieurs sites Web sont hébergés sur le même serveur virtuel, l'établissement de liaison SSL est terminé avant que le nom d'hôte attendu ne soit envoyé au serveur virtuel. Par conséquent, l'appliance ne peut pas déterminer quel certificat présenter au client après l'établissement d'une connexion. Ce problème est résolu en activant SNI sur le serveur virtuel. SNI est une extension TLS (Transport Layer Security) utilisée par le client pour fournir le nom d'hôte lors de l'initiation de la prise de contact. L'appliance ADC compare ce nom d'hôte au nom commun et, s'il ne correspond pas, le compare à l'autre nom de l'objet (SAN). Si le nom correspond, l'appliance présente le certificat correspondant au client.

Un certificat SSL générique permet d'activer le cryptage SSL sur plusieurs sous-domaines si la même organisation contrôle ces domaines et si le nom de domaine de deuxième niveau est le même. Par exemple, un certificat générique émis à un réseau sportif sous le nom commun « *.sports.net » peut

être utilisé pour sécuriser des domaines, tels que « login.sports.net » et « help.sports.net ». Il ne peut pas sécuriser le domaine « login.ftp.sports.net ».

Remarque :
Sur une appliance ADC, seules les entrées DNS de nom de domaine, d'URL et d'ID de messagerie dans le champ **SAN** sont comparées.

Vous pouvez lier plusieurs certificats de serveur à un seul serveur virtuel SSL ou à un service transparent à l'aide de l'option -SNIcert. Le serveur ou le service virtuel émet ces certificats si SNI est activé sur le serveur ou le service virtuel. Vous pouvez activer SNI à tout moment.

Liez plusieurs certificats de serveur à un seul serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer SNI et vérifier la configuration :

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )]

bind ssl vserver <vServerName>@ -certkeyName <string> -SNICert

show ssl vserver <vServerName>
<!--NeedCopy-->
```

Pour lier plusieurs certificats de serveur à un service transparent à l'aide de l'interface de ligne de commande, remplacez `vserver` par service et `vservername` par nom de service dans les commandes précédentes.

Remarque : Créez le service SSL avec l'option `-clearTextPort 80`.

Liez plusieurs certificats de serveur à un seul serveur virtuel SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel SSL et, dans **Certificats**, sélectionnez **Certificat de serveur**.
3. Ajoutez un certificat ou sélectionnez-en un dans la liste, puis cliquez sur **Certificat de serveur pour SNI**.
4. Dans **Paramètres avancés**, sélectionnez **Paramètres SSL**.
5. Cliquez sur **Activer SNI**.

Prise en charge de SNI sur le service dorsal

> **Remarque** : Le SNI n'est pas pris en charge sur un service dorsal DTLS.

L'appliance NetScaler prend en charge l'indication du nom de serveur (SNI) sur le back-end. En d'autres termes, le nom commun est envoyé en tant que nom de serveur dans le client Hello au serveur principal pour que l'établissement de la liaison soit réussi. Ce support permet de répondre aux exigences de sécurité des clients des intégrateurs de systèmes fédéraux. En outre, SNI offre l'avantage d'utiliser un seul port au lieu d'ouvrir des centaines d'adresses IP et de ports différents sur un pare-feu.

Les exigences de sécurité des clients de Federal System Integrator incluent la prise en charge d'Active Directory Federation Services (ADFS) 3.0 en 2012R2 et des serveurs WAP. Pour répondre à cette exigence, la prise en charge du SNI au niveau du back-end d'une appliance NetScaler est requise.

> **Remarque :**
>
> Pour que SNI fonctionne, le nom du serveur dans le client Hello doit correspondre au nom d'hôte configuré sur le service principal lié à un serveur virtuel SSL. Par exemple, si le nom d'hôte du serveur principal est www.mail.example.com, le service principal compatible SNI doit être configuré avec le nom du serveur sous la forme https://www.mail.example.com. Et ce nom d'hôte doit correspondre au nom du serveur indiqué dans le Hello client.

Prise en charge du SNI dynamique sur le service dorsal

L'appliance NetScaler prend en charge le SNI dynamique sur les connexions TLS principales. En d'autres termes, l'appliance apprend le SNI dans la connexion client et l'utilise dans la connexion côté serveur. Il n'est plus nécessaire de spécifier un nom commun dans le service, le groupe de services ou le profil SSL. Le nom commun reçu dans l'extension SNI du message Client Hello est transféré à la connexion SSL dorsale.

Auparavant, vous deviez configurer le SNI statique sur les services SSL, les groupes de services et les profils SSL. Par conséquent, seule l'extension SNI statique configurée a été envoyée au serveur. Si un client devait accéder à plusieurs domaines en même temps, l'appliance ADC n'était pas en mesure d'envoyer le SNI reçu du client au service principal. Au lieu de cela, il a envoyé le nom commun statique qui a été configuré. Désormais, si le serveur principal est configuré pour plusieurs domaines, le serveur peut répondre avec le bon certificat en fonction du SNI reçu dans le message Client Hello de l'appliance.

Point à noter :

- Le SNI doit être activé sur le frontal et le bon certificat SNI doit être lié au serveur virtuel SSL. Si vous n'activez pas le SNI sur le serveur frontal, les informations SNI ne sont pas transmises au serveur principal.
- Lorsque l'authentification du serveur est activée, le certificat de serveur est vérifié par le certificat de l'autorité de certification et les entrées de nom commun/SAN du certificat de serveur

correspondent au SNI. Par conséquent, le certificat de l'autorité de certification doit être lié au service.

- La réutilisation de la connexion dorsale et de la session SSL est basée sur le SNI lorsque le SNI dynamique est activé.

Les moniteurs SSL n'envoient pas de SNI lorsque le SNI dynamique est activé. Pour le sondage basé sur SNI, attachez un profil principal sur lequel le SNI statique est configuré aux moniteurs SSL. Le moniteur doit être configuré avec le même en-tête personnalisé que SNI.

Configurez SNI sur le service principal à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add service <name>  <IP>  <serviceType>  <port>

add lb vserver <name>  <IPAddress> <serviceType>  <port>

bind lb vserver <name> <serviceName>

set ssl service <serviceName> -SNIEnable ENABLED -commonName <string>

set ssl profile <name> -SNIEnable ENABLED
<!--NeedCopy-->
```

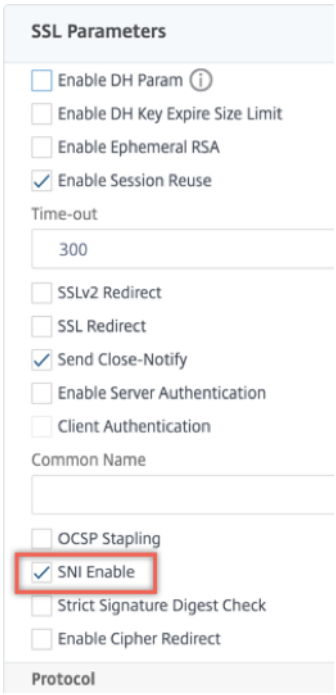
Exemple :

```
    add service service_ssl 198.51.100.100 SSL 443

    add lb vserver ssl-vs 203.0.113.200 SSL 443

    bind lb vserver ssl-vs service_ssl

    set ssl service service_ssl -SNIEnable ENABLED  - commonName www.
       example.com

    set ssl profile sslprof -SNIEnable ENABLED
<!--NeedCopy-->
```

Configurez SNI sur le service principal à l'aide de l'interface graphique

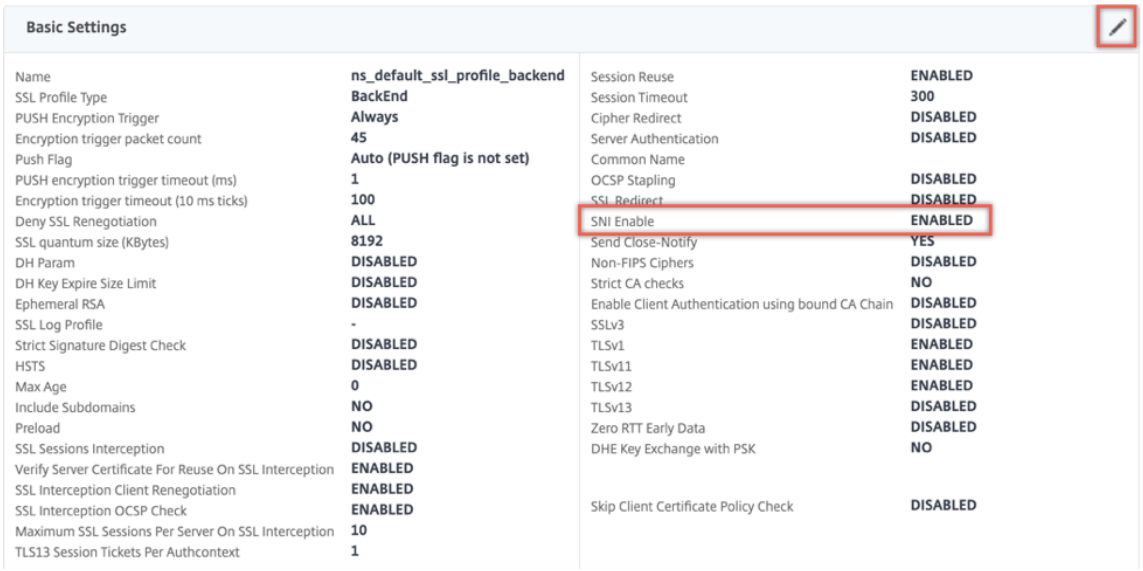
1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Sélectionnez un service SSL, puis dans **Paramètres avancés**, cliquez sur **Paramètres SSL**.

3. Cliquez sur **Activer SNI**.



Configurez le SNI sur le profil SSL à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profil SSL**.
2. Cliquez sur **Ajouter**.
3. Dans **les paramètres de base**, sélectionnez **Activer SNI**.



4. Cliquez sur **OK**.

Lier un moniteur sécurisé à un service principal compatible SNI

Vous pouvez lier des moniteurs sécurisés de type HTTP, HTTP-ECV, TCP ou TCP-ECV aux services principaux et aux groupes de services qui prennent en charge SNI. Toutefois, les sondes de surveillance n'envoient pas l'extension SNI si le SNI dynamique est activé. Pour envoyer des sondes SNI, activez le SNI statique dans le profil SSL principal et liez le profil au moniteur. Définissez l'en-tête personnalisé du moniteur sur le nom du serveur envoyé en tant qu'extension SNI dans le Hello client de la sonde de surveillance.

Configurez et liez un moniteur sécurisé à un service principal compatible SNI à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

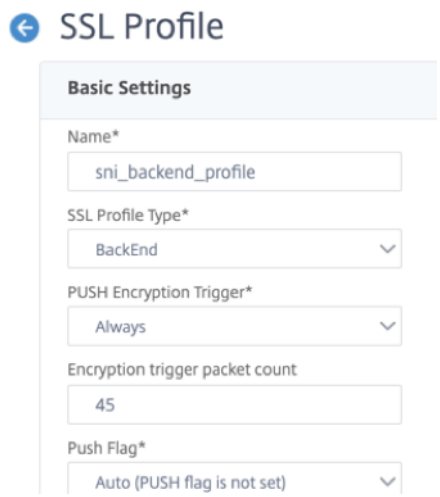
```
add lb monitor <monitorName> <type> -secure YES
add ssl profile <name> -sslProfileType BackEnd
set lb monitor <monitorName> <type> -customHeaders <string> -sslprofile
    <backend ssl profile>
set ssl profile <name> -sniEnable ENABLED -commonName <string>
bind service <name> -monitorName <string>
<!--NeedCopy-->
```

Exemple :

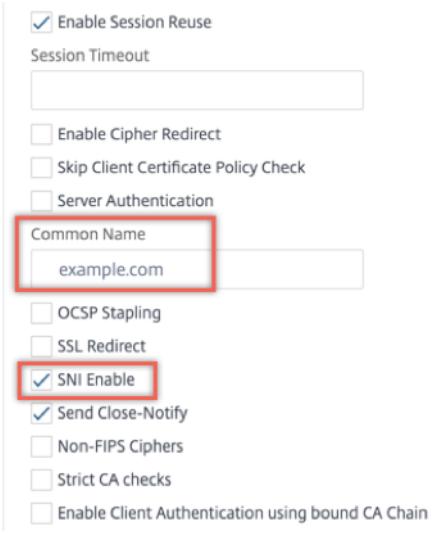
```
add ssl profile sni_backend_profile -sslProfileType BackEnd
set ssl profile sni_backend_profile -sniEnable ENABLED -commonName
   example.com
add lb monitor http-ecv-mon HTTP-ECV -secure YES
set monitor http-ecv-mon HTTP-ECV -customHeaders "Host: example.com\r\n
   " -sslprofile sni_backend_profile
bind service ssl_service  - monitorName http-ecv-mon
<!--NeedCopy-->
```

Configurez et liez un moniteur sécurisé à un service principal activé SNI à l'aide de l'interface graphique

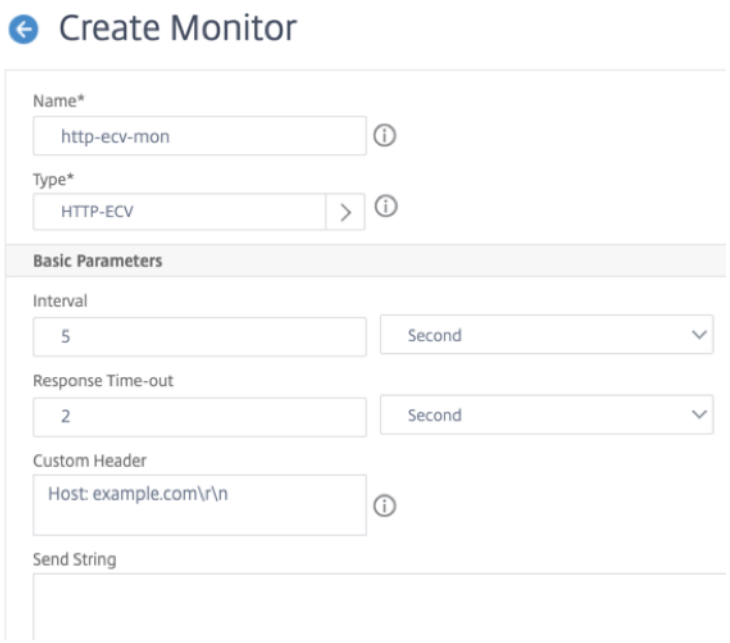
1. Accédez à **Système > Profils > Profils SSL**.
2. Cliquez sur **Ajouter**.
3. Spécifiez un nom pour le profil et dans **Type de profil SSL**, sélectionnez **Backend**.



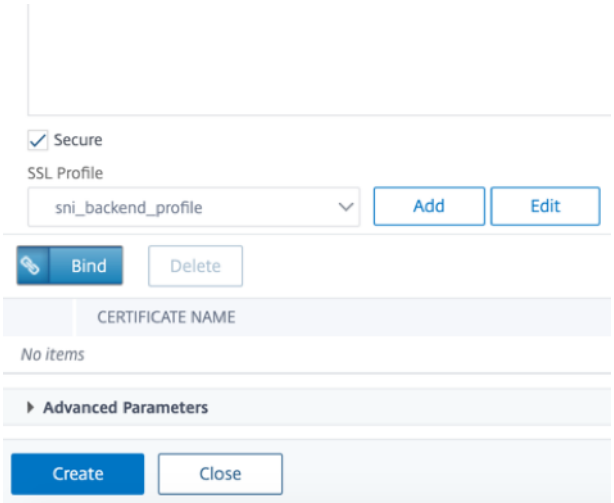
4. Spécifiez le nom commun (identique à l'en-tête de l'hôte) et sélectionnez **Activer SNI**.



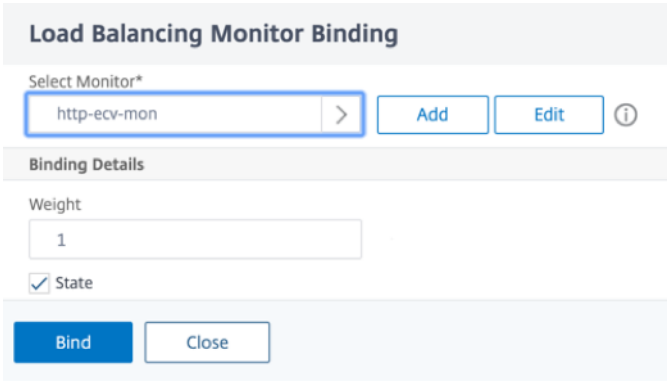
5. Cliquez sur **OK**.
6. Accédez à **Gestion du trafic > Équilibrage de charge > Surveiller**.
7. Cliquez sur **Ajouter**.
8. Spécifiez un nom pour le moniteur. Dans **Type**, sélectionnez HTTP, HTTP-ECV, TCP ou TCP-ECV.
9. Spécifiez un **en-tête personnalisé**.



10. Sélectionnez **Sécurisé**.
11. Dans **Profil SSL**, sélectionnez le profil SSL principal créé au cours des étapes précédentes.
12. Cliquez sur **Create**.



13. Accédez à **Traffic Management > Load Balancing > Services**.
14. Sélectionnez un service SSL et cliquez sur **Modifier**.
15. Dans **Moniteurs**, cliquez sur **Ajouter une liaison**, sélectionnez le moniteur créé au cours des étapes précédentes, puis cliquez sur **Lier**.



Configurez et liez un moniteur sécurisé à un service principal compatible SNI à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Surveiller**.
2. Ajoutez un moniteur de type **HTTP-ECV** ou **TCP-ECV**et spécifiez un **en-tête personnalisé**.
3. Sélectionnez **Créer**.
4. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
5. Sélectionnez un service SSL et cliquez sur **Modifier**.
6. Dans **Moniteurs**, cliquez sur **Ajouter une liaison**, sélectionnez le moniteur créé à l'étape 3, puis cliquez sur **Lier**.

Autoriser la prise de contact pour un nom de serveur inconnu

> **Remarque**
>
> Cette fonctionnalité est disponible dans les versions 13.1 build 45.x et ultérieures.

Lorsque le SNI est activé et que l'appliance NetScaler reçoit un bonjour client avec un nom de serveur inconnu, elle met fin à l'établissement de connexion SSL. À partir de la version 13.1 build 45.x, l'appliance permet à l'établissement de liaison SSL de se poursuivre même pour un nom de serveur inconnu, et laisse au client le soin de décider d'abandonner ou de terminer l'établissement de connexion. Vous pouvez configurer ce paramètre sur un profil SSL frontal lorsque le SNI est **ACTIVÉ** à l'aide du `allowUnknownSNI` paramètre.

Gardez ce paramètre désactivé si vous devez utiliser une action de transfert pour une règle basée sur le SSI. Par exemple, vous avez activé le SNI sur le serveur virtuel v1 et configuré une politique pour transférer toutes les demandes relatives à un domaine spécifique (www.example.com) vers le serveur virtuel v2. Auparavant, toutes les demandes reçues sur la version 1 pour ce domaine étaient automatiquement transférées vers la version 2. Toutefois, si le `allowunknownSNI` paramètre est activé, la demande est traitée sur v1. Le paramètre doit être désactivé pour que l'appliance puisse traiter la demande sur la version 1.

Configurer l'autorisation d'un SNI inconnu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

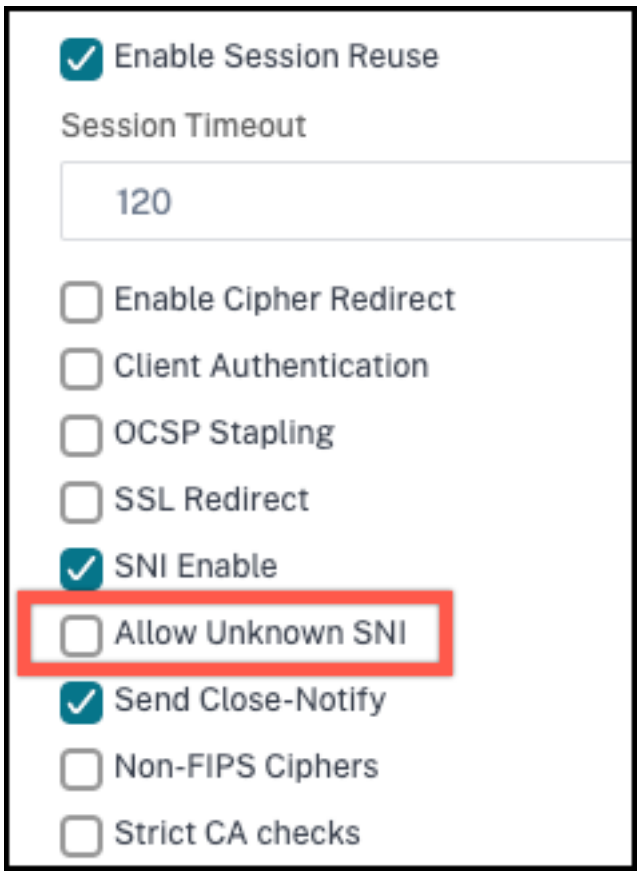
```
set ssl profile default_profile -SNIEnable Enabled -allowUnknownSNI <
DISABLED/ENABLED>
```

Le paramètre 'AllowUnknownSNI est désactivé par défaut. Par conséquent, l'appliance abandonne l'établissement de liaison pour un nom de serveur inconnu. Pour activer ce paramètre, tapez :

```
set ssl profile default_profile -SNIEnable Enabled -allowUnknownSNI ENABLED
```

Configurer l'autorisation d'un SNI inconnu à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils** > **Profil SSL**.
2. Si vous ajoutez un profil, sélectionnez **FrontEnd** dans la liste des **types de profil SSL** . Dans le cas contraire, vous pouvez modifier un profil frontal existant.
3. Sélectionnez **Autoriser un SNI inconnu**.



4. Cliquez sur **OK**, puis sur **Terminé**.

Ajouter ou mettre à jour une paire de clés de certificat

> **Remarques :**
>
> Si vous ne possédez pas de certificat ni de clé existants, reportez-vous à la section Créer un certificat.
>
> Pour créer une paire de clés de certificat ECDSA, cliquez sur Créer une paire de clés de certificat ECDSA.
>
> À partir de la version 41.x, les noms de certificats pouvant contenir jusqu'à 63 caractères sont pris en charge.
>
> Depuis la version 13.0 build 79.x, les paires de clés de certificat protégées par mot de passe sont toujours ajoutées avec succès. Auparavant, si une option de mot de passe fort était activée sur une appliance NetScaler, les paires de clés de certificat protégées par mot de passe n'étaient parfois pas ajoutées. Toutefois, la configuration de la clé de certificat est perdue si vous rétrogradez vers une version antérieure. De plus, dans la réponse de l'API NITRO pour les paires de clés de certificat, la `passplain` variable est envoyée à la place de la `passcrypt` variable.

Pour toute transaction SSL, le serveur a besoin d'un certificat valide et de la paire de clés privées et publiques correspondante. Les données SSL sont cryptées avec la clé publique du serveur, qui est disponible via le certificat du serveur. Le déchiffrement nécessite la clé privée correspondante. Le mot de passe de la clé privée utilisée lors de l'ajout d'une paire de clés de certificat SSL est enregistré à l'aide d'une clé de chiffrement unique pour chaque appliance NetScaler.

L'appliance ADC décharge les transactions SSL du serveur. Par conséquent, le certificat et la clé privée du serveur doivent être présents sur l'appliance, et le certificat doit être associé à la clé privée correspondante. Cette paire de clés de certificat doit être liée au serveur virtuel qui traite les transactions SSL.

Remarque : Le certificat par défaut d'une appliance NetScaler est de 2048 bits. Dans les versions précédentes, le certificat par défaut était de 512 bits ou 1024 bits. Après la mise à niveau vers la version 11.0, vous devez supprimer toutes vos anciennes paires de clés de certificat en commençant par `"ns-"`, puis redémarrer l'appliance pour générer automatiquement un certificat par défaut de 2 048 bits.

Le certificat et la clé doivent tous deux se trouver dans le stockage local de l'appliance NetScaler avant de pouvoir être ajoutés à l'appliance. Si votre fichier de certificat ou de clé ne se trouve pas sur l'appliance, téléchargez-le sur l'appliance avant de créer la paire.

Important : Les certificats et les clés sont stockés par défaut dans le répertoire /nsconfig/ssl. Si vos certificats ou clés sont stockés dans un autre emplacement, vous devez fournir le chemin absolu vers les fichiers de l'appliance NetScaler. Les appliances NetScaler FIPS ne prennent pas en charge les clés externes (clés non FIPS). Sur un dispositif FIPS, vous ne pouvez pas charger de clés à partir d'un périphérique de stockage local tel qu'un disque dur ou une mémoire flash. Les clés FIPS doivent être présentes dans le module de sécurité matériel (HSM) de l'appliance.

Seules les clés RSA sont prises en charge sur les appliances NetScaler.

Définissez la période de notification et autorisez le moniteur d'expiration à émettre une invite avant l'expiration du certificat.

L'appliance NetScaler prend en charge les formats d'entrée suivants pour le certificat et les fichiers de clé privée :

- PEM - Messagerie renforcée pour la confidentialité
- DER - Règle de codage distincte
- PFX - Échange d'informations personnelles

Le logiciel détecte automatiquement le format. Par conséquent, vous n'êtes plus obligé de spécifier le format dans le paramètre inform. Si vous spécifiez le format (correct ou incorrect), le logiciel l'ignore. Le format du certificat et du fichier de clé doivent être identiques.

Remarque : Un certificat doit être signé à l'aide de l'un des algorithmes de hachage suivants :

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Une appliance MPX prend en charge les certificats de 512 bits ou plus, jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service
- Certificat d'autorité de certification 4096 bits (y compris les certificats intermédiaires et racine)
- Certificat 4096 bits sur le serveur principal
- Certificat client 4096 bits (si l'authentification client est activée sur le serveur virtuel)

Un dispositif virtuel VPX prend en charge les certificats de 512 bits ou plus, jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service
- Certificat d'autorité de certification 4096 bits (y compris les certificats intermédiaires et racine)
- Certificat 4096 bits sur le serveur principal
- Certificat client 4096 bits (si l'authentification client est activée sur le serveur virtuel)

À partir de la version 13.1 build 17.x, toutes les plateformes NetScaler prennent en charge les certificats signés à l'aide des algorithmes RSASSA-PSS.
Ces algorithmes sont pris en charge dans la validation du chemin d'accès au certificat X.509.
Le tableau suivant présente les jeux de paramètres RSASSA-PSS pris en charge par l'appliance NetScaler.

ID de clé publique	Fonction de génération de masque (MGF)	Fonction MGF Digest	Fonction Signature Digest	Longueur de salt
rsaEncryption	MGF1	SHA-256	SHA-256	32 octets
rsaEncryption	MGF1	SHA-384	SHA-384	48 octets
rsaEncryption	MGF1	SHA-512	SHA-512	64 octets

> **Remarque**
>
> Une appliance NetScaler SDX prend en charge les certificats de 512 bits ou plus. Chaque instance NetScaler VPX hébergée sur l'appliance prend en charge les tailles de certificat précédentes pour une appliance virtuelle VPX. Toutefois, si une puce SSL est attribuée à une instance, cette instance prend en charge les tailles de certificat prises en charge par une appliance MPX.

Ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une paire de clés de certificat et vérifier la configuration :

```
add ssl certKey <certkeyName> -cert <string>[(-key <string> [-password
    ]) | -fipsKey <string>] [-inform ( DER | PEM )] [<passplain>] [-
    expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]]

show ssl certKey [<certkeyName>]
<!--NeedCopy-->
```

Exemple :

```
add ssl certKey sslckey -cert server_cert.pem -key server_key.pem -
    password ssl -expiryMonitor ENABLED -notificationPeriod 30
 Done
Note: For FIPS appliances, replace -key with -fipskey

show ssl certKey sslckey
        Name: sslckey           Status: Valid,   Days to expiration
            :8418
        Version: 3
        Serial Number: 01
        Signature Algorithm: md5WithRSAEncryption
        Issuer:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.root.com
        Validity
```



```
                Not Before: Jul 15 02:25:01 2005 GMT
                Not After : Nov 30 02:25:01 2032 GMT
        Subject:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.server.com
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048
 Done
<!--NeedCopy-->
```

Mettre à jour ou supprimer une paire de clés de certificat en utilisant l'interface de ligne de commande

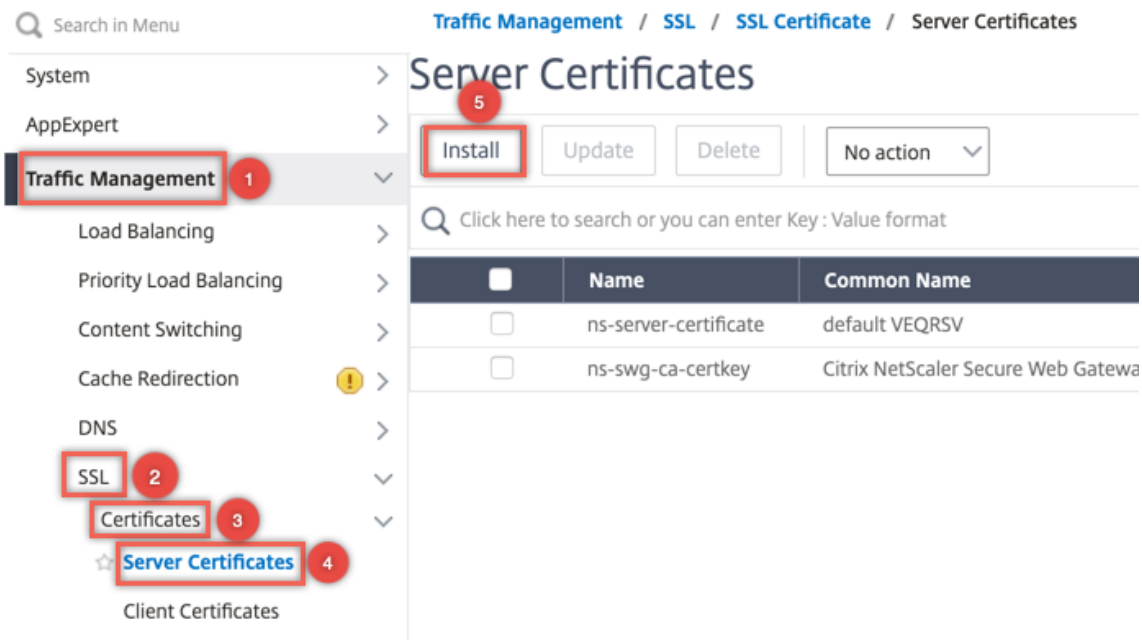
Pour modifier le moniteur d'expiration ou la période de notification dans une paire de clés de certificat, utilisez la commande `set ssl certkey`. Pour remplacer le certificat ou la clé d'une paire de clés de certificat, utilisez la commande `update ssl certkey`. La commande `update ssl certkey` possède un paramètre supplémentaire pour remplacer la vérification du domaine. Pour les deux commandes, entrez le nom d'une paire de clés de certificat existante. Pour supprimer une paire de clés de certificat SSL, utilisez la commande `rm ssl certkey`, qui n'accepte que l'argument <`certkeyName`>.

Exemple :

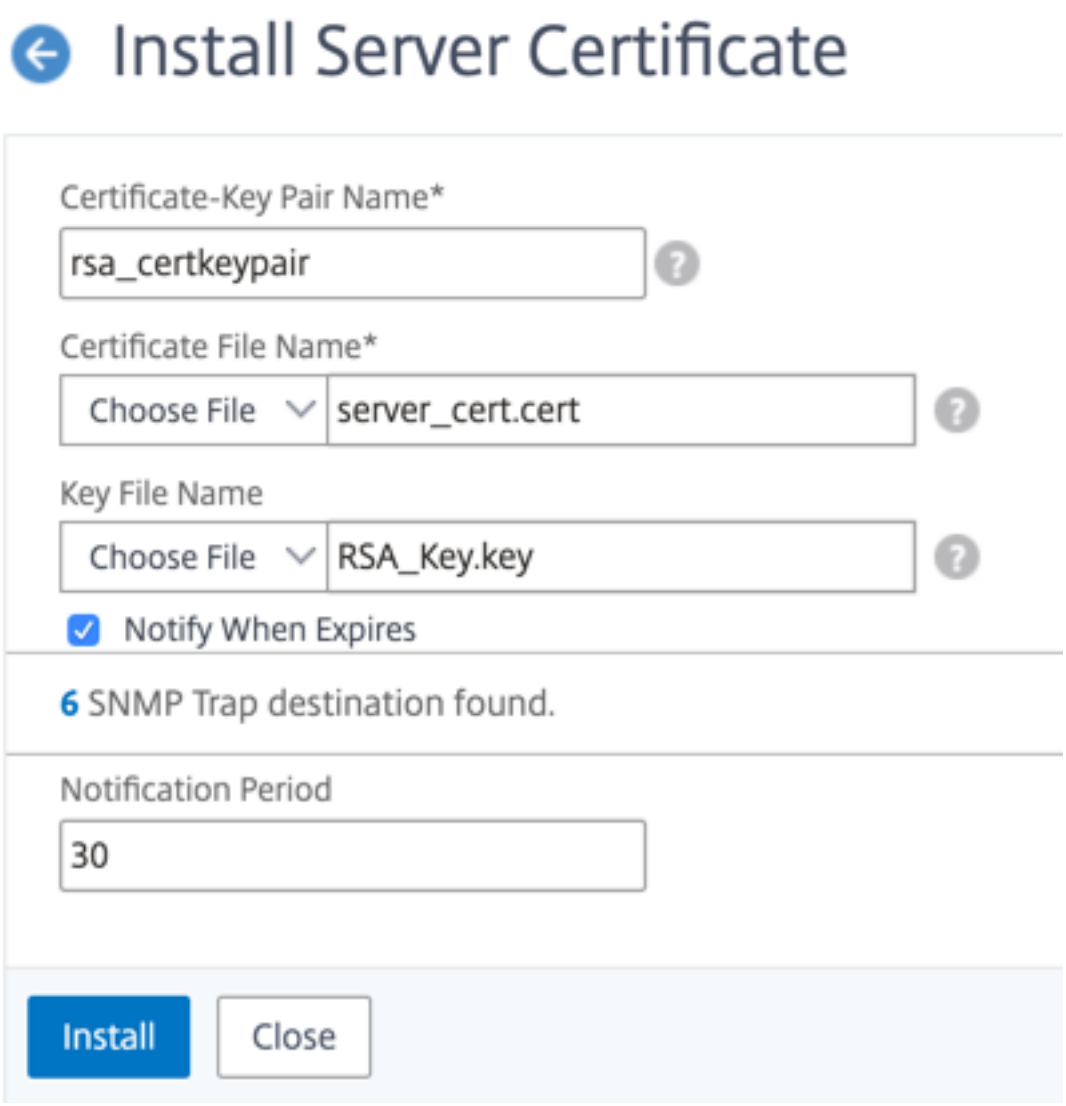
```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED )
       [-notificationPeriod <positive_integer>]]

update ssl certKey <certkeyName> [-cert <string> [-password]] [-key
       <string> | -fipsKey <string>] [-inform <inform>] [-noDomainCheck
          ]
<!--NeedCopy-->
```

Ajouter ou mettre à jour une paire de clés de certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Certificats > Serveur**.



2. Entrez les valeurs des paramètres suivants et cliquez sur **Installer**.
   - Nom de la paire de clés de certificat : nom du certificat et de la paire de clés privées.
   - Nom du fichier de certificat : certificat signé reçu de l'autorité de certification.
   - Nom du fichier de clé : nom et, éventuellement, chemin d'accès au fichier de clé privée utilisé pour former la paire de clés de certificat.



Lier la paire de clés de certificat au serveur virtuel SSL

Important : associez tous les certificats intermédiaires à ce certificat avant de lier le certificat à un serveur virtuel SSL. Pour plus d'informations sur la liaison des certificats, voir Créer une chaîne de certificats.

Le certificat utilisé pour le traitement des transactions SSL doit être lié au serveur virtuel qui reçoit les données SSL. Si plusieurs serveurs virtuels reçoivent des données SSL, une paire de clés de certificat valide doit être liée à chacun d'eux.

Utilisez un certificat SSL valide et existant que vous avez chargé sur l'appliance NetScaler. À des fins de test, vous pouvez également créer votre propre certificat SSL sur l'appliance. Les certificats intermédiaires créés à l'aide d'une clé FIPS sur l'appliance ne peuvent pas être liés à un serveur virtuel SSL.

Lors de la prise de contact SSL, dans le message de demande de certificat lors de l'authentification client, le serveur répertorie les noms distincts (DN) de toutes les autorités de certification (CA) liées au serveur. Le serveur accepte un certificat client uniquement à partir de cette liste. Si vous ne souhaitez pas que le nom de nom unique d'un certificat d'autorité de certification spécifique soit envoyé au client SSL, définissez l'indicateur `skipCA`. Ce paramètre indique que le nom unique du certificat d'autorité de certification particulière ne doit pas être envoyé au client SSL.

Pour plus d'informations sur la création de votre propre certificat, consultez Gestion des certificats.

Remarque : Citrix vous recommande d'utiliser uniquement des certificats SSL valides émis par une autorité de certification approuvée.

Liez une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une paire de clés de certificat SSL à un serveur virtuel et vérifier la configuration :

```
1 - bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName
     > -CA -skipCAName
2 - show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Exemple :

```
1 bind ssl vs vs1 -certkeyName cert2 -CA -skipCAName
2  Done
3 sh ssl vs vs1
4
5  Advanced SSL configuration for VServer vs1:
6
7  DH: DISABLED
8
9  Ephemeral RSA: ENABLED Refresh Count: 0
10
11  Session Reuse: ENABLED Timeout: 120 seconds
12
13  Cipher Redirect: DISABLED
14
15  SSLv2 Redirect: DISABLED
16
17  ClearText Port: 0
18
19  Client Auth: DISABLED
20
```



```
 SSL Redirect: DISABLED

 Non FIPS Ciphers: DISABLED

 SNI: DISABLED

 OCSP Stapling: DISABLED

 HSTS: DISABLED

 IncludeSubDomains: NO

 HSTS Max-Age: 0

 SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: DISABLED
    TLSv1.2: DISABLED

 Push Encryption Trigger: Always

 Send Close-Notify: YES

 Strict Sig-Digest Check: DISABLED

ECC Curve: P_256, P_384, P_224, P_521

 1) CertKey Name: cert1 CA Certificate OCSPCheck: Optional CA_Name Sent
 2) CertKey Name: cert2 CA Certificate OCSPCheck: Optional CA_Name
    Skipped
 1) Cipher Name: DEFAULT

Description: Default cipher list with encryption strength >= 128bit
Done
<!--NeedCopy-->
```

Délier une paire de clés de certificat SSL d'un serveur virtuel à l'aide de l'interface de ligne de commande

Si vous essayez de délier une paire de clés de certificat d'un serveur virtuel à l'aide de la commande `unbind ssl certKey <certkeyName>`, un message d'erreur s'affiche. L'erreur apparaît car la syntaxe de la commande a changé. À l'invite de commandes, tapez la commande suivante :

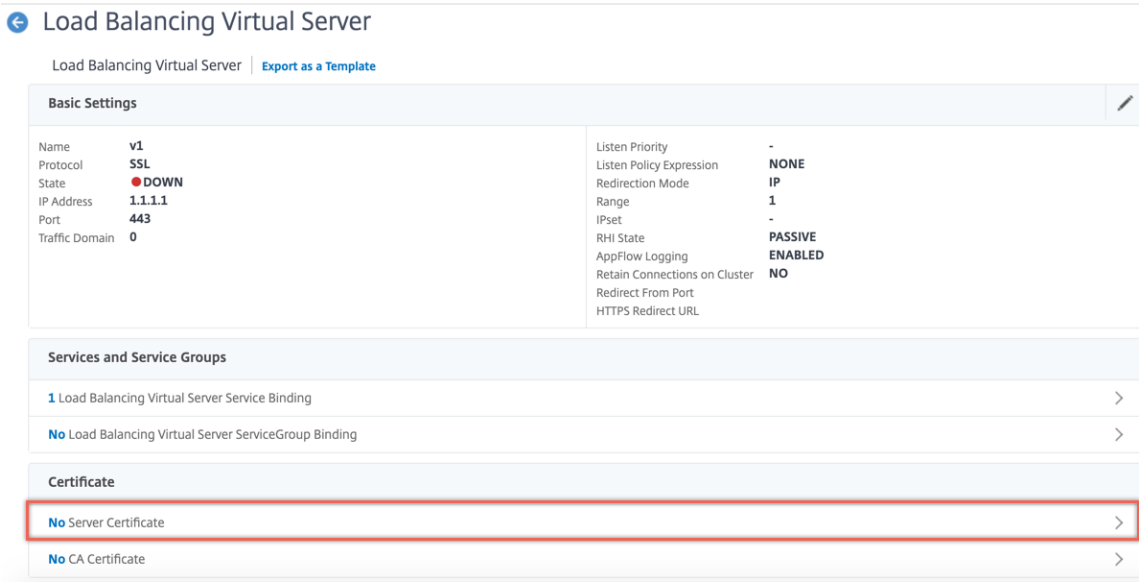
```
unbind ssl vserver <vServerName> -certkeyName <string>
<!--NeedCopy-->
```


Exemple :

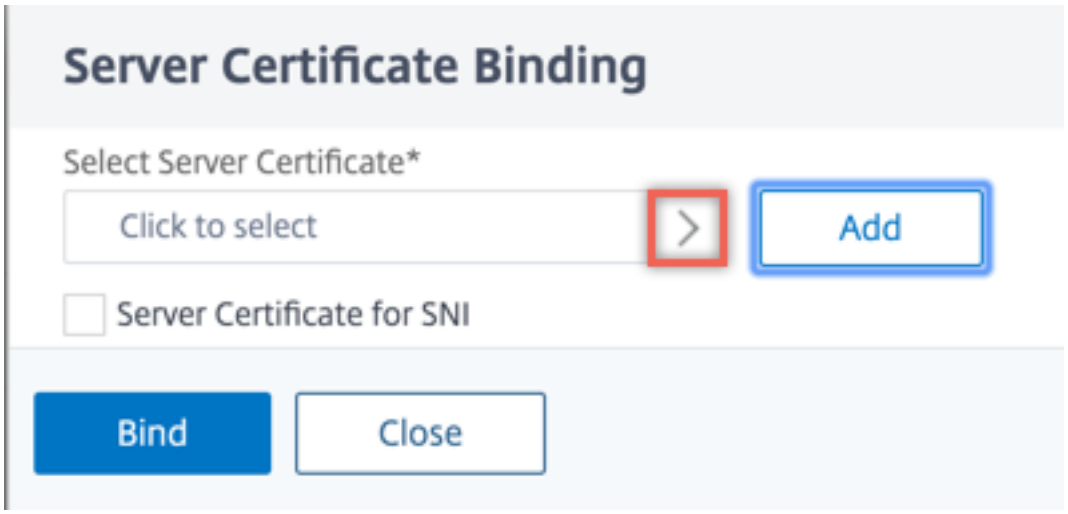
```
unbind ssl vserver vssl -certkeyName sslckey
<!--NeedCopy-->
```

Liez une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface graphique

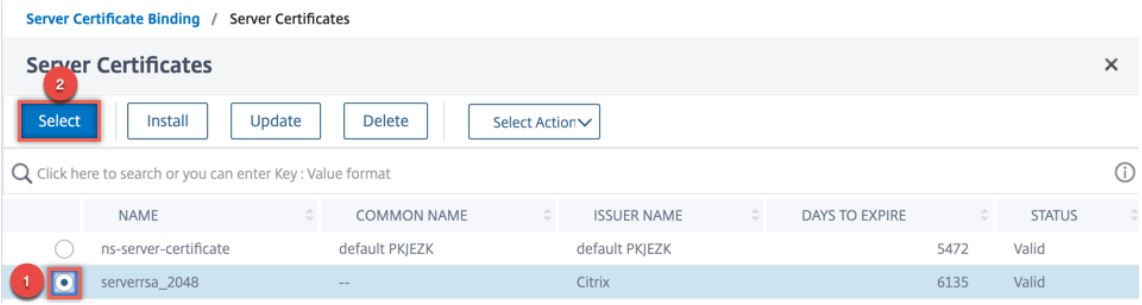
1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et ouvrez un serveur virtuel SSL. Cliquez à l'intérieur de la section **Certificat** .



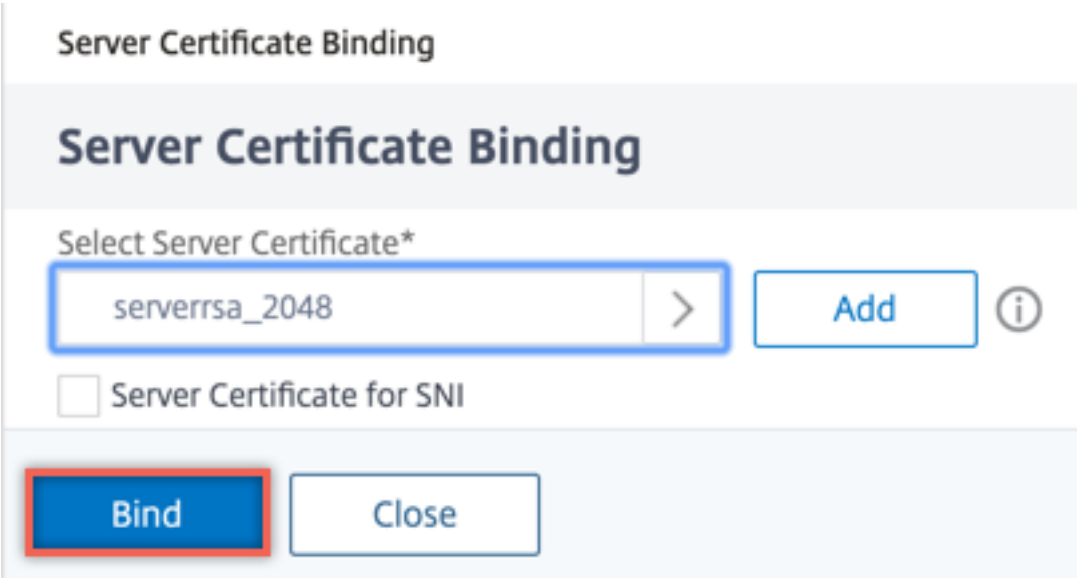
2. Cliquez sur la flèche pour sélectionner la paire de clés de certificat.



3. Sélectionnez la paire de clés de certificat dans la liste.



4. Liez la paire de clés de certificat au serveur virtuel. Pour ajouter un certificat de serveur en tant que certificat SNI, sélectionnez **Certificat de serveur pour SNI**.



Paramètres du serveur virtuel SSL

Définissez la configuration SSL avancée pour un serveur virtuel SSL. Vous pouvez également définir plusieurs de ces paramètres dans un profil SSL. Pour plus d'informations sur les paramètres pouvant être définis dans un profil SSL, consultez Paramètres de profil SSL.

Définir les paramètres du serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl vserver <vServerName>@ [-clearTextPort <port>] [-dh ( ENABLED |
    DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-
    dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED |
    DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED |
    DISABLED )[-sessTimeout <positive_integer>]] [-cipherRedirect (
    ENABLED | DISABLED ) [-cipherURL <URL>]] [-sslv2Redirect ( ENABLED |
     DISABLED )[-sslv2URL <URL>]] [-clientAuth ( ENABLED | DISABLED ) [-
```



```
      clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
      DISABLED )][-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl2 (
      ENABLED | DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 (
      ENABLED | DISABLED )] [-tls11 ( ENABLED | DISABLED )] [-tls12 (
      ENABLED | DISABLED )][-tls13 ( ENABLED | DISABLED )] [-SNIEnable (
      ENABLED | DISABLED )][-ocspStapling ( ENABLED | DISABLED )] [-
      pushEncTrigger <pushEncTrigger>] [-sendCloseNotify ( YES | NO )] [-
      dtlsProfileName <string>] [-sslProfile <string>] [-HSTS ( ENABLED |
      DISABLED )][-maxage <positive_integer>] [-IncludeSubdomains ( YES |
      NO )][-strictSigDigestCheck ( ENABLED | DISABLED )] [-
      zeroRttEarlyData (ENABLED | DISABLED )] [-
      tls13SessionTicketsPerAuthContext <positive_integer>] [-
      dheKeyExchangeWithPsk ( YES | NO )]
2 <!--NeedCopy-->
```

Paramètres de Diffie-Hellman (DH)

Pour utiliser des chiffrements sur l'appliance qui nécessitent un échange de clés DH pour configurer la transaction SSL, activez l'échange de clés DH sur l'appliance. Configurez d'autres paramètres en fonction de votre réseau.

Pour répertorier les chiffrements pour lesquels les paramètres DH doivent être définis à l'aide de l'interface de ligne de commande, tapez : sh cipher DH.

Pour répertorier les chiffrements pour lesquels les paramètres DH doivent être définis à l'aide de l'utilitaire de configuration, accédez à **Gestion du trafic > SSL > Groupes de chiffrement**, puis double-cliquez sur **DH**.

Pour plus d'informations sur la façon d'activer l'échange de clés DH, voir Générer une clé Diffie-Hellman (DH).

Configurer les paramètres DH à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer les paramètres DH et vérifier la configuration :

```
1 -  `set ssl vserver <vserverName> -dh <Option> -dhCount <
     RefreshCountValue> -filepath <string>
2 -  show ssl vserver <vServerName>`
3 <!--NeedCopy-->
```

Exemple :


```
set ssl vserver vs-server -dh ENABLED  -dhFile /nsconfig/ssl/ns-server.
    cert -dhCount 1000
Done

show ssl vserver vs-server

            Advanced SSL configuration for VServer vs-server:
            DH: ENABLED
            Ephemeral RSA: ENABLED          Refresh Count: 1000
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
                ENABLED  TLSv1.2: ENABLED

    1)      Cipher Name: DEFAULT
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Configurer les paramètres DH à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer le paramètre DH**, puis spécifiez un nombre d'actualisations et un chemin d'accès au fichier.

RSA éphémère

Le RSA éphémère permet aux clients d'exportation de communiquer avec le serveur sécurisé même si le certificat de serveur ne prend pas en charge les clients d'exportation (certificat 1024 bits). Si vous souhaitez empêcher les clients d'exportation d'accéder à l'objet ou à la ressource Web sécurisé, vous devez désactiver l'échange de clés RSA éphémère.

Par défaut, cette fonctionnalité est activée sur l'appliance NetScaler, le nombre de rafraîchissements étant défini sur zéro (utilisation infinie).

Remarque :

La clé RSA éphémère est automatiquement générée lorsque vous liez un chiffrement d'exportation à un serveur ou service virtuel SSL basé sur SSL ou TCP. Lorsque vous supprimez le chiffrement d'exportation, la clé eRSA n'est pas supprimée. Il est réutilisé ultérieurement lorsqu'un autre chiffrement d'exportation est lié à un serveur ou service virtuel SSL basé sur SSL ou TCP. La clé eRSA est supprimée au redémarrage du système.

Configurer RSA éphémère à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le RSA éphémère et vérifier la configuration :

```
set ssl vserver <vServerName> -eRSA (enabled | disabled) -eRSACount <
   positive_integer>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver vs-server -eRSA ENABLED -eRSACount 1000
 Done

show ssl vserver vs-server

        Advanced SSL configuration for VServer vs-server:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
           ENABLED  TLSv1.2: ENABLED
```



```
22
23 1)      Cipher Name: DEFAULT
24         Description: Predefined Cipher Alias
25  Done
26 <!--NeedCopy-->
```

Configurer le RSA éphémère à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer le RSA éphémère**et spécifiez un nombre d'actualisations.

Réutilisation des sessions

Pour les transactions SSL, l'établissement de la prise de contact SSL initiale nécessite des opérations de chiffrement à clé publique gourmandes en CPU. La plupart des opérations de prise de contact sont associées à l'échange de la clé de session SSL (message d'échange de clé client). Lorsqu'une session client est inactive pendant un certain temps et qu'elle est ensuite reprise, l'établissement de liaison SSL est généralement recommencé. Lorsque la réutilisation de session est activée, l'échange de clés de session est évité pour les demandes de reprise de session reçues du client.

La réutilisation des sessions est activée par défaut sur l'appliance NetScaler. L'activation de cette fonctionnalité réduit la charge du serveur, améliore le temps de réponse et augmente le nombre de transactions SSL par seconde (TPS) que le serveur peut prendre en charge.

Configurer la réutilisation de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la réutilisation de session et vérifier la configuration :

```
1 set ssl vserver <vServerName> -sessReuse ( ENABLED | DISABLED ) -
     sessTimeout <positive_integer>
2 show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Exemple :

```
1 set ssl vserver vs-ssl -sessreuse enabled -sesstimeout 600
2  Done
3
4 show ssl vserver vs-ssl
5
```



```
6          Advanced SSL configuration for VServer vs-ssl:
7          DH: DISABLED
8          Ephemeral RSA: ENABLED          Refresh Count: 1000
9          Session Reuse: ENABLED          Timeout: 600 seconds
10         Cipher Redirect: DISABLED
11         SSLv2 Redirect: DISABLED
12         ClearText Port: 0
13         Client Auth: DISABLED
14         SSL Redirect: DISABLED
15         Non FIPS Ciphers: DISABLED
16         SNI: DISABLED
17         OCSP Stapling: DISABLED
18         HSTS: DISABLED
19         HSTS IncludeSubDomains: NO
20         HSTS Max-Age: 0
21         SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
               ENABLED  TLSv1.2: ENABLED
22
23 1)      CertKey Name: Auth-Cert-1       Server Certificate
24
25 1)      Cipher Name: DEFAULT
26         Description: Predefined Cipher Alias
27  Done
28 <!--NeedCopy-->
```

Configuration de la réutilisation de session à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer la réutilisation de session**et spécifiez une durée pendant laquelle la session doit rester active.

Paramètres du protocole SSL

L'appliance NetScaler prend en charge les protocoles SSLv3, TLSv1, TLSv1.1 et TLSv1.2. Chacun de ces protocoles peut être défini sur l'appliance en fonction de votre déploiement et du type de clients qui se connectent à l'appliance.

Les versions 1.0, 1.1 et 1.2 du protocole TLS sont plus sécurisées que les anciennes versions du protocole TLS/SSL. Toutefois, pour prendre en charge les systèmes hérités, de nombreuses implémentations TLS conservent une compatibilité descendante avec le protocole SSLv3. Lors d'une connexion SSL, la version de protocole la plus élevée commune au client et au serveur virtuel SSL configuré sur l'appliance NetScaler est utilisée.

Lors de la première tentative de prise de contact, un client TLS propose la version de protocole la plus élevée qu'il prend en charge. Si la prise de contact échoue, le client propose une version de protocole inférieure. Par exemple, si une prise de contact avec TLS version 1.1 échoue, le client tente de renégocier en proposant le protocole TLSv1.0. Si cette tentative échoue, le client tente de nouveau avec le protocole SSLv3. Un attaquant « homme au milieu » (MITM) peut rompre la poignée de main initiale et déclencher une renégociation avec le protocole SSLv3, puis exploiter une vulnérabilité dans SSLv3. Pour atténuer ces attaques, vous pouvez désactiver SSLv3 ou ne pas autoriser la renégociation à l'aide d'un protocole rétrogradé. Toutefois, cette approche peut ne pas être pratique si votre déploiement inclut des systèmes hérités. Une autre solution consiste à reconnaître une valeur de suite de chiffrement de signalisation (TLS_FALLBACK_SCSV) dans la demande du client.

Une valeur TLS_FALLBACK_SCSV dans un message Hello client indique au serveur virtuel que le client a déjà tenté de se connecter avec une version de protocole supérieure et que la demande actuelle est une solution de secours. Si le serveur virtuel détecte cette valeur et qu'il prend en charge une version supérieure à celle indiquée par le client, il rejette la connexion avec une alerte fatale. La prise de contact réussit si l'une des conditions suivantes est remplie :

- La valeur TLS_FALLBACK_SCSV n'est pas incluse dans le message Hello du client.
- La version du protocole dans le client hello est la version de protocole la plus élevée prise en charge par le serveur virtuel.

Configurer la prise en charge du protocole SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la prise en charge du protocole SSL et vérifier la configuration :

```
set ssl vserver <vServerName> -ssl2 ( ENABLED | DISABLED ) -ssl3 (
    ENABLED | DISABLED ) -tls1 ( ENABLED | DISABLED ) -tls11 ( ENABLED |
     DISABLED ) -tls12 ( ENABLED | DISABLED )

show ssl vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver vs-ssl -tls11 ENABLED -tls12 ENABLED
Done

sh ssl vs vs-ssl

        Advanced SSL configuration for VServer vs-ssl:
            DH: DISABLED
            Ephemeral RSA: ENABLED                          Refresh
               Count: 0
```



```
9               Session Reuse: ENABLED                                  Timeout
                    : 120 seconds
10              Cipher Redirect: DISABLED
11              SSLv2 Redirect: DISABLED
12              ClearText Port: 0
13              Client Auth: DISABLED
14              SSL Redirect: DISABLED
15              Non FIPS Ciphers: DISABLED
16              SNI: DISABLED
17              SSLv2: DISABLED        SSLv3: ENABLED    TLSv1.0: ENABLED
                    TLSv1.1: ENABLED  TLSv1.2: ENABLED
18              Push Encryption Trigger: Always
19              Send Close-Notify: YES
20              1 bound certificate:
21
22      1)      CertKey Name: mycert  Server Certificate
23              1 configured cipher:
24
25      1)      Cipher Name: DEFAULT
26              Description: Predefined Cipher Alias
27
28  Done
29  <!--NeedCopy-->
```

Configurer le support du protocole SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez un protocole à activer.

Notification rapprochée

Une notification de fermeture est un message sécurisé qui indique la fin de la transmission de données SSL. Un paramètre de notification de fermeture est requis au niveau mondial. Ce paramètre s'applique à tous les serveurs virtuels, services et groupes de services. Pour plus d'informations sur le paramètre global, consultez la section « Paramètres SSL globaux » plus loin dans cette page.

Outre le paramètre global, vous pouvez définir le paramètre de notification de fermeture au niveau du serveur virtuel, du service ou du groupe de services. Vous avez donc la possibilité de définir le paramètre pour une entité et de le désactiver pour une autre entité. Veillez toutefois à définir ce paramètre au niveau global. Sinon, le paramètre au niveau de l'entité ne s'applique pas.

Configurer la notification de fermeture au niveau de l'entité à l'aide de la CLI

À l'invite de commandes, tapez l'une des commandes suivantes pour configurer la fonction de notification de fermeture et vérifier la configuration :

1. Pour configurer au niveau du serveur virtuel, tapez :

```
set ssl vserver <vServerName> -sendCloseNotify ( YES | NO )
show ssl vserver <vServerName>
<!--NeedCopy-->
```

1. Pour configurer au niveau du service, tapez :

```
set ssl service <serviceName> -sendCloseNotify ( YES | NO )
show ssl service <serviceName>
<!--NeedCopy-->
```

1. Pour configurer au niveau du groupe de services, tapez :

```
set ssl serviceGroup <serviceGroupName> -sendCloseNotify ( YES | NO )
show ssl serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver sslvsvr -sendCloseNotify YES

Done
<!--NeedCopy-->
```

Configurez la fonctionnalité de notification de fermeture au niveau de l'entité à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Envoyer une notification de fermeture**.

Paramètres SSL globaux

La personnalisation avancée de votre configuration SSL résout des problèmes spécifiques. Vous pouvez utiliser la commande `set ssl parameter` ou l'utilitaire de configuration pour spécifier les éléments suivants :

- Taille quantique à utiliser pour les transactions SSL.

- Taille de la mémoire CRL.
- Taille du cache OCSP.
- Refuser la renégociation SSL.
- Définissez l'indicateur PUSH pour les enregistrements déchiffrés, chiffrés ou tous les enregistrements.
- Supprimer les demandes si le client initie la prise de contact pour un domaine et envoie une demande HTTP pour un autre domaine.
- Définissez l'heure après laquelle le chiffrement est déclenché.
  Remarque : L'heure que vous spécifiez s'applique uniquement si vous utilisez la commande `set ssl vserver` ou l'utilitaire de configuration pour définir le chiffrement basé sur le minuteur.
- Vérification du certificat de conformité NDCPP — S'applique lorsque l'appliance agit en tant que client (connexion principale). Lors de la vérification du certificat, ignorez le nom commun si le SAN est présent dans le certificat SSL.
- Activez un cluster hétérogène d'appliances basées sur la puce Cavium, telles que MPX 14000, et d'appliances basées sur la puce Intel Coleto, telles que les appliances MPX 15000 avec un nombre différent de moteurs de paquets. (Prise en charge ajoutée dans la version 13.0 build 47.x).
- Activer la renégociation sécurisée au back-end (Support ajouté à partir de la version 1.0 build 58.x).
- Contrôle du trafic SSL adaptatif (prise en charge ajoutée dans la version 13.0 build 58.x).

Configurer les paramètres SSL globaux à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer les paramètres SSL avancés et vérifier la configuration :

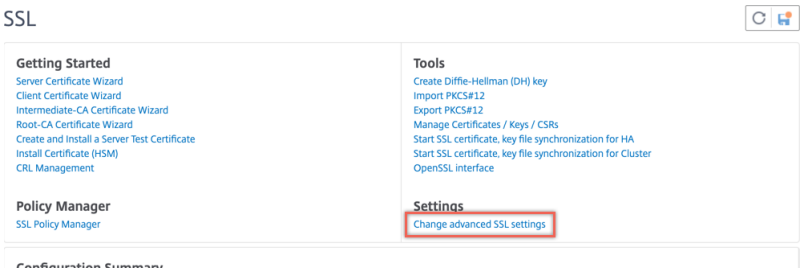
```
1 set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB <
    positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout
    <positive_integer>] [-sendCloseNotify (YES | NO)] [-
    encryptTriggerPktCount <positive_integer>] [-denySSLReneg <
    denySSLReneg>] [-insertionEncoding (Unicode|UTF-8)] [-ocspCacheSize
    <positive_integer>][- pushFlag <positive_integer>] [-
    dropReqWithNoHostHeader (YES | NO)] [-pushEncTriggerTimeout <
    positive_integer>] [-ndcppComplianceCertCheck ( YES | NO)] [-
    heterogeneousSSLHW (ENABLED | DISABLED )]
2 show ssl parameter
3 <!--NeedCopy-->
```

Exemple :

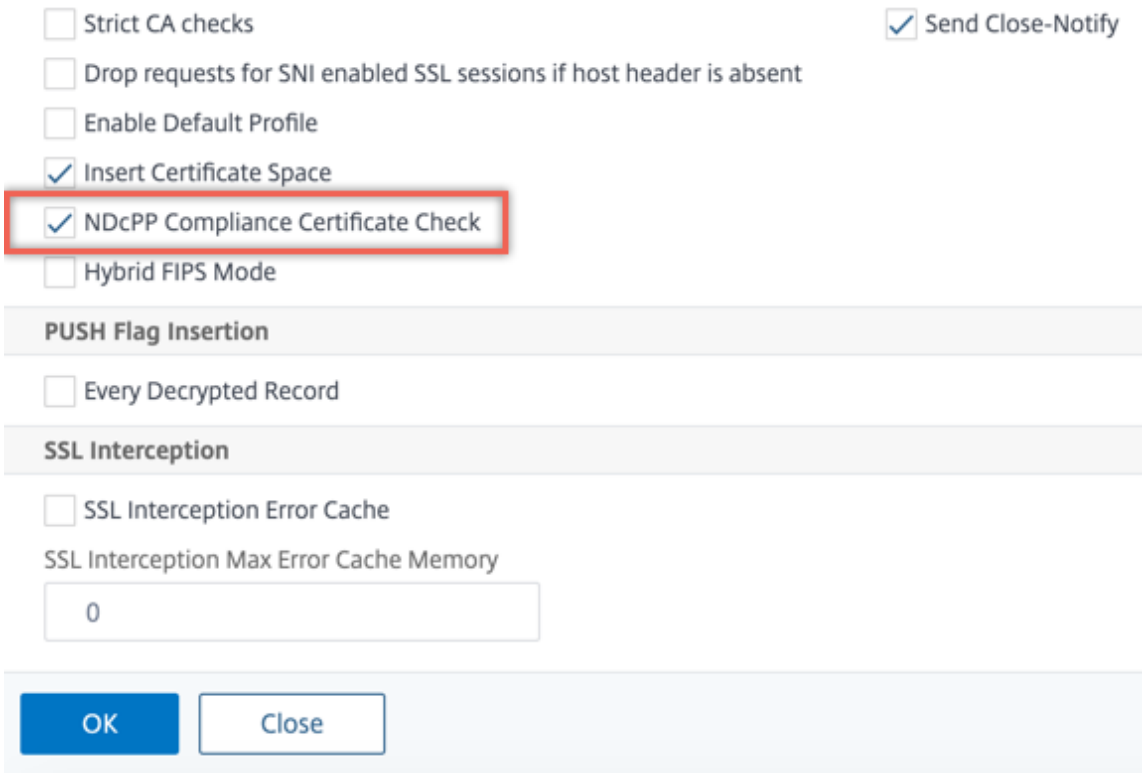

```
set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCAChecks
    no -ssltriggerTimeout 100 -sendClosenotify no -
    encryptTriggerPktCount 45 -denySSLReneg NONSECURE -insertionEncoding
     unicode -ocspCacheSize 10 -pushFlag 3 -dropReqWithNoHostHeader YES
     -pushEncTriggerTimeout 100 ms -ndcppComplianceCertCheck YES
Done

show ssl parameter
Advanced SSL Parameters
-----------------------
    SSL quantum size                                    : 8 KB
    Max CRL memory size                                 : 256 MB
    Strict CA checks                                    : NO
    Encryption trigger timeout                          : 100 ms
    Send Close-Notify                                   : NO
    Encryption trigger packet count                     : 45
    Deny SSL Renegotiation                              : NONSECURE
    Subject/Issuer Name Insertion Format                : Unicode
    OCSP cache size                                     : 10 MB
    Push flag                                           : 0x3 (On
       every decrypted and encrypted record)
    Strict Host Header check for SNI enabled SSL sessions : YES
    PUSH encryption trigger timeout                     : 100 ms
    Crypto Device Disable Limit                         : 0
    Global undef action for control policies            : CLIENTAUTH
    Global undef action for data policies               : NOOP
    Default profile                                     : DISABLED
    SSL Insert Space in Certificate Header              : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
    Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
    Software Crypto acceleration CPU Threshold          : 0
    Hybrid FIPS Mode                                    : DISABLED
    Signature and Hash Algorithms supported by TLS1.2   : ALL
    SSL Interception Error Learning and Caching         : DISABLED
    SSL Interception Maximum Error Cache Memory         : 0 Bytes
    NDCPP Compliance Certificate Check                  : YES
    Heterogeneous SSL HW (Cavium and Intel Based)       : ENABLED
 Done
<!--NeedCopy-->
```

Configurer la vérification du certificat de conformité NDCPP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL** et, dans le groupe **Paramètres**, sélectionnez **Modifier les paramètres SSL avancés**.



2. Sélectionnez **Vérification du certificat de conformité du NDCPP**. Cliquez sur **OK**.



Prise en charge de la renégociation sécurisée au niveau du back-end d'une appliance NetScaler

Remarque : Cette fonctionnalité est prise en charge dans les versions 13.0 build 58.x et ultérieures. Dans les versions et versions précédentes, seule la renégociation non sécurisée était prise en charge sur le back-end.

La fonctionnalité est prise en charge sur les plateformes suivantes :
• VPX
• Plates-formes MPX contenant des puces N2 ou N3
• Plateformes basées sur puce Intel Coleto SSL

La fonctionnalité n'est pas encore prise en charge sur la plateforme FIPS.

La renégociation sécurisée est refusée par défaut sur le back-end d'un boîtier ADC. En d'autres termes,

le paramètre denySSLReneg est défini sur ALL (par défaut).

Pour autoriser la renégociation sécurisée sur le serveur principal, sélectionnez l'un des paramètres suivants pour le paramètre denySSLReneg :

- NON
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NON SÉCURISÉ

Activer la renégociation sécurisée à l'aide du CLI

À l'invite de commande, tapez :

```
set ssl parameter -denySSLReneg <denySSLReneg>
```

Exemple :

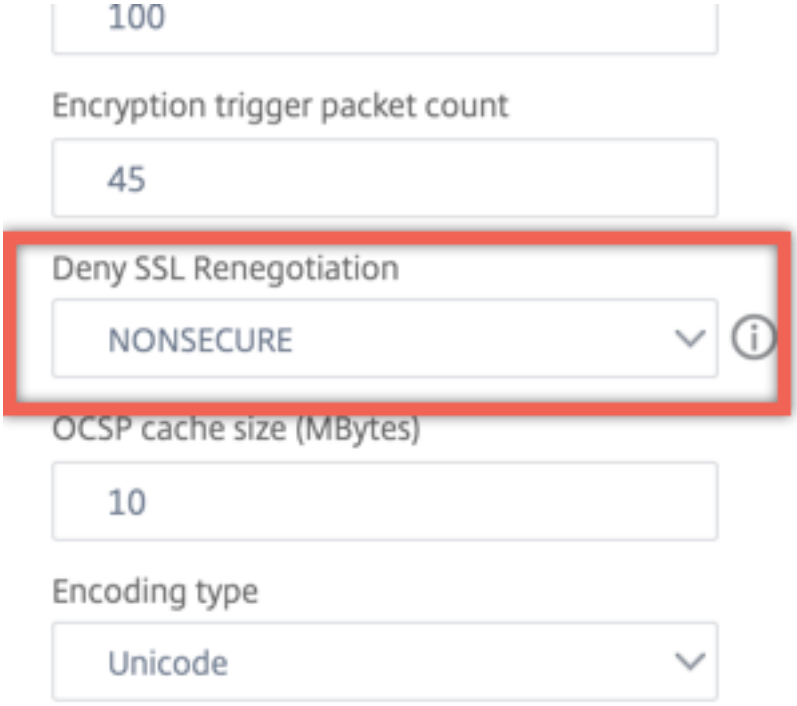
```
set ssl parameter -denySSLReneg NONSECURE
 Done

sh ssl parameter
Advanced SSL Parameters
-----------------------
    SSL quantum size                                    : 8 KB
    Max CRL memory size                                 : 256 MB
    Strict CA checks                                    : NO
    Encryption trigger timeout                          : 100 ms
    Send Close-Notify                                   : YES
    Encryption trigger packet count                     : 45
    Deny SSL Renegotiation                              : NONSECURE
    Subject/Issuer Name Insertion Format                : Unicode
    OCSP cache size                                     : 10 MB
    Push flag                                           : 0x0 (Auto)
    Strict Host Header check for SNI enabled SSL sessions : NO
    Match HTTP Host header with SNI                     : CERT
    PUSH encryption trigger timeout                     : 1 ms
    Crypto Device Disable Limit                         : 0
    Global undef action for control policies            : CLIENTAUTH
    Global undef action for data policies               : NOOP
    Default profile                                     : ENABLED
    SSL Insert Space in Certificate Header              : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
    Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
    Software Crypto acceleration CPU Threshold          : 0
    Hybrid FIPS Mode                                    : DISABLED
```



```
    Signature and Hash Algorithms supported by TLS1.2     : ALL
    SSL Interception Error Learning and Caching           : DISABLED
    SSL Interception Maximum Error Cache Memory           : 0 Bytes
    NDCPP Compliance Certificate Check                    : NO
    Heterogeneous SSL HW (Cavium and Intel Based)         : DISABLED
    Crypto Operation Queue Limit                          : 150%
 Done
<!--NeedCopy-->
```

Activer la renégociation sécurisée à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Modifier les paramètres SSL avancés**.
2. Définissez **Refuser la renégociation SSL** sur n'importe quelle valeur autre que ALL.



Contrôle du trafic SSL adaptatif

Remarque : Cette fonctionnalité est prise en charge dans les versions 13.0 build 58.x et ultérieures.

Lorsqu'un trafic élevé est reçu sur l'appliance et que la capacité d'accélération de chiffrement est pleine, l'appliance commence à mettre les connexions en file d'attente pour un traitement ultérieur. Actuellement, la taille de cette file d'attente est fixée à 64 K et l'appliance commence à abandonner les connexions si cette valeur est dépassée.

À partir de la version 13.0 build 58.x, l'utilisateur peut configurer une valeur représentant un pourcentage de la capacité réelle. Grâce à cette amélioration, l'appliance abandonne les nouvelles connexions si le nombre d'éléments dans la file d'attente est supérieur à la limite calculée de manière adaptative et dynamique. Cette approche contrôle les connexions SSL entrantes et empêche la consommation excessive de ressources et d'autres défaillances, telles que l'échec de la surveillance de l'équilibrage de charge ou la lenteur de réponse aux applications sécurisées, sur l'appliance.

Si la file d'attente est vide, l'appliance peut continuer à accepter les connexions. Si la file d'attente n'est pas vide, le système de chiffrement a atteint sa capacité et l'appliance commence à mettre les connexions en file d'attente.

La limite est calculée en fonction des éléments suivants :

- Capacité réelle de l'appareil.
- Valeur configurée par l'utilisateur en pourcentage de la capacité réelle. La valeur par défaut est fixée à 150 %.

Par exemple, si la capacité réelle d'un appareil est de 1 000 opérations/seconde à un moment donné et que le pourcentage par défaut est configuré, la limite après laquelle l'appliance abandonne les connexions est de 1 500 (150 % sur 1 000).

Pour configurer la limite de file d'attente des opérations à l'aide de l'interface

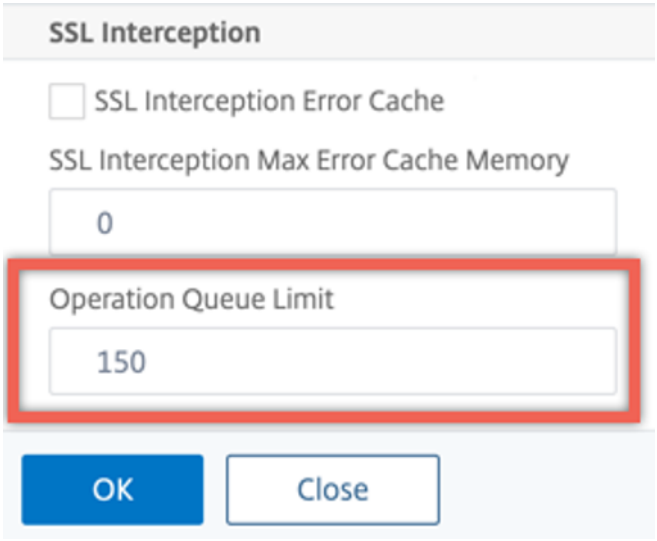
À l'invite de commande, tapez :

```
set ssl parameter -operationQueueLimit <positive_integer>
```

Limite de**file d'attente des opérations : limite** en pourcentage de capacité de la file d'attente des opérations de chiffrement au-delà de laquelle les nouvelles connexions SSL ne sont pas acceptées tant que la file d'attente n'est Valeur par défaut : 150. Valeur minimale : 0. Valeur maximale : 10 000.

Pour configurer la limite de file d'attente des opérations à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL**.
2. Dans **Paramètres**, cliquez sur **Modifier les paramètres SSL avancés**.
3. Entrez une valeur dans **Limite de file d'attente des opérations**. La valeur par défaut est 150.
4. Cliquez sur **OK**.



Déploiements de cluster hétérogènes

À partir de la version 13.0 build 47.x, vous pouvez créer un déploiement en cluster hétérogène d'appliances NetScaler MPX avec un nombre différent de moteurs de paquets en définissant le paramètre SSL « Heterogene SSL HW » sur ENABLED. Par exemple, pour former un cluster d'appliances basées sur la puce Cavium (MPX 14000 ou similaire) et d'appliances basées sur une puce Intel Coleto (MPX 15000 ou similaire), activez le paramètre SSL « Heterogeneous SSL HW. » Pour former un cluster de plates-formes utilisant la même puce, conservez la valeur par défaut (DISABLED) pour ce paramètre.

> **Remarques :**
>
> Les fonctionnalités suivantes ne sont pas prises en charge dans un cluster hétérogène :
>
> - Instances VPX hébergées sur des appliances NetScaler SDX.
> - Protocole SSLv3 sur les entités SSL, telles que le serveur virtuel, les services, le groupe de services et les services internes.
> - Seuil du processeur d'accélération crypto logicielle (utilisant du matériel et des logiciels pour améliorer les performances de chiffrement ECDSA et ECDHE).

Pour plus d'informations sur les plates-formes prises en charge dans un cluster hétérogène, reportez-vous à la section https://docs.citrix.com/en-us/citrix-adc/current-release/clustering/support-for-heterogeneous-cluster.html.

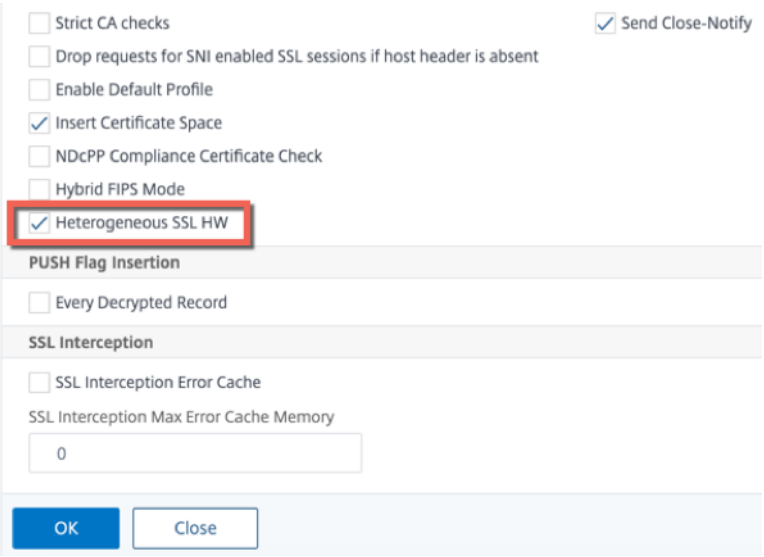
Activer un cluster hétérogène à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl parameter -heterogeneousSSLHW ENABLED
```


Activer un cluster hétérogène à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL** et, dans le groupe **Paramètres**, sélectionnez **Modifier les paramètres SSL avancés**.
2. Sélectionnez **HW SSL hétérogène**. Cliquez sur **OK**.



Mécanisme de déclenchement de chiffrement basé sur l'indicateur PU

Le mécanisme de déclenchement du chiffrement basé sur l'indicateur TCP PSH vous permet désormais d'effectuer les opérations suivantes :

- Fusionnez les paquets consécutifs dans lesquels l'indicateur PSH est défini en un seul enregistrement SSL, ou ignorez l'indicateur PSH.
- Effectuez un chiffrement basé sur le minuteur, dans lequel la valeur du délai d'expiration est définie globalement à l'aide de la commande `set ssl parameter -pushEncTriggerTimeout <positive_integer>`.

Configurer le chiffrement basé sur l'indicateur PUSH à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer le chiffrement basé sur l'indicateur PUSH et vérifier la configuration :

```
set ssl vserver <vServerName> [-pushEncTrigger <pushEncTrigger>]

show ssl vserver
<!--NeedCopy-->
```

Exemple :


```
set ssl vserver vserver1 -pushEncTrigger always

Done

sh ssl vserver vserver1

            Advanced SSL configuration for VServer vserver1:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: ENABLED

                Refresh Count: 0
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Push Encryption Trigger: Always
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: DISABLED
            DHE Key Exchange With PSK: NO
            Tickets Per Authentication Context: 1
            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT
            Description: Default cipher list with encryption strength
                >= 128bit
Done
<!--NeedCopy-->
```

Configurer le chiffrement basé sur l'indicateur PUSH à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et ouvrez un serveur

virtuel SSL.

2. Dans la section **Paramètres SSL**, dans la liste **Déclencheur de chiffrement PUSH**, sélectionnez une valeur.

Support de l'algorithme de hachage de signature TLS1.2

L'appliance NetScaler est entièrement compatible avec l'extension de hachage de signature TLS1.2.

Dans une poignée de main SSL, un client envoie une liste des algorithmes de hachage de signature pris en charge. Le client indique au serveur quelles paires d'algorithmes de hachage de signature peuvent être utilisées dans les messages d'établissement de liaison SSL (SKE et CCV) en utilisant l'extension « signature_algorithms ». Le champ « extension_data » de cette extension contient une valeur « supported_signature_algorithms » dans le message Client Hello. L'établissement de liaison SSL se poursuit si le serveur prend en charge l'un de ces algorithmes de hachage de signature. Si le serveur ne prend en charge aucun de ces algorithmes, la connexion est interrompue.

De même, si le serveur demande un certificat client pour l'authentification du client, le message de demande de certificat contient une valeur « supported_signature_algorithms ». Le certificat client est sélectionné en fonction de cet algorithme de hachage de signature.

> **Remarque :**
>
> L'appliance NetScaler agit comme un serveur pour un client et comme un client pour le serveur principal.

L'appliance prend uniquement en charge RSA-SHA1 et RSA-SHA256 sur le frontal, et RSA-MD5, RSA-SHA1 et RSA-SHA256 sur le serveur principal.

L'appliance MPX/SDX/VPX prend en charge les combinaisons de hachage de signature suivantes. Sur une appliance SDX, si une puce SSL est attribuée à une instance VPX, la prise en charge du chiffrement d'une appliance MPX s'applique. Sinon, le support de chiffrement normal d'une instance VPX s'applique.

- Sur une instance VPX et sur une appliance MPX/SDX sans puces N3 :
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224
  - RSA-SHA256
  - RSA-SHA384
  - RSA-SHA512
- Sur un appareil MPX/SDX équipé de puces N3 :
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224

- RSA-SHA256
- RSA-SHA384
- RSA-SHA512
- ECDSA-SHA1
- ECDSA-SHA224
- ECDSA-SHA256
- ECDSA-SHA384
- ECDSA-SHA512

Par défaut, tous les algorithmes de hachage de signature sont activés. Toutefois, vous ne pouvez activer que quelques algorithmes de hachage de signature à l'aide de la commande suivante :

```
set ssl parameter -sigDigestType <sigDigestType>

Parameters

sigDigestType

Signature digest algorithms supported by the appliance. The platform
    determines the list of algorithms supported by default.

              On VPX: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384
                   RSA-

              SHA512

              On MPX with N3 cards: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-

              SHA256 RSA-SHA384 RSA-SHA512 ECDSA-SHA1 ECDSA-SHA224
                  ECDSA-

              SHA256 ECDSA-SHA384 ECDSA-SHA512

              Other MPX Platforms: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-
                  SHA256 RSA-SHA384 RSA-

              SHA512.

    set ssl parameter -sigDigestType RSA-SHA224 RSA-SHA256 RSA-SHA384
        RSA-SHA512
<!--NeedCopy-->
```

Validez le certificat homologue

Selon la RFC 5246, le certificat homologue doit être signé à l'aide de l'un des algorithmes de hachage de signature inclus dans l'extension Client Hello. Vous pouvez utiliser le paramètre `strictSigDigestCheck`. Selon la liste de hachage de signature envoyée par le client, si vous l'activez `strictSigDigestCheck`, l'appliance renvoie un certificat signé par l'un des algorithmes de hachage de signature mentionnés dans l'extension Client Hello. Si l'homologue ne possède pas de certificat approprié, la connexion est abandonnée. Si ce paramètre est désactivé, le hachage de la signature n'est pas vérifié dans le certificat homologue.

Vous pouvez configurer une vérification stricte du résumé des signatures sur un serveur et un service virtuels SSL. Si vous activez ce paramètre sur un serveur virtuel SSL, le certificat de serveur envoyé par le serveur doit être signé par l'un des algorithmes de hachage de signature répertoriés dans l'extension Client Hello. Si l'authentification client est activée, le certificat client reçu par le serveur doit être signé à l'aide de l'un des algorithmes de hachage de signature répertoriés dans la demande de certificat envoyée par le serveur.

Si vous activez ce paramètre sur un service SSL, le certificat de serveur reçu par le client doit être signé par l'un des algorithmes de hachage de signature répertoriés dans l'extension Client Hello. Le certificat client doit être signé à l'aide de l'un des algorithmes de hachage de signature répertoriés dans le message de demande de certificat.

Si le profil par défaut est activé, vous pouvez l'utiliser pour configurer une vérification stricte du résumé de signature sur un serveur virtuel SSL, un service SSL et un profil SSL.

Configurez la vérification stricte du résumé de signature sur un serveur virtuel, un service ou un profil SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl vserver <vServerName> -strictSigDigestCheck ( ENABLED |
    DISABLED )

set ssl service <serviceName> -strictSigDigestCheck ( ENABLED |
    DISABLED )

set ssl profile <name>-strictSigDigestCheck ( ENABLED | DISABLED )

Parameters

strictSigDigestCheck

              Check whether peer entity certificate is signed using one
                  of the signature-hash algorithms supported by the
                 NetScaler appliance.

```



```
                Possible values: ENABLED, DISABLED

                Default: DISABLED
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver v1 -strictSigDigestCheck Enabled
set ssl service s1 -strictSigDigestCheck Enabled
set ssl profile p1 -strictSigDigestCheck Enabled
<!--NeedCopy-->
```

> **Important :**
>
> Si des chiffrements DH, ECDHE ou ECDSA sont configurés sur l'appliance, le message SKE doit être signé à l'aide de l'un des hachages de signature communs à la liste des clients et à la liste configurée sur l'appliance. S'il n'y a pas de hachage de signature commun, la connexion est supprimée.

Configurer SSL pour l'accès à l'interface utilisateur ADC Admin

Une paire de clés de certificat est requise pour l'accès HTTPS à l'utilitaire de configuration et pour les appels de procédure distante sécurisés. Sur une appliance NetScaler MPX ou une appliance virtuelle VPX, une paire de clés de certificat est automatiquement liée aux services internes. Cependant, il se peut que ce certificat ne soit pas approuvé par les navigateurs. Vous devez télécharger des certificats d'autorité de certification valides dans le navigateur pour terminer l'authentification sans erreur.

Configurez le protocole HTTPS sécurisé à l'aide de l'interface

Pour configurer HTTPS sécurisé à l'aide de l'interface de ligne de commande, procédez comme suit :

1. Ajoutez une paire de clés de certificat.

```
add certkey server -cert servercert -key serverkey
<!--NeedCopy-->
```

2. Liez cette paire de clés de certificat aux services internes suivants.

```
bind ssl service nshttps-127.0.0.1-443 -certkeyname server

bind ssl service nshttps-::11-443 -certkeyname server
<!--NeedCopy-->
```


Configurez le HTTPS sécurisé à l'aide de l'interface graphique

Pour configurer le protocole HTTPS sécurisé à l'aide de l'interface graphique, procédez comme suit :

1. Accédez à **Gestion du trafic > SSL > Certificats**.
2. Dans le volet d'informations, cliquez sur **Installer**.
3. Dans la boîte de dialogue **Install Certificate**, saisissez les détails du certificat.
4. Cliquez sur **Installer**, puis sur **Fermer**.
5. Accédez à **Traffic Management > Load Balancing > Services**.
6. Dans le volet de détails, sous l'onglet **Action**, cliquez sur **Services internes**.
7. Sélectionnez `nshttps-127.0.0.1-443` dans la liste, puis cliquez sur **Ouvrir**.
8. Dans l'onglet **Paramètres SSL**, dans le volet **Disponible**, sélectionnez le certificat créé à l'étape 4, cliquez sur **Lier**, puis sur **OK**.
9. Sélectionnez `nshttps-::1-443` dans la liste, puis cliquez sur **Ouvrir**.
10. Dans l'onglet **Paramètres SSL**, dans le volet **Disponible**, sélectionnez le certificat créé à l'étape 4, cliquez sur **Lier**, puis sur **OK**.
11. Cliquez sur **OK**.

Prise en charge du protocole TLSv1.3 tel que défini dans la RFC 8446

June 2, 2023

Les appliances NetScaler VPX et NetScaler MPX prennent désormais en charge le protocole TLSv1.3, spécifié dans la RFC 8446.

> **Remarques :**
>
> - Depuis la version 13.0 build 71.x et les versions ultérieures, l'accélération matérielle TLS1.3 est prise en charge sur les plates-formes suivantes :
>   - MPX 5900
>   - MPX/SDX 8900
>   - MPX/SDX 9100
>   - MPX/SDX 15000
>   - MPX/SDX 15000-50G
>   - MPX/SDX 16000
>   - MPX/SDX 26000
>   - MPX/SDX 26000-50S
>   - MPX/SDX 26000-100G
> - La prise en charge logicielle uniquement du protocole TLSv1.3 est disponible sur toutes les autres appliances NetScaler MPX et SDX, à l'exception des appliances NetScaler FIPS.

> - TLSv1.3 n'est pris en charge qu'avec le profil amélioré. Pour activer le profil amélioré, voir Activer le profil par défaut.
> - Pour utiliser TLS1.3, vous devez utiliser un client conforme à la spécification RFC 8446.

Fonctionnalités NetScaler prises en charge

Les fonctionnalités SSL suivantes sont prises en charge :

1. Suites de chiffrement TLSv1.3 :
   - TLS1.3-AES256-GCM-SHA384 (0x1302)
   - TLS1.3_CHACHA20_POLY1305_SHA256 (0x1303)
   - TLS1.3-AES128_GCM-SHA256 (0x1301)
2. Courbes ECC pour l'échange de clés éphémère Diffie-Hellman :
   - P_256
   - P_384
   - P_521
3. Poignées de contact abrégées lorsque la reprise de session basée sur des tickets est activée
4. Données d'application précoce 0-RTT
5. Authentification client facultative ou obligatoire basée sur un certificat, avec prise en charge de la validation OCSP et CRL des certificats clients
6. Extension du nom du serveur : sélection du certificat du serveur à l'aide de SNI
7. Négociation du protocole d'application (ALPN) à l'aide de l'extension application_level_protocol_negotiation
8. Agrafage OCSP
9. Les messages de journal et les enregistrements AppFlow sont produits pour les prises de contact TLSv1.3.
10. Enregistrement facultatif des secrets de trafic TLS 1.3 par l'utilitaire de capture de `nstrace` paquets.
11. Interopérabilité avec les clients TLS implémentant la RFC 8446. Par exemple, Mozilla Firefox, Google Chrome et OpenSSL.

Navigateurs pris en charge

Les versions de navigateur suivantes sont prises en charge et compatibles avec l'implémentation du protocole TLS 1.3 par NetScaler :

- Google Chrome - Version 72.0.3626.121 (version officielle) (64 bits)

- Mozilla Firefox - 65.0.2 (64 bits)
- Opera - Version:58.0.3135.79

Configuration

TLSv1.3 est désactivé par défaut sur un profil SSL.

Ajouter un profil SSL à l'aide de la CLI

À l'invite de commande, tapez :

```
add ssl profile <tls13-profile-name>
<!--NeedCopy-->
```

Exemple :

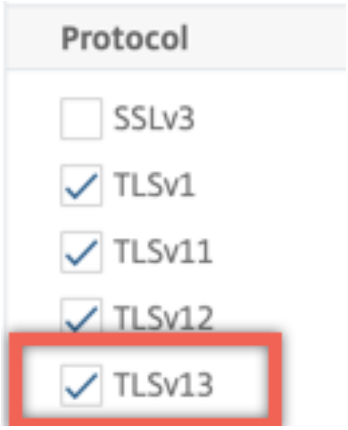
```
add ssl profile tls13profile

sh ssl profile tls13profile
1)  Name: tls13profile           (Front-End)
    SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1.1: ENABLED
       TLSv1.2: ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED                        Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED                              Refresh Count: 0
    Deny SSL Renegotiation                                ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:             1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions: NO
    Push flag:            0x0 (Auto)
```



```
27      SSL quantum size:                               8 kB
28      Encryption trigger timeout           100 mS
29      Encryption trigger packet count:                45
30      Subject/Issuer Name Insertion Format: Unicode
31
32      SSL Interception: DISABLED
33      SSL Interception OCSP Check: ENABLED
34      SSL Interception End to End Renegotiation: ENABLED
35      SSL Interception Maximum Reuse Sessions per Server:  10
36      Session Ticket: DISABLED
37      HSTS: DISABLED
38      HSTS IncludeSubDomains: NO
39      HSTS Max-Age: 0
40
41      ECC Curve: P_256, P_384, P_224, P_521
42
43  1)  Cipher Name: DEFAULT Priority :1
44      Description: Predefined Cipher Alias
45  Done
46  <!--NeedCopy-->
```

Ajouter un profil SSL à l'aide de l'interface graphique

1. Accédez à **Système > Profils**. Sélectionnez **Profils SSL**.
2. Cliquez sur **Ajouter** et spécifiez un nom pour le profil.
3. Dans **Protocol**, sélectionnez **TLSv13**.



4. Cliquez sur **OK**.

Lier un profil SSL à un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl vserver <vServerName> -sslProfile <tls13-profile-name>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver ssl-vs -sslProfile tls13profile
```

Lier un profil SSL à un serveur virtuel SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez un serveur virtuel SSL.
2. Dans **Paramètres avancés**, cliquez sur **Profil SSL**.
3. Sélectionnez le profil TLSv1.3 créé précédemment.
4. Cliquez sur **OK**.
5. Cliquez sur **Terminé**.

Paramètres de profil SSL pour le protocole TLSv1.3

1. Activez ou désactivez les paramètres TLS1.3 dans un profil SSL.

   tls13 : état de la prise en charge du protocole TLSv1.3 pour le profil SSL.

   Valeurs possibles : ENABLED, DISABLED

   Valeur par défaut : DISABLED

   ```
   set ssl profile tls13profile -tls13 enable
   <!--NeedCopy-->
   ```

   ```
   set ssl profile tls13profile -tls13 disable
   <!--NeedCopy-->
   ```

2. Définissez le nombre de tickets de session émis.

   tls13SessionTicketsPerAuthContext : Nombre de tickets émis par le serveur virtuel SSL lorsque TLS1.3 est négocié, que la reprise basée sur les tickets est activée et que (1) une négociation se termine ou (2) l'authentification du client se termine après l'établissement de la liaison.

   Cette valeur peut être augmentée pour permettre aux clients d'ouvrir plusieurs connexions parallèles à l'aide d'un nouveau ticket pour chaque connexion.

Aucun billet n'est envoyé si la reprise est désactivée.

Valeur par défaut : 1

Valeur minimale : 1

Valeur maximale : 10

```
set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 1

set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 10
<!--NeedCopy-->
```

3. Jeu d'échange de clés DH

   `dheKeyExchangeWithPsk`: indique si un serveur virtuel SSL nécessite un échange de clés DHE lorsqu'une clé prépartagée est acceptée lors d'une prise de contact de reprise de session TLS 1.3. Un échange de clés DHE garantit le secret de transmission, même si les clés de ticket sont compromises, au détriment des ressources supplémentaires nécessaires pour effectuer l'échange de clés **DHE** .

   Les paramètres disponibles fonctionnent comme suit, si le ticket de session est activé :

   OUI : L'échange de clés DHE est requis lorsqu'une clé pré-partagée est acceptée, que le client prenne ou non en charge l'échange de clés. La prise de contact est annulée avec une alerte fatale, si le client ne prend pas en charge l'échange de clés DHE lorsqu'il propose une clé pré-partagée.

   NON : L'échange de clés DHE est effectué lorsqu'une clé pré-partagée est acceptée, uniquement si le client le demande.

   Valeurs possibles : OUI, NON

   Valeur par défaut : NON

```
set ssl profile tls13profile dheKeyExchangeWithPsk yes

set ssl profile tls13profile dheKeyExchangeWithPsk no
<!--NeedCopy-->
```

4. Activer ou désactiver l'acceptation anticipée des données 0-RTT

   `zeroRttEarlyData`: état des données relatives aux premières applications du protocole TLS 1.3. Les paramètres applicables fonctionnent comme suit :

   ACTIVÉ : Les premières données d'application peuvent être traitées avant la fin de la prise de contact.
   DÉSACTIVÉ : les premières données d'application sont ignorées.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

```
set ssl profile tls13profile -zeroRttEarlyData ENABLED

set ssl profile tls13profile -zeroRttEarlyData DISABLED
<!--NeedCopy-->
```

Groupe de chiffrement par défaut

Le groupe de chiffrement par défaut inclut les chiffrements TLS1.3.

```
sh cipher DEFAULT
1) Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035

2)  Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
...
...
27) Cipher Name: TLS1.3-AES256-GCM-SHA384         Priority : 27
    Description: TLSv1.3 Kx=any      Au=any  Enc=AES-GCM(256) Mac=AEAD
         HexCode=0x1302

28) Cipher Name: TLS1.3_CHACHA20_POLY1305_SHA256     Priority : 28
    Description: TLSv1.3 Kx=any      Au=any  Enc=CHACHA20/POLY1305(256)
         Mac=AEAD   HexCode=0x1303

29) Cipher Name: TLS1.3-AES128_GCM-SHA256        Priority : 29
    Description: TLSv1.3 Kx=any      Au=any  Enc=AES-GCM(128) Mac=AEAD
         HexCode=0x1301
Done
<!--NeedCopy-->
```

Limitations

- TLSv1.3 n'est pas pris en charge sur le serveur principal.
- TLSv1.3 n'est pas pris en charge sur une appliance Citrix Secure Web Gateway et sur une appliance NetScaler FIPS.

- Seuls les certificats RSA avec des clés de 1024 bits et plus sont pris en charge dans un handshake TLSv1.3.

Restrictions relatives

Les opérateurs de serveur TLSv1.3 doivent garder à l'esprit les restrictions de sécurité suivantes relatives à la compatibilité descendante décrites dans la RFC 8446. La configuration par défaut sur un boîtier NetScaler est conforme à ces restrictions. Toutefois, une appliance NetScaler n'impose pas le respect de ces règles.

- La sécurité des suites de chiffrement RC4 est considérée comme insuffisante comme décrit dans le document RFC7465. Les implémentations ne doivent pas proposer ou négocier de suites de chiffrement RC4 pour aucune version de TLS.
- Les anciennes versions de TLS permettaient l'utilisation de chiffrements à faible intensité. Les chiffrements dont la force est inférieure à 112 bits ne doivent pas être proposés ou négociés pour aucune version de TLS.
- La sécurité de SSL 3.0 [SSLv3] est considérée comme insuffisante comme décrit dans la RFC7568, et ne doit pas être négociée. Désactivez SSLv3 lorsque TLSv1.3 est activé (SSLv3 est désactivé par défaut).
- La sécurité de SSL 2.0 [SSLv2] est considérée comme insuffisante comme décrit dans la RFC6176, et ne doit pas être négociée. Désactivez SSLv2 lorsque TLS 1.3 est activé (SSLv2 est désactivé par défaut).

> **Remarque :**
>
> Pour plus d'informations sur le dépannage des protocoles exécutés sur TLS1.3, consultez Déchiffrement du trafic TLS1.3 du suivi des paquets.

Articles pratiques

May 5, 2023

Les articles pratiques sont des articles simples et faciles à utiliser qui décrivent les étapes de configuration pour les déploiements courants. Cliquez sur un lien pour consulter l'article.

Créez une demande de signature de certificat et utilisez des certificats SSL sur une appliance NetScaler

Configurer l'action SSL pour transférer le trafic client

Configurer l'action SSL pour transférer le trafic client si un chiffrement n'est pas pris en charge sur l'ADC

Certificats SSL

May 5, 2023

Un certificat SSL, qui fait partie de toute transaction SSL, est un formulaire de données numérique (X509) qui identifie une entreprise (domaine) ou un individu. Le certificat possède un composant de clé publique visible par tout client qui souhaite lancer une transaction sécurisée avec le serveur. La clé privée correspondante, qui réside en toute sécurité sur l'appliance NetScaler, est utilisée pour effectuer le chiffrement et le déchiffrement par clé asymétrique (ou clé publique).

Vous pouvez obtenir un certificat SSL et une clé de l'une des manières suivantes :

- À partir d'une autorité de certification (CA) autorisée, telle que Verisign
- En générant un nouveau certificat SSL et une nouvelle clé sur l'appliance NetScaler

Vous pouvez également utiliser un certificat SSL existant sur l'appliance.

Les certificats sont classés en quatre types par l'appliance NetScaler :

- **Certificats de serveur :** un certificat de serveur authentifie l'identité du serveur auprès du client. Sur le front-end, l'appliance ADC joue le rôle de serveur. Vous liez un certificat de serveur et une clé privée à un serveur virtuel SSL sur l'appliance ADC.
- **Certificats clients :** Un certificat client authentifie l'identité du client auprès du serveur. Sur le back-end, l'appliance ADC agit en tant que client. Vous liez un certificat client et une clé privée au service SSL ou au groupe de services sur l'appliance ADC.
- **Certificats d'autorité de certification :** les certificats d'autorité de certification délivrent les certificats d'utilisateur final (certificats client et serveur). Un certificat d'autorité de certification peut être une autorité de certification racine approuvée (auto-signée par l'autorité de certification) ou une autorité de certification intermédiaire (signée par une autorité de certification racine approuvée). En règle générale, les certificats d'autorité de certification n'ont pas besoin de clés privées.
- **Certificats inconnus :** Tous les autres certificats entrent dans cette catégorie.

Important : Citrix vous recommande d'utiliser des certificats obtenus auprès d'autorités de certification autorisées, telles que Verisign, pour toutes vos transactions SSL. Utilisez les certificats générés sur l'appliance NetScaler à des fins de test uniquement, et non dans le cadre d'un déploiement en direct.

- Si, lors de l'ajout d'une paire de clés de certificat, vous ajoutez un fichier de certificat portant le même nom qu'un fichier de certificat existant, le fichier de certificat d'origine est écrasé sans avertissement. Cette action peut entraîner des problèmes après le redémarrage de la solution matérielle-logicielle, car le fichier de certificat d'origine n'est plus disponible dans le `/nsconfig/ssl` répertoire.
- La suppression de tout certificat ou fichier clé dans un environnement de cluster limite la configuration de l'appliance ADC. Rajoutez les fichiers au même emplacement pour apporter des modifications de configuration.

Remarque : vous pouvez utiliser le tableau de bord SSL ADM pour faciliter la gestion des certificats SSL et définir des notifications pour les certificats qui ne sont pas utilisés ou qui expirent bientôt. Pour plus d'informations, voir Gestion des certificats SSL.

Créer un certificat

July 31, 2023

Une autorité de certification (CA) est une entité qui émet des certificats numériques destinés à être utilisés dans la cryptographie à clé publique. Les applications, telles que les navigateurs Web, qui effectuent des transactions SSL font confiance aux certificats émis ou signés par une autorité de certification. Ces applications tiennent à jour une liste des autorités de certification auxquelles elles font

confiance. Si l'une des autorités de certification de confiance signe le certificat utilisé pour la transaction sécurisée, l'application poursuit la transaction.

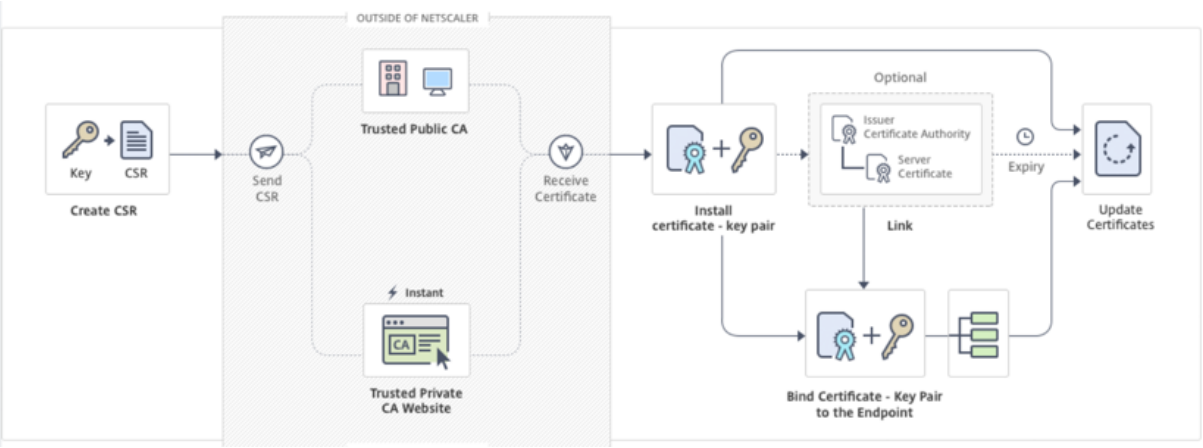
Attention : Citrix vous recommande d'utiliser des certificats obtenus auprès d'autorités de certification autorisées, telles que Verisign, pour toutes vos transactions SSL. Utilisez les certificats générés sur l'appliance NetScaler à des fins de test uniquement, et non dans le cadre d'un déploiement en direct.

Pour importer un certificat et une clé existants, reportez-vous à la section Importer un certificat.

Procédez comme suit pour créer un certificat et le lier à un serveur virtuel SSL. Les seuls caractères spéciaux autorisés dans les noms de fichiers sont le trait de soulignement et le point. Les caractères spéciaux ne sont pas autorisés comme premier caractère du nom de fichier.

- Créez une clé privée.
- Créez une demande de signature de certificat (CSR).
- Soumettez le CSR à une autorité de certification.
- Créez une paire de clés de certificat.
- Liez la paire de clés de certificat à un serveur virtuel SSL

Le schéma suivant illustre le flux de travail.



Comment créer et installer un nouveau certificat

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Créer une clé privée

> **Remarques :**
>
> - À partir de la version 12.1 build 49.x, vous pouvez utiliser l'algorithme AES256 au format de clé PEM pour chiffrer une clé privée sur l'appliance. L'AES avec clé 256 bits est plus efficace et plus sécurisé sur le plan mathématique par rapport à la clé 56 bits du Data Encryption

> Standard (DES).
>
> - À partir de la version 12.1 build 50.x, vous pouvez créer une clé RSA au format PKCS #8.

La clé privée est la partie la plus importante d'un certificat numérique. Par définition, cette clé ne doit être partagée avec personne et doit être conservée en toute sécurité sur l'appliance NetScaler. Toutes les données chiffrées avec la clé publique ne peuvent être déchiffrées qu'à l'aide de la clé privée.

Le certificat que vous recevez de l'autorité de certification n'est valide qu'avec la clé privée qui a été utilisée pour créer la demande de signature de certificat. La clé est requise pour ajouter le certificat à l'appliance NetScaler.

L'appliance prend uniquement en charge les algorithmes de cryptage RSA pour créer des clés privées. Vous pouvez soumettre l'un ou l'autre type de clé privée à l'autorité de certification (CA). Le certificat que vous recevez de l'autorité de certification n'est valide qu'avec la clé privée qui a été utilisée pour créer la demande de signature de certificat. La clé est requise pour ajouter le certificat à l'appliance NetScaler.

Important :

> - Veillez à limiter l'accès à votre clé privée. Toute personne ayant accès à votre clé privée peut déchiffrer vos données SSL.
> - La longueur du nom de clé SSL autorisé inclut la longueur du chemin d'accès absolu si le chemin est inclus dans le nom de la clé.

Tous les certificats et clés SSL sont stockés dans le dossier `/nsconfig/ssl` de l'appliance. Pour plus de sécurité, vous pouvez utiliser l'algorithme DES ou triple DES (3DES) pour chiffrer la clé privée stockée sur l'appliance.

Créer une clé privée RSA à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

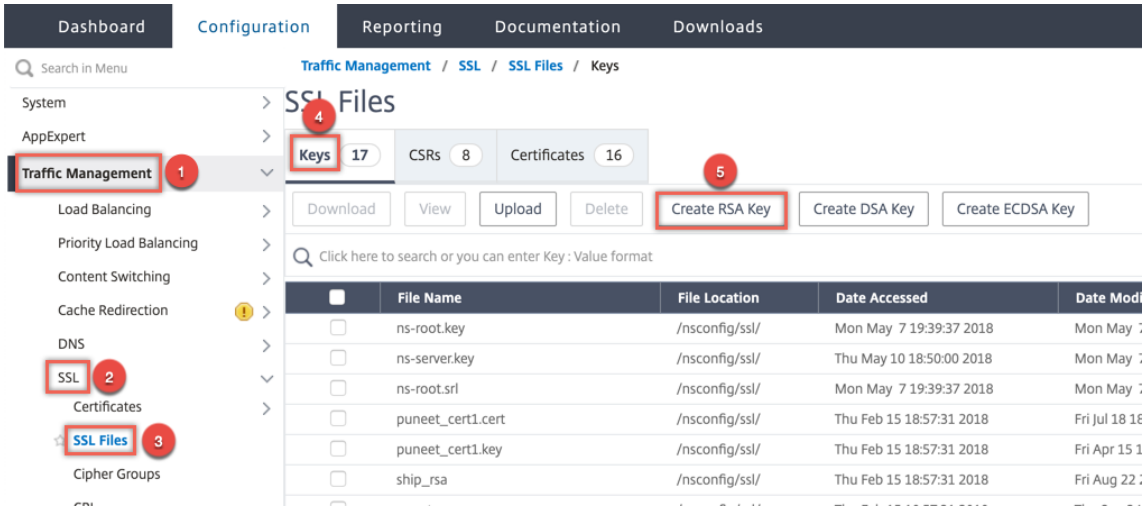
```
create ssl rsakey <keyFile> <bits> [-exponent ( 3 | F4 )] [-keyform (
    DER | PEM )] [-des | -des3 | -aes256] {
 -password  }
  [-pkcs8]
<!--NeedCopy-->
```

Exemple :

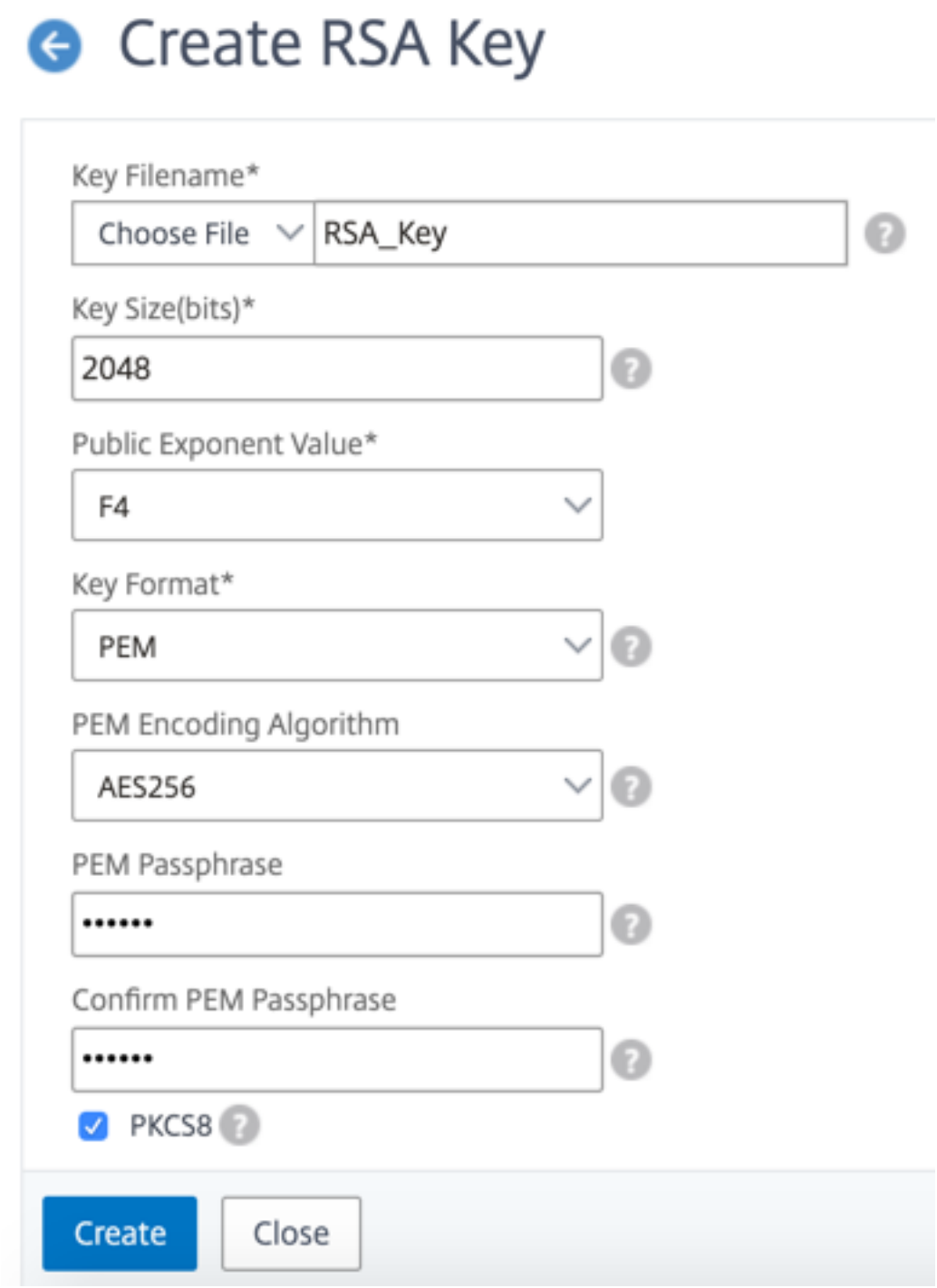
```
create rsakey testkey 2048 -aes256 -password 123456 -pkcs8
<!--NeedCopy-->
```


Créer une clé privée RSA à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Fichiers SSL**.
2. Dans l'onglet **Clés**, sélectionnez **Créer une clé RSA**.



3. Entrez des valeurs pour les paramètres suivants et cliquez sur **Créer**.
   - **Key Filename** : nom du fichier de clé RSA et, éventuellement, chemin d'accès au fichier clé RSA. /nsconfig/ssl/ est le chemin par défaut.
   - **Taille de la clé** : taille, en bits, de la clé RSA. Peut aller de 512 bits à 4096 bits.
   - **Valeur de l'exposant public** : exposant public pour la clé RSA. L'exposant fait partie de l'algorithme de chiffrement et est nécessaire à la création de la clé RSA.
   - **Format de clé** : format dans lequel le fichier de clé RSA est stocké sur l'appliance.
   - **Algorithme de codage PEM** : cryptez la clé RSA générée à l'aide de l'algorithme AES 256, DES ou Triple-DES (DES3). Par défaut, les clés privées ne sont pas chiffrées.
   - **Phrase secrète PEM** : si la clé privée est cryptée, saisissez une phrase de passe pour la clé.



Sélectionnez un algorithme de codage AES256 dans une clé RSA à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Fichiers SSL > Créer une clé RSA**.

2. Dans **Format de clé**, sélectionnez **PEM**.
3. Dans **Algorithme de codage PEM**, sélectionnez **AES256**.
4. Sélectionnez **PKCS8**.

Créer une demande de signature de certificat à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

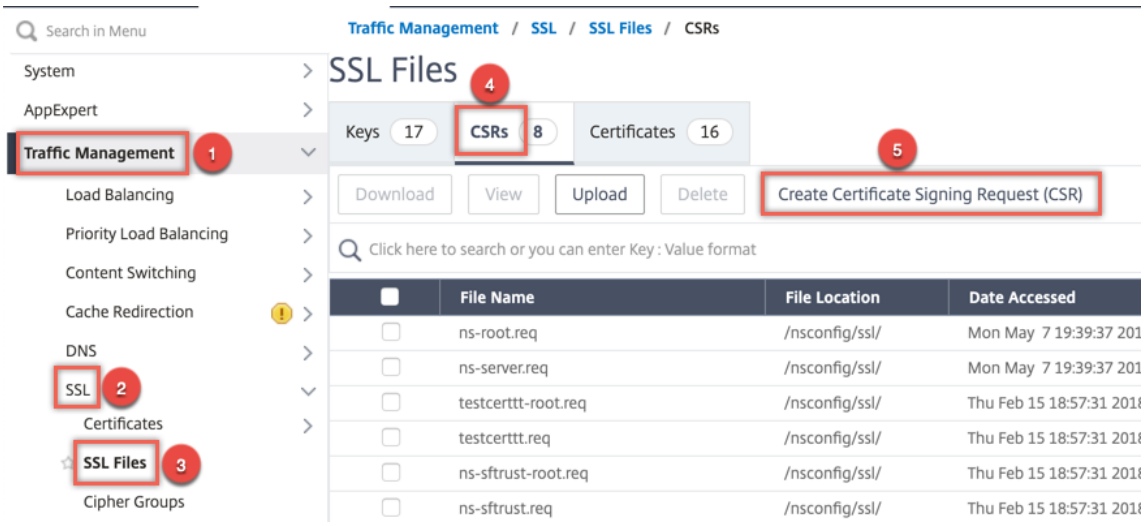
```
create ssl certreq <reqFile> -keyFile <input_filename> | -fipsKeyName <
   string>) [-keyForm (DER | PEM) {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName <string>
     -organizationUnitName <string> -localityName <string> -commonName
    <string> -emailAddress <string> {
 -challengePassword  }
  -companyName <string> -digestMethod ( SHA1 | SHA256 )
<!--NeedCopy-->
```

Exemple :

```
create ssl certreq priv_csr_sha256 -keyfile priv_2048_2 -keyform PEM -
   countryName IN -stateName Karnataka -localityName Bangalore -
   organizationName Citrix -organizationUnitName NS -digestMethod
   SHA256
<!--NeedCopy-->
```

Créer une demande de signature de certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL**.
2. Dans Certificat **SSL**, cliquez sur **Créer une demande de signature de certificat (CSR)**.



3. Dans Méthode **de synthèse**, sélectionnez **SHA256**.

Pour plus d'informations, reportez-vous à la section Créer une CSR .

Prise en charge du nom alternatif du sujet dans une demande de signature de certificat

Le champ Subject Alternative Name (SAN) d'un certificat vous permet d'associer plusieurs valeurs, telles que des noms de domaine et des adresses IP, à un seul certificat. En d'autres termes, vous pouvez sécuriser plusieurs domaines, tels que www.exemple.com, www.exemple1.com, www.exemple2.com, avec un seul certificat.

Certains navigateurs, tels que Google Chrome, ne prennent plus en charge un nom commun dans une demande de signature de certificat (CSR). Ils appliquent le SAN dans tous les certificats approuvés publiquement.

L'appliance NetScaler prend en charge l'ajout de valeurs SAN lors de la création d'un CSR. Vous pouvez envoyer une demande de signature de certificat avec une entrée SAN à une autorité de certification pour obtenir un certificat signé avec cette entrée SAN. Lorsque l'appliance reçoit une demande, elle recherche un nom de domaine correspondant dans les entrées SAN du certificat de serveur. Si une correspondance est trouvée, il envoie le certificat au client et termine la négociation SSL. Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique pour créer une demande de signature de certificat avec des valeurs SAN.

> **Remarque :** L'appliance NetScaler traite uniquement les valeurs SAN basées sur le DNS.

Créer une demande de signature de certificat avec l'autre nom de l'objet à l'aide de l'interface

```
1 create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
     <string>) [-subjectAltName <string>] [-keyform ( DER | PEM )  {
2  -PEMPassPhrase  }
```



```
3   ] -countryName <string> -stateName <string> -organizationName <string>
        [-organizationUnitName <string>] [-localityName <string>] [-
       commonName <string>] [-emailAddress <string>] {
4   -challengePassword  }
5    [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
6   <!--NeedCopy-->
```

Paramètres :

SubjectAltName : L'autre nom de l'objet (SAN) est une extension de X.509 qui permet d'associer différentes valeurs à un certificat de sécurité à l'aide d'un champ SubjectAltName. Ces valeurs sont appelées « Subject Alternative Names » (SAN). Les noms incluent :

1. Adresses IP (préfixe avec « IP : » Exemple : IP : 198.51.10.5 IP : 192.0.2.100)
2. Noms DNS (préfixe avec « DNS : » Exemple : DNS : www.exemple.com DNS : www.exemple.org DNS : www.exemple.net)

Sur la ligne de commande, entrez des valeurs entre guillemets. Séparez deux valeurs par un espace. Les guillemets ne sont pas obligatoires dans l'interface graphique.
Longueur maximale : 127

Exemple :

```
1  create certReq test1.csr -keyFile test1.ky -countryName IN -stateName
       Kar -organizationName citrix -commonName ctx.com -subjectAltName "
       DNS:*.example.com DNS:www.example.org DNS:www.example.net"
2  <!--NeedCopy-->
```

> **Remarque :**
>
> Sur une appliance FIPS, vous devez remplacer le nom du fichier clé par le nom de la clé FIPS si vous créez la clé FIPS directement sur l'appliance.
>
> ```
> 1  create certReq <csrname> -fipsKeyName fipskey.ky -countryName IN -
>        stateName Kar -organizationName citrix -commonName ctx.com -
>        subjectAltName "DNS:www.example.com DNS:www.example.org DNS:www.
>        example.net"
> 2  <!--NeedCopy-->
> ```

Créer un CSR à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Fichiers SSL**.
2. Dans l'onglet **CSR**, cliquez sur **Create Certificate Signing Request (CSR)**.
3. Entrez les valeurs et cliquez sur **Créer**.

Limitations

Pour utiliser le SAN lors de la création d'un certificat SSL, vous devez spécifier explicitement les valeurs du SAN. Les valeurs ne sont pas lues automatiquement à partir du fichier CSR.

Soumettre le CSR à l'autorité de certification

La plupart des autorités de certification (CA) acceptent les soumissions de certificats par e-mail. L'autorité de certification renvoie un certificat valide à l'adresse e-mail à partir de laquelle vous soumettez le CSR.

La demande de signature de certificat est stockée dans le dossier `/nsconfig/ssl`.

Générer un certificat de test

> **Remarque :**
>
> Pour générer un certificat de test de serveur, reportez-vous à la section Génération d'un certificat de test de serveur.

L'appliance NetScaler possède une suite d'outils CA intégrée que vous pouvez utiliser pour créer des certificats autosignés à des fins de test.

Attention : étant donné que c'est l'appliance NetScaler qui signe ces certificats, et non une véritable autorité de certification, vous ne devez pas les utiliser dans un environnement de production. Si vous tentez d'utiliser un certificat auto-signé dans un environnement de production, les utilisateurs reçoivent un avertissement « certificat non valide » à chaque accès au serveur virtuel.

L'appliance prend en charge la création des types de certificats suivants :

- Certificats Root-CA
- Certificats CA intermédiaires
- Certificats d'utilisateur final
  - certificats de serveur
  - certificats clients

Avant de générer un certificat, créez une clé privée et utilisez-la pour créer une demande de signature de certificat (CSR) sur l'appliance. Ensuite, au lieu d'envoyer le CSR à une autorité de certification, utilisez les outils NetScaler CA pour générer un certificat.

Création d'un certificat à l'aide d'un assistant

1. Accédez à **Gestion du trafic > SSL**.
2. Dans le volet d'informations, sous **Démarrage**, sélectionnez l'assistant correspondant au type de certificat que vous souhaitez créer.
3. Suivez les instructions qui s'affichent à l'écran.

Créer un certificat d'autorité de certification racine à l'aide de la CLI

À l'invite de commandes, tapez la commande suivante :

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
<!--NeedCopy-->
```

Dans l'exemple suivant, csreq1 est le CSR et rsa1 est la clé privée qui a été créée précédemment.

Exemple :

```
create ssl cert cert1 csreq1 ROOT_CERT -keyFile rsa1 -keyForm PEM -days
     365

  Done
<!--NeedCopy-->
```

Créer un certificat CA intermédiaire à l'aide de l'interface de ligne de commande

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
     [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
     DER | PEM )] [-CAkey <input_filename>] [-CAkeyForm ( DER | PEM )]
    [-CAserial <output_filename>]
<!--NeedCopy-->
```

Dans l'exemple suivant, csr1 est la CSR créée précédemment. Cert1 et rsakey1 sont le certificat et la clé correspondante du certificat auto-signé (autorité de certification racine), et pvtkey1 est la clé privée du certificat d'autorité de certification intermédiaire.

Exemple :

```
create ssl cert certsy csr1 INTM_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23
Done

create ssl rsakey pvtkey1 2048 -exponent F4 -keyform PEM
Done
<!--NeedCopy-->
```


Créer un certificat d'autorité de certification racine à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL** et, dans le groupe Mise en route, sélectionnez **Assistant Certificat d'autorité de certification racine**et configurez un certificat d'autorité de certification racine.

Créer un certificat CA intermédiaire à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL** et, dans le groupe Mise en route, sélectionnez **Assistant Certificat d'autorité de certification intermédiaire**et configurez un certificat d'autorité de certification intermédiaire.

Créer un certificat d'utilisateur final

Un certificat d'utilisateur final peut être un certificat client ou un certificat de serveur. Pour créer un certificat d'utilisateur final de test, spécifiez le certificat d'autorité de certification intermédiaire ou le certificat d'autorité de certification racine auto-signé.

> **Remarque :** Pour créer un certificat d'utilisateur final à des fins de production, spécifiez un certificat d'autorité de certification approuvée et envoyez la demande de signature de certificat à une autorité de certification (CA).

Créer un certificat d'utilisateur final de test à l'aide de l'interface de ligne de commande

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days<positive_integer>]
    [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
    DER | PEM )] [-CAkey<input_filename>] [-CAkeyForm ( DER | PEM )] [-
    CAserial <output_filename>]
<!--NeedCopy-->
```

S'il n'y a pas de certificat intermédiaire, utilisez les valeurs de certificat (cert1) et de clé privée (rsakey1) du certificat d'autorité de certification racine dans `CAcert` et `CAkey`.

Exemple :

```
create ssl cert cert12 csr1 SRVR_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23

Done
<!--NeedCopy-->
```

S'il existe un certificat intermédiaire, utilisez les valeurs de certificat (`certsy`) et de clé privée (pvtkey1) du certificat intermédiaire dans `CAcert` et `CAkey`.

Exemple :

```
create ssl cert cert12 csr1 SRVR_CERT -CAcert certsy -CAkey pvtkey1 -
    CAserial 23

Done
<!--NeedCopy-->
```

Création d'un certificat SAN auto-signé à l'aide d'OpenSSL

Pour créer un certificat SAN auto-signé avec plusieurs autres noms d'objet, effectuez les opérations suivantes :

1. Créez un fichier de configuration OpenSSL sur votre ordinateur local en modifiant les champs associés selon les exigences de l'entreprise.

   Remarque : Dans l'exemple suivant, le fichier de configuration est « req.conf ».

   ```
   [req]
   distinguished_name = req_distinguished_name
   x509_extensions = v3_req
   prompt = no
   [req_distinguished_name]
   C = US
   ST = VA
   L = SomeCity
   O = MyCompany
   OU = MyDivision
   CN = www.company.com
   [v3_req]
   keyUsage = keyEncipherment, dataEncipherment
   extendedKeyUsage = serverAuth
   subjectAltName = @alt_names
   [alt_names]
   DNS.1 = www.company.net
   DNS.2 = company.com
   DNS.3 = company.net
   <!--NeedCopy-->
   ```

2. Téléchargez le fichier dans le répertoire /nsconfig/ssl de l'appliance NetScaler.
3. Connectez-vous à NetScaler CLI en tant qu' `nsroot` utilisateur et passez à l'invite du shell.
4. Exécutez la commande suivante pour créer le certificat :

   ```
   cd /nsconfig/ssl
   ```



```
openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout cert.
    pem -out cert.pem -config req.conf -extensions 'v3_req'
<!--NeedCopy-->
```

5. Exécutez la commande suivante pour vérifier le certificat :

```
openssl x509 -in cert.pem -noout  - text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
ed:90:c5:f0:61:78:25:ab
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
    www.company.com
Validity
Not Before: Nov 6 22:21:38 2012 GMT
Not After : Nov 6 22:21:38 2014 GMT
Subject: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
    www.company.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
…
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage:
Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Subject Alternative Name:
DNS:www.company.net, DNS:company.com, DNS:company.net
Signature Algorithm: md5WithRSAEncryption …
<!--NeedCopy-->
```

Installer, lier et mettre à jour des certificats

July 31, 2023

Pour installer un certificat, reportez-vous à la section Ajouter ou mettre à jour une paire de clés de certificat.

Certificats de liaison

De nombreux certificats de serveur sont signés par plusieurs autorités de certification (CA) hiérarchiques, ce qui signifie que les certificats forment une chaîne comme celle-ci :

```
Root CA
|
+----------- Intermediate CA
|
+----------------------- End-Entity (Server) Certificate
```

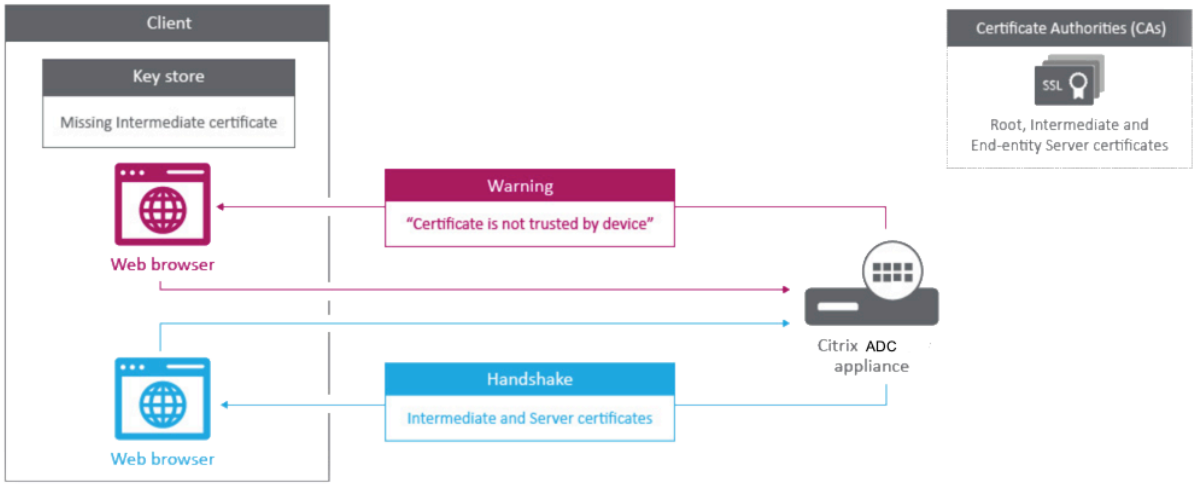
Parfois, l'autorité de certification intermédiaire est divisée en un certificat d'autorité de certification intermédiaire principal et secondaire. Ensuite, les certificats forment une chaîne comme celle-ci :

```
Root CA
|
+------ Primary Intermediate CA
|+-------------- Secondary Intermediate CA
|
+----------------------- End-Entity (Server) Certificate
```

Les machines clientes contiennent généralement le certificat d'autorité de certification racine dans leur magasin de certificats local, mais pas un ou plusieurs certificats d'autorité de certification intermédiaires. L'appliance ADC doit envoyer un ou plusieurs certificats d'autorité de certification intermédiaires aux clients.

Remarque : L'appliance ne doit pas envoyer le certificat d'autorité de certification racine au client. Le modèle de relation d'approbation de l'infrastructure à clé publique (PKI) exige que les certificats d'autorité de certification racine soient installés sur les clients par le biais d'une méthode hors bande. Par exemple, les certificats sont inclus avec le système d'exploitation ou le navigateur Web. Le client ignore un certificat d'autorité de certification racine envoyé par l'appliance.

Parfois, une autorité de certification intermédiaire que les navigateurs Web standard ne reconnaissent pas comme une autorité de certification de confiance émet le certificat de serveur. Dans ce cas, un ou plusieurs certificats d'autorité de certification doivent être envoyés au client avec le propre certificat du serveur. Sinon, le navigateur met fin à la session SSL car il ne parvient pas à authentifier le certificat du serveur.



Reportez-vous aux sections suivantes pour ajouter le serveur et les certificats intermédiaires :

- Liaison manuelle des certificats
- Liaison automatique des certificats
- Création d'une chaîne de certificats

Comment associer un certificat d'autorité intermédiaire

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Liaison manuelle des certificats

Remarque : Cette fonctionnalité n'est pas prise en charge sur la plate-forme NetScaler FIPS ni dans une configuration de cluster.

Au lieu d'ajouter et de lier des certificats individuels, vous pouvez désormais regrouper un certificat de serveur et jusqu'à neuf certificats intermédiaires dans un seul fichier. Vous pouvez spécifier le nom du fichier lors de l'ajout d'une paire de clés de certificat. Avant cela, assurez-vous que les conditions préalables suivantes sont remplies.

- Les certificats contenus dans le fichier sont dans l'ordre suivant :
  - Certificat de serveur (doit être le premier certificat du fichier)
  - Facultativement, une clé de serveur
  - Certificat intermédiaire 1 (ic1)
  - Certificat intermédiaire 2 (ic2)
  - Certificat intermédiaire 3 (ic3), etc.
    Remarque : des fichiers de certificats intermédiaires sont créés pour chaque certificat intermédiaire portant le nom "<certificatebundlename>.pem_ic<
    n>" où n est compris entre 1 et 9. Par exemple, bundle.pem_ic1, où **bundle** est le nom du jeu de certificats et ic1 est le premier certificat intermédiaire de l'ensemble.
- L'option Bundle est sélectionnée.
- Le dossier ne contient pas plus de neuf certificats intermédiaires.

Le fichier est analysé et le certificat de serveur, les certificats intermédiaires et la clé de serveur (le cas échéant) sont identifiés. Tout d'abord, le certificat et la clé du serveur sont ajoutés. Ensuite, les certificats intermédiaires sont ajoutés, dans l'ordre dans lequel ils ont été ajoutés au fichier, et liés en conséquence.

Une erreur est signalée si l'une des conditions suivantes existe :

- Un fichier de certificat pour l'un des certificats intermédiaires existe sur l'appliance.
- La clé est placée avant le certificat du serveur dans le fichier.
- Un certificat intermédiaire est placé avant le certificat du serveur.

- Les certificats intermédiaires ne sont pas placés dans le fichier dans le même ordre que celui où ils ont été créés.
- Aucun certificat n'est présent dans le fichier.
- Un certificat n'est pas au format PEM approprié.
- Le nombre de certificats intermédiaires dans le fichier est supérieur à neuf.

Ajouter un jeu de certificats à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour créer un jeu de certificats et vérifier la configuration :

```
add ssl certKey <certkeyName> -cert <string> -key <string> -bundle (YES
    | NO)

show ssl

show ssl certlink
<!--NeedCopy-->
```

Dans l'exemple suivant, le jeu de certificats (bundle.pem) contient les fichiers suivants :

Certificat de serveur (bundle) lié à bundle_ic1

Premier certificat intermédiaire (bundle_ic1) lié à bundle_ic2

Deuxième certificat intermédiaire (bundle_ic2) lié à bundle_ic3

Troisième certificat intermédiaire (bundle_ic3)

```
add ssl certKey bundletest -cert bundle9.pem -key bundle9.pem -bundle
   yes

sh ssl certkey

1)      Name: ns-server-certificate
        Cert Path: ns-server.cert
        Key Path: ns-server.key
        Format: PEM
        Status: Valid,   Days to expiration:5733
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
```



```
        Issuer:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Validity
                Not Before: Apr 21 15:56:16 2016 GMT
                Not After : Mar  3 06:30:56 2032 GMT
        Subject:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

2)      Name: servercert
        Cert Path: complete/server/server_rsa_1024.pem
        Key Path: complete/server/server_rsa_1024.ky
        Format: PEM
        Status: Valid,   Days to expiration:7150
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 1F
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:  C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix
        Validity
                Not Before: Sep  2 09:54:07 2008 GMT
                Not After : Jan 19 09:54:07 2036 GMT
        Subject:  C=IN,ST=KAR,O=Citrix Pvt Ltd,CN=Citrix
        Public Key Algorithm: rsaEncryption
        Public Key size: 1024

3)      Name: bundletest
        Cert Path: bundle9.pem
        Key Path: bundle9.pem
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Validity
                Not Before: Nov 28 06:43:11 2014 GMT
                Not After : Nov 25 06:43:11 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=Server9
```



```
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

4)      Name: bundletest_ic1
        Cert Path: bundle9.pem_ic1
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA8
        Validity
                Not Before: Nov 28 06:42:56 2014 GMT
                Not After : Nov 25 06:42:56 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

5)      Name: bundletest_ic2
        Cert Path: bundle9.pem_ic2
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA7
        Validity
                Not Before: Nov 28 06:42:55 2014 GMT
                Not After : Nov 25 06:42:55 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA8
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

6)      Name: bundletest_ic3
        Cert Path: bundle9.pem_ic3
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
```



```
104         Certificate Type: Intermediate CA
105         Version: 3
106         Serial Number: 01
107         Signature Algorithm: sha256WithRSAEncryption
108         Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA6
109         Validity
110                 Not Before: Nov 28 06:42:53 2014 GMT
111                 Not After : Nov 25 06:42:53 2024 GMT
112         Subject:  C=IN,ST=ka,O=sslteam,CN=ICA7
113         Public Key Algorithm: rsaEncryption
114         Public Key size: 2048
115
116 7)      Name: bundletest_ic4
117         Cert Path: bundle9.pem_ic4
118         Format: PEM
119         Status: Valid,   Days to expiration:3078
120         Certificate Expiry Monitor: ENABLED
121         Expiry Notification period: 30 days
122         Certificate Type: Intermediate CA
123         Version: 3
124         Serial Number: 01
125         Signature Algorithm: sha256WithRSAEncryption
126         Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA5
127         Validity
128                 Not Before: Nov 28 06:42:51 2014 GMT
129                 Not After : Nov 25 06:42:51 2024 GMT
130         Subject:  C=IN,ST=ka,O=sslteam,CN=ICA6
131         Public Key Algorithm: rsaEncryption
132         Public Key size: 2048
133
134 8)      Name: bundletest_ic5
135         Cert Path: bundle9.pem_ic5
136         Format: PEM
137         Status: Valid,   Days to expiration:3078
138         Certificate Expiry Monitor: ENABLED
139         Expiry Notification period: 30 days
140         Certificate Type: Intermediate CA
141         Version: 3
142         Serial Number: 01
143         Signature Algorithm: sha256WithRSAEncryption
144         Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA4
145         Validity
146                 Not Before: Nov 28 06:42:50 2014 GMT
147                 Not After : Nov 25 06:42:50 2024 GMT
148         Subject:  C=IN,ST=ka,O=sslteam,CN=ICA5
```



```
149          Public Key Algorithm: rsaEncryption
150          Public Key size: 2048
151
152  9)      Name: bundletest_ic6
153          Cert Path: bundle9.pem_ic6
154          Format: PEM
155          Status: Valid,   Days to expiration:3078
156          Certificate Expiry Monitor: ENABLED
157          Expiry Notification period: 30 days
158          Certificate Type: Intermediate CA
159          Version: 3
160          Serial Number: 01
161          Signature Algorithm: sha256WithRSAEncryption
162          Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA3
163          Validity
164                  Not Before: Nov 28 06:42:48 2014 GMT
165                  Not After : Nov 25 06:42:48 2024 GMT
166          Subject:  C=IN,ST=ka,O=sslteam,CN=ICA4
167          Public Key Algorithm: rsaEncryption
168          Public Key size: 2048
169
170  10)     Name: bundletest_ic7
171          Cert Path: bundle9.pem_ic7
172          Format: PEM
173          Status: Valid,   Days to expiration:3078
174          Certificate Expiry Monitor: ENABLED
175          Expiry Notification period: 30 days
176          Certificate Type: Intermediate CA
177          Version: 3
178          Serial Number: 01
179          Signature Algorithm: sha256WithRSAEncryption
180          Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA2
181          Validity
182                  Not Before: Nov 28 06:42:46 2014 GMT
183                  Not After : Nov 25 06:42:46 2024 GMT
184          Subject:  C=IN,ST=ka,O=sslteam,CN=ICA3
185          Public Key Algorithm: rsaEncryption
186          Public Key size: 2048
187
188  11)     Name: bundletest_ic8
189          Cert Path: bundle9.pem_ic8
190          Format: PEM
191          Status: Valid,   Days to expiration:3078
192          Certificate Expiry Monitor: ENABLED
193          Expiry Notification period: 30 days
```



```
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA1
        Validity
                Not Before: Nov 28 06:42:45 2014 GMT
                Not After : Nov 25 06:42:45 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA2
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

12)     Name: bundletest_ic9
        Cert Path: bundle9.pem_ic9
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=RootCA4096
        Validity
                Not Before: Nov 28 06:42:43 2014 GMT
                Not After : Nov 25 06:42:43 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA1
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048
Done

sh ssl certlink

1)      Cert Name: bundletest    CA Cert Name: bundletest_ic1
2)      Cert Name: bundletest_ic1        CA Cert Name: bundletest_ic2
3)      Cert Name: bundletest_ic2        CA Cert Name: bundletest_ic3
4)      Cert Name: bundletest_ic3        CA Cert Name: bundletest_ic4
5)      Cert Name: bundletest_ic4        CA Cert Name: bundletest_ic5
6)      Cert Name: bundletest_ic5        CA Cert Name: bundletest_ic6
7)      Cert Name: bundletest_ic6        CA Cert Name: bundletest_ic7
8)      Cert Name: bundletest_ic7        CA Cert Name: bundletest_ic8
9)      Cert Name: bundletest_ic8        CA Cert Name: bundletest_ic9
Done
<!--NeedCopy-->
```

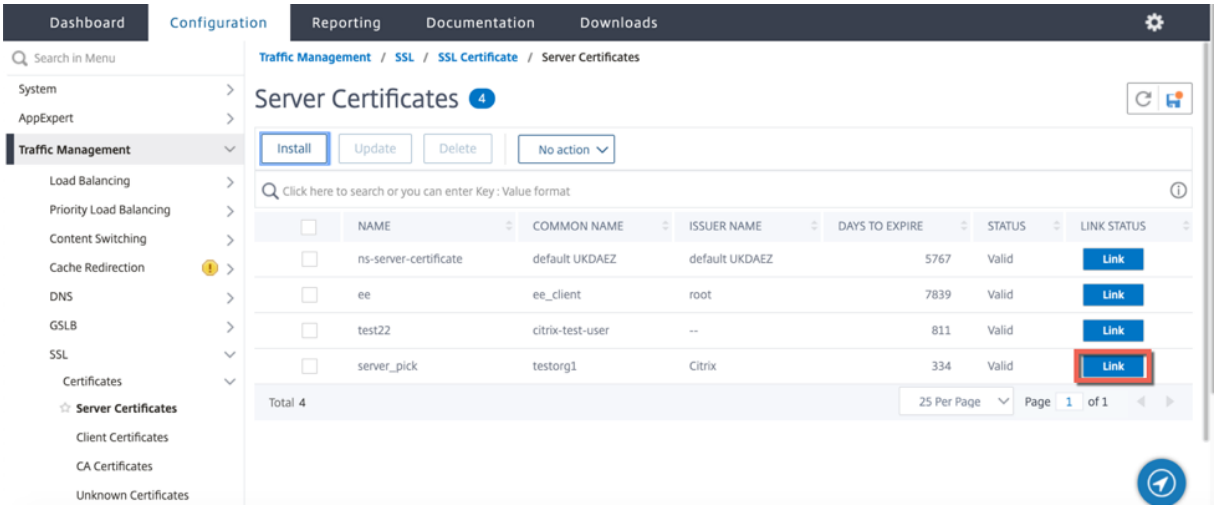

Ajouter un jeu de certificats à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Certificats** > **Certificats CA**.
2. Dans le volet d'informations, cliquez sur **Installer**.
3. Dans la boîte de dialogue **Installer le certificat**, tapez les détails, tels que le certificat et le nom du fichier de clé, puis sélectionnez **Ensemble de certificats**.
4. Cliquez sur **Installer**, puis sur **Fermer**.

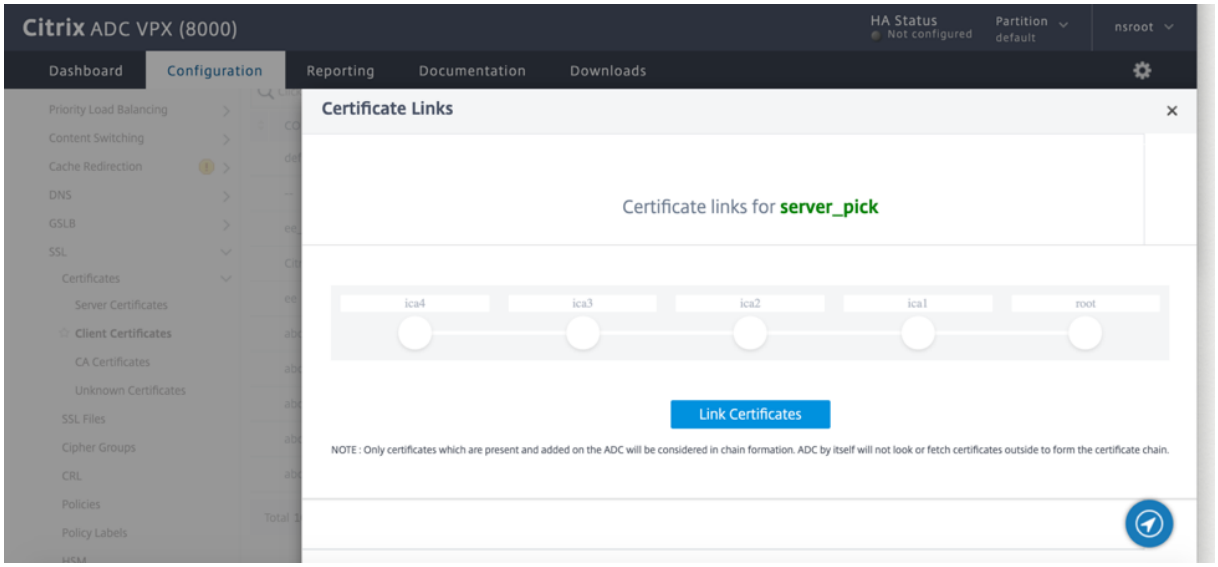
Liaison automatique des certificats

Remarque : Cette fonctionnalité est disponible à partir de la version 13.0 build 47.x.

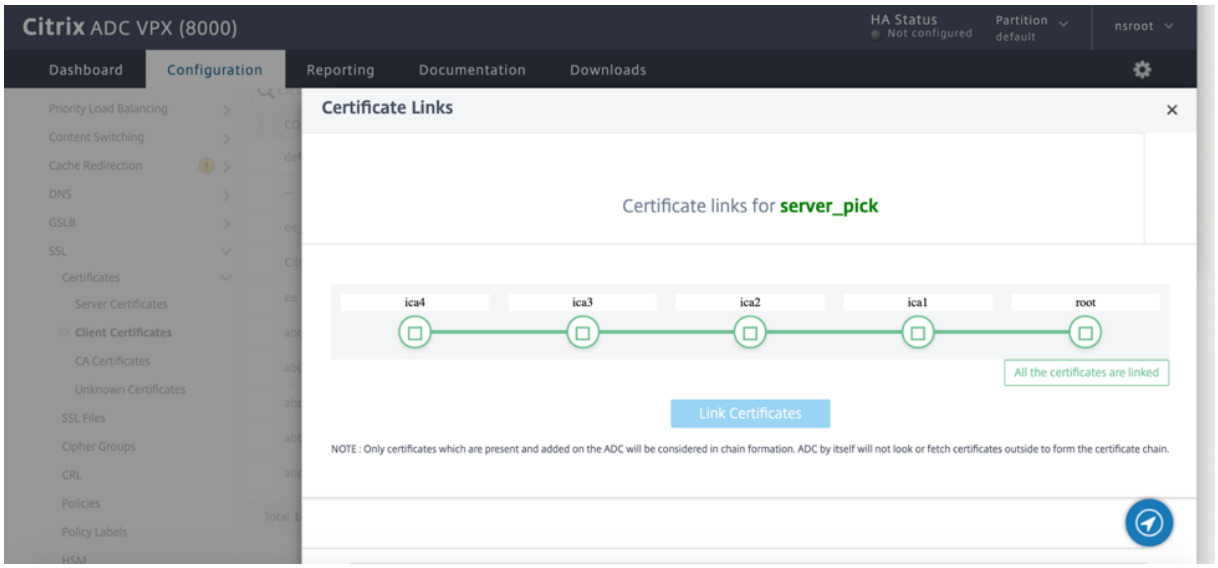
Vous n'avez plus besoin de lier manuellement un certificat à son émetteur jusqu'au certificat racine. Si les certificats d'autorité de certification intermédiaires et le certificat racine sont présents sur l'appliance, vous pouvez cliquer sur le bouton **Lier** dans le certificat d'utilisateur final.



La chaîne de potentiel apparaît.



Cliquez sur **Lier le certificat** pour lier tous les certificats.



Création d'une chaîne de certificats

Au lieu d'utiliser un ensemble de certificats (un seul fichier), vous pouvez créer une chaîne de certificats. La chaîne relie le certificat du serveur à son émetteur (l'autorité de certification intermédiaire). Cette approche nécessite que le fichier de certificat de l'autorité de certification intermédiaire soit installé sur l'appliance ADC et que l'application cliente doive faire confiance à l'un des certificats de la chaîne. Par exemple, liez Cert-Intermédiaire-A au Cert-Intermédiaire-B, où Cert-Intermédiaire-B est lié au Cert-Intermédiaire-C, qui est un certificat approuvé par l'application cliente.

Remarque : L'appliance prend en charge l'envoi d'un maximum de 10 certificats dans la chaîne de certificats envoyés au client (un certificat de serveur et neuf certificats d'autorité de certification).

Créer une chaîne de certificats à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour créer une chaîne de certificats et vérifier la configuration. (Répétez la première commande pour chaque nouveau maillon de la chaîne.)

```
link ssl certkey <certKeyName> <linkCertKeyName>
show ssl certlink
<!--NeedCopy-->
```

Exemple :

```
link ssl certkey siteAcertkey CAcertkey
Done

show ssl certlink

linked certificate:
       1) Cert Name: siteAcertkey CA Cert Name: CAcertkey
Done
<!--NeedCopy-->
```

Créer une chaîne de certificats à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Certificats**.
2. Sélectionnez un certificat de serveur, puis dans la liste **Action**, sélectionnez **Lier**et spécifiez un nom de certificat d'autorité de certification.

Prise en charge du bundle de certificats SSL

> **Remarque**
>
> Cette fonctionnalité est disponible à partir de la version 13.1 build 12.x.

La conception actuelle d'un bundle de certificats présente les inconvénients suivants :

- L'ajout d'un bundle de certificats ajoute plusieurs commandes dans la configuration. Par conséquent, vous ne pouvez pas ajouter un autre bundle de certificats si les deux ensembles partagent un certificat intermédiaire commun.
- La suppression d'un bundle de certificats est un processus manuel. Vous devez supprimer manuellement les fichiers dans un ordre spécifique.
- La mise à jour d'un bundle de certificats n'est pas prise
- Le cluster n'est pas supporté.

La nouvelle conception d'un bundle de certificats résout tous ces problèmes. La nouvelle entité fonctionne sur un fichier de bundle de certificats. Il n'est donc pas nécessaire de créer des fichiers pour

chaque certificat intermédiaire. La suppression est également simple avec cette nouvelle entité.

Deux ensembles de certificats peuvent partager une partie de la chaîne de certificats intermédiaires. Vous pouvez également ajouter une paire de clés de certificat à l'aide du même certificat de serveur et de la même clé qui font également partie d'un bundle de certificats.

Dans l'exemple suivant :

1. Le bundle de certificats bundle1.pem contient un certificat de serveur (S1) et des certificats intermédiaires (IC1 et IC2).
2. Le certificat du serveur est server_cert.pem (S1).
3. Les certificats intermédiaires sont ic1.pem (IC1) et ic2.pem (IC2).

Vous pouvez ajouter un bundle de certificats contenant S1, IC1 et IC2.

```
add ssl certkeybundle b1 -bundlefile bundle1.pem
```

Vous pouvez également ajouter une paire de clés de certificat à l'aide de S1 et IC1.

```
add ssl certkey server-cert -cert server_cert.pem
```

```
add ssl certkey ic1 -cert ic1.pem
```

Important !

- La création du lot échoue si l'ordre suivant n'est pas respecté :
  - Le certificat de serveur (SC) doit être placé en haut du fichier de bundle.
  - `IC[1-9]` sont des certificats intermédiaires. `IC[i]` est émis par `IC[i+1]`. Les certificats doivent être placés dans un ordre et tous les certificats intermédiaires doivent être présents dans le lot.
- Les certificats doivent être au format PEM uniquement.
- La clé de certificat du serveur (SCK) peut être placée n'importe où dans le bundle.
- Un maximum de 9 certificats intermédiaires sont pris en charge.

Pour ajouter un bundle de certificats

À l'invite de commande, tapez :

```
add ssl certKeyBundle <bundle_name> -bundlefile <bundle_file_name> -passplain
 <>
```

Exemple :

```
add ssl certkeyBundle cert_bundle -bundlefile bundle_4096.pem
```

Pour supprimer un bundle de certificats

À l'invite de commande, tapez :


```
rm ssl certKeyBundle <bundle_name>
```

Exemple :

```
rm ssl certkeybundle cert_bundle
```

Pour lier un bundle de certificats à un serveur virtuel SSL

À l'invite de commande, tapez :

```
bind ssl vserver <vip-name> -certkeybundleName <certkeybundle_name> [ -
SNICertkeybundle]
```

Exemple :

```
1  bind ssl vserver v_server -certkeyBundleName cert_bundle
2
3  show ssl certkeyBundle cert_bundle
4
5  1) Name: cert_bundle
6          Bundle path: bundle_4096.pem
7          Certificate:
8                  Status: Valid,   Days to expiration:278
9                  Serial Number: 83
10                 Subject:  C=IN,ST=KAR,O=CITRIX,CN=4096.com
11                 Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
12                 Signature Algorithm: sha256WithRSAEncryption
13                 Validity
14                         Not Before: Jul 13 10:17:57 2021 GMT
15                         Not After : Jul 13 10:17:57 2022 GMT
16                 Public Key Algorithm: rsaEncryption
17                 Public Key size: 4096
18                 SAN ENTRIES: None
19
20
21         CA Certificate:
22                 Status: Valid,   Days to expiration:278
23                 Serial Number: 82
24                 Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
25                 Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
26                 Signature Algorithm: sha256WithRSAEncryption
27                 Validity
28                         Not Before: Jul 13 10:15:37 2021 GMT
29                         Not After : Jul 13 10:15:37 2022 GMT
30                 Public Key Algorithm: rsaEncryption
31                 Public Key size: 4096
```



```
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 81
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:13:20 2021 GMT
                        Not After : Jul 13 10:13:20 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 00
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:10:23 2021 GMT
                        Not After : Jul 13 10:10:23 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 2048
                SAN ENTRIES: None

1)      Vserver Name: v_server
<!--NeedCopy-->
```

Pour lier un bundle de certificats à un serveur virtuel SSL en tant que bundle de certificats SNI

À l'invite de commande, tapez :

```
bind ssl vserver <vip-name> -certkeybundleName b2 -SNICertkeybundle
```

Exemple :

```
bind ssl vserver v_server -certkeyBundleName cert_bundle -
    sniCertkeybundle

sh ssl certkeybundle cert_bundle

1) Name: cert_bundle
```



```
        Bundle path: bundle_4096.pem
        Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 83
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=4096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:17:57 2021 GMT
                        Not After : Jul 13 10:17:57 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None


        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 82
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:15:37 2021 GMT
                        Not After : Jul 13 10:15:37 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 81
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:13:20 2021 GMT
                        Not After : Jul 13 10:13:20 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 00
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
```



```
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:10:23 2021 GMT
                        Not After : Jul 13 10:10:23 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 2048
                SAN ENTRIES: None

1)    Vserver Name: v_server
2)    Vserver Name: v_server
<!--NeedCopy-->
```

Pour dissocier un bundle de certificats d'un serveur virtuel SSL

À l'invite de commande, tapez :

```
unbind ssl vserver <vip-name> -certkeybundleName <certkeybundle_name> [ -SNICertkeybundle]
```

Exemple :

```
unbind ssl vserver v_server -certkeybundleName cert_bundle
```

Scénarios utilisateur pour la liaison de bundle de certificats

Les scénarios suivants expliquent comment l'appliance ADC traite une demande liée à des bundles de certificats.

Scénario 1 : Une paire de clés de certificat et un bundle de certificats contenant le même certificat de serveur sont liés au même serveur virtuel SSL

Lors de la liaison d'une paire de clés de certificat et d'un ensemble de certificats contenant le même certificat de serveur au même serveur virtuel SSL, l'ordre des commandes détermine la liaison finale.

Par exemple,

- Le bundle de certificats bundle1.pem contient le certificat de serveur S1 et les certificats intermédiaires IC1 et IC2.
- Le fichier de certificat server_cert.pem contient S1.

bundle1.pem et server_cert.pem ont tous deux le même certificat de serveur S1.

Si les commandes suivantes sont exécutées dans l'ordre spécifié, la liaison du certificat du serveur au serveur virtuel SSL remplace la liaison du groupe de certificats à ce serveur virtuel.

1. `add ssl certkeybundle b1 -bundlefile bundle1.pem`
2. `add ssl certkey server_cert -cert server_cert.pem`
3. `bind ssl vserver v1 -certkeybundle b1`
4. `bind ssl vserver v1 -cert server_cert`

Scénario 2 : deux bundles de certificats contiennent la même chaîne de certificats intermédiaire

Vous pouvez ajouter deux bundles de certificats avec la même chaîne de certificats intermédiaire. Les deux groupes agissent en tant qu'entités indépendantes.

Dans l'exemple suivant, le bundle de certificats 1 contient le certificat de serveur S1 et les certificats intermédiaires IC1 et IC2 dans cet ordre. Le lot de certificats 2 contient le certificat serveur S2 et les certificats intermédiaires IC1 et IC2 dans cet ordre.

- Bundle de certificats1.pem (S1, IC1, IC2)
- Bundle de certificats 2.pem (S2, IC1, IC2)

Lorsque S1 dans le bundle 1 est sélectionné dans le processus d'établissement de liaison SSL, la chaîne de certificats intermédiaire du bundle 1 est envoyée au client.

```
add ssl certkeybundle bundle-1 -bundlefile bundle1.pem
add ssl certkeybundle bundle-2 -bundlefile bundle2.pem
```

Scénario 2 : deux bundles de certificats contiennent des certificats intermédiaires courants dans la chaîne

Vous pouvez ajouter deux bundles de certificats avec certains certificats intermédiaires courants dans la chaîne.

Dans l'exemple suivant, le bundle 1 contient le certificat de serveur S1 et les certificats intermédiaires IC1 et IC2. Le bundle de certificats 2 contient le certificat de serveur S2 et les certificats intermédiaires IC1, IC2 et IC3.

Bundle de certificats1.pem (S1, IC1, IC2)
Bundle de certificats2.pem (S2, IC1, IC2, IC3)

```
add ssl certkeybundle bundle-1 -bundlefile bundle1.pem
add ssl certkeybundle bundle-2 -bundlefile bundle2.pem
```

Lorsque S1 dans le bundle 1 est sélectionné dans le processus d'établissement de liaison SSL, la chaîne de certificats intermédiaire du bundle 1 est envoyée au client. C'est-à-dire qu' `(S1→IC1→IC2)` il est envoyé au client. IC3 n'est pas ajouté.

Lorsque S2 dans le groupe-2 est sélectionné dans le processus d'établissement de liaison SSL, la chaîne de certificats intermédiaire du groupe-2 n'est envoyée qu'au client. C'est-à-dire qu' (S1→IC1 →IC2→IC3) il est envoyé au client.

Limitations du bundle de certificats

- La surveillance de l'état d'un certificat dans le bundle de certificats n'est pas prise en charge.
- La mise à jour d'un bundle de certificats n'est pas prise
- Les bundles de certificats ne peuvent être liés qu'à des serveurs virtuels SSL.
- L'agrafage OCSP n'est pas pris en charge.

Mettre à jour un certificat de serveur existant

Pour modifier manuellement un certificat de serveur existant, vous devez effectuer les étapes suivantes :

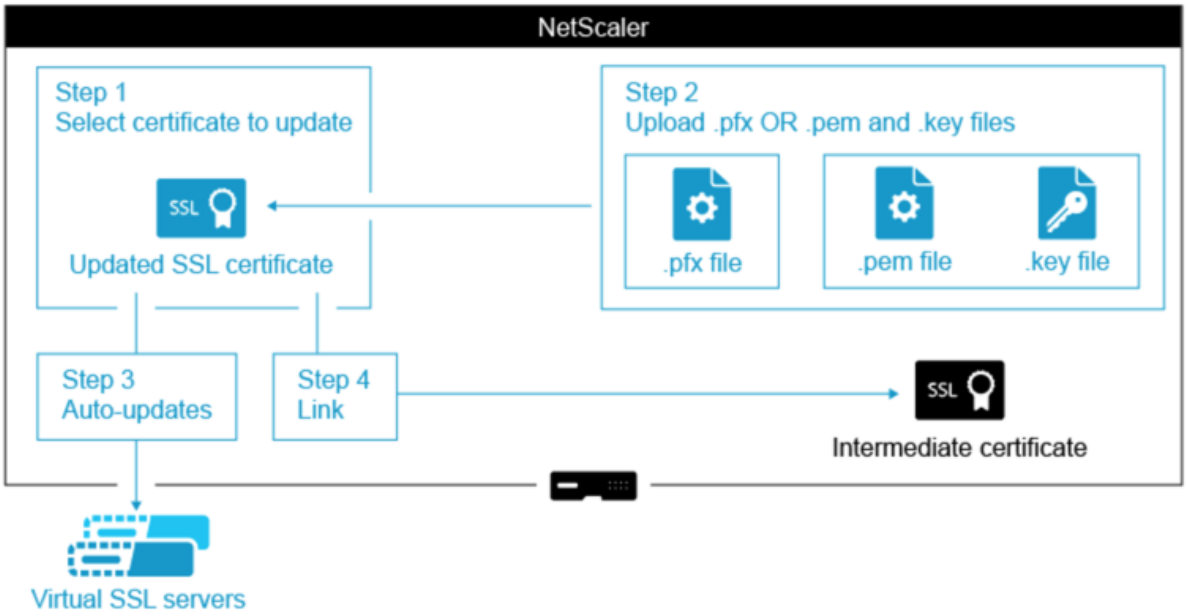
1. Dissociez l'ancien certificat du serveur virtuel.
2. Supprimez le certificat de l'appliance.
3. Ajoutez le nouveau certificat à l'appliance.
4. Liez le nouveau certificat au serveur virtuel.

Pour réduire les temps d'arrêt lors du remplacement d'une paire de clés de certificat, vous pouvez mettre à jour un certificat existant. Si vous souhaitez remplacer un certificat par un certificat qui a été émis pour un autre domaine, vous devez désactiver les vérifications de domaine avant de mettre à jour le certificat.

Pour recevoir des notifications concernant les certificats arrivant à expiration, vous pouvez activer le moniteur d'expiration.

Lorsque vous supprimez ou dissociez un certificat d'un serveur virtuel ou d'un service SSL configuré, le serveur virtuel ou le service devient inactif. Ils sont actifs après qu'un nouveau certificat valide leur est lié. Pour réduire les temps d'arrêt, vous pouvez utiliser la fonctionnalité de mise à jour pour remplacer une paire de clés de certificat liée à un serveur virtuel SSL ou à un service SSL.

Schéma général expliquant comment mettre à jour un certificat SSL sur l'appliance NetScaler.



Comment mettre à jour un certificat existant

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Mettre à jour une paire de clés de certificat existante à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour mettre à jour une paire de clés de certificat existante et vérifier la configuration :

```
update ssl certkey <certkeyName> -cert <string> -key <string>

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Exemple :

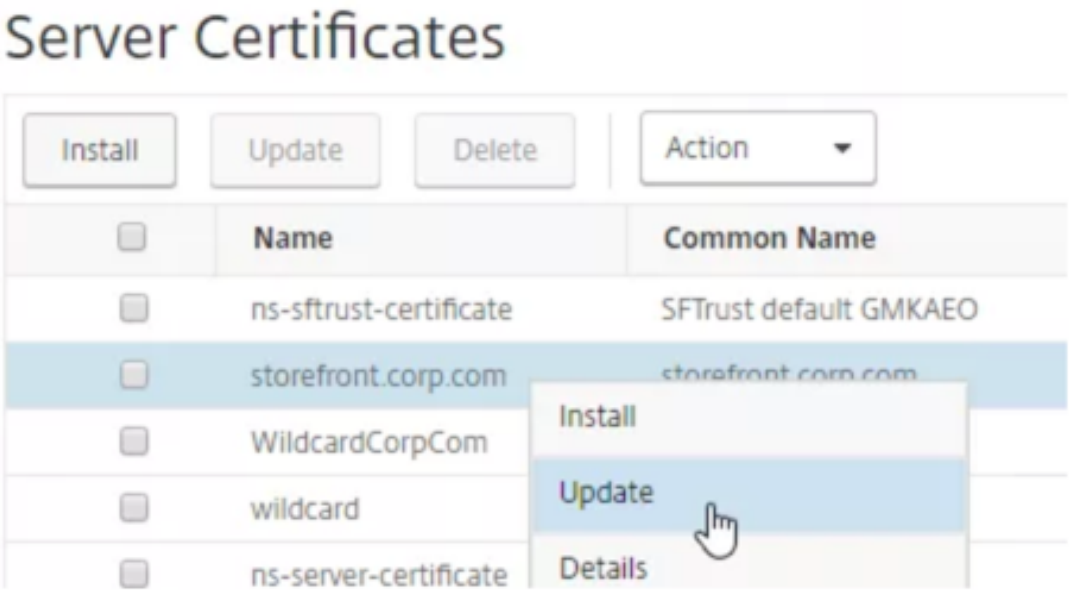
```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
   nsconfig/ssl/pkey.pem

Done

show ssl certkey siteAcertkey

Name: siteAcertkey       Status: Valid
          Version: 3
          Serial Number: 02
```



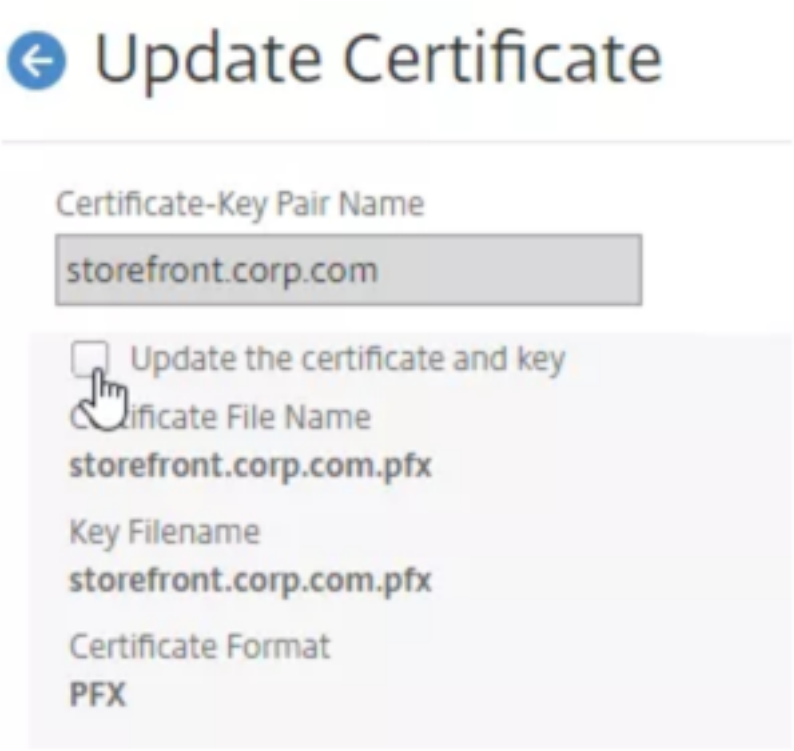
```
            Signature Algorithm: md5WithRSAEncryption
            Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech
            Validity
                 Not Before: Nov 11 14:58:18 2001 GMT
                 Not After: Aug 7 14:58:18 2004 GMT
            Subject: /C=US/ST-CA/L=San Jose/O=CA/OU=Security
            Public Key Algorithm: rsaEncryption
            Public Key size: 2048
Done
<!--NeedCopy-->
```

Mettre à jour une paire de clés de certificat existante à l'aide de l'interface graphique

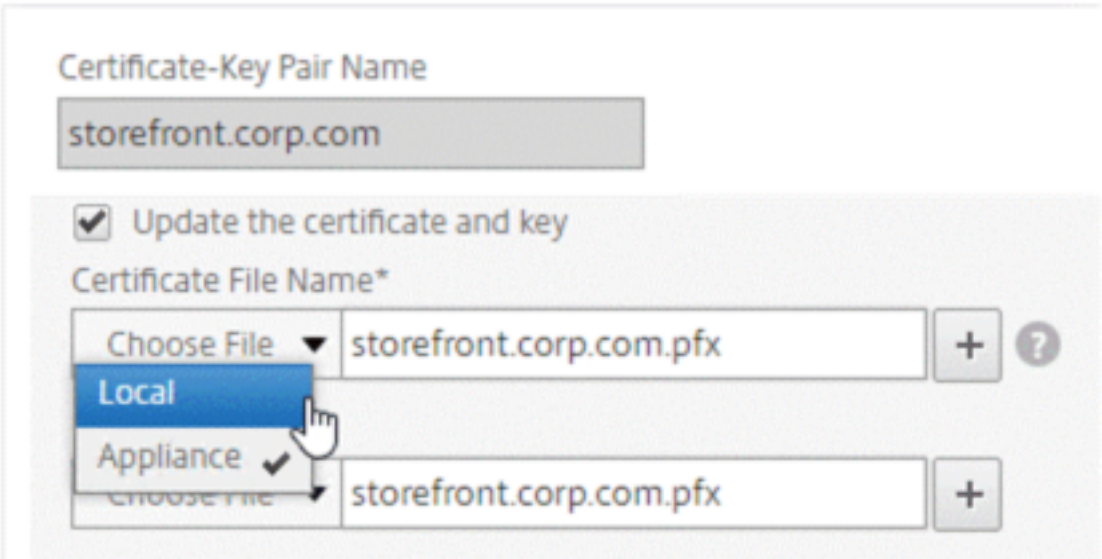
1. Accédez à **Gestion du trafic** > **SSL** > **Certificats > Certificatsde serveur**.
2. Sélectionnez le certificat que vous souhaitez mettre à jour, puis cliquez sur **Mettre à jour**.



3. Sélectionnez **Mettre à jour le certificat et la clé**.



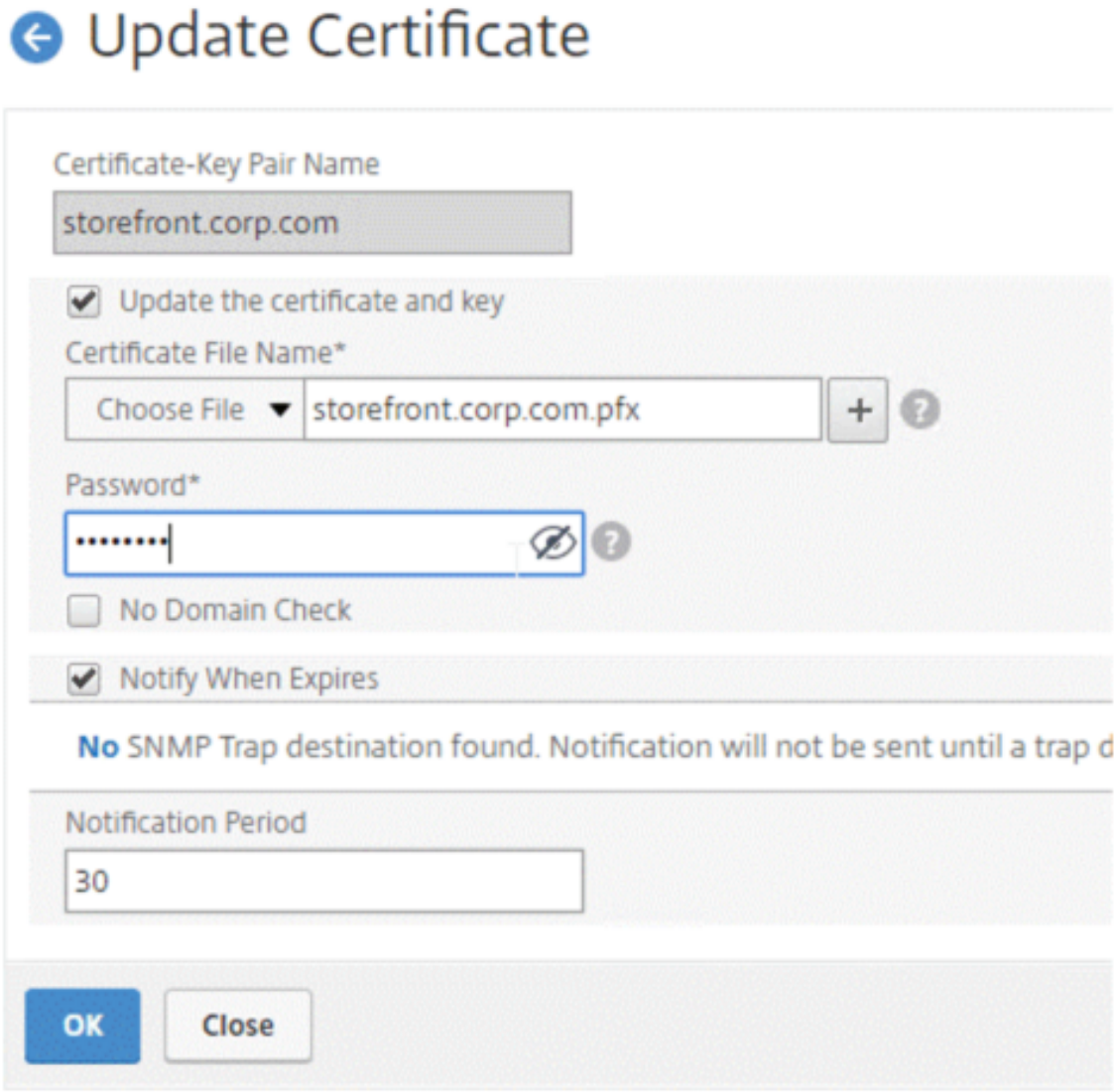
4. Dans **Nom du fichier de certificat**, cliquez sur **Choisir un fichier** > **Local**et accédez au fichier .pfx ou au fichier PEM de certificat mis à jour.



   - Si vous chargez un fichier .pfx, vous êtes invité à spécifier le mot de passe du fichier .pfx.
   - Si vous chargez un fichier PEM de certificat, vous devez également télécharger un fichier de clé de certificat. Si la clé est cryptée, vous devez spécifier le mot de passe de cryptage.
5. Si le nom commun du nouveau certificat ne correspond pas à l'ancien certificat, sélectionnez

Aucune vérification de domaine.

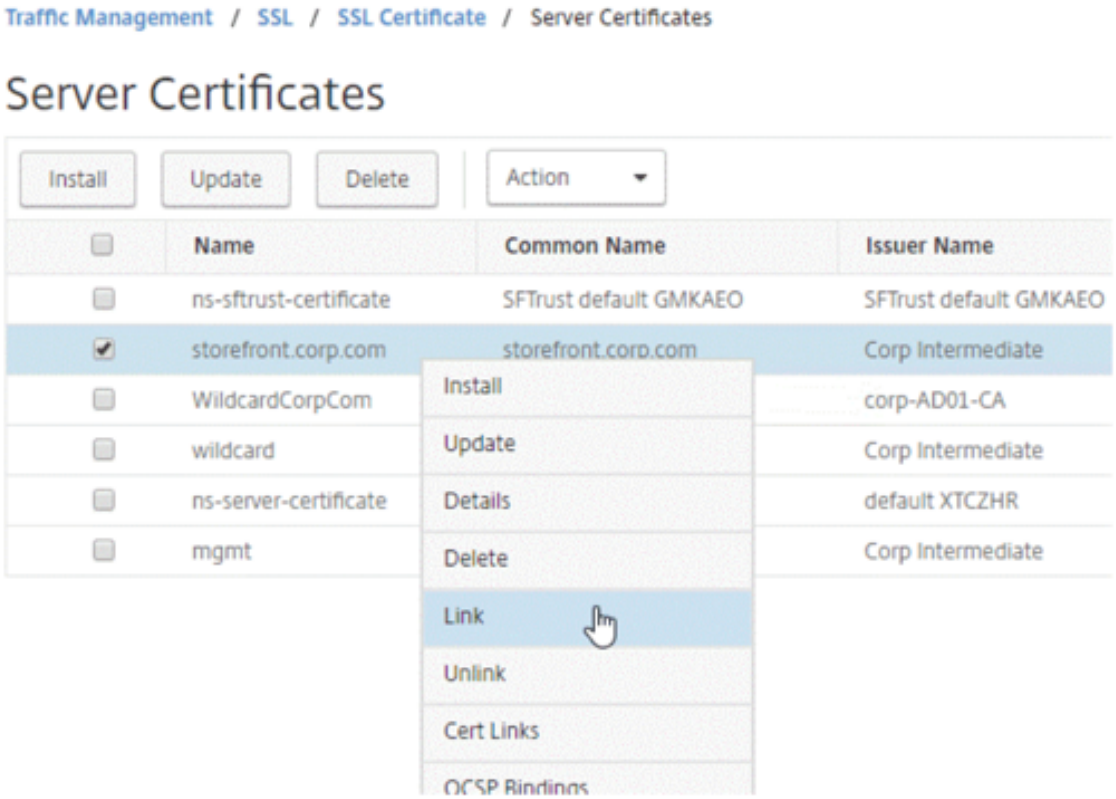
6. Cliquez sur **OK**. Tous les serveurs virtuels SSL auxquels ce certificat est lié sont automatiquement mis à jour.



7. Après avoir remplacé le certificat, vous devrez peut-être mettre à jour le lien de certificat vers un nouveau certificat intermédiaire. Pour plus d'informations sur la mise à jour d'un certificat intermédiaire sans rompre les liens, voir Mettre à jour un certificat intermédiaire sans rompre les liens.

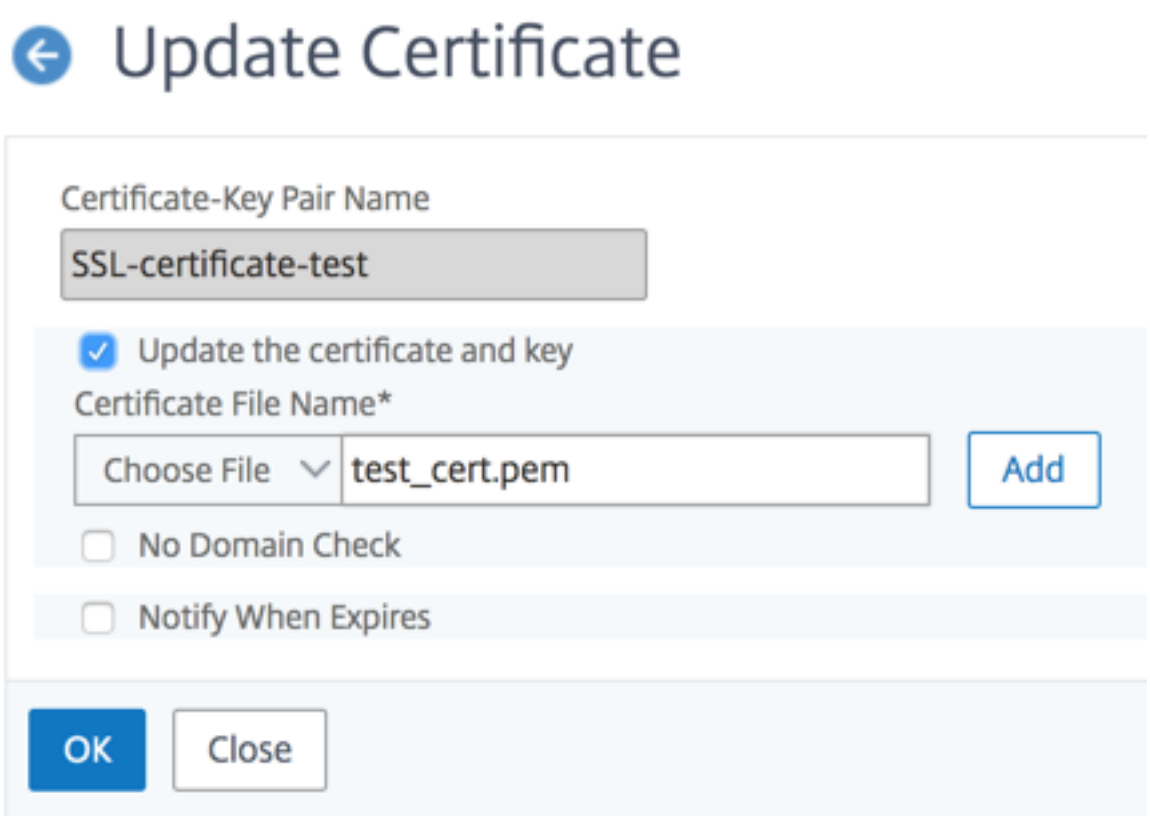
   - Cliquez avec le bouton droit sur le certificat mis à jour, puis cliquez sur **Liaisons**de certificats, pour voir s'il est lié à un certificat intermédiaire.
   - **Si le certificat n'est pas lié, cliquez avec le bouton droit sur le certificat mis à jour, puis cliquez sur Lier pour le lier à un certificat intermédiaire.** Si vous ne voyez pas d'option de liaison, vous devez d'abord installer un nouveau certificat intermédiaire sur l'appliance

sous le nœud **Certificats de l'autorité** de certification.



Mettre à jour un certificat de CA existant

Les étapes pour mettre à jour un certificat d'autorité de certification existant sont les mêmes que pour mettre à jour un certificat de serveur existant. La seule différence est que vous n'avez pas besoin de clé dans le cas des certificats d'autorité de certification.



Désactiver les vérifications de

Lorsqu'un certificat SSL est remplacé sur l'appliance, le nom de domaine mentionné sur le nouveau certificat doit correspondre au nom de domaine du certificat remplacé. Par exemple, si vous avez un certificat émis sur abc.com et que vous le mettez à jour avec un certificat émis sur def.com, la mise à jour du certificat échoue.

Toutefois, si vous souhaitez que le serveur qui héberge un domaine particulier héberge un nouveau domaine, désactivez la vérification du domaine avant de mettre à jour son certificat.

Désactiver la vérification de domaine pour un certificat à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour désactiver la vérification du domaine et vérifier la configuration :

```
update ssl certKey <certkeyName> -noDomainCheck

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Exemple :


```
update ssl certKey sv -noDomainCheck

Done

show ssl certkey sv

Name: sv
Cert Path: /nsconfig/ssl/complete/server/server_rsa_512.pem
Key Path: /nsconfig/ssl/complete/server/server_rsa_512.ky
Format: PEM
Status: Valid,   Days to expiration:9349
Certificate Expiry Monitor: DISABLED
Done
<!--NeedCopy-->
```

Désactiver la vérification de domaine pour un certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Certificats**, sélectionnez un certificat, puis cliquez sur **Mettre à jour**.
2. Sélectionnez **Aucune vérification de domaine**.

Remplacez le certificat par défaut d'un boîtier ADC par un certificat d'autorité de certification de confiance qui correspond au nom d'hôte de l'appliance

La procédure suivante suppose que le certificat par défaut (`ns-server-certificate`) est lié aux services internes.

1. Accédez à **Gestion du trafic > SSL > Certificats SSL > Créer une demande de certificat**.
2. Dans le champ Nom courant, saisissez `test.citrixadc.com`.
3. Soumettez le CSR à une autorité de certification approuvée.
4. Après avoir reçu le certificat de l'autorité de certification approuvée, copiez le fichier `/nsconfig/ssl` dans le répertoire.
5. Accédez à **Gestion du trafic > SSL > Certificats > Certificats de serveur**.
6. Sélectionnez le certificat de serveur par défaut (`ns-server-certificate`) et cliquez sur **Mettre à jour**.
7. Dans la boîte de dialogue **Mettre à jour** le **certificat, dans Nom du fichier du**certificat, accédez au certificat reçu de l'autorité de certification après la signature.
8. Dans le champ **Nom du fichier clé**, spécifiez le nom de fichier de clé privée par défaut (`ns-server.key`).
9. Sélectionnez **Aucune vérification de domaine**.
10. Cliquez sur **OK**.

Activer le moniteur d'expiration

Un certificat SSL est valide pour une période déterminée. Un déploiement typique inclut plusieurs serveurs virtuels qui traitent les transactions SSL, et les certificats qui leur sont liés peuvent expirer à des moments différents. Un moniteur d'expiration configuré sur l'appliance crée des entrées dans les journaux d'audit Syslog et ns de l'appliance lorsqu'un certificat configuré doit expirer.

Si vous souhaitez créer des alertes SNMP pour l'expiration du certificat, vous devez les configurer séparément.

Activer un moniteur d'expiration pour un certificat à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour activer un moniteur d'expiration pour un certificat et vérifier la configuration :

```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED ) [-
    notificationPeriod <positive_integer>]]

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Exemple :

```
set ssl certKey sv -expiryMonitor ENABLED  - notificationPeriod 60
Done
<!--NeedCopy-->
```

Activer un moniteur d'expiration pour un certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Certificats**, sélectionnez un certificat, puis cliquez sur **Mettre à jour**.
2. Sélectionnez **Notifier à l'expiration**et spécifiez éventuellement une période de notification.

Mettre à jour un certificat intermédiaire sans rompre les liens

Vous pouvez désormais mettre à jour un certificat intermédiaire sans rompre les liens existants. L'extension 'AuthorityKeyIdentifier', dans le certificat lié émis par le certificat à remplacer, ne doit pas contenir de champ de numéro de série du certificat d'autorité (« AuthorityCertSerialNumber »). Si l'extension 'AuthorityKeyIdentifier' contient un champ de numéro de série, les numéros de série du certificat de l'ancien et du nouveau certificat doivent être identiques. Vous pouvez mettre à jour n'importe quel nombre de certificats dans le lien, un par un, si la condition précédente est remplie. Auparavant, les liens étaient rompus si un certificat intermédiaire était mis à jour.

Par exemple, il existe quatre certificats : CertACertB, CertC, et CertD. Le certificat CertA est l'émetteur pour CertB, CertB est l'émetteur pour CertC, etc. Si vous souhaitez remplacer un certificat intermédiaire CertB par CertB_new, sans rompre le lien, la condition suivante doit être remplie :

Le numéro de série du certificat de CertB doit correspondre au numéro de série du certificat CertB_new si les deux conditions suivantes sont remplies :

- L'extension AuthorityKeyIdentifier est présente dans CertC.
- Cette extension contient un champ de numéro de série.

Si le nom commun d'un certificat change, spécifiez lors de la mise à jour du certificat nodomaincheck.

Dans l'exemple précédent, pour remplacer « www.example.com » dans CertD par « *.example.com », sélectionnez le paramètre « Aucune vérification de domaine ».

Mettez à jour le certificat à l'aide du CLI

À l'invite de commande, tapez :

```
update ssl certKey <certkeyName> -cert <string> [-password] -key <
   string>  [-noDomainCheck]
<!--NeedCopy-->
```

Exemple :

```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
   nsconfig/ssl/pkey.pem -noDomainCheck
<!--NeedCopy-->
```

Afficher une chaîne de certificats

Un certificat contient le nom de l'autorité émettrice et le sujet à qui le certificat est délivré. Pour valider un certificat, vous devez consulter l'émetteur de ce certificat et confirmer si vous lui faites confiance. Si vous ne faites pas confiance à l'émetteur, vous devez savoir qui a émis le certificat d'émetteur. Remontez la chaîne jusqu'à ce que vous atteigniez le certificat d'autorité de certification racine ou un émetteur en qui vous avez confiance.

Dans le cadre de l'établissement de liaison SSL, lorsqu'un client demande un certificat, l'appliance présente un certificat et la chaîne de certificats d'émetteur présents sur l'appliance. Un administrateur peut afficher la chaîne de certificats des certificats présents sur l'appliance et installer les certificats manquants.

Afficher la chaîne de certificats pour les certificats présents sur l'appliance à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
show ssl certchain <cert_name>
<!--NeedCopy-->
```

Exemples

Il existe 3 certificats : c1, c2 et c3. Le certificat c3 est le certificat d'autorité de certification racine et signe c2, et c2 signe c1. Les exemples suivants illustrent la sortie de la commande `show ssl certchain c1` dans différents scénarios.

Scénario 1 :

Le certificat c2 est lié à c1, et c3 est lié à c2.

Le certificat c3 est un certificat d'autorité de certification racine.

Si vous exécutez la commande suivante, les liens du certificat vers le certificat d'autorité de certification racine s'affichent.

```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate name: c2              linked; not a root
       certificate
    2) Certificate name: c3              linked; root certificate
Done
<!--NeedCopy-->
```

Scénario 2 :

Le certificat c2 est lié à c1.

Le certificat c2 n'est pas un certificat d'autorité de certification racine.

Si vous exécutez la commande suivante, les informations selon lesquelles le certificat c3 est un certificat d'autorité de certification racine mais n'est pas lié à c2 s'affichent.

```
show ssl certchain c1

Certificate chain  details of certificate name c1 are:
    1) Certificate Name: c2              linked; not a root
       certificate
    2) Certificate Name: c3              not linked; root certificate
```



```
6      Done
7  <!--NeedCopy-->
```

Scénario 3 :

Les certificats c1, c2 et c3 ne sont pas liés mais sont présents sur l'appliance.

Si vous exécutez la commande suivante, les informations relatives à tous les certificats commençant par l'émetteur du certificat c1 s'affichent. Il est également précisé que les certificats ne sont pas liés.

```
1  show ssl certchain c1
2
3  Certificate chain details of certificate name c1 are:
4      1) Certificate Name: c2                not linked; not a root
          certificate
5      2) Certificate Name: c3                not linked; root certificate
6      Done
7  <!--NeedCopy-->
```

Scénario 4 :

Le certificat c2 est lié à c1.

Le certificat c3 n'est pas présent sur l'appliance.

Si vous exécutez la commande suivante, les informations relatives au certificat lié à c1 s'affichent. Vous êtes invité à ajouter un certificat dont le nom d'objet est spécifié dans c2. Dans ce cas, l'utilisateur est invité à ajouter le certificat d'autorité de certification racine c3.

```
1  show ssl certchain c1
2
3  Certificate chain details of certificate name c1 are:
4      1) Certificate Name: c2                linked; not a root
          certificate
5      2) Certificate Name: /C=IN/ST=ka/O=netscaler/CN=test
6         Action: Add a certificate with this subject name.
7  Done
8  <!--NeedCopy-->
```

Scénario 5 :

Un certificat n'est pas lié au certificat c1 et le certificat émetteur de c1 n'est pas présent sur l'appliance.

Si vous exécutez la commande suivante, vous êtes invité à ajouter un certificat portant le nom du sujet dans le certificat c1.

```
1  sh ssl certchain c1
2
```



```
Certificate chain details of certificate name c1 are:
    1) Certificate Name: /ST=KA/C=IN
       Action: Add a certificate with this subject name.
<!--NeedCopy-->
```

Générer un certificat de test de serveur

May 5, 2023

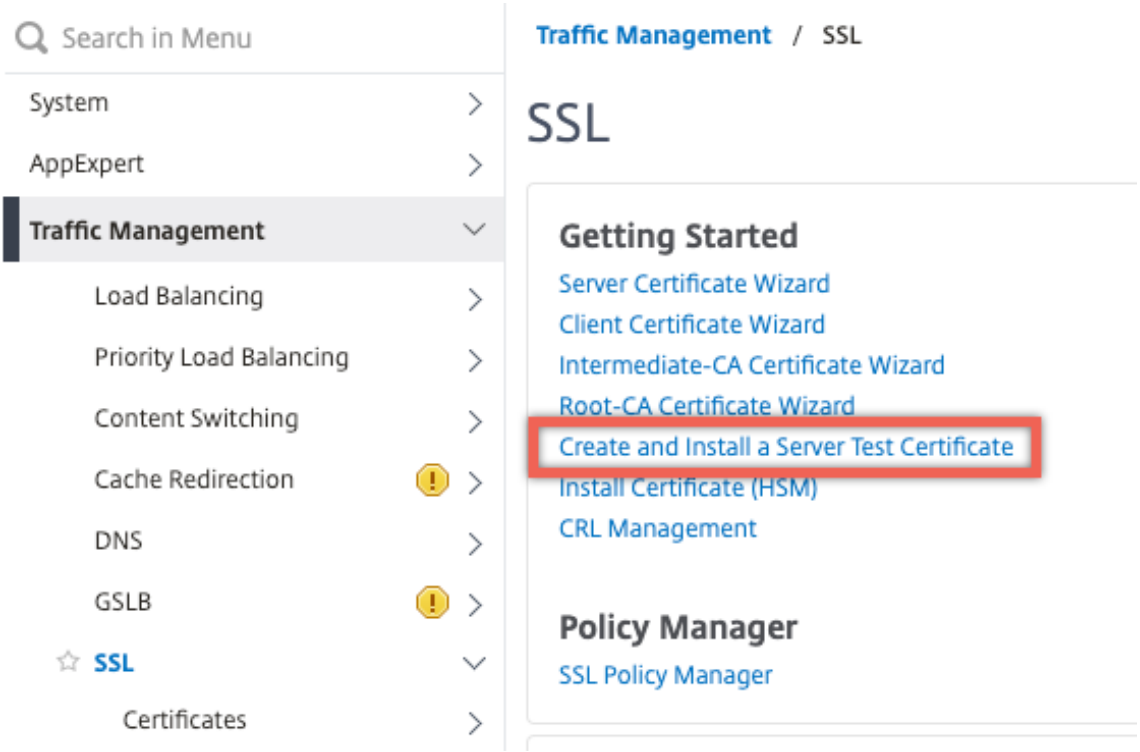
L'appliance NetScaler vous permet de créer un certificat de test pour l'authentification du serveur à l'aide d'un assistant graphique intégré à l'utilitaire de configuration. Un certificat de serveur est utilisé pour authentifier et identifier un serveur lors d'une connexion SSL. Généralement, une autorité de certification approuvée émet un certificat de serveur. Le serveur envoie le certificat à un client qui l'utilise pour authentifier le serveur.

Pour émettre un certificat de test de serveur, l'appliance fait office d'autorité de certification. Ce certificat peut être lié à un serveur virtuel SSL pour l'authentification lors d'une liaison SSL avec un client. Ce certificat est uniquement destiné à des fins de test. Ne pas utiliser dans un environnement de production.

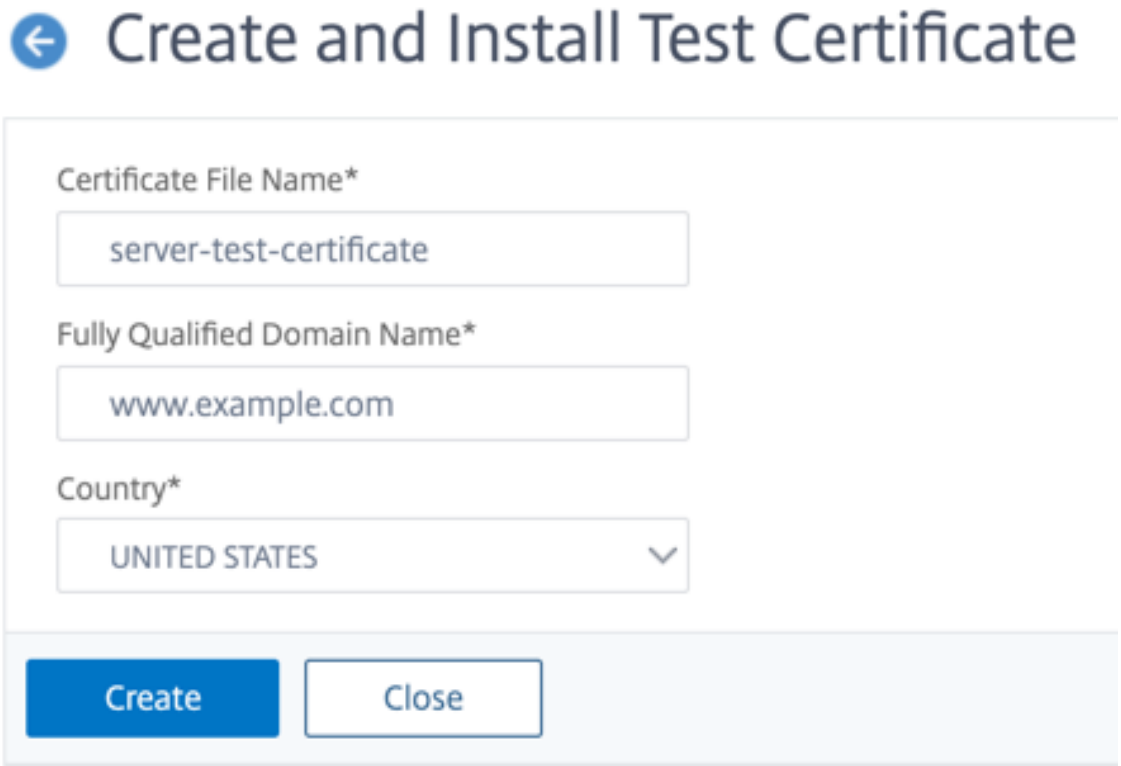
Vous pouvez installer le certificat de test du serveur sur n'importe quel serveur virtuel utilisant le protocole SSL ou SSL_TCP.

Générez un certificat de test de serveur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL** et, dans le **groupe Certificats SSL**, sélectionnez **Créer et installer un certificat de test de serveur**.



2. Entrez les détails des paramètres et cliquez sur **Créer**.



Importation et conversion de fichiers SSL

May 8, 2023

Vous pouvez désormais importer des ressources SSL, telles que des certificats, des clés privées, des CRL et des clés DH, à partir d'hôtes distants même si l'accès FTP à ces hôtes n'est pas disponible. Cette fonctionnalité est particulièrement utile dans les environnements où l'accès du shell à l'hôte distant est restreint. Les dossiers par défaut sont créés dans /nsconfig/ssl comme suit :

- Pour les fichiers de certificat : /nsconfig/ssl/certfile
- Pour les clés privées : le fichier /nsconfig/ssl/keyfile
- Pour les CRL : /var/netscaler/ssl/crlfile
- Pour les clés DH : /nsconfig/ssl/dhfile

Les importations depuis les serveurs HTTP et HTTPS sont prises en charge. Toutefois, l'importation échoue si le fichier se trouve sur un serveur HTTPS nécessitant une authentification par certificat client pour y accéder.

> **Remarque :**
>
> La commande d'importation n'est pas enregistrée dans le fichier de configuration (ns.conf), car la réimportation du fichier après un redémarrage peut provoquer une erreur.

Importer un fichier de certificat

Vous pouvez utiliser l'interface de ligne de commande et l'interface graphique pour importer un fichier (ressource) à partir d'un hôte distant.

Importer un fichier de certificat depuis un hôte distant à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
import ssl certFile [<name>] [<src>]
<!--NeedCopy-->
```

Exemple :

```
import ssl certfile my-certfile http://www.example.com/file_1
<!--NeedCopy-->
```

```
show ssl certfile
     Name : my-certfile
     URL : http://www.example.com/file_1
```



```
<!--NeedCopy-->
```

Pour supprimer un fichier de certificat, utilisez la `rm ssl certFile` commande qui accepte uniquement l'argument « nom ».

Importer un fichier clé depuis un hôte distant à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
import ssl keyFile [<name>] [<src>]
<!--NeedCopy-->
```

Exemple :

```
import ssl keyfile my-keyfile http://www.example.com/key_file
<!--NeedCopy-->
```

```
show ssl keyfile
     Name : my-keyfile
     URL : http://www.example.com/key_file
<!--NeedCopy-->
```

Pour supprimer un fichier clé, utilisez la `rm ssl keyFile` commande qui accepte uniquement l'argument « nom ».

Importer un fichier CRL depuis un hôte distant à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
import ssl crlFile [<name>] [<src>]
<!--NeedCopy-->
```

Pour supprimer un fichier CRL, utilisez la `rm ssl crlFile` commande qui accepte uniquement l' <name> argument \.

Exemple :

```
import ssl crlfile my-crlfile http://www.example.com/crl_file

show ssl crlfile

    Name : my-crlfile
    URL : http://www.example.com/crl_file
<!--NeedCopy-->
```


Importer un fichier DH depuis un hôte distant à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
import ssl dhFile [<name>] [<src>]
<!--NeedCopy-->
```

Exemple :

```
import ssl dhfile my-dhfile http://www.example.com/dh_file
show ssl dhfile
     Name : my-dhfile
     URL : http://www.example.com/dh_file
<!--NeedCopy-->
```

Pour supprimer un fichier DH, utilisez la `rm ssl dhFile` commande qui accepte uniquement l' <name> argument \.

Importer une ressource SSL à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Importations**, puis sélectionnez l'onglet approprié.

Importer des certificats PKCS #8 et PKCS #12

Si vous souhaitez utiliser des certificats et des clés que vous possédez déjà sur d'autres serveurs ou applications sécurisés de votre réseau, vous pouvez les exporter, puis les importer vers l'appliance NetScaler. Vous devrez peut-être convertir les certificats et les clés exportés avant de pouvoir les importer dans l'appliance NetScaler.

Pour savoir comment exporter des certificats à partir de serveurs ou d'applications sécurisés de votre réseau, consultez la documentation du serveur ou de l'application à partir duquel vous souhaitez exporter.

> **Remarque :**
>
> Pour l'installation sur l'appliance NetScaler, les noms de clé et de certificat ne peuvent pas contenir d'espaces ni de caractères spéciaux autres que ceux pris en charge par le système de fichiers UNIX. Respectez la convention de dénomination appropriée lorsque vous enregistrez la clé et le certificat exportés.

Une paire de certificats et de clés privées est généralement envoyée au format PKCS #12. L'appliance prend en charge les formats PEM et DER pour les certificats et les clés. Pour convertir PKCS #12 en PEM ou DER, ou PEM ou DER en PKCS #12, consultez la section « Convertir les certificats SSL pour l'importation ou l'exportation » plus loin sur cette page.

L'appliance NetScaler ne prend pas en charge les clés PEM au format PKCS #8. Vous pouvez toutefois convertir ces clés dans un format compatible à l'aide de l'interface OpenSSL, à laquelle vous pouvez accéder depuis la CLI ou l'utilitaire de configuration. Avant de convertir la clé, vous devez vérifier que la clé privée est au format PKCS #8. Les clés au format PKCS #8 commencent généralement par le texte suivant :

```
-----BEGIN ENCRYPTED PRIVATE KEY-----



leuSSZQZKgrgUQ==



-----END ENCRYPTED PRIVATE KEY-----
<!--NeedCopy-->
```

Ouvrez l'interface OpenSSL depuis la CLI

1. Ouvrez une connexion SSH à l'appliance à l'aide d'un client SSH, tel que PuTTY.
2. Connectez-vous à l'appliance à l'aide des informations d'identification de l'administrateur.
3. À l'invite de commandes, tapez shell.
4. À l'invite du shell, tapez `openssl`.

Ouvrez l'interface OpenSSL à partir de l'interface graphique

Accédez à **Gestion du trafic > SSL** et, dans le groupe Outils, sélectionnez l'interface **OpenSSL**.

Convertir un format de clé PKCS #8 non pris en charge en un format de clé pris en charge chiffré à l'aide de l'interface OpenSSL

À l'invite OpenSSL, tapez l'une des commandes suivantes, selon que le format de clé non pris en charge est de type RSA ou ECDSA :

```
OpenSSL>rsa- in <PKCS#8 Key Filename> -des3 -out <encrypted Key
   Filename>

OpenSSL>ec -in <PKCS#8 Key Filename> -des3 -out <encrypted Key Filename
   >
<!--NeedCopy-->
```


Paramètres pour convertir un format de clé non pris en charge en format de clé pris en charge

- **Nom de fichier de la clé PKCS #8 :** nom du fichier d'entrée de la clé privée PKCS #8 incompatible.
- **Nom de fichier de la clé cryptée :** nom du fichier de sortie de la clé privée cryptée compatible au format PEM.
- **Nom de fichier de clé non chiffrée :** nom du fichier de sortie de la clé privée non cryptée compatible au format PEM.

Convertir des certificats SSL pour l'importation ou l'exportation

Une appliance NetScaler prend en charge les formats PEM et DER pour les certificats SSL. D'autres applications, telles que les navigateurs clients et certains serveurs sécurisés externes, nécessitent différents formats de norme de cryptographie à clé publique (PKCS). L'appliance peut convertir le format PKCS #12 en format PEM ou DER pour importer un certificat dans l'appliance, et peut convertir le format PEM ou DER en PKCS #12 pour exporter un certificat. Pour plus de sécurité, la conversion d'un fichier à importer peut inclure le chiffrement de la clé privée à l'aide de l'algorithme DES ou DES3.

> **Remarque :**
>
> Si vous utilisez l'interface graphique pour importer un certificat PKCS #12 et que le mot de passe contient un signe dollar ($), un guillemet (') ou un caractère d'échappement (), l'importation risque d'échouer. Si tel est le cas, le message ERREUR : mot de passe non valide s'affiche. Si vous devez utiliser un caractère spécial dans le mot de passe, veillez à le préfixer avec un caractère d'échappement (), sauf si toutes les importations sont effectuées à l'aide de l'interface de ligne de commande.

Convertir le format d'un certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
convert ssl pkcs12 <outfile> [-import [-pkcs12File <inputFilename>] [-
    des | -des3] [-export [-certFile <inputFilename>] [-keyFile <
    inputFilename>]]
<!--NeedCopy-->
```

Au cours de l'opération, vous êtes invité à saisir un mot de passe d'importation ou un mot de passe d'exportation. Pour un fichier crypté, vous êtes également invité à saisir une phrase secrète.

Exemple :

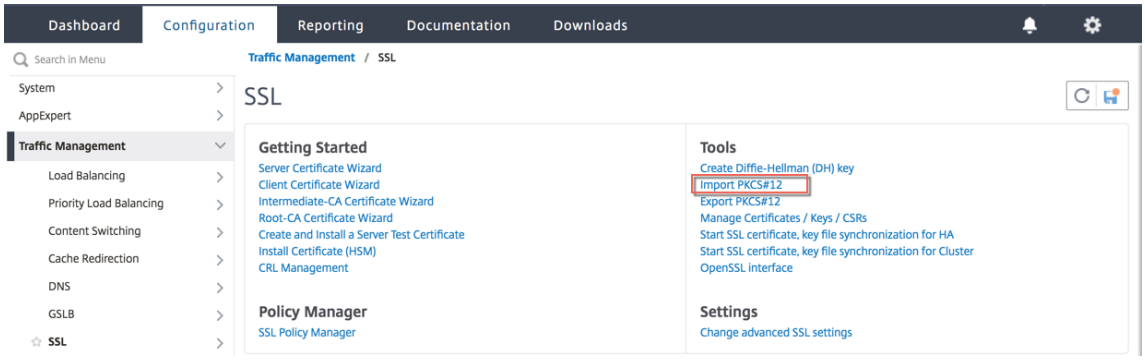
```
convert ssl pkcs12 Cert-Import-1.pem -import -pkcs12File Cert-Import-1.
    pfx -des

```



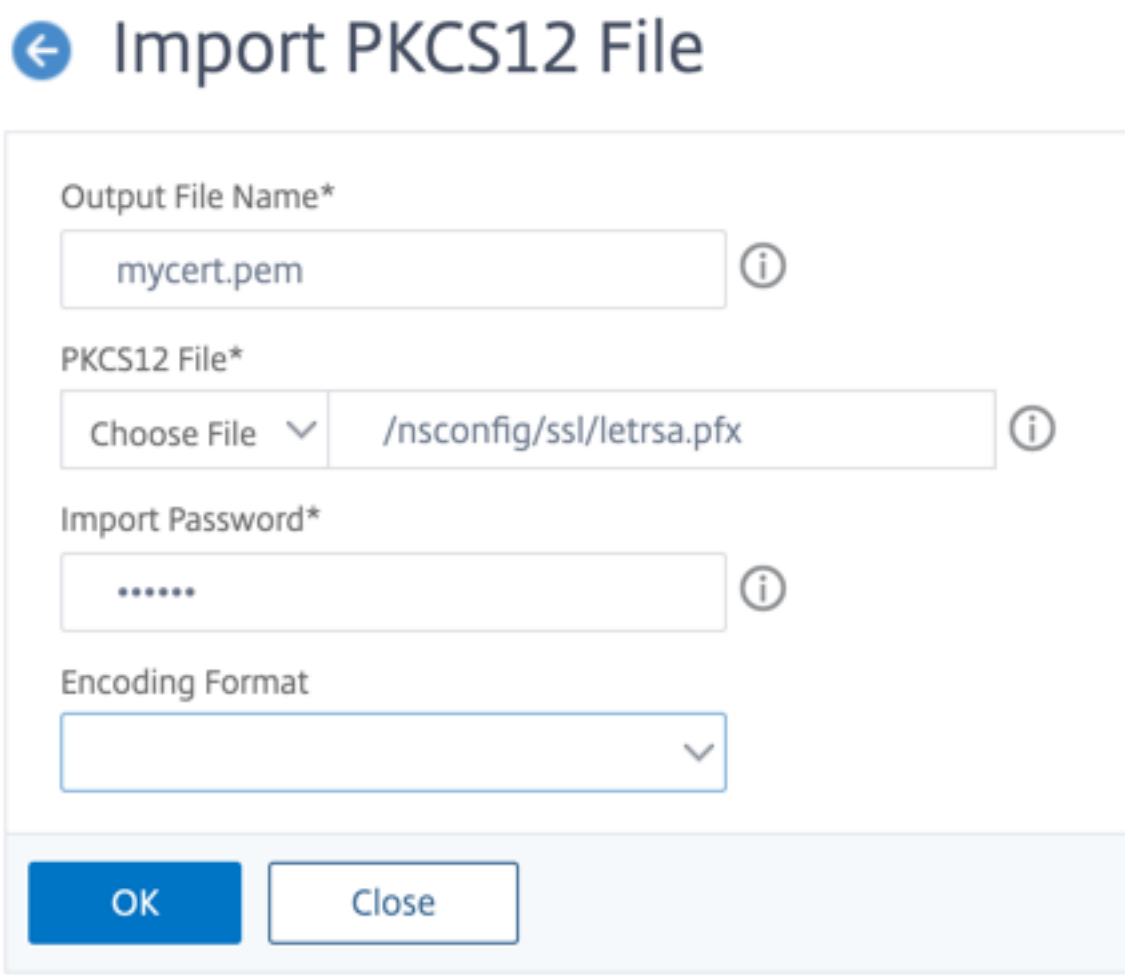
```
convert ssl pkcs12 Cert-Client-1.pfx -export -certFile Cert-Client-1 -
    keyFile Key-Client-1
<!--NeedCopy-->
```

Convertir le format d'un certificat à l'aide de l'interface graphique

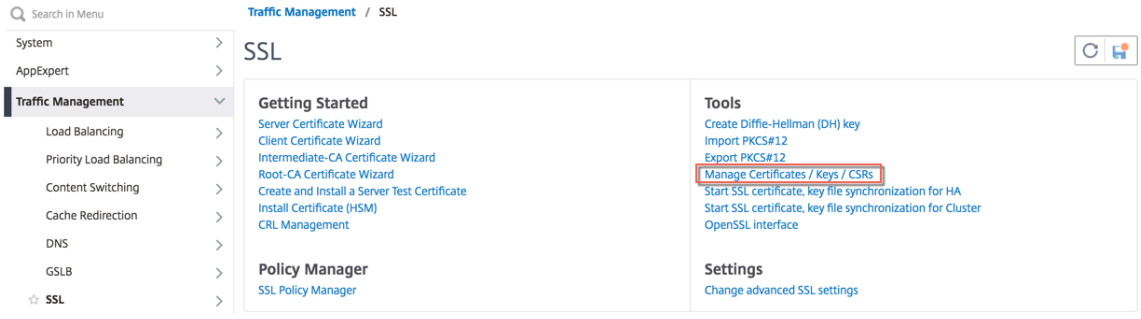
1. Accédez à **Gestion du trafic > SSL** et, dans le groupe **Outils**, sélectionnez **Importer PKCS #12**.



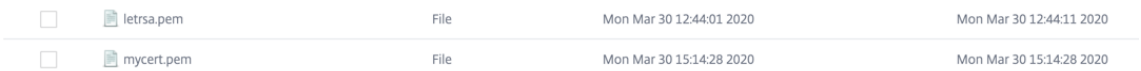
2. Spécifiez le nom du certificat PEM dans le champ **Nom du fichier de sortie** .
3. Accédez à l'emplacement du certificat PFX sur votre ordinateur local ou sur l'appliance.



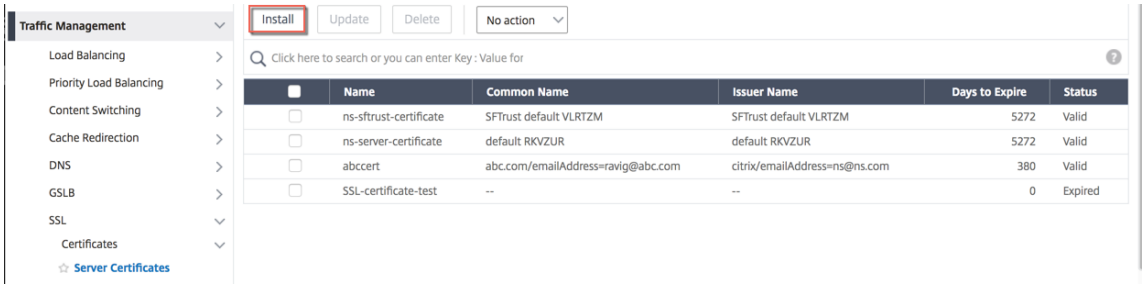
4. Cliquez sur **OK**.
5. Cliquez sur **Gérer les certificats, les clés et les CSR** pour afficher le fichier PEM converti.



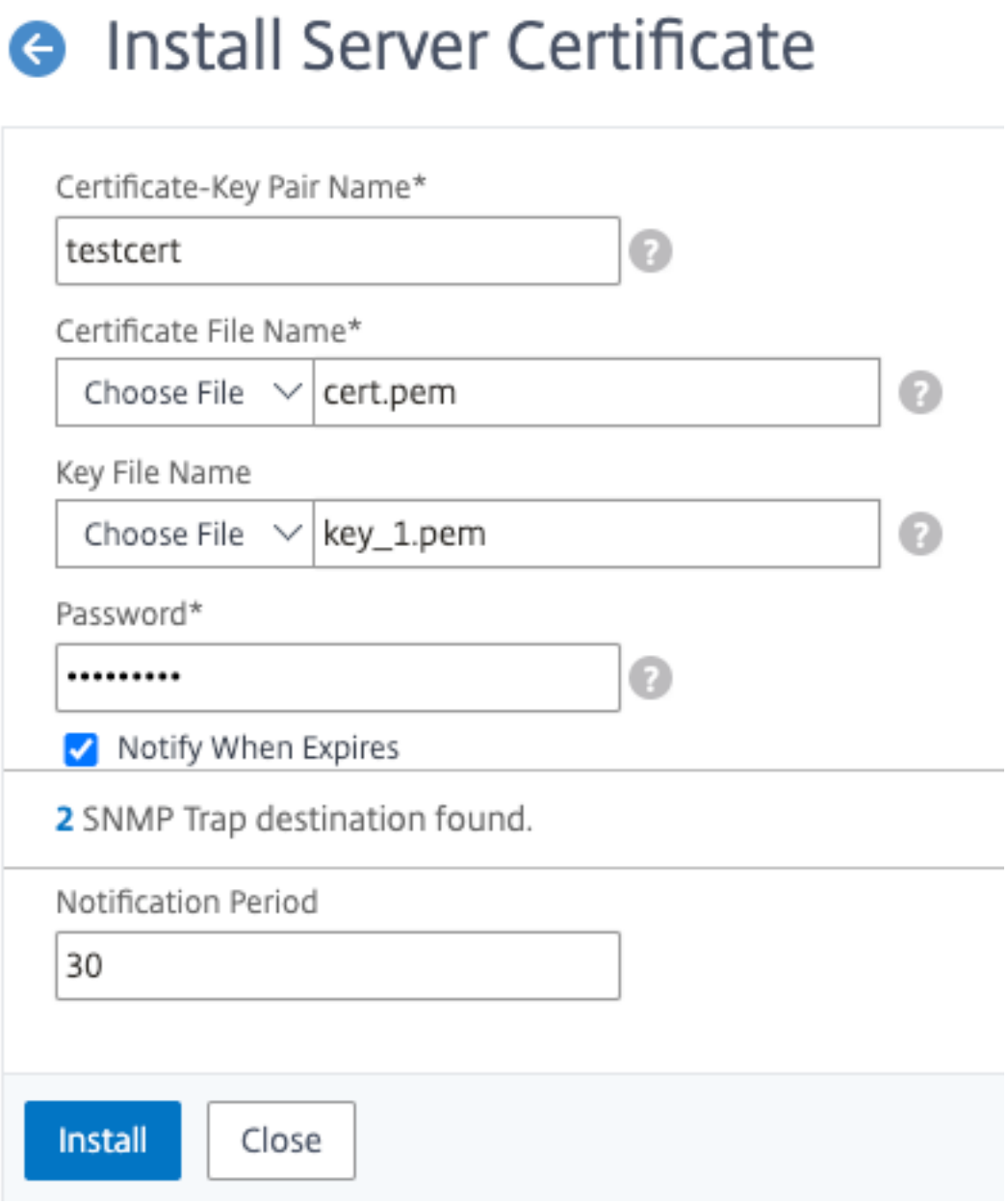
6. Vous pouvez afficher le fichier PFX chargé et le fichier PEM converti.



7. Accédez à **SSL** > **Certificats > Certificatsde serveur**et cliquez sur**Installer**.



8. Spécifiez un nom de **paire de clés de certificat**.
9. Accédez à l'emplacement du fichier PEM.
10. Spécifiez le mot de passe lorsque vous y êtes invité.
11. Cliquez sur **Installer**.



12. Liez la paire de clés de certificat à un serveur virtuel SSL.

Liez un certificat SSL à un serveur virtuel sur l'appliance NetScaler

June 2, 2023

Un certificat SSL est un élément essentiel des processus de cryptage et de déchiffrement SSL. Le certificat est utilisé lors d'une connexion SSL pour établir l'identité du serveur SSL, qui est l'appliance NetScaler car elle fait office de point de terminaison SSL pour les clients.

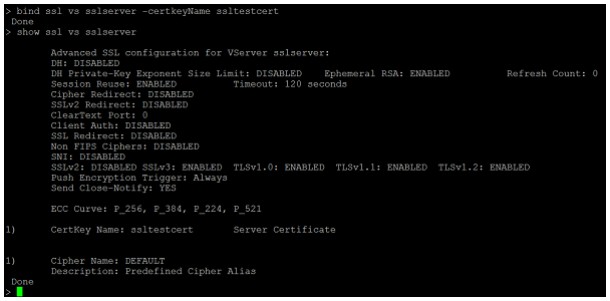
Le certificat utilisé pour traiter les transactions SSL doit être lié au serveur virtuel (SSL) qui reçoit les données SSL.

Pour lier un certificat SSL à un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

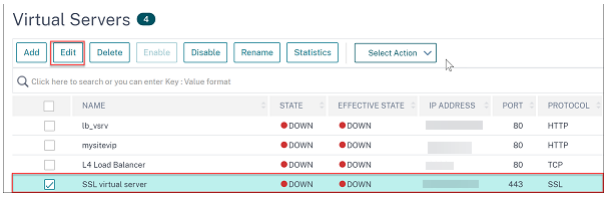
```
bind ssl vs <vServerName> -certkeyName <certificate-KeyPairName>
show ssl vs <vServerName>
<!--NeedCopy-->
```

Exemple :



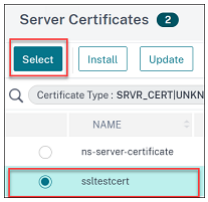
Pour lier un certificat SSL à un serveur virtuel SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel de type SSL, puis cliquez sur **Modifier**.



3. Dans la page **Serveur virtuel d'équilibrage de charge**, sous la section **Certificats**, cliquez sur **Aucun certificat de serveur**.

4. Dans la page **Liaison de certificat du serveur**, cliquez **sur Cliquez pour sélectionner**.
5. Sélectionnez le certificat SSL, puis cliquez sur **Sélectionner**.



6. Cliquez sur **Liaison pour lier** le certificat SSL au serveur virtuel.
7. Cliquez sur **Terminé**.

   Vous avez terminé de lier le certificat SSL au serveur virtuel.

> **Remarque**
>
> Lorsque vous essayez de lier une paire de clés de certificat à un serveur virtuel auquel une paire de clés de certificat est déjà liée, NetScaler dissocie l'ancienne clé de certificat et lie la nouvelle. Le message suivant s'affiche :
>
> ```
> Warning: Current certificate replaces the previous binding
> ```
>
> Les connexions existantes pour lesquelles l'établissement de connexion est terminé ne sont pas affectées. Les autres connexions sont interrompues.

Profils SSL

May 5, 2023

Vous pouvez utiliser un profil SSL pour spécifier la manière dont une appliance NetScaler traite le trafic SSL. Un profil est un ensemble de paramètres SSL pour les entités SSL, telles que les serveurs virtuels, les services et les groupes de services, et offre facilité de configuration et flexibilité. Vous n'êtes pas limité à la configuration d'un seul ensemble de paramètres globaux.

Vous pouvez créer plusieurs ensembles (profils) de paramètres globaux et attribuer différents ensembles à différentes entités SSL. Les profils SSL sont classés en deux catégories :

- **Profils frontaux** : contiennent les paramètres applicables à l'entité frontale (entité qui reçoit des demandes d'un client).
- **Profils dorsaux** : contiennent les paramètres applicables à l'entité principale (entité qui envoie les demandes des clients à un serveur).

Contrairement à un profil TCP ou HTTP, un profil SSL est facultatif. Une fois les profils SSL activés, tous les points de terminaison SSL héritent des profils par défaut. Le même profil peut être réutilisé sur plusieurs entités. Si aucun profil n'est associé à une entité, les valeurs définies au niveau global s'appliquent. Pour les services appris de manière dynamique, les valeurs globales actuelles s'appliquent.

Par rapport à l'autre méthode qui nécessite la configuration de paramètres SSL, de chiffrements et de courbes ECC sur des points de terminaison SSL individuels, les profils SSL de l'appliance NetScaler simplifient la gestion de la configuration en agissant comme un point unique de configuration SSL pour tous les points de terminaison associés. À l'aide des profils SSL, vous pouvez résoudre les problèmes de configuration liés à la réorganisation des chiffrements et aux interruptions de service lors de la réorganisation des chiffrements.

Les profils SSL aident à définir les paramètres SSL et les liaisons de chiffrement requis sur les points de terminaison SSL sur lesquels il est généralement impossible de définir ces paramètres et liaisons. Les profils SSL peuvent également être définis sur des écrans sécurisés.

L'infrastructure des profils SSL a été améliorée pour utiliser les derniers chiffrements et protocoles. Les différences entre le profil existant (ancien profil) et le profil SSL amélioré (nouveau profil) sont mises en évidence.

Différences entre l'ancienne et la nouvelle infrastructure de profils SSL

Différences	Ancien profil	Nouveau profil
Chiffres et courbes ECC inclus dans le profil	Non	Oui
Insertion d'un chiffre ou d'un groupe de chiffrement au milieu d'une liste existante	Dissociez tous les chiffrements et reliez-les à nouveau dans l'ordre de priorité requis.	Ajoutez un code et attribuez-lui une priorité. Si aucune priorité n'est spécifiée, la priorité la plus faible de la liste est attribuée au chiffrement.
Délier tous les chiffrements	`unbind ssl vserver <name> ciphername -ALL`	`unbind ssl profile -cipherName FlushAllCiphers` (Les versions 12.1 et ultérieures incluent le paramètre FlushAllCiphers pour dissocier tous les chiffrements ou groupes de chiffrement d'un profil, car ALL est traité comme un groupe de chiffrement.)

Différences	Ancien profil	Nouveau profil
État du SSLv3	s/o	Désactivé sur le profil frontal par défaut (ns_default_ssl_profile_frontend). Remarque : Avant d'activer ce profil, SSLv3 est activé globalement. Une fois le profil activé, SSLv3 est désactivé sur le profil frontal par défaut.

Infrastructure de profils SSL

May 5, 2023

Des vulnérabilités dans la mise en œuvre de SSLv3 et RC4 ont mis en évidence la nécessité d'utiliser les derniers chiffrements et protocoles pour négocier les paramètres de sécurité d'une connexion réseau. La mise en œuvre de toute modification de la configuration, telle que la désactivation de SSLv3 sur des milliers de points de terminaison SSL, est un processus fastidieux. Par conséquent, les paramètres qui faisaient partie de la configuration des points de terminaison SSL ont été déplacés vers les profils SSL, ainsi que les chiffrements par défaut. Pour mettre en œuvre des modifications dans la configuration, y compris la prise en charge du chiffrement, il vous suffit de modifier le profil lié aux entités.

Les profils SSL frontaux et dorsaux par défaut contiennent tous les chiffrements et les courbes ECC par défaut, en plus des paramètres qui faisaient partie des anciens profils. Des exemples de sorties pour les profils par défaut sont fournis en annexe. L'opération Activer le profil par défaut lie automatiquement le profil frontal par défaut à toutes les entités frontales, et le profil principal par défaut à toutes les entités principales. Vous pouvez modifier un profil par défaut en fonction de votre déploiement. Vous pouvez également créer des profils personnalisés et les lier à des entités SSL.

Le profil frontal contient des paramètres applicables à une entité frontale (l'entité qui reçoit les demandes d'un client). Il s'agit généralement d'un serveur virtuel SSL, d'un service SSL transparent ou de services internes sur l'appliance NetScaler. Le profil principal contient des paramètres applicables à une entité principale (entité de l'appliance ADC qui envoie les demandes des clients à un serveur principal). Généralement, cette entité est un service SSL ou un groupe de services sur l'appliance NetScaler. Si vous essayez de configurer un paramètre non pris en charge, l'erreur `ERROR: Specified parameters are not applicable for this type of SSL profile` apparaît. Certains paramètres SSL, tels que la taille de la mémoire CRL, la taille du cache OCSP, le contrôle UnDefaction et les données UnDefaction, ne font partie d'aucun profil, car ces paramètres

sont indépendants des entités. Ces paramètres sont présents dans **Gestion du trafic > SSL > Paramètres SSL avancés**. Pour plus d'informations sur les paramètres SSL pris en charge sur un moniteur sécurisé, voir Définir les paramètres SSL sur un moniteur sécurisé.

Un profil SSL prend en charge les opérations suivantes :

- **Ajouter** : crée un profil SSL sur l'appliance NetScaler. Spécifiez si le profil est frontal ou dorsal. La valeur par défaut est le front-end.
- **Définir** : — Modifie les paramètres d'un profil existant.
- **Non défini** : rétablit les valeurs par défaut des paramètres spécifiés. Si vous ne spécifiez aucun paramètre, un message d'erreur s'affiche. Si vous annulez la définition d'un profil sur une entité, le profil n'est pas lié à l'entité.
- **Supprimer** : supprime un profil. Un profil utilisé par une entité ne peut pas être supprimé. L'effacement de la configuration supprime toutes les entités. Par conséquent, les profils sont également supprimés.
- **Lier** : lie un profil à une entité SSL.
- **Dissocier** : dissocie un profil d'une entité SSL.
- **Afficher** : affiche tous les profils disponibles sur l'appliance NetScaler. Si un nom de profil est spécifié, les détails de ce profil sont affichés. Si une entité est spécifiée, les profils associés à cette entité sont affichés.

> **Important :**
>
> - Un profil SSL a priorité sur les paramètres SSL. En d'autres termes, si vous configurez des paramètres SSL à l'aide de la commande `set ssl parameter`, puis que vous liez ultérieurement un profil à une entité SSL, les paramètres du profil sont prioritaires.
> - Après la mise à niveau, si vous activez les profils par défaut, vous ne pouvez pas annuler les modifications. En d'autres termes, les profils ne peuvent pas être désactivés. Enregistrez la configuration et créez une copie du fichier de configuration (ns.conf) avant d'activer les profils. Toutefois, si vous ne souhaitez pas utiliser les fonctionnalités du profil par défaut, vous pouvez continuer à utiliser les anciens profils SSL. Pour plus d'informations sur ces profils, voir Profil SSL hérité.
> - À partir de la version 11.1 51.x, dans l'interface graphique et CLI, une invite de confirmation est ajoutée lorsque vous activez le profil par défaut pour empêcher l'activation par erreur.

À partir de la version 13.1 build 17.x, les protocoles inférieurs à TLSv1.2 sont désactivés sur les services internes SSL. Si le profil par défaut (amélioré) est activé, le profil `ns_default_ssl_profile_internal_fronte` est lié aux services internes SSL et les protocoles SSLv3, TLSv1.0 et TLSv1.1 sont désactivés dans le profil.

Commande :

```
1 set ssl parameter -defaultProfile ENABLED
```



```
2     Save your configuration before enabling the Default profile. You
         cannot undo the changes. Are you sure you want to enable the
         Default profile? [Y/N]Y
3  Done
4  <!--NeedCopy-->
```

Par défaut, certains paramètres SSL, appelés *paramètres globaux*, s'appliquent à tous les points de terminaison SSL. Toutefois, si un profil est lié à un point de terminaison SSL, les paramètres globaux ne s'appliquent pas. Les paramètres spécifiés dans le profil s'appliquent à la place.

Points à noter

1. Un profil peut être lié à plusieurs serveurs virtuels, mais un serveur virtuel ne peut être lié qu'à un seul profil.
2. Pour supprimer un profil lié à un serveur virtuel, dissociez d'abord le profil.
3. Un chiffrement ou un groupe de chiffrement peut être lié à plusieurs profils ayant des priorités différentes.
4. Un profil peut comporter plusieurs chiffrements et groupes de chiffrement liés à différentes priorités.
5. Les modifications apportées à un groupe de chiffrement sont immédiatement répercutées dans tous les profils et dans tous les serveurs virtuels auxquels l'un des profils est lié.
6. Si une suite de chiffrement fait partie d'un groupe de chiffrement, modifiez le groupe de chiffrement pour supprimer cette suite de chiffrement avant de supprimer la suite de chiffrement du profil.
7. Si vous n'attribuez pas de priorité à une suite de chiffrement ou à un groupe de chiffrement associé à un profil, la priorité la plus basse du profil lui est attribuée.
8. Vous pouvez créer un groupe de chiffrement personnalisé (également appelé groupe de chiffrement défini par l'utilisateur) à partir de groupes de chiffrement et de suites de chiffrement existants. Si vous créez le groupe de chiffrement A et que vous y ajoutez des groupes de chiffrement X et Y existants, dans cet ordre, Y est affecté à une priorité inférieure à X. En d'autres termes, le groupe ajouté en premier a une priorité supérieure.
9. Si une suite de chiffrement fait partie de deux groupes de chiffrement attachés au même profil, la suite de chiffrement n'est pas ajoutée en tant que partie du deuxième groupe de chiffrement. La suite de chiffrement ayant la priorité la plus élevée est en vigueur lorsque le trafic est traité.
10. Les groupes de chiffrement ne sont pas développés dans le profil. Par conséquent, le nombre de lignes dans le fichier de configuration (ns.conf) est considérablement réduit. Par exemple, si deux groupes de chiffrement contenant 15 chiffrements chacun sont liés à un millier de serveurs virtuels SSL, l'extension ajoute 30*1 000 entrées liées au chiffrement dans le fichier de configuration. Avec le nouveau profil, il n'aurait que deux entrées : une pour chaque groupe de chiffrement lié à un profil.

11. La création d'un groupe de chiffrement défini par l'utilisateur à partir de chiffrements et de groupes de chiffrement existants est une opération de copier-coller. Les modifications apportées au groupe d'origine ne sont pas reflétées dans le nouveau groupe.
12. Un groupe de chiffrement défini par l'utilisateur répertorie tous les profils dont il fait partie.
13. Un profil répertorie tous les serveurs virtuels SSL, les services et les groupes de services auxquels il est lié.
14. Si la fonctionnalité de profil SSL par défaut est activée, utilisez le profil pour définir ou modifier l'un des attributs d'une entité SSL. Par exemple, un serveur virtuel, un service, un groupe de services ou un service interne.

Enregistrez la configuration en utilisant l'interface de ligne de commande

À l'invite de commande, tapez :

```
save config

shell

root@ns# cd /nsconfig

root@ns# cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber
   >
<!--NeedCopy-->
```

Exemple :

```
save config
shell
root@ns# cd /nsconfig
root@ns# cp ns.conf ns.conf.NS.11.0.jun.16
<!--NeedCopy-->
```

Activer le profil par défaut

> **Important :**
>
> - Enregistrez votre configuration avant de mettre à niveau le logiciel et d'activer les profils par défaut.
> - À partir de la version 11.1 build 51.x, dans l'interface graphique et l'interface de ligne de commande, une invite de confirmation s'affiche lorsque vous activez le profil par défaut pour éviter de l'activer par erreur.

Commande : La commande suivante active le profil par défaut et lie ce profil aux entités SSL auxquelles un profil est déjà lié. En d'autres termes, si un profil (par exemple P1) est déjà lié à une entité SSL, le profil frontal par défaut ou le profil principal par défaut remplace P1. L'ancien profil (P1) n'est pas supprimé. Il s'agit désormais d'un profil SSL amélioré qui contient les paramètres précédents, ainsi que les chiffrements et les courbes ECC. Si vous ne souhaitez pas obtenir le profil par défaut, vous pouvez lier explicitement P1 à l'entité SSL.

```
1 set ssl parameter -defaultProfile ENABLED
2     Save your configuration before enabling the Default profile. You
          cannot undo the changes. Are you sure you want to enable the
          Default profile? [Y/N]Y
3 Done
4 <!--NeedCopy-->
```

Mettez à niveau le logiciel vers une version qui prend en charge l'infrastructure de profil améliorée, puis activez les profils par défaut.

> **Remarques :**
>
> - Si un profil hérité (P1) est déjà lié à une entité SSL et que vous activez le profil par défaut, le profil par défaut remplace la liaison précédente. En d'autres termes, le profil par défaut est lié aux entités SSL. Si vous ne souhaitez pas que le profil par défaut soit lié, vous devez lier à nouveau P1 à l'entité SSL.
> - Une seule opération (Activer le profil par défaut ou `set ssl parameter -defaultProfile ENABLED`) active (lie) à la fois le profil frontal par défaut et le profil principal par défaut.

Paramètres faisant partie des profils par défaut

Exécutez les commandes suivantes pour répertorier les paramètres qui font partie des profils frontaux et dorsaux par défaut.

```
1 sh ssl profile ns_default_ssl_profile_frontend
2 sh ssl profile ns_default_ssl_profile_backend
3 <!--NeedCopy-->
```

Exemple :

```
1 > sh ssl profile ns_default_ssl_profile_frontend
2 1)  Name: ns_default_ssl_profile_frontend   (Front-End)
3     SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
          ENABLED  TLSv1.3: DISABLED
4     Client Auth: DISABLED
5     Use only bound CA certificates: DISABLED
6     Strict CA checks:   NO
```



```
    Session Reuse: ENABLED  Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED  Refresh Count: 0
    Deny SSL Renegotiation  ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:  NO
    Match HTTP Host header with SNI:    CERT
    Push flag:  0x0 (Auto)
    SSL quantum size:   8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45
    Subject/Issuer Name Insertion Format:   Unicode

    SSL Interception: DISABLED
    SSL Interception OCSP Check: ENABLED
    SSL Interception End to End Renegotiation: ENABLED
    SSL Interception Maximum Reuse Sessions per Server: 10
    Session Ticket: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    HSTS Preload: NO
    Allow Extended Master Secret: NO
    Send ALPN Protocol: NONE


    ECC Curve: P_256, P_384, P_224, P_521

1)  Cipher Name: DEFAULT    Priority :1
    Description: Predefined Cipher Alias


> sh ssl profile ns_default_ssl_profile_backend
```

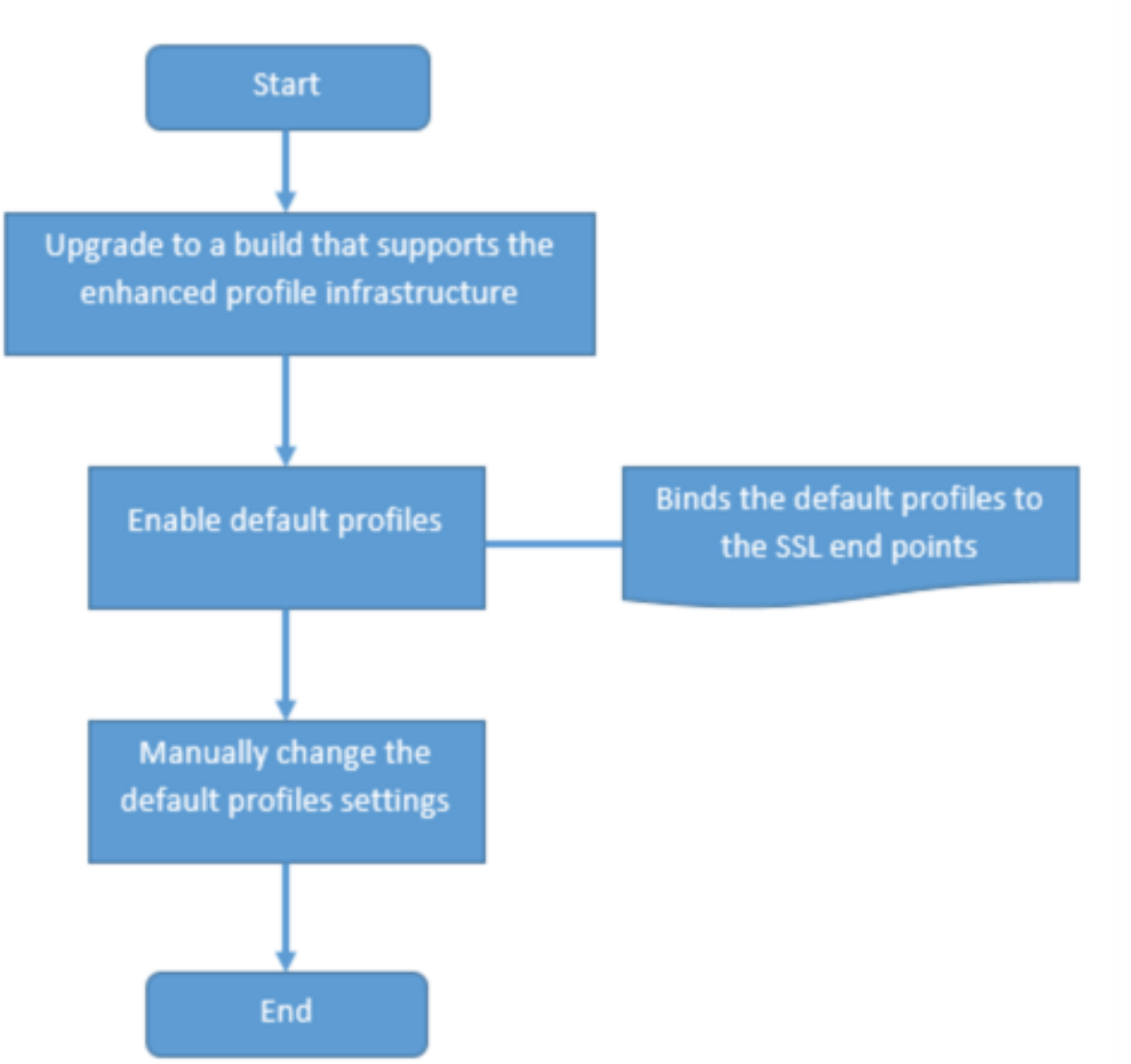


```
1)  Name: ns_default_ssl_profile_backend    (Back-End)
    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Server Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED  Timeout: 300 seconds
    DH: DISABLED
    Ephemeral RSA: DISABLED
    Deny SSL Renegotiation  ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:  NO
    Push flag:  0x0 (Auto)
    SSL quantum size:   8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45

    Allow Extended Master Secret: NO

    ECC Curve: P_256, P_384, P_224, P_521

1)  Cipher Name: DEFAULT_BACKEND    Priority :1
    Description: Predefined Cipher Alias
 Done
 <!--NeedCopy-->
```

Cas d'utilisation

Une fois que vous avez activé les profils par défaut, ils sont liés à tous les points de terminaison SSL. Les profils par défaut sont modifiables. Si votre déploiement utilise la plupart des paramètres par défaut et ne modifie que quelques paramètres, vous pouvez modifier les profils par défaut. Les modifications sont immédiatement répercutées sur tous les points finaux. Vous pouvez également créer des profils SSL personnalisés avec certains paramètres personnalisés et certains paramètres par défaut et les lier aux entités SSL.

L'organigramme suivant explique les étapes que vous devez effectuer :



1. Pour plus d'informations sur la mise à niveau du logiciel, consultez la section Mise à niveau du logiciel système.
2. Activez les profils par défaut à l'aide de l'interface de ligne de commande ou de l'interface graphique.
   - Sur la ligne de commande, tapez : `set ssl parameter -defaultProfile ENABLED`
   - Si vous préférez utiliser l'interface graphique, accédez à **Gestion du trafic** > **SSL > Modifier les paramètres SSLavancés**, faites défiler la page vers le bas et sélectionnez**Activer le profil par défaut**.

Si un profil n'était pas lié à un point de terminaison avant la mise à niveau, un profil par défaut est lié au point de terminaison SSL. Si un profil était lié à un point final avant la mise à niveau, le même profil est lié après la mise à niveau et des chiffrements par défaut sont ajoutés au profil.

1. (Facultatif) Modifiez manuellement tous les paramètres du profil par défaut.
    - Sur la ligne de commande, tapez : `set ssl profile <name>` suivi des paramètres à modifier.
    - Si vous préférez utiliser l'interface graphique, accédez à **Système** > **Profils**. Dans **Profils SSL**, sélectionnez un profil et cliquez sur **Modifier**.

Paramètres du profil SSL

Vous pouvez définir les paramètres SSL suivants dans un profil SSL. Vous pouvez définir certains de ces paramètres dans un serveur virtuel SSL. Pour plus d'informations sur les paramètres du serveur virtuel SSL, consultez Paramètres du serveur virtuel SSL.

Prise en charge de la renégociation sécurisée au niveau du back-end d'une appliance NetScaler

Remarque : Ce paramètre est introduit dans la version 13.0 build 58.x et ultérieures. Dans les versions et versions précédentes, seule la renégociation non sécurisée était prise en charge sur le back-end.

La fonctionnalité est prise en charge sur les plateformes suivantes :

- VPX
- Plates-formes MPX contenant des puces N2 ou N3
- Plates-formes à puce Intel Coleto SSL

La fonctionnalité n'est pas encore prise en charge sur la plateforme FIPS.

La renégociation sécurisée est refusée par défaut sur le back-end d'un boîtier ADC. En d'autres termes, le paramètre `denySSLReneg` est défini sur ALL (par défaut).

Pour autoriser la renégociation sécurisée sur le serveur principal, sélectionnez l'un des paramètres suivants pour le paramètre `denySSLReneg` :

- NON
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NON SÉCURISÉ

Activer la renégociation sécurisée à l'aide du CLI

À l'invite de commande, tapez :

```
set ssl profile <name> -denySSLReneg <denySSLReneg>
```

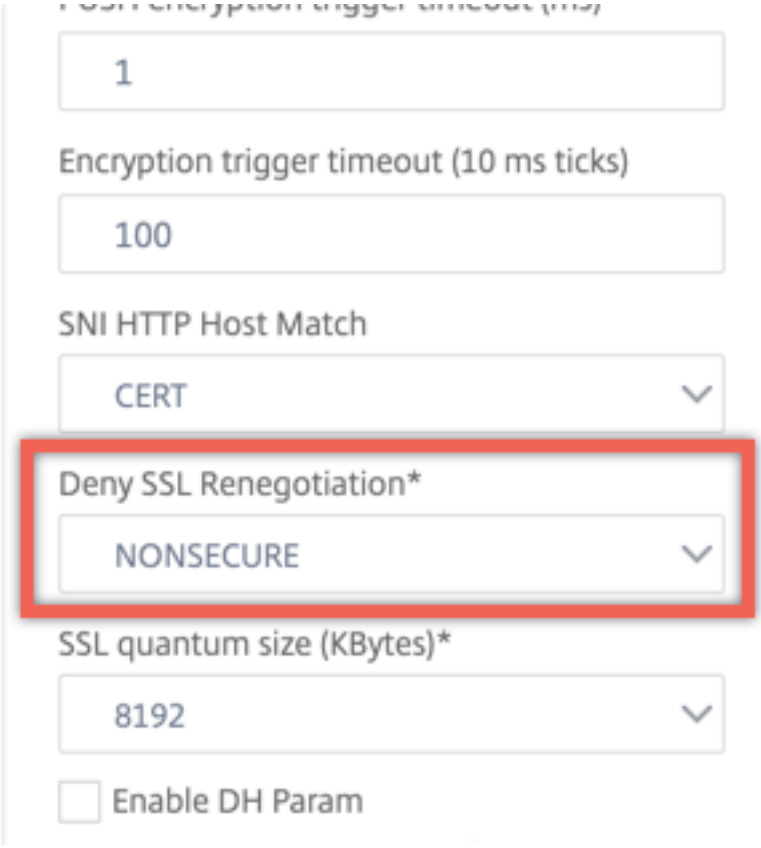
Exemple :


```
set ssl profile ns_default_ssl_profile_backend -denySSLReneg NONSECURE
 Done

sh ssl profile ns_default_ssl_profile_backend
1)  Name: ns_default_ssl_profile_backend    (Back-End)
    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Server Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:       NO
    Session Reuse: ENABLED      Timeout: 300 seconds
    DH: DISABLED
    Ephemeral RSA: DISABLED
    Deny SSL Renegotiation      NONSECURE
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:      NO
    Push flag:  0x0 (Auto)
    SSL quantum size:       8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45

    ECC Curve: P_256, P_384, P_224, P_521

1)  Cipher Name: DEFAULT_BACKEND        Priority :2
    Description: Predefined Cipher Alias

1)  Service Name: s187
 Done
<!--NeedCopy-->
```

Activer la renégociation sécurisée à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profil SSL**.
2. Ajoutez ou modifiez un profil.

3. Définissez **Refuser la renégociation SSL** sur n'importe quelle valeur autre que ALL.



Validation de l'en-tête

Remarque : Ce paramètre est introduit dans la version 13.0 build 52.x.

Avec HTTP/1.1, les clients devaient utiliser plusieurs connexions pour traiter plusieurs demandes. Avec HTTP/2, les clients peuvent réutiliser les connexions entre les domaines couverts par le même certificat. Pour une session activée SNI, l'appliance ADC doit être en mesure de contrôler la façon dont l'en-tête d'hôte HTTP est validé pour tenir compte de ce changement. Dans les versions précédentes, la demande était supprimée si le paramètre était activé (défini sur « Oui ») et si la demande ne contenait pas l'en-tête d'hôte pour une session activée SNI. Si le paramètre était désactivé (défini sur « Non »), l'appliance n'a pas effectué la validation. Un nouveau paramètre `SNIHTTPHostMatch` est ajouté à un profil SSL et des paramètres globaux SSL pour avoir un meilleur contrôle sur cette validation. Ce paramètre peut prendre trois valeurs : CERT, STRICT et NONE. Ces valeurs fonctionnent comme suit pour les sessions activées pour SNI uniquement. Le SNI doit être activé sur le serveur virtuel SSL ou le profil lié au serveur virtuel, et la demande HTTP doit contenir l'en-tête de l'hôte.

- CERT - La connexion est transférée si la valeur d'en-tête d'hôte dans la demande est couverte par le certificat utilisé pour établir cette session SSL.
- STRICT - La connexion est transférée uniquement si la valeur de l'en-tête d'hôte dans la de-

mande correspond à la valeur du nom du serveur transmise dans le message Client Hello de la connexion SSL.

- NON - La valeur de l'en-tête de l'hôte n'est pas validée.

Valeurs possibles : NO, CERT, STRICT
Valeur par défaut : CERT

Avec l'introduction du nouveau paramètre `SNIHTTPHostMatch`, le comportement du paramètre `dropReqWithNoHostHeader` change. La définition du paramètre `dropReqWithNoHostHeader` n'affecte plus la façon dont l'en-tête de l'hôte est validé par rapport au certificat SNI.

Définir les paramètres de profil SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl profile <name> [-ssllogProfile <string>] [-dh ( ENABLED | DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED | DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED | DISABLED )
[-sessTimeout <positive_integer>]] [-cipherRedirect ( ENABLED | DISABLED ) [-cipherURL <URL>]] [-clientAuth ( ENABLED | DISABLED )[-clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
DISABLED )] [-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 ( ENABLED | DISABLED )] [-tls11 ( ENABLED| DISABLED )] [-tls12 ( ENABLED | DISABLED )] [-tls13 ( ENABLED |DISABLED )] [-SNIEnable ( ENABLED | DISABLED )] [-ocspStapling (ENABLED | DISABLED )] [-serverAuth ( ENABLED | DISABLED )] [-commonName <string>] [-pushEncTrigger <pushEncTrigger>] [-sendCloseNotify ( YES |
NO )] [-clearTextPort <port|*>] [-insertionEncoding ( Unicode | UTF-8)] [-denySSLReneg <denySSLReneg>] [-quantumSize <quantumSize>]
[-strictCAChecks ( YES | NO )] [-encryptTriggerPktCount <positive_integer>] [-pushFlag <positive_integer>][-dropReqWithNoHostHeader ( YES | NO )] [-SNIHTTPHostMatch <SNIHTTPHostMatch>] [-pushEncTriggerTimeout <positive_integer>]
[-sslTriggerTimeout <positive_integer>] [-clientAuthUseBoundCAChain ( ENABLED | DISABLED )] [-sslInterception ( ENABLED | DISABLED )][-ssliReneg ( ENABLED | DISABLED )] [-ssliOCSPCheck ( ENABLED | DISABLED )] [-ssliMaxSessPerServer <positive_integer>] [-HSTS ( ENABLED| DISABLED )] [-maxage <positive_integer>] [-IncludeSubdomains ( YES | NO )] [-preload ( YES | NO )] [-sessionTicket ( ENABLED | DISABLED )][-sessionTicketLifeTime <positive_integer>] [-sessionTicketKeyRefresh (ENABLED | DISABLED )]
{
```

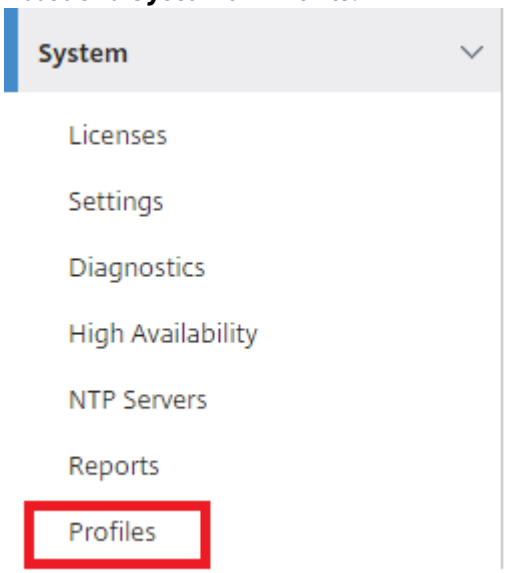


```
 -sessionTicketKeyData  }
  [-sessionKeyLifeTime <positive_integer>] [-prevSessionKeyLifeTime <
     positive_integer>]
[-cipherName <string> -cipherPriority <positive_integer>][-
   strictSigDigestCheck ( ENABLED | DISABLED )]
[-skipClientCertPolicyCheck ( ENABLED | DISABLED )] [-zeroRttEarlyData
   ( ENABLED | DISABLED )] [-tls13SessionTicketsPerAuthContext
<positive_integer>] [-dheKeyExchangeWithPsk ( YES | NO )]
<!--NeedCopy-->
```

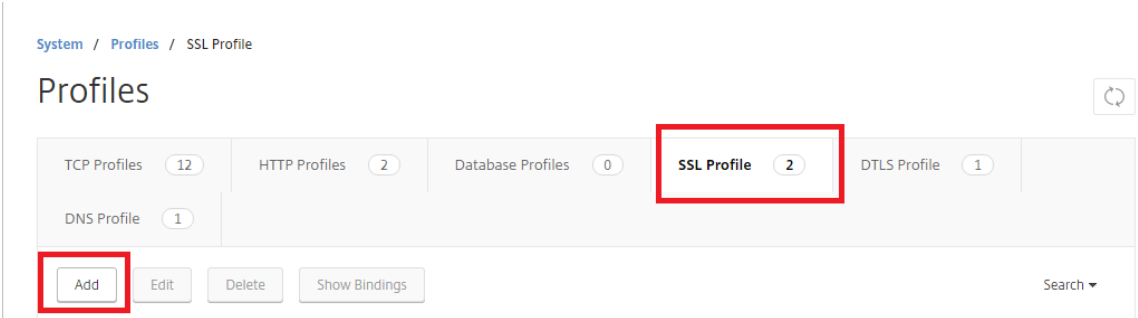
Définition des paramètres de profil SSL à l'aide de l'interface graphique

Pour ajouter un profil :

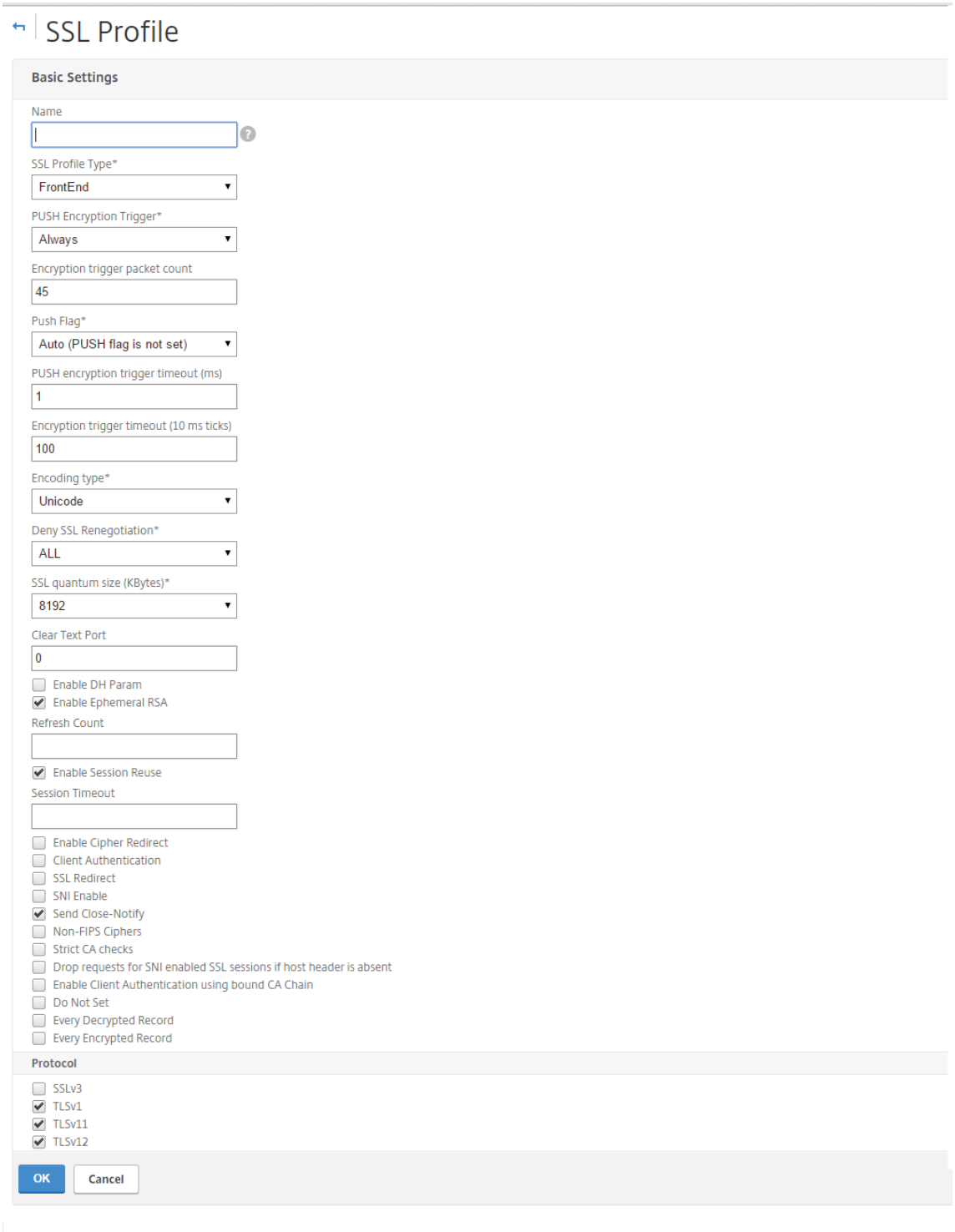
1. Accédez à **Système > Profils**.



2. Sélectionnez **Profils SSL**. Cliquez sur **Ajouter**.



3. Spécifiez des valeurs pour les différents paramètres.



4. Cliquez sur **OK**.
5. Cliquez sur **Terminé**.

Pour réutiliser un profil SSL existant :

1. Accédez à **Système > Profils**.
2. Sélectionnez un profil existant et cliquez sur **Ajouter**.

3. Spécifiez un autre nom, modifiez tous les paramètres, puis cliquez sur **OK**.
4. Cliquez sur **Terminé**.

Extension du ticket de session TLS

Une prise de contact SSL est une opération gourmande en CPU. Si la réutilisation de session est activée, l'opération d'échange de clés serveur/client est ignorée pour les clients existants. Ils sont autorisés à reprendre leurs sessions. Cette action améliore le temps de réponse et augmente le nombre de transactions SSL par seconde qu'un serveur peut prendre en charge. Toutefois, le serveur doit stocker les détails de chaque état de session, ce qui consomme de la mémoire et est difficile à partager entre plusieurs serveurs si les demandes sont équilibrées de charge entre les serveurs.

Les appliances NetScaler prennent en charge l'extension SessionTicket TLS. L'utilisation de cette extension indique que les détails de session sont stockés sur le client plutôt que sur le serveur. Le client doit indiquer qu'il prend en charge ce mécanisme en incluant l'extension TLS du ticket de session dans le message Hello du client. Pour les nouveaux clients, cette extension est vide. Le serveur envoie un nouveau ticket de session dans le message d'établissement de liaison NewSessionTicket. Le ticket de session est chiffré à l'aide d'une paire de clés connue uniquement du serveur. Si un serveur ne peut pas émettre de nouveau ticket maintenant, il effectue une prise de contact normale.

Cette fonctionnalité n'est disponible que dans les profils SSL frontaux, et uniquement au niveau de la partie frontale de la communication dans laquelle l'appliance agit en tant que serveur et génère des tickets de session.

Limitations

- Cette fonctionnalité n'est pas prise en charge sur une plate-forme FIPS.
- Cette fonctionnalité est prise en charge uniquement avec les versions TLS 1.1 et 1.2.
- La persistance des ID de session SSL n'est pas prise en charge avec les tickets de session.

Activer l'extension de ticket de session TLS à l'aide de la CLI

À l'invite de commande, tapez :

```
set ssl profile <name> -sessionTicket (ENABLED | DISABLED ) [-
   sessionTicketLifeTime <positive_integer>
<!--NeedCopy-->
```

Arguments :

SessionTicket : état de l'extension du ticket de session TLS. L'utilisation de cette extension indique que les détails de session sont stockés sur le client plutôt que sur le serveur, tel que défini dans la RFC 5077.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

SessionTicketLifetime : spécifiez un délai, en secondes, après lequel le ticket de session expire et une nouvelle poignée de main SSL doit être initiée.

Valeur par défaut : 300

Valeur minimale : 0

Valeur maximale : 172800

Exemple :

```
1 add ssl profile profile1 -sessionTicket ENABLED -sessionTicketlifeTime
     300
2 Done
3 <!--NeedCopy-->
```

Activer l'extension de ticket de session TLS à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils**. Sélectionnez **Profils SSL**.
2. Cliquez sur **Ajouter** et spécifiez un nom pour le profil.
3. Sélectionnez **Ticket de session**.
4. Vous pouvez également spécifier Durée de **vie du ticket de session (en secondes)**.

Implémentation sécurisée des tickets de session

En utilisant des tickets de session TLS, les clients peuvent utiliser des poignées de contact abrégées pour une reconnexion plus rapide aux serveurs. Toutefois, si les tickets de session ne sont pas chiffrés ou modifiés pendant de longues périodes, ils peuvent présenter un risque pour la sécurité. Vous pouvez sécuriser les tickets de session en les chiffrant à l'aide d'une clé symétrique. Pour atteindre la confidentialité, vous pouvez spécifier un intervalle de temps pendant lequel la clé du ticket de session est actualisée.

L'appliance génère les clés de ticket de session par défaut. Toutefois, si plusieurs appliances d'un déploiement doivent déchiffrer les tickets de session des autres, elles doivent toutes utiliser la même clé de ticket de session. Par conséquent, vous devez définir (ajouter ou charger) les mêmes données de clé de ticket de session manuellement sur toutes les appliances. Les données clés du ticket de session incluent les informations suivantes :

- Nom du ticket de session.
- Clé AES de session utilisée pour chiffrer ou déchiffrer le ticket.
- Clé HMAC de session utilisée pour calculer le résumé du ticket.

Vous pouvez désormais configurer les données de clé de ticket de session d'une longueur de 64 octets pour prendre en charge les clés HMAC 256 bits, comme recommandé dans la RFC 5077. Des longueurs de clé de 48 octets sont également prises en charge pour la compatibilité ascendante.

> **Remarque :**
>
> Lorsque vous saisissez manuellement les données clés du ticket de session, assurez-vous que la configuration de toutes les appliances NetScaler dans une configuration HA ou dans une configuration de cluster est la même.

Le paramètre `sessionTicketKeyLifeTime` spécifie la fréquence à laquelle une clé de ticket de session est actualisée. Vous pouvez définir le paramètre `prevSessionTicketKeyLifeTime` pour spécifier la durée pendant laquelle la clé de ticket de session précédente sera conservée pour le décryptage des tickets à l'aide de cette clé, après la génération d'une nouvelle clé. Le paramètre `prevSessionTicketKeyLifeTime` prolonge la durée pendant laquelle un client peut utiliser une poignée de main abrégée pour se reconnecter. Par exemple, si `sessionTicketKeyLifeTime` est défini sur 10 minutes et `prevSessionTicketKeyLifeTime` sur 5 minutes, une nouvelle clé est générée après 10 minutes et utilisée pour toutes les nouvelles sessions. Cependant, les clients déjà connectés disposent de 5 minutes supplémentaires pendant lesquelles les tickets précédemment émis sont honorés pour une poignée de main abrégée.

Configurer les données des tickets de session SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl profile <name> -sessionTicket ENABLED -sessionTicketLifeTime <
    positive_integer> -sessionTicketKeyRefresh ( ENABLED | DISABLED )] -
    sessionTicketKeyLifeTime <positive_integer> [-
    prevSessionTicketKeyLifeTime <positive_integer>]
<!--NeedCopy-->
```

Arguments :

SessionTicket : utilisez les tickets de session comme décrit par la RFC 5077. L'établissement de la prise de contact initiale nécessite des opérations de chiffrement à clé publique gourmandes en CPU. Avec le **paramètre** ENABLED, un serveur envoie un ticket de session à un client, que le client peut utiliser pour effectuer une prise de contact abrégée.

Valeurs possibles : ACTIVÉ, DÉSACTIVÉ. Par défaut : DÉSACTIVÉ

SessionTicketLifetime : durée de vie, en secondes, du ticket de session. Passé ce délai, les clients ne peuvent pas utiliser ce ticket pour reprendre leurs sessions.

Valeur maximale : 172800. Valeur minimale : 0. Par défaut : 300.

SessionTicketKeyRefresh : lorsque la durée spécifiée par le paramètre de durée de vie de la clé de ticket de session expire, régénérez la clé de ticket de session utilisée pour chiffrer ou déchiffrer les tickets de session. Activé automatiquement si SessionTicket est activé. Désactivé si un administrateur saisit les données du ticket de session.

Valeurs possibles : ACTIVÉ, DÉSACTIVÉ. Par défaut : ACTIVÉ

SessionKeyLifetime : durée de vie, en secondes, d'une clé symétrique utilisée pour chiffrer les tickets de session émis par une appliance NetScaler.

Valeur maximale : 86400. Valeur minimale : 600. Par défaut : 3000

PrevSessionKeyLifetime : durée, en secondes, pendant laquelle la clé symétrique précédente utilisée pour chiffrer les tickets de session reste valide pour les clients existants après l'expiration de la durée de vie de la clé du ticket de session. Pendant ce temps, les clients existants peuvent reprendre leurs sessions en utilisant la clé de ticket de session précédente. Les tickets de session pour les nouveaux clients sont chiffrés à l'aide de la nouvelle clé.

Valeur maximale : 172800. Valeur minimale : 0. Par défaut : 0

Exemple :

```
set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED
    -sessionTicketlifeTime 120 -sessionTicketKeyRefresh ENABLED -
    sessionTicketKeyLifeTime 100 -prevSessionTicketKeyLifeTime 60

Done

show ssl profile ns_default_ssl_profile_frontend

     Session Ticket: ENABLED
     Session Ticket Lifetime: 120 (secs)
     Session Key Auto Refresh: ENABLED
     Session Key Lifetime: 100 (secs)
     Previous Session Key Lifetime: 60 (secs)
<!--NeedCopy-->
```

Configurer les données des tickets de session SSL à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils**, puis sélectionnez **Profil SSL**.
2. Sélectionnez **ns_default_ssl_profile_frontend** et cliquez sur **Modifier**.
3. Dans la section **Paramètres de base**, cliquez sur l'icône en forme de crayon et définissez les paramètres suivants :
    - Ticket de session

- Durée de vie du billet de session (secondes)
- Actualisation automatique de la clé du ticket
- Durée de vie de la clé du ticket de session (secondes)
- Durée de vie des clés du ticket de session précédente (secondes)

4. Cliquez sur **OK**.

Tapez les données du ticket de session SSL manuellement à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl profile <name> -sessionTicket ENABLED

set ssl profile <name> -sessionTicketKeyData

show ssl profile ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

Arguments :

SessionTicket : utilisation de tickets de session tel que décrit par la RFC 5077. L'établissement de la prise de contact initiale nécessite des opérations de chiffrement à clé publique gourmandes en CPU. Avec le **paramètre** ENABLED, un serveur envoie un ticket de session à un client, que le client peut utiliser pour effectuer une prise de contact abrégée.

Valeurs possibles : ACTIVÉ, DÉSACTIVÉ. Par défaut : DÉSACTIVÉ

sessionTicketKeyData: Contains the session ticket name (0-15 bytes), the session AES key used to encrypt or decrypt the session ticket (16-31 bytes), and the session HMAC key used to compute the digest of the ticket (32-63 bytes). Externally generated by an administrator and added to a NetScaler appliance.

Longueur maximale : 64 octets

Exemple :

```
set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED

Done

set ssl profile ns_default_ssl_profile_frontend -sessionTicketKeyData
    1111111111111111111111111111111111111111111111111

Done
```



```
8
9  show ssl profile ns_default_ssl_profile_frontend
10
11     1) Name: ns_default_ssl_profile_frontend (Front-End)
12     SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1.2: ENABLED
13     Client Auth: DISABLED
14     Use only bound CA certificates: DISABLED
15     Strict CA checks: NO
16     Session Reuse: ENABLED Timeout: 120 seconds
17     DH: DISABLED
18     DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA: ENABLED
           Refresh Count: 0
19     Deny SSL Renegotiation ALL
20     Non FIPS Ciphers: DISABLED
21     Cipher Redirect: DISABLED
22     SSL Redirect: DISABLED
23     Send Close-Notify: YES
24     Push Encryption Trigger: Always
25     PUSH encryption trigger timeout: 1 ms
26     SNI: DISABLED
27     OCSP Stapling: DISABLED
28     Strict Host Header check for SNI enabled SSL sessions: NO
29     Push flag: 0x0 (Auto)
30     SSL quantum size: 8 kB
31     Encryption trigger timeout 100 mS
32     Encryption trigger packet count: 45
33     Subject/Issuer Name Insertion Format: Unicode
34     Session Ticket: ENABLED
35     Session Ticket Lifetime: 300 (secs)
36     Session Key Auto Refresh: DISABLED
37     Session Key Lifetime: 3000 (secs)
38     Previous Session Key Lifetime: 0 (secs)
39     Session Key Data: 84
          dad1afc6d56b0deeb0a7fd7f299a207e8d8c15cdd087a5684a11a329fd732e87a0535d9088
40     47
          e8c181ba266f5c8838ae472cb3ab9255b683bf922fad32cee816c329989ef7cdeb278e93ac
41
42     ECC Curve: P_256, P_384, P_224, P_521
43
44     1) Cipher Name: DEFAULT Priority :4
45     Description: Predefined Cipher Alias
46
47     1) Internal Service Name (Front-End): nsrnatsip-127.0.0.1-5061
```



```
48      2) Internal Service Name (Front-End): nskrpcs-127.0.0.1-3009
49      3) Internal Service Name (Front-End): nshttps-::1l-443
50      4) Internal Service Name (Front-End): nsrpcs-::1l-3008
51      5) Internal Service Name (Front-End): nshttps-127.0.0.1-443
52      6) Internal Service Name (Front-End): nsrpcs-127.0.0.1-3008
53      7) Vserver Name: v1
54
55  Done
56  <!--NeedCopy-->
```

Saisissez les données du ticket de session SSL manuellement à l'aide de l'interface graphique

1. Accédez à **Système > Profils**, puis sélectionnez **Profil SSL**.
2. Sélectionnez **ns_default_ssl_profile_frontend** et cliquez sur **Modifier**.
3. Dans la section **Paramètres de base**, cliquez sur l'icône en forme de crayon et définissez les paramètres suivants :
   - Ticket de session
   - Données clés du ticket de session
   - Confirmer les données clés du ticket
4. Cliquez sur **OK**.

Prise en charge de l'extension du secret principal dans le cadre de l'établissement de contacts SSL sur les plateformes NetScaler non FIPS

Remarque : Ce paramètre est introduit dans la version 13.0 build 61.x.

Extended Master Secret (EMS) est une extension facultative du protocole TLS (Transport Layer Security). Un nouveau paramètre est ajouté qui s'applique à la fois aux profils SSL frontaux et dorsaux afin de prendre en charge l'EMS sur l'appliance NetScaler. Si le paramètre est activé et que l'homologue prend en charge EMS, l'appliance ADC utilise le calcul EMS. Si l'homologue ne prend pas en charge EMS, le calcul EMS n'est pas utilisé pour la connexion même si le paramètre est activé sur l'appliance. Pour plus d'informations sur EMS, consultez la RFC 7627.

Remarque : EMS ne s'applique qu'aux poignées de mains qui utilisent le protocole TLS version 1.0, 1.1 ou 1.2.

Support de plateforme pour EMS

- Plates-formes MPX et SDX contenant des puces Cavium N3 ou des cartes cryptographiques Intel Coleto Creek. Les plates-formes suivantes sont livrées avec des puces Intel Coleto :

- MPX 5900
- MPX/SDX 8900
- MPX/SDX 26000
- MPX/SDX 26000-50S
- MPS/SDX 26000-100G
- MPX/SDX 15000-50G

Vous pouvez également utiliser la commande `show hardware` pour déterminer si votre matériel est équipé de puces Coleto (COL) ou N3.

- Plateformes MPX et SDX sans cartes cryptographiques (logiciel uniquement).
- Plates-formes logicielles uniquement : VPX, CPX et BLX.

Le service EMS ne peut pas être activé sur les plateformes suivantes :

- Plates-formes FIPS MPX 9700 et MPX 14000 FIPS.
- Plateformes MPX et SDX contenant des puces cryptographiques Cavium N2.

Si le paramètre est activé, l'appliance ADC tente d'utiliser EMS dans les connexions TLS 1.2, TLS 1.1 et TLS 1.0. Le paramètre n'affecte pas les connexions TLS 1.3 ou SSLv3.

Pour permettre à EMS d'être négocié avec l'homologue, activez le paramètre sur le profil SSL lié au serveur virtuel (frontal) ou au service (backend).

Activer EMS à l'aide du CLI

À l'invite de commande, tapez :

```
set ssl profile <profile name> [-allowExtendedMasterSecret (YES | NO)]
```

Exemples

```
1 set ssl profile ns_default_ssl_profile_frontend  -
     allowExtendedMasterSecret YES
2
3 set ssl profile ns_default_ssl_profile_backend  -
     allowExtendedMasterSecret YES
4 <!--NeedCopy-->
```

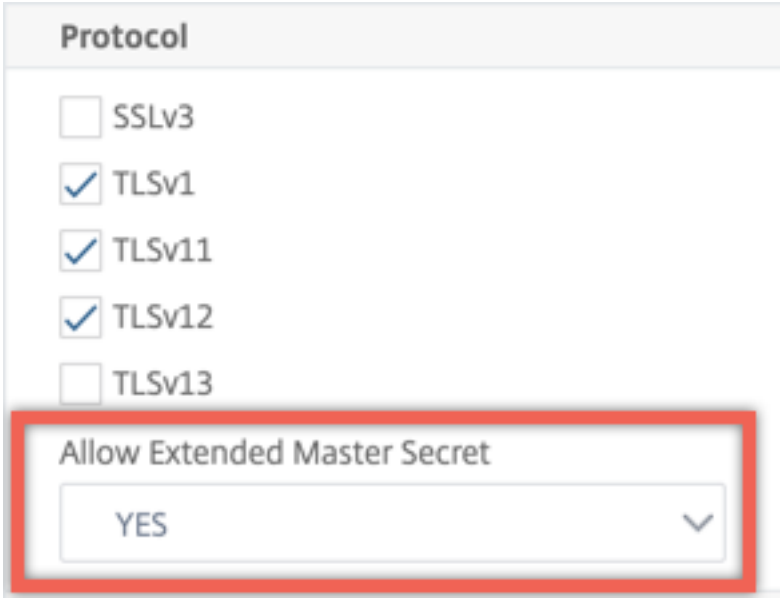
Le tableau suivant indique la valeur par défaut du `allowExtendedMasterSecret` paramètre sur différents profils par défaut et définis par l'utilisateur.

Profile	Paramètre par défaut
Profil frontal par défaut	NON

Profile	Paramètre par défaut
Profil sécurisé frontal par défaut	OUI
Profil dorsal par défaut	NON
Profil défini par l'utilisateur	NON

Activer EMS en utilisant l'interface graphique

1. Accédez à **Système > Profils > Profil SSL**.
2. Ajoutez un profil ou modifiez un profil.
3. Définissez **Autoriser le secret principal étendu** sur OUI.



Prise en charge du traitement de l'extension ALPN dans le message Hello du client

Remarque : Cette fonctionnalité est prise en charge dans la version 13.0 build 61.x et ultérieure.

Un paramètre `alpnProtocol` est ajouté aux profils SSL frontaux pour négocier le protocole d'application dans l'extension ALPN pour les connexions gérées par le serveur virtuel SSL_TCP. Seul le protocole spécifié dans le profil SSL est négocié, si le même protocole est reçu dans l'extension ALPN du message Hello client.

Remarque : Le paramètre `alpnProtocol` est pris en charge uniquement sur les profils SSL frontaux et s'applique aux connexions SSL gérées par des serveurs virtuels de type SSL_TCP.

Définissez le protocole dans le profil SSL frontal à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl profile ns_default_ssl_profile_frontend -alpnProtocol <protocol_name
>
```

Le paramètre `alpnProtocol` peut prendre trois valeurs. Longueur maximale : 4096 octets.

- **AUCUN :** La négociation du protocole d'application n'a pas lieu. il s'agit du réglage par défaut.
- **HTTP1 :** HTTP1 peut être négocié en tant que protocole d'application.
- **HTTP2 :** HTTP2 peut être négocié en tant que protocole d'application.

Exemple :

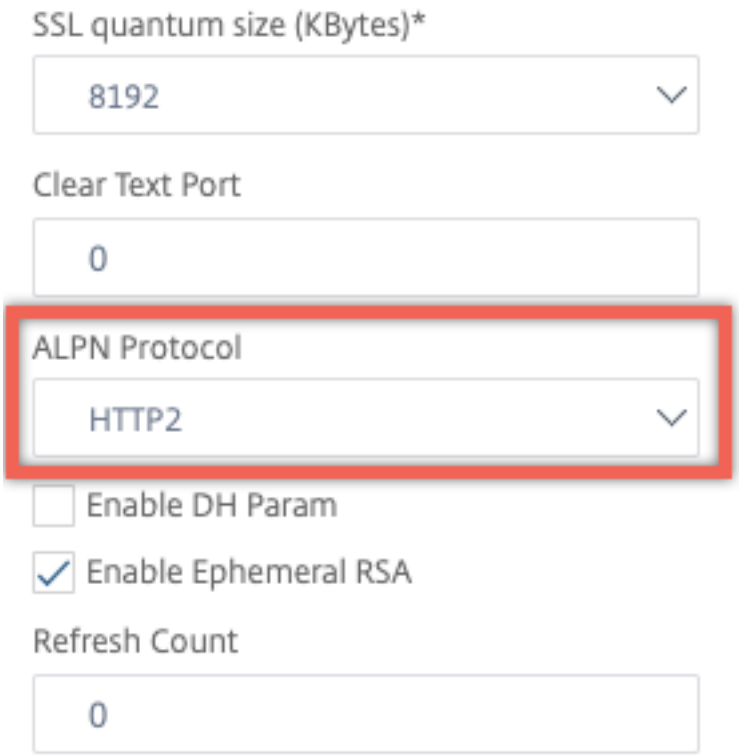
```
1  set ssl profile ns_default_ssl_profile_frontend -ALPNProtocol HTTP2
2  > sh ssl profile ns_default_ssl_profile_frontend
3  1)  Name: ns_default_ssl_profile_frontend   (Front-End)
4      SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
          ENABLED  TLSv1.3: DISABLED
5      Client Auth: DISABLED
6      Use only bound CA certificates: DISABLED
7      Strict CA checks:   NO
8      Session Reuse: ENABLED  Timeout: 120 seconds
9      DH: DISABLED
10     DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
          ENABLED  Refresh Count: 0
11     Deny SSL Renegotiation  ALL
12     Non FIPS Ciphers: DISABLED
13     Cipher Redirect: DISABLED
14     SSL Redirect: DISABLED
15     Send Close-Notify: YES
16     Strict Sig-Digest Check: DISABLED
17     Zero RTT Early Data: DISABLED
18     DHE Key Exchange With PSK: NO
19     Tickets Per Authentication Context: 1
20     Push Encryption Trigger: Always
21     PUSH encryption trigger timeout:    1 ms
22     SNI: DISABLED
23     OCSP Stapling: DISABLED
24     Strict Host Header check for SNI enabled SSL sessions:  NO
25     Match HTTP Host header with SNI:    CERT
26     Push flag:  0x0 (Auto)
27     SSL quantum size:   8 kB
28     Encryption trigger timeout  100 mS
29     Encryption trigger packet count:    45
30     Subject/Issuer Name Insertion Format:   Unicode
```



```
31
32      SSL Interception: DISABLED
33      SSL Interception OCSP Check: ENABLED
34      SSL Interception End to End Renegotiation: ENABLED
35      SSL Interception Maximum Reuse Sessions per Server: 10
36      Session Ticket: DISABLED
37      HSTS: DISABLED
38      HSTS IncludeSubDomains: NO
39      HSTS Max-Age: 0
40      HSTS Preload: NO
41      Allow Extended Master Secret: NO
42      Send ALPN Protocol: HTTP2
43
44   Done
45   <!--NeedCopy-->
```

Définissez le protocole dans le profil SSL frontal à l'aide de l'interface graphique

1. Accédez à **Système > Profils**, puis sélectionnez **Profil SSL**.
2. Sélectionnez **ns_default_ssl_profile_frontend** et cliquez sur **Modifier**.
3. Dans la liste **Protocole ALPN**, sélectionnez **HTTP2**.



Charger une ancienne configuration

L'activation des profils par défaut n'est pas réversible. Toutefois, si vous décidez que votre déploiement ne nécessite pas les profils par défaut, vous pouvez charger une ancienne configuration que vous avez enregistrée avant d'activer les profils par défaut. Les modifications entrent en vigueur après le redémarrage de l'appliance.

Charger une ancienne configuration en utilisant l'interface de ligne de commande

À l'invite de commande, tapez :

```
shell

root@ns# clear config

root@ns# cd /nsconfig

root@ns# cp ns.conf.NS.11.0.jun.16 ns.conf

root@ns# reboot
<!--NeedCopy-->
```

Profil frontal sécurisé

August 20, 2021

En plus d'un frontal par défaut et d'un profil principal par défaut, un nouveau profil frontal sécurisé par défaut est disponible à partir de la version 12.1. Les paramètres requis pour une note A+ (à partir de mai 2018) de Qualys SSL Labs sont préchargés dans ce profil. Auparavant, vous deviez définir explicitement chacun des paramètres requis pour une évaluation A+ sur un profil frontal SSL ou un serveur virtuel SSL. Vous pouvez maintenant lier le profil ns_default_ssl_profile_secure_frontend à votre serveur virtuel SSL et les paramètres requis sont automatiquement définis sur votre serveur virtuel SSL.

> **Remarque :**
>
> Le profil frontal sécurisé n'est pas modifiable.

Lorsque vous activez le profil par défaut, le profil frontal par défaut est automatiquement lié à tous les serveurs virtuels SSL. Pour obtenir une note A+, vous devez lier explicitement le profil ns_default_ssl_profile_secure_frontend et lier également un certificat de serveur SHA2/SHA256 à votre serveur virtuel SSL.

Paramètres sécurisés du profil frontal

Les paramètres avec leurs paramètres par défaut sont listés ici :

```
SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2: ENABLED
      TLSv1.3: DISABLED

Deny SSL Renegotiation: NONSECURE

HSTS: ENABLED

HSTS IncludeSubDomains: YES

HSTS Max-Age: 15552000

Cipher Name: SECURE    Priority :1
<!--NeedCopy-->
```

Secure cipher alias

Un nouvel alias de chiffrement sécurisé est ajouté et lié au profil frontal sécurisé. Pour répertorier les chiffrements qui font partie de cet alias, à l'invite de commandes, tapez : show cipher SECURE

```
show cipher SECURE

    1) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 1
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc030
    2) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 2
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128)
              Mac=AEAD   HexCode=0xc02f
    3) Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
       Priority : 3
           Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc02c
    4) Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
       Priority : 4
           Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128)
              Mac=AEAD   HexCode=0xc02b
Done
<!--NeedCopy-->
```


Configuration

Procédez comme suit :

1. Ajoutez un serveur virtuel d'équilibrage de charge de type SSL.
2. Liez un certificat SHA2/SHA256.
3. Activez le profil par défaut.
4. Liez le profil frontal sécurisé au serveur virtuel SSL.

Obtenez une note A+ pour un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add lb vserver <name> <serviceType> <IPAddress> <port>
bind ssl vserver <vServerName> -certkeyName <string>
set ssl parameter -defaultProfile ENABLED
set ssl vserver <vServerName> -sslProfile
   ns_default_ssl_profile_secure_frontend
show ssl vserver [<vServerName>]
<!--NeedCopy-->
```

Exemple :

```
add lb vserver ssl-vsvr SSL 192.0.2.240 443

bind ssl vserver ssl-vsvr -certkeyName letrsa

set ssl parameter -defaultProfile ENABLED

Save your configuration before enabling the Default profile. You cannot
    undo the changes. Are you sure you want to enable the Default
   profile? [Y/N]y

set ssl vserver ssl-vsvr -sslProfile
   ns_default_ssl_profile_secure_frontend
<!--NeedCopy-->
```

```
sh ssl vserver ssl-vsvr

    Advanced SSL configuration for VServer ssl-vsvr:
    Profile Name :ns_default_ssl_profile_secure_frontend
    1) CertKey Name: letrsa     Server Certificate
Done
<!--NeedCopy-->
```



```
sh ssl profile ns_default_ssl_profile_secure_frontend

    1) Name: ns_default_ssl_profile_secure_frontend (Front-End)
    SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:                  NO
    Session Reuse: ENABLED   Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED     Refresh Count: 0
    Deny SSL Renegotiation                NONSECURE
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:  1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:
                           NO
    Push flag:              0x0 (Auto)
    SSL quantum size:                8 kB
    Encryption trigger timeout       100 mS
    Encryption trigger packet count: 45
    Subject/Issuer Name Insertion Format:  Unicode
    SSL Interception: DISABLED
    SSL Interception OCSP Check: ENABLED
    SSL Interception End to End Renegotiation: ENABLED
    SSL Interception Maximum Reuse Sessions per Server:   10
    Session Ticket: DISABLED
    HSTS: ENABLED
    HSTS IncludeSubDomains: YES
    HSTS Max-Age: 15552000
    ECC Curve: P_256, P_384, P_224, P_521
    1) Cipher Name: SECURE    Priority :1
    Description: Predefined Cipher Alias
    1) Vserver Name: v2
```



```
42 Done
43 <!--NeedCopy-->
```

Obtenez une note A+ pour un serveur virtuel SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis sélectionnez un serveur virtuel SSL.
2. Dans Paramètres avancés, cliquez sur Profil SSL.
3. Sélectionnez ns_default_ssl_profile_secure_frontend.
4. Cliquez sur OK.
5. Cliquez sur Terminé.

Annexe A : exemple de migration de la configuration SSL après la mise à niveau

January 21, 2021

Remarque : Ce contenu a été supprimé car le script de migration SSL pour le nouveau profil par défaut n'est plus pris en charge.

Annexe B : paramètres de profil SSL front-end et back-end par défaut

January 21, 2021

Un profil frontal par défaut possède les paramètres suivants :

```
1  sh ssl profile ns_default_ssl_profile_frontend
2
3  1)Name: ns_default_ssl_profile_frontend
4
5       Configuration for Front-End SSL profile
6       DH: DISABLED
7       Ephemeral RSA: ENABLED          Refresh Count: 0
8       Session Reuse: ENABLED          Timeout: 120 seconds
9       Non FIPS Ciphers: DISABLED
10      Cipher Redirect: ENABLED   Redirect URL: http://10.102.28.212/
            redirect.html
11      Client Auth: DISABLED
12      SSL Redirect: DISABLED
```



```
13       SNI: DISABLED
14       SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
             ENABLED
15       Push Encryption Trigger: Always
16       PUSH encryption trigger timeout:     1 ms
17       Send Close-Notify: YES
18       Push flag: 0x0 (Auto)
19       Deny SSL Renegotiation          NO
20       SSL quantum size:          8 kB
21       Strict CA checks:          NO
22       Encryption trigger timeout 100 mS
23       Encryption trigger packet count:     45
24       Use only bound CA certificates: DISABLED
25       Subject/Issuer Name Insertion Format: Unicode
26       Strict Host Header check for SNI enabled SSL sessions:          NO
27
28       ECC Curve: P_256, P_384, P_521
29
30  1)   Cipher Name: AES     Priority :2
31       Description: Predefined Cipher Alias
32
33  1)   Vserver Name: v1
34  2)   Vserver Name: nshttps-::1l-443
35  3)   Vserver Name: nsrpcs-::1l-3008
36  4)   Vserver Name: nskrpcs-127.0.0.1-3009
37  5)   Vserver Name: nshttps-127.0.0.1-443
38  6)   Vserver Name: nsrpcs-127.0.0.1-3008
39  Done
40  <!--NeedCopy-->
```

Un profil principal par défaut possède les paramètres suivants :

```
1  sh ssl profile ns_default_ssl_profile_backend
2
3  1)Name: ns_default_ssl_profile_backend
4
5       Configuration for Back-End SSL profile
6       Session Reuse: ENABLED          Timeout: 300 seconds
7       Non FIPS Ciphers: DISABLED
8       Server Auth: DISABLED
9       SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED  TLSv1.2:
            DISABLED
10      Push Encryption Trigger: Always
11      PUSH encryption trigger timeout:     1 ms
12      Send Close-Notify: YES
```



```
      Push flag: 0x0 (Auto)
      Deny SSL Renegotiation          ALL
      SSL quantum size:          8 kB
      Strict CA checks:          NO
      Encryption trigger timeout 100 mS
      Encryption trigger packet count:     45
      Use only bound CA certificates: DISABLED

      ECC Curve: P_256, P_224, P_521

1)    Cipher Name: AES     Priority :1
      Description: Predefined Cipher Alias

2)    Cipher Name: RC4     Priority :2
      Description: Predefined Cipher Alias

1)    Service Name: s2
2)    Service Name: s1
Done
<!--NeedCopy-->
```

Profil SSL hérité

May 5, 2023

> **Remarque :**
>
> Citrix recommande d'utiliser les profils améliorés au lieu des profils hérités. Pour plus d'informations sur l'infrastructure de profils améliorée, voir Infrastructure de profils SSL.

Important :

> Liez un profil SSL à un serveur virtuel SSL. Ne liez pas un profil DTLS à un serveur virtuel SSL. Pour plus d'informations sur les profils DTLS, consultez Profils DTLS.

Vous pouvez utiliser un profil SSL pour spécifier la manière dont NetScaler traite le trafic SSL. Le profil est un ensemble de paramètres SSL pour les entités SSL, telles que les serveurs virtuels, les services et les groupes de services, et offre facilité de configuration et flexibilité. Vous n'êtes pas limité à la configuration d'un seul ensemble de paramètres globaux. Vous pouvez créer plusieurs ensembles (profils) de paramètres globaux et attribuer différents ensembles à différentes entités SSL. Les profils SSL sont classés en deux catégories :

- Profils frontaux, contenant les paramètres applicables à l'entité frontale. En d'autres termes, ils

s'appliquent à l'entité qui reçoit les demandes d'un client.

- Profils principaux, contenant les paramètres applicables à l'entité principale. En d'autres termes, ils s'appliquent à l'entité qui envoie les demandes des clients à un serveur.

Contrairement à un profil TCP ou HTTP, un profil SSL est facultatif. Il n'existe donc pas de profil SSL par défaut. Le même profil peut être réutilisé sur plusieurs entités. Si aucun profil n'est associé à une entité, les valeurs définies au niveau global s'appliquent. Pour les services appris de manière dynamique, les valeurs globales actuelles s'appliquent.

Le tableau suivant répertorie les paramètres qui font partie de chaque profil.

Profilé frontal	Profil principal
Redirection de chiffrement, URL de chiffrement	par Nysl Reneg
Port de texte clair*	Déclencheur de chiffrement PktCount
Authentification du client, certificat du client	Chiffres non FIPS
par Nysl Reneg	Gâchette PushEnc
dh, DHFichier, DHCount	Délai d'expiration du déclencheur PushEnc
DropReq sans en-tête d'hôte	Drapeau Push
Déclencheur de chiffrement PktCount	Taille quantique
Resa, Compte ERSA	Authentification du serveur
Codage d'insertion	Nom commun
Chiffres non FIPS	Réutilisation de ses, expiration du délai d'expiration de ses
Gâchette PushEnc	`SNIEnable`
Délai d'expiration du déclencheur PushEnc	ssl3
Drapeau Push	Délai d'expiration du déclencheur SSL
Taille quantique	Checks de cache stricts
Redirection et réécriture du port	tls1
Envoyer une notification de fermeture	-
Réutilisation de ses, expiration du délai d'expiration de ses	-
`SNIEnable`	-
ssl3	-
Redirection SSL	-

Profilé frontal	Profil principal
Délai d'expiration du déclencheur SSL	-
Checks de cache stricts	-
tls1, tls11, tls12	-

* Le paramètre ClearTextPort s'applique uniquement à un serveur virtuel SSL.

Un message d'erreur s'affiche si vous essayez de définir un paramètre qui ne fait pas partie du profil. Par exemple, si vous essayez de définir le paramètre ClientAuth dans un profil principal.

Certains paramètres SSL, tels que la taille de la mémoire CRL, la taille du cache OCSP, le contrôle UnDefaction et les données UnDefaction, ne font partie d'aucun des profils précédents, car ces paramètres sont indépendants des entités.

Un profil SSL prend en charge les opérations suivantes :

- Ajouter : crée un profil SSL sur NetScaler. Spécifiez si le profil est frontal ou dorsal. Le front-end est la valeur par défaut.
- Définir : modifie les paramètres d'un profil existant.
- Désactiver : définit les paramètres spécifiés à leurs valeurs par défaut. Si vous ne spécifiez aucun paramètre, un message d'erreur s'affiche. Si vous annulez la définition d'un profil sur une entité, le profil n'est pas lié à l'entité.
- Supprimer : supprime un profil. Un profil utilisé par une entité ne peut pas être supprimé. L'effacement de la configuration supprime toutes les entités. Par conséquent, les profils sont également supprimés.
- Afficher : affiche tous les profils disponibles sur NetScaler. Si un nom de profil est spécifié, les détails de ce profil sont affichés. Si une entité est spécifiée, les profils associés à cette entité sont affichés.

Création d'un profil SSL à l'aide de l'interface de ligne de commande

- Pour ajouter un profil SSL, tapez :

```
add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )]
<!--NeedCopy-->
```

- Pour modifier un profil existant, tapez :

```
set ssl profile <name>
<!--NeedCopy-->
```


- Pour annuler la définition d'un profil existant, tapez :

```
unset ssl profile <name> [-dh] [-dhFile] [-dhCount] [-eRSA] ...
<!--NeedCopy-->
```

- Pour annuler la définition d'un profil existant pour une entité, tapez :

```
unset ssl vserver <vServerName>  - sslProfile
<!--NeedCopy-->
```

- Pour supprimer un profil existant, tapez :

```
rm ssl profile <name>
<!--NeedCopy-->
```

- Pour afficher un profil existant, tapez :

```
sh ssl profile <name>
<!--NeedCopy-->
```

Création d'un profil SSL à l'aide de l'interface graphique

Accédez à **Système** > **Profils**, sélectionnez l'onglet Profils SSL et créez un profil SSL.

Permettre un contrôle plus strict de la validation des certificats clients

L'appliance NetScaler accepte les certificats d'autorité de certification intermédiaire valides si une seule autorité de certification racine les a émis. En d'autres termes, si seul le certificat Root-CA est lié au serveur virtuel et que Root-CA valide l'un des certificats intermédiaires envoyés avec le certificat client, l'appliance fait confiance à la chaîne de certificats et l'établissement de liaison est réussi.

Toutefois, si un client envoie une chaîne de certificats lors de la connexion, les certificats intermédiaires peuvent être validés à l'aide d'un répondeur CRL ou OCSP uniquement si ce certificat est lié au serveur virtuel SSL. Par conséquent, même si l'un des certificats intermédiaires est révoqué, la prise de contact est réussie. Dans le cadre de l'établissement de la liaison, le serveur virtuel SSL envoie la liste des certificats d'autorité de certification qui lui sont liés. Pour un contrôle plus strict, vous pouvez configurer le serveur virtuel SSL pour qu'il accepte uniquement un certificat signé par l'un des certificats CA liés à ce serveur virtuel. Pour ce faire, vous devez activer le `ClientAuthUseBoundCAChain` paramètre dans le profil SSL lié au serveur virtuel. La connexion échoue si l'un des certificats d'autorité de certification liés au serveur virtuel n'a pas signé le certificat client.

Par exemple, disons que deux certificats clients, clientcert1 et clientcert2, sont signés par les certificats intermédiaires int-CA-A et int-CA-B, respectivement. Les certificats intermédiaires sont signés

par le certificat racine Root-CA. Int-CA-A et Root-CA sont liés au serveur virtuel SSL. Dans le cas par défaut (ClientAuthUseBoundCachain désactivé), clientcert1 et clientcert2 sont acceptés. Toutefois, si ClientAuthUseBoundCachain est activé, l'appliance NetScaler accepte uniquement clientcert1.

Contrôle plus strict de la validation des certificats clients à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez : `set ssl profile <name> -ClientAuthUseBoundCAChain Enabled`

Permettre un contrôle plus strict sur la validation des certificats clients à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils**, sélectionnez l'onglet **Profils SSL** et créez un profil SSL ou sélectionnez un profil existant.
2. Sélectionnez **Activer l'authentification client à l'aide de la chaîne de certification liée**.

Listes de révocation des certificats

May 5, 2023

Un certificat émis par une autorité de certification reste généralement valide jusqu'à sa date d'expiration. Toutefois, dans certaines circonstances, l'autorité de certification peut révoquer le certificat émis avant la date d'expiration. Par exemple, lorsque la clé privée d'un propriétaire est compromise, le nom d'une entreprise ou d'un individu change, ou l'association entre le sujet et l'autorité de certification change.

Une liste de certificats révoqués (CRL) identifie les certificats non valides par numéro de série et émetteur.

Les autorités de certification émettent régulièrement des CRL. Vous pouvez configurer l'appliance NetScaler pour qu'elle utilise une CRL afin de bloquer les demandes des clients qui présentent des certificats non valides.

Si vous possédez déjà un fichier CRL provenant d'une autorité de certification, ajoutez-le à l'appliance NetScaler. Vous pouvez configurer les options d'actualisation. Vous pouvez également configurer NetScaler pour synchroniser automatiquement le fichier CRL à un intervalle spécifié, à partir d'un emplacement Web ou d'un emplacement LDAP. L'appliance prend en charge les CRL au format de fichier PEM ou DER. Assurez-vous de spécifier le format de fichier du fichier CRL ajouté à l'appliance NetScaler.

Si vous avez utilisé l'ADC en tant que CA pour créer des certificats utilisés dans des déploiements SSL, vous pouvez également créer une CRL pour révoquer un certificat particulier. Cette fonctionnalité peut être utilisée, par exemple, pour garantir que les certificats autosignés créés sur NetScaler ne sont utilisés ni dans un environnement de production ni au-delà d'une date donnée.

Remarque :

Par défaut, les CRL sont stockées dans le répertoire /var/netscaler/ssl de l'appliance NetScaler.

Création d'une CRL sur l'appliance ADC

Comme vous pouvez utiliser l'appliance ADC pour agir en tant qu'autorité de certification et créer des certificats autosignés, vous pouvez également révoquer les certificats suivants :

- Les certificats que vous avez créés.
- Certificats dont vous êtes propriétaire du certificat CA.

L'appliance doit révoquer les certificats non valides avant de créer une CRL pour ces certificats. L'appliance stocke les numéros de série des certificats révoqués dans un fichier d'index et met à jour le fichier chaque fois qu'elle révoque un certificat. Le fichier d'index est automatiquement créé la première fois qu'un certificat est révoqué.

Révoquer un certificat ou créer une CRL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-revoke <
   input_filename> | -genCRL <output_filename>)
<!--NeedCopy-->
```

Exemple :

```
create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -revoke Invalid-1

create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -genCRL CRL-1
<!--NeedCopy-->
```

Révoquer un certificat ou créer une CRL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL** et, dans le groupe Mise en route, sélectionnez Gestion des CRL.
2. Entrez les détails du certificat et, dans la liste **Choisir une opération**, sélectionnez **Révoquer le certificat**ou **Générer une CRL**.

Ajouter une CRL existante à l'ADC

Avant de configurer la CRL sur l'appliance NetScaler, assurez-vous que le fichier CRL est stocké localement sur l'appliance NetScaler. Dans une configuration HA, le fichier CRL doit être présent sur les deux appliances ADC et le chemin du répertoire vers le fichier doit être le même sur les deux appliances.

Ajouter une CRL sur NetScaler à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter une CRL sur NetScaler et vérifier la configuration :

```
add ssl crl <crlName> <crlPath> [-inform (DER | PEM)]

show ssl crl [<crlName>]
<!--NeedCopy-->
```

Exemple :

```
> add ssl crl crl-one /var/netscaler/ssl/CRL-one -inform PEM

Done

> show ssl crl crl-one

            Name: crl-one   Status: Valid,  Days to expiration: 29
            CRL Path: /var/netscaler/ssl/CRL-one
            Format: PEM     CAcert: samplecertkey
            Refresh: DISABLED
            Version: 1
            Signature Algorithm: sha1WithRSAEncryption
            Issuer:  C=US,ST=California,L=Santa Clara,O=NetScaler Inc.,
               OU=SSL Acceleration,CN=www.ns.com/emailAddress=
               support@NetScaler appliance.com
            Last_update:Jun 15 10:53:53 2010 GMT
            Next_update:Jul 15 10:53:53 2010 GMT

    1)      Serial Number: 00
            Revocation Date:Jun 15 10:51:16 2010 GMT
     Done
<!--NeedCopy-->
```

Ajouter une CRL sur NetScaler à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **SSL** > **CRL**, puis ajoutez une CRL.

Configurer les paramètres d'actualisation de la CRL

Une CRL est générée et publiée par une autorité de certification périodiquement ou, parfois, immédiatement après la révocation d'un certificat particulier. Citrix vous recommande de mettre régulièrement à jour les CRL sur l'appliance NetScaler, afin de vous protéger contre les clients qui tentent de se connecter avec des certificats non valides.

L'appliance NetScaler peut actualiser les CRL à partir d'un emplacement Web ou d'un annuaire LDAP. Lorsque vous spécifiez des paramètres d'actualisation et un emplacement Web ou un serveur LDAP, il n'est pas nécessaire que la CRL soit présente sur le disque dur local au moment de l'exécution de la commande. La première actualisation stocke une copie sur le disque dur local, dans le chemin spécifié par le paramètre Fichier CRL. Le chemin d'accès par défaut pour le stockage de la CRL est /var/netscaler/ssl.

Remarque : Dans les versions 10.0 et ultérieures, la méthode d'actualisation d'une CRL n'est pas incluse par défaut. Spécifiez une méthode HTTP ou LDAP. Si vous effectuez une mise à niveau d'une version antérieure vers la version 10.0 ou ultérieure, vous devez ajouter une méthode et exécuter à nouveau la commande.

Configurer l'actualisation automatique de la CRL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer l'actualisation automatique de la CRL et vérifier la configuration :

```
set ssl crl <crlName> [-refresh ( ENABLED | DISABLED )] [-CAcert <
    string>] [-server <ip_addr|ipv6_addr|*> | -url <URL>] [-method (
    HTTP | LDAP )] [-port <port>] [-baseDN <string>] [-scope ( Base |
    One )] [-interval <interval>] [-day <positive_integer>] [-time <HH:
    MM>][-bindDN <string>] {
 -password  }
  [-binary ( YES | NO )]

show ssl crl [<crlName>]
<!--NeedCopy-->
```

Exemple :

```
    set CRL crl1  -refresh enabled -method ldap -inform DER -CAcert ca1
        -server 10.102.192.192 -port 389 -scope base -baseDN "cn=
       clnt_rsa4_multicert_der,ou=eng,o=ns,c=in" -time 00:01

    set ssl crl crl1 -refresh enabled -method http -cacert ca1 -port 80
        -time 00:10 -url http://10.102.192.192/crl/ca1.crl

```



```
5
6       > sh crl
7
8       1)          Name: crl1        Status: Valid,     Days to expiration:
            355
9                    CRL Path: /var/netscaler/ssl/crl1
10                   Format: PEM      CAcert: ca1
11                   Refresh: ENABLED          Method: HTTP
12                   URL: http://10.102.192.192/crl/ca1.crl
                        Port:80
13                   Refresh Time: 00:10
14                   Last Update: Successful, Date:Tue Jul  6 14:38:13 2010
15      Done
16  <!--NeedCopy-->
```

Configurer l'actualisation automatique des CRL à l'aide de LDAP ou HTTP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > CRL.**
2. Ouvrez une CRL et sélectionnez **Activer l'actualisation automatique de la CRL.**

> **Remarque**
>
> Si la nouvelle CRL a été actualisée dans le référentiel externe avant son heure de mise à jour réelle, telle que spécifiée par le champ **Heure de la dernière mise à jour** de la CRL, vous devez procéder comme suit : Actualisez
>
> immédiatement la CRL sur l'appliance NetScaler.

Pour afficher l'heure de la dernière mise à jour, sélectionnez la CRL, puis cliquez sur **Détails**.

Synchroniser les CRL

L'appliance NetScaler utilise la dernière CRL distribuée pour empêcher les clients dont les certificats ont été révoqués d'accéder à des ressources sécurisées.

Si les CRL sont régulièrement mises à jour, l'appliance NetScaler a besoin d'un mécanisme automatique pour récupérer les dernières CRL du référentiel. Vous pouvez configurer l'appliance pour qu'elle mette à jour automatiquement les CRL à un intervalle d'actualisation spécifié.

L'appliance gère une liste interne des CRL qui doivent être mises à jour à intervalles réguliers. À ces intervalles spécifiés, l'appliance analyse la liste pour détecter les CRL qui doivent être mises à jour. Il se connecte ensuite au serveur LDAP ou HTTP distant, récupère les dernières CRL, puis met à jour la liste de CRL locale avec les nouvelles CRL.

> **Remarque :**
>
> Si la vérification de la CRL est définie sur obligatoire lorsque le certificat de l'autorité de certification est lié au serveur virtuel et que l'actualisation initiale de la CRL échoue, l'action suivante est entreprise pour les connexions :
>
> toutes les connexions d'authentification client ayant le même émetteur que la CRL sont rejetées comme RÉVOKED jusqu'à ce que la CRL soit correctement actualisée.

Vous pouvez spécifier l'intervalle auquel l'actualisation de la CRL doit être effectuée. Vous pouvez également spécifier l'heure exacte.

Synchroniser l'actualisation automatique des CRL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
set ssl crl <crlName> [-interval <interval>] [-day <integer>] [-time <
    HH:MM>]
<!--NeedCopy-->
```

Exemple :

```
set ssl crl CRL-1 -refresh ENABLE -interval MONTHLY -days 10 -time
    12:00
<!--NeedCopy-->
```

Synchroniser l'actualisation des CRL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > CRL.**
2. Ouvrez une CRL, sélectionnez **Activer l'actualisation automatique de la CRL**et spécifiez l'intervalle.

Procéder à l'authentification du client à l'aide d'une liste de révocation de certificats

Si une liste de révocation de certificats (CRL) est présente sur une appliance NetScaler, une vérification de la CRL est effectuée, que l'exécution de la vérification de la CRL soit définie comme obligatoire ou facultative.

Le succès ou l'échec d'une poignée de mains dépend de la combinaison des facteurs suivants :

- Règle de vérification de la CRL
- Règle de vérification des certificats clients
- État de la CRL configurée pour le certificat CA

Le tableau suivant répertorie les résultats des combinaisons possibles pour une poignée de mains impliquant un certificat révoqué.

Tableau 1. Résultat d'une prise de contact avec un client à l'aide d'un certificat révoqué

Règle pour la vérification des CRL	Règle de vérification des certificats clients	État de la CRL configurée pour le certificat CA	Résultat d'une poignée de main avec un certificat révoqué
Facultatif	Facultatif	Manquant	Succès
Facultatif	Obligatoire	Manquant	Succès
Facultatif	Obligatoire	Présent	Échec
Obligatoire	Facultatif	Manquant	Succès
Obligatoire	Obligatoire	Manquant	Échec
Obligatoire	Facultatif	Présent	Succès
Obligatoire	Obligatoire	Présent	Échec
Facultatif/Obligatoire	Facultatif	Expiré	Succès
Facultatif/Obligatoire	Obligatoire	Expiré	Échec

Remarque :

- La vérification de la CRL est facultative par défaut. Pour passer de facultatif à obligatoire ou inversement, vous devez d'abord dissocier le certificat du serveur virtuel SSL, puis le lier à nouveau après avoir modifié l'option.
- Dans la sortie de la `sh ssl vserver` commande, OCSP check : optional implique qu'une vérification CRL est également facultative. Les paramètres de contrôle CRL s'affichent dans la sortie de la `sh ssl vserver` commande uniquement si le contrôle CRL est défini sur obligatoire. Si la vérification CRL est définie comme facultative, les détails de la vérification CRL n'apparaissent pas.

Pour configurer la vérification CRL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
bind ssl vserver <vServerName> -certkeyName <string> [(-CA -crlCheck (
    Mandatory | Optional ))]
sh ssl vserver
<!--NeedCopy-->
```


Exemple :

```
bind ssl vs v1 -certkeyName ca -CA -crlCheck mandatory
> sh ssl vs v1

Advanced SSL configuration for VServer v1:

DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1
    .2: ENABLED
Push Encryption Trigger: Always
Send Close-Notify: YES

ECC Curve: P_256, P_384, P_224, P_521

1) CertKey Name: ca CA Certificate CRLCheck: Mandatory CA_Name Sent

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Configurer la vérification CRL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel SSL.
2. Cliquez dans la section **Certificats** .
3. Sélectionnez un certificat et, dans la liste de **contrôle OCSP et CRL**, sélectionnez **CRL**Obligatoire.

Résultat d'une prise de contact avec un certificat révoqué ou valide

Règle de vérification de la CRL	Règle de vérification des certificats clients	État de la CRL configurée pour le certificat CA	Résultat d'une poignée de main avec un certificat révoqué	Résultat d'une poignée de main avec un certificat valide
Obligatoire	Obligatoire	Présent	Échec	Succès
Obligatoire	Obligatoire	Expiré	Échec	Échec
Obligatoire	Obligatoire	Manquant	Échec	Échec
Obligatoire	Obligatoire	Indéfini	Échec	Échec
Facultatif	Obligatoire	Présent	Échec	Succès
Facultatif	Obligatoire	Expiré	Succès	Succès
Facultatif	Obligatoire	Manquant	Succès	Succès
Facultatif	Obligatoire	Indéfini	Succès	Succès
Obligatoire	Facultatif	Présent	Succès	Succès
Obligatoire	Facultatif	Expiré	Succès	Succès
Obligatoire	Facultatif	Manquant	Succès	Succès
Obligatoire	Facultatif	Indéfini	Succès	Succès
Facultatif	Facultatif	Présent	Succès	Succès
Facultatif	Facultatif	Expiré	Succès	Succès
Facultatif	Facultatif	Manquant	Succès	Succès
Facultatif	Facultatif	Indéfini	Succès	Succès

Surveiller l'état des certificats avec OCSP

May 5, 2023

Le protocole OCSP (Online Certificate Status Protocol) est un protocole Internet utilisé pour déterminer l'état d'un certificat SSL client. Les appliances NetScaler prennent en charge l'OCSP tel que défini dans la RFC 2560. OCSP offre des avantages significatifs par rapport aux listes de révocation de certificats (CRL) en termes d'informations en temps opportun. Le statut de révocation à jour d'un certificat client est particulièrement utile dans les transactions impliquant des sommes d'argent importantes et des transactions boursières de grande valeur. Il utilise également moins de ressources système et réseau. L'implémentation d'OCSP par NetScaler inclut le traitement par lots des deman-

des et la mise en cache des réponses.

Mise en œuvre de l'OCSP

La validation OCSP sur une appliance NetScaler commence lorsque l'appliance reçoit un certificat client lors d'une connexion SSL. Pour valider le certificat, l'appliance crée une demande OCSP et la transmet au répondeur OCSP. Pour ce faire, l'appliance utilise une URL configurée localement. La transaction est suspendue jusqu'à ce que l'appliance évalue la réponse du serveur et détermine si elle doit autoriser ou rejeter la transaction. Si la réponse du serveur est retardée au-delà de la durée configurée et qu'aucun autre répondeur n'est configuré, l'appliance autorise la transaction ou affiche une erreur, selon que le contrôle OCSP a été défini comme facultatif ou obligatoire, respectivement.

L'appliance prend en charge le traitement par lots des demandes OCSP et la mise en cache des réponses OCSP afin de réduire la charge sur le répondeur OCSP et de fournir des réponses plus rapides.

traitement par lots de demandes OCSP

Chaque fois que l'appliance reçoit un certificat client, elle envoie une demande au répondeur OCSP. Pour éviter de surcharger le répondeur OCSP, l'appliance peut demander l'état de plusieurs certificats clients dans la même demande. Pour que cette fonctionnalité fonctionne efficacement, un délai d'attente doit être défini afin que le traitement d'un seul certificat ne soit pas trop retardé pendant l'attente de la création d'un lot.

Mise en cache des réponses OCSP

La mise en cache des réponses reçues du répondeur OCSP permet de répondre plus rapidement aux clients et de réduire la charge sur le répondeur OCSP. Dès réception de l'état de révocation d'un certificat client de la part du répondeur OCSP, l'appliance met la réponse en cache localement pendant une durée prédéfinie. Lorsqu'un certificat client est reçu lors d'une connexion SSL, l'appliance vérifie d'abord dans son cache local la présence d'une entrée pour ce certificat. Si une entrée est trouvée qui est toujours valide (dans le délai d'expiration du cache), elle est évaluée et le certificat client est accepté ou rejeté. Si aucun certificat n'est trouvé, l'appliance envoie une demande au répondeur OCSP et stocke la réponse dans son cache local pendant une durée configurée.

> **Remarque** : À partir de la version 12.1 build 49.x, la limite du délai d'expiration du cache est désormais portée à un maximum de 43 200 minutes (30 jours). Auparavant, la limite était de 1440 minutes (un jour). L'augmentation de la limite permet de réduire les recherches sur le serveur OCSP et d'éviter tout échec de connexion SSL/TLS au cas où le serveur OCSP ne serait pas accessible en raison de problèmes de réseau ou autres.

Configuration du répondeur OCSP

La configuration d'OCSP implique d'ajouter un répondeur OCSP, de lier le répondeur OCSP à un certificat d'autorité de certification (CA) et de lier le certificat à un serveur virtuel SSL. Si vous devez lier un certificat différent à un répondeur OCSP déjà configuré, vous devez d'abord dissocier le répondeur, puis lier le répondeur à un autre certificat.

Ajouter un répondeur OCSP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer OCSP et vérifier la configuration :

```
add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED )
    [-cacheTimeout <positive_integer>]] [ -batchingDepth <
    positive_integer>][-batchingDelay <positive_integer>] [-resptimeout
    <positive_integer>] [-responderCert <string> | -trustResponder] [-
    producedAtTimeSkew <positive_integer>][-signingCert <string>][-
    useNonce ( YES | NO )][ -insertClientCert( YES | NO )]
<!--NeedCopy-->
```

```
bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]
<!--NeedCopy-->
```

```
bind ssl vserver <vServerName>@ (-certkeyName <string> ( CA [-ocspCheck
     ( Mandatory | Optional )]))
<!--NeedCopy-->
```

```
show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Exemple :

```
add ssl ocspResponder ocsp_responder1 -url "http:// www.myCA.org:80/
    ocsp/" -cache ENABLED -cacheTimeout 30 -batchingDepth 8 -
    batchingDelay 100 -resptimeout 100 -responderCert responder_cert -
    producedAtTimeSkew 300 -signingCert sign_cert  -insertClientCert YES
<!--NeedCopy-->
```

```
bind ssl certKey ca_cert -ocspResponder ocsp_responder1 -priority 1
<!--NeedCopy-->
```

```
bind ssl vserver vs1 -certkeyName ca_cert -CA -ocspCheck Mandatory
```



```
<!--NeedCopy-->
```

```
sh ocspResponder ocsp_responder1

    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done
<!--NeedCopy-->
```

```
show certkey ca_cert

    Name: ca_cert     Status: Valid,   Days to expiration:8907
    Version: 3
    …

    1)  VServer name: vs1      CA Certificate
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
Done
<!--NeedCopy-->
```

```
sh ssl vs vs1

    Advanced SSL configuration for VServer vs1:
    DH: DISABLED
    …

    1) CertKey Name: ca_cert CA Certificate OCSPCheck: Mandatory
    1) Cipher Name: DEFAULT
      Description: Predefined Cipher Alias
    Done
<!--NeedCopy-->
```


Modifier un répondeur OCSP à l'aide de l'interface de ligne de commande

Vous ne pouvez pas modifier le nom du répondeur. Tous les autres paramètres peuvent être modifiés à l'aide de la `set ssl ocspResponder` commande.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
    ] [-cacheTimeout <positive_integer>] [-batchingDepth <
    positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout
     <positive_integer>] [ -responderCert <string> | -trustResponder][-
    producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
    useNonce ( YES | NO )]

unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Configuration d'un répondeur OCSP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Répondeur OCSP**et configurez un répondeur OCSP.
2. Accédez à **Gestion du trafic** > **SSL** > **Certificats**, sélectionnez un certificat, puis dans la liste **Action**, sélectionnez **Liaisons OCSP**. Liez un répondeur OCSP.
3. Accédez à **Gestion du trafic** > **Équilibrage** de charge > **Serveurs virtuels**, ouvrez un serveur virtuel et cliquez dans la section Certificats pour lier un certificat d'autorité de certification.
4. Si vous le souhaitez, **sélectionnez « OCSP Obligatoire »**.

Agrafage OCSP

May 5, 2023

L'implémentation de CRL et OCSP par NetScaler indique uniquement l'état de révocation des certificats clients. Pour vérifier l'état de révocation d'un certificat de serveur reçu lors d'une poignée de main SSL, un client doit envoyer une demande à une autorité de certification.

Pour les sites Web à fort trafic, de nombreux clients reçoivent le même certificat de serveur. Si chaque

client envoyait une requête concernant l'état de révocation du certificat du serveur, l'autorité de certification serait inondée de demandes OCSP pour vérifier la validité du certificat.

Solution d'agrafage OCSP

Pour éviter tout encombrement inutile, l'appliance NetScaler prend désormais en charge l'agrafage OCSP. En d'autres termes, au moment de la négociation SSL, l'appliance peut désormais envoyer l'état d'un certificat de serveur à un client après avoir validé la réponse d'un répondeur OCSP. L'état d'un certificat de serveur est « agrafé » au certificat que l'appliance envoie au client dans le cadre de la négociation SSL. Pour utiliser la fonctionnalité d'agrafage OCSP, vous devez l'activer sur un serveur virtuel SSL et ajouter un répondeur OCSP sur l'appliance.

> Remarques
>
> - À partir de la version 13.1-30.x, tous les certificats intermédiaires incluent désormais l'extension de réponse OCSP lorsque les conditions suivantes sont remplies :
>
>   – TLS 1.3 protocol is used
>   – Client sends a status request
>
>   Auparavant, seul le certificat du serveur incluait cette extension dans la réponse à la demande d'état du client.
> - Avec les autres protocoles (y compris TLS 1.2), le serveur envoie la réponse OCSP uniquement pour le certificat du serveur. En d'autres termes, la RFC 6961 n'est pas prise en charge avec le protocole TLS 1.2.
> - Les appliances NetScaler prennent en charge l'agrafage OCSP tel que défini dans la RFC 6066.
> - L'agrafage OCSP est uniquement pris en charge sur le front-end des appliances NetScaler.
> - L'appliance ADC se comporte comme suit lorsque le protocole TLS 1.3 est utilisé : si la réponse OCSP mise en cache n'est pas valide (vide ou a expiré), une demande est envoyée au répondeur OCSP mais la négociation SSL est terminée sans attendre la réponse. Lorsque la réponse est reçue, elle est mise en cache et est disponible pour les futures demandes d'état des clients.
> - La prise en charge de l'agrafage OCSP par NetScaler est limitée aux prises de contact utilisant le protocole TLS version 1.0 ou supérieure.

Mise en cache des réponses OCSP des certificats de serveur

> Remarque
>
> À partir de la version 13.1-30.x, lorsque le protocole TLS 1.3 est utilisé, la réponse OCSP est mise

> en cache pour le certificat du serveur et tous les certificats intermédiaires.

Lors de la négociation SSL, lorsqu'un client demande l'état de révocation du certificat de serveur, l'appliance vérifie d'abord dans son cache local une entrée pour ce certificat. Si une entrée valide est trouvée, elle est évaluée et le certificat du serveur et son état sont présentés au client. Si aucune entrée d'état de révocation n'est trouvée, l'appliance envoie une demande d'état de révocation du certificat de serveur au répondeur OCSP. S'il reçoit une réponse, il envoie le certificat et l'état de révocation au client. Si le champ de mise à jour suivant est présent dans la réponse OCSP, la réponse est mise en cache pendant la durée configurée (valeur spécifiée dans le champ timeout).

> **Remarque** : À partir de la version 12.1 build 49.x, vous pouvez effacer la réponse mise en cache, du certificat du serveur, du répondeur OCSP avant même l'expiration du délai d'expiration. Auparavant, il n'était pas possible d'ignorer l'état mis en cache dans la paire de clés de certificat tant que le délai d'expiration configuré n'était pas écoulé.

Pour effacer l'état mis en cache à l'aide de l'interface de ligne de commande, à l'invite de commandes, tapez :

```
clear ssl certKey <certkey name> -ocspstaplingCache
<!--NeedCopy-->
```

Exemple :

```
clear ssl certKey s1 -ocspstaplingCache
<!--NeedCopy-->
```

Pour effacer l'état du cache à l'aide de l'interface graphique

1. Dans l'interface graphique, accédez à **Gestion du trafic** > **SSL** > **Certificats > Certificats** d'autorité de **certification**.
2. Dans le volet d'informations, sélectionnez un certificat.
3. Dans la liste **Sélectionner une action**, sélectionnez **Effacer**. Lorsque vous êtes invité à confirmer, cliquez sur **Oui**.

Configuration de l'agrafage OCSP

La configuration de l'agrafage OCSP implique l'activation de la fonctionnalité et la configuration OCSP. Pour configurer OCSP, vous devez ajouter un répondeur OCSP, lier le répondeur OCSP à un certificat d'autorité de certification et lier le certificat à un serveur virtuel SSL.

> **Remarque :**
>
> Les répondeurs OCSP avec uniquement une URL basée sur HTTP sont pris en charge.

Activer l'agrafage OCSP à l'aide de la CLI

À l'invite de commande, tapez :

```
set ssl vserver <name> -ocspstapling [ENABLED | DISABLED]
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver vip1 -ocspStapling ENABLED
Done

sh ssl vserver vip1

     Advanced SSL configuration for VServer vip1:
     DH: DISABLED
     DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA:
        ENABLED Refresh Count: 0
     Session Reuse: ENABLED Timeout: 120 seconds
     Cipher Redirect: DISABLED
     SSLv2 Redirect: DISABLED
     ClearText Port: 0
     Client Auth: DISABLED
     SSL Redirect: DISABLED
     Non FIPS Ciphers: DISABLED
     SNI: ENABLED
     OCSP Stapling: ENABLED
     SSLv2: DISABLED SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED
          TLSv1.2: ENABLED
     Push Encryption Trigger: Always
     Send Close-Notify: YES

     ECC Curve: P_256, P_384, P_224, P_521

    1) CertKey Name: server_certificate1 Server Certificate

    1) Cipher Name: DEFAULT
     Description: Default cipher list with encryption strength >= 128
        bit
Done
<!--NeedCopy-->
```

Remarque : Si le profil par défaut (amélioré) est activé, utilisez la `set ssl profile <profile name> -ocspStapling [ENABLED | DISABLED]` commande pour activer ou désactiver OCSP.

Activer l'agrafage OCSP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Serveur virtuel**.
2. Ouvrez un serveur virtuel et, dans **Paramètres SSL**, sélectionnez **Agrafage OCSP**.

Configuration OCSP

Un répondeur OCSP est ajouté dynamiquement ou manuellement pour envoyer des demandes d'agrafage OCSP. Un répondeur interne est ajouté dynamiquement lorsque vous ajoutez un certificat de serveur et son certificat d'émetteur en fonction de l'URL OCSP dans le certificat de serveur. Un répondeur OCSP manuel est ajouté à partir de la CLI ou de l'interface graphique. Pour envoyer une demande OCSP pour un certificat de serveur, l'appliance NetScaler sélectionne un répondeur OCSP en fonction de la priorité qui lui est attribuée lors de sa liaison à un certificat émetteur. Si un répondeur ne parvient pas à envoyer une demande d'agrafage OCSP, le répondeur ayant la priorité la plus élevée est sélectionné pour envoyer la demande. Par exemple, si un seul répondeur est configuré manuellement et qu'il échoue et qu'il existe un répondeur lié dynamiquement, il est sélectionné pour l'envoi de la demande OCSP.

Si l'URL OCSP est autre que HTTP, aucun répondeur OCSP interne n'est créé.

> **Remarque**
>
> Un répondeur OCSP ajouté manuellement a priorité sur un répondeur ajouté dynamiquement.

Différence entre un répondeur OCSP créé manuellement et un répondeur OCSP créé en interne

Répondeur OCSP créé manuellement	Répondeur OCSP créé en interne (dynamiquement)
Créé manuellement et explicitement lié au certificat de l'émetteur avec une priorité.	Créé et lié par défaut, lors de l'ajout d'un certificat de serveur et de son certificat d'émetteur (certificat d'autorité de certification). Le nom commence par « ns_internal_ ».
La priorité entre 1 et 127 est réservée à un répondeur configuré.	La priorité est automatiquement attribuée à partir de 128.
L'URL et la profondeur de traitement par lots peuvent être modifiées.	L'URL et la profondeur du lot ne peuvent pas être modifiées.

Supprimé directement.	Supprimé uniquement lorsque vous supprimez le certificat du serveur ou le certificat de l'autorité de certification.
Peut être lié à n'importe quel certificat d'autorité de certification.	Lié par défaut à un seul certificat d'autorité de certification. Ne peut être lié à aucun autre certificat d'autorité de certification.
Enregistré dans la configuration (ns.conf).	Les commandes d'ajout ne sont pas enregistrées dans la configuration. Seules les commandes d'ensemble sont enregistrées.
Si vous liez trois répondeurs OCSP au même certificat émetteur avec les priorités 1, 2 et 3 respectivement, et que vous dissociez ultérieurement la priorité 2, les autres priorités ne sont pas affectées.	Trois répondeurs OCSP sont automatiquement liés à un certificat d'émetteur avec les priorités 128, 129 et 130 respectivement. Si vous supprimez le certificat de serveur qui a été utilisé pour créer un répondeur lié avec la priorité 129, ce répondeur est supprimé. De plus, la priorité du répondeur suivant (priorité 130) passe automatiquement à 129.

Exemple de traitement des demandes :

1. Ajoutez un serveur virtuel (VIP1).
2. Ajoutez le certificat d'émetteur (CA1) et liez-le à VIP1.
3. Ajoutez trois certificats S1, S2 et S3. Les répondeurs internes resp1, resp2 et resp3 respectivement sont créés par défaut.
4. Liez S3 à VIP1.
5. Une demande est envoyée à VIP1. Responder resp3 est sélectionné.

Pour créer dynamiquement un répondeur OCSP interne, l'appliance a besoin des éléments suivants :

- Certificat de l'émetteur du certificat du serveur (généralement le certificat de l'autorité de certification).
- Paire de clés de certificat du certificat du serveur. Ce certificat doit contenir l'URL OCSP fournie par l'autorité de certification. L'URL est utilisée comme nom du répondeur interne ajouté dynamiquement.

Un répondeur OCSP interne possède les mêmes valeurs par défaut qu'un répondeur configuré manuellement.

> **Remarque :**
>
> La mise en cache est désactivée par défaut sur un répondeur interne. Utilisez la commande `set ssl ocspResponder` pour activer la mise en cache.

Configurer OCSP à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour configurer OCSP et vérifier la configuration :

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>] [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <positive_integer>]] [-bundle ( YES | NO )]

add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED ) [-cacheTimeout <positive_integer>]] [-resptimeout <positive_integer>] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew <positive_integer>][-signingCert <string>][-useNonce ( YES | NO )][-insertClientCert ( YES | NO )]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <positive_integer>]

show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Paramètres :

httpMethod:

Méthode HTTP utilisée pour envoyer des requêtes OCSP. Pour les demandes de moins de 255 octets, vous pouvez configurer la méthode HTTP GET pour les requêtes adressées à un serveur OCSP. Si vous spécifiez la méthode GET mais que la longueur est supérieure à 255 octets, l'appliance utilise la méthode par défaut (POST).

Valeurs possibles : GET, POST

Valeur par défaut : POST

ocspUrlResolveTimeout:

Durée, en millisecondes, d'attente d'une résolution d'URL OCSP. Passé ce délai, le répondeur ayant la priorité la plus élevée est sélectionné. Si tous les répondeurs échouent, un message d'erreur s'affiche ou la connexion est interrompue, selon les paramètres du serveur virtuel.

Valeur minimale : 100

Valeur maximale : 2000

Exemple :

```
add ssl certkey root_ca1  - cert root_cacert.pem
add ssl ocspResponder ocsp_responder1 -url "http:// www.myCA.org:80/
    ocsp/" -cache ENABLED -cacheTimeout 30  -resptimeout 100 -
    responderCert responder_cert -producedAtTimeSkew 300 -signingCert
    sign_cert  -insertClientCert YES
bind ssl certKey root_ca1 -ocspResponder ocsp_responder1 -priority 1
sh ocspResponder ocsp_responder1
    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done

show certkey root_ca1
    Name: root_ca1     Status: Valid,   Days to expiration:8907
    Version: 3
    …
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
    Done
<!--NeedCopy-->
```

Modifier OCSP à l'aide de la CLI

Vous ne pouvez pas modifier le nom d'un répondeur OCSP, mais vous pouvez utiliser la `set ssl ocspResponder` commande pour modifier n'importe quel autre paramètre.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
    ] [-cacheTimeout <positive_integer>]  [-resptimeout <
    positive_integer>] [ -responderCert <string> | -trustResponder][-
    producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
    useNonce ( YES | NO )]

```



```
unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Configurer OCSP à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Répondeur OCSP**et configurez un répondeur OCSP.
2. Accédez à **Gestion du trafic** > **SSL** > **Certificats**, sélectionnez un certificat, puis dans la liste **Action**, sélectionnez **Liaisons OCSP**. **Liez un répondeur OCSP**.
3. Accédez à **Gestion du trafic** > **Équilibrage** de charge > **Serveurs virtuels**, ouvrez un serveur virtuel et cliquez dans la section Certificats pour lier un certificat d'autorité de certification.
4. Le cas échéant, sélectionnez **OCSP obligatoire**.

> **Remarque :**
>
> Le paramètre d'insertion du certificat client dans `add ssl ocspResponder` et les commandes `set ssl ocspResponder` n'est plus valide. Autrement dit, le paramètre est ignoré lors de la configuration.

Chiffrements disponibles sur les appliances NetScaler

May 5, 2023

Votre appliance NetScaler est livrée avec un ensemble prédéfini de groupes de chiffrement. Pour utiliser des chiffrements qui ne font pas partie du groupe de chiffrement DEFAULT, vous devez les lier explicitement à un serveur virtuel SSL. Vous pouvez également créer un groupe de chiffrement défini par l'utilisateur pour lier au serveur virtuel SSL. Pour plus d'informations sur la création d'un groupe de chiffrement défini par l'utilisateur, voir Configurer des groupes de chiffrement définis par l'utilisateur sur l'appliance ADC.

> **Remarques**
>
> - Depuis la version 13.0 build 71.x et les versions ultérieures, l'accélération matérielle TLS1.3 est prise en charge sur les plates-formes suivantes :
>   - MPX 5900
>   - MPX/SDX 8900

- MPX/SDX 9100
- MPX/SDX 15000
- MPX/SDX 15000-50G
- MPX/SDX 16000
- MPX/SDX 26000
- MPX/SDX 26000-50S
- MPX/SDX 26000-100G

- La prise en charge logicielle uniquement du protocole TLSv1.3 est disponible sur toutes les autres appliances NetScaler MPX et SDX, à l'exception des appliances NetScaler FIPS.

- TLSv1.3 n'est pris en charge qu'avec le profil amélioré. Pour activer le profil amélioré, voir Activer le profil amélioré.
- Pour utiliser TLS1.3, vous devez utiliser un client conforme à la spécification RFC 8446.
- Le chiffrement RC4 n'est pas inclus dans le groupe de chiffrement par défaut de l'appliance NetScaler. Cependant, il est pris en charge dans le logiciel des appliances N3. Le chiffrement RC4, y compris la prise de contact, est effectué dans le logiciel.
- Citrix recommande de ne pas utiliser ce chiffrement car il est considéré comme non sécurisé et déconseillé par la RFC 7465.
- Utilisez la commande « show hardware » pour déterminer si votre appliance est équipée de puces N3.

```
sh hardware

Platform: NSMPX-22000 16\*CPU+24\*IX+12\*E1K+2\*E1K+4*CVM N3 2200100

Manufactured on: 8/19/2013

CPU: 2900MHZ

Host Id: 1006665862

Serial no: ENUK6298FT

Encoded serial no: ENUK6298FT
<!--NeedCopy-->
```

- Pour afficher des informations sur les suites de chiffrement liées par défaut au niveau du frontal (à un serveur virtuel), tapez : `sh cipher DEFAULT`
- Pour afficher des informations sur les suites de chiffrement liées par défaut au niveau du serveur principal (à un service), tapez : `sh cipher DEFAULT_BACKEND`
- Pour afficher des informations sur tous les groupes de chiffrement (alias) définis sur l'appliance,

tapez : `sh cipher`

- Pour afficher des informations sur toutes les suites de chiffrement qui font partie d'un groupe de chiffrement spécifique, tapez : `sh cipher <alias name>`. Par exemple, sh chiffre ECDHE.

Les liens suivants répertorient les suites de chiffrement prises en charge sur différentes plateformes NetScaler et sur les modules matériels de sécurité (HSM) externes :

- Appliance**NetScaler MPX/SDX Intel Lewisburg : prise en charge du chiffrement sur une appliance basée**sur unepuce SSL NetScaler MPX/SDX Intel Lewisburg
- Appliance**NetScaler MPX/SDX (N3) : prise en charge du chiffrement surune appliance**NetScaler MPX/SDX (N3)
- Appliance Intel Coleto**NetScaler MPX/SDX : prise en charge du chiffrement sur une appliance NetScaler MPX/SDX basée sur une puce SSLIntel Coleto**NetScaler MPX/SDX
- Appliance**NetScaler VPX : prise en charge du chiffrement surune appliance**NetScaler VPX
- Appliance**NetScaler MPX/SDX 14000 FIPS : prise en charge du chiffrementsur une appliance NetScaler MPX/SDX 14000 FIPS**
- **HSM externe (Thales/Safenet)** : chiffrement pris en charge sur un HSM externe (Thales/Safenet)
- Appliance**NetScaler MPX/SDX (N2) : prise en charge du chiffrement surune appliance**NetScaler MPX/SDX (N2)
- Appliance**NetScaler MPX 9700 FIPS : prise en charge du chiffrement sur un appareil**NetScalerMPX 9700 FIPS avec le firmware 2.2
- Appliances**NetScaler VPX FIPS et MPX FIPS : prise en charge du chiffrement surles appliances NetScaler VPX FIPS**et MPX FIPS

> **Remarque :**
>
> Pour la prise en charge du chiffrement DTLS, consultez la section Prise en charge du chiffrement DTLS sur les appliances NetScaler VPX, MPX et SDX.

Tableau1 - Prise en charge du serveur virtuel/service frontend interne :

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	** FIPS MPX/SDX 14000	MPX 5900/8900 MPX 15000-50 G MPX 26000-100 G
—	—	—	—	—	—
TLS 1.3	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	Non pris en charge	13.1 toutes les versions
	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	Non pris en charge	13.0 toutes les versions
	12,1—50,x (sauf TLS1.3-CHACHA20-POLY1305-SHA256)	12,1—50,x (sauf TLS1.3-CHACHA20-POLY1305-SHA256)	12.1–50.x	Non pris en charge	12.1–50.x
TLS 1.1/1.2	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions
	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions

	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12,0 à 57. x pour MPX 15000-50G, 12,0 à 60,x pour MPX 26000-100G
	11.1 all builds	11.1 all builds	11.1 all builds	11.1–56.x for MPX 5900/8900 and MPX 15000-50G, 11.1-60.x for MPX 26000-100G
	11.0 all builds	11.0 all builds	11.0 all builds	11.0 all builds	11.0–70.x (only on MPX 5900/8900)
	10.5 all builds	10.5 all builds	10.5–57.x	10.5–59.1359.e	10.5–67.x, 10.5-63.47 (only on MPX 5900/8900)
ECDHE/DHE (Example TLS1-ECDHE-RSA-AES128-SHA)	13.1 all builds	13.1 all builds	13.1 all builds	13.1 all builds	13.1 all builds
	13.0 all builds	13.0 all builds	13.0 all builds	13.0 all builds	13.0 all builds
	12.1 all builds	12.1 all builds	12.1 all builds	12.1 all builds	12.1 all builds for MPX 5900/8900, 12.1-50.x for MPX 15000-50G and MPX 26000-100G
	12.0 all builds	12.0 all builds	12.0 all builds	12.0 all builds	12.0 all builds for MPX 5900/8900, 12.0-57.x for MPX 15000-50G, 12.0-60.x for MPX 26000-100G
	11.1 all builds	11.1 all builds	11.1 all builds	11.1–51.x	11.1–56.x for MPX 5900/8900 and MPX 15000-50G, 11.1-60.x for MPX 26000-100G
	11.0 all builds	11.0 all builds	11.0 all builds		11.0–70.114 (only on MPX 5900/8900)
	10.5–53.x	10.5–53.x	10.5 all builds		10.5–67.x, 10.5-63.47 (only on MPX 5900/8900)
AES-GCM (Example TLS1.2-AES128-GCM-SHA256)	13.1 all builds	13.1 all builds	13.1 all builds	13.1 all builds	13.1 all builds
	13.0 all builds	13.0 all builds	13.0 all builds	13.0 all builds	13.0 all builds
	12.1 all builds	12.1 all builds	12.1 all builds	12.1 all builds	12.1 all builds for MPX 5900/8900, 12.1-50.x for MPX 15000-50G and MPX 26000-100G
	12.0 all builds	12.0 all builds	12.0 all builds	12.0 all builds	12.0 all builds for MPX 5900/8900, 12.0-57.x for MPX 15000-50G, 12.0-60.x for MPX 26000-100G
	11.1 all builds	11.1 all builds	11.1 all builds	11.1–51.x (See note)	11.1–56.x for MPX 5900/8900 and MPX 15000-50G, 11.1-60.x for MPX 26000-100G
	11.0 all builds	11.0 all builds	11.0–66.x		11.0–70.114 (only on MPX 5900/8900)
	10.5–53.x	10.5–53.x			10.5–67.x, 10.5-63.47 (only on MPX 5900/8900)
SHA-2 Ciphers (Example TLS1.2-AES-128-SHA256)	13.1 all builds	13.1 all builds	13.1 all builds	13.1 all builds	13.1 all builds
	13.0 all builds	13.0 all builds	13.0 all builds	13.0 all builds	13.0 all builds
	12.1 all builds	12.1 all builds	12.1 all builds	12.1 all builds	12.1 all builds for MPX 5900/8900, 12.1-50.x for MPX 15000-50G and MPX 26000-100G
	12.0 all builds	12.0 all builds	12.0 all builds	12.0 all builds	12.0 all builds for MPX 5900/8900, 12.0-57.x for MPX 15000-50G, 12.0-60.x for MPX 26000-100G

	11.1 all builds	11.1 all builds	11.1 all builds	11.1–52.x	11.1–56.x for MPX 5900/8900 and MPX 15000-50G, 11.1-60.x for MPX 26000-100G
	11.0 all builds	11.0 all builds	11.0–66.x		11.0–72.x, 11.0-70.114 (only on MPX 5900/8900)
	10.5–53.x	10.5–53.x			10.5–67.x, 10.5-63.47 (only on MPX 5900/8900)
ECDSA (Example TLS1-ECDHE-ECDSA-AES256-SHA)	Not supported	13.1 all builds	13.1 all builds	13.1 all builds	13.1 all builds
	Not supported	13.0 all builds	13.0 all builds	13.0 all builds	13.0 all builds
	Not supported	12.1 all builds	12.1 all builds	12.1 all builds	12.1 all builds for MPX 5900/8900, 12.1-50.x for MPX 15000-50G and MPX 26000-100G
	Not supported	12.0 all builds	12.0-57.x	Not supported	12.0 all builds for MPX 5900/8900, 12.0-57.x for MPX 15000-50G, 12.0-60.x for MPX 26000-100G
		11.1 all builds			11.1–56.x, 11.1-54.126 (Only ECC curves P_256 and P_384 are supported.)
CHACHA20	Not supported	13.1 all builds	13.1 all builds	Not supported	13.1 all builds
	Not supported	13.0 all builds	13.0 all builds	Not supported	13.0 all builds
	Not supported	Not supported	12.1 all builds	Not supported	12.1–49.x (only on MPX 5900/8900)
	Not supported	Not supported	12.0–56.x	Not supported	Not supported

Tableau 2 - Prise en charge des services dorsaux :

Le protocole TLS 1.3 n’est pas pris en charge sur le serveur principal.

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	** FIPS MPX/SDX 14000	MPX 5900/8900 MPX 15000-50 G MPX 26000-100 G
TLS 1.1/1.2	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions
	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	** FIPS MPX/SDX 14000	MPX 5900/8900 MPX 15000-50 G MPX 26000-100 G
	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12,0 à 57. x pour MPX 15000-50G, 12,0 à 60,x pour MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11.1 toutes les versions	11,1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11,1-60.x pour MPX 26000-100G
	11.0–50.x	11.0–50.x	11.0–66.x		11,0 à 70,119 (uniquement sur MPX 5900/8900)
	10.5–59.x	10.5–59.x		10.5–59.1359.e	10,5—67,x, 10,5-63,47 (uniquement sur MPX 5900/8900)
ECDHE/DHE (Exemple TLS1-ECDHE-RSA-AES128-SHA)	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	** FIPS MPX/SDX 14000	MPX 5900/8900 MPX 15000-50 G MPX 26000-100 G
	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	12.0–56.x	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12,0 à 57. x pour MPX 15000-50G, 12,0 à 60,x pour MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions		11.1–51.x	11,1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11,1-60.x pour MPX 26000-100G
	11.0–50.x	11.0–50.x			11,0 à 70,119 (uniquement sur MPX 5900/8900)

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	** FIPS MPX/SDX 14000	MPX 5900/8900 MPX 15000-50 G MPX 26000-100 G
	10.5–58.x	10.5–58.x			10,5—67,x, 10,5-63,47 (uniquement sur MPX 5900/8900)
AES-GCM (exemple TLS1.2-AES128-GCM-SHA256)	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions
	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	12.0 toutes les versions	12.0 toutes les versions	Non pris en charge	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12,0 à 57. x pour MPX 15000-50G, 12,0 à 60,x pour MPX 26000-100G

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	** FIPS MPX/SDX 14000	MPX 5900/8900 MPX 15000-50 G MPX 26000-100 G
	11.1 toutes les versions	11.1 toutes les versions		11.1–51.x	11,1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11,1-60.x pour MPX 26000-100G
Chiffrements SHA-2 (exemple TLS1.2-AES-128-SHA256)	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions
	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions
	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	** FIPS MPX/SDX 14000	MPX 5900/8900 MPX 15000-50 G MPX 26000-100 G
	12.0 toutes les versions	12.0 toutes les versions	Non pris en charge	12.0 toutes les versions	12.0 toutes les versions pour MPX 5900/8900, 12,0 à 57. x pour MPX 15000-50G, 12,0 à 60,x pour MPX 26000-100G
	11.1 toutes les versions	11.1 toutes les versions		11.1–52.x	11,1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11,1-60.x pour MPX 26000-100G
ECDSA (Exemple TLS1-ECDHE-ECDSA-AES256-SHA)	Non pris en charge	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions	13.1 toutes les versions
	Non pris en charge	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions	13.0 toutes les versions

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	** FIPS MPX/SDX 14000	MPX 5900/8900 MPX 15000-50 G MPX 26000-100 G
	Non pris en charge	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes les versions	12.1 toutes versions pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	Non pris en charge	12.0 toutes les versions	12.0–57.x	Non pris en charge	12.0 toutes les versions pour MPX 5900/8900, 12,0 à 57. x pour MPX 15000-50G, 12,0 à 60,x pour MPX 26000-100G
		11.1–51.x			11,1—56.x pour MPX 5900/8900 et MPX 15000-50G, 11,1-60.x pour MPX 26000-100G (seules les courbes CCE P_256 et P_384 sont prises en charge.)

Protocole/Plate-forme	MPX/SDX (N2)	MPX/SDX (N3)	VPX	** FIPS MPX/SDX 14000	MPX 5900/8900 MPX 15000-50 G MPX 26000-100 G
CHACHA20	Non pris en charge	13.1 toutes les versions	13.1 toutes les versions	Non pris en charge	13.1 toutes les versions
	Non pris en charge	13.0 toutes les versions	13.0 toutes les versions	Non pris en charge	13.0 toutes les versions
	Non pris en charge	Non pris en charge	12.1 toutes les versions	Non pris en charge	12.1–49.x pour MPX 5900/8900, 12.1-50.x pour MPX 15000-50G et MPX 26000-100G
	Non pris en charge	Non pris en charge	12.0–56.x	Non pris en charge	Non pris en charge

Pour obtenir la liste détaillée des chiffrements ECDSA pris en charge, voir Prise en charge des suites de chiffrement ECDSA.

> **Remarques**
>
> - La suite de chiffrement TLS-Fallback_Scsv est prise en charge sur tous les dispositifs à partir de la version 10.5 build 57.x
> - La prise en charge de HTTP Strict Transport Security (HSTS) est basée sur des règles.
> - Tous les certificats signés SHA-2 (SHA256, SHA384, SHA512) sont pris en charge sur le frontal de tous les matériels. Dans la version 11.1 build 54.x et ultérieures, ces certificats sont également pris en charge sur le back-end de tous les dispositifs. Dans les versions 11.0 et antérieures, seuls les certificats signés SHA256 sont pris en charge sur le back-end de tous les dispositifs.
> - Dans la version 11.1 build 52.x et antérieure, les chiffrements suivants ne sont pris en charge que sur l'avant des appliances MPX 9700 et MPX/SDX 14000 FIPS :
>   - TLS1.2-ECDHE-RSA-AES-256-SHA384
>   - TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 From release 11.1 build 53.x, and in release

12.0, these ciphers are also supported on the back end.

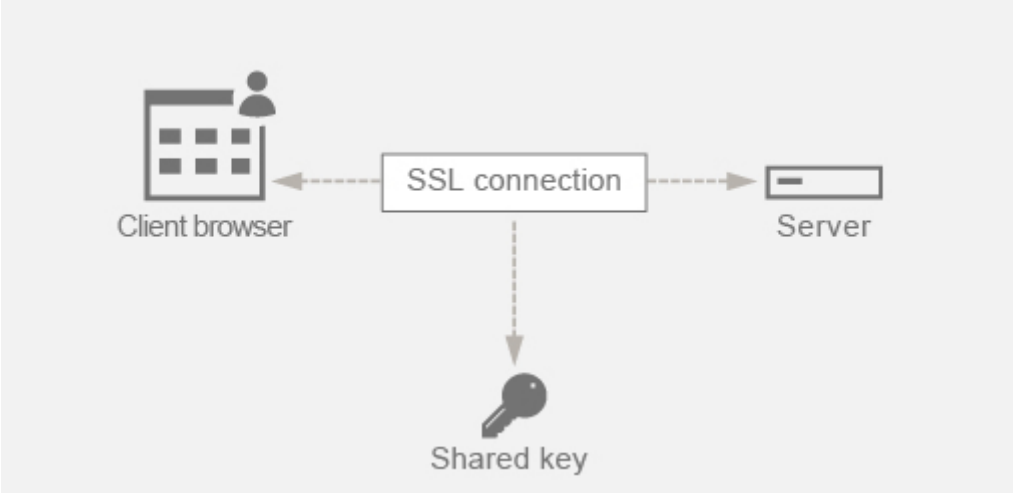
- Tous les chiffrements Chacha20-Poly1035 utilisent une fonction pseudo-aléatoire (PSF) TLS avec la fonction de hachage SHA-256.

Secret Perfect Forward (PFS)

Perfect Forward Secrecy garantit la protection des communications SSL actuelles même si la clé de session d'un serveur Web est compromise ultérieurement.

Pourquoi avez-vous besoin de Perfect Forward Secrecy (PFS) ?

Une connexion SSL est utilisée pour sécuriser les données transmises entre un client et un serveur. Cette connexion commence par la poignée de main SSL qui a lieu entre le navigateur d'un client et le serveur Web contacté. C'est au cours de cette poignée de contact que le navigateur et le serveur échangent certaines informations pour parvenir à une clé de session qui sert de moyen de chiffrer les données tout au long de la communication.

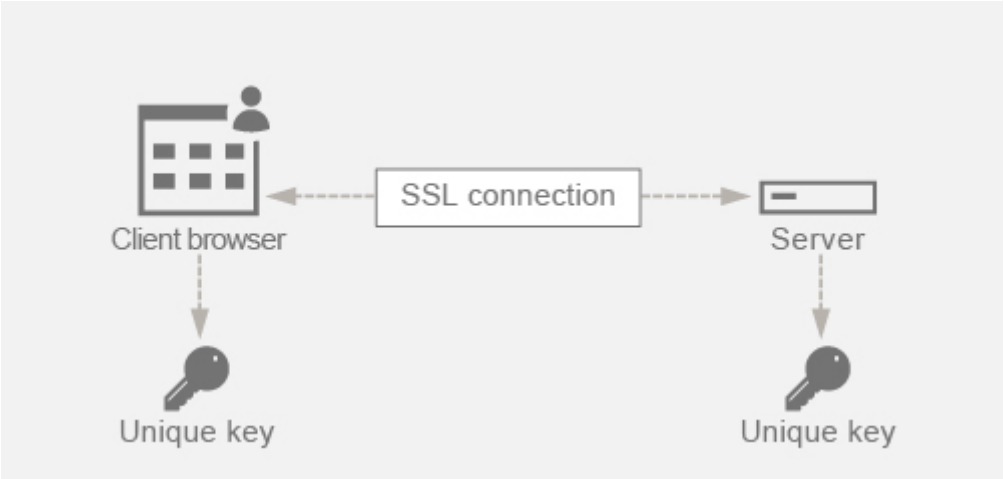


Le RSA est l'algorithme le plus couramment utilisé pour l'échange de clés. Le navigateur utilise la clé publique du serveur pour chiffrer et envoyer le secret pré-maître à un serveur. Ce secret pré-maître est utilisé pour arriver à la clé de session. Le problème de l'approche d'échange de clés RSA est que si un attaquant parvient à obtenir la clé privée du serveur à tout moment dans le futur, il obtient le secret pré-maître à l'aide duquel la clé de session peut être obtenue. Cette clé de session peut désormais être utilisée par l'attaquant pour déchiffrer toutes les conversations SSL. Par conséquent, votre communication SSL historique qui était sécurisée auparavant n'est plus sécurisée car la clé privée volée du serveur peut être utilisée pour atteindre la clé de session et ainsi décrypter également toute conversation historique enregistrée.

Le besoin est de pouvoir protéger les communications SSL passées même si la clé privée du serveur a été compromise. La configuration de Perfect Forward Secrecy (PFS) permet de résoudre ce problème.

Comment PFS aide-t-il ?

PFS protège la communication SSL passée en demandant au client et au serveur de convenir d'une nouvelle clé pour chaque session et en gardant secret le calcul de cette clé de session. Il fonctionne sur la base que la compromission d'une clé de serveur ne doit pas entraîner de compromis sur la clé de session. La clé de session est dérivée séparément aux deux extrémités et n'est jamais transférée sur le fil. Les clés de session sont également détruites une fois la communication terminée. Ces faits garantissent que même si quelqu'un accède à la clé privée du serveur, il ne sera pas en mesure d'accéder à la clé de session. Par conséquent, ils ne seraient pas en mesure de déchiffrer les données passées.



Explication avec exemple

Supposons que nous utilisons DHE pour atteindre le PFS. L'algorithme DH garantit que même si un pirate obtient la clé privée du serveur, il ne peut pas accéder à la clé de session. La raison en est que la clé de session et les nombres aléatoires (utilisés pour arriver à la clé de session) sont gardés secrets aux deux extrémités et ne sont jamais échangés sur le réseau.
PFS peut être atteint en utilisant l'échange de clés Diffie-Hellman éphémère qui crée de nouvelles clés temporaires pour chaque session SSL.

L'autre côté de la création d'une clé pour chaque session est qu'elle nécessite un calcul supplémentaire. Cependant, ce problème peut être résolu en utilisant la courbe elliptique dont les tailles de clé sont plus petites.

Configurer PFS sur l'appliance NetScaler

Le PFS peut être configuré sur un NetScaler en configurant des chiffrements DHE ou ECDHE. Ces chiffrements garantissent que la clé de session secrète créée n'est pas partagée sur le fil (algorithme DH) et que la clé de session ne reste vivante que pendant une courte période (éphémère). Les deux configurations sont expliquées dans les sections suivantes.

Remarque : L'utilisation de chiffrements ECDHE au lieu de DHE permet de sécuriser la communication avec des tailles de clés plus petites.

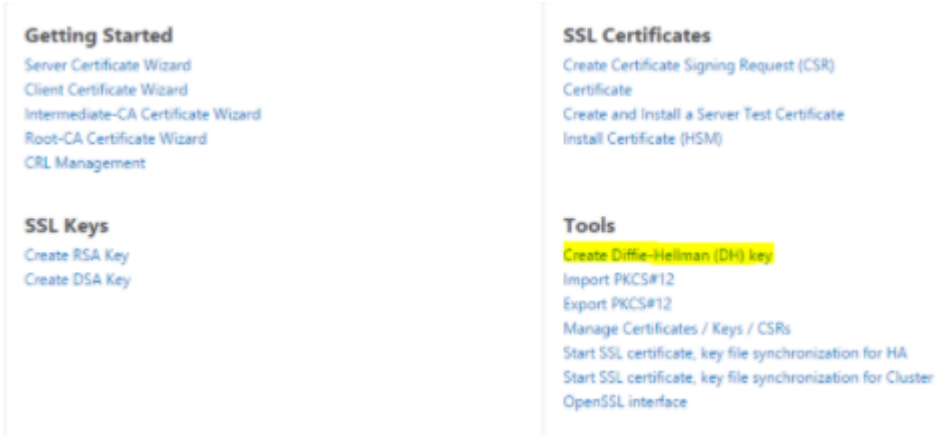
Configurer DHE à l'aide de l'interface graphique

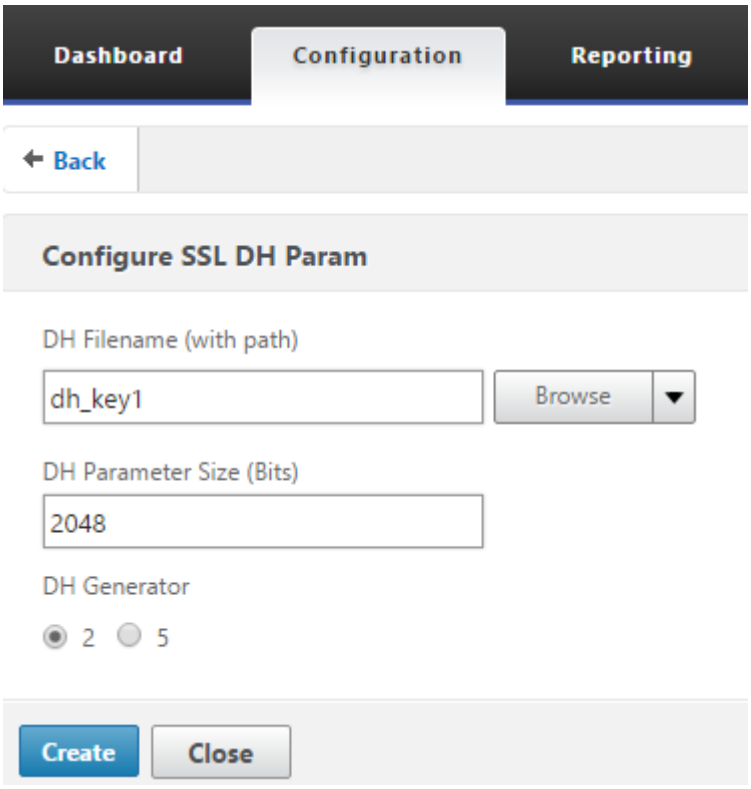
1. Générez une clé DH.

   a. Accédez à **Gestion du trafic > SSL > Outils**.

   b. Cliquez sur **Créer une clé DH (Diffie Helman)**.

   Remarque : La génération d'une clé DH de 2 048 bits peut prendre jusqu'à 30 minutes.



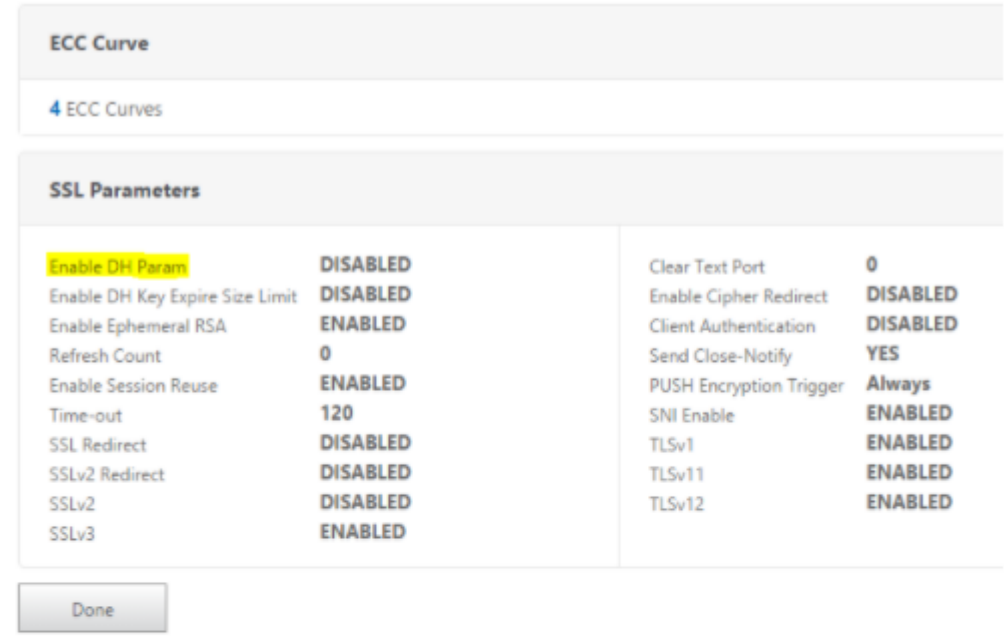


2. Activez DH Param pour le serveur virtuel SSL et attachez la clé DH au serveur virtuel SSL.

   a. Accédez à **Configuration > Gestion du trafic > Serveurs virtuels**.

   b. Sélectionnez le serveur virtuel sur lequel vous souhaitez activer DH.

   c. Cliquez sur **Modifier**, cliquez sur **Paramètres SSL**, puis sur **Activer le paramètre DH**.



3. Liez les chiffrements DHE au serveur virtuel.

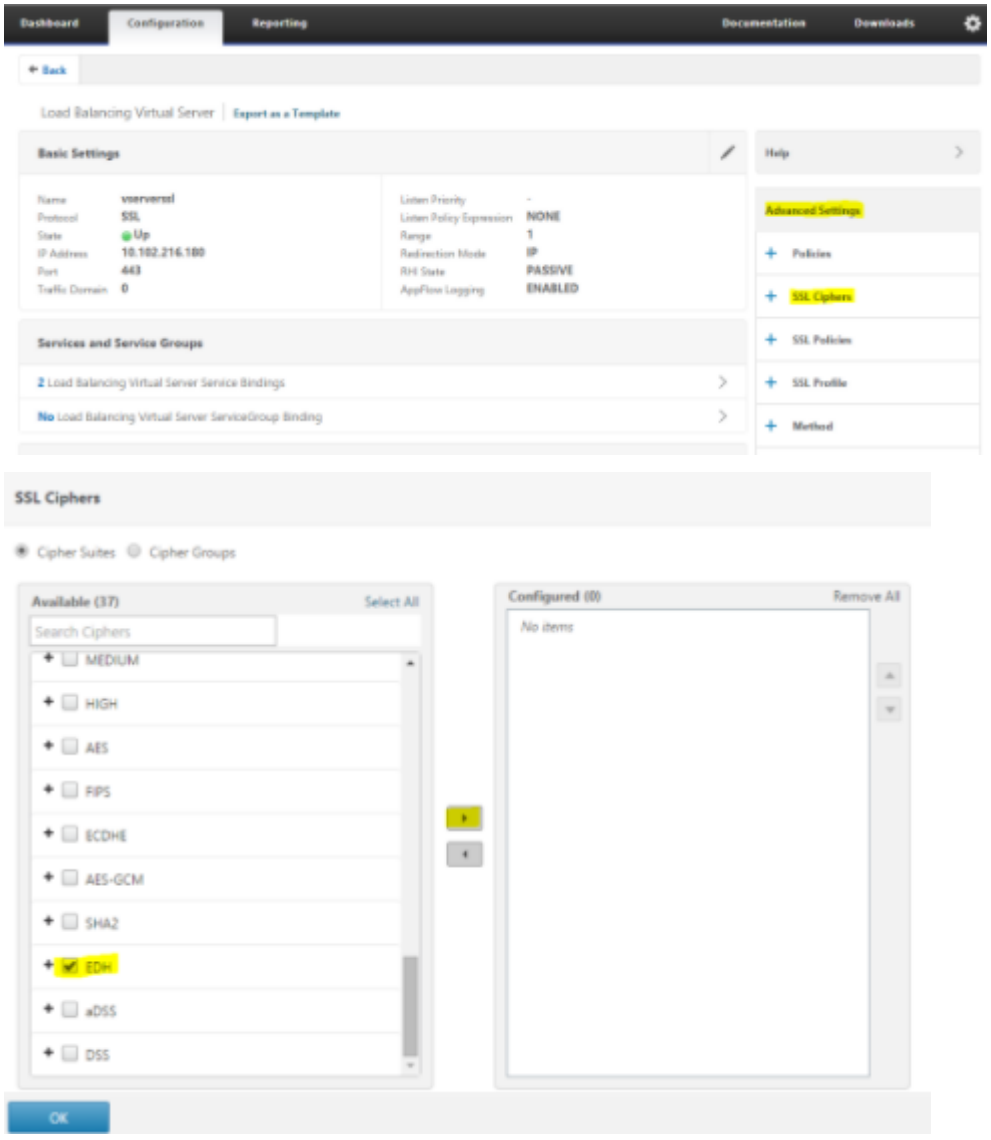
   a. Accédez à **Configuration > Gestion du trafic > Serveurs virtuels**.

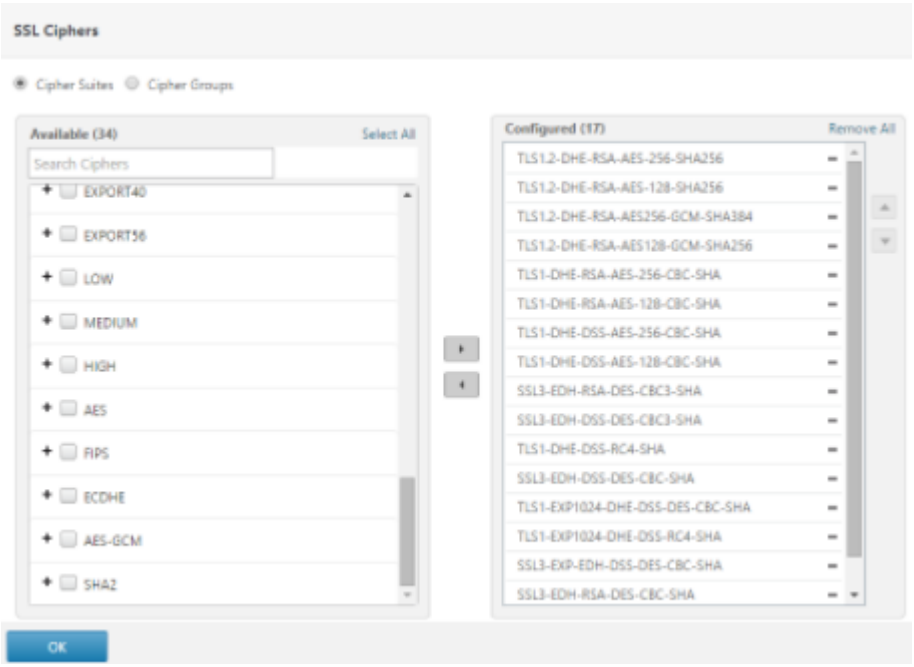
   b. Sélectionnez le serveur virtuel sur lequel vous souhaitez activer DH et cliquez sur l'icône

crayon pour le modifier.

c. Sous **Paramètres avancés**, cliquez sur l'icône plus en regard de **Chiffrements SSL**, sélectionnez les groupes de chiffrement DHE et cliquez sur **OK** pour lier.

Remarque : Assurez-vous que les chiffrements DHE se trouvent en haut de la liste des chiffrements liés au serveur virtuel.





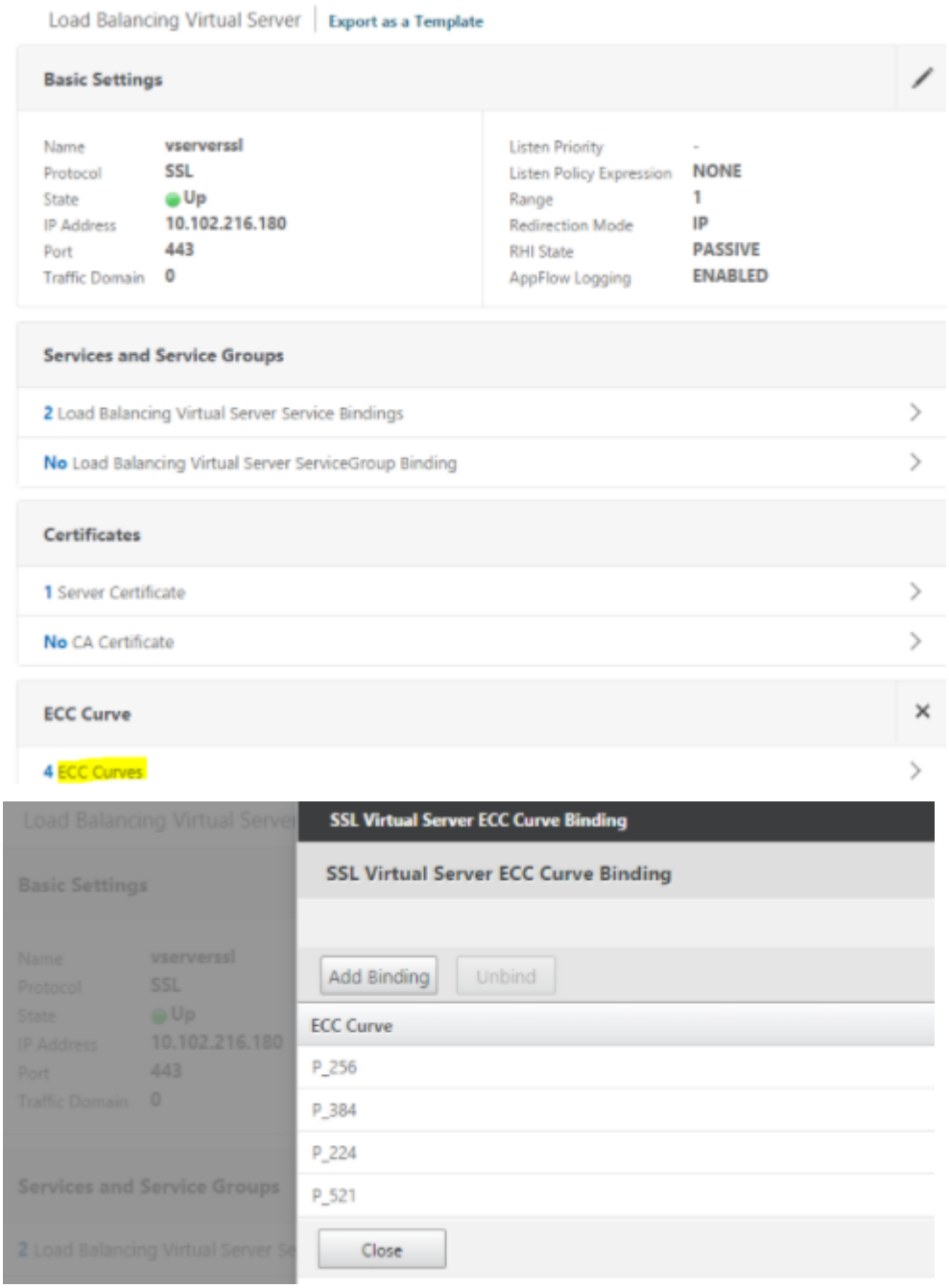
Configurer ECDHE à l'aide de l'interface graphique

1. Liez les courbes ECC au serveur virtuel SSL.

   a. Accédez à **Configuration > Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

   b. Sélectionnez le serveur virtuel SSL que vous souhaitez modifier, cliquez sur **Courbe ECC**, puis sur **Ajouter une liaison**.

   c. Liez la courbe ECC requise au serveur virtuel.

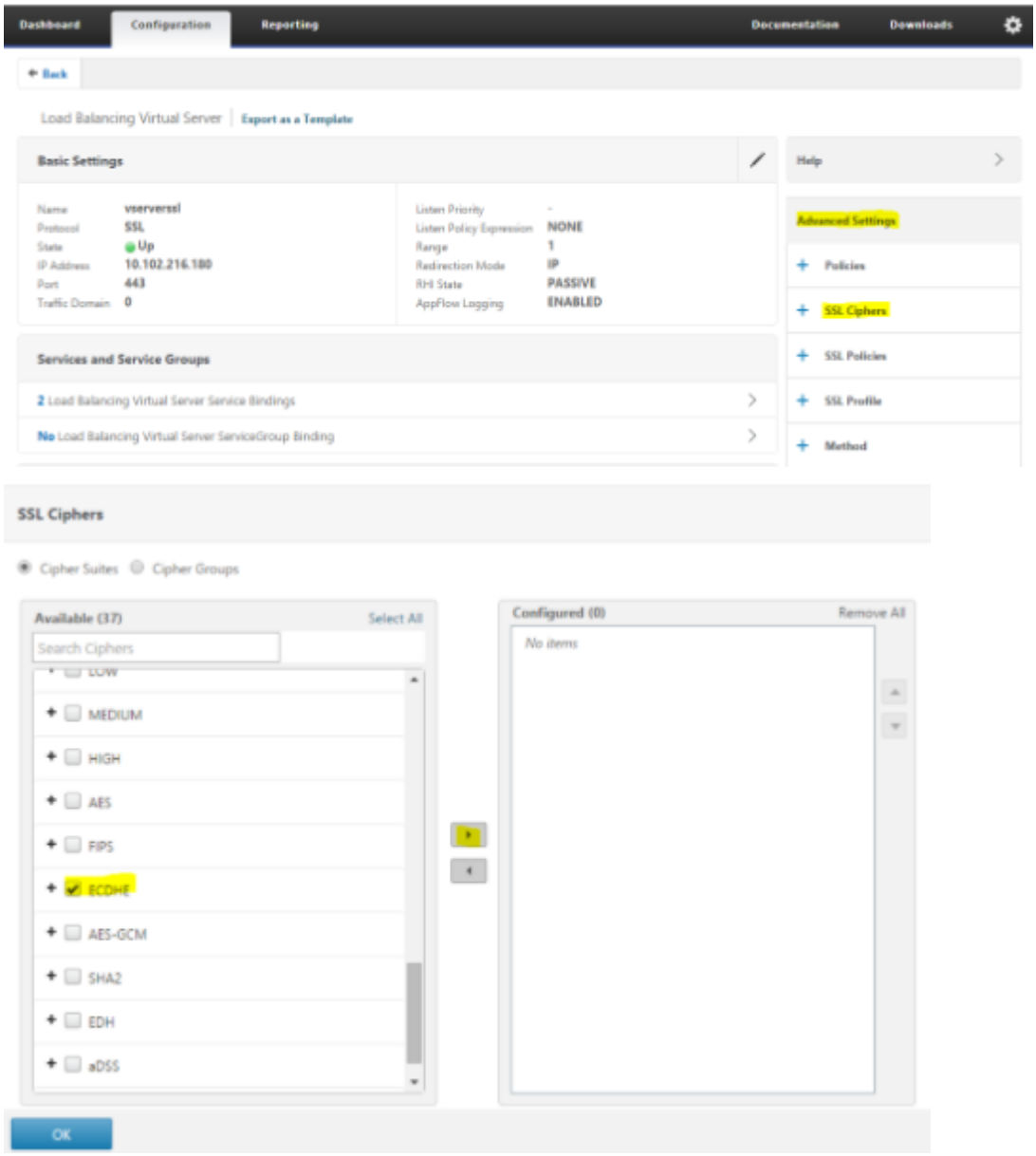


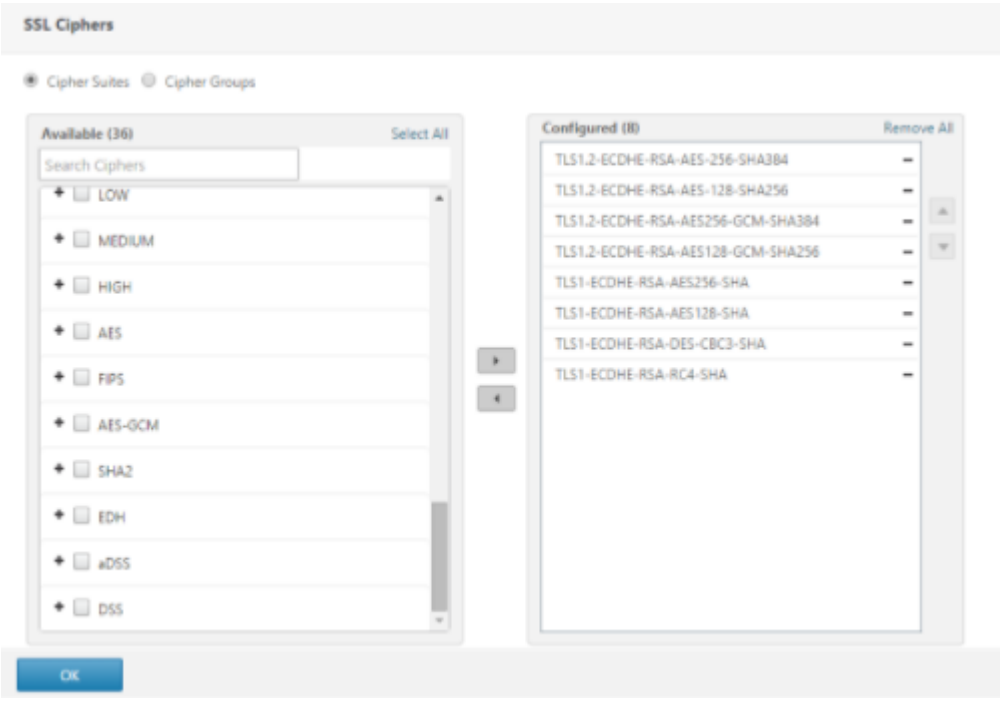
2. Liez les chiffrements ECDHE au serveur virtuel.

   a. Accédez à **Configuration > Gestion du trafic > Serveurs virtuels** et sélectionnez le serveur virtuel sur lequel vous souhaitez activer le DH.

   b. Cliquez sur **Modifier > Chiffrements SSL, sélectionnez les** groupes de chiffrement ECDHE, puis cliquez sur **Lier**.

   Remarque : Assurez-vous que les chiffrements ECDHE figurent en haut de la liste des chiffrements liés au serveur virtuel.





Remarque : Dans chaque cas, vérifiez que l'appliance NetScaler prend en charge les chiffrements que vous souhaitez utiliser pour la communication.

Configurer PFS à l'aide d'un profil SSL

Remarque : L'option permettant de configurer PFS (chiffrement ou ECC) à l'aide d'un profil SSL est introduite à partir de la version 11.0 64.x. Ignorez la section suivante si vous utilisez des versions antérieures.

Pour activer PFS à l'aide d'un profil SSL, une configuration similaire (comme expliqué dans les sections de configuration précédentes) doit être effectuée mais sur le profil SSL au lieu de la configurer directement sur un serveur virtuel.

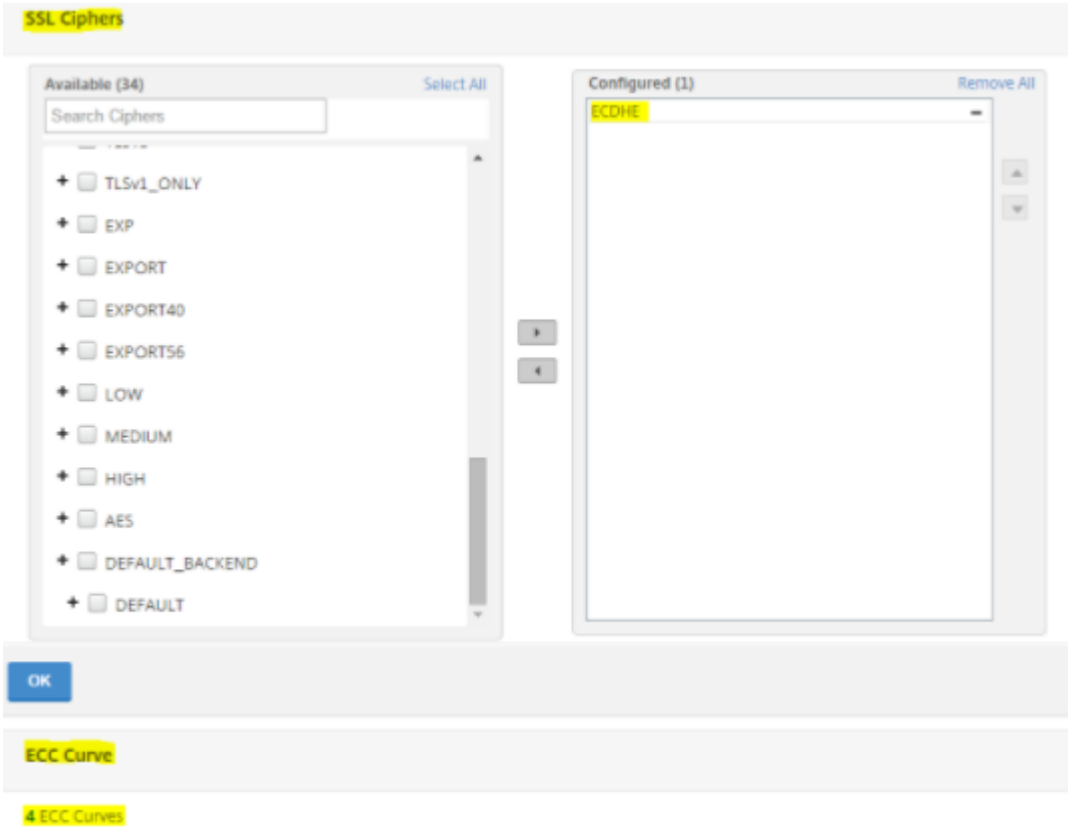
Configurer PFS à l'aide d'un profil SSL à l'aide de l'interface graphique

1. Liez les courbes ECC et les chiffrements ECDHE sur le profil SSL.

   Remarque : les courbes ECC sont déjà liées par défaut à tous les profils SSL.

   a. Accédez à **Système > Profils > Profils SSL** et choisissez le profil sur lequel vous souhaitez activer PFS.

   b. Liez les chiffrements ECDHE.



2. Liez le profil SSL au serveur virtuel.

   a. Accédez à **Configuration > Gestion du trafic > Serveurs virtuels** et sélectionnez le serveur virtuel.

   b. Cliquez sur l'icône crayon pour modifier le profil SSL.

   c. Cliquez sur **OK**, puis sur **Terminé**.

Configurer PFS avec SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

1. Liez les courbes ECC au profil SSL.

```
bind sslprofile <SSLProfileName> -eccCurveName <Name_of_curve>
<!--NeedCopy-->
```


2. Liez le groupe de chiffrement ECDHE.

```
bind sslprofile <SSLProfileName> cipherName <ciphergroupName>
<!--NeedCopy-->
```

3. Définissez la priorité du chiffrement ECDHE sur 1.

```
set sslprofile <SSLProfileName> cipherName <ciphergroupName>
   cipherPriority <positive_integer>
<!--NeedCopy-->
```

4. Liez le profil SSL au serveur virtuel.

```
set SSL vserver <vservername> sslProfile <SSLProfileName>
<!--NeedCopy-->
```

Chiffrements ECDHE

May 5, 2023

Toutes les appliances NetScaler prennent en charge le groupe de chiffrement ECDHE sur le front-end et le back-end. Sur une appliance SDX, si une puce SSL est attribuée à une instance VPX, la prise en charge du chiffrement d'une appliance MPX s'applique. Sinon, le support de chiffrement normal d'une instance VPX s'applique.

Pour plus d'informations sur les versions et les plateformes qui prennent en charge ces chiffrements, consultez la section Chiffrements disponibles sur les appliancesNetScaler.

Les suites de chiffrement ECDHE utilisent la cryptographie à courbe elliptique (ECC). En raison de la taille réduite de ses touches, l'ECC est particulièrement utile dans un environnement mobile (sans fil) ou un environnement de réponse vocale interactif, où chaque milliseconde est importante. Les touches plus petites permettent d'économiser de l'énergie, de la mémoire, de la bande passante et des coûts de calcul.

Une appliance NetScaler prend en charge les courbes ECC suivantes :

- P_256
- P_384
- P_224
- P_521

Remarque : Si vous effectuez une mise à niveau à partir d'une version antérieure à la version 10.1 build 121.10, vous devez lier explicitement les courbes ECC à vos serveurs et services virtuels SSL

existants. Les courbes sont liées par défaut à tous les serveurs et services virtuels que vous créez après la mise à niveau.

Vous pouvez lier une courbe ECC aux entités frontales et dorsales SSL. Par défaut, les quatre courbes sont liées, dans l'ordre suivant : P_256, P_384, P_224, P_521. Pour modifier l'ordre, vous devez d'abord dissocier toutes les courbes, puis les lier dans l'ordre souhaité.

Liez des courbes ECC à un serveur virtuel SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind ssl vserver <vServerName > -eccCurveName <eccCurveName >
```

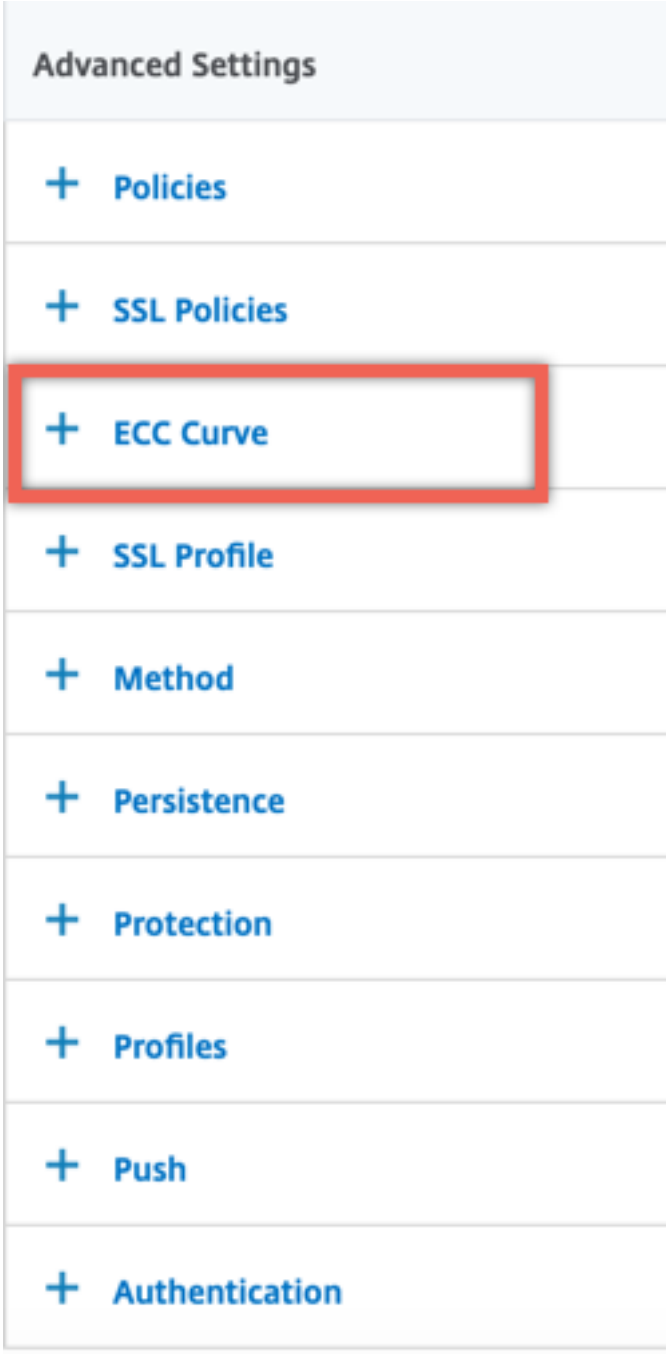
Exemple :

```
bind ssl vserver  v1 -eccCurveName P_224

sh ssl vserver v1

Advanced SSL configuration for VServer v1:
DH: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED
   TLSv1.2: DISABLED
Push Encryption Trigger: Always
Send Close-Notify: YES
ECC Curve: P_224

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

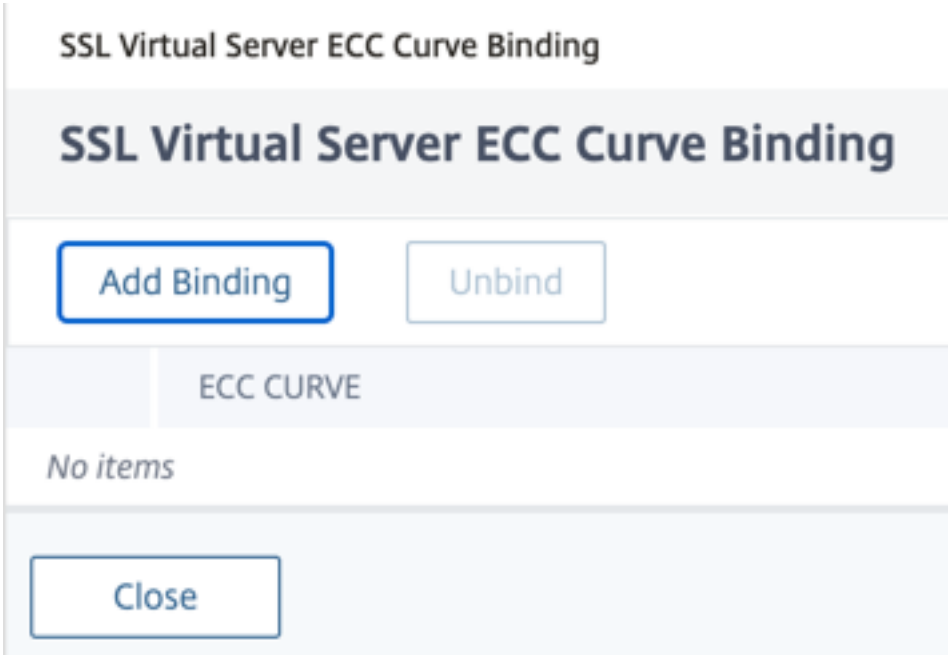
Liez des courbes ECC à un serveur virtuel SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

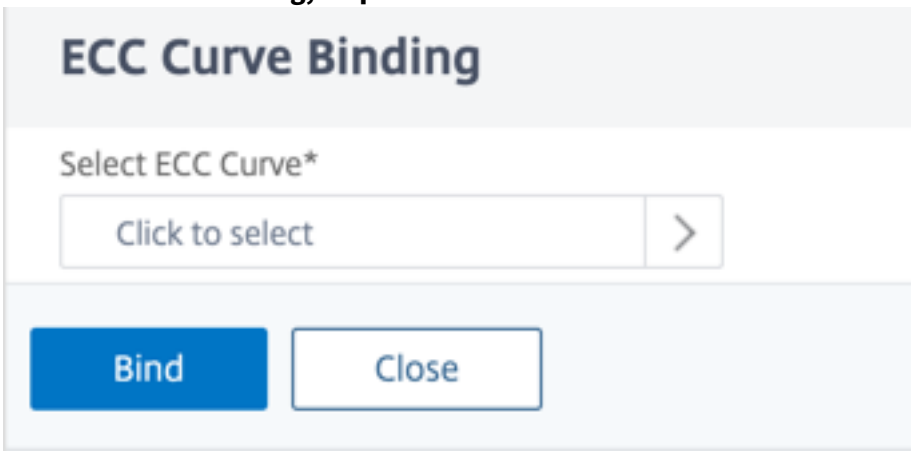
2. Sélectionnez un serveur virtuel SSL et cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, cliquez sur **Courbe ECC**.



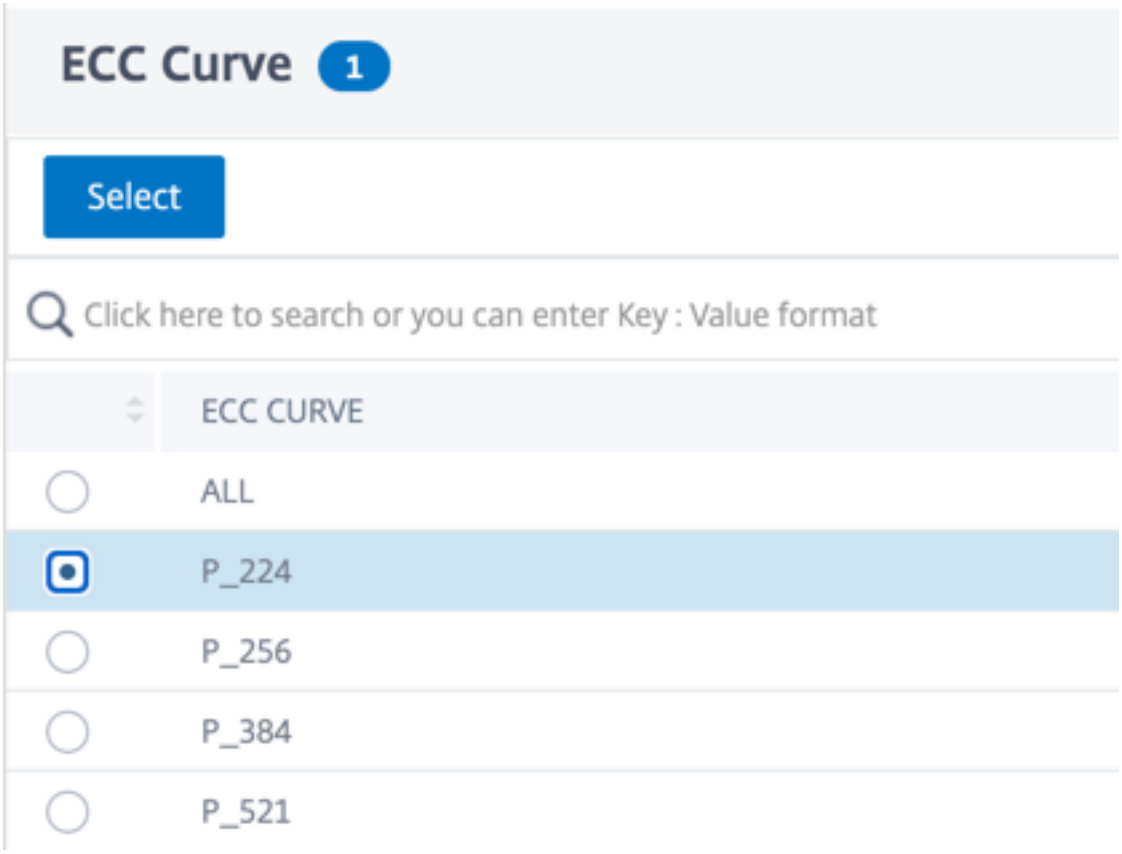
4. Cliquez à l'intérieur de la section de la courbe ECC.
5. Sur la page de **liaison ECC Curve du serveur virtuel SSL**, cliquez sur **Ajouter une liaison**.



6. Dans **ECC Curve Binding, cliquez sur Sélectionner une courbeECC**.



7. Sélectionnez une valeur, puis cliquez sur **Sélectionner**.



8. Cliquez sur **Bind**.
9. Cliquez sur **Fermer**.
10. Cliquez sur **Terminé**.

Liez des courbes ECC à un service SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind ssl service <vServerName > -eccCurveName <eccCurveName >
```

Exemple :

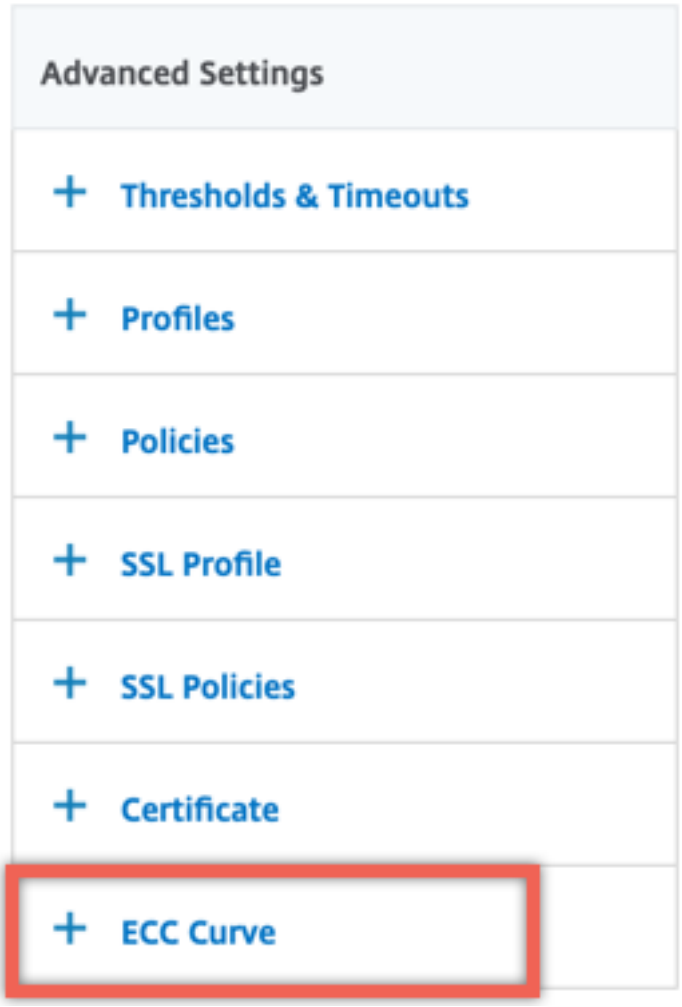
```
1  > bind ssl service sslsvc -eccCurveName P_224
2   Done
3  > sh ssl service sslsvc
4
5      Advanced SSL configuration for Back-end SSL Service sslsvc:
6      DH: DISABLED
7      DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
           DISABLED
8      Session Reuse: ENABLED      Timeout: 300 seconds
9      Cipher Redirect: DISABLED
10     ClearText Port: 0
```



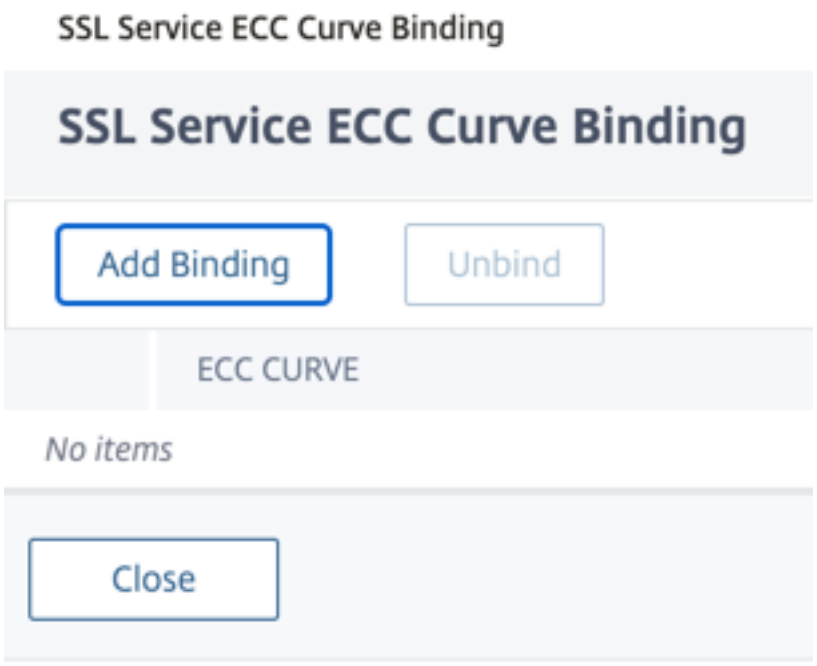
```
    Server Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: DISABLED
    OCSP Stapling: DISABLED
    SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: ???
    DHE Key Exchange With PSK: ???
    Tickets Per Authentication Context: ???

    ECC Curve: P_224


1)  Cipher Name: DEFAULT_BACKEND
    Description: Default cipher list for Backend SSL session
 Done
<!--NeedCopy-->
```

Liez des courbes ECC à un service SSL à l'aide de l'interface graphique

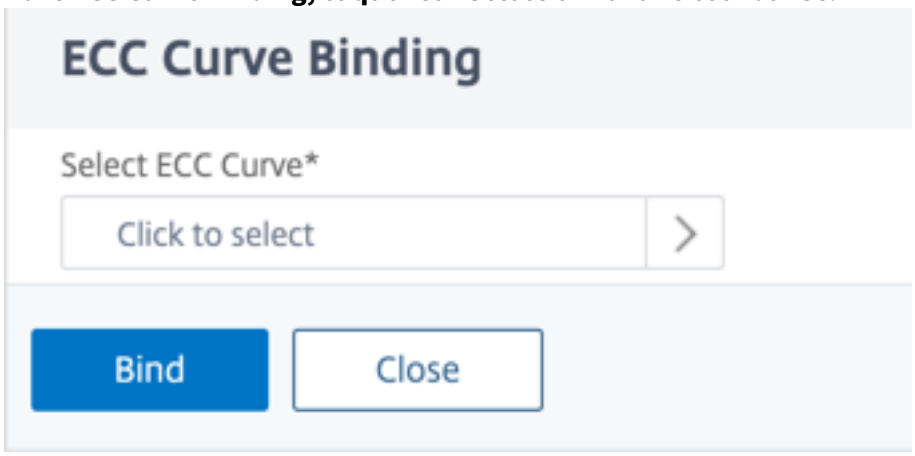
1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Sélectionnez un service SSL et cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, cliquez sur **Courbe ECC**.



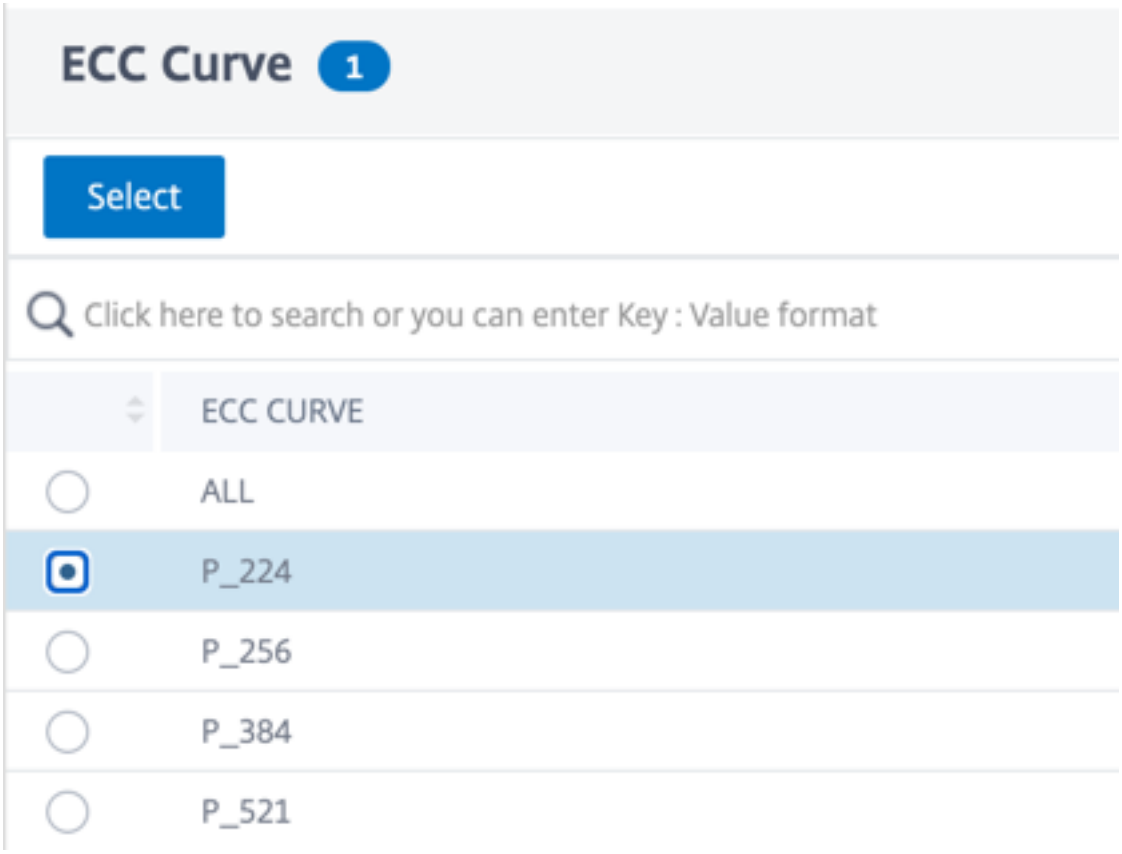
4. Cliquez à l'intérieur de la section de la courbe ECC.
5. Sur la page de **liaison ECC Curve du service SSL**, cliquez sur **Ajouter une liaison**.



6. Dans **ECC Curve Binding, cliquez sur Sélectionner une courbeECC**.



7. Sélectionnez une valeur, puis cliquez sur **Sélectionner**.



8. Cliquez sur **Bind**.
9. Cliquez sur **Fermer**.
10. Cliquez sur **Terminé**.

Génération de paramètres Diffie-Hellman et réalisation d'un PFS avec DHE

June 20, 2023

L'échange de clés Diffie-Hellman (DH) permet à deux parties impliquées dans une transaction SSL de se mettre d'accord sur un secret partagé via un canal non sécurisé. Ces parties n'ont aucune connaissance préalable l'une de l'autre. Ce secret peut être converti en matériel de clé cryptographique pour des algorithmes de chiffrement à clé symétrique nécessitant un tel échange de clés.

Cette fonction est désactivée par défaut. La fonctionnalité a été configurée pour prendre en charge les chiffrements qui utilisent DH comme algorithme d'échange de clés.

> **Remarque** :
>
> La génération de paramètres DH de 2048 bits peut prendre beaucoup de temps (jusqu'à 30 min-

> utes).

Générez des paramètres DH à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante :

```
create ssl dhparam <dhFile> [<bits>] [-gen (2 | 5)]
<!--NeedCopy-->
```

Exemple :

```
create ssl dhparam Key-DH-1 512 -gen 2
<!--NeedCopy-->
```

Générez des paramètres DH à l'aide de l'interface graphique

Accédez à **Gestion du trafic** > **SSL** et, dans le groupe **Outils**, sélectionnez **Créer une clé Diffie-Hellman (DH)**, puis **Configurer**le paramètre SSL DH.

> **Remarque :**
>
> Pour plus d'informations sur les paramètres DH, voir Paramètres Diffie-Hellman.

Obtenir un secret avant parfait avec DHE

La génération de paramètres DH est une opération gourmande en ressources du processeur. Dans les versions précédentes, la génération de paramètres, sur une appliance VPX, prenait beaucoup de temps car elle était effectuée dans le logiciel. La génération de paramètres est optimisée en définissant le `dhKeyExpSizeLimit` paramètre. Vous pouvez définir ce paramètre pour un serveur virtuel SSL ou un profil SSL, puis lier le profil à un serveur virtuel.

Vous pouvez maintenir le secret de transmission parfait (PFS) sur les appliances NetScaler MPX en définissant le nombre de DH sur zéro. Par conséquent, les paramètres DH sont générés pour chaque transaction (le minimum `DHcount` est de 0) sur les appliances NetScaler MPX. Ces paramètres sont générés sans baisse significative des performances, car le fonctionnement est optimisé. Auparavant, le nombre minimum de DH autorisé était de 500. En d'autres termes, vous ne pouvez pas régénérer la clé pour un maximum de 500 transactions.

> **Limitation :**
>
> Sur une appliance NetScaler VPX, si vous définissez le nombre de DH sur zéro, les paramètres DH ne sont pas régénérés. Par conséquent, vous devez définir le nombre de DH à 500 pour maintenir le PFS. Les paramètres DH sont régénérés après 500 transactions.

Optimisez la génération de paramètres DH à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes 1 et 2, ou tapez la commande 3 :

```
1. add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )] [-dhCount <positive_integer>] [-dh ( ENABLED | DISABLED) -dhFile <string>] [-dhKeyExpSizeLimit ( ENABLED | DISABLED)]
2. set ssl vserver <vServerName> [-sslProfile <string>]
<!--NeedCopy-->
```

```
3. set ssl vserver <vServerName> [-dh ( ENABLED | DISABLED) -dhFile <string>] [-dhCount <positive_integer>] [-dhKeyExpSizeLimit ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Optimisez la génération des paramètres DH à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer la limite de taille d'expiration de la clé DH**.

Redirection de chiffrement

August 20, 2021

Pendant la poignée de main SSL, le client SSL (généralement un navigateur Web) annonce la suite de chiffrements qu'il prend en charge, dans l'ordre de préférence de chiffrement configuré. À partir de cette liste, le serveur SSL sélectionne ensuite un chiffrement correspondant à sa propre liste de chiffrements configurés.

Si les chiffrements annoncés par le client ne correspondent pas aux chiffrements configurés sur le serveur SSL, la connexion SSL échoue. L'échec est annoncé par un message d'erreur cryptique affiché dans le navigateur. Ces messages mentionnent rarement la cause exacte de l'erreur.

Avec la redirection de chiffrement, vous pouvez configurer un serveur virtuel SSL pour fournir des messages d'erreur précis et significatifs en cas d'échec d'une connexion SSL. En cas d'échec d'une connexion SSL, l'appliance ADC redirige l'utilisateur vers une URL configurée précédemment ou, si aucune URL n'est configurée, affiche une page d'erreur générée en interne.

Configurer la redirection de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la redirection de chiffrement et vérifier la configuration :

```
1 -  set ssl vserver <vServerName> -cipherRedirect < ENABLED | DISABLED>
     -cipherURL < URL>
2 -  show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Exemple :

```
1  set ssl vserver vs-ssl -cipherRedirect ENABLED -cipherURL http://
       redirectURl
2
3  Done
4
5  show ssl vserver vs-ssl
6
7  Advanced SSL configuration for VServer vs-ssl:
8  DH: DISABLED
9  Ephemeral RSA: ENABLED          Refresh Count: 1000
10 Session Reuse: ENABLED          Timeout: 600 seconds
11 Cipher Redirect: ENABLED        Redirect URL: http://redirectURl
12 SSLv2 Redirect: DISABLED
13 ClearText Port: 0
14 Client Auth: DISABLED
15 SSL Redirect: DISABLED
16 Non FIPS Ciphers: DISABLED
17 SNI: DISABLED
18 OCSP Stapling: DISABLED
19 HSTS: DISABLED
20 HSTS IncludeSubDomains: NO
21 HSTS Max-Age: 0
22 SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2: ENABLED
       TLSv1.2: ENABLED
23     1)      CertKey Name: Auth-Cert-1       Server Certificate
24     1)      Cipher Name: DEFAULT
25             Description: Predefined Cipher Alias
26 Done
27 <!--NeedCopy-->
```


Configurer la redirection de chiffrement à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**et ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer la redirection de chiffrement** et spécifiez une URL de redirection.

Utiliser du matériel et des logiciels pour améliorer les performances de chiffrement ECDHE et ECDSA

May 5, 2023

> **Remarque :**
>
> Cette amélioration s'applique uniquement aux plateformes suivantes :
>
> - MPX/SDX 11000
> - MPX/SDX 14000
> - MPX 22000, MPX 24000 et MPX 25000
> - FIPS MPX/SDX 14000

Auparavant, les calculs ECDHE et ECDSA sur une appliance NetScaler étaient effectués uniquement sur le matériel (puces Cavium), ce qui limitait le nombre de sessions SSL à tout moment. Grâce à cette amélioration, certaines opérations sont également effectuées dans le logiciel. C'est-à-dire que le traitement est effectué à la fois sur les puces Cavium et sur les cœurs du processeur afin d'améliorer les performances de chiffrement ECDHE et ECDSA.

Le traitement est d'abord effectué dans le logiciel, jusqu'au seuil de chiffrement logiciel configuré. Une fois ce seuil atteint, les opérations sont transférées vers le matériel. Par conséquent, ce modèle hybride utilise à la fois du matériel et des logiciels pour améliorer les performances du protocole SSL. Vous pouvez activer le modèle hybride en définissant le paramètre « SoftwareCryptoThreshold » en fonction de vos besoins. Pour désactiver le modèle hybride, définissez ce paramètre sur 0.

Les avantages sont maximaux si l'utilisation actuelle du processeur n'est pas trop élevée, car le seuil du processeur n'est pas exclusif aux calculs ECDHE et ECDSA. Par exemple, si la charge de travail actuelle de l'appliance consomme 50 % des cycles du processeur et que le seuil est défini à 80 %, les calculs ECDHE et ECDSA ne peuvent en utiliser que 30 %. Une fois que le seuil de chiffrement logiciel configuré de 80 % est atteint, les calculs ECDHE et ECDSA supplémentaires sont transférés vers le matériel. Dans ce cas, l'utilisation réelle du processeur peut dépasser 80 %, car les calculs ECDHE et ECDSA sur le matériel consomment certains cycles du processeur.

Activez le modèle hybride à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl parameter -softwareCryptoThreshold <positive_integer>

Synopsis:

softwareCryptoThreshold:

NetScaler CPU utilization threshold (as a percentage) beyond which
   crypto operations are not done in software. A value of zero implies
   that CPU is not utilized for doing crypto in software.

Default = 0

Min = 0

Max = 100
<!--NeedCopy-->
```

Exemple :

```
set ssl parameter - softwareCryptoThreshold 80
Done

show ssl parameter
Advanced SSL Parameters

SSL quantum size                  : 8 KB
Max CRL memory size               : 256 MB
Strict CA checks                  : NO
Encryption trigger timeout        : 100 ms
Send Close-Notify                 : YES
Encryption trigger packet c       : 45
Deny SSL Renegotiation            : ALL
Subject/Issuer Name Insertion Format : Unicode
OCSP cache size                   : 10 MB
Push flag                         : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout   : 1 ms
Crypto Device Disable Limit       : 0
Global undef action for control policies : CLIENTAUTH
Global undef action for data policies : NOOP
Default profile                   : DISABLED
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors    : NO
```



```
Disable TLS 1.1/1.2 for dynamic and VPN services : NO
Software Crypto acceleration CPU Threshold : 80
Signature and Hash Algorithms supported by TLS1.2 : ALL
<!--NeedCopy-->
```

Activez le modèle hybride à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Modifier les paramètres SSL avancés**.
2. Entrez une valeur pour le **seuil de chiffrement logiciel (%)**.

Définir une alarme SNMP pour le taux de change ECDHE

L'échange de clés basé sur l'ECDHE peut entraîner une baisse des transactions par seconde sur l'appliance. À partir de la version 13.0 build 52.x, vous pouvez configurer une alarme SNMP pour les transactions basées sur ECDHE. Dans cette alarme, vous pouvez définir le seuil et les limites normales du taux de change ECDHE. Un nouveau compteur `nsssl_tot_sslInfo_ECDHE_Tx` est ajouté. Ce compteur est la somme de tous les compteurs de transactions basés sur l'ECDHE situés sur le front-end et le back-end de l'appliance. Lorsque l'échange de clés basé sur l'ECDHE dépasse les limites configurées, une interruption SNMP est envoyée. Un autre piège est envoyé lorsque la valeur revient à la valeur normale configurée.

Définissez une alarme SNMP pour le taux de change ECDHE à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging ( ENABLED | DISABLED ) -
    severity <severity>
 -state ( ENABLED | DISABLED ) -thresholdValue <positive_integer>  [-
     normalValue <positive_integer>] -time <secs>
<!--NeedCopy-->
```

Exemple :

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging eNABLED -severity critical
    -state eNABLED -thresholdValue 100 -normalValue 50
<!--NeedCopy-->
```


Prise en charge des suites de chiffrement ECDSA

May 5, 2023

Les suites de chiffrement ECDSA utilisent la cryptographie à courbe elliptique (ECC). En raison de sa taille réduite, il est utile dans les environnements où la puissance de traitement, l'espace de stockage, la bande passante et la consommation d'énergie sont limitées.

Lorsque le groupe de chiffrement ECDHE_ECDSA est utilisé, le certificat du serveur doit contenir une clé publique compatible ECDSA.

Le tableau suivant répertorie les chiffrements ECDSA pris en charge sur les appliances NetScaler MPX et SDX avec puces N3, les appliances NetScaler VPX, les appliances MPX 5900/26000 et MPX/SDX 8900/15000.

Nom du code	Priority	Description	algorithme d'échange de clés	algorithme d'authentification	Algorithme de chiffrement (taille de clé)	Algorithme de code d'authentification de message (MAC)	Code hexadécimal
TLS1-ECDHE-ECDSA-AES128-SHA	1	SSLv3	ECC-DHE	ECDSA	AES (128)	SHA1	0xc009
TLS1-ECDHE-ECDSA-AES256-SHA	2	SSLv3	ECC-DHE	ECDSA	AES (256)	SHA1	0xc00a
TLS1.2-ECDHE-ECDSA-AES128-SHA256	3	TLSv1.2	ECC-DHE	ECDSA	AES (128)	SHA-256	0xc023

Nom du code	Priority	Description	algorithme d'échange de clés	algorithme d'authentification	Algorithme de chiffrement (taille de clé)	Algorithme de code d'authentification de message (MAC)	Code hexadécimal
TLS1.2-ECDHE-ECDSA-AES256-SHA384	4	TLSv1.2	ECC-DHE	ECDSA	AES (256)	SHA-384	0xc024
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	5	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(128)	SHA-256	0xc02b
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	6	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(256)	SHA-384	0xc02c
TLS1-ECDHE-ECDSA-RC4-SHA	7	SSLv3	ECC-DHE	ECDSA	RC4(128)	SHA1	0xc007
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	8	SSLv3	ECC-DHE	ECDSA	3DES(168)	SHA1	0xc008

Nom du code	Priority	Description	algorithme d'échange de clés	algorithme d'authentification	Algorithme de chiffrement (taille de clé)	Algorithme de code d'authentification de message (MAC)	Code hexadécimal
TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305	9	TLSv1.2	ECC-DHE	ECDSA	CHACHA20/	AVANT	0xcca9

Sélection de certificat et chiffrement ECDSA/RSA

Vous pouvez lier simultanément des certificats de serveur ECDSA et RSA à un serveur virtuel SSL. Lorsque les certificats ECDSA et RSA sont liés au serveur virtuel, celui-ci sélectionne automatiquement le certificat de serveur approprié à présenter au client. Si la liste de chiffrement du client inclut des chiffrements RSA, mais pas des chiffrements ECDSA, le serveur virtuel présente le certificat du serveur RSA. Si les deux chiffrements figurent dans la liste du client, le certificat de serveur présenté dépend de la priorité de chiffrement définie sur le serveur virtuel. C'est-à-dire que si RSA a une priorité plus élevée, le certificat RSA est présenté. Si l'ECDSA a une priorité plus élevée, le certificat ECDSA est présenté au client.

Authentification du client à l'aide d'un certificat ECDSA ou RSA

Pour l'authentification du client, le certificat CA lié au serveur virtuel peut être signé ECDSA ou RSA. L'appliance prend en charge une chaîne de certificats mixte. Par exemple, la chaîne de certificats suivante est prise en charge.

Certificat client (ECDSA) <-> Certificat CA (RSA) <-> Certificat intermédiaire (RSA) <-> Certificat racine (RSA)

Le tableau suivant présente les courbes elliptiques prises en charge par les différentes appliances NetScaler dotées de groupes de chiffrement ECDSA et de certificats ECDSA :

Courbes elliptiques	Plates-formes prises en charge
prime256v1	Toutes les plateformes, y compris FIPS.
secp384r1	Toutes les plateformes, y compris FIPS.

Courbes elliptiques	Plates-formes prises en charge
secp521r1	MPX 5900, MPX/SDX 8900, MPX/SDX 15000, MPX/SDX 26000, VPX
secp224r1	MPX 5900, MPX/SDX 8900. MPX/SDX 15000, MPX/SDX 26000, VPX

Créer une paire de clés de certificat ECDSA

Vous pouvez créer une paire de clés de certificat ECDSA directement sur une appliance NetScaler à l'aide de l'interface de ligne de commande ou de l'interface graphique. Auparavant, vous pouviez installer et lier une paire de clés de certificat ECC sur l'appliance, mais vous deviez utiliser OpenSSL pour créer une paire de clés de certificat.

Seules les courbes P_256 et P_384 sont prises en charge.

> **Remarque**
>
> Ce support est disponible sur toutes les plateformes sauf MPX 9700/1050/12500/15500.

Pour créer une paire de clés de certificat ECDSA à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
create ssl ecdsaKey <keyFile> -curve ( P_256 | P_384 ) [-keyform ( DER | PEM )] [-des | -des3] {
 -password  }
  [-pkcs8]
<!--NeedCopy-->
```

Exemple :

```
create ecdsaKey ec_p256.ky -curve P_256 -pkcs8
Done
create ecdsaKey ec_p384.ky -curve P_384
Done
<!--NeedCopy-->
```

Pour créer une paire de clés de certificat ECDSA à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > SSL > Fichiers SSL > Clés**, puis cliquez sur **Créer une clé ECDSA**.
2. Pour créer une clé au format PKCS #8, sélectionnez **PKCS8**.

Configurer les groupes de chiffrement définis par l'utilisateur sur l'appliance ADC

May 5, 2023

Un groupe de chiffrement est un ensemble de suites de chiffrement que vous liez à un serveur virtuel, à un service ou à un groupe de services SSL sur l'appliance NetScaler. Une suite de chiffrement comprend un protocole, un algorithme d'échange de clés (Kx), un algorithme d'authentification (Au), un algorithme de chiffrement (Enc) et un algorithme de code d'authentification de message (Mac). Votre appliance est livrée avec un ensemble prédéfini de groupes de chiffrement. Lorsque vous créez un service SSL ou un groupe de services SSL, le groupe de chiffrement ALL y est automatiquement lié. Toutefois, lorsque vous créez un serveur virtuel SSL ou un service SSL transparent, le groupe de chiffrement DEFAULT y est automatiquement lié. En outre, vous pouvez créer un groupe de chiffrement défini par l'utilisateur et le lier à un serveur virtuel, à un service ou à un groupe de services SSL.

Remarque : Si votre appliance MPX ne possède aucune licence, seul le code de chiffrement EXPORT est lié à votre serveur virtuel, service ou groupe de services SSL.

Pour créer un groupe de chiffrement défini par l'utilisateur, vous devez d'abord créer un groupe de chiffrement, puis lier des chiffrements ou des groupes de chiffrement à ce groupe. Si vous spécifiez un alias de chiffrement ou un groupe de chiffrement, tous les chiffrements de l'alias ou du groupe de chiffrement sont ajoutés au groupe de chiffrement défini par l'utilisateur. Vous pouvez également ajouter des chiffrements individuels (suites de chiffrement) à un groupe défini par l'utilisateur. Toutefois, vous ne pouvez pas modifier un groupe de chiffrement prédéfini. Avant de supprimer un groupe de chiffrement, dissociez toutes les suites de chiffrement du groupe.

La liaison d'un groupe de chiffrement à un serveur virtuel, à un service ou à un groupe de services SSL ajoute les chiffrements aux chiffrements existants qui sont liés à l'entité. Pour lier un groupe de chiffrement spécifique à l'entité, vous devez d'abord dissocier les chiffrements ou le groupe de chiffrement lié à l'entité. Liez ensuite le groupe de chiffrement spécifique à l'entité. Par exemple, pour lier uniquement le groupe de chiffrement AES à un service SSL, procédez comme suit :

1. Dissociez le groupe de chiffrement par défaut ALL qui est lié par défaut au service lors de sa création.

```
unbind ssl service <service name> -cipherName ALL
<!--NeedCopy-->
```

2. Liez le groupe de chiffrement AES au service

```
bind ssl service <Service name> -cipherName AE
<!--NeedCopy-->
```


Si vous souhaitez lier le groupe de chiffrement DES en plus d'AES, à l'invite de commande, tapez :

```
bind ssl service <service name> -cipherName DES
<!--NeedCopy-->
```

Remarque : L'appliance virtuelle NetScaler gratuite prend uniquement en charge le groupe de chiffrement DH.

Configurer un groupe de chiffrement défini par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un groupe de chiffrement ou pour ajouter des chiffrements à un groupe créé précédemment, puis vérifiez les paramètres :

```
add ssl cipher <cipherGroupName>
bind ssl cipher <cipherGroupName> -cipherName <cipherGroup/cipherName>
show ssl cipher <cipherGroupName>
<!--NeedCopy-->
```

Exemple :

```
add ssl cipher test

Done

bind ssl cipher test -cipherName ECDHE

Done

sh ssl cipher test

1)      Cipher Name: TLS1-ECDHE-RSA-AES256-SHA  Priority : 1
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1   HexCode
   =0xc014
2)      Cipher Name: TLS1-ECDHE-RSA-AES128-SHA  Priority : 2
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1   HexCode
   =0xc013
3)      Cipher Name: TLS1.2-ECDHE-RSA-AES-256-SHA384    Priority : 3
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA-384
   HexCode=0xc028
4)      Cipher Name: TLS1.2-ECDHE-RSA-AES-128-SHA256    Priority : 4
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA-256
   HexCode=0xc027
```



```
5)      Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 5
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256) Mac=AEAD
   HexCode=0xc030
6)      Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 6
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128) Mac=AEAD
   HexCode=0xc02f
7)      Cipher Name: TLS1-ECDHE-ECDSA-AES256-SHA        Priority : 7
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA1
   HexCode=0xc00a
8)      Cipher Name: TLS1-ECDHE-ECDSA-AES128-SHA        Priority : 8
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA1
   HexCode=0xc009
9)      Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-SHA384   Priority : 9
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA-384
   HexCode=0xc024
10)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-SHA256   Priority : 10
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA-256
   HexCode=0xc023
11)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
   Priority : 11
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256) Mac=AEAD
   HexCode=0xc02c
12)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
   Priority : 12
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128) Mac=AEAD
   HexCode=0xc02b
13)     Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA        Priority : 13
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1   HexCode
   =0xc012
14)     Cipher Name: TLS1-ECDHE-ECDSA-DES-CBC3-SHA      Priority : 14
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=3DES(168) Mac=SHA1
   HexCode=0xc008
15)     Cipher Name: TLS1-ECDHE-RSA-RC4-SHA     Priority : 15
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=RC4(128)  Mac=SHA1   HexCode
   =0xc011
16)     Cipher Name: TLS1-ECDHE-ECDSA-RC4-SHA   Priority : 16
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=RC4(128)  Mac=SHA1
   HexCode=0xc007
17)     Cipher Name: TLS1.2-ECDHE-RSA-CHACHA20-POLY1305 Priority : 17
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=CHACHA20/POLY1305(256) Mac
   =AEAD   HexCode=0xcca8
18)     Cipher Name: TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305
   Priority : 18
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=CHACHA20/POLY1305(256)
   Mac=AEAD   HexCode=0xcca9
```



```
Done

bind ssl cipher test -cipherName TLS1-ECDHE-RSA-DES-CBC3-SHA
<!--NeedCopy-->
```

Dissocier les chiffrements d'un groupe de chiffrement à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour dissocier les chiffrements d'un groupe de chiffrement défini par l'utilisateur et vérifiez les paramètres :

```
show ssl cipher <cipherGroupName>

unbind ssl cipher <cipherGroupName> -cipherName <string>

show ssl cipher <cipherGroupName>
<!--NeedCopy-->
```

Supprimer un groupe de chiffrement à l'aide de l'interface de ligne de commande

Remarque : Vous ne pouvez pas supprimer un groupe de chiffrement intégré. Avant de supprimer un groupe de chiffrement défini par l'utilisateur, assurez-vous qu'il est vide.

À l'invite de commandes, tapez les commandes suivantes pour supprimer un groupe de chiffrement défini par l'utilisateur et vérifiez la configuration :

```
rm ssl cipher <userDefCipherGroupName> [<cipherName> ...]
show ssl cipher <cipherGroupName>

<!--NeedCopy-->
```

Exemple :

```
rm ssl cipher test Done

sh ssl cipher test ERROR: No such resource [cipherGroupName, test]
<!--NeedCopy-->
```

Configurer un groupe de chiffrement défini par l'utilisateur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Groupes de chiffrement**.

2. Cliquez sur **Ajouter**.
3. Spécifiez le nom du groupe de chiffrement.
4. Cliquez sur **Ajouter** pour afficher les chiffrements et les groupes de chiffrement disponibles.
5. Sélectionnez un chiffre ou un groupe de chiffrements, puis cliquez sur le bouton fléché pour les ajouter.
6. Cliquez sur **Create**.
7. Cliquez sur **Fermer**.

Pour lier un groupe de chiffrement à un serveur virtuel, à un service ou à un groupe de services SSL à l'aide de l'interface deligne de commande :

À l'invite de commandes, tapez l'une des commandes suivantes :

```
bind ssl vserver <vServerName> -cipherName <string>

bind ssl service <serviceName> -cipherName <string>

bind ssl serviceGroup <serviceGroupName> -cipherName <string>

<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver ssl_vserver_test -cipherName test
Done

bind ssl service  nshttps -cipherName test
Done

bind ssl servicegroup  ssl_svc  -cipherName test
Done
<!--NeedCopy-->
```

Pour lier un groupe de chiffrement à un serveur virtuel, à un service ou à un groupe de services SSL à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.

   Pour le service, remplacez les serveurs virtuels par des services. Pour les groupes de services, remplacez les serveurs virtuels par des groupes de services.

   Ouvrez le serveur virtuel, le service ou le groupe de services.

2. Dans **Paramètres avancés**, sélectionnez **Chiffrements SSL.**
3. Liez un groupe de chiffrement au serveur virtuel, au service ou au groupe de services.

Lier des chiffrements individuels à un serveur virtuel ou à un service SSL

Vous pouvez également lier des chiffrements individuels, au lieu d'un groupe de chiffrement, à un serveur ou à un service virtuel.

Pour lier un chiffrement à l'aide de l'interface de ligne de commande :
À l'invite de commandes, tapez :

```
bind ssl vserver <vServerName> -cipherName <string>
bind ssl service <serviceName> -cipherName <string>
<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver v1 -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
Done

bind ssl service sslsvc -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
Done
<!--NeedCopy-->
```

Pour lier un chiffrement à un serveur virtuel SSL à l'aide de l'interface graphique :

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel SSL et cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, sélectionnez **Chiffrements SSL.**
4. Dans **Cipher Suites**, sélectionnez **Ajouter**.
5. Recherchez le code dans la liste disponible et cliquez sur la flèche pour l'ajouter à la liste configurée.
6. Cliquez sur **OK**.
7. Cliquez sur **Terminé**.

Pour lier un chiffrement à un service SSL, répétez les étapes précédentes après le remplacement du serveur virtuel par le service.

Matrice de prise en charge des certificats de serveur sur l'appliance ADC

May 5, 2023

À partir de la version 13.0 build 41.x, l'appliance ADC prend en charge les messages de certificat de serveur qui sont fragmentés en plusieurs enregistrements si la taille totale est inférieure à 32 Ko. Auparavant, la taille maximale prise en charge était de 16 Ko et la fragmentation n'était pas prise en charge.

L'appliance NetScaler prend en charge les certificats de serveur suivants.

Tableau 1 : Prise en charge des services frontaux (FE) et dorsaux (BE)

Certificat de serveur/plate-forme	MPX/SDX (PUCES N2) FE	MPX/SDX (PUCES N2)	MPX/SDX (PUCES N3) FE	MPX/SDX (PUCES N3)	VPX FE	VPX BE
MD5	O	O	O	O	O	O
SHA1	O	O	O	O	O	O
SHA224	O	O	O	O	O	O
SHA256	O	O	O	O	O	O
SHA384	O	O	O	O	O	O
SHA512	O	O	O	O	O	O
Clé RSA	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits
Touche DH	1024 bits et 2048 bits	1024 bits et 2048 bits	1024 bits et 2048 bits	1024 bits et 2048 bits	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits

Certificat de serveur/plate-forme	MPX/SDX 14030/14060/14080 FIPS FE	MPX/SDX 14030/14060/14080 FIPS BE
MD5	O	O
SHA1	O	O
SHA224	O	O
SHA256	O	O
SHA384	O	O
SHA512	O	O
Clé RSA	2048 bits et 3072 bits	2048 bits et 3072 bits
Touche DH	N	N

Certificat de serveur/plate-forme	MPX 5900, MPX/SDX 8900, MPX/SDX 9100, MPX/SDX 15000, MPX/SDX 15000-50G, MPX/SDX 16000, MPX/SDX 26000, MPX/SDX 26000-50G, MPX/SDX 26000-100G (frontal)	MPX 5900, MPX/SDX 8900, MPX/SDX 9100 MPX/SDX 15000, MPX/SDX 15000-50G, MPX/SDX 16000, MPX/SDX 26000, MPX/SDX 26000-50G, MPX/SDX 26000-100G (back-end)
MD5	O	O
SHA1	O	O
SHA224	O	O
SHA256	O	O
SHA384	O	O
SHA512	O	O
Clé RSA	1024, 2048, 3072 et 4096 bits	1024, 2048, 3072 et 4096 bits
Touche DH	1024 bits et 2048 bits	1024 bits et 2048 bits

Remarques

- Les certificats 4K nécessitent des cycles CPU plus élevés et peuvent affecter les performances des appliances bas de gamme.
- Dans les versions 11.1 et antérieures, une appliance NetScaler prend en charge les extensions « algorithmes de signature » suivantes dans le message d'accueil du client principal : RSA-MD5, RSA-SHA1 et RSA-SHA256.
  L'appliance NetScaler ne prend pas en charge les extensions d'algorithmes de signature SHA 384 et SHA 512. Par conséquent, certains serveurs, tels que les serveurs Windows IIS, réinitialisent la connexion.
- À partir de la version 12.0, une appliance NetScaler prend en charge toutes les extensions signature_algorithms.

Authentification client ou Mutual TLS (MTLS)

May 5, 2023

Dans une transaction SSL classique, le client qui se connecte à un serveur via une connexion sécurisée vérifie la validité du serveur. Pour ce faire, il vérifie le certificat du serveur avant d'initier la transaction

SSL. Toutefois, il peut arriver que vous souhaitiez configurer le serveur pour authentifier le client qui s'y connecte.

Remarque : À partir de la version 13.0 build 41.x, l'appliance NetScaler prend en charge les messages de demande de certificat qui sont fragmentés en plusieurs enregistrements si la taille totale est inférieure à 32 Ko. Auparavant, la taille maximale prise en charge était de 16 Ko et la fragmentation n'était pas prise en charge.

Lorsque l'authentification du client est activée sur un serveur virtuel SSL, l'appliance NetScaler demande le certificat client lors de l'établissement de connexion SSL. L'appliance vérifie que le certificat présenté par le client est soumis à des contraintes normales, telles que la signature de l'émetteur et la date d'expiration.

À partir de la version 13.1 build 42.x, l'appliance NetScaler prend en charge la validation des certificats croisés. En d'autres termes, si un certificat est signé par plusieurs émetteurs, la validation est réussie s'il existe au moins un chemin valide vers le certificat racine. Auparavant, si l'un des certificats de la chaîne de certificats était signé de manière croisée et comportait plusieurs chemins d'accès au certificat racine, l'appliance ADC ne recherchait qu'un seul chemin. Et si ce chemin n'était pas valide, la validation échouait.

> **Remarque Pour que**
>
> l'appliance puisse vérifier les signatures de l'émetteur, le certificat de l'autorité de certification qui a émis le certificat client doit être :
>
> - Installé sur l'appareil.
> - Lié au serveur virtuel avec lequel le client effectue des transactions.

Si le certificat est valide, l'appliance autorise le client à accéder à toutes les ressources sécurisées. Mais si le certificat n'est pas valide, l'appliance abandonne la demande du client lors de l'établissement de la liaison SSL.

L'appliance vérifie le certificat client en formant d'abord une chaîne de certificats, en commençant par le certificat client et en terminant par le certificat d'autorité de certification racine du client (par exemple, Verisign). Le certificat d'autorité de certification racine peut contenir un ou plusieurs certificats d'autorité de certification intermédiaires (si l'autorité de certification racine n'émet pas directement le certificat client).

Avant d'activer l'authentification client sur l'appliance NetScaler, assurez-vous qu'un certificat client valide est installé sur le client. Activez ensuite l'authentification du client pour le serveur virtuel qui gère les transactions. Enfin, liez le certificat de l'autorité de certification qui a émis le certificat client au serveur virtuel sur l'appliance.

Remarque : Une appliance NetScaler MPX prend en charge une taille de paire de clés de certificat comprise entre 512 bits et 4 096 bits. Le certificat doit être signé à l'aide de l'un des algorithmes de hachage suivants :

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Sur une appliance SDX, si une puce SSL est attribuée à une instance VPX, la prise en charge de la taille de la paire de clés de certificat d'une appliance MPX s'applique. Sinon, la prise en charge normale de la taille de paire de clés de certificat d'une instance VPX s'applique.

Une appliance virtuelle NetScaler (instance VPX) prend en charge les certificats d'au moins 512 bits, jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service
- Certificat CA 4096 bits
- Certificat 4096 bits sur le serveur physique

À partir de la version 13.1 build 17.x, toutes les plateformes NetScaler prennent en charge les certificats signés à l'aide des algorithmes RSASSA-PSS.
Ces algorithmes sont pris en charge dans la validation du chemin d'accès au certificat X.509.
Le tableau suivant présente les jeux de paramètres RSASSA-PSS pris en charge par l'appliance NetScaler.

ID de clé publique	Fonction de génération de masque (MGF)	Fonction MGF Digest	Fonction Signature Digest	Longueur de salt
rsaEncryption	MGF1	SHA-256	SHA-256	32 octets
rsaEncryption	MGF1	SHA-384	SHA-384	48 octets
rsaEncryption	MGF1	SHA-512	SHA-512	64 octets

Remarque : À partir de la version 13.0 build 79.x, l'authentification du client avec un certificat client RSA 4096 bits est prise en charge lors d'une négociation SSL sur la plate-forme VPX.

Remarques :

- Pour connaître les limitations MPX FIPS, consultez Limitations MPX FIPS.
- Pour connaître les limitations SDX FIPS, reportez-vous à la section Limitations FIPS SDX.

Fournir le certificat client

Avant de configurer l'authentification du client, un certificat client valide doit être installé sur le client. Un certificat client inclut des détails sur le système client spécifique qui crée des sessions sécurisées avec l'appliance NetScaler. Chaque certificat client est unique et ne doit être utilisé que par un seul système client.

Que vous obteniez le certificat client auprès d'une autorité de certification, que vous utilisiez un certificat client existant ou que vous créiez un certificat client sur l'appliance NetScaler, vous devez convertir le certificat au format approprié. Sur l'appliance NetScaler, les certificats sont stockés au format PEM ou DER et doivent être convertis au format PKCS #12 avant d'être installés sur le système client. Après avoir converti le certificat et l'avoir transféré vers le système client, assurez-vous qu'il est installé sur ce système et configuré pour l'application cliente. L'application, telle qu'un navigateur Web, doit faire partie des transactions SSL.

Pour obtenir des instructions sur la façon de convertir un certificat du format PEM ou DER au format PKCS #12, voir Importer et convertir des fichiers SSL.

Pour obtenir des instructions sur la façon de générer un certificat client, reportez-vous à la section Créer un certificat.

Activer l'authentification basée sur le certificat client

Par défaut, l'authentification du client est désactivée sur l'appliance NetScaler et toutes les transactions SSL se déroulent sans authentifier le client. Vous pouvez configurer l'authentification du client pour qu'elle soit facultative ou obligatoire dans le cadre de l'établissement de liaison SSL.

Si l'authentification du client est facultative, l'appliance demande le certificat client mais procède à la transaction SSL même si le client présente un certificat non valide. Si l'authentification du client est obligatoire, l'appliance met fin à l'établissement de liaison SSL si le client SSL ne fournit pas de certificat valide.

Attention : Citrix vous recommande de définir des stratégies de contrôle d'accès appropriées avant de modifier la vérification d'authentification basée sur le certificat client sur facultative.

Remarque : L'authentification du client est configurée pour des serveurs virtuels SSL individuels, et non globalement.

Activer l'authentification basée sur le certificat client à l'aide de la CLI

À l'invite de commandes, tapez les commandes suivantes pour activer l'authentification basée sur le certificat client et vérifier la configuration :

```
set ssl vserver <vServerName> [-clientAuth (ENABLED | DISABLED)] [-
    clientCert (MANDATORY | OPTIONAL)]
```



```
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Exemple :

```
set ssl vserver vssl -clientAuth ENABLED -clientCert Mandatory
Done
show ssl vserver vssl

Advanced SSL configuration for VServer vssl:
DH: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.2: ENABLED TLSv1
   .2: ENABLED

1) CertKey Name: sslckey Server Certificate

1) Policy Name: client_cert_policy Priority: 0

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Activer l'authentification basée sur le certificat client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**, puis ouvrez un serveur virtuel.
2. Dans la section **Paramètres SSL**, sélectionnez **Authentification du client**, puis dans la liste des **certificats clients**, sélectionnez **Obligatoire**.

> **Remarque :**
>
> Si l'authentification du client est définie sur obligatoire et si le certificat client contient des extensions de stratégie, la validation du certificat échoue. À partir de la version 12.0-56.x, vous pouvez définir un paramètre dans le profil SSL frontal pour ignorer cette vérification. Le paramètre est désactivé par défaut. En d'autres termes, la vérification est effectuée par défaut.

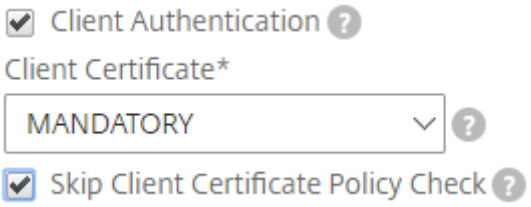
Ignorer la vérification de l'extension de stratégie lors de l'authentification du client à l'aide

À l'invite de commande, tapez :

```
set ssl profile ns_default_ssl_profile_frontend -clientauth ENABLED -
    skipClientCertPolicyCheck ENABLED

Parameter

skipClientCertPolicyCheck

              Control policy extension check, if present inside the
                 X509 certificate chain. Applicable only if client
                 authentication is enabled and client certificate is
                 set to mandatory. Possible values functions as follows
                 :

- ENABLED: Skip the policy check during client authentication.

- DISABLED: Perform policy check during client authentication.

Possible values: ENABLED, DISABLED

Default: DISABLED
<!--NeedCopy-->
```

Ignorer la vérification de l'extension de stratégie lors de l'authentification du client à l'aide

1. Accédez à **Système** > **Profils** > **Profils SSL**.
2. Créez un nouveau profil frontal ou modifiez un profil frontal existant.
3. Vérifiez que l'authentification du client est activée et que le certificat client est défini sur obligatoire.
4. Sélectionnez **Ignorer la vérification de stratégie de certificat client**



Lier les certificats d'autorité de certification au serveur virtuel

Une autorité de certification dont le certificat est présent sur l'appliance NetScaler doit émettre le certificat client utilisé pour l'authentification du client. Liez ce certificat au serveur virtuel NetScaler qui effectue l'authentification du client.

Liez le certificat d'autorité de certification au serveur virtuel SSL de telle sorte que l'appliance puisse former une chaîne de certificats complète lorsqu'elle vérifie le certificat client. Sinon, la formation de la chaîne de certificats échoue et le client se voit refuser l'accès même si son certificat est valide.

Vous pouvez lier des certificats d'autorité de certification au serveur virtuel SSL dans n'importe quel ordre. L'appliance passe la commande appropriée lors de la vérification du certificat client.

Par exemple, si le client présente un certificat émis par **CA_A, où CA_Aest une**autorité de certification intermédiaire dont le certificat est émis par**CA_B**, dont le certificat est à son tour émis par une autorité de certification racine approuvée, **Root_CA**, une chaîne de certificats contenant ces trois certificats doit être liée au serveur virtuel sur l'appliance NetScaler.

Pour obtenir des instructions sur la liaison d'un ou de plusieurs certificats au serveur virtuel, voir Lier la paire de clés de certificat au serveur virtuel SSL.

Pour obtenir des instructions sur la création d'une chaîne de certificats, voir Créer une chaîne de certificats.

Contrôle plus strict de la validation des certificats clients

L'appliance NetScaler accepte les certificats CA intermédiaires valides s'ils sont émis par une seule autorité de certification racine. En d'autres termes, si seul le certificat d'autorité de certification racine est lié au serveur virtuel et que l'autorité de certification racine valide tout certificat intermédiaire envoyé avec le certificat client, l'appliance fait confiance à la chaîne de certificats et l'établissement de liaison réussit.

Toutefois, si un client envoie une chaîne de certificats dans la négociation, aucun des certificats intermédiaires ne peut être validé à l'aide d'un répondeur CRL ou OCSP, sauf si ce certificat est lié au serveur virtuel SSL. Par conséquent, même si l'un des certificats intermédiaires est révoqué, la prise de contact est réussie. Dans le cadre de l'établissement de la liaison, le serveur virtuel SSL envoie la liste des certificats d'autorité de certification qui lui sont liés. Pour un contrôle plus strict, vous pouvez

configurer le serveur virtuel SSL pour qu'il accepte uniquement un certificat signé par l'un des certificats d'autorité de certification liés à ce serveur virtuel. Pour ce faire, vous devez activer le paramètre **ClientAuthUseBoundCachain** dans le profil SSL lié au serveur virtuel. La connexion échoue si l'un des certificats d'autorité de certification liés au serveur virtuel n'a pas signé le certificat client.

Par exemple, disons que deux certificats clients, clientcert1 et clientcert2, sont signés par les certificats intermédiaires int-CA-A et int-CA-B, respectivement. Les certificats intermédiaires sont signés par le certificat racine Root-CA. Int-CA-A et Root-CA sont liés au serveur virtuel SSL. Dans le cas par défaut (ClientAuthUseBoundCachain désactivé), clientcert1 et clientcert2 sont acceptés. Toutefois, si ClientAuthUseBoundCachain est activé, l'appliance NetScaler accepte uniquement clientcert1.

Contrôle plus strict de la validation des certificats clients à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl profile <name> -ClientAuthUseBoundCAChain Enabled
<!--NeedCopy-->
```

Permettre un contrôle plus strict sur la validation des certificats clients à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils**, sélectionnez l'onglet **Profils SSL** et créez un profil SSL ou sélectionnez un profil existant.
2. Sélectionnez **Activer l'authentification client à l'aide de la chaîne de certification liée**.

Authentification du serveur

May 5, 2023

Étant donné que l'appliance NetScaler effectue le déchargement et l'accélération SSL pour le compte d'un serveur Web, elle n'authentifie généralement pas le certificat du serveur Web. Toutefois, vous pouvez authentifier le serveur dans les déploiements qui nécessitent un cryptage SSL de bout en bout.

Dans ce cas, l'appliance devient le client SSL et effectue une transaction sécurisée avec le serveur SSL. Il vérifie qu'une autorité de certification dont le certificat est lié au service SSL a signé le certificat du serveur et vérifie la validité du certificat du serveur.

Pour authentifier le serveur, activez l'authentification du serveur et liez le certificat de l'autorité de certification qui a signé le certificat du serveur au service SSL sur l'appliance ADC. Lorsque vous liez le certificat, vous devez spécifier la liaison en tant qu'option CA.

À partir de la version 13.1 build 42.x, l'appliance NetScaler prend en charge la validation des certificats croisés. En d'autres termes, si un certificat est signé par plusieurs émetteurs, la validation est réussie s'il existe au moins un chemin valide vers le certificat racine. Auparavant, si l'un des certificats de la chaîne de certificats était signé de manière croisée et comportait plusieurs chemins d'accès au certificat racine, l'appliance ADC ne recherchait qu'un seul chemin. Et si ce chemin n'était pas valide, la validation échouait.

Activer (ou désactiver) l'authentification par certificat de serveur

Vous pouvez utiliser l'interface de ligne de commande et l'interface graphique pour activer et désactiver l'authentification par certificat de serveur.

Activer (ou désactiver) l'authentification par certificat de serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer l'authentification par certificat de serveur et vérifier la configuration :

```
set ssl service <serviceName> -serverAuth ( ENABLED | DISABLED )
show ssl service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
set ssl service ssl-service-1 -serverAuth ENABLED

show ssl service ssl-service-1

            Advanced SSL configuration for Back-end SSL Service ssl-
               service-1:`
            DH: DISABLED
            Ephemeral RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            Server Auth: ENABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
    1)      Cipher Name: ALL
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```


Activer (ou désactiver) l'authentification par certificat de serveur à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services**, puis ouvrez un service SSL.
2. Dans la section Paramètres SSL, sélectionnez Activer l'authentification du serveur et spécifiez un nom commun.
3. Dans Paramètres avancés, sélectionnez Certificats et liez un certificat CA au service.

Liez le certificat CA au service à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier le certificat CA au service et vérifier la configuration :

```
bind ssl service <serviceName> -certkeyName <string> -CA

show ssl service <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind ssl service ssl-service-1 -certkeyName samplecertkey -CA

show ssl service ssl-service-1

            Advanced SSL configuration for Back-end SSL Service ssl-
               service-1:
            DH: DISABLED
            Ephemeral RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            Server Auth: ENABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
    1)      CertKey Name: samplecertkey     CA Certificate
       CRLCheck: Optional
    1)      Cipher Name: ALL
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```


Configuration d'un nom commun pour l'authentification des certificats de serveur

Dans le cadre du chiffrement de bout en bout avec l'authentification du serveur activée, vous pouvez inclure un nom commun dans la configuration d'un service ou d'un groupe de services SSL. Le nom que vous spécifiez est comparé au nom commun figurant dans le certificat du serveur lors d'une liaison SSL. Si les deux noms correspondent, la poignée de main est réussie.
Si les noms communs ne correspondent pas, le nom commun spécifié pour le service ou le groupe de services est comparé aux valeurs du champ de nom alternatif du sujet (SAN) du certificat. Si elle correspond à l'une de ces valeurs, la poignée de main est réussie. Cette configuration est particulièrement utile si, par exemple, deux serveurs sont protégés par un pare-feu et que l'un des serveurs usurpe l'identité de l'autre. Si le nom commun n'est pas coché, un certificat présenté par l'un ou l'autre des serveurs est accepté si l'adresse IP correspond.

Remarque : seules les entrées DNS du nom de domaine, de l'URL et de l'identifiant de messagerie figurant dans le champ SAN sont comparées.

Configurer la vérification du nom commun pour un service ou un groupe de services SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour spécifier l'authentification du serveur avec vérification par nom commun et vérifier la configuration :

1. Pour configurer un nom commun dans un service, tapez :

```
set ssl service <serviceName> -commonName <string> -serverAuth
   ENABLED
show ssl service <serviceName>
<!--NeedCopy-->
```

2. Pour configurer un nom commun dans un groupe de services, tapez :

```
set ssl serviceGroup <serviceGroupName> -commonName <string> -
   serverAuth ENABLED
show ssl serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Exemple :

```
set ssl service svc1 -commonName xyz.com -serverAuth ENABLED

show ssl service svc

     Advanced SSL configuration for Back-end SSL Service svc1:
     DH: DISABLED
     Ephemeral RSA: DISABLED
```



```
8       Session Reuse: ENABLED Timeout: 300 seconds
9       Cipher Redirect: DISABLED
10      SSLv2 Redirect: DISABLED
11      Server Auth: ENABLED Common Name: www.xyz.com
12      SSL Redirect: DISABLED
13      Non FIPS Ciphers: DISABLED
14      SNI: DISABLED
15      SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
16     1) CertKey Name: cacert CA Certificate OCSPCheck: Optional
17     1) Cipher Name: ALL
18      Description: Predefined Cipher Alias
19 Done
20 <!--NeedCopy-->
```

Configurer la vérification du nom commun pour un service ou un groupe de services SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Services** ou accédez à **Gestion du trafic > Équilibrage de charge > Groupes de services**, puis ouvrez un service ou un groupe de services.
2. Dans la section **Paramètres SSL**, sélectionnez **Activer l'authentification du serveur**et spécifiez un nom commun.

Actions et stratégies SSL

May 5, 2023

Une stratégie SSL évalue le trafic entrant et applique une action prédéfinie aux demandes qui correspondent à une règle (expression). Configurez les actions avant de créer les stratégies, afin de pouvoir spécifier une action lorsque vous créez une stratégie. Pour mettre une stratégie en vigueur, effectuez l'une des opérations suivantes :

- Liez la stratégie à un serveur virtuel sur l'appliance, afin qu'elle s'applique uniquement au trafic circulant via ce serveur virtuel.
- Liez la stratégie globalement, afin qu'elle s'applique à tout le trafic passant par l'appliance.

Les actions SSL définissent les paramètres SSL que vous pouvez appliquer aux demandes sélectionnées. Vous associez une action à une ou plusieurs stratégies. Les données des demandes ou réponses de connexion client sont comparées à une règle spécifiée dans la stratégie, et l'action est appliquée aux connexions qui correspondent à la règle (expression).

Vous pouvez configurer des stratégies classiques avec des expressions classiques et des stratégies de stratégie avancées avec des expressions de stratégie avancées pour SSL.

Remarque : Les utilisateurs qui ne sont pas expérimentés dans la configuration des stratégies au niveau de l'interface de ligne de commande trouvent généralement l'utilisation de l'utilitaire de configuration beaucoup plus facile.

Vous pouvez associer une action définie par l'utilisateur ou une action intégrée à une stratégie avancée. Les stratégies classiques autorisent uniquement les actions définies par l'utilisateur. Dans la stratégie avancée, vous pouvez également regrouper les stratégies sous une étiquette de stratégie, auquel cas elles ne sont appliquées que lorsqu'elles sont appelées à partir d'une autre stratégie.

Les actions et stratégies SSL sont couramment utilisées, notamment l'authentification client par répertoire, la prise en charge de l'accès Web Outlook et les insertions d'en-têtes SSL. Les insertions d'en-tête basées sur SSL contiennent les paramètres SSL requis par un serveur dont le traitement SSL a été déchargé vers l'appliance NetScaler.

Stratégies SSL

May 5, 2023

Les politiques de l'appliance NetScaler aident à identifier les connexions spécifiques que vous souhaitez traiter. Le traitement est basé sur les actions configurées pour cette stratégie particulière. Une fois que vous avez créé la stratégie et configuré une action pour celle-ci, vous devez effectuer l'une des opérations suivantes :

- Liez la stratégie à un serveur virtuel sur l'appliance, afin qu'elle s'applique uniquement au trafic circulant via ce serveur virtuel.
- Liez la politique de manière globale, afin qu'elle s'applique à tout le trafic passant par n'importe quel serveur virtuel configuré sur l'appliance NetScaler.

La fonctionnalité SSL de l'appliance NetScaler prend en charge les politiques avancées (avancées). Pour obtenir une description complète des expressions de stratégie avancées, de leur fonctionnement et de leur configuration manuelle, consultez Stratégies et expressions. Pour plus d'informations sur les expressions SSL, consultez Expressions de stratégie avancées : analyse SSL.

> **Remarque :**
>
> Les utilisateurs qui ne sont pas expérimentés dans la configuration des stratégies dans l'interface de ligne de commande trouvent généralement l'utilisation de l'utilitaire de configuration beaucoup plus facile.

Les stratégies SSL exigent que vous créiez une action avant de créer une stratégie, afin de pouvoir spécifier les actions lors de la création des stratégies.

Dans les stratégies avancées SSL, vous pouvez également utiliser les actions intégrées. Pour plus d'informations sur les actions intégrées, consultez Actions intégrées SSL et actions définies parl'utilisateur.

Stratégies avancées SSL

Une stratégie SSL Advanced, également connue sous le nom de stratégie avancée, définit un contrôle ou une action de données à exécuter sur les demandes. Les stratégies SSL peuvent donc être classées en tant que stratégies de contrôle et stratégies de données :

- **Politique de contrôle**. Une stratégie de contrôle utilise une action de contrôle, telle que forcer l'authentification du client.
  Remarque : Dans la version 10.5 ou ultérieure, le paramètre Refuser la renégociation SSL (DenySSLReneg) est défini, par défaut, sur ALL. Toutefois, les stratégies de contrôle, telles que CLIENTAUTH, déclenchent une négociation de renégociation. Si vous utilisez de telles stratégies, vous devez définir DenySSLReneg sur NO.
- **Politique de données**. Une stratégie de données utilise une action de données, telle que l'insertion de certaines données dans la demande.

Les éléments essentiels d'une politique sont une expression et une action. L'expression identifie les demandes sur lesquelles l'action doit être exécutée.

Vous pouvez configurer une stratégie avancée avec une action intégrée ou une action définie par l'utilisateur. Vous pouvez configurer une stratégie avec une action intégrée sans créer d'action distincte. Toutefois, pour configurer une stratégie avec une action définie par l'utilisateur, configurez d'abord l'action, puis configurez la stratégie.

Vous pouvez spécifier une action supplémentaire, appelée action UNDEF, à effectuer lorsque l'application de l'expression à une demande a un résultat non défini.

Configuration de la stratégie SSL

Vous pouvez configurer une stratégie SSL Advanced à l'aide de l'interface de ligne de commande et de l'interface graphique.

Configurer une stratégie SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add ssl policy <name> -rule <expression> -Action <string> [-undefAction
      <string>] [-comment <string>]
2 <!--NeedCopy-->
```


Configurer une stratégie SSL à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Stratégies** et, sous l'onglet **Stratégies**, cliquez sur *Ajouter*.

Prise en charge des stratégies SSL avec le protocole TLS1.3

À partir de la version 13.0 build 71.x et ultérieure, la prise en charge des stratégies SSL avec le protocole TLS1.3 est ajoutée. Lorsque le protocole TLSv1.3 est négocié pour une connexion, les règles de stratégie qui inspectent les données TLS reçues du client déclenchent désormais l'action configurée.

Par exemple, si la règle de stratégie suivante renvoie true, le trafic est transféré vers le serveur virtuel défini dans l'action.

```
1 add ssl action action1 -forward vserver2
2 add ssl policy pol1 -rule client.ssl.client_hello.sni.contains( “xyz” )
      -action action1
3 <!--NeedCopy-->
```

Limitations

- Les stratégies de contrôle ne sont pas prises en charge.
- Les actions suivantes ne sont pas prises en charge :
  - DOCLIENTAUTH
  - NOCLIENTAUTH
  - caCertGrpName
  - Vérification du certificat client
  - ssllogProfile

Actions intégrées SSL et actions définies par l'utilisateur

May 5, 2023

À moins que vous n'ayez uniquement besoin des actions intégrées à vos politiques, vous devez créer les actions avant de créer les politiques. Vous pouvez ensuite spécifier les actions lorsque vous créez les politiques. Les actions intégrées sont de deux types : les actions de contrôle et les actions de données. Vous utilisez des actions de contrôle dans des politiques de contrôle et des actions de données dans des politiques de données.

Les actions de contrôle intégrées sont les suivantes :

- DoClientAuth : effectuez l'authentification par certificat client. (Non pris en charge pour TLS1.3)

- NoClientAuth : n'effectuez pas d'authentification par certificat client. (Non pris en charge pour TLS1.3)

Les actions de données intégrées sont les suivantes :

- Réinitialiser : fermez la connexion en envoyant un paquet RST au client.
- Supprimer : supprimez tous les paquets du client. La connexion reste ouverte jusqu'à ce que le client la ferme.
- NOOP : transfère le paquet sans effectuer aucune opération sur celui-ci.

Remarque : Les actions dépendantes de l'authentification du client, telles que ClientCertVerification et SSLLogProfile, ne sont pas prises en charge par le protocole TLS 1.3.

Vous pouvez créer des actions de données définies par l'utilisateur. Si vous activez l'authentification du client, vous pouvez créer une action SSL pour insérer les données du certificat client dans l'en-tête de la demande avant de transmettre la demande au serveur Web.

Si l'évaluation d'une politique aboutit à un état non défini, une action UNDEF est exécutée. Pour une politique de données ou une politique de contrôle, vous pouvez spécifier RESET, DROP ou NOOP comme action UNDEF. Pour une politique de contrôle, vous avez également la possibilité de spécifier DOCLIENTAUTH ou NOCLIENTAUTH.

Exemples d'actions intégrées dans une politique

Dans l'exemple suivant, si le client envoie un code autre qu'un code de catégorie EXPORT, l'appliance NetScaler demande l'authentification du client. Le client doit fournir un certificat valide pour que la transaction soit réussie.

```
1 add ssl policy pol1 -rule CLIENT.SSL.CIPHER_EXPORTABLE.NOT -reqAction
     DOCLIENTAUTH
2 <!--NeedCopy-->
```

Les exemples suivants supposent que l'authentification du client est activée.

Si la version du certificat fourni par l'utilisateur correspond à la version de la politique, aucune action n'est entreprise et le paquet est transféré :

```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction NOOP
2 <!--NeedCopy-->
```

Si la version du certificat fourni par l'utilisateur correspond à la version de la politique, la connexion est interrompue :

```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction DROP
```



```
<!--NeedCopy-->
```

Si la version du certificat fourni par l'utilisateur correspond à la version de la politique, la connexion est réinitialisée :

```
add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
   reqAction RESET
<!--NeedCopy-->
```

Vérification du certificat client avec authentification client basée sur des politiques

Vous pouvez définir la vérification du certificat client comme obligatoire ou facultative lorsque vous avez configuré l'authentification client basée sur des politiques. La valeur par défaut est obligatoire.

Définissez la vérification du certificat client sur facultative à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ssl action <name> ((-clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) [-
   clientCertVerification ( Mandatory | Optional )]
<!--NeedCopy-->
```

Exemple :

```
add ssl action sslact -clientauth DOCLIENTAUTH -clientcertverification
   OPTIONAL
<!--NeedCopy-->
```

Définissez la vérification du certificat client sur facultative à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Stratégies**.
2. Dans l'onglet **Actions SSL**, cliquez sur **Ajouter**.
3. Spécifiez un nom et dans la liste de **vérification des certificats clients**, sélectionnez **Facultatif**.

Actions SSL définies par l'utilisateur

Outre les actions intégrées, vous pouvez également configurer d'autres actions SSL en fonction de votre déploiement. Ces actions sont appelées actions définies par l'utilisateur.

Configurer une action SSL définie par l'utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une action et vérifier la configuration :

```
add SSL action <name> -clientAuth(DOCLIENTAUTH | NOCLIENTAUTH) -
    clientCert (ENABLED | DISABLED) certHeader <string> -clientHeader <
    string> -clientCertSerialNumber (ENABLED | DISABLED) -
    certSerialHeader <string> -clientCertSubject (ENABLED | DISABLED) -
    certSubjectHeader <string> -clientCertHash (ENABLED | DISABLED) -
    certHashHeader <string> -clientCertIssuer (ENABLED | DISABLED) -
    certIssuerHeader <string> -sessionID (ENABLED | DISABLED) -
    sessionIDheader <string> -cipher (ENABLED | DISABLED) -cipherHeader
    <string> -clientCertNotBefore (ENABLED | DISABLED) -
    certNotBeforeHeader <string> -clientCertNotAfter (ENABLED | DISABLED
    ) -certNotAfterHeader <string> -OWASupport (ENABLED | DISABLED)
<!--NeedCopy-->
```

```
show ssl action [<name>]
<!--NeedCopy-->
```

Exemple :

```
add ssl action Action-SSL-ClientCert -clientCert ENABLED -certHeader "X
    -Client-Cert"
<!--NeedCopy-->
```

```
show ssl action Action-SSL-ClientCert

1)      Name: Action-SSL-ClientCert
        Data Insertion Action:
        Cert Header: ENABLED            Cert Tag: X-Client-Cert
Done
<!--NeedCopy-->
```

Configurer une action SSL définie par l'utilisateur à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Stratégies** et, sous l'onglet **Actions**, cliquez sur **Ajouter**.

Configurer une action SSL pour transférer le trafic client vers un autre serveur virtuel

Les administrateurs peuvent configurer une action SSL pour transférer le trafic client reçu sur un serveur virtuel SSL vers un autre serveur virtuel afin d'éviter le déchargement SSL. Ou pour mettre

fin à la connexion sur l'appliance ADC. Ce serveur virtuel peut être du type SSL, TCP ou SSL_BRIDGE. Par exemple, les administrateurs peuvent choisir de transmettre la demande à un autre serveur virtuel pour une action ultérieure au lieu de mettre fin à la connexion dans l'un des cas suivants :

- L'appliance ne possède pas de certificat.
- L'appliance ne prend pas en charge un chiffrement spécifique.

Pour atteindre ce qui précède, un nouveau point de liaison « CLIENTHELLO_REQ » est ajouté pour évaluer le trafic client lorsqu'un bonjour client est reçu. Si la politique liée au serveur virtuel recevant le trafic client est évaluée comme vraie après avoir analysé le client hello, le trafic est transféré vers un autre serveur virtuel. Si ce serveur virtuel est de type SSL, il effectue l'établissement de la liaison. Si ce serveur virtuel est de type TCP ou SSL_BRIDGE, le serveur principal effectue l'établissement de la liaison.

Dans la version 12.1-49.x, seules les actions de transfert et de réinitialisation sont prises en charge pour le point de liaison CLIENTHELLO_REQ. Les préfixes d'expression suivants sont disponibles :

- CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
- CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION
- CLIENT.SSL.CLIENT_HELLO.IS_RENEGOTIATE
- CLIENT.SSL.CLIENT_HELLO.IS_REUSE
- CLIENT.SSL.CLIENT_HELLO.IS_SCSV
- CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET
- CLIENT.SSL.CLIENT_HELLO.LENGTH
- CLIENT.SSL.CLIENT_HELLO.SNI
- CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPROTOCOL (à partir de la version 13.0 build 61.x)

Pour obtenir une description de ces préfixes, voir Expressions de stratégie avancées : analyse SSL.

Un paramètre `forward` est ajouté à la commande `add SSL action` et un nouveau point de liaison `CLIENTHELLO_REQ` est ajouté à la commande `bind ssl vserver`.

Configuration à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ssl action <name> -forward <virtual server name>

add ssl policy <name> -rule <expression> -action <string>

bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type <type>
<!--NeedCopy-->
```

EXEMPLE :


```
add ssl action act1 -forward v2

add ssl policy pol1 -rule client.ssl.client_hello.ciphers.has_hexcode(0
   x002f) -action act1

bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
<!--NeedCopy-->
```

Configuration à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Stratégies**.

Créez une action SSL :

1. Dans **Actions SSL**, cliquez sur **Ajouter**.
2. Dans **Créer une action SSL**, attribuez un nom à l'action.
3. Dans **Forward Action Virtual Server**, sélectionnez un serveur virtuel existant ou ajoutez un nouveau serveur virtuel vers lequel transférer le trafic.
4. Définissez éventuellement d'autres paramètres.
5. Cliquez sur **Create**.

Créez une politique SSL :

1. Dans **Politiques SSL**, cliquez sur **Ajouter**.
2. Dans **Créer une politique SSL**, attribuez un nom à la politique.
3. Dans **Action**, sélectionnez l'action que vous avez créée précédemment.
4. Dans **Expression Editor**, entrez la règle à évaluer.
5. Cliquez sur **Create**.

Créez ou ajoutez un serveur virtuel et une politique de liaison :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ajoutez ou sélectionnez un serveur virtuel.
3. Dans **Paramètres avancés**, cliquez sur **Stratégies SSL**.
4. Cliquez dans la section Politique SSL.
5. Dans **Sélectionner une stratégie**, sélectionnez la politique que vous avez créée précédemment.
6. Dans **Policy Binding**, spécifiez une priorité pour la politique.
7. Dans **Type**, sélectionnez **CLIENTHELLO_REQ**.
8. Cliquez sur **Bind**.
9. Cliquez sur **Terminé**.

Pour connaître la configuration de bout en bout pour les cas d'utilisation les plus courants, consultez les rubriques suivantes :

- Configurez l'action SSL pour transférer le trafic client si l'appliance ne possède pas de certificat SNI (spécifique au domaine).
- Configurez une action SSL pour transférer le trafic client en fonction du protocole dans l'extension ALPN du message Hello du client.
- Configurez l'action SSL pour transférer le trafic client si un chiffrement n'est pas pris en charge sur ADC.

Action SSL pour sélectionner sélectivement des autorités de certification basées sur SNI pour l'authentification du client

Vous pouvez envoyer uniquement la liste des autorités de certification basée sur le SNI (domaine) dans la demande de certificat client plutôt que la liste de toutes les autorités de certification liées à un serveur virtuel SSL. Par exemple, lorsqu'un bonjour client est reçu, seuls les certificats CA basés sur l'expression de politique SSL (par exemple, SNI) sont envoyés. Pour envoyer un ensemble spécifique de certificats, vous devez créer un groupe de certificats CA. Liez ensuite ce groupe à une action SSL, puis liez l'action à une politique SSL. Si la politique liée au serveur virtuel recevant le trafic client est évaluée comme vraie après avoir analysé le client hello, seul un groupe de certificats CA spécifique est envoyé dans le certificat de demande du client.

Auparavant, vous deviez lier des certificats CA à un serveur virtuel SSL. Grâce à cette amélioration, vous pouvez simplement ajouter des groupes de certificats CA et les associer à une action SSL.

Remarque : Activez l'authentification du client et le SNI sur le serveur virtuel SSL. Liez les bons certificats SNI au serveur virtuel.

Procédez comme suit :

1. Ajoutez un groupe de certificats CA.
2. Ajoutez des paires de clés de certificat.
3. Liez les paires de clés de certificat à ce groupe.
4. Ajoutez une action SSL.
5. Ajoutez une politique SSL. Spécifiez l'action dans la politique.
6. Liez la politique à un serveur virtuel SSL. Spécifiez le point de liaison sous la forme CLIENTHELLO_REQ.

Configuration à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes dans l'ordre suivant :

```
add ssl caCertGroup <caCertGroupName>
```



```
add ssl certkey <certkey_name> -cert <cert> -key <key>
bind ssl caCertGroup <caCertGroupName> <certkey_name>
add ssl action <name> -caCertGrpName <string>
add ssl policy <name> -rule <expression> -action <string>
bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type CLIENTHELLO_REQ
<!--NeedCopy-->
```

Exemple :

```
add ssl cacertGroup ca_cert_group

add ssl certkey ca_certkey1 -cert cacert1 -key cakey1
add ssl certkey ca_certkey2 -cert cacert2 -key cakey2
add ssl certkey snicert -cert snicert -key snikey

bind ssl cacertGroup ca_cert_group ca_certkey1
bind ssl caCertGroup ca_cert_group ca_certkey2
<!--NeedCopy-->
```

```
sh ssl caCertGroup ca_cert_group

CA GROUP NAME:     ca_cert_group
ACTIONS REFERRING: 1

1) CertKey Name: ca_certkey1   CA Certificate   CRLCheck: Optional
   CA_Name Sent
2) CertKey Name: ca_certkey2   CA Certificate   CRLCheck: Optional
   CA_Name Sent
<!--NeedCopy-->
```

```
add ssl action pick_ca_group -cacertGrpName ca_cert_group
<!--NeedCopy-->
```

```
sh ssl action pick_ca_group
1) Name: pick_ca_group
   Type: Data Insertion
   PickCaCertGroup: ca_cert_group
   Hits: 0
   Undef Hits: 0
   Action Reference Count: 1
<!--NeedCopy-->
```



```
add ssl policy snipolicy -rule client.ssl.client_hello.sni.contains("
    abc") -action pick_ca_group
bind ssl vserver v_SSL -policyName snipolicy -type CLIENTHELLO_REQ -
    priority 10
<!--NeedCopy-->
```

```
sh ssl policy snipolicy
    Name: snipolicy
    Rule: client.ssl.client_hello.sni.contains("abc")
    Action: pick_ca_group
    UndefAction: Use Global
    Hits: 0
    Undef Hits: 0


    Policy is bound to following entities
1)  Bound to: CLIENTHELLO_REQ VSERVER v_SSL
    Priority: 10
<!--NeedCopy-->
```

```
set ssl vserver v_SSL -clientauth ENABLED -SNIEnable ENABLED
bind ssl vserver v_SSL -certkeyName snicert -sniCert
<!--NeedCopy-->
```

```
sh ssl vserver v_SSL

    Advanced SSL configuration for VServer v_SSL:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED   Refresh Count: 0
    Session Reuse: ENABLED   Timeout: 120 seconds
    Cipher Redirect: DISABLED
    SSLv2 Redirect: DISABLED
    ClearText Port: 0
    Client Auth: ENABLED   Client Cert Required: Mandatory
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: ENABLED
    OCSP Stapling: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED
         TLSv1.2: ENABLED  TLSv1.3: DISABLED
```



```
    Push Encryption Trigger: Always
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1

    ECC Curve: P_256, P_384, P_224, P_521

1)  CertKey Name: snicert   Server Certificate for SNI


    Data policy
1)  Policy Name: snipolicy  Priority: 10



1)  Cipher Name: DEFAULT
    Description: Default cipher list with encryption strength >= 128bit
<!--NeedCopy-->
```

Configuration à l'aide de l'interface graphique

Créez un groupe de certificats CA et liez les certificats au groupe :

1. Accédez à **Gestion du trafic > SSL > Groupe de certificats d'autorité**de certification.
2. Cliquez sur **Ajouter** et attribuez un nom au groupe.
3. Cliquez sur **Create**.
4. Sélectionnez le **groupe de certificats CA**, puis cliquez sur **Afficher les liaisons**.
5. Cliquez sur **Bind**.
6. Sur la page **CA Certificate Binding**, sélectionnez un certificat existant ou cliquez sur Ajouter pour ajouter un nouveau certificat.
7. Cliquez sur **Sélectionner**, puis sur **Lier**.
8. Pour lier un autre certificat, répétez les étapes 5 à 7.
9. Cliquez sur **Fermer**.

Accédez à **Gestion du trafic > SSL > Stratégies**.

Créez une action SSL :

1. Dans **Actions SSL**, cliquez sur **Ajouter**.
2. Dans **Créer une action SSL**, attribuez un nom à l'action.
3. Dans **Forward Action Virtual Server**, sélectionnez un serveur virtuel existant ou ajoutez un serveur virtuel vers lequel transférer le trafic.

4. Définissez éventuellement d'autres paramètres.
5. Cliquez sur **Create**.

Créez une politique SSL :

1. Dans **Politiques SSL**, cliquez sur **Ajouter**.
2. Dans **Créer une politique SSL**, attribuez un nom à la politique.
3. Dans **Action**, sélectionnez l'action créée précédemment.
4. Dans **Expression Editor**, entrez la règle à évaluer.
5. Cliquez sur **Create**.

Créez ou ajoutez un serveur virtuel et une politique de liaison :

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
2. Ajoutez ou sélectionnez un serveur virtuel.
3. Dans **Paramètres avancés**, cliquez sur **Stratégies SSL**.
4. Cliquez dans la section Politique SSL.
5. Dans **Sélectionner une stratégie**, sélectionnez la politique que vous avez créée précédemment.
6. Dans **Policy Binding**, spécifiez une priorité pour la politique.
7. Dans **Type**, sélectionnez **CLIENTHELLO_REQ**.
8. Cliquez sur **Bind**.
9. Cliquez sur **Terminé**.

Dissocier un groupe de certificats CA à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Groupe de certificats d'autorité**de certification.
2. Sélectionnez un groupe de certificats et cliquez sur **Afficher les liaisons**.
3. Sélectionnez le certificat à supprimer du groupe et cliquez sur **Dissocier.**
4. Si vous êtes invité à confirmer, cliquez sur **Oui••.
5. Cliquez sur **Fermer**.

Supprimer un groupe de certificats CA à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Groupe de certificats d'autorité**de certification.
2. Sélectionnez un groupe de certificats et cliquez sur **Supprimer**.
3. Si vous y êtes invité, cliquez sur **Oui**.

Liaison de stratégie SSL

May 5, 2023

Vous pouvez lier les politiques SSL de manière globale ou uniquement à un serveur virtuel de type SSL. Les politiques liées globalement sont évaluées une fois que toutes les politiques liées aux services, aux serveurs virtuels ou à d'autres points de liaison NetScaler ont été évaluées. Si les données entrantes correspondent à l'une des règles configurées dans la politique SSL, la politique est déclenchée et l'action qui y est associée est exécutée.

Lorsque vous liez une politique SSL à un serveur virtuel, vous devez sélectionner l'un des points de liaison suivants :

- DEMANDE (point de liaison par défaut). L'évaluation des politiques est effectuée dans la couche HTTP une fois l'établissement de connexion SSL terminé.)
- INTERCEPT_REQ (Cette option s'applique à une configuration de Citrix Secure Web Gateway. Pour plus d'informations, voir Infrastructure de stratégies SSL pour l'interceptionSSL).
- CLIENTHELLO_REQ

De même, lorsque vous dissociez une politique d'un serveur virtuel, vous devez spécifier le point de liaison.

Si vous spécifiez CLIENTHELLO_REQ comme point de liaison, la politique est évaluée lorsqu'un message d'bonjour client est reçu. Les actions autorisées sont RESET, FORWARD et `caCertGrpName`. L'action de réinitialisation met fin à la connexion. L'action de transfert transmet la demande à un serveur virtuel d'équilibrage de charge pour traitement. L'action `caCertGrpName` sélectionne les autorités de certification basées sur SNI pour l'authentification du client. Pour plus d'informations sur les actions SSL, consultez Actions intégrées SSL et actions définies parl'utilisateur.

Remarque : L'action cacertgrpName n'est pas prise en charge avec le protocole TLS 1.3.

Liez une politique SSL à l'échelle mondiale à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour lier une politique SSL globale et vérifier la configuration :

```
bind ssl global - policyName <string> [- priority <positive_integer>]
show ssl global
<!--NeedCopy-->
```

Exemple :

```
bind ssl global -policyName Policy-SSL-2 -priority 90
Done

sh ssl global

```



```
6       1) Name: Policy-SSL-2 Priority: 90
7       2) Name: Policy-SSL-1 Priority: 100
8       Done
9 <!--NeedCopy-->
```

Liez une politique SSL de manière globale à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **SSL** > **Politiques**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales**.
3. **Dans la**boîte de dialogue Lier/dissocier les politiques SSL à l'ensemble, cliquez sur**Insérer une politique.**
4. Dans la liste **Nom de la politique**, sélectionnez une politique.
5. Vous pouvez également faire glisser l'entrée vers une nouvelle position dans la banque de règles pour mettre à jour automatiquement le niveau de priorité.
6. Cliquez sur **OK**. Un message apparaît dans la barre d'état, indiquant que la stratégie a été correctement liée.

Liez ou dissociez une politique SSL à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez la commande suivante pour lier une politique SSL à un serveur virtuel et vérifier la configuration :

```
1 bind ssl vserver <vServerName> -policyName <string> -priority <
     positive_integer> -type <type>
2
3 unbind ssl vserver <vServerName> -policyName <string> -priority <
     positive_integer> -type <type>
4
5 <!--NeedCopy-->
```

Exemple :

```
1 bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
2 <!--NeedCopy-->
```

```
1 unbind ssl vserver v1 -policyName pol1 -priority 1 -type
     CLIENTHELLO_REQ
2 <!--NeedCopy-->
```

```
1 show ssl vserver vs-server
2
```



```
Advanced SSL configuration for VServer vs-server:

DH: DISABLED

Ephemeral RSA: ENABLED          Refresh Count: 1000

Session Reuse: ENABLED          Timeout: 120 seconds

Cipher Redirect: DISABLED

SSLv2 Redirect: DISABLED

ClearText Port: 80

Client Auth: DISABLED

SSL Redirect: ENABLED

SSL-REDIRECT Port Rewrite: ENABLED

Non FIPS Ciphers: DISABLED

SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      Policy Name: ssl-policy-1        Priority: 10

1)      Cipher Name: DEFAULT

            Description: Predefined Cipher Alias

Done
<!--NeedCopy-->
```

Liez une politique SSL à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez un serveur virtuel SSL.
2. Dans **Paramètres avancés**, sélectionnez **Stratégie SSL**. Cliquez dans la section **Stratégie SSL** pour lier une politique au serveur virtuel.
3. Sur la page **Policy Binding**, sélectionnez une politique existante ou ajoutez-en une nouvelle.
4. Spécifiez la priorité et le type (point de liaison) de la politique.
5. Sélectionnez **Bind**.
6. Sélectionnez **Terminé**.

Étiquettes de stratégie SSL

June 2, 2023

Les étiquettes de stratégie sont des supports pour les stratégies. Une étiquette de stratégie permet de gérer un groupe de stratégies, appelé banque de stratégies, qui peut être invoquée à partir d'une autre stratégie. Les étiquettes de stratégie SSL peuvent être des étiquettes de contrôle ou des étiquettes de données, selon le type de stratégie inclus dans l'étiquette de stratégie. Vous pouvez ajouter uniquement des stratégies de données dans une étiquette de stratégie de données et uniquement des stratégies de contrôle dans une étiquette de stratégie de contrôle. Pour créer la banque de stratégies, liez les stratégies à l'étiquette et spécifiez l'ordre d'évaluation de chaque stratégie par rapport aux autres dans la banque de stratégies pour l'étiquette de stratégie. Dans l'interface de ligne de commande, vous entrez deux commandes pour créer une étiquette de stratégie et lier des stratégies à cette étiquette de stratégie. Dans l'utilitaire de configuration, vous pouvez sélectionner des options dans une boîte de dialogue.

Remarque : Les étiquettes de stratégie de contrôle de type ne sont pas prises en charge avec le protocole TLS 1.3.

Créez une étiquette de stratégie SSL et liez les stratégies à l'étiquette à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ssl policylabel <labelName> -type ( CONTROL | DATA )

bind ssl policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>) ]
<!--NeedCopy-->
```

Exemple :

```
add ssl policylabel cpl1 -type CONTROL
add ssl policylabel dpl1 -type DATA

add ssl action act1 -clientauth DOCLIENTAUTH
add ssl policy ctrlpol -rule HTTP.REQ.METHOD.EQ("GET") -action act1

add ssl action act2 -clientCert ENABLED -certHeader "X-Client-Cert"
add ssl policy datapol -rule CLIENT.SSL.CLIENT_CERT.EXISTS -action act2

bind ssl policylabel cpl1 ctrlpol 1
bind ssl policylabel dpl1 datapol 1
```



```
12
13 > sh ssl policylabel
14 Control policylabels
15 1)    Label Name: cpl1
16     Type: CONTROL
17     Number of bound policies: 1
18     Number of times invoked: 0
19
20 Data policylabels
21 1)  Label Name: dpl1
22     Type: DATA
23     Number of bound policies: 1
24     Number of times invoked: 0
25 Done
26 >
27 <!--NeedCopy-->
```

Configurer une étiquette de stratégie SSL et lier les stratégies à l'étiquette à l'aide de l'interface graphique

Accédez à **Gestion du trafic > SSL > Étiquettes de stratégie**, puis configurez une étiquette de stratégie SSL.

Journalisation SSL sélective

September 27, 2022

Dans un vaste déploiement comprenant des milliers de serveurs virtuels, toutes les informations liées à SSL sont enregistrées. Auparavant, il n'était pas facile de filtrer les succès et les échecs de l'authentification client et de la prise de contact SSL pour quelques serveurs virtuels critiques. L'utilisation de l'ensemble du journal pour obtenir ces informations a été une tâche fastidieuse et fastidieuse car l'infrastructure n'offrait pas le contrôle nécessaire pour filtrer les journaux. Vous pouvez désormais enregistrer les informations relatives au protocole SSL pour un serveur virtuel spécifique ou pour un groupe de serveurs virtuels dans le `ns.log`. Ces informations sont particulièrement utiles en cas d'échec de débogage.

Avec le paramètre DEBUG, toutes les informations relatives au SSL sont enregistrées `ns.log`. Toutefois, lorsque vous configurez un profil de journal SSL, seules les informations relatives à l'authentification du client et à la connexion SSL sont enregistrées. Pour enregistrer ces informations, effectuez les opérations suivantes :

1. Définissez DEBUG sur les paramètres Syslog.
2. Configurez un profil de journal SSL. Activez la journalisation de l'authentification du client et des échoues/réussites de l'établissement de connexion SSL et des échecs uniquement Tous les quatre sont enregistrés lorsque vous associez le profil de journal SSL au profil SSL. Seuls les échecs ou les succès de l'authentification du client et les échecs ne sont enregistrés que lorsque vous associez le profil de journal SSL à l'action SSL.
3. Joignez le profil de journal SSL à un profil SSL ou à une action SSL.

Voir l'exemple de sortie ns.log pour une authentification client réussie à la fin de cette page.

Définir le niveau DEBUG

Définissez le niveau du journal Syslog sur DEBUG. À l'invite de commandes, tapez :

```
set audit syslogParams -logLevel DEBUG
```

Lorsque le débogage est défini, les journaux SSL pour le front-end (serveurs virtuels) et le back-end (services et groupes de services) sont inclus. Toutefois, la journalisation SSL sélective ne permet de contrôler que le frontal.

Profil de journal SSL

Un profil de journal SSL permet de contrôler la journalisation des événements suivants pour un serveur virtuel ou un groupe de serveurs virtuels :

- Succès et échecs de l'authentification du client, ou échecs uniquement.
- Succès et échecs de l'établissement de liaison SSL, ou échecs uniquement.

Par défaut, tous les paramètres sont désactivés.

Un profil de journal SSL peut être défini sur un profil SSL ou sur une action SSL. S'il est défini sur un profil SSL, vous pouvez enregistrer à la fois l'authentification du client et les informations de réussite et d'échec de la prise de contact SSL. Si cette option est définie sur une action SSL, vous pouvez uniquement consigner les informations de réussite et d'échec de l'authentification du client, car la prise de contact est terminée avant l'évaluation de la stratégie.

Le succès et les échecs de l'authentification client et de la prise de contact SSL sont consignés même si vous ne configurez pas de profil de journal SSL. Toutefois, la journalisation sélective n'est possible que si un profil de journal SSL est utilisé.

> **Remarque :**
>
> Le profil de journal SSL est pris en charge dans les configurations de cluster et de haute disponibilité.

Ajouter un profil de journal SSL à l'aide de la CLI

À l'invite de commandes, tapez :

```
add ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )] [-
    ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
    DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Paramètres :

Nom :

Nom du profil de journal SSL. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Impossible de modifier une fois le profil créé.

Le nom est un argument obligatoire. Longueur maximale : 127

`sslLogClAuth`:

Consignez tous les événements d'authentification client. Inclut les événements de réussite et d'échec.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

`ssllogClAuthFailures`:

Consignez tous les échecs d'authentification du client.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

`sslLogHS`:

Consigne tous les événements liés à la prise de contact SSL. Inclut les événements de réussite et d'échec.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

`sslLogHSfailures`:

Enregistrez tous les événements d'échec liés à la prise de contact SSL.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

Exemple :


```
> add ssl logprofile ssllog10 -sslLogClAuth ENABLED -sslLogHS ENABLED

 Done

sh ssllogprofile ssllog10

1)      Name: ssllog10

        SSL log ClientAuth [Success/Failures] : ENABLED

        SSL log ClientAuth [Failures] : DISABLED

        SSL log Handshake [Success/Failures] : ENABLED

        SSL log Handshake [Failures] : DISABLED

 Done
<!--NeedCopy-->
```

Ajouter un profil de journal SSL à l'aide de l'interface graphique

Accédez à **Système > Profils > Profil de journal SSL** et ajoutez un profil.

Modifier un profil de journal SSL à l'aide de la CLI

À l'invite de commandes, tapez :

```
set ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )][-
   ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
   DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Exemple :

```
set ssllogprofile ssllog10 -ssllogClAuth en -ssllogClAuthFailures en -
   ssllogHS en -ssllogHSfailures en

Done

sh ssllogprofile ssllog10

    1)            Name: ssllog10

```



```
                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : ENABLED
                    SSL log Handshake [Failures] : ENABLED
     Done
<!--NeedCopy-->
```

Modifier un profil de journal SSL à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profil de journal SSL**, sélectionnez un profil, puis cliquez sur **Modifier**.
2. Apportez des modifications et cliquez sur **OK**.

Afficher tous les profils de journaux SSL à l'aide de la CLI

À l'invite de commandes, tapez :

```
sh ssl logprofile
<!--NeedCopy-->
```

Exemple :

```
sh ssl logprofile

    1)            Name: ssllogp1
                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : ENABLED

    2)            Name: ssllogp2
                    SSL log ClientAuth [Success/Failures] : DISABLED
                    SSL log ClientAuth [Failures] : DISABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : DISABLED

    3)            Name: ssllogp3
                    SSL log ClientAuth [Success/Failures] : DISABLED
                    SSL log ClientAuth [Failures] : DISABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : DISABLED

    4)            Name: ssllog10
```



```
                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : ENABLED
                    SSL log Handshake [Failures] : ENABLED
Done
<!--NeedCopy-->
```

Afficher tous les profils de journaux SSL à l'aide de l'interface graphique

Accédez à **Système > Profils > Profil de journal SSL**. Tous les profils sont listés.

Attacher un profil de journal SSL à un profil SSL

Vous pouvez attacher (définir) un profil de journal SSL à un profil SSL lorsque vous créez un profil SSL, ou plus tard en modifiant le profil SSL. Vous pouvez consigner à la fois l'authentification du client et les succès et les échecs de la poignée

> **Important :**
>
> Le profil SSL par défaut doit être activé pour que vous puissiez joindre un profil de journal SSL. Pour plus d'informations sur l'activation du profil SSL par défaut, consultez Activer le profil par défaut.

Attacher un profil de journal SSL à un profil SSL à l'aide de l'interface de ligne de

À l'invite de commandes, tapez :

```
set ssl profile <name> [-ssllogProfile <string>]
<!--NeedCopy-->
```

Exemple :

```
set ssl profile fron_1 -ssllogProfile ssllog10
<!--NeedCopy-->
```

Attacher un profil de journal SSL à un profil SSL à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profil SSL**.
2. Cliquez sur **Modifier** et dans **Profil de journal SSL**, spécifiez un profil.

Attacher un profil de journal SSL à une action SSL

Vous pouvez définir un profil de journal SSL uniquement lors de la création d'une action SSL. Vous ne pouvez pas modifier une action SSL pour définir le profil de journal. Associez l'action à une stratégie. Vous pouvez uniquement consigner les réussites et les échecs d'authentification des clients.

Attacher un profil de journal SSL à une action SSL à l'aide de la CLI

À l'invite de commandes, tapez :

```
add ssl action <name> -clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) -
   ssllogProfile <string>
<!--NeedCopy-->
```

Exemple :

```
> add ssl action act1 -clientAuth DoCLIENTAUTH -ssllogProfile ssllog10

Done

> sh ssl action act1

    1)            Name: act1
                    Type: Client Authentication (DOCLIENTAUTH)
                    Hits: 0
                    Undef Hits: 0
                    Action Reference Count: 0
                    SSLlogProfile: ssllog10
Done
<!--NeedCopy-->
```

Attacher un profil de journal SSL à une action SSL à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Stratégies**, puis cliquez sur **Actions SSL**.
2. Cliquez sur **Ajouter**.
3. Dans Authentification client, sélectionnez **ACTIVÉ**.
4. Dans Profil de journal SSL, sélectionnez un profil dans la liste ou cliquez sur « + » pour créer un profil.
5. Cliquez sur **Créer**.

Exemple de sortie du fichier journal

Voici un exemple de sortie de journal`ns.log` pour une authentification client réussie.


```
1 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 158 0 :  SPCBId 671 -
    ClientIP 10.102.1.98 - ClientPort 49451 - VserverServiceIP
    10.102.57.82 - VserverServicePort 443 - ClientVersion TLSv1.2 -
    CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" - Session
    New - CLIENT_AUTHENTICATED -SerialNumber "2A" - SignatureAlgorithm "
    sha1WithRSAEncryption" - ValidFrom "Sep 22 09:15:20 2008 GMT" -
    ValidTo "Feb  8 09:15:20 2036 GMT" - HandshakeTime 10 ms
2 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 159 0 :  SPCBId 671
    - IssuerName " C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix"
3 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 160 0 :  SPCBId 671
     - SubjectName " C=IN,ST=KAR,O=Citrix Pvt Ltd,OU=A,CN=B"
4 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 161 0 :  Backend SPCBId
     674 - ServerIP 10.102.57.85 - ServerPort 443 - ProtocolVersion
    TLSv1.2 - CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" -
     Session Reuse - SERVER_AUTHENTICATED -SerialNumber "3E" -
    SignatureAlgorithm "sha1WithRSAEncryption" - ValidFrom "Sep 24
    06:40:37 2008 GMT" - ValidTo "Feb 10 06:40:37 2036 GMT" -
    HandshakeTime 1 ms
5 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 162 0 :  SPCBId 674
    - IssuerName " C=IN,ST=KAR,O=Citrix Pvt Ltd"
6 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 163 0 :  SPCBId 674
     - SubjectName " C=IN,ST=P,L=Q,O=R"
7 <!--NeedCopy-->
```

Prise en charge du protocole DTLS

May 5, 2023

> **Remarques**
>
> - Le protocole DTLS 1.2 est pris en charge sur les appliances suivantes :
>   - NetScaler MPX/SDX (N2 and N3 based) and VPX appliances. It is not supported on external HSMs.
>   - NetScaler appliances containing Intel Coleto and Intel Lewisburg SSL chips.

  - Front-end of NetScaler VPX appliances.
  - Front-end of NetScaler appliances containing Intel Coleto SSL chips. For more information about the platforms containing Intel Coleto SSL chips, see Support for Intel Coleto SSL chip-based platforms.
  - Front-end of NetScaler MPX (N3 based) appliances except the MPX 14000 FIPS appliances.

- Les groupes de services de type DTLS ne sont pas pris en charge.
- Pour plus d'informations sur la prise en charge du Enlightened Data Transport (EDT) pour NetScaler Gateway, consultez la section Support du transport de données éclairé HDX.
- Pour plus d'informations sur les plateformes et les versions prises en charge, consultez la matrice de compatibilité matérielle-logicielle de NetScaler MPX

Les protocoles SSL et TLS ont traditionnellement été utilisés pour sécuriser le trafic en continu. Ces deux protocoles sont basés sur le protocole TCP, qui est lent. De plus, TLS ne peut pas gérer les paquets perdus ou réordonnés.

UDP est le protocole préféré pour les applications audio et vidéo, telles que Lync, Skype, iTunes, YouTube, les vidéos de formation et Flash. Toutefois, UDP n'est ni sécurisé ni fiable. Le protocole DTLS est conçu pour sécuriser les données via UDP et est utilisé pour des applications telles que le streaming multimédia, la VOIP et les jeux en ligne pour la communication. Dans DTLS, chaque message de prise de main se voit attribuer un numéro de séquence spécifique au sein de cette prise de liaison. Lorsqu'un homologue reçoit un message de prise de main, il peut rapidement déterminer si ce message est le prochain message attendu. Si c'est le cas, l'homologue traite le message. Si ce n'est pas le cas, le message est mis en file d'attente pour être traité une fois que tous les messages précédents ont été reçus.

Créez un serveur virtuel DTLS et un service de type UDP. Par défaut, un profil DTLS (nsdtls_default_profile) est lié au serveur virtuel. Vous pouvez éventuellement créer et lier un profil DTLS défini par l'utilisateur au serveur virtuel.

Remarque : Les chiffrements RC4 ne sont pas pris en charge sur un serveur virtuel DTLS.

Configuration DTLS

Vous pouvez utiliser la ligne de commande (CLI) ou l'utilitaire de configuration (GUI) pour configurer DTLS sur votre appliance ADC.

Remarque : Le protocole DTLS 1.2 est pris en charge sur le front-end d'une appliance NetScaler VPX. Lors de la configuration d'un serveur virtuel DTLSv1.2, spécifiez DTLS12. La valeur par défaut est DTLS1.

À l'invite de commande, tapez :


```
set ssl vserver DTLS [-dtls1 ( ENABLED | DISABLED )] [-dtls12 ( ENABLED |
DISABLED )]
```

Créer une configuration DTLS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add lb vserver <vserver_name> DTLS <IPAddress>  <port>
add service  <service_name>  <IPAddress> UDP 443
bind lb vserver  <vserver_name>  <udp_service_name>
<!--NeedCopy-->
```

Les étapes suivantes sont facultatives :

```
add dtlsProfile dtls-profile -maxretryTime <positive_integer>
set ssl vserver <vserver_name> -dtlsProfileName <dtls_profile_name>
<!--NeedCopy-->
```

Créer une configuration DTLS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Créez un serveur virtuel de type DTLS et liez un service UDP au serveur virtuel.
3. Un profil DTLS par défaut est lié au serveur virtuel DTLS. Pour lier un profil différent, dans Paramètres SSL, sélectionnez un autre profil DTLS. Pour créer un profil, cliquez sur le signe plus (+) en regard de Profil DTLS.

Prise en charge de SNI sur un serveur virtuel DTLS

Pour plus d'informations sur SNI, voir Configurer un serveur virtuel SNI pour l'hébergement sécurisé de plusieurs sites.

Configurer SNI sur un serveur virtuel DTLS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl vserver <vServerName> -SNIEnable ENABLED
bind ssl vserver <vServerName> -certkeyName <string> -SNICert
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Exemple :


```
set ssl vserver v1 -sniEnable ENABLED
bind ssl vserver  v1 -certkeyName san2 -sniCert
bind ssl vserver  v1 -certkeyName san13  - sniCert
bind ssl vserver  v1 -certkeyName san17  - sniCert
<!--NeedCopy-->
```

```
sh ssl vserver v1

Advanced SSL configuration for VServer v1:
DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED
Refresh Count: 0
Session Reuse: ENABLED
Timeout: 1800 seconds
Cipher Redirect: DISABLED

ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: ENABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
DTLSv1: ENABLED
Send Close-Notify: YES
Strict Sig-Digest Check: DISABLED
Zero RTT Early Data: DISABLED
DHE Key Exchange With PSK: NO
Tickets Per Authentication Context: 1

DTLS profile name: nsdtls_default_profile

ECC Curve: P_256, P_384, P_224, P_521

1) CertKey Name: ca
CA Certificate  OCSPCheck: OptionalCA_Name Sent
2) CertKey Name: san2 Server Certificate for SNI
3) CertKey Name: san17 Server Certificate for SNI
4) CertKey Name: san13 Server Certificate for SNI


```



```
1) Cipher Name: DEFAULT
Description: Default cipher list with encryption strength >= 128bit
Done
<!--NeedCopy-->
```

Configurez SNI sur un serveur virtuel DTLS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Ouvrez un serveur virtuel DTLS et, dans Certificats, cliquez sur **Certificat de serveur**.
3. Ajoutez un certificat ou sélectionnez un certificat dans la liste, puis sélectionnez **Certificat de serveur pour SNI**.
4. Dans **Paramètres avancés**, cliquez sur **Paramètres SSL**.
5. Sélectionnez **Activer SNI**.

Fonctionnalités non prises en charge par un serveur virtuel DTLS

Les options suivantes ne peuvent pas être activées sur un serveur virtuel DTLS :

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Déclencheur de cryptage push
- SSLv2Redirect
- SSLv2URL

Paramètres non utilisés par un serveur virtuel DTLS

Un serveur virtuel DTLS ignore les paramètres SSL suivants, même s'ils sont définis :

- Nombre de paquets de déclencheurs de chiffrement
- Délai de déclenchement du chiffrement PUSH
- Taille quantique SSL
- Délai d'expiration du déclencheur
- Format d'insertion du nom du sujet/émetteur

Configuration de la renégociation sur un service DTLS

La renégociation non sécurisée est prise en charge sur un service DTLS. Vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique pour configurer ce paramètre.

Configurer la renégociation sur un service DTLS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl parameter -denysslreneg NONSECURE
<!--NeedCopy-->
```

Exemple :

```
set ssl parameter -denysslreneg NONSECURE


sh ssl parameter
Advanced SSL Parameters
-----------------------
SSL quantum size                                    : 8 KB
Max CRL memory size                                 : 256 MB
Strict CA checks                                    : NO
Encryption trigger timeout                          : 100 ms
Send Close-Notify                                   : YES
Encryption trigger packet count                     : 45
Deny SSL Renegotiation                              : NONSECURE
Subject/Issuer Name Insertion Format                : Unicode
OCSP cache size                                     : 10 MB
Push flag                                           : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout                     : 1 ms
Crypto Device Disable Limit                         : 0
Global undef action for control policies            : CLIENTAUTH
Global undef action for data policies               : NOOP
Default profile                                     : DISABLED
SSL Insert Space in Certificate Header              : YES
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
Software Crypto acceleration CPU Threshold          : 0
Hybrid FIPS Mode                                    : DISABLED
Signature and Hash Algorithms supported by TLS1.2   : ALL
SSL Interception Error Learning and Caching         : DISABLED
SSL Interception Maximum Error Cache Memory         : 0 Bytes
Done
<!--NeedCopy-->
```

Configurer la renégociation sur un service DTLS à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**.

2. Sélectionnez un service DTLS et cliquez sur **Modifier**.
3. Accédez à **SSL** > **Paramètres avancés**.
4. Sélectionnez **Refuser la renégociation SSL**.

Fonctionnalités non prises en charge par un service DTLS

Les options suivantes ne peuvent pas être activées sur un service DTLS :

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Déclencheur de cryptage push
- SSLv2Redirect
- SSLv2URL
- SNI
- Renégociation sécurisée

Paramètres non utilisés par un service DTLS

Un service DTLS ignore les paramètres SSL suivants, même s'ils sont définis :

- Nombre de paquets de déclencheurs de chiffrement
- Délai de déclenchement du chiffrement PUSH
- Taille quantique SSL
- Délai d'expiration du déclencheur
- Format d'insertion du nom du sujet/émetteur

> **Remarque :**
>
> La connexion de réutilisation de session SSL échoue sur un service DTLS car la réutilisation de session n'est actuellement pas prise en charge sur les services DTLS.
>
> **Solution :** désactivez manuellement la réutilisation de session sur un service DTLS. À l'interface de ligne de commande, tapez :
>
> ```
> set ssl service <dtls-service-name> -sessReuse DISABLED
> ```

Profil DTLS

Un profil DTLS avec les paramètres par défaut est automatiquement lié à un serveur virtuel DTLS. Toutefois, vous pouvez créer un profil DTLS avec des paramètres spécifiques en fonction de vos besoins.

Utilisez un profil DTLS avec un serveur virtuel DTLS ou un serveur virtuel DTLS VPN. Vous ne pouvez pas utiliser de profil SSL avec un serveur virtuel DTLS.

> **Remarque :**
>
> Modifiez le paramètre de taille d'enregistrement maximale dans le profil DTLS en fonction des modifications du MTU et de la taille des paquets. Par exemple, la taille d'enregistrement maximale par défaut de 1459 octets est calculée en fonction de la taille d'un en-tête d'adresse IPv4. Avec les enregistrements IPv6, la taille de l'en-tête est plus grande et, par conséquent, la taille d'enregistrement maximale doit être réduite pour répondre aux critères suivants.

```
max record size + UDP header(8bytes)+ IP header size < MTU
```

Exemple :

```
Default DTLS profile
    1) Name: nsdtls_default_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: ENABLED
    Terminate Session: DISABLED
    Max Packet Count: 120 bytes

Custom DTLS profile
    1) Name: ns_dtls_profile_ipv6_1
    PMTU Discovery: DISABLED
    Max Record Size: 1450 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: ENABLED
    Terminate Session: DISABLED
    Max Packet Count: 120 bytes
<!--NeedCopy-->
```

Créer un profil DTLS à l'aide de l'interface de ligne de commande

> **Remarques :**
>
> - Le paramètre `helloverifyrequest` est activé par défaut. L'activation de ce paramètre permet d'atténuer le risque qu'un attaquant ou des robots subisse le débit réseau, entraînant potentiellement un épuisement de la bande passante sortante. C'est-à-dire qu'il aide à atténuer l'attaque d'amplification DDoS DTLS.
> - Le paramètre `maxHoldQlen` est ajouté. Ce paramètre définit le nombre de datagrammes pouvant être mis en file d'attente à la couche DTLS pour traitement. Une valeur élevée du

> paramètre `maxHoldQlen` peut entraîner une accumulation de mémoire au niveau de la couche DTLS si le multiplexage UDP transmet un trafic UDP élevé. Par conséquent, il est recommandé de configurer une valeur inférieure. La valeur minimale est 32, la valeur maximale est 65535 et la valeur par défaut est 32.

Un nouveau paramètre `maxBadmacIgnorecount` est introduit dans le profil DTLS pour ignorer les enregistrements MAC erronés reçus dans une session DTLS. À l'aide de ce paramètre, les enregistrements erronés jusqu'à la valeur définie dans le paramètre sont ignorés. L'appliance met fin à la session uniquement après que la limite est atteinte et envoie une alerte.

Ce paramètre n'est effectif que si le paramètre `terminateSession` est activé.

```
ssl dtlsProfile <name> -maxRetryTime <positive_integer> -
    helloVerifyRequest ( ENABLED | DISABLED ) -terminateSession (ENABLED
     | DISABLED ) -maxHoldQLen <positive_integer> -maxBadmacIgnorecount
    <positive_integer>

helloVerifyRequest
              Send a Hello Verify request to validate the client.
              Possible values: ENABLED, DISABLED
              Default value: ENABLED

terminateSession
              Terminate the session if the message authentication code
                  (MAC)
              of the client and server do not match.
              Possible values: ENABLED, DISABLED
              Default value: DISABLED

maxHoldQLen
              Maximum number of datagrams that can be queued at DTLS
                  layer for
              processing
              Default value: 32
              Minimum value: 32
              Maximum value: 65535

maxBadmacIgnorecount
              Maximum number of bad MAC errors to ignore for a
                  connection prior disconnect. Disabling parameter
                  terminateSession
terminates session immediately when bad MAC is detected in the
    connection.
              Default value: 100
              Minimum value: 1
```



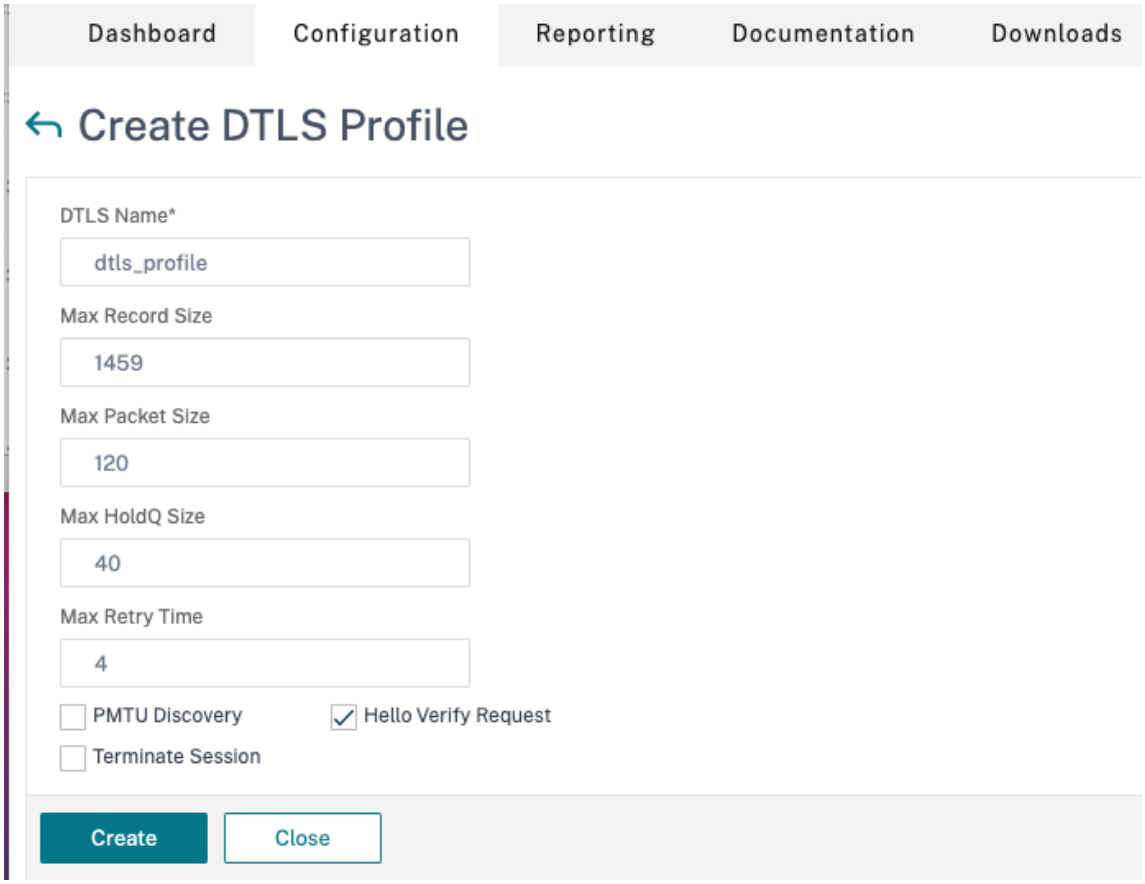
```
                Maximum value: 65535
<!--NeedCopy-->
```

Exemple :

```
> add ssl dtlsprofile dtls_profile -maxRetryTime 4 -helloVerifyRequest
   ENABLED -terminateSession ENABLED -maxHoldQLen 40 -
   maxBadmacIgnorecount 150
 Done
> sh dtlsprofile dtls_profile
1)  Name: dtls_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 4 sec
    Hello Verify Request: ENABLED
    Terminate Session: ENABLED
    Max Packet Count: 120 bytes
    Max HoldQ Size: 40 datagrams
    Max bad-MAC Ignore Count: 150

 Done
<!--NeedCopy-->
```

Créer un profil DTLS à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profils DTLS**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un profil DTLS**, saisissez les valeurs des différents paramètres.



3. Cliquez sur **Create**.

Exemple de configuration DTLS de bout en bout

```
enable ns feature SSL LB

add server s1 198.51.100.2

en ns mode usnip

add service svc_dtls s1 DTLS 443

add lb vserver v1 DTLS 10.102.59.244 443

bind ssl vserver v1 -ciphername ALL

add ssl certkey servercert -cert servercert_aia_valid.pem -key
   serverkey_aia.pem

bind ssl vserver v1 -certkeyname servercert

```



```
17 bind lb vserver lb1 svc_dtls
18
19 sh lb vserver v1
20
21                     v1 (10.102.59.244:4433) - DTLS     Type: ADDRESS
22                     State: UP
23                     Last state change was at Fri Apr 27 07:00:27 2018
24                     Time since last state change: 0 days, 00:00:04.810
25                     Effective State: UP
26                     Client Idle Timeout: 120 sec
27                     Down state flush: ENABLED
28                     Disable Primary Vserver On Down : DISABLED
29                     Appflow logging: ENABLED
30                     No. of Bound Services :  1 (Total) 0 (Active)
31                     Configured Method: LEASTCONNECTION
32                     Current Method: Round Robin, Reason: A new service
                          is bound         BackupMethod: ROUNDROBIN
33                     Mode: IP
34                     Persistence: NONE
35                     L2Conn: OFF
36                     Skip Persistency: None
37                     Listen Policy: NONE
38                     IcmpResponse: PASSIVE
39                     RHIstate: PASSIVE
40                     New Service Startup Request Rate: 0 PER_SECOND,
                          Increment Interval: 0
41                     Mac mode Retain Vlan: DISABLED
42                     DBS_LB: DISABLED
43                     Process Local: DISABLED
44                     Traffic Domain: 0
45                     TROFS Persistence honored: ENABLED
46                     Retain Connections on Cluster: NO
47
48     1) svc_dtls (10.102.59.190: 4433) - DTLS State: UP  Weight: 1
49 Done
50
51
52 sh ssl vserver v1
53
54                     Advanced SSL configuration for VServer v1:
55                     DH: DISABLED
56                     DH Private-Key Exponent Size Limit: DISABLED
                                  Ephemeral RSA: ENABLED
                                                      Refresh Count: 0
57                     Session Reuse: ENABLED                Timeout:
```



```
                          1800 seconds
                      Cipher Redirect: DISABLED
                      ClearText Port: 0
                      Client Auth: DISABLED
                      SSL Redirect: DISABLED
                      Non FIPS Ciphers: DISABLED
                      SNI: DISABLED
                      OCSP Stapling: DISABLED
                      HSTS: DISABLED
                      HSTS IncludeSubDomains: NO
                      HSTS Max-Age: 0
                      DTLSv1: ENABLED
                      Send Close-Notify: YES
                      Strict Sig-Digest Check: DISABLED
                      Zero RTT Early Data: DISABLED
                      DHE Key Exchange With PSK: NO
                      Tickets Per Authentication Context: 1
                      DTLS profile name: nsdtls_default_profile

                      ECC Curve: P_256, P_384, P_224, P_521

    1)            CertKey Name: servercert               Server
       Certificate

    1)            Cipher Name: DEFAULT
                    Description: Default cipher list with encryption
                       strength >= 128bit

    2)            Cipher Name: ALL
                    Description: All ciphers supported by NetScaler,
                       excluding NULL ciphers
     Done

sh service svc_dtls

                      svc_dtls (10.102.59.190:4433) - DTLS
                      State: UP
                      Last state change was at Fri Apr 27 07:00:26 2018
                      Time since last state change: 0 days, 00:00:22.790
                      Server Name: s1
                      Server ID : None                Monitor Threshold
                       : 0
                      Max Conn: 0        Max Req: 0           Max
                       Bandwidth: 0 kbits
                      Use Source IP: NO
```



```
                        Client Keepalive(CKA): NO
                        Access Down Service: NO
                        TCP Buffering(TCPB): NO
                        HTTP Compression(CMP): NO
                        Idle timeout: Client: 120 sec           Server: 120
                            sec
                        Client IP: DISABLED
                        Cacheable: NO
                        SC: OFF
                        SP: OFF
                        Down state flush: ENABLED
                        Monitor Connection Close : NONE
                        Appflow logging: ENABLED
                        Process Local: DISABLED
                        Traffic Domain: 0

     1)             Monitor Name: ping-default
                                      State: UP               Weight: 1
                                                          Passive: 0
                                    Probes: 5              Failed [Total
                                       : 0 Current: 0]
                                     Last response: Success - ICMP echo
                                        reply received.
                           Response Time: 2.77 millisec
      Done

sh ssl service svc_dtls

                        Advanced SSL configuration for Back-end SSL Service
                            svc_dtls:
                        DH: DISABLED
                        DH Private-Key Exponent Size Limit: DISABLED
                                  Ephemeral RSA: DISABLED
                        Session Reuse: ENABLED                 Timeout:
                           1800 seconds
                        Cipher Redirect: DISABLED
                        ClearText Port: 0
                        Server Auth: DISABLED
                        SSL Redirect: DISABLED
                        Non FIPS Ciphers: DISABLED
                        SNI: DISABLED
                        OCSP Stapling: DISABLED
                        DTLSv1: ENABLED
                        Send Close-Notify: YES
                        Strict Sig-Digest Check: DISABLED
```



```
                      Zero RTT Early Data: ???
                      DHE Key Exchange With PSK: ???
                      Tickets Per Authentication Context: ???
                      DTLS profile name: nsdtls_default_profile
                      ECC Curve: P_256, P_384, P_224, P_521
    1)              Cipher Name: DEFAULT_BACKEND
                      Description: Default cipher list for Backend SSL
                         session
     Done


> sh dtlsProfile nsdtls_default_profile
1)  Name: nsdtls_default_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: DISABLED
    Terminate Session: ENABLED
    Max Packet Count: 120 bytes
    Max HoldQ Size: 32 datagrams
    Max bad-MAC Ignore Count: 10

 Done
<!--NeedCopy-->
```

Prise en charge DTLS de l'adresse IPv6

DTLS est également pris en charge avec les adresses IPv6. Toutefois, pour utiliser DTLS avec des adresses IPv6, la taille d'enregistrement maximale doit être ajustée dans le profil DTLS.

Si la valeur par défaut est utilisée pour la taille d'enregistrement maximale, la connexion DTLS initiale peut échouer. Ajustez la taille d'enregistrement maximale à l'aide d'un profil DTLS.

Prise en charge du chiffrement DTLS

Par défaut, un groupe de chiffrement DTLS est lié lorsque vous créez un serveur ou un service virtuel DTLS. DEFAULT_DTLS contient les chiffrements pris en charge par une entité DTLS frontale. Ce groupe est lié par défaut lorsque vous créez un serveur virtuel DTLS. DEFAULT_DTLS_BACKEND contient les chiffrements pris en charge par une entité DTLS dorsale. Ce groupe est lié par défaut à un service principal DTLS. DTLS_FIPS contient les chiffrements pris en charge sur la plate-forme NetScaler FIPS. Ce groupe est lié par défaut à un serveur virtuel DTLS ou à un service créé sur une plate-forme FIPS.

Prise en charge du chiffrement DTLS sur les appliances NetScaler VPX, MPX/SDX (basées sur N2 et N3)

Comment lire les tableaux :

À moins qu'un numéro de version ne soit spécifié, une suite de chiffrement est prise en charge pour toutes les versions d'une version.

Exemple :

- **11.1, 12.1, 13.0, 13.1** : Toutes les builds des versions 11.1, 12.1, 13.0, 13.1.
- **-NA-** : non applicable.

Prise en charge du chiffrement DTLS sur les appliances NetScaler VPX, MPX/SDX (basées sur N2, N3 et Coleto)

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds pris en charge (frontal)	Builds prises en charge (back-end)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.1, 12.1, 13.0, 13.1	12.1, 13.0, 13.1
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	11.1, 12.1, 13.0, 13.1	12.1, 13.0, 13.1
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_D	11.1, 12.1, 13.0, 13.1	-NA-
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11.1, 12.1, 13.0, 13.1	12.1, 13.0, 13.1
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11.1, 12.1, 13.0, 13.1	-NA-
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	11.1, 12.1, 13.0, 13.1	-NA-
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1, 13.0, 13.1	12.1, 13.0, 13.1
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0, 13.1	12.1, 13.0, 13.1
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12.1, 13.0, 13.1	-NA-

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds pris en charge (frontal)	Builds prises en charge (back-end)
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0, 13.1	12.1, 13.0, 13.1
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12.1, 13.0, 13.1	12.1, 13.0, 13.1

Pour afficher la liste des chiffrements par défaut pris en charge sur le frontal, à l'invite de commandes, tapez :

```
show ssl cipher DEFAULT_DTLS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0039
6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x0033
7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```

Pour afficher la liste des chiffrements par défaut pris en charge sur le back-end, à l'invite de commandes, tapez :


```
show ssl cipher DEFAULT_DTLS_BACKEND
1)  Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0039
6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x0033
7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```

Support du chiffrement DTLS sur la plate-forme NetScaler MPX 14000 FIPS

Remarque : EDT est pris en charge sur la plateforme FIPS si les conditions suivantes sont remplies :

- La valeur MSS UDT définie sur StoreFront est 900.
- La version du client Windows est 4.12 ou ultérieure.
- La version du VDA compatible DTLS est 7.17 ou ultérieure.
- La version VDA non-DTLS est 7.15 LTSR CU3 ou ultérieure.

Comment lire les tableaux :

À moins qu'un numéro de version ne soit spécifié, une suite de chiffrement est prise en charge pour toutes les versions d'une version.

Exemple :

- **11.1, 12.1, 13.0, 13.1** : Toutes les builds des versions 11.1, 12.1, 13.0, 13.1.
- **-NA-** : non applicable.

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds pris en charge (frontal)	Builds prises en charge (back-end)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.1, 12.1–49.x, 13.0, 13.1	12.1–49.x, 13.0, 13.1
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	11.1, 12.1–49.x, 13.0, 13.1	12.1–49.x, 13.0, 13.1
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_D	11.1, 12.1–49.x, 13.0, 13.1	-NA-
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11.1, 12.1–49.x, 13.0, 13.1	12.1–49.x, 13.0, 13.1
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11.1, 12.1–49.x, 13.0, 13.1	-NA-
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	11.1, 12.1–49.x, 13.0, 13.1	-NA-
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1–49.x, 13.0, 13.1	12.1–49.x, 13.0, 13.1
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	12.1–49.x, 13.0, 13.1	12.1–49.x, 13.0, 13.1
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12.1–49.x, 13.0, 13.1	-NA-
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1–49.x, 13.0, 13.1	12.1–49.x, 13.0, 13.1
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12.1–49.x, 13.0, 13.1	12.1–49.x, 13.0, 13.1
TLS1-ECDHE-ECDSA-AES128-SHA	0xc009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	13.1–21.x	13.1–21.x
TLS1-ECDHE-ECDSA-AES256-SHA	0xc00a	TLS_ECDHE_ECDS	13.1–21.x	13.1–21.x

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds pris en charge (frontal)	Builds prises en charge (back-end)
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	0xc008	TLS_ECDHE_ECDSA_WITH_3DES_CBC_SHA	13.1–21.x	13.1–21.x

Pour afficher la liste des chiffrements par défaut pris en charge sur une appliance NetScaler FIPS, à l'invite de commande, tapez :

```
show ssl cipher DTLS_FIPS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA  Priority : 5
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
6)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 6
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```

Prise en charge du chiffrement DTLSv1.2 sur les appliances VPX frontales, les appliances MPX/SDX (basées sur Coleto et N3)

Le tableau suivant répertorie les chiffrements supplémentaires pris en charge par le protocole DTLSv1.2.

Nom de la suite de chiffrement	Code Hex	Nom de la suite de chiffrement Wireshark	Builds prises en charge (frontal VPX)	Builds prises en charge (basé sur Coleto)	Builds prises en charge (basé sur N3)
—	—	—	—	—	—
TLS1.2-AES256-GCM-SHA384	0x009d	TLS_RSA_WITH_AES_256_GCM_SHA384	13.0–47.x, 13.1

13.0–52.x, 13.1 | 13.0–58.x, 13.1 |
TLS1.2-AES128-GCM-SHA256	0x009c	TLS_RSA_WITH_AES_128_GCM_SHA256	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	0xc030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	0xc02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-DHE-RSA-AES256-GCM-SHA384	0x009f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-DHE-RSA-AES128-GCM-SHA256	0x009e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-AES-256-SHA256	0x003d	TLS_RSA_WITH_AES_256_CBC_SHA256	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-AES-128-SHA256	0x003c	TLS_RSA_WITH_AES_128_CBC_SHA256	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-ECDHE-RSA-AES-256-SHA384	0xc028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-ECDHE-RSA-AES-128-SHA256	0xc027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-DHE-RSA-AES-256-SHA256	0x006b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1.2-DHE-RSA-AES-128-SHA256	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	13.0–47.x, 13.1	13.0–52.x, 13.1	13.0–58.x, 13.1
TLS1-ECDHE-ECDSA-AES128-SHA	0xc009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	13.1–21.x	NA
TLS1-ECDHE-ECDSA-AES256-SHA|0xc00a|TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA|13.1–21.x|NA|
TLS1-ECDHE-ECDSA-DES-CBC3-SHA|0xc008|TLS_ECDHE_ECDSA_WITH_3DES_CBC_SHA|13.1–21.x|NA|
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	0xc02b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	13.1–21.x	NA
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	0xc02c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	13.1–21.x	NA
TLS1.2-ECDHE-ECDSA-AES128-SHA256	0xc023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	13.1–21.x	NA
TLS1.2-ECDHE-ECDSA-AES256-SHA384	0xc024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	13.1–21.x	NA

Support pour les plates-formes basées sur des puces SSL Intel Coleto et Intel Lewisburg

May 5, 2023

Les appliances suivantes sont livrées avec des puces Intel Coleto :

- MPX 5900
- MPX/SDX 8900
- MPX/SDX 15000
- MPX/SDX 15000-50G
- MPX/SDX 26000
- MPX/SDX 26000-50S
- MPX/SDX 26000-100 G

L'appliance suivante est livrée avec des puces Intel Lewisburg :

- MPX/SDX 9100
- MPX/SDX 16000

Utilisez la commande « show hardware » pour déterminer si votre appareil possède des puces Coleto (COL) ou Lewisburg (LBG).

```
> sh hardware

    Platform: NSMPX-8900 8\*CPU+4\*F1X+6\*E1K+1\*E1K+1*COL 8955 30010
    Manufactured on: 10/18/2016
    CPU: 2100MHZ
    Host Id: 0
    Serial no: CRAC5CR8UA
    Encoded serial no: CRAC5CR8UA
 Done
<!--NeedCopy-->
```

```
> sh hardware
        Platform: NSMPX-9100 10\*CPU+64GB+8\*F2X+E1K+1*LBG C627 35000
        Manufactured on: 10/1/2021
        CPU: 2300MHZ
        Host Id: 161644678
        Serial no: N2Z3ZD9S21
        Encoded serial no: N2Z3ZD9S21
        Netscaler UUID: 41a26261-227e-11ec-b4db-3cecef56f86b
        BMC Revision: 1.00
Done
```



```
<!--NeedCopy-->
```

Limitations

Les algorithmes de chiffrement, protocoles et fonctionnalités suivants ne sont pas pris en charge :

- Chiffrement DH 512
- protocole SSLv3
- Coffre-fort à clés Azure
- GnuTLS
- Certificats ECDSA avec courbes ECC P_224 et P521
- Déchargement par DNSSEC

> Remarque La
>
> prise en charge du module de sécurité matérielle (HSM) de Thales Luna Network est disponible dans la version 13.1 build 33.x et les versions ultérieures.

Afficher l'utilisation logicielle des puces SSL sur les plateformes NetScaler MPX et SDX

À partir de la version 13.1 build 21.x, des compteurs sont ajoutés pour afficher plus de détails sur l'utilisation logicielle des puces SSL sur les plateformes suivantes :

- Plates-formes MPX et SDX livrées avec des puces Intel Coleto.
- Plates-formes MPX livrées avec des puces Intel Lewisburg.

> **Remarque**
>
> Cette fonctionnalité n'est pas prise en charge sur les plateformes suivantes :
>
> - SDX 9100
> - MPX/SDX 16000

À l'invite de commande, tapez :

```
> stat ssl

SSL Summary

1.  SSL cards present 4
2.  SSL cards UP 4
    SSL engine status 1
    SSL sessions (Rate) 19849
    SSL Crypto Utilization Asym (%) 88
    SSL Crypto Utilization Symm (%) 1

```



```
Crypto Utilization(%)
Asymmetric Crypto Utilization 86.30
Symmetric Crypto Utilization 0.97

System
Transactions Rate (/s) Total
SSL transactions 19849 45900312
SSLv2 transactions 0 0
SSLv3 transactions 0 0
TLSv1 transactions 0 0
TLSv1.1 transactions 0 0
TLSv1.2 transactions 19849 45900312
TLSv1.3 transactions 0 0
DTLSv1 transactions 0 0
DTLSv1.2 transactions 0 0

Front End
Sessions Rate (/s) Total
SSL sessions 19849 45937019
SSLv2 sessions 0 0
SSLv3 sessions 0 0
TLSv1 sessions 0 0
TLSv1.1 sessions 0 0
TLSv1.2 sessions 19849 45937019
TLSv1.3 sessions 0 0
DTLSv1 sessions 0 0
DTLSv1.2 sessions 0 0
New SSL sessions 19881 50722628
SSL session misses 0 0
SSL session hits 0 0

Back End
Sessions Rate (/s) Total
SSL sessions 0 137
SSLv3 sessions 0 0
TLSv1 sessions 0 0
TLSv1.1 sessions 0 0
TLSv1.2 sessions 0 137
DTLSv1 sessions 0 0
Session multiplex attempts 0 0
Session multiplex successes 0 0
Session multiplex failures 0 0

Encryption/Decryption statistics
Crypto Operation Rate (bytes/s) Total Bytes
```



```
Bytes encrypted 24338213 27705995030
Bytes decrypted 24664169 27942280990
Done
<!--NeedCopy-->
```

Les valeurs des compteurs suivants sont obtenues en interrogeant le matériel :

```
-  SSL Crypto Utilization Asym (%) 88
-  SSL Crypto Utilization Symm (%) 1
<!--NeedCopy-->
```

Les valeurs des compteurs suivants sont obtenues à l'aide du logiciel. Les valeurs peuvent varier légèrement par rapport aux valeurs interrogées sur le matériel.

- Utilisation de la cryptographie (%)
- Utilisation asymétrique de la cryptographie 85.92
- RSA Crypto Utilization 11.43
  RSA_4K 0.00
  RSA_2K 11.43
  RSA_1K 0.00
  RSA_Others 0.00
- DH Crypto Utilization 74.50
  ECDH Crypto Utilization 0.00
  ECDH_P224 0.00
  ECDH_P256 0.00
  ECDH_P384 0.00
  ECDH_P521 0.00
- ECDSA Crypto Utilization 0.00
  ECDSA_P224 0.00
  ECDSA_P256 0.00
  ECDSA_P384 0.00
  ECDSA_P521 0.00
- Symmetric Crypto Utilization 0.72

Pour une utilisation granulaire par chiffrement, exécutez la commande suivante.

```
> stat ssl -detail

SSL Offloading

1.  SSL cards present 4
2.  SSL cards UP 4
    SSL engine status 1
```



```
    SSL sessions (Rate) 19862
    SSL Crypto Utilization Asym (%) 88
    SSL Crypto Utilization Symm (%) 1

Crypto Utilization(%)

Asymmetric Crypto Utilization 85.92

RSA Crypto Utilization 11.43
RSA_4K 0.00
RSA_2K 11.43
RSA_1K 0.00
RSA_Others 0.00

DH Crypto Utilization 74.50

ECDH Crypto Utilization 0.00
ECDH_P224 0.00
ECDH_P256 0.00
ECDH_P384 0.00
ECDH_P521 0.00

ECDSA Crypto Utilization 0.00
ECDSA_P224 0.00
ECDSA_P256 0.00
ECDSA_P384 0.00
ECDSA_P521 0.00

Symmetric Crypto Utilization 0.72
System
Transactions Rate (/s) Total
SSL transactions 19861 46039342
SSLv2 transactions 0 0
SSLv3 transactions 0 0
TLSv1 transactions 0 0
TLSv1.1 transactions 0 0
TLSv1.2 transactions 19861 46039342
TLSv1.3 transactions 0 0
DTLSv1 transactions 0 0
DTLSv1.2 transactions 0 0
Server in record 117437 277622634
Front End
Sessions Rate (/s) Total
SSL sessions 19862 46076050
SSLv2 sessions 0 0
```



```
SSLv3 sessions 0 0
TLSv1 sessions 0 0
TLSv1.1 sessions 0 0
TLSv1.2 sessions 19862 46076050
TLSv1.3 sessions 0 0
DTLSv1 sessions 0 0
DTLSv1.2 sessions 0 0
New SSL sessions 19801 50861234
SSL session misses 0 0
SSL session hits 0 0
Session Renegotiation
SSL session renegotiations 0 0
SSLv3 session renegotiations 0 0
TLSv1 session renegotiations 0 0
TLSv1.1 session renegotiations 0 0
TLSv1.2 session renegotiations 0 0
DTLSv1 session renegotiations 0 0
DTLSv1.2 session renegotiations 0 0
Key Exchanges
RSA 512-bit key exchanges 0 0
RSA 1024-bit key exchanges 0 2032658
RSA 2048-bit key exchanges 0 143
RSA 3072-bit key exchanges 0 7757028
RSA 4096-bit key exchanges 0 2238698
DH 512-bit key exchanges 0 0
DH 1024-bit key exchanges 0 0
DH 2048-bit key exchanges 19862 5477702
DH 4096-bit key exchanges 0 0
ECDHE 521 curve key exchanges 0 0
ECDHE 384 curve key exchanges 0 0
ECDHE 256 curve key exchanges 0 28569821
ECDHE 224 curve key exchanges 0 0
Total ECDHE key exchanges 0 28569821
Ciphers Negotiated
RC4 40-bit encryptions 0 0
RC4 56-bit encryptions 0 0
RC4 64-bit encryptions 0 0
RC4 128-bit encryptions 0 0
DES 40-bit encryptions 0 0
DES 56-bit encryptions 0 0
3DES 168-bit encryptions 0 0
AES 128-bit encryptions 0 0
AES 256-bit encryptions 19862 17506229
RC2 40-bit encryptions 0 0
RC2 56-bit encryptions 0 0
```



```
RC2 128-bit encryptions 0 0
AES-GCM 128-bit encryptions 0 0
AES-GCM 256-bit encryptions 0 28569821
Null cipher encryptions 0 0
Hashes
MD5 hashes 0 0
SHA hashes 0 12028527
SHA256 hashes 19862 5477702
SHA384 hashes 0 0
Handshakes
SSLv2 SSL handshakes 0 0
SSLv3 SSL handshakes 0 0
TLSv1 SSL handshakes 0 0
TLSv1.1 SSL handshakes 0 0
TLSv1.2 SSL handshakes 19862 46076050
TLSv1.3 SSL handshakes 0 0
DTLSv1 SSL handshakes 0 0
DTLSv1.2 SSL handshakes 0 0
Client Authentications
SSLv2 client authentications 0 0
SSLv3 client authentications 0 0
TLSv1 client authentications 0 0
TLSv1.1 client authentications 0 0
TLSv1.2 client authentications 0 0
TLSv1.3 client authentications 0 0
DTLSv1 client authentications 0 0
DTLSv1.2 client authentications 0 0
Authentications
RSA authentications 19862 17506229
DH authentications 0 0
DSS (DSA) authentications 0 0
ECDSA authentications 0 28569821
Null authentications 0 0
Back End
Sessions Rate (/s) Total
SSL sessions 0 137
SSLv3 sessions 0 0
TLSv1 sessions 0 0
TLSv1.1 sessions 0 0
TLSv1.2 sessions 0 137
DTLSv1 sessions 0 0
Session multiplex attempts 0 0
Session multiplex successes 0 0
Session multiplex failures 0 0
Session Renegotiation
```



```
SSL session renegotiations 0 0
SSLv3 session renegotiations 0 0
TLSv1 session renegotiations 0 0
TLSv1.1 back-end session renegot 0 0
TLSv1.2 back-end session renegot 0 0
DTLSv1 session renegotiations 0 0
Key Exchanges
RSA 512-bit key exchanges 0 0
RSA 1024-bit key exchanges 0 0
RSA 2048-bit key exchanges 0 137
RSA 3072-bit key exchanges 0 0
RSA 4096-bit key exchanges 0 0
DH 512-bit key exchanges 0 0
DH 1024-bit key exchanges 0 0
DH 2048-bit key exchanges 0 0
DH 4096-bit key exchanges 0 0
ECDHE 521 curve key exchanges 0 0
ECDHE 384 curve key exchanges 0 0
ECDHE 256 curve key exchanges 0 0
ECDHE 224 curve key exchanges 0 0
Ciphers Negotiated
RC4 40-bit encryptions 0 0
RC4 56-bit encryptions 0 0
RC4 64-bit encryptions 0 0
RC4 128-bit encryptions 0 0
DES 40-bit encryptions 0 0
DES 56-bit encryptions 0 0
3DES 168-bit encryptions 0 0
AES 128-bit encryptions 0 0
AES 256-bit encryptions 0 137
RC2 40-bit encryptions 0 0
RC2 56-bit encryptions 0 0
RC2 128-bit encryptions 0 0
AES-GCM 128-bit encryptions 0 0
AES-GCM 256-bit encryptions 0 0
Null encryptions 0 0
Hashes
MD5 hashes 0 0
SHA hashes 0 137
SHA256 hashes 0 0
SHA384 hashes 0 0
Handshakes
SSLv3 handshakes 0 0
TLSv1 handshakes 0 0
TLSv1.1 handshakes 0 0
```



```
TLSv1.2 handshakes 0 137
DTLSv1 handshakes 0 0
Client Authentications
SSLv3 client authentications 0 0
TLSv1 client authentications 0 0
TLSv1.1 client authentications 0 0
TLSv1.2 client authentications 0 0
DTLSv1 client authentications 0 0
Authentications
RSA authentications 0 137
DH authentications 0 0
DSS authentications 0 0
ECDSA authentications 0 0
Null authentications 0 0
System Total
RSA key exchanges offloaded 0 0
RSA sign operations offloaded 0 0
DH key exchanges offloaded 19841 5481037
RC4 encryptions offloaded 0 0
DES encryptions offloaded 0 0
AES encryptions offloaded 0 0
AES-GCM 128-bit encryptions offl 0 0
AES-GCM 256-bit encryptions offl 0 0
Encryption/Decryption statistics
Crypto Operation Rate (bytes/s) Total Bytes
Bytes encrypted 12129801 27790903638
Bytes encrypted in hardware 12129801 27790903638
Bytes encrypted in software 0 0
Bytes encrypted on the front-end 5450907 13430410630
Bytes encrypted in hardware on t 5450907 13430410630
Bytes encrypted in software on t 0 0
Bytes encrypted on the back-end 6678894 14360493008
Bytes encrypted in hardware on t 6678894 14360493008
Bytes encrypted in software on t 0 0
Bytes decrypted 12449504 28029427518
Bytes decrypted in hardware 12449504 28029427518
Bytes decrypted in software 0 0
Bytes decrypted on the front-end 8190208 19876552670
Bytes decrypted in hardware on t 8190208 19876552670
Bytes decrypted in software on t 0 0
Bytes decrypted on the back-end 4259296 8152874848
Bytes decrypted in hardware on t 4259296 8152874848
Bytes decrypted in software on t 0 0
SSL
Rate (/s) Total
```



```
Total SPCB in use -87 84656
Active SSL sessions -30309 5615559
Current queue size -1 4153
CardQ
Rate (/s) Total
In Q count for current card -1 4153
In BulkQ count for current card 0 0
In KeyQ count for current card -1 4153
Done
<!--NeedCopy-->
```

> Remarques
>
> - La partition d'administration est prise en charge, mais l'utilisation de toutes les partitions est indiquée dans la partition par défaut. Sur les partitions non définies par défaut, ces valeurs s'affichent sous la forme 0.
> - Dans une configuration de cluster, l'adresse CLIP affiche l'utilisation moyenne pour tous les nœuds du cluster. Pour une utilisation spécifique à un nœud, exécutez la commande sur l'interface de ligne de commande de chaque nœud. Ces données peuvent être incorrectes pour une plate-forme SDX si les nœuds du cluster sont hébergés sur le même matériel.
> - Pour les instances VPX sur la plate-forme SDX, l'utilisation de chaque instance VPX est affichée.

Appareils VPX FIPS

June 2, 2023

L'appliance NetScaler VPX FIPS est en cours de validation (actuellement en IUT https://csrc.nist.gov/projects/cryptographic-module-validation-program/modules-in-process/iut-list) pour la norme FIPS 140-3 niveau 1 par le National Institute of Standards and Technology (NIST). De plus amples informations sur la norme FIPS 140-3 et le programme de validation sont disponibles sur le site Web du NIST et du Programme de validation des modules cryptographiques (CMVP) du Centre canadien pour la cybersécurité (CCCS) à l'adresse. https://csrc.nist.gov/projects/cryptographic-module-validation-program

> **Remarque**
>
> - Seules les versions du microprogramme répertoriées sous « NetScaler Release 13.1-FIPS » sur la page de téléchargement de NetScaler sont prises en charge sur les plateformes MPX 8900 FIPS, MPX 9100 FIPS, MPX 15000-50G FIPS et VPX FIPS.
> - Si vous avez configuré des stratégies classiques sur votre appliance NetScaler FIPS

exécutant la version logicielle 12.1-FIPS, consultez https://support.citrix.com/article/CTX234821/citrix-adc-deprecated-classic-policy-based-features-and-functionalities-faqs avant d'effectuer une mise à niveau vers la version 13.1-FIPS.

- Le protocole TLS 1.3 sur 13.1-FIPS ne peut être configuré qu'à l'aide de profils SSL améliorés. Pour plus d'informations sur la façon de configurer TLS 1.3 à l'aide de profils, consultez le support du protocole TLSv1.3 tel que défini dansla RFC 8446.

Composants requis

- Pour les hyperviseurs sur site, téléchargez la version spéciale sur le site Web de Citrix. Téléchargez le package VPX FIPS complet pour l'hyperviseur correspondant.
- Une appliance NetScaler VPX FIPS nécessite une licence d'instance FIPS et un pool de bande passante pour fonctionner comme prévu dans le modèle de licence groupé. Pour les licences non groupées, une seule licence VPX FIPS de la capacité de bande passante requise est requise.

Configuration

Le module est disponible sous la forme d'un progiciel qui inclut à la fois le logiciel d'application et le système d'exploitation. Après avoir acheté la licence NetScaler VPX FIPS, procurez-vous la dernière image NetScaler VPX FIPS sur le site Web de Citrix.

Procédez comme suit :

1. Téléchargez la dernière image FIPS de NetScaler VPX vers l'un des hyperviseurs suivants : ESXi, Citrix Hypervisor, Hyper-V, KVM, AWS, Azure ou GCP.

   Remarque :

   VPX FIPS est qualifié sur ESX 7.0.3.

2. Appliquez la licence NetScaler VPX FIPS Platform et la licence NetScaler VPX Bandwidth, puis redémarrez à chaud l'appliance.
3. Une fois l'appliance démarrée, exécutez la commande suivante sur l'interface de ligne de commande :

   ```
   > show system fipsStatus
   <!--NeedCopy-->
   ```

   Vous devez obtenir le résultat suivant.

   ```
   FipsStatus: System is operating in FIPS mode
   NetScaler Cryptographic Module v1.0
   NetScaler Control Plane Cryptographic Library v1.0
   NetScaler Data Plane Cryptographic Library v1.0
   ```



```
Done
<!--NeedCopy-->
```

Si vous obtenez le résultat suivant, consultez la section de résolution des problèmes pour connaître les étapes à suivre.

```
FipsStatus: "System is operating in non FIPS mode"
Done
>
<!--NeedCopy-->
```

4. Suivez les instructions de configuration du Guide de déploiement sécurisé.

Pour plus d'informations sur l'authentification à distance à l'aide de RADIUS, voir Configurer l'authentification à distance à l'aide de RADIUS.

Chiffrements pris en charge sur une appliance VPX FIPS

Tous les chiffrements pris en charge sur une appliance FIPS NetScaler MPX/SDX 14000, à l'exception du chiffrement 3DES, sont pris en charge sur une appliance FIPS VPX. Pour obtenir la liste complète des chiffrements pris en charge sur une appliance NetScaler VPX FIPS, consultez la rubrique suivante :

- Support du chiffrement sur les appliances NetScaler VPX FIPS et MPX FIPS.

Mettre à niveau une appliance VPX FIPS

Suivez les étapes décrites dans Mettre à niveau une appliance autonome NetScaler pour mettre à niveau l'appliance VPX FIPS.

Important : remplacez la commande `./installns` par `./installns -F`.

Limitations

- L'authentification TACACS n'est pas prise en charge sur l'appliance VPX FIPS.
- VPX FIPS est une image distincte. La mise à niveau de la version logicielle de la version VPX vers la version VPX FIPS n'est pas prise en charge. De plus, la version du logiciel VPX FIPS ne peut pas être rétrogradée ou mise à niveau vers la version du logiciel VPX.
- L'image VPX FIPS n'est pas prise en charge sur une appliance NetScaler SDX et NetScaler SDX FIPS.
- NetScaler VPX FIPS sur GCP ne prend actuellement en charge que le déploiement autonome. Le déploiement HA n'est pas pris en charge.

Dépannage

Lorsque vous exécutez la `show system fipsStatus` commande, le résultat est le suivant :

```
FipsStatus: "System is operating in non FIPS mode"
Done
>
<!--NeedCopy-->
```

La raison peut être l'une des suivantes :

1. La licence est expirée ou incorrecte.
2. Le système ne peut pas fonctionner en mode FIPS. Cette erreur peut être due à un échec POST sur le cœur de gestion ou le moteur de paquets.

Pour résoudre :

1. Vérifiez que la licence NetScaler VPX FIPS appropriée est installée et qu'elle n'a pas expiré.
2. Vérifiez qu'il n'y a pas d'échec de démarrage automatique (POST) sur le cœur de gestion ou sur un moteur de paquets. Exécutez la commande suivante :

   ```
   >shell
   #nsconmsg -g drbg -g ssl_err -g fips -d statswt0
   <!--NeedCopy-->
   ```

   Le compteur `nsssl_err_fips_post_failed counter` s'affiche par incréments en cas d'échec du POST lors du démarrage du moteur de paquets. C'est-à-dire qu'il y a une défaillance du plan de données.

   Si le compteur ne s'incrémente pas, recherchez dans le fichier journal une entrée (`/var/log/FIPS-post.log`) de test d'algorithme ayant échoué. C'est-à-dire qu'il faut vérifier la présence d'une défaillance POST sur le cœur de gestion (défaillance du plan de contrôle).

   Dans les deux cas, contactez le support NetScaler.

Appareils MPX FIPS

June 2, 2023

Les appliances NetScaler MPX 8900 FIPS, MPX 9100 FIPS et MPX 15000-50G FIPS sont en cours de validation (actuellement en IUT https://csrc.nist.gov/projects/cryptographic-module-validation-program/modules-in-process/iut-list) par un laboratoire tiers pour les exigences de sécurité de la norme FIPS 140-3 niveau 1. De plus amples informations sur la norme FIPS 140-3 et le programme de validation

sont disponibles sur le site Web du National Institute of Standards and Technology (NIST) et du Centre canadien pour la cybersécurité (CCCS) du Programme de validation des modules cryptographiques (CMVP) à l'adresse. https://csrc.nist.gov/projects/cryptographic-module-validation-program

> **Remarques**
>
> - Les appliances MPX 8900 FIPS, MPX 9100 FIPS et MPX 15000-50G FIPS n'utilisent plus de module de sécurité matérielle tiers. Les exigences à valider selon la FIPS sont intégrées au système.
> - Seules les versions du microprogramme répertoriées sous « NetScaler Release 13.1-FIPS » sur la page de téléchargement de NetScaler sont prises en charge sur les plateformes MPX 8900 FIPS, MPX 9100 FIPS, MPX 15000-50G FIPS et VPX FIPS.
> - Si vous avez configuré des stratégies classiques sur votre appliance NetScaler FIPS exécutant la version logicielle 12.1-FIPS, consultez https://support.citrix.com/article/CTX234821/citrix-adc-deprecated-classic-policy-based-features-and-functionalities-faqs avant d'effectuer une mise à niveau vers la version 13.1-FIPS.
> - Le protocole TLS 1.3 sur 13.1-FIPS ne peut être configuré qu'à l'aide de profils SSL améliorés. Pour plus d'informations sur la façon de configurer TLS 1.3 à l'aide de profils, consultez le support du protocole TLSv1.3 tel que défini dansla RFC 8446.

Composants requis

- Licence de plateforme FIPS en plus d'une licence de bande passante.

Chiffrements pris en charge sur les appliances FIPS MPX 8900, FIPS MPX 9100 et MPX 15000-50G FIPS

Tous les chiffrements pris en charge sur une appliance FIPS NetScaler MPX/SDX 14000, à l'exception du chiffrement 3DES, sont pris en charge sur les appliances FIPS MPX 8900, MPX 9100 et MPX 15000-50G FIPS. Pour obtenir la liste complète des chiffrements pris en charge sur ces appliances, consultez la section Prise en charge du chiffrement sur les appliances NetScaler VPX FIPS et MPX FIPS.

Limitation

L'authentification TACACS n'est pas prise en charge sur l'appliance MPX FIPS.

Configuration

1. Une fois l'appliance démarrée, exécutez la commande suivante sur l'interface de ligne de commande :


```
> show system fipsStatus
<!--NeedCopy-->
```

2. Vous devez obtenir le résultat suivant.

```
FipsStatus: "System is operating in FIPS mode"
Done
>
<!--NeedCopy-->
```

3. Si vous obtenez le résultat suivant, vérifiez la licence.

```
FipsStatus: "System is operating in non FIPS mode"
Done
>
<!--NeedCopy-->
```

Effectuez les étapes suivantes pour initialiser l'appliance MPX pour le mode de fonctionnement FIPS.

1. Appliquez des exigences strictes en matière de phrases secrètes.
2. Remplacez le certificat TLS par défaut.
3. Désactivez l'accès HTTP à l'interface graphique Web.
4. Après la configuration initiale, désactivez l'authentification locale et configurez l'authentification à distance à l'aide de LDAP.

Appliquez des exigences strictes en matière de phrases de passe à l'aide de l'interface graphique

Les phrases secrètes sont utilisées pour dériver des clés à l'aide de PBKDF2. En tant qu'administrateur, activez des exigences strictes en matière de phrases de passe à l'aide de l'interface graphique.

1. Accédez à **Système > Paramètres**.
2. Dans la section Paramètres, cliquez sur **Modifier les paramètres généraux du système**.
3. Dans le champ **Mot de passe** sécurisé, sélectionnez **Tout activer**.
4. Dans le champ **Longueur minimale du mot** de passe, tapez « 8 ».
5. Cliquez sur **OK**.

Remplacer le certificat TLS par défaut

Par défaut, l'appliance MPX FIPS inclut un certificat RSA provisionné en usine pour les connexions TLS (et).`ns-server.certns-server.key` Ce certificat n'est pas destiné à être utilisé dans des déploiements de production et doit être remplacé. Remplacez le certificat par défaut par un nouveau certificat après l'installation initiale.

Pour remplacer le certificat TLS par défaut :

1. À l'invite de commandes, tapez la commande suivante pour définir le nom d'hôte de l'appliance.

   ```
   set ns hostName <hostname>
   ```

Création d'une demande de signature de certificat (CSR) à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Fichiers SSL**.
2. Dans l'onglet **CSR**, cliquez sur **Create Certificate Signing Request (CSR)**.
3. Entrez les valeurs et cliquez sur **Créer**.

   > **Remarque**
   >
   > Le champ **Nom commun** contient la valeur du nom d'hôte défini à l'aide de l'ADC CLI.

4. Soumettez le fichier CSR à une autorité de certification (CA) approuvée. Le fichier CSR est disponible dans le répertoire `/nsconfig/ssl`.
5. Après avoir reçu le certificat de la part de l'autorité de certification, copiez le fichier dans le `/nsconfig/ssl` répertoire.
6. Accédez à **Gestion du trafic > SSL > Certificats > Certificats de serveur**.
7. Sélectionnez **ns-server-certificate**.
8. Cliquez sur **Update**.
9. Cliquez sur **Mettre à jour le certificat et la clé**.
10. Dans le champ **Nom du fichier de certificat**, sélectionnez le fichier de certificat qui a été reçu de l'autorité de certification (CA). Choisissez **Local** si le fichier se trouve sur votre ordinateur local. Sinon, choisissez **Appliance**.
11. Dans le champ **Nom du fichier clé**, spécifiez le nom de fichier de clé privée par défaut (`ns-server.key`).
12. Sélectionnez l'option **Aucune vérification de domaine** .
13. Cliquez sur **OK**.

Désactiver l'accès HTTP à l'interface graphique Web

Pour protéger le trafic vers l'interface administrative et l'interface graphique Web, l'appliance doit être configurée pour utiliser le protocole HTTPS. Après avoir ajouté de nouveaux certificats, utilisez l'interface de ligne de commande pour désactiver l'accès HTTP à l'interface de gestion de l'interface graphique.

À l'invite de commande, tapez :


```
set ns ip <NSIP> -gui SECUREONLY
```

Désactiver l'authentification locale et configurer l'authentification à distance à l'aide de LDAP

Le compte superutilisateur est un compte par défaut doté de privilèges d'accès à l'interface de ligne de commande racine qui sont requis pour la configuration initiale. Lors de la configuration initiale, désactivez l'authentification du système local pour bloquer l'accès à tous les comptes locaux (y compris le compte superutilisateur) et pour vous assurer que les privilèges de superutilisateur ne sont attribués à aucun compte utilisateur.

Pour désactiver l'authentification du système local et activer l'authentification du système externe à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
set system parameter -localauth disabled
```

Suivez les instructions de la section Configuration de l'authentification LDAP pour configurer l'authentification du système externe afin d'utiliser LDAP.

Configurer l'authentification à distance à l'aide de RADIUS

Vous pouvez configurer l'authentification RADIUS dans les environnements FIPS.

> **Remarque :**
>
> L'option **Tester l'accessibilité de RADIUS** n'est pas prise en charge pour RADIUS.

Configurer RADIUS sur TLS à l'aide de la CLI

À l'invite de commandes, tapez :

```
1 add authentication radiusAction <name> [-serverIP] [-serverPort ] [-
     transport <transport>] [-targetLBVserver <string>]
2 <!--NeedCopy-->
```

Exemple

```
1 add authentication radiusAction RadAction -serverIP 1.1.1.1 -radkey 123
     -transport TLS -targetLBVserver rad-lb
2 <!--NeedCopy-->
```

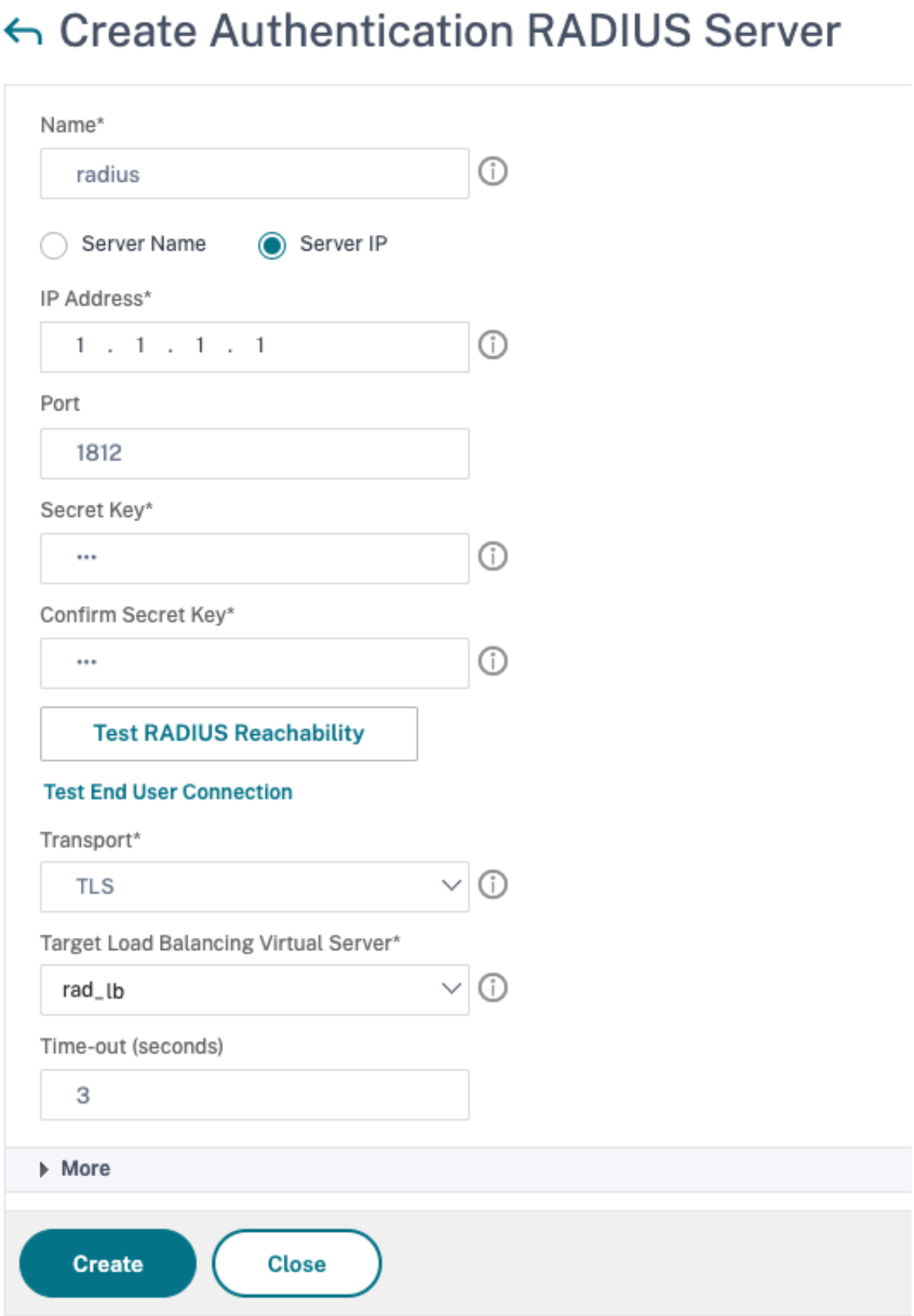
> **Remarque :**
>
> - Pour le type de transport TLS, configurez un serveur virtuel d'équilibrage de charge cible de type TCP et liez un service de type SSL_TCP à ce serveur virtuel.

> - Le nom du serveur n'est pas pris en charge.
> - L'adresse IP et le numéro de port configurés pour l'action RADIUS doivent correspondre à l'adresse IP et au numéro de port du serveur virtuel d'équilibrage de charge cible configuré.

Configurer RADIUS sur TLS à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Actions > Serveurs**.
2. Sélectionnez un serveur existant ou créez-en un.

   Pour plus d'informations sur la création d'un serveur, consultez Pour configurer un serveur RADIUS à l'aide de l'interface graphique.



3. Dans **Transport**, sélectionnez **TLS**.
4. Dans **Target Load Balancing Virtual Server**, sélectionnez le serveur virtuel. Pour plus d'informations sur la création d'un serveur virtuel d'équilibrage de charge, consultez la section Création d'un serveur virtuel.

   > **Remarque :**
   >
   > - Pour le type de transport TLS, configurez un serveur virtuel d'équilibrage de charge cible de type TCP et liez un service de type SSL_TCP à ce serveur virtuel.
   > - Le nom du serveur n'est pas pris en charge.
   > - L'adresse IP et le numéro de port configurés pour l'action RADIUS doivent correspondre à l'adresse IP et au numéro de port du serveur virtuel d'équilibrage de charge cible configuré.

5. Cliquez sur **Create**.

Appareils FIPS MPX 14000

May 5, 2023

> **Important :**
>
> - La plate-forme FIPS MPX 9700/10500/12500/15500 est en fin de vie.
> - Les étapes de configuration des appliances FIPS NetScaler MPX 14000 et NetScaler MPX 9700/10500/12500/15500 FIPS sont différentes. Les appareils MPX 14000 FIPS n'utilisent pas le firmware v2.2. Une clé FIPS créée sur le module de sécurité matérielle (HSM) de la plate-forme MPX 9700 ne peut pas être transférée vers le HSM de la plate-forme MPX 14000. L'inverse n'est pas non plus pris en charge. Toutefois, si vous avez importé une clé RSA en tant que clé FIPS, vous pouvez copier la clé RSA sur la plate-forme MPX 14000. Importez-le ensuite en tant que clé FIPS. Seules les clés 2048 bits et 3072 bits sont prises en charge.
> - Les versions du microprogramme répertoriées sous « NetScaler Release 12.1-FIPS » et « NetScaler Release 12.1-NDCPP » sur la page de téléchargement de NetScaler ne sont pas prises en charge sur les plateformes MPX 14000 FIPS ou SDX 14000 FIPS. Ces plateformes peuvent utiliser les autres versions les plus récentes du microprogramme NetScaler disponibles sur la page des téléchargements.

Un appareil FIPS est équipé d'un module cryptographique inviolable (inviolable) — un Cavium CNN3560-NFBE-G — conçu pour répondre aux spécifications FIPS 140-2 Niveau 3 (de la version 12.0 build 56.x). Les paramètres de sécurité critiques (CSP), principalement la clé privée du serveur, sont stockés et générés en toute sécurité dans le module cryptographique, également appelé HSM. Les

CSP ne sont jamais accessibles à l'extérieur des limites du HSM. Seul le superutilisateur (`nsroot`) peut effectuer des opérations sur les clés stockées dans le HSM.

Avant de configurer un dispositif FIPS, vous devez vérifier l'état de la carte FIPS, puis initialiser la carte. Créez une clé FIPS et un certificat de serveur, et ajoutez toute configuration SSL supplémentaire.

Pour plus d'informations sur les chiffrements FIPS pris en charge, consultez Algorithmes et chiffrements approuvés FIPS.

Pour plus d'informations sur la configuration des appliances FIPS dans une configuration HA, voir Configurer FIPS sur les appliances dans une configuration HA.

Limitations

1. La renégociation SSL à l'aide du protocole SSLv3 n'est pas prise en charge sur le back-end d'une appliance MPX FIPS.
2. Les clés 1024 bits et 4096 bits et la valeur de l'exposant 3 ne sont pas prises en charge.
3. Le certificat serveur 4096 bits n'est pas pris en charge.
4. Le certificat client 4096 bits n'est pas pris en charge (si l'authentification client est activée sur le serveur principal).

Configurer le HSM

Avant de configurer le HSM sur une appliance FIPS MPX 14000, vérifiez l'état de votre carte FIPS pour vérifier que le pilote s'est correctement chargé. Initialisez ensuite la carte.

À l'invite de commande, tapez :

```
1 show fips
2
3 FIPS Card is not configured
4 <!--NeedCopy-->
```

Le message « ERREUR : opération non autorisée - aucune carte FIPS présente dans le système » s'affiche si le pilote n'est pas correctement chargé.

Initialiser la carte FIPS

L'appliance doit être redémarrée trois fois pour que la carte FIPS soit correctement initialisée.

> **Important**
>
> - Vérifiez que le `/nsconfig/fips` répertoire a bien été créé sur l'appliance.
> - N'enregistrez pas la configuration avant de redémarrer l'appliance pour la troisième fois.

Pour initialiser la carte FIPS, effectuez les opérations suivantes :

1. Réinitialisez la carte FIPS (`reset fips`).
2. Redémarrez l'appliance (`reboot`).
3. Définissez le mot de passe du responsable de la sécurité pour les partitions 0 et 1, et le mot de passe utilisateur pour la partition (`set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -hsmLabel NSFIPS`).

   Remarque : L'exécution de la commande set ou reset prend plus de 60 secondes.
4. Enregistrez la configuration (`saveconfig`).
5. Vérifiez que la clé chiffrée par mot de passe pour la partition principale (master_pek.key) a été créée dans le répertoire `/nsconfig/fips/`.
6. Redémarrez l'appliance (`reboot`).
7. Vérifiez que la clé chiffrée par mot de passe pour la partition par défaut (default_pek.key) a été créée dans le répertoire `/nsconfig/fips/`.
8. Redémarrez l'appliance (`reboot`).
9. Vérifiez que la carte FIPS est UP (`show fips`).

Initialisez la carte FIPS à l'aide de l'interface de ligne de commande

La commande `set fips` initialise le module de sécurité matérielle (HSM) sur la carte FIPS et définit un nouveau mot de passe du responsable de la sécurité et un nouveau mot de passe utilisateur.

Attention : Cette commande efface toutes les données de la carte FIPS. Vous y êtes invité avant de poursuivre l'exécution de la commande. Un redémarrage est nécessaire avant et après l'exécution de cette commande pour que les modifications s'appliquent. Enregistrez la configuration après avoir exécuté cette commande et avant de redémarrer l'appliance.

À l'invite de commandes, tapez les commandes suivantes :

```
1 reset fips
2
3 reboot
4
5 set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS
6
7 This command will erase all data on the FIPS card. You must save the
     configuration (saveconfig) after executing this command. Do you want
      to continue?(Y/N)y
8
9 <!--NeedCopy-->
```


Remarque : Le message suivant s'affiche lorsque vous exécutez la `set fips` commande :

```
This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. [Note: On
   MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
   default, and the -initHSM Level-2 option is internally converted to
   Level-3]  Do you want to continue?(Y/N)y

saveconfig

reboot

reboot

show fips

        FIPS HSM Info:
                HSM Label               : NetScaler FIPS
                Initialization          : FIPS-140-2 Level-3
                HSM Serial Number       : 3.1G1836-ICM000136
                HSM State               : 2
                HSM Model               : NITROX-III CNN35XX-NFBE
                Hardware Version        : 0.0-G
                Firmware Version        : 1.0
                Firmware Build          : NFBE-FW-1.0-48
                Max FIPS Key Memory     : 102235
                Free FIPS Key Memory    : 102231
                Total SRAM Memory       : 557396
                Free SRAM Memory        : 262780
                Total Crypto Cores      : 63
                Enabled Crypto Cores    : 63

<!--NeedCopy-->
```

Créer une clé FIPS

Vous pouvez créer une clé FIPS sur votre appliance FIPS MPX 14000 ou importer une clé FIPS existante dans l'appliance. L'appliance FIPS MPX 14000 ne prend en charge que les clés 2048 bits et 3072 bits et une valeur d'exposant F4 (dont la valeur est 65537). Pour les clés PEM, aucun exposant n'est requis. Vérifiez que la clé FIPS a été créée correctement. Créez une demande de signature de certificat et un certificat de serveur. Enfin, ajoutez la paire de clés de certificat à votre appliance.

Spécifiez le type de clé (RSA ou ECDSA). Pour les clés ECDSA, spécifiez uniquement la courbe. La création de clés ECDSA avec les courbes P_256 et P_384 est prise en charge.

> **Remarque :**
>
> Les clés 1024 bits et 4096 bits et une valeur d'exposant de 3 ne sont pas prises en charge.

Créer une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent ( 3 | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
<!--NeedCopy-->
```

Example1:

```
create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4


show ssl fipskey f1

FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (Hex: 0x10001)

<!--NeedCopy-->
```

Example2:

```
> create fipskey f2 -keytype ECDSA -curve P_256


> sh fipskey f2
    FIPS Key Name: f2   Key Type: ECDSA Curve: P_256

<!--NeedCopy-->
```

Créer une clé FIPS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Clés FIPS, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Créer une clé FIPS, spécifiez les valeurs des paramètres suivants :
   - Nom de clé FIPS* : nom de clé FIPSKey
   - Module* : module
   - Exposant* : exposant

*Paramètre obligatoire

4. Cliquez sur **Créer**, puis sur **Fermer**.
5. Sous l'onglet Touches FIPS, vérifiez que les paramètres affichés pour la clé FIPS que vous avez créée sont corrects.

Importer une clé FIPS

Pour utiliser une clé FIPS existante avec votre appliance FIPS, vous devez transférer la clé FIPS du disque dur de l'appliance vers son HSM.

Remarque : Pour éviter les erreurs lors de l'importation d'une clé FIPS, assurez-vous que le nom de la clé importée est identique au nom de clé d'origine lors de sa création.

Importer une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-
   wrapKeyName <string>] [-iv<string>] -exponent  F4 ]
<!--NeedCopy-->
```

Exemple :

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4


import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM

<!--NeedCopy-->
```

Vérifiez que la clé FIPS est créée ou importée correctement en exécutant la commande `show fipskey`.

```
show fipskey
1)      FIPS Key Name: Key-FIPS-2

<!--NeedCopy-->
```

Importer une clé FIPS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Clés FIPS, cliquez sur **Importer**.

3. Dans la boîte de dialogue Importer en tant que clé FIPS, sélectionnez le fichier de clé FIPS et définissez les valeurs des paramètres suivants :

   - Nom de la clé FIPS*
   - Nom du fichier clé* : pour placer le fichier dans un emplacement autre que celui par défaut, spécifiez le chemin complet ou cliquez sur **Parcourir** et accédez à un emplacement.
   - Exposant*

   *Paramètre obligatoire

4. Cliquez sur **Importer**, puis cliquez sur **Fermer**.
5. Sous l'onglet Touches FIPS, vérifiez que les paramètres affichés pour la clé FIPS que vous avez importée sont corrects.

Exporter une clé FIPS

Citrix vous recommande de créer une sauvegarde de toute clé créée dans le HSM FIPS. Si une clé du HSM est supprimée, vous ne pouvez plus créer la même clé et tous les certificats associés sont rendus inutiles.

Outre l'exportation d'une clé en tant que sauvegarde, vous devrez peut-être exporter une clé pour le transfert vers une autre appliance.

La procédure suivante fournit des instructions sur l'exportation d'une clé FIPS vers le `/nsconfig/ssl` dossier du CompactFlash de l'appliance et sur la sécurisation de la clé exportée à l'aide d'une méthode de chiffrement à clé asymétrique forte.

Exportation d'une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
export ssl fipsKey <fipsKeyName> -key <string>
<!--NeedCopy-->
```

Exemple :

```
export fipskey Key-FIPS-1 -key Key-FIPS-1.key
<!--NeedCopy-->
```

Exporter une clé FIPS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Clés FIPS, cliquez sur **Exporter**.

3. Dans la boîte de dialogue Exporter la clé FIPS vers un fichier, spécifiez les valeurs des paramètres suivants :

   - Nom de clé FIPS* : nom de clé FIPSKey
   - Nom du fichier* : touche (Pour placer le fichier à un emplacement autre que celui par défaut, vous pouvez spécifier le chemin d'accès complet ou cliquer sur le bouton Parcourir et accéder à un emplacement.)

   *Paramètre obligatoire

4. Cliquez sur **Exporter**, puis sur **Fermer**.

Importer une clé externe

Vous pouvez transférer les clés FIPS créées dans le HSM de l'appliance NetScaler. Vous pouvez également transférer des clés privées externes (telles que des clés créées sur un NetScaler, Apache ou IIS standard) vers une appliance NetScaler FIPS. Les clés externes sont créées en dehors du HSM, à l'aide d'un outil tel qu'OpenSSL. Avant d'importer une clé externe dans le HSM, copiez-la sur le lecteur flash de l'appliance sous `/nsconfig/ssl`.

Sur les appliances FIPS MPX 14000, le paramètre -exponent de la commande **`import`** `ssl fipskey` n'est pas requis lors de l'importation d'une clé externe. L'exposant public correct est détecté automatiquement lorsque la clé est importée et la valeur du paramètre -exponent est ignorée.

L'appliance NetScaler FIPS ne prend pas en charge les clés externes avec un exposant public autre que 3 ou F4.

Vous n'avez pas besoin d'une clé d'enroulement sur les appliances FIPS MPX 14000.

Vous ne pouvez pas importer de clé FIPS externe chiffrée directement sur une appliance FIPS MPX 14000. Pour importer la clé, vous devez d'abord la déchiffrer, puis l'importer. Pour déchiffrer la clé, à l'invite du shell, tapez :

```
1 openssl rsa -in <EncryptedKey.key> > <DecryptedKey.out>
2 <!--NeedCopy-->
```

Remarque : Si vous importez une clé RSA en tant que clé FIPS, Citrix vous recommande de supprimer la clé RSA de l'appliance à des fins de sécurité.

Importer une clé externe en tant que clé FIPS à l'aide de l'interface de ligne de commande

1. Copiez la clé externe sur le lecteur flash de l'appliance.
2. Si la clé est au format .pfx, vous devez d'abord la convertir au format PEM. À l'invite de commande, tapez :


```
convert ssl pkcs12 <output file> -import -pkcs12File <input .pfx file name> -password <password>
<!--NeedCopy-->
```

3. À l'invite de commandes, tapez les commandes suivantes pour importer la clé externe en tant que clé FIPS et vérifier les paramètres :

```
import ssl fipsKey <fipsKeyName> -key <string> -informPEM
show ssl fipskey<fipsKeyName>
<!--NeedCopy-->
```

Exemple :

```
convert ssl pkcs12 iis.pem -password 123456 -import -pkcs12File iis.pfx

import fipskey Key-FIPS-2 -key iis.pem -inform PEM

show ssl fipskey key-FIPS-2

FIPS Key Name: Key-FIPS-2 Modulus: 0   Public Exponent: F4 (Hex value 0x10001)
<!--NeedCopy-->
```

Importer une clé externe en tant que clé FIPS à l'aide de l'interface graphique

1. Si la clé est au format .pfx, vous devez d'abord la convertir au format PEM.
   a) Accédez à **Gestion du trafic > SSL**.
   b) Dans le volet d'informations, sous Outils, cliquez sur **Importer PKCS #12**.
   c) Dans la boîte de dialogue Importer un fichier PKCS12, définissez les paramètres suivants :
      - Nom du fichier de sortie*
      - Nom du fichier PKCS12* : spécifiez le nom du fichier .pfx.
      - Mot de passe d'importation*
      - Format d'encodage

      *Un paramètre obligatoire
2. Accédez à **Gestion du trafic > SSL > FIPS**.
3. Dans le volet d'informations, sous l'onglet Clés FIPS, cliquez sur **Importer**.
4. Dans la boîte de dialogue Importer en tant que clé FIPS, sélectionnez le fichier PEM et définissez les valeurs des paramètres suivants :
   - Nom de la clé FIPS*

- Nom du fichier clé* : pour placer le fichier dans un emplacement autre que celui par défaut, vous pouvez spécifier le chemin d'accès complet ou cliquer sur Parcourir et accéder à un emplacement.

*Paramètre obligatoire

5. Cliquez sur **Importer**, puis cliquez sur **Fermer**.
6. Sous l'onglet Touches FIPS, vérifiez que les paramètres affichés pour la clé FIPS que vous avez importée sont corrects.

Configurer FIPS sur des appliances dans une configuration HA

Vous pouvez configurer deux appliances dans une paire HA en tant qu'appliances FIPS.

Composants requis

- Le module de sécurité matérielle (HSM) doit être configuré sur les deux appliances. Pour plus d'informations, voir Configurer le HSM.
- Lorsque vous utilisez l'interface graphique, vérifiez que les appliances sont déjà dans une configuration HA. Pour plus d'informations sur la configuration d'une configuration HA, voir Haute disponibilité.

> **Remarque :**
>
> Citrix recommande d'utiliser l'utilitaire de configuration (GUI) pour cette procédure. Si vous utilisez la ligne de commande (CLI), assurez-vous de suivre attentivement les étapes indiquées dans la procédure. La modification de l'ordre des étapes ou la spécification d'un fichier d'entrée incorrect peut entraîner une incohérence nécessitant un redémarrage de l'appliance. En outre, si vous utilisez l'interface de ligne de commande, la commande `create ssl fipskey` n'est pas propagée au nœud secondaire. Lorsque vous exécutez la commande avec les mêmes valeurs d'entrée pour la taille du module et l'exposant sur deux dispositifs FIPS différents, les clés générées ne sont pas les mêmes. Créez la clé FIPS sur l'un des nœuds, puis transférez-la vers l'autre nœud. Toutefois, si vous utilisez l'utilitaire de configuration pour configurer des dispositifs FIPS dans une configuration HA, la clé FIPS que vous créez est automatiquement transférée vers le nœud secondaire. Le processus de gestion et de transfert des clés FIPS est connu sous le nom de gestion sécurisée des informations (SIM).

Important : La configuration de la haute disponibilité doit être terminée dans un délai de six minutes. Si la procédure échoue à une étape quelconque, procédez comme suit :

> 1. Redémarrez l'appliance ou attendez 10 minutes.
> 2. Supprimez tous les fichiers créés par la procédure.
> 3. Répétez la procédure de configuration HA.

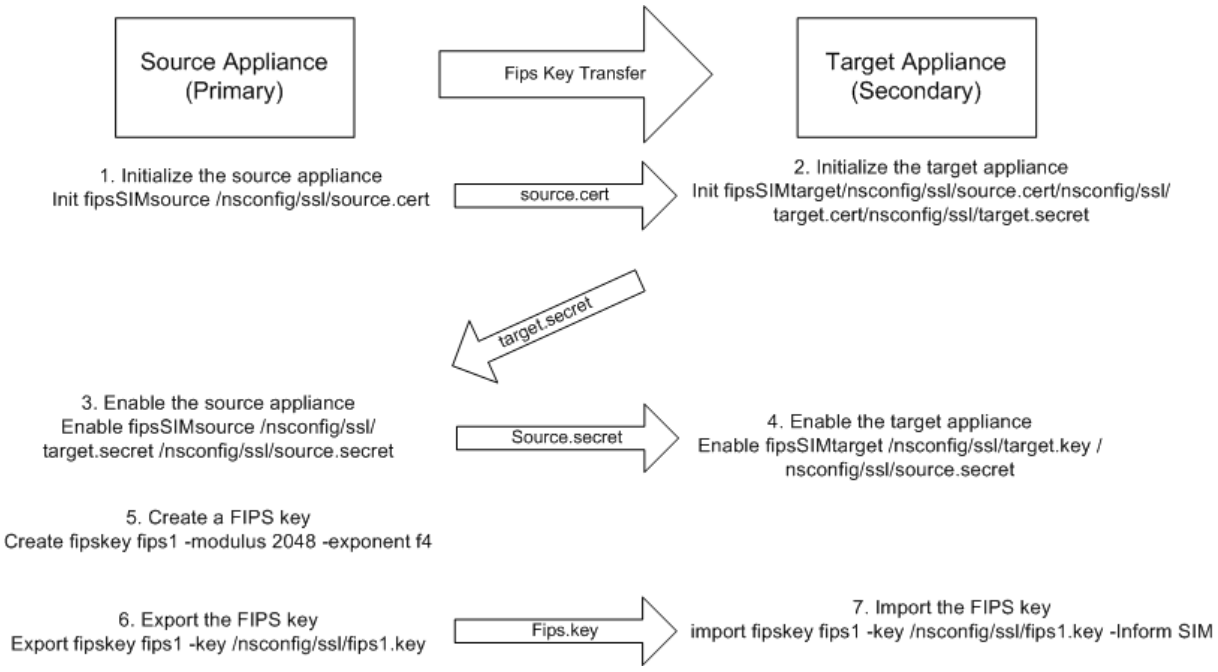
> Ne réutilisez pas les noms de fichiers existants.

Dans la procédure suivante, l'appliance A est le nœud principal et l'appliance B est le nœud secondaire.

Configurer FIPS sur des appliances dans une configuration HA à l'aide de l'interface de ligne de commande

Le diagramme suivant résume le processus de transfert sur l'interface de ligne de commande.

Figure 1. Transférer le récapitulatif des clés FIPS



1. **Sur l'appliance A**, ouvrez une connexion SSH à l'appliance à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur l'appliance à l'aide des informations d'identification de l'administrateur.
3. Initialisez l'appliance A en tant qu'appliance source. À l'invite de commande, tapez :

   ```
   1 init ssl fipsSIMsource <certFile>
   2 <!--NeedCopy-->
   ```

   Exemple :

   ```
   init fipsSIMsource /nsconfig/ssl/nodeA.cert
   ```

4. Copiez ce fichier <certFile> sur l'appliance B, dans le dossier /nconfig/ssl.

   Exemple :

   ```
   scp /nsconfig/ssl/nodeA.cert nsroot@198.51.100.10:/nsconfig/ssl
   ```


5. **Sur l'appliance B**, ouvrez une connexion SSH à l'appliance à l'aide d'un client SSH, tel que PuTTY.
6. Ouvrez une session sur l'appliance à l'aide des informations d'identification de l'administrateur.
7. Initialisez l'appliance B en tant qu'appliance cible. À l'invite de commande, tapez :

```
init ssl fipsSIMtarget <certFile> <keyVector> <targetSecret>
<!--NeedCopy-->
```

Exemple :

```
init fipsSIMtarget /nsconfig/ssl/nodeA.cert /nsconfig/ssl/nodeB.key /
nsconfig/ssl/nodeB.secret
```

8. Copiez ce fichier <targetSecret> sur l'appliance A.

Exemple :

```
scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.20:/nsconfig/
ssl
```

9. **Sur l'appliance A**, activez l'appliance A en tant qu'appliance source. À l'invite de commande, tapez :

```
enable ssl fipsSIMSource <targetSecret> <sourceSecret>
<!--NeedCopy-->
```

Exemple :

```
enable fipsSIMsource /nsconfig/ssl/nodeB.secret /nsconfig/ssl/nodeA.
secret
```

10. Copiez ce fichier <sourceSecret> sur l'appliance B.

Exemple :

```
scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.10:/nsconfig/
ssl
```

11. **Sur l'appliance B**, activez l'appliance B en tant qu'appliance cible. À l'invite de commande, tapez :

```
enable ssl fipsSIMtarget <keyVector> <sourceSecret>
<!--NeedCopy-->
```

Exemple :

```
enable fipsSIMtarget /nsconfig/ssl/nodeB.key /nsconfig/ssl/nodeA.secret
```

12. **Sur l'appliance A**, créez une clé FIPS, comme décrit dans Créer une clé FIPS.

13. Exportez la clé FIPS vers le disque dur de l'appliance, comme décrit dans Exporter une clé FIPS.
14. Copiez la clé FIPS sur le disque dur de l'appliance secondaire à l'aide d'un utilitaire de transfert de fichiers sécurisé, tel que SCP.
15. **Sur l'appliance B**, importez la clé FIPS du disque dur dans le HSM de l'appliance, comme décrit dans Importer une clé FIPS.

Configurer FIPS sur des appliances dans une configuration HA à l'aide de l'interface graphique

1. Sur l'appliance à configurer en tant qu'appliance source (principale), accédez à **Gestion du trafic > SSL > FIPS**.
2. Dans le volet d'informations, sous l'onglet Informations FIPS, cliquez sur **Activer la carte SIM**.
3. Dans la boîte de dialogue **Activer la carte SIM pour la paire HA**, dans la zone de texte **Nom du fichier de certificat**, tapez le nom du fichier. Le nom du fichier doit contenir le chemin d'accès à l'emplacement où le certificat FIPS doit être stocké sur l'appliance source.
4. Dans la zone de texte **Nom du fichier vectoriel clé**, tapez le nom du fichier. Le nom du fichier doit contenir le chemin d'accès à l'emplacement où le vecteur de clé FIPS doit être stocké sur l'appliance source.
5. Dans la zone de texte **Nom du fichier secret cible**, tapez l'emplacement de stockage des données secrètes sur le dispositif cible.
6. Dans la zone de texte **Nom du fichier secret source**, tapez l'emplacement de stockage des données secrètes sur le dispositif source.
7. Sous **Secondary System Login Credential**, entrez les valeurs du **nom d'utilisateur et dumot de passe**.
8. Cliquez sur **OK**. Les appliances FIPS sont maintenant configurées en mode HA.

Remarque : Après avoir configuré les appliances dans HA, créez une clé FIPS, comme décrit dans Créer une clé FIPS. La clé FIPS est automatiquement transférée de l'appliance principale à l'appliance secondaire.

Créer une demande de signature de certificat à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
    <string>) [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName<string>
    [-organizationUnitName <string>] [-localityName <string>] [-
    commonName <string>] [-emailAddress <string>] {
 -challengePassword  }
```



```
5    [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
6 <!--NeedCopy-->
```

Exemple :

```
1 >create certreq f1.req  - fipsKeyName  f1 -countryName US  -stateName CA
      -organizationName Citrix -companyName Citrix -commonName ctx -
     emailAddress test@example.com
2 Done
3 <!--NeedCopy-->
```

Créer un certificat de serveur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 create ssl cert <certFile> <reqFile> <certType> [-keyFile <
     input_filename>] [-keyform ( DER | PEM ) {
2  -PEMPassPhrase  }
3  ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
      input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
      input_filename>][-CAkeyForm ( DER | PEM )] [-CAserial <
      output_filename>]
4 <!--NeedCopy-->
```

Exemple :

```
1 create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
     root.key -CAserial ns-root.srl -days 1000
2 Done
3 <!--NeedCopy-->
```

L'exemple précédent crée un certificat de serveur à l'aide d'une autorité de certification racine locale sur l'appliance.

Ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
     string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>][-
     expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
     positive_integer>]] [-bundle ( YES | NO )]
2 <!--NeedCopy-->
```


Exemple :

```
add certkey cert1 -cert f1.cert -fipsKey f1

<!--NeedCopy-->
```

Après avoir créé la clé FIPS et le certificat de serveur, vous pouvez ajouter la configuration SSL générique. Activez les fonctionnalités requises pour votre déploiement. Ajoutez des serveurs, des services et des serveurs virtuels SSL. Liez la paire de clés de certificat et le service au serveur virtuel SSL. Enregistrez la configuration.

```
enable ns feature SSL LB

add server s1 10.217.2.5

add service sr1 s1 HTTP 80

add lb vserver v1 SSL 10.217.2.172 443

bind ssl vserver v1  -certkeyName cert1

bind lb vserver v1 sr1

saveconfig

<!--NeedCopy-->
```

La configuration de base de votre appliance MPX 14000 FIPS est maintenant terminée.

Pour plus d'informations sur la configuration de HTTPS sécurisé, cliquez sur Configurer FIPS.

Pour plus d'informations sur la configuration du RPC sécurisé, cliquez sur Configurer FIPS pour la première fois.

Mettre à jour la licence sur un dispositif FIPS MPX 14000

Toute mise à jour de la licence sur cette plate-forme nécessite deux redémarrages.

1. Mettez à jour la licence dans le `/nsconfig/license` dossier.
2. Redémarrez l'appliance.
3. Ouvrez une session sur l'appliance.
4. Redémarrez l'appliance à nouveau.
   Remarque : N'ajoutez pas de nouvelles commandes, n'enregistrez pas la configuration et ne vérifiez pas l'état du système avant le deuxième redémarrage.

5. Ouvrez une session sur l'appliance et vérifiez que FIPS est initialisé en exécutant la commande `show ssl fips`.

Prise en charge du mode FIPS hybride sur les plates-formes FIPS MPX 14000 et SDX 14000 FIPS

> **Remarque :**
>
> Cette fonctionnalité n'est prise en charge que sur la nouvelle plate-forme FIPS MPX/SDX 14000 contenant une carte FIPS principale et une ou plusieurs cartes secondaires. Il n'est pas pris en charge sur une plate-forme VPX ou une plate-forme contenant un seul type de carte matérielle.

Sur une plateforme FIPS, le chiffrement et le déchiffrement asymétriques et symétriques sont effectués sur la carte FIPS pour des raisons de sécurité. Toutefois, vous pouvez effectuer une partie de cette activité (asymétrique) sur une carte FIPS et décharger le chiffrement et le déchiffrement en masse (symétrique) sur une autre carte sans compromettre la sécurité de vos clés.

La nouvelle plateforme FIPS MPX/SDX 14000 contient une carte principale et une ou plusieurs cartes secondaires. Si vous activez le mode FIPS hybride, les commandes de déchiffrement secret prémaître sont exécutées sur la carte principale car la clé privée est stockée sur cette carte. Toutefois, le chiffrement et le déchiffrement en masse sont déchargés sur la carte secondaire. Ce déchargement augmente considérablement le débit de chiffrement en masse sur une plate-forme FIPS MPX/SDX 14000 par rapport au mode FIPS non hybride et à la plate-forme FIPS MPX 9700/10500/12500/15000 existante. L'activation du mode FIPS hybride améliore également la transaction SSL par seconde sur cette plate-forme.

> **Remarques :**
>
> - Le mode FIPS hybride est désactivé par défaut pour répondre aux exigences de certification strictes, où tous les calculs cryptographiques doivent être effectués dans un module certifié FIPS. Activez le mode hybride pour décharger le chiffrement et le déchiffrement en masse sur la carte secondaire.
> - Sur une plate-forme FIPS SDX 14000, vous devez d'abord attribuer une puce SSL à l'instance VPX avant d'activer le mode hybride.

Activer le mode FIPS hybride à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set SSL parameter -hybridFIPSMode {
 ENABLED|DISABLED }


Arguments
```



```
6
7  hybridFIPSMode
8
9  When this mode is enabled, system will use additional crypto hardware
       to accelerate symmetric crypto operations.
10
11 Possible values: ENABLED, DISABLED
12
13 Default value: DISABLED
14 <!--NeedCopy-->
```

Exemple :

```
1      set SSL parameter -hybridFIPSMode ENABLED
2      show SSL parameter
3      Advanced SSL Parameters
4      -----------------------
5      . . . . . .
6      Hybrid FIPS Mode    : ENABLED
7      . . . . . .
8
9  <!--NeedCopy-->
```

Activer le mode FIPS hybride à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres SSL avancés**.
3. Dans la boîte de dialogue **Modifier les paramètres SSL avancés**, sélectionnez **Mode FIPS hybride**.

Limites :

1. La renégociation n'est pas prise en charge.
2. La commande `stat ssl parameter` sur une plate-forme SDX 14000 n'affiche pas le pourcentage d'utilisation de la carte secondaire correct. Il affiche toujours 0,00% d'utilisation.

```
1  stat ssl
2
3  SSL Summary
4  # SSL cards present 1
5  # SSL cards UP  1
6  # Secondary SSL cards present   4
7  # Secondary SSL cards UP    4
```



```
SSL engine status       1
SSL sessions (Rate)     963
Secondary card utilization (%)     0.00
<!--NeedCopy-->
```

Appliances FIPS SDX 14000

June 2, 2023

> **Remarque**
>
> Les versions du microprogramme répertoriées sous « NetScaler version 12.1-FIPS » et « NetScaler version 12.1-NDCPP » sur la page de téléchargement de NetScaler ne sont pas prises en charge sur les plateformes MPX 14000 FIPS ou SDX 14000 FIPS. Ces plateformes peuvent utiliser les autres versions les plus récentes du microprogramme NetScaler disponibles sur la page des téléchargements.

Une appliance NetScaler SDX est une plate-forme mutualisée sur laquelle vous pouvez provisionner et gérer plusieurs instances virtuelles de NetScaler. L'appliance SDX répond aux exigences de cloud computing et de mutualisation en permettant à un seul administrateur de configurer et de gérer l'appliance et de déléguer l'administration de chaque instance hébergée aux locataires.

Une appliance FIPS NetScaler SDX 14030/14060/14080 fournit les fonctionnalités d'une appliance SDX avec la fonctionnalité FIPS. Il est équipé d'un module cryptographique inviolable (inviolable), un Cavium CNN3560-NFBE-G, conçu pour être conforme aux spécifications FIPS 140-2 de niveau 3 (à partir de la version 12.0 build 56.x). Les paramètres de sécurité critiques (CSP), principalement la clé privée du serveur, sont stockés et générés de manière sécurisée à l'intérieur du module cryptographique. Ce module est également appelé module de sécurité matérielle (HSM). Les CSP ne sont jamais accessibles à l'extérieur des limites du HSM. Seul le superutilisateur (`nsroot`) peut effectuer des opérations sur les clés stockées dans le HSM.

Une appliance FIPS NetScaler SDX 14030/14060/14080 contient un module FIPS HSM avec 63 cœurs. Le module HSM FIPS peut être partitionné jusqu'à 32 partitions au maximum. L'administrateur SDX peut attribuer un stockage de clés dédié, des ressources cryptographiques et un nombre de cœurs FIPS SSL cryptographiques à chaque partition. Les clés et les ressources allouées à une partition sont dédiées et sécurisées et aucune autre partition ne peut y accéder ni les partager.

La partition HSM FIPS que vous créez peut être affectée ou attachée à une instance VPX au moment du provisionnement de l'instance, ou ultérieurement en modifiant l'instance. La partition FIPS créée et attachée à une instance agit comme un module HSM virtuel pour cette instance.

Les instances VPX sur un dispositif FIPS SDX 14030/14060/14080 se voient attribuer une partition de

fonction virtuelle (VF) FIPS, qui est traitée comme une carte virtuelle FIPS ou un HSM isolé. Par conséquent, les étapes pour configurer une partition FIPS dans une instance VPX sont similaires à celles pour configurer un dispositif FIPS MPX. Pour plus de détails sur la conformité, consultez les détails de la stratégie de sécurité sur le site Web du National Institute of Standards and Technology (NIST) des États-Unis.

Pour plus d'informations sur la configuration des appliances FIPS dans une configuration haute disponibilité, voir Configurer les appliances FIPS dans une configuration HA.

> **Important**
>
> Chaque clé inclut une clé privée et une clé publique. Par conséquent, il occupe deux espaces clés. Par conséquent, le nombre maximum de clés est limité à une clé de moins de la moitié de la taille du magasin de clés.

La plate-forme FIPS SDX 14000 prend en charge un mode FIPS hybride. Ce mode vous permet de décharger une partie de l'activité de chiffrement et de déchiffrement sur une carte non-FIPS. Pour plus d'informations, voir Mode FIPS hybride.

Limitations

January 21, 2021

1. La renégociation SSL à l'aide du protocole SSLv3 n'est pas prise en charge sur le back-end d'une appliance SDX FIPS.
2. Les clés 1024 bits et 4096 bits et une valeur exposant de 3 ne sont pas prises en charge.
3. La sauvegarde et la restauration ne sont pas prises en charge.
4. Les domaines de cluster et d'administration ne sont pas pris en charge.
5. Vous ne pouvez attacher qu'une seule partition FIPS à une instance.
6. Une instance avec une partition FIPS ne peut être affectée qu'à un seul cœur de CPU.
7. Vous pouvez attribuer une partition FIPS ou un cœur SSL à une instance, mais pas les deux.
8. Le certificat de serveur 4096 bits n'est pas pris en charge.
9. Le certificat client 4096 bits n'est pas pris en charge (si l'authentification client est activée sur le serveur principal).

Terminologie

May 5, 2023

Zeroize : réinitialisez le HSM. Toutes les données du HSM sont supprimées. Cette étape est obligatoire avant l'initialisation du HSM.

Initialiser : définissez les fonctionnalités du HSM. L'appliance NetScaler SDX FIPS est conforme à la norme FIPS-140-2 niveau 2. Vous pouvez créer des partitions après avoir initialisé la puce.

Taille du magasin de clés : nombre de clés pouvant être stockées sur une partition. Un maximum de 102 235 touches peut être spécifié. Le nombre maximum de clés pouvant être stockées est inférieur à la moitié du nombre spécifié. Par exemple, si vous spécifiez 100, vous ne pouvez créer que 49 clés car l'une des clés est la paire de clés RSA qui consomme 2 magasins de clés.

Capacité du cœur de chiffrement : nombre de cœurs de chiffrement affectés à une partition. Un maximum de 63 cœurs sont disponibles.

Contexte SSL : nombre de connexions SSL simultanées pouvant être créées sur une partition.

Initialiser le HSM

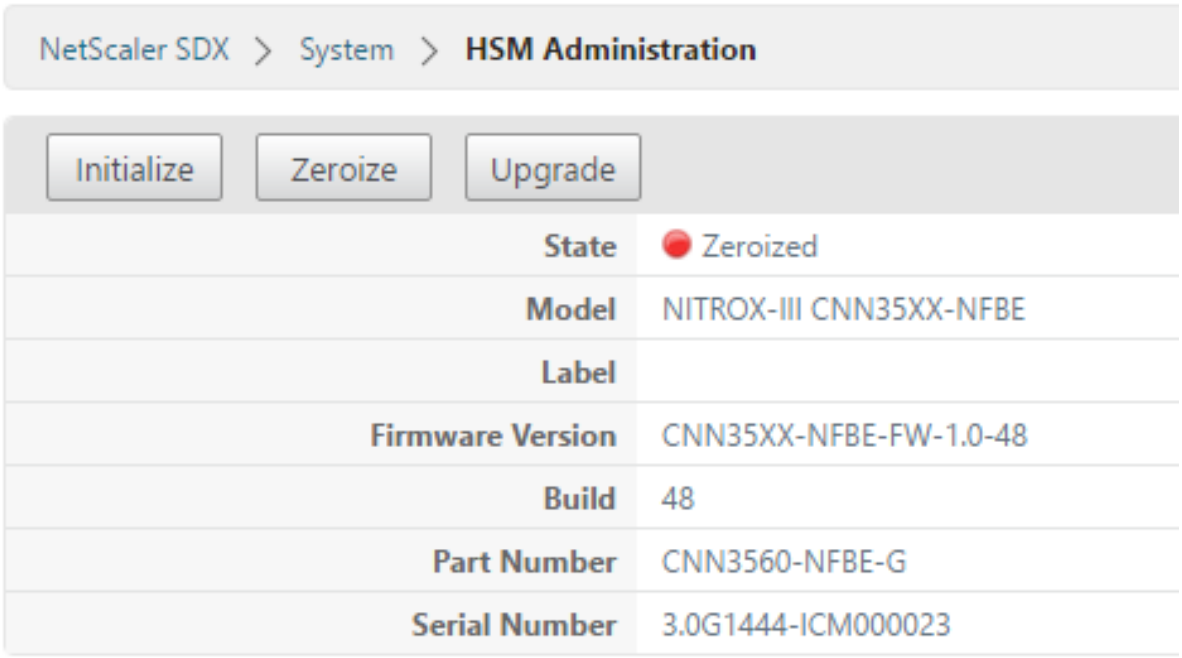
January 21, 2021

Avant d'initialiser le HSM, vous devez d'abord le mettre à zéro.

Mettre à zéro le HSM à l'aide du service de gestion

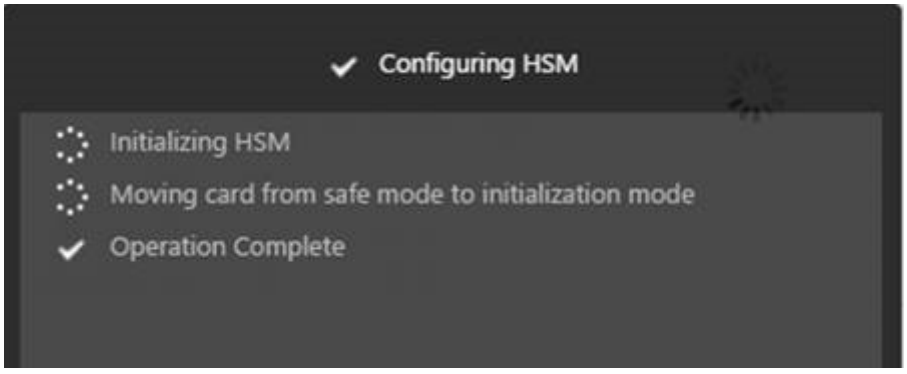
1. Ouvrez un navigateur et connectez-vous à l'appliance.
2. Sous l'onglet **Configuration**, accédez à **Système > Administration HSM**et, dans le plan de détails, cliquez sur **Mise à zéro**.

Toutes les données sont effacées de la puce FIPS, et l'état apparaît comme « mis à zéro ». Toutes les partitions HSM créées précédemment sont supprimées.

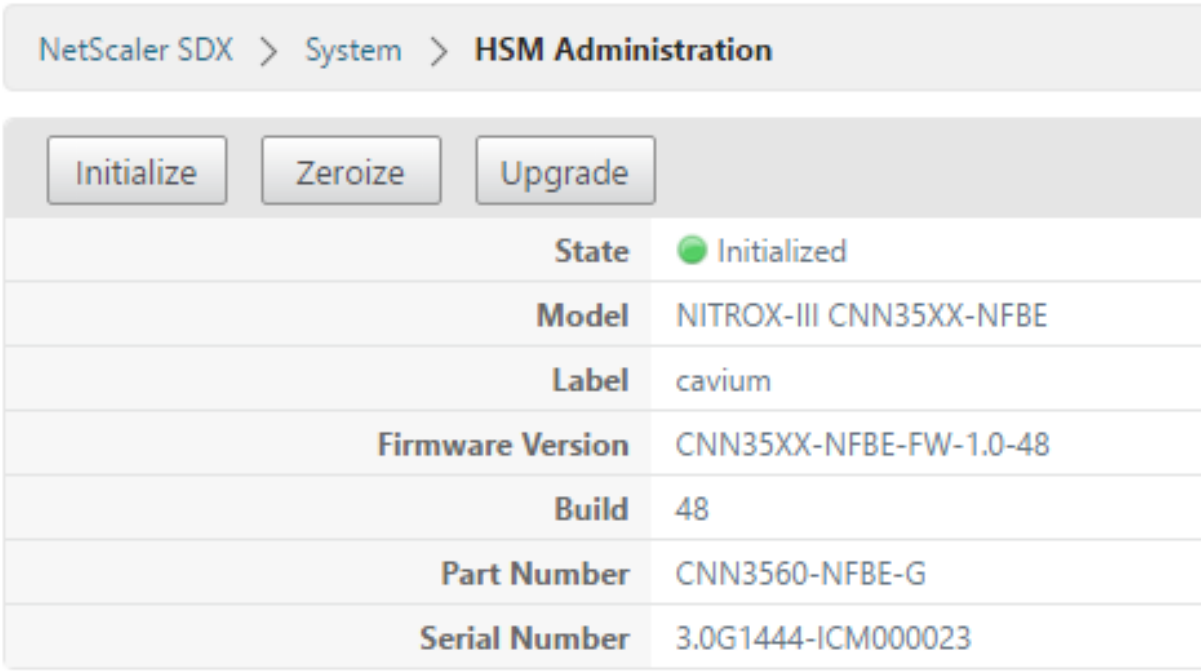


Initialiser le HSM à l'aide du service de gestion

1. Sous l'onglet **Configuration**, accédez à **Système > Administration HSM**et, dans le plan de détails, cliquez sur **Initialiser**.
2. Tapez un nouveau nom d'utilisateur, spécifiez un mot de passe, puis cliquez sur **OK**.



L'état de la carte apparaît comme « Initialisé ».



Créer des partitions

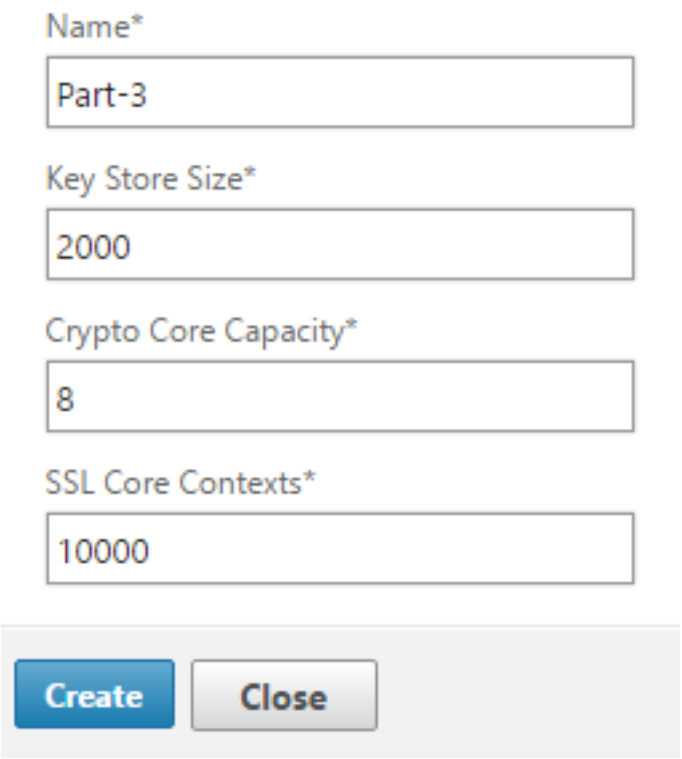
May 5, 2023

Créez des partitions pour différents locataires et spécifiez les ressources cryptographiques pour chaque partition. Une partition est attribuée à chaque instance, et une partition ne peut être attribuée qu'à une seule instance. La suppression d'une instance entraîne la suppression de la partition attribuée à l'instance. Par conséquent, les données de partition sont également supprimées et ne sont pas laissées non sécurisées ou accessibles ultérieurement. Le nombre de clés et l'attribution du contexte SSL dépendent de votre application. Pour plus d'informations sur le nombre de cœurs à attribuer, consultez la fiche technique de NetScaler.

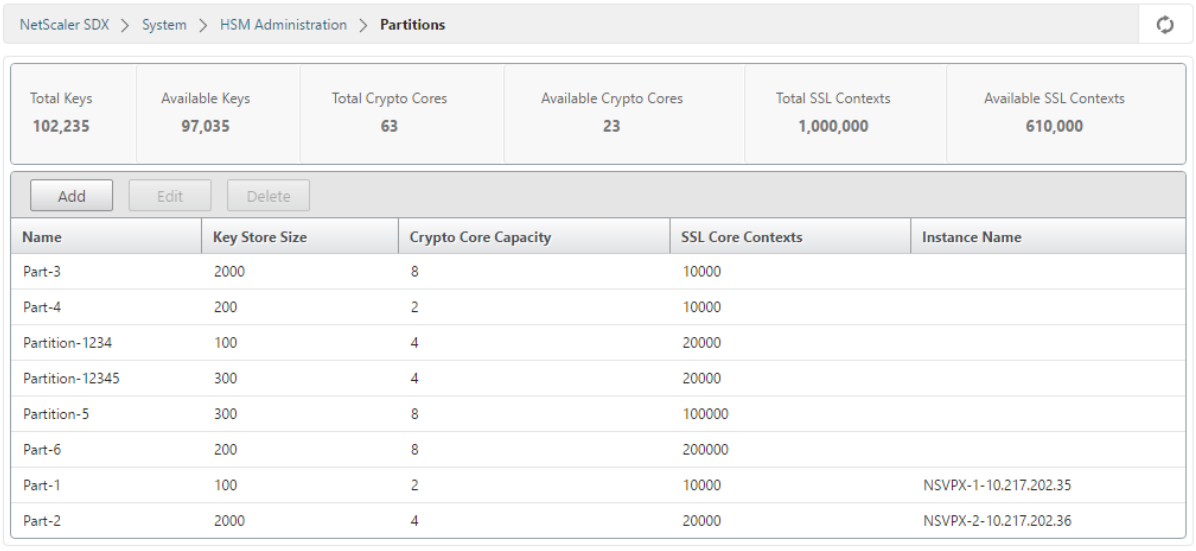
> **Important**
>
> Une fois que vous avez attribué une taille de stockage de clés et des cœurs à une partition HSM, vous ne pouvez pas les modifier au moment de l'exécution. Commencez par détacher la partition de l'instance.

Création d'une partition à l'aide du service de gestion

1. Dans l'onglet Configuration, accédez à **Système** > **Administration HSM** > **Partitions**, puis dans le plan de détails, cliquez sur **Ajouter**.
2. Spécifiez le nom de la partition et les ressources à affecter à cette partition.
3. Cliquez sur **OK**.



La page récapitulative affiche toutes les partitions qui ont été créées. Certaines partitions se voient attribuer une instance tandis que d'autres sont des partitions libres.



Name	Key Store Size	Crypto Core Capacity	SSL Core Contexts	Instance Name
Part-3	2000	8	10000	
Part-4	200	2	10000	
Partition-1234	100	4	20000	
Partition-12345	300	4	20000	
Partition-5	300	8	100000	
Part-6	200	8	200000	
Part-1	100	2	10000	NSVPX-1-10.217.202.35
Part-2	2000	4	20000	NSVPX-2-10.217.202.36

Provisionner une nouvelle instance ou modifier une instance existante et attribuer une partition

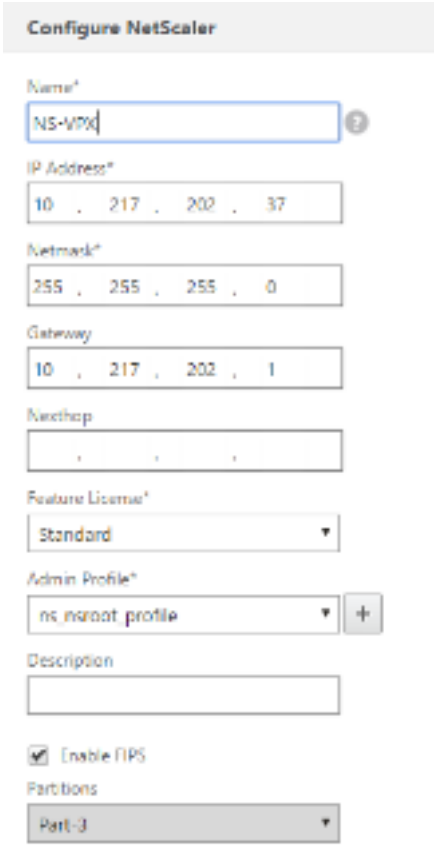
August 10, 2022

Après avoir créé les partitions, vous devez les affecter aux instances.

> **Important :**
>
> - Vous ne pouvez attacher qu'une seule partition FIPS à une instance.
> - Une instance avec une partition FIPS ne peut se voir attribuer qu'un seul cœur de processeur.

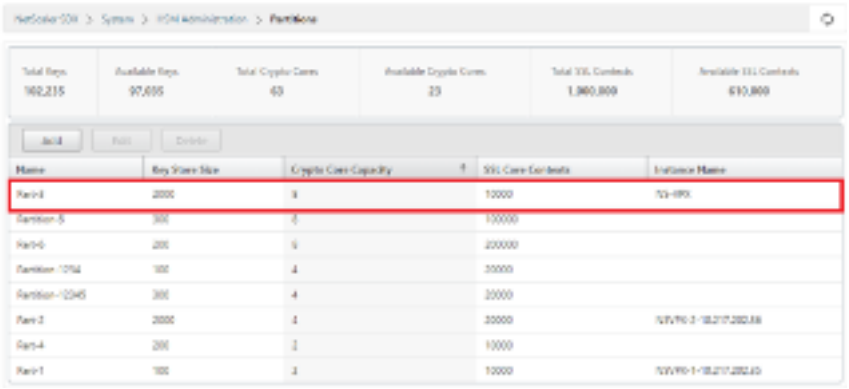
Provisionner une nouvelle instance ou modifier une instance existante

1. Dans l'onglet Configuration, accédez à **NetScaler** > **Instances**, puis ajoutez ou modifiez une instance.
2. Sélectionnez **Activer FIPS**, puis dans la liste **Partitions**, sélectionnez une partition à attacher à cette instance.



Vous pouvez vérifier que la partition est attachée à une instance à l'aide de l'interface graphique ou de l'interface de ligne de commande.

Dans l'interface graphique, accédez à **Système** > **Administration HSM** > **Partitions**. Le nom de l'instance attachée à la partition s'affiche.



Pour annuler l'attribution d'une partition FIPS ¸ accédez à **NetScaler** > **Instances**. Modifiez l'instance et **désactivez la case à cocher Activer FIPS** .

Dans l'interface de ligne de commande, à l'invite de commandes, tapez les commandes suivantes :

```
show fips

FIPS Card is not configured
 Done
<!--NeedCopy-->
```

Si vous voyez le résultat suivant, consultez la section de dépannage pour le débogage.

ERREUR : Opération non autorisée - aucune carte FIPS présente dans le système

> Remarque
>
> Lorsqu'une partition est détachée de l'une des instances VPX existantes, les données de la partition sont effacées. En conséquence, toute configuration actuelle (par exemple les clés FIPS) est perdue. Une fois qu'une partition est détachée ou rattachée à une instance VPX nouvelle ou précédemment liée, elle doit être initialisée conformément aux instructions de la section Configurer le HSM avant de pouvoir utiliser la partition pour des connexions sécurisées.
>
> Pendant ce temps (une fois la partition détachée ou rattachée), l'instance VPX correspondante est accessible via l'interface graphique via HTTP et via la CLI à l'aide de SSH.

Configurer le HSM pour une instance sur une appliance FIPS SDX 14030/14060/14080

December 3, 2021

Vérifiez d'abord l'état de votre carte FIPS pour vérifier que le pilote est correctement chargé, puis initialisez la carte.

À l'invite de commandes, tapez :

```
show fips

FIPS Card is not configured

Done
<!--NeedCopy-->
```

Si le pilote n'est pas chargé correctement, le message « ERREUR : opération non autorisée - aucune carte FIPS présente dans le système » s'affiche.

Initialiser la carte FIPS

> **Important :**
>
> Vérifiez que le `/nsconfig/fips` répertoire a bien été créé sur l'appliance.

N'enregistrez pas la configuration avant de redémarrer l'appliance pour la troisième fois.

Pour initialiser la carte FIPS, effectuez les opérations suivantes :

1. Réinitialisez la carte FIPS (`reset fips`).
2. Redémarrez l'appliance (`reboot`).
3. Définissez le mot de passe du responsable de la sécurité pour les partitions 0 et 1, et le mot de passe utilisateur pour la partition (`set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -hsmLabel NSFIPS`).

   Remarque : L'exécution de la commande set ou reset prend plus de 60 secondes.
4. Enregistrez la configuration (`saveconfig`).
5. Vérifiez que la clé chiffrée par mot de passe pour la partition principale (master_pek.key) a été créée dans le répertoire /nsconfig/fips/.
6. Redémarrez l'appliance (`reboot`).
7. Vérifiez que la carte FIPS est UP (`show fips`).

Initialisez la carte FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
reset fips

reboot

set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -
   hsmLabel <string>
<!--NeedCopy-->
```

> **Remarque** : Le message suivant s'affiche lorsque vous exécutez la commande **set fips** :

```
This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. [Note: On
   MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
   default, and the -initHSM Level-2 option is internally converted to
   Level-3]  Do you want to continue?(Y/N)y

saveconfig

reboot

show fips
<!--NeedCopy-->
```

Exemple :

```
reset fips

Done

reboot

set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS

This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. [Note: On
   MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
   default, and the -initHSM Level-2 option is internally converted to
   Level-3]  Do you want to continue?(Y/N)y

Done

saveconfig
```



```
14
15 Done
16
17 reboot
18
19 show fips
20
21     FIPS HSM Info:
22     HSM Label : NSFIPS
23     Initialization : FIPS-140-2 Level-2
24     HSM Serial Number : 3.0G1532-ICM000228
25     HSM State : 2
26     HSM Model : NITROX-III CNN35XX-NFBE
27     Hardware Version : 0.0-G
28     Firmware Version : 1.0
29     Firmware Build : NFBE-FW-1.0-48
30     Max FIPS Key Memory : 1000
31     Free FIPS Key Memory : 1000
32     Total SRAM Memory : 557396
33     Free SRAM Memory : 238088
34     Total Crypto Cores : 4
35     Enabled Crypto Cores : 4
36 Done
37 <!--NeedCopy-->
```

Créer une clé FIPS pour une instance sur une appliance FIPS SDX 14030/14060/14080

August 20, 2021

Vous pouvez créer une clé FIPS sur votre instance ou importer une clé FIPS existante dans l'instance. Une appliance FIPS SDX 14030/14060/14080 ne prend en charge que les clés 2048 bits et 3072 bits et une valeur exposant F4. Pour les clés PEM, un exposant n'est pas requis. Vérifiez que la clé FIPS est créée correctement. Créez une demande de signature de certificat et un certificat de serveur. Enfin, ajoutez la paire de clés de certificat à votre instance.

> **Remarque :**
>
> Les clés 1024 bits et 4096 bits et une valeur exposant de 3 ne sont pas prises en charge.

Créer une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent (3 | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
<!--NeedCopy-->
```

Exemple :

```
create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4

Done

show ssl fipskey ddvws

FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (Hex: 0x10001)

Done
<!--NeedCopy-->
```

Importer une clé FIPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-wrapKeyName <string>] [-iv<string>] [-exponent F4 ]
<!--NeedCopy-->
```

Exemple :

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4
Done
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM
Done
<!--NeedCopy-->
```

Vérifiez que la clé FIPS est créée ou importée correctement en exécutant la commande **show fipskey**.

```
show fipskey
1)      FIPS Key Name: Key-FIPS-2
Done
<!--NeedCopy-->
```


Créer une demande de signature de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
    <string>) [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName<string>
     [-organizationUnitName <string>] [-localityName <string>] [-
     commonName <string>] [-emailAddress <string>] {
 -challengePassword  }
  [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
<!--NeedCopy-->
```

Exemple :

```
create certreq f1.req  - fipsKeyName f1 -countryName US -stateName CA -
    organizationName Citrix -companyName Citrix -commonName ctx -
    emailAddress test@example.com`
`Done
<!--NeedCopy-->
```

Créer un certificat de serveur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM ) {
 -PEMPassPhrase  }
 ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
     input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
     input_filename>] [-CAkeyForm ( DER | PEM )] [-CAserial <
     output_filename>]
<!--NeedCopy-->
```

Exemple :

```
create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
    root.key -CAserial ns-root.srl -days 1000
Done
<!--NeedCopy-->
```

L'exemple précédent crée un certificat de serveur à l'aide d'une autorité de certification racine locale sur l'appliance.

Ajouter une paire de clés de certificat à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
   string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>]
   [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod   <
   positive_integer>]] [-bundle ( YES | NO )]
<!--NeedCopy-->
```

Exemple :

```
add certkey cert1 -cert f1.cert -fipsKey f1
Done
<!--NeedCopy-->
```

Après avoir créé la clé FIPS et le certificat de serveur, vous pouvez ajouter la configuration SSL générique. Activez les fonctionnalités requises pour votre déploiement. Ajoutez des serveurs, des services et des serveurs virtuels SSL. Liez la paire de clés de certificat et le service au serveur virtuel SSL et enregistrez la configuration.

```
enable ns feature SSL LB
Done
add server s1 10.217.2.5
Done
add service sr1 s1 HTTP 80
Done
add lb vserver v1 SSL 10.217.2.172 443
Done
bind ssl vserver v1  - certkeyName cert1
Done
bind lb vserver v1 sr1
Done
saveconfig
Done
<!--NeedCopy-->
```

Pour plus d'informations sur la configuration du protocole HTTPS sécurisé et du RPC sécurisé, cliquez ici.

Mettre à niveau le microprogramme FIPS HSM sur une instance VPX

June 2, 2023

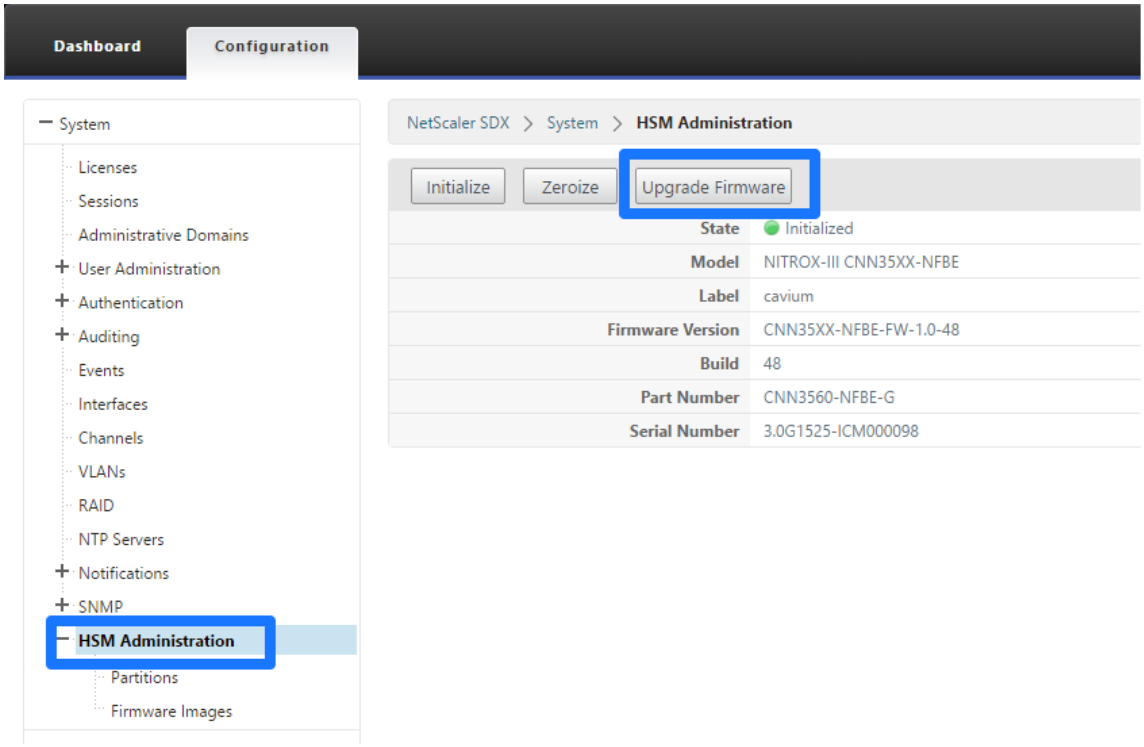
> **Remarque**
>
> Cette mise à niveau s'applique à la carte FIPS de l'appliance SDX 14000.

Des mises à jour du microprogramme FIPS HSM sont publiées de temps à autre. Téléchargez le microprogramme le plus récent depuis la page de téléchargement de NetScaler et chargez-le sur l'appliance. Le processus de mise à niveau peut prendre jusqu'à 10 minutes. L'instance est redémarrée après la mise à niveau.

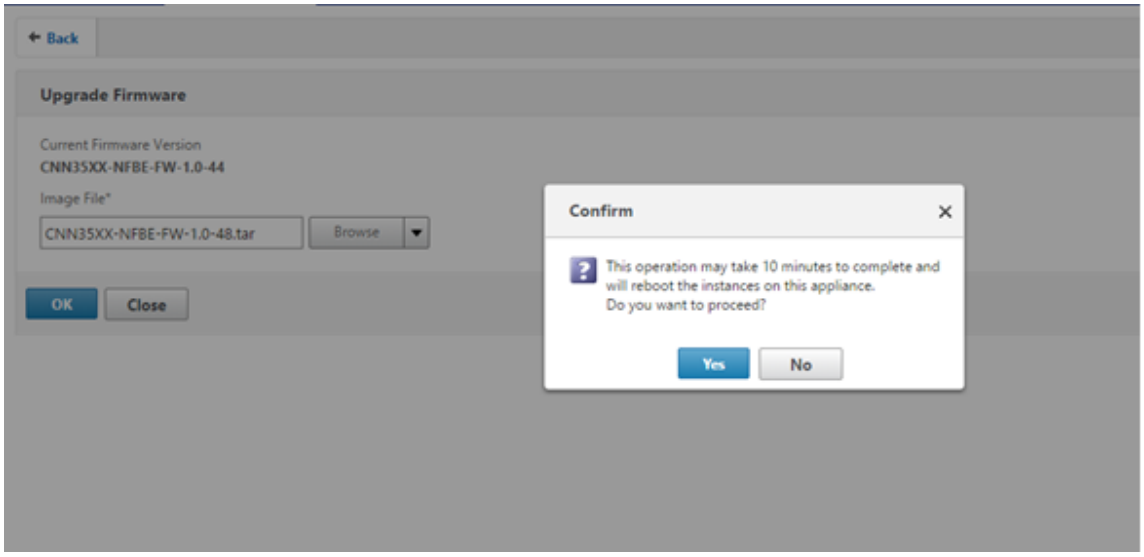
Mettre à niveau le microprogramme FIPS HSM

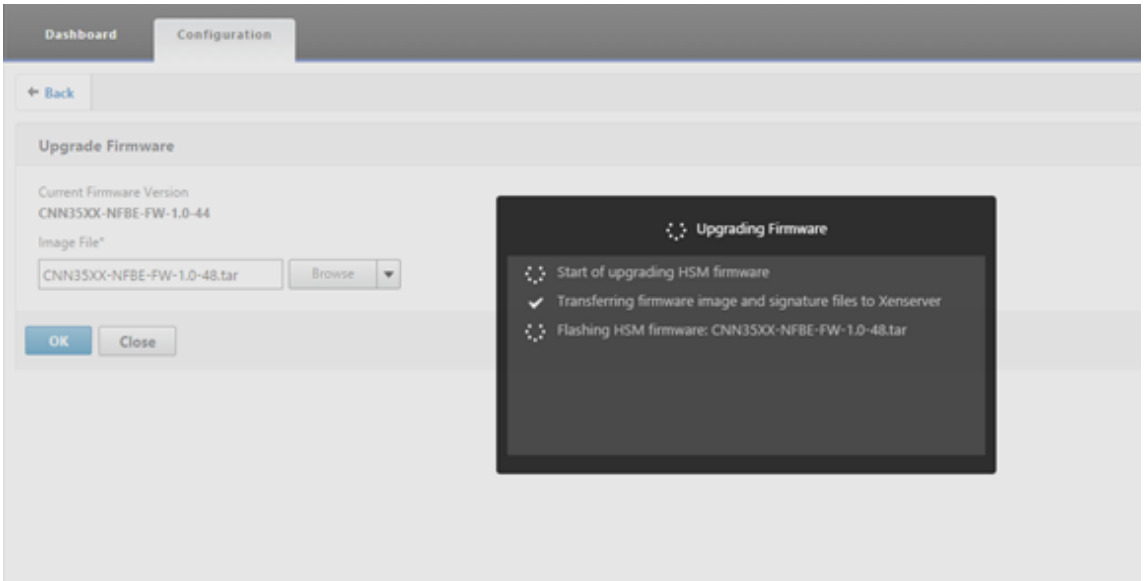
1. Accédez à **Système > Administration HSM > Images du microprogramme**.
2. Sélectionnez **Charger**.

3. Accédez au dossier contenant l'image du microprogramme et sélectionnez le fichier.
4. Accédez à **Système > Administration HSM**, puis sélectionnez **Mettre à niveau le microprogramme**.



5. Sélectionnez l'image du microprogramme vers laquelle effectuer la mise à niveau, puis cliquez sur **OK**.





Prise en charge du module de sécurité matérielle Thales Luna Network

May 5, 2023

Une appliance NetScaler non FIPS stocke la clé privée du serveur sur le disque dur. Sur un appareil FIPS, la clé est stockée dans un module cryptographique appelé module de sécurité matériel (HSM). Le stockage d'une clé dans le HSM la protège contre les attaques physiques et logicielles. De plus, les clés sont cryptées avec des chiffrements spéciaux approuvés par la FIPS.

Seules les appliances FIPS NetScaler MPX/SDX 14000 prennent en charge les cartes FIPS. La prise en charge de la norme FIPS n'est pas disponible sur les autres appliances MPX/SDX, ni sur les appliances NetScaler VPX. Cette limitation est corrigée par la prise en charge d'un HSM réseau Thales Luna sur toutes les appliances NetScaler MPX, SDX et VPX, à l'exception des appliances FIPS MPX/SDX 14000.

> **Remarque**
>
> La prise en charge des appliances répertoriées dans Support pour les plates-formes basées sur des puces SSL Intel Coleto et Intel Lewisburg est disponible dans la version 13.1 build 33.x et les versions ultérieures.

Un réseau HSM Thales Luna est conçu pour protéger les clés cryptographiques critiques et accélérer les opérations cryptographiques sensibles dans un large éventail d'applications de sécurité.

Matrice des versions prises en charge

Version de NetScaler	Version de l'appliance logicielle	Version du microprogramme	Version du client
11.1, 12.0, 12.1	5.2.3-1	6.2.1	6.0.0
11.1, 12.0, 12.1	6.2.2-5	6.10.9	6.2.2
13.0	7.2.0-220	7.0.3	7.2.2 (7.2.0-220)
13.1	7.2.0-220	7.0.3	10.3.0

Composants requis

May 5, 2023

Avant de pouvoir utiliser un HSM du réseau Thales Luna avec NetScaler, assurez-vous que les conditions suivantes sont remplies :

- Un HSM du réseau Thales Luna est installé sur le réseau, prêt à être utilisé et accessible à NetScaler. C'est-à-dire que l'adresse NSIP ou l'adresse SNIP est ajoutée en tant que client autorisé sur le HSM.
- Des licences sont disponibles pour prendre en charge le nombre requis de partitions sur le HSM.
- Le réseau HSM de Thales Luna et NetScaler peuvent établir des connexions entre eux via le port 1792.
- Vous utilisez NetScaler version 11.1 ou ultérieure.
- L'appliance NetScaler ne contient pas de carte FIPS Cavium.

> **Important**
>
> Les HSM réseau Thales Luna ne sont pas pris en charge sur les appliances FIPS MPX 9700/10500/12500/15500.

Configurer un client Thales Luna sur ADC

May 5, 2023

Une fois que vous avez configuré le HSM Thales Luna et créé les partitions requises, vous devez créer des clients et les affecter à des partitions. Commencez par configurer les clients Thales Luna sur NetScaler et par configurer les liens de confiance réseau (NTL) entre les clients Thales Luna et le HSM Thales Luna. Un exemple de configuration est fourni dans l' annexe.

> **Remarque**
>
> Si vous effectuez une mise à niveau vers la version 13.1 du logiciel, vous devez installer le client Thales Luna version 10.3.0 et suivre les étapes suivantes.

1. Remplacez le répertoire par /var/safenet et installez le client Thales Luna. À l'invite shell, tapez :

```
cd /var/safenet
<!--NeedCopy-->
```

Pour installer le client Thales Luna version 6.0.0, tapez :

```
install_client.sh -v 600
<!--NeedCopy-->
```

Pour installer le client Thales Luna version 6.2.2, tapez :

```
install_client.sh -v 622
<!--NeedCopy-->
```

Pour installer le client Thales Luna version 7.2.2, tapez :

```
install_client.sh -v 722
<!--NeedCopy-->
```

Pour installer le client Thales Luna version 10.3.0, tapez :

```
install_client.sh -v 1030
<!--NeedCopy-->
```

2. Configurez les NTL entre le client Thales Luna (ADC) et HSM.

Une fois le répertoire '/var/safenet/' créé, effectuez les tâches suivantes sur ADC.

a) Changez le répertoire en « /var/safenet/config/ » et exécutez le script « safenet_config ». À l'invite shell, tapez :

```
cd /var/safenet/config

sh safenet_config
<!--NeedCopy-->
```

Ce script copie le fichier « Chrystoki.conf » dans le répertoire /etc/. Il génère également un lien symbolique 'LibCryptoki2_64.so' dans le répertoire '/usr/lib/'.

b) Créer et transférer un certificat et une clé entre l'ADC et le HSM Thales Luna.

Pour communiquer en toute sécurité, l'ADC et le HSM doivent échanger des certificats. Créez un certificat et une clé sur l'ADC, puis transférez-les vers le HSM. Copiez le certificat HSM dans l'ADC.

i) Changez de répertoire en /var/safenet/safenet/lunaclient/bin.

ii) Créez un certificat sur l'ADC. À l'invite shell, tapez :

```
./vtl createCert -n <ip address of NetScaler>
<!--NeedCopy-->
```

Cette commande ajoute également le certificat et le chemin de clé au fichier « /etc/Chrystoki.conf ».

iii) Copiez ce certificat sur le HSM. À l'invite shell, tapez :

```
scp /var/safenet/safenet/lunaclient/cert/client/<ip address of NS
   >.pem <LunaSA_HSM account>@<IP address of Luna SA>
<!--NeedCopy-->
```

iv) Copiez le certificat HSM sur NetScaler. À l'invite shell, tapez :

```
scp <HSM account>@<HSM IP>:server.pem  /var/safenet/safenet/
   lunaclient/server_<HSM ip>.pem
<!--NeedCopy-->
```

3. Enregistrez le NetScaler en tant que client et attribuez-lui une partition sur le Thales Luna HSM.

   Connectez-vous au HSM et créez un client. Entrez le NSIP comme adresse IP du client. Cette adresse doit être l'adresse IP de l'ADC à partir duquel vous avez transféré le certificat vers le HSM. Une fois le client enregistré avec succès, attribuez-lui une partition. Exécutez les commandes suivantes sur le HSM.

   a) Utilisez SSH pour vous connecter au HSM Thales Luna et entrez le mot de passe.

   b) Enregistrez le NetScaler sur le HSM Thales Luna. Le client est créé sur le HSM. L'adresse IP est l'adresse IP du client. C'est-à-dire l'adresse NSIP.

   À l'invite, tapez :

   ```
   client register  -client <client name> -ip <NetScaler ip>
   <!--NeedCopy-->
   ```

   c) Attribuez au client une partition à partir de la liste des partitions. Pour afficher les partitions disponibles, tapez :

   ```
   <luna_sh> partition list
   <!--NeedCopy-->
   ```


Attribuez une partition à partir de cette liste. Type :

```
<lunash:> client assignPartition -client <Client Name> -par <
   Partition Name>
<!--NeedCopy-->
```

4. Enregistrez le HSM avec son certificat sur NetScaler.

   Sur l'ADC, remplacez le répertoire par « /var/safenet/safenet/lunaclient/bin » et, à l'invite du shell, tapez :

```
./vtl addserver -n <IP addr of HSM> -c /var/safenet/safenet/
   lunaclient/server_<HSM_IP>.pem
<!--NeedCopy-->
```

   Pour supprimer le HSM inscrit sur l'ADC, tapez :

```
./vtl deleteServer -n <HSM IP> -c <cert path>
<!--NeedCopy-->
```

   Pour répertorier les serveurs HSM configurés sur l'ADC, tapez :

```
./vtl listServer
<!--NeedCopy-->
```

   > **Remarque :**
   >
   > Avant de supprimer le HSM à l'aide de `vtl`, assurez-vous que toutes les clés de ce HSM sont supprimées manuellement de l'appliance. Les clés HSM ne peuvent pas être supprimées après la suppression du serveur HSM.

5. Vérifiez la connectivité des liens d'approbation réseau (NLT) entre l'ADC et le HSM. À l'invite shell, tapez :

```
./vtl verify
<!--NeedCopy-->
```

   Si la vérification échoue, passez en revue toutes les étapes. Les erreurs sont dues à une adresse IP incorrecte dans les certificats clients.

6. Enregistrez la configuration.

   Les étapes précédentes mettent à jour le fichier de configuration « /etc/Chrystoki.conf ». Ce fichier est supprimé au démarrage de l'ADC. Copiez la configuration dans le fichier de configuration par défaut, qui est utilisé lors du redémarrage d'un ADC.

   À l'invite shell, tapez :


```
root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

La pratique recommandée consiste à exécuter cette commande chaque fois qu'il y a une modification de la configuration associée à Thales Luna.

7. Démarrez le processus de passerelle Thales Luna.

   À l'invite shell, tapez :

```
sh /var/safenet/gateway/start_safenet_gw
<!--NeedCopy-->
```

8. Configurez le démarrage automatique du démon de Gateway au démarrage.

   Créez le fichier « safenet_is_enrolled », qui indique que Thales Luna HSM est configuré sur cet ADC. Chaque fois que ADC redémarre et que ce fichier est trouvé, la Gateway est automatiquement démarrée.

   À l'invite shell, tapez :

```
touch /var/safenet/safenet_is_enrolled
<!--NeedCopy-->
```

9. Redémarrez l'appliance NetScaler. À l'invite de commande, tapez :

```
reboot
<!--NeedCopy-->
```

Configurer les HSM Thales Luna dans une configuration haute disponibilité sur ADC

May 5, 2023

La configuration des HSM Thales Luna en haute disponibilité (HA) garantit un service ininterrompu même si tous les appareils, sauf un, ne sont pas disponibles. Dans une configuration HA, chaque HSM rejoint un groupe HA en mode actif. Les HSM Thales Luna dans une configuration HA fournissent un équilibrage de charge de tous les membres du groupe afin d'augmenter les performances et le temps de réponse tout en garantissant un service haute disponibilité. Pour plus d'informations, contactez le service commercial et le support de Thales Luna.

Pré-requis :

- Au moins deux appareils Thales Luna HSM. Tous les périphériques d'un groupe HA doivent avoir une authentification PED (chemin d'accès approuvé) ou une authentification par mot de passe. Une combinaison d'authentification par chemin sécurisé et d'authentification par mot de passe dans un groupe HA n'est pas prise en charge.
- Les partitions de chaque périphérique HSM doivent avoir le même mot de passe même si l'étiquette (nom) est différente.
- Toutes les partitions de HA doivent être attribuées au client (appliance NetScaler).

Après avoir configuré un client Thales Luna sur ADC, comme décrit dans Configurer un client Thales Luna sur ADC, effectuez les étapes suivantes pour configurer les HSM Thales Luna dans HA :

1. Sur l'invite du shell NetScaler, lancez `lunacm` (/usr/safenet/lunaclient/bin)

   Exemple :

   ```
   root@ns# cd /var/safenet/safenet/lunaclient/bin/

   root@ns# ./lunacm
   <!--NeedCopy-->
   ```

2. Identifiez les ID d'emplacement des partitions. Pour répertorier les emplacements (partitions) disponibles, tapez :

   ```
   lunacm:> slot list
   <!--NeedCopy-->
   ```

   Exemple :

   ```
       Slot Id ->              0
       HSM Label ->            trinity-p1
       HSM Serial Number ->    481681014
       HSM Model ->            LunaSA 6.2.1
       HSM Firmware Version -> 6.10.9
       HSM Configuration ->    Luna SA Slot (PED) Signing With
           Cloning Mode
       HSM Status ->           OK

       Slot Id ->              1
       HSM Label ->            trinity-p2
       HSM Serial Number ->    481681018
       HSM Model ->            LunaSA 6.2.1
       HSM Firmware Version -> 6.10.9
       HSM Configuration ->    Luna SA Slot (PED) Signing With
           Cloning Mode
       HSM Status ->           OK

   ```



```
17       Slot Id ->              2
18       HSM Label ->            neo-p1
19       HSM Serial Number ->    487298014
20       HSM Model ->            LunaSA 6.2.1
21       HSM Firmware Version -> 6.10.9
22       HSM Configuration ->    Luna SA Slot (PED) Signing With
             Cloning Mode
23      HSM Status ->           OK
24
25      Slot Id ->              3
26      HSM Label ->            neo-p2
27      HSM Serial Number ->    487298018
28      HSM Model ->            LunaSA 6.2.1
29      HSM Firmware Version -> 6.10.9
30      HSM Configuration ->    Luna SA Slot (PED) Signing With
            Cloning Mode
31      HSM Status ->           OK
32
33      Slot Id ->              7
34      HSM Label ->            hsmha
35      HSM Serial Number ->    1481681014
36      HSM Model ->            LunaVirtual
37      HSM Firmware Version -> 6.10.9
38      HSM Configuration ->    Luna Virtual HSM (PED) Signing With
            Cloning Mode
39      HSM Status ->           N/A - HA Group
40
41      Slot Id ->              8
42      HSM Label ->            newha
43      HSM Serial Number ->    1481681018
44      HSM Model ->            LunaVirtual
45      HSM Firmware Version -> 6.10.9
46      HSM Configuration ->    Luna Virtual HSM (PED) Signing With
            Cloning Mode
47      HSM Status ->           N/A - HA Group
48
49      Current Slot Id: 0
50  <!--NeedCopy-->
```

3. Créez le groupe HA. La première partition est appelée partition principale. Vous pouvez ajouter plusieurs partitions secondaires.

```
1  lunacm:> hagroup createGroup -slot <slot number of primary
       partition> -label <group name> -password <partition password >
2
```



```
lunacm:> hagroup createGroup -slot 1 -label gp12 -password ******
<!--NeedCopy-->
```

4. Ajoutez les membres secondaires (partitions HSM). Répétez cette étape pour toutes les partitions à ajouter au groupe HA.

```
lunacm:> hagroup addMember -slot <slot number of secondary
    partition to be added> -group <group name> -password <partition
     password>
<!--NeedCopy-->
```

Code :

```
lunacm:> hagroup addMember -slot 2 -group gp12 -password ******
<!--NeedCopy-->
```

5. Activez le mode HA uniquement.

```
lunacm:> hagroup HAOnly  - enable
<!--NeedCopy-->
```

6. Activez le mode de restauration actif.

```
lunacm:.>hagroup recoveryMode  - mode active
<!--NeedCopy-->
```

7. Définissez l'intervalle de restauration automatique (en secondes). Le délai par défaut est de 60 secondes.

```
lunacm:.>hagroup interval  - interval <value in seconds>
<!--NeedCopy-->
```

Exemple :

```
lunacm:.>hagroup interval  - interval 120
<!--NeedCopy-->
```

8. Définissez le nombre de tentatives de restauration. Une valeur de -1 permet un nombre infini de tentatives.

```
lunacm:> hagroup retry -count <xxx>
<!--NeedCopy-->
```

Exemple :


```
lunacm:> hagroup retry -count 2
<!--NeedCopy-->
```

9. Copiez la configuration depuis le répertoire `Chrystoki.conf` de configuration SafeNet.

```
cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

10. Redémarrez l'appliance ADC.

```
reboot
<!--NeedCopy-->
```

Après avoir configuré Thales Luna HSM dans HA, reportez-vous à la section Autre configuration ADC pour plus de configuration sur ADC.

Autres configurations ADC

August 20, 2021

1. Générez une clé sur le HSM.

   Utilisez des outils tiers pour créer des clés sur le HSM.

2. Ajoutez une clé HSM sur ADC.

   Important Le caractère # n'est pas pris en charge dans un nom de clé. Si le nom de clé inclut ce caractère, l'opération de clé de chargement échoue.

   Pour ajouter une clé HSM Thales Luna à l'aide de l'interface de ligne de commande :

   À l'invite de commandes, tapez :

```
add ssl hsmkey <KeyName> -hsmType SAFENET -serialNum <serial #> -
   password
<!--NeedCopy-->
```

   où :

   -keyName est la clé créée sur le HSM à l'aide d'outils tiers.

   -SerialNum est le numéro de série de la partition sur le HSM sur lequel les clés sont générées.

   Remarque : Pour HSM dans une configuration haute disponibilité, utilisez le numéro de série du groupe haute disponibilité.

-password est le mot de passe de la partition sur laquelle les clés sont présentes.

Pour ajouter une clé HSM Thales Luna à l'aide de l'interface graphique :

Accédez à **Gestion du trafic** > **SSL** > **HSM** et ajoutez une clé HSM. Vous devez spécifier le type HSM comme **SAFENET**.

3. Ajoutez une paire de clés de certificat sur ADC. Utilisez d'abord un outil tiers pour générer un certificat associé à la clé. Ensuite, copiez le certificat dans le répertoire /nsconfig/ssl/ de ADC.

   Remarque : La clé doit être une clé HSM.

   Pour ajouter une paire certkey sur ADC à l'aide de l'interface de ligne de commande :

   À l'invite de commandes, tapez :

   ```
   add ssl certkey <CertkeyName> -cert <cert name> -hsmkey <KeyName>
   <!--NeedCopy-->
   ```

   Pour ajouter une paire certkey sur ADC à l'aide de l'interface graphique :

   a) Accédez à **Gestion du trafic** > **SSL**.
   b) Dans **Mise en route**, sélectionnez **Installer le certificat (HSM)**et créez une paire de clés de certificat à l'aide d'une clé HSM.

4. Créez un serveur virtuel et liez la paire de clés de certificat à ce serveur virtuel.

Pour plus d'informations sur la création d'un serveur virtuel, cliquez sur Configuration du serveur virtuel SSL.

Pour plus d'informations sur l'ajout d'une paire de clés de certificat, cliquez sur Ajouter ou mettre à jour une paire de clés de certificat.

Pour plus d'informations sur la liaison d'une paire de clés de certificat à un serveur virtuel SSL, cliquez sur Lier la paire de clés de certificat au serveur virtuel SSL.

Appliances NetScaler dans une configuration à haute disponibilité

May 5, 2023

Vous pouvez configurer une configuration haute disponibilité (HA) sur les appliances NetScaler avec une configuration Thales Luna HSM de l'une des deux manières suivantes :

- Tout d'abord, configurez un HSM Thales Luna sur les deux nœuds, en utilisant le même HSM et la même partition. Ensuite, créez une paire HA. Enfin, ajoutez la configuration NetScaler, telle que les clés, les paires de clés de certificat et les serveurs virtuels, sur le nœud principal.

- Si un HSM Thales Luna est déjà configuré sur un nœud avec la configuration NetScaler, ajoutez une configuration similaire sur l'autre nœud. Copiez « /var/safenet/sfgw_ident_file » du premier nœud vers l'autre et redémarrez le binaire safenet_gw. Une fois la passerelle opérationnelle, ajoutez les nœuds dans une configuration HA.

Limitations

May 5, 2023

1. Pour toute modification de la configuration liée au HSM dans une configuration existante, telle que l'ajout ou la suppression d'un HSM, ou la création d'une configuration HA, copiez « /etc/Chrystoki.conf » dans « /var/safenet/config'.
2. Après avoir ajouté, supprimé ou redémarré un HSM, vous devez redémarrer le binaire « /var/safenet/gateway/safenet_gw ». Si vous ne redémarrez pas le binaire de la passerelle, le HSM ne servira aucun trafic après son ajout ou après son redémarrage.
3. Pour redémarrer ou arrêter le binaire « /var/safenet/gateway/safenet_gw » actuel, utilisez

   ```
   kill  - SIGTERM <PID>
   kill  - SIGINT <PID>
   <!--NeedCopy-->
   ```

   C'est important ! Ne pas utiliser `kill -9 <PID>` ou `kill -6 <PID>`
4. Avant de supprimer un HSM existant de ADC, supprimez de ADC, toutes les clés et paires de clés de certificat associées à ce HSM. Vous ne pouvez pas supprimer ces fichiers de l'ADC après avoir supprimé le HSM.
5. Sur une appliance NetScaler autonome, les HSM Thales Luna en HA sont pris en charge pour Luna version 6.2 et versions ultérieures.
6. Les chiffrements EXPORT ne sont pas pris en charge.
7. L'opération de mise à jour des paires de clés de certificat n'est pas prise en charge.
8. Lorsque vous générez une clé HSM sur un outil tiers, les noms des clés privée et publique doivent être identiques. Lorsque vous ajoutez la clé HSM sur la solution matérielle-logicielle, indiquez ce nom comme nom de clé.
9. Le ## caractère n'est pas pris en charge dans un nom de clé et un mot de passe de partition.
10. Les partitions de cluster et d'administration ne sont pas prises en charge.

Annexe

May 5, 2023

Exemples de commandes avec leurs sorties :

Exécuter le script

```
1      root@ns# pwd
2     /var/safenet/config
3     root@ns# sh safenet_config
4 <!--NeedCopy-->
```

Créer un certificat

```
1     root@ns# cd /var/safenet/safenet/lunaclient/bin
2     root@ns# ./vtl createcert -n 10.102.59.175
3     Private Key created and written to: /var/safenet/safenet/lunaclient
         /cert/client/10.102.59.175Key.pem
4     Certificate created and written to: /var/safenet/safenet/lunaclient
         /cert/client/10.102.59.175.pem
5 <!--NeedCopy-->
```

Copiez le certificat sur le HSM

```
1     root@ns# scp /var/safenet/safenet/lunaclient/cert/client
         /10.102.59.175.pem admin@10.217.2.7:
2     admin@10.217.2.7's password:
3
4     10.102.59.175.pem          100%  818     0.8KB/s   00:00
5 <!--NeedCopy-->
```

Copiez le certificat et la clé du HSM vers l'appliance NetScaler

```
1     root@ns# scp admin@10.217.2.7:server.pem /var/Thales Luna/safenet/
         lunaclient/server.2.7.pem
2     admin@10.217.2.7's password:
3
4     server.pem            100% 1164     1.1KB/s   00:01
5 <!--NeedCopy-->
```


Utiliser SSH pour se connecter au Thales Luna HSM

```
    ssh admin@10.217.2.7
    Connecting to 10.217.2.7:22...
    Connection established.
    To escape to local shell, press 'Ctrl+Alt+]'.

    Last login: Thu Jun 23 02:20:29 2016 from 10.252.243.11

    Luna SA 5.2.3-1 Command Line Shell - Copyright (c) 2001-2014
       SafeNet, Inc. All rights reserved.

    [Safenet1] lunash:>hsm login


      Please enter the HSM Administrators' password:
      > *******

    'hsm login' successful.


    Command Result : 0 (Success)
    [Safenet1] lunash:>
<!--NeedCopy-->
```

Enregistrez le NetScaler sur le HSM Thales Luna

```
    [Safenet1] lunash:>client register -client ns175 -ip 10.102.59.175

    'client register' successful.


    Command Result : 0 (Success)
    [Safenet1] lunash:>
<!--NeedCopy-->
```

Attribuer au client une partition à partir de la liste des partitions

```
    [Safenet1] lunash:>client assignPartition -client ns175 -partition
       p2

    'client assignPartition' successful.
```



```
4
5
6       Command Result : 0 (Success)
7       [Safenet1] lunash:>
8   <!--NeedCopy-->
```

Enregistrez le HSM avec son certificat sur NetScaler

```
1       root@ns# ./vtl addserver -n 10.217.2.7 -c /var/safenet/safenet/
            lunaclient/server.2.7.pem
2
3       New server 10.217.2.7 successfully added to server list.
4   <!--NeedCopy-->
```

Vérifiez la connectivité des liens de confiance réseau (NTL) entre l'ADC et le HSM

```
1       root@ns# ./vtl verify
2
3       The following Luna SA Slots/Partitions were found:
4
5       Slot        Serial #                  Label
6       ====      ================          =====
7          0              477877010          p2
8   <!--NeedCopy-->
```

Enregistrez la configuration

```
1       root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
2   <!--NeedCopy-->
```

Configurer le démarrage automatique du démon de Gateway au démarrage

```
1       touch /var/safenet/safenet_is_enrolled
2   <!--NeedCopy-->
```


Questions fréquentes

May 5, 2023

- **Comment puis-je vérifier que le processus Thales Luna est en cours d'exécution ?**

  À l'invite du shell NetScaler, tapez :

```
ps - aux | grep safenet_gw
<!--NeedCopy-->
```

- **Comment vérifier la connectivité des liens d'approbation réseau (NTL) entre ADC et le HSM ?**

  Après avoir configuré Thales Luna, remplacez le répertoire par « /var/safenet/safenet/lunaclient/bin » et tapez :

```
./vtl verify
<!--NeedCopy-->
```

Prise en charge de Azure Key Vault

May 5, 2023

L'appliance NetScaler s'intègre aux HSM externes (SafeNet et Thales) pour les déploiements sur site. Pour les déploiements cloud, l'appliance ADC s'intègre à Azure Key Vault. L'appliance stocke ses clés privées dans le coffre de clés pour faciliter la gestion et la sécurité de la clé privée dans le domaine du cloud public. Vous n'avez plus besoin de stocker et de gérer les clés à différents emplacements pour les appliances ADC déployées dans plusieurs centres de données et fournisseurs de cloud.

L'utilisation d'ADC avec le niveau de tarification Azure Key Vault Premium, qui fournit des clés soutenues par HSM, garantit la conformité FIPS 140-2 niveau 2.

Azure Key Vault est une offre standard de Microsoft. Pour plus d'informations sur Azure Key Vault, consultez la documentation Microsoft Azure.

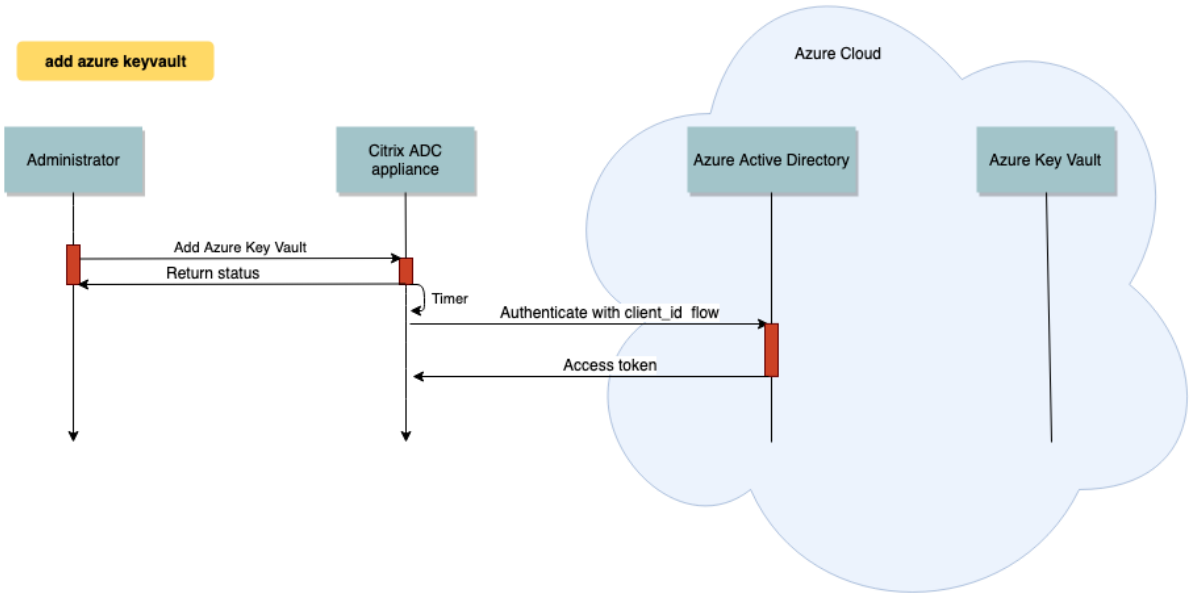
> **Remarque :**
>
> L'intégration de NetScaler à Azure Key Vault est prise en charge par le protocole TLS 1.3.

Aperçu de l'architecture

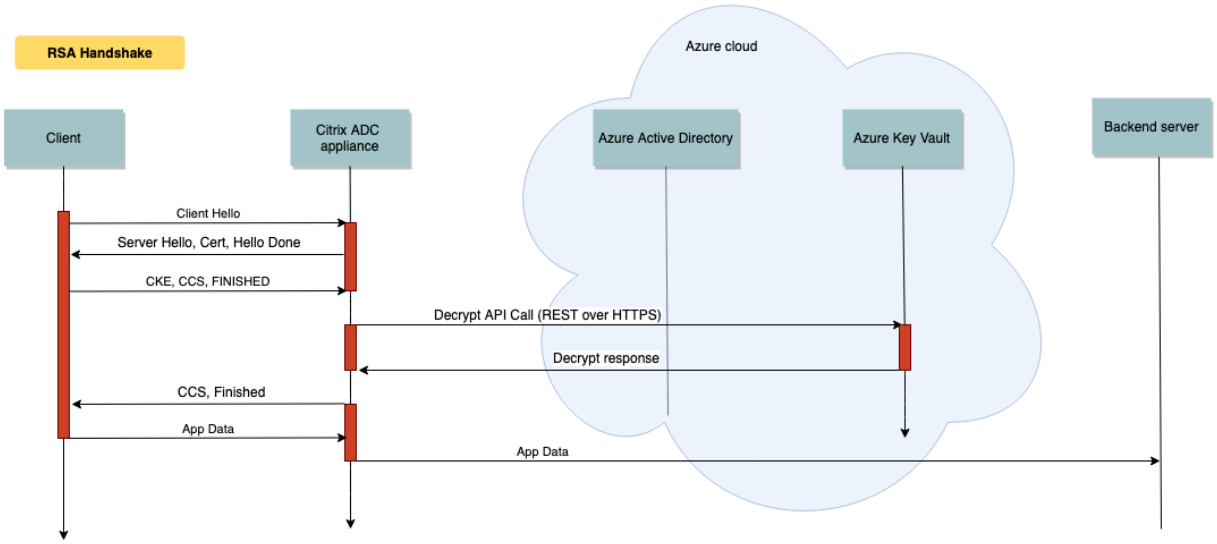
Azure Key Vault est un service permettant de stocker des secrets en toute sécurité dans le cloud Azure. En stockant vos clés dans Azure Key Vault, vous réduisez les risques de vol de clés. Une fois le coffre-

fort de clés configuré, vous pouvez y stocker vos clés. Configurez des serveurs virtuels sur l'appliance ADC pour effectuer des opérations de clé privée dans le coffre de clés. L'appliance ADC accède à la clé pour chaque prise de contact SSL.

Le schéma suivant illustre le processus pour obtenir un jeton d'accès auprès d'Azure Active Directory après authentification. Ce jeton est utilisé avec les appels d'API REST pour les opérations de chiffrement utilisant des clés privées.



Le schéma suivant montre une poignée de main RSA typique. Le message d'échange de clés client (CKE) chiffré à l'aide de la clé publique est déchiffré à l'aide de la clé privée stockée dans le coffre de clés.



Lors d'une liaison ECDHE, le message d'échange de clés de serveur (SKE) envoyé par l'appliance NetScaler est signé à l'aide de la clé privée stockée dans le Key Vault.

Composants requis

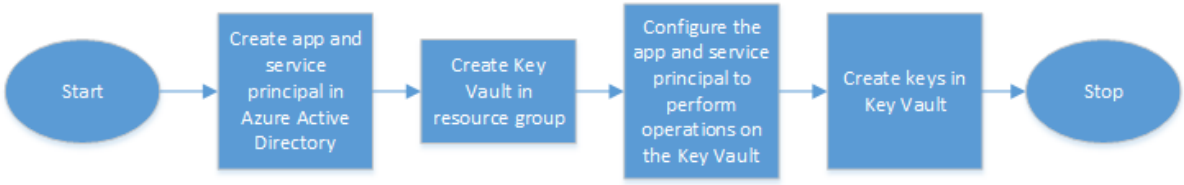
1. Vous devez disposer d'un abonnement Azure.
2. (Facultatif) Installez Azure CLI sur une machine Linux. Pour obtenir des instructions, consultez la documentation Azure https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-apt?view=azure-cli-latest.
3. Terminez la configuration sur le portail Azure avant de configurer les entités sur l'appliance ADC.

Configurer l'intégration d'ADC Azure Key Vault

Effectuez d'abord la configuration sur le portail Azure, puis la configuration sur l'appliance ADC.

Effectuez les étapes suivantes sur le portail Azure

L'organigramme suivant montre le flux de haut niveau pour la configuration requise sur le portail Azure.

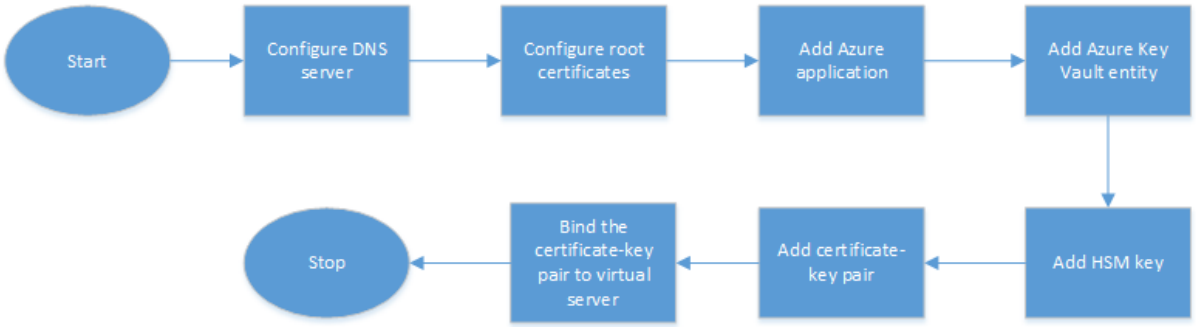


1. Créez le principal d'application et de service dans Azure Active Directory.
2. Créez Key Vault dans un groupe de ressources.
3. Configurez l'application et le principal de service pour effectuer des opérations de signature et de déchiffrement sur le coffre de clés.
4. Créez des clés dans le coffre de clés de l'une des manières suivantes :
    a) En important un fichier clé.
    b) En générant un certificat.

Pour plus d'informations sur les commandes permettant de configurer les étapes précédentes, consultez la documentation Azure à l'adresse https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals.

Effectuez les étapes suivantes sur l'appliance ADC

L'organigramme suivant montre le flux de haut niveau pour la configuration requise sur l'appliance ADC.



1. Configurez un serveur DNS.
2. Configurez les certificats racine pour vérifier les certificats présentés par Azure.
3. Créez une application Azure.
4. Créez une entité Azure Key Vault.
5. Créez une clé HSM.
6. Créez une paire de clés de certificat.
7. Liez la paire de clés de certificat à un serveur virtuel.

Configurer un serveur DNS

Un serveur DNS est requis pour la résolution de nom de l'hôte Key Vault et du point de terminaison Azure Active Directory.

Pour configurer un serveur DNS à l'aide de la CLI

À l'invite de commande, tapez :

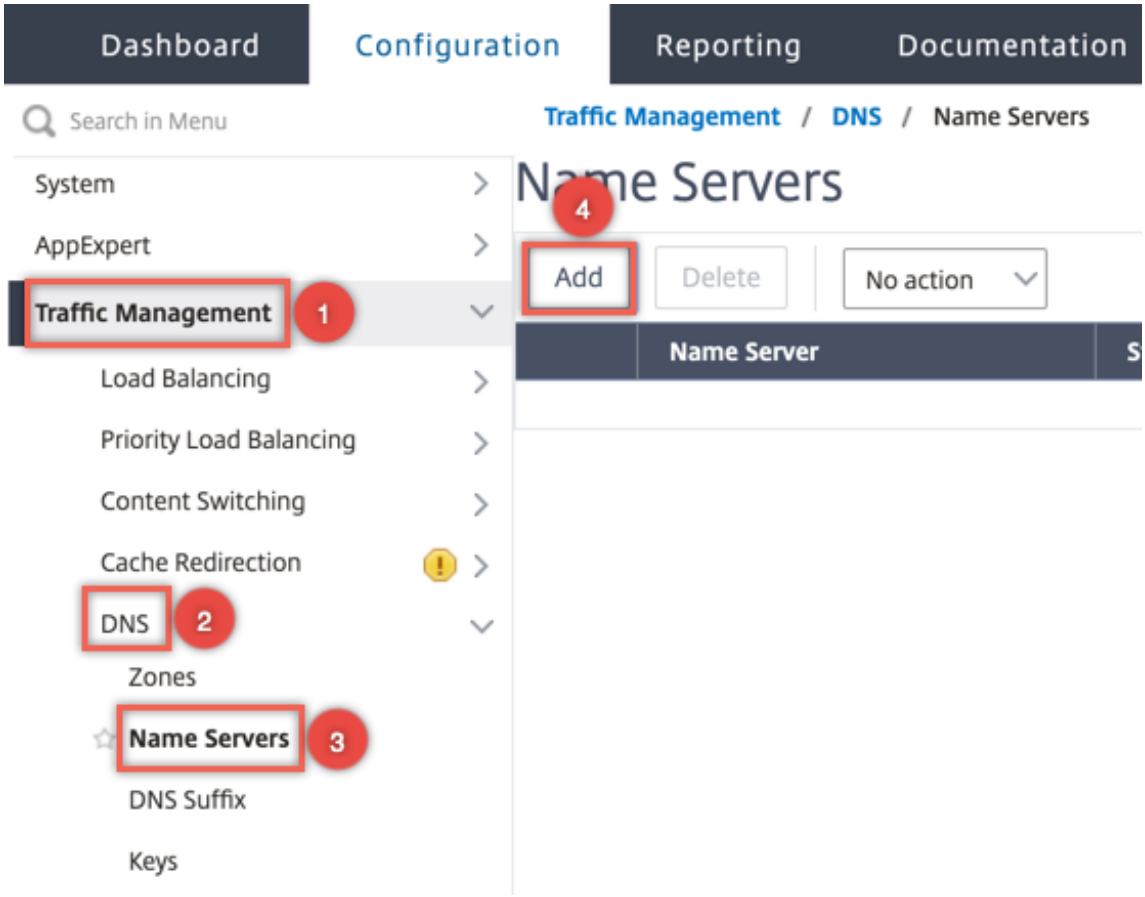

```
add dns nameserver <IP address>
<!--NeedCopy-->
```

Exemple :

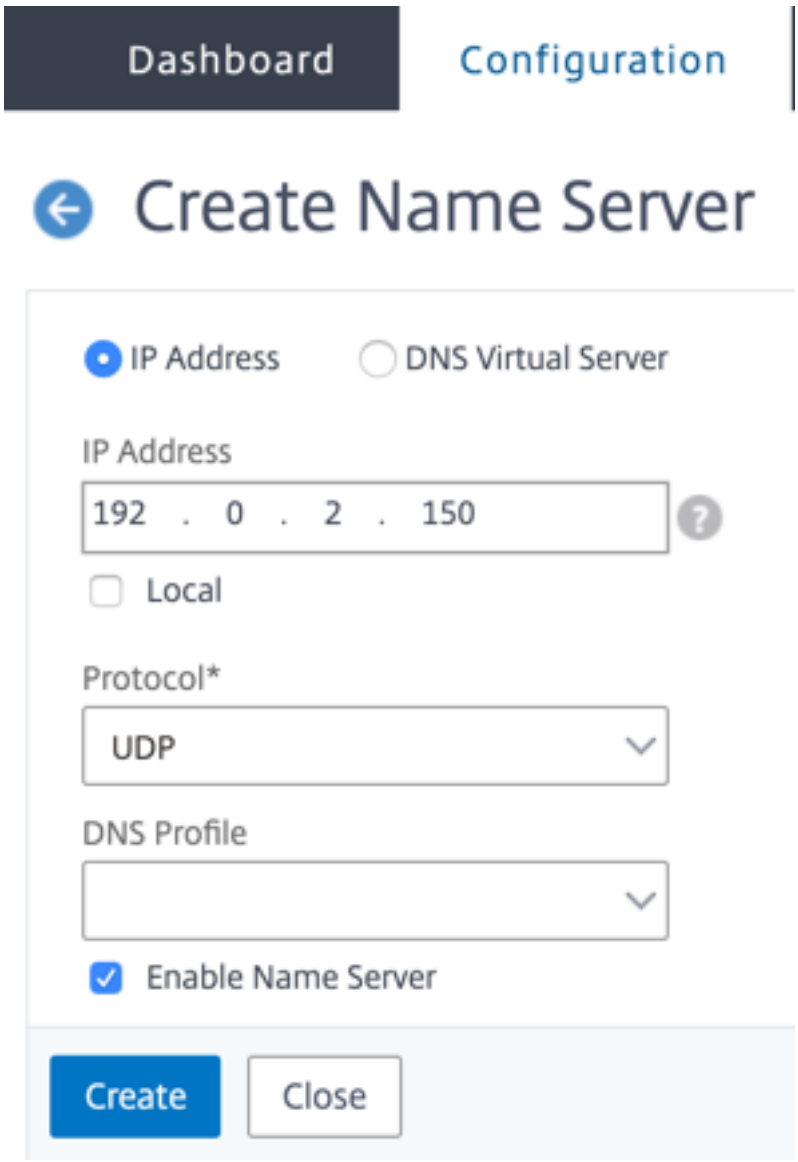
```
add dns nameserver 192.0.2.150
<!--NeedCopy-->
```

Pour configurer un serveur DNS à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > DNS > Serveurs de noms**. Cliquez sur **Ajouter**.



2. Entrez des valeurs pour les paramètres suivants :
   - Adresse IP : adresse IP d'un serveur de noms externe ou, si le paramètre Local est défini, adresse IP d'un serveur DNS local (LDNS).
   - Protocol : protocole utilisé par le serveur de noms. UDP_TCP n'est pas valide si le serveur de noms est un serveur virtuel DNS configuré sur l'appliance.



3. Cliquez sur **Create**.

Ajouter et lier un certificat racine

Téléchargez les certificats racine du certificat présenté par Azure Key Vault `https://<vault_name>.vault.azure.net` et Azure Active Directory (AAD) https://login.microsoftonline.com et chargez-le sur l'appliance ADC. Ces certificats sont nécessaires pour valider le certificat présenté par Azure Key Vault et AAD. Liez un ou plusieurs certificats au groupe de certificats de l'autorité de certification `ns_callout_certs`.

Pour ajouter un certificat racine à l'aide de la CLI

À l'invite de commande, tapez :


```
add ssl certkey <certkeyname> -cert <certname>
bind ssl caCertGroup <caCertGroupName> <certkeyName>
<!--NeedCopy-->
```

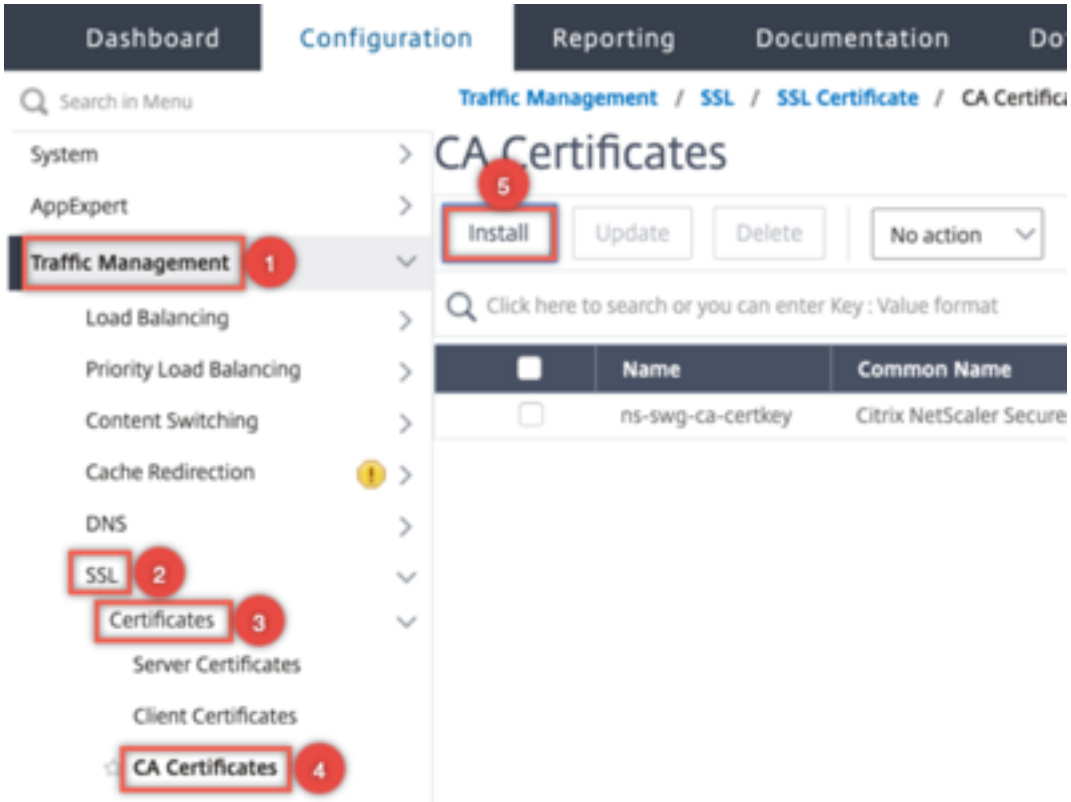
Exemple :

Dans l'exemple suivant, le certificat racine présenté par Azure Key Vault et AAD est identique.

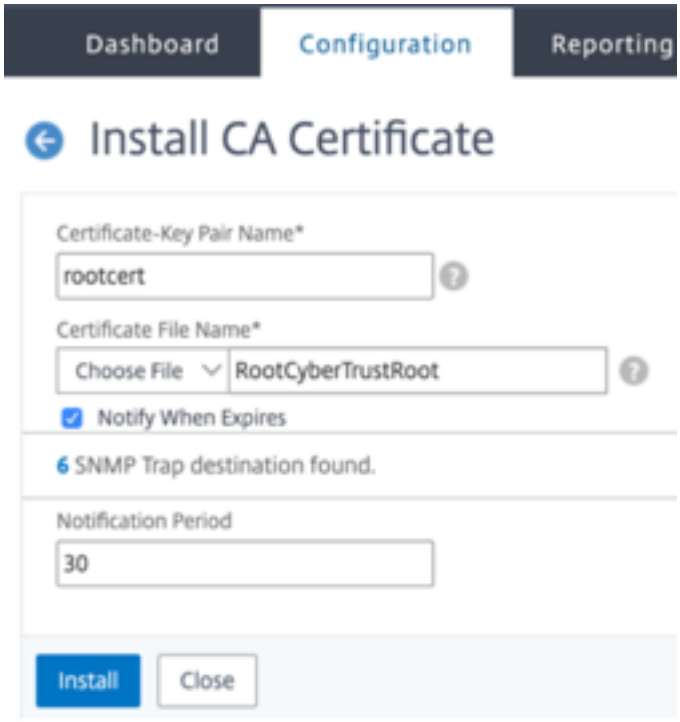
```
add ssl certKey rootcert -cert RootCyberTrustRoot.crt
bind ssl cacertGroup ns_callout_certs  rootcert
<!--NeedCopy-->
```

Pour ajouter un certificat racine à l'aide de l'interface graphique

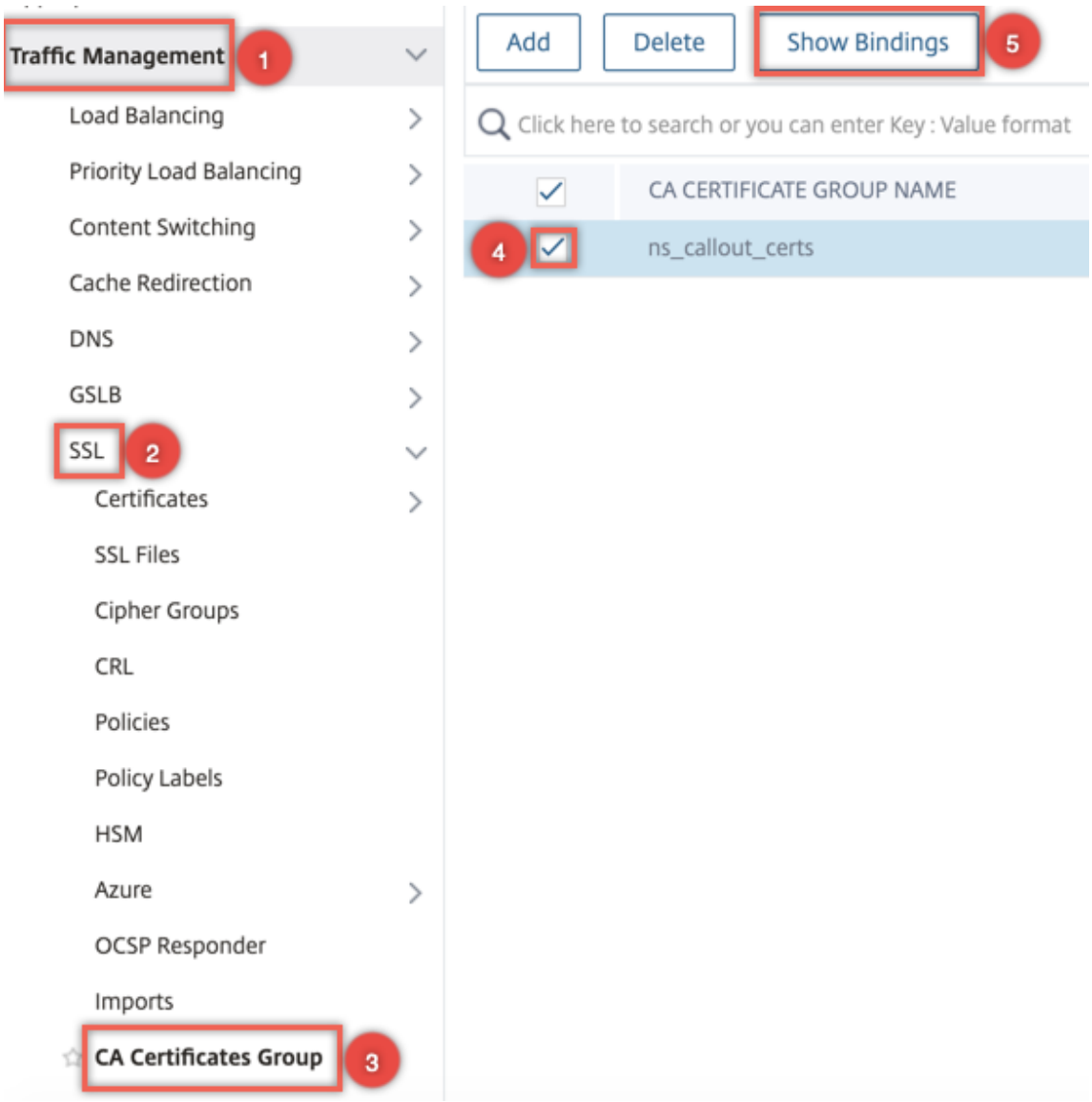
1. Accédez à **Gestion du trafic > SSL > Certificats > Certificats CA**.



2. Entrez des valeurs pour les paramètres suivants :
   - Nom de la paire de clés de certificat
   - Nom du fichier de certificat



3. Cliquez sur **Installer**.
4. Accédez à **Gestion du trafic > SSL > Groupe de certificats d'autorité**de certification.
5. Sélectionnez **ns_callout_certs** et cliquez sur **Afficher les liaisons**.



6. Cliquez sur **Bind**.
7. Sélectionnez le certificat d'autorité de certification créé précédemment et cliquez sur **Sélectionner**.
8. Cliquez sur **Lier**, puis sur **Fermer**.

Configurer une application Azure

L'entité d'application Azure contient les informations d'identification requises pour s'authentifier auprès d'Azure Active Directory et obtenir le jeton d'accès. En d'autres mots, pour obtenir l'autorisation d'accès aux ressources et aux API Key Vault, ajoutez l'ID d'application Azure, le secret (mot de passe) et l'ID de locataire sur l'appliance ADC.
Lorsque vous configurez l'entité Application Azure à l'aide de l'interface de ligne de commande,

vous devez entrer le mot de passe Si vous utilisez l'interface graphique, l'entité d'application Azure contient les informations d'identification requises pour s'authentifier auprès d'Azure Active Directory et obtenir le jeton d'accès.

Pour configurer une application Azure à l'aide de la CLI

À partir de la version 13.0-61.x, un paramètre, VaultResource, est ajouté à la commande `add azure application` pour obtenir le domaine du groupe de ressources avant que le jeton d'accès ne soit accordé à l'application. Ce paramètre est ajouté car le nom de domaine peut être différent selon les régions. Par exemple, le domaine peut être `vault.azure.net` ou `vault.usgov.net`.

À l'invite de commande, tapez :

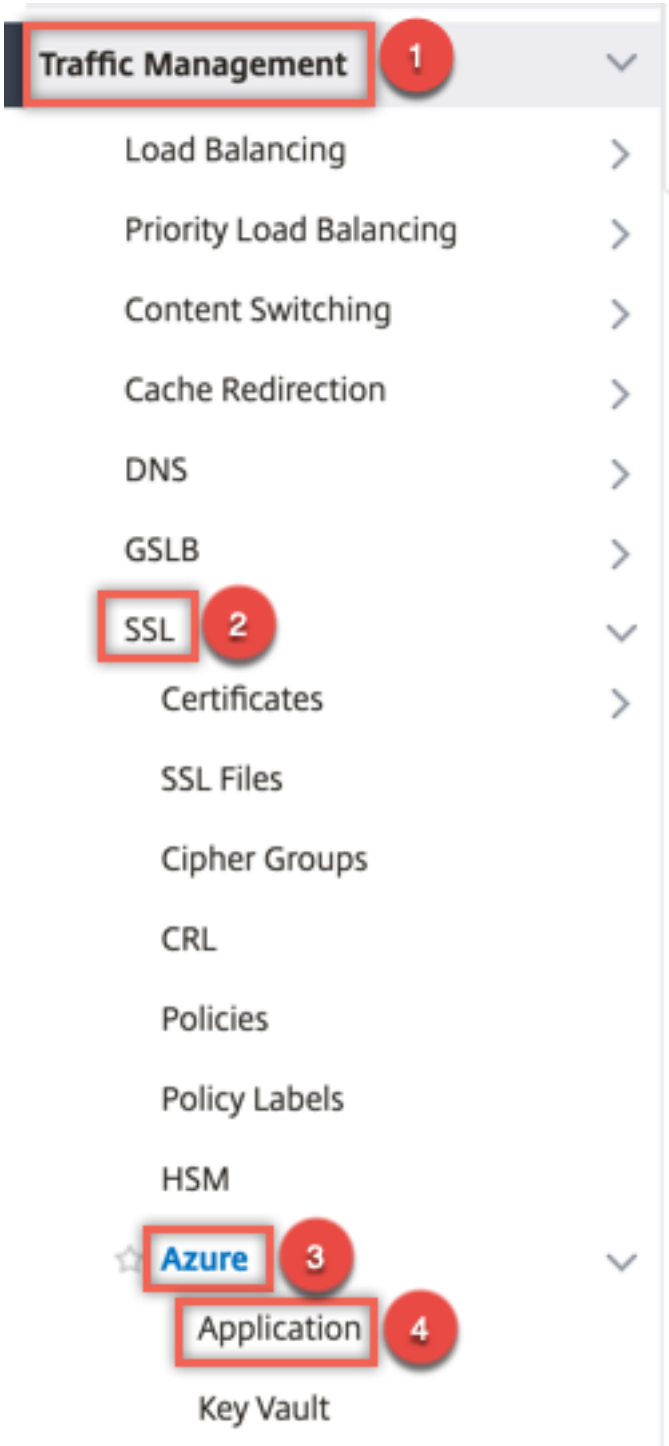
```
add azure application <name> -clientID <string> -clientSecret -tenantID
    <string> -vaultResource <string> [-tokenEndpoint <URL>]
show azure application
<!--NeedCopy-->
```

Exemple :

```
add azure application app10 -clientiD 12345t23aaa5 -clientsecret
   csHzOoEzmuY= -vaultResource example.vault.azure.net -tenantID 33583
   ee9ca5b
 Done
> sh azure application app10
1)  Name:  app10            ClientID:  12345t23aaa5
    TokenEndpoint:  "https://login.microsoftonline.com/33583ee9ca5b/"
    TenantID:  33583ee9ca5b  VaultResource:  example.vault.azure.net
 Done

<!--NeedCopy-->
```

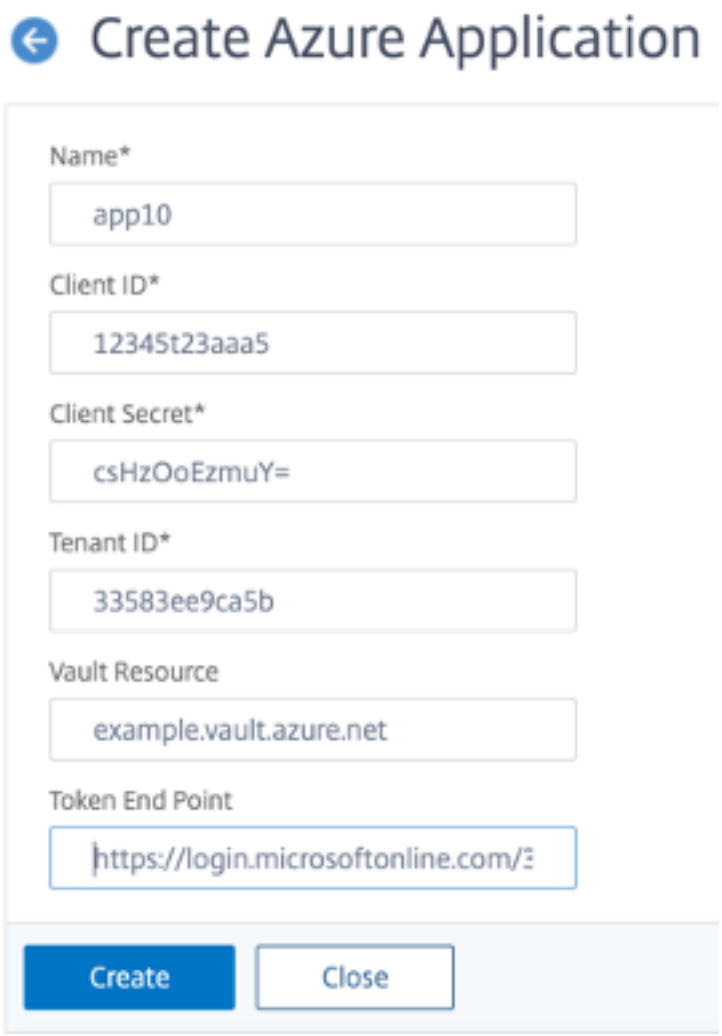
Pour configurer une application Azure à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Azure > Application**.



2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Entrez des valeurs pour les paramètres suivants :
   - Nom : nom de l'objet d'application sur l'appliance NetScaler.
   - ID client : ID d'application généré lorsqu'une application est créée dans Azure Active Directory à l'aide de l'interface de ligne de commande Azure ou du portail Azure (GUI).

- Secret client : mot de passe de l'application configurée dans Azure Active Directory. Le mot de passe est spécifié dans l'interface de ligne de commande Azure ou généré dans le portail Azure (GUI).
- ID du locataire : ID du répertoire dans Azure Active Directory dans lequel l'application a été créée.
- Vault Resource : ressource Vault pour laquelle un jeton d'accès est accordé. Exemple `vault.azure.net`.
- Point final du jeton : URL à partir de laquelle le jeton d'accès peut être obtenu. Si le point final du jeton n'est pas spécifié, la valeur par défaut est `https://login.microsoftonline.com/<tenant id>`.



Configurer Azure Key Vault

Créez un objet Azure Key Vault sur l'appliance ADC.

Pour configurer Azure Key Vault à l'aide de la CLI

À l'invite de commande, tapez :

```
add azure keyVault <name> -azureVaultName <string> -azureApplication
       <string>
show azure keyvault
<!--NeedCopy-->
```

Exemple :

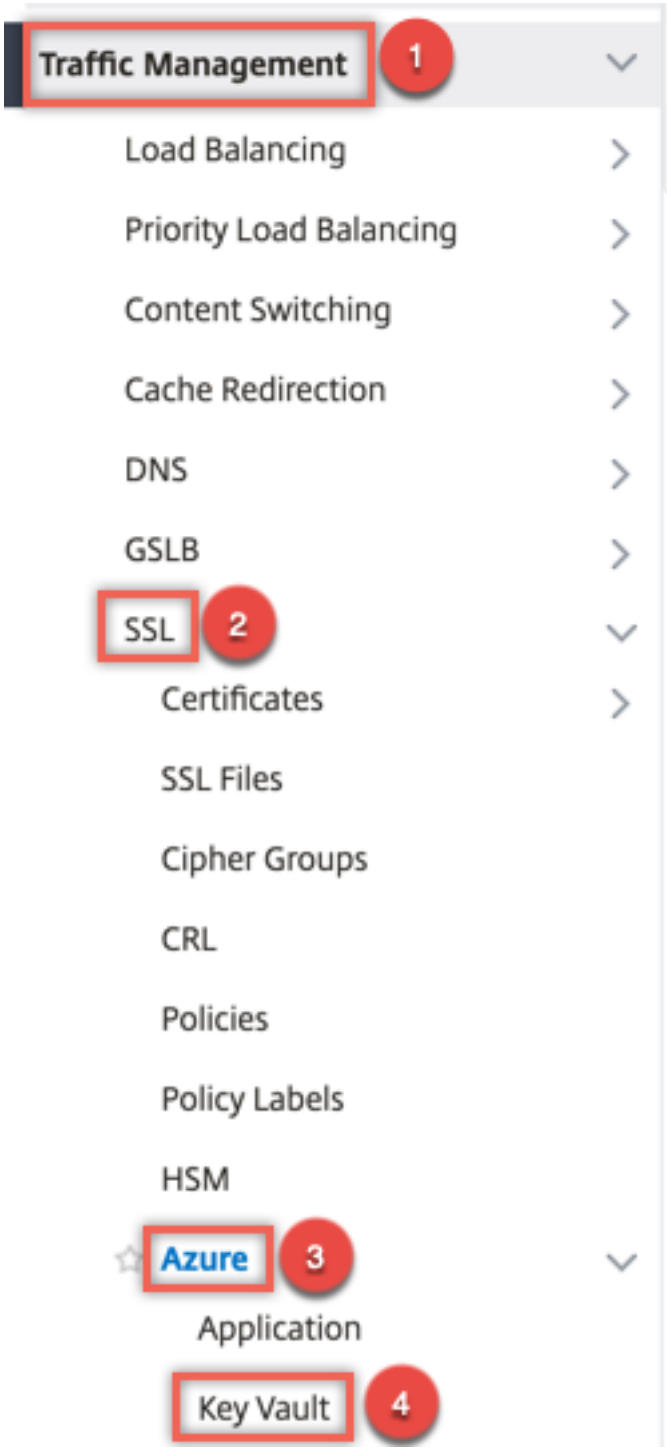
```
add azure keyvault kv1 -azureapplication app10 -azurevaultName pctest.
   vault.azure.net
> sh azure keyVault
1)  Name:  kv1               AzureVaultName:  pctest.vault.azure.net
  AzureApplication:  app10  State:  "Access token obtained"
 Done
<!--NeedCopy-->
```

Le tableau suivant répertorie les différentes valeurs que l'état d'Azure Key Vault peut prendre, ainsi qu'une brève description de chaque état.

State	Description
`Created`	État initial de l'objet Key Vault. L'authentification n'a pas été tentée.
`Could not reach token end point`	Indique l'un des éléments suivants : serveur DNS non configuré, certificat émetteur non lié à un groupe de certificats d'autorité de certification ou problèmes de réseau.
`Authorization failed`	Informations d'identification d'application incorrectes
`Token parse error`	La réponse d'Azure Active Directory n'est pas au format attendu.
`Access token obtained`	Authentification réussie par Azure Active Directory.

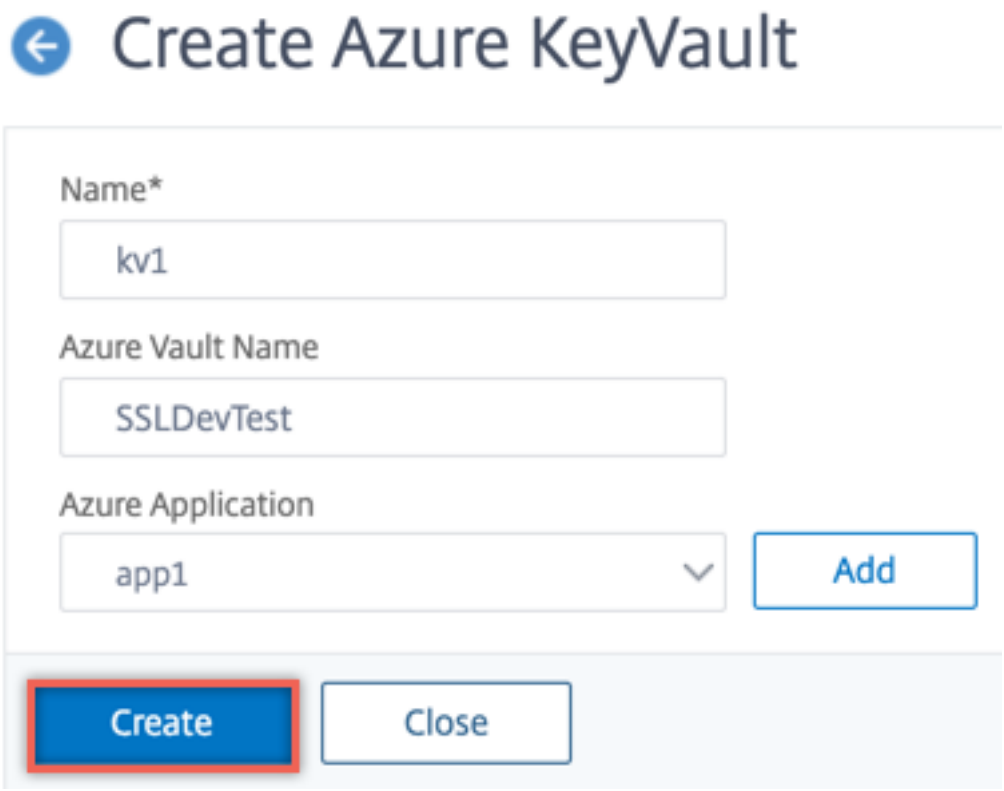
Pour configurer le coffre-fort de clés Azure à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Azure > Key Vault**.



2. Entrez des valeurs pour les paramètres suivants :
   - Nom : nom du coffre de clés.
   - Nom du coffre de clés Azure : nom du coffre de clés configuré dans le cloud Azure à l'aide de l'interface de ligne de commande Azure ou du portail Azure (GUI) avec nom de domaine.
   - Nom de l'application Azure : nom de l'objet Application Azure créé sur l'appliance ADC.

L'objet Application Azure portant ce nom est utilisé pour l'authentification auprès d'Azure Active Directory.



Ajouter une clé HSM

Le stockage de votre clé privée dans le HSM garantit la conformité FIPS 140-2 niveau 2.

Pour ajouter une clé HSM à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ssl hsmKey <hsmKeyName> [-hsmType <hsmType>] [-key <string> |
       -serialNum <string>] {
 -password  }
  [-keystore <string>]
<!--NeedCopy-->
```

Exemple :

```
add ssl hsmKey h1 -keystore kv1 -key san15key -hsmType KEYVAULT


> sh ssl hsmKey h1
```



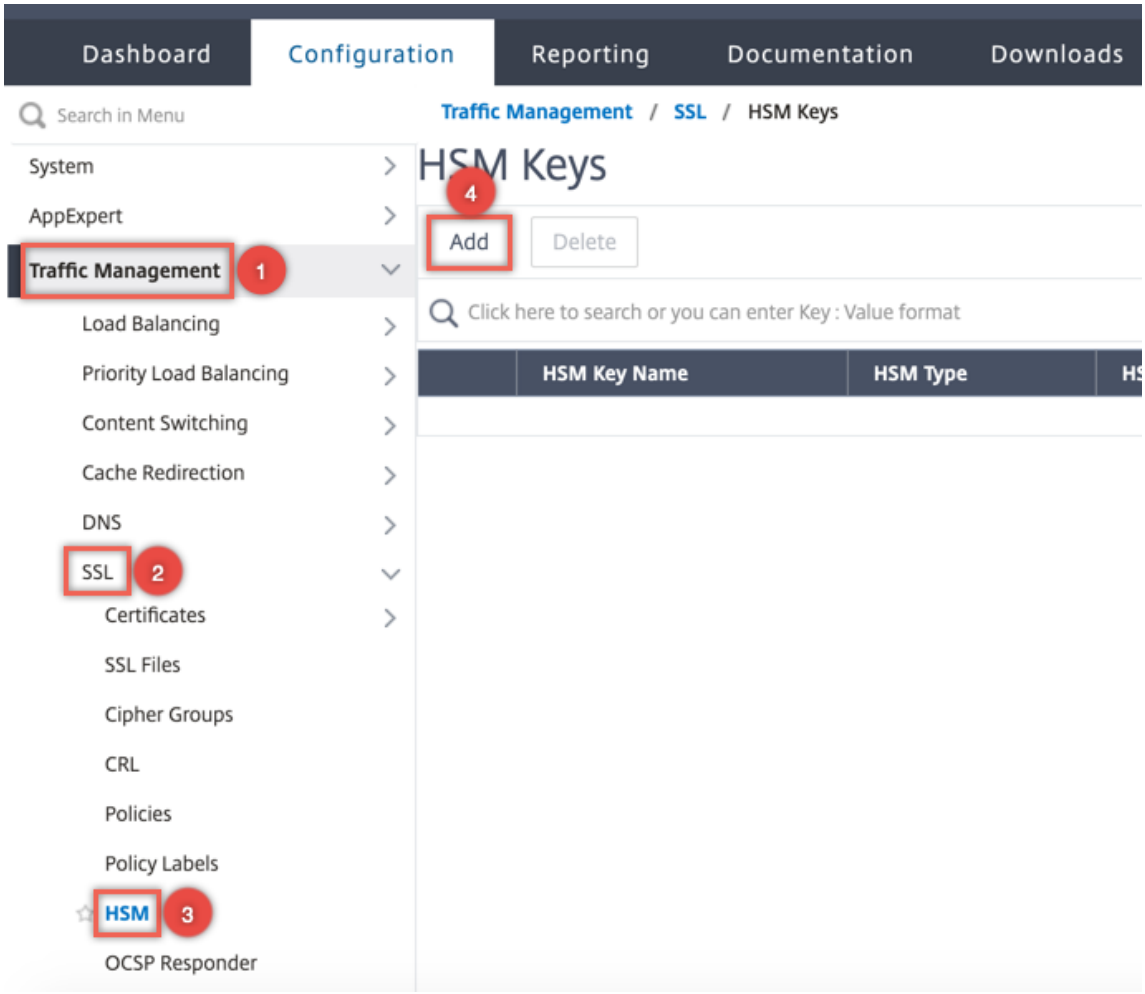
```
    HSM Key Name: h1       Type: KEYVAULT
    Key: san15key
    Key store: kv1
    State:  “Created”
 Done
<!--NeedCopy-->
```

Le tableau suivant répertorie les différentes valeurs que l’état d’une clé HSM peut prendre, ainsi qu’une brève description de chaque état.

State	Description
Created	La clé HSM est ajoutée sur l’appliance ADC. Aucune opération clé n’a encore été tentée.
Token d’accès non disponible	Le jeton d’accès n’est pas disponible lors d’une tentative d’opération de clé
Non autorisé	L’application Azure configurée n’est pas autorisée à effectuer l’opération clé.
N’existe pas	La clé n’existe pas dans Azure Key Vault.
Injoignable	L’hôte Key Vault n’est pas accessible sur le réseau.
Marqué en bas	La touche HSM est marquée DOWN sur l’appliance ADC en raison d’erreurs de seuil lors du fonctionnement de la clé.
Opérations clés réussies	Réponse réussie reçue de Key Vault pour l’opération des clés.
Les opérations clés ont échoué	Réponse en cas d’échec reçue de Key Vault pour le fonctionnement des clés.
Opération de clé étranglée	La demande d’opération de clé est ralentie par le coffre de clés.

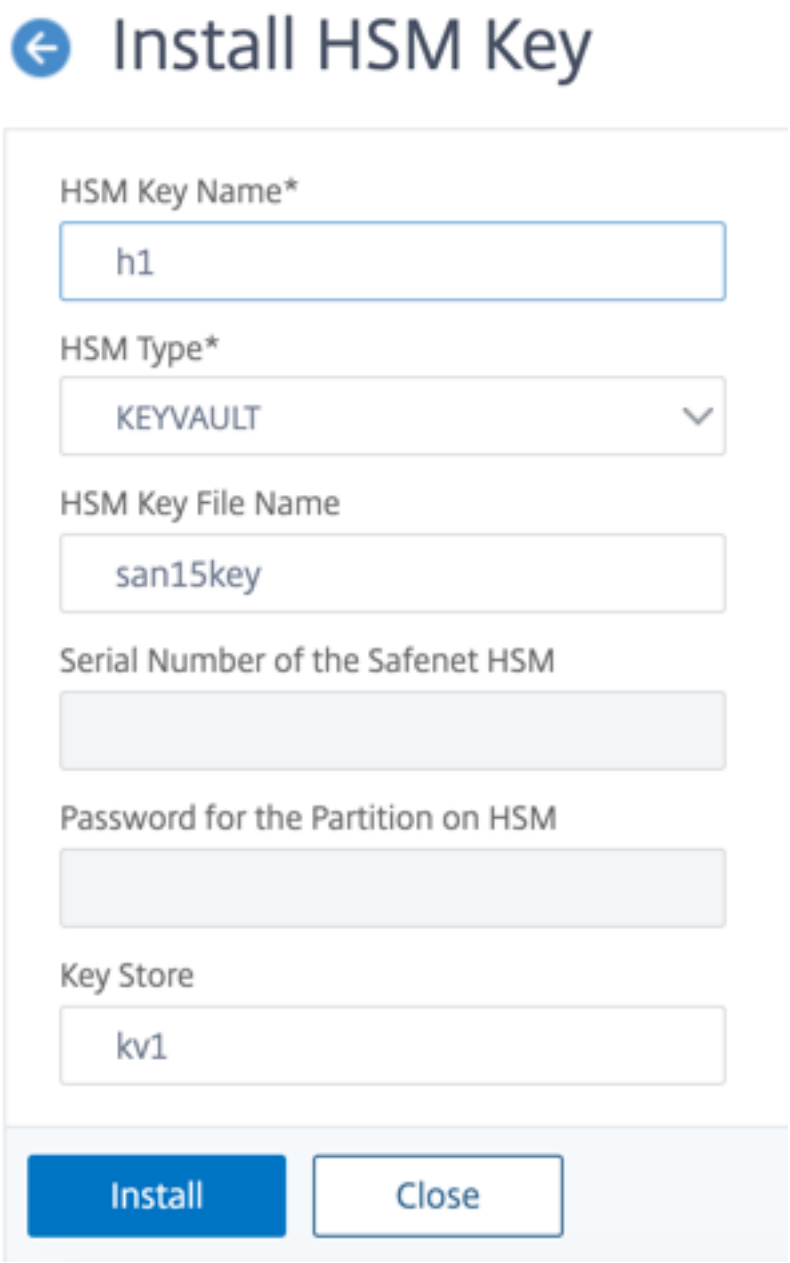
Pour ajouter une clé HSM à l’aide de l’interface graphique

1. Accédez à **Gestion du trafic > SSL > HSM**.



2. Entrez des valeurs pour les paramètres suivants.

   - Nom de la clé HSM : nom de la clé.
   - Type HSM : type de HSM.
   - Magasin de clés : nom de l'objet de stockage de clés représentant le HSM dans lequel la clé est stockée. Par exemple, le nom de l'objet Key Vault ou de l'objet d'authentification Azure Key Vault. S'applique uniquement au KEYVAULT type HSM.



3. Cliquez sur **Ajouter**.

Ajouter une paire de clés de certificat

Ajoutez une paire de clés de certificat à l'aide de la clé HSM créée précédemment.

Pour ajouter une paire de clés de certificat à l'aide de la CLI

À l'invite de commande, tapez :

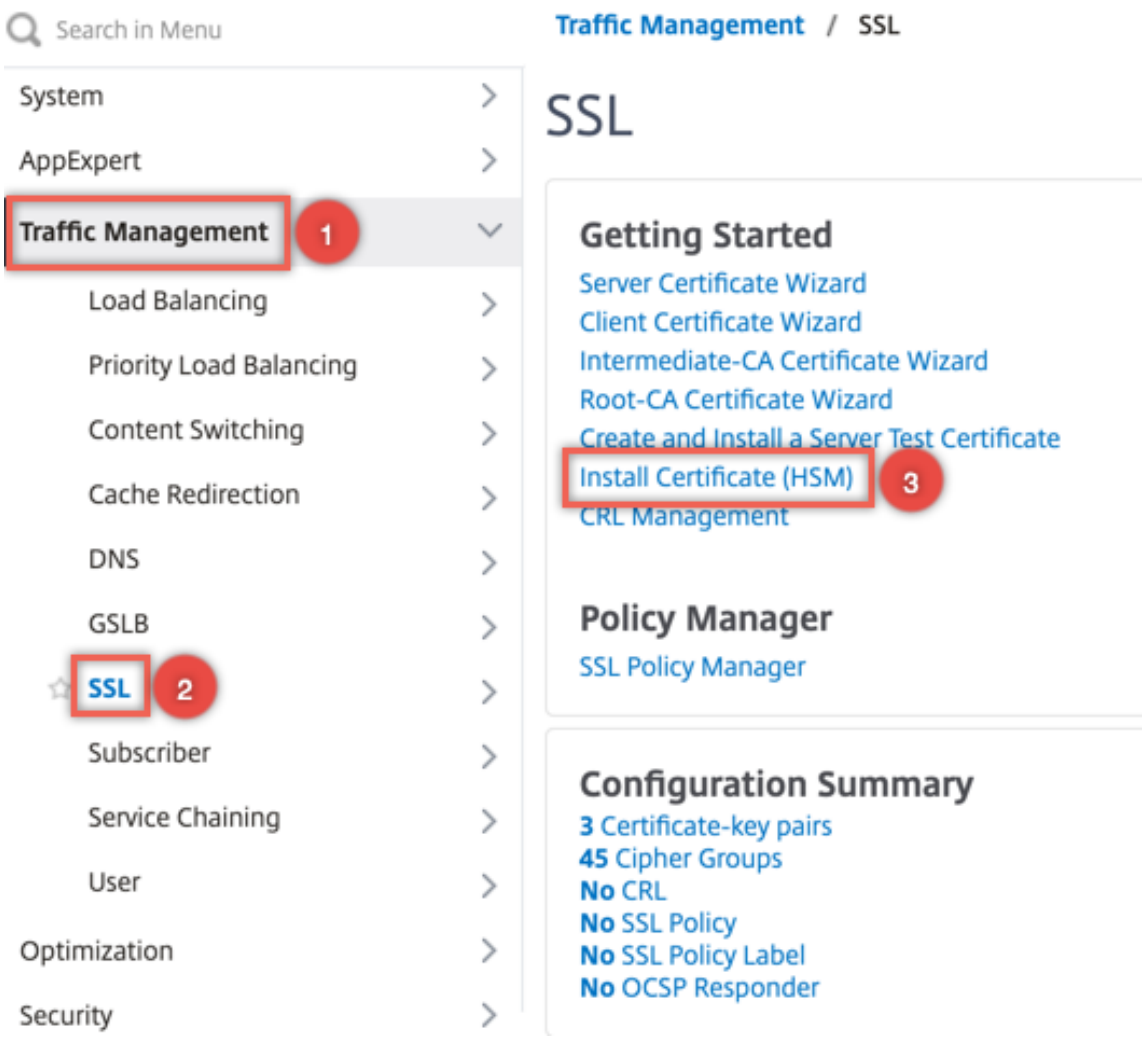

```
add ssl certKey <certkeyName> (-cert <string> [-password]) -hsmKey <
   string>]
show ssl certkey
<!--NeedCopy-->
```

Exemple :

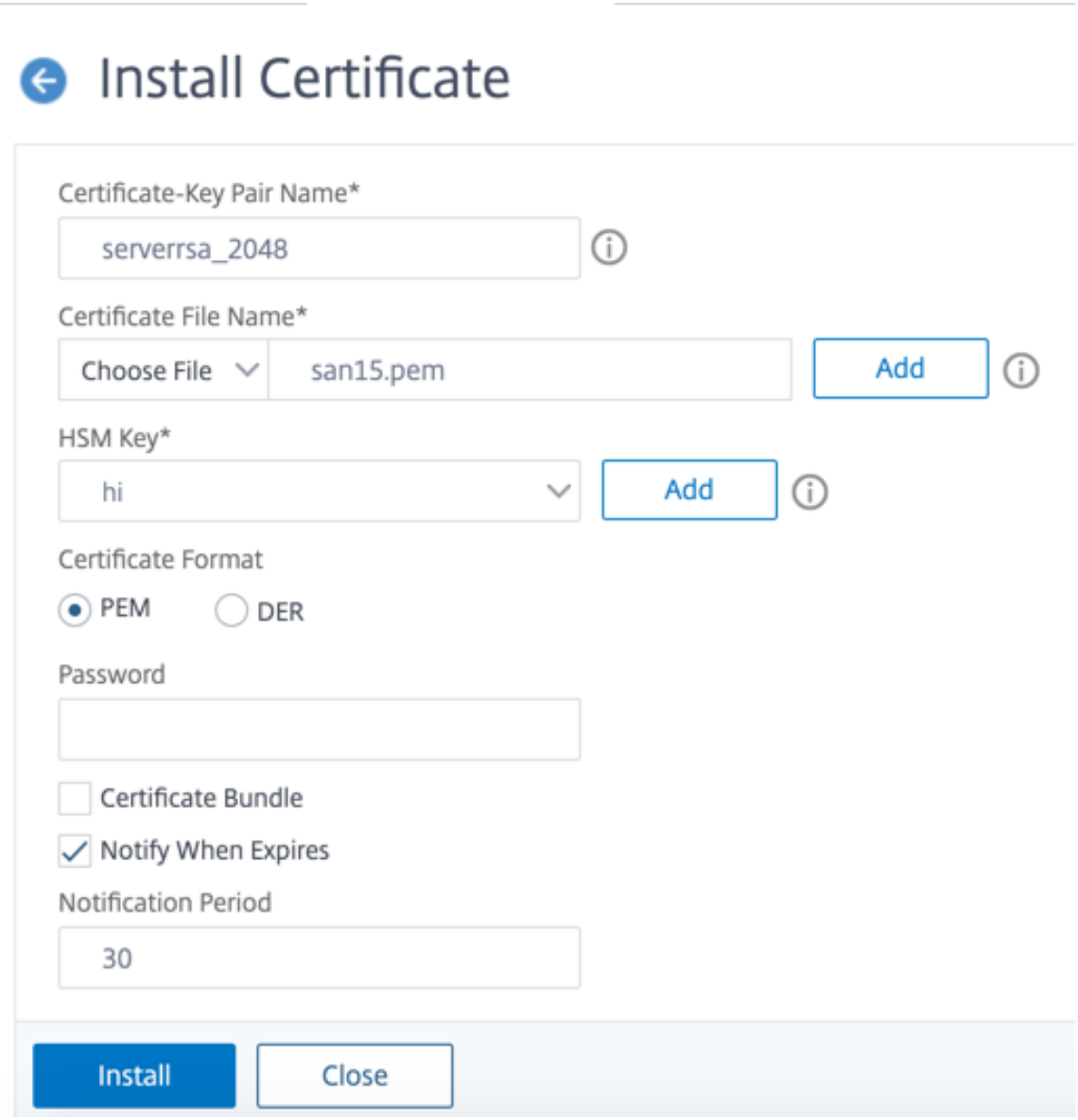
```
add ssl certKey serverrsa_2048 -cert /nsconfig/ssl/san_certs/san15.pem
   -hsmKey h1
> sh ssl certkey serverrsa_2048
    Name: serverrsa_2048        Status: Valid,   Days to expiration
       :9483
    Version: 3
    Serial Number: F5CFF9EF1E246022
    Signature Algorithm: sha256WithRSAEncryption
    Issuer:  C=in,O=citrix,CN=ca
    Validity
        Not Before: Mar 20 05:42:57 2015 GMT
        Not After : Mar 12 05:42:57 2045 GMT
    Certificate Type:   "Server Certificate"
    Subject:  C=in,O=citrix
    Public Key Algorithm: rsaEncryption
    Public Key size: 2048
    Ocsp Response Status: NONE
 Done
<!--NeedCopy-->
```

Pour ajouter une paire de clés de certificat à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Certificat d'installation (HSM)**.



2. Entrez des valeurs pour les paramètres suivants :
   - Nom de la paire de clés de certificat
   - Nom du fichier de certificat
   - Clé HSM



3. Cliquez sur **Installer**.

Liez la paire de clés de certificat à un serveur virtuel

Le certificat utilisé pour le traitement des transactions SSL doit être lié au serveur virtuel qui reçoit les données SSL.

Pour lier la paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
show ssl vserver <vServerName>
```



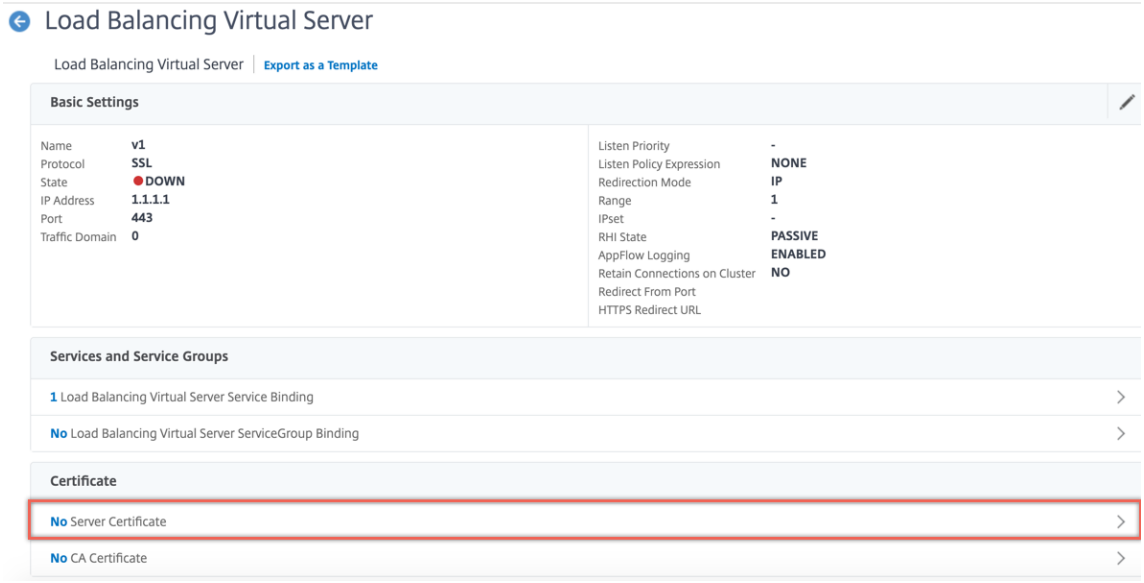
```
<!--NeedCopy-->
```

Exemple :

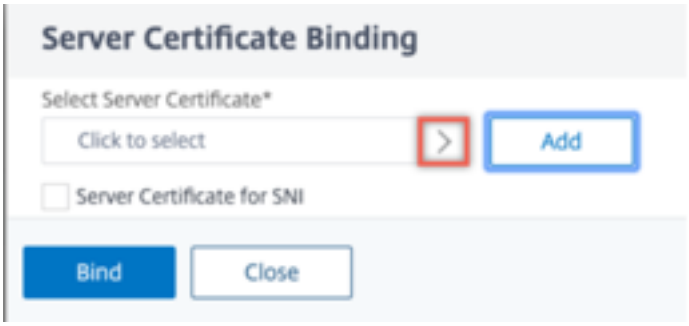
```
bind ssl vserver v1 -certkeyName serverrsa_2048

sh ssl vserver v1

    Advanced SSL configuration for VServer v1:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED      Refresh Count: 0
    Session Reuse: ENABLED      Timeout: 120 seconds
    Cipher Redirect: DISABLED
    ClearText Port: 0
    Client Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: DISABLED
    OCSP Stapling: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    HSTS Preload: NO
    SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Push Encryption Trigger: Always
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1

    ECC Curve: P_256, P_384, P_224, P_521

1)  CertKey Name: serverrsa_2048    Server Certificate



1)  Cipher Name: DEFAULT
    Description: Default cipher list with encryption strength >= 128bit
 Done
<!--NeedCopy-->
```

Pour lier une paire de clés de certificat SSL à un serveur virtuel à l'aide de l'interface graphique

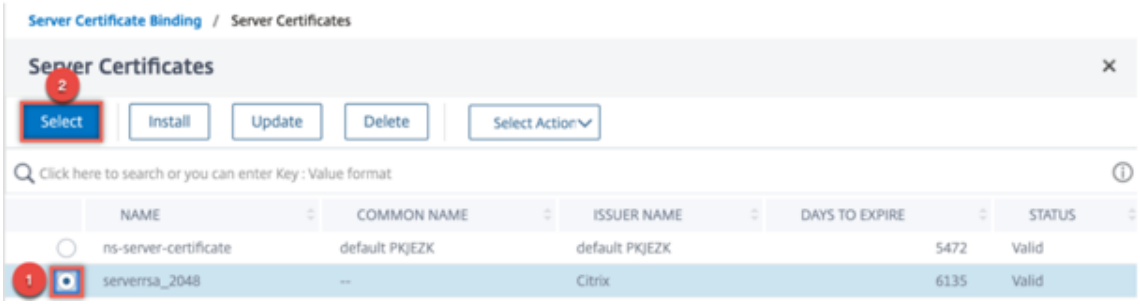
1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et ouvrez un serveur virtuel SSL. Cliquez à l'intérieur de la section Certificat .



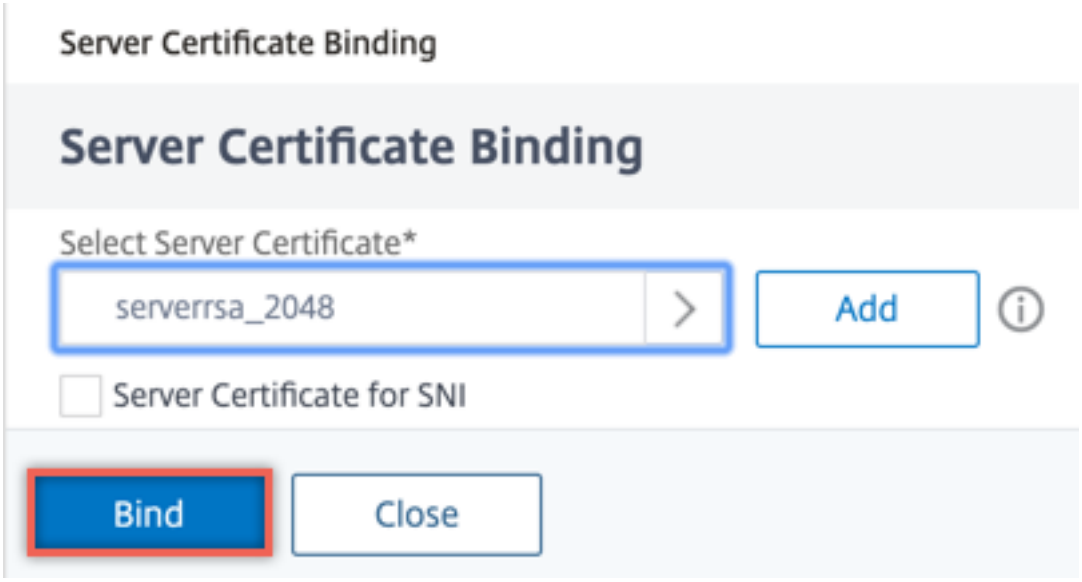
2. Cliquez sur la flèche pour sélectionner la paire de clés de certificat.



3. Sélectionnez la paire de clés de certificat dans la liste.



4. Liez la paire de clés de certificat au serveur virtuel.



Limitations

- Le nombre d'appels simultanés vers Azure Key Vault pour des opérations clés est limité. Les performances de l'appliance ADC dépendent des limites de Key Vault. Pour plus d'informations, reportez-vous à la documentation de Microsoft Azure Key Vault.
- Les clés EC ne sont pas prises en charge.
- Les protocoles EDT et DTLS ne sont pas pris en charge.
- Les appareils ADC équipés de puces SSL Intel Coleto ne sont pas pris en charge.
- Les partitions de clustering et d'administration ne sont pas prises en charge.
- Vous ne pouvez pas mettre à jour l'entité Application Azure, l'objet Azure Key Vault et la paire certificat-clé HSM après les avoir ajoutés à l'appliance ADC.
- Un ensemble de certificats avec des clés HSM n'est pas pris en charge.
- Une erreur n'apparaît pas si la clé HSM et le certificat ne correspondent pas. Lors de l'ajout d'une paire de clés de certificat, assurez-vous que la clé HSM et le certificat correspondent.
- Vous ne pouvez pas lier une clé HSM à un serveur virtuel DTLS.
- Vous ne pouvez pas signer les demandes OCSP à l'aide d'une paire de clés de certificat créée à l'aide d'une clé HSM.
- Vous ne pouvez pas lier une paire de clés de certificat à un service SSL si la paire de clés de certificat est créée à l'aide d'une clé HSM.

Questions fréquentes

Lorsqu'elles sont intégrées à Azure Key Vault, les clés privées sont-elles stockées dans la mémoire de l'appliance ADC ?

Non, les clés privées ne sont pas stockées dans la mémoire de l'appliance ADC. Pour chaque transaction SSL, l'appliance envoie une demande à Key Vault.

L'intégration est-elle conforme à la norme FIPS 140-2 niveau 2 ?

Oui, la solution intégrée prend en charge la norme FIPS 140-2 niveau 2.

Quels types de clés sont pris en charge ?

Seuls les types de clés RSA sont pris en charge.

Quelles sont les tailles de clés prises en charge ?

Les clés RSA 1 024 bits, 2 048 bits et 4096 bits sont prises en charge.

Quels chiffrements sont pris en charge ?

Tous les chiffrements pris en charge par l'appliance ADC, y compris les chiffrements TLSv1.3 avec ECDHE et SHA256 sont pris en charge.

Les transactions sont-elles enregistrées ?

L'appliance ADC enregistre chaque transaction qu'elle effectue avec le coffre de clés. Les détails tels que l'heure, l'adresse IP du coffre-fort, le port, la réussite ou l'échec de la connexion et les erreurs sont consignés.
Voici un exemple de sortie de journal SSL.

```
1 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
       0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 896 0 :
     Backend SPCBId 30894 - ServerIP 104.211.224.186 - ServerPort 443
      - ProtocolVersion TLSv1.2 - CipherSuite "ECDHE-RSA-AES256-GCM-
     SHA384 TLSv1.2 Non-Export 256-bit" - Session New -
     SERVER_AUTHENTICATED -SerialNumber "200005
     A75B04365827852D630000000005A75B" - SignatureAlgorithm "
     sha256WithRSAEncryption" - ValidFrom "Mar 17 03:28:42 2019 GMT"
     - ValidTo "Mar 17 03:28:42 2021 GMT" - HandshakeTime 40 ms
2 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
```



```
        0-PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 897 0 :
      SPCBId 30894 - IssuerName " C=US,ST=Washington,L=Redmond,O=
      Microsoft Corporation,OU=Microsoft IT,CN=Microsoft IT TLS CA 2"
3 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
        0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 898 0 :
      SPCBId 30894 - SubjectName " CN=vault.azure.net"
4 <!--NeedCopy-->
```

Dépannage

May 5, 2023

Si la fonctionnalité SSL ne fonctionne pas comme prévu après la configuration, vous pouvez utiliser certains outils courants pour accéder aux ressources NetScaler et diagnostiquer le problème.

Ressources pour le dépannage

Pour de meilleurs résultats, utilisez les ressources suivantes pour résoudre un problème SSL sur une appliance NetScaler :

- Le fichier ns.log correspondant
- Le dernier fichier ns.conf
- Le fichier des messages
- Le `newnslog` dossier concerné
- Fichiers de traçage
- Une copie des fichiers de certificat, si possible
- Une copie du fichier clé, si possible
- Le message d'erreur, le cas échéant

Outre ces ressources, vous pouvez utiliser l'application Wireshark personnalisée pour les fichiers de trace NetScaler afin d'accélérer le dépannage.

Résolution des problèmes liés au protocole SSL

Pour résoudre un problème SSL, procédez comme suit :

- Vérifiez que l'appliance NetScaler possède une licence pour le déchargement SSL et l'équilibrage de charge.
- Vérifiez que les fonctionnalités de déchargement SSL et d'équilibrage de charge sont activées sur l'appliance.
- Vérifiez que l'état du serveur virtuel SSL ne s'affiche pas comme DOWN.

- Vérifiez que l'état du service lié au serveur virtuel ne s'affiche pas comme DOWN.
- Vérifiez qu'un certificat valide est lié au serveur virtuel.
- Vérifiez que le service utilise un port approprié, de préférence le port 443.

Déchiffrer le trafic TLS1.3 à partir du traçage de paquets

Pour résoudre les problèmes liés aux protocoles qui s'exécutent sur TLS1.3, vous devez d'abord déchiffrer le trafic TLS1.3. Pour décrypter TLS 1.3 dans Wireshark, les secrets doivent être exportés dans le format du journal des clés NSS. Pour plus d'informations sur le format du journal de clés, voir Format du journal de clés NSS.

Pour plus d'informations sur la façon de capturer une trace de paquets, voir Capture des clés de session SSL pendant un suivi.

Remarque : NetScaler enregistre automatiquement les secrets de chaque connexion dans le format approprié pour la version du protocole TLS/SSL utilisée.

L'actualisation de la CRL ne se produit pas sur le nœud secondaire dans une configuration HA

L'actualisation ne se produit pas car le serveur CRL n'est accessible qu'au nœud principal via un réseau privé.

Solution : Ajoutez un service sur le nœud principal avec l'adresse IP du serveur CRL. Ce service fait office de proxy pour le serveur CRL. Lorsque la configuration est synchronisée entre les nœuds, l'actualisation des listes de révocation des droits de révocation fonctionne pour les nœuds principaux et secondaires via le service configuré sur le nœud principal.

FAQ SSL

May 5, 2023

Questions de base

L'accès HTTPS à l'interface graphique échoue sur une instance VPX. Comment puis-je y accéder ?

Une paire de clés de certificat est requise pour l'accès HTTPS à l'interface graphique. Sur une appliance NetScaler, une paire de clés de certificat est automatiquement liée aux services internes. Sur une appliance MPX ou SDX, la taille de clé par défaut est de 1024 octets, et sur une instance VPX, la taille de clé par défaut est de 512 octets. Cependant, la plupart des navigateurs actuels n'acceptent

pas une clé de moins de 1024 octets. Par conséquent, l'accès HTTPS à l'utilitaire de configuration VPX est bloqué.

Citrix vous recommande d'installer une paire de clés de certificat d'au moins 1 024 octets et de la lier au service interne pour l'accès HTTPS à l'utilitaire de configuration. Vous pouvez également mettre à jour le `ns-server-certificate` à 1024 octets. Vous pouvez utiliser l'accès HTTP à l'utilitaire de configuration ou à l'interface de ligne de commande pour installer le certificat.

Si j'ajoute une licence à une appliance MPX, la liaison de la paire de clés de certificat est perdue. Comment puis-je résoudre ce problème ?

Si aucune licence n'est présente sur une appliance MPX lors de son démarrage, que vous ajoutez une licence ultérieurement et que vous redémarrez l'appliance, vous risquez de perdre la liaison du certificat. Réinstallez le certificat et liez-le au service interne

Citrix vous recommande d'installer une licence appropriée avant de démarrer l'appliance.

Quelles sont les différentes étapes de la mise en place d'un canal sécurisé pour une transaction SSL ?

La configuration d'un canal sécurisé pour une transaction SSL implique les étapes suivantes :

1. Le client envoie une demande HTTPS pour un canal sécurisé au serveur.
2. Après avoir sélectionné le protocole et le chiffrement, le serveur envoie son certificat au client.
3. Le client vérifie l'authenticité du certificat du serveur.
4. Si l'un des contrôles échoue, le client affiche le feedback correspondant.
5. Si les chèques sont réussis ou si le client décide de continuer même en cas d'échec, le client crée une clé temporaire jetable. Cette clé est appelée *secret pré-maître* et le client chiffre cette clé à l'aide de la clé publique du certificat du serveur.
6. Le serveur, à la réception du secret pré-maître, le déchiffre à l'aide de la clé privée du serveur et génère les clés de session. Le client génère également les clés de session à partir du secret pré-maître. Ainsi, le client et le serveur disposent désormais d'une clé de session commune, qui est utilisée pour le chiffrement et le déchiffrement des données de l'application.

Je comprends que le SSL est un processus gourmand en ressources processeur. Quel est le coût du processeur associé au processus SSL ?

Les deux étapes suivantes sont associées au processus SSL :

- La poignée de main initiale et la configuration du canal sécurisé à l'aide de la technologie des clés publiques et privées.

- Chiffrement des données en masse à l'aide de la technologie à clé symétrique.

Les deux étapes précédentes peuvent affecter les performances du serveur et nécessitent un traitement intensif du processeur pour les raisons suivantes :

1. La poignée de main initiale implique la cryptographie à clé publique-privée, qui est très gourmande en processeur en raison de la grande taille des clés (1024 bits, 2048 bits, 4096 bits).
2. Le chiffrement/déchiffrement des données est également coûteux en termes de calcul, selon la quantité de données qui doivent être cryptées ou décryptées.

Quelles sont les différentes entités d'une configuration SSL ?

Une configuration SSL comporte les entités suivantes :

- Écran Server certificate
- Certificat d'autorité de certification (CA)
- Suite de chiffrement qui spécifie les protocoles pour les tâches suivantes :
  - Échange initial de clés
  - Authentification des serveurs et clients
  - algorithme de chiffrement en masse
  - Authentification des messages
- Authentification client
- CRL
- Outil de génération de clés de certificat SSL qui vous permet de créer les fichiers suivants :
  - Demande de certificat
  - Certificat auto-signé
  - Clés RSA
  - Paramètres DH

Je souhaite utiliser la fonctionnalité de déchargement SSL de l'appliance NetScaler. Quelles sont les différentes options pour recevoir un certificat SSL ?

Vous devez recevoir un certificat SSL avant de pouvoir configurer la configuration SSL sur l'appliance NetScaler. Vous pouvez utiliser l'une des méthodes suivantes pour recevoir un certificat SSL :

- Demandez un certificat auprès d'une autorité de certification (CA) agréée.
- Utilisez le certificat de serveur existant.
- Créez une paire de clés de certificat sur l'appliance NetScaler.

Remarque : Ce certificat est un certificat de test signé par la racine de test CA générée par l'appliance NetScaler. Les certificats de test signés par le Root-CA de test ne sont pas acceptés par les navigateurs.

Le navigateur affiche un message d'avertissement indiquant que le certificat du serveur ne peut pas être authentifié.

- À des fins autres que de test, vous devez fournir un certificat d'autorité de certification et une clé d'autorité de certification valides pour signer le certificat du serveur.

Quelles sont les exigences minimales pour une configuration SSL ?

Les exigences minimales pour configurer une configuration SSL sont les suivantes :

- Procurez-vous les certificats et les clés.
- Créez un serveur virtuel SSL d'équilibrage de charge.
- Liez les services HTTP ou SSL au serveur virtuel SSL.
- Liez une paire de clés de certificat au serveur virtuel SSL.

Quelles sont les limites des différents composants du SSL ?

Les composants SSL ont les limites suivantes :

- Taille en bits des certificats SSL : 4096.
- Nombre de certificats SSL : dépend de la mémoire disponible sur l'appliance.
- Nombre maximum de certificats CA SSL intermédiaires liés : 9 par chaîne.
- Révocations de CRL : dépend de la mémoire disponible sur l'appliance.

Quelles sont les différentes étapes du chiffrement des données de bout en bout sur une appliance NetScaler ?

Les étapes du processus de chiffrement côté serveur sur une appliance NetScaler sont les suivantes :

1. Le client se connecte au SSL VIP configuré sur l'appliance NetScaler sur le site sécurisé.
2. Après avoir reçu la demande sécurisée, l'appliance déchiffre la demande et applique des techniques de commutation de contenu et des politiques d'équilibrage de charge de la couche 4 à 7. Ensuite, il sélectionne le meilleur serveur Web principal disponible pour la demande.
3. L'appliance NetScaler crée une session SSL avec le serveur sélectionné.
4. Après avoir établi la session SSL, l'appliance chiffre la demande du client et l'envoie au serveur Web à l'aide de la session SSL sécurisée.
5. Lorsque l'appliance reçoit la réponse cryptée du serveur, elle déchiffre et rechiffre les données. Ensuite, il envoie les données au client en utilisant la session SSL côté client.

La technique de multiplexage de l'appliance NetScaler permet à l'appliance de réutiliser les sessions SSL qui ont été établies avec les serveurs Web. Par conséquent, l'appliance évite les échanges de clés

gourmands en ressources CPU, appelés « établissement de *main complet* ». Ce processus permet de réduire le nombre total de sessions SSL sur le serveur et de maintenir la sécurité de bout en bout.

Certificats et clés

Puis-je placer le certificat et les fichiers clés à n'importe quel endroit ? Existe-t-il un emplacement recommandé pour stocker ces fichiers ?

Vous pouvez stocker le certificat et les fichiers clés sur l'appliance NetScaler ou sur un ordinateur local. Citrix vous recommande toutefois de stocker les fichiers de certificat et de clé dans le `/nsconfig/ssl` répertoire de l'appliance NetScaler. Le `/etc` répertoire existe dans la mémoire flash de l'appliance NetScaler. Cette action assure la portabilité et facilite la sauvegarde et la restauration des fichiers de certificats sur l'appliance.

Remarque : Assurez-vous que le certificat et les fichiers clés sont stockés dans le même répertoire.

Quelle est la taille maximale de la clé de certificat prise en charge par l'appliance NetScaler ?

Une appliance NetScaler exécutant une version logicielle antérieure à la version 9.0 prend en charge une taille de clé de certificat maximale de 2 048 bits. Les versions 9.0 et ultérieures prennent en charge une taille de clé de certificat maximale de 4 096 bits. Cette limite s'applique aux certificats RSA.

Une appliance MPX prend en charge les certificats de 512 bits jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service
- Certificat d'autorité de certification 4096 bits (y compris les certificats intermédiaires et racine)
- Certificat 4096 bits sur le serveur principal
- Certificat client 4096 bits (si l'authentification client est activée sur le serveur virtuel)

Une appliance virtuelle prend en charge les certificats de 512 bits jusqu'aux tailles suivantes :

- Certificat de serveur 4096 bits sur le serveur virtuel
- Certificat client 4096 bits sur le service
- Certificat d'autorité de certification 4096 bits (y compris les certificats intermédiaires et racine)
- Certificat 4096 bits sur le serveur principal à partir de la version 12.0-56.x. Les anciennes versions prennent en charge les certificats 2048 bits.
- Certificat client 2048 bits (si l'authentification du client est activée sur le serveur virtuel) à partir de la version 12.0-56.x.

Quelle est la taille maximale du paramètre DH pris en charge sur l'appliance NetScaler ?

L'appliance NetScaler prend en charge un paramètre DH d'un maximum de 2 048 bits.

Quelle est la longueur maximale de la chaîne de certificats, c'est-à-dire le nombre maximum de certificats dans une chaîne, pris en charge par une appliance NetScaler ?

Une appliance NetScaler peut envoyer un maximum de 10 certificats par chaîne lors de l'envoi d'un message de certificat de serveur. Une chaîne de la longueur maximale inclut le certificat de serveur et neuf certificats CA intermédiaires.

Quels sont les différents formats de certificats et de clés pris en charge par l'appliance NetScaler ?

L'appliance NetScaler prend en charge les formats de certificat et de clé suivants :

- Courrier électronique à confidentialité améliorée (PEM)
- Règle de codage distinguée (DER)

Le nombre de certificats et de clés que je peux installer sur l'appliance NetScaler est-il limité ?

Non. Le nombre de certificats et de clés pouvant être installés est limité uniquement par la mémoire disponible sur l'appliance NetScaler.

J'ai enregistré le certificat et les fichiers clés sur l'ordinateur local. Je souhaite transférer ces fichiers vers l'appliance NetScaler à l'aide du protocole FTP. Existe-t-il un mode préféré pour transférer ces fichiers vers l'appliance NetScaler ?

Oui. Si vous utilisez le protocole FTP, vous devez utiliser le mode binaire pour transférer le certificat et les fichiers clés vers l'appliance NetScaler.

Remarque : Par défaut, le FTP est désactivé. Citrix recommande d'utiliser le protocole SCP pour transférer les fichiers de certificats et de clés. L'utilitaire de configuration utilise implicitement SCP pour se connecter à l'appliance.

Quel est le chemin de répertoire par défaut pour le certificat et la clé ?

Le chemin de répertoire par défaut pour le certificat et la clé est « /nsconfig/ssl ».

Lors de l'ajout d'une paire de certificats et de clés, que se passe-t-il si je ne précise pas de chemin absolu vers les fichiers de certificat et de clé ?

Lorsque vous ajoutez une paire de clés de certificat, spécifiez un chemin absolu vers les fichiers de certificat et de clé. Si vous ne le spécifiez pas, l'appliance ADC recherche ces fichiers dans le répertoire par défaut et tente de les charger dans le noyau. Le répertoire par défaut est `/nsconfig/ssl`. Par exemple, si les fichiers cert1024.pem et rsa1024.pem sont disponibles dans le `/nsconfig/ssl` répertoire de l'appliance, les deux commandes suivantes sont réussies :

```
1 add ssl certKey cert1 -cert cert1204.pem -key rsa1024.pem
2 <!--NeedCopy-->
```

```
1 add ssl certKey cert1 -cert /nsconfig/ssl/cert1204.pem -key /nsconfig/
     ssl/rsa1024.pem
2 <!--NeedCopy-->
```

J'ai configuré une configuration de haute disponibilité. Je souhaite implémenter la fonctionnalité SSL sur la configuration. Comment dois-je gérer les fichiers de certificat et de clé dans une configuration de haute disponibilité ?

Dans une configuration haute disponibilité, vous devez stocker le certificat et les fichiers clés à la fois sur l'appliance NetScaler principale et secondaire. Le chemin du répertoire pour les fichiers de certificat et de clé doit être le même sur les deux appliances avant d'ajouter une paire de clés de certificat SSL sur l'appliance principale.

HSM nCipher nShield®

Lors de l'intégration à nCipher nShield® HSM, devons-nous tenir compte d'une configuration spécifique lors de l'ajout de l'appliance NetScaler à HA ?

Configurez les mêmes périphériques nCipher sur les deux nœuds dans HA. Les commandes de configuration nCipher ne se synchronisent pas dans HA. Pour plus d'informations sur les conditions préalables à NCipher NShield® HSM, consultez Prérequis.

Doit-on intégrer individuellement les deux appliances avec NCipher NShield® HSM et RFS ? Devons-nous effectuer cette action avant ou après la configuration HA ?

Vous pouvez terminer l'intégration avant ou après la configuration HA. Si l'intégration est effectuée après la configuration HA, les clés importées sur le nœud principal avant de configurer le nœud secondaire ne sont pas synchronisées avec le nœud secondaire. Par conséquent, Citrix recommande l'intégration de nCipher avant la configuration HA.

Devons-nous importer la clé dans les appliances NetScaler principale et secondaire, ou les clés sont-elles synchronisées entre le nœud principal et le nœud secondaire ?

Si nCipher est intégré sur les deux appareils avant de former le HA, les clés sont automatiquement synchronisées à partir de RFS au cours du processus d'intégration.

Étant donné que le HSM ne se trouve pas sur l'appliance NetScaler, mais sur nCipher, qu'arrive-t-il aux clés et aux certificats lorsqu'un nœud tombe en panne et est remplacé ?

Si un nœud tombe en panne, vous pouvez synchroniser les clés et les certificats avec le nouveau nœud en intégrant NCipher sur le nouveau nœud. Exécutez ensuite les commandes suivantes :

```
sync ha files ssl
force ha sync
<!--NeedCopy-->
```

Les certificats sont synchronisés et ajoutés si les clés sont synchronisées au cours du processus d'intégration de nCipher.

Chiffrements

Qu'est-ce qu'un chiffrement nul ?

Les chiffrements sans chiffrement sont appelés chiffrements nuls. Par exemple, NULL-MD5 est un chiffrement NULL.

Les chiffrements NULL sont-ils activés par défaut pour un VIP SSL ou un service SSL ?

Non Les chiffrements nuls ne sont pas activés par défaut pour un VIP SSL ou un service SSL.

Quelle est la procédure pour supprimer les chiffrements nuls ?

Pour supprimer les chiffrements NULL d'un VIP SSL, exécutez la commande suivante :

```
bind ssl cipher <SSL_VIP> REM NULL
<!--NeedCopy-->
```

Pour supprimer les chiffrements NULL d'un service SSL, exécutez la commande suivante :

```
bind ssl cipher <SSL_Service> REM NULL -service
<!--NeedCopy-->
```


Quels sont les différents alias de chiffrement pris en charge par l'appliance NetScaler ?

Pour répertorier les alias de chiffrement pris en charge par l'appliance, à l'invite de commande, tapez :

```
sh cipher
<!--NeedCopy-->
```

Quelle est la commande permettant d'afficher tous les chiffrements prédéfinis de l'appliance NetScaler ?

Pour afficher tous les chiffrements prédéfinis de l'appliance NetScaler, tapez :

```
show ssl cipher
<!--NeedCopy-->
```

Quelle est la commande permettant d'afficher les détails d'un chiffrement individuel de l'appliance NetScaler ?

Pour afficher les détails d'un chiffrement individuel de l'appliance NetScaler, sur l'interface de ligne de commande, tapez :

```
show ssl cipher <Cipher_Name/Cipher_Alias_Name/Cipher_Group_Name>
<!--NeedCopy-->
```

Exemple :

```
show cipher SSL3-RC4-SHA
     1) Cipher Name: SSL3-RC4-SHA
     Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128)
    Mac=SHA1
     Done
<!--NeedCopy-->
```

Quel est l'intérêt d'ajouter les chiffrements prédéfinis de l'appliance NetScaler ?

L'ajout des chiffrements prédéfinis de l'appliance NetScaler entraîne l'ajout des chiffrements NULL à un VIP SSL ou à un service SSL.

Est-il possible de modifier l'ordre du chiffrement sans le dissocier d'un groupe de chiffrement sur une appliance NetScaler ?

Oui. Il est possible de modifier l'ordre du chiffrement sans dissocier les chiffrements d'un groupe de chiffrement personnalisé. Toutefois, vous ne pouvez pas modifier la priorité dans les groupes de chiffrement intégrés. Pour modifier la priorité d'un chiffrement lié à une entité SSL, commencez par dissocier le chiffrement du serveur virtuel, du service ou du groupe de services.

Remarque : Si le groupe de chiffrement lié à une entité SSL est vide, l'établissement de connexion SSL échoue car il n'existe aucun chiffrement négocié. Le groupe de chiffrement doit contenir au moins un chiffre.

L'ECDSA est-il pris en charge sur l'appliance NetScaler ?

L'ECDSA est pris en charge sur les plateformes NetScaler suivantes. Pour plus de détails sur les versions prises en charge, consultez le Tableau 1 et le Tableau 2 de la section Chiffrements disponibles sur les appliances NetScaler.

- Appliances NetScaler MPX et SDX avec puces N3
- NetScaler MPX 5900/8900/15000/26000
- NetScaler SDX 8900/1500
- Appliances NetScaler VPX

L'appliance NetScaler VPX prend-elle en charge les chiffrements AES-GCM/SHA2 sur le front-end ?

Oui, les chiffrements AES-GCM/SHA2 sont pris en charge sur l'appliance NetScaler VPX. Pour plus de détails sur les versions prises en charge, consultez la section Chiffrements disponibles sur les appliances NetScaler.

Certificats

Le nom distinctif figurant dans un certificat client est-il disponible pendant toute la durée de la session utilisateur ?

Oui. Vous pouvez accéder au nom unique du certificat client dans les requêtes suivantes pendant la durée de la session utilisateur. C'est-à-dire, même une fois que la connexion SSL est terminée et que le certificat n'est pas envoyé à nouveau par le navigateur. Utilisez une variable et une affectation comme indiqué dans l'exemple de configuration suivant :

Exemple :

```
1 add ns variable v2 -type "text(100)"
```



```
2
3 add ns assignment a1 -variable "$v2" -set       "CLIENT.SSL.CLIENT_CERT
    .SUBJECT.TYPECAST_NVLIST_T('=','/').VALUE("CN")"
4
5 add rewrite action act1 insert_http_header subject "$v2"  // example:
    to insert the distinguished name in the header
6
7 add rewrite policy pol1 true a1
8
9 add rewrite policy pol2 true act1
10
11 bind rewrite global pol1 1 next -type RES_DEFAULT
12
13 bind rewrite global pol2 2 next -type RES_DEFAULT
14
15 set rewrite param -undefAction RESET
16 <!--NeedCopy-->
```

Pourquoi dois-je lier le certificat du serveur ?

La liaison des certificats de serveur est la condition de base pour permettre à la configuration SSL de traiter les transactions SSL.

Pour lier le certificat de serveur à un VIP SSL, dans l'interface de ligne de commande, tapez :

```
1 bind ssl vserver <vServerName> -certkeyName <cert_name>
2 <!--NeedCopy-->
```

Pour lier le certificat de serveur à un service SSL, dans l'interface de ligne de commande, tapez :

```
1 bind ssl service <serviceName> -certkeyName <cert_name>
2 <!--NeedCopy-->
```

Combien de certificats puis-je associer à un VIP SSL ou à un service SSL ?

Sur une appliance FIPS NetScaler VPX, MPX/SDX (N3) et MPX/SDX 14000, vous pouvez lier deux certificats à un serveur virtuel SSL ou à un service SSL si le SNI est désactivé. Les certificats doivent être de type RSA et ECDSA. Si le SNI est activé, vous pouvez lier plusieurs certificats de serveur de type RSA ou ECDSA. Sur une appliance FIPS NetScaler MPX (N2) ou MPX 9700, si le SNI est désactivé, vous ne pouvez lier qu'un seul certificat de type RSA. Si le SNI est activé, vous pouvez lier plusieurs certificats de serveur de type RSA uniquement.

Que se passe-t-il si je dissocie ou remplace un certificat de serveur ?

Lorsque vous dissociez ou remplacez un certificat de serveur, toutes les connexions et sessions SSL créées à l'aide du certificat existant sont interrompues. Lorsque vous remplacez un certificat existant, le message suivant s'affiche :

```
ERROR:

Warning: Current certificate replaces the previous binding.
<!--NeedCopy-->
```

Comment installer un certificat intermédiaire sur une appliance NetScaler et créer un lien vers un certificat de serveur ?

Consultez l'article suivant http://support.citrix.com/article/ctx114146 pour plus d'informations sur l'installation d'un certificat intermédiaire.

Pourquoi le message d'erreur « La ressource existe déjà » s'affiche-t-il lorsque j'essaie d'installer un certificat sur NetScaler ?

Consultez l'article suivant http://support.citrix.com/article/CTX117284 pour obtenir des instructions sur la résolution de l'erreur « La ressource existe déjà ».

Je souhaite créer un certificat de serveur sur une appliance NetScaler afin de tester et d'évaluer le produit. Quelle est la procédure pour créer un certificat de serveur ?

Procédez comme suit pour créer un certificat de test.

Remarque : Un certificat créé à l'aide de cette procédure ne peut pas être utilisé pour authentifier tous les utilisateurs et navigateurs. Après avoir utilisé le certificat à des fins de test, vous devez obtenir un certificat de serveur signé par une autorité de certification racine autorisée.

Pour créer un certificat de serveur auto-signé :

1. Pour créer un certificat Root CA, dans l'interface de ligne de commande, tapez :

```
create ssl rsakey /nsconfig/ssl/test-ca.key 1024

create ssl certreq /nsconfig/ssl/test-ca.csr -keyfile /nsconfig/
   ssl/test-ca.key

Enter the required information when prompted, and then type the
   following command:

```



```
create ssl cert /nsconfig/ssl/test-ca.cer /nsconfig/ssl/test-ca.
    csr ROOT_CERT -keyfile /nsconfig/ssl/test-ca.key
<!--NeedCopy-->
```

2. Procédez comme suit pour créer un certificat de serveur et le signer à l'aide du certificat d'autorité de certification racine que vous venez de créer

   a) Pour créer la demande et la clé, dans l'interface de ligne de commande, tapez :

```
create ssl rsakey /nsconfig/ssl/test-server.key 1024

    create ssl certreq /nsconfig/ssl/test-server.csr -keyfile
       /nsconfig/ssl/test-server.key
<!--NeedCopy-->
```

   b) Entrez les informations requises lorsque vous y êtes invité.

   c) Pour créer un fichier de numéro de série, dans l'interface de ligne de commande, tapez :

```
shell
 # echo '01' >
/nsconfig/ssl/serial.txt
 # exit
<!--NeedCopy-->
```

   d) Pour créer un certificat de serveur signé par le certificat de l'autorité de certification racine créé à l'étape 1, dans l'interface de ligne de commande, tapez :

```
create ssl cert /nsconfig/ssl/test-server.cer /nsconfig/ssl/
    test-server.csr SRVR_CERT -CAcert /nsconfig/ssl/test-ca.cer
     -CAkey /nsconfig/ssl/test-ca.key -CAserial /nsconfig/ssl/
    serial.txt
<!--NeedCopy-->
```

   e) Pour créer une paire de clés de certificat NetScaler, qui est l'objet en mémoire qui contient les informations de certificat du serveur pour les connexions SSL et le chiffrement en bloc, sur l'interface de ligne de commande, tapez :

```
add ssl certkey test-certkey -cert /nsconfig/ssl/test-server.
    cer -key /nsconfig/ssl/test-server.key
<!--NeedCopy-->
```

   f) Pour lier la paire de clés de certification au serveur virtuel SSL, dans l'interface de ligne de commande, tapez :


```
bind ssl vserver <vServerName> -certkeyName <cert_name>
<!--NeedCopy-->
```

J'ai reçu une appliance NetScaler sur laquelle la version 9.0 du logiciel NetScaler est installée. J'ai remarqué la présence d'un fichier de licence supplémentaire sur l'appliance. La politique de licence a-t-elle été modifiée à compter de la version 9.0 du logiciel NetScaler ?

Oui. À partir de la version 9.0 du logiciel NetScaler, l'appliance peut ne pas disposer d'un seul fichier de licence. Le nombre de fichiers de licence dépend de l'édition du logiciel NetScaler. Par exemple, si vous avez installé l'édition Advanced, vous aurez peut-être besoin de fichiers de licence supplémentaires pour bénéficier de toutes les fonctionnalités des différentes fonctionnalités. Toutefois, si vous avez installé l'édition Premium, l'appliance ne possède qu'un seul fichier de licence.

Comment exporter le certificat depuis l'Internet Information Service (IIS) ?

Il existe de nombreuses méthodes, mais en utilisant la méthode suivante, le certificat et la clé privée appropriés pour le site Web sont exportés. Cette procédure doit être effectuée sur le serveur IIS lui-même.

1. Ouvrez l'outil d'administration du gestionnaire des services Internet (IIS).
2. Développez le nœud Sites Web et localisez le site Web compatible SSL que vous souhaitez diffuser via l'appliance NetScaler.
3. Cliquez avec le bouton droit sur ce site Web et cliquez sur Propriétés.
4. Cliquez sur l'onglet Sécurité du répertoire et, dans la section Communications sécurisées de la fenêtre, cochez la case Afficher le certificat.
5. Cliquez sur l'onglet Détails, puis sur Copier dans un fichier.
6. Sur la page Bienvenue dans l'assistant d'exportation de certificats, cliquez sur Suivant.
7. Sélectionnez Oui, exportez la clé privée, puis cliquez sur Suivant.

   Remarque : La clé privée DOIT être exportée pour que SSL Offload fonctionne sur NetScaler.
8. Assurez-vous que le bouton radio Personal Information Exchange -PKCS #12 est sélectionné et cochez *uniquement* la case Inclure tous les certificats dans le chemin de certification si possible. Cliquez sur Next.
9. Entrez un mot de passe et cliquez sur Suivant.
10. Entrez un nom de fichier et un emplacement, puis cliquez sur Suivant. Donnez au fichier l'extension .PFX.
11. Cliquez sur Finish.

Comment convertir le certificat PKCS #12 et l'installer sur NetScaler ?

1. Déplacez le fichier de certificat .PFX exporté vers un emplacement à partir duquel il peut être copié vers l'appliance NetScaler. C'est-à-dire à une machine qui autorise l'accès SSH à l'interface de gestion d'une appliance NetScaler. Copiez le certificat sur l'appliance à l'aide d'un utilitaire de copie sécurisé tel que SCP.
2. Accédez au shell BSD et convertissez le certificat (par exemple, Cert.pfx) au format .PEM :

```
root@ns# openssl pkcs12 -in cert.PFX -out cert.PEM
<!--NeedCopy-->
```

3. Pour vous assurer que le certificat converti est au bon format x509, vérifiez que la commande suivante ne génère aucune erreur :

```
root@ns# openssl x509 -in cert.PEM -text
<!--NeedCopy-->
```

4. Vérifiez que le fichier de certificat contient une clé privée. Commencez par exécuter la commande suivante :

```
root@ns# cat cert.PEM

Verify that the output file includes an RSA PRIVATE KEY section.

-----BEGIN RSA PRIVATE KEY-----
Mkm^s9KMs9023pz/s...
-----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

Voici un autre exemple de section RSA PRIVATE KEY :

```
    Bag Attributes
    1.3.6.1.4.1.311.17.2: <No Values>
    localKeyID: 01 00 00 00
    Microsoft CSP Name: Microsoft RSA SChannel Cryptographic
    Provider
    friendlyName:
    4b9cef4cc8c9b849ff5c662fd3e0ef7e_76267e3e-6183-4d45-886e-6
       e067297b38f

    Key Attributes
    X509v3 Key Usage: 10
    -----BEGIN RSA PRIVATE KEY-----
    Proc-Type: 4,ENCRYPTED
    DEK-Info: DES-EDE3-CBC,43E7ACA5F4423968
```



```
    pZJ2SfsSVqMbRRf6ug37Clua5gY0Wld4frPIxFXyJquUHr31dilW5ta3hbIaQ+
        Rg

    ... (more random characters)
    v8dMugeRplkaH2Uwt/mWBk4t71Yv7GeHmcmjafK8H8iW80ooPO3D/ENV8X4U/
        tlh

    5eU6ky3WYZ1BTy6thxxLlwAullynVXZEflNLxq1oX+ZYl6djgjE3qg==
    -----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

Voici une section CERTIFICAT DE SERVEUR :

```
    Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: AG Certificate
    subject=/C=AU/ST=NSW/L=Wanniassa/O=Dave Mother
    Asiapacific/OU=Support/CN=davemother.food.lan
    issuer=/DC=lan/DC=food/CN=hotdog
    -----BEGIN CERTIFICATE-----
    MIIFiTCCBHGgAwIBAgIKCGryDgAAAAAHzANBgkqhkiG9w0BAQUFADA8MRMwEQYK


    ... (more random characters) 5
        pLDWYVHhLkA1pSxvFjNJHRSIydWHc5ltGyKqIUcBezVaXyel94pNSUYx07NpPV
        /

    MY2ovQyQZM8gGe3+lGFum0VHbv/y/gB9HhFesog=
    -----END CERTIFICATE-----
<!--NeedCopy-->
```

La section suivante contient un CERTIFICAT DE CA INTERMÉDIAIRE :

```
    Bag Attributes: <Empty Attributes>
    subject=/DC=lan/DC=food/CN=hotdog
    issuer=/DC=lan/DC=food/CN=hotdog
    -----BEGIN CERTIFICATE-----
    MIIESDCCAzCgAwIBAgIQah20fCRYTY9LRXYMIRaKGjANBgkqhkiG9w0BAQUFADA8


    ... (more random characters)
        Nt0nksawDnbKo86rQcNnY5xUs7c7pj2zxj/IOsgNHUp5W6dDI9pQoqFFaDk
        =

    -----END CERTIFICATE-----
```



```
<!--NeedCopy-->
```

D’autres certificats CA intermédiaires peuvent suivre, en fonction du chemin de certification du certificat exporté.

5. Ouvrez le fichier .PEM dans un éditeur de texte
6. Localisez la première ligne du fichier .PEM et la première instance de la ligne suivante, puis copiez ces deux lignes et toutes les lignes qui les séparent :

```
-----END CERTIFICATE-----

Note: Make sure that last copied line is the first
-----END CERTIFICATE----- line in the .PEM file.

<!--NeedCopy-->
```

7. Collez les lignes copiées dans un nouveau fichier. Appelez le nouveau fichier de manière intuitive, par exemple cert-key.pem. Cette paire de clés de certificat est destinée au serveur hébergeant le service HTTPS. Ce fichier doit contenir à la fois la section intitulée RSA PRIVATE KEY et la section intitulée SERVER CERTIFICATE dans l’exemple précédent.

   Remarque : Le fichier de paire de clés de certificat contient la clé privée et doit être conservé en toute sécurité.

8. Localisez toutes les sections suivantes commençant par —BEGIN CERTIFICATE— et se terminant par —END CERTIFICATE—, et copiez chacune de ces sections dans un nouveau fichier distinct.

   Ces sections correspondent aux certificats des autorités de certification fiables qui ont été inclus dans le parcours de certification. Ces sections doivent être copiées et collées dans de nouveaux fichiers individuels pour ces certificats. Par exemple, la section INTERMEDIATE CA CERTIFICATE de l’exemple précédent doit être copiée et collée dans un nouveau fichier).

   Pour plusieurs certificats d’autorité de certification intermédiaires dans le fichier d’origine, créez des fichiers pour chaque certificat d’autorité de certification intermédiaire dans l’ordre dans lequel ils apparaissent dans le fichier. Gardez une trace (en utilisant des noms de fichiers appropriés) de l’ordre dans lequel les certificats apparaissent, car ils doivent être liés entre eux dans le bon ordre lors d’une étape ultérieure.

9. Copiez le fichier de clé de certificat (cert-key.pem) et tous les fichiers de certificat CA supplémentaires dans le répertoire /nsconfig/ssl de l’appliance NetScaler.
10. Quittez le shell BSD et accédez à l’invite NetScaler.
11. Suivez les étapes de la section « Installer les fichiers de clé de certificat sur l’appliance » pour installer la clé/le certificat une fois chargé sur l’appareil.

Comment convertir le certificat PKCS #7 et l'installer sur l'appliance NetScaler ?

Vous pouvez utiliser OpenSSL pour convertir un certificat PKCS #7 en un format reconnaissable par l'appliance NetScaler. La procédure est identique à celle des certificats PKCS #12, sauf que vous appelez OpenSSL avec des paramètres différents. Les étapes de conversion des certificats PKCS #7 sont les suivantes :

1. Copiez le certificat sur l'appliance à l'aide d'un utilitaire de copie sécurisé, tel que SCP.
2. Convertissez le certificat (par exemple, Cert.P7b) au format PEM :

```
1 openssl pkcs7 -inform DER -in cert.p7b -print_certs -text -out
     cert.pem
2 <!--NeedCopy-->
```

3. Suivez les étapes 3 à 7 décrites dans la réponse pour les certificats PKCS #12.
   Remarque : Avant de charger le certificat PKCS #7 converti sur l'appliance, vérifiez qu'il contient une clé privée, exactement comme décrit à l'étape 3 pour la procédure PKCS #12. Les certificats PKCS #7, en particulier les certificats exportés depuis IIS, ne contiennent généralement pas de clé privée.

Lorsque je lie un chiffrement à un serveur ou à un service virtuel à l'aide de la commande bind cipher, le message d'erreur « Commande obsolète » s'affiche. « ?

La commande permettant de lier un chiffrement à un serveur ou à un service virtuel a changé.

Utilisez la `bind ssl vserver <vsername> -ciphername <ciphername>` commande pour lier un chiffrement SSL à un serveur virtuel SSL.

Utilisez la `bind ssl service <serviceName> -ciphername <ciphername>` commande pour lier un chiffrement SSL à un service SSL.

Remarque : Les nouveaux chiffrements et groupes de chiffrement sont ajoutés à la liste existante et ne sont pas remplacés.

Pourquoi ne puis-je pas créer un groupe de chiffrement et y lier des chiffrements à l'aide de la commande add cipher ?

La fonctionnalité d'ajout de la commande de chiffrement a été modifiée dans la version 10. La commande crée uniquement un groupe de chiffrement. Pour ajouter des chiffrements au groupe, utilisez la commande bind cipher.

OpenSSL

Comment utiliser OpenSSL pour convertir des certificats entre PEM et DER ?

Pour utiliser OpenSSL, vous devez disposer d'une installation fonctionnelle du logiciel OpenSSL et pouvoir exécuter OpenSSL à partir de la ligne de commande.

Les certificats x509 et les clés RSA peuvent être stockés dans différents formats.

Les deux formats courants sont les suivants :

- DER (format binaire utilisé principalement par les plateformes Java et Macintosh)
- PEM (représentation en base64 de DER avec des informations d'en-tête et de pied de page, principalement utilisée par les plateformes UNIX et Linux).

Une clé et le certificat correspondant, en plus du certificat racine et de tout certificat intermédiaire, peuvent également être stockés dans un seul fichier PKCS #12 (.P12, .PFX).

Procédure

Utilisez la commande **OpenSSL** pour effectuer la conversion entre les formats comme suit :

1. Pour convertir un certificat PEM en DER :

```
x509 -in input.crt -inform PEM -out output.crt -outform DER
<!--NeedCopy-->
```

2. Pour convertir un certificat DER en PEM :

```
x509 -in input.crt -inform DER -out output.crt -outform PEM
<!--NeedCopy-->
```

3. Pour convertir une clé de PEM en DER :

```
rsa -in input.key -inform PEM -out output.key -outform DER
<!--NeedCopy-->
```

4. Pour convertir une clé de DER en PEM :

```
rsa -in input.key -inform DER -out output.key -outform PEM
<!--NeedCopy-->
```

Remarque : Si la clé que vous importez est cryptée à l'aide d'un chiffrement symétrique compatible, vous êtes invité à saisir la phrase secrète.

Remarque : Pour convertir une clé vers ou depuis le format obsolète NET (serveur Netscape), remplacez NET par PEM ou DER selon le cas. La clé stockée est cryptée dans un chiffrement symétrique RC4 faible et non salé, de sorte qu'une phrase de passe est demandée. Une phrase de passe vide est acceptable.

Limites du système

Quels sont les chiffres importants à retenir ?

1. Créer une demande de certificat :
    - Nom du fichier de demande : 63 caractères maximum
    - Nom du fichier clé : 63 caractères maximum
    - Phrase secrète PEM (pour clé cryptée) : 31 caractères maximum
    - Nom commun : 63 caractères maximum
    - Ville : 127 caractères maximum
    - Nom de l'organisation : 63 caractères maximum
    - Nom de l'État/de la province : 63 caractères maximum
    - Adresse e-mail : 255 caractères maximum
    - Unité d'organisation : 63 caractères maximum
    - Mot de passe du défi : 20 caractères maximum
    - Nom de l'entreprise : 127 caractères maximum
2. Créer un certificat :
    - Nom du fichier de certificat : 63 caractères maximum
    - Nom du fichier de demande de certificat : 63 caractères maximum
    - Nom du fichier clé : 63 caractères maximum
    - Phrase secrète PEM : 31 caractères maximum
    - Période de validité : maximum 3650 jours
    - Nom du fichier de certificat CA : 63 caractères maximum
    - Nom du fichier de clé CA : 63 caractères maximum
    - Phrase secrète PEM : 31 caractères maximum
    - Fichier contenant le numéro de série CA : 63 caractères maximum
3. Créez et installez un certificat de test de serveur :
    - Nom du fichier de certificat : 31 caractères maximum
    - Nom de domaine complet : 63 caractères maximum
4. Créez une clé Diffie-Hellman (DH) :
    - Nom du fichier DH (avec chemin) : 63 caractères maximum
    - Taille du paramètre DH : maximum 2048 bits
5. Importer la clé PKCS12 :
    - Nom du fichier de sortie : 63 caractères maximum
    - Nom du fichier PKCS12 : 63 caractères maximum
    - Mot de passe d'importation : 31 caractères maximum
    - Phrase secrète PEM : 31 caractères maximum

- Vérifier le mot de passe PEM : 31 caractères maximum

6. Exporter PKCS12
    - Nom du fichier PKCS12 : 63 caractères maximum
    - Nom du fichier de certificat : 63 caractères maximum
    - Nom du fichier clé : 63 caractères maximum
    - Mot de passe d'exportation : 31 caractères maximum
    - Phrase secrète PEM : 31 caractères maximum
7. Gestion des CRL :
    - Nom du fichier de certificat CA : 63 caractères maximum
    - Nom du fichier de clé CA : 63 caractères maximum
    - Mot de passe du fichier clé CA : 31 caractères maximum
    - Nom du fichier d'index : 63 caractères maximum
    - Nom du fichier de certificat : 63 caractères maximum
8. Créez une clé RSA :
    - Nom du fichier clé : 63 caractères maximum
    - Taille de clé : 4 096 bits maximum
    - Phrase secrète PEM : 31 caractères maximum
    - Vérifier le mot de passe : 31 caractères maximum
9. Modifiez les paramètres SSL avancés :
    - Taille de mémoire CRL maximale : 1024 Mo maximum
    - Délai d'expiration du déclencheur du chiffrement (10 mS) : 200 maximum
    - Nombre de paquets déclencheurs de chiffrement : 50 maximum
    - Taille du cache OCSP : 512 Mo maximum
10. Certificat d'installation :
    - Nom de la paire de clés de certificat : 31 caractères maximum
    - Nom du fichier de certificat : 63 caractères maximum
    - Nom du fichier de clé privée : 63 caractères maximum
    - Mot de passe : 31 caractères maximum
    - Période de notification : 100 maximum
11. Créez un groupe de chiffrement :
    - Nom du groupe de chiffrement : 39 caractères maximum
12. Créez une CRL :
    - Nom CRL : 31 caractères maximum
    - Fichier CRL : 63 caractères maximum
    - URL : 127 caractères maximum

- DN de base : 127 caractères maximum
- Bind DN : 127 caractères maximum
- Mot de passe : 31 caractères maximum
- Nombre de jours : 31 jours maximum

13. Créez une politique SSL :
    - Nom : 127 caractères maximum
14. Créer une action SSL :
    - Nom : 127 caractères maximum
15. Créez un répondeur OCSP :
    - Nom : 32 caractères maximum
    - URL : 128 caractères maximum
    - Profondeur de dosage : 8 maximum
    - Délai de traitement par lots : maximum 10 000
    - Sticisme de production à la fois : 86 400 au maximum
    - Délai d'expiration de la demande : 120 000 maximum
16. Créez un serveur virtuel :
    - Nom : 127 caractères maximum
    - URL de redirection : 127 caractères maximum
    - Délai d'expiration du client : 3 1536 000 secondes maximum
17. Créer un service :
    - Nom : 127 caractères maximum
    - Délai d'inactivité (secondes) :
      Client : 31536000 maximum
      Serveur : 31536000 maximum
18. Créer un groupe de services :
    - Nom du groupe de services : 127 caractères maximum
    - ID du serveur : Maximum 4294967295
    - Délai d'inactivité (secondes) :
      Client : valeur maximale 31536000
      Serveur : maximum 31536000
19. Créer un moniteur :
    - Nom : 31 caractères maximum
20. Créer un serveur :
    - Nom du serveur : 127 caractères maximum

- Nom de domaine : 255 caractères maximum
- Résoudre une nouvelle tentative : 20 939 secondes maximum

Inspection du contenu

May 5, 2023

Ces derniers temps, les types d'appareils permettant d'afficher divers contenus multimédia se sont développés. Les types d'appareils peuvent être des téléphones mobiles, des tablettes et des ordinateurs de bureau. Les fournisseurs d'infrastructures intermédiaires doivent transformer le contenu original d'un serveur Web en un format adapté à l'appareil qui demande le contenu. Les appareils externes inspectent le contenu qui est transcodant et le renvoient au client. Le protocole le plus couramment utilisé pour y parvenir est l'ICAP. L'ICAP permet de placer l'appliance NetScaler dans différents déploiements. L'ICAP utilise la technique d'inspection du contenu qui inspecte les données pour détecter les malwares et les problèmes de sécurité.

> **Remarque**
>
> HTTP/2 n'est pas compatible avec l'inspection du contenu. Les applications utilisant HTTP/2 peuvent ne pas fonctionner correctement si le trafic est envoyé via l'inspection du contenu.

ICAP pour l'inspection de contenu à distance

May 5, 2023

Le protocole ICAP (Internet Content Adaptation Protocol) est un protocole léger simple permettant d'exécuter le service de transformation à valeur ajoutée sur les messages HTTP. Dans un scénario typique, un client ICAP transmet les requêtes et les réponses HTTP à un ou plusieurs serveurs ICAP pour traitement. Les serveurs ICAP effectuent la transformation du contenu des demandes et renvoient les réponses avec les mesures appropriées à prendre pour la demande ou la réponse.

ICAP sur une appliance NetScaler

Dans une configuration NetScaler, l'appliance agit comme un client ICAP interagissant avec des serveurs ICAP tiers (tels que la protection contre les programmes malveillants et la protection contre la perte de données (DLP)). Lorsque l'appliance reçoit un trafic Web entrant, elle intercepte le trafic et utilise une stratégie d'inspection du contenu pour évaluer si la requête HTTP nécessite un traitement ICAP. Si c'est le cas, l'appliance déchiffre et envoie le message sous forme de texte brut aux serveurs ICAP. Les serveurs ICAP exécutent le service de transformation de contenu sur le

message de demande et renvoient une réponse à l'appliance. Les messages adaptés peuvent être une requête HTTP ou une réponse HTTP. Si l'appliance interagit avec plusieurs serveurs ICAP, elle effectue l'équilibrage de charge des serveurs ICAP. Ce scénario se produit lorsqu'un seul serveur ICAP n'est pas suffisant pour gérer la totalité du trafic. Une fois que les serveurs ICAP ont renvoyé un message modifié, l'appliance transmet le message modifié au serveur d'origine principal.

L'appliance NetScaler fournit également un service ICAP sécurisé si le trafic entrant est de type HTTPS. L'appliance utilise un service TCP basé sur SSL pour établir une connexion sécurisée entre l'appliance et les serveurs ICAP.

Fonctionnement de la modification de requête ICAP (REQMOD)

En mode modification de la demande (REQMOD), l'appliance NetScaler transmet la requête HTTP reçue du client au serveur ICAP. Le serveur ICAP effectue ensuite l'une des opérations suivantes :

1. Renvoie une version modifiée de la demande et l'appliance envoie à son tour la demande modifiée au serveur d'origine principal ou achemine la demande modifiée vers un autre serveur ICAP.
2. Répond par un message indiquant qu'aucune adaptation n'est requise.
3. Renvoie une erreur et l'appliance renvoie le message d'erreur à l'utilisateur.

Fonctionnement de la modification de réponse ICAP (RESPMOD)

En mode modification de la réponse (RESPMOD), l'appliance NetScaler envoie une réponse HTTP au serveur ICAP (la réponse envoyée par l'appliance est généralement la réponse envoyée par le serveur d'origine). Le serveur ICAP effectue ensuite l'une des opérations suivantes :

1. Envoie une version modifiée de la réponse et l'appliance envoie à son tour la réponse à l'utilisateur ou achemine la réponse vers un autre serveur ICAP.
2. Répond par un message indiquant qu'aucune adaptation n'est requise.
3. Renvoie une erreur et l'appliance envoie à son tour le message d'erreur à l'utilisateur.

Licence ICAP

La fonctionnalité ICAP fonctionne sur une configuration NetScaler autonome ou à haute disponibilité avec l'édition de licence NetScaler Premium ou Advanced.

Configurer ICAP pour le service de transformation de contenu

Pour utiliser ICAP pour le service de transformation de contenu, vous devez d'abord activer les fonctionnalités d'inspection du contenu et d'équilibrage de charge. Une fois les fonctionnalités activées, vous pouvez effectuer les tâches suivantes :

Pour activer l'inspection du contenu

Si vous souhaitez que l'appliance NetScaler agisse en tant que client ICAP, vous devez d'abord activer les fonctionnalités d'inspection du contenu et d'équilibrage de charge.

À l'invite de commande, tapez :

```
enable ns feature contentInspection LoadBalancing
<!--NeedCopy-->
```

Ajouter un profil ICAP

Les configurations ICAP d'une appliance NetScaler sont spécifiées dans une entité appelée profil ICAP. Le profil possède un ensemble de paramètres ICAP. Les paramètres comprennent des paramètres permettant de générer dynamiquement une demande ICAP, de recevoir la réponse ICAP et de consigner les données d'inspection de contenu.

Pour générer dynamiquement une requête ICAP au serveur ICAP, un nouveau paramètre, « InsertHttpRequest », est ajouté au profil ICAP. Si ce paramètre est configuré, l'appliance prend la valeur configurée en tant qu'expression de stratégie, évalue l'expression et inclut le résultat sous forme de requête ou de réponse HTTP encapsulée, puis l'envoie au serveur ICAP. En outre, un nouveau paramètre « InsertiCapHeaders » est configurable pour évaluer et inclure dynamiquement les en-têtes ICAP.

Lorsque l'appliance envoie une demande ICAP sans recevoir de réponse au serveur ICAP, la connexion cesse de répondre. Cela se produit jusqu'à ce que le serveur ICAP envoie une réponse ou qu'une session soit libérée. Ce comportement peut être géré en configurant l'option de délai d'expiration de réponse ICAP. Vous pouvez définir un paramètre de délai d'expiration de la demande pour l'action en cas de réponse ICAP retardée. Si l'appliance NetScaler ne reçoit pas de réponse dans le délai de demande configuré, l'action de délai de demande est exécutée.

ReqTimeoutAction : les valeurs possibles sont BYPASS, RESET, DROP.
BYPASS : Cela ignore la réponse du serveur ICAP distant et envoie la requête/réponse au client/serveur.
RESET (par défaut) : Réinitialisez la connexion client en la fermant.
DROP : supprime la demande sans envoyer de réponse à l'utilisateur

Pour évaluer une réponse ICAP, une nouvelle expression de stratégie `ICAP.RES` est utilisée dans l'expression de retour de légende d'inspection de contenu. Cette expression évalue la réponse ICAP de la même manière que l'expression `HTTP.RES` dans `HTTP_CALLOUT`.

Par exemple, lorsqu'une appliance NetScaler reçoit une requête HTTP pour un service hébergé derrière l'adresse IP virtuelle NetScaler, l'appliance peut être amenée à vérifier l'authentification du client auprès d'un serveur externe et à prendre une mesure.

À l'invite de commande, tapez :

```
add ns icapProfile <name> [-preview ( ENABLED | DISABLED )][-previewLength
 <positive_integer>] -uri <string> [-hostHeader <string>] [-userAgent <
string>] -Mode ( REQMOD | RESPMOD )[-queryParams <string>] [-connectionKeepAlive
 ( ENABLED | DISABLED )][-allow204 ( ENABLED | DISABLED )] [-insertICAPHeaders
 <string>][-insertHTTPRequest <string>] [-reqTimeout <positive_integer>][-
reqTimeoutAction <reqTimeoutAction>] [-logAction <string>]
```

Exemple :

```
add icapprofile reqmod-profile -mode RESPMOD -uri  “/req_scan”  -hostHeader
 “Webroot.reqsca”  -useragent  “NS_SWG-Proxy”
```

```
add ns icapProfile icap_prof1 -uri "/example"-Mode REQMOD -reqtimeout 4 -
reqtimeoutaction BYPASS
```

```
> add icapProfile reqmode-profile -uri '/example'-mode REQMOD -insertHTTPRequest
 q{ HTTP.REQ.METHOD + ""+ HTTP.REQ.URL + "HTTP/1.1\r\n"+ "Host: "+ HTTP.REQ
.HOSTNAME + "\r\n\r\n"}
```

Consigner l'action d'inspection du contenu ICAP

Pour générer dynamiquement des enregistrements de flux de journaux d'inspection de contenu ou des journaux SYSLOG, vous pouvez utiliser l'expression de stratégie basée sur ICAP.RES sur la réponse ICAP. Ce paramètre est configurable dans le profil ICAP pour configurer l'expression de stratégie afin de générer les enregistrements de journaux dynamiques.

À l'invite de commande, tapez :

```
add audit messageaction icap_log_expr INFORMATIONAL icap.res.full_header
```

```
set icapProfile reqmode-profile -logAction messageaction
```

Ajouter un service ICAP en tant que service TCP ou SSL_TCP

Après avoir activé la fonction d'inspection de contenu, vous devez ajouter un service ICAP pour les serveurs ICAP qui feront partie de la configuration de l'équilibrage de charge. Le service que vous ajoutez fournit la connexion ICAP entre l'appliance NetScaler et les serveurs virtuels d'équilibrage de charge.

Remarque : En tant qu'administrateur, vous pouvez ajouter un service ICAP et configurer directement l'adresse IP du serveur ICAP dans l'action Inspection du contenu.

À l'invite de commandes, tapez ce qui suit :


```
add service <name> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add service icapsv1 10.10.10.10 SSL_TCP 1345
add service icapsv2 10.10.10.11 SSL_TCP 1345
```

Ajouter un serveur virtuel d'équilibrage de charge basé sur TCP ou SSL_TCP

Après avoir créé un service ICAP, vous devez créer un serveur virtuel pour accepter le trafic ICAP et équilibrer la charge des serveurs ICAP.

> **Remarque :**
>
> Vous pouvez également utiliser un service TCP basé sur SSL sur un canal sécurisé. Vous utilisez un service SSL_TCP et vous vous liez à l'action Inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver vicap TCP 0.0.0.0 - persistenceType NONE -cltTimeout
    9000

add lb vserver vicap SSL_TCP 0.0.0.0 0 - persistenceType NONE -
    cltTimeout 9000
<!--NeedCopy-->
```

Liez le service ICAP au serveur virtuel d'équilibrage de charge

Après avoir créé un service ICAP et un serveur virtuel, vous devez lier le service ICAP au serveur virtuel.

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver vicap icapsv1
<!--NeedCopy-->
```


Ajouter une action d'inspection de contenu

Après avoir activé la fonction d'inspection du contenu, vous devez ajouter une action ICAP pour gérer les informations de demande ICAP. Le profil et les services ICAP, ou le serveur virtuel d'équilibrage de charge qui sont créés, sont liés à l'action ICAP. Si le serveur ICAP est en panne, vous pouvez configurer le paramètre `ifserverdown` pour que l'appliance exécute l'une des actions suivantes.

CONTINUER : Si l'utilisateur souhaite contourner l'inspection du contenu lorsque le serveur distant est en panne, vous pouvez choisir l'action « CONTINUER », par défaut.
RESET (par défaut) : Cette action répond au client en fermant la connexion avec RST.
DROP : Cette action supprime silencieusement les paquets sans envoyer de réponse à l'utilisateur.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection action <name> -type ICAP -serverName <string> -
    icapProfileName <string>

add ContentInspection action <name> -type ICAP -serverip <ip> -
    serverport <port> -icapProfileName <string>
<!--NeedCopy-->
```

> **Remarque :**
>
> Si vous pouvez configurer le service ICAP au lieu d'un serveur virtuel d'équilibrage de charge, vous pouvez mentionner le nom du service dans l'option \<-serverip>. Lors de l'ajout de l'action Inspection de contenu, le service TCP est automatiquement créé pour l'adresse IP donnée avec le port 1344 et il est utilisé pour la communication ICAP.

Exemple :

```
add ContentInspection action ci_act_lb -type ICAP -serverName vicap -
    icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverName icapsv1
    -icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverip 1.1.1.1 -
    serverport 1344 -icapProfileName icap_reqmod
<!--NeedCopy-->
```

Ajouter des politiques d'inspection de contenu

Après avoir créé une action Inspection de contenu, vous devez créer des stratégies d'inspection de contenu pour évaluer les demandes de traitement ICAP et de journalisation d'audit. La stratégie est basée

sur une règle qui consiste en une ou plusieurs expressions. La règle est associée à l'action d'inspection du contenu qui est associée si une demande correspond à la règle.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Exemple :

```
add ContentInspection policy ci_pol_basic - rule true - action
    ci_act_svc

add ContentInspection policy ci_pol_HTTP - rule HTTP.REQ.URL.CONTAINS(
    "html" ) - action ci_act_svc
<!--NeedCopy-->
```

Liez les stratégies d'inspection de contenu au serveur virtuel de commutation de contenu ou d'équilibrage de charge

Pour appliquer une stratégie ICAP, vous devez la lier globalement ou la lier à un serveur virtuel de commutation de contenu ou d'équilibrage de charge, qui fait office d'interface avec l'application. Lorsque vous liez la stratégie, vous devez lui attribuer une priorité. La priorité détermine l'ordre dans lequel les stratégies que vous définissez sont évaluées.

> **Remarque :**
>
> Le serveur virtuel d'application doit être de type HTTP/SSL/CS-PROXY.

Pour plus d'informations sur la configuration d'une configuration d'équilibrage de charge pour le transfert du trafic vers le serveur d'origine principal après la transformation du contenu, reportez-vous à la section Équilibrage de charge.

Configurer le service ICAP sécurisé

Pour établir une connexion sécurisée entre l'appliance NetScaler et les serveurs Web ICAP, l'appliance utilise un service TCP basé sur SSL ou un serveur virtuel d'équilibrage de charge lié à une action ICAP.

Pour établir une connexion ICAP sécurisée, effectuez les tâches suivantes :

1. Ajoutez un service TCP basé sur SSL.
2. Liez le service TCP basé sur SSL au serveur virtuel d'équilibrage de charge de type TCP ou SSL_TCP.
3. Liez le service TCP basé sur SSL ou le serveur virtuel d'équilibrage de charge à l'action Content Inspection.

Ajouter un service TCP basé sur SSL au serveur virtuel d'équilibrage de charge

Pour établir une connexion sécurisée entre l'appliance NetScaler et les serveurs Web ICAP, l'appliance utilise un service TCP basé sur SSL ou un serveur virtuel d'équilibrage de charge lié à une action ICAP.

Pour établir une connexion ICAP sécurisée, effectuez les tâches suivantes :

1. Ajoutez un service TCP basé sur SSL.
2. Liez le service TCP basé sur SSL au serveur virtuel d'équilibrage de charge de type TCP ou SSL_TCP.

Liez le service TCP basé sur SSL ou le serveur virtuel d'équilibrage de charge à l'action Content Inspection

Ajouter un service TCP basé sur SSL au serveur virtuel d'équilibrage de charge

Après avoir activé la fonction d'inspection de contenu, vous devez ajouter un service ICAP sécurisé qui fera partie de la configuration de l'équilibrage de charge. Le service que vous ajoutez fournit une connexion ICAP sécurisée entre l'appliance NetScaler et les serveurs virtuels d'équilibrage de charge.

À l'invite de commandes, tapez ce qui suit :

```
add service <name> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Exemple :

```
add service icapsv2 10.102.29.200 SSL_TCP 1344 -gslb NONE -maxclient
    0 -maxReq 0 -cip DISABLED -usip NO -useproxport YES -sp ON -
    cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB NO -CMP NO
<!--NeedCopy-->
```

Liez le service TCP basé sur SSL au serveur virtuel d'équilibrage de charge SSL_TCP ou TCP

Après avoir créé un service ICAP sécurisé, vous devez lier le service au serveur virtuel d'équilibrage de charge. Elle est requise si vous utilisez un serveur virtuel d'équilibrage de charge pour équilibrer la charge des serveurs ICAP.

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Exemple :


```
bind lb vserver vicap icapsv2
<!--NeedCopy-->
```

Liez le service TCP basé sur SSL ou le serveur virtuel d'équilibrage de charge à l'action Content Inspection

Vous ajoutez une action ICAP pour gérer les informations de la demande ICAP et vous liez également le service TCP basé sur SSL à l'action.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection action <name> -type ICAP -serverName <string> -
    icapProfileName <string>
<!--NeedCopy-->
```

Exemple :

```
add ContentInspection action ci_act_svc -type ICAP -serverName icapsv2
    -icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverName vicap -
    icapProfileName icap_reqmod
<!--NeedCopy-->
```

Configurer le protocole ICAP à l'aide de l'interface graphique

1. Accédez à **Équilibrage de charge** > **Services** et cliquez sur **Ajouter**.
2. Sur la page **Services**, entrez les détails du service.
3. Accédez à **Équilibrage de charge** > **Serveurs virtuels**. Ajoutez un serveur virtuel d'équilibrage de charge de type HTTP/SSL. Vous pouvez également sélectionner un serveur virtuel et cliquer sur **Modifier**.
4. Après avoir saisi les informations de base du serveur, cliquez sur **Continuer**.
5. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
6. Accédez à la section **Stratégies** et cliquez sur l'icône en forme de **crayon** pour configurer la stratégie d'inspection du contenu.
7. Sur la page **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.
8. Dans la section **Liaison de stratégie**, cliquez **sur+** pour ajouter une stratégie d'inspection du contenu.
9. Dans la page **Créer une stratégie ICAP**, entrez un nom pour la stratégie.
10. Dans le champ **Action**, cliquez sur le signe « + » pour ajouter une action ICAP.
11. Dans la page **Créer une action ICAP**, entrez le nom de l'action.

12. Entrez le nom de l'action.
13. Dans le champ **Nom du serveur**, entrez le nom du service TCP déjà créé.
14. Dans le champ **Profil ICAP**, cliquez sur le signe « + » pour ajouter un profil ICAP.
15. Dans la page **Créer un profil ICAP**, entrez un nom de profil, un URI et MODE.
16. Cliquez sur **Create**.
17. Dans la page **Créer une action ICAP**, cliquez sur **Créer**.
18. Dans la page **Créer une stratégie ICAP**, entrez « true » dans l' **éditeur d'expression**, puis cliquez sur **Créer**.
19. Cliquez sur **Bind**.
20. Lorsque vous êtes invité à activer la fonction d'inspection du contenu, cliquez sur **Oui**.
21. Cliquez sur **Terminé**.

Pour plus d'informations sur la configuration de l'interface graphique NetScaler pour l'équilibrage de charge et le transfert du trafic vers le serveur d'origine principal après la transformation du contenu, consultez la section Équilibrage de charge.

Configurer le protocole ICAP sécurisé à l'aide de l'interface graphique

1. Accédez à **Équilibrage de charge** > **Services** et cliquez sur **Ajouter**.
2. Sur la page **Services**, entrez les détails du service.
3. Accédez à **Équilibrage de charge** > **Serveurs virtuels**. Ajoutez un serveur virtuel de type HTTP/SSL. Vous pouvez également sélectionner un serveur virtuel et cliquer sur **Modifier**.
4. Après avoir saisi les informations de base du serveur, cliquez sur **Continuer**.
5. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
6. Accédez à la section **Stratégies** et cliquez sur l'icône en forme de **crayon** pour configurer la stratégie d'inspection du contenu.
7. Sur la page **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.
8. Dans la section **Liaison de stratégie**, cliquez **sur+** pour ajouter une stratégie d'inspection du contenu.
9. Dans la page **Créer une stratégie ICAP**, entrez un nom pour la stratégie.
10. Dans le champ **Action**, cliquez sur le signe « + » pour ajouter une action ICAP.
11. Dans la page **Créer une action ICAP**, entrez le nom de l'action.
12. Entrez le nom de l'action.
13. Dans le champ **Nom du serveur**, entrez le nom du service TCP_SSL déjà créé.
14. Dans le champ **Profil ICAP**, cliquez sur le signe « + » pour ajouter un profil ICAP.
15. Dans la page **Créer un profil ICAP**, entrez un nom de profil, un URI et MODE.
16. Cliquez sur **Create**.
17. Dans la page **Créer une action ICAP**, cliquez sur **Créer**.
18. Dans la page **Créer une stratégie ICAP**, entrez « true » dans l' **éditeur d'expression**, puis cliquez sur **Créer**.

19. Cliquez sur **Bind**.
20. Lorsque vous êtes invité à activer la fonction d'inspection du contenu, cliquez sur **Oui**.
21. Cliquez sur **Terminé**.

Prise en charge des journaux d'audit pour l'inspection à

Si le contenu d'une demande entrante ou d'une réponse sortante est inspecté, l'appliance NetScaler enregistre les détails ICAP. L'appliance stocke les détails sous forme de message de journal dans le fichier ns.log.

Chaque message de journal contient généralement les informations suivantes :

```
<Source IP> <Destination IP> <Domain> <ICAP server IP><ICAP Mode> <
    Service URI> <ICAP response> <Policy action>
<!--NeedCopy-->
```

Restriction : le mode streaming d'App Firewall n'est pas pris en charge avec la fonction d'inspection de contenu.

Exemple de message de journal de requêtes inspecté par le contenu :

```
Apr 18 14:45:41 <local0.info> 10.106.97.104 04/18/2018:14:45:41 GMT 0-
    PPE-0 : default CI ICAP_LOG 788 0 : Source 10.102.1.98:39048 -
    Destination 10.106.97.89:8011 - Domain 10.106.97.89 - Content-Type
    application/x-www-form-urlencoded - ICAP Server 10.106.97.99:1344 -
    Mode REQMOD - Service /example - Response 204 - Action FORWARD
<!--NeedCopy-->
```

Exemple de message du journal des réponses inspecté par le contenu :

```
Apr 18 12:34:08 <local0.info> 10.106.97.104 04/18/2018:12:34:08 GMT 0-
    PPE-0 : default CI ICAP_LOG 71 0 : Source 10.106.97.105:18552 -
    Destination 10.106.97.99:80 - Domain NA - Content-Type NA - ICAP
    Server 10.106.97.99:1344 - Mode RESPMOD - Service /example -
    Response 400 - Action Internal Error
<!--NeedCopy-->
```

Intégration en ligne des appareils avec NetScaler

May 5, 2023

Les dispositifs de sécurité tels que le système de prévention des intrusions (IPS) et le pare-feu de nouvelle génération (NGFW) protègent les serveurs contre les attaques réseau. Ces appareils sont dé-

ployés en mode ligne de couche 2 et leur fonction principale est de protéger les serveurs contre les attaques réseau et de signaler les menaces de sécurité sur le réseau.

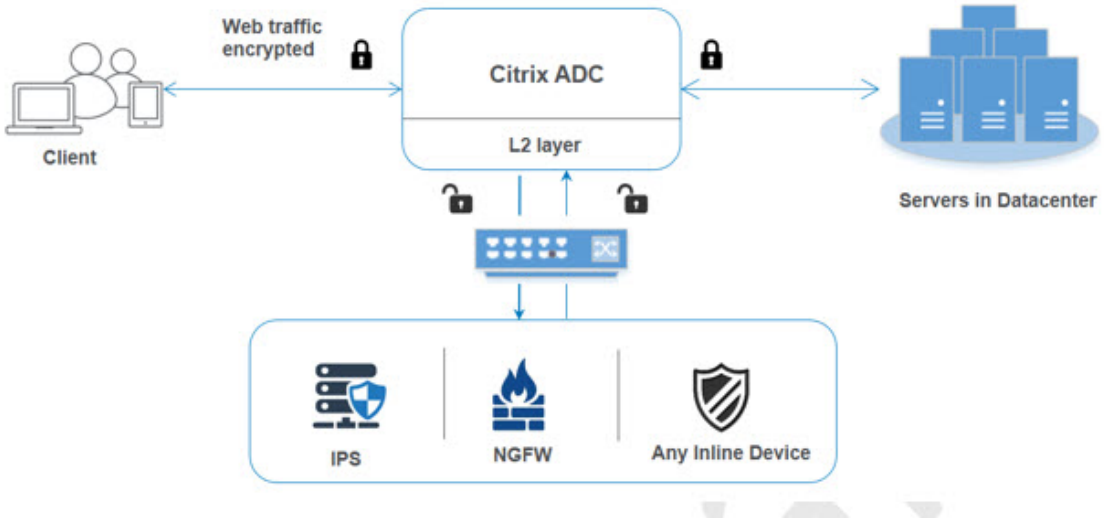
Pour prévenir les menaces vulnérables et fournir une protection de sécurité avancée, une appliance NetScaler est intégrée à un ou plusieurs appareils en ligne. Les appareils en ligne peuvent être n'importe quel dispositif de sécurité tel que IPS, NGFW.

Voici certains des cas d'utilisation qui bénéficient de l'intégration en ligne des appareils avec l'appliance NetScaler :

- **Inspection du trafic chiffré**. La plupart des appliances IPS et NGFW contournent le trafic crypté, rendant ainsi les serveurs vulnérables aux attaques. Une appliance NetScaler peut déchiffrer le trafic et l'envoyer à des appareils en ligne pour inspection. Elle renforce la sécurité du réseau du client.
- **Déchargement des appareils en ligne du traitement TLS/SSL**. Le traitement TLS/SSL est coûteux et le problème peut entraîner une augmentation du processeur du système dans les appliances IPS ou NGFW si elles déchiffrent le trafic. Le trafic chiffré augmentant rapidement, ces systèmes ne parviennent pas à déchiffrer et à inspecter le trafic chiffré. NetScaler permet de décharger les appareils en ligne du traitement TLS/SSL. Il en résulte que le dispositif en ligne prend en charge un volume élevé d'inspections du trafic.
- **Dispositifs d'équilibrage de charge en ligne.** L'appliance NetScaler équilibre la charge de plusieurs appareils en ligne lorsque le volume de trafic est élevé.
- **Sélection intelligente du trafic**. Le contenu de chaque paquet entrant dans l'appliance peut faire l'objet d'une inspection, par exemple le téléchargement de fichiers texte. L'utilisateur peut configurer l'appliance NetScaler pour sélectionner un trafic spécifique (par exemple, des fichiers .exe) à inspecter et envoyer le trafic à des appareils en ligne pour le traitement des données

Comment NetScaler est intégré aux appareils en ligne

Le schéma suivant montre comment NetScaler est intégré aux dispositifs de sécurité en ligne.



Lorsque vous intégrez des appareils en ligne à l'appliance NetScaler, le composant interagit comme suit :

1. Un client envoie une demande à l'appliance NetScaler.
2. L'appliance reçoit la demande et l'envoie à un appareil en ligne sur la base d'une évaluation des politiques.
   Remarque : S'il existe deux appareils en ligne ou plus, l'appliance équilibre la charge des appareils et envoie le trafic.
   Si le trafic entrant est chiffré, l'appliance déchiffre les données et les envoie sous forme de texte brut au périphérique en ligne pour inspection du contenu.
3. Le périphérique en ligne inspecte les données à la recherche de menaces et décide de supprimer, de réinitialiser ou de renvoyer les données à l'appliance.
4. S'il existe des menaces de sécurité, le périphérique modifie les données et les envoie à l'appliance.
5. NetScaler rechiffre à son tour les données et transmet la demande au serveur principal.
6. Le serveur principal envoie la réponse à l'appliance NetScaler.
7. L'appliance déchiffre à nouveau les données et les envoie au périphérique en ligne pour inspection.
8. L'appliance chiffre à nouveau les données et envoie la réponse au client

Licences logicielles

Pour déployer l'intégration des appareils en ligne, votre appliance NetScaler doit être provisionnée avec l'une des licences suivantes :

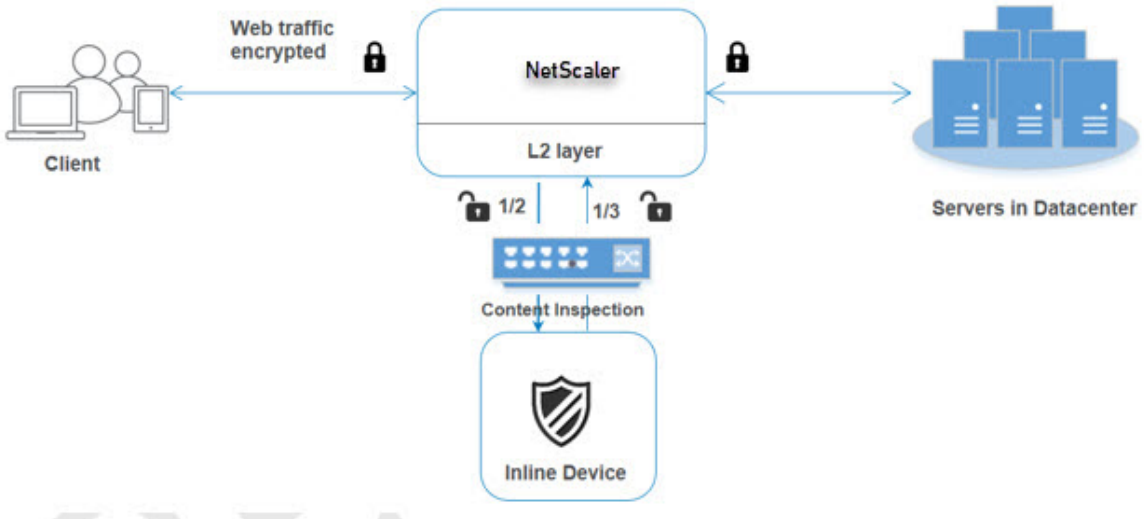
1. ADC Premium
2. ADC Avancé
3. Telco Advanced
4. Télécoms Premium
5. Licence SWG

Configuration de l'intégration de périphériques en ligne

Vous pouvez configurer une appliance NetScaler avec un appareil en ligne de trois manières différentes. Les scénarios de configuration sont les suivants.

Scénario 1 pour l'utilisation d'un seul appareil en ligne

Si vous souhaitez intégrer un dispositif de sécurité (IPS ou NGFW) en mode intégré, vous devez d'abord activer la fonctionnalité d'inspection du contenu et activer NetScaler dans MBF (transfert basé sur Mac) en mode global. Une fois que vous avez activé les fonctionnalités, vous devez ajouter le profil d'inspection du contenu, ajouter l'action d'inspection du contenu pour les appareils en ligne afin de réinitialiser, de bloquer ou de supprimer le trafic en fonction de l'inspection. Ajoutez ensuite la politique d'inspection du contenu pour l'appliance afin de décider quel sous-ensemble de trafic envoyer aux appareils en ligne. Configurez ensuite le serveur virtuel d'équilibrage de charge avec la connexion de couche 2 activée sur le serveur. Enfin, liez la politique d'inspection du contenu au serveur virtuel d'équilibrage de charge.



Activer le mode MBF (transfert basé sur Mac)

Si vous souhaitez que l'appliance NetScaler soit intégrée à des appareils en ligne tels que des solutions IPS ou des pare-feux, vous devez activer ce mode. Pour plus d'informations sur MBF, consultez la

rubrique Configurer le transfert sur Mac.

À l'invite de commande, tapez :

```
enable ns mode mbf
```

Activer l'inspection du contenu

Si vous souhaitez que l'appliance NetScaler déchiffre puis envoie le contenu pour inspection aux appareils en ligne, vous devez activer les fonctionnalités d'inspection du contenu et d'équilibrage de charge.

```
enable ns feature contentInspection LoadBalancing
```

Ajouter une méthode de connexion de couche 2

Pour gérer la réponse générée par les périphériques en ligne, l'appliance utilise le canal VLAN comme méthode de couche 2 (méthode L2ConnMethod) de communication avec les périphériques en ligne.

À l'invite de commande, tapez :

```
set l4param -l2ConnMethod <l2ConnMethod>
```

Exemple

```
set l4param -l2ConnMethod VlanChannel
```

Ajouter un profil d'inspection du contenu pour le service

La configuration des appareils en ligne pour une appliance NetScaler peut être spécifiée dans une entité appelée profil d'inspection du contenu. Le profil contient un ensemble de paramètres qui expliquent comment intégrer un appareil en ligne.

À l'invite de commande, tapez :

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface "1/2" -egressInterface "1/3"
```

Ajouter un moniteur IPS-TCP

Si vous souhaitez configurer des moniteurs, vous devez ajouter un moniteur défini par l'utilisateur.
Remarque : Si vous souhaitez configurer des moniteurs, vous devez utiliser un moniteur personnalisé. Lorsque vous ajoutez un moniteur, vous devez activer le paramètre transparent.

À l'invite de commande, tapez :

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr>] [-destPort
 <port>] [-transparent ( YES | NO )]
```

Exemple :

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

Ajouter un service

Ajoutez un service. Spécifiez une adresse IP fictive qui n'appartient à aucun des appareils, y compris les appareils en ligne. Réglez `use source IP address` (USIP) sur OUI. Réglez `useproxyport` sur NON. Par défaut, la surveillance de l'état est activée, liez le service à un moniteur de santé et définissez également l'option TRANSPARENT dans le moniteur sur ON. À l'invite de commande, tapez :

```
add service <Service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip ON -useproxyport OFF
```

Exemple :

```
add service ips_service 192.168.10.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```

Ajouter un moniteur de santé

Par défaut, le moniteur de santé est activé et vous avez également la possibilité de le désactiver, si nécessaire. À l'invite de commande, tapez :

```
add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent <
YES, NO>
```

Exemple :

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

Liez le service au moniteur de santé

Après avoir configuré le moniteur de santé, vous devez lier le service au moniteur de santé. À l'invite de commande, tapez :

```
bind service <name> -monitorName <name>
```

Exemple :

```
bind service ips_svc -monitorName ips_tcp
```


Ajouter une action d'inspection du contenu pour le service

Après avoir activé la fonctionnalité d'inspection du contenu, puis après avoir ajouté le profil et le service en ligne, vous devez ajouter l'action d'inspection du contenu pour traiter la demande. En fonction de l'action d'inspection du contenu, le dispositif en ligne peut supprimer, réinitialiser ou bloquer l'action après avoir inspecté les données.

Si le serveur ou le service Inline est en panne, vous pouvez configurer le `ifserverdown` paramètre dans l'appliance pour effectuer l'une des actions suivantes.

CONTINUER : Si l'utilisateur souhaite contourner l'inspection du contenu lorsque le serveur distant est en panne, vous pouvez choisir l'action « CONTINUER », par défaut.
RESET (par défaut) : Cette action répond au client en fermant la connexion avec RST.
DROP : Cette action supprime silencieusement les paquets sans envoyer de réponse à l'utilisateur.

À l'invite de commande, tapez :

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action <action_name> -type InlineINSPECTION -serverName
 Service_name/Vserver_name>
```

Exemple :

```
add ContentInspection action <Inline_action> -type InlineSPECTION -serverName
 Inline_service1
```

Ajouter une stratégie d'inspection du contenu pour l'inspection

Après avoir créé une action d'inspection du contenu, vous devez ajouter des stratégies d'inspection du contenu pour évaluer les demandes d'inspection. La stratégie est basée sur une règle qui consiste en une ou plusieurs expressions. La stratégie évalue et sélectionne le trafic à inspecter en fonction de la règle.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Exemple

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Pour recevoir le trafic Web, vous devez ajouter un serveur virtuel d'équilibrage de charge. Vous devez également activer la connexion layer2 sur le serveur virtuel.

À l'invite de commande, tapez :

```
add lb vserver <name> <vserver name> -l2Conn ON
```

Exemple :

```
add lb vserver HTTP_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Lier la stratégie d'inspection du contenu au serveur virtuel de commutation de contenu ou au serveur virtuel d'équilibrage de charge de type HTTP/SSL

Vous liez le serveur virtuel d'équilibrage de charge ou le serveur virtuel de commutation de contenu de type HTTP/SSL à la politique d'inspection du contenu.
À l'invite de commandes, tapez ce qui suit :

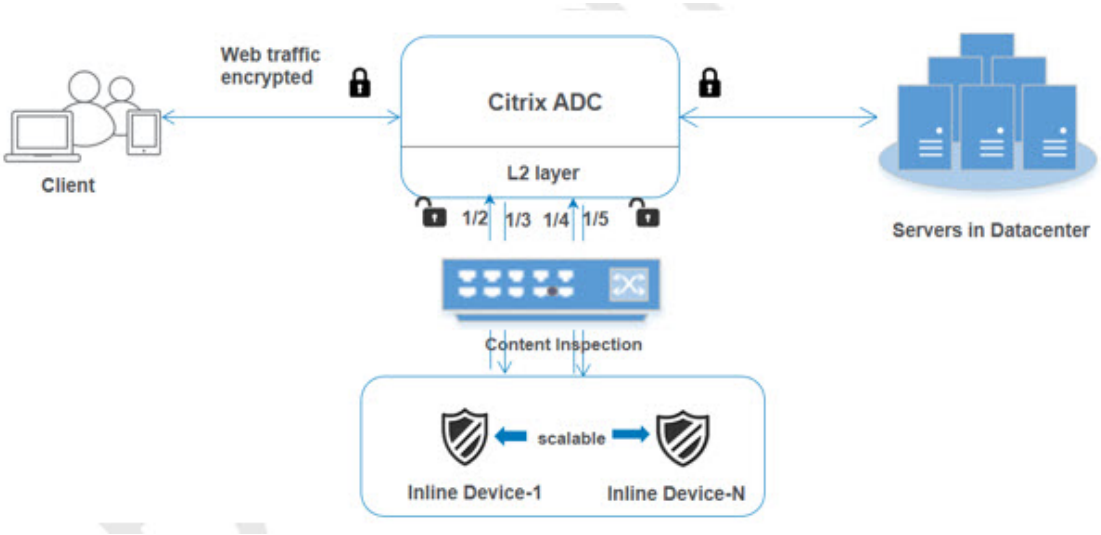
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Exemple :

```
bind lb vserver HTTP_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```

Scénario 2 : équilibrage de charge de plusieurs appareils en ligne à l'aide d'interfaces dédiées

Si vous utilisez deux appareils en ligne ou plus, vous devez équilibrer la charge des appareils à l'aide de différents services d'inspection du contenu dans une configuration VLAN dédiée. Dans ce cas, l'appliance NetScaler équilibre la charge des appareils en plus d'envoyer un sous-ensemble de trafic à chaque appareil via une interface dédiée.
Pour les étapes de configuration de base, reportez-vous au scénario 1.



Ajouter un profil d'inspection du contenu1 pour service1

Les configurations en ligne d'une appliance NetScaler peuvent être spécifiées dans une entité appelée profil d'inspection du contenu. Le profil possède un ensemble de paramètres d'appareil. Le profil d'inspection du contenu1 est créé pour le service en ligne 1 et la communication se fait via des interfaces dédiées 1/2 et 1/3.

À l'invite de commande, tapez :

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface "1/2" -egressInterface "1/3"
```

Ajouter le profil d'inspection du contenu2 pour service2

Le profil d'inspection du contenu2 est ajouté pour service2 et le périphérique en ligne communique avec l'appliance via `1/4` des interfaces dédiées. `1/5`
À l'invite de commande, tapez :

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface "1/4" -egressInterface "1/5"
```


Ajouter le service 1 pour l'appareil en ligne 1

Après avoir activé la fonction d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 1 pour que le périphérique en ligne 1 fasse partie de la configuration de l'équilibrage de charge. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commande, tapez :

```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_1> -healthmonitor OFF -usip ON -useproxyport OFF
```

Exemple :

```
add service Inline_service1 10.102.29.200 TCP 80 -contentInspectionProfileName
 Inline_profile1 -healthmonitor OFF -usip ON -useproxyport OFF
```

Ajouter le service 2 pour l'appareil en ligne 2

Après avoir activé la fonctionnalité d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 2 pour le périphérique en ligne 2. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commande, tapez :

```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```

Exemple :

```
add service Inline_service1 10.29.20.205 TCP 80 -contentInspectionProfileName
 Inline_profile2 -healthmonitor OFF -usip ON -useproxyport OFF
```

Ajouter un serveur virtuel d'équilibrage de charge

Après avoir ajouté le profil en ligne et les services, vous devez ajouter un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge des services.

À l'invite de commande, tapez :

```
add lb vserver <vserver_name> TCP <Pvt_IP3> <port>
```

Exemple :

```
add lb vserver lb-Inline_vserver TCP *
```

Liez le service 1 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur virtuel d'équilibrage de charge au premier service.

À l'invite de commande, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-Inline_vserver Inline_service1
```

Liez le service 2 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur au deuxième service.

À l'invite de commande, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-Inline_vserver Inline_service2
```

Ajouter une action d'inspection du contenu pour le service

Après avoir activé la fonctionnalité Inspection du contenu, vous devez ajouter l'action Inspection du contenu pour gérer les informations de demande en ligne. En fonction de l'action sélectionnée, le dispositif intégré abandonne, se réinitialise ou se bloque après avoir examiné le sous-ensemble de trafic donné.

À l'invite de commande, tapez :

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action < action_name > -type InlineINSPECTION -
serverName Service_name/Vserver_name>
```

Exemple :

```
add ContentInspection action Inline_action -type InlineINSPECTION -serverName
 lb-Inline_vserver
```

Ajouter une stratégie d'inspection du contenu pour l'inspection

Après avoir créé une action d'inspection du contenu, vous devez ajouter la stratégie d'inspection du contenu pour évaluer les demandes de service. La stratégie est basée sur une règle qui consiste en une ou plusieurs expressions. La règle est associée à l'action d'inspection du contenu qui est associée si une demande correspond à la règle.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Ajoutez un serveur virtuel de commutation de contenu ou d'équilibrage de charge pour accepter le trafic Web. Vous devez également activer la connexion layer2 sur le serveur virtuel.
Pour plus d'informations sur l'équilibrage de charge, consultez la rubrique Fonctionnement de l'équilibrage de charge.

À l'invite de commande, tapez :

```
add lb vserver <name> <vserver name> -l2Conn ON
```

Exemple :

```
add lb vserver http_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Lier la stratégie d'inspection du contenu au serveur virtuel d'équilibrage de charge de type HTTP/SSL

Vous devez lier le serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <L7InlineREQUEST | L4Inline-REQUEST>
```

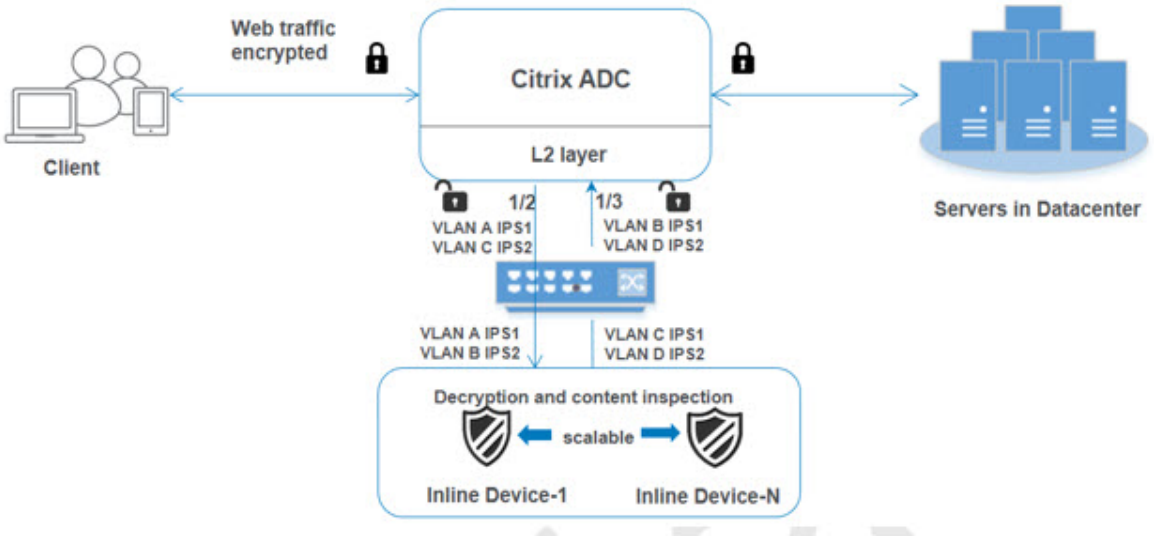
Exemple :

```
bind lb vserver http_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```

Scénario 3 : équilibrage de charge de plusieurs appareils en ligne à l'aide d'interfaces partagées

Vous pouvez vous référer à cette configuration si vous utilisez plusieurs appareils en ligne et si vous souhaitez équilibrer la charge des appareils à l'aide de différents services dans une interface VLAN

partagée. Cette configuration utilisant des interfaces VLAN partagées est similaire au cas d'utilisation 2. Pour la configuration de base, reportez-vous au scénario 2.



Liez le VLAN A avec l'option de partage activée

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 100 -ifnum 1/2 tagged
```

Liez le VLAN B avec l'option de partage activée

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 200 -ifnum 1/3 tagged
```

Liez le VLAN C avec l'option de partage activée

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 300 -ifnum 1/2 tagged
```


Liez le VLAN D avec l'option de partage activée

À l'invite de commandes, tapez ce qui suit :

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 400 -ifnum 1/3 tagged
```

Ajouter un profil d'inspection du contenu1 pour service1

Les configurations en ligne d'une appliance NetScaler peuvent être spécifiées dans une entité appelée profil d'inspection du contenu. Le profil possède un ensemble de paramètres d'appareil. Le profil d'inspection du contenu est créé pour le service en ligne 1 et la communication se fait via 1/2 et 1/3 d'interfaces dédiées.

À l'invite de commande, tapez :

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface "1/2" -egressInterface "1/3" -egressVlan 100 -ingressVlan
 300
```

Ajouter le profil d'inspection du contenu2 pour service2

Le profil d'inspection du contenu2 est ajouté pour service2 et le périphérique en ligne communique avec l'appliance via `1/2` des interfaces dédiées. `1/3`

À l'invite de commande, tapez :

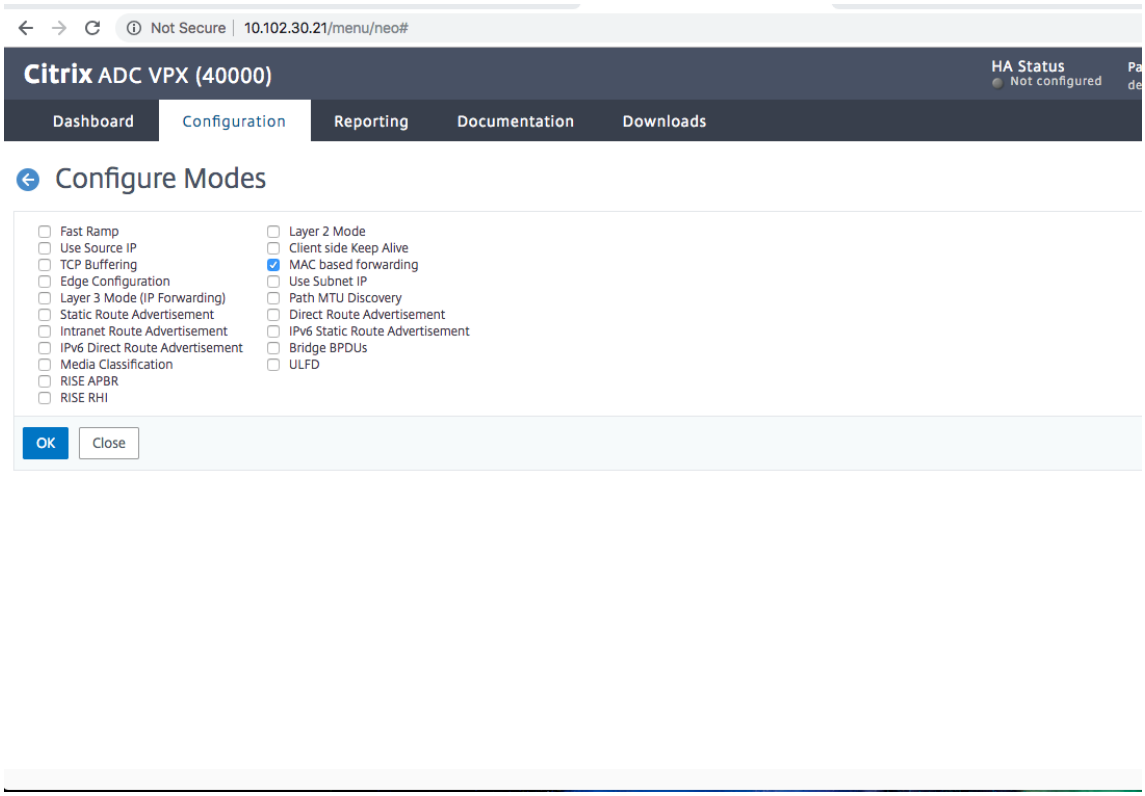
```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

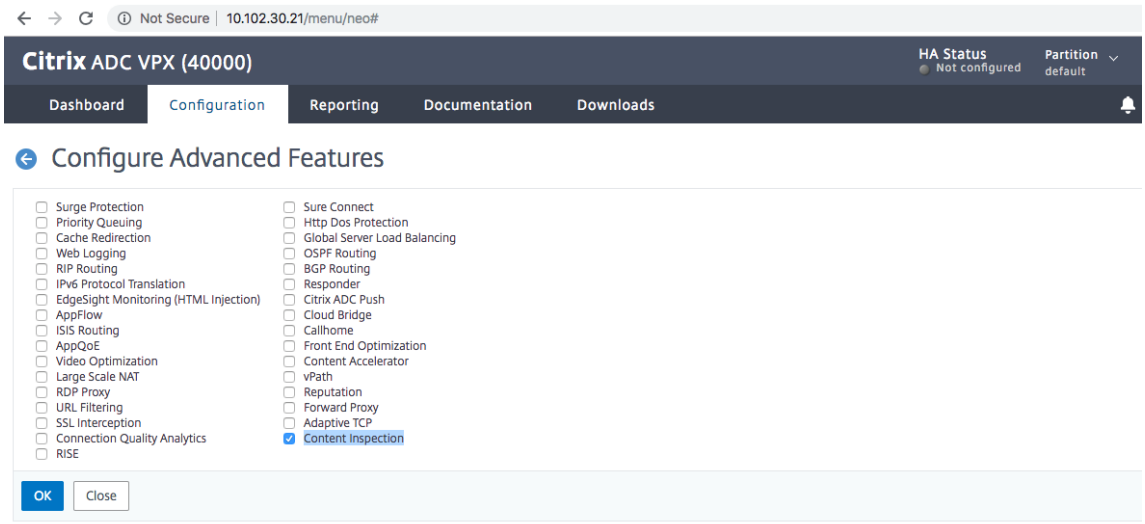
```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface "1/2" -egressInterface "1/3" -egressVlan 200 -ingressVlan
 400
```


Configuration de l'intégration des services en ligne à l'aide de l'interface graphique NetScaler

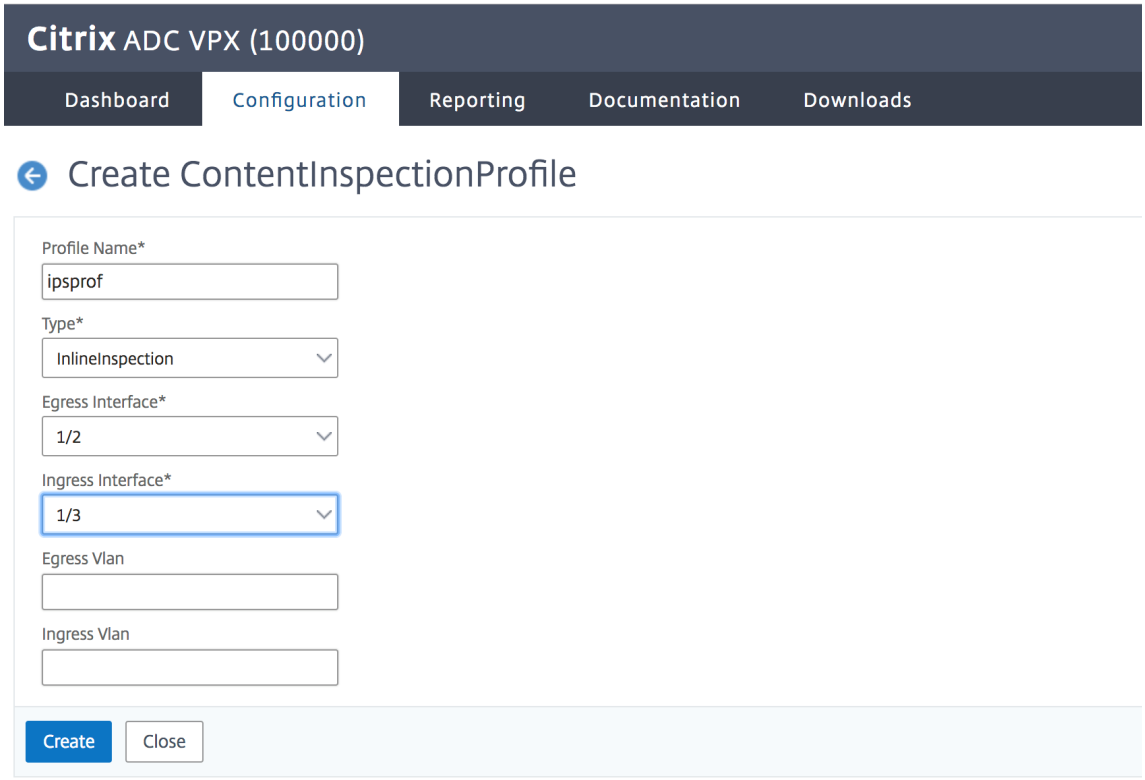
1. Connectez-vous à l'appliance NetScaler et accédez à l'onglet **Configuration** .
2. Accédez à **Système** > **Paramètres** > **Configurer les modes**.
3. Sur la page **Configurer les modes**, sélectionnez **Transfert basé sur Mac**.
4. Cliquez sur **OK** et sur **Fermer**.



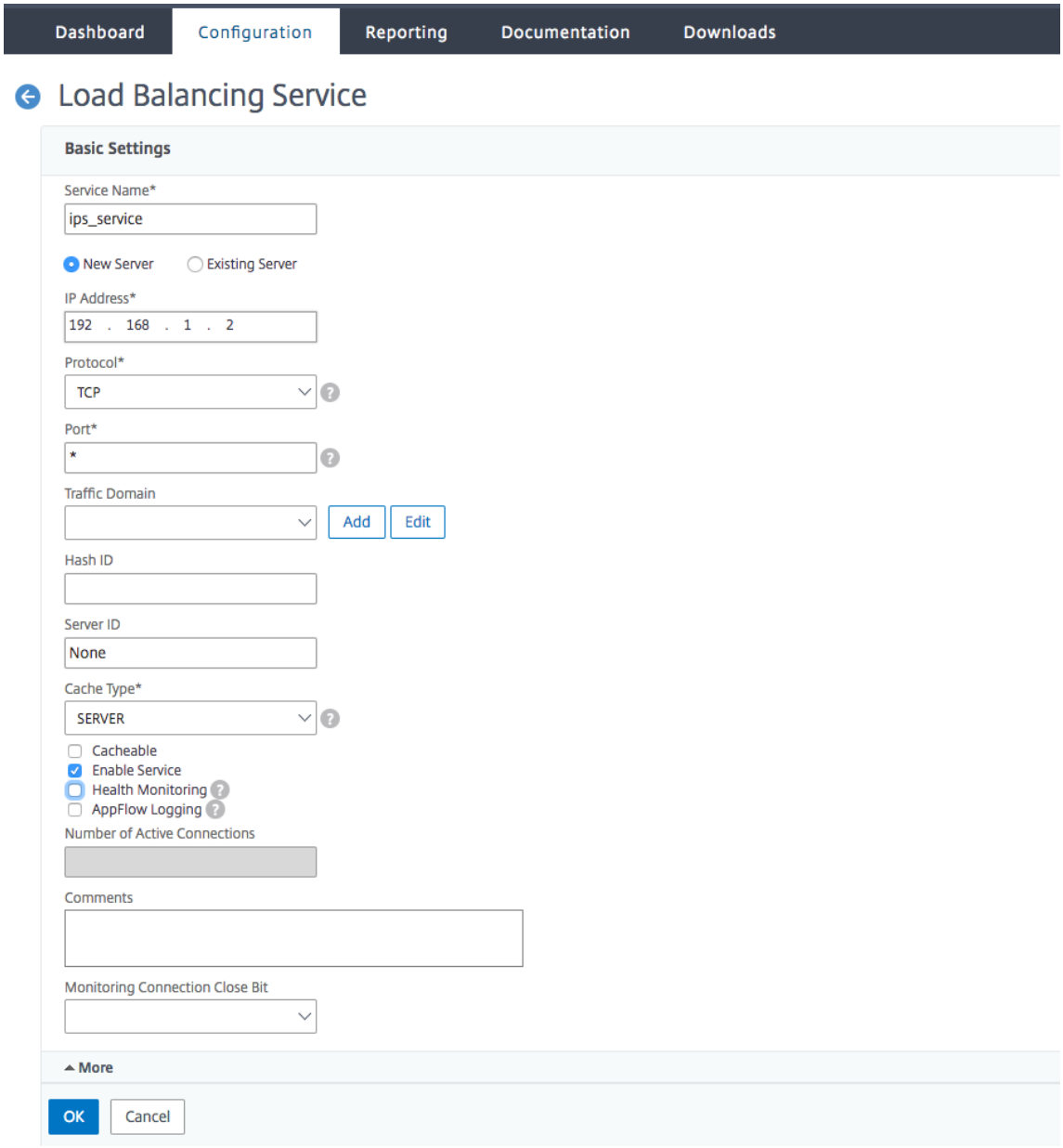
5. Accédez à **Système** > **Paramètres** > **Configurer les fonctionnalités avancées** .
6. Sur la page **Configurer les fonctionnalités avancées**, sélectionnez **Inspection du contenu**.
7. Cliquez sur **OK** et sur **Fermer**.



8. Accédez à **Sécurité** > **Inspection du contenu** > **ContentInspection Profiles**.
9. **Sur la page**Profils d'inspection du contenu**, cliquez sur Ajouter.**
10. Sur la page **Créer des profils d'inspection du contenu**, définissez les paramètres suivants.
    a) Nom du profil. Nom du profil d'inspection du contenu.
    b) Tapez. Sélectionnez le type de profil comme InlineInspection.
    c) Interface de sortie. Interface via laquelle l'appliance envoie le trafic depuis NetScaler vers le périphérique Inline.
    d) Interface d'entrée. Interface via laquelle l'appliance reçoit le trafic du périphérique en ligne vers NetScaler.
    e) VLAN de sortie. ID VLAN d'interface via lequel le trafic est envoyé au périphérique en ligne.
    f) VLAN d'entrée. ID VLAN d'interface via lequel l'appliance reçoit le trafic d'Inline vers NetScaler (s'il est configuré).

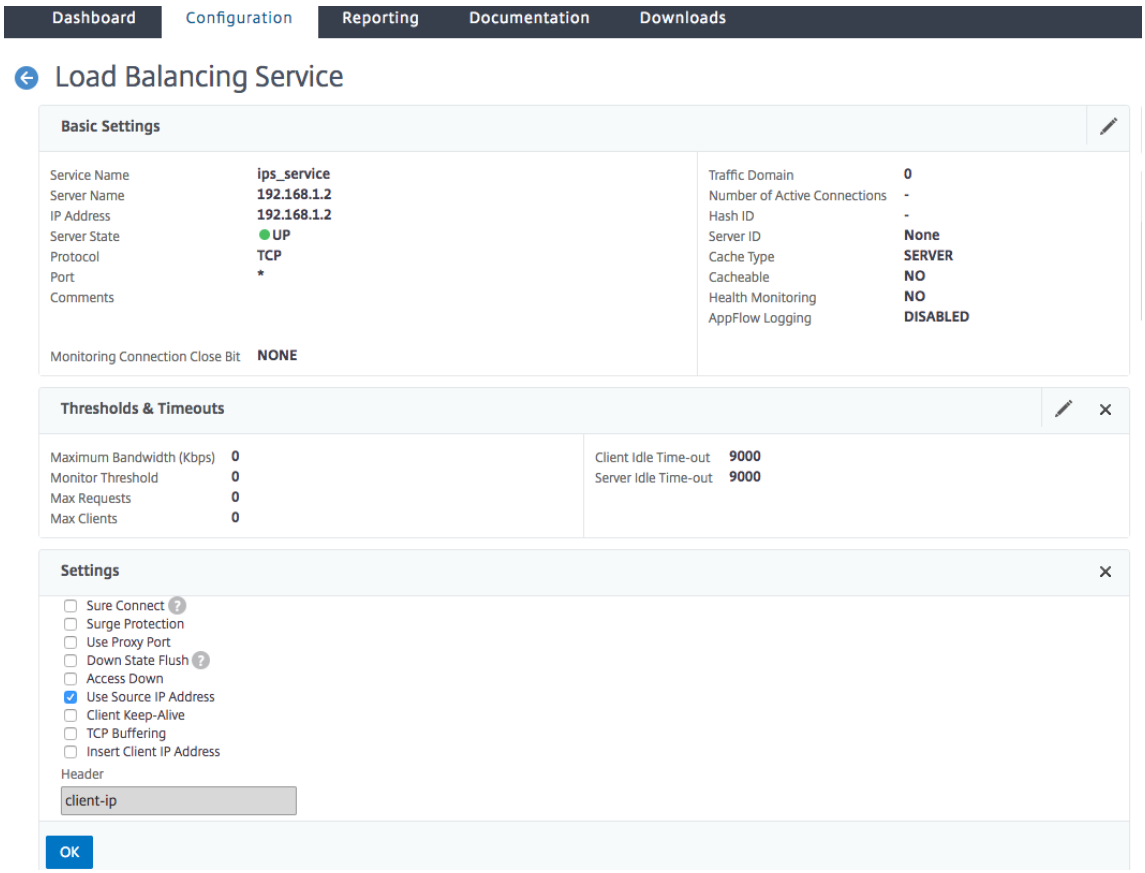


11. Cliquez sur **Créer** et **Fermer**.
12. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
13. Sur la page **Services**, définissez les paramètres suivants :
    a) Nom du service. Nom du service d'équilibrage de charge.
    b) Adresse IP Utilisez une adresse IP fictive. Remarque : aucun appareil ne doit être propriétaire de l'adresse IP.
    c) Protocole. Sélectionnez le type de protocole TCP.
    d) Port. Entrez *
    e) Surveillance de l'état de santé. Désélectionnez cette option et activez-la uniquement si vous souhaitez lier le service au moniteur de type TCP. Si vous souhaitez lier un moniteur à un service, l' TRANSPARENT option du moniteur doit être activée. Reportez-vous à l'étape 14 pour savoir comment ajouter un moniteur et comment le lier au service.
    f) Cliquez sur **OK**.

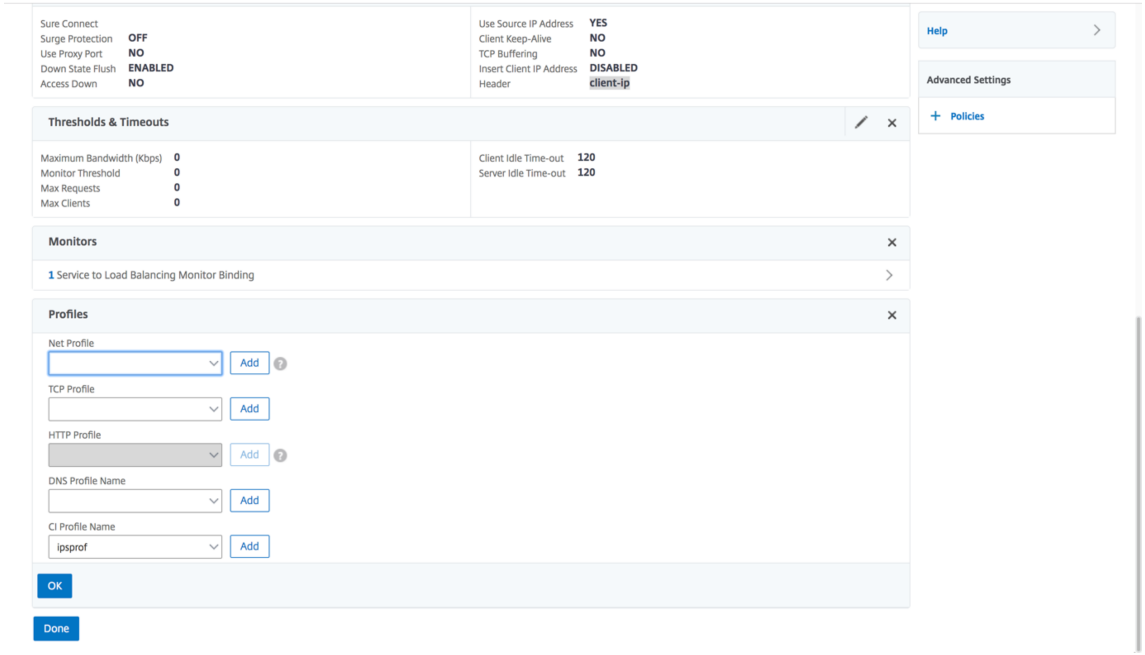


14. Dans la section **Paramètres**, modifiez ce qui suit et cliquez sur **OK**.

    a) Utiliser le port proxy : désactivez-le
    b) Utiliser l'adresse IP source : activez-la



15. Dans la section **Paramètres avancés**, cliquez sur **Profils**.
16. Accédez à la section **Profils**, ajoutez le profil d'inspection du contenu intégré et cliquez sur **OK.**

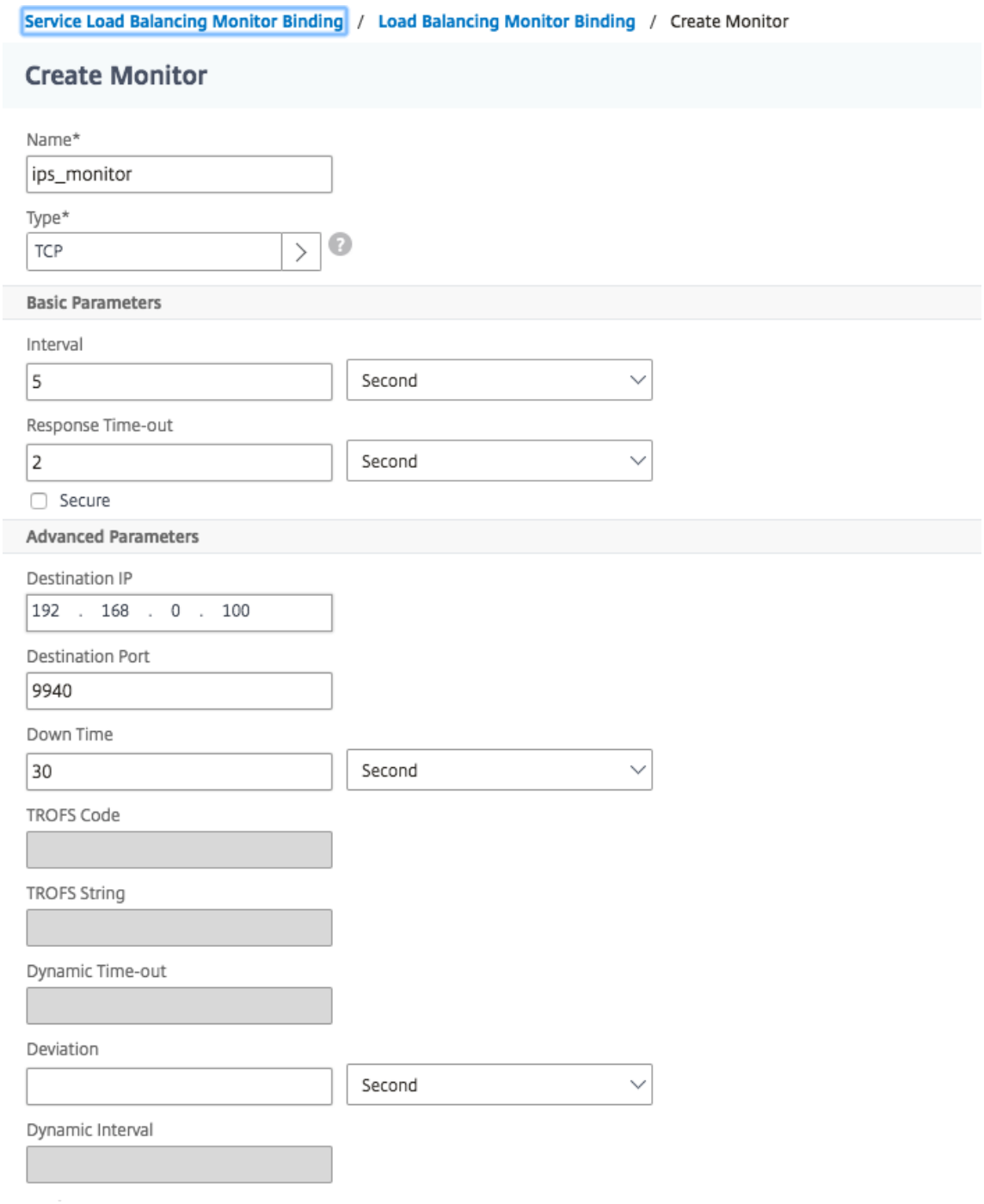


17. **Accédez à la section**Moniteurs**, puis**Ajouter des liaisons**>**Sélectionnez Moniteur**> Ajouter.**

a) Nom : Nom du moniteur
b) Type : Sélectionnez le type TCP
c) IP de destination, PORT : adresse IP et port de destination.
d) Transparent : Allumer

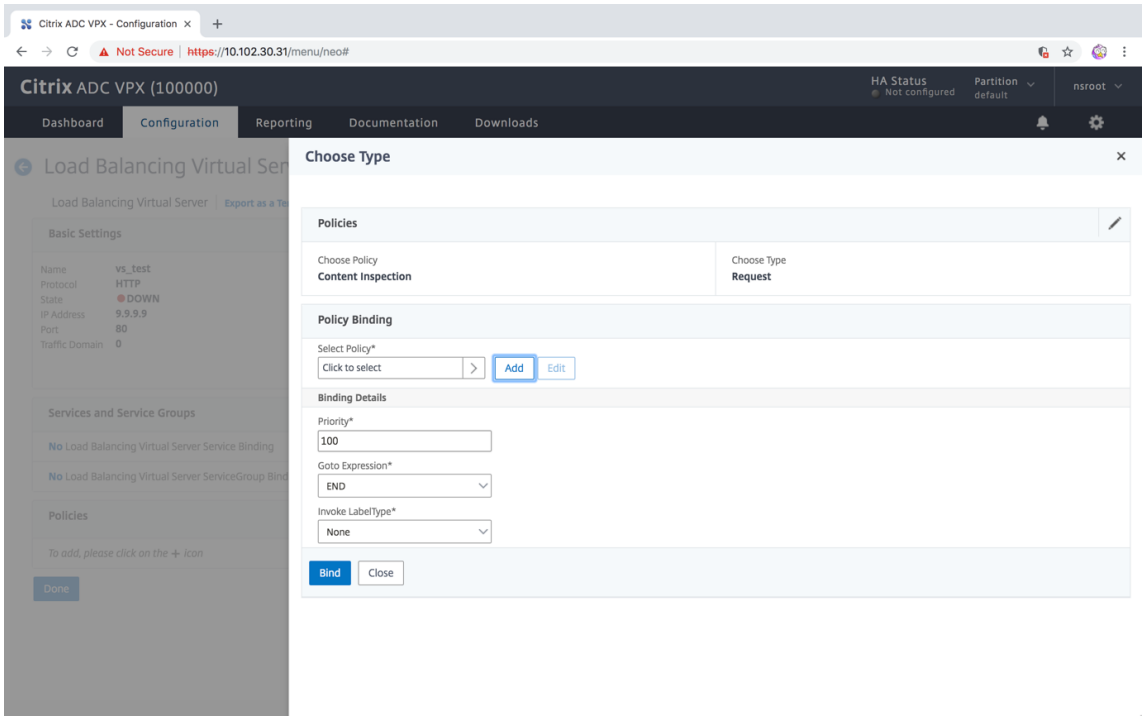
Remarque : Les paquets de surveillance doivent transiter par le périphérique en ligne pour surveiller l'état du périphérique en ligne.

18. Cliquez sur **Create**.

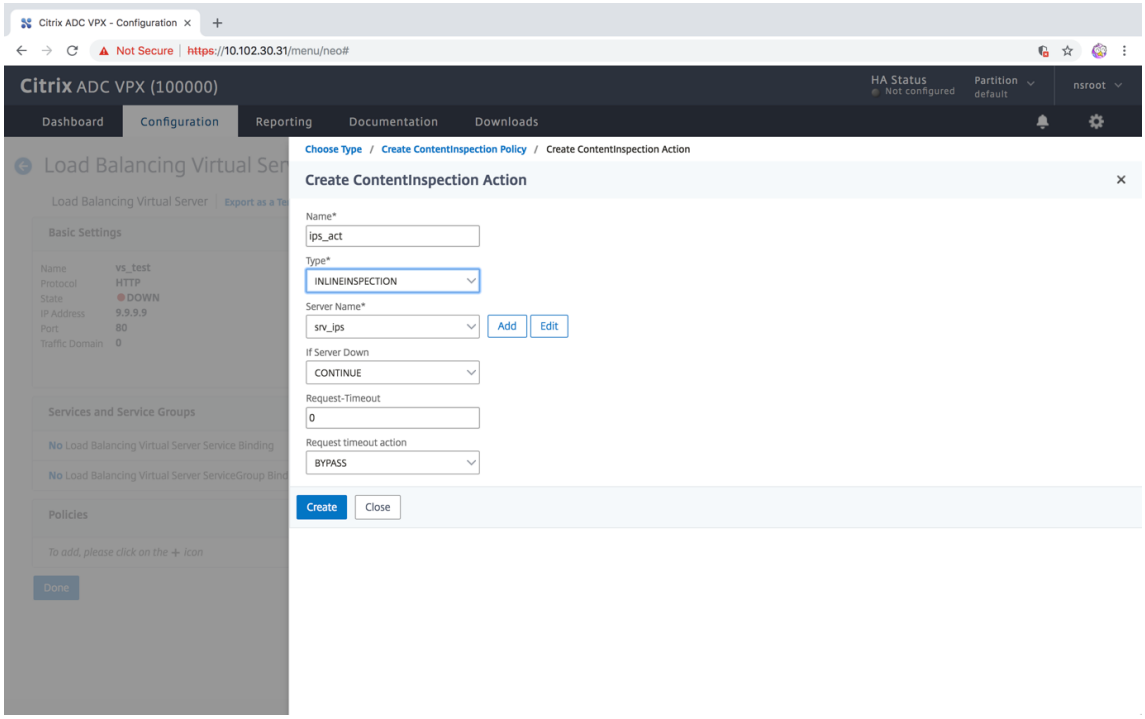


19. Cliquez sur **Terminé**.
20. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**. Ajoutez un serveur virtuel de type HTTP ou SSL.
21. Après avoir saisi les détails du serveur, cliquez sur **OK**, puis de nouveau **sur OK**.
22. Dans la section **Paramètres du trafic** du serveur virtuel d'équilibrage de charge, activez les paramètres de couche 2.

23. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
24. Accédez à la section **Politiques** et cliquez sur l'icône « + » pour configurer la politique d'inspection du contenu.
25. Sur la page **Choisir une politique**, sélectionnez Inspection du contenu. Cliquez sur **Continuer**.
26. Dans la section **Policy Binding**, cliquez sur **Ajouter** pour ajouter une politique d'inspection du contenu.



27. Sur la page **Créer une politique d'inspection du contenu**, entrez le nom de la politique d'inspection du contenu en ligne.
28. Dans le champ **Action**, cliquez sur **Ajouter** pour créer une action d'inspection du contenu en ligne.
29. Sur la page **Créer une action CI**, définissez les paramètres suivants :
    a) Nom. Nom de la stratégie en ligne d'inspection du contenu.
    b) Tapez. Sélectionnez le type InlineInspection.
    c) Serveur. Sélectionnez le serveur/le service en tant qu'appareils en ligne.
    d) Si le serveur est en panne. Sélectionnez une opération si le serveur tombe en panne.
    e) Délai d'expiration de la demande. Sélectionnez une valeur de délai d'expiration. Vous pouvez utiliser les valeurs par défaut.
    f) Action de délai d'expiration de demande. Sélectionnez une action de délai d'expiration. Vous pouvez utiliser les valeurs par défaut.
30. Cliquez sur **Create**.



31. Cliquez sur **Create**.
32. Sur la page **Créer une politique CI**, entrez d'autres détails :
33. Cliquez sur **OK** et sur **Fermer**.

Intégration avec IPS ou NGFW en tant que périphériques en ligne à l'aide du proxy de transfert SSL

August 20, 2021

Les dispositifs de sécurité tels que le système de prévention des intrusions (IPS) et le pare-feu de nouvelle génération (NGFW) protègent les serveurs contre les attaques réseau. Ces périphériques peuvent inspecter le trafic en direct et sont généralement déployés en mode Inline de couche 2. L'appliance proxy de transfert SSL assure la sécurité des utilisateurs et du réseau d'entreprise lors de l'accès aux ressources sur Internet.

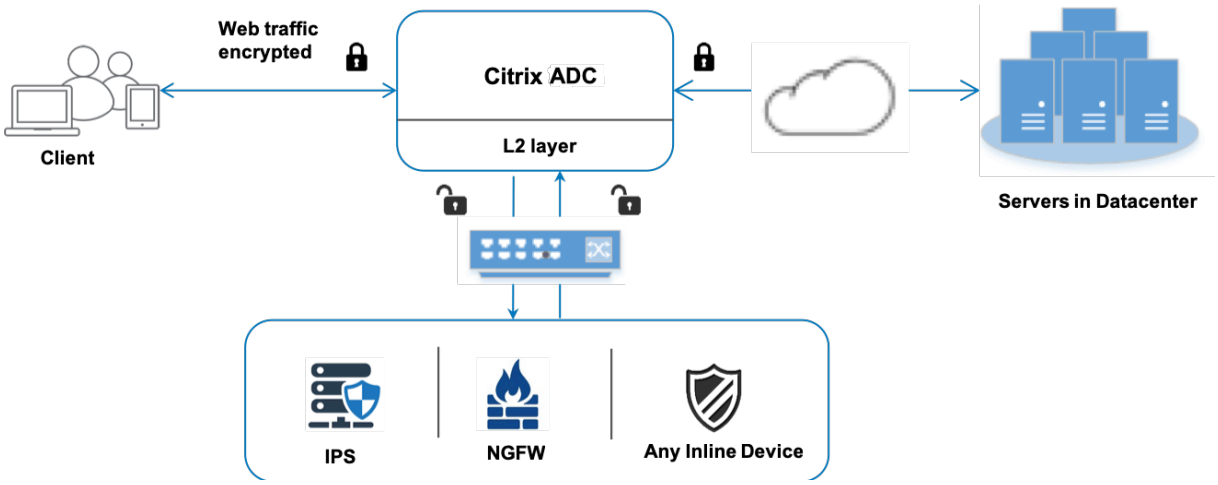
Une appliance proxy de transfert SSL peut être intégrée à un ou plusieurs périphériques en ligne pour prévenir les menaces et fournir une protection de sécurité avancée. Les périphériques en ligne peuvent être n'importe quel périphérique de sécurité, tel que IPS et NGFW.

Certains cas d'utilisation dans lesquels vous pouvez tirer parti de l'appliance proxy de transfert SSL et de l'intégration de périphériques en ligne sont les suivants :

- **Inspection du trafic chiffré :** la plupart des appliances IPS et NGFW contournent le trafic chiffré, ce qui peut rendre les serveurs vulnérables aux attaques. Une appliance proxy de transfert SSL peut déchiffrer le trafic et l'envoyer aux périphériques en ligne pour inspection. Cette intégration améliore la sécurité réseau du client.
- **Déchargement des périphériques en ligne du traitement TLS/SSL : le traitement** TLS/SSL est coûteux, ce qui peut entraîner une utilisation élevée du processeur dans les appliances IPS ou NGFW s'ils décryptent également le trafic. Une appliance proxy de transfert SSL aide à décharger le traitement TLS/SSL des périphériques en ligne. Par conséquent, les appareils en ligne peuvent inspecter un volume plus élevé de trafic.
- **Chargement des périphériques en ligne d'équilibrage :** si vous avez configuré plusieurs périphériques en ligne pour gérer le trafic lourd, un dispositif proxy de transfert SSL peut équilibrer la charge et répartir le trafic uniformément vers ces périphériques.
- **Sélection intelligente du trafic :** au lieu d'envoyer tout le trafic au périphérique en ligne pour inspection, l'appliance effectue une sélection intelligente du trafic. Par exemple, il ignore l'envoi de fichiers texte pour inspection aux périphériques en ligne.

Intégration par proxy SSL avec des périphériques en ligne

Le diagramme suivant montre comment un proxy de transfert SSL est intégré aux périphériques de sécurité en ligne.



Lorsque vous intégrez des périphériques en ligne à l'appliance proxy de transfert SSL, les composants interagissent comme suit :

1. Un client envoie une requête à un dispositif proxy de transfert SSL.
2. L'appliance envoie les données au périphérique en ligne pour inspection du contenu en fonction de l'évaluation de la stratégie. Pour le trafic HTTPS, l'appliance décrypte les données et les envoie en texte brut au périphérique en ligne pour inspection du contenu.

> **Remarque**
>
> S'il y a au moins deux périphériques en ligne, la charge de l'appliance équilibre les périphériques et envoie le trafic.

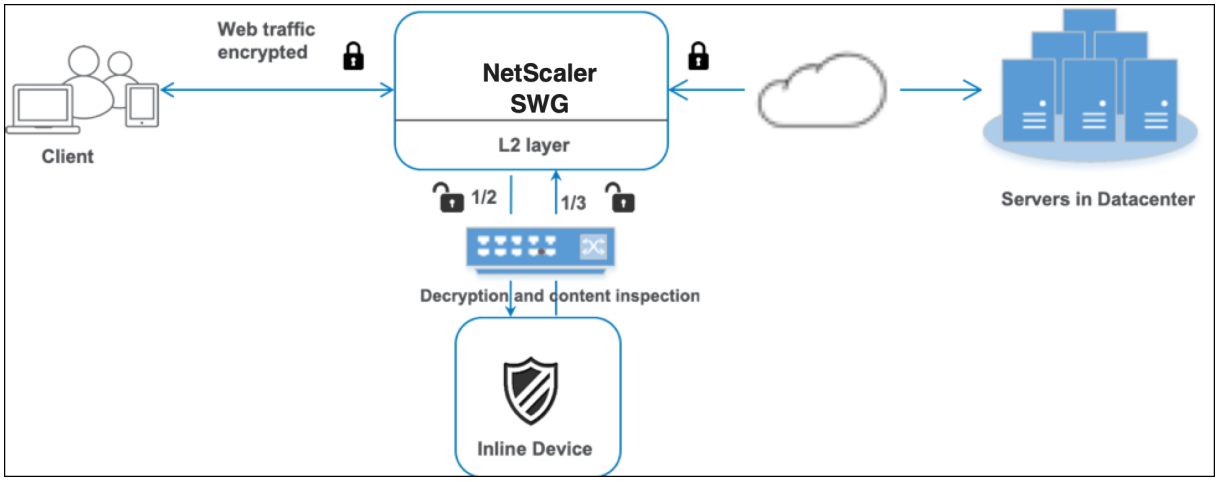
3. Ajoutez une commutation de contenu ou un serveur virtuel d'équilibrage de charge HTTP/HTTPS.
4. Le périphérique en ligne inspecte les données à la recherche de menaces et décide de supprimer, de réinitialiser ou de renvoyer les données à l'appliance.
5. S'il existe des menaces de sécurité, le périphérique modifie les données et les envoie à l'appliance.
6. Pour le trafic HTTPS, l'appliance chiffre à nouveau les données et transmet la demande au serveur principal.
7. Le serveur principal envoie la réponse à l'appliance.
8. L'appliance déchiffre à nouveau les données et les envoie au périphérique en ligne pour inspection.
9. Le périphérique en ligne inspecte les données. S'il existe des menaces de sécurité, le périphérique modifie les données et les envoie à l'appliance.
10. L'appliance recrypte les données et envoie la réponse au client.

Configuration de l'intégration de périphériques en ligne

Vous pouvez configurer une appliance proxy de transfert SSL avec un périphérique en ligne de trois manières différentes :

Scénario 1 : Utilisation d'un seul périphérique en ligne

Pour intégrer un périphérique de sécurité (IPS ou NGFW) en mode Inline, vous devez activer l'inspection du contenu et le transfert basé sur Mac (MBF) en mode global sur l'appliance proxy SSL. Ensuite, ajoutez un profil d'inspection de contenu, un service TCP, une action d'inspection de contenu pour les périphériques en ligne pour réinitialiser, bloquer ou supprimer le trafic basé sur l'inspection. Ajoutez également une stratégie d'inspection du contenu utilisée par l'appliance pour décider du sous-ensemble de trafic à envoyer aux périphériques en ligne. Enfin, configurez le serveur virtuel proxy avec la connexion de couche 2 activée sur le serveur et liez la stratégie d'inspection de contenu à ce serveur virtuel proxy.



Procédez comme suit :

1. Activer le mode de transfert basé sur Mac (MPF).
2. Activez la fonction d'inspection du contenu.
3. Ajoutez un profil d'inspection de contenu pour le service. Le profil d'inspection du contenu contient les paramètres de périphérique en ligne qui intègrent le dispositif proxy SSL à un périphérique en ligne.
4. (Facultatif) Ajoutez un moniteur TCP.

   > **Remarque :**
   >
   > Les périphériques transparents n'ont pas d'adresse IP. Par conséquent, pour effectuer des vérifications de l'état, vous devez lier explicitement un moniteur.

5. Ajoutez un service. Un service représente un périphérique en ligne.
6. (Facultatif) Liez le service au moniteur TCP.
7. Ajoutez une action d'inspection du contenu pour le service.
8. Ajoutez une stratégie d'inspection du contenu et spécifiez l'action.
9. Ajoutez un serveur virtuel proxy HTTP ou HTTPS (commutation de contenu).
10. Liez la stratégie d'inspection de contenu au serveur virtuel.

Configurer à l'aide de la CLI

Tapez les commandes suivantes à l'invite de commandes. Des exemples sont donnés après la plupart des commandes.

1. Activez MBF.

```
enable ns mode mbf
```


1. Activez la fonctionnalité.

```
enable ns feature contentInspection
```

1. Ajouter un profil d'inspection de contenu.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile ipsprof -type InlineInspection -ingressinterface
 "1/2" -egressInterface "1/3"
```

1. Ajoutez un service. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Par défaut, la surveillance de l'intégrité est ACTIVÉE, lie le service à un moniteur d'intégrité et définit également l'option TRANSPARENT dans le moniteur ON.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service 198.51.100.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```

1. Ajoutez un moniteur de santé. Par défaut, le moniteur de santé est activé et vous avez également la possibilité de le désactiver, si nécessaire. À l'invite de commandes, tapez :

   ```
   add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent
    <YES, NO>
   ```

Exemple :

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

1. Liez le service au moniteur de santé

Après avoir configuré le moniteur de santé, vous devez lier le service au moniteur de santé. À l'invite de commandes, tapez :

```
bind service <name> -monitorName <name>
```

Exemple :

```
bind service ips_svc -monitorName ips_tcp
```

1. Ajoutez une action d'inspection du contenu.


```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Exemple :

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
ips_service
```

1. Ajoutez une stratégie d'inspection du contenu.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Exemple :

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Ajoutez un serveur virtuel proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -cltTimeout <secs> -Listenpolicy
 <expression> -authn401 ( ON | OFF )-authnVsName <string> -l2Conn ON
```

> **Remarque :**
>
> Les serveurs virtuels d'équilibrage de charge de type HTTP/SSL sont également pris en charge.

Exemple :

```
add cs vserver transparentcs PROXY * * -cltTimeout 180 -Listenpolicy exp1 -
authn401 on -authnVsName swg-auth-vs-trans-http -l2Conn ON
```

1. Liez la stratégie au serveur virtuel.

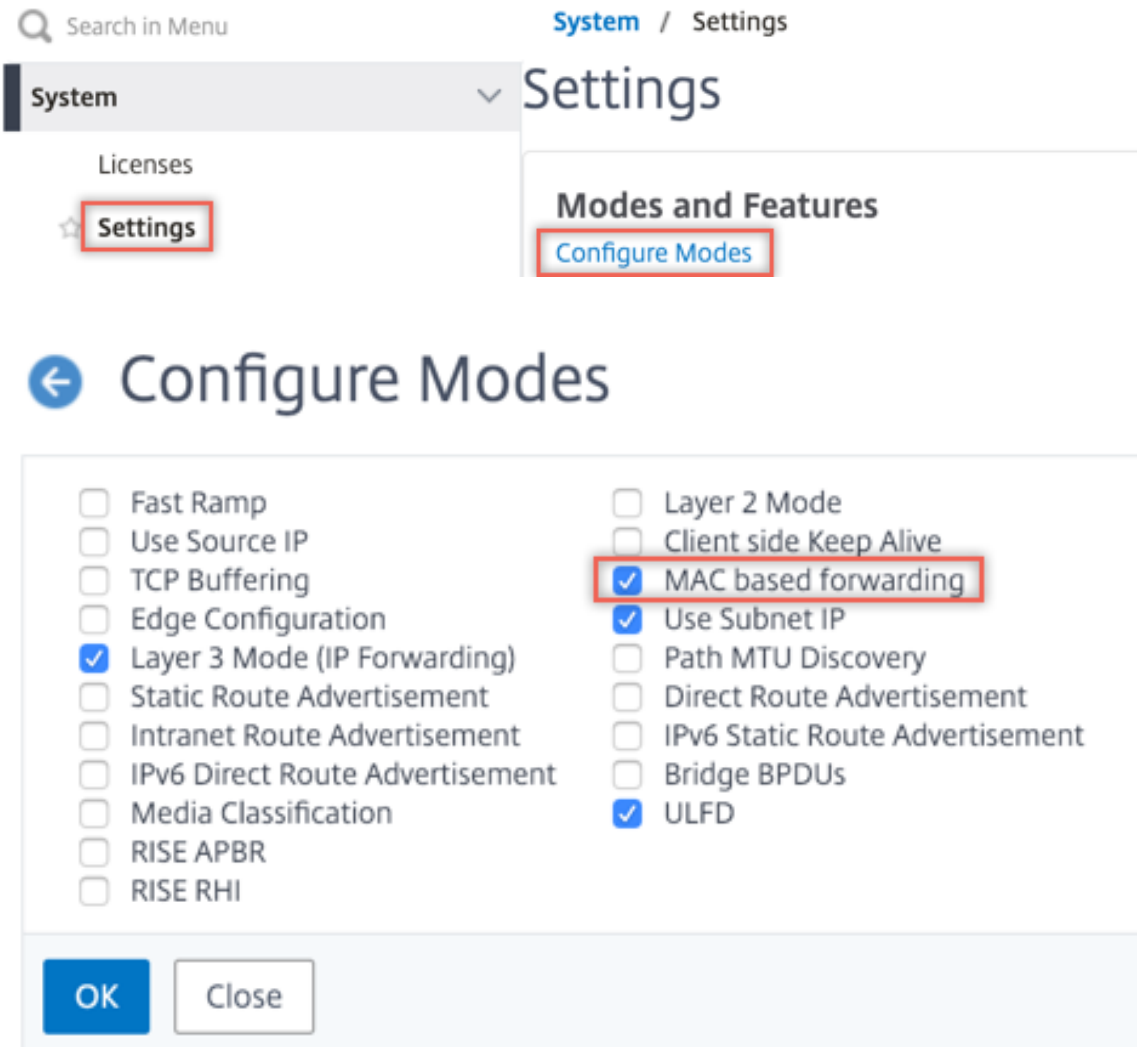
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Exemple :

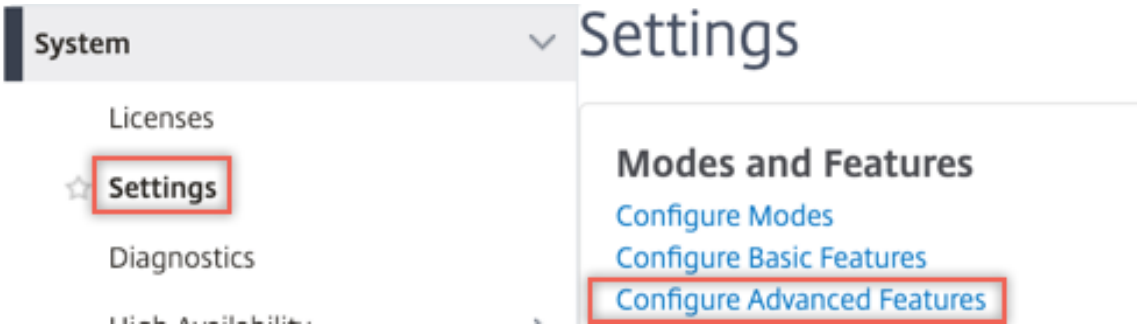
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

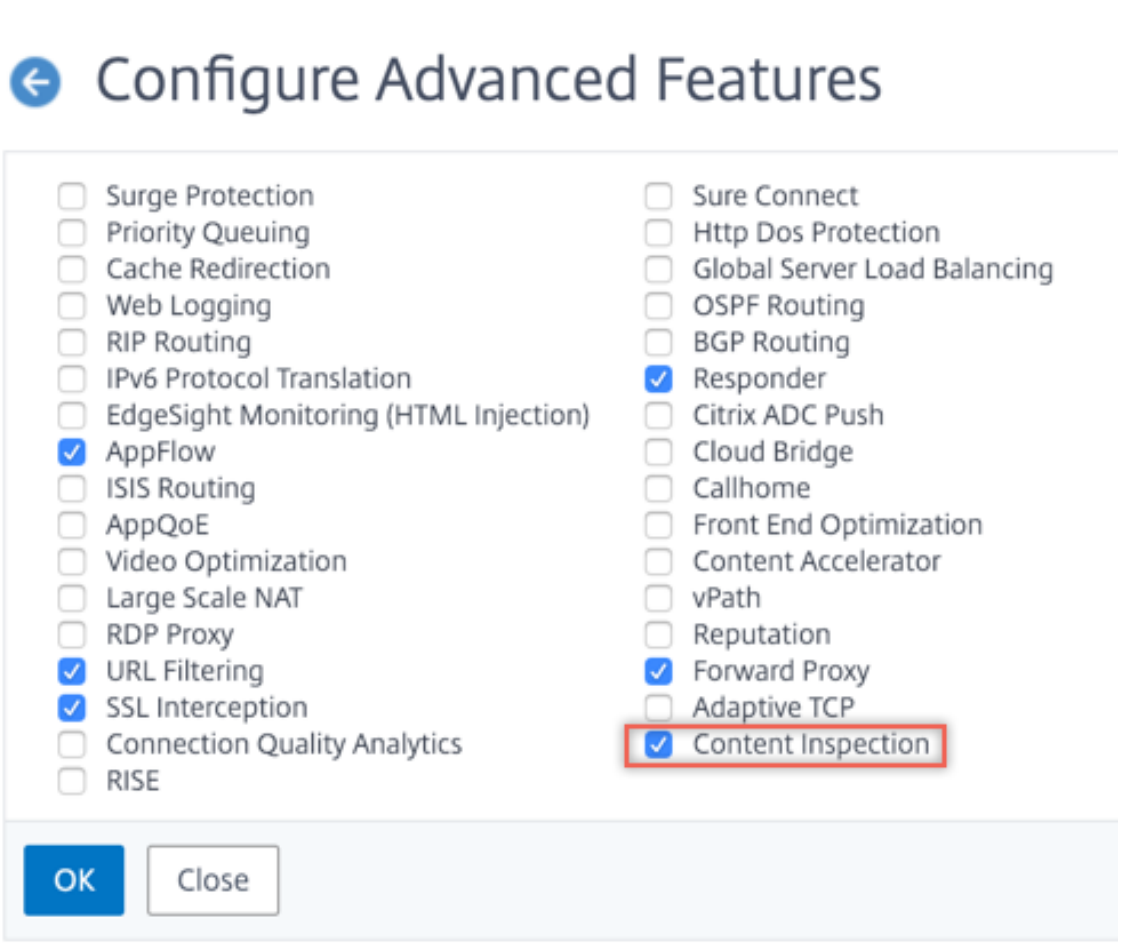
Configurer à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.

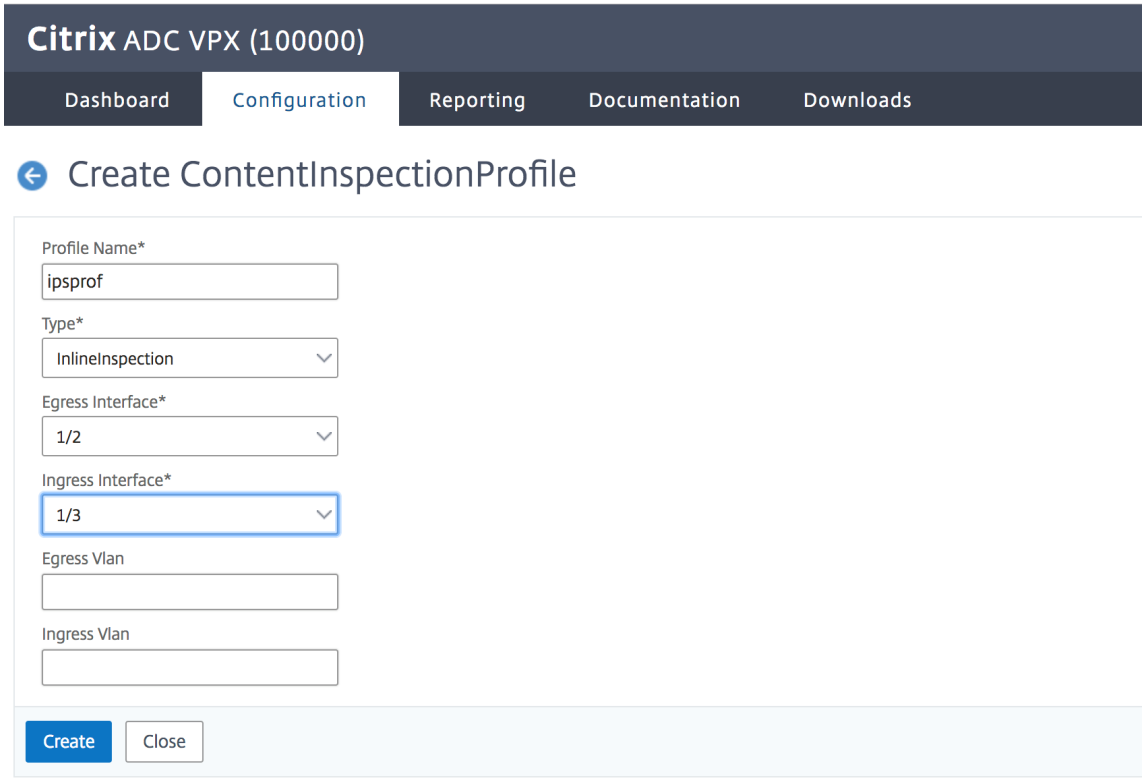


2. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.

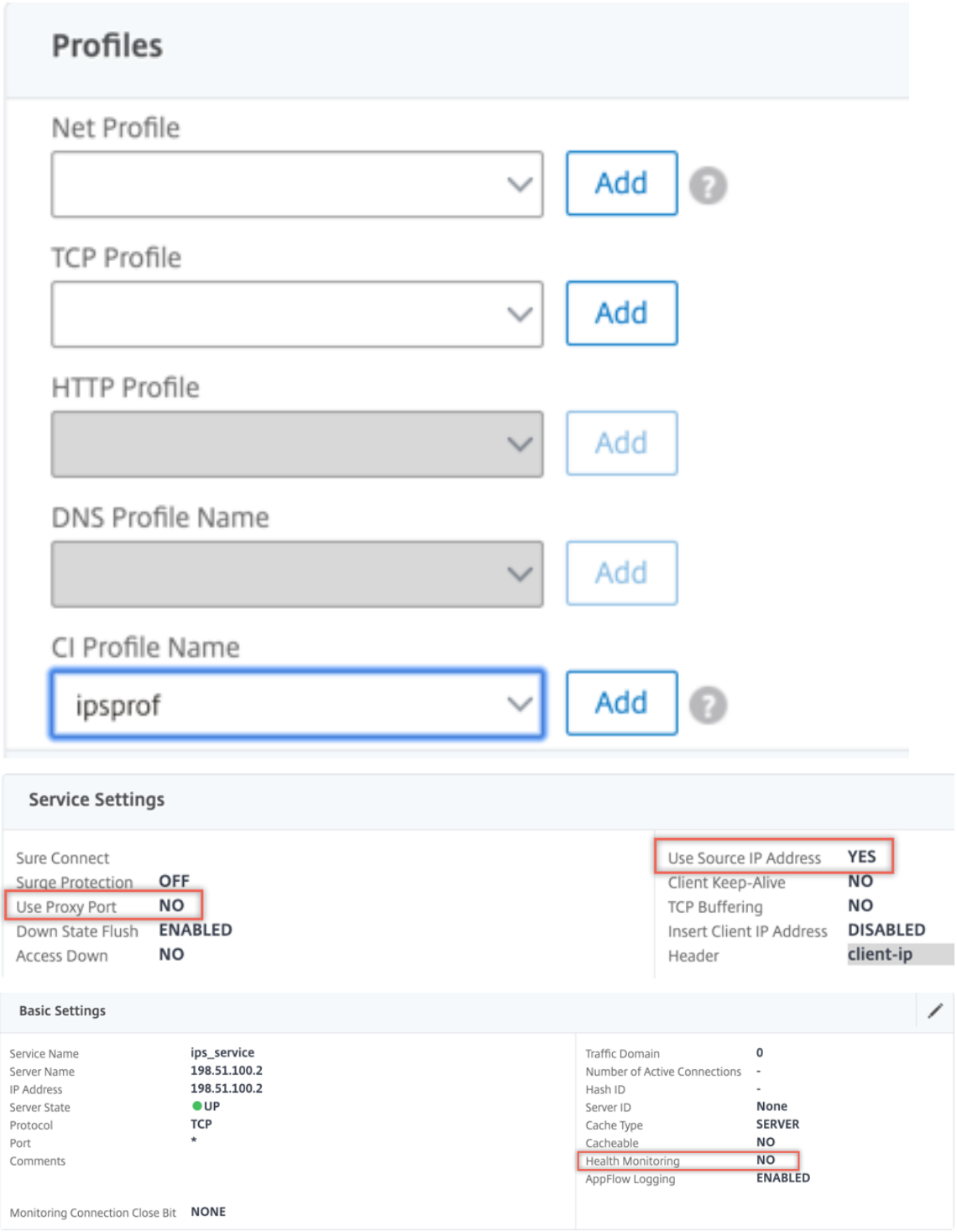




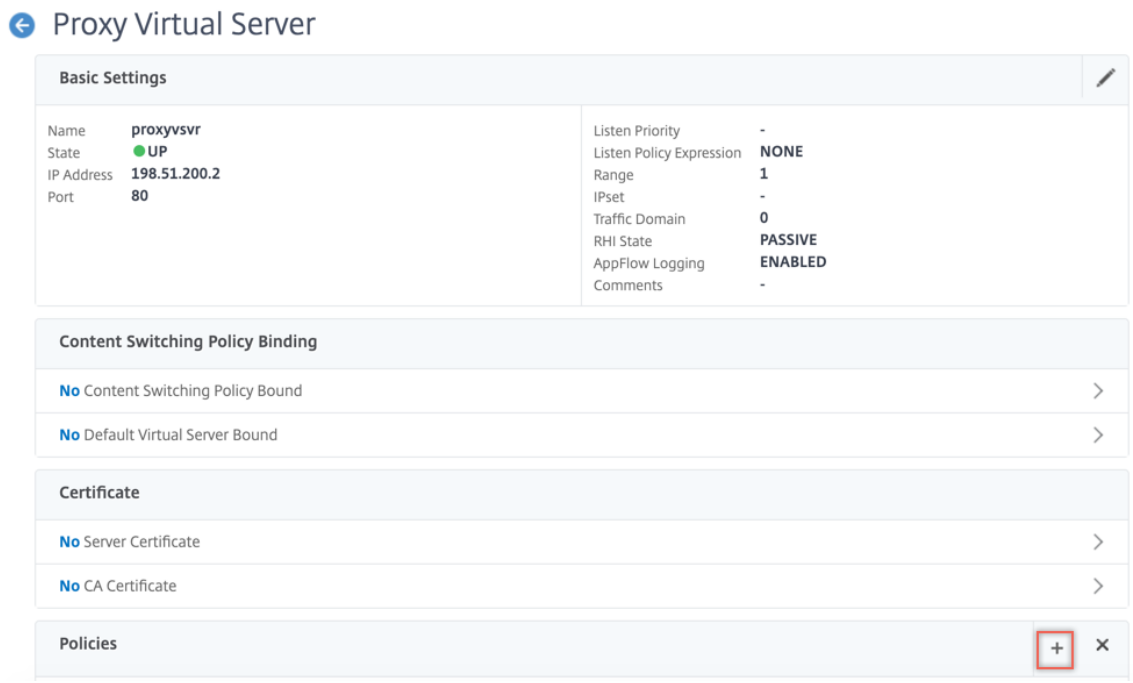
3. Accédez à **Secure Web Gateway > Inspection du contenu > Profils d'inspection du contenu**. Cliquez sur **Ajouter**.



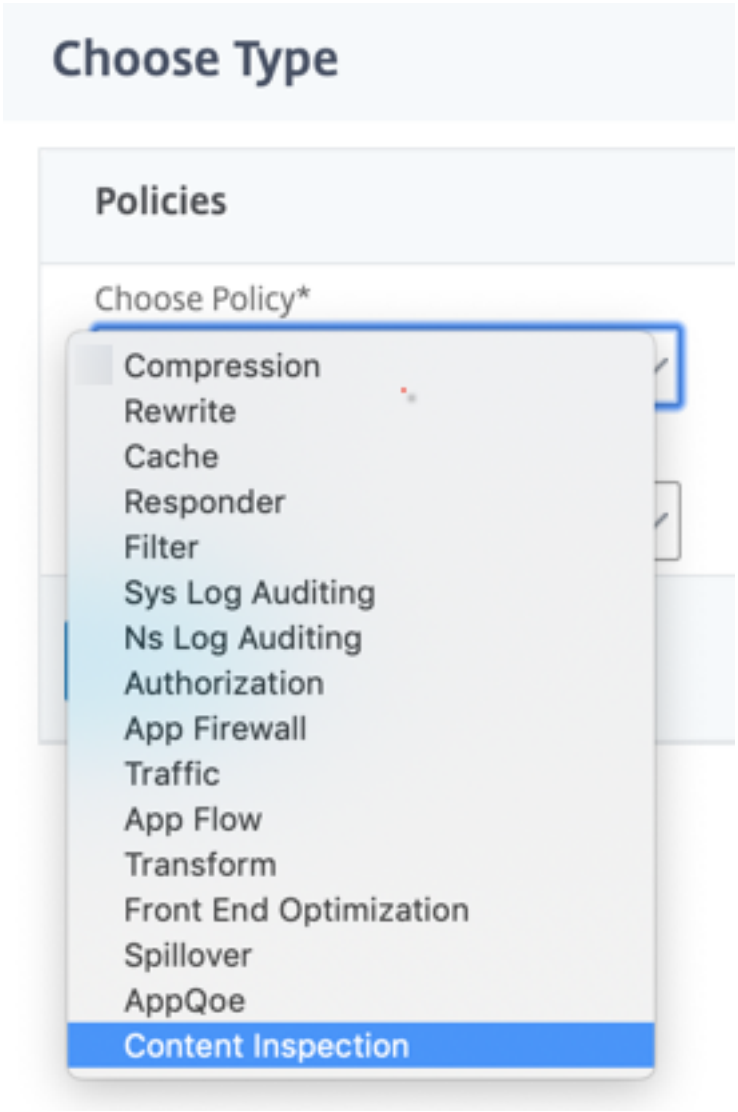
4. Accédez à **Équilibrage de charge > Services > Ajouter** et ajouter un service. Dans **Paramètres avancés**, cliquez sur **Profils**. Dans la liste **Nom du profil CI**, sélectionnez le profil d'inspection du contenu créé précédemment. Dans **Paramètres de service**, définissez **Utiliser l'adresse IP source**sur YES et **Utiliser le port proxy**sur Non. Dans **Paramètres de base**, définissez le **contrôle de l'intégrité** sur NO. Activez la surveillance de l'intégrité uniquement si vous liez ce service à un moniteur TCP. Si vous liez un moniteur à un service, définissez l'option TRANSPARENT du moniteur sur ON.



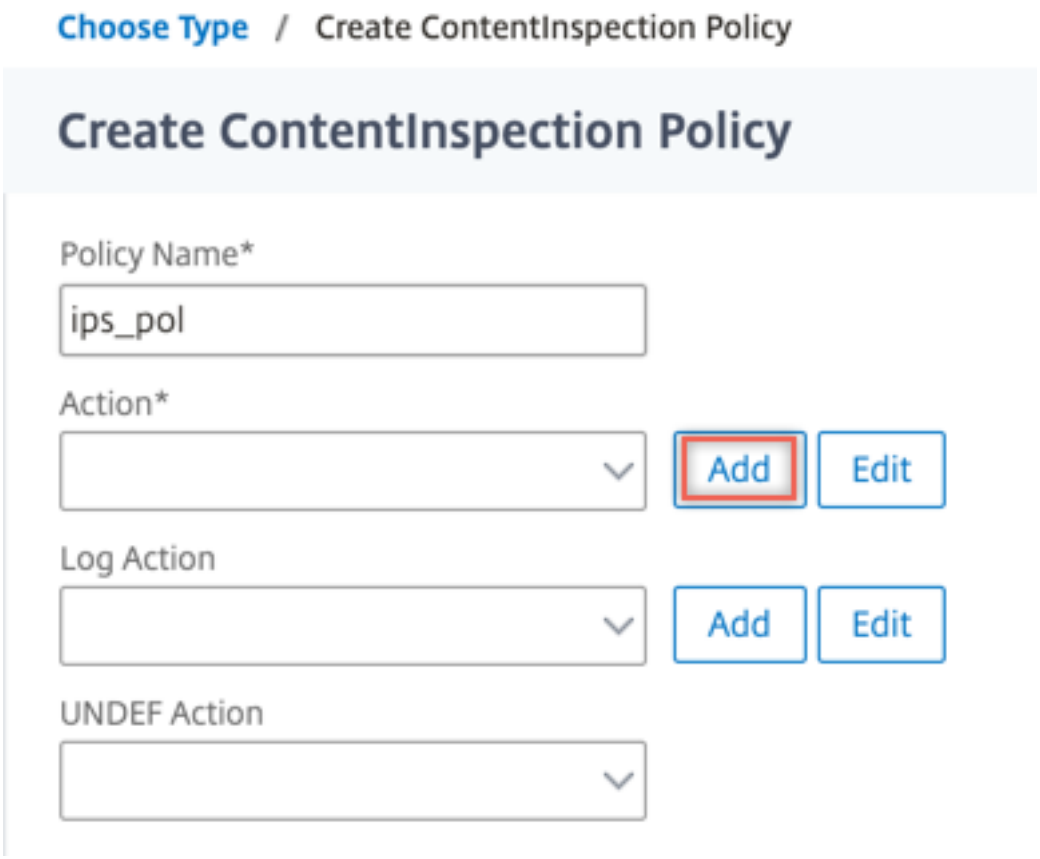
5. Accédez à **Secure Web Gateway > Servers virtuels Proxy > Ajouter**. Spécifiez un nom, une adresse IP et un port. Dans **Paramètres avancés**, sélectionnez **Stratégies**. Cliquez sur le signe « + ».



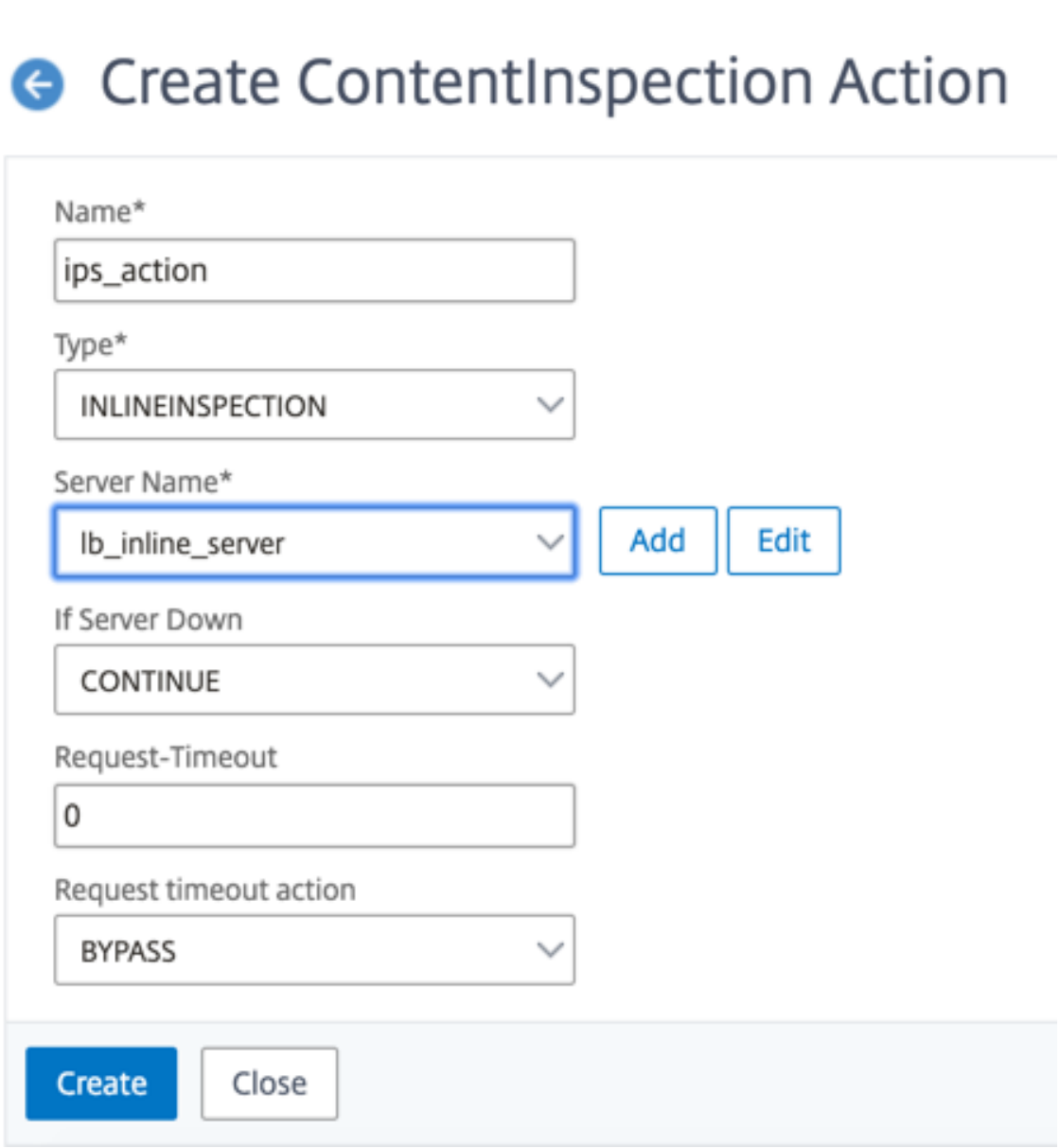
6. Dans **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



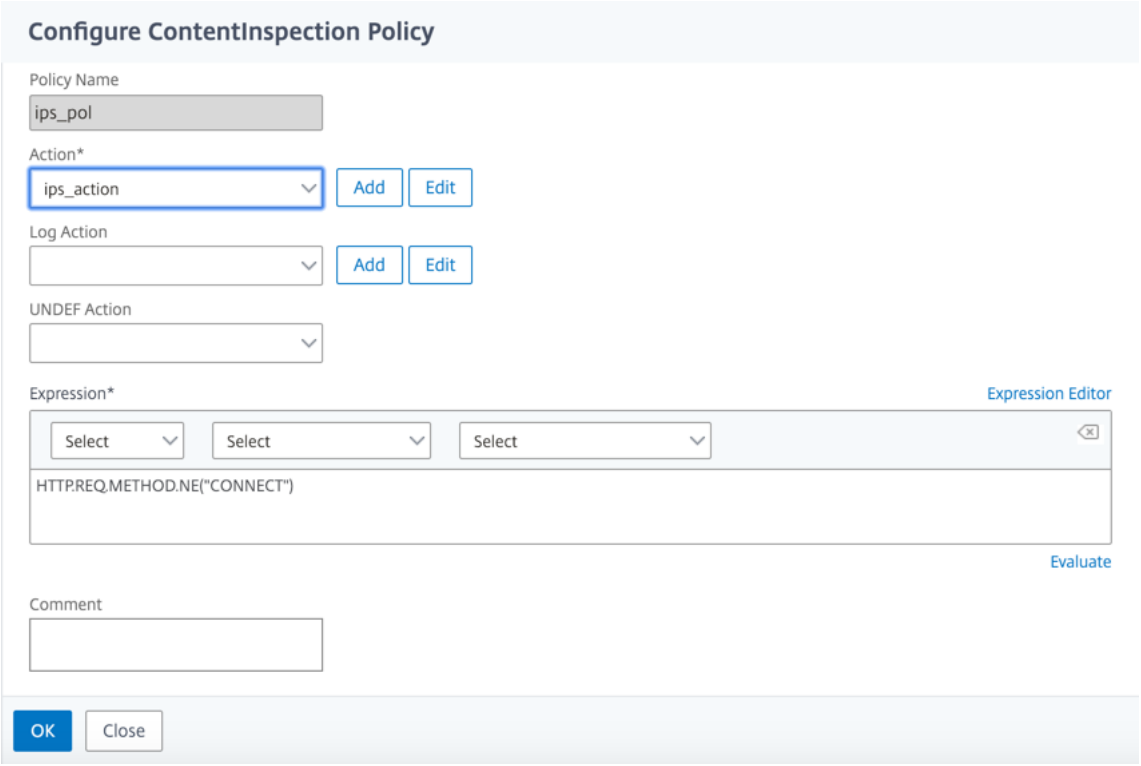
7. Cliquez sur **Ajouter**. Spécifiez un nom. Dans **Action**, cliquez sur **Ajouter**.



8. Spécifiez un nom. Dans **Type**, sélectionnez **INLINEINSPECTION**. Dans **Nom du serveur**, sélectionnez le service TCP créé précédemment.



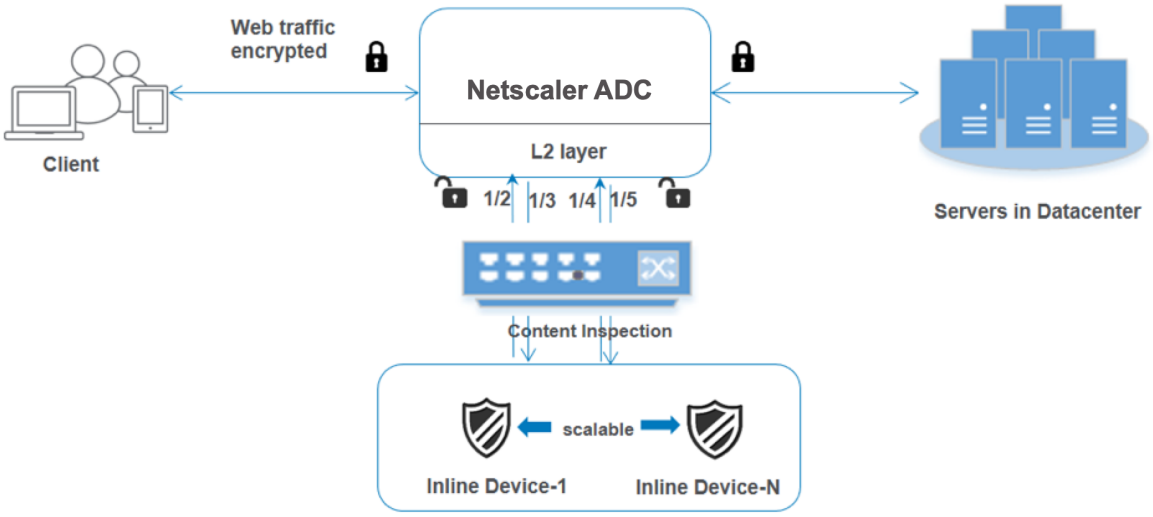
9. Cliquez sur **Créer**. Spécifiez la règle et cliquez sur **Créer**.



10. Cliquez sur **Bind**.
11. Cliquez sur **Terminé**.

Scénario 2 : équilibrage de la charge de plusieurs périphériques en ligne avec interfaces dédiées

Si vous utilisez au moins deux périphériques en ligne, vous pouvez équilibrer la charge des périphériques à l'aide de différents services d'inspection de contenu avec des interfaces dédiées. Dans ce cas, la charge de l'appliance proxy de transfert SSL équilibre le sous-ensemble du trafic envoyé à chaque périphérique via une interface dédiée. Le sous-ensemble est décidé en fonction des stratégies configurées. Par exemple, les fichiers TXT ou image peuvent ne pas être envoyés pour inspection aux périphériques en ligne.



La configuration de base reste la même que dans le scénario 1. Toutefois, vous devez créer un profil d'inspection de contenu pour chaque périphérique en ligne et spécifier l'interface d'entrée et de sortie dans chaque profil. Ajoutez un service pour chaque périphérique en ligne. Ajoutez un serveur virtuel d'équilibrage de charge et spécifiez-le dans l'action d'inspection du contenu. Effectuez les étapes supplémentaires suivantes :

1. Ajoutez des profils d'inspection de contenu pour chaque service.
2. Ajoutez un service pour chaque périphérique.
3. Ajoutez un serveur virtuel d'équilibrage de charge.
4. Spécifiez le serveur virtuel d'équilibrage de charge dans l'action d'inspection du contenu.

Configurer à l'aide de la CLI

Tapez les commandes suivantes à l'invite de commandes. Des exemples sont donnés après chaque commande.

1. Activez MBF.

```
enable ns mode mbf
```

1. Activez la fonctionnalité.

```
enable ns feature contentInspection
```

1. Ajouter le profil 1 pour le service 1.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :


```
add contentInspection profile ipsprof1 -type InlineInspection -ingressInterface
 "1/2"-egressInterface "1/3"
```

1. Ajouter le profil 2 pour le service 2.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile ipsprof2 -type InlineInspection -ingressInterface
 "1/4"-egressInterface "1/5"
```

1. Ajouter le service 1. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Activez la surveillance de l'intégrité avec le moniteur TCP avec l'option TRANSPARENT activée.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Ajouter le service 2. Spécifiez une adresse IP fictive qui n'appartient à aucun des périphériques, y compris les périphériques en ligne. Définissez `use source IP address` (USIP) sur YES. Définissez `useproxyport` sur NO. Activez la surveillance de l'état avec l'option TRANSPARENT activée.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Ajoutez un serveur virtuel d'équilibrage de charge.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Exemple :

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

1. Liez les services au serveur virtuel d'équilibrage de charge.


```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Exemple :

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Spécifiez le serveur virtuel d'équilibrage de charge dans l'action d'inspection du contenu.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Exemple :

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Ajoutez une stratégie d'inspection du contenu. Spécifiez l'action d'inspection du contenu dans la stratégie.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Exemple :

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Ajoutez un serveur virtuel proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Exemple :

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Liez la stratégie d'inspection de contenu au serveur virtuel.

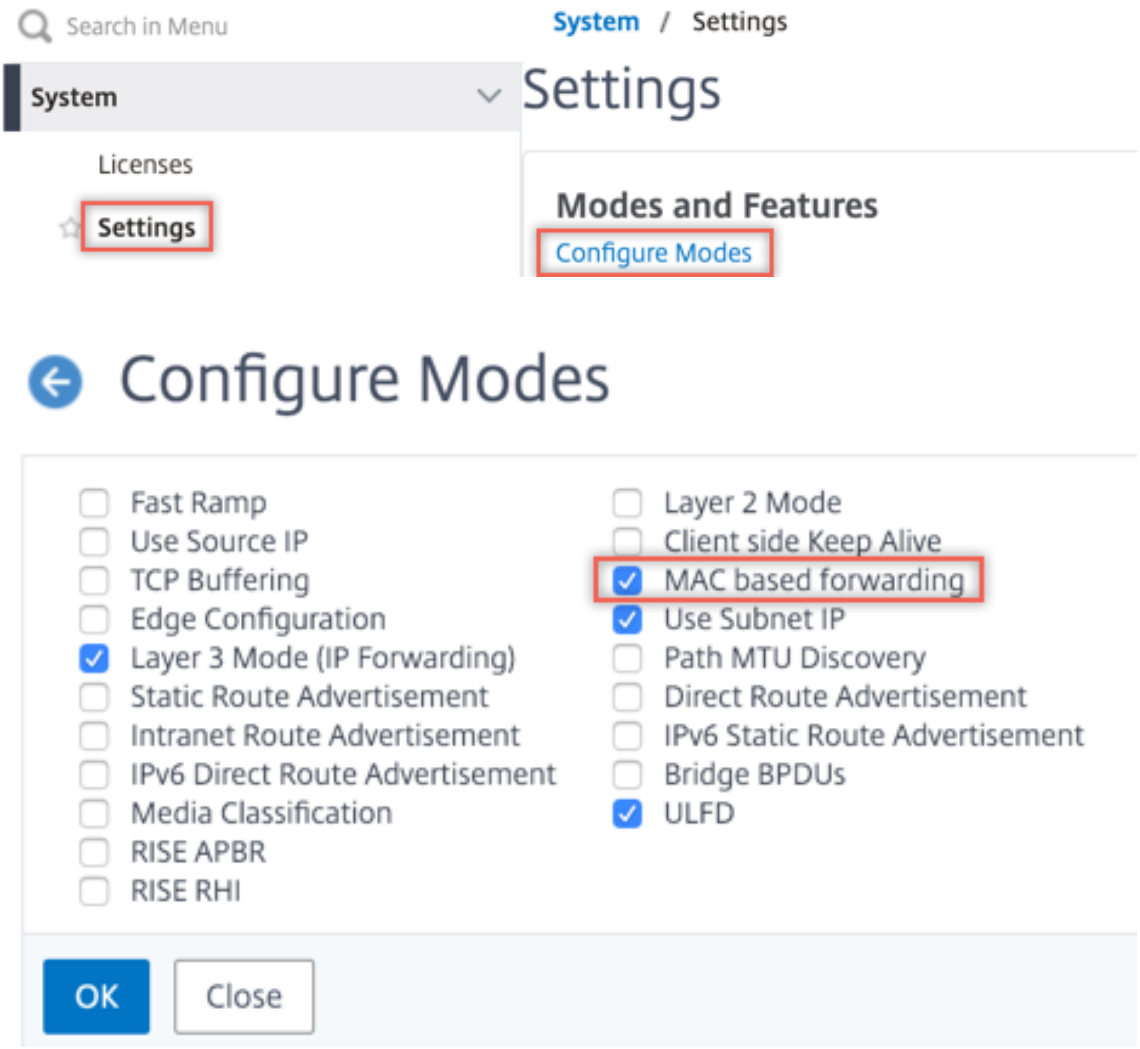
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Exemple :

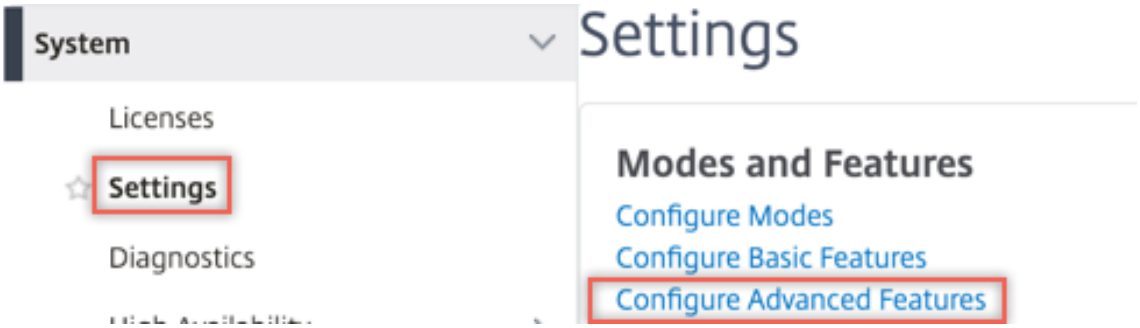
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

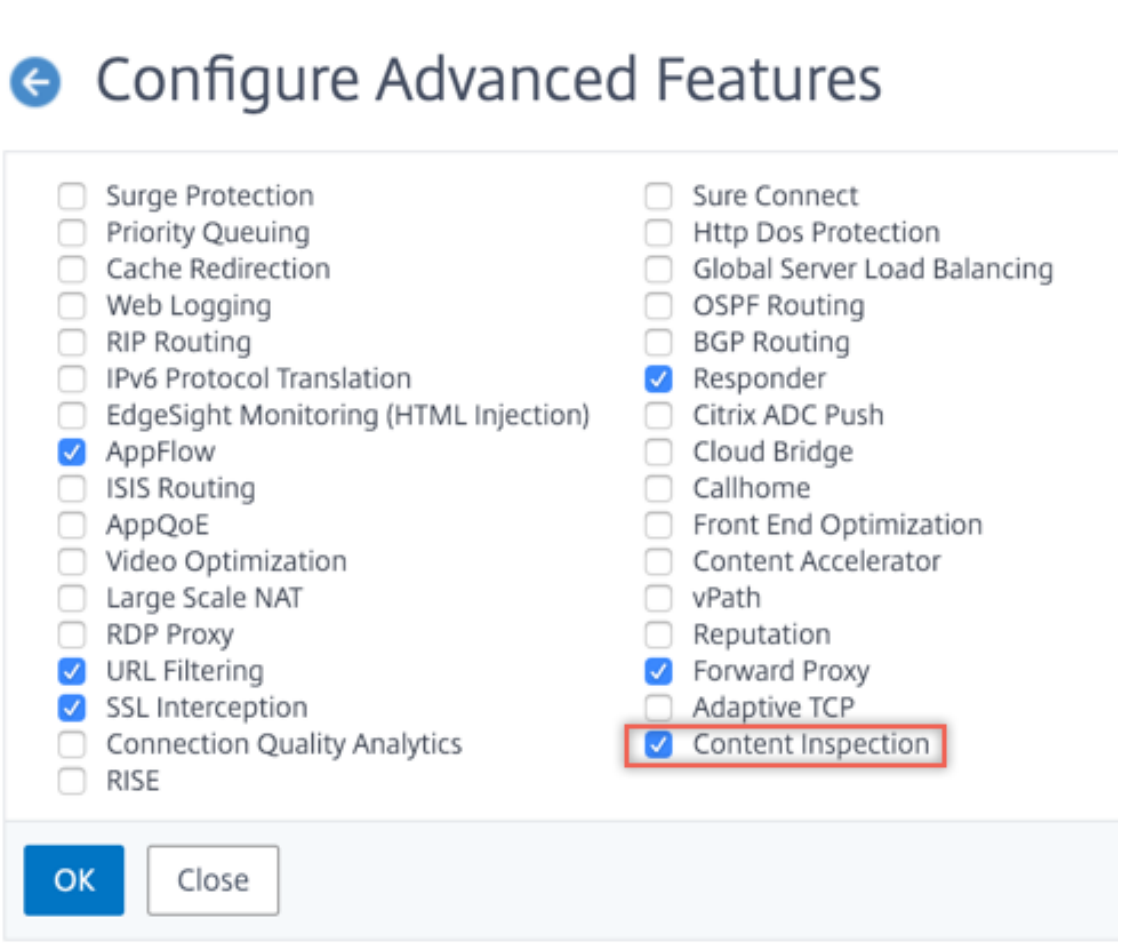
Configuration à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.

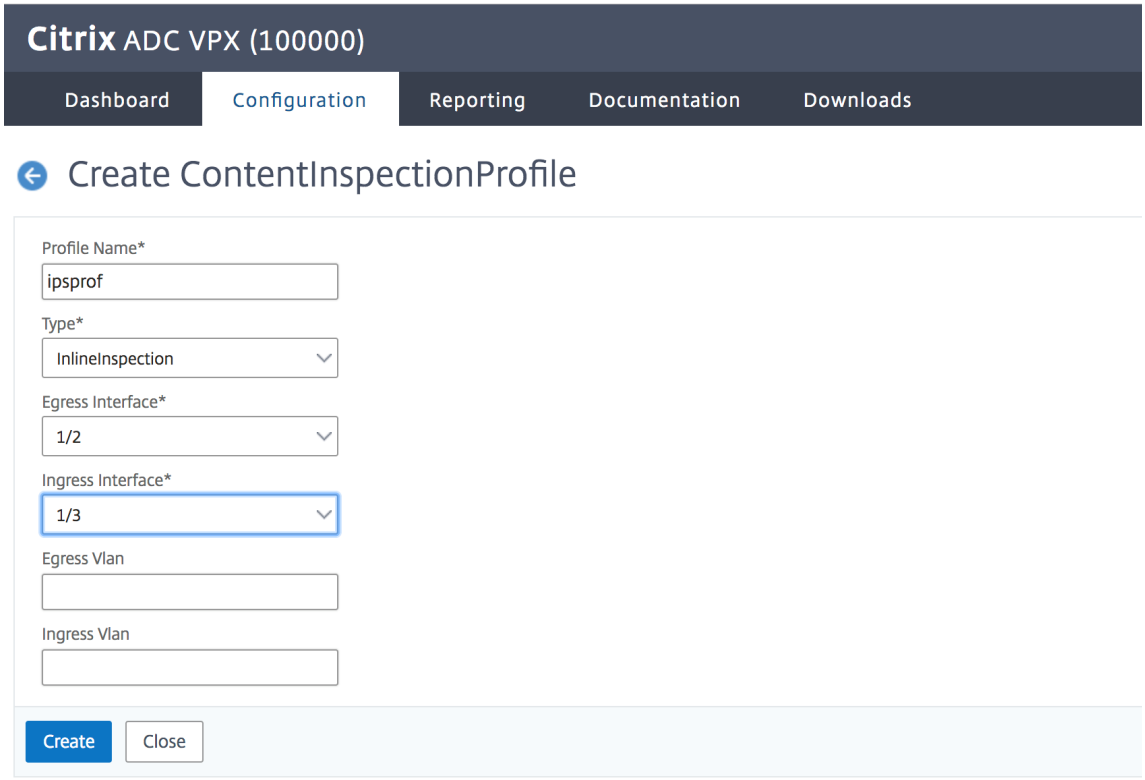


2. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.

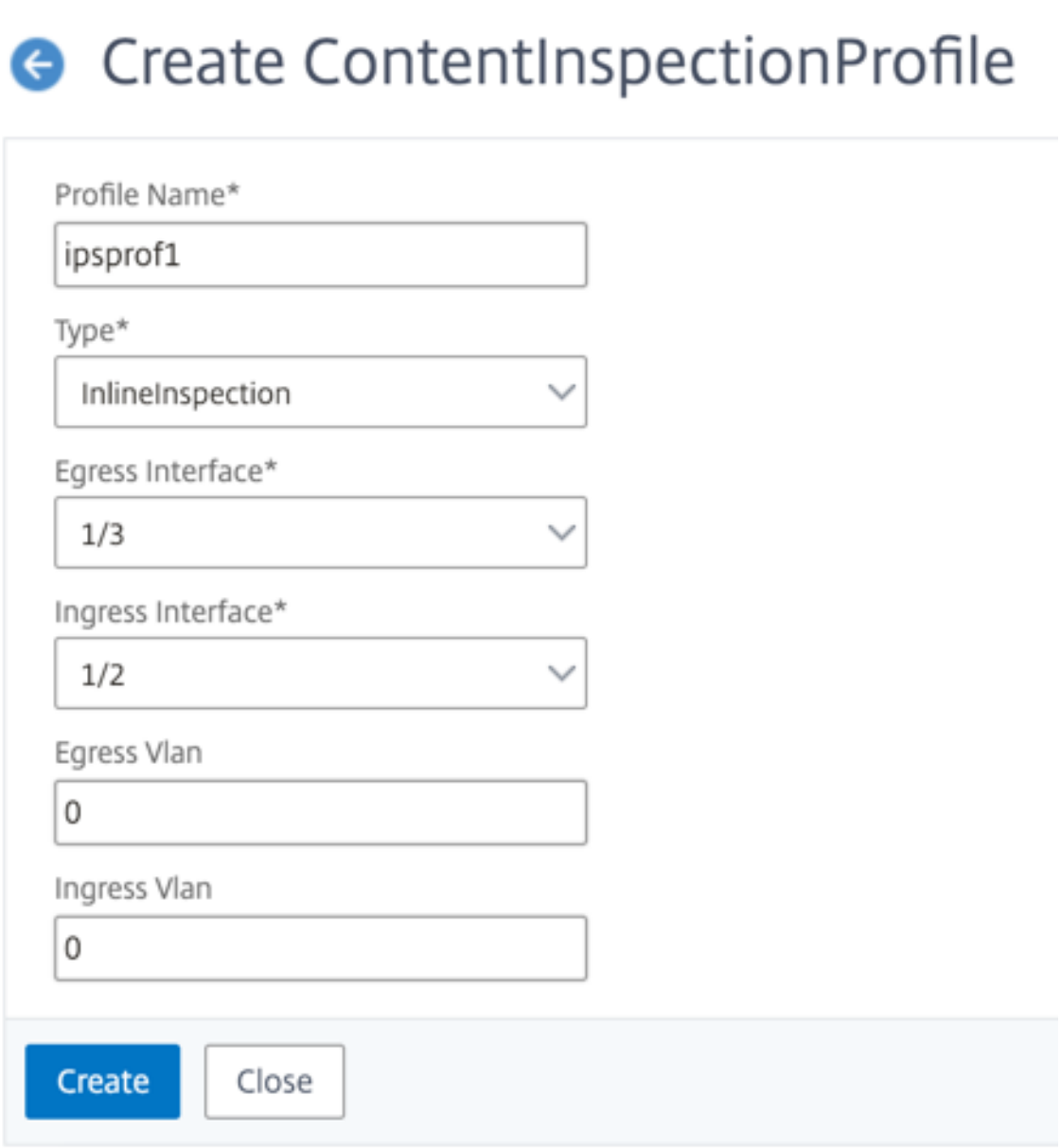




3. Accédez à **Secure Web Gateway > Inspection du contenu > Profils d'inspection du contenu**. Cliquez sur **Ajouter**.

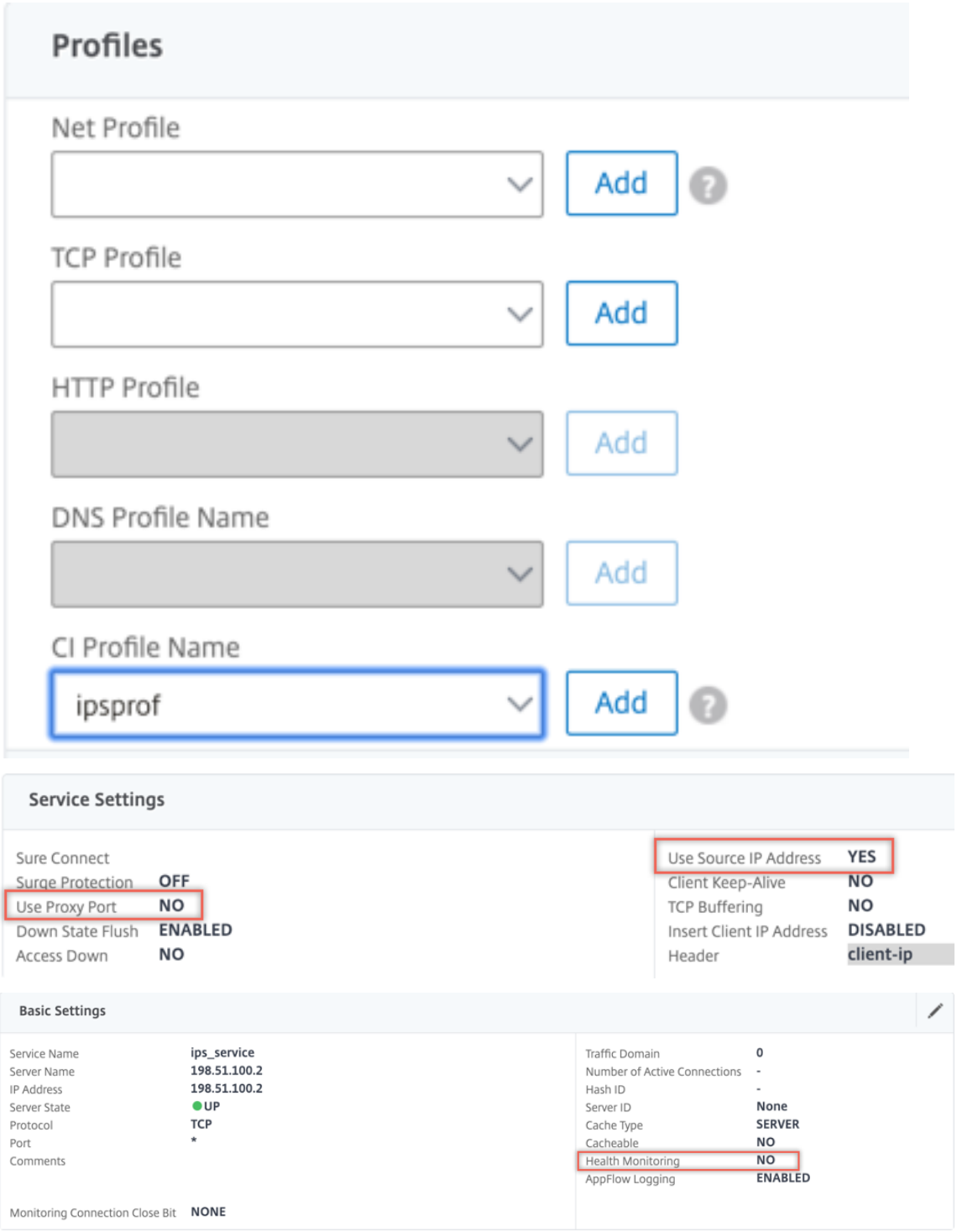


Spécifiez les interfaces d'entrée et de sortie.



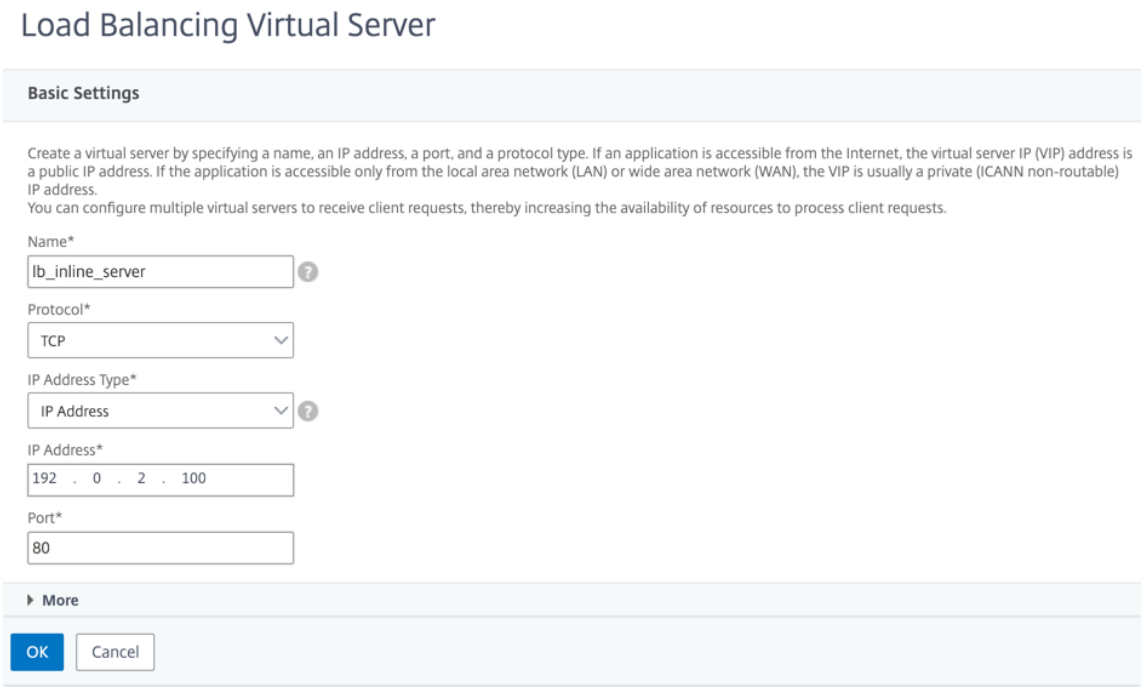
Créez deux profils. Spécifiez une interface d'entrée et de sortie différente dans le second profil.

4. Accédez à **Équilibrage de charge > Services > Ajouter** et ajouter un service. Dans **Paramètres avancés**, cliquez sur **Profils**. Dans la liste **Nom du profil CI**, sélectionnez le profil d'inspection du contenu créé précédemment. Dans **Paramètres de service**, définissez **Utiliser l'adresse IP source**sur YES et **Utiliser le port proxy**sur Non. Dans **Paramètres de base**, définissez le **contrôle de l'intégrité** sur NO. Activez la surveillance de l'intégrité uniquement si vous liez ce service à un moniteur TCP. Si vous liez un moniteur à un service, définissez l'option TRANSPARENT du moniteur sur ON.



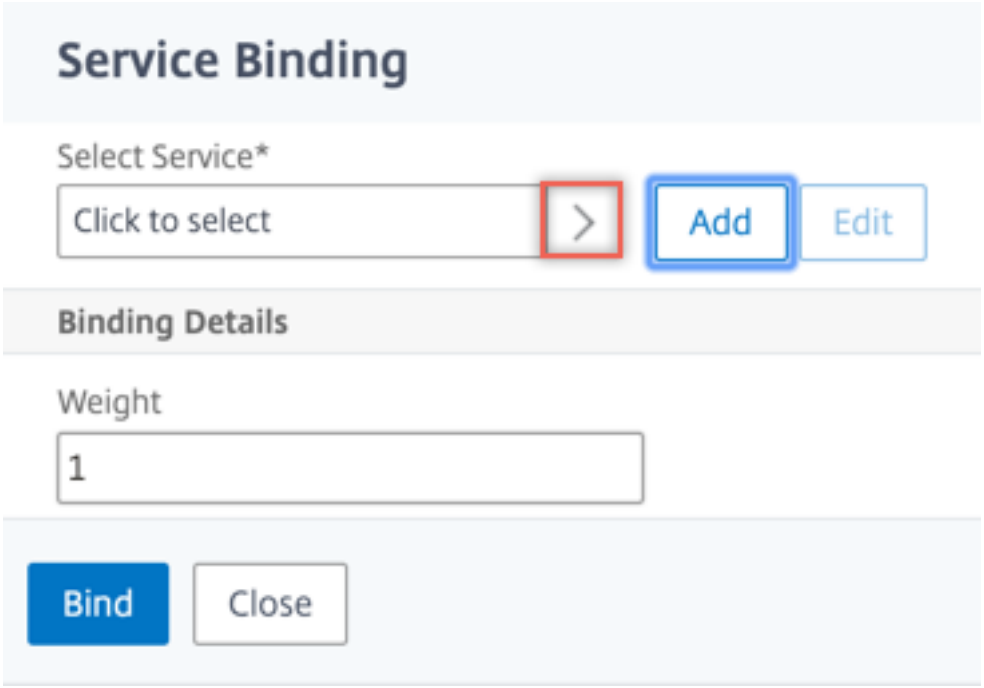
Créez deux services. Spécifiez les adresses IP factices qui ne sont la propriété d'aucun des périphériques, y compris les périphériques en ligne.

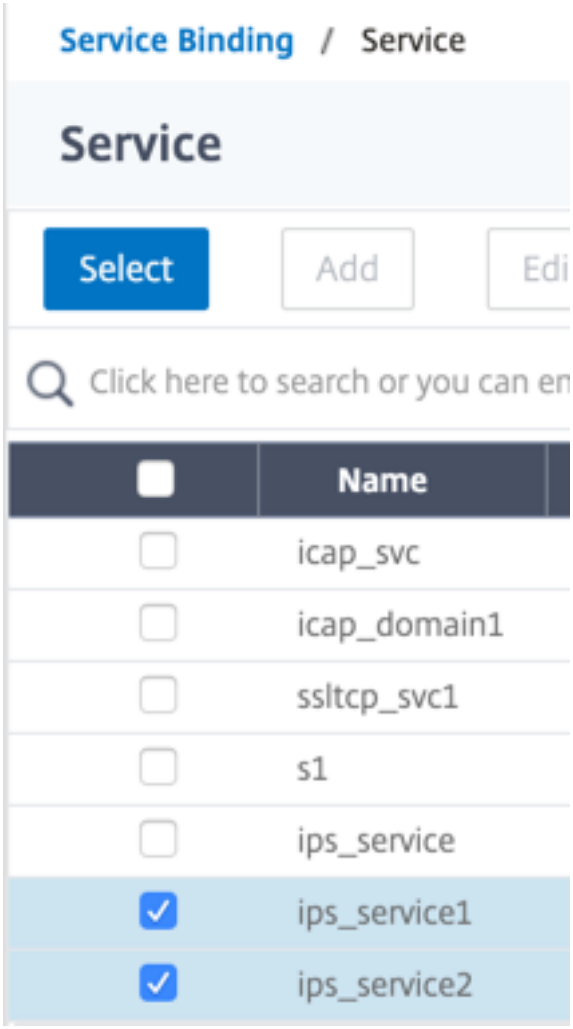
5. Accédez à **Équilibrage de charge > Serveurs virtuels > Ajouter**. Créez un serveur virtuel d'équilibrage de charge TCP.

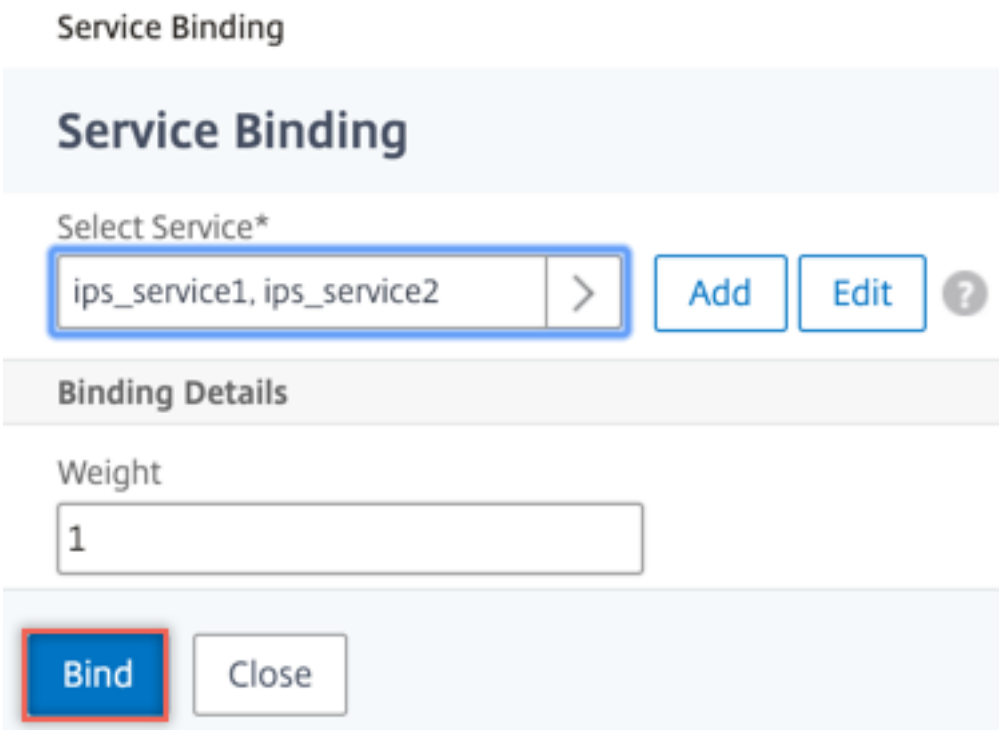


Cliquez sur **OK**.

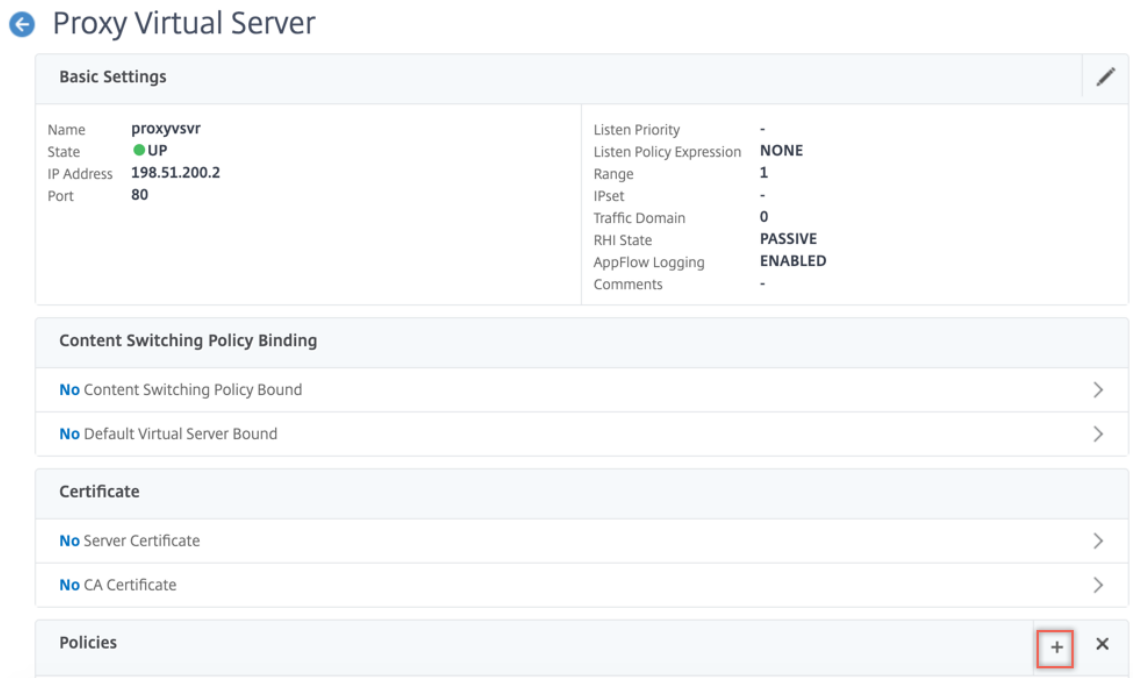
6. Cliquez dans la section **Load Balancing Virtual Server Service Liaison**. Dans **Liaison de service**, cliquez sur la flèche dans **Sélectionner un service**. Sélectionnez les deux services créés précédemment, puis cliquez sur **Sélectionner**. Cliquez sur **Bind**.



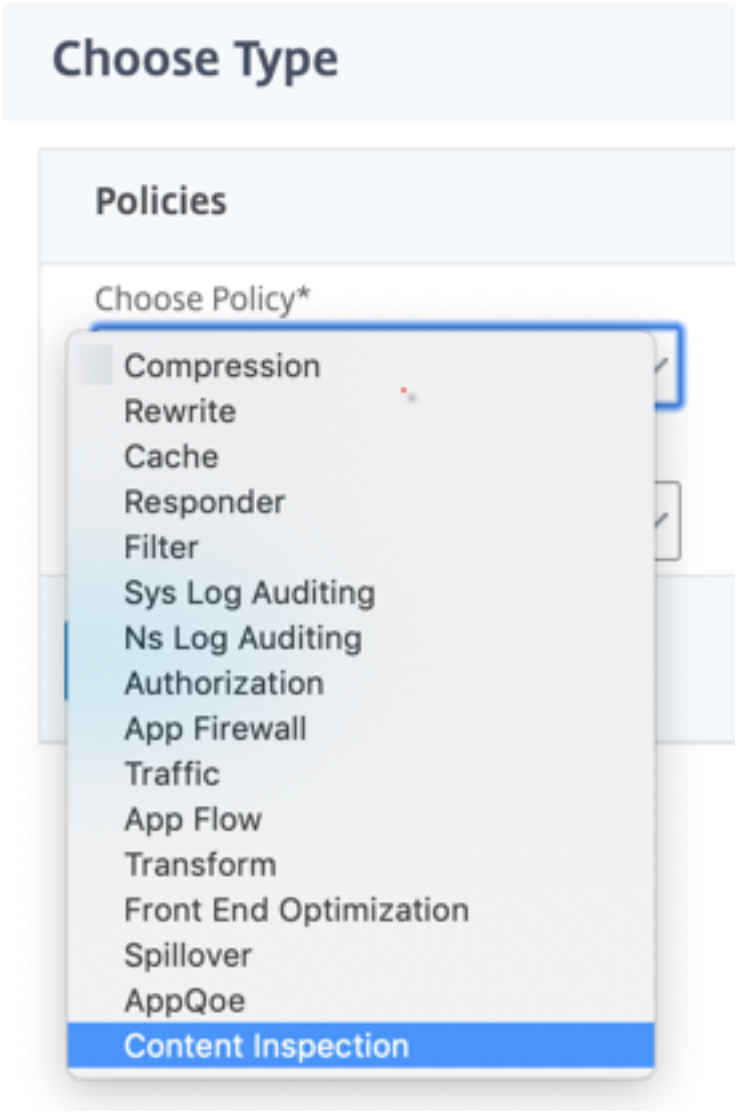




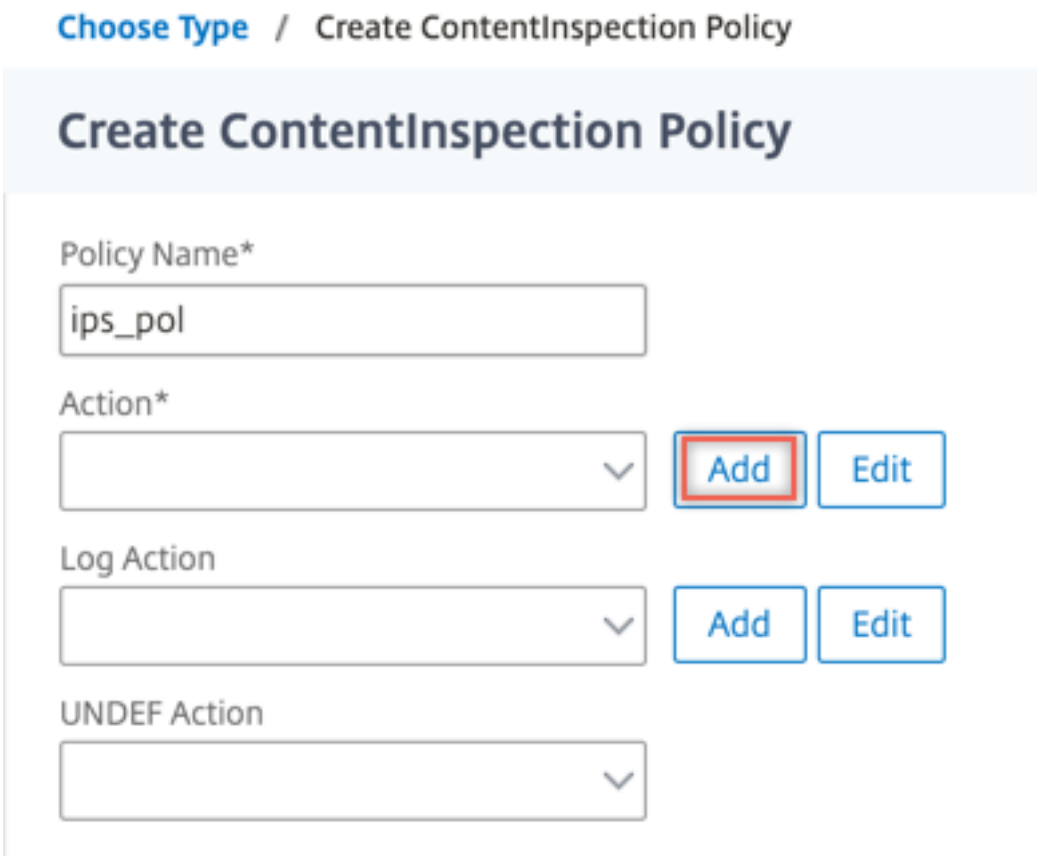
7. Accédez à **Secure Web Gateway > Servers virtuels Proxy > Ajouter**. Spécifiez un nom, une adresse IP et un port. Dans **Paramètres avancés**, sélectionnez **Stratégies**. Cliquez sur le signe « + ».



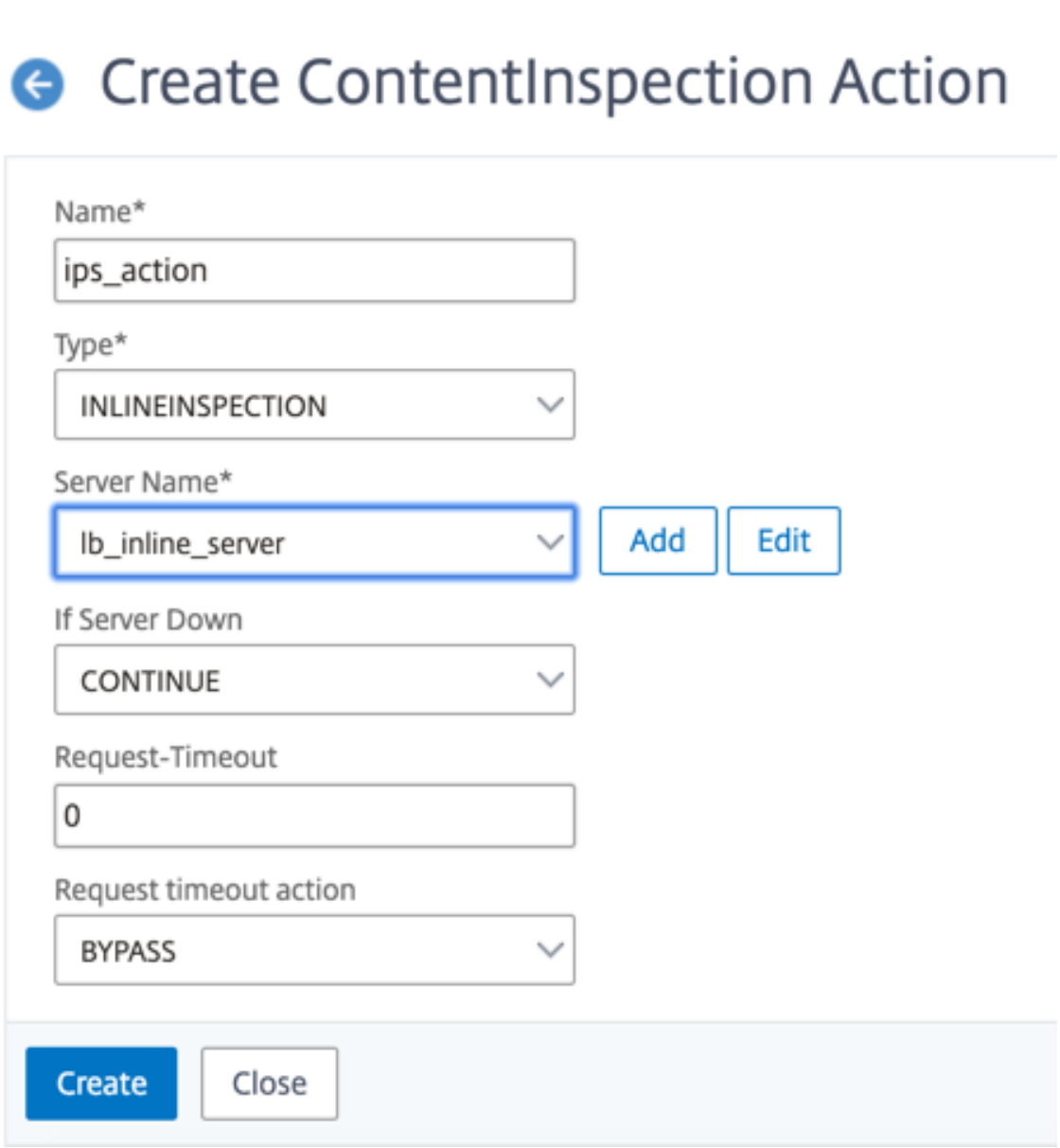
8. Dans **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



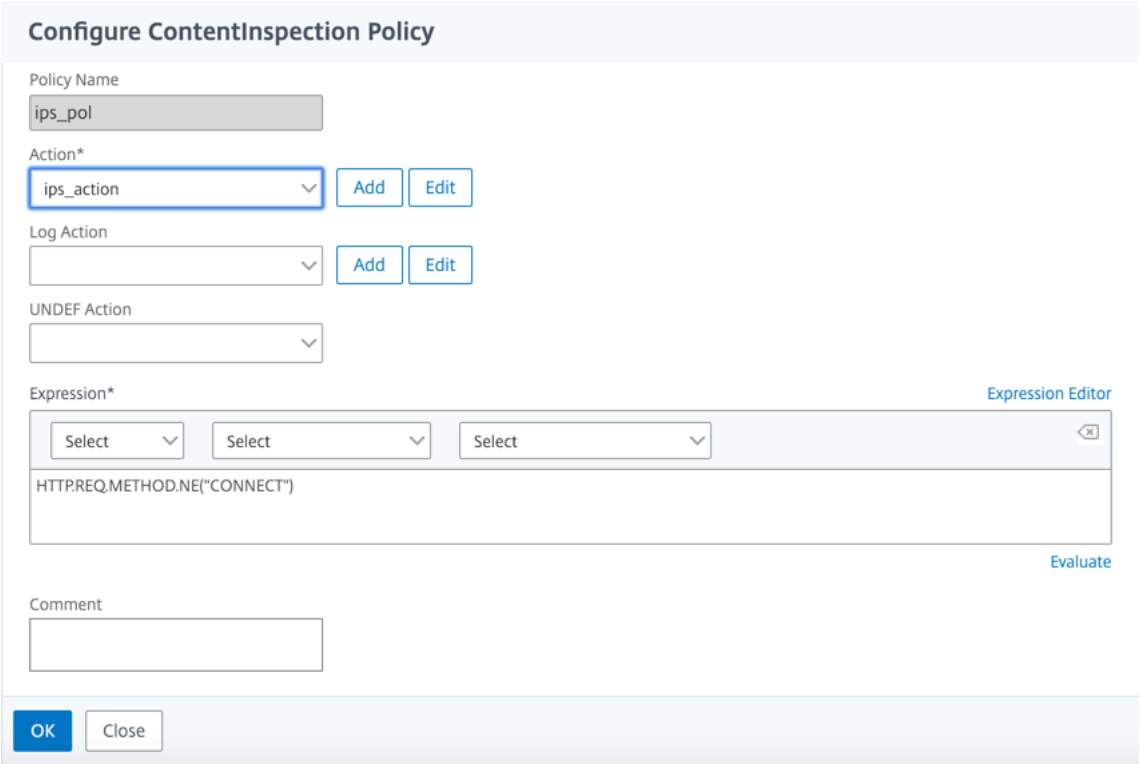
9. Cliquez sur **Ajouter**. Spécifiez un nom. Dans **Action**, cliquez sur **Ajouter**.



10. Spécifiez un nom. Dans **Type**, sélectionnez **INLINEINSPECTION**. Dans **Nom du serveur**, sélectionnez le serveur virtuel d'équilibrage de charge créé précédemment.



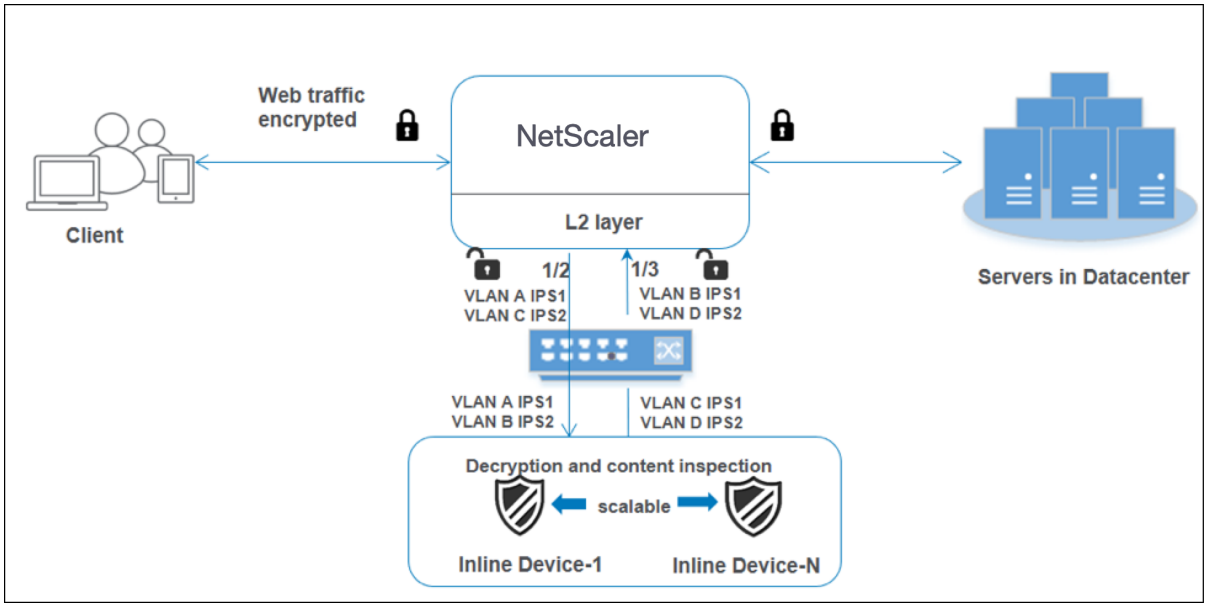
11. Cliquez sur **Créer**. Spécifiez la règle et cliquez sur **Créer**.



12. Cliquez sur **Bind**.
13. Cliquez sur **Terminé**.

Scénario 3 : équilibrage de la charge de plusieurs périphériques en ligne avec des interfaces partagées

Si vous utilisez au moins deux périphériques en ligne, vous pouvez équilibrer la charge des périphériques à l'aide de différents services d'inspection de contenu avec des interfaces partagées. Dans ce cas, la charge de l'appliance proxy de transfert SSL équilibre le sous-ensemble du trafic envoyé à chaque périphérique via une interface partagée. Le sous-ensemble est décidé en fonction des stratégies configurées. Par exemple, les fichiers TXT ou image peuvent ne pas être envoyés pour inspection aux périphériques en ligne.



La configuration de base reste la même que dans le scénario 2. Pour ce scénario, liez les interfaces à différents VLAN pour séparer le trafic de chaque périphérique en ligne. Spécifiez les VLAN dans les profils d'inspection de contenu. Effectuez les étapes supplémentaires suivantes :

1. Liez les interfaces partagées à différents VLAN.
2. Spécifiez les VLAN d'entrée et de sortie dans les profils d'inspection de contenu.

Configuration à l'aide de l'interface de ligne de commande

Tapez les commandes suivantes à l'invite de commandes. Des exemples sont donnés après chaque commande.

1. Activez MBF.

```
enable ns mode mbf
```

1. Activez la fonctionnalité.

```
enable ns feature contentInspection
```

1. Liez les interfaces partagées à différents VLAN.

```
bind vlan <id> -ifnum <interface> -tagged
```

Exemple :

```
bind vlan 100  - ifnum 1/2 tagged
bind vlan 200  - ifnum 1/3 tagged
bind vlan 300  - ifnum 1/2 tagged
bind vlan 400  - ifnum 1/3 tagged
<!--NeedCopy-->
```


1. Ajouter le profil 1 pour le service 1. Spécifiez les VLAN d'entrée et de sortie dans le profil.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile ipsprof1 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 100 -ingressVlan 300
```

1. Ajouter le profil 2 pour le service 2. Spécifiez les VLAN d'entrée et de sortie dans le profil.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile ipsprof2 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 200 -ingressVlan 400
```

1. Ajouter le service 1.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Ajouter le service 2.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Exemple :

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Ajoutez un serveur virtuel d'équilibrage de charge.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Exemple :

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

1. Liez les services au serveur virtuel d'équilibrage de charge.


```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Exemple :

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Spécifiez le serveur virtuel d'équilibrage de charge dans l'action d'inspection du contenu.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Exemple :

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Ajoutez une stratégie d'inspection du contenu. Spécifiez l'action d'inspection du contenu dans la stratégie.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Exemple :

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Ajoutez un serveur virtuel proxy.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Exemple :

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Liez la stratégie d'inspection de contenu au serveur virtuel.

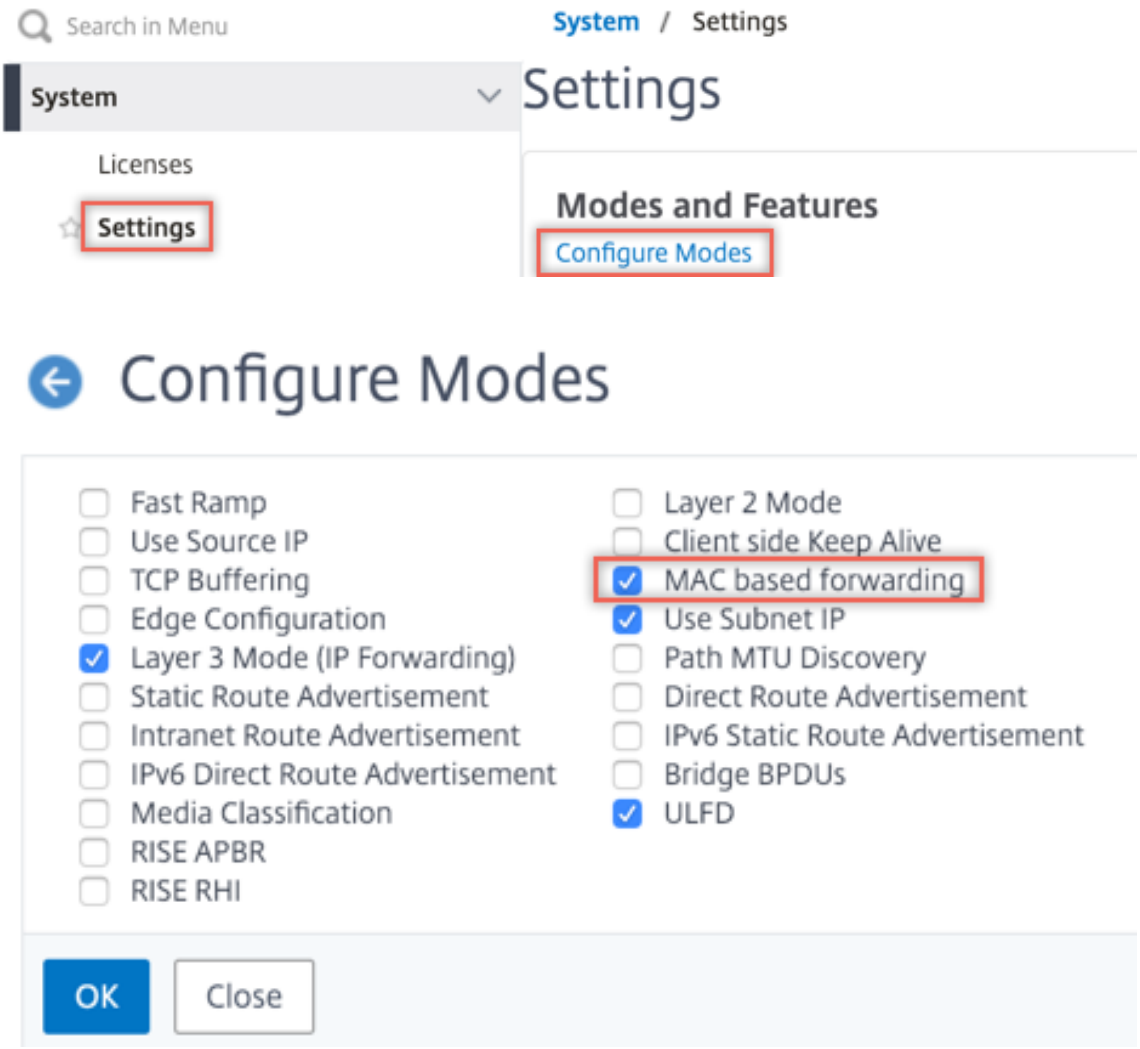
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Exemple :

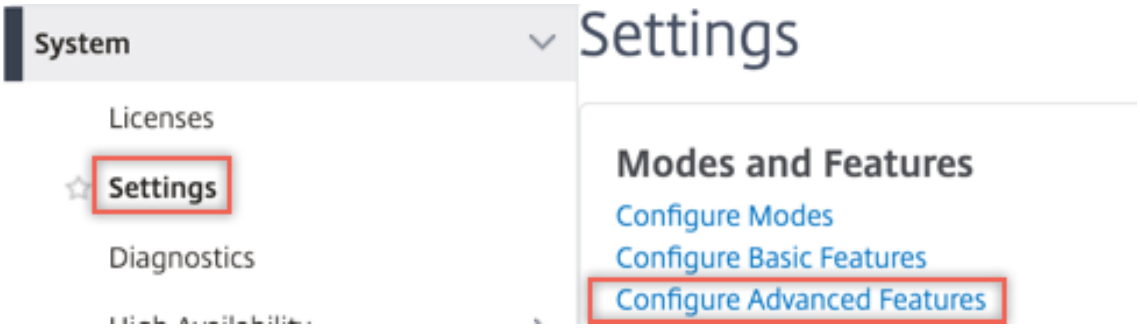
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

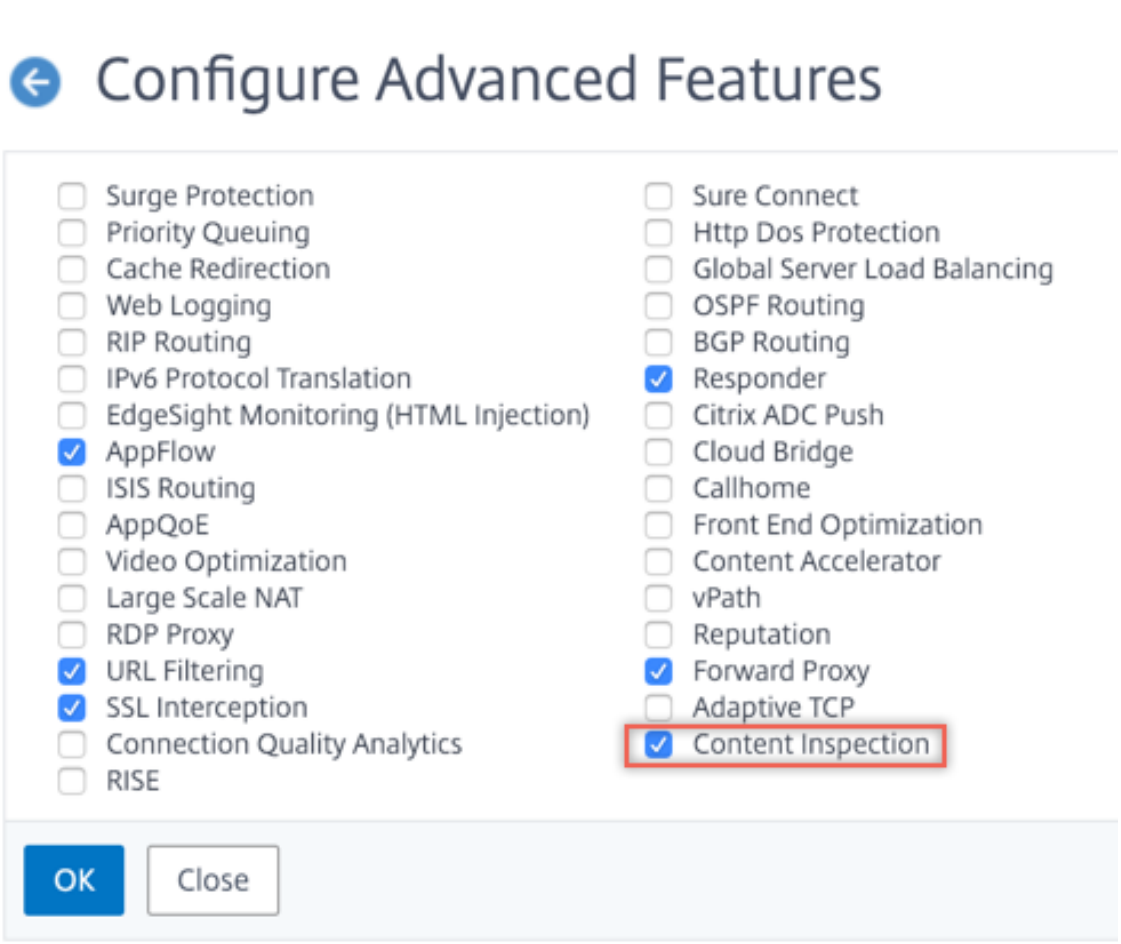
Configuration à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les modes**.

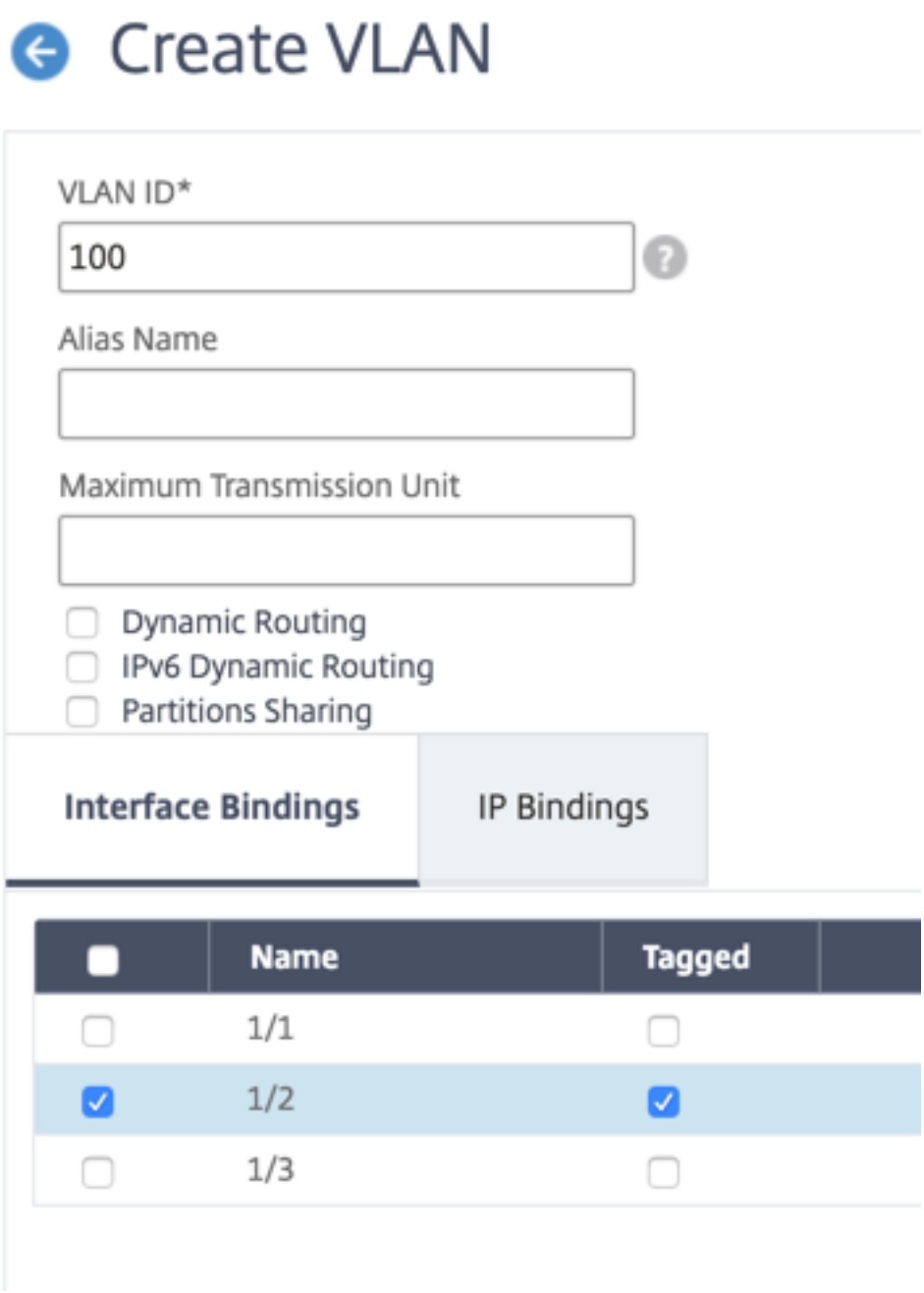


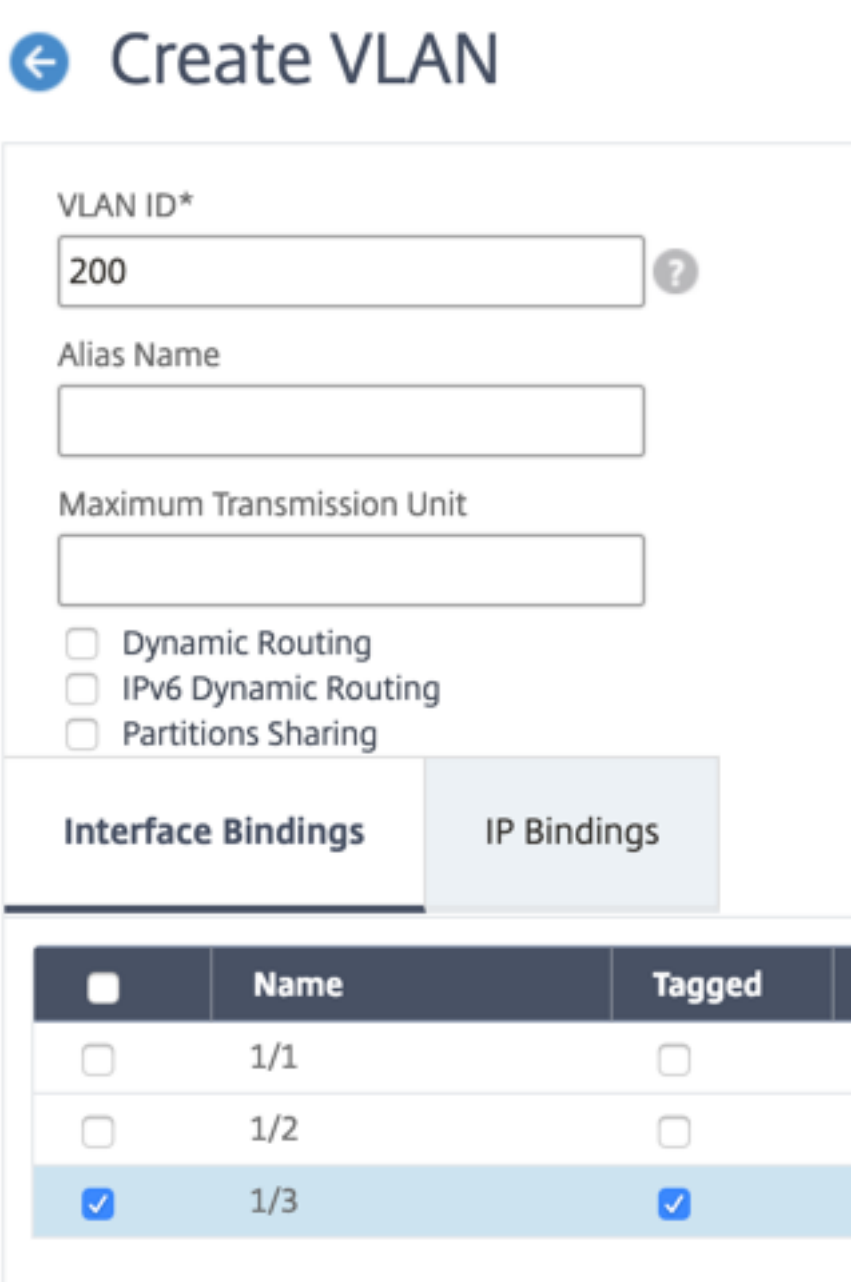
2. Accédez à **Système > Paramètres**. Dans **Modes et fonctionnalités**, cliquez sur **Configurer les fonctionnalités avancées**.

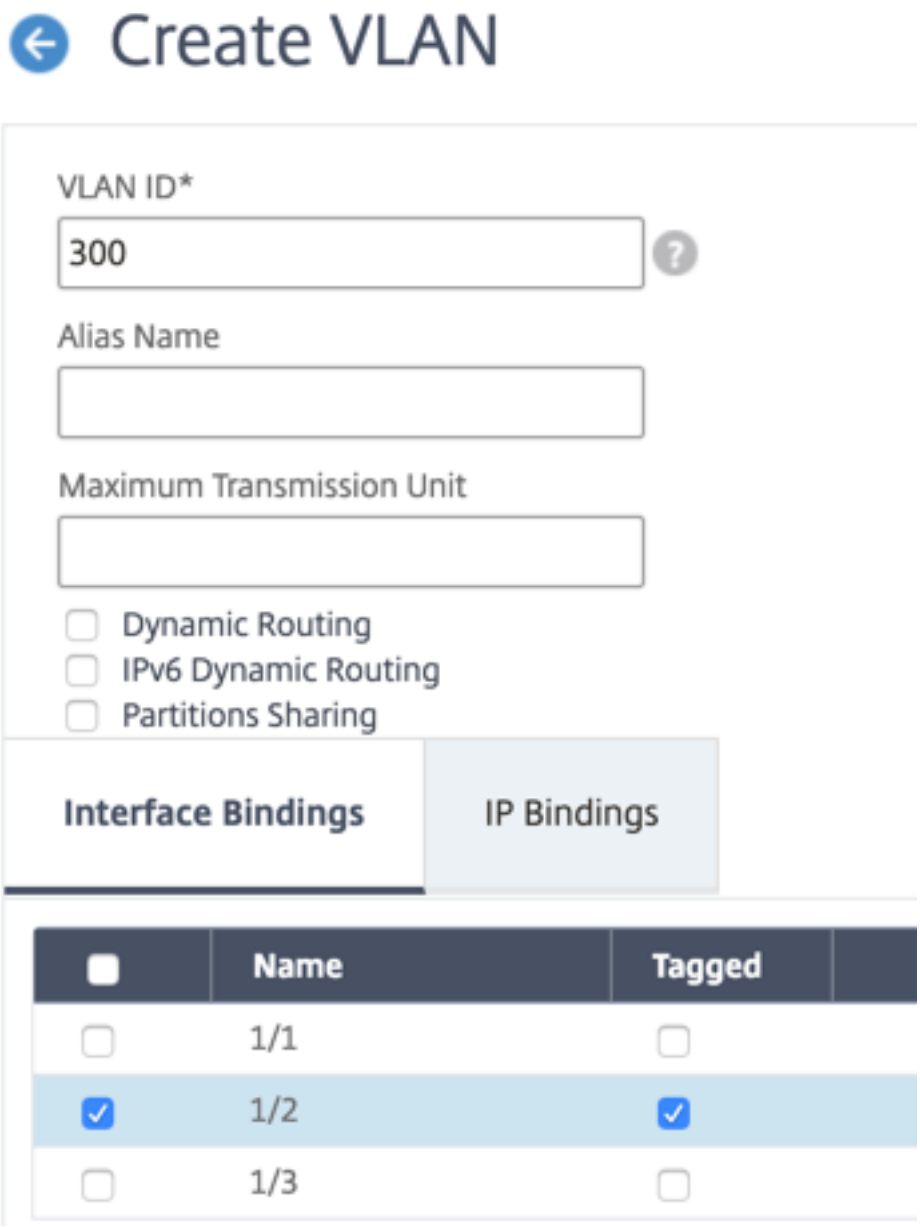


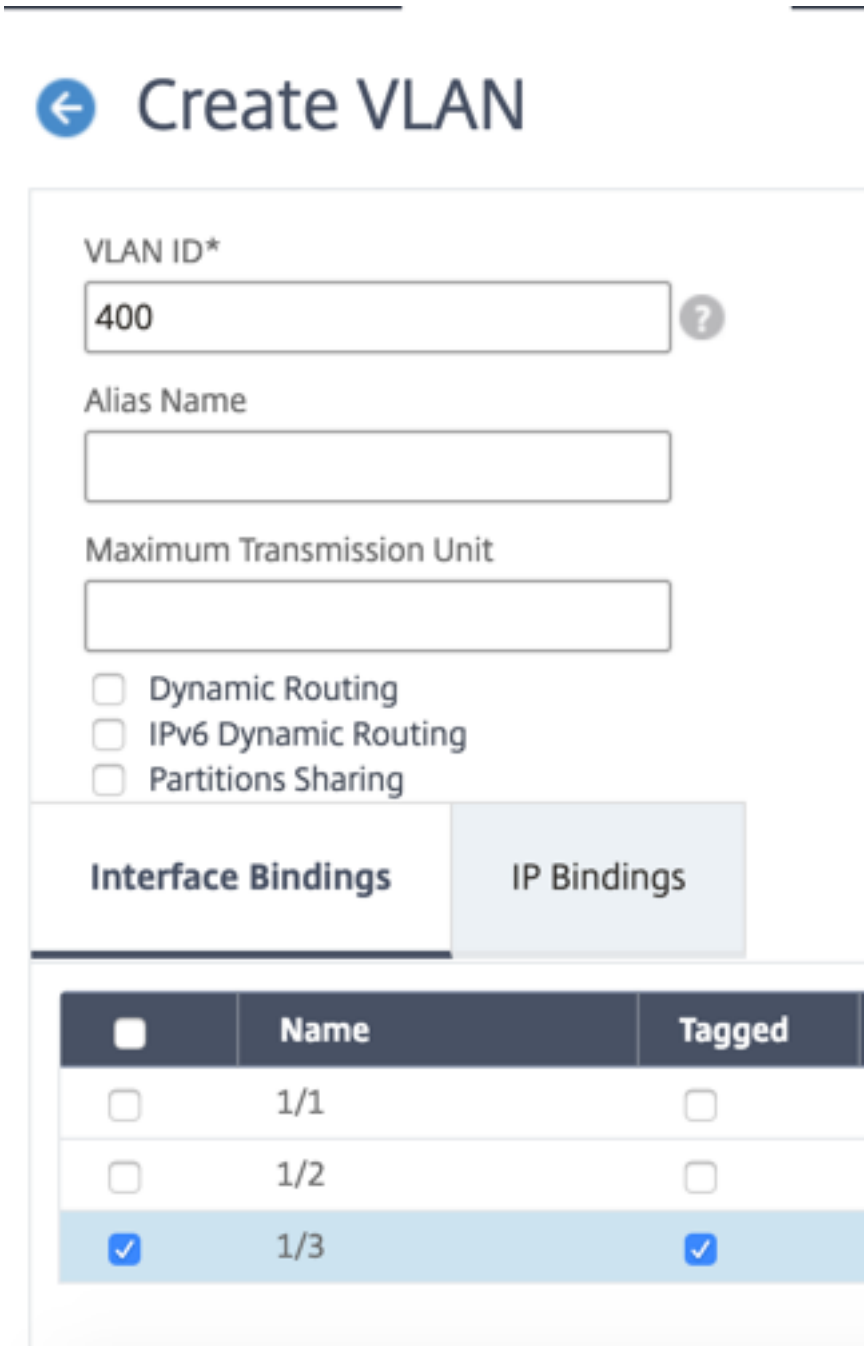


3. Accédez à **Système > Réseau > VLAN > Ajouter**. Ajoutez quatre VLAN et marquez-les sur les interfaces.

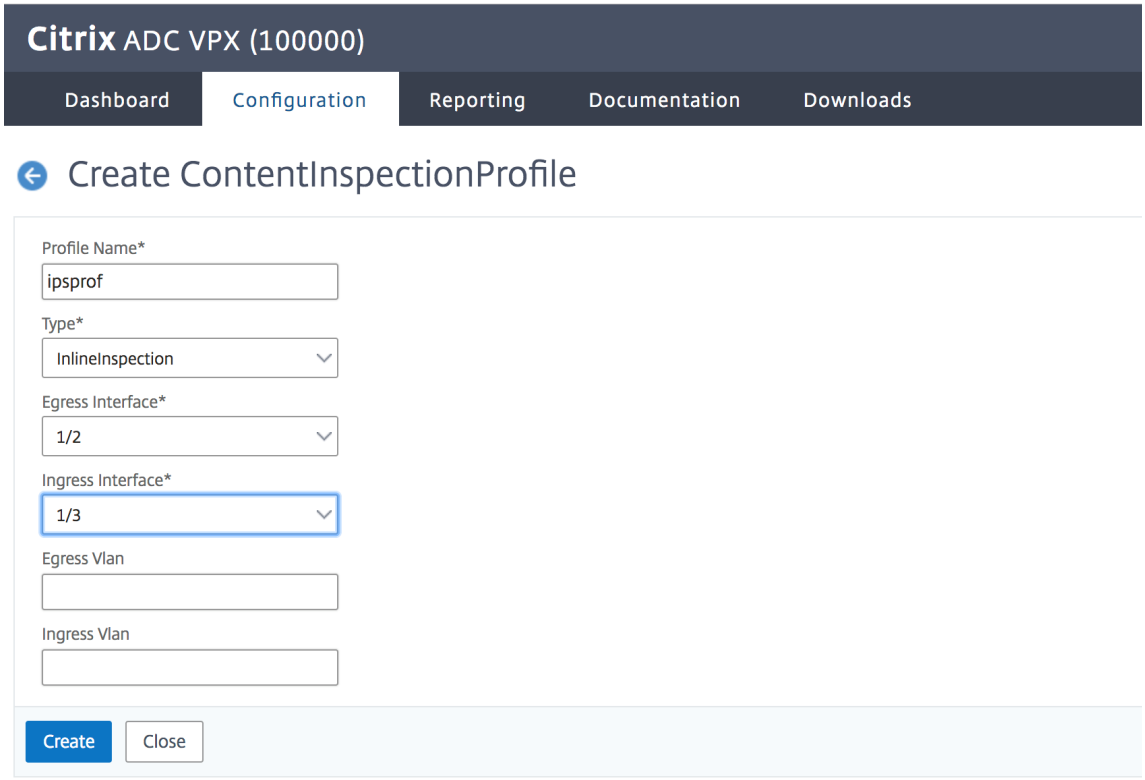




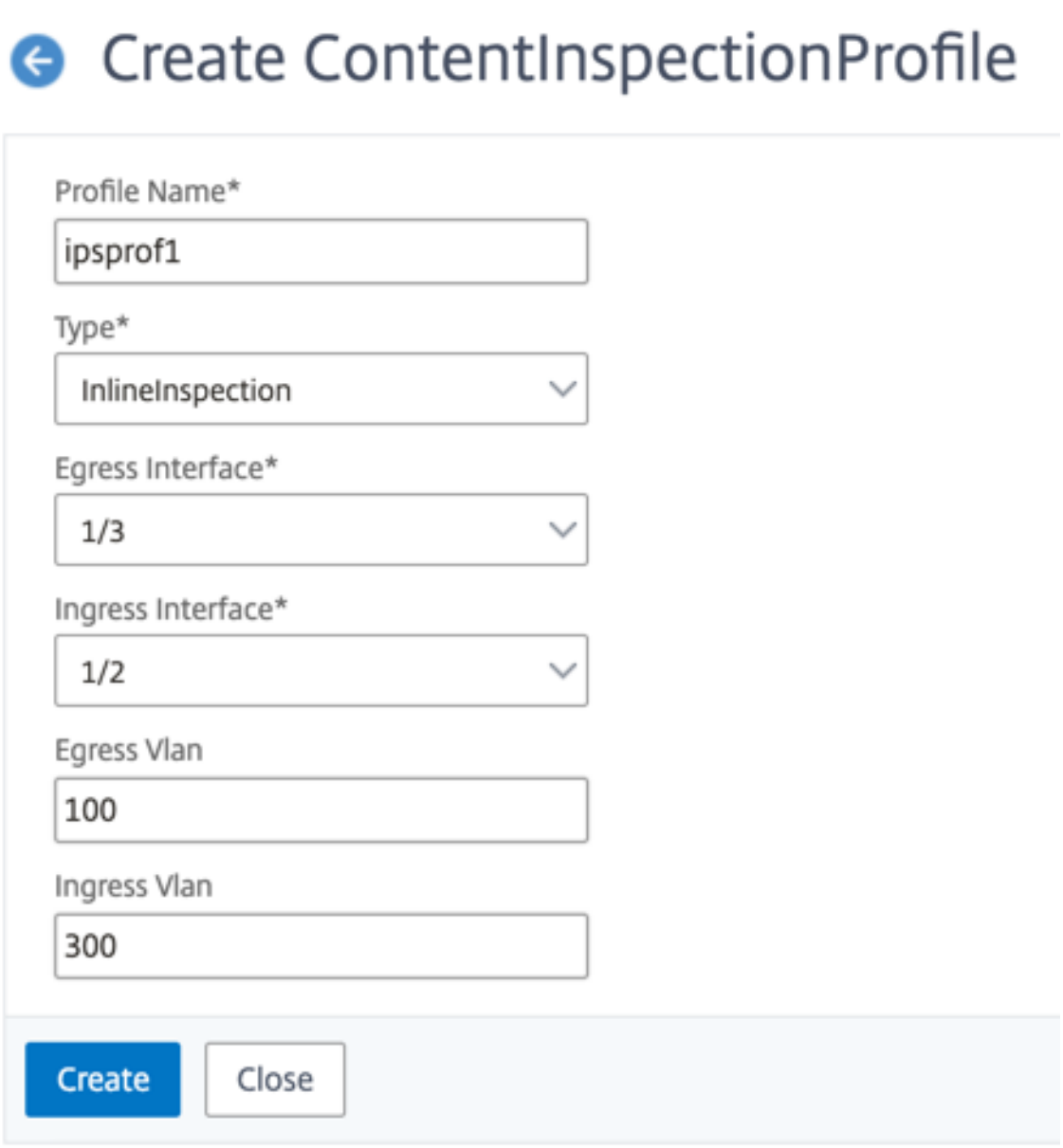




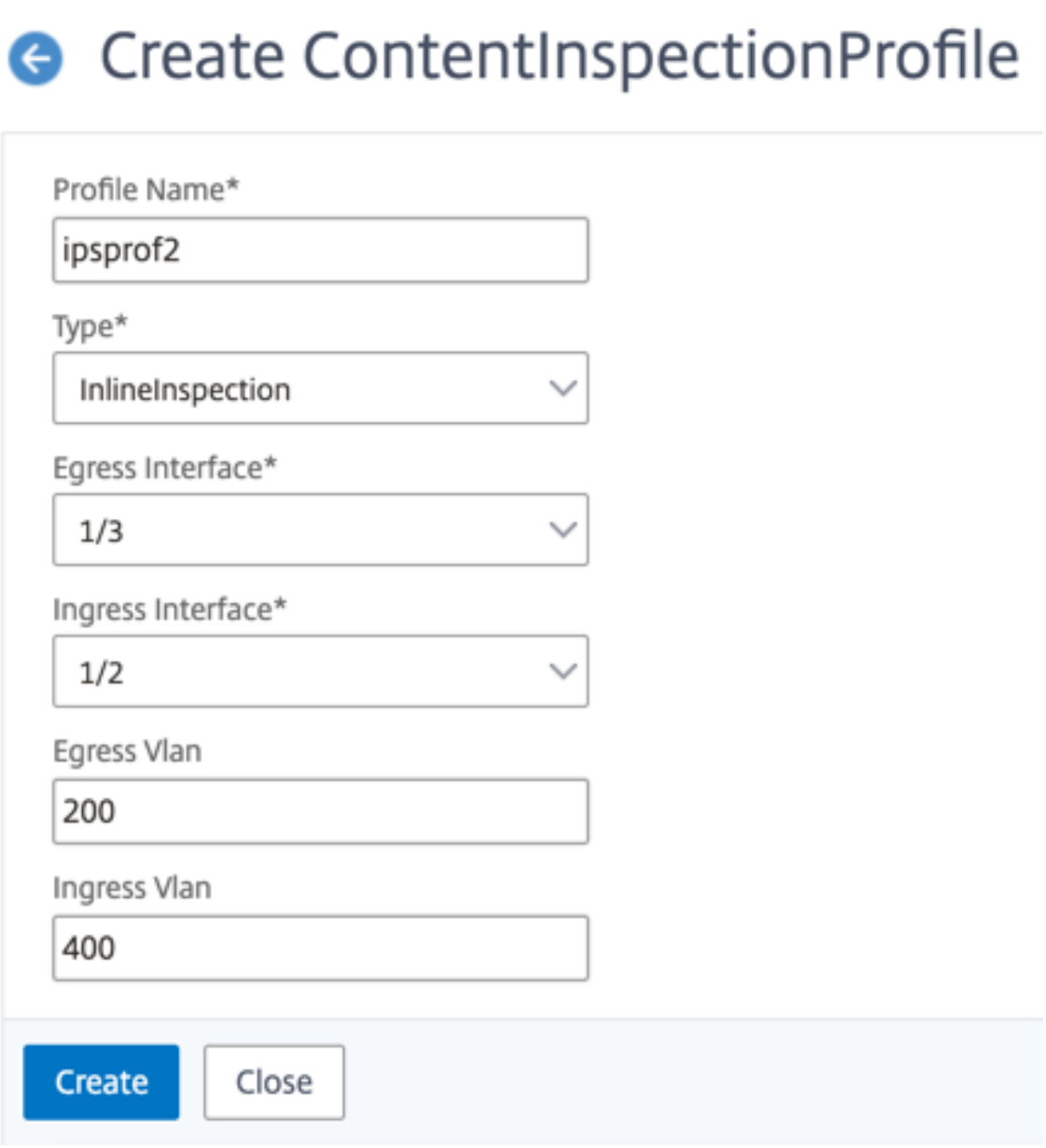
4. Accédez à **Secure Web Gateway > Inspection du contenu > Profils d'inspection du contenu**. Cliquez sur **Ajouter**.



Spécifiez les VLAN d'entrée et de sortie.

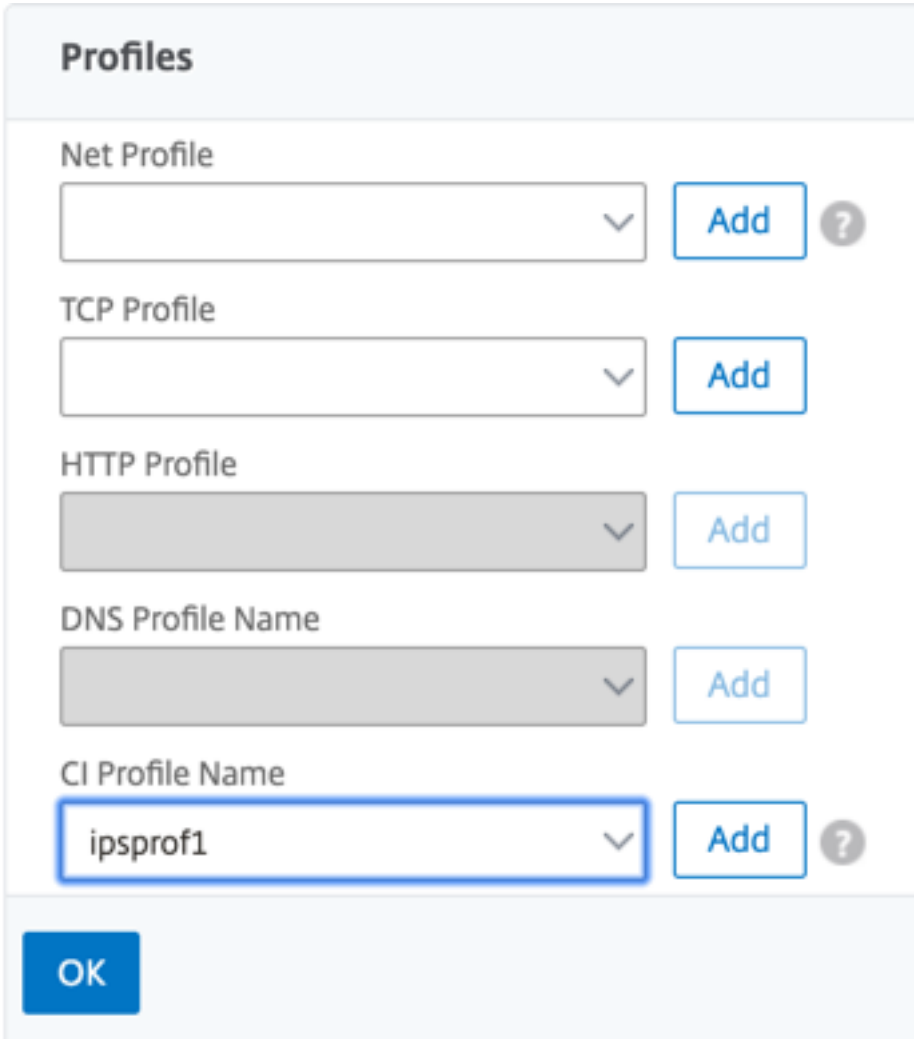


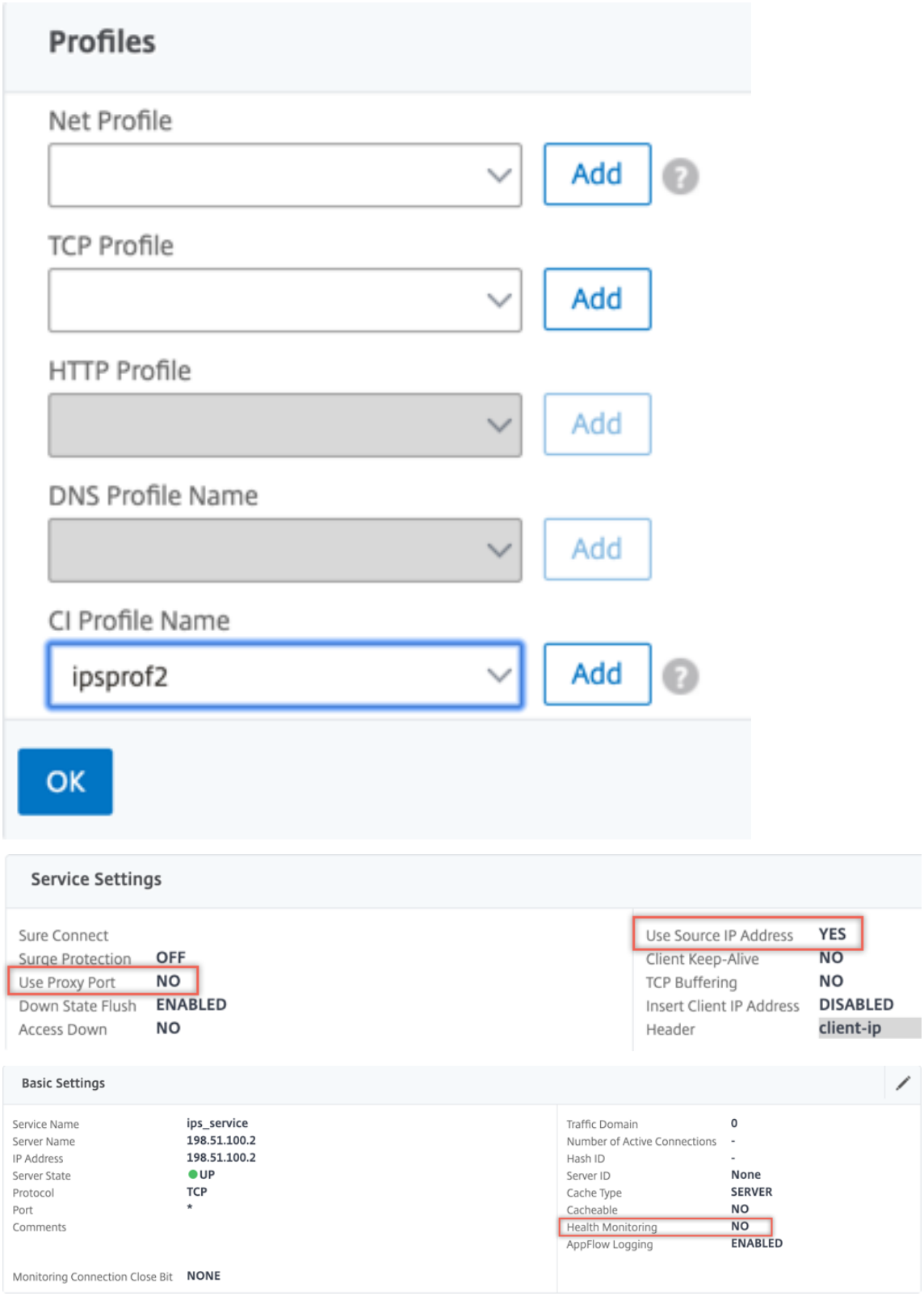
Créez d'autres profils. Spécifiez un VLAN d'entrée et de sortie différent dans le second profil.



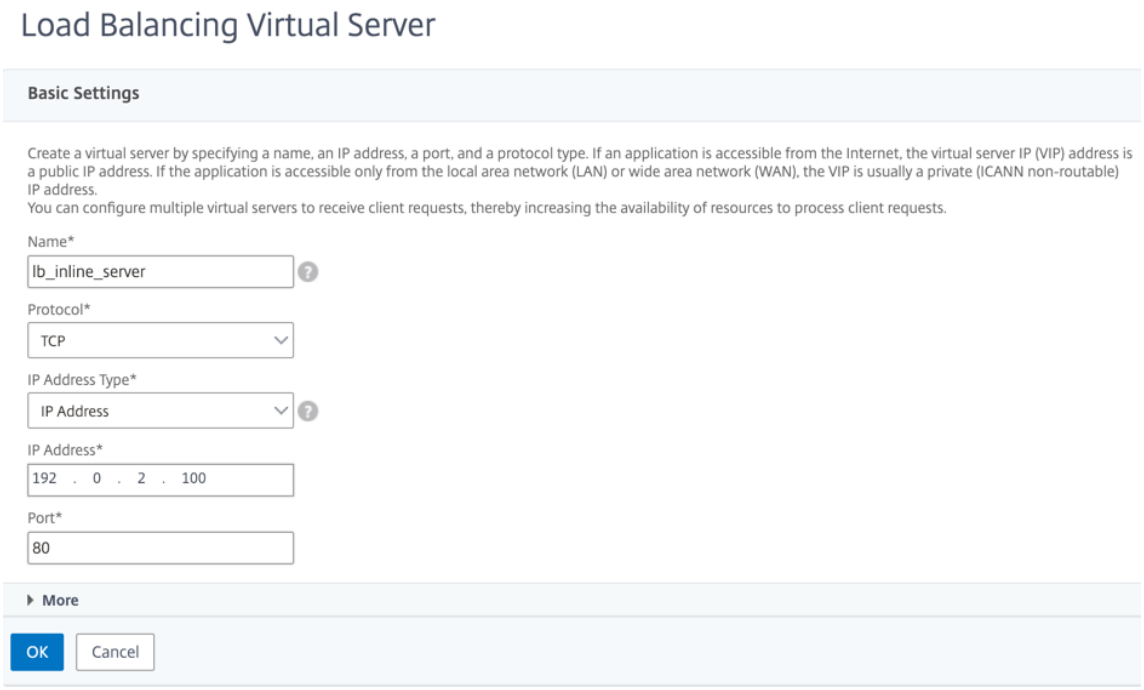
5. Accédez à **Équilibrage de charge > Services > Ajouter** et ajouter un service. Dans **Paramètres avancés**, cliquez sur **Profils**. Dans la liste **Nom du profil CI**, sélectionnez le profil d'inspection du contenu créé précédemment. Dans **Paramètres de service**, définissez **Utiliser l'adresse IP source**sur YES et **Utiliser le port proxy**sur Non. Dans **Paramètres de base**, définissez le **contrôle de l'intégrité** sur NO.

   Créez deux services. Spécifiez les adresses IP factices qui ne sont la propriété d'aucun des périphériques, y compris les périphériques en ligne. Spécifiez le profil 1 dans le service 1 et le profil 2 dans le service 2.

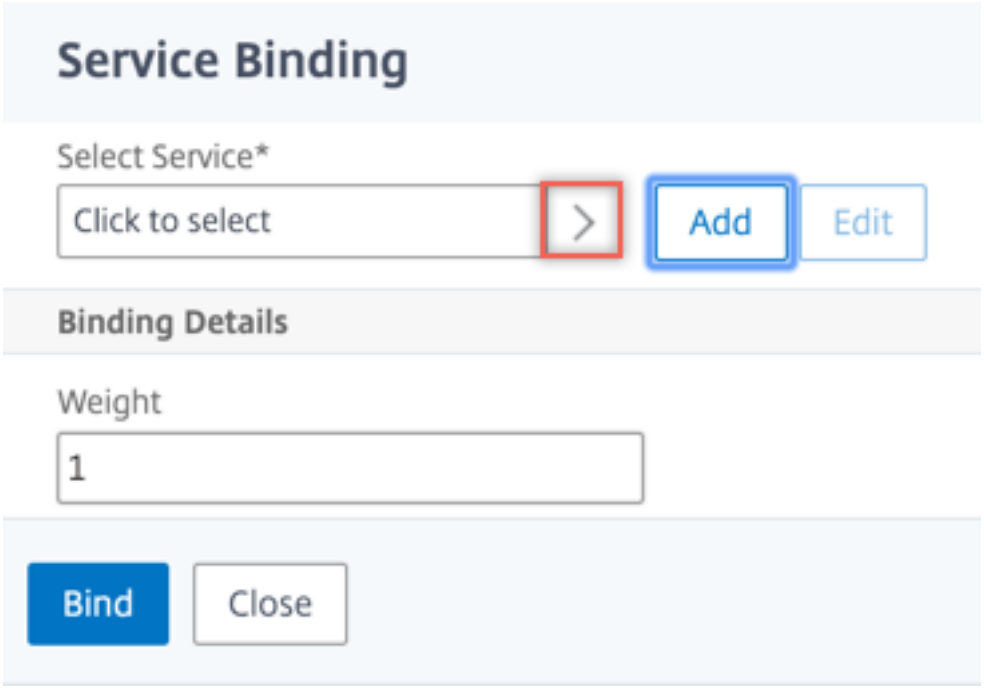


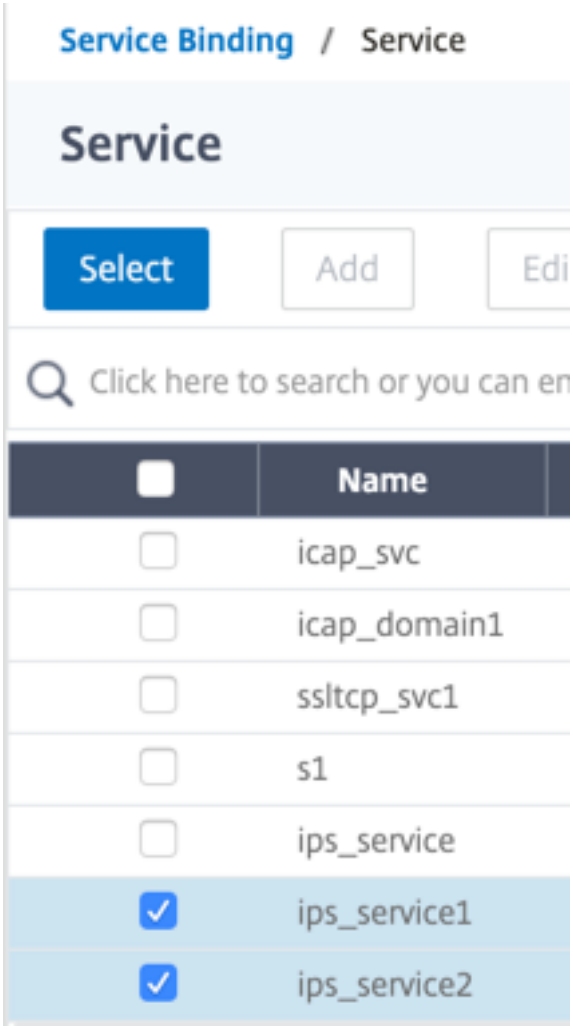


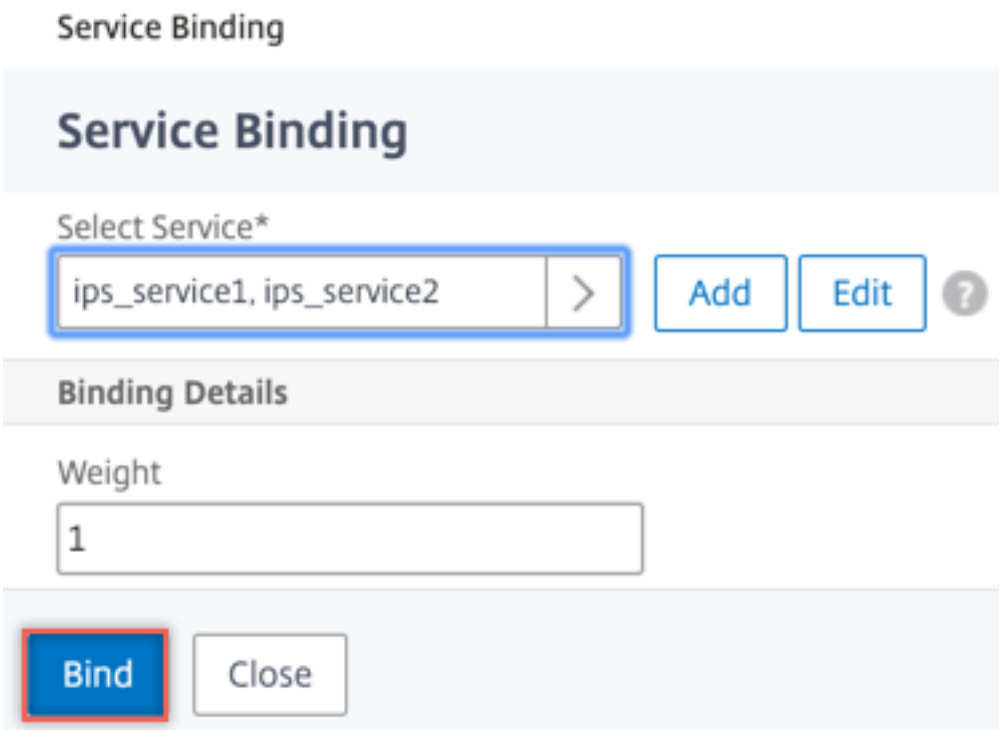
6. Accédez à **Équilibrage de charge > Serveurs virtuels > Ajouter**. Créez un serveur virtuel d'équilibrage de charge TCP.



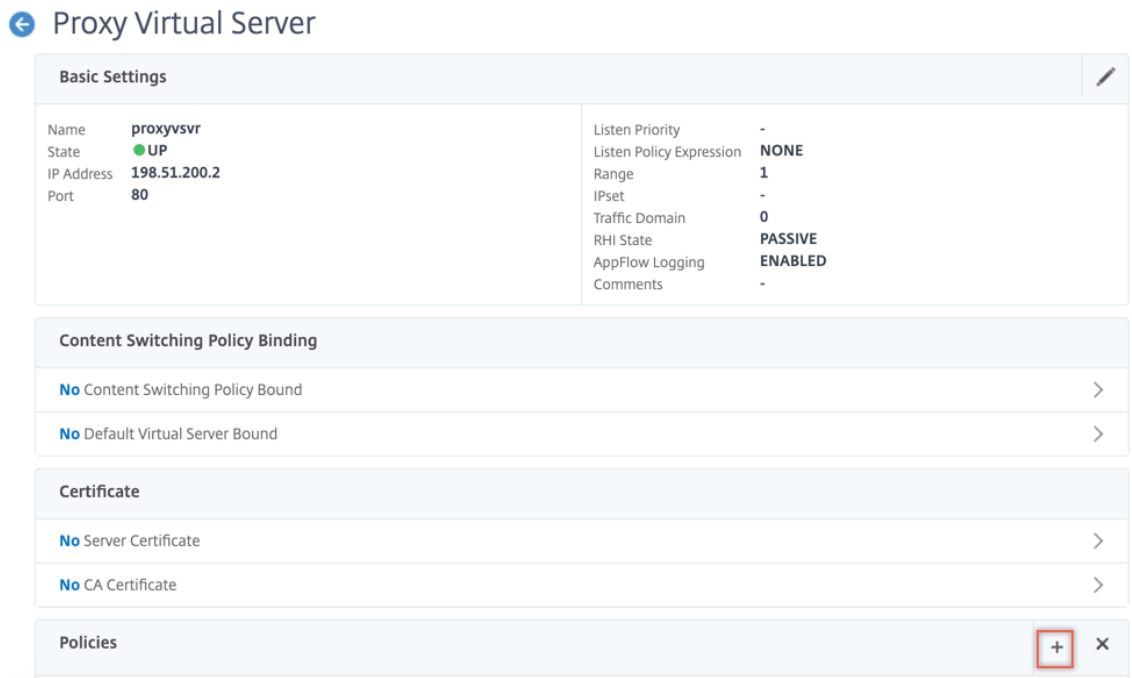
7. Cliquez sur **OK**.
8. Cliquez dans la section **Load Balancing Virtual Server Service Liaison**. Dans **Liaison de service**, cliquez sur la flèche dans **Sélectionner un service**. Sélectionnez les deux services créés précédemment, puis cliquez sur **Sélectionner**. Cliquez sur **Bind**.



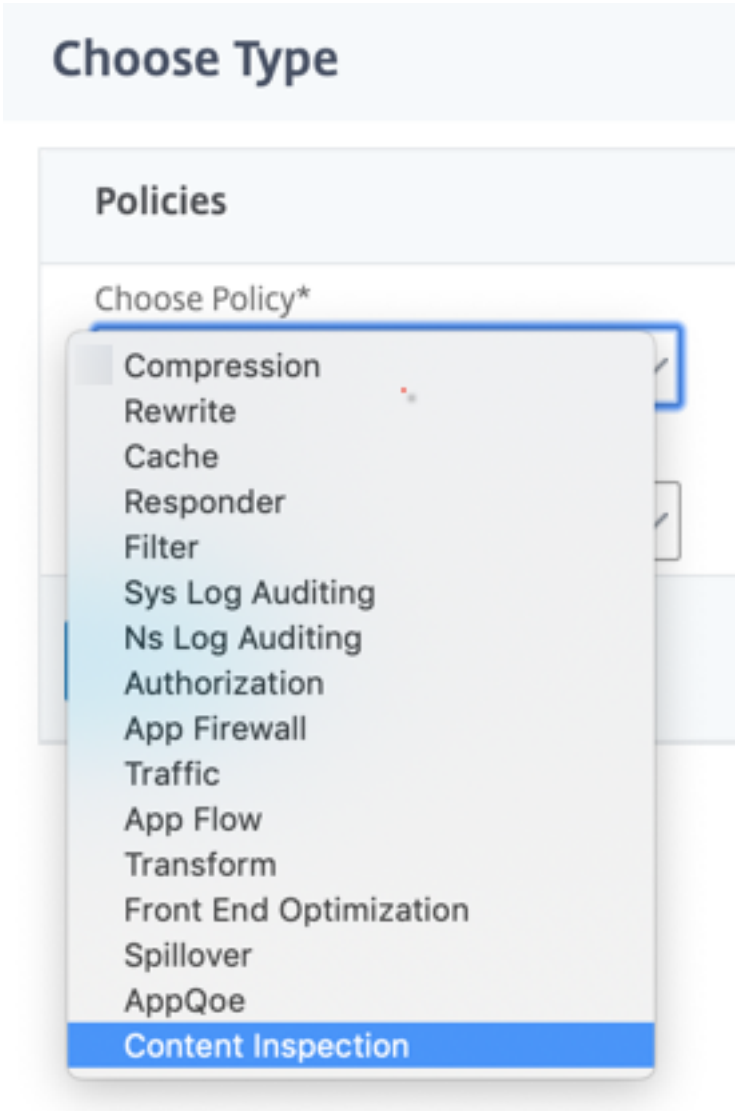




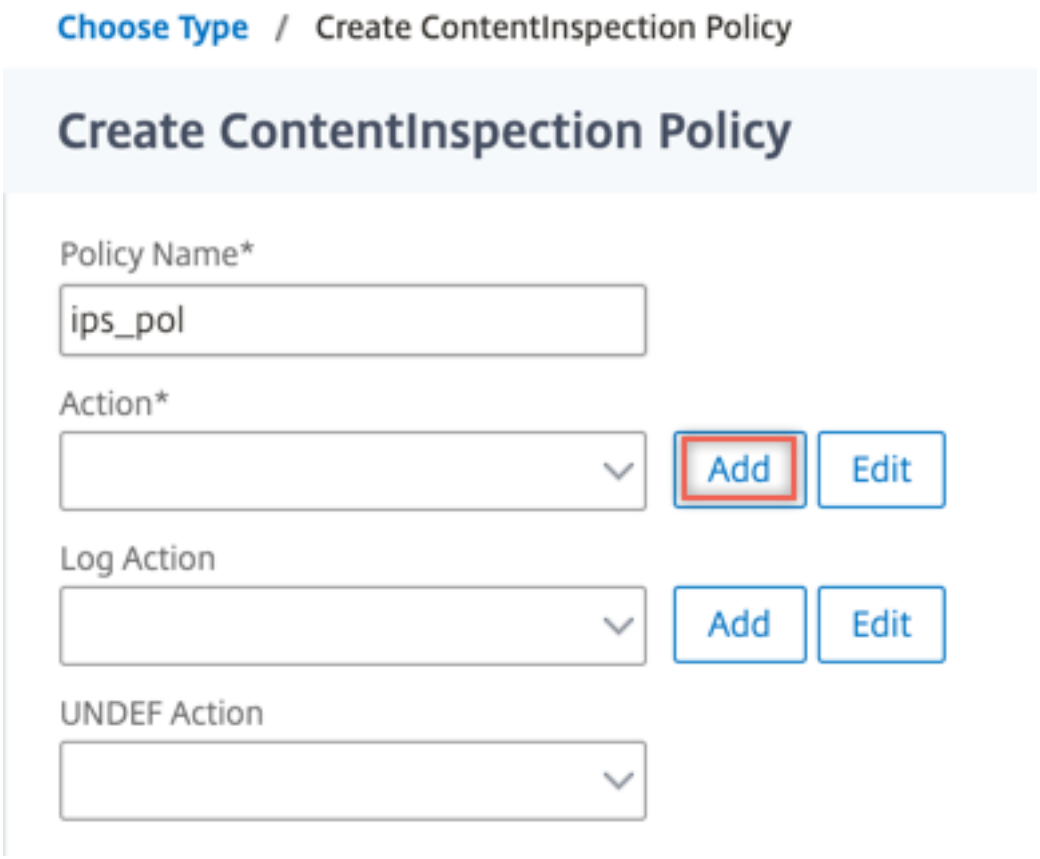
9. Accédez à **Secure Web Gateway > Servers virtuels Proxy > Ajouter**. Spécifiez un nom, une adresse IP et un port. Dans **Paramètres avancés**, sélectionnez **Stratégies**. Cliquez sur le signe « + ».



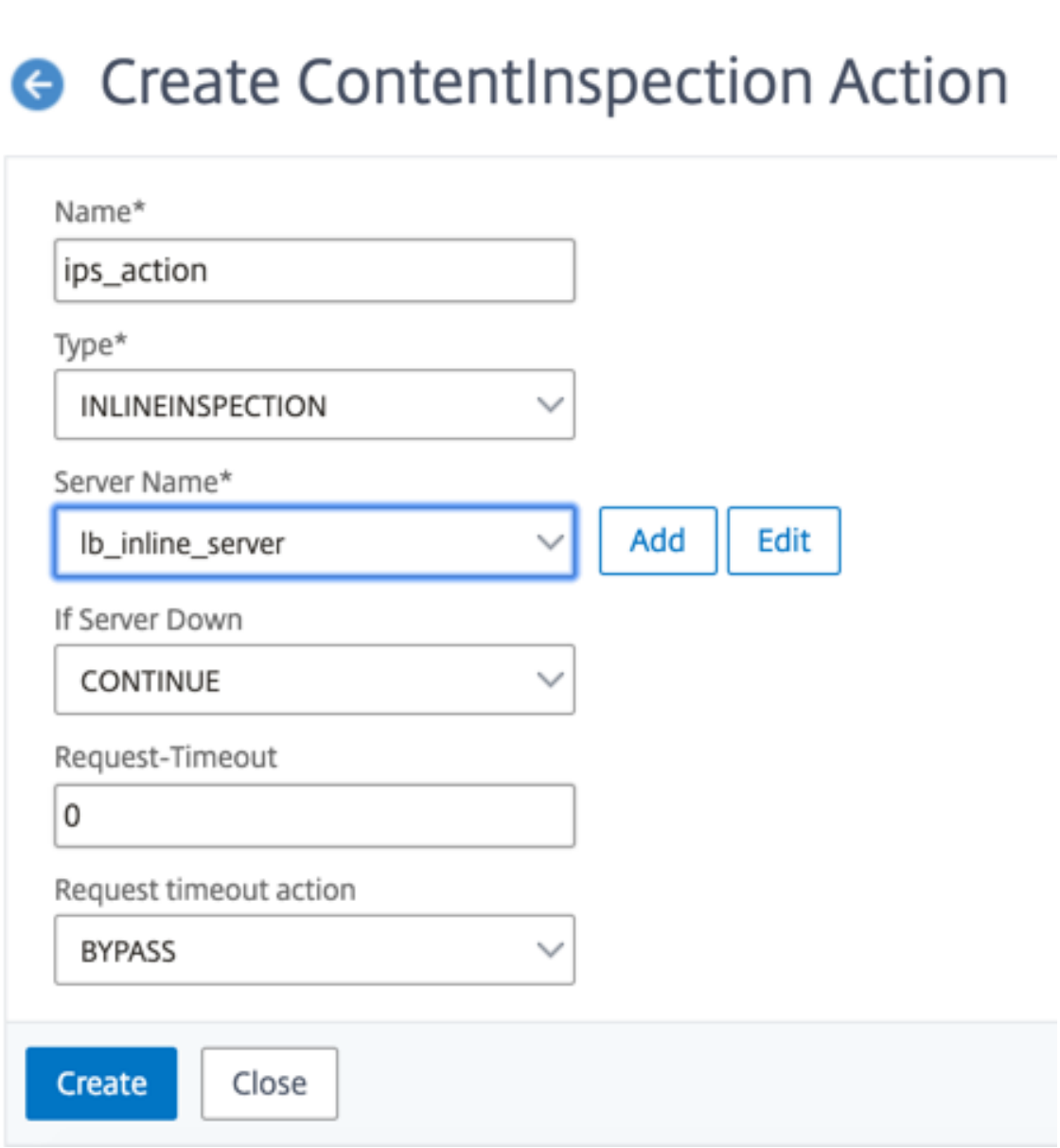
10. Dans **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



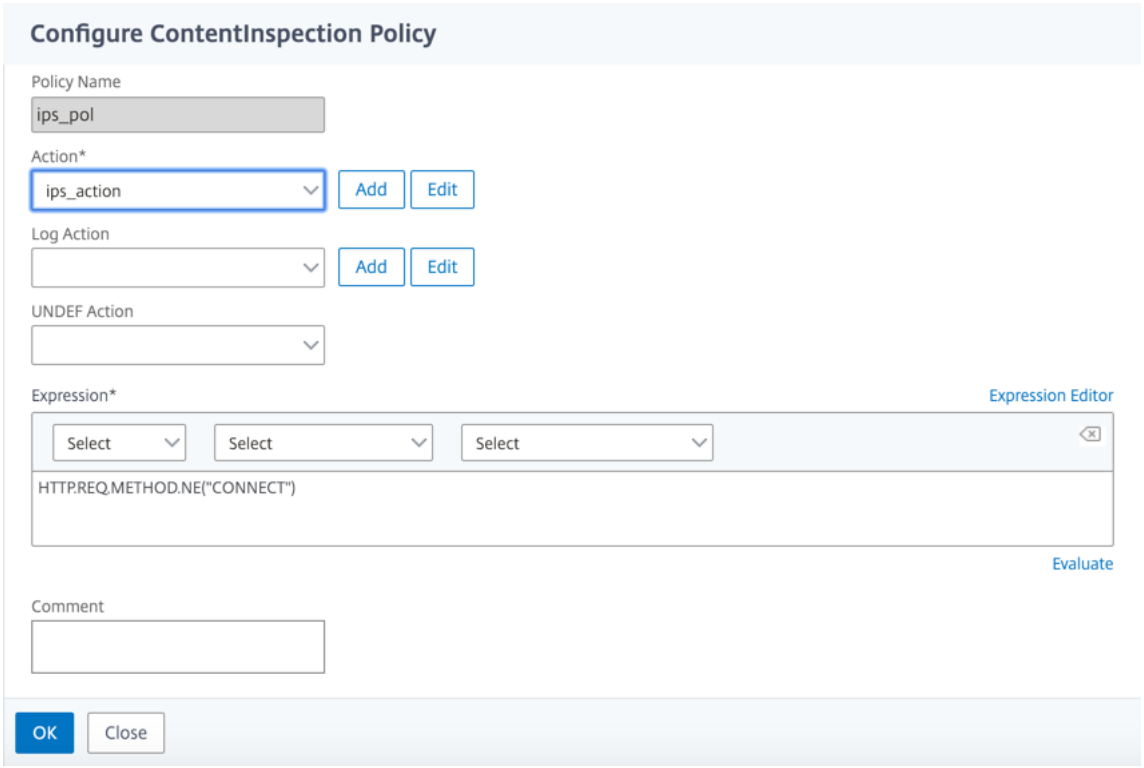
11. Cliquez sur **Ajouter**. Spécifiez un nom. Dans **Action**, cliquez sur **Ajouter**.



12. Spécifiez un nom. Dans **Type**, sélectionnez **INLINEINSPECTION**. Dans **Nom du serveur**, sélectionnez le serveur virtuel d'équilibrage de charge créé précédemment.



13. Cliquez sur **Créer**. Spécifiez la règle et cliquez sur **Créer**.



14. Cliquez sur **Bind**.
15. Cliquez sur **Terminé**.

Intégration de NetScaler à des dispositifs de sécurité passifs (système de détection des intrusions)

May 5, 2023

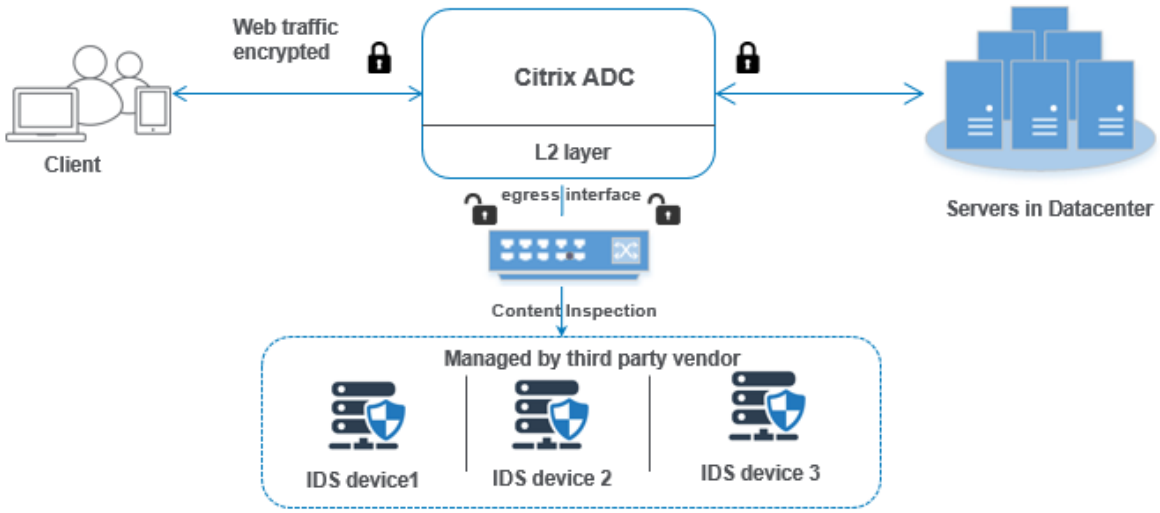
Une appliance NetScaler est désormais intégrée à des dispositifs de sécurité passifs tels que le système de détection des intrusions (IDS). Ces appareils passifs stockent des journaux et déclenchent des alertes lorsqu'ils détectent un trafic défectueux ou non conforme. Il génère également des rapports à des fins de conformité. Si l'appliance NetScaler est intégrée à deux appareils IDS ou plus et que le volume de trafic est élevé, l'appliance peut équilibrer la charge des appareils en clonant le trafic au niveau du serveur virtuel.

Pour une protection de sécurité avancée, une appliance NetScaler est intégrée à des dispositifs de sécurité passifs tels que le système IDS déployé en mode détection uniquement. Ces appareils stockent le journal et déclenchent des alertes lorsqu'ils détectent un trafic mauvais ou non conforme. Il génère également des rapports à des fins de conformité. Vous trouverez ci-dessous certains des avantages de l'intégration de NetScaler à un appareil IDS.

- **Inspection du trafic chiffré**. La plupart des dispositifs de sécurité contournent le trafic chiffré, ce qui rend les serveurs vulnérables aux attaques. Une appliance NetScaler peut déchiffrer le trafic et l'envoyer aux appareils IDS afin d'améliorer la sécurité du réseau du client.
- **Déchargement des appareils en ligne du traitement TLS/SSL**. Le traitement TLS/SSL est coûteux et il entraîne un processeur système élevé dans les dispositifs de détection d'intrusion s'ils décryptent le trafic. Le trafic chiffré augmentant rapidement, ces systèmes ne parviennent pas à déchiffrer et à inspecter le trafic chiffré. NetScaler permet de décharger le trafic du traitement TLS/SSL vers les appareils IDS. Cette façon de décharger les données permet à un dispositif IDS de prendre en charge un volume élevé d'inspection du trafic.
- **Périphériques IDS d'équilibrage**de L'appliance NetScaler équilibre la charge de plusieurs appareils IDS lorsque le volume de trafic est élevé en clonant le trafic au niveau du serveur virtuel.
- **Réplication du trafic vers des appareils passifs**. Le trafic entrant dans l'appliance peut être répliqué vers d'autres appareils passifs pour générer des rapports de conformité. Par exemple, peu d'agences gouvernementales exigent que chaque transaction soit enregistrée sur certains appareils passifs.
- **Fanning du trafic vers plusieurs appareils passifs**. Certains clients préfèrent répartir ou répliquer le trafic entrant sur plusieurs appareils passifs.
- **Sélection intelligente du trafic**. Chaque paquet entrant dans l'appliance peut ne pas faire l'objet d'une inspection de contenu, par exemple le téléchargement de fichiers texte. L'utilisateur peut configurer l'appliance NetScaler pour sélectionner un trafic spécifique (par exemple, des fichiers .exe) à inspecter et envoyer le trafic aux appareils IDS pour le traitement des données.

Comment NetScaler est intégré à un appareil IDS doté d'une connectivité L2

Le schéma suivant montre comment IDS est intégré à une appliance NetScaler.



L'interaction entre les composants est donnée comme suit :

1. Un client envoie une requête HTTP/HTTPS à l'appliance NetScaler.
2. L'appliance intercepte le trafic et le réplique sur un périphérique IDS en fonction de l'évaluation de la stratégie d'inspection du contenu.
3. Si le trafic est chiffré, l'appliance déchiffre les données et les envoie en texte brut.
4. Sur la base de l'évaluation de la stratégie, l'appliance applique une action d'inspection de contenu de type « MIROIR ».
5. Le service IDS ou le service d'équilibrage de charge (pour plusieurs intégrations de périphériques IDS) est configuré dans l'action.
6. Le périphérique IDS est configuré en tant que type de service d'inspection de contenu « Tout » sur l'appliance. Le service d'inspection de contenu est ensuite associé au profil d'inspection de contenu de type « MIRROR » qui spécifie l'interface de sortie par laquelle les données doivent être transmises au dispositif IDS. Vous pouvez également configurer une balise VLAN dans le profil d'inspection du contenu.

   > **Remarque :**
   >
   > - L'adresse IP utilisée pour le service ou le serveur IDS est une adresse fictive.
   > - L'appliance NetScaler ne prend pas en charge le canal LA pour l'interface de sortie.

7. L'appareil réplique ensuite les données via l'interface de sortie vers un ou plusieurs dispositifs IDS.
8. De même, lorsque le serveur principal envoie une réponse à NetScaler, l'appliance réplique les données et les transmet au périphérique IDS.
9. Si votre appliance est intégrée à un ou plusieurs appareils IDS et si vous préférez équilibrer la charge des appareils, vous pouvez utiliser le serveur virtuel d'équilibrage de charge.

Licences logicielles

Pour déployer l'intégration des appareils en ligne, votre appliance NetScaler doit être provisionnée avec l'une des licences suivantes :

1. ADC Premium
2. ADC Avancé
3. Telco Advanced
4. Télécoms Premium

Configuration de l'intégration du système de détection

Vous pouvez intégrer le périphérique IDS à NetScaler de deux manières différentes.

Scénario 1 : intégration avec un seul appareil IDS

Voici les étapes que vous devez configurer à l'aide de l'interface de ligne de commande.

1. Activer l'inspection du contenu
2. Ajoutez un profil d'inspection de contenu de type MIRROR pour le service représentant le périphérique IDS
3. Ajouter un service IDS de type « ANY »
4. Ajouter une action d'inspection de contenu de type « MIRROR »
5. Ajout d'une stratégie d'inspection du contenu pour l'inspection IDS
6. Lier la stratégie d'inspection de contenu au service virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Activer l'inspection du contenu

Si vous souhaitez que l'appliance NetScaler envoie le contenu pour inspection aux appareils IDS, vous devez activer les fonctionnalités d'inspection du contenu et d'équilibrage de charge indépendamment du déchiffrement effectué.

À l'invite de commande, tapez :

```
enable ns feature contentInspection LoadBalancing
```

Add Content Inspection profile de type « MIRROR »

Le profil d'inspection du contenu de type « MIRROR » explique comment vous pouvez vous connecter au périphérique IDS.
À l'invite de commandes, tapez.

```
add contentInspection profile <name> -type MIRROR -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 10
```

Ajouter un service IDS

Vous devez configurer un service de type « ANY » pour chaque périphérique IDS intégré à l'appliance. Le service contient les détails de configuration de l'appareil IDS. Le service représente l'appareil IDS.

À l'invite de commande, tapez :

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```


Exemple :

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Ajout d'une action d'inspection de contenu de type MIRROR pour le service IDS

Après avoir activé la fonctionnalité Inspection du contenu, puis ajouté le profil et le service IDS, vous devez ajouter l'action Inspection du contenu pour traiter la demande. En fonction de l'action d'inspection du contenu, l'appliance peut supprimer, réinitialiser, bloquer ou envoyer des données au périphérique IDS.

À l'invite de commande, tapez :

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Exemple :

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Ajout d'une stratégie d'inspection du contenu pour l'inspection IDS

Après avoir créé une action d'inspection du contenu, vous devez ajouter des stratégies d'inspection du contenu pour évaluer les demandes d'inspection. La stratégie est basée sur une règle qui consiste en une ou plusieurs expressions. La stratégie évalue et sélectionne le trafic à inspecter en fonction de la règle.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Lier la stratégie d'inspection de contenu au service virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Pour recevoir le trafic Web, vous devez ajouter un serveur virtuel d'équilibrage de charge.
À l'invite de commande, tapez :

```
add lb vserver <name> <vserver name>
```

Exemple :

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```


Lier la stratégie d'inspection du contenu au serveur virtuel de commutation de contenu ou au serveur virtuel d'équilibrage de charge de type HTTP/SSL

Vous devez lier le serveur virtuel d'équilibrage de charge ou le serveur virtuel de commutation de contenu de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

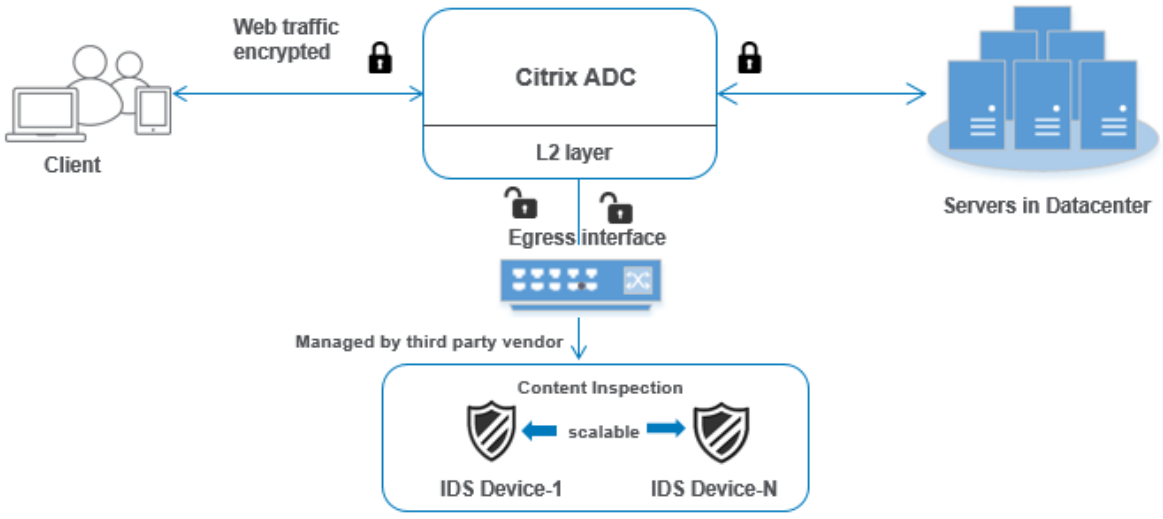
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Exemple :

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Scénario 2 : équilibrage de charge de plusieurs périphériques IDS

Si vous utilisez deux appareils IDS ou plus, vous devez équilibrer la charge des appareils à l'aide de différents services d'inspection de contenu. Dans ce cas, l'appliance NetScaler équilibre la charge des appareils en plus d'envoyer un sous-ensemble de trafic à chaque appareil.
Pour les étapes de configuration de base, reportez-vous au scénario 1.



Voici les étapes que vous devez configurer à l'aide de l'interface de ligne de commande.

1. Ajouter le profil d'inspection de contenu 1 de type MIRROR pour le service IDS 1
2. Ajouter le profil d'inspection de contenu 2 de type MIRROR pour le service IDS 2
3. Ajouter le service IDS 1 de type ANY pour le périphérique IDS 1
4. Ajouter le service IDS 2 de type ANY pour le périphérique IDS 2
5. Ajouter un serveur virtuel d'équilibrage de charge de type ANY
6. Lier le service IDS 1 au serveur virtuel d'équilibrage de charge

7. Lier le service IDS 2 au serveur virtuel d'équilibrage de charge
8. Ajoutez une action d'inspection du contenu pour l'équilibrage de charge des périphériques IDS.
9. Ajouter une stratégie d'inspection du contenu pour l'inspection
10. Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL
11. Lier la stratégie d'inspection du contenu au serveur virtuel d'équilibrage de charge de type HTTP/SSL

Ajouter le profil d'inspection de contenu 1 de type MIRROR pour le service IDS 1

La configuration IDS peut être spécifiée dans une entité appelée profil d'inspection du contenu. Le profil possède un ensemble de paramètres d'appareil. Le profil d'inspection du contenu1 est créé pour le service IDS 1.

À l'invite de commande, tapez :

```
add contentInspection profile <name> -type ANY -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Exemple :

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

Ajouter le profil d'inspection de contenu 2 pour le type MIRROR for IDS service 2

Le profil d'inspection du contenu 2 est ajouté pour le service 2 et le périphérique en ligne communique avec l'appliance via l'interface de sortie 1/1.

À l'invite de commande, tapez :

```
add contentInspection profile <name> -type MIRROR -egressInterface -egressVlan
 <positive_integer>]
```

Exemple :

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

Ajouter le service IDS 1 de type ANY pour le périphérique IDS 1

Après avoir activé la fonction d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 1 pour que le périphérique en ligne 1 fasse partie de la configuration de l'équilibrage de charge. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commande, tapez :


```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Exemple :

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Remarque**
>
> L'adresse IP mentionnée dans l'exemple est fictive.

Ajouter le service IDS 2 de type ANY pour le périphérique IDS 2

Après avoir activé la fonctionnalité d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 2 pour le périphérique en ligne 2. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commande, tapez :

```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```

Exemple :

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Remarque**
>
> L'adresse IP mentionnée dans l'exemple est fictive.

Ajouter un serveur virtuel d'équilibrage de charge

Après avoir ajouté le profil en ligne et les services, vous devez ajouter un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge des services.

À l'invite de commande, tapez :

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Exemple :

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

Lier le service IDS 1 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur virtuel d'équilibrage de charge au premier service.

À l'invite de commande, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-IDS_vserver IDS_service1
```

Lier le service IDS 2 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur au deuxième service.

À l'invite de commande, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-IDS_vserver IDS_service2
```

Ajouter une action d'inspection de contenu pour le service IDS

Après avoir activé la fonctionnalité Inspection du contenu, vous devez ajouter l'action Inspection du contenu pour gérer les informations de demande en ligne. En fonction de l'action sélectionnée, l'appliance supprime, réinitialise, bloque ou envoie du trafic vers le périphérique IDS.

À l'invite de commande, tapez :

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Exemple :

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Ajouter une stratégie d'inspection du contenu pour l'inspection

Après avoir créé une action d'inspection du contenu, vous devez ajouter une stratégie d'inspection du contenu pour évaluer les demandes de service.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```


Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Ajoutez un serveur virtuel de commutation de contenu ou d'équilibrage de charge pour accepter le trafic Web. Vous devez également activer la connexion layer2 sur le serveur virtuel.

Pour plus d'informations sur l'équilibrage de charge, reportez-vous à la rubrique **Fonctionnement de l'équilibrage de charge** .

À l'invite de commande, tapez :

```
add lb vserver <name> <vserver name>
```

Exemple :

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```

Lier la stratégie d'inspection du contenu au serveur virtuel d'équilibrage de charge de type HTTP/SSL

Vous devez lier le serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <REQUEST>
```

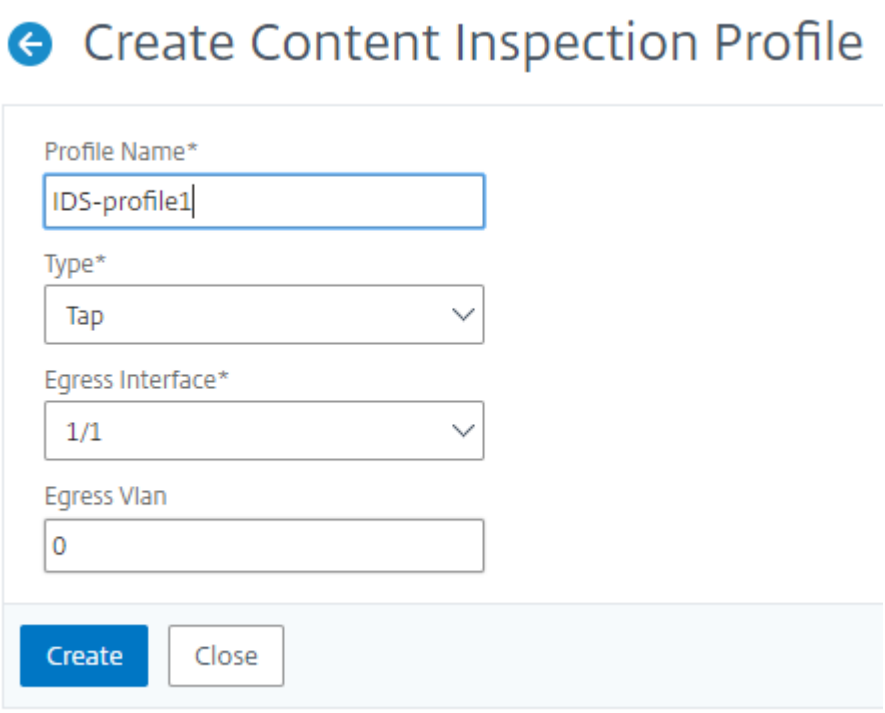
Exemple :

```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

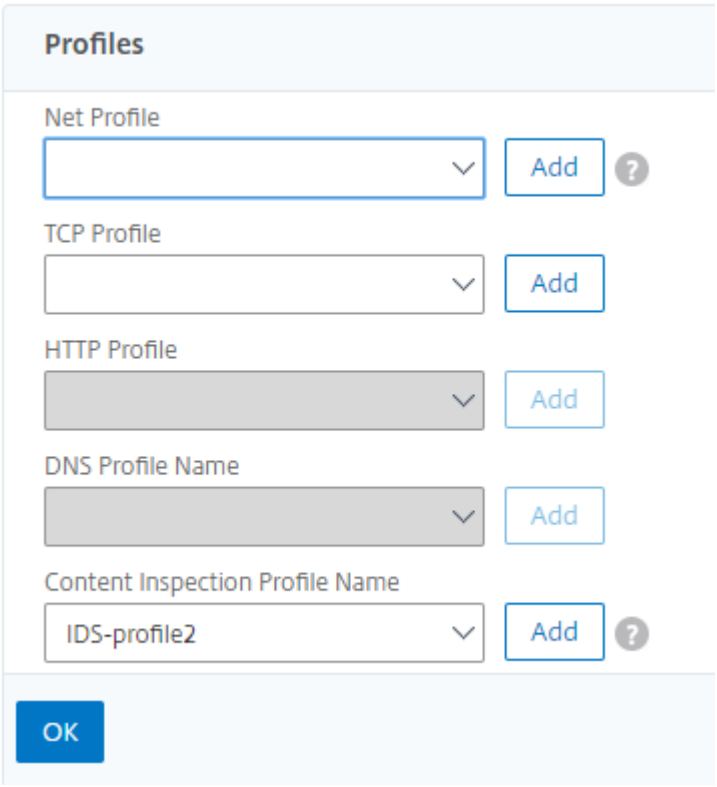
Configuration de l'intégration des services en ligne à l'aide de l'interface graphique NetScaler

1. Accédez à **Sécurité** > **Inspection du contenu** > **Profils d'inspection du contenu**.
2. Sur la page **Profil d'inspection du contenu**, cliquez sur **Ajouter**.
3. Sur la page **Créer un profil d'inspection du contenu**, définissez les paramètres suivants.
    a) Nom du profil. Nom du profil d'inspection du contenu pour IDS.
    b) Tapez. Sélectionnez les types de profil en tant que MIROIR.
    c) Interface de sortie. Interface par laquelle le trafic est envoyé depuis NetScaler vers le périphérique IDS.
    d) VLAN de sortie (facultatif). ID VLAN de l'interface par laquelle le trafic est envoyé au périphérique IDS.

4. Cliquez sur **Create**.



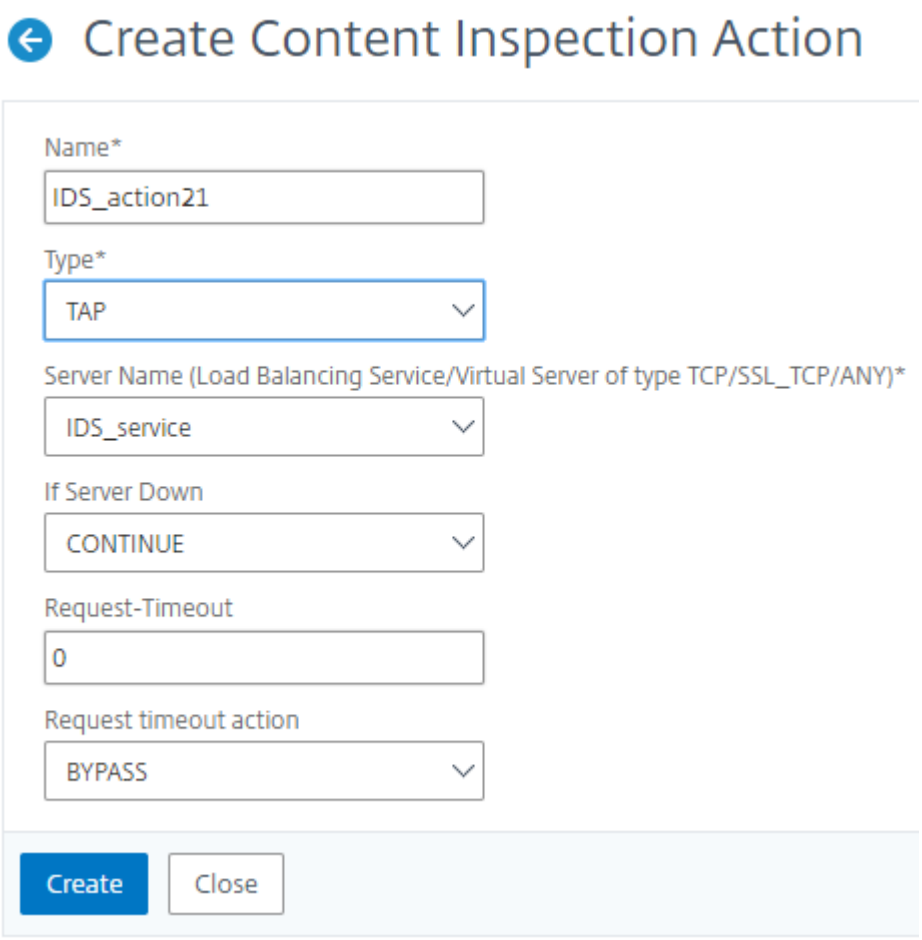
5. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
6. Sur la page **Service d'équilibrage de charge**, entrez les détails du service d'inspection du contenu.
7. Dans la section **Paramètres avancés**, cliquez sur **Profils**.
8. Accédez à la section **Profils** et cliquez sur l'icône **Crayon** pour ajouter le profil d'inspection du contenu.
9. Cliquez sur **OK**.



10. Accédez à **Équilibrage de charge** > **Serveurs**. Ajoutez un serveur virtuel de type HTTP ou SSL.
11. Après avoir saisi les détails du serveur, cliquez sur **OK**, puis de nouveau **sur OK**.
12. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
13. Accédez à la section **Stratégies** et cliquez sur l'icône en forme de **crayon** pour configurer la stratégie d'inspection du contenu.
14. Sur la page **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.
15. Dans la section **Liaison de stratégie**, cliquez sur « + » pour ajouter une stratégie d'inspection du contenu.
16. Sur la page **Créer une stratégie de CI**, entrez un nom pour la stratégie d'inspection du contenu en ligne.
17. Dans le champ **Action**, cliquez sur le signe « + » pour créer une action d'inspection du contenu IDS de type MIRROR.
18. Sur la page **Créer une action de CI**, définissez les paramètres suivants.
    a) Nom. Nom de la stratégie en ligne d'inspection du contenu.
    b) Tapez. Sélectionnez le type en tant que MIROIR.
    c) Nom du serveur. Sélectionnez le nom du serveur/service en tant que périphériques en ligne.

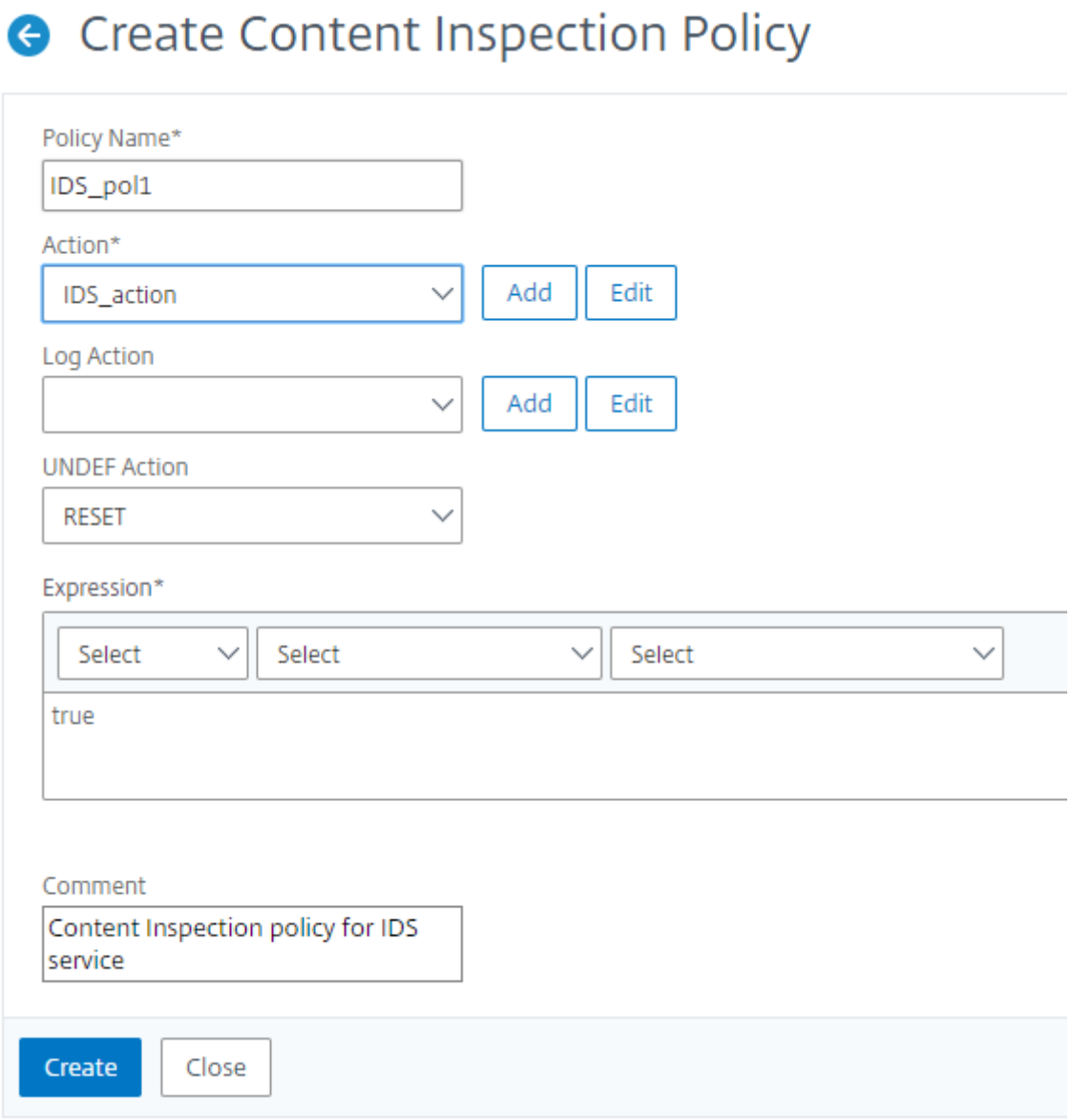
d) Si le serveur est en panne. Sélectionnez une opération si le serveur tombe en panne.
e) Délai d'expiration de la demande. Sélectionnez une valeur de délai d'expiration. Les valeurs par défaut peuvent être utilisées.
f) Action de délai d'expiration de demande. Sélectionnez une action de délai d'expiration. Les valeurs par défaut peuvent être utilisées.

19. Cliquez sur **Create**.



20. Sur la page **Créer une stratégie de CI**, entrez d'autres détails.
21. Cliquez sur **OK** et sur **Fermer**.

Pour plus d'informations sur la configuration de l'interface graphique NetScaler pour l'équilibrage de charge et la réplication du trafic vers les appareils IDS, consultez la section Équilibrage de charge.



Pour plus d'informations sur la configuration de l'interface graphique NetScaler pour l'équilibrage de charge et le transfert du trafic vers le serveur d'origine principal après la transformation du contenu, consultez la rubrique Équilibrage de charge .

Intégration de NetScaler Layer 3 à des dispositifs de sécurité passifs (système de détection des intrusions)

May 5, 2023

Une appliance NetScaler est désormais intégrée à des dispositifs de sécurité passifs tels que le sys-

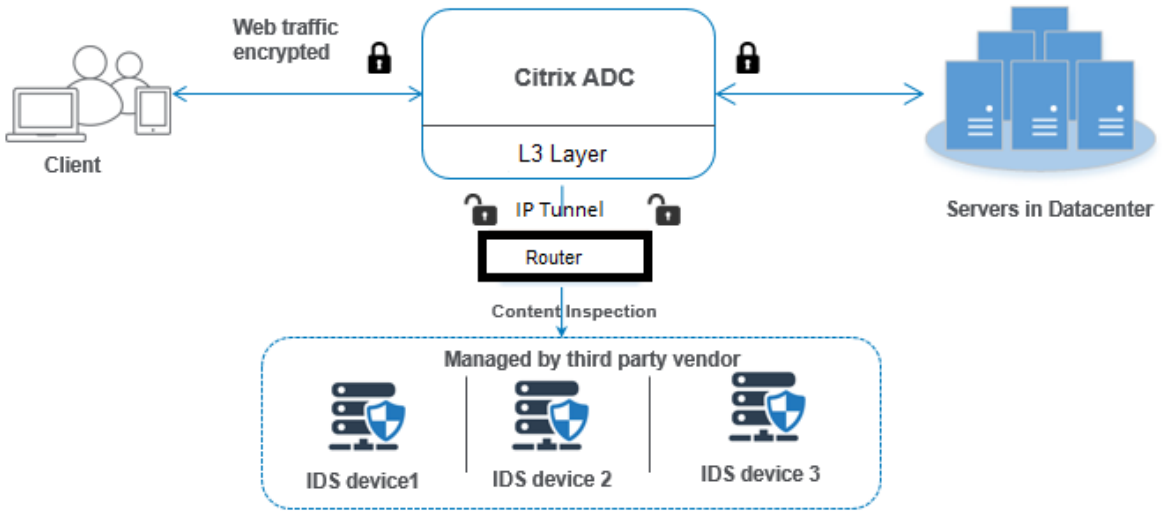
tème de détection des intrusions (IDS). Dans cette configuration, l'appliance envoie une copie du trafic d'origine en toute sécurité aux appareils IDS distants. Ces appareils passifs stockent des journaux et déclenchent des alertes lorsqu'ils détectent un trafic défectueux ou non conforme. Il génère également des rapports à des fins de conformité. Si une appliance NetScaler est intégrée à deux appareils IDS ou plus et que le volume de trafic est élevé, l'appliance peut équilibrer la charge des appareils en clonant le trafic au niveau du serveur virtuel.

Pour une protection de sécurité avancée, une appliance NetScaler est intégrée à des dispositifs de sécurité passifs tels que le système IDS déployé en mode détection uniquement. Ces appareils stockent le journal et déclenchent des alertes lorsqu'ils détectent un trafic mauvais ou non conforme. Il génère également des rapports à des fins de conformité. Vous trouverez ci-dessous certains des avantages de l'intégration de NetScaler à un appareil IDS.

- **Inspection du trafic chiffré**. La plupart des dispositifs de sécurité contournent le trafic chiffré, ce qui rend les serveurs vulnérables aux attaques. Une appliance NetScaler peut déchiffrer le trafic et l'envoyer aux appareils IDS afin d'améliorer la sécurité du réseau du client.
- **Déchargement des appareils en ligne du traitement TLS/SSL**. Le traitement TLS/SSL est coûteux et il entraîne un processeur système élevé dans les dispositifs de détection d'intrusion s'ils décryptent le trafic. Le trafic chiffré augmentant rapidement, ces systèmes ne parviennent pas à déchiffrer et à inspecter le trafic chiffré. NetScaler permet de décharger le trafic du traitement TLS/SSL vers les appareils IDS. Cette façon de décharger les données permet à un dispositif IDS de prendre en charge un volume élevé d'inspection du trafic.
- **Périphériques IDS d'équilibrage**de L'appliance NetScaler équilibre la charge de plusieurs appareils IDS lorsque le volume de trafic est élevé en clonant le trafic au niveau du serveur virtuel.
- **Réplication du trafic vers des appareils passifs**. Le trafic entrant dans l'appliance peut être répliqué vers d'autres appareils passifs pour générer des rapports de conformité. Par exemple, peu d'agences gouvernementales exigent que chaque transaction soit enregistrée sur certains appareils passifs.
- **Fanning du trafic vers plusieurs appareils passifs**. Certains clients préfèrent répartir ou répliquer le trafic entrant sur plusieurs appareils passifs.
- **Sélection intelligente du trafic**. Chaque paquet entrant dans l'appliance peut ne pas faire l'objet d'une inspection de contenu, par exemple le téléchargement de fichiers texte. L'utilisateur peut configurer l'appliance NetScaler pour sélectionner un trafic spécifique (par exemple, des fichiers .exe) à inspecter et envoyer le trafic aux appareils IDS pour le traitement des données.

Comment NetScaler est intégré à un appareil IDS doté d'une connectivité L3

Le schéma suivant montre comment l'IDS est intégré à une appliance NetScaler.



L'interaction entre les composants est donnée comme suit :

1. Un client envoie une requête HTTP/HTTPS à l'appliance NetScaler.
2. L'appliance intercepte le trafic et envoie les données à des dispositifs IDS distants dans différents centres de données ou même dans un cloud. Cette intégration s'effectue via la couche 3 à tunnel IP. Pour plus d'informations sur le tunneling IP dans une appliance NetScaler, consultez la rubrique Tunnels IP.
3. Si le trafic est chiffré, l'appliance déchiffre les données et les envoie en texte brut.
4. Sur la base de l'évaluation de la stratégie, l'appliance applique une action d'inspection de contenu de type « MIROIR ».
5. Un service IDS ou un service d'équilibrage de charge (pour plusieurs intégrations de dispositifs IDS) est configuré dans l'action.
6. Le périphérique IDS est configuré en tant que type de service d'inspection de contenu « Tout » sur l'appliance. Le service d'inspection de contenu est ensuite associé au profil d'inspection de contenu de type « MIRROR » et au paramètre de tunnel qui spécifie l'interface de couche 3 à tunnel IP via laquelle les données sont transmises au dispositif IDS.

   > **Remarque :**
   >
   > Vous pouvez également configurer une balise VLAN dans le profil d'inspection du contenu.

7. De même, lorsque le serveur principal envoie une réponse à NetScaler, l'appliance réplique les données et les transmet au périphérique IDS.
8. Si votre appliance est intégrée à un ou plusieurs appareils IDS et si vous préférez équilibrer la charge des appareils, vous pouvez utiliser le serveur virtuel d'équilibrage de charge.

Licences logicielles

Pour déployer l'intégration IDS, votre appliance NetScaler doit être approvisionnée avec l'une des licences suivantes :

1. ADC Premium
2. ADC Avancé

Configuration de l'intégration du système de détection

Vous pouvez intégrer un appareil IDS à un NetScaler de deux manières différentes.

Scénario 1 : intégration avec un seul appareil IDS

Voici les étapes que vous devez configurer à l'aide de l'interface de ligne de commande.

1. Activer l'inspection du contenu
2. Ajoutez un profil d'inspection de contenu de type MIRROR pour le service représentant le périphérique IDS
3. Ajouter un service IDS de type « ANY »
4. Ajouter une action d'inspection de contenu de type « MIRROR »
5. Ajout d'une stratégie d'inspection du contenu pour l'inspection IDS
6. Lier la stratégie d'inspection de contenu au service virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Activer l'inspection du contenu

Si vous souhaitez que l'appliance NetScaler envoie le contenu pour inspection aux appareils IDS, vous devez activer les fonctionnalités d'inspection du contenu et d'équilibrage de charge indépendamment du déchiffrement effectué.

À l'invite de commande, tapez :

```
enable ns feature contentInspection LoadBalancing
```

Ajouter un profil d'inspection du contenu de type « MIRROR »

Le profil d'inspection du contenu de type « MIRROR » explique comment vous pouvez vous connecter au périphérique IDS.
À l'invite de commandes, tapez.

> **Remarque :**
>
> Le paramètre de tunnel IP doit être utilisé uniquement pour la topologie IDS de couche 3.

> Sinon, vous devez utiliser l'interface de sortie avec l'option VLAN de sortie. Les types de tunnels GRE/IPIP sont pris en charge par la topologie IDS de couche 3.

```
add contentInspection profile <name> -type MIRROR -ipTunnel <iptunnel_name>
```

Exemple :

```
add contentInspection profile IDS_profile1 -type MIRROR -ipTunnel ipsect-
tunnel1
```

Ajouter un service IDS

Vous devez configurer un service de type « ANY » pour chaque périphérique IDS intégré à l'appliance. Le service contient les détails de configuration de l'appareil IDS. Le service représente l'appareil IDS.

À l'invite de commande, tapez :

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```

Exemple :

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Ajout d'une action d'inspection de contenu de type MIRROR pour le service IDS

Après avoir activé la fonctionnalité Inspection du contenu, puis ajouté le profil et le service IDS, vous devez ajouter l'action Inspection du contenu pour traiter la demande. En fonction de l'action d'inspection du contenu, l'appliance peut supprimer, réinitialiser, bloquer ou envoyer des données au périphérique IDS.

À l'invite de commande, tapez :

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Exemple :

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Ajout d'une stratégie d'inspection du contenu pour l'inspection IDS

Après avoir créé une action d'inspection du contenu, vous devez ajouter des stratégies d'inspection du contenu pour évaluer les demandes d'inspection. La stratégie est basée sur une règle qui consiste en une ou plusieurs expressions. La stratégie évalue et sélectionne le trafic à inspecter en fonction de la règle.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Lier la stratégie d'inspection de contenu au service virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Pour recevoir le trafic Web, vous devez ajouter un serveur virtuel d'équilibrage de charge.
À l'invite de commande, tapez :

```
add lb vserver <name> <vserver name>
```

Exemple :

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```

Lier la stratégie d'inspection du contenu au serveur virtuel de commutation de contenu ou au serveur virtuel d'équilibrage de charge de type HTTP/SSL

Vous devez lier le serveur virtuel d'équilibrage de charge ou le serveur virtuel de commutation de contenu de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

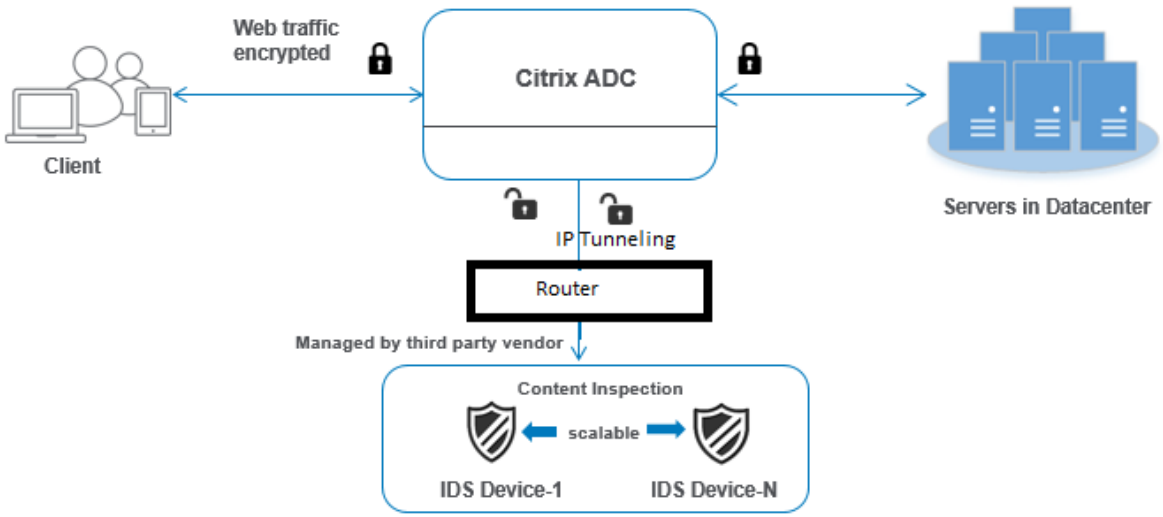
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Exemple :

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Scénario 2 : équilibrage de charge de plusieurs périphériques IDS

Si vous utilisez deux appareils IDS ou plus, vous devez équilibrer la charge des appareils IDS à l'aide de différents services d'inspection du contenu. Dans ce cas, l'appliance NetScaler équilibre la charge des appareils en plus d'envoyer un sous-ensemble de trafic à chaque appareil.
Pour les étapes de configuration de base, reportez-vous au scénario 1.



Voici les étapes que vous devez configurer à l'aide de l'interface de ligne de commande.

1. Ajouter le profil d'inspection de contenu 1 de type MIRROR pour le service IDS 1
2. Ajouter le profil d'inspection de contenu 2 de type MIRROR pour le service IDS 2
3. Ajouter le service IDS 1 de type ANY pour le périphérique IDS 1
4. Ajouter le service IDS 2 de type ANY pour le périphérique IDS 2
5. Ajouter un serveur virtuel d'équilibrage de charge de type ANY
6. Lier le service IDS 1 au serveur virtuel d'équilibrage de charge
7. Lier le service IDS 2 au serveur virtuel d'équilibrage de charge
8. Ajoutez une action d'inspection du contenu pour l'équilibrage de charge des périphériques IDS.
9. Ajouter une stratégie d'inspection du contenu pour l'inspection
10. Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL
11. Lier la stratégie d'inspection du contenu au serveur virtuel d'équilibrage de charge de type HTTP/SSL

Ajouter le profil d'inspection de contenu 1 de type MIRROR pour le service IDS 1

La configuration IDS peut être spécifiée dans une entité appelée profil d'inspection du contenu. Le profil possède un ensemble de paramètres d'appareil. Le profil d'inspection du contenu1 est créé pour le service IDS 1.

> **Remarque** :
> le paramètre de tunnel IP doit être utilisé uniquement pour la topologie IDS de couche 3. Sinon, vous devez utiliser l'interface de sortie avec l'option VLAN de sortie. Les types de tunnels GRE/IPIP sont pris en charge par la topologie IDS de couche 3.

À l'invite de commande, tapez :


```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```

Exemple :

```
add contentInspection profile IDS_profile1 -type MIRROR - ipTunnel ipsect_tunnel1
```

Ajouter le profil d'inspection de contenu 2 pour le type MIRROR for IDS service 2

Le profil d'inspection du contenu 2 est ajouté pour le service 2 et le périphérique en ligne communique avec l'appliance via l'interface de sortie 1/1.

À l'invite de commande, tapez :

```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```

Exemple :

```
add contentInspection profile IDS_profile2 -type ANY - ipTunnel ipsect_tunnel2
```

Ajouter le service IDS 1 de type ANY pour le périphérique IDS 1

Après avoir activé la fonctionnalité d'inspection du contenu et ajouté le profil intégré, vous devez ajouter un service en ligne 1 pour que le périphérique intégré 1 fasse partie de la configuration d'équilibrage de charge. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commande, tapez :

```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Exemple :

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Remarque** :
>
> L'adresse IP mentionnée dans l'exemple est fictive.

Ajouter le service IDS 2 de type ANY pour le périphérique IDS 2

Après avoir activé la fonctionnalité d'inspection du contenu et ajouté le profil en ligne, vous devez ajouter un service en ligne 2 pour le périphérique en ligne 2. Le service que vous ajoutez fournit tous les détails de configuration en ligne.

À l'invite de commande, tapez :


```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```

Exemple :

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Remarque** :
>
> L'adresse IP mentionnée dans l'exemple est fictive.

Ajouter un serveur virtuel d'équilibrage de charge

Après avoir ajouté le profil en ligne et les services, vous devez ajouter un serveur virtuel d'équilibrage de charge pour l'équilibrage de charge des services.

À l'invite de commande, tapez :

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Exemple :

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

Lier le service IDS 1 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur virtuel d'équilibrage de charge au premier service.

À l'invite de commande, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-IDS_vserver IDS_service1
```

Lier le service IDS 2 au serveur virtuel d'équilibrage de charge

Après avoir ajouté le serveur virtuel d'équilibrage de charge, liez maintenant le serveur au deuxième service.

À l'invite de commande, tapez :

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Exemple :

```
bind lb vserver lb-IDS_vserver IDS_service2
```


Ajouter une action d'inspection de contenu pour le service IDS

Après avoir activé la fonctionnalité Inspection du contenu, vous devez ajouter l'action Inspection du contenu pour gérer les informations de demande en ligne. En fonction de l'action sélectionnée, l'appliance supprime, réinitialise, bloque ou envoie du trafic vers le périphérique IDS.

À l'invite de commande, tapez :

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Exemple :

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Ajouter une stratégie d'inspection du contenu pour l'inspection

Après avoir créé une action d'inspection du contenu, vous devez ajouter la stratégie d'inspection du contenu pour évaluer les demandes de service.

À l'invite de commandes, tapez ce qui suit :

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Exemple :

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Ajouter un serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL

Ajoutez un serveur virtuel de commutation de contenu ou d'équilibrage de charge pour accepter le trafic Web. Vous devez également activer la connexion layer2 sur le serveur virtuel.

Pour plus d'informations sur l'équilibrage de charge, reportez-vous à la rubrique Fonctionnement de l'équilibrage de charge .

À l'invite de commande, tapez :

```
add lb vserver <name> <vserver name>
```

Exemple :

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```


Lier la stratégie d'inspection du contenu au serveur virtuel d'équilibrage de charge de type HTTP/SSL

Vous devez lier le serveur virtuel de commutation de contenu ou d'équilibrage de charge de type HTTP/SSL à la stratégie d'inspection du contenu.

À l'invite de commandes, tapez ce qui suit :

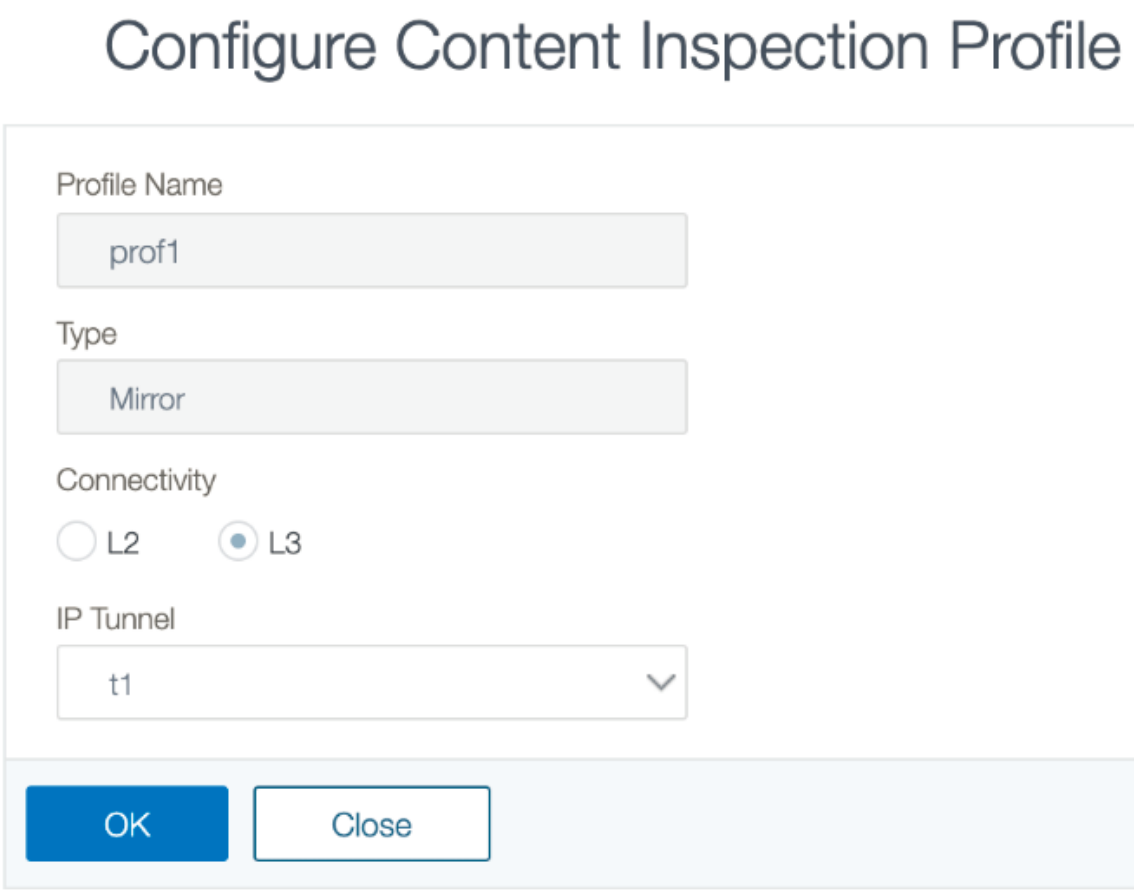
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -type <REQUEST>
```

Exemple :

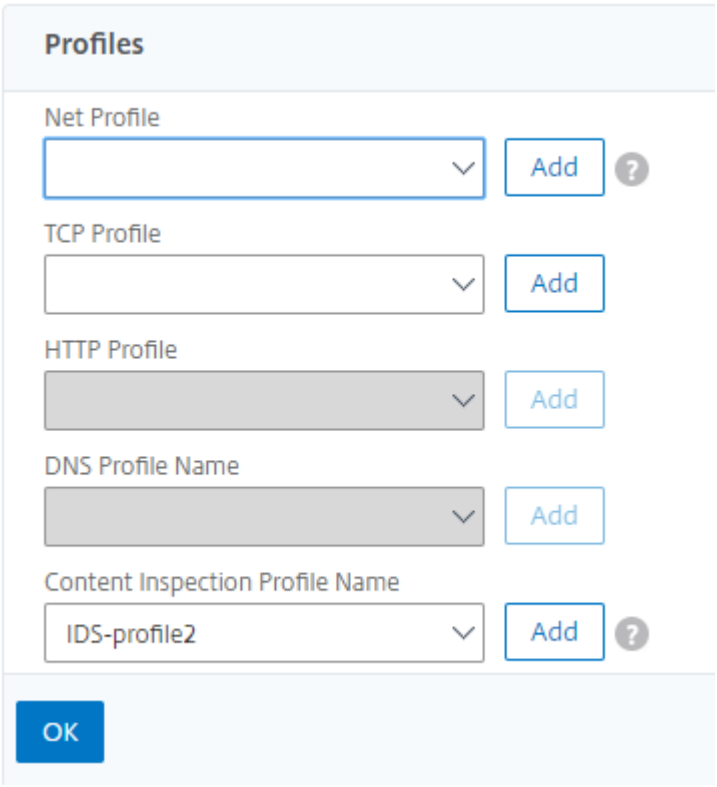
```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type REQUEST
```

Configuration de l'intégration des services en ligne à l'aide de l'interface graphique NetScaler

1. Accédez à **Sécurité** > **Inspection du contenu** > **ContentInspection Profiles**.
2. Sur la page **ContentInspection Profile**, cliquez sur **Ajouter**.
3. Dans la page **Create ContentInspectionProfile**, définissez les paramètres suivants.
    a) Nom du profil. Nom du profil d'inspection du contenu pour IDS.
    b) Tapez. Sélectionnez les types de profil en tant que MIROIR.
    c) Connectivité. Interface de couche 2 ou de couche 3.
    d) Tunnel IP. Sélectionnez le canal de communication réseau entre les deux réseaux.
4. Cliquez sur **Create**.



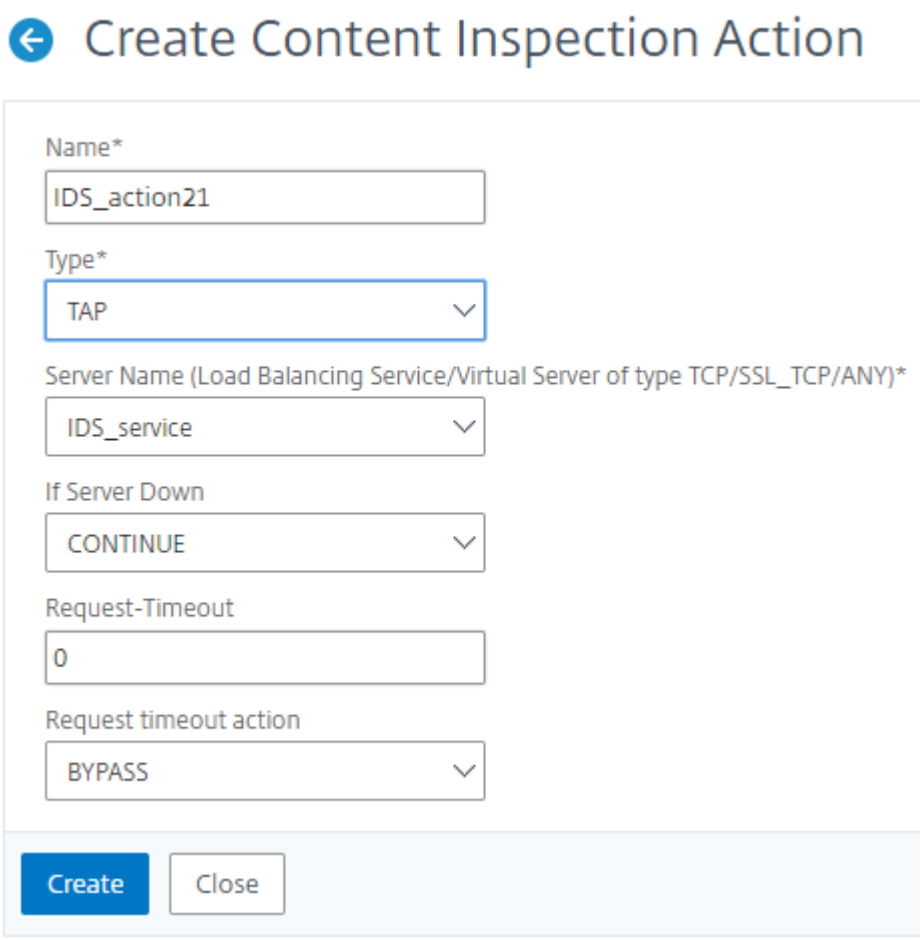
5. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**, puis cliquez sur **Ajouter**.
6. Sur la page **Service d'équilibrage de charge**, entrez les détails du service d'inspection du contenu.
7. Dans la section **Paramètres avancés**, cliquez sur **Profils**.
8. Accédez à la section **Profils** et cliquez sur l'icône **Crayon** pour ajouter le profil d'inspection du contenu.
9. Cliquez sur **OK**.



10. Accédez à **Équilibrage de charge** > **Serveurs**. Ajoutez un serveur virtuel de type HTTP ou SSL.
11. Après avoir saisi les détails du serveur, cliquez sur **OK**, puis de nouveau **sur OK**.
12. Dans la section **Paramètres avancés**, cliquez sur **Stratégies**.
13. Accédez à la section **Stratégies** et cliquez sur l'icône en forme de **crayon** pour configurer la stratégie d'inspection du contenu.
14. Sur la page **Choisir une stratégie**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.
15. Dans la section **Liaison de stratégie**, cliquez sur « + » pour ajouter une stratégie d'inspection du contenu.
16. Sur la page **Créer une stratégie de CI**, entrez un nom pour la stratégie d'inspection du contenu en ligne.
17. Dans le champ **Action**, cliquez sur le signe « + » pour créer une action d'inspection du contenu IDS de type MIRROR.
18. Sur la page **Créer une action de CI**, définissez les paramètres suivants.
    a) Nom. Nom de la stratégie en ligne d'inspection du contenu.
    b) Tapez. Sélectionnez le type en tant que MIROIR.
    c) Nom du serveur. Sélectionnez le nom du serveur/service en tant que périphériques en ligne.

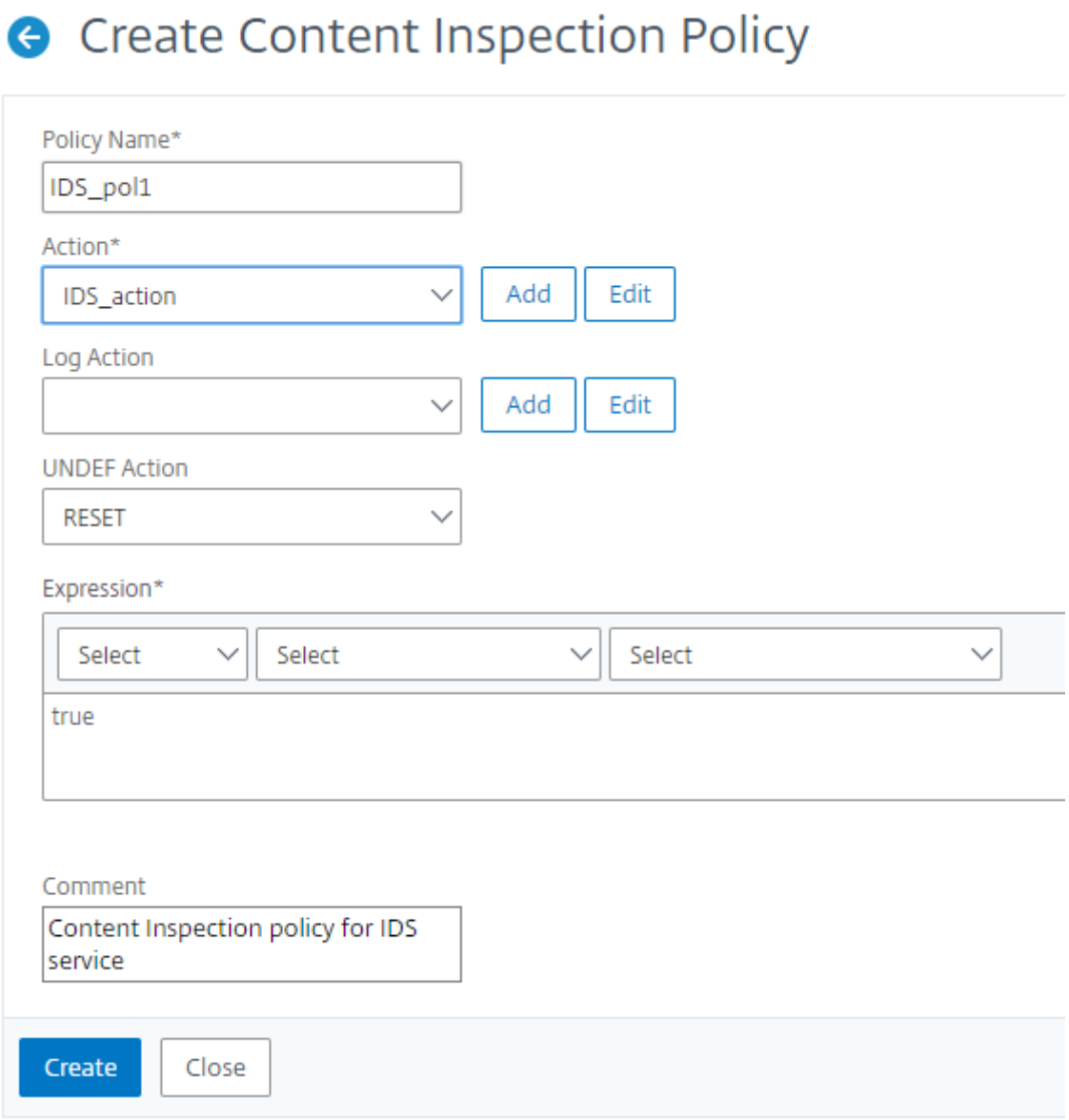
d) Si le serveur est en panne. Sélectionnez une opération si le serveur tombe en panne.
e) Délai d'expiration de la demande. Sélectionnez une valeur de délai d'expiration. Les valeurs par défaut peuvent être utilisées.
f) Action de délai d'expiration de demande. Sélectionnez une action de délai d'expiration. Les valeurs par défaut peuvent être utilisées.

19. Cliquez sur **Create**.



20. Sur la page **Créer une stratégie de CI**, entrez d'autres détails.
21. Cliquez sur **OK** et sur **Fermer**.

Pour plus d'informations sur la configuration de l'interface graphique NetScaler pour l'équilibrage de charge et la réplication du trafic vers les appareils IDS, consultez la section Équilibrage de charge.



Pour plus d'informations sur la configuration de l'interface graphique NetScaler pour l'équilibrage de charge et le transfert du trafic vers le serveur d'origine principal après la transformation du contenu, consultez la section Équilibrage de charge.

Statistiques d'inspection de contenu pour ICAP, IPS et IDS

January 21, 2021

Les statistiques d'inspection de contenu pour les périphériques ICAP, IDS (Inline Device Integration) et IPS (Intrusion Prevention System) sont une sortie détaillée (résumé) des détails de demande, de réponse et d'action du serveur.

Les statistiques d'inspection du contenu sont un ensemble de données statistiques qui incluent la requête HTTP/HTTPS envoyée pour l'inspection du contenu. Réponse HTTP/HTTPS reçue des périphériques IPS, IDS et ICAP et action serveur back-end.

Pour afficher les statistiques d'inspection de contenu à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

```
stat contentInspection
```

```
ContentInspection Stats

Inline Statistics
                                  Total
Requests                           10
Responses                           6
Request Bytes Sent                 3235
Request Bytes Received             2977
Response Bytes Sent                17302
Response Bytes Received            19681
Serverdown Reset Action taken       1
Serverdown Drop Action taken        0
Serverdown BYPASS Action taken      0
Inline device Generated Response    3

Mirror Statistics
                                  Total
Requests                           4
Responses                          4
Requests Bytes Sent               2763
Responses Bytes Sent              16732
Serverdown Reset Action taken      0
Serverdown Drop Action taken       0
Serverdown BYPASS Action taken     1

ICAP Statistics
                                  Total
REQMOD requests Sent                6
RESPMOD requests Sent               4
Preview requests                    1
204 Responses Received              6
100 Continue Responses Received     1
204 NO content Received             5
Adaptive Requests                   0
Adaptive Responses                  4
Callout requests Initiated          1
```



```
Callout requests completed          1
ICAP Req/Resp Errors handled        1
Serverdown Reset Action taken       1
Serverdown Drop Action taken        0
Serverdown BYPASS Action taken      1

Done
<!--NeedCopy-->
```

Proxy de transfert SSL

May 5, 2023

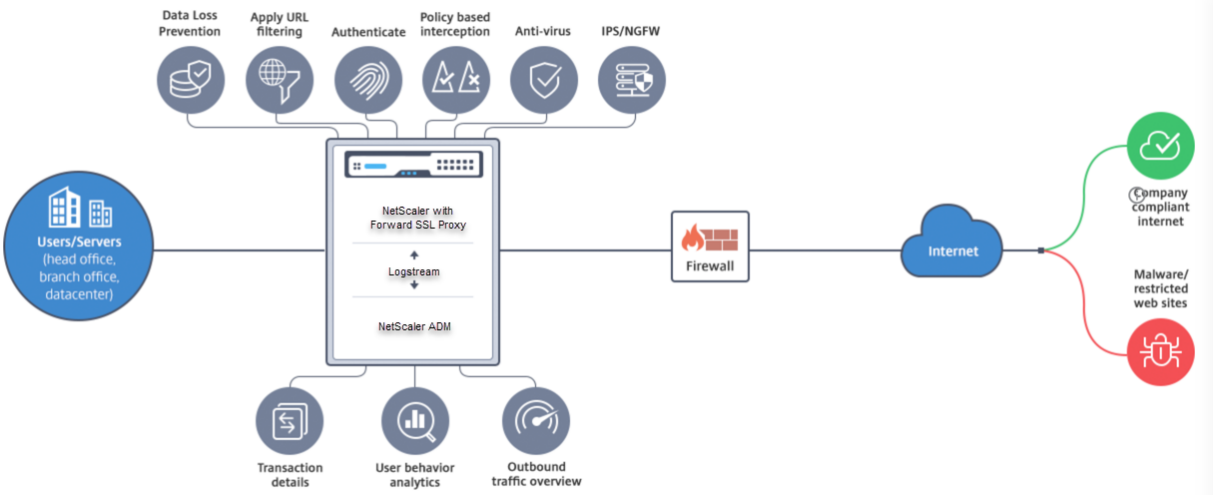
Remarque : La fonctionnalité proxy de transfert SSL est disponible avec la licence ADC Premium.

Le trafic Web a augmenté de façon exponentielle ces dernières années, et les entreprises comptent de plus en plus sur Internet pour leurs activités quotidiennes. Ceci, combiné à l'émergence de terminaux plus diversifiés, à la mobilité et au BYOD, ainsi qu'à une base croissante d'attaquants, fait des utilisateurs des cibles faciles pour les malwares modernes. Ils sont de plus en plus vulnérables au vol d'identité et à la compromission de leurs données. Traditionnellement, les entreprises inspectaient le trafic HTTP à la recherche de malwares et de virus. Ils ont contourné le trafic HTTPS/TLS, car il n'était pas aussi important. Il a été utilisé avec parcimonie pour les contenus sensibles et fiables. Mais cela a rapidement changé, car la plupart des sites Internet publics préfèrent désormais utiliser le protocole HTTPS pour protéger la confidentialité des utilisateurs. Par conséquent, l'impossibilité d'inspecter les paquets chiffrés permet des malwares ou des intrusions dans le réseau de l'entreprise. La solution de proxy SSL Forward propose des outils que les entreprises peuvent utiliser pour se protéger contre les menaces Internet.

Un proxy est un serveur qui contrôle tout le trafic entre les utilisateurs et les applications Internet ou SaaS. Puisque tout le trafic passe par ce proxy, il exécute des fonctions liées à la sécurité, telles que l'authentification des utilisateurs et la catégorisation des URL.

La figure suivante présente une vue d'ensemble de l'implémentation du proxy de transfert SSL. Le trafic circule à travers le réseau de l'entreprise à partir du siège social, des succursales, du centre de données et des employés distants. Une appliance NetScaler située à la périphérie du réseau fait office de proxy. L'appliance peut fonctionner en mode proxy transparent ou en mode proxy explicite et propose des contrôles pour intercepter le trafic Internet, y compris HTTPS. Les politiques configurées sur l'appliance déterminent si elle intercepte, contourne ou bloque une demande particulière. L'accès aux sites restreints peut être bloqué à l'aide du filtrage des URL. Un utilisateur est authentifié avant de se connecter au réseau de l'entreprise. Toutes les demandes et réponses sont balisées pour identifier

l'utilisateur, et l'accès au site Internet est classé par catégorie. L'activité des utilisateurs est enregistrée et utilisée pour générer des rapports. En cas de violation, les administrateurs peuvent isoler le système infecté, déterminer si les périphériques des autres utilisateurs qui ont visité ce site Web sont compromis et prendre les mesures appropriées. Lorsque vous intégrez NetScaler Application Delivery Management (ADM) au proxy de transfert SSL, l'activité utilisateur enregistrée et les enregistrements suivants dans l'appliance sont exportés vers NetScaler ADM à l'aide de. `logstream` NetScaler ADM rassemble et présente des informations sur les activités des utilisateurs, qu'il s'agisse des sites Web visités ou du temps passé en ligne. Il fournit également des informations sur l'utilisation de la bande passante et les menaces détectées, telles que les logiciels malveillants et les sites de phishing. Vous pouvez utiliser ces indicateurs clés pour surveiller votre réseau et utiliser la fonction de proxy de transfert SSL pour prendre des mesures correctives.



Le proxy de transfert SSL permet aux directeurs informatiques d'effectuer les opérations suivantes :

- Gagnez en visibilité sur le trafic sécurisé autrement contourné.
- Bloquez l'accès à des sites malveillants ou inconnus et évitez d'infecter les utilisateurs au sein de l'entreprise.
- Contrôlez l'accès à certains sites Web, tels que le courrier personnel, les réseaux sociaux et les sites Web de recherche d'emploi, depuis le réseau de l'entreprise.
- Appliquez des politiques de contrôle du contenu intelligentes pour garantir une productivité maximale des utilisateurs.

Premiers pas avec la fonctionnalité de proxy de transfert SSL

May 5, 2023

Important :

- La vérification OCSP nécessite une connexion Internet pour vérifier la validité des certificats. Si votre appliance n'est pas accessible depuis Internet à l'aide de l'adresse NSIP, ajoutez des listes de contrôle d'accès (ACL) pour effectuer la NAT de l'adresse NSIP à l'adresse IP du sous-réseau (SNIP). Le SNIP doit être en mesure d'accéder à Internet. Par exemple,

```
add ns acl a1 ALLOW -srcIP = <NSIP> -destIP  "!="
    10.0.0.0-10.255.255.255

add rnat RNAT-1 a1

bind rnat RNAT-1 <SNIP>

apply acls
<!--NeedCopy-->
```

- Spécifiez un serveur de noms DNS pour résoudre les noms de domaine.
- Assurez-vous que la date de l'appliance est synchronisée avec celle des serveurs NTP. Si la date n'est pas synchronisée, l'appliance ne peut pas vérifier efficacement si un certificat du serveur d'origine a expiré.

Pour utiliser la fonctionnalité de proxy de transfert SSL, vous devez effectuer les tâches suivantes :

- Ajoutez un serveur proxy en mode explicite ou transparent.
- Activez l'interception SSL.
  - Configurez un profil SSL.
  - Ajoutez et liez des stratégies SSL au serveur proxy.
  - Ajoutez et liez une paire de clés de certification CA pour l'interception SSL.

Remarque :

Une appliance ADC configurée en mode proxy transparent ne peut intercepter que les protocoles HTTP et HTTPS. Pour contourner tout autre protocole, tel que telnet, vous devez ajouter la stratégie d'écoute suivante sur le serveur virtuel proxy.

Le serveur virtuel accepte désormais uniquement le trafic entrant HTTP et HTTPS.

```
set cs vserver transparent-pxy1 PROXY * * -cltTimeout 180 -Listenpolicy
    "CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443)"`
<!--NeedCopy-->
```

Vous devrez peut-être configurer les fonctionnalités suivantes, en fonction de votre déploiement :

- Service d'authentification (recommandé) : pour authentifier les utilisateurs. Sans le service d'authentification, l'activité de l'utilisateur est basée sur l'adresse IP du client.
- Filtrage d'URL : pour filtrer les URL par catégories, score de réputation et listes d'URL.

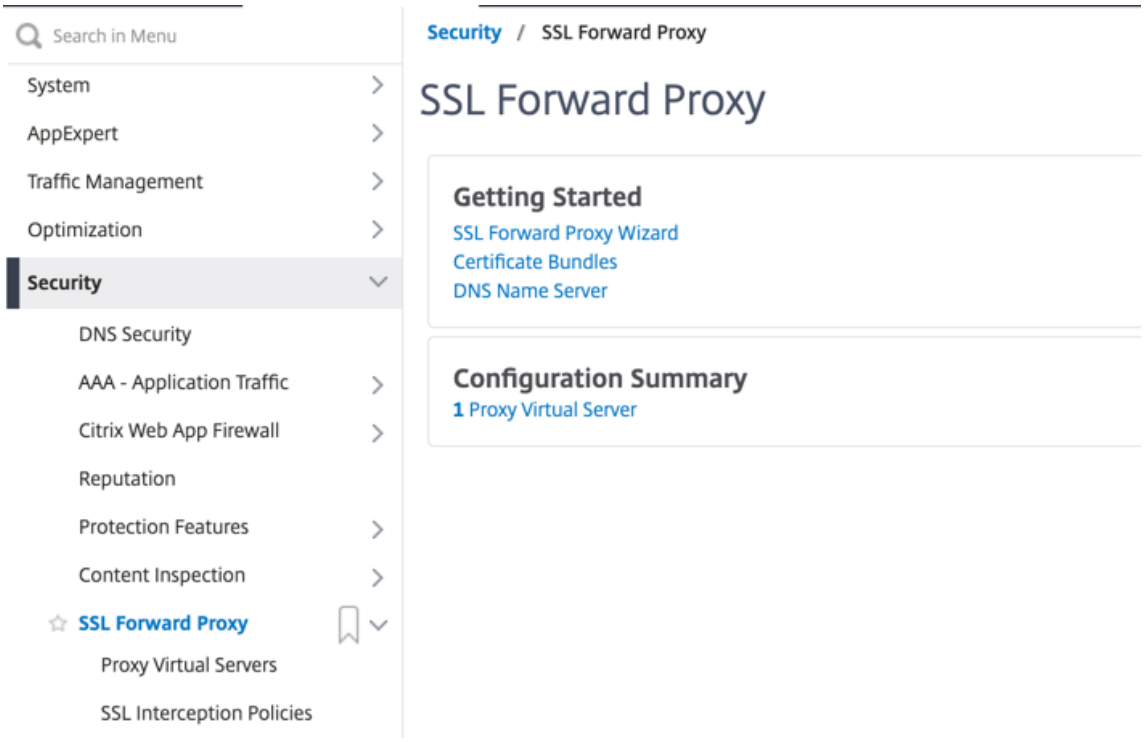
- Analyses : pour visualiser l'activité des utilisateurs, les indicateurs de risque des utilisateurs, la consommation de bande passante et la ventilation des transactions dans NetScaler Application Delivery Management (ADM).

Remarque : SSL Forward Proxy implémente les normes HTTP et HTTPS les plus courantes, suivies de produits similaires. Cette implémentation est faite sans navigateur spécifique à l'esprit et est compatible avec la plupart des navigateurs courants. SSL Forward Proxy a été testé avec des navigateurs courants et des versions récentes de Google Chrome, Internet Explorer et Mozilla Firefox.

Assistant de transfert de proxy SSL

L'assistant de proxy de transfert SSL fournit aux administrateurs un outil permettant de gérer l'intégralité du déploiement du proxy de transfert SSL à l'aide d'un navigateur Web. Il aide les clients à mettre en place rapidement un service proxy de transfert SSL et simplifie la configuration en suivant une séquence d'étapes bien définies.

1. Accédez à **Sécurité > Proxy de transfert SSL**. Dans **Mise en route**, cliquez sur **Assistant proxy de transfert SSL**.



2. Suivez les étapes de l'assistant pour configurer votre déploiement.

Ajouter une stratégie d'écoute au serveur proxy transparent

1. Accédez à **Sécurité > Proxy SSL Forward** > **Serveurs virtuels proxy**. Sélectionnez le serveur proxy transparent et cliquez sur **Modifier**.

2. Modifiez **les paramètres de base**, puis cliquez sur **Plus**.
3. Dans **Priorité d'écoute**, saisissez 1.
4. Dans **Expression de stratégie d'écoute**, entrez l'expression suivante :

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

Cette expression suppose des ports standard pour le trafic HTTP et HTTPS. Si vous avez configuré différents ports, par exemple 8080 pour HTTP ou 8443 pour HTTPS, modifiez l'expression pour refléter ces ports.

Limitations

Le proxy de transfert SSL n'est pas pris en charge dans une configuration de cluster, dans les partitions d'administration et sur une appliance NetScaler FIPS.

Modes proxy

May 5, 2023

L'appliance NetScaler agit en tant que proxy du client pour se connecter à Internet et aux applications SaaS. En tant que proxy, il accepte tout le trafic et détermine le protocole du trafic. À moins que le trafic ne soit HTTP ou SSL, il est transféré tel quel vers la destination. Lorsque l'appliance reçoit une demande d'un client, elle intercepte la demande et exécute certaines actions, telles que l'authentification des utilisateurs, la catégorisation des sites et la redirection. Il utilise des politiques pour déterminer le trafic à autoriser et le trafic à bloquer.

L'appliance gère deux sessions différentes, l'une entre le client et le proxy et l'autre entre le proxy et le serveur d'origine. Le proxy s'appuie sur des politiques définies par le client pour autoriser ou bloquer le trafic HTTP et HTTPS. Il est donc important que vous définissiez des politiques pour contourner les données sensibles, telles que les informations financières. L'appliance propose un ensemble complet d'attributs de trafic de couche 4 à 7 et d'attributs d'identité utilisateur pour créer des politiques de gestion du trafic.

Pour le trafic SSL, le proxy vérifie le certificat du serveur d'origine et établit une connexion légitime avec le serveur. Il émule ensuite le certificat de serveur, le signe à l'aide d'un certificat CA installé sur NetScaler et présente le certificat de serveur créé au client. Vous devez ajouter le certificat CA en tant que certificat de confiance au navigateur du client pour que la session SSL soit correctement établie.

L'appliance prend en charge les modes proxy transparents et explicites. En mode proxy explicite, le client doit spécifier une adresse IP dans son navigateur, à moins que l'organisation n'envoie le

paramètre sur le périphérique du client. Cette adresse est l'adresse IP d'un serveur proxy configuré sur l'appliance ADC. Toutes les demandes client sont envoyées à cette adresse IP. Pour un proxy explicite, vous devez configurer un serveur virtuel de commutation de contenu de type PROXY et spécifier une adresse IP et un numéro de port valide.

Le proxy transparent, comme son nom l'indique, est transparent pour le client. En d'autres termes, les clients peuvent ne pas savoir qu'un serveur proxy effectue la médiation de leurs demandes. L'appliance ADC est configurée dans le cadre d'un déploiement en ligne et accepte de manière transparente tout le trafic HTTP et HTTPS. Pour un proxy transparent, vous devez configurer un serveur virtuel de commutation de contenu de type PROXY, avec des astérisques (* *) comme adresse IP et port. Lorsque vous utilisez l' **assistant SSL Forward Proxy** dans l'interface graphique, vous n'avez pas à spécifier d'adresse IP ni de port.

> **Remarque**
>
> Pour intercepter des protocoles autres que HTTP et HTTPS en mode proxy transparent, vous devez ajouter une stratégie d'écoute et la lier au serveur proxy.

Configurer le proxy de transfert SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add cs vserver <name> PROXY <ipaddress> <port>
<!--NeedCopy-->
```

Arguments :

Nom :

Nom du serveur proxy. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Ne peut pas être modifié après la création du serveur virtuel CS.

L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comporte un ou plusieurs espaces, mettez-le entre guillemets doubles ou simples (par exemple, « mon serveur » ou « mon serveur »).

Cet argument est obligatoire. Longueur maximale : 127

Adresse IP :

Adresse IP du serveur proxy.

Port :

Numéro de port du serveur proxy. Valeur minimale : 1

Exemple de proxy explicite :

```
add cs vserver swgVS PROXY 192.0.2.100 80
<!--NeedCopy-->
```

Exemple de proxy transparent :

```
add cs vserver swgVS PROXY * *
<!--NeedCopy-->
```

Ajoutez une politique d'écoute au serveur proxy transparent à l'aide de l'interface graphique

1. Accédez à **Sécurité** > **Proxy transfert SSL** > **Serveurs virtuels proxy**. Sélectionnez le serveur proxy transparent et cliquez sur **Modifier**.
2. Modifiez **les paramètres de base**, puis cliquez sur **Plus**.
3. Dans **Priorité d'écoute**, saisissez 1.
4. Dans **Expression de stratégie d'écoute**, entrez l'expression suivante :

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

> **Remarque**
>
> Cette expression suppose des ports standard pour le trafic HTTP et HTTPS. Si vous avez configuré différents ports, par exemple 8080 pour HTTP ou 8443 pour HTTPS, modifiez l'expression précédente pour spécifier ces ports.

Interception SSL

May 5, 2023

Une appliance NetScaler configurée pour l'interception SSL agit en tant que proxy. Il peut intercepter et déchiffrer le trafic SSL/TLS, inspecter la demande non chiffrée et permettre à un administrateur d'appliquer les règles de conformité et les contrôles de sécurité. L'interception SSL utilise une stratégie qui spécifie le trafic à intercepter, bloquer ou autoriser. Par exemple, le trafic à destination et en provenance de sites Web financiers, tels que les banques, ne doit pas être intercepté, mais tout autre trafic peut être intercepté et les sites sur liste noire peuvent être identifiés et bloqués. Citrix vous recommande de configurer une stratégie générique pour intercepter le trafic et des stratégies plus spécifiques pour contourner un certain trafic.

Le client et le proxy établissent une liaison HTTPS/TLS. Le proxy établit une autre liaison HTTPS/TLS avec le serveur et reçoit le certificat du serveur. Le proxy vérifie le certificat du serveur pour le compte du client et vérifie également la validité du certificat du serveur à l'aide du protocole OCSP (Online Certificate Status Protocol). Il régénère le certificat du serveur, le signe à l'aide de la clé du certificat CA installé sur l'appliance et le présente au client. Par conséquent, un certificat est utilisé entre le client et l'appliance NetScaler, et un autre entre l'appliance et le serveur principal.

> **Important**
>
> Le certificat d'autorité de certification utilisé pour signer le certificat de serveur doit être préinstallé sur tous les périphériques clients, de sorte que le certificat de serveur régénéré soit approuvé par le client.

Pour le trafic HTTPS intercepté, le serveur proxy déchiffre le trafic sortant, accède à la requête HTTP en texte clair et peut utiliser n'importe quelle application de couche 7 pour traiter le trafic, par exemple en examinant l'URL en texte brut et en autorisant ou en bloquant l'accès en fonction de la politique de l'entreprise et de la réputation de l'URL. Si la décision politique est d'autoriser l'accès au serveur d'origine, le serveur proxy transmet la demande recryptée au service de destination (sur le serveur d'origine). Le proxy déchiffre la réponse à partir du serveur d'origine, accède à la réponse HTTP en texte clair et applique éventuellement toutes les stratégies à la réponse. Le proxy chiffre ensuite à nouveau la réponse et la transmet au client. Si la décision de stratégie consiste à bloquer la demande au serveur d'origine, le proxy peut envoyer une réponse d'erreur, telle que HTTP 403, au client.

Pour effectuer une interception SSL, en plus du serveur proxy configuré précédemment, vous devez configurer les éléments suivants sur l'appliance ADC :

- Profil SSL
- Politique SSL
- Boutique de certificats CA
- Apprentissage automatique des erreurs SSL et mise en cache

> **Remarque :**
>
> Le trafic HTTP/2 n'est pas intercepté par la fonctionnalité d'interception SSL.

Magasin de certificats d'interception SSL

Un certificat SSL, qui fait partie de toute transaction SSL, est un formulaire de données numérique (X509) qui identifie une entreprise (domaine) ou un individu. Un certificat SSL est émis par une autorité de certification (CA). Une autorité de certification peut être privée ou publique. Les certificats émis par des autorités de certification publiques, telles que Verisign, sont approuvés par les applications qui effectuent des transactions SSL. Ces applications tiennent à jour une liste d'autorités de certification qu'elles ont confiance.

En tant que proxy de transfert, l'appliance ADC assure le chiffrement et le déchiffrement du trafic entre un client et un serveur. Il agit comme un serveur pour le client (utilisateur) et comme un client pour le serveur. Avant qu'une appliance puisse traiter le trafic HTTPS, elle doit valider l'identité d'un serveur afin d'empêcher toute transaction frauduleuse. Par conséquent, en tant que client du serveur d'origine, l'appliance doit vérifier le certificat du serveur d'origine avant de l'accepter. Pour vérifier un certificat de serveur, tous les certificats (par exemple, les certificats racine et intermédiaire) utilisés pour signer et émettre le certificat de serveur doivent être présents sur l'appliance. Un ensemble de certificats d'autorité de certification par défaut est préinstallé sur une appliance. L'appliance peut utiliser ces certificats pour vérifier presque tous les certificats de serveur d'origine courants. Ce jeu par défaut ne peut pas être modifié. Toutefois, si votre déploiement nécessite davantage de certificats CA, vous pouvez créer un ensemble de ces certificats et l'importer dans l'appliance. Un bundle peut également contenir un seul certificat.

Lorsque vous importez un bundle de certificats dans l'appliance, l'appliance télécharge le bundle depuis l'emplacement distant et, après avoir vérifié que le bundle ne contient que des certificats, l'installe sur l'appliance. Vous devez appliquer un ensemble de certificats avant de pouvoir l'utiliser pour valider un certificat de serveur. Vous pouvez également exporter un ensemble de certificats pour modification ou le stocker dans un emplacement hors connexion en tant que sauvegarde.

Importez et appliquez un bundle de certificats CA sur l'appliance à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
import ssl certBundle <name> <src>
apply ssl certBundle <name>
<!--NeedCopy-->
```

```
show ssl certBundle
<!--NeedCopy-->
```

ARGUMENTS :

Nom :

Nom à attribuer au bundle de certificats importé. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comporte un ou plusieurs espaces, mettez-le entre guillemets simples ou doubles (par exemple, « mon fichier » ou « mon fichier »).

Longueur maximale : 31

src :

URL spécifiant le protocole, l'hôte et le chemin, y compris le nom du fichier, vers le bundle de certificats à importer ou à exporter. Par exemple, `http://www.example.com/cert_bundle_file`.

REMARQUE : L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS nécessitant une authentification par certificat client pour y accéder.

Longueur maximale : 2047

Exemple :

```
import ssl certbundle swg-certbundle http://www.example.com/cert_bundle
apply ssl certBundle swg-certbundle
<!--NeedCopy-->
```

```
show ssl certbundle

            Name : swg-certbundle(Inuse)

            URL : http://www.example.com/cert_bundle

    Done
<!--NeedCopy-->
```

Importez et appliquez un bundle de certificats CA sur l'appliance à l'aide de l'interface graphique

1. Accédez à **Sécurité > Proxy transfert SSL > Démarrage > Offres groupées de certificats**.
2. Procédez comme suit :
   - Sélectionnez un ensemble de certificats dans la liste.
   - Pour ajouter un lot de certificats, cliquez sur « + » et spécifiez un nom et une URL source. Cliquez sur **OK**.
3. Cliquez sur **OK**.

Supprimer un bundle de certificats CA de l'appliance à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
remove certBundle <cert bundle name>
<!--NeedCopy-->
```

Exemple :


```
remove certBundle mytest-cacert
<!--NeedCopy-->
```

Exportez un bundle de certificats CA depuis l'appliance à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
export certBundle <cert bundle name> <Path to export>
<!--NeedCopy-->
```

ARGUMENTS :

Nom :

Nom à attribuer au bundle de certificats importé. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comporte un ou plusieurs espaces, mettez-le entre guillemets simples ou doubles (par exemple, « mon fichier » ou « mon fichier »).

Longueur maximale : 31

src :

URL spécifiant le protocole, l'hôte et le chemin, y compris le nom du fichier, vers le bundle de certificats à importer ou à exporter. Par exemple, `http://www.example.com/cert_bundle_file`.

REMARQUE : L'importation échoue si l'objet à importer se trouve sur un serveur HTTPS nécessitant une authentification par certificat client pour y accéder.

Longueur maximale : 2047

Exemple :

```
export certBundle mytest-cacert http://192.0.2.20/
<!--NeedCopy-->
```

Importer, appliquer et vérifier un ensemble de certificats CA depuis le magasin de certificats CA de Mozilla

À l'invite de commande, tapez :


```
> import certbundle mozilla_public_ca https://curl.haxx.se/ca/cacert.pem
Done
<!--NeedCopy-->
```

Pour appliquer le bundle, tapez :

```
> apply certbundle mozilla_public_ca
Done
<!--NeedCopy-->
```

Pour vérifier l'ensemble de certificats en cours d'utilisation, tapez :

```
> sh certbundle | grep mozilla
                Name : mozilla_public_ca (Inuse)
<!--NeedCopy-->
```

Limitations

- Les lots de certificats ne sont pas pris en charge dans une configuration de cluster ou sur une appliance partitionnée.
- Le protocole TLSv1.3 n'est pas pris en charge avec le proxy SSL Forward.

Infrastructure de politique SSL pour l'interception SSL

Une stratégie agit comme un filtre sur le trafic entrant. Les politiques de l'appliance ADC aident à définir la manière de gérer les connexions et les demandes par proxy. Le traitement est basé sur les actions configurées pour cette stratégie. Autrement dit, les données des demandes de connexion sont comparées à une règle spécifiée dans la stratégie et l'action est appliquée aux connexions qui correspondent à la règle (expression). Après avoir défini une action à attribuer à la politique et créé la politique, vous devez la lier à un serveur proxy afin qu'elle s'applique au trafic passant par ce serveur proxy.

Une stratégie SSL pour l'interception SSL évalue le trafic entrant et applique une action prédéfinie aux requêtes qui correspondent à une règle (expression). La décision d'intercepter, de contourner ou de réinitialiser une connexion est prise en fonction de la politique SSL définie. Vous pouvez configurer l'une des trois actions d'une stratégie : Intercept, BYPASS ou RESET. Vous devez spécifier une action lorsque vous créez une politique. Pour mettre en œuvre une politique, vous devez la lier à un serveur proxy sur l'appliance. Pour spécifier qu'une politique est destinée à l'interception SSL, vous devez spécifier le type (point de liaison) comme INTERCEPT_REQ lorsque vous liez la politique à un serveur proxy. Lorsque vous dissociez une politique, vous devez spécifier le type INTERCEPT_REQ.

> **Remarque** :
>
> Le serveur proxy ne peut pas prendre la décision d'intercepter à moins que vous ne spécifiiez une politique.

L'interception du trafic peut être basée sur n'importe quel attribut de poignée de main SSL. Le domaine le plus couramment utilisé est le domaine SSL. Le domaine SSL est généralement indiqué par les attributs de l'établissement de connexion SSL. Il peut s'agir de la valeur de l'indicateur de nom de serveur extraite du message Hello client SSL, le cas échéant, ou de la valeur de nom alternatif de serveur (SAN) extraite du certificat du serveur d'origine. La stratégie d'interception SSL présente un attribut spécial, DETECTED_DOMAIN. Cet attribut permet aux clients de créer plus facilement des stratégies d'interception basées sur le domaine SSL à partir du certificat du serveur d'origine. Le client peut faire correspondre le nom de domaine avec une chaîne, une liste d'URL (jeu d'URL ou`patset`) ou une catégorie d'URL dérivée du domaine.

Créer une stratégie SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ssl policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Exemples :

Les exemples suivants concernent les politiques comportant des expressions qui utilisent l'`detected_domain` attribut pour vérifier la présence d'un nom de domaine.

Ne pas intercepter le trafic vers une institution financière, telle que XYZBANK

```
add ssl policy pol1 -rule client.ssl.detected_domain.contains("XYZBANK"
    ) -action BYPASS
<!--NeedCopy-->
```

Ne pas autoriser un utilisateur à se connecter à YouTube depuis le réseau de l'entreprise

```
add ssl policy pol2 -rule client.ssl.client.ssl.detected_domain.
    url_categorize(0,0).category.eq ("YouTube") -action RESET
<!--NeedCopy-->
```

Intercepter tout le trafic utilisateur

```
add ssl policy pol3 - rule true - action INTERCEPT
<!--NeedCopy-->
```


Si le client ne souhaite pas utiliser le domaine detected_domain, il peut utiliser l'un des attributs de handshake SSL pour extraire et déduire le domaine.

Par exemple, aucun nom de domaine ne figure dans l'extension SNI du message d'accueil du client. Le nom de domaine doit être extrait du certificat du serveur d'origine. Les exemples suivants concernent les stratégies avec des expressions qui vérifient la présence d'un nom de domaine dans le nom de sujet du certificat du serveur d'origine.

Intercepter tout le trafic utilisateur vers n'importe quel domaine Yahoo

```
1 add ssl policy pol4 -rule client.ssl.origin_server_cert.subject.
     contains("yahoo")  - action INTERCEPT
2 <!--NeedCopy-->
```

Interceptez tout le trafic utilisateur pour la catégorie « Shopping/Retail »

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
     subject.URL_CATEGORIZE(0,0).CATEGORY.eq("Shopping/Retail") -action
     INTERCEPT
2 <!--NeedCopy-->
```

Intercepter tout le trafic utilisateur vers une URL non classée

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
     subject.url_categorize(0,0).category.eq("Uncategorized") -action
     INTERCEPT
2 <!--NeedCopy-->
```

Les exemples suivants concernent les stratégies qui correspondent au domaine par rapport à une entrée d'un jeu d'URL.

Interceptez tout le trafic utilisateur si le nom de domaine dans SNI correspond à une entrée de l'ensemble d'URL « top100 »

```
1 add ssl policy pol_url_set  -rule client.ssl.client_hello.SNI.
     URLSET_MATCHES_ANY("top100") -action INTERCEPT
2 <!--NeedCopy-->
```

Interceptez tout le trafic utilisateur du nom de domaine si le certificat du serveur d'origine correspond à une entrée de l'ensemble d'URL « top100 »

```
1 add ssl policy pol_url_set  -rule client.ssl.origin_server_cert.subject
     .URLSET_MATCHES_ANY("top100") -action INTERCEPT
2 <!--NeedCopy-->
```


Créer une stratégie SSL sur un serveur proxy à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL > Stratégies**.
2. Dans l'onglet **Politiques SSL**, cliquez sur **Ajouter** et spécifiez les paramètres suivants :
   - Nom de la stratégie
   - Action de politique : sélectionnez l'interception, le contournement ou la réinitialisation.
   - Expression
3. Cliquez sur **Create**.

Liez une politique SSL à un serveur proxy à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type  INTERCEPT_REQ
<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver <name> -policyName pol1 -priority 10 -type
   INTERCEPT_REQ
<!--NeedCopy-->
```

Liez une politique SSL à un serveur proxy à l'aide de l'interface graphique

1. Accédez à **Sécurité > Proxy SSL Forward > Serveurs virtuels proxy**.
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.
3. Dans **Paramètres avancés**, cliquez sur **Stratégies SSL**.
4. Cliquez à l'intérieur de la zone **Politique SSL** .
5. Dans **Sélectionner une stratégie**, sélectionnez une politique à lier.
6. Dans **Type**, sélectionnez **INTERCEPT_REQ**.
7. Cliquez sur **Lier**, puis sur **OK** .

Dissocier une stratégie SSL à un serveur proxy à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
unbind ssl vserver <vServerName> -policyName <string> -type
   INTERCEPT_REQ
<!--NeedCopy-->
```


Expressions SSL utilisées dans les politiques SSL

Expression	Description
`CLIENT.SSL.CLIENT_HELLO.SNI.*`	Renvoie l'extension SNI sous forme de chaîne. Évaluez la chaîne pour voir si elle contient le texte spécifié. Exemple : client.ssl.client_hello.sni.contains () "xyz.com"
`CLIENT.SSL.ORIGIN_SERVER_CERT.*`	Renvoie un certificat, reçu d'un serveur principal, sous forme de chaîne. Évaluez la chaîne pour voir si elle contient le texte spécifié. Exemple : client.ssl.origin_server_cert.subject.contains () "xyz.com"
`CLIENT.SSL.DETECTED_DOMAIN.*`	Renvoie un domaine, soit à partir de l'extension SNI, soit à partir du certificat du serveur d'origine, sous forme de chaîne. Évaluez la chaîne pour voir si elle contient le texte spécifié. Exemple : client.ssl.detected_domaine.contains ("xyz.com")

Erreur SSL | AutoLearning

L'appliance ajoute un domaine à la liste de contournement SSL si le mode d'apprentissage est activé. Le mode d'apprentissage est basé sur le message d'alerte SSL reçu d'un client ou d'un serveur d'origine. En d'autres termes, l'apprentissage dépend du client ou du serveur qui envoie un message d'alerte. Il n'y a pas d'apprentissage si un message d'alerte n'est pas envoyé. L'appliance apprend si l'une des conditions suivantes est remplie :

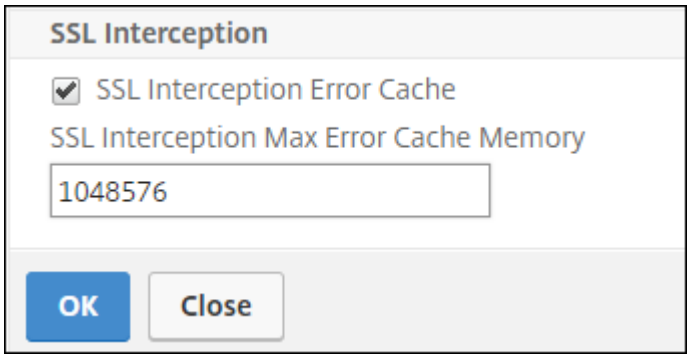
1. Une demande de certificat client est reçue du serveur.
2. L'une des alertes suivantes est reçue dans le cadre de la poignée de main :
    - BAD_CERTIFICATE
    - CERTIFICAT_NON PRIS EN CHARGE
    - CERTIFICATE_RÉVOQUÉ
    - CERTIFICATE_EXPIRÉ
    - CERTIFICAT_INCONNU
    - UNKNOWN_CA (Si un client utilise le pinning, il envoie ce message d'alerte s'il reçoit un

certificat de serveur.)
- HANDSHAKE_FAILURE

Pour activer l'apprentissage, vous devez activer le cache d'erreurs et spécifier la mémoire réservée à l'apprentissage.

Permettre l'apprentissage à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > SSL**.
2. Dans **Paramètres**, cliquez sur **Modifier les paramètres SSL avancés**.
3. Dans **Interception SSL**, sélectionnez **SSL Interception Error Cache**.
4. Dans **SSL Interception Max Error Cache Memory**, spécifiez la mémoire (en octets) à réserver.



5. Cliquez sur **OK**.

Permettre l'apprentissage à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl parameter -ssliErrorCache ( ENABLED | DISABLED ) -
    ssliMaxErrorCacheMem <positive_integer>
<!--NeedCopy-->
```

Arguments :

Cache d'erreurs SSL :

Activez ou désactivez l'apprentissage dynamique et mettez en cache les informations apprises pour prendre ultérieurement la décision d'intercepter ou de contourner les demandes. Lorsqu'elle est activée, l'appliance effectue une recherche dans le cache pour décider s'il convient de contourner la demande.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

Cachemem d'erreur SSLIMaxErrorCachemem :

Spécifiez la mémoire maximale, en octets, qui peut être utilisée pour mettre en cache les données apprises. Cette mémoire est utilisée comme cache LRU afin que les anciennes entrées soient remplacées par de nouvelles entrées une fois la limite de mémoire définie atteinte. La valeur 0 détermine automatiquement la limite.

Valeur par défaut : 0

Valeur minimale : 0

Valeur maximale : 4294967294

Profil SSL

Un profil SSL est un ensemble de paramètres SSL, tels que des chiffrements et des protocoles. Un profil est utile si vous avez des paramètres communs à différents serveurs. Au lieu de spécifier les mêmes paramètres pour chaque serveur, vous pouvez créer un profil, spécifier les paramètres du profil, puis lier le profil à différents serveurs. Si aucun profil SSL frontal personnalisé n'est créé, le profil frontal par défaut est lié aux entités côté client. Ce profil vous permet de configurer les paramètres de gestion des connexions côté client.

Pour l'interception SSL, vous devez créer un profil SSL et activer l'interception SSL dans le profil. Un groupe de chiffrement par défaut est lié à ce profil, mais vous pouvez configurer d'autres chiffrements en fonction de votre déploiement. Liez un certificat CA d'interception SSL à ce profil, puis liez le profil à un serveur proxy. Pour l'interception SSL, les paramètres essentiels d'un profil sont ceux utilisés pour les actions suivantes :

- Vérifiez l'état OCSP du certificat du serveur d'origine.
- Déclenchez la renégociation du client si le serveur d'origine demande une renégociation.
- Vérifiez le certificat du serveur d'origine avant de réutiliser la session SSL frontale.

Utilisez le profil principal par défaut lorsque vous communiquez avec les serveurs d'origine. Définissez tous les paramètres côté serveur, tels que les suites de chiffrement, dans le profil principal par défaut. Un profil principal personnalisé n'est pas pris en charge.

Pour obtenir des exemples des paramètres SSL les plus couramment utilisés, consultez la section « Exemple de profil » à la fin de cette section.

La prise en charge du chiffre/protocole diffère sur le réseau interne et externe. Dans les tableaux suivants, la connexion entre les utilisateurs et une appliance ADC est le réseau interne. Le réseau externe se trouve entre l'appliance et Internet.

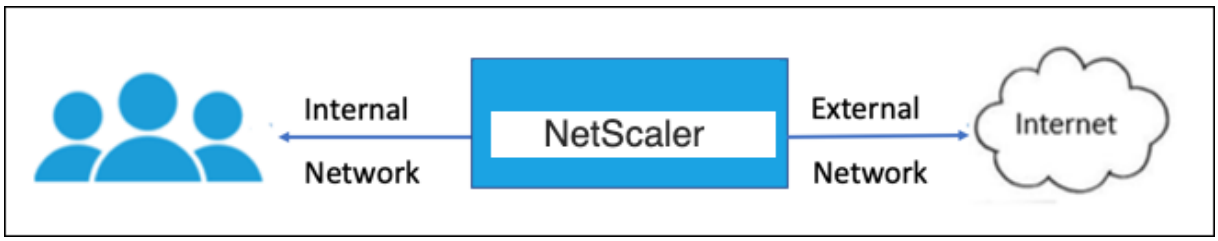


Tableau 1 : Matrice de prise en charge du chiffre/protocole pour le réseau interne

Reportez-vous au Tableau 1 : Support relatif au serveur virtuel/au service frontend ou au service interne dans Ciphersdisponibles sur les appliances NetScaler.

Tableau 2 : Matrice de prise en charge du chiffre/protocole pour le réseau externe

Reportez-vous au Tableau 2 : Support relatif aux services principaux dans Ciphers disponibles surles appliances NetScaler.

Ajouter un profil SSL et activer l'interception SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add ssl profile <name> -sslinterception ENABLED -ssliReneg ( ENABLED |
 DISABLED )-ssliOCSPCheck ( ENABLED | DISABLED )-ssliMaxSessPerServer <
positive_integer>
```

Arguments :

Interception SSL :

Activez ou désactivez l'interception des sessions SSL.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

SSL LireNeg :

Activez ou désactivez le déclenchement de la renégociation du client lorsqu'une demande de renégociation est reçue du serveur d'origine.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

Vérification SSLIOCSPCheck :

Activez ou désactivez la vérification OCSP pour un certificat de serveur d'origine.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : ENABLED

SSL Limax SESSpar serveur :

Nombre maximum de sessions SSL à mettre en cache par serveur d'origine dynamique. Une session SSL unique est créée pour chaque extension SNI reçue du client dans un message d'accueil du client. La session correspondante est utilisée pour la réutilisation de la session serveur.

Valeur par défaut : 10

Valeur minimale : 1

Valeur maximale : 1000

Exemple :

```
add ssl profile swg_ssl_profile  -sslinterception ENABLED

Done

sh ssl profile swg_ssl_profile

1)    Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                    Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0

                Deny SSL Renegotiation
                    ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

```



```
29                  SSL Redirect: DISABLED
30
31                  Send Close-Notify: YES
32
33                  Strict Sig-Digest Check: DISABLED
34
35                  Push Encryption Trigger: Always
36
37                  PUSH encryption trigger timeout:             1 ms
38
39                  SNI: DISABLED
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                NO
44
45                  Push flag:            0x0 (Auto)
46
47                  SSL quantum size:                            8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:               45
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                       Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
```



```
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75 1)            Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79 Done
80 <!--NeedCopy-->
```

Liez un certificat CA d'interception SSL à un profil SSL à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind ssl profile <name> -ssliCACertkey <ssli-ca-cert>
```

Exemple :

```
1  bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert
2
3  Done
4
5  sh ssl profile swg_ssl_profile
6
7  1)            Name: swg_ssl_profile (Front-End)
8
9                  SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                       .1: ENABLED  TLSv1.2: ENABLED
10
11                 Client Auth: DISABLED
12
13                 Use only bound CA certificates: DISABLED
14
15                 Strict CA checks:                                NO
16
17                 Session Reuse: ENABLED
                       Timeout: 120 seconds
18
19                 DH: DISABLED
20
21                 DH Private-Key Exponent Size Limit: DISABLED
                       Ephemeral RSA: ENABLED
                       Refresh Count: 0
```



```
22
23                  Deny SSL Renegotiation
                       ALL
24
25                  Non FIPS Ciphers: DISABLED
26
27                  Cipher Redirect: DISABLED
28
29                  SSL Redirect: DISABLED
30
31                  Send Close-Notify: YES
32
33                  Strict Sig-Digest Check: DISABLED
34
35                  Push Encryption Trigger: Always
36
37                  PUSH encryption trigger timeout:              1 ms
38
39                  SNI: DISABLED
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                          NO
44
45                  Push flag:             0x0 (Auto)
46
47                  SSL quantum size:                              8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:                45
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                       Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
```



```
64
65                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75 1)             Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79 1)             SSL Interception CA CertKey Name: swg_ca_cert
80
81 Done
82 <!--NeedCopy-->
```

Liez un certificat CA d'interception SSL à un profil SSL à l'aide de l'interface graphique

1. Accédez à **Système** > **Profils** > **Profil SSL**.
2. Cliquez sur **Ajouter**.
3. Spécifiez un nom pour le profil.
4. Activez l' **interception des sessions SSL**.
5. Cliquez sur **OK**.
6. Dans **Paramètres avancés**, cliquez sur **Clé de certificat**.
7. Spécifiez une clé de certificat CA d'interception SSL à lier au profil.
8. Cliquez sur **Sélectionner**, puis sur **Lier**.
9. Configurez éventuellement des chiffrements en fonction de votre déploiement.
   - Cliquez sur l'icône Modifier, puis sur **Ajouter**.
   - Sélectionnez un ou plusieurs groupes de chiffrement, puis cliquez sur la flèche droite.
   - Cliquez sur **OK**.
10. Cliquez sur **Terminé**.

Lier un profil SSL à un serveur proxy à l'aide de l'interface graphique

1. Accédez à **Sécurité** >**Proxy SSL Forward** > **Serveurs virtuels proxy**, puis ajoutez un serveur ou sélectionnez un serveur à modifier.
2. Dans **Profile SSL**, cliquez sur l'icône Modifier.
3. Dans la liste des **profils SSL**, sélectionnez le profil SSL que vous avez créé précédemment.
4. Cliquez sur **OK**.
5. Cliquez sur **Terminé**.

Exemple de profil :

```
Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED              TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                    Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0

                Deny SSL Renegotiation
                    ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

                SSL Redirect: DISABLED

                Send Close-Notify: YES

                Strict Sig-Digest Check: DISABLED

                Push Encryption Trigger: Always
```



```
30
31                  PUSH encryption trigger timeout:              1 ms
32
33                  SNI: DISABLED
34
35                  OCSP Stapling: DISABLED
36
37                  Strict Host Header check for SNI enabled SSL sessions:
                                NO
38
39                  Push flag:             0x0 (Auto)
40
41                  SSL quantum size:                             8 kB
42
43                  Encryption trigger timeout           100 mS
44
45                  Encryption trigger packet count:               45
46
47                  Subject/Issuer Name Insertion Format: Unicode
48
49                  SSL Interception: ENABLED
50
51                  SSL Interception OCSP Check: ENABLED
52
53                  SSL Interception End to End Renegotiation: ENABLED
54
55                  SSL Interception Maximum Reuse Sessions per Server:  10
56
57                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
58
59                  HSTS: DISABLED
60
61                  HSTS IncludeSubDomains: NO
62
63                  HSTS Max-Age: 0
64
65                  ECC Curve: P_256, P_384, P_224, P_521
66
67  1)            Cipher Name: DEFAULT Priority :1
68
69                  Description: Predefined Cipher Alias
70
71  1)            SSL Interception CA CertKey Name: swg_ca_cert
72  <!--NeedCopy-->
```


Gestion des identités utilisateur

May 5, 2023

Le nombre croissant de failles de sécurité et la popularité croissante des appareils mobiles ont mis en évidence la nécessité de s'assurer que l'utilisation de l'Internet externe est conforme aux politiques de l'entreprise. Seuls les utilisateurs autorisés doivent être autorisés à accéder aux ressources externes mises en service par le personnel de l'entreprise. La gestion des identités permet de vérifier l'identité d'une personne ou d'un appareil. Il ne détermine pas les tâches que l'individu peut effectuer ni les fichiers qu'il peut voir.

Un déploiement de proxy de transfert SSL identifie l'utilisateur avant d'autoriser l'accès à Internet. Toutes les demandes et réponses de l'utilisateur sont examinées. L'activité des utilisateurs est enregistrée et les enregistrements sont exportés vers NetScaler Application Delivery Management (ADM) à des fins de création de rapports. Dans NetScaler ADM, vous pouvez consulter les statistiques relatives aux activités des utilisateurs, aux transactions et à la consommation de bande passante.

Par défaut, seule l'adresse IP de l'utilisateur est enregistrée, mais vous pouvez configurer la fonctionnalité pour enregistrer plus de détails sur l'utilisateur. Vous pouvez utiliser ces informations d'identité pour créer des stratégies d'utilisation Internet plus riches pour des utilisateurs spécifiques.

L'appliance NetScaler prend en charge les modes d'authentification suivants pour une configuration de proxy explicite.

- **Protocole LDAP (Lightweight Directory Access Protocol)**. Authentifie l'utilisateur via un serveur d'authentification LDAP externe. Pour plus d'informations, consultez Politiques d'authentification LDAP.
- **RADIUS**. Authentifie l'utilisateur via un serveur RADIUS externe. Pour plus d'informations, consultez la section Authentification RADIUS.
- **TACACS+**. Authentifie l'utilisateur via un serveur d'authentification TACACS (Terminal Access Controller Access-Control System) externe. Pour plus d'informations, voir Politiques d'authentification TACACS.
- **Negotiate**. Authentifie l'utilisateur via un serveur d'authentification Kerberos. S'il y a une erreur dans l'authentification Kerberos, l'appliance utilise l'authentification NTLM. Pour plus d'informations, consultez la section Négociation des politiques d'authentification.

Pour le proxy transparent, seule l'authentification LDAP basée sur IP est prise en charge. Lorsqu'une demande client est reçue, le proxy authentifie l'utilisateur en vérifiant une entrée pour l'adresse IP du client dans Active Directory. Il crée ensuite une session en fonction de l'adresse IP de l'utilisateur.

Toutefois, si vous configurez le SSonameAttribute dans une action LDAP, une session est créée en utilisant le nom d'utilisateur au lieu de l'adresse IP. Les stratégies classiques ne sont pas prises en charge pour l'authentification dans une configuration de proxy transparente.

> **Remarque**
>
> Pour un proxy explicite, vous devez définir le nom de connexion LDAP sur **SAMAccountName**. Pour un proxy transparent, vous devez définir le nom de connexion LDAP sur **NetworkAddress** et attribute1 sur **SAMAccountName**.

Exemple de proxy explicite :

```
add authentication ldapAction swg-auth-action-explicit -serverIP
    10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
    CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
    freebsd123$ -ldapLoginName sAMAccountName
<!--NeedCopy-->
```

Exemple de proxy transparent :

```
add authentication ldapAction swg-auth-action-explicit -serverIP
    10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
    CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
    freebsd123$ -ldapLoginName networkAddress -authentication disable -
    Attribute1 sAMAccountName
<!--NeedCopy-->
```

Configuration de l'authentification des utilisateurs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add authentication vserver <vserver name> SSL

bind ssl vserver <vserver name> -certkeyName <certkey name>

add authentication ldapAction <action name> -serverIP <ip_addr> -
    ldapBase <string> -ldapBindDn <string> -ldapBindDnPassword -
    ldapLoginName <string>

add authentication Policy <policy name> -rule <expression> -action <
    string>

bind authentication vserver <vserver name> -policy <string> -priority <
    positive_integer>
```



```
10
11 set cs vserver <name> -authn401 ON -authnVsName <string>
12 <!--NeedCopy-->
```

Arguments :

Nom du serveur virtuel :

Nom du serveur virtuel d'authentification auquel lier la stratégie.

Longueur maximale : 127

Type de service :

Type de protocole du serveur virtuel d'authentification. Toujours SSL.

Valeurs possibles : SSL

Valeur par défaut : SSL

Nom de l'action :

Nom de la nouvelle action LDAP. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Impossible de modifier une fois l'action LDAP ajoutée. L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comprend un ou plusieurs espaces, inscrivez-le entre guillemets doubles ou simples (par exemple, « mon action d'authentification » ou « mon action d'authentification »).

Longueur maximale : 127

IP du serveur :

Adresse IP attribuée au serveur LDAP.

Base LDAP :

Base (nœud) à partir de laquelle lancer les recherches LDAP. Si le serveur LDAP s'exécute localement, la valeur par défaut de base est dc=netscaler, dc=com. Longueur maximale : 127

LDAPBindDN :

Nom unique complet (DN) utilisé pour la liaison au serveur LDAP.

Par défaut : CN=Manager, dc=netscaler, dc=com

Longueur maximale : 127

Mot de**passe LDAPBindDN** :

Mot de passe utilisé pour la liaison au serveur LDAP.

Longueur maximale : 127

Nom du plugin LDA :

Attribut de nom de connexion LDAP. L'appliance NetScaler utilise le nom de connexion LDAP pour interroger des serveurs LDAP externes ou Active Directory. Longueur maximale : 127

Nom de la stratégie :

Nom de la stratégie d'AUTHENTIFICATION avancée. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne doit contenir que des lettres, des chiffres et le trait d'union (-), le point (.), la livre (#), l'espace (), à (@), égal à (=), deux-points (:) et les caractères de soulignement. Impossible de modifier une fois qu'une stratégie d'AUTHENTIFICATION a été créée. L'exigence suivante s'applique uniquement à l'interface de ligne de commande :

Si le nom comprend un ou plusieurs espaces, inscrivez le nom entre guillemets doubles ou simples (par exemple, « ma stratégie d'authentification » ou « ma stratégie d'authentification »).

Longueur maximale : 127

règle :

Nom de la règle, ou expression de stratégie avancée, utilisée par la stratégie pour déterminer s'il faut tenter d'authentifier l'utilisateur auprès du serveur d'AUTHENTIFICATION.

Longueur maximale : 1499

action :

Nom de l'action d'authentification à effectuer si la stratégie correspond.

Longueur maximale : 127

Priorité :

Entier positif spécifiant la priorité de la stratégie. Un nombre inférieur indique une priorité plus élevée. Les stratégies sont évaluées dans l'ordre de leurs priorités, et la première stratégie correspondant à la demande est appliquée. Doit être unique dans la liste des stratégies liées au serveur virtuel d'authentification.

Valeur minimale : 0

Valeur maximale : 4294967295

Exemple :

```
add authentication vserver swg-auth-vs SSL

Done

bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey

```



```
Done

add authentication ldapAction swg-auth-action-explicit -serverIP
    192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
    Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword zzzzz
     -ldapLoginName sAMAccountName

Done

add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
    action-explicit
Done

bind authentication vserver swg-auth-vs -policy swg-auth-policy -
    priority 1

Done

set cs vserver testswg -authn401 ON -authnVsName swg-auth-vs

Done
<!--NeedCopy-->
```

Activer la journalisation des noms d'utilisateur à l'aide de la CLI

À l'invite de commande, tapez :

```
set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

Arguments :

Nom d'utilisateur AAA

Activez l'authentification AppFlow, l'autorisation et l'audit de la journalisation des noms d'utilisateur.

Valeurs possibles : ENABLED, DISABLED

Valeur par défaut : DISABLED

Exemple :

```
set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

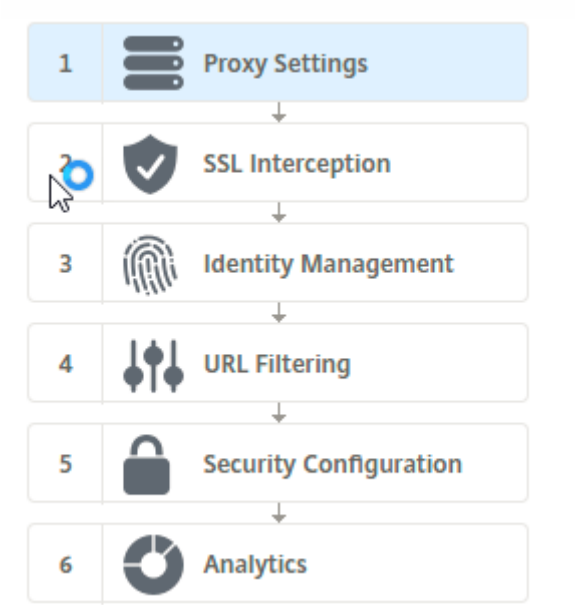

Filtrage d'URL

May 5, 2023

Le filtrage des URL permet de contrôler les sites Web selon des règles en utilisant les informations contenues dans les URL. Cette fonctionnalité permet aux administrateurs réseau de surveiller et de contrôler l'accès des utilisateurs aux sites Web malveillants sur le réseau.

Mise en route

Si vous êtes un nouvel utilisateur et que vous souhaitez configurer le filtrage des URL, vous devez terminer la configuration initiale du proxy SSL Forward. Pour commencer à utiliser le filtrage d'URL, vous devez d'abord vous connecter à l'assistant de proxy SSL Forward. L'assistant vous guide à travers une série d'étapes de configuration avant d'appliquer les politiques de filtrage d'URL.



> **Remarque**
>
> Avant de commencer, assurez-vous qu'une licence valide pour la fonctionnalité URL Threat Intelligence est installée sur votre appliance. Si vous utilisez une version d'essai, assurez-vous d'acheter une licence valide pour continuer à utiliser cette fonctionnalité sur l'appliance ADC.

Connectez-vous à l'assistant de transfert de proxy SSL

L'assistant de proxy SSL Forward vous guide à travers une série de tâches de configuration simplifiées et le volet droit affiche la séquence de flux correspondante. Vous pouvez utiliser cet assistant pour appliquer des politiques de filtrage d'URL à une liste d'URL ou à une liste prédéfinie de catégories.

Étape 1 : Configurer les paramètres de proxy

Configurez d'abord un serveur proxy via lequel le client accède à la passerelle. Ce serveur est de type SSL et fonctionne en mode explicite ou transparent. Pour plus d'informations sur la configuration du serveur proxy, voir Modes proxy.

Étape 2 : Configurer l'interception SSL

Après avoir configuré le serveur proxy, vous devez configurer le proxy d'interception SSL pour intercepter le trafic crypté sur l'appliance NetScaler. Dans le cas du filtrage d'URL, le proxy SSL intercepte le trafic et n'autorise pas les URL bloquées alors que tout autre trafic peut être contourné. Pour plus d'informations sur la configuration de l'interception SSL, consultez Interception SSL.

Étape 3 : Configurer la gestion des identités

Un utilisateur est authentifié avant d'être autorisé à se connecter au réseau de l'entreprise. L'authentification offre la flexibilité nécessaire pour définir des stratégies spécifiques pour un utilisateur ou un groupe d'utilisateurs, en fonction de leurs rôles. Pour plus d'informations sur l'authentification des utilisateurs, voir Gestion de l'identité des utilisateurs.

Étape 4 : Configurer le filtrage des URL

L'administrateur peut appliquer une stratégie de filtrage d'URL à l'aide de la fonctionnalité Catégorisation d'URL ou à l'aide de la fonctionnalité Liste d'URL.

Catégorisation des URL. Contrôle l'accès aux sites Web et aux pages Web en filtrant le trafic en fonction d'une liste prédéfinie de catégories.

Liste d'URL. Contrôle l'accès aux sites Web et pages Web mis en liste noire en refusant l'accès aux URL figurant dans un ensemble d'URL importé dans l'appliance.

Étape 5 : Configuration de la configuration de sécurité

Cette étape vous permet de configurer un score de réputation et de permettre aux utilisateurs de contrôler l'accès aux sites Web en refusant l'accès si le score est trop bas. Votre score de réputation peut aller de un à quatre, et vous pouvez configurer le seuil à partir duquel le score devient inacceptable. Pour les scores qui dépassent le seuil, vous pouvez sélectionner une action de stratégie pour autoriser, bloquer ou rediriger le trafic. Pour plus d'informations, voir Score de réputation d'URL.

Étape 6 : Configurer l'analyse de proxy de transfert SSL

Cette étape vous permet d'activer l'analyse de proxy SSL pour catégoriser le trafic Web, la catégorie d'URL de journalisation dans les journaux de transactions utilisateur et l'affichage des analyses de trafic. Pour plus d'informations sur l'analyse de proxy transfert SSL, consultez Analytics.

Étape 7 : Cliquez sur « Terminé » pour terminer la configuration initiale et continuer à gérer la configuration du filtrage d'URL

Liste des URL

May 5, 2023

La fonctionnalité de liste d'URL permet aux entreprises clientes de contrôler l'accès à des sites Web et à des catégories de sites Web spécifiques. La fonctionnalité filtre les sites Web en appliquant une politique de réponse liée à un algorithme de correspondance d'URL. L'algorithme compare l'URL entrante à un ensemble d'URL comprenant jusqu'à un million (1 000 000) d'entrées. Si la demande d'URL entrante correspond à une entrée de l'ensemble, l'appliance utilise la politique de réponse pour évaluer la demande (HTTP/HTTPS) et contrôler l'accès à celle-ci.

Types d'ensembles d'URL

Chaque entrée d'un ensemble d'URL peut inclure une URL et, éventuellement, ses métadonnées (catégorie d'URL, groupes de catégories ou toute autre donnée associée). Pour les URL avec métadonnées, l'appliance utilise une expression de stratégie qui évalue les métadonnées. Pour plus d'informations, voir Jeu d'URL.

Le proxy de transfert SSL prend en charge les ensembles d'URL personnalisés. Vous pouvez également utiliser des jeux de motifs pour filtrer les URL.

Ensemble d'URL personnalisé. Vous pouvez créer un ensemble d'URL personnalisé contenant jusqu'à 1 000 000 d'entrées d'URL et l'importer sous forme de fichier texte dans votre appliance.

Jeu de motifs. Une appliance ADC peut utiliser des ensembles de modèles pour filtrer les URL avant d'accorder l'accès aux sites Web. Un jeu de motifs est un algorithme de correspondance de chaînes qui recherche une correspondance exacte entre une URL entrante et jusqu'à 5000 entrées. Pour plus d'informations, voir Jeu de motifs.

Chaque URL d'un ensemble d'URL importé peut avoir une catégorie personnalisée sous la forme de métadonnées d'URL. Votre organisation peut héberger l'ensemble et configurer l'appliance ADC pour mettre à jour régulièrement l'ensemble sans intervention manuelle.

Une fois l'ensemble mis à jour, l'appliance NetScaler détecte automatiquement les métadonnées. La catégorie est désormais disponible en tant qu'expression de politique permettant d'évaluer l'URL et d'appliquer une action telle qu'autoriser, bloquer, rediriger ou avertir l'utilisateur.

Expressions de politique avancées utilisées avec les ensembles d'URL

Le tableau suivant décrit les expressions de base que vous pouvez utiliser pour évaluer le trafic entrant.

1. .URLSET_MATCHES_ANY : prend la valeur TRUE si l'URL correspond exactement à n'importe quelle entrée de l'ensemble d'URL.
2. .GET_URLSET_METADATA () - L'expression GET_URLSET_METADATA () renvoie les métadonnées associées si l'URL correspond exactement à n'importe quel modèle de l'ensemble d'URL. Une chaîne vide est renvoyée s'il n'y a pas de correspondance.
3. `.GET_ URLSET_METADATA().EQ(<METADATA)- .GET_ URLSET_METADATA().EQ(<METADATA)`
4. .GET_URLSET_METADATA () .TYPECAST_LIST_T (',') .GET (0) .EQ () : donne la valeur TRUE si les métadonnées correspondantes se trouvent au début de la catégorie. Ce modèle peut être utilisé pour encoder des champs distincts dans les métadonnées, mais correspondre uniquement au premier champ.
5. HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) : joint les paramètres d'hôte et d'URL, qui peuvent ensuite être utilisés pour la mise en correspondance.

Types d'actions du répondeur

> **Remarque :** Dans le tableau, HTTP.REQ.URL est généralisé sous la forme. `<URL expression>`

Le tableau suivant décrit les actions qui peuvent être appliquées au trafic Internet entrant.

Action du répondeur	Description
Allow	Autorisez la demande à accéder à l'URL cible.
Rediriger	Redirigez la demande vers l'URL spécifiée comme cible.
Bloquer	Refusez la demande.

Composants requis

Configurez un serveur DNS si vous importez un ensemble d'URL à partir de l'URL d'un nom d'hôte. Cette configuration n'est pas requise si vous utilisez une adresse IP.

À l'invite de commande, tapez :

```
add dns nameServer ((<IP> [-local])| <dnsVserverName>)[-state (ENABLED |
DISABLED )] [-type <type>] [-dnsProfileName <string>]
```

Exemple :

```
add dns nameServer 10.140.50.5
```

Configuration d'une liste d'URL

Pour configurer une liste d'URL, vous pouvez utiliser l'assistant de proxy de transfert SSL Citrix ou l'interface de ligne de commande (CLI) NetScaler. Sur l'appliance NetScaler, vous devez d'abord configurer la politique du répondeur, puis lier la politique à un ensemble d'URL.

Citrix vous recommande d'utiliser l'assistant de proxy de transfert SSL Citrix comme option préférée pour configurer une liste d'URL. Utilisez l'assistant pour lier une politique de réponse à un ensemble d'URL. Vous pouvez également lier la stratégie à un jeu de motifs.

Configurer une liste d'URL à l'aide de l'assistant de proxy de transfert SSL

Pour configurer la liste d'URL pour le trafic HTTPS à l'aide de l'interface graphique :

1. Accédez à **la page Sécurité** > **Proxy SSL Forward** .
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   a) Cliquez sur **SSL Forward Proxy Wizard**.
   b) Sélectionnez une configuration existante et cliquez sur **Modifier**.
3. Dans la section **Filtrage d'URL**, cliquez sur **Modifier**.
4. Cochez la case **Liste d'URL** pour activer la fonctionnalité.
5. Sélectionnez une politique de **liste d'URL** et cliquez sur **Bind**.
6. Cliquez sur **Continuer**, puis **Terminé**.

Pour plus d'informations, voir Comment créer une stratégie de liste d'URL.

Configurer une liste d'URL à l'aide de l'interface de ligne de commande

Pour configurer une liste d'URL, procédez comme suit.

1. Configurez un serveur virtuel proxy pour le trafic HTTP et HTTPS.
2. Configurez l'interception SSL pour intercepter le trafic HTTPS.
3. Configurez une liste d'URL contenant un ensemble d'URL pour le trafic HTTP.
4. Configurez la liste d'URL contenant les URL définies pour le trafic HTTPS.
5. Configurez un ensemble d'URL privées.

> **Remarque**
>
> Si vous avez déjà configuré une appliance ADC, vous pouvez ignorer les étapes 1 et 2 et procéder à la configuration à l'étape 3.

Configuration d'un serveur virtuel proxy pour le trafic Internet

L'appliance NetScaler prend en charge les serveurs virtuels proxy transparents et explicites. Pour configurer un serveur virtuel proxy pour le trafic Internet en mode explicite, procédez comme suit :

1. Ajoutez un serveur virtuel SSL proxy.
2. Liez une stratégie de répondeur au serveur virtuel proxy.

Pour ajouter un serveur virtuel proxy à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
add cs vserver <name> <serviceType> <IPAddress> <port>
<!--NeedCopy-->
```

Exemple :

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
<!--NeedCopy-->
```

Pour lier une politique de répondeur à un serveur virtuel proxy à l'aide de l'interface de ligne de commande :

```
bind ssl vserver <vServerName> -policyName <string> [-priority <
   positive_integer>]
<!--NeedCopy-->
```

> **Remarque**
>
> Si vous avez déjà configuré l'intercepteur SSL dans le cadre de la configuration de NetScaler, vous pouvez ignorer la procédure suivante.

Configurer l'interception SSL pour le trafic HTTPS

Pour configurer l'interception SSL pour le trafic HTTPS, procédez comme suit :

1. Liez une paire de clés de certificat d'autorité de certification au serveur virtuel proxy.
2. Activez le profil SSL par défaut.
3. Créez un profil SSL frontal, liez-le au serveur virtuel proxy et activez l'interception SSL dans le profil SSL frontal.

Pour lier une paire de clés de certificat CA au serveur virtuel proxy à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
<!--NeedCopy-->
```

Pour configurer un profil SSL frontal à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
set ssl parameter -defaultProfile ENABLED

add ssl profile <name> -sslInterception ENABLED -ssliMaxSessPerServer <
   positive_integer>
<!--NeedCopy-->
```

Pour lier un profil SSL frontal à un serveur virtuel proxy à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl vserver <vServer name>  -sslProfile <name>
<!--NeedCopy-->
```

Configurer une liste d'URL en important un jeu d'URL pour le trafic HTTP

Pour plus d'informations sur la configuration d'un jeu d'URL pour le trafic HTTP, voir Jeu d'URL.

Effectuer une correspondance de sous-domaine explicite

Vous pouvez désormais effectuer une correspondance de sous-domaine explicite pour un ensemble d'URL importé. Un nouveau paramètre, « SubdomainExactMatch », est ajouté à la commande.
`import policy URLset`

Lorsque vous activez le paramètre, l'algorithme de filtrage d'URL effectue une correspondance explicite entre les sous-domaines. Par exemple, si l'URL entrante est `news.example.com` et si l'entrée du jeu d'URL l'est `example.com`, l'algorithme ne correspond pas aux URL.

À l'invite de commande, tapez :
`import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch] [-canaryUrl <URL>]`

Exemple

```
import policy urlset test -url http://10.78.79.80/top-1k.csv -privateSet -
subdomainExactMatch -interval 900
```

Configurer un ensemble d'URL pour le trafic HTTPS

Pour configurer un ensemble d'URL pour le trafic HTTPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
1 add ssl policy <name> -rule <expression> -action <string> [-undefAction
      <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Exemple :

```
1 add ssl policy pol1 -rule "client.ssl.client_hello.SNI.
     URLSET_MATCHES_ANY("top1m") -action INTERCEPT
2 <!--NeedCopy-->
```

Pour configurer une URL définie pour le trafic HTTPS à l'aide de l'assistant de transfert de proxy SSL

Citrix vous recommande d'utiliser l'assistant de proxy de transfert SSL comme option préférée pour configurer une liste d'URL. Utilisez l'assistant pour importer un ensemble d'URL personnalisé et le lier à une politique de réponse.

1. Accédez à **Sécurité > Proxy SSL Forward > Filtrage des URL > Listes d'URL**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Stratégie de liste d'URL**, spécifiez le nom de la stratégie.
4. Sélectionnez une option pour importer un ensemble d'URL.
5. Sur la page de **l'onglet Politique de liste** d'URL, cochez la case **Importer un ensemble d'URL** et spécifiez les paramètres d'ensemble d'URL suivants.
   a) Nom du jeu d'URL : nom du jeu d'URL personnalisé.
   b) URL : adresse Web de l'emplacement auquel accéder au jeu d'URL.
   c) Remplacer (Overwrite) : écrase un jeu d'URL précédemment importé.
   d) Délimiteur : séquence de caractères qui délimite un enregistrement de fichier CSV.
   e) Séparateur de lignes —Séparateur de lignes utilisé dans le fichier CSV.
   f) Intervalle : intervalle en secondes, arrondi au nombre de secondes le plus proche égal à 15 minutes, auquel l'ensemble d'URL est mis à jour.
   g) Jeu privé : option permettant d'empêcher l'exportation du jeu d'URL.
   h) URL Canary : URL interne permettant de vérifier si le contenu de l'ensemble d'URL doit rester confidentiel. La longueur maximale de l'URL est de 2 047 caractères.

6. Sélectionnez une action de répondeur dans la liste déroulante.
7. Cliquez sur **Créer** et **Fermer**.

Configurer un ensemble d'URL privées

Si vous configurez un jeu d'URL privé et que son contenu reste confidentiel, l'administrateur réseau peut ne pas connaître les URL répertoriées sur la liste rouge de l'ensemble. Dans ce cas, vous pouvez configurer une URL Canary et l'ajouter à l'ensemble d'URL. À l'aide de l'URL Canary, l'administrateur peut demander que l'ensemble d'URL privé soit utilisé pour chaque demande de recherche. Vous pouvez vous référer à la section Assistant pour obtenir la description de chaque paramètre.

Pour importer un ensemble d'URL à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
    rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
    ] [-canaryUrl <URL>]
<!--NeedCopy-->
```

Exemple :

```
import policy urlset test1 -url http://10.78.79.80/alytra/top-1k.csv -
    private -canaryUrl http://www.in.gr
<!--NeedCopy-->
```

Afficher le jeu d'URL importé

Vous pouvez désormais afficher les ensembles d'URL importés en plus des ensembles d'URL ajoutés. Un nouveau paramètre « importé » est ajouté à la `show urlset` commande. Si vous activez cette option, l'appliance affiche tous les ensembles d'URL importés et distingue les jeux d'URL importés des ensembles d'URL ajoutés.

À l'invite de commande, tapez :

```
show policy urlset [<name>] [-imported]
```

Exemple

```
show policy urlset -imported
```

Configurer la messagerie du journal d'audit

La journalisation des audits vous permet de passer en revue une condition ou une situation à n'importe quelle phase d'un processus de liste d'URL. Lorsqu'une appliance NetScaler reçoit une URL entrante, si la politique du répondeur comporte une expression de politique avancée URL Set, la

fonctionnalité du journal d'audit collecte les informations relatives à l'ensemble d'URL dans l'URL. Il stocke les détails sous forme de message de journal pour toute cible autorisée par la journalisation des audits.

Le message du journal contient les informations suivantes :

1. Horodatage.
2. Type de message de journal.
3. Les niveaux de journalisation prédéfinis (Critique, Erreur, Notification, Avertissement, Informatif, Débogage, Alerte et Urgence).
4. Informations sur les messages du journal, telles que le nom de l'ensemble d'URL, l'action de politique, l'URL.

Pour configurer la journalisation d'audit pour la fonctionnalité Liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message de journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, consultez la rubrique Audit Logging .

Sémantique des modèles d'URL

August 20, 2021

Le tableau suivant présente les modèles d'URL utilisés pour spécifier la liste des pages que vous souhaitez filtrer. Par exemple, le modèle, www.example.com/bar, ne correspond qu'à une page sur www.example.com/bar. Pour faire correspondre toutes les pages dont l'URL commence par 'www.example.com/bar', vous ajoutez un astérisque (*) à la fin de l'URL.

Sémantique pour le modèle d'URL pour correspondre au mappage des métadonnées

La sémantique de correspondance des motifs est disponible sous forme de tableau. Pour plus d'informations, consultez la page PDF Pattern Semantics .

Mappage des catégories URL

August 20, 2021

Liste des catégories et groupes de catégories de tiers. Pour plus d'informations, consultez la page Mappage des catégories d'URL .

Cas d'utilisation : filtrage d'URL à l'aide d'un jeu d'URL personnalisé

May 5, 2023

Si vous êtes un client d'entreprise qui souhaite contrôler l'accès à des sites Web et à des catégories de sites Web spécifiques, utilisez un ensemble d'URL personnalisé lié à une stratégie de répondeur. L'infrastructure réseau de votre organisation peut utiliser un filtre d'URL pour bloquer l'accès à des sites Web malveillants ou dangereux. Par exemple, les sites Web présentant des adultes, la violence, les jeux, la drogue, la politique ou les portails d'emploi. Outre le filtrage des URL, vous pouvez créer une liste personnalisée d'URL et l'importer dans l'appliance ADC. Par exemple, les stratégies de votre organisation peuvent exiger le blocage de l'accès à certains sites Web tels que les réseaux sociaux, les portails commerciaux et les portails d'emplois.

Chaque URL de la liste peut avoir une catégorie personnalisée sous forme de métadonnées. L'organisation peut héberger la liste des URL sous la forme d'une URL définie sur l'appliance NetScaler. Configurez l'appliance pour mettre à jour périodiquement l'ensemble sans nécessiter d'intervention manuelle.

Une fois l'ensemble mis à jour, l'appliance NetScaler détecte automatiquement les métadonnées. La stratégie de répondeur utilise les métadonnées d'URL (détails de la catégorie) pour évaluer l'URL entrante et appliquer une action telle que permettre, bloquer, rediriger ou notifier l'utilisateur.

Pour ce faire, configurez dans votre réseau, vous pouvez effectuer les tâches suivantes :

1. Importation d'un jeu d'URL personnalisé
2. Ajouter un ensemble d'URL personnalisé
3. Configurez une liste d'URL personnalisée dans l'assistant Proxy de transfert SSL.

Importation d'un ensemble d'URL personnalisé à l'aide de l'interface

À l'invite de commande, tapez :

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
    rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
    ] [-canaryUrl <URL>]

import policy urlset test1  - url http://10.78.79.80/alytra/top-1k.csv
<!--NeedCopy-->
```

Ajouter un ensemble d'URL personnalisé à l'aide de la CLI

À l'invite de commande, tapez :


```
add urlset <urlset_name>
```

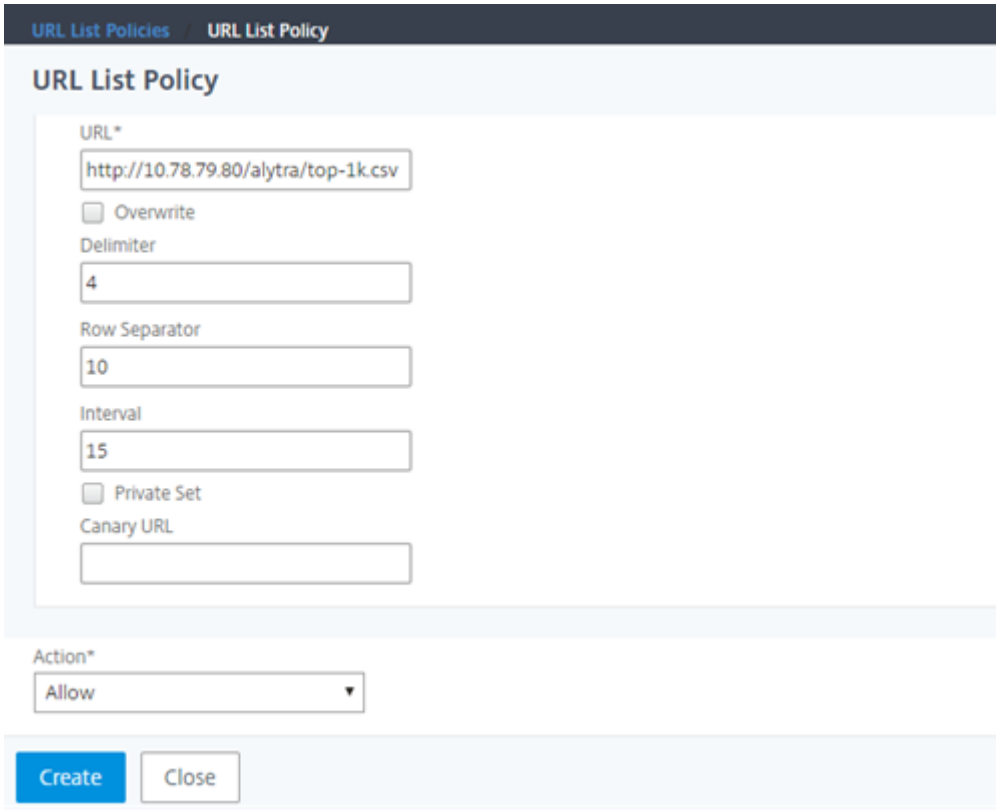
Exemple :

```
add urlset test1
```

Configurer une liste d'URL à l'aide de l'assistant Proxy de transfert SSL

Citrix recommande d'utiliser l'assistant Proxy de transfert SSL comme option préférée pour configurer une liste d'URL. Utilisez l'Assistant pour importer un ensemble d'URL personnalisé et le lier à une stratégie de répondeur.

1. Accédez à **Sécurité > Proxy de transfert SSL > Filtrage d'URL > Listes d'URL**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Stratégie de liste d'URL**, spécifiez le nom de la stratégie.
4. Sélectionnez une option pour importer un jeu d'URL.
5. Dans la page de l'onglet **Stratégie de liste** d' **URL, activez la case à cocher Importer un jeu** d'URL et spécifiez les paramètres de jeu d'URL suivants.
   a) Nom du jeu d'URL : nom du jeu d'URL personnalisé.
   b) URL : adresse Web de l'emplacement auquel accéder au jeu d'URL.
   c) Remplacer (Overwrite) : écrase un jeu d'URL précédemment importé.
   d) Délimiteur : séquence de caractères qui délimite un enregistrement de fichier CSV.
   e) Séparateur de lignes —Séparateur de lignes utilisé dans le fichier CSV.
   f) Intervalle : intervalle en secondes, arrondi aux 15 minutes les plus proches, au cours duquel le jeu d'URL est mis à jour.
   g) Jeu privé : option permettant d'empêcher l'exportation du jeu d'URL.
   h) URL Canary —URL interne permettant de tester si le contenu de l'ensemble d'URL doit rester confidentiel. La longueur maximale de l'URL est de 2 047 caractères.
6. Sélectionnez une action de répondeur dans la liste déroulante.
7. Cliquez sur **Créer** et **Fermer**.



Sémantique des métadonnées pour les ensembles d'URL personnalisés

Pour importer un ensemble d'URL personnalisé, ajoutez les URL à un fichier texte et liez-le à une stratégie de répondeur afin de bloquer les URL de réseaux sociaux.

Voici des exemples d'URL que vous pouvez ajouter au fichier texte :

Actualités, CNN.com

Actualités, BBC.com

Google.com, moteur de recherche

yahoo.com, moteur de recherche

Facebook.com, Réseaux sociaux

twitter.com, Réseaux sociaux

Configurer une stratégie de répondeur pour bloquer les URL des médias sociaux à l'aide de l'interface de ligne de commande

```
1 add responder action act_url_unauthorized respondwith '"HTTP/1.1 451
     Unavailable For Legal Reasons\r\n\r\nURL is NOT authorized\n"'
```



```
2
3 add responder policy pol_url_meta_match 'HTTP.REQ.HOSTNAME.APPEND(HTTP.
     REQ.URL).GET_URLSET_METADATA("u1").EQ("Social Media")'
     act_url_unauthorized
4 <!--NeedCopy-->
```

Catégorisation des URL

May 5, 2023

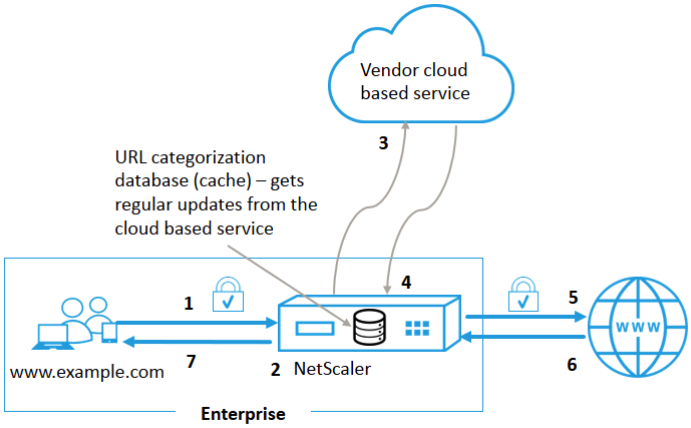
La catégorisation des URL limite l'accès des utilisateurs à des sites Web et à des catégories de sites Web spécifiques. En tant que service abonné en collaboration avec NetSTAR, la fonctionnalité permet aux entreprises clientes de filtrer le trafic Web à l'aide d'une base de données de catégorisation commerciale. La NetSTAR base de données contient un grand nombre (milliards) d'URL classées en différentes catégories, telles que les réseaux sociaux, les jeux de hasard, le contenu pour adultes, les nouveaux médias et les achats. En plus de la catégorisation, chaque URL possède un score de réputation mis à jour en fonction du profil de risque historique du site. Nous pouvons utiliser NetSTAR les données pour filtrer le trafic en configurant des politiques avancées basées sur des catégories, des groupes de catégories (tels que le terrorisme, les drogues illégales) ou des scores de réputation du site.

Par exemple, vous pouvez bloquer l'accès à des sites dangereux, tels que des sites connus pour être infectés par des logiciels malveillants. Vous pouvez également restreindre de manière sélective l'accès à des contenus tels que du contenu pour adultes ou des médias de divertissement en streaming pour les utilisateurs professionnels. Vous pouvez également capturer les détails transactionnels de l'utilisateur et les détails du trafic sortant pour surveiller les analyses du trafic Web sur le serveur NetScaler ADM.

NetScaler charge ou télécharge des données depuis l' NetSTAR appareil préconfiguré nsv10.netstar-inc.com et incompasshybridpc.netstar-inc.com est utilisé comme hôte cloud par défaut pour les demandes de catégorisation dans le cloud. Ces URL doivent être accessibles via le pare-feu pour que le filtrage des URL fonctionne correctement. L'appliance utilise son adresse NSIP comme adresse IP source et 443 comme port de destination pour la communication.

Fonctionnement de la catégorisation des URL

La figure suivante montre comment un service de catégorisation d'URL NetScaler est intégré à une base de données commerciale de catégorisation d'URL et à des services cloud pour des mises à jour fréquentes.



Les composants interagissent comme suit :

1. Un client envoie une demande d'URL liée à Internet.
2. Le proxy de transfert SSL applique une stratégie à la demande en fonction des détails de la catégorie, tels que la catégorie, le groupe de catégories et le score de réputation du site. Les détails des catégories sont extraits de la base de données de catégorisation d'URL. Si la base de données renvoie les détails de la catégorie, le processus passe à l'étape 5.
3. Si la base de données manque les détails de catégorisation, la demande est envoyée à un service de recherche basé sur le cloud géré par un fournisseur de catégorisation d'URL. Toutefois, l'appliance n'attend pas de réponse. Au lieu de cela, l'URL est marquée comme non classée et une application de stratégie est effectuée (passez à l'étape 5). L'appliance continue de surveiller les commentaires des requêtes dans le cloud et met à jour le cache afin que les futures demandes puissent bénéficier de la recherche dans le cloud.
4. L'appliance ADC reçoit les détails de la catégorie d'URL (catégorie, groupe de catégories et score de réputation) du service basé sur le cloud et les stocke dans la base de données de catégorisation.
5. La stratégie autorise l'URL et la demande est envoyée au serveur d'origine. Sinon, l'appliance supprime, redirige ou répond par une page HTML personnalisée.
6. Le serveur d'origine répond avec les données demandées à l'appliance ADC.
7. L'appliance envoie la réponse au client.

Cas d'utilisation : utilisation d'Internet dans le cadre de la conformité des entreprises

Vous pouvez utiliser la fonctionnalité de filtrage d'URL pour détecter et mettre en œuvre des stratégies de conformité afin de bloquer les sites qui enfreignent la conformité de l'entreprise. Par exemple, des sites tels que des sites pour adultes, des médias en streaming, des réseaux sociaux qui peuvent être considérés comme non productifs ou qui consomment trop de bande passante Internet dans un

réseau d'entreprise. Le blocage de l'accès à ces sites Web peut améliorer la productivité des employés, réduire les coûts d'exploitation liés à l'utilisation de la bande passante et réduire les frais généraux liés à la consommation réseau.

Composants requis

La fonctionnalité de catégorisation des URL ne fonctionne sur une plate-forme NetScaler que si elle dispose d'un service d'abonnement optionnel avec des fonctionnalités de filtrage des URL et des informations sur les menaces pour le proxy SSL Forward. L'abonnement permet aux clients de télécharger les dernières catégorisations de menaces pour les sites Web, puis d'appliquer ces catégories au proxy direct SSL. Avant d'activer et de configurer la fonctionnalité, vous devez installer les licences suivantes :

- `CNS_WEBF_SSERVER_Retail.lic`
- `CNS_XXXX_SERVER_PLT_Retail.lic`

Où, XXXXX est le type de plate-forme, par exemple : V25000

Expressions de stratégie du répondeur

Le tableau suivant répertorie les différentes expressions de stratégie que vous pouvez utiliser pour vérifier si une URL entrante doit être autorisée, redirigée ou bloquée.

1. `<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)` - Renvoie un objet URL_CATEGORY. Si `<min_reputation>` est supérieur à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est inférieure à `<min_reputation>`. Si `<max_reputation>` est supérieur à 0, l'objet renvoyé ne contient pas de catégorie dont la réputation est supérieure à `<max_reputation>`. Si la catégorie ne parvient pas à résoudre en temps opportun, la valeur undef est renvoyée.
2. `<url_category>. CATEGORY()` - Retourne la chaîne de catégorie de cet objet. Si l'URL ne comporte pas de catégorie ou si l'URL est mal formée, la valeur renvoyée est « Inconnu ».
3. `<url_category>. CATEGORY_GROUP()` - Retourne une chaîne identifiant le groupe de catégories de l'objet. Ce regroupement est un regroupement de catégories de niveau supérieur, ce qui est utile dans les opérations nécessitant des informations moins détaillées sur la catégorie d'URL. Si l'URL ne comporte pas de catégorie ou si l'URL est mal formée, la valeur renvoyée est « Inconnu ».
4. `<url_category>. REPUTATION()` - Retourne le score de réputation sous la forme d'un nombre compris entre 0 et 5, où 5 indique la réputation la plus risquée. S'il existe la catégorie « Inconnu », la valeur de réputation est 1.

Types de stratégie :

1. Stratégie de sélection des demandes d'URL appartenant à la catégorie Moteur de recherche - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ( "Search Engine" )`
2. Politique de sélection des demandes d'URL appartenant au groupe de catégorie Adulte - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY_GROUP().EQ( "Adult" )'`
3. Politique de sélection des demandes pour les URL des moteurs de recherche dont le score de réputation est inférieur à 4 - `add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY( "Search Engine" )`
4. Politique de sélection des demandes pour les moteurs de recherche et les URL d'achat - `add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ ( "good_categories" )`
5. Politique de sélection des demandes pour les URL des moteurs de recherche dont le score de réputation est égal ou supérieur à 4 - `add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0). CATEGORY().EQ( "Search Engines" )`
6. Stratégie pour sélectionner les demandes d'URL qui se trouvent dans la catégorie Moteur de recherche et les comparer à un jeu d'URL - `'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ( "Search Engine" )&& HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY( "u1" )'`

Types de stratégie du répondeur

Il existe deux types de stratégies utilisées dans une fonctionnalité de catégorisation d'URL et chacun de ces types de stratégie est expliqué dans le tableau suivant :

Type de stratégie	Description
URL Category	Classez le trafic Web en fonction des résultats de l'évaluation qui bloque, autorise ou redirige le trafic.
Score de réputation d'URL	Détermine le score de réputation du site Web et vous permet de contrôler l'accès en fonction du seuil de score de réputation défini par l'administrateur.

Configurer la catégorisation d'URL

Pour configurer la catégorisation des URL sur une appliance NetScaler, procédez comme suit :

1. Activer le filtrage des URL.

2. Configurez un serveur proxy pour le trafic Web.
3. Configurez l'interception SSL pour le trafic Web en mode explicite.
4. Configurez la mémoire partagée pour limiter la mémoire cache.
5. Configurez les paramètres de catégorisation d'URL.
6. Configurez la catégorisation d'URL à l'aide de l'assistant de proxy de transfert SSL Citrix.
7. Configurez les paramètres de catégorisation d'URL à l'aide de l'assistant de proxy de transfert SSL.
8. Configurer le chemin de la base de données initiale et le nom du serveur de cloud

Étape 1 : Activation du filtrage des URL

Pour activer la catégorisation d'URL, activez la fonction de filtrage d'URL et activez les modes de catégorisation d'URL.

Pour activer la catégorisation d'URL à l'aide de la CLI

À l'invite de commande, tapez :

```
enable ns feature URLFiltering
```

```
disable ns feature URLFiltering
```

Étape 2 : Configurer un serveur proxy pour le trafic Web en mode explicite

L'appliance NetScaler prend en charge les serveurs virtuels proxy transparents et explicites. Pour configurer un serveur virtuel proxy pour le trafic SSL en mode explicite, procédez comme suit :

1. Ajoutez un serveur proxy.
2. Liez une stratégie SSL au serveur proxy.

Pour ajouter un serveur proxy à l'aide de la CLI

À l'invite de commande, tapez :

```
add cs vserver <name> [-td <positive_integer>] <serviceType> [-cltTimeout <
secs>]
```

Exemple :

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
```

Lier une stratégie SSL à un serveur virtuel proxy à l'aide de l'interface de ligne de commande

```
bind ssl vserver <vServerName> -policyName <string> [-priority <positive_integer
>]
```


Étape 3 : Configurer l'interception SSL pour le trafic HTTPS

Pour configurer l'interception SSL pour le trafic HTTPS, procédez comme suit :

1. Liez une paire de clés de certificat d'autorité de certification au serveur virtuel proxy.
2. Configurez le profil SSL par défaut avec des paramètres SSL.
3. Liez un profil SSL frontal au serveur virtuel proxy et activez l'interception SSL dans le profil SSL frontal.

Pour lier une paire de clés de certificat d'autorité de certification au serveur virtuel proxy à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -CA -
skipCAName
```

Pour configurer le profil SSL par défaut à l'aide de la CLI

À l'invite de commande, tapez :

```
set ssl profile <name> -denySSLReneg <denySSLReneg> -sslInterception (
ENABLED | DISABLED)-ssliMaxSessPerServer positive_integer>
```

Lier un profil SSL frontal à un serveur virtuel proxy à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ssl vserver <vServer name> -sslProfile ssl_profile_interception
```

Étape 4 : Configurer la mémoire partagée pour limiter la mémoire cache

Pour configurer la mémoire partagée afin de limiter la mémoire cache à l'aide de la CLI

À l'invite de commande, tapez :

```
set cache parameter [-memLimit <megaBytes>]
```

Où, la limite de mémoire configurée pour la mise en cache est définie sur 10 Mo.

Étape 5 : Configurer les paramètres de catégorisation d'URL

Pour configurer les paramètres de catégorisation d'URL à l'aide de la CLI

À l'invite de commande, tapez :

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-
TimeOfDayToUpdateDB <HH:MM>]
```


Exemple :

```
set urlfiltering parameter -urlfilt_hours_betweenDB_updates 20
```

Étape 6 : Configurer la catégorisation d'URL à l'aide de l'assistant de proxy de transfert SSL Citrix

1. Connectez-vous à l'appliance NetScaler et accédez à la page **Security** > **SSL Forward Proxy** .
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   a) Cliquez sur **Assistant Proxy de transfert SSL** pour créer une nouvelle configuration.
   b) Sélectionnez une configuration existante et cliquez sur **Modifier**.
3. Dans la section **Filtrage d'URL**, cliquez sur **Modifier**.
4. Cochez la case **Catégorisation d'URL** pour activer la fonctionnalité.
5. Sélectionnez une stratégie de **catégorisation d'URL** et cliquez sur **Lier**.
6. Cliquez sur **Continuer**, puis **Terminé**.

Pour plus d'informations sur la stratégie de catégorisation d'URL, voir Comment créer une stratégie de catégorisation d'URL.

Étape 7 : Configuration des paramètres de catégorisation d'URL à l'aide d'un Assistant Proxy de transfert SSL

1. Connectez-vous à l'appliance **NetScaler** et accédez à **Sécurité > Filtrage des URL**.
2. Sur la page **Filtrage d'URL**, cliquez sur **le lien Modifier les paramètres de filtrage d'URL** .
3. Dans la page **Configuration des paramètres de filtrage d'URL**, spécifiez les paramètres suivants.
   a) Heures entre les mises à jour des bases Heures de filtrage d'URL entre les mises à jour de Valeur minimale : 0 et valeur maximale : 720.
   b) Heure de mise à jour de la base de données. Heure de la journée de filtrage d'URL pour mettre à jour la base
   c) Hôte Cloud. Le chemin d'accès URL du serveur cloud.
   d) Chemin de base de données Seed Chemin d'accès URL du serveur de recherche de base de données de départ.
4. Cliquez sur **OK** et sur **Fermer**.

Exemple de configuration :

```
1 enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering
2
3 enable ns mode FR L3 Edge USNIP PMTUD
4
5 set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
      -sslInterception ENABLED -ssliMaxSessPerServer 100
```



```
6
7  add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key
8
9  set cache parameter -memLimit 100
10
11 add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
12
13 add responder action act1 respondwith ""HTTP/1.1 200 OK\r\n\r\n" + http
       .req.url.url_categorize(0,0).reputation + "\n""
14
15 add responder policy p1 "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
       Shopping/Retail") || HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
       Search Engines & Portals
16
17 ")" act1
18
19 bind cs vserver starcs_PROXY -policyName p1 -priority 10 -
       gotoPriorityExpression END -type REQUEST
20
21 add dns nameServer 10.140.50.5
22
23 set ssl parameter -denySSLReneg NONSECURE -defaultProfile ENABLED -
       sigDigestType RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-
       SHA512 -ssliErrorCache ENABLED
24
25 -ssliMaxErrorCacheMem 100000000
26
27 add ssl policy pol1 -rule "client.ssl.origin_server_cert.subject.
       URL_CATEGORIZE(0,0).CATEGORY.eq("Search Engines & Portals")"" -
       action INTERCEPT
28
29 add ssl policy pol3 -rule "client.ssl.origin_server_cert.subject.ne("
       citrix")" -action INTERCEPT
30
31 add ssl policy swg_pol -rule "client.ssl.client_hello.SNI.
       URL_CATEGORIZE(0,0).CATEGORY.ne("Uncategorized")" -action INTERCEPT
32
33 set urlfiltering parameter -HoursBetweenDBUpdates 3 -
       TimeOfDayToUpdateDB 03:00
34 <!--NeedCopy-->
```


Configurer le chemin de la base de données initiale et le nom du serveur de cloud

Vous pouvez désormais configurer le chemin de la base de données de départ et le nom du serveur de recherche cloud pour le réglage manuel du nom du serveur de recherche cloud et du chemin de la base de données de départ Pour ce faire, deux nouveaux paramètres, « CloudHost » et « SeedDbPath », sont ajoutés au paramètre de filtrage d'URL.

À l'invite de commande, tapez :

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-
TimeOfDayToUpdateDB <HH:MM>] [-LocalDatabaseThreads <positive_integer>] [-
CloudHost <string>] [-SeedDBPath <string>]
```

Exemple :

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00 -CloudHost localhost -SeedDBPath /mypath
```

La communication entre une appliance NetScaler et NetSTAR peut nécessiter un serveur de noms de domaine. Vous pouvez tester à l'aide d'une simple console ou d'une connexion Telnet à partir de l'appliance.

Exemple :

```
root@ns# telnet nsv10.netstar-inc.com 443
Trying 1.1.1.1...
Connected to nsv10.netstar-inc.com.
Escape character is '^]'.

root@ns# telnet incompasshybridpc.netstar-inc.com 443
Trying 10.10.10.10...
Connected to incompasshybridpc.netstar-inc.com.
Escape character is '^]'.
<!--NeedCopy-->
```

Configurer la messagerie du journal d'audit

La journalisation d'audit vous permet de passer en revue une condition ou une situation dans n'importe quelle phase du processus de catégorisation d'URL. Lorsqu'une appliance NetScaler reçoit une URL entrante, si la politique du répondeur comporte une expression de filtrage d'URL, la fonctionnalité du journal d'audit collecte les informations relatives aux ensembles d'URL dans l'URL. Il stocke les informations sous forme de messages de journal pour toute cible autorisée par la journalisation d'audit.

- Adresse IP source (adresse IP du client qui a fait la demande).

- Adresse IP de destination (adresse IP du serveur demandé).
- URL demandée contenant le schéma, l'hôte et le nom de domaine (http://www.example.com).
- Catégorie d'URL renvoyée par le cadre de filtrage d'URL.
- Groupe de catégories d'URL renvoyé par le cadre de filtrage d'URL.
- Numéro de réputation d'URL renvoyé par le cadre de filtrage d'URL.
- Action du journal d'audit effectuée par la stratégie.

Pour configurer la journalisation d'audit pour une fonctionnalité de liste d'URL, vous devez effectuer les tâches suivantes :

1. Activer le journal d'audit :
2. Action Créer un message de journal d'audit.
3. Définissez la stratégie de répondeur de liste d'URL avec l'action de message Journal d'audit.

Pour plus d'informations, consultez la rubrique Audit Logging .

Stockage des erreurs d'échec à l'aide de la messagerie SYSLOG

À n'importe quel stade du processus de filtrage d'URL, en cas de défaillance au niveau du système, l'appliance ADC utilise le mécanisme du journal d'audit pour stocker les journaux dans le fichier ns.log. Les erreurs sont stockées sous forme de messages texte au format SYSLOG afin qu'un administrateur puisse les consulter ultérieurement dans un ordre chronologique d'occurrence des événements. Ces journaux sont également envoyés à un serveur SYSLOG externe pour archivage. Pour plus d'informations, consultez l'article CTX229399.

Par exemple, si un échec se produit lorsque vous initialisez le SDK de filtrage d'URL, le message d'erreur est stocké dans le format de messagerie suivant.

```
Oct 3 15:43:40 <local0.err> ns URLFiltering[1349]: Error initializing
NetStar SDK (SDK error=-1). (status=1).
```

L'appliance NetScaler stocke les messages d'erreur dans quatre catégories d'échec différentes :

- **Échec du téléchargement**. Si une erreur se produit lorsque vous tentez de télécharger la base de données de catégorisation.
- **échec de l'intégration**. Si une erreur se produit lors de l'intégration d'une mise à jour dans la base de données de catégorisation existante.
- **Échec d'initialisation**. Si une erreur se produit lorsque vous initialisez la fonctionnalité de catégorisation d'URL, définissez des paramètres de catégorisation ou mettez fin à un service de catégorisation.
- **Échec de récupération**. Si une erreur se produit lorsque l'appliance récupère les détails de catégorisation de la demande.

Configurer des interruptions SNMP pour les événements NetStar

La fonction de filtrage d'URL génère des interruptions SNMP si les conditions suivantes se produisent :

- La mise à jour de base de données NetStar échoue ou réussit.
- L'initialisation du SDK NetStar échoue ou réussit.

L'appliance possède un ensemble d'entités conditionnelles appelées alarmes SNMP. Lorsqu'une condition de l'alarme SNMP est remplie, l'appliance génère des interruptions et les envoie à une destination d'interruption spécifiée. Par exemple, si l'initialisation du SDK NetStar échoue, un OID SNMP 1.3.6.1.4.1.5951.1.1.0.183 est généré et envoyé à la destination d'interruption.

Pour que l'appliance génère des interruptions, vous devez d'abord activer et configurer les alarmes SNMP. Ensuite, vous spécifiez la destination d'interruption à laquelle l'appliance envoie les messages d'interruption générés.

Activer une alarme SNMP

L'appliance NetScaler génère des interruptions uniquement pour les alarmes SNMP activées. Certaines alarmes sont activées par défaut, mais vous pouvez les désactiver.

Lorsque vous activez une alarme SNMP, la fonction de filtrage d'URL génère des messages d'interruption lorsqu'un événement de réussite ou d'échec se produit. Certaines alarmes sont activées par défaut.

Pour activer une alarme SNMP à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
enable snmp alarm <trapName>
show snmp alarm <trapName>
```

Pour activer une alarme SNMP à l'aide de l'interface graphique NetScaler

1. Accédez à **Système** > **SNMP** > **Alarmes**, puis sélectionnez l'alarme.
2. Cliquez sur **Actions** et sélectionnez **Activer**.

Configurer l'alarme SNMP à l'aide du CLI

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue
 <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Exemple :


```
set snmp alarm URL-FIL-DB-UPDATE-STATUS -state ENABLED
set snmp alarm URL-FIL-INIT-SDK -state ENABLED
```

Configurer les alarmes SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Alarmes**, sélectionnez une alarme et configurez les paramètres de l'alarme.

Pour plus d'informations sur les interruptions SNMP, consultez la rubrique SNMP

Score de réputation d'URL

October 5, 2021

La fonction de catégorisation d'URL fournit un contrôle basé sur des stratégies pour restreindre les URL sur la liste rouge. Vous pouvez contrôler l'accès aux sites Web en fonction de la catégorie d'URL, du score de réputation ou de la catégorie d'URL et du score de réputation. Si les administrateurs réseau surveillent un utilisateur accédant à des sites Web à haut risque, ils peuvent utiliser une stratégie de répondeur liée au score de réputation d'URL pour bloquer ces sites Web à risque.

À la réception d'une demande d'URL entrante, la solution matérielle-logicielle récupère la catégorie et le score de réputation dans la base de données de catégorisation des URL. En fonction du score de réputation renvoyé par la base de données, la solution matérielle-logicielle attribue une note de réputation aux sites Web. La valeur peut aller de 1 à 4, 4 étant le type de site Web le plus risqué, comme indiqué dans le tableau suivant.

Évaluation de la réputation des URL	Commentaire de réputation
1	Site propre
2	Site inconnu
3	Potentiellement dangereux ou affilié à un site dangereux
4	Site malveillant

Cas d'utilisation : filtrage par score de réputation d'URL

Imaginez une organisation d'entreprise avec un administrateur réseau qui surveille les transactions des utilisateurs et la consommation de bande passante réseau. Si des logiciels malveillants peuvent pénétrer sur le réseau, l'administrateur doit améliorer la sécurité des données et contrôler l'accès aux sites Web malveillants et dangereux accédant au réseau. Pour protéger le réseau contre de telles

menaces, l'administrateur peut configurer la fonctionnalité de filtrage d'URL pour autoriser ou refuser l'accès par score de réputation d'URL.

Pour plus d'informations sur la surveillance du trafic sortant et des activités des utilisateurs sur le réseau, consultez Analytics.

Si un employé de l'organisation tente d'accéder à un site Web de réseau social, l'appliance ADC reçoit une demande d'URL. Il interroge la base de données de catégorisation d'URL pour récupérer la catégorie d'URL en tant que réseau social et un score de réputation 3, qui indique un site Web potentiellement dangereux. La solution matérielle-logicielle vérifie ensuite la stratégie de sécurité configurée par l'administrateur, par exemple en bloquant l'accès aux sites ayant une cote de réputation de 3 ou plus. Il applique ensuite l'action de stratégie pour contrôler l'accès au site Web.

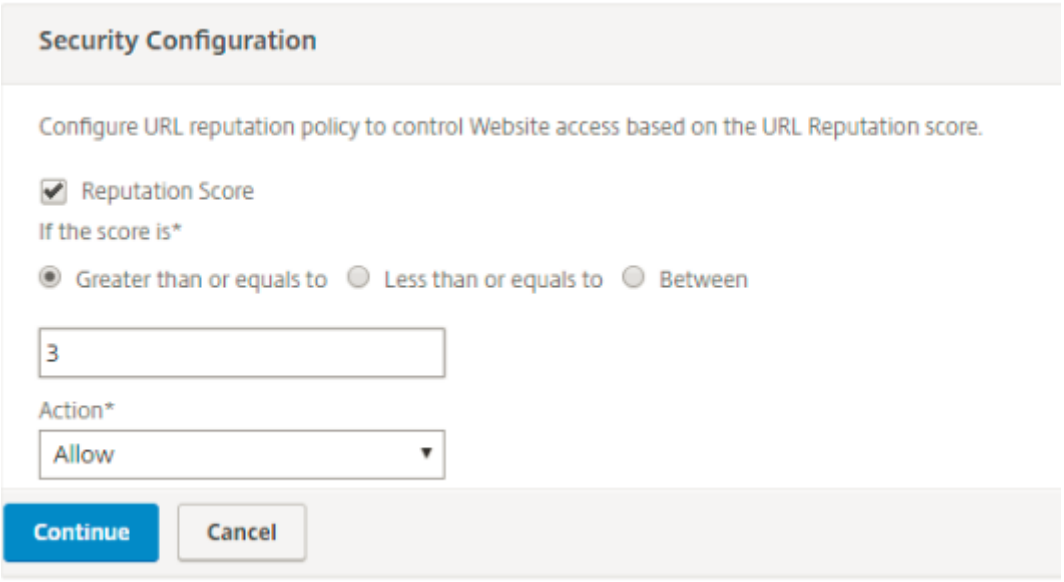
Pour implémenter cette fonctionnalité, vous devez configurer le score de réputation d'URL et les niveaux de seuil de sécurité à l'aide de l'assistant Proxy de transfert SSL.

Configurer le score de réputation à l'aide de l'interface graphique

Citrix vous recommande d'utiliser l'assistant de transfert de proxy SSL pour configurer le score de réputation et les niveaux de sécurité. En fonction du seuil configuré, vous pouvez sélectionner une action de stratégie pour autoriser, bloquer ou rediriger le trafic.

1. Accédez à **Sécurité** > **Proxy SSL Forward**.
2. Dans le volet d'informations, cliquez sur **SSL Forward Proxy Wizard**.
3. Dans la page de détails, spécifiez les paramètres du serveur proxy.
4. Cliquez sur **Continuer** pour spécifier d'autres paramètres tels que l'interception SSL et l'identification de la gestion.
5. Cliquez sur **Continuer** pour accéder à la section **Configuration de la sécurité** .
6. Dans la section **Configuration de la sécurité**, cochez la case **Score de réputation** pour contrôler l'accès en fonction du score de réputation d'URL.
7. Sélectionnez le niveau de sécurité et spécifiez la valeur de seuil du score de réputation :
    a) Supérieur ou égal à : autorise ou bloque un site Web si la valeur de seuil est supérieure ou égale à N, où N est compris entre un et quatre.
    b) Inférieur ou égal à : autorise ou bloque un site Web si la valeur de seuil est inférieure ou égale à N, où N est compris entre un et quatre.
    c) Entre : autorise ou bloque un site Web si la valeur de seuil est comprise entre N1 et N2 et que la plage est comprise entre un et quatre.
8. Sélectionnez une action de répondeur dans la liste déroulante.
9. Cliquez sur **Continuer** et **fermer**.

L'image suivante montre la section **Configuration de la sécurité** de l'assistant Proxy de transfert SSL. Activez l'option Score de réputation d'URL pour configurer les paramètres de stratégie.



Analyse

May 5, 2023

Dans l'appliance NetScaler, tous les enregistrements utilisateur et les enregistrements suivants sont enregistrés. Lorsque vous intégrez NetScaler Application Delivery Management (ADM) à l'appliance NetScaler, l'activité utilisateur enregistrée et les enregistrements suivants dans l'appliance sont exportés vers NetScaler ADM à l'aide de cette fonctionnalité. `logstream`

NetScaler ADM rassemble et présente des informations sur les activités des utilisateurs, telles que les sites Web visités et la bande passante dépensée. Il signale également l'utilisation de la bande passante et les menaces détectées, telles que les logiciels malveillants et les sites de phishing. Vous pouvez utiliser ces mesures clés pour surveiller votre réseau et prendre des mesures correctives avec l'appliance Citrix SWG. Pour plus d'informations, consultez Citrix SSL Forward Proxy Analytics.

Pour intégrer l'appliance NetScaler à NetScaler ADM :

1. Dans l'appliance NetScaler, lors de la configuration de la fonctionnalité de proxy de transfert SSL, activez Analytics et fournissez les détails de l'instance NetScaler ADM que vous souhaitez utiliser pour les analyses.
2. Dans NetScaler ADM, ajoutez l'appliance NetScaler en tant qu'instance à NetScaler ADM. Pour plus d'informations, voir Ajouter des instances à NetScalerADM.

Cas d'utilisation : sécurisation d'un réseau d'entreprise à l'aide du protocole ICAP pour l'inspection à distance des programmes malveillants

May 5, 2023

L'appliance NetScaler agit comme un proxy et intercepte tout le trafic client. L'appliance utilise des politiques pour évaluer le trafic et transmet les demandes des clients au serveur d'origine sur lequel réside la ressource. L'appliance déchiffre la réponse du serveur d'origine et transmet le contenu en texte brut au serveur ICAP pour une vérification antimalware. Le serveur ICAP répond par un message indiquant « Aucune adaptation requise », une erreur ou une demande modifiée. En fonction de la réponse du serveur ICAP, le contenu demandé est soit transféré au client, soit un message approprié est envoyé.

Pour ce cas d'utilisation, vous devez effectuer une configuration générale, une configuration liée au proxy et à l'interception SSL, ainsi qu'une configuration ICAP sur l'appliance NetScaler.

Configuration générale

Configurez les entités suivantes :

- Adresse NSIP
- Adresse IP du sous-réseau (SNIP)
- Serveur de noms DNS
- Paire de clés de certificat CA pour signer le certificat du serveur pour l'interception SSL

Configuration du serveur proxy et de l'interception SSL

Configurez les entités suivantes :

- Serveur proxy en mode explicite pour intercepter tout le trafic HTTP et HTTPS sortant.
- Profil SSL pour définir les paramètres SSL, tels que les chiffrements et les paramètres, pour les connexions.
- Politique SSL pour définir des règles d'interception du trafic. Définissez cette valeur sur true pour intercepter toutes les demandes des clients.

Pour plus de détails, consultez les rubriques suivantes :

- Modes proxy
- Interception SSL

Dans l'exemple de configuration suivant, le service de détection des programmes malveillants se trouve à `www.example.com`l'adresse.

Exemple de configuration générale :

```
add dns nameServer 203.0.113.2

add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key ns_swg_ca.key
<!--NeedCopy-->
```

Exemple de configuration du serveur proxy et de l'interception SSL :

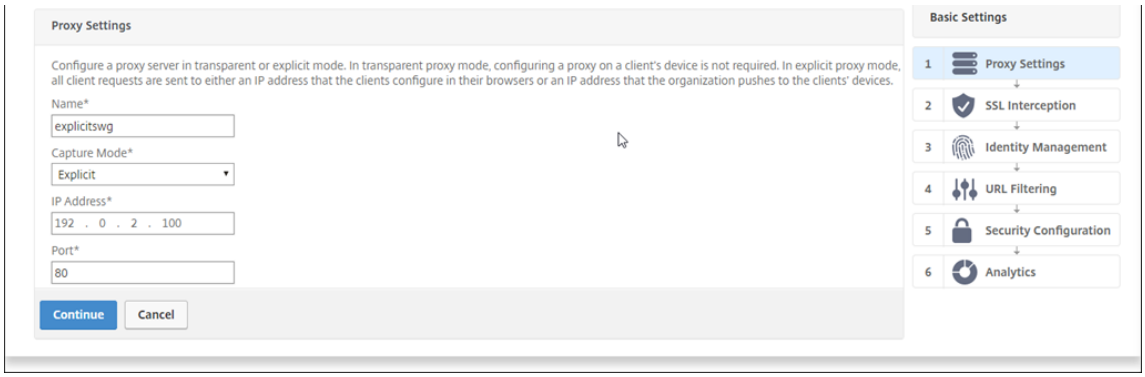
```
add cs vserver explicitswg PROXY 192.0.2.100 80 -Authn401 ENABLED -authnVsName explicit-auth-vs

set ssl parameter -defaultProfile ENABLED

add ssl profile swg_profile -sslInterception ENABLED

bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey

set ssl vserver explicitswg -sslProfile swg_profile

add ssl policy ssli-pol_ssli -rule true -action INTERCEPT

bind ssl vserver explicitswg -policyName ssli-pol_ssli -priority 100 -type INTERCEPT_REQ
<!--NeedCopy-->
```

Exemple de configuration ICAP :

```
add service icap_svc 203.0.113.225 TCP 1344

enable ns feature contentinspection

add icapprofile icapprofile1 -uri /example.com -Mode RESMOD

add contentInspection action CiRemoteAction -type ICAP -serverName icap_svc -icapProfileName icapprofile1

add contentInspection policy CiPolicy -rule "HTTP.REQ.METHOD.NE("CONNECT")" -action CiRemoteAction

bind cs vserver explicitswg -policyName  CiPolicy -priority 200 -type response
<!--NeedCopy-->
```


Configurer les paramètres du proxy

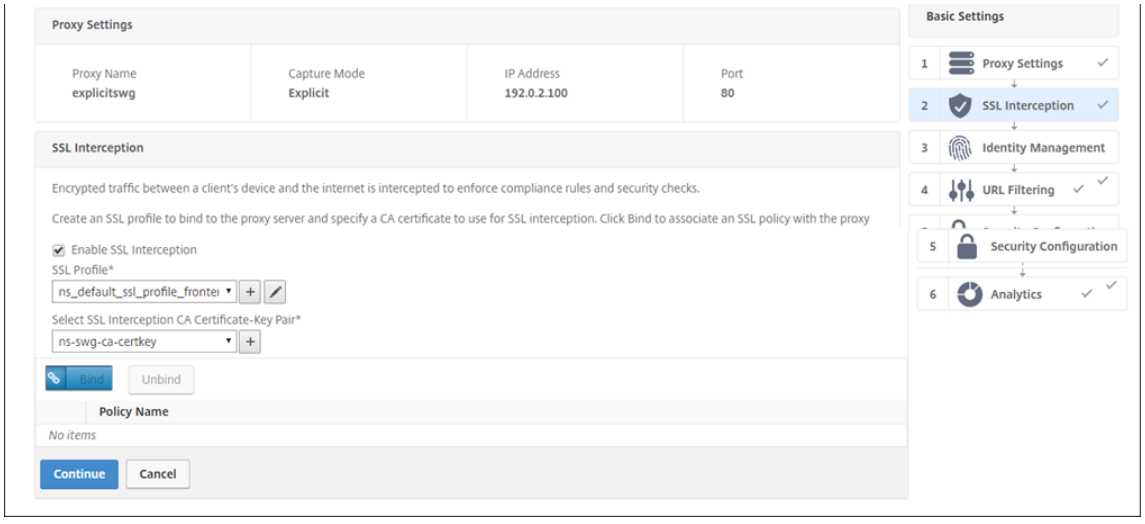
1. Accédez à **Sécurité** > **Proxy de transfert SSL> Assistant de transfert de proxy**SSL.
2. Cliquez sur **Commencer**, puis cliquez sur **Continuer**.
3. Dans la boîte de dialogue **Paramètres du proxy**, saisissez un nom pour le serveur proxy explicite.
4. Pour le **mode Capture,** sélectionnez **Explicit**.
5. Entrez une adresse IP et un numéro de port.



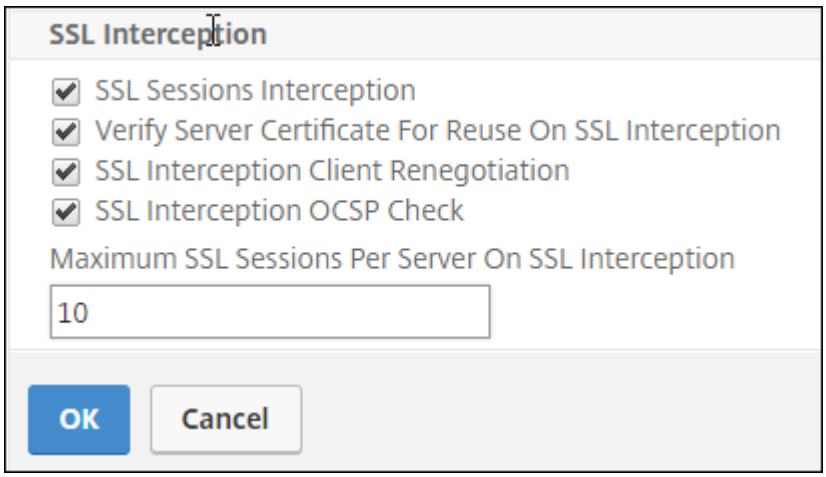
6. Cliquez sur **Continuer**.

Configurez les paramètres d'interception SSL

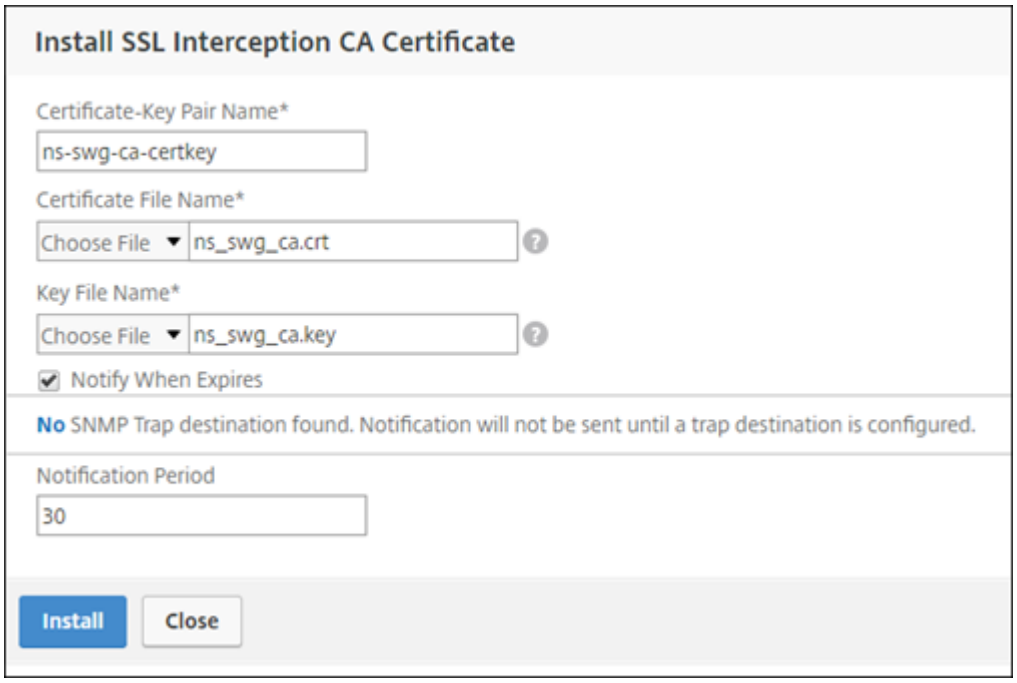
1. Sélectionnez **Activer l'interception SSL**.



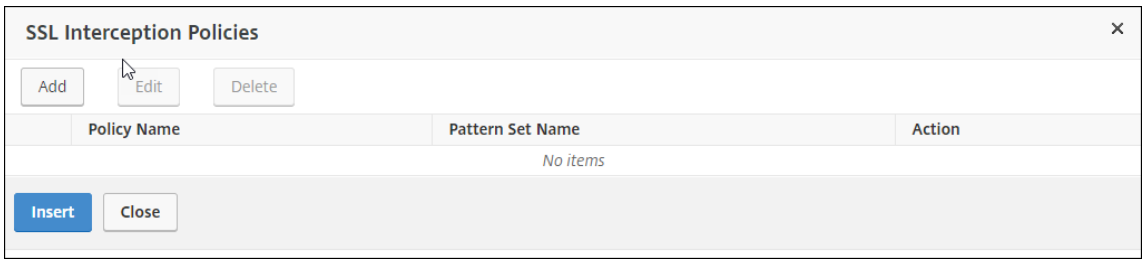
2. Dans **Profil SSL**, sélectionnez un profil existant ou cliquez sur « + » pour ajouter un nouveau profil SSL frontal. Activez l' **interception des sessions SSL** dans ce profil. Si vous sélectionnez un profil existant, passez à l'étape suivante.



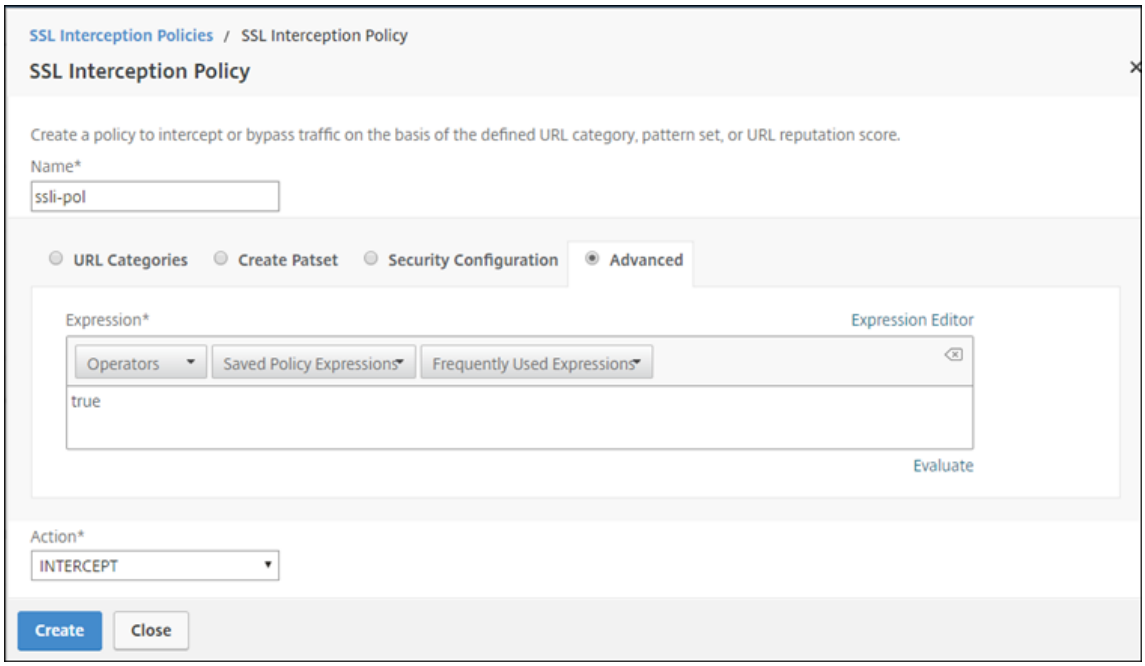
3. Cliquez sur **OK**, puis sur **Terminé**.
4. Dans **Sélectionner une paire de clés de certificat CA d'interception SSL**, sélectionnez un certificat existant ou cliquez sur « + » pour installer une paire de clés de certificat CA pour l'interception SSL. Si vous sélectionnez un certificat existant, passez à l'étape suivante.



5. Cliquez sur **Installer**, puis sur **Fermer**.
6. Ajoutez une stratégie pour intercepter tout le trafic. Cliquez sur **Bind**. Cliquez sur **Ajouter** pour ajouter une nouvelle politique ou sélectionnez une politique existante. Si vous sélectionnez une politique existante, cliquez sur **Insérer**et ignorez les trois étapes suivantes.



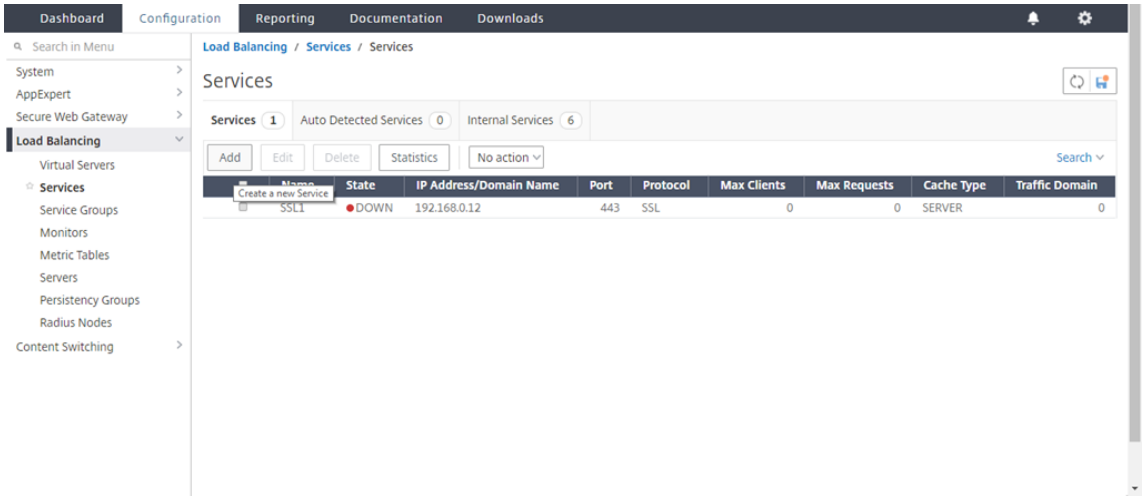
7. Entrez le nom de la stratégie et sélectionnez **Avancé**. Dans l'éditeur d'expressions, saisissez true.
8. Pour **Action**, sélectionnez **INTERCEPTER**.



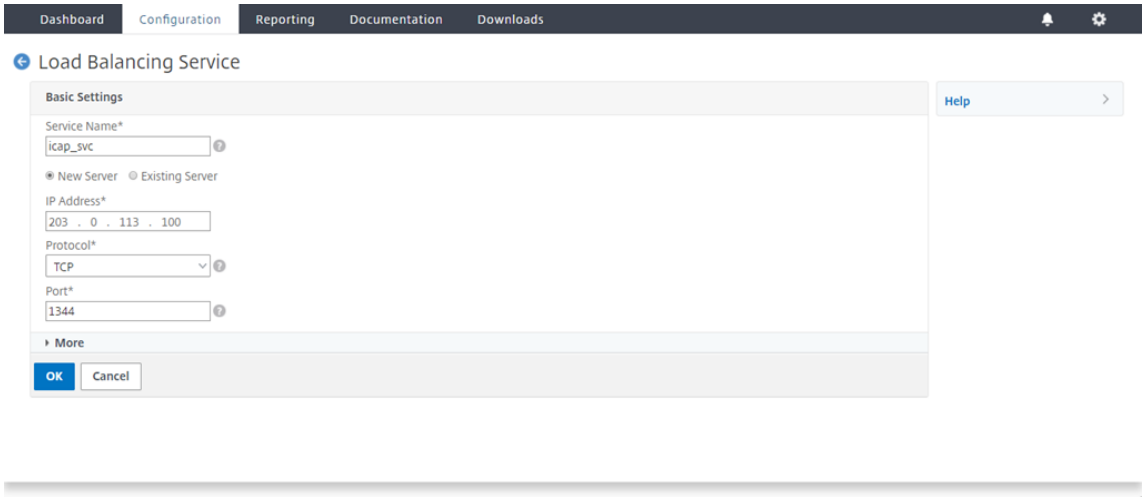
9. Cliquez sur **Create**.
10. Cliquez quatre fois sur **Continuer**, puis sur **OK**.

Configuration des paramètres ICAP

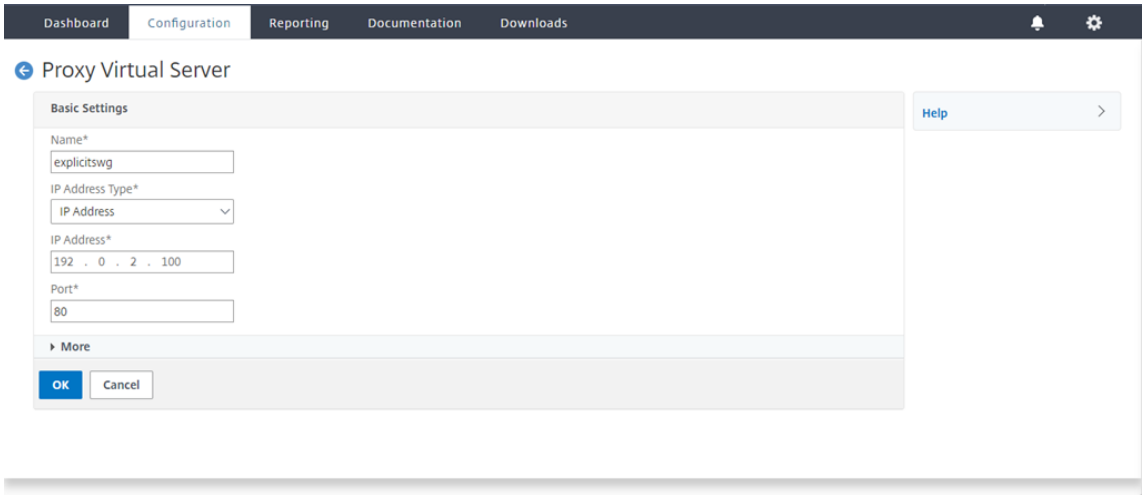
1. Accédez à **Équilibrage de charge** > **Services** et cliquez sur **Ajouter**.



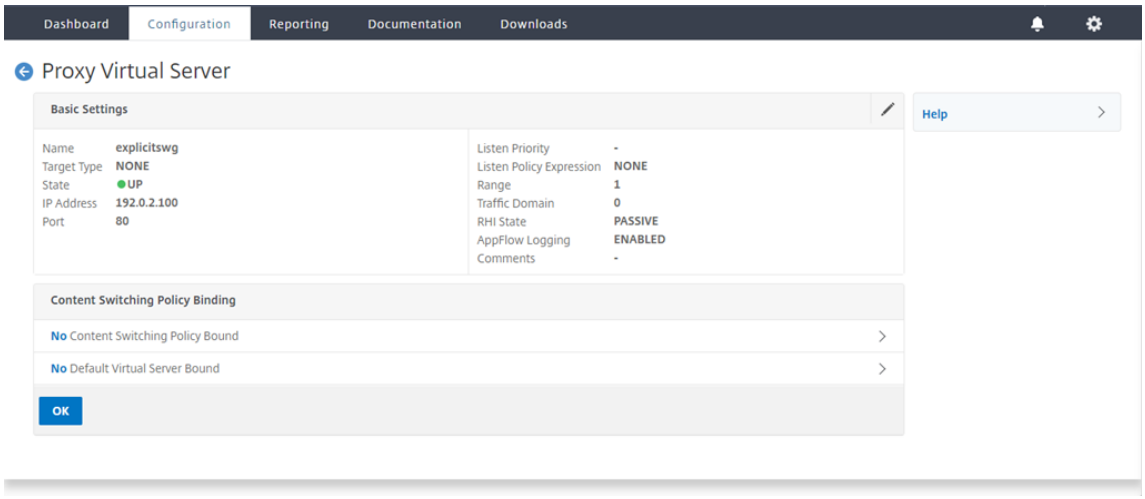
2. Entrez un nom et une adresse IP. Dans **Protocole**, sélectionnez **TCP**. Dans **Port**, tapez **1344**. Cliquez sur **OK**.



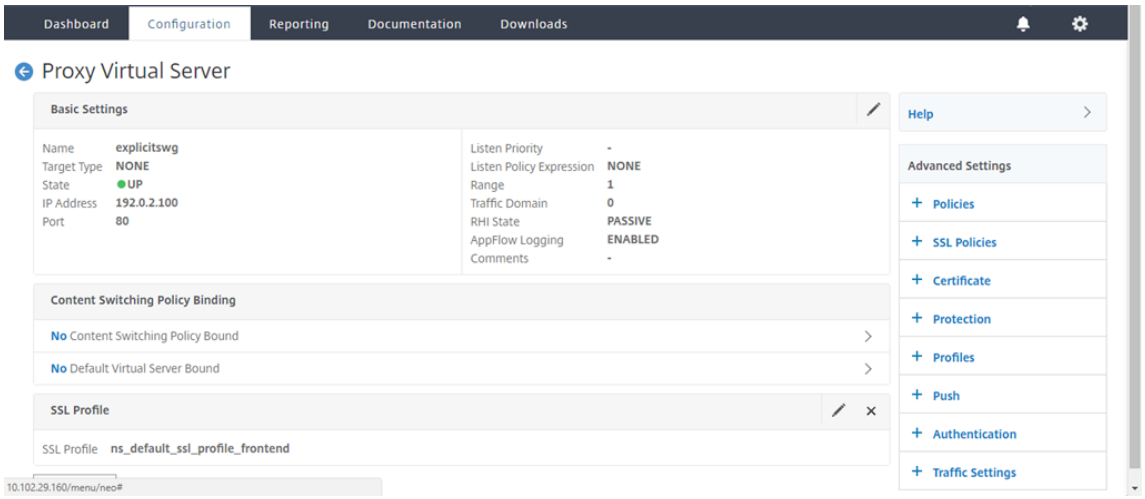
3. Accédez à **SSL Forward Proxy** > **Serveurs virtuels proxy**. Ajoutez un serveur virtuel proxy ou sélectionnez un serveur virtuel et cliquez sur **Modifier**. Après avoir saisi les détails, cliquez sur **OK**.



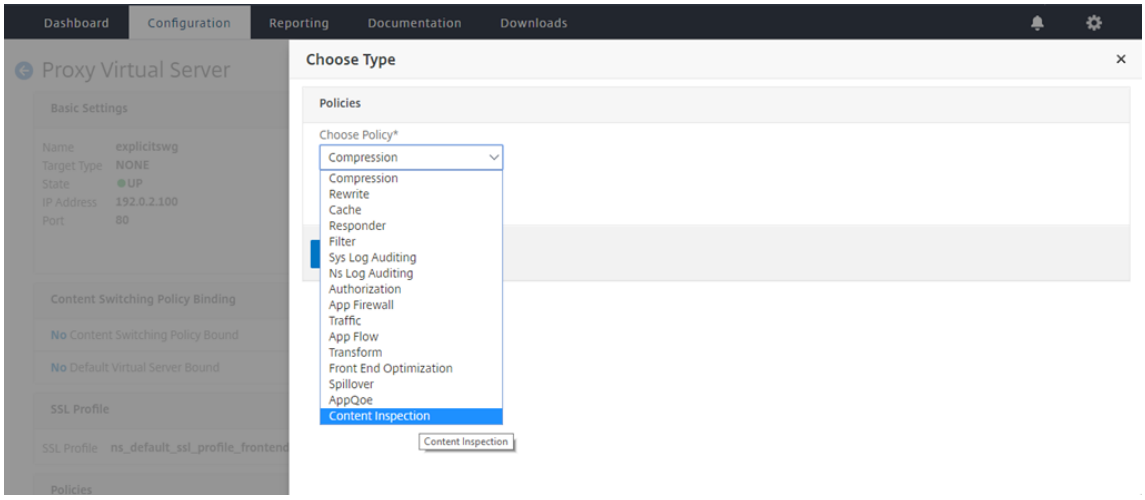
Cliquez à nouveau sur **OK** .



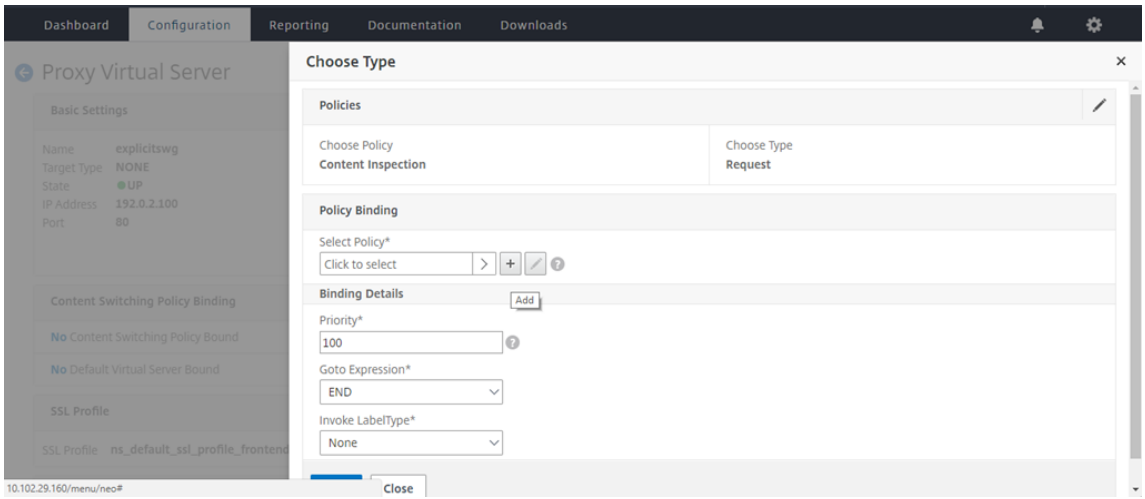
4. Dans **Paramètres avancés**, cliquez sur **Politiques**.



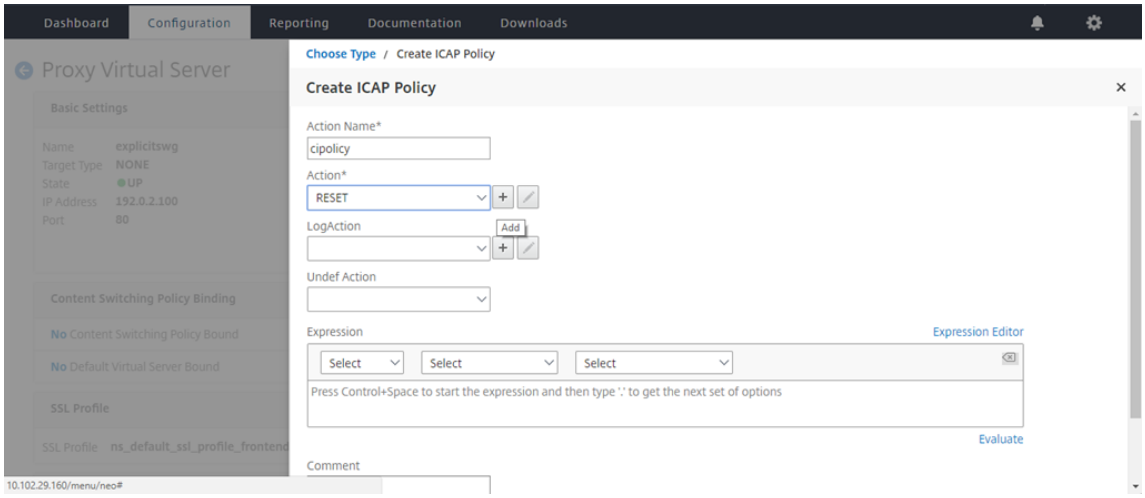
5. Dans **Choisir une politique**, sélectionnez **Inspection du contenu**. Cliquez sur **Continuer**.



6. Dans **Sélectionner une politique**, cliquez sur le signe « + » pour ajouter une politique.

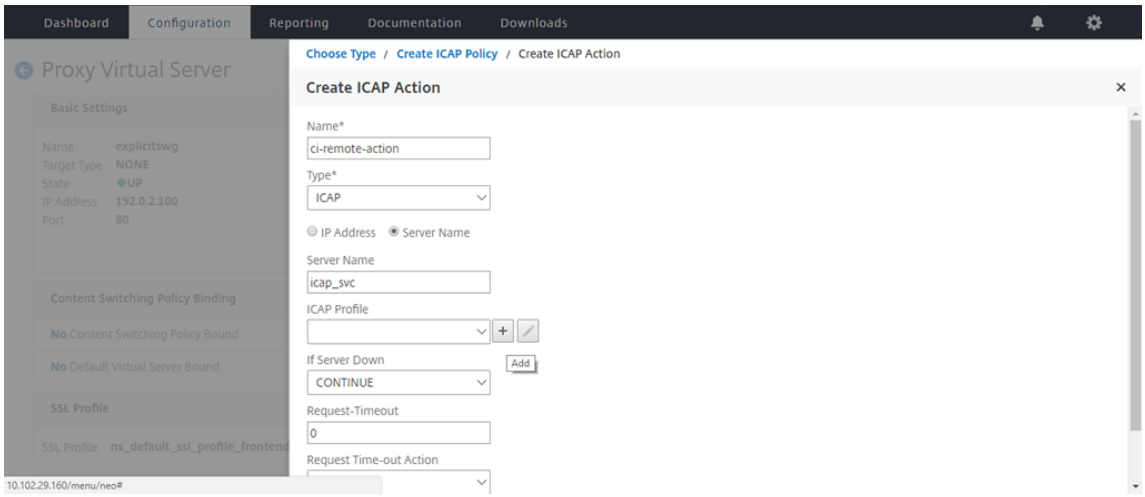


7. Entrez un nom pour la stratégie. Dans **Action**, cliquez sur le signe « + » pour ajouter une action.

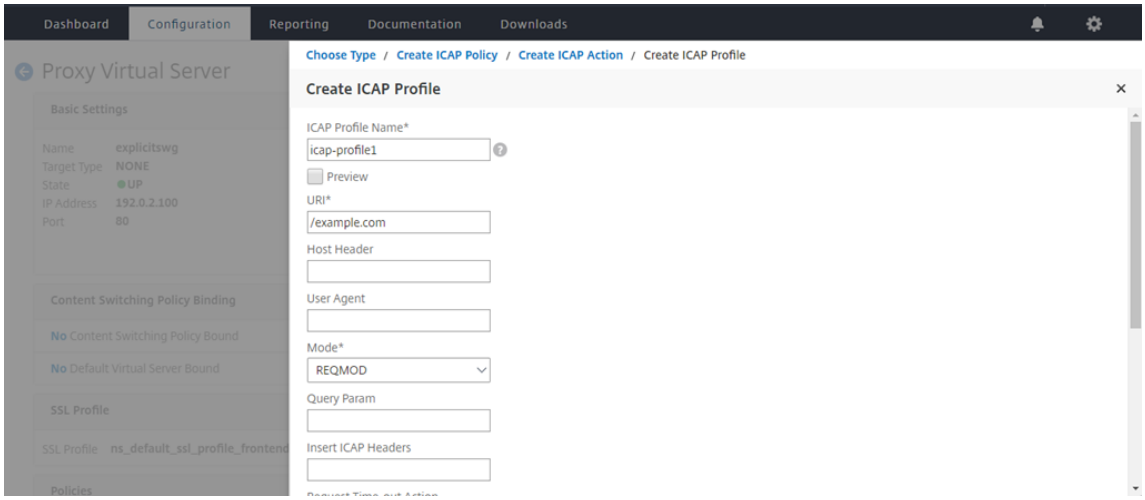


8. Tapez le nom de l'action. Dans **Nom du serveur**, tapez le nom du service TCP créé précédem-

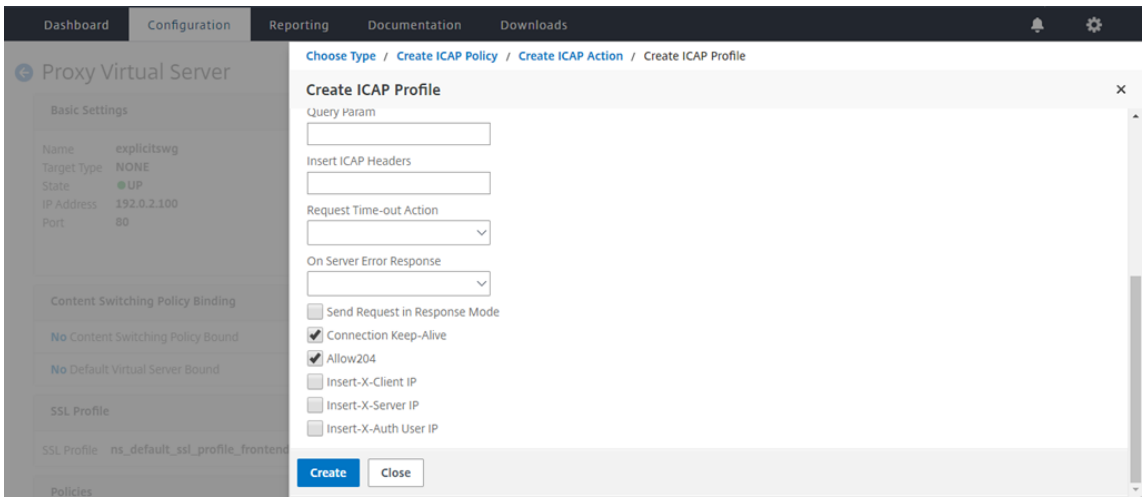
ment. Dans le **profil ICAP**, cliquez sur le signe « + » pour ajouter un profil ICAP.



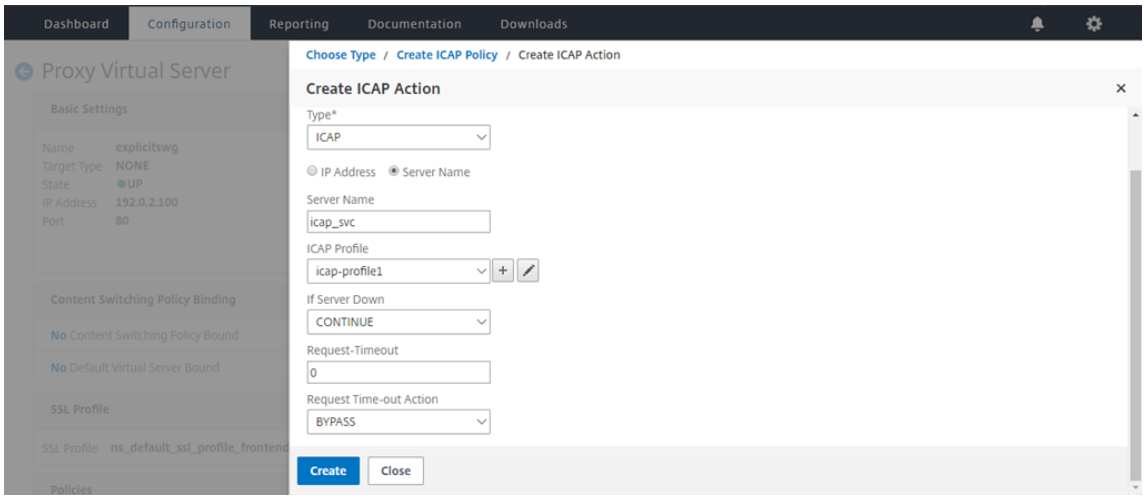
9. Tapez un nom de profil, une URI. Dans **Mode**, sélectionnez **REQMOD**.



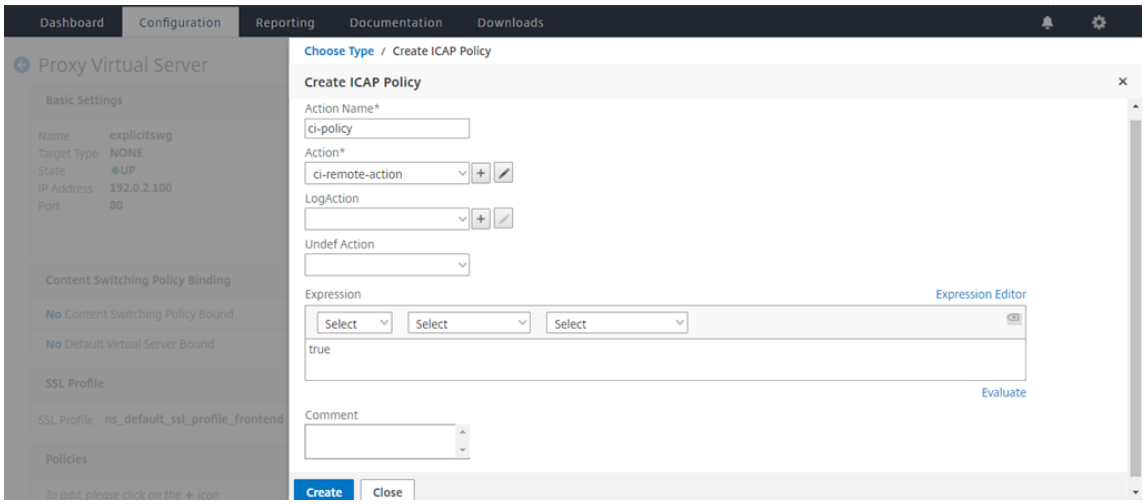
10. Cliquez sur **Create**.



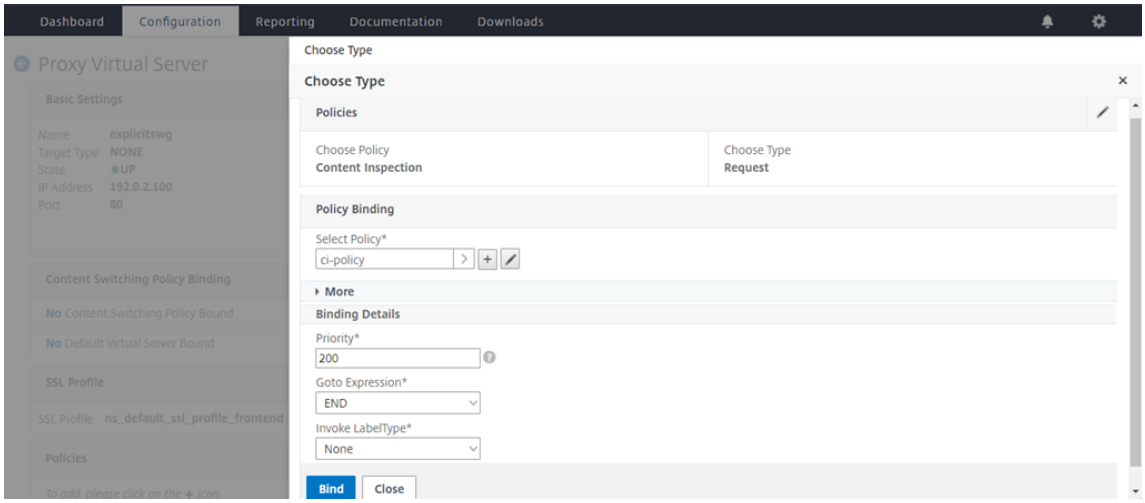
11. Dans la page **Créer une action ICAP**, cliquez sur **Créer**.



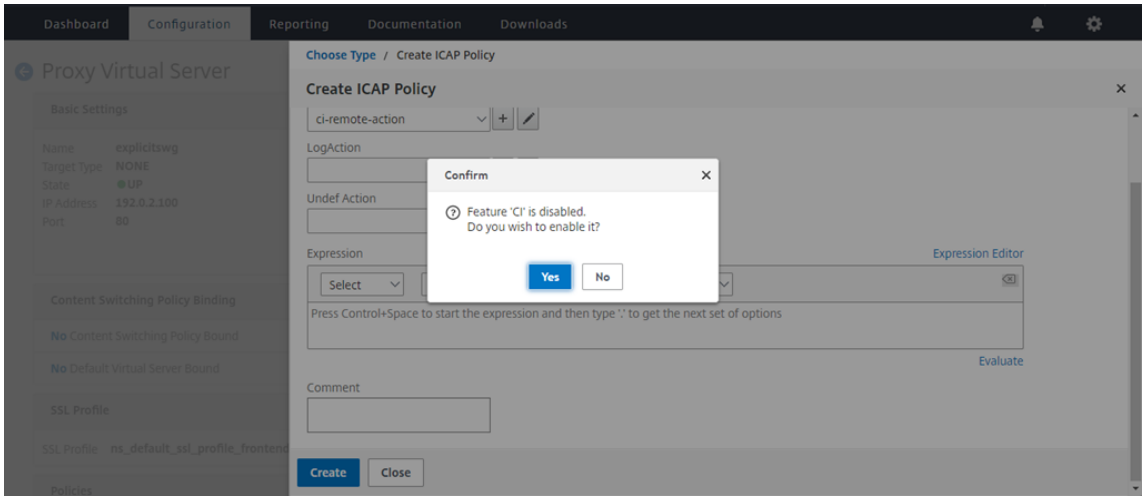
12. Sur la page **Créer une politique ICAP**, saisissez true dans l' **éditeur d'expressions**. Cliquez ensuite sur **Créer**.



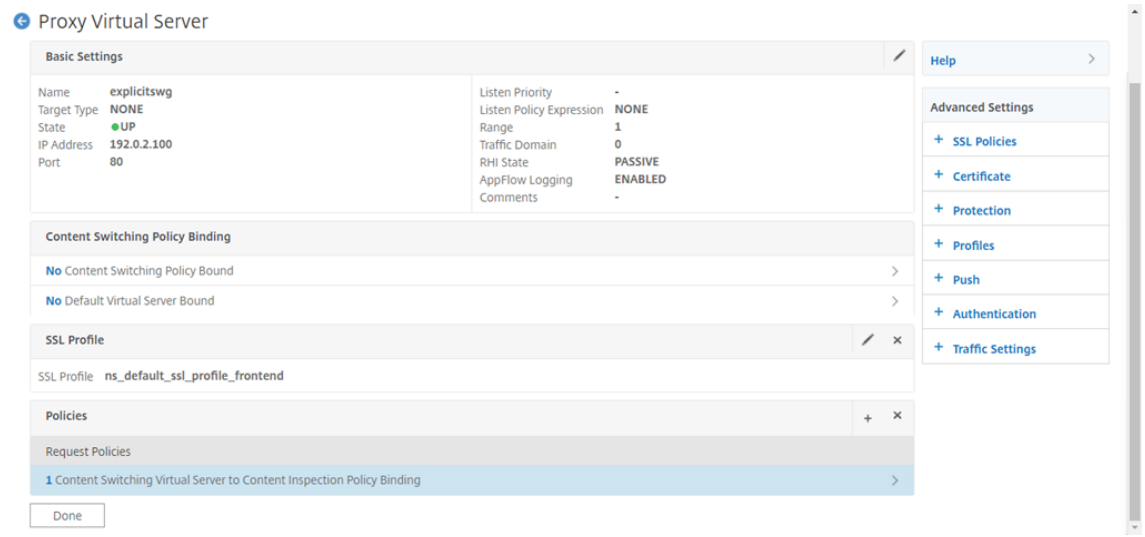
13. Cliquez sur **Bind**.



14. Lorsque vous êtes invité à activer la fonction d'inspection du contenu, sélectionnez **Oui**.



15. Cliquez sur **Terminé**.



Exemples de transactions ICAP entre l'appliance NetScaler et le serveur ICAP dans RESPMOD

Demande de l'appliance NetScaler au serveur ICAP :

```
RESPMOD icap://10.106.137.15:1344/resp ICAP/1.0

Host: 10.106.137.15

Connection: Keep-Alive

Encapsulated: res-hdr=0, res-body=282

HTTP/1.1 200 OK

Date: Fri, 01 Dec 2017 11:55:18 GMT

Server: Apache/2.2.21 (Fedora)

Last-Modified: Fri, 01 Dec 2017 11:16:16 GMT

ETag: "20169-45-55f457f42aee4"

Accept-Ranges: bytes

Content-Length: 69

Keep-Alive: timeout=15, max=100

Content-Type: text/plain; charset=UTF-8

X5O!P%@AP[4PZX54(P^)7CC)7 }
 $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
<!--NeedCopy-->
```

Réponse du serveur ICAP à l'appliance NetScaler :

```
ICAP/1.0 200 OK

Connection: keep-alive

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Encapsulated: res-hdr=0, res-body=224

```



```
Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

ISTag: "9.8-13.815.00-3.100.1027-1.0"

X-Virus-ID: Eicar_test_file

X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;

HTTP/1.1 403 Forbidden

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Cache-Control: no-cache

Content-Type: text/html; charset=UTF-8

Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

Content-Length: 5688

<html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset
    =UTF-8"/>

...

...

</body></html>
<!--NeedCopy-->
```

Articles pratiques

January 21, 2021

Voici quelques instructions de configuration ou cas d'utilisation fonctionnelle disponibles sous forme d'articles « How to » pour vous aider à gérer votre déploiement de proxy SSL.

Filtrage d'URL

Comment créer une stratégie de catégorisation d'URL

Comment créer une stratégie de liste d'URL

Comment autoriser une URL exceptionnelle

Comment bloquer les sites Web de la catégorie pour adultes

Security

May 5, 2023

Les rubriques suivantes couvrent les informations de configuration et d'installation des fonctionnalités de sécurité de NetScaler. La plupart de ces fonctionnalités sont basées sur des politiques.

Filtrage de contenu	Bloque les requêtes HTML inappropriées, empêchant ainsi les requêtes d'atteindre les serveurs Web.
Protection contre les surtensions	Détecte toute augmentation rapide du nombre de tentatives de connexion et ajuste la vitesse à laquelle les connexions sont autorisées à se poursuivre vers le serveur, afin d'éviter toute surcharge du serveur.
Options de sécurité DNS	Assistant d'interface utilisateur simplifié pour créer des politiques de protection contre les attaques DNS.

Protection contre les surtensions

May 5, 2023

Lorsqu'un pic de demandes client surcharge un serveur, la réponse du serveur devient lente et le serveur n'est pas en mesure de répondre aux nouvelles demandes. La fonction de protection contre les surtensions garantit que les connexions au serveur se produisent à une vitesse que le serveur peut gérer. Le taux de réponse dépend de la configuration de la protection contre les surtensions. L'appliance NetScaler suit également le nombre de connexions au serveur et utilise ces informations pour ajuster la vitesse à laquelle elle ouvre de nouvelles connexions au serveur.

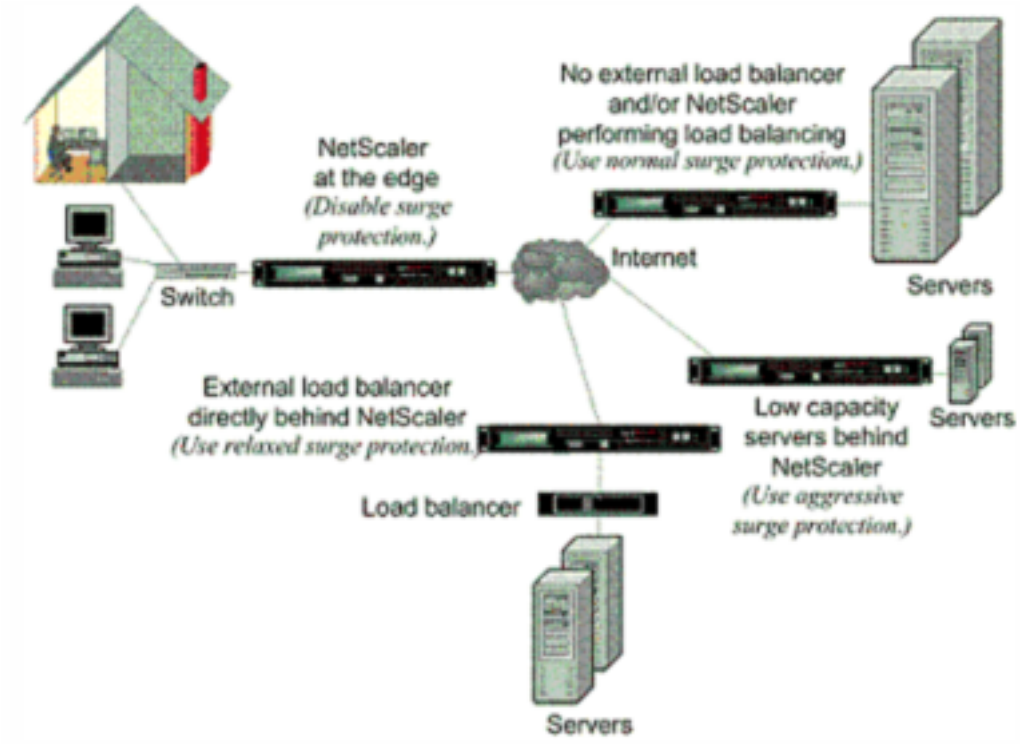
La protection contre les surtensions est activée par défaut. Si vous ne souhaitez pas utiliser de protection contre les surtensions, comme c'est le cas pour certaines configurations spéciales, vous devez la

désactiver.

Les paramètres par défaut de protection contre les surtensions sont suffisants pour la plupart des utilisations, mais vous pouvez configurer la protection contre les surtensions pour l'adapter à vos besoins. Tout d'abord, vous pouvez définir la valeur de l'accélérateur pour lui indiquer comment gérer de manière agressive les tentatives de connexion. Ensuite, vous pouvez définir la valeur seuil de base pour contrôler le nombre maximum de connexions simultanées autorisées par l'appliance NetScaler avant de déclencher la protection contre les surtensions. (La valeur du seuil de base par défaut est définie par la valeur de l'accélérateur, mais après avoir défini la valeur de l'accélérateur, vous pouvez la changer à n'importe quel nombre souhaité.)

La figure suivante illustre comment la protection contre les surtensions est configurée pour gérer le trafic vers un site Web.

Figure 1. Illustration fonctionnelle de la protection contre les surtensions de NetScaler



> **Remarque**
>
> Si l'appliance NetScaler est installée à la périphérie du réseau, où elle interagit avec les périphériques réseau du côté client d'Internet, la fonction de protection contre les surtensions doit être désactivée. La protection contre les surtensions doit également être désactivée si vous activez le mode USIP (Using Source IP) sur votre appliance.

Lorsque la protection contre les surtensions est désactivée et qu'une augmentation du nombre de demandes se produit, le serveur accepte autant de demandes qu'il peut traiter simultanément, puis commence à abandonner les demandes. Au fur et à mesure que le serveur devient plus surchargé, il

diminue et le taux de réponse est réduit à zéro. Lorsque le serveur se rétablit après le crash, plusieurs minutes plus tard, il envoie des réinitialisations pour toutes les demandes en attente, qui présentent un comportement anormal, et répond également aux nouvelles demandes avec réinitialisation. Le processus se répète pour chaque augmentation des demandes. Par conséquent, un serveur qui fait l'objet d'une attaque DDoS et qui reçoit plusieurs pics de demandes peut devenir indisponible pour les utilisateurs légitimes.

Lorsque la protection contre les surtensions est activée et qu'une augmentation du nombre de demandes se produit, la protection contre les surtensions gère le taux de demandes adressées au serveur, en envoyant des demandes au serveur uniquement aussi rapidement que le serveur peut traiter ces demandes. Cela permet au serveur de répondre correctement à chaque demande dans l'ordre dans lequel elle a été reçue. Lorsque la surtension est terminée, les demandes en attente sont effacées aussi rapidement que le serveur peut les traiter, jusqu'à ce que le taux de demandes corresponde au taux de réponse.

Désactiver et réactiver la protection contre les surtensions

May 5, 2023

La fonction de protection contre les surtensions est activée par défaut. Lorsque la protection contre les surtensions est activée, elle est active pour tous les services que vous ajoutez.

Désactiver ou réactiver la protection contre les surtensions à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'un des ensembles de commandes suivants pour désactiver ou réactiver la protection contre les surtensions et vérifier la configuration :

```
1 -  disable ns feature SurgeProtection
2 -  show ns feature
3 -  enable ns feature SurgeProtection
4 -  show ns feature
5 <!--NeedCopy-->
```

Exemple :

```
1 disable ns feature SurgeProtection
2  Done show ns feature
3
4         Feature                       Acronym             Status
5         -------                       -------             ------
```



```
1)     Web Logging                    WL                   ON
2)     Surge Protection               SP                   OFF
.
.
.
24)    NetScaler Push                 push                 OFF
Done
<!--NeedCopy-->
```

```
enable ns feature SurgeProtection
Done
> show ns feature

        Feature                       Acronym              Status
        -------                       -------              ------
1)     Web Logging                    WL                   ON
2)     Surge Protection               SP                   ON
.
.
.

24)    NetScaler Push                 push                 OFF
Done
>
<!--NeedCopy-->
```

Désactiver ou réactiver la protection contre les surtensions à l'aide de l'interface graphique

1. Dans le volet de navigation, développez **Système**, puis sélectionnez **Paramètres**.
2. Dans le volet d'informations, cliquez sur **Modifier les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, désactivez la sélection de la case à cocher **Protection contre** les surtensions pour désactiver la fonction de protection contre les surtensions, ou cochez la case pour activer la fonction.
4. Cliquez sur **OK**.
5. Dans la boîte de dialogue Activer/Désactiver les fonctionnalités, cliquez sur Oui. Un message apparaît dans la barre d'état indiquant que la fonction a été activée ou désactivée.

Désactiver ou réactiver la protection contre les surtensions pour un service particulier à l'aide de l'interface graphique

1. Accédez à **Traffic Management > Load Balancing > Services**. La liste des services configurés s'affiche dans le volet de détails.
2. Dans le volet d'informations, sélectionnez le service pour lequel vous souhaitez désactiver ou réactiver la fonctionnalité de protection contre les surtensions, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le service**, cliquez sur l' **onglet Avancé**et faites défiler l'écran vers le bas.
4. Dans le cadre Autres, désactivez la case à cocher **Protection contre les surtensions** pour désactiver la fonction de protection contre les surtensions, ou activez la case à cocher pour activer la fonction.
5. Cliquez sur **OK**. Un message apparaît dans la barre d'état indiquant que la fonction a été activée ou désactivée.
   Remarque : La protection contre les surtensions ne fonctionne que lorsque la fonction et le paramètre de service sont activés.

Définir des seuils de protection contre les surtensions

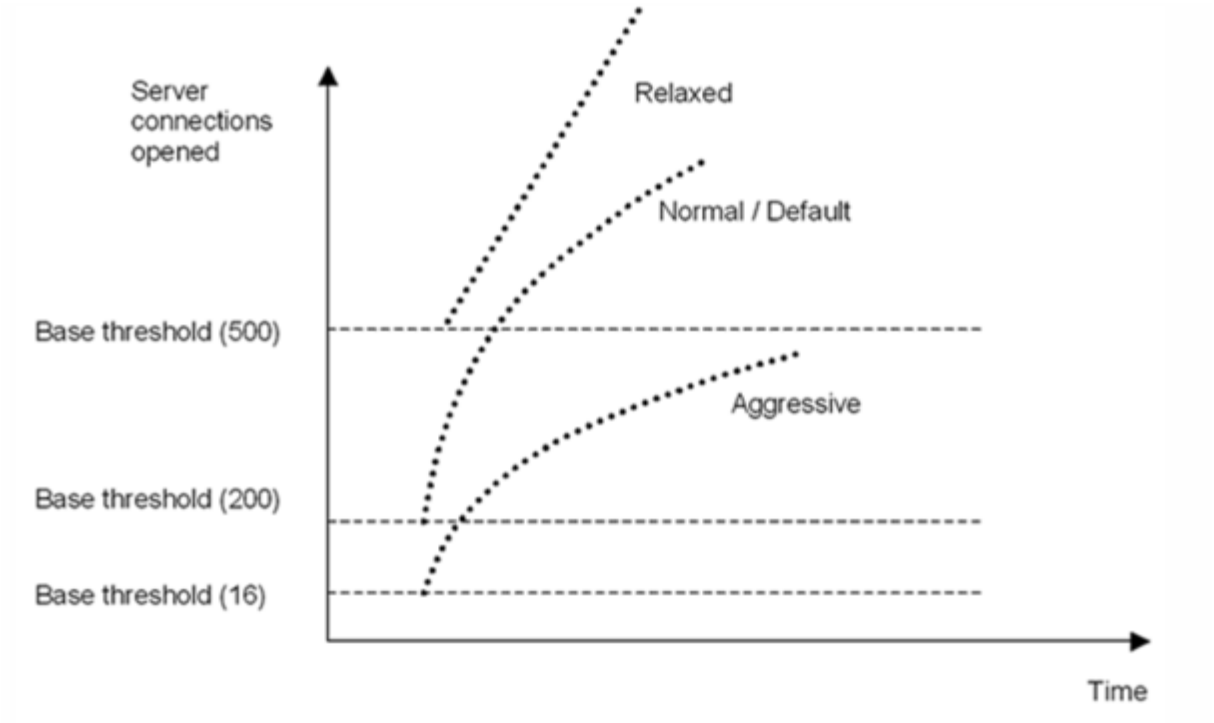
May 5, 2023

Pour définir la vitesse à laquelle l'appliance NetScaler ouvre des connexions au serveur, vous devez configurer les valeurs de seuil et de limitation pour la protection contre les surtensions.

> **Remarque**
>
> Les valeurs de seuil sont configurées globalement, mais elles sont appliquées par serveur d'équilibrage de charge individuel ou par service.

La figure suivante montre les courbes de protection contre les surtensions qui résultent du réglage de la vitesse d'accélération sur relâché, normal ou agressif. Selon la configuration de la capacité du serveur, vous pouvez définir des valeurs de seuil de base pour générer des courbes de protection contre les surtensions appropriées.

Figure 1. Courbes de protection contre

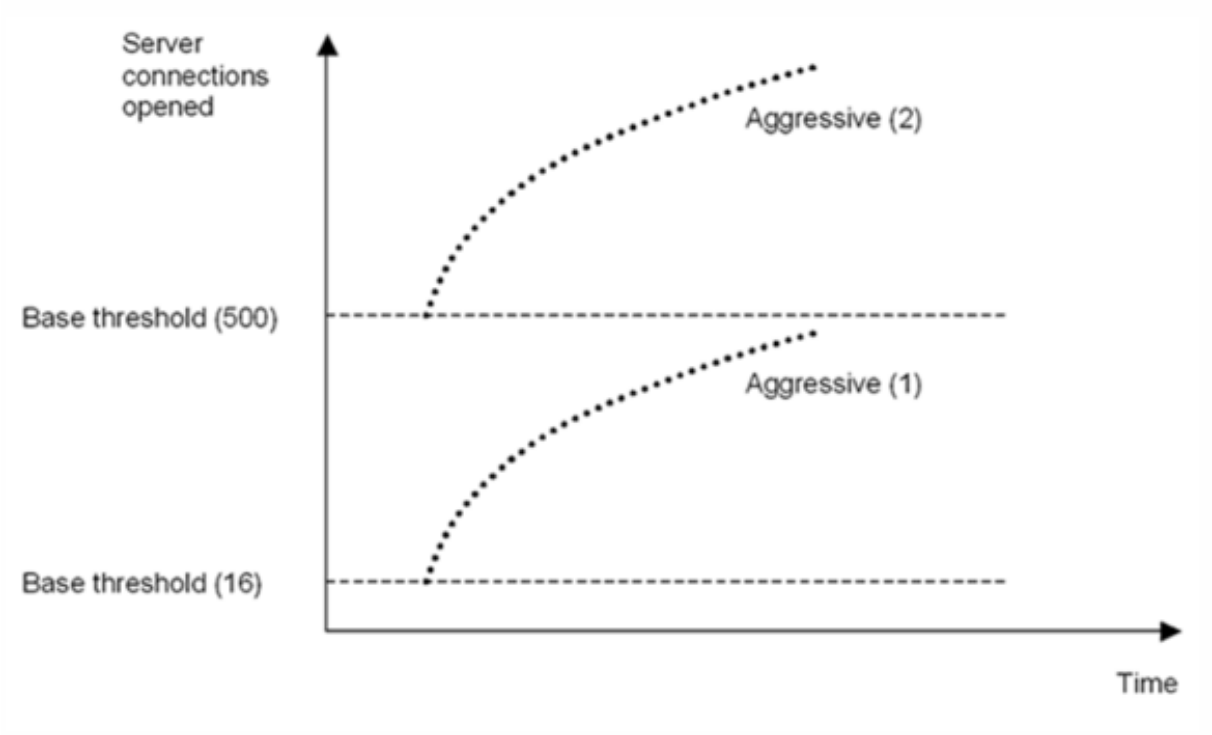


Vos paramètres de configuration affectent le comportement de la protection contre les surtensions de la manière suivante :

- Si vous ne spécifiez pas de taux d'accélération, il est réglé sur normal (valeur par défaut) et le seuil de base est défini sur 200, comme indiqué dans la figure précédente.
- Si vous spécifiez un taux d'accélération (agressif, normal ou détendu) sans spécifier de seuil de base, la courbe reflète les valeurs par défaut du seuil de base pour ce taux d'accélération. Par exemple, si vous réglez le taux d'accélération sur relâché, la courbe résultante aura la valeur seuil de base de 500.
- Si vous spécifiez uniquement le seuil de base, l'ensemble de la courbe de protection contre les surtensions se déplace vers le haut ou vers le bas, en fonction de la valeur que vous spécifiez, comme indiqué dans la figure suivante.
- Si vous spécifiez à la fois un seuil de base et un taux d'accélération, la courbe de protection contre les surtensions résultante est basée sur le taux d'accélération défini et ajustée en fonction de la valeur définie pour le seuil de base.

Dans la figure suivante, la courbe inférieure (Agressif 1) se produit lorsque le taux d'accélération est réglé sur agressif mais que le seuil de base n'est pas défini. La courbe supérieure (Agressif 2) apparaît lorsque le seuil de base est réglé sur 500, mais que le taux d'accélération n'est pas réglé. La deuxième courbe supérieure (Agressif 2) se produit également lorsque le seuil de base est réglé sur 500 et que le taux d'accélération est réglé sur agressif.

Figure 2. Taux agressif avec le seuil par défaut ou un seuil de base défini



Définir le seuil de protection contre les surtensions à l'aide de l'interface graphique

1. Dans le volet de navigation, développez Système, puis sélectionnez Paramètres.
2. Dans le volet d'informations, cliquez sur Paramètres système globaux.
3. Si vous souhaitez définir un seuil de base différent de celui par défaut pour le taux d'accélération, dans la boîte de dialogue Configurer les paramètres généraux, zone de texte Seuil de base, entrez le nombre maximal de connexions serveur simultanées autorisées avant le déclenchement de la protection contre les surtensions. Le seuil de base est le nombre maximal de connexions au serveur pouvant être ouvertes avant l'activation de la protection contre les surtensions. La valeur maximale de ce paramètre est de 32 767 connexions au serveur. Le réglage par défaut de cette valeur est contrôlé par le taux d'accélération que vous choisissez à l'étape suivante.

   Remarque : Si vous ne définissez pas de valeur explicite ici, la valeur par défaut sera utilisée.
4. Dans la liste déroulante Throttle, sélectionnez un taux d'accélération. L'accélération est la vitesse à laquelle l'appliance NetScaler autorise l'ouverture de connexions au serveur. L'accélérateur peut être réglé sur les valeurs suivantes :

   - **Agressif :** choisissez cette option lorsque la capacité de gestion des connexions et des surtensions du serveur est faible et que la connexion doit être gérée avec soin. Lorsque vous réglez l'accélérateur sur agressif, le seuil de base est défini sur une valeur par défaut

de 16, ce qui signifie que la protection contre les surtensions est déclenchée chaque fois qu'il y a 17 connexions simultanées ou plus au serveur.

- **Normal :** choisissez cette option lorsqu'aucun équilibreur de charge externe ne se trouve derrière l'appliance NetScaler ou en aval. Le seuil de base est défini sur une valeur de 200, ce qui signifie que la protection contre les surtensions est déclenchée chaque fois qu'il y a 201 connexions simultanées ou plus au serveur. Normal est l'option d'accélération par défaut.
- **Détendu :** choisissez cette option lorsque l'appliance NetScaler effectue un équilibrage de charge entre un grand nombre de serveurs Web et peut donc gérer un grand nombre de connexions simultanées. Le seuil de base est défini sur une valeur de 500, ce qui signifie que la protection contre les surtensions n'est déclenchée que lorsqu'il y a 501 connexions simultanées ou plus au serveur.

5. Cliquez sur OK. Un message apparaît dans la barre d'état indiquant que les paramètres globaux sont configurés.

Éviter la file d'attente de surtension

May 5, 2023

Lorsqu'un serveur physique reçoit une vague de demandes, il met du temps à répondre aux clients qui y sont actuellement connectés, ce qui laisse les utilisateurs insatisfaits et mécontents. Souvent, la surcharge provoque également les clients à recevoir des pages d'erreur. Pour éviter de telles surcharges, l'appliance NetScaler fournit des fonctionnalités telles que la protection contre les surtensions, qui contrôle la vitesse à laquelle de nouvelles connexions à un service peuvent être établies.

L'appliance effectue le multiplexage des connexions entre les clients et les serveurs physiques. Lorsqu'elle reçoit une demande d'un client pour accéder à un service sur un serveur, l'appliance recherche une connexion gratuite déjà établie avec le serveur. S'il trouve une connexion libre, il utilise cette connexion pour établir un lien virtuel entre le client et le serveur. S'il ne trouve pas de connexion libre existante, l'appliance établit une nouvelle connexion avec le serveur et établit un lien virtuel entre un client et le serveur. Toutefois, si l'appliance ne peut pas établir de nouvelle connexion avec le serveur, elle envoie la demande client à une file d'attente de surtension. Si tous les serveurs physiques liés au serveur virtuel d'équilibrage de charge ou de commutation de contenu atteignent la limite supérieure du nombre de connexions client (valeur client maximale, seuil de protection contre les surtensions ou capacité maximale du service), l'appliance ne peut établir de connexion avec aucun serveur. La fonction de protection contre les surtensions utilise la file d'attente pour réguler la vitesse à laquelle les connexions sont ouvertes avec les serveurs physiques. L'appliance gère une file d'attente de surtension différente pour chaque service lié au serveur virtuel.

La longueur d'une file d'attente d'urgence augmente chaque fois qu'une demande arrive pour laque-

lle l'appliance ne peut pas établir de connexion, et elle diminue chaque fois qu'une demande de la file d'attente est envoyée au serveur ou qu'une demande arrive à expiration et est supprimée de la file d'attente.

Si la file d'attente d'un service ou d'un groupe de services devient trop longue, vous pouvez la vider. Vous pouvez vider la file d'attente d'un service ou d'un groupe de services spécifique, ou de tous les services et groupes de services liés à un serveur virtuel d'équilibrage de charge. Le fait de vider une file d'attente d'urgence n'affecte pas les connexions existantes. Seules les demandes présentes dans la file d'attente d'urgence sont supprimées. Pour ces demandes, le client doit faire une nouvelle demande.

Vous pouvez également vider la file d'attente d'un serveur virtuel de commutation de contenu. Si un serveur virtuel de commutation de contenu transmet certaines demandes à un serveur virtuel d'équilibrage de charge particulier et que le serveur virtuel d'équilibrage de charge reçoit également d'autres demandes, lorsque vous videz la file d'attente du serveur virtuel de commutation de contenu, seules les demandes reçues de ce serveur virtuel de commutation de contenu sont vidées. Les autres requêtes de la file d'attente de surtension du serveur virtuel d'équilibrage de charge ne sont pas vidées.

Remarque :

> - Vous ne pouvez pas vider les files d'attente de surtension des serveurs virtuels de redirection de cache, d'authentification, de VPN ou de serveurs virtuels GSLB ou des services GSLB.
> - N'utilisez pas la fonctionnalité Protection contre les surtensions si USIP (USIP) est activée.

Videz une file d'attente d'urgence à l'aide de l'interface de ligne de commande

La commande flush ns SurgeQ fonctionne de la manière suivante :

- Vous pouvez spécifier le nom d'un service, d'un groupe de services ou d'un serveur virtuel dont la file d'attente doit être vidée.
- Si vous spécifiez un nom lors de l'exécution de la commande, la file d'attente de surtension de l'entité spécifiée est vidé. Si plusieurs entités portent le même nom, l'appliance vid les files d'attente de surtension de toutes ces entités.
- Si vous spécifiez le nom d'un groupe de services, ainsi qu'un nom de serveur et un port lors de l'exécution de la commande, l'appliance vide la file d'attente de surtension du membre du groupe de services spécifié uniquement.
- Vous ne pouvez pas spécifier directement un membre de groupe de services <serverName> and <port> sans spécifier le nom du groupe de services <name> et vous ne pouvez pas spécifier <port> sans un <serverName>. Spécifiez le <serverName> et <port> si vous souhaitez vider la file d'attente de surtension pour un membre du groupe de services spécifique.
- Si vous exécutez la commande sans spécifier de nom, l'appliance vide les files d'attente de surtension de toutes les entités présentes sur l'appliance.

- Si un membre du groupe de services est identifié par un nom de serveur, vous devez spécifier le nom du serveur dans cette commande ; vous ne pouvez pas spécifier son adresse IP.

À l'invite de commande, tapez :

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
```

Exemples

1. `flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80`

   La commande précédente vide la file d'attente de surtension du service ou du serveur virtuel appelé SVC1ANZGB et dont l'adresse IP est 10.10.10.

2. `flush ns surgeQ`

   La commande précédente vide toutes les files d'attente de surtension de l'appliance.

Purger une file d'attente de surtension à l'aide de l'interface graphique

Accédez à Gestion du trafic > Commutation de contenu > Serveurs virtuels, sélectionnez un serveur virtuel et, dans la liste Action, sélectionnez Vider la file d'attente de surtension.

Options de sécurité DNS

May 5, 2023

Vous pouvez désormais configurer les options de sécurité DNS à partir de la page Ajouter un profil de sécurité DNS dans l'interface graphique de NetScaler. Pour configurer les options de sécurité DNS à partir de l'interface de ligne de commande NetScaler ou de l'API NITRO, utilisez les composants AppExpert. Pour obtenir des instructions, consultez la documentation de l'API NITRO et le NetScaler Command Reference Guide.

L'une des options, la protection contre l'empoisonnement du cache, est activée par défaut et ne peut pas être désactivée. Vous pouvez appliquer les autres options à tous les points de terminaison DNS ou à des serveurs virtuels DNS spécifiques de votre déploiement, comme indiqué dans le tableau suivant :

Option de sécurité	Peut-il être appliqué à tous les points de terminaison DNS ?	Peut-il être appliqué à des serveurs virtuels DNS spécifiques ?
Protection DDoS DNS	Oui	Oui

Option de sécurité	Peut-il être appliqué à tous les points de terminaison DNS ?	Peut-il être appliqué à des serveurs virtuels DNS spécifiques ?
Gestion des exceptions : serveurs sur liste blanche/liste noire	Oui	Oui
Empêchez les attaques aléatoires de sous-domaines	Oui	Oui
Contourner le cache	Oui	Non
Appliquer les transactions DNS via TCP	Oui	Oui
Fournissez les détails de la racine dans la réponse DNS	Oui	Non

Protection contre l'empoisonnement du cache

Une attaque par empoisonnement du cache redirige les utilisateurs de sites légitimes vers des sites Web malveillants.

Par exemple, l'attaquant remplace une adresse IP authentique dans le cache DNS par une adresse IP fausse qu'il contrôle. Lorsque le serveur répond à des demandes provenant de ces adresses IP, le cache est empoisonné. Les demandes ultérieures d'adresses du domaine sont redirigées vers le site de l'attaquant.

L'option Protection contre l'empoisonnement du cache empêche l'insertion de données corrompues dans la base de données qui met en cache les demandes et les réponses du serveur DNS. Cette fonctionnalité est intégrée aux appliances NetScaler et est toujours activée.

Protection DDoS DNS

Vous pouvez configurer l'option Protection DDoS DNS pour chaque type de requête que vous soupçonnez d'être utilisée dans une attaque DDoS. Pour chaque type, l'appliance supprime toutes les demandes reçues après le dépassement d'une valeur seuil pour le nombre de demandes reçues au cours d'une période spécifiée (tranche de temps). Vous pouvez également configurer cette option pour consigner un avertissement sur le serveur SYSLOG. Par exemple :

- **DROP :** - Sélectionnez cette option pour déposer des requêtes sans journalisation. Supposons que vous ayez activé une protection d'enregistrement avec une valeur de seuil 15, une tranche de temps de 1 seconde et que vous avez choisi DROP. Lorsque les demandes entrantes dépassent 15 requêtes en 1 seconde, les paquets commencent à être supprimés.

- **AVERTISSEMENT :** - Sélectionnez cette option pour enregistrer et déposer les demandes. Supposons que vous ayez activé une protection d'enregistrement avec une valeur de seuil 15, une tranche de temps de 1 seconde et que vous avez choisi WARN. Lorsque les demandes entrantes dépassent 15 requêtes en 1 seconde, un message d'avertissement est enregistré indiquant une menace, puis les paquets sont supprimés. Citrix vous recommande de définir des valeurs de seuil pour WARN inférieures à la valeur seuil de DROP pour un type d'enregistrement. Ce paramètre aide les administrateurs à identifier une attaque en enregistrant un message d'avertissement avant que l'attaque ne se produise et que NetScaler ne commence à supprimer les demandes entrantes.

Définir un seuil pour le trafic entrant à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Sécurité** > **Sécurité DNS**.
2. Sur la page du **profil de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, procédez comme suit :
4. Étendez la **protection DNS contre les attaques DDoS**.
   a) Sélectionnez le type d'enregistrement et entrez le seuil et la valeur de la tranche de temps.
   b) Sélectionnez **DROP** ou **WARN**.
   c) Répétez les étapes a et b pour chacun des autres types d'enregistrement contre lesquels vous souhaitez vous protéger.
5. Cliquez sur **Envoyer**.

Gérer les exceptions — serveurs de listes d'autorisations/listes de blocage

Gérer les exceptions vous permet d'ajouter des exceptions à la liste de blocage ou à autoriser la liste des noms de domaine et des adresses IP. Par exemple :

- Lorsqu'une adresse IP particulière est identifiée en train de publier une attaque, cette adresse IP peut être ajoutée à la liste de blocage.
- Lorsque les administrateurs constatent qu'il y a un nombre inattendu de demandes pour un nom de domaine particulier, il est possible d'ajouter ce nom de domaine à la liste de blocage.
- `NXDomains` et certains des domaines existants pouvant consommer les ressources du serveur peuvent être mis sur liste noire.
- Lorsque les administrateurs autorisent les noms de domaine de liste ou les adresses IP, les requêtes ou requêtes provenant uniquement de ces domaines ou adresses IP reçoivent une réponse et toutes les autres sont supprimées.

Créez une liste d'autorisation ou une liste bloquée à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.

2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, procédez comme suit :
   a) Développez la **gestion des exceptions : serveurs sur liste blanche/liste noire.**
   b) Sélectionnez **Bloquer pour bloquer** les requêtes provenant de domaines/adresses de la liste noire, ou sélectionnez **Autoriser uniquement pour autoriser** les requêtes provenant de domaines/adresses de la liste blanche.
   c) Dans la zone **Nom de domaine/Adresse IP**, entrez les noms de domaine, les adresses IP ou les plages d'adresses IP. Utilisez des virgules pour séparer les entrées.
   Remarque : Si vous sélectionnez l'**option avancée**, vous pouvez utiliser les options « commencer par », « contient » et « se termine par » pour définir les critères.
   Par exemple, vous pouvez définir des critères pour bloquer une requête DNS commençant par « image » ou se terminant par « .co.ru » ou contenant des « sites mobiles ». «
4. Cliquez sur **Envoyer**.

Empêchez les attaques aléatoires de sous-domaines

Dans les attaques aléatoires de sous-domaines, les requêtes sont envoyées à des sous-domaines aléatoires et inexistants de domaines légitimes. Cette action augmente la charge sur les résolveurs et serveurs DNS. En conséquence, ils peuvent devenir surchargés et ralentir.

L'option Empêcher les attaques aléatoires sur des sous-domaines indique au répondeur DNS de supprimer les requêtes DNS qui dépassent une certaine longueur.

Supposons que example.com est un nom de domaine qui vous appartient et que la demande de résolution parvient donc à votre serveur DNS. L'attaquant peut ajouter un sous-domaine aléatoire à example.com et envoyer une demande. En fonction de la longueur de requête spécifiée et du nom de domaine complet, les requêtes aléatoires sont supprimées.

Par exemple, si la requête est www.image987trending.example.com, elle est supprimée si la longueur de la requête est définie sur 20.

Spécifier une longueur de requête DNS à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.
2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, procédez comme suit :
   a) Développez **Prévenir les attaques aléatoires sur des sous-domaines**.
   b) Entrez la valeur numérique de la longueur de la requête.
4. Cliquez sur **Envoyer**.

Contourner le cache

Lors d'une attaque, les données déjà mises en cache doivent être protégées. Pour protéger le cache, de nouvelles demandes pour certains domaines ou certains types d'enregistrements ou codes de réponse peuvent être envoyées aux serveurs d'origine plutôt que mises en cache.

L'option Contourner le cache indique à l'appliance NetScaler de contourner le cache pour des domaines, des types d'enregistrements ou des codes de réponse spécifiques lorsqu'une attaque est détectée.

Contournez le cache pour les domaines ou les types d'enregistrements ou les types de réponse spécifiés à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.
2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, développez **Contournement du cache** et entrez les noms de domaine. Vous pouvez également choisir les types d'enregistrement ou les types de réponses pour lesquels le cache doit être contourné.
    - Cliquez sur **Domaines** et saisissez les noms de domaine. Utilisez des virgules pour séparer les entrées.
    - Cliquez sur **Types d'enregistrement** et choisissez les types d'enregistrement.
    - Cliquez sur **Types de réponse** et choisissez le type de réponse.
4. Cliquez sur **Envoyer**.

Appliquer les transactions DNS via TCP

Certaines attaques DNS peuvent être évitées si les transactions sont obligées d'utiliser le protocole TCP au lieu de l'UDP. Par exemple, lors d'une attaque par un bot, le client envoie un flot de requêtes mais ne peut pas gérer les réponses. Si l'utilisation du protocole TCP est imposée pour ces transactions, les robots ne peuvent pas comprendre les réponses et ne peuvent donc pas envoyer de requêtes via TCP.

Forcer les domaines ou les types d'enregistrements à fonctionner au niveau TCP à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.
2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, développez **Appliquer les transactions DNS via TCP** et entrez les noms de domaine et/ ou choisissez les types d'enregistrements pour lesquels les transactions DNS doivent être appliquées via TCP.

- Cliquez sur **Domaines** et saisissez les noms de domaine. Utilisez des virgules pour séparer les entrées.
- Cliquez sur **Types d'enregistrements**, puis choisissez les types d'enregistrements.

4. Cliquez sur **Envoyer**.

Fournissez les détails de la racine dans la réponse DNS

Dans certaines attaques, l'attaquant envoie un flot de requêtes pour des domaines non liés qui ne sont pas configurés ou mis en cache sur l'appliance NetScaler. Si le `dnsRootReferral` paramètre est ENABLED, il expose tous les serveurs racine.

L'option Fournir les détails de la racine dans la réponse DNS indique à l'appliance NetScaler de restreindre l'accès aux références root pour une requête qui n'est ni configurée ni mise en cache. L'appliance envoie une réponse vide.

L'option Fournissez les détails racine dans l'option Réponse DNS peut également atténuer ou bloquer les attaques d'amplification. Lorsque le paramètre DNSRootReferral est DÉSACTIVÉ, il n'y a aucune référence racine dans les réponses de NetScaler et elles ne sont donc pas amplifiées.

Activer ou désactiver l'accès au serveur racine à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Sécurité DNS**.
2. Dans la page **Profils de sécurité DNS**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil de sécurité DNS**, procédez comme suit :
   a) Développez **Fournissez les détails de la racine dans la réponse DNS**.
   b) Cliquez **sur ON** ou **OFF** pour autoriser ou restreindre l'accès au serveur racine.
4. Cliquez sur **Envoyer**.

Système

May 5, 2023

Cette section fournit des informations au niveau du système sur NetScaler. Cela inclut une explication détaillée des fonctionnalités au niveau du système, les scénarios dans lesquels les fonctionnalités peuvent être utilisées, les étapes de configuration et des exemples pour vous aider à mieux comprendre les fonctionnalités.

- Opérations de base
- Authentification et autorisation
- Configurations TCP
- Configurations HTTP

- SNMP
- Journalisation de l'audit
- Journalisation du serveur Web
- Call Home
- Outil de création de rapports
- CloudBridge Connector
- Haute disponibilité
- Optimisation TCP

Opérations de base système

May 5, 2023

Les configurations suivantes vous permettent d'effectuer des opérations de base du système sur une appliance NetScaler.

Comment afficher, enregistrer et effacer la configuration de NetScaler

Les configurations NetScaler sont stockées dans le. `/nsconfig/ns.conf directory` Pour que les configurations soient disponibles entre les sessions, vous devez enregistrer la configuration après chaque modification de configuration.

Afficher la configuration en cours à l'aide de l'interface de commande

À l'invite de commande, tapez :

```
1 show ns runningConfig
2 <!--NeedCopy-->
```

Afficher la configuration en cours d'exécution à l'aide de l'interface graphique

1. Accédez à **Système** > **Diagnostics** et, dans le **groupe Configuration de la vue**, cliquez sur **Exécuter la configuration.**

Afficher la différence entre les deux fichiers de configuration à l'aide de l'interface de commande

À l'invite de commande, tapez :


```
diff ns config <configfile> <configfile2>
<!--NeedCopy-->
```

Afficher la différence entre les deux fichiers de configuration à l'aide de l'interface graphique

1. Accédez à **Système** > **Diagnostics** et, dans le **groupe Afficher la configuration**, cliquez sur **Différence de configuration**.

Enregistrez les configurations NetScaler à l'aide de l'interface de commande

À l'invite de commande, tapez :

```
save ns config
<!--NeedCopy-->
```

Enregistrez les configurations NetScaler à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, dans le coin supérieur droit, cliquez sur l'icône **Enregistrer** .

Afficher les configurations enregistrées à l'aide de l'interface de commande

À l'invite de commande, tapez :

```
show ns ns.conf
<!--NeedCopy-->
```

Afficher les configurations enregistrées à l'aide de l'interface graphique

Accédez à **Système** > **Diagnostics** et, dans le groupe **Afficher la configuration**, cliquez sur **Configuration enregistrée**.

Effacez la configuration de NetScaler à l'aide de l'interface de commande

Vous disposez des trois options suivantes pour effacer la configuration de NetScaler.

Niveau de base. Effacer votre configuration au niveau de base efface tous les paramètres sauf les suivants :

- `Nsroot` mot de passe
- Fuseau horaire

- Serveur NTP
- Connexion au serveur ADM
- Informations sur le fichier de licence
- NSIP, MIP(s) et SNIP(s)
- Paramètres réseau (paramètres de passerelle par défaut, VLAN, RHI, NTP et DNS)
- Définitions de nœuds HA
- Paramètres des fonctionnalités et des modes
- Mot de passe administrateur par défaut (`nsroot`)

Niveau étendu. L'effacement de votre configuration au niveau étendu efface tous les paramètres, à l'exception des suivants :

- NSIP et SNIP (s)
- Paramètres réseau (paramètres de passerelle par défaut, VLAN, RHI, NTP et DNS)
- Définitions de nœuds HA

Les paramètres de fonction et de mode reviennent à leurs valeurs par défaut.

Niveau complet. Si vous effacez votre configuration au niveau complet, tous les paramètres retrouvent leurs valeurs par défaut d'usine. Toutefois, le NSIP et la passerelle par défaut ne sont pas modifiés, car leur modification peut entraîner la perte de connectivité réseau de l'appliance.

À l'invite de commande, tapez :

```
clear ns config -force
<!--NeedCopy-->
```

Exemple : Pour effacer de manière forcée les configurations de base d'une appliance.

```
clear ns config -force basic
<!--NeedCopy-->
```

Effacer la configuration de NetScaler à l'aide de l'interface graphique

Accédez à **Système** > **Diagnostics** et, dans le groupe Maintenance, cliquez sur **Effacer la configuration** et sélectionnez le niveau de configuration à effacer de l'appliance.

Comment redémarrer ou arrêter l'appliance pour les configurations NetScaler non enregistrées

L'appliance NetScaler peut être redémarrée ou arrêtée à distance à partir des interfaces utilisateur disponibles. Lorsque vous redémarrez ou arrêtez une appliance NetScaler autonome, les configurations non enregistrées (configurations effectuées depuis l'émission de la dernière commande save ns config) sont perdues.

Dans une configuration haute disponibilité, lorsque l'appliance principale est redémarrée ou arrêtée, l'appliance secondaire prend le relais et devient la solution principale. Les configurations non enregistrées de l'ancien serveur principal sont disponibles sur le nouveau dispositif principal.

Vous pouvez également redémarrer l'appliance en redémarrant uniquement le logiciel NetScaler et en ne redémarrant pas le système d'exploitation sous-jacent. C'est ce qu'on appelle un redémarrage à chaud. Par exemple, lorsque vous ajoutez une nouvelle licence ou que vous modifiez l'adresse IP, vous pouvez redémarrer à chaud l'appliance NetScaler pour que ces modifications soient effectuées.

> **Remarque :**
>
> Vous pouvez effectuer un redémarrage à chaud uniquement sur une appliance NetScaler autonome.

Redémarrez l'appliance à l'aide de l'interface de commande

À l'invite de commande, tapez :

```
reboot [-warm]
<!--NeedCopy-->
```

Redémarrez une appliance NetScaler à l'aide de l'interface graphique

1. Dans la page de configuration, cliquez sur **Redémarrer**.
2. Lorsque vous êtes invité à redémarrer, sélectionnez **Enregistrer la configuration** pour vous assurer que vous ne perdez aucune configuration.

> **Remarque :**
>
> Vous pouvez effectuer un redémarrage à chaud en sélectionnant Redémarrage à chaud.

Arrêtez une appliance à l'aide de l'interface de commande

À l'invite shell, tapez :

- `shutdown -p now` : Arrête le logiciel et éteint NetScaler. Pour redémarrer NetScaler MPX, appuyez sur l'interrupteur secteur. Pour redémarrer NetScaler VPX, redémarrez l'instance VPX.
- `shutdown -h now` : Arrête le logiciel et laisse NetScaler activé. Appuyez sur n'importe quelle touche pour redémarrer NetScaler. Cette commande ne désactive pas NetScaler. Par conséquent, ne mettez pas l'alimentation secteur hors tension et ne retirez pas les câbles d'alimentation CA.

> **Remarque :**
>
> Vous ne pouvez pas arrêter une appliance via l'interface utilisateur graphique de NetScaler.

Comment synchroniser l'horloge système avec les serveurs du réseau

Vous pouvez configurer votre appliance NetScaler pour synchroniser son horloge locale avec un serveur NTP (Network Time Protocol). Cela garantit que son horloge dispose des mêmes paramètres de date et d'heure que les autres serveurs de votre réseau.

Vous pouvez configurer la synchronisation de l'horloge sur votre appliance en ajoutant des entrées de serveur NTP au fichier ntp.conf à partir de l'interface graphique ou de l'interface de ligne de commande, ou en modifiant manuellement le fichier ntp.conf, puis en démarrant le démon NTP (NTDP). La configuration de la synchronisation de l'horloge ne change pas si l'appliance est redémarrée, mise à niveau ou rétrogradée. Toutefois, la configuration n'est pas propagée vers le NetScaler secondaire dans une configuration haute disponibilité.

L'interface graphique de NetScaler vous permet de configurer le fuseau horaire et l'adresse IP du serveur NTP nécessaires à la synchronisation de l'horloge sur l'écran du premier utilisateur (FTU).

> **Remarque :**
>
> Si vous n'avez pas de serveur NTP local, vous pouvez trouver une liste des serveurs NTP publics en libre accès sur le site NTP officiel <http://www.ntp.org>, sous Liste des serveurs de temps publics. Avant de configurer votre NetScaler pour utiliser un serveur NTP public, veillez à lire la page Règles d'engagement (lien inclus sur toutes les pages des serveurs de temps publics).
>
> Dans la version 11 de NetScaler, la version NTP a été mise à jour de 4.2.6p3 à 4.2.8p2.

Prérequis

Pour configurer la synchronisation de l'horloge, vous devez configurer les entités suivantes :

1. Serveurs NTP
2. Synchronisation NTP.

Ajouter un serveur NTP à l'aide de l'interface de commande

À l'invite de commandes, tapez les commandes suivantes pour ajouter un serveur NTP et vérifier la configuration :

- `add ntp server (<serverIP> | <serverName>)[-minpoll <positive_integer>] [-maxpoll <positive_integer>]`
- `show ntp server`

Exemple :

```
add ntp server 10.102.29.30 -minpoll 6 -maxpoll 11
<!--NeedCopy-->
```

Ajouter un serveur NTP à l'aide de l'interface graphique

Accédez à **Système** > **Serveurs NTP**, puis créez le serveur NTP.

Activer la synchronisation NTP à l'aide de l'interface de commande

Lorsque vous activez la synchronisation NTP, NetScaler démarre le démon NTP et utilise les entrées du serveur NTP dans le fichier ntp.conf pour synchroniser ses paramètres d'heure locale. Si vous ne souhaitez pas synchroniser l'heure de l'appliance avec les autres serveurs du réseau, vous pouvez désactiver la synchronisation NTP, ce qui arrête le démon NTP (NTDP).

À l'invite de commandes, tapez l'une des commandes suivantes :

```
enable ntp sync
<!--NeedCopy-->
```

Activer la synchronisation NTP à l'aide de l'interface graphique

Accédez à **Système** > **Serveurs NTP**, cliquez sur **Action** et sélectionnez **Synchronisation NTP**.

Configurer la synchronisation de l'horloge pour modifier un fichier ntp.conf à l'aide de l'interface graphique

1. Ouvrez une session sur l'interface de ligne de commande.
2. Passez à l'invite du shell.
3. Copiez le fichier `/etc/ntp.conf` dans `/nsconfig/ntp.conf`, à moins que `/nsconfig directory` ne contienne déjà un fichier `ntp.conf`.
4. Pour chaque serveur NTP que vous souhaitez ajouter, vous devez ajouter les deux lignes suivantes au fichier `/nsconfig/ntp.conf`:

   ```
   server <IP address for NTP server> iburst

   restrict <IP address for NTP server> mask <netmask> nomodify
      notrap nopeer noquery
   <!--NeedCopy-->
   ```


> **Remarque :**
>
> Pour des raisons de sécurité, il devrait y avoir une entrée de restriction correspondante pour chaque entrée de serveur.

Exemple

Dans l'exemple suivant, un administrateur a inséré # caractères pour « commenter » une entrée NTP existante, puis a ajouté une entrée :

```
#server 1.2.3.4 iburst

#restrict 1.2.3.4 mask 55.255.255.255 nomodify notrap nopeer
    noquery

server 10.102.29.160 iburst

restrict 10.102.29.160 mask 255.255.255.255 nomodify notrap nopeer
     noquery
<!--NeedCopy-->
```

5. Si le répertoire /nsconfig ne contient pas de fichier nommé rc.netscaler, créez le fichier.
6. Ajoutez l'entrée suivante à /nsconfig/rc.netscaler: /bin/sh /etc/ntpd_ctl full_start

   Cette entrée démarre le service ntpd, vérifie le fichier ntp.conf et consigne les messages dans le répertoire /var/log.

   Ce processus s'exécute à chaque redémarrage de NetScaler.
7. Redémarrez l'appliance NetScaler pour activer la synchronisation de l'horloge. Ou, pour démarrer le processus de synchronisation de l'heure sans redémarrer l'appliance, entrez les commandes suivantes à l'invite de l'interpréteur de commandes :

```
rm /etc/ntp.conf
ln -s /nsconfig/ntp.conf /etc/ntp.conf
/bin/sh /etc/ntpd_ctl full_start
<!--NeedCopy-->
```

Comment configurer le délai d'expiration de session pour les connexions client inactives

Un intervalle d'expiration de session est fourni pour limiter la durée pendant laquelle une session (interface graphique, CLI ou API) reste active lorsqu'elle n'est pas utilisée. Pour NetScaler, le délai d'expiration de la session système peut être configuré aux niveaux suivants :

- **Délai d'expiration au niveau utilisateur.** Applicable à l'utilisateur spécifique.

Type d'interface	Configuration du délai d'exécution
GUI	Accédez à **Système > Administration des utilisateurs > Utilisateurs**, sélectionnez un utilisateur et modifiez le paramètre de délai d'expiration de l'utilisateur.
LIGNE DE COMMANDE	À l'invite de commandes, entrez la commande suivante : `set system user <name> -timeout <secs>`

- **Délai d'expiration de niveau groupe d'utilisateurs.** Applicable à tous les utilisateurs du groupe.

Type d'interface	Configuration du délai d'exécution
GUI	Accédez à **Système > Administration des utilisateurs > Groupes**, sélectionnez un groupe et modifiez le paramètre de délai d'expiration du groupe.
LIGNE DE COMMANDE	À l'invite de commande, entrez la commande suivante :`set system group <groupName> -timeout <secs>`

- **Délai d'expiration du système global.** Applicable à tous les utilisateurs et utilisateurs des groupes qui n'ont pas de délai d'expiration configuré.

Type d'interface	Configuration du délai d'exécution
GUI	Accédez à **Système > Paramètres**, cliquez sur **Modifier les paramètres système globaux** et mettez à jour la valeur du délai d'expiration si nécessaire.
LIGNE DE COMMANDE	À l'invite de commandes, entrez la commande suivante : `set system parameter -timeout <secs>`

La valeur de délai d'expiration spécifiée pour un utilisateur a la priorité la plus élevée. Si le délai

d'expiration n'est pas configuré pour l'utilisateur, le délai configuré pour un groupe membre est pris en compte. Si le délai d'expiration n'est pas spécifié pour un groupe (ou si l'utilisateur n'appartient pas à un groupe), la valeur de délai d'expiration configurée globalement est prise en compte. Si le délai d'expiration n'est configuré à aucun niveau, la valeur par défaut de 900 secondes est définie comme délai d'expiration de la session système.

En outre, vous pouvez spécifier des durées d'expiration pour chacune des interfaces auxquelles vous accédez. Toutefois, la valeur de délai d'expiration spécifiée pour une interface spécifique est limitée à la valeur de délai d'expiration configurée pour l'utilisateur qui accède à l'interface. Par exemple, considérons un utilisateur « publicadmin » dont le délai d'expiration est de 20 minutes. Désormais, lors de l'accès à une interface, l'utilisateur doit spécifier une valeur de délai d'expiration inférieure à 20 minutes.

> **Remarque :**
>
> Vous pouvez choisir de conserver une vérification des valeurs de délai minimum et maximum en spécifiant le délai d'expiration comme restreint (dans l'interface de ligne de commande, en spécifiant le paramètre *RestrictedTimeout*). Ce paramètre est fourni pour tenir compte des versions précédentes de NetScaler où la valeur du délai d'expiration n'était pas limitée.

- Lorsque cette option est activée, la valeur minimale du délai d'attente configurable est de 5 minutes (300 secondes) et la valeur maximale est de 1 jour (86400 secondes). Si la valeur du délai d'expiration est déjà configurée sur une valeur supérieure à 1 jour, lorsque ce paramètre est activé, vous êtes invité à le modifier. Si vous ne modifiez pas la valeur, la valeur du délai d'expiration sera automatiquement reconfigurée sur la durée d'expiration par défaut de 15 minutes (900 secondes) au prochain redémarrage. La même chose se produira si la valeur du délai d'expiration configurée est inférieure à 5 minutes.
- Lorsque cette option est désactivée, les durées d'expiration configurées sont prises en compte.
- **Durée du délai d'attente à chaque interface :**

Type d'interface	Configuration du délai d'exécution
LIGNE DE COMMANDE	Spécifiez la valeur du délai d'expiration sur l'invite de commande à l'aide de la commande suivante : `set cli mode -timeout <secs>`
API	Spécifiez la valeur du délai d'expiration dans la charge utile de connexion.

Comment régler la date et l'heure du système pour synchroniser l'horloge avec un serveur de temps

Pour modifier la date et l'heure du système, vous devez utiliser l'interface shell du système d'exploitation FreeBSD sous-jacent. Toutefois, pour afficher la date et l'heure du système, vous pouvez utiliser l'interface de ligne de commande ou l'interface graphique.

Afficher la date et l'heure du système à l'aide de l'interface de commande

À l'invite de commande, tapez :

```
1 show ns config
2 <!--NeedCopy-->
```

Afficher la date et l'heure du système à l'aide de l'interface graphique

Accédez à **Système** et sélectionnez l'onglet **Informations système** pour afficher la date système.

Comment configurer les ports de gestion HTTP et HTTPS pour les services internes

Dans un déploiement en mode IP unique d'une appliance NetScaler, une adresse IP unique est utilisée comme adresses NSIP, SNIP et VIP. Cette adresse IP unique utilise différents numéros de port pour fonctionner en tant qu'adresses NSIP, SNIP et VIP.

Les ports 80 et 443 sont des ports bien connus pour les services HTTP et HTTPS. Auparavant, les ports 80 et 443 de l'adresse IP NetScaler (NSIP) étaient des ports dédiés aux services de gestion HTTP et HTTPS internes. Ces ports étant réservés aux services internes, vous ne pouvez pas utiliser ces ports connus pour fournir des services de données HTTP et HTTPS à partir d'une adresse VIP, qui a la même adresse que l'adresse NSIP dans un déploiement en mode IP unique.

Pour répondre à cette exigence, vous pouvez désormais configurer des ports pour les services de gestion HTTP et HTTPS internes (de l'adresse NSIP) autres que les ports 80 et 443.

La liste suivante répertorie les numéros de port par défaut pour les services de gestion HTTP et HTTPS internes dans les appliances NetScaler MPX, VPX et CPX :

- Appliances NetScaler MPX et VPX : 80 (HTTP) et 443 (HTTPS)
- Appliances NetScaler CPX : 9080 (HTTP) et 9443 (HTTPS)

Configurez les ports de gestion HTTP et HTTPS à l'aide de l'interface de commande

Vous pouvez configurer un port HTTP et un port HTTPS sur n'importe quelle valeur sur l'appliance NetScaler afin de prendre en charge le service de gestion HTTP et HTTPS. Toutefois, par défaut, l'appliance NetScaler utilise 80 et 443 ports pour les connexions HTTP et HTTPS.

À l'invite de commande, tapez :

```
set ns param  - mgmtHttpPort<port>
<!--NeedCopy-->
```

Exemple :

```
set ns param -mgmtHttpPort 2000
<!--NeedCopy-->
```

Pour configurer un port HTTPS à l'aide de l'interface de commande

À l'invite de commande, tapez :

```
set ns param  - mgmtHttpsPort<port>
<!--NeedCopy-->
```

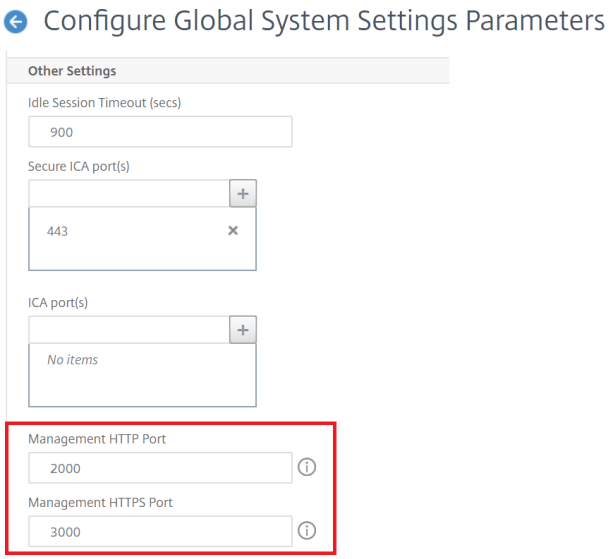
Exemple :

```
set ns param -mgmtHttpsPort 3000
<!--NeedCopy-->
```

Configurez les ports de gestion HTTP et HTTPS à l'aide de l'interface graphique

Suivez les étapes ci-dessous pour configurer les valeurs des ports HTTP et HTTPS :

1. Accédez à **Système** > **Paramètres** > **Modifier les paramètres globaux du système**.
2. Dans la page **Configurer les paramètres globaux du système**, sous la section **Autres** paramètres, définissez les paramètres suivants.
    a) Port HTTP de gestion. Définissez la valeur du port sur 2000. Par défaut = 80, Min = 1, Max = 65534.
    b) Port HTTPS de gestion. Définissez la valeur du port sur 3000. Par défaut = 443, Min = 1, Max = 65534.



Configurez le service d'interface graphique HTTP interne à l'aide de l'interface graphique NetScaler, de la CLI NetScaler ou des API NetScaler NITRO

Sur une appliance NetScaler, `/etc/httpd.conf` il s'agit du fichier de configuration du service d'interface graphique HTTP interne qui gère les connexions à l'interface graphique de NetScaler.

Au lieu d'utiliser le `httpd.conf` fichier pour configurer le service d'interface graphique HTTP interne, vous pouvez désormais utiliser l'interface graphique NetScaler, la CLI NetScaler ou les API NetScaler NITRO. Par exemple, vous pouvez utiliser l'interface de ligne de commande NetScaler pour modifier le nombre maximum de clients pouvant se connecter simultanément au service d'interface graphique HTTP interne.

Le service d'interface graphique HTTP interne a le format de nom suivant : **nshttpd-gui-<loop back IP address>-80**

Utilisez les opérations de commande du service NetScaler pour configurer le service d'interface graphique HTTP interne.

Pour modifier le service GUI HTTP interne à l'aide de l'interface de ligne de commande :

- Utilisez la commande `set service`. Pour plus d'informations, reportez-vous à la section Set Service.
- Utilisez la commande `show service` pour vérifier la configuration. Pour plus d'informations, voir Show Service.

Exemple de configuration :

Dans l'exemple de configuration suivant, le paramètre `maxClient` est défini sur 300 pour le service GUI HTTP interne.


```
> sh service nshttpd-gui-127.0.0.1-80
                nshttpd-gui-127.0.0.1-80 (127.0.0.1:80) - HTTP
                State: UP
                Last state change was at Wed Mar 16 20:16:16 2022
                Time since last state change: 0 days, 22:31:00.970
                Server Name: #ns-internal-127.0.0.1#
                Server ID : None                Monitor Threshold : 0
                Max Conn: 0       Max Req: 0          Max Bandwidth: 0
                   kbits
                Use Source IP: NO
                Client Keepalive(CKA): NO
                Monitoring Owner: 0
                Access Down Service: NO
                TCP Buffering(TCPB): NO
                HTTP Compression(CMP): NO
                Idle timeout: Client: 180 sec        Server: 360 sec
                Client IP: ENABLED cip-header
                Cacheable: NO
                SC: ???
                SP: OFF
                Down state flush: DISABLED
                Monitor Connection Close : NONE
                Appflow logging: DISABLED
                TCP profile name: nstcp_internal_apps
                HTTP profile name: nshttp_default_internal_apps
                Process Local: DISABLED
                Traffic Domain: 0

Done

> set service nshttpd-gui-127.0.0.1-80 -maxclient 300
Done

> sh service nshttpd-gui-127.0.0.1-80
                nshttpd-gui-127.0.0.1-80 (127.0.0.1:80) - HTTP
                State: UP

                ...

                Max Conn: 300  Max Req: 0          Max Bandwidth: 0
                   kbits

                ...

```



```
43 Done
44
45 <!--NeedCopy-->
```

Déclenchez une restauration de mémoire à l'aide de l'interface

Vous pouvez déclencher une récupération de mémoire à partir de l'interface de ligne de commande.

À l'invite de commandes, tapez la commande suivante :

```
start ns memrecovery [-percentage <positive_integer>]
```

Exemple :

```
start nsmemrecovery -percentage 30
```

Pour vérifier la quantité réelle de mémoire récupérée, utilisez la commande suivante à l'invite de commandes :

```
stat system memory
```

Comment allouer un processeur de gestion supplémentaire pour le traitement et la surveillance des données

Si vous avez besoin de meilleures performances pour la configuration et la surveillance d'une appliance NetScaler MPX, vous pouvez allouer un processeur de gestion supplémentaire à partir du pool de moteurs de paquets de l'appliance. Cette fonctionnalité est prise en charge sur certains modèles NetScaler MPX et sur tous les modèles VPX à l'exception des instances VPX qui s'exécutent sur des appliances NetScaler SDX. Il affecte la sortie de la CPU du système stat et des commandes du système stat.

Modèles NetScaler MPX pris en charge :

- 25xxx
- 22xxx
- 14xxx
- 115xx
- 15xxx
- 26xxx

> **Remarque :**
>
> Pour les modèles NetScaler MPX 26xxx dotés de plus de 20 cœurs, la fonctionnalité de processeur de gestion supplémentaire obligatoire est activée par défaut. Pour les modèles NetScaler VPX,

> une licence prenant en charge au moins 12 processeurs virtuels est requise pour activer cette fonctionnalité.

Allouez un processeur de gestion supplémentaire à l'aide de l'interface de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `enable extramgmtcpu`
- `disable extramgmtcpu`

> **Remarque :**
>
> Une fois que vous avez activé et désactivé cette fonctionnalité, l'appliance NetScaler affiche un avertissement vous invitant à redémarrer l'appliance pour que les modifications prennent effet.

Pour afficher l'état configuré et effectif d'un processeur de gestion supplémentaire.

À l'invite de commande, tapez :

```
1 show extramgmtcpu
2 <!--NeedCopy-->
```

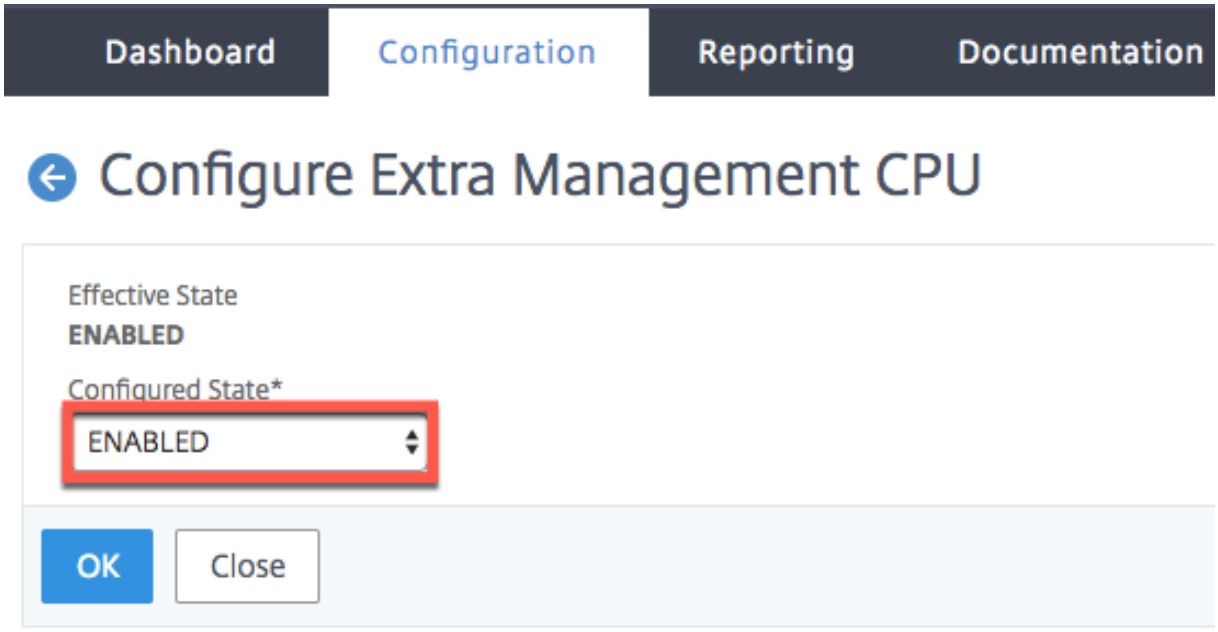
Exemple :

```
1 > show extramgmtcpu
2 ConfiguredState:  ENABLED EffectiveState:  ENABLED
3 <!--NeedCopy-->
```

> **Remarque :**
>
> Dans cet exemple, la commande show est entrée avant le redémarrage de l'appliance.

Allouez un processeur de gestion supplémentaire à l'aide de l'interface graphique

Pour allouer un processeur de gestion supplémentaire à l'aide de l'interface graphique, accédez à **Système** > **Paramètres** et cliquez sur **Configurer le processeur de gestion supplémentaire**. Dans le menu déroulant **État configuré**, sélectionnez **Activé**, puis **OK**.



Pour vérifier l'utilisation du processeur, accédez à **Système** > **Paramètres** > **Tableau de bord**.

Configurez un processeur de gestion supplémentaire à l'aide de l'API NITRO

Utilisez les méthodes et formats NITRO suivants pour activer, désactiver et afficher un processeur de gestion supplémentaire.

Pour activer un processeur de gestion supplémentaire, procédez comme suit :

```
HTTP Method: POST

URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=enable

Payload: {
 "systemextramgmtcpu":{
  }
  }


curl -v -X POST -H "Content-Type: application/json" -u nsroot:nsroot
   http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=
   enable -d '{
 "systemextramgmtcpu":{
  }
  }
 '
<!--NeedCopy-->
```


Pour désactiver un processeur de gestion supplémentaire

```
HTTP Method: POST
URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=disable
Payload: {
 "systemextramgmtcpu":{
  }
  }

curl -v -X POST -H "Content-Type: application/json" -u nsroot:nsroot
    http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=
    disable -d '{
 "systemextramgmtcpu":{
  }
  }
 '
<!--NeedCopy-->
```

Pour afficher un processeur de gestion supplémentaire

```
HTTP Method: GET
URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu
<!--NeedCopy-->
```

Exemple :

```
curl -v -X GET -H "Content-Type: application/json" -u nsroot:nsroot
    http://10.102.201.92/nitro/v1/config/systemextramgmtcpu
<!--NeedCopy-->
```

Statistiques et surveillance avant et après l'ajout d'un processeur de gestion supplémentaire

Les exemples suivants montrent les différences entre la sortie des commandes CPU et stat system avant et après l'ajout d'un processeur de gestion supplémentaire.

```
stat system cpu
<!--NeedCopy-->
```

Cette commande affiche les statistiques des processeurs.

Voici un exemple de sortie avant d'ajouter un processeur de gestion supplémentaire sur l'un des modèles pris en charge.

Exemple


```
> stat system cpu

    CPU statistics

    ID         Usage

    8              1

    7              1

    11             2

    1              1

    6              1

    9              1

    3              1

    5              1

    4              1

    10             1

    2              1
<!--NeedCopy-->
```

Voici la sortie après l'ajout d'un processeur de gestion supplémentaire sur le même appareil MPX.

```
    > stat system cpu

    CPU statistics

    ID         Usage

    9              1

    7              1

    5              1

    8              1
```



```
14
15      11              2
16
17      10              1
18
19      6               1
20
21      4               1
22
23      3               1
24
25      2               1
26  <!--NeedCopy-->
```

```
1  stat system
2  <!--NeedCopy-->
```

Cette commande affiche l'utilisation du processeur. Dans l'exemple suivant, la sortie avant l'ajout d'un processeur de gestion supplémentaire sur l'un des modèles pris en charge est la suivante :

Gestion de l'utilisation supplémentaire du processeur (%) 0.00

Exemple

```
1      > stat system
2
3      NetScaler Executive View
4
5      System Information:
6
7      Up since         Wed Oct 11 11:17:54 2017
8
9      /flash Used (%)                          0
10
11     Packet CPU usage (%)                  1.30
12
13     Management CPU usage (%)              4.00
14
15     Mgmt CPU0 usage (%)                   4.00
16
17     Mgmt Additional-CPU  usage (%)        0.00
18
19     Memory usage (MB)                     2167
20
21     InUse Memory (%)                      5.76
```



```
22
23     /var Used (%)                          0
24 <!--NeedCopy-->
```

Dans l'exemple suivant, la sortie après l'ajout d'un processeur de gestion supplémentaire sur la même appliance MPX est :

Gestion de l'utilisation supplémentaire du processeur (%) 0,80

```
1  > stat system
2
3
4  NetScaler Executive View
5
6  System Information:
7
8  Up since        Wed Oct 11 11:55:56 2017
9
10 /flash Used (%)                        0
11
12 Packet CPU usage (%)                1.20
13
14 Management CPU usage (%)            5.70
15
16 Mgmt CPU0 usage (%)                10.60
17
18 Mgmt Additional-CPU  usage (%)      0.80
19
20 Memory usage (MB)                   1970
21
22 InUse Memory (%)                    5.75
23
24 /var Used (%)                          0
25
26 <!--NeedCopy-->
```

Comment faire pour sauvegarder et restaurer votre appliance pour récupérer la configuration perdue

Lorsque votre appliance est corrompue ou nécessite une mise à niveau, vous pouvez sauvegarder la configuration de votre système. La procédure de sauvegarde s'effectue via l'interface CLI ou GUI. l'appliance vous permet également d'importer le fichier de sauvegarde à partir d'une source externe. Toutefois, vous ne pouvez le faire que via l'interface graphique et il n'y a pas de prise en charge via l'interface CLI.

Points à retenir

Vous devez vous souvenir des points suivants lorsque vous sauvegardez et restaurez votre appliance.

- La configuration réseau doit être prise en charge sur une nouvelle plate-forme.
- La nouvelle version de la plate-forme doit être identique au fichier de sauvegarde ou à une version ultérieure.

Sauvegarder une appliance NetScaler

Selon les besoins en matière de données et de sauvegarde, vous pouvez créer une sauvegarde « de base » ou une sauvegarde « complète ».

- **Sauvegarde de base.** Vous pouvez effectuer ce type de sauvegarde si vous souhaitez sauvegarder des fichiers qui changent constamment. Les fichiers que vous pouvez sauvegarder se trouvent dans le tableau suivant.

Pour plus d'informations sur les détails de base de la sauvegarde, reportez-vous à la rubrique Tableau
.

- **Sauvegarde complète.** En plus des fichiers sauvegardés par une sauvegarde de base, une sauvegarde complète contient moins de fichiers mis à jour. Les fichiers qui sont sauvegardés lorsque vous utilisez l'option de sauvegarde « complète » sont les suivants :

Répertoire	Sous-répertoire ou fichiers
nsconfig	ssl*, licence*, fips*
/var/	netscaler/ssl/*, wi/java_home/jre/lib/security/cacerts/*, wi/java_home/lib/security/cacerts/*

Les données sauvegardées sont stockées sous forme de fichier TAR compressé dans le répertoire `/var/ns_sys_backup/`. Pour éviter les problèmes dus à l'indisponibilité de l'espace disque, vous pouvez stocker jusqu'à 50 fichiers de sauvegarde dans ce répertoire. Vous pouvez utiliser la commande `rm system backup` pour supprimer les fichiers de sauvegarde existants et créer d'autres sauvegardes.

> **Remarque :**
>
> Lorsque l'opération de sauvegarde est en cours, n'exécutez pas de commandes qui affectent la configuration.
>
> Si un fichier qui doit être sauvegardé n'est pas disponible, l'opération ignore ce fichier.

Sauvegarder une appliance NetScaler à l'aide de l'interface de commande

Suivez la procédure ci-dessous pour sauvegarder une appliance NetScaler à l'aide de l'interface de commande NetScaler.

À l'invite de commandes, procédez comme suit :

1. Enregistrez les configurations NetScaler.

```
save ns config
<!--NeedCopy-->
```

1. Créez le fichier de sauvegarde.

```
create system backup [<fileName>] -level <basic | full> -comment <
   string>
<!--NeedCopy-->
```

> **Remarque :**
>
> Si le nom de fichier n'est pas spécifié, l'appliance crée un fichier TAR avec la convention de dénomination suivante :`backup_<level>_<nsip_address>_<date-timestamp>.tgz`.

Exemple : Pour sauvegarder l'appliance complète à l'aide de la convention de dénomination par défaut pour le fichier de sauvegarde.

```
> create system backup -level full
<!--NeedCopy-->
```

1. Vérifiez que le fichier de sauvegarde a été créé.

```
show system backup
<!--NeedCopy-->
```

Vous pouvez afficher les propriétés d'un fichier de sauvegarde spécifique à l'aide du paramètre `fileName`.

Restaurez une appliance NetScaler à l'aide de l'interface de commande

> **Important :**
>
> Vous ne pouvez pas restaurer votre appliance si vous renommez ou modifiez votre fichier de sauvegarde.

Lorsque vous restaurez votre appliance, l'opération de restauration dézippe le fichier de sauvegarde du répertoire `/var/ns_sys_backup/`. Une fois que les fichiers ne sont pas enregistrés, ils sont copiés dans les répertoires respectifs.

Restaurez le NetScaler à partir d'un fichier de sauvegarde local à l'aide de l'interface de commande

> **Remarque :**
>
> Citrix vous recommande de sauvegarder la configuration actuelle avant de restaurer une configuration précédente. Toutefois, si vous ne souhaitez pas que la commande de restauration crée automatiquement une sauvegarde de la configuration actuelle, utilisez le paramètre `-skipBackup`.

À l'invite de commandes, procédez comme suit :

1. Obtenez la liste des fichiers de sauvegarde disponibles sur l'appliance.

```
show system backup
<!--NeedCopy-->
```

2. Restaurez l'appliance en spécifiant l'un des fichiers de sauvegarde.

```
restore system backup <filename> [-skipBackup]
```

Exemple : Pour effectuer une restauration à l'aide d'une sauvegarde complète d'une appliance

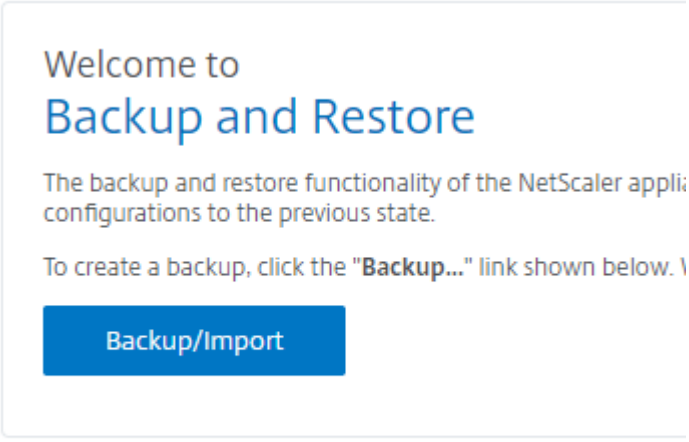
```
> restore system backup backup_full_<nsip_address>_<date-timestamp>.tgz
```

3. Redémarrez l'appliance.

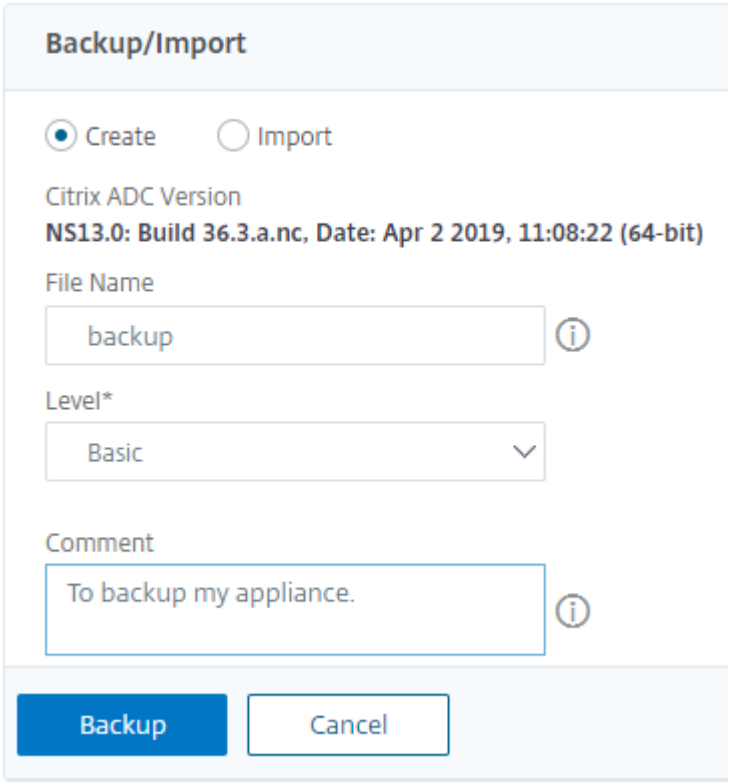
```
reboot
```

Sauvegarde et restauration d'une appliance NetScaler à l'aide de l'interface graphique

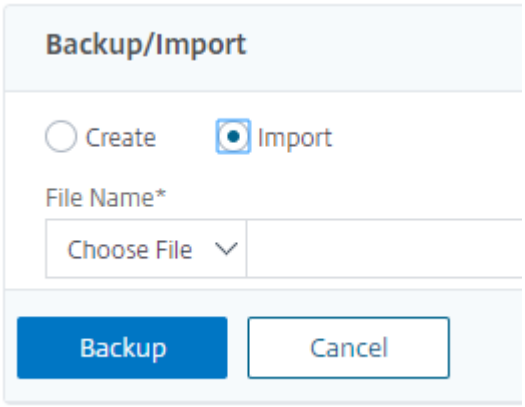
1. Accédez à **Système** > **Sauvegarde et restauration**.



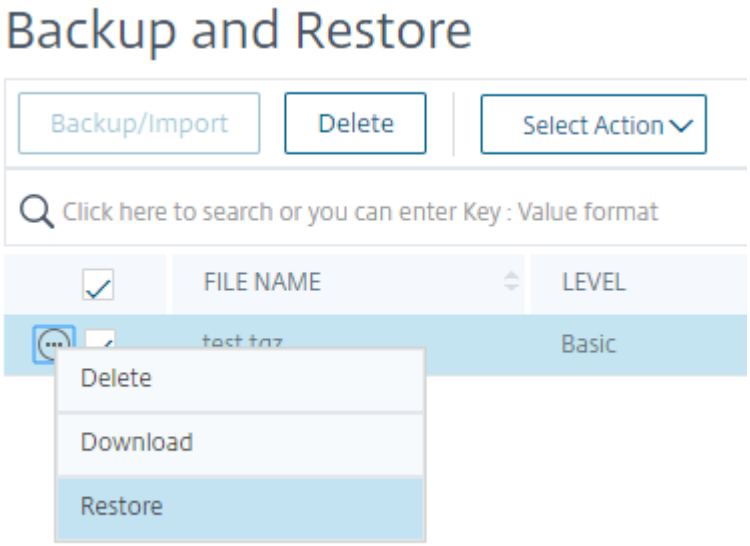
2. Cliquez sur **Sauvegarde/Importer** pour démarrer le processus.
3. Dans la page **Sauvegarde/Importation**, sélectionnez **Créer** et définissez les paramètres suivants.
   a) Nom du fichier. Nom du fichier de sauvegarde de l'appliance.
   b) Niveau. Sélectionnez un niveau de sauvegarde de base ou complet.
   c) Commentaire. Fournissez une brève description de la sauvegarde.
4. Cliquez sur **Sauvegarde**.



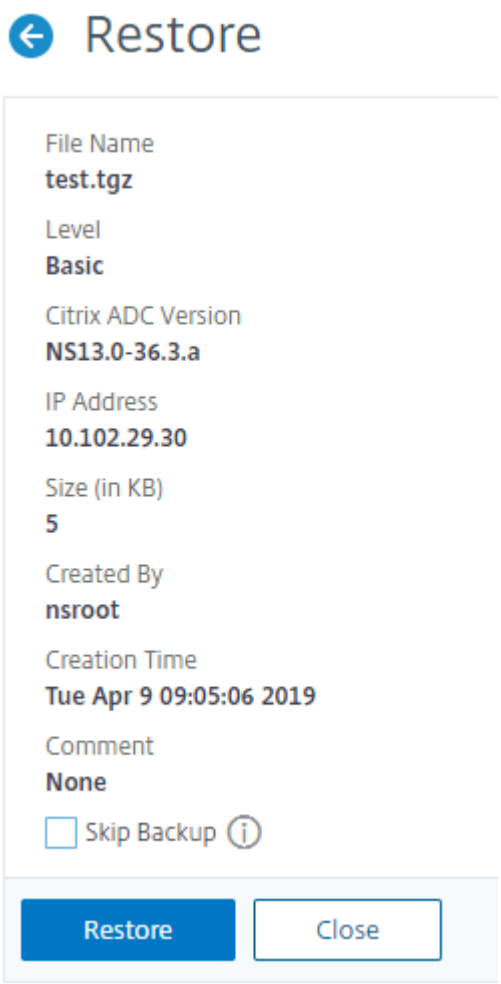
5. Si vous souhaitez importer une sauvegarde, vous devez sélectionner **Importer**.



6. Une fois la sauvegarde terminée, vous pouvez sélectionner le fichier et cliquer sur **Télécharger**.
7. Pour restaurer, sélectionnez le fichier de sauvegarde et cliquez sur **Restaurer**.



8. Dans la page **Restaurer**, vérifiez les détails du fichier de sauvegarde et cliquez sur **Restaurer**.



9. Après la restauration, vous devez redémarrer l'appliance.

Pour plus d'informations sur la façon de sauvegarder et de restaurer des instances NetScaler, consultez la rubrique Sauvegarde et restauration à l'aide de NetScaler ADM.

Pour plus d'informations sur la sauvegarde et la restauration d'une appliance SDX, voir Sauvegarde et restauration de l'appliance SDX

Pour plus d'informations sur les opérations effectuées sur la sauvegarde système, reportez-vous à la rubrique Sauvegarde système .

Comment générer un ensemble de support technique pour résoudre les problèmes liés à l'appliance

Pour vous aider à analyser et à résoudre les problèmes liés à une appliance NetScaler, vous pouvez générer un bundle de support technique sur l'appliance et l'envoyer au support technique de Citrix. Le bundle de support technique NetScaler est une archive tar compressée contenant des données

de configuration système et des statistiques. Il collecte les données suivantes à partir de l'appliance NetScaler sur laquelle vous générez le bundle :

- **Fichiers de configuration**. Tous les fichiers du répertoire /flash/nsconfig.
- **Fichiers Newnslog**. Le newnslog actuellement en cours d'exécution et certains fichiers précédents. Pour réduire la taille du fichier d'archive, la collection `newnslog` est limitée à 500 Mo, 6 fichiers ou 7 jours, selon la première éventualité. Si des données plus anciennes sont nécessaires, elles peuvent nécessiter une collecte manuelle.
- **Fichiers journaux**. Fichiers dans /var/log/messages , */var/log/ns.log* et d'autres fichiers sous /var/log et /var/nslog.
- **Fichiers principaux de l'application**. Fichiers créés dans le répertoire /var/core au cours de la dernière semaine, le cas échéant.
- **Sortie de certaines commandes d'affichage de l'interface de ligne de commande**.
- **Sortie de certaines commandes de statistiques de l'interface de ligne de commande**.
- **Sortie des commandes du shell BSD**.

Vous pouvez utiliser une seule commande pour générer le bundle de support technique et le télécharger en toute sécurité sur le serveur de support technique Citrix. Pour effectuer le chargement, vous devez spécifier vos informations d'identification Citrix. Lorsque vous générez le bundle, vous pouvez spécifier le numéro de dossier ou de demande de service qui vous a été attribué par le support technique de Citrix. Si vous avez déjà généré un bundle de support technique, vous pouvez télécharger le fichier d'archive existant sur le serveur de support technique Citrix en spécifiant le nom du fichier avec le chemin complet.

Le bundle de support technique est enregistré sur l'appliance NetScaler dans une archive à l'emplacement suivant :

```
1 /var/tmp/support/support.tgz
2 <!--NeedCopy-->
```

Le chemin est un lien symbolique vers le collecteur le plus récent pour un accès facile. Le nom complet du fichier varie en fonction de la topologie de déploiement, mais il suit généralement un format similaire à :

```
1 collector_<P/S>\_<NS IP>\_<DateTime>.tgz.
2 <!--NeedCopy-->
```

Si votre appliance NetScaler ne dispose pas d'une connectivité Internet directe, vous pouvez utiliser un serveur proxy pour télécharger directement le bundle de support technique sur le serveur de support technique Citrix. Le format de base de la chaîne de proxy est le suivant :

```
1 proxy_IP:<proxy_port>
2 <!--NeedCopy-->
```


Si le serveur proxy nécessite une authentification, le format est le suivant :

```
username:password@proxsy_IP:<proxy_port>
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour les appliances NetScaler faisant partie d'une paire haute disponibilité, vous devez générer le bundle de support technique sur chacun des deux nœuds.
>
> Pour les appliances NetScaler dans une configuration en cluster, vous pouvez générer le bundle de support technique sur chaque nœud individuellement, ou vous pouvez générer des archives abrégées plus petites pour tous les nœuds à l'aide de l'adresse IP du cluster.
>
> Pour les partitions d'administration NetScaler, vous devez générer le bundle de support technique à partir de la partition d'administration par défaut. Pour obtenir le bundle de support technique pour une partition spécifique, vous devez spécifier le nom de la partition pour laquelle vous souhaitez générer le bundle de support technique. Si vous ne spécifiez pas le nom de la partition, les données sont collectées à partir de toutes les partitions d'administration.

Générez le bundle de support technique NetScaler à l'aide de l'interface de commande

À l'invite de commande, tapez :

```
show techsupport [-scope <scope> <partitionName>] [-upload [-proxy <
    string>] [-casenumber <string>] [-file <string>] [-description <
    string>] [-userName <string> -password ]]
<!--NeedCopy-->
```

Sr. Non	Tâche	Commande
1	Générez et téléchargez le bundle de support technique sur le serveur de support technique Citrix.	show techsupport –upload –userName account1 –password xxxxxxx
2	Générez et téléchargez le bundle de support technique sur le serveur de support technique Citrix via un serveur proxy	show techsupport –upload –proxy 1.1.1.1:80 –userName account1 –password xxxxxxx

Sr. Non	Tâche	Commande
3	Téléchargez un bundle de support technique existant sur le serveur de support technique Citrix.	show techsupport –upload -file,/var/tmp/support/collector_P_10.102.29. –userName account1 –password xxxxxxx
4	Générez de petites archives abrégées pour tous les nœuds d'une configuration de cluster. Exécutez cette commande à l'aide de l'adresse IP du cluster	show techsupport –scope CLUSTER
5	Générez un bundle de support technique spécifique à une partition d'administration. Exécutez cette commande sur la partition d'administration par défaut.	show techsupport –scope PARTITION partition1

Comment collecter le pack de support technique des appliances SDX et VPX pour une analyse des informations

Une appliance NetScaler possède un mécanisme intégré pour collecter les fichiers journaux. Les fichiers journaux sont à leur tour envoyés à Citrix Insight Services pour analyse.

> **Remarque :**
>
> Toutes les procédures s'appliquent à la version logicielle 9.2 ou ultérieure.

Téléchargez le bundle de support technique à partir des appliances NetScaler MPX et VPX

Pour exécuter un fichier collecteur à l'aide de l'interface graphique NetScaler, vous devez suivre la procédure suivante :

> **Remarque :**
>
> La procédure s'applique à la version logicielle 9.2 ou ultérieure.

1. Accédez à **Système** > **Diagnostic**.

2. Dans la section **Outils de support technique**, cliquez sur le lien **Générer un fichier de support** .
3. Dans la page **Support technique**, définissez les paramètres suivants :
   a) Portée. Pour collecter des données à partir d'un ou de plusieurs nœuds.
   b) Cloison. Nom de la partition.
   c) Options de chargement du support technique Citrix. Définissez toutes les options telles que le serveur proxy, le numéro de dossier de service, le nom du fichier d'archive du collecteur et une brève description du fichier d'archive pour le téléchargement du pack de support technique.
   d) Compte Citrix. Entrez vos informations d'identification Citrix.
4. Cliquez sur **Exécuter**.
5. Le pack de support technique est généré.
6. Cliquez sur **Oui** pour télécharger le pack de support technique sur votre bureau local.

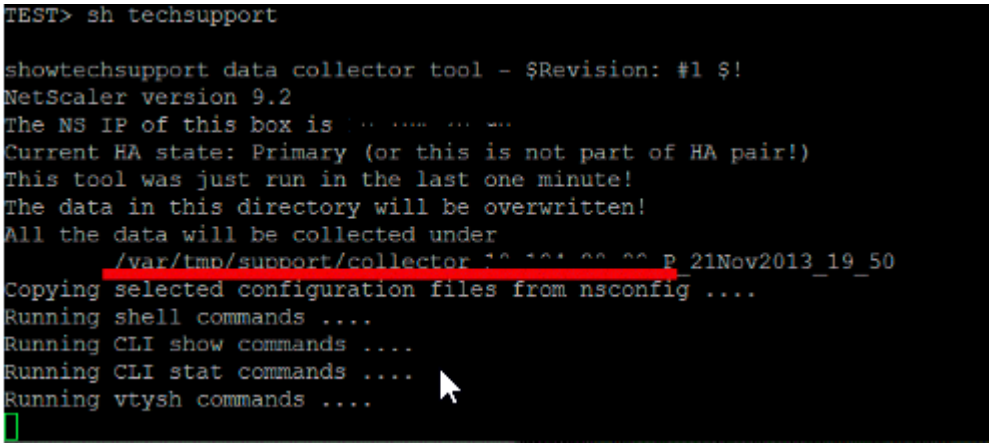
Obtenez le pack de support technique à l'aide de l'interface de commande

1. Téléchargez le fichier à partir de l'appliance à l'aide d'un utilitaire Secure FTP (SFTP) ou Secure Copy (SCP) `WinSCP`, par exemple, et téléchargez-le sur Citrix Insight Services pour analyse.

> **Remarque :**
>
> Dans les versions du logiciel NetScaler antérieures à 9.0, le script du collecteur doit être téléchargé séparément et exécuté.

```
1 > show techsupport -scope CLUSTER
2 <!--NeedCopy-->
```

1. Cette opération collecte les informations de support technique de tous les nœuds du cluster et compresse les fichiers dans une seule archive.
2. Une fois que l'appliance a généré l'archive du collecteur, l'emplacement du fichier s'affiche comme illustré dans la capture d'écran suivante.



Le fichier est stocké dans `/var/tmp/support` et vous pouvez le vérifier en vous connectant à un dispositif NetScaler et en exécutant la commande suivante à partir d'une invite de shell.

```
root@NS# cd /var/tmp/support/
root@NS# ls -l
<!--NeedCopy-->
```

Obtenir un bundle de diagnostic auprès de NetScaler SDX à l'aide de l'interface graphique

1. Ouvrez l'interface graphique de NetScaler SDX.
2. Développez le nœud **Diagnostics** .
3. Sélectionnez le nœud **Support technique** .
4. Cliquez sur Générer un fichier de support technique.
5. Sélectionnez **Appliance** (y compris les instances) dans le menu déroulant.
6. Cliquez sur **Ajouter**.
7. Sélectionnez une ou plusieurs instances à ajouter.
8. Cliquez sur **OK**. Attendez que le processus soit terminé.
9. Sélectionnez le nom du bundle qui a été généré, puis cliquez sur **Télécharger**
10. Téléchargez le fichier groupé sur Citrix Insight Services.

Plus de ressources

Regarder une vidéo

Lire un autre sujet

Doc de référence de commande

Authentification et autorisation des utilisateurs du système

May 5, 2023

Pour configurer l'authentification et l'autorisation des utilisateurs NetScaler, vous devez d'abord définir les utilisateurs qui ont accès à l'appliance NetScaler, puis vous pouvez organiser ces utilisateurs en groupes. Après avoir configuré les utilisateurs et les groupes, vous devez configurer les politiques de commande pour définir les types d'accès et attribuer les politiques aux utilisateurs et/ou aux groupes.

Vous devez vous connecter en tant qu'administrateur pour configurer les utilisateurs, les groupes et les politiques de commande. *Le nom d'utilisateur de l'administrateur NetScaler par défaut est nsroot.* Une fois connecté en tant qu'administrateur par défaut, vous devez modifier le mot de passe du compte nsroot. Une fois que vous avez modifié le mot de passe, aucun utilisateur ne peut accéder à l'appliance NetScaler tant que vous n'avez pas créé un compte pour cet utilisateur. Si vous oubliez le mot de passe administrateur après l'avoir modifié par rapport au mot de passe par défaut, vous pouvez le réinitialiser sur nsroot.

> **Remarque :**
>
> - Les utilisateurs locaux peuvent s'authentifier auprès de NetScaler même si des serveurs d'authentification externes sont configurés. Vous pouvez limiter cela en désactivant le paramètre localAuth de la commande set system parameter.
> - Pour une sécurité renforcée, Citrix vous recommande de modifier le mot de passe nsroot. Il est conseillé de changer fréquemment le mot de passe. Pour plus d'informations sur la modification du mot de passe nsroot, reportez-vous à la rubrique Réinitialisation du mot de passe administrateur par défaut (nsroot) .

Utilisateurs, groupes d'utilisateurs et stratégies de commande

May 5, 2023

Vous devez d'abord définir un utilisateur avec un compte, puis organiser tous les utilisateurs en groupes. Vous pouvez créer des stratégies de commande ou utiliser des stratégies de commande

intégrées pour réguler l'accès des utilisateurs aux commandes.

> **Remarque :**
>
> Si vous préférez en savoir plus sur la configuration des utilisateurs et des groupes d'utilisateurs dans le cadre de la configuration de l'authentification et des autorisations NetScaler pour la gestion du trafic, consultez la rubrique Configurer les utilisateurs et les groupes .

Vous pouvez également personnaliser l'invite de ligne de commande pour un utilisateur. Les invites peuvent être définies dans la configuration d'un utilisateur, dans la configuration d'un groupe d'utilisateurs et dans les paramètres de configuration globale du système. L'invite qui s'affiche pour un utilisateur est présentée dans l'ordre de priorité suivant :

1. Affichez l'invite telle que définie dans la configuration de l'utilisateur.
2. Affichez l'invite telle que définie dans la configuration du groupe de l'utilisateur.
3. Affichez l'invite telle que définie dans les paramètres de configuration globale du système.

Vous pouvez désormais spécifier une valeur de délai pour les sessions CLI inactives pour un utilisateur du système. Si la session CLI d'un utilisateur est inactive pendant une durée supérieure à la valeur du délai d'expiration, l'appliance NetScaler met fin à la connexion. Le délai d'expiration peut être défini dans une configuration utilisateur, dans une configuration de groupe d'utilisateurs ou dans les paramètres de configuration système globaux. Le délai d'expiration des sessions CLI inactives pour un utilisateur est déterminé dans l'ordre de priorité suivant :

1. Configuration utilisateur.
2. Configuration du groupe pour le groupe de l'utilisateur.
3. Paramètres de configuration système globaux.

Un administrateur root NetScaler peut configurer la limite maximale de sessions simultanées pour les utilisateurs du système. En limitant cette limite, vous pouvez réduire le nombre de connexions ouvertes et améliorer les performances du serveur. Tant que le nombre de CLI se situe dans la limite configurée, les utilisateurs simultanés peuvent se connecter à l'interface graphique autant de fois que nécessaire. Toutefois, si le nombre de sessions CLI atteint la limite configurée, les utilisateurs ne peuvent plus se connecter à l'interface graphique. Par exemple, si le nombre de sessions simultanées est configuré sur 20, les utilisateurs simultanés peuvent se connecter à 19 sessions CLI. Mais si l'utilisateur est connecté à la session CLI `20<sup>th</sup>`, toute tentative de connexion à l'interface graphique, à la CLI ou à NITRO entraîne un message d'erreur (ERREUR : limite de connexion au CFE dépassée).

> **Remarque :**
>
> Par défaut, le nombre de sessions simultanées est configuré sur 20 et le nombre maximum de sessions simultanées est configuré sur 40.

Configurer les comptes utilisateur

Pour configurer les comptes utilisateur, il vous suffit de spécifier des noms d'utilisateur et des mots de passe. Vous pouvez modifier les mots de passe et supprimer des comptes utilisateur à tout moment.

> **Remarque :**
>
> Tous les caractères d'un mot de passe ne sont pas acceptés. Toutefois, cela fonctionne si vous tapez les caractères entre guillemets.
>
> De plus, la chaîne ne doit pas dépasser une longueur maximale de 127 caractères.

Pour créer un compte utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un compte utilisateur et vérifier la configuration :

- `add system user <username> [-externalAuth ( ENABLED | DISABLED )] [-promptString <string>] [-timeout \<secs>] [-logging ( ENABLED | DISABLED )] [-maxsession <positive_integer>]`
- `show system user <userName>`

Les utilisateurs externes peuvent configurer le paramètre « journalisation » pour collecter des journaux externes à l'aide d'un mécanisme de journalisation Web ou d'audit. Si le paramètre est activé, le client d'audit s'authentifie auprès de l'appliance NetScaler pour collecter des journaux.

Exemple :

```
> add system user johnd -promptString user-%u-at-%T
```

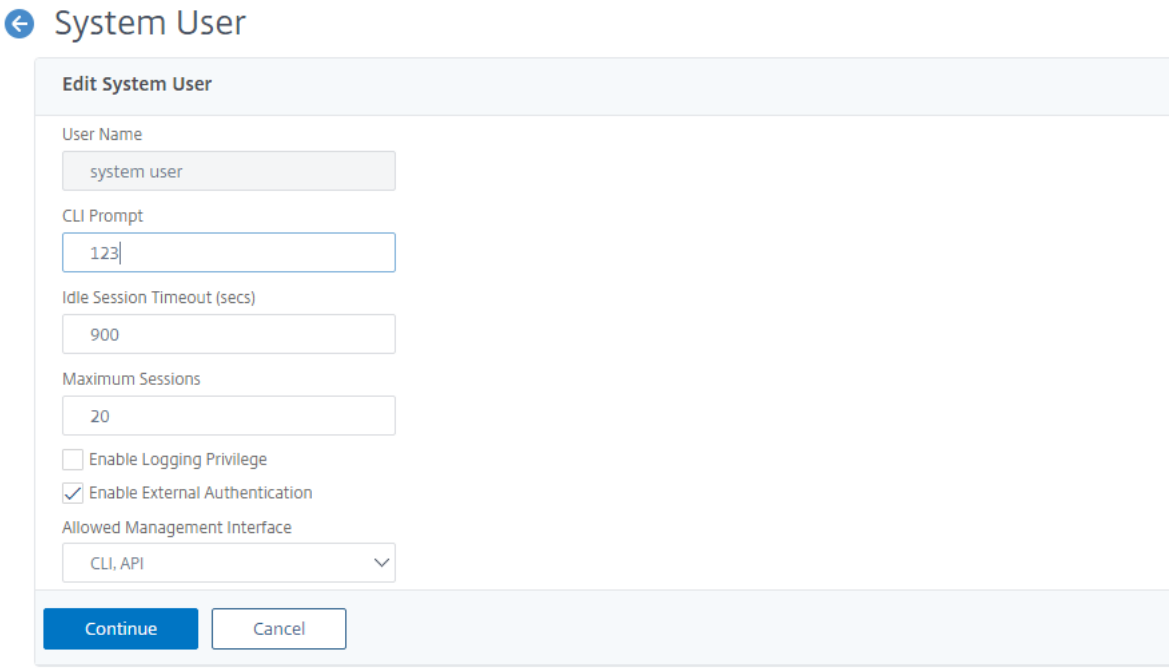
```
1 Enter password:
2 Confirm password:
3 > show system user johnd
4 user name: john
5      Timeout:900 Timeout Inherited From: Global
6      External Authentication: ENABLED
7      Logging: DISABLED
8      Maximum Client Sessions: 20
9 <!--NeedCopy-->
```

Pour la description des paramètres, reportez-vous à la rubrique Référence de la commande utilisateur Authentification et autorisation .

Configurer un compte utilisateur à l'aide de l'interface graphique NetScaler

1. Accédez à **Système** > **Administration** des **utilisateurs > Utilisateurs**, puis créez l'utilisateur.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour créer un utilisateur système.

3. Sur la page **Créer un groupe de systèmes**, définissez les paramètres suivants :
   a) Nom d'utilisateur. Nom du groupe d'utilisateurs.
   b) Invite CLI. L'invite que vous préférez définir pour l'accès à l'interface CLI.
   c) Délai d'expiration de la session inactive (secondes). Définissez la durée pendant laquelle un utilisateur peut rester inactif avant l'expiration et la fermeture de la session.
   d) Nombre maximum de sessions. Définissez le nombre maximum de sessions qu'un utilisateur peut essayer.
   e) Activez le privilège de journalisation. Activez le privilège de journalisation pour l'utilisateur.
   f) Activez l'authentification externe. Sélectionnez cette option si vous souhaitez utiliser un serveur d'authentification externe pour authentifier l'utilisateur.
   g) Interface de gestion autorisée. Sélectionnez les interfaces NetScaler auxquelles le groupe d'utilisateurs est autorisé à accéder.
   h) Stratégies de commande. Liez les stratégies de commande au groupe d'utilisateurs.
   i) Partitions. Liez les partitions au groupe d'utilisateurs.
4. Cliquez sur **Créer** et **Fermer**.



Configuration de groupes d'utilisateurs

Après avoir configuré un groupe d'utilisateurs, vous pouvez facilement accorder les mêmes droits d'accès à tous les membres du groupe. Pour configurer un groupe, vous devez le créer et y lier des utilisateurs. Vous pouvez associer chaque compte utilisateur à plusieurs groupes. La liaison de comptes

utilisateur à plusieurs groupes peut permettre une plus grande flexibilité lors de l'application des stratégies de commande.

Pour créer un groupe d'utilisateurs à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour créer un groupe d'utilisateurs et vérifier la configuration :

- `add system group <groupName> [-promptString <string>] [-timeout <secs>]`
- `show system group <groupName>`

Exemple :

```
> add system group Managers -promptString Group-Managers-at-%h
```

Lier un compte utilisateur à un groupe à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier un compte utilisateur à un groupe et vérifier la configuration :

- `bind system group <groupName> -userName <userName>`
- `show system group <groupName>`

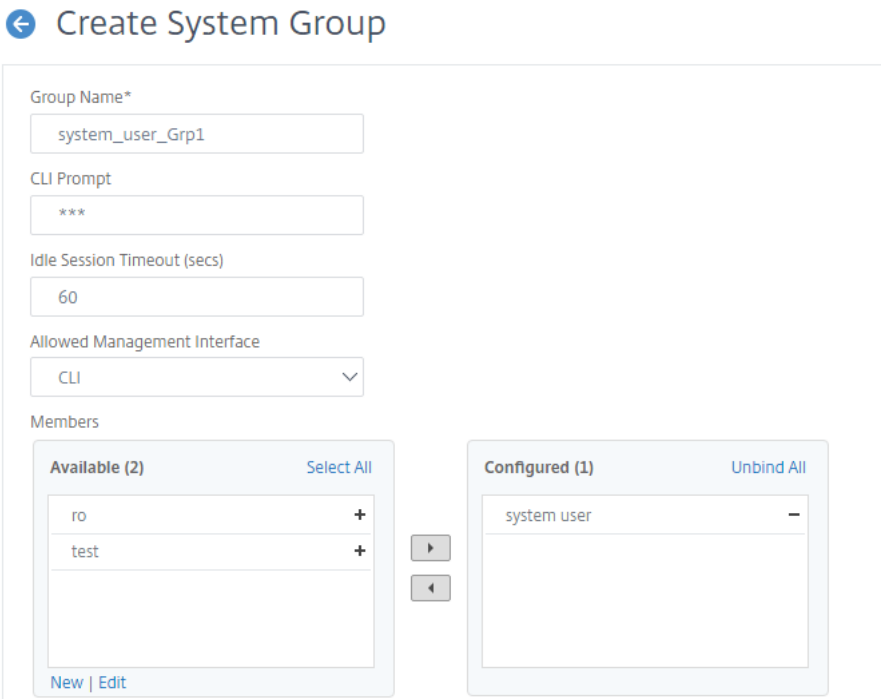
Exemple :

```
> bind system group Managers -userName user1
```

Configurer un groupe d'utilisateurs à l'aide de l'interface graphique NetScaler

1. Accédez à **Système** > **Administration des utilisateurs** > **Groupes**, puis créez le groupe d'utilisateurs.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour créer un groupe d'utilisateurs système.
3. Sur la page **Créer un groupe de systèmes**, définissez les paramètres suivants :
   a) Nom du groupe. Nom du groupe d'utilisateurs.
   b) Invite CLI. L'invite que vous préférez définir pour l'accès à l'interface CLI.
   c) Délai d'expiration de la session inactive (secondes). Définissez la durée pendant laquelle un utilisateur peut rester inactif avant l'expiration et la fermeture de la session.
   d) Interface de gestion autorisée. Sélectionnez les interfaces NetScaler auxquelles le groupe d'utilisateurs est autorisé à accéder.
   e) Membres. Ajoutez des comptes d'utilisateurs au groupe.
   f) Stratégies de commande. Liez les stratégies de commande au groupe d'utilisateurs.
   g) Partitions. Liez les partitions au groupe d'utilisateurs.

4. Cliquez sur **Créer** et **Fermer**.



> **Remarque :**
>
> Pour ajouter des membres au groupe, dans la section Membres, cliquez sur **Ajouter**. Sélectionnez les utilisateurs dans la liste Disponible et ajoutez-les à la liste des utilisateurs configurés.

Configuration des stratégies de commande

Les stratégies de commande réglementent les commandes, les groupes de commandes, les serveurs virtuels et les autres entités que les utilisateurs et les groupes d'utilisateurs sont autorisés à utiliser.

L'appliance fournit un ensemble de stratégies de commande intégrées et vous pouvez configurer des stratégies personnalisées. Pour appliquer les stratégies, vous devez les lier à des utilisateurs ou à des groupes.

Voici les points clés à garder à l'esprit lors de la définition et de l'application des stratégies de commande.

- Vous ne pouvez pas créer de stratégies de commande globales. Les stratégies de commande doivent être directement liées aux utilisateurs et aux groupes de l'appliance.
- Les utilisateurs ou les groupes auxquels aucune stratégie de commande n'est associée sont soumis à la stratégie de commande par défaut (DENY-ALL) et ne peuvent donc exécuter aucune commande de configuration tant que les stratégies de commande appropriées ne sont pas liées à leurs comptes.
- Tous les utilisateurs héritent des stratégies des groupes auxquels ils appartiennent.

- Vous devez attribuer une priorité à une stratégie de commande lorsque vous la liez à un compte utilisateur ou à un compte de groupe. Cela permet à l'appliance de déterminer quelle stratégie est prioritaire lorsque deux stratégies contradictoires ou plus s'appliquent au même utilisateur ou au même groupe.
- Si deux stratégies de commande différentes ayant la même priorité sont liées à un compte utilisateur ou à un compte de groupe, la première stratégie liée a la priorité la plus élevée.
- Les commandes suivantes sont disponibles par défaut pour tous les utilisateurs et ne sont pas affectées par les commandes que vous spécifiez :
- aide, affiche l'attribut CLI, définit l'invite CLI, efface l'invite CLI, affiche l'invite CLI, alias, unalias, historique, quit, exit, whoami, config, définit le mode CLI, désactive le mode CLI et affiche le mode CLI.

Le tableau suivant décrit les stratégies intégrées.

Nom de la stratégie	Autorise
lecture seule	Accès en lecture seule à toutes les commandes show, à l'exception des commandes show ns RunningConfig, show ns ns.conf et des commandes show pour le groupe de commandes NetScaler.
opérateur	Accès en lecture seule et accès aux commandes pour activer et désactiver les services et les serveurs.
network	Accès complet, à l'exception des commandes SSL set et unset, show ns ns.conf, show ns runningConfig et show gslb runningConfig.
sysadmin	[Inclus dans NetScaler 12.0 et versions ultérieures] Un administrateur système est inférieur à un superutilisateur en termes d'accès autorisé sur l'appliance. Un utilisateur sysadmin peut effectuer toutes les opérations NetScaler avec les exceptions suivantes : pas d'accès au shell NetScaler, ne peut pas effectuer de configurations utilisateur, ne peut pas effectuer de configurations de partition et certaines autres configurations conformément à la politique de commande sysadmin.

Nom de la stratégie	Autorise
superutilisateur	Accès complet. Mêmes privilèges que l'utilisateur nsroot.

Création de stratégies de commande personnalisées

La prise en charge des expressions régulières est proposée aux utilisateurs disposant des ressources nécessaires pour gérer davantage d'expressions personnalisées, ainsi qu'aux déploiements qui nécessitent la flexibilité offerte par les expressions régulières. Pour la plupart des utilisateurs, les stratégies de commande intégrées sont suffisantes. Les utilisateurs qui ont besoin de niveaux de contrôle supplémentaires mais qui ne sont pas familiarisés avec les expressions régulières souhaiteront peut-être n'utiliser que des expressions simples, telles que celles présentées dans les exemples fournis dans cette section, afin de garantir la lisibilité des stratégies.

Lorsque vous utilisez une expression régulière pour créer une stratégie de commande, tenez compte des points suivants.

- Lorsque vous utilisez des expressions régulières pour définir des commandes qui sont affectées par une stratégie de commande, vous devez placer les commandes entre guillemets doubles. Par exemple, pour créer une stratégie de commande qui inclut toutes les commandes commençant par **show**, tapez ce qui suit :
- "^show .*$"
- Pour créer une stratégie de commande qui inclut toutes les commandes commençant par rm, tapez ce qui suit :
- "^rm .*$"
- Les expressions régulières utilisées dans les stratégies de commande ne distinguent pas les majuscules des minuscules.

Le tableau suivant répertorie des exemples d'expressions régulières pour les stratégies de commande :

Spécification de la commande	Correspond à ces commandes
"^rm\s+.*$"	Toutes les actions de suppression, car toutes les actions de suppression commencent par la chaîne rm, suivie d'un espace et d'autres paramètres tels que des groupes de commandes, des types d'objets de commande et des arguments.

Spécification de la commande	Correspond à ces commandes
“^show\s+.*$”	Toutes les commandes d’affichage, car toutes les actions d’affichage commencent par la chaîne show, suivie d’un espace et d’autres paramètres tels que des groupes de commandes, des types d’objets de commande et des arguments.
“^shell$”	La commande shell seule, mais non combinée à des paramètres supplémentaires tels que des groupes de commandes, des types d’objets de commande et des arguments.
“^add\s+vserver\s+.*$”	Toutes créent des actions de serveur virtuel, qui consistent à ajouter une commande de serveur virtuel suivie d’un espace et de paramètres supplémentaires tels que des groupes de commandes, des types d’objets de commande et des arguments.
“^add\s+(lb\s+vserver)\s+.*”	Toutes créent des actions de serveur virtuel lb, qui consistent en la commande add lb virtual server suivie d’un espace et d’autres paramètres tels que des groupes de commandes, des types d’objets de commande et des arguments.

Pour plus d’informations sur les stratégies de commande intégrées, reportez-vous au tableau Tableau des stratégies de commandes intégrées .

Pour créer une stratégie de commande à l’aide de l’interface de ligne de commande

À l’invite de commande, tapez les commandes suivantes pour créer une stratégie de commande et vérifier la configuration :

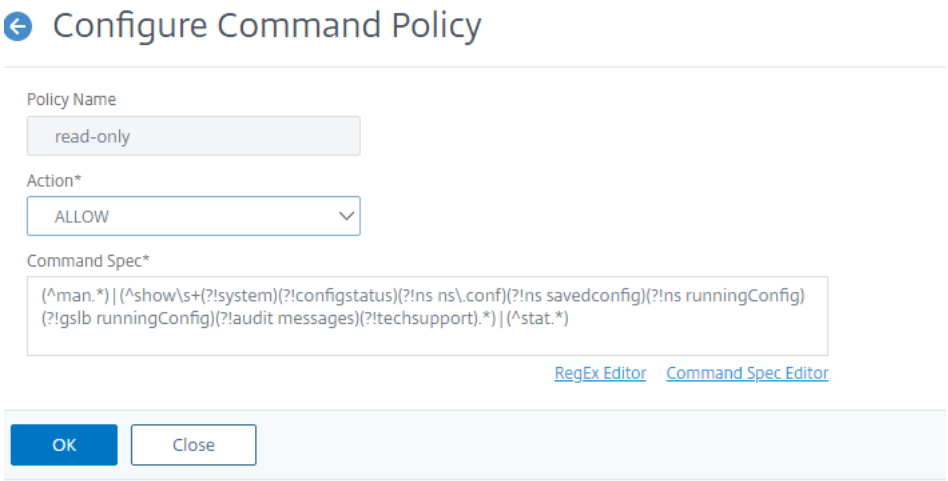
- `add system cmdPolicy <policyname> <action> <cmdspec>`
- `show system cmdPolicy <policyName>`

Exemple :

```
add system cmdPolicy USER-POLICY ALLOW (\ server\ )|(\ service(Group)*\ )
|(\ vserver\ )|(\ policy\ )|(\ policylabel\ )|(\ limitIdentifier\ )|(^show\
 (?!(system|ns\ (ns.conf|runningConfig)))|(save)|(stat\ .*serv)
```


Configurer une politique de commande à l'aide de l'interface graphique NetScaler

1. Accédez à **Système** > **Administration des utilisateurs** > **Stratégies de commande**.
2. Dans le volet d'informations, cliquez sur **Ajouter** pour créer une stratégie de commande.
3. Sur la page **Configurer la stratégie de commande**, définissez les paramètres suivants :
   a) Nom de la stratégie
   b) Action
   c) Spécification de commande.
4. Cliquez sur **OK**.



Liez les stratégies de commande aux comptes d'utilisateurs et aux groupes d'utilisateurs

Une fois que vous avez défini vos stratégies de commande, vous devez les lier aux comptes d'utilisateurs et aux groupes appropriés. Lorsque vous liez une stratégie, vous devez lui attribuer une priorité afin que l'appliance puisse déterminer la stratégie de commande à suivre en cas de conflit entre deux stratégies de commande applicables ou plus.

Les stratégies de commande sont évaluées dans l'ordre suivant :

- Les stratégies de commande directement liées aux utilisateurs et aux groupes correspondants sont évaluées en fonction d'un numéro de priorité. Une stratégie de commande avec un numéro de priorité inférieur est évaluée avant une stratégie avec un numéro de priorité plus élevé. Par conséquent, les privilèges que la stratégie de commande à numéro inférieur accorde ou refuse explicitement ne sont pas annulés par une stratégie de commande à numéro plus élevé.
- Lorsque deux stratégies de commande, l'une liée à un compte utilisateur et l'autre à un groupe, ont le même numéro de priorité, la stratégie de commande directement liée au compte utilisateur est évaluée en premier.

Pour lier des stratégies de commande à un utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez les commandes suivantes pour lier une stratégie de commande à un utilisateur et vérifier la configuration :

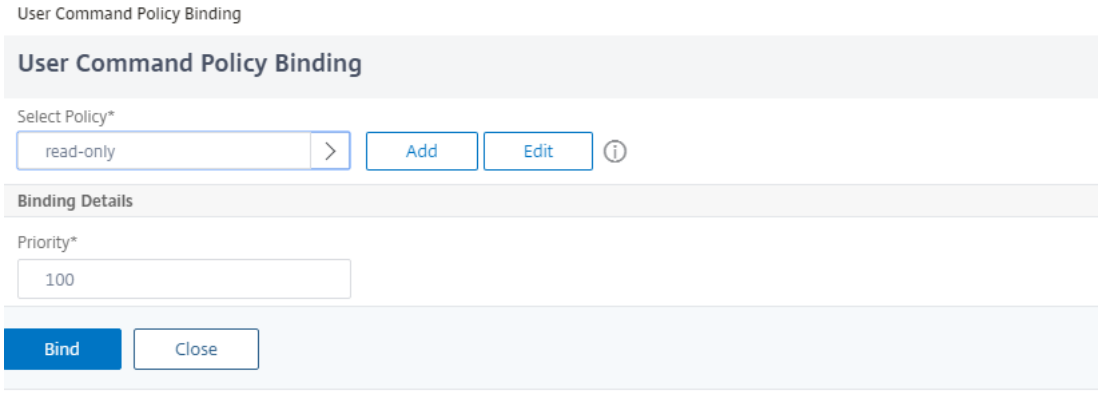
- `bind system user <userName> -policyName <policyName> <priority>`
- `show system user <userName>`

Exemple :

```
> bind system user user1 -policyName read_all 1
```

Liez les politiques de commande à un compte utilisateur à l'aide de l'interface graphique NetScaler

Accédez à **Système** > **Administration** des **utilisateurs > Utilisateurs**, sélectionnez l'utilisateur et liez les stratégies de commande.



Vous pouvez éventuellement modifier la priorité par défaut pour vous assurer que la stratégie est évaluée dans le bon ordre.

Pour lier des stratégies de commande à un groupe à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour lier une stratégie de commande à un groupe d'utilisateurs et vérifier la configuration :

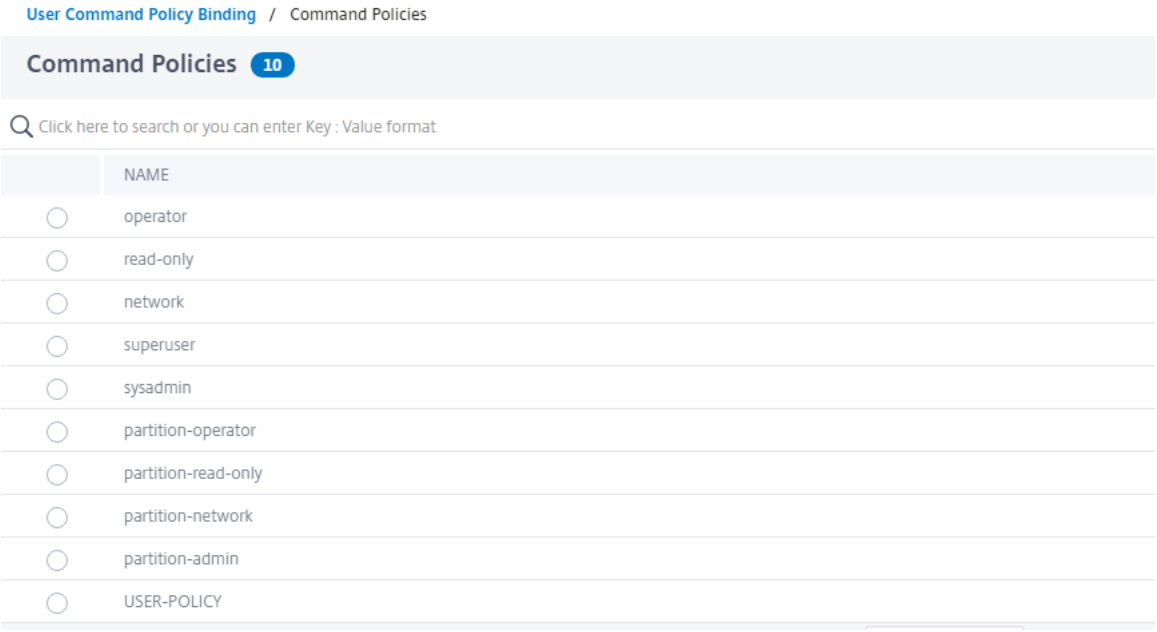
- `bind system group <groupName> -policyName <policyName> <priority>`
- `show system group <groupName>`

Exemple :

```
> bind system group Managers -policyName read_all 1
```


Liez les politiques de commande à un groupe d'utilisateurs à l'aide de l'interface graphique NetScaler

Accédez à **Système** > **Administration des utilisateurs** > **Groupes**, sélectionnez le groupe et liez les stratégies de commande.



Vous pouvez éventuellement modifier la priorité par défaut pour vous assurer que la stratégie est évaluée dans le bon ordre.

Exemple d'utilisation : gestion des comptes utilisateurs, des groupes d'utilisateurs et des stratégies de commande dans une entreprise de fabrication

L'exemple suivant montre comment créer un ensemble complet de comptes d'utilisateurs, de groupes et de stratégies de commande et lier chaque stratégie aux groupes et utilisateurs appropriés. La société Example Manufacturing, Inc., compte trois utilisateurs qui peuvent accéder à l'appliance NetScaler :

- **John Doe.** Le responsable informatique. John doit être en mesure de voir toutes les parties de la configuration de NetScaler mais n'a rien à modifier.
- **María Ramiez.** L'administrateur informatique principal. Maria doit être en mesure de voir et de modifier toutes les parties de la configuration de NetScaler à l'exception des commandes NetScaler (qui, selon la politique locale, doivent être exécutées lorsque vous êtes connecté en tant que nsroot).
- **Michael Baldrock.** L'administrateur informatique chargé de l'équilibrage de charge. Michael doit pouvoir voir toutes les parties de la configuration de NetScaler, mais doit uniquement modifier les fonctions d'équilibrage de charge.

Le tableau suivant présente la répartition des informations réseau, des noms de compte utilisateur, des noms de groupes et des stratégies de commande pour l'entreprise témoin.

Champ	Valeur	Remarque
Nom d'hôte NetScaler	ns01.example.net	S/O
Comptes utilisateur	johnd, mariar et michaelb	John Doe, responsable informatique, Maria Ramirez, administratrice informatique et Michael Baldrock, administrateur informatique.
Groups	Managers et SysOps	Tous les responsables et tous les administrateurs informatiques.
Stratégies de commande	read_all, modify_lb et modify_all	Autorisez l'accès complet en lecture seule, autorisez l'accès de modification à l'équilibrage de charge et autorisez l'accès complet aux modifications.

La description suivante explique le processus de création d'un ensemble complet de comptes d'utilisateurs, de groupes et de politiques de commande sur l'appliance NetScaler nommée ns01.example.net.

La description inclut des procédures pour lier les comptes d'utilisateurs et les groupes appropriés les uns aux autres, et pour lier les stratégies de commande appropriées aux comptes d'utilisateurs et aux groupes.

Cet exemple montre comment vous pouvez utiliser la priorisation pour accorder un accès et des privilèges précis à chaque utilisateur du service informatique.

L'exemple suppose que l'installation et la configuration initiales ont déjà été effectuées sur NetScaler.

Configuration des comptes utilisateurs, des groupes et des stratégies de commande pour un exemple d'organisation

1. Utilisez la procédure décrite dans la section Configuration des comptes utilisateurs pour créer les comptes utilisateur **johnd**, **mariar**et **michaelb**.
2. Utilisez la procédure décrite dans Configuration des groupes d'utilisateurs pour créer des

groupes d'utilisateurs **Managers** et **SysOps**, puis liez les utilisateurs **mariar** et **michaelb** au groupe **SysOps** et l'utilisateur **johnd** au groupe **Managers** .

3. Utilisez la procédure décrite dans Création de stratégies de commande personnalisées pour créer les stratégies de commande suivantes :
   - **read_all** avec l'action **Autoriser** et la spécification de la commande `"(^show\s+(?!system)(?!ns ns.conf)(?!ns runningConfig).*)|(^stat.*)"`
   - **modify_lb** avec l'action **Autoriser** et la spécification de la commande `"^set\s+lb\s+.*$"`
   - modify_all avec l'action Autoriser et la spécification`"^\S+\s+(?!system).*"`de commande
4. Utilisez la procédure décrite dans « Liaison des stratégies de commande aux utilisateurs et aux groupes » pour lier la stratégie de commande **read_all** au groupe **SysOps**, avec la valeur de priorité **1**.
5. Utilisez la procédure décrite dans « Liaison des stratégies de commande aux utilisateurs et aux groupes » pour lier la stratégie de commande **modify_lb** à l'utilisateur **michaelb**, avec la valeur de priorité **5**.

La configuration que vous venez de créer donne les résultats suivants :

- John Doe, le responsable informatique, dispose d'un accès en lecture seule à l'ensemble de la configuration de NetScaler, mais il ne peut pas y apporter de modifications.
- Maria Ramirez, la responsable informatique, dispose d'un accès quasi complet à toutes les zones de la configuration de NetScaler. Elle doit se connecter uniquement pour exécuter des commandes au niveau NetScaler.
- Michael Baldrock, l'administrateur informatique responsable de l'équilibrage de charge, dispose d'un accès en lecture seule à la configuration de NetScaler et peut modifier les options de configuration pour l'équilibrage de charge.

L'ensemble de stratégies de commande qui s'applique à un utilisateur spécifique est une combinaison de stratégies de commande appliquées directement au compte de l'utilisateur et de stratégies de commande appliquées à un ou plusieurs groupes dont l'utilisateur est membre.

Chaque fois qu'un utilisateur entre une commande, le système d'exploitation recherche les stratégies de commande correspondant à cet utilisateur jusqu'à ce qu'il trouve une stratégie comportant une action ALLOW ou DENY correspondant à la commande. Lorsqu'il trouve une correspondance, le système d'exploitation arrête sa recherche de stratégie de commande et autorise ou refuse l'accès à la commande.

Si le système d'exploitation ne trouve aucune politique de commande correspondante, il refuse à l'utilisateur l'accès à la commande, conformément à la politique de refus par défaut de l'appliance NetScaler.

> **Remarque :**
>
> Lorsque vous placez un utilisateur dans plusieurs groupes, veillez à ne pas créer de restrictions ou de privilèges involontaires en matière de commandes utilisateur. Pour éviter ces conflits, lorsque vous organisez vos utilisateurs en groupes, tenez compte de la procédure de recherche et des règles de classement des politiques de NetScaler.

Gestion des comptes utilisateurs et des mots de passe

June 20, 2023

NetScaler vous permet de gérer les comptes utilisateurs et la configuration des mots de passe. Vous trouverez ci-dessous certaines des activités que vous pouvez effectuer pour un compte utilisateur système ou un compte utilisateur `nsroot` administratif sur l'appliance.

- Verrouillage du compte utilisateur du système
- Verrouiller le compte utilisateur du système pour l'accès à la gestion
- Déverrouillez un compte utilisateur système verrouillé pour accéder à la gestion
- Désactiver l'accès à la gestion pour le compte utilisateur du système
- Forcer le changement de mot de passe pour les utilisateurs administratifs `nsroot`
- Supprimer les fichiers sensibles d'un compte utilisateur du système
- Configuration robuste des mots de passe pour les utilisateurs du système

Verrouillage du compte utilisateur du système

Pour empêcher les attaques de sécurité par force brute, vous pouvez configurer la configuration du verrouillage des utilisateurs. La configuration permet à un administrateur réseau d'empêcher un utilisateur du système de se connecter à un dispositif NetScaler. Et déverrouillez également le compte utilisateur avant l'expiration de la période de verrouillage.

À l'invite de commande, tapez :

```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
persistentLoginAttempts (ENABLED | DISABLED)
```

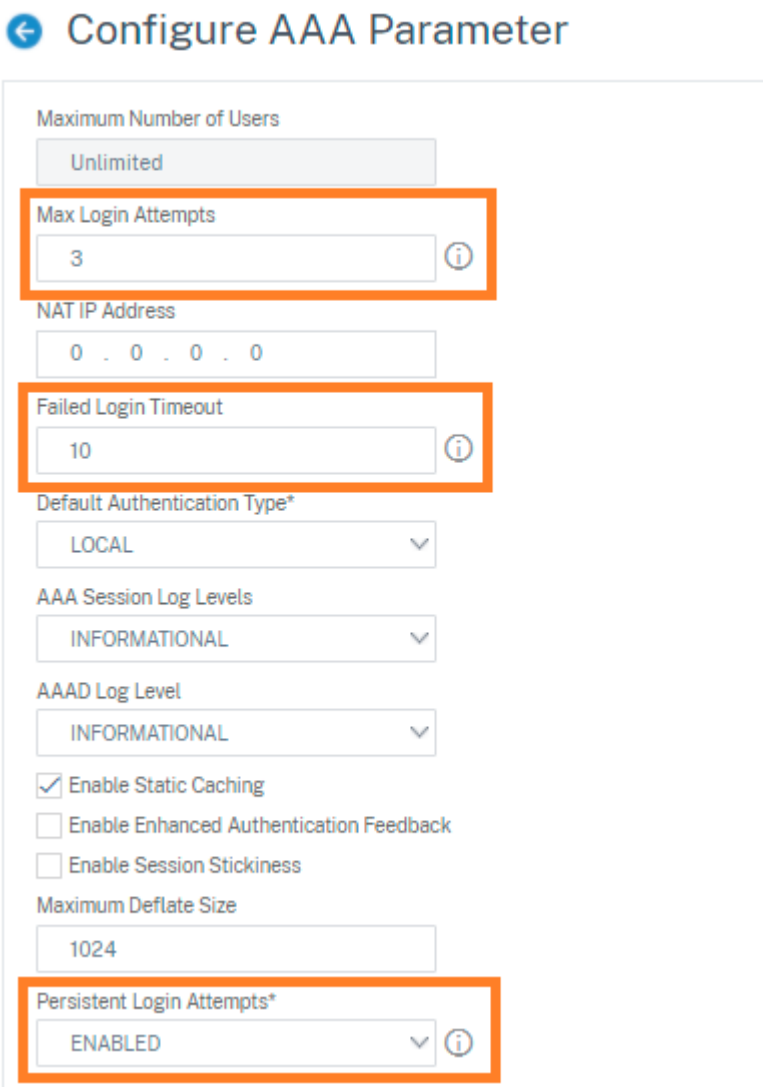
> **Remarque**
>
> Le paramètre « PersistentLoginAttempts » doit être activé pour obtenir les détails du stockage persistant des tentatives de connexion infructueuses des utilisateurs lors des redémarrages.

Exemple :

```
set aaa parameter -maxloginAttempts 3 -failedLoginTimeout 10 -persistentLoginAttempts
 ENABLED
```


Configurer le verrouillage du compte utilisateur du système à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Paramètres d'authentification > Modifier les paramètres d'authentification AAA**.
2. Sur la page **Configurer le paramètre AAA**, définissez les paramètres suivants :
   a) Nombre maximum de tentatives de connexion. Le nombre maximum de tentatives de connexion que l'utilisateur peut essayer.
   b) Échec du délai de connexion. Le nombre maximum de tentatives de connexion non valides par l'utilisateur.
   c) Tentatives de connexion persistantes. Stockage permanent des tentatives de connexion infructueuses des utilisateurs lors des redémarrages.
3. Cliquez sur **OK**.



Lorsque vous définissez les paramètres, le compte utilisateur est bloqué pendant 10 minutes pendant

au moins trois tentatives de connexion non valides. De plus, l'utilisateur ne peut pas se connecter même avec des informations d'identification valides pendant 10 minutes.

> **Remarque**
>
> Si un utilisateur verrouillé essaie de se connecter à l'appliance, un message d'erreur `RBA Authentication Failure: maxlogin attempt reached for test.` s'affiche.

Verrouiller le compte utilisateur du système pour l'accès à la gestion

L'appliance NetScaler vous permet de verrouiller un utilisateur du système pendant 24 heures et de lui refuser l'accès.

L'appliance NetScaler prend en charge la configuration à la fois pour l'utilisateur du système et pour les utilisateurs externes.

> **Remarque**
>
> La fonctionnalité n'est prise en charge que si vous désactivez l'option `persistentLoginAttempts` dans le paramètre `aaa`.

À l'invite de commandes, tapez :

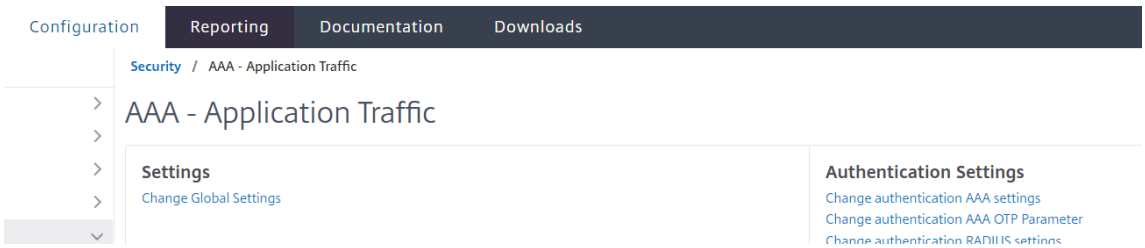
```
set aaa parameter -persistentLoginAttempts DISABLED
```

Maintenant, pour verrouiller un compte d'utilisateur, à l'invite de commandes, tapez :

```
lock aaa user test
```

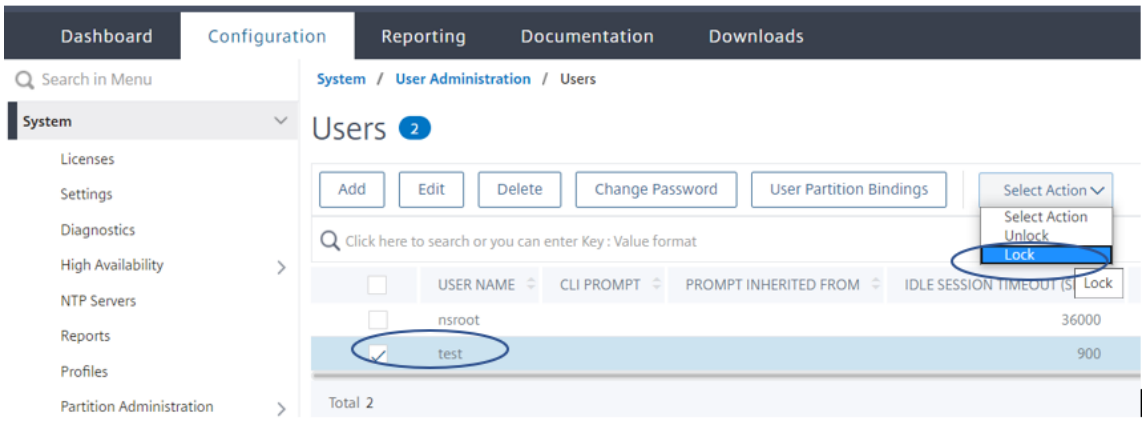
Verrouiller un compte utilisateur du système à l'aide de l'interface graphique

1. Accédez à **Configuration > Sécurité > Trafic des applications AAA > Paramètres d'authentification > Modifier les paramètres d'authentification AAA**.



2. Dans **Configurer le paramètre AAA**, dans la liste des **tentatives de connexion persistantes**, sélectionnez **DÉSACTIVÉ**.
3. Accédez à **Système > Administration des utilisateurs > Utilisateurs**.
4. Sélectionnez un utilisateur.

5. Dans la liste Sélectionner une action, sélectionnez **Verrouiller**.



> **Remarque**
>
> L'interface graphique de NetScaler ne propose pas d'option permettant de verrouiller les utilisateurs externes. Pour verrouiller un utilisateur externe, l'administrateur ADC doit utiliser l'interface de ligne de commande.
> Lorsqu'un utilisateur du système verrouillé (verrouillé par une commande utilisateur d'authentification, d'autorisation et d'audit) tente de se connecter à NetScaler, l'appliance affiche un message d'erreur intitulé « Échec de l'authentification RBA : le test utilisateur est verrouillé pendant 24 heures ».
>
> Lorsqu'un utilisateur est bloqué pour se connecter à l'accès de gestion, l'accès à la console est exempté. L'utilisateur verrouillé peut se connecter à la console.

Déverrouillez un compte utilisateur système verrouillé pour accéder à la gestion

Les utilisateurs du système et les utilisateurs externes peuvent être verrouillés pendant 24 heures à l'aide de la commande utilisateur de verrouillage, d'authentification, d'autorisation et d'audit.

> **Remarque**
>
> L'appliance ADC permet aux administrateurs de déverrouiller l'utilisateur verrouillé et la fonctionnalité ne nécessite aucun paramètre dans la commande « PersistentLoginAttempts ».

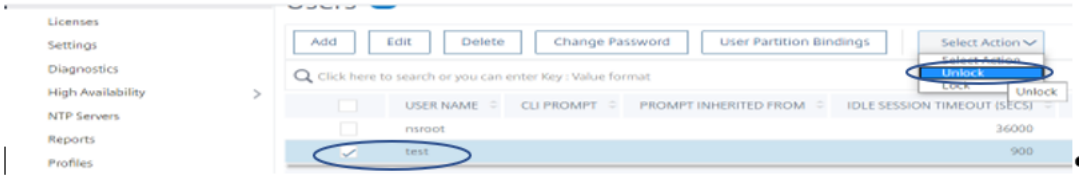
À l'invite de commande, tapez :

```
unlock aaa user test
```

Configurer le déverrouillage utilisateur du système à l'aide de l'interface graphique

1. Accédez à **Système > Administration des utilisateurs > Utilisateurs**.
2. Sélectionnez un utilisateur.

3. Cliquez sur **Déverrouiller**.



L'interface graphique NetScaler répertorie uniquement les utilisateurs du système créés dans l'ADC. Il n'existe donc aucune option dans l'interface graphique permettant de déverrouiller les utilisateurs externes. Pour déverrouiller un utilisateur externe, l'administrateur `nsroot` doit utiliser l'interface de ligne de commande.

Désactiver l'accès à la gestion pour le compte utilisateur du système

Lorsque l'authentification externe est configurée sur l'appliance et qu'en tant qu'administrateur, vous préférez refuser l'accès aux utilisateurs du système pour qu'ils se connectent à l'accès de gestion, vous devez désactiver l'option LocalAuth dans le paramètre système.

À l'invite de commandes, tapez ce qui suit :

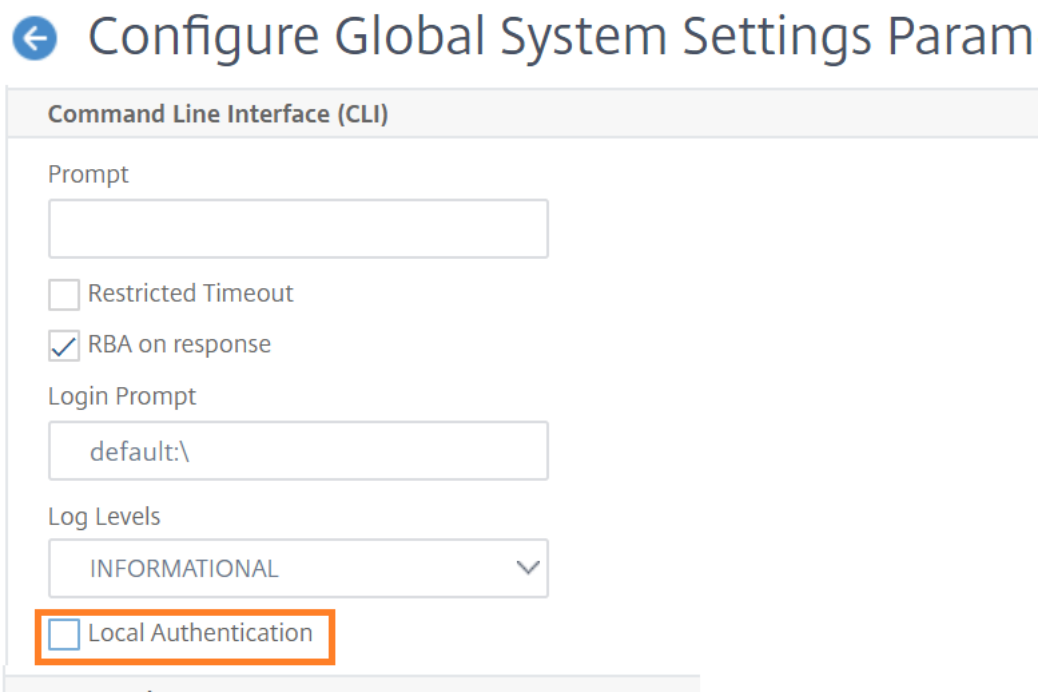
```
set system parameter localAuth <ENABLED|DISABLED>
```

Exemple :

```
set system parameter localAuth DISABLED
```

Désactiver l'accès de gestion à l'utilisateur du système à l'aide de l'interface graphique

1. Accédez à **Configuration > Système > Paramètres > Modifier les paramètres généraux du système**.
2. Dans **la section Interface de ligne de commande (CLI)**, désélectionnez la case **Authentification locale** .



En désactivant cette option, les utilisateurs du système local ne peuvent pas se connecter à l'accès de gestion ADC.

> **Remarque**
>
> Le serveur d'authentification externe doit être configuré et accessible pour interdire l'authentification des utilisateurs du système local dans les paramètres système. Si le serveur externe configuré dans ADC pour l'accès à la gestion est inaccessible, les utilisateurs du système local peuvent se connecter à l'appliance. Le comportement est configuré à des fins de restauration.

Forcer le changement de mot de passe pour les utilisateurs administratifs

Pour une authentification `nsroot` sécurisée, l'appliance NetScaler invite l'utilisateur à remplacer le mot de passe par défaut par un nouveau si l' `forcePasswordChange` option est activée dans le paramètre système. Vous pouvez modifier votre mot de passe `nsroot` depuis l'interface de ligne de commande ou l'interface graphique, lors de votre première connexion avec les informations d'identification par défaut

À l'invite de commande, tapez :

```
set system parameter -forcePasswordChange ( ENABLED | DISABLED )
```

Exemple de session SSH pour NSIP :

```
1 ssh nsroot@1.1.1.1
```



```
Connecting to 1.1.1.1:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].
###############################################################################

WARNING: Access to this system is for authorized users only #
Disconnect IMMEDIATELY if you are not an authorized user! #

###############################################################################

Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
Done
<!--NeedCopy-->
```

Supprimer les fichiers sensibles d'un compte utilisateur du système

Pour gérer les données sensibles telles que les clés autorisées et les clés publiques d'un compte utilisateur du système, vous devez activer `removeSensitiveFiles` cette option. Les commandes qui suppriment les fichiers sensibles lorsque le paramètre système est activé sont les suivantes :

- rm cluster instance
- rm cluster node
- nœud de haute disponibilité rm
- effacer la configuration complète
- join cluster
- add cluster instance

À l'invite de commande, tapez :

```
set system parameter removeSensitiveFiles ( ENABLED | DISABLED )
```

Exemple :

```
set system parameter -removeSensitiveFiles ENABLED
```

Configuration robuste des mots de passe pour les utilisateurs du système

Pour une authentification sécurisée, l'appliance NetScaler invite les utilisateurs et les administrateurs du système à définir des mots de passe forts pour se connecter à l'appliance. Le mot de passe doit être long et doit être une combinaison des éléments suivants :

- Un caractère minuscule
- Un caractère en majuscule

- Un caractère numérique
- Un caractère spécial

À l'invite de commande, tapez :

```
set system parameter -strongpassword <value> -minpasswordlen <value>
```

Où,

`Strongpassword`. Après avoir activé le mot de passe fort (`enable all` / `enablelocal`), tous les mots de passe ou informations sensibles doivent comporter les éléments suivants :

- Au moins 1 caractère minuscule
- Au moins 1 caractère majuscule
- Au moins 1 caractère numérique
- Au moins 1 caractère spécial

Exclure la liste dans `enablelocal` is - `NS_FIPS`, `NS_CRL`, `NS_RSAKEY`, `NS_PKCS12`, NS_PKCS8, NS_LDAP, `NS_TACACS`, `NS_TACACSACTION`, `NS_RADIUS`, `NS_RADIUSACTION`, `NS_ENCRYPTION_PARAMS` . Aucune vérification du mot de passe fort n'est donc effectuée sur ces commandes ObjectType pour l'utilisateur du système.

Valeurs possibles : `enableall`, `enablelocal`, désactivé
Valeur par défaut : désactivé

`minpasswordlen`. Longueur minimale du mot de passe utilisateur du système. Lorsque le mot de passe fort est activé par défaut, la longueur minimale est de 4. La valeur saisie par l'utilisateur peut être supérieure ou égale à 4. La valeur minimale par défaut est 1 lorsque le mot de passe fort est désactivé. La valeur maximale est 127 dans les deux cas.

Valeur minimale : 1
Valeur maximale : 127

Exemple :

```
set system parameter -strongpassword enablelocal -minpasswordlen 6
```

Compte utilisateur par défaut

Le compte `nsrecover` utilisateur peut être utilisé par l'administrateur pour récupérer l'appliance NetScaler. Vous pouvez vous connecter à l'appliance ADC `nsrecover` si les utilisateurs du système par défaut (`nsroot`) ne peuvent pas se connecter en raison de problèmes imprévus. Le login `nsrecover` est indépendant des configurations utilisateur et vous permet d'accéder directement à l'invite du shell. Vous êtes toujours autorisé à vous connecter via le `nsrecover`? même si la limite de configuration maximale est atteinte.

Comment réinitialiser le mot de passe administrateur (nsroot)

June 2, 2023

Le compte administrateur root (`nsroot`) de NetScaler fournit un accès complet à toutes les fonctionnalités de l'ADC. Ainsi, pour préserver la sécurité, le compte administratif ne doit être utilisé que si nécessaire.

En tant qu'administrateur, il est recommandé de modifier votre mot de passe. Si vous oubliez votre mot de passe, vous devez d'abord le réinitialiser au mot de passe par défaut, puis le remplacer par un nouveau mot de passe.

En tant qu'administrateur `nsroot`, pour réinitialiser votre mot de passe, vous devez vous connecter à votre appliance et modifier le mot de passe. Toutefois, si vous ne vous souvenez pas du mot de passe, vous pouvez redémarrer l'appliance en mode mono-utilisateur. Montez le système de fichiers en mode lecture/écriture, puis supprimez l'entrée **NetScaler** du fichier ns.conf. Pour terminer, redémarrez et connectez-vous à votre appliance avec le mot de passe par défaut, puis définissez un nouveau mot de passe.

Procédez comme suit pour réinitialiser le mot de passe de votre administrateur racine :

1. Connectez un ordinateur au port de console de NetScaler et ouvrez une session.

   > **Remarque**
   >
   > Vous ne pouvez pas ouvrir une session à l'aide de SSH pour effectuer cette procédure. Vous devez vous connecter directement à l'appliance.

2. Redémarrez NetScaler.
3. Appuyez sur CTRL+C lorsque le message suivant s'affiche :

   ```
   Press [Ctrl-C] for command prompt, or any other key to boot immediately
   .
   Booting [kernel] in ## seconds.
   ```

4. Exécutez la commande suivante pour démarrer NetScaler en mode utilisateur unique :
   `boot -s`

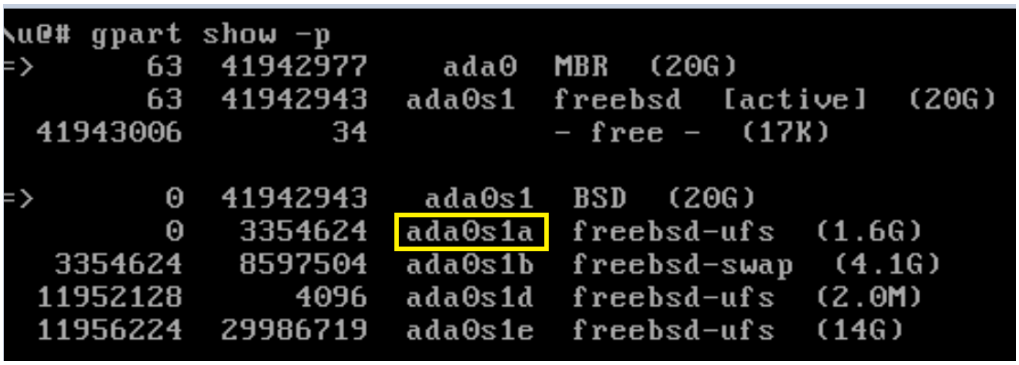
   Après le démarrage de l'appliance, le message suivant s'affiche :

   Entrez le chemin d'accès complet du shell ou `RETURN for /bin/sh:`

5. Appuyez sur ENTRÉE pour afficher l'invite # et tapez les commandes suivantes pour monter les systèmes de fichiers :

   a) Exécutez la commande suivante pour vérifier la cohérence du disque :

   ```
   fsck_ufs /dev/ada0s1a
   ```


> **Remarque**
>
> Votre clé USB possède un nom de périphérique spécifique en fonction de votre NetScaler. Exécutez la commande suivante sur l'ADC CLI et copiez le nom se terminant par « 1a. »
>
> ```
> gpart show -p
> ```
>
> Par exemple,
>
> 
>

b) Accédez au répertoire de développement et entrez « ls » pour vérifier les détails du lecteur.

c) Exécutez la commande suivante pour afficher les partitions montées :

```
df
```

> **Remarque**
>
> Si la partition flash n'est pas répertoriée, vous devez la monter manuellement.

d) Exécutez la commande suivante pour monter le lecteur flash :

```
mount /dev/ad0s1a /flash
```

6. Exécutez la commande suivante pour accéder au répertoire `nsconfig` :

```
cd /flash/nsconfig
```

7. Exécutez les commandes suivantes pour réécrire le fichier ns.conf et supprimer le jeu de commandes système par défaut pour l'administrateur :

a) Exécutez la commande suivante pour créer un fichier de configuration qui ne possède pas de commandes par défaut pour l'administrateur :

```
grep -v "set system user nsroot" ns.conf > new.conf
```

b) Exécutez la commande suivante pour effectuer une sauvegarde du fichier de configuration existant :

```
mv ns.conf old.ns.conf
```

c) Exécutez la commande suivante pour renommer le nouveau fichier .conf en ns.conf :


```
mv new.conf ns.conf
```

8. Exécutez la commande suivante pour redémarrer NetScaler :

   ```
   reboot
   ```

9. Connectez-vous à l'aide des informations d'identification d'administrateur par défaut.
10. Exécutez la commande suivante pour réinitialiser le mot de passe administrateur :

    ```
    set system user nsroot <New_Password>
    ```

    > **Remarque**
    >
    > Pour utiliser le « ? » dans une chaîne de mot de passe, précédez ce caractère par le caractère \.

    Par exemple, `yourexamplepasswd?` est défini pour le compte administrateur après avoir effectué l'opération suivante :

    ```
    > set system user nsroot yourexamplepasswd\?
    ```

> **Remarque**
>
> Pour réinitialiser un mot de passe oublié (`nsroot`) dans une configuration haute disponibilité, il est recommandé d'arrêter le nœud homologue. Si le nœud homologue est actif, le mot de passe est écrasé, car la synchronisation de configuration est déclenchée lorsque le nœud apparaît après le redémarrage.

Lisez également l'article CTX224027 pour savoir comment fonctionne l'accès SSH sécurisé à l'appliance NetScaler.

Authentification utilisateur externe

May 5, 2023

Le service d'authentification d'une appliance NetScaler peut être local ou externe. Dans l'authentification des utilisateurs externes, l'appliance utilise un serveur externe tel que LDAP, RADIUS ou TACACS+ pour authentifier l'utilisateur. Pour authentifier un utilisateur externe et lui accorder l'accès à l'appliance, vous devez appliquer une stratégie d'authentification. L'authentification du système NetScaler utilise des politiques d'authentification avancées avec des expressions de politique avancées. Les politiques d'authentification avancées sont également utilisées pour la gestion des utilisateurs du système dans une appliance NetScaler partitionnée.

> **Remarque**
>
> Si votre appliance utilise toujours des stratégies classiques et ses expressions, vous devez cesser

> de l'utiliser et migrer votre utilisation de stratégie classique vers l'infrastructure de stratégie avancée.

Une fois que vous avez créé une stratégie d'authentification, vous devez la lier à l'entité globale du système. Vous pouvez configurer un serveur d'authentification externe (par exemple, TACACS) en liant une seule stratégie d'authentification à l'entité globale du système. Vous pouvez également configurer une cascade de serveurs d'authentification en liant plusieurs stratégies à l'entité globale du système.

> **Remarque**
>
> Lorsqu'un utilisateur externe se connecte à l'appliance, le système génère un message d'erreur « Utilisateur n'existe pas » dans le `ns.log` fichier. L'occurrence est due au fait que le système exécute la commande systemuser_systemcmdpolicy_binding pour initialiser l'interface graphique de l'utilisateur.

Authentification LDAP (en utilisant des serveurs LDAP externes)

Vous pouvez configurer l'appliance NetScaler pour authentifier l'accès des utilisateurs auprès d'un ou de plusieurs serveurs LDAP. L'autorisation LDAP nécessite des noms de groupe identiques dans Active Directory, sur le serveur LDAP et sur l'appliance. Les caractères et la casse doivent également être les mêmes.

Pour plus d'informations sur les stratégies d'authentification LDAP, consultez la rubrique Stratégies d'authentification LDAP .

Par défaut, l'authentification LDAP est sécurisée à l'aide du protocole SSL/TLS. Il existe deux types de connexions LDAP sécurisées. Dans le premier type, le serveur LDAP accepte la connexion SSL/TLS sur un port distinct du port utilisé pour accepter les connexions LDAP claires. Une fois que les utilisateurs ont établi la connexion SSL/TLS, le trafic LDAP peut être envoyé via la connexion. Le second type permet à la fois des connexions LDAP non sécurisées et sécurisées, et le port unique le gère sur le serveur. Dans ce scénario, pour créer une connexion sécurisée, le client établit d'abord une connexion LDAP claire. Ensuite, la commande **LDAP** StartTLS est envoyée au serveur via la connexion. Si le serveur LDAP prend en charge StartTLS, la connexion est convertie en une connexion LDAP sécurisée à l'aide de TLS.

Les numéros de port des connexions LDAP sont les suivants :

- 389 pour les connexions LDAP non sécurisées
- 636 pour les connexions LDAP sécurisées
- 3268 pour les connexions LDAP non sécurisées Microsoft
- 3269 pour les connexions LDAP sécurisées Microsoft

Les connexions LDAP qui utilisent la commande StartTLS utilisent le numéro de port 389. Si les numéros de port 389 ou 3268 sont configurés sur l'appliance, celle-ci essaie d'utiliser StartTLS pour

établir la connexion. Si un autre numéro de port est utilisé, les tentatives de connexion utilisent SSL/TLS. Si StartTLS ou SSL/TLS ne peuvent pas être utilisés, la connexion échoue.

Lors de la configuration du serveur LDAP, la casse des caractères alphabétiques doit correspondre à celle du serveur et de l'appliance. Si le répertoire racine du serveur LDAP est spécifié, tous les sous-répertoires sont également recherchés pour trouver l'attribut utilisateur. Dans les grands répertoires, cela peut affecter les performances. Pour cette raison, Citrix vous recommande d'utiliser une unité d'organisation spécifique.

Le tableau suivant répertorie des exemples de nom unique (DN) de base.

serveur LDAP	DN de base
Microsoft Active Directory	DC=Citrix, DC=local
Novell eDirectory	DC=Citrix, DC=net
IBM Directory Server	cn=utilisateurs
Lotus Domino	OU=ville, O=Citrix, C=États-Unis
Sun ONE directory (anciennement iPlanet)	OU=personnes, DC=Citrix, DC=com

Le tableau suivant répertorie des exemples de nom distinctif (DN) de liaison.

serveur LDAP	DN de liaison
Microsoft Active Directory	CN=Administrateur, CN=Utilisateurs, DC=Citrix, DC=Local
Novell eDirectory	cn=admin, DC=Citrix, DC=net
IBM Directory Server	LDAP_DN
Lotus Domino	CN=Administrateur de notes, O=Citrix, C=États-Unis
Sun ONE directory (anciennement iPlanet)	uid=admin, OU=Administrateurs, OU=Gestion de la topologie, O=NetScaperoot

serveur LDAP	DN de liaison
Microsoft Active Directory	CN=Administrateur, CN=Utilisateurs, DC=Citrix, DC=Local
Novell eDirectory	cn=admin, DC=Citrix, DC=net

serveur LDAP	DN de liaison
IBM Directory Server	LDAP_DN
Lotus Domino	CN=Administrateur de notes, O=Citrix, C=États-Unis
Sun ONE directory (anciennement iPlanet)	uid=admin, OU=Administrateurs, OU=Gestion de la topologie, O=NetScaperoot

Configuration de l'authentification utilisateur LDAP à l'aide de l'interface

Effectuez les étapes suivantes pour configurer l'authentification LDAP pour les utilisateurs externes.

Configuration de la stratégie LDAP

À l'invite de commandes, procédez comme suit :

Étape 1 : créez une action LDAP.

```
add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> } } >] [-authTimeout <positive_integer>] [-ldapBase
<string>] [-ldapBindDn <string>] { -ldapBindDnPassword } [-ldapLoginName <
string>] [-groupAttrName <string>] [-subAttributeName <string>]
```

Exemple :

```
add authentication ldapAction ldap_act -serverIP <IP> -authTimeout 30 -
ldapBase "CN=xxxxx,DC=xxxx,DC=xxx"-ldapBindDn "CN=xxxxx,CN=xxxxx,DC=xxxx,DC
=xxx"-ldapBindDnPassword abcd -ldapLoginName sAMAccountName -groupattrName
memberOf -subAttributeName CN
```

Pour la description des paramètres, reportez-vous à la rubrique Référence des commandes d'authentification et d'autorisation .

Étape 2 : Créez une stratégie LDAP classique.

```
add authentication ldapPolicy <name> <rule> [<reqAction>]
```

Exemple :

```
add authentication ldappolicy ldap_pol_classic ns_true ldap_act
```

> **Remarque**
>
> Vous pouvez configurer à l'aide d'une stratégie LDAP classique ou avancée, mais Citrix vous recommande d'utiliser une stratégie d'authentification avancée car les stratégies classiques

> sont obsolètes à partir de la version NetScaler 13.0.

Étape 3 : Créer une stratégie LDAP avancée

```
add authentication Policy <name> <rule> [<reqAction>]
```

Exemple :

```
add authentication policy ldap_pol_advance -rule true -action ldap_act
```

Étape 4 : Liez la stratégie LDAP au système global

À l'invite de la ligne de commande, procédez comme suit :

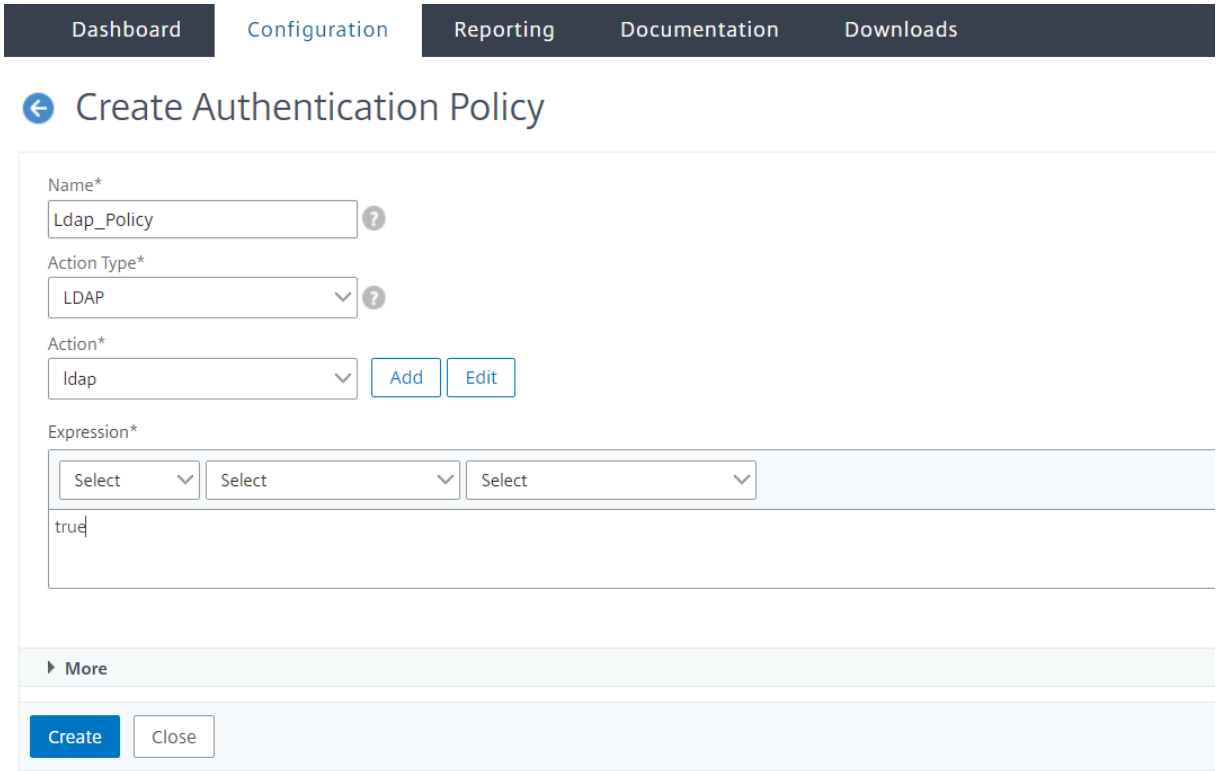
```
bind system global <policyName> [-priority <positive_integer]
```

Exemple :

```
bind system global ldap_pol_advanced -priority 10
```

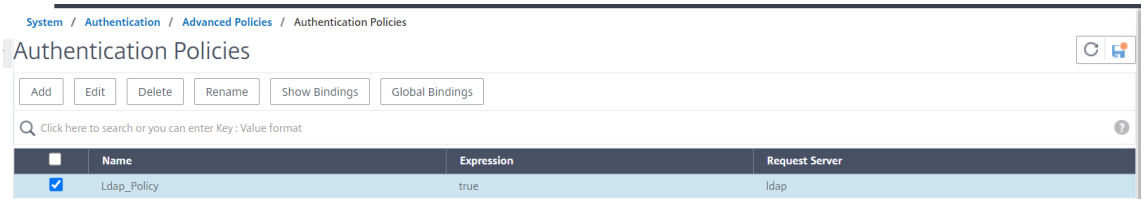
Configurer l'authentification utilisateur LDAP à l'aide de l'interface graphique NetScaler

1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.
2. Cliquez sur **Ajouter** pour créer une stratégie d'authentification de type LDAP.
3. Cliquez sur **Créer** et **Fermer**.

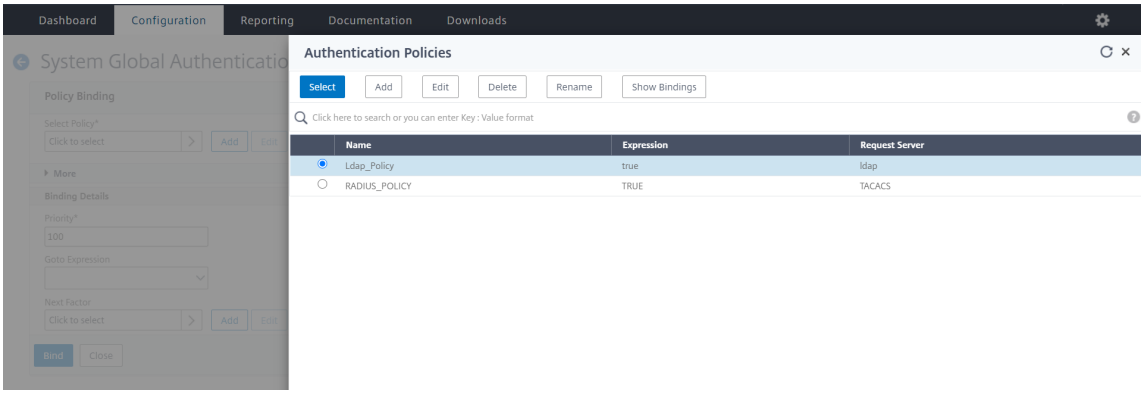


Liez une politique d'authentification au système global pour l'authentification LDAP à l'aide de l'interface graphique NetScaler

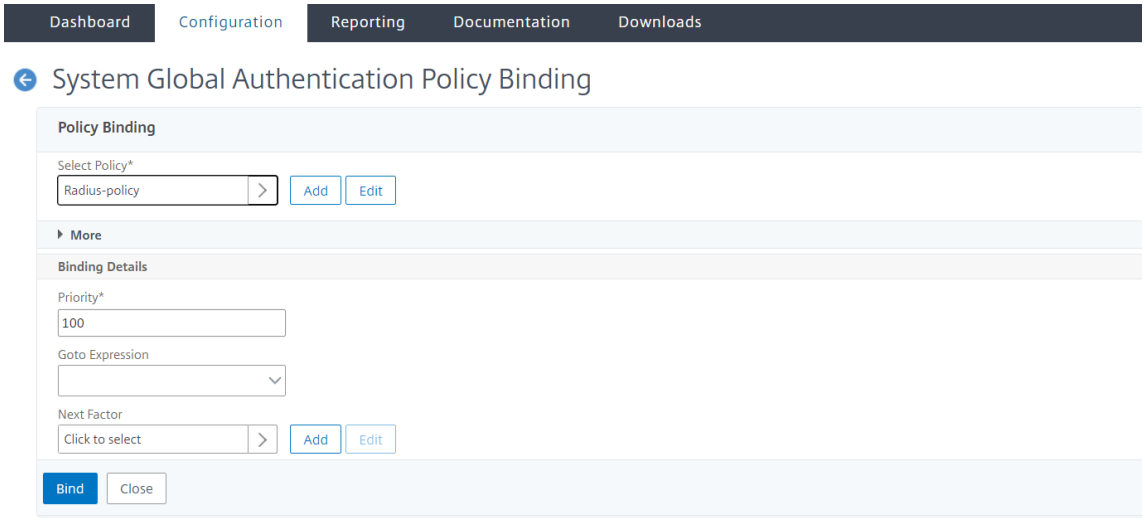
1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégies d'authentificationStratégie**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales** pour créer une liaison de stratégie d'authentification globale du système.
3. Cliquez sur **Global Bindings**.



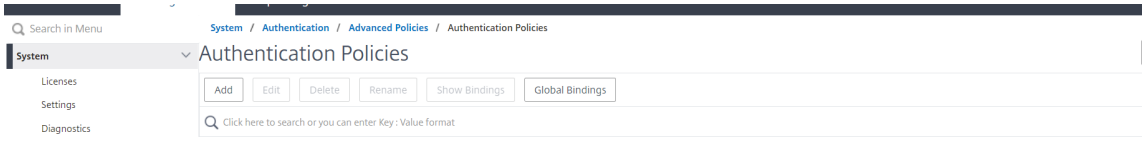
4. Sélectionnez un profil d'authentification.



5. Sélectionnez la stratégie LDAP.
6. Dans la page **Liaison de stratégie d'authentification globale du système**, définissez les paramètres suivants :
   a) Sélectionnez Policy.
   b) Détails de la liaison



7. Cliquez sur **Lier** et **Terminé**.
8. Cliquez sur **Global Bindings** (Liaisons globales) pour confirmer que la stratégie est liée au système global.



Déterminer les attributs dans l'annuaire LDAP

Si vous avez besoin d'aide pour déterminer les attributs de votre annuaire LDAP, vous pouvez facilement les rechercher avec le navigateur LDAP gratuit de Softerra.

Vous pouvez télécharger le navigateur LDAP sur le site Web de Softerra LDAP Administrator à l'adresse <http://www.ldapbrowser.com>. Une fois le navigateur installé, définissez les attributs suivants :

- Le nom d'hôte ou l'adresse IP de votre serveur LDAP.
- Le port de votre serveur LDAP. La valeur par défaut est 389.
- Le champ DN de base peut être laissé vide.
- Les informations fournies par le navigateur LDAP peuvent vous aider à déterminer le DN de base requis pour l'onglet Authentification.
- La vérification de liaison anonyme détermine si le serveur LDAP nécessite des informations d'identification utilisateur pour que le navigateur s'y connecte. Si le serveur LDAP nécessite des informations d'identification, laissez la case à cocher désactivée.

Après avoir terminé les paramètres, le navigateur LDAP affiche le nom du profil dans le volet gauche et se connecte au serveur LDAP.

Pour plus d'informations, consultez la rubrique LDAP .

Prise en charge de l'authentification par clé pour les utilisateurs LDAP

Avec l'authentification par clé, vous pouvez désormais extraire la liste des clés publiques stockées sur l'objet utilisateur dans le serveur LDAP via SSH. Au cours du processus d'authentification basée sur les rôles (RBA), l'appliance NetScaler doit extraire les clés SSH publiques du serveur LDAP. La clé publique récupérée, compatible avec SSH, doit vous permettre de vous connecter via la méthode RBA.

Un nouvel attribut « sshPublicKey » est introduit dans les commandes « add authentication ldapAction » et « set authentication ldapAction ». En utilisant cet attribut, vous pouvez obtenir les avantages suivants :

- Peut stocker la clé publique récupérée, et l'action LDAP utilise cet attribut pour récupérer les informations de clé SSH à partir du serveur LDAP.
- Peut extraire des noms d'attributs d'une taille maximale de 24 Ko.

> **Remarque**
>
> Le serveur d'authentification externe, tel que LDAP, est utilisé uniquement pour récupérer les informations de clé SSH. Il n'est pas utilisé à des fins d'authentification.

Voici un exemple de flux d'événements via SSH :

- Le démon SSH envoie une demande AAA_AUTHENTICATE avec le champ de mot de passe vide au port du démon d'authentification, d'autorisation et d'audit.
- Si LDAP est configuré pour stocker la clé publique SSH, l'authentification, l'autorisation et l'audit répondent avec l' `sshPublicKey` attribut ainsi que d'autres attributs.
- Le démon SSH vérifie ces clés avec les clés client.
- Le démon SSH transmet le nom d'utilisateur dans la charge utile de la requête, et l'authentification, l'autorisation et l'audit renvoient les clés spécifiques à cet utilisateur ainsi que les clés génériques.

Pour configurer l'attribut SSHPublicKey, tapez les commandes suivantes à l'invite de commandes :

- Avec l'opération add, vous pouvez ajouter l'attribut « SSHPublicKey » lors de la configuration de la commande `ldapAction`.

```
add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr
|*> | { -serverName <string> } } [-serverPort <port>] … [-Attribute1 <
string>] … [-Attribute16 <string>][-sshPublicKey <string>][-authentication
 off]<!--NeedCopy-->
```

- Avec l'opération set, vous pouvez configurer l'attribut « sshPublicKey » à une commande ldapAction déjà ajoutée.

```
set authentication ldapAction <name> [-sshPublicKey <string>][-authentication
 off]<!--NeedCopy-->
```


Authentification RADIUS (à l'aide de serveurs RADIUS externes)

Vous pouvez configurer l'appliance NetScaler pour authentifier l'accès des utilisateurs à un ou plusieurs serveurs RADIUS. Si vous utilisez des produits RSA SecurID, SafeWord ou Gemalto Protiva, utilisez un serveur RADIUS.

Pour plus d'informations sur les politiques d'authentification RADIUS, consultez Authentification RADIUS.

Votre configuration peut nécessiter l'utilisation d'une adresse IP du serveur d'accès réseau (IP NAS) ou d'un identifiant de serveur d'accès réseau (ID NAS). Lorsque vous configurez l'appliance pour utiliser un serveur d'authentification RADIUS, suivez les directives suivantes :

- Si vous activez l'utilisation de l'adresse IP du NAS, l'appliance envoie son adresse IP configurée au serveur RADIUS, plutôt que l'adresse IP source utilisée pour établir la connexion RADIUS.
- Si vous configurez l'ID NAS, l'appliance envoie l'identificateur au serveur RADIUS. Si vous ne configurez pas l'ID NAS, l'appliance envoie son nom d'hôte au serveur RADIUS.
- Lorsque l'adresse IP du NAS est activée, l'appliance ignore tout ID NAS qu'elle a utilisé pour communiquer avec le serveur RADIUS.

Configuration de l'authentification utilisateur RADIUS à l'aide de l'interface

À l'invite de commandes, procédez comme suit :

Étape 1 : créer une action RADIUS

```
add authentication radiusaction <name> -serverip <ip> -radkey <key> -
radVendorID <id> -radattributetype <value>
```

Où, attribut
`radVendorID` RADIUS Vendor ID, utilisé pour l'extraction du groupe RADIUS.
`radAttributeType` Type d'attribut RADIUS, utilisé pour l'extraction de groupes RADIUS.

Exemple :

```
add authentication radiusaction RADserver531 rad_action -serverip 1.1.1.1 -
radkey key123 -radVendorID 66 -radattributetype 6
```

Étape 2 : créer une stratégie RADIUS classique.

```
add authentication radiusPolicy <name> <rule> [<reqAction>]
```

Exemple :

```
add authentication radiuspolicy radius_pol_classic ns_true radius_act
```

> **Remarque**
>
> Vous pouvez configurer à l'aide d'une stratégie RADIUS classique ou avancée. Citrix vous recom-

> mande d'utiliser la stratégie d'authentification avancée car les politiques classiques sont obsolètes à partir de la version 13.0 de NetScaler.

Étape 3 : Créer une stratégie RADIUS avancée

```
add authentication policy <policyname> -rule true -action <radius action name>
```

Exemple :

```
add authentication policy rad_pol_advanced -rule true -action radserver531rad_action
```

Étape 4 : Liez la stratégie RADIUS au système global.

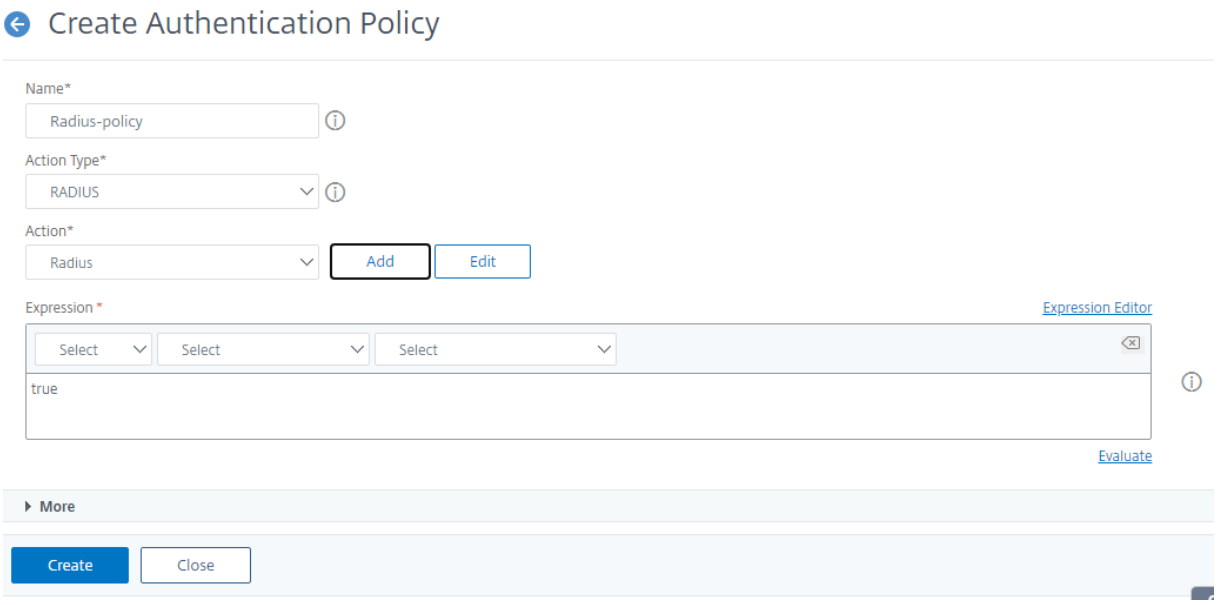
```
bind system global <policyName> -priority <positive_integer
```

Exemple :

```
bind system global radius_pol_advanced -priority 10
```

Configuration de l'authentification utilisateur RADIUS à l'aide de l'interface

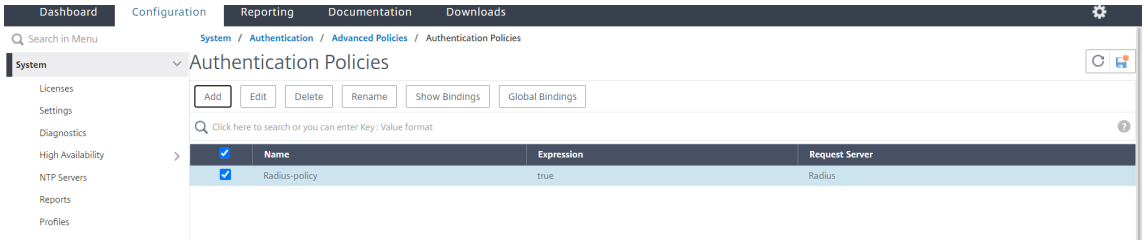
1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.
2. Cliquez sur **Ajouter** pour créer une stratégie d'authentification de type RADIUS.
3. Cliquez sur **Créer** et **Fermer**.



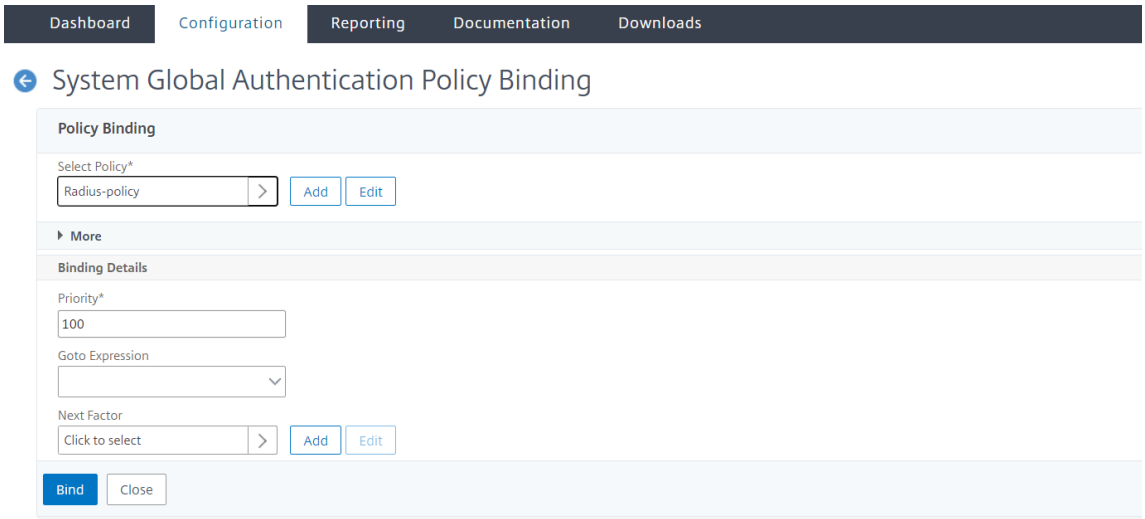
Liez la stratégie d'authentification au système global pour l'authentification RADIUS à l'aide de l'interface graphique

1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.

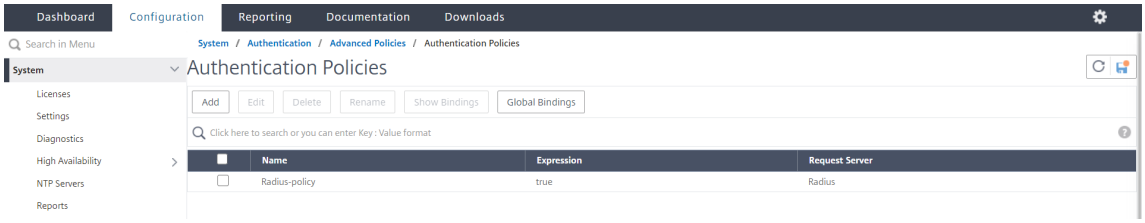
2. Dans le volet d'informations, cliquez sur **Liaisons globales** pour créer une liaison de stratégie d'authentification globale du système.
3. Cliquez sur **Global Bindings**.



4. Sélectionnez RADIUS.
5. Dans la page **Liaison de stratégie d'authentification globale du système**, définissez les paramètres suivants :
   a) Sélectionnez une stratégie.
   b) Détails de la reliure



6. Cliquez sur **Lier** et **fermer**.
7. Cliquez sur **Global Bindings** (Liaisons globales) pour confirmer que la stratégie est liée au système global.



Choisissez les protocoles d'authentification utilisateur RADIUS

L'appliance NetScaler prend en charge les implémentations de RADIUS configurées pour utiliser l'un des nombreux protocoles d'authentification des utilisateurs, notamment :

- Protocole d'authentification par mot
- Protocole CHAP (Challenge-Handshake Authentication Protocol)
- Protocole d'authentification Microsoft Challenge-Handshake (MS-CHAP version 1 et version 2)

Si votre déploiement est configuré pour utiliser l'authentification RADIUS et que votre serveur RADIUS est configuré avec un protocole d'authentification par mot de passe. Vous pouvez renforcer l'authentification des utilisateurs en attribuant un secret partagé fort au serveur RADIUS. Les secrets partagés RADIUS forts se composent de séquences aléatoires de lettres majuscules et minuscules, de chiffres et de ponctuation, et ont une longueur minimale de 22 caractères. Si possible, utilisez un programme de génération de caractères aléatoires pour déterminer les secrets partagés RADIUS.

Pour mieux protéger le trafic RADIUS, attribuez un secret partagé différent à chaque appliance ou serveur virtuel. Lorsque vous définissez des clients sur le serveur RADIUS, vous pouvez également attribuer un secret partagé distinct à chaque client. Vous devez également configurer séparément chaque stratégie qui utilise l'authentification RADIUS.

Configuration de l'extraction d'adresses IP

Vous pouvez configurer l'appliance pour extraire l'adresse IP d'un serveur RADIUS. Lorsqu'un utilisateur s'authentifie auprès du serveur RADIUS, le serveur renvoie une adresse IP encadrée qui lui est attribuée. Voici les attributs pour l'extraction d'adresses IP :

- Permet à un serveur RADIUS distant de fournir une adresse IP à partir du réseau interne pour un utilisateur connecté à l'appliance.
- Permet la configuration de n'importe quel attribut RADIUS utilisant le type d'adresse IP, y compris ceux codés par le fournisseur.

Lors de la configuration du serveur RADIUS pour l'extraction d'adresses IP, vous configurez l'identificateur fournisseur et le type d'attribut.

L'identifiant du fournisseur permet au serveur RADIUS d'attribuer une adresse IP au client à partir d'un pool d'adresses IP configurées sur le serveur RADIUS. L'ID et les attributs du fournisseur sont utilisés pour établir l'association entre le client RADIUS et le serveur RADIUS. L'ID du fournisseur est l'attribut de la réponse RADIUS qui fournit l'adresse IP du réseau interne. La valeur zéro indique que l'attribut n'est pas codé par le fournisseur. Le type d'attribut est l'attribut d'adresse IP distante dans une réponse RADIUS. La valeur minimale est 1 et la valeur maximale est 255.

Une configuration courante consiste à extraire l' *adresse IP encadrée* de l'attribut **RADIUS**. L'ID du fournisseur est défini sur zéro ou n'est pas spécifié. Le type d'attribut est défini sur huit.

Extraction de groupe pour RADIUS à l'aide de l'interface

1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Radius**, puis sélectionnez une stratégie.
2. Sélectionnez ou créez une stratégie RADIUS.
3. Dans la page **Configurer le serveur RADIUS d'authentification**, définissez les paramètres suivants.
   a) **Identifiant fournisseur du groupe**
   b) **Type d'attribut de groupe**
4. Cliquez sur **OK** et sur **Fermer**.

Authentification TACACS+ (à l'aide de serveurs TACACS+ externes)

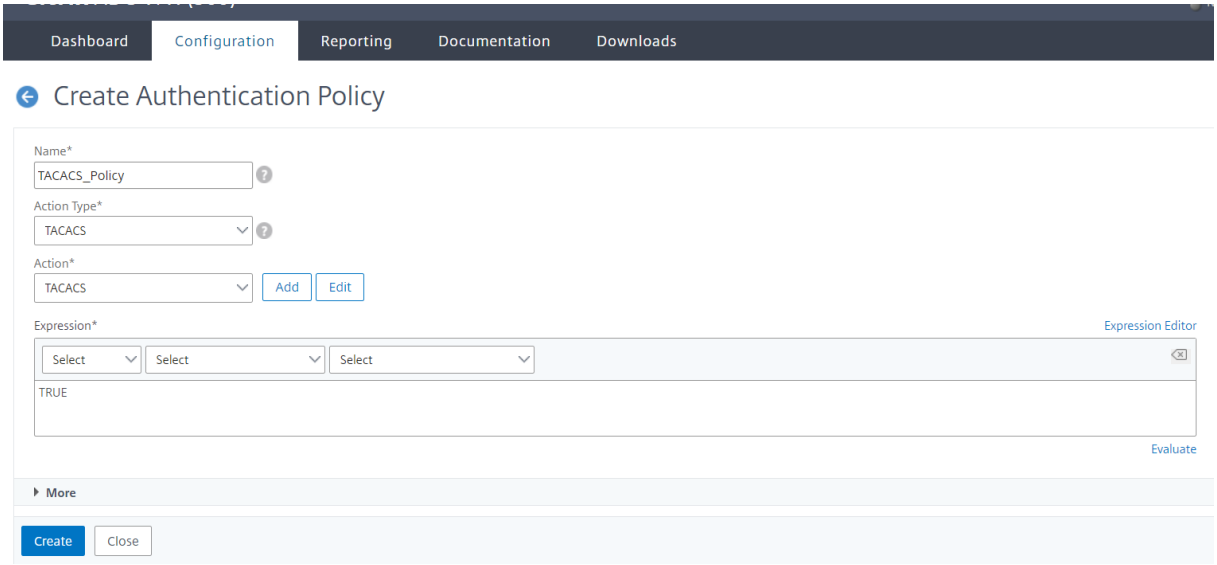
> **Important**
>
> - Citrix vous recommande de ne pas modifier les configurations associées TACACS lorsque vous exécutez une commande « clear ns config ».
> - La configuration liée à TACACS liée aux stratégies avancées est effacée et réappliquée lorsque le `RBAconfig` paramètre est défini sur NO dans la commande « clear ns config » pour la stratégie avancée.
> - Lorsque le `RBAconfig` paramètre est défini sur NON dans le cadre de l'opération « effacer la configuration », NetScaler conserve les sessions d'accès de gestion, en plus de conserver les configurations RBA et les politiques TACACS.

Vous pouvez configurer un serveur TACACS+ pour l'authentification. Comme pour l'authentification RADIUS, TACACS+ utilise une clé secrète, une adresse IP et le numéro de port. Le numéro de port par défaut est 49. Pour configurer l'appliance afin qu'elle utilise un serveur TACACS+, fournissez l'adresse IP du serveur et le code secret TACACS+. Vous devez spécifier le port uniquement lorsque le numéro de port du serveur utilisé est autre que le numéro de port par défaut 49.

Pour plus d'informations, voir Authentification TACACS.

Configurer l'authentification TACACS+ à l'aide de l'interface graphique

1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.
2. Cliquez sur **Ajouter** pour créer une stratégie d'authentification de type TACACS.
3. Cliquez sur **Créer** et **Fermer**.



Une fois les paramètres du serveur TACACS+ configurés sur l'appliance, liez la stratégie à l'entité globale du système.

Liez les stratégies d'authentification à l'entité globale du système à l'aide de la CLI

Lorsque les stratégies d'authentification sont configurées, liez les stratégies à l'entité globale du système.

À l'invite de la ligne de commande, procédez comme suit :

```
bind system global <policyName> [-priority <positive_integer>]
```

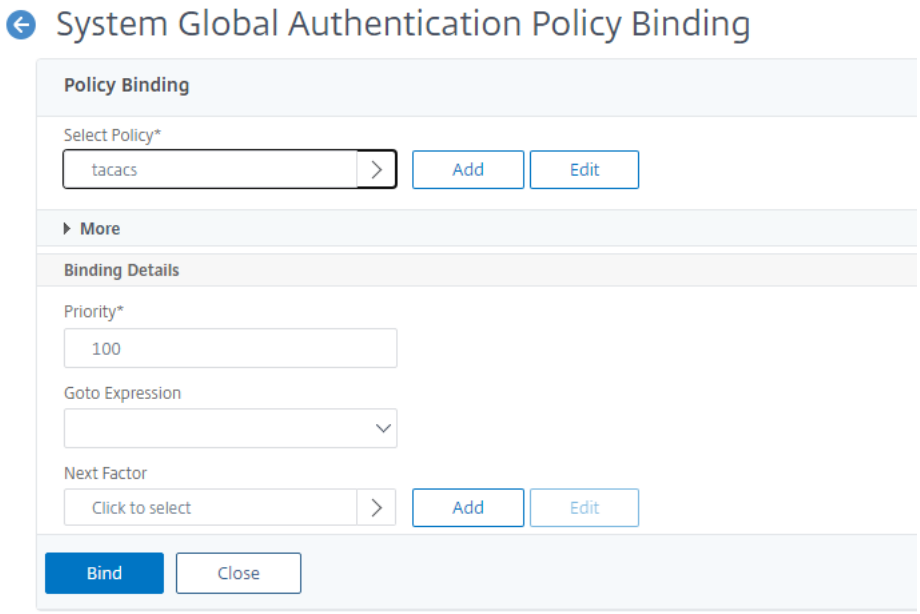
Exemple :

```
bind system global pol_classic -priority 10
```

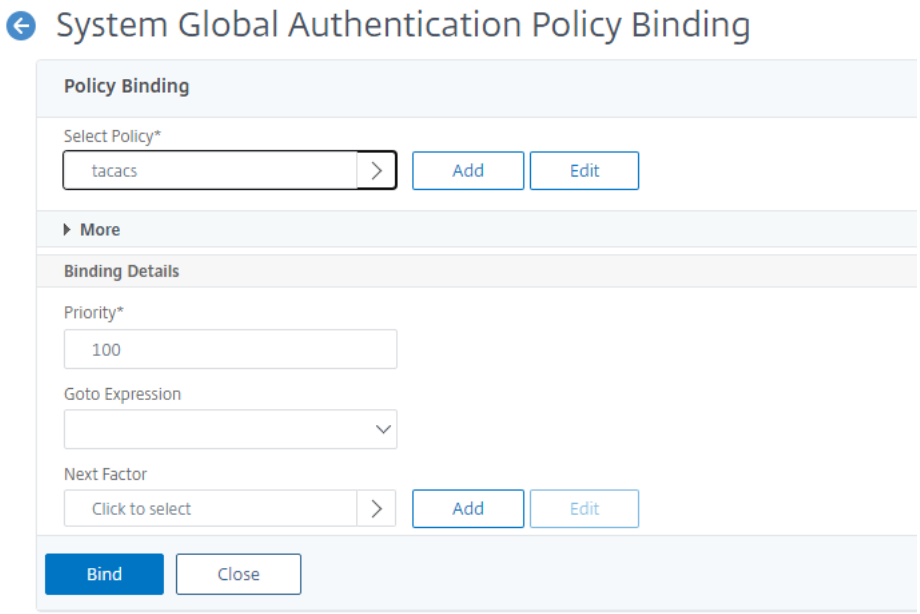
Lisez également l'article de Citrix CTX113820 pour en savoir plus sur l'authentification externe à l'aide de TACACS.

Lier les stratégies d'authentification à l'entité globale du système à l'aide de l'interface graphique

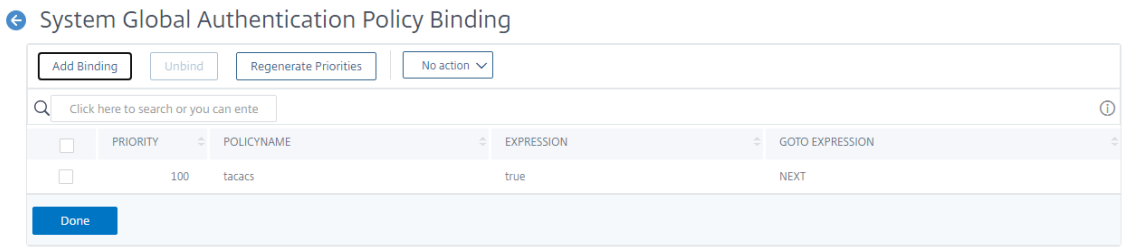
1. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégies d'authentification** > **Stratégie**.
2. Dans le volet d'informations, cliquez sur **Liaisons globales** pour créer une liaison de stratégie d'authentification globale du système.
3. Cliquez sur **Global Bindings**.



4. Sélectionnez la stratégie TACACS.
5. Dans la page Liaison de stratégie d'authentification globale du système, définissez les paramètres suivants :
   a) Sélectionnez Policy.
   b) Détails de la liaison



6. Cliquez sur **Lier** et **fermer**.
7. Cliquez sur **Global Bindings** (Liaisons globales) pour confirmer la stratégie liée au système global.



Pour plus d'informations sur l'extraction de groupe TACACS, consultez l'article CTX220024de Citrix.

Afficher le nombre de tentatives d'ouverture de session infructueuses pour les utilisateurs externes

L'appliance NetScaler affiche le nombre de tentatives de connexion non valides à l'utilisateur externe lorsque vous tentez au moins une connexion infructueuse avant de vous connecter à la console de gestion NetScaler.

> **Remarque**
>
> Actuellement, NetScaler prend uniquement en charge l'authentification interactive au clavier pour les utilisateurs externes lorsque le paramètre « PersistentLoginAttempts » est activé dans le paramètre système.

À l'invite de commande, tapez :

```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
persistentLoginAttempts (ENABLED | DISABLED )]
```

Exemple :

```
set aaa parameter -maxloginAttempts 5 -failedLoginTimeout 4 -persistentLoginAttempts
 ENABLED
```

```
1  Following msg will be seen to external user when he tries 1 invalid
       login attempt before successfully login to the ADC management access
       .
2
3  Connection established.
4  To escape to local shell, press 'Ctrl+Alt+]'.
5  ##############################################################################
   #
6
       #
7  #         WARNING: Access to this system is for authorized users only
                  #
```



```
#         Disconnect IMMEDIATELY if you are not an authorized user!
                #
#

    #
##############################################################################


WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Mon Aug 24 17:09:00 2020 from 10.10.10.10

The number of unsuccessful login attempts since the last successful
   login : 1
Done
>
The number of unsuccessful login attempts since the last successful
   login : 1
Done
>
<!--NeedCopy-->
```

Authentification par clé SSH pour les utilisateurs du système local

May 5, 2023

Pour disposer d'un accès utilisateur sécurisé à l'appliance NetScaler, vous pouvez utiliser l'authentification par clé publique du serveur SSH. L'authentification par clé SSH est préférée à l'authentification traditionnelle basée sur un nom d'utilisateur ou un mot de passe pour les raisons suivantes :

- Offre une puissance cryptographique supérieure à celle des mots de passe utilisateur.
- Élimine la nécessité de se souvenir de mots de passe compliqués et prévient les attaques d'épaule qui sont possibles si des mots de passe sont utilisés.
- Fournit une connexion sans mot de passe pour sécuriser davantage les scénarios d'automatisation.

NetScaler prend en charge l'authentification par clé SSH en appliquant le concept de clé publique et privée. L'authentification par clé SSH dans NetScaler peut être activée pour un utilisateur spécifique ou pour tous les utilisateurs locaux.

> **Remarque**
>
> Cette fonctionnalité est prise en charge uniquement pour les utilisateurs locaux de NetScaler et n'est pas prise en charge pour les utilisateurs externes.

Authentification par clé SSH pour les utilisateurs du système local

Dans une appliance NetScaler, un administrateur peut configurer une authentification par clé SSH pour un accès sécurisé au système. Lorsqu'un utilisateur se connecte à NetScaler à l'aide d'une clé privée, le système authentifie l'utilisateur à l'aide de la clé publique configurée sur l'appliance.

Configurer l'authentification par clé SSH pour les utilisateurs du système local NetScaler à l'aide de l'interface de ligne de commande

La configuration suivante vous aide à configurer l'authentification par clé pour les utilisateurs du système local NetScaler.

1. Connectez-vous à une appliance NetScaler à l'aide des informations d'identification de l'administrateur.
2. Par défaut, votre `sshd_config` fichier accède à ce chemin : **AuthorizedKeysFile /nsconfig/ssh/authorized_keys.**
3. **Ajoutez la clé publique au fichier authorized_keys : /nsconfig/ssh/authorized_keys.** Le chemin du fichier pour `sshd_config` est `/etc/sshd_config`.
4. Copiez le `sshd_config` fichier dans `/nsconfig` pour vous assurer que les modifications persistent même après le redémarrage de l'appliance.
5. Vous pouvez utiliser la commande suivante pour redémarrer votre `sshd` processus.

```
    kill -HUP `cat /var/run/sshd.pid`
<!--NeedCopy-->
```

> **Remarque**
>
> Si le fichier authorized_keys n'est pas disponible, vous devez d'abord en créer un, puis y ajouter la clé publique. **Assurez-vous que le fichier possède les autorisations suivantes pour les authorized_keys**.
>
> `root@NetScaler## chmod 0644 authorized_keys`

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
    1994
The Regents of the University of California. All rights reserved.
root@ns# cd /nsconfig/ssh
```



```
root@ns# vi authorized_keys
### Add public keys in authorized_keys file
<!--NeedCopy-->
```

Authentification par clé SSH spécifique à l'utilisateur pour les utilisateurs du système local

Dans une appliance NetScaler, un administrateur peut désormais configurer une authentification par clé SSH spécifique à l'utilisateur pour un accès sécurisé au système. L'administrateur doit d'abord configurer l' `Authorizedkeysfile` option dans le `sshd_config` fichier, puis y ajouter la clé publique pour un utilisateur du système. `authorized_keys`

> **Remarque**
>
> Si le fichier authorized_keys n'est pas disponible pour un utilisateur, l'administrateur doit d'abord en créer un, puis y ajouter la clé publique.

Configurer l'authentification par clé SSH spécifique à l'utilisateur à l'aide de l'interface de ligne de commande

La procédure suivante vous aide à configurer l'authentification par clé SSH spécifique à l'utilisateur pour les utilisateurs du système local NetScaler.

1. Connectez-vous à une appliance NetScaler à l'aide des informations d'identification de l'administrateur.
2. À l'invite shell, accédez au fichier `sshd_config` et ajoutez la ligne de configuration suivante :

   `AuthorizedKeysFile ~/.ssh/authorized_keys`

   > **Remarque**
   >
   > Le ~ est le répertoire personnel et diffère selon les utilisateurs. Il s'étend aux différents répertoires d'accueil.

3. Modifiez le répertoire en dossier utilisateur système et ajoutez les clés publiques dans le `authorized_keys` fichier.

   `/var/pubkey/<username>/.ssh/authorized_keys`

Une fois que vous avez terminé les étapes précédentes, redémarrez le `sshd` processus sur votre appliance à l'aide de la commande suivante :

```
    kill -HUP `cat /var/run/sshd.pid`

<!--NeedCopy-->
```


> **Remarque**
>
> Si le fichier authorized_keys n'est pas disponible, vous devez d'abord en créer un, puis ajouter la clé publique.

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
    1994
The Regents of the University of California. All rights reserved.
root@ns# cd /var/pubkey/<username>/
root@ns# ls
.ssh
root@ns# cd .ssh
root@ns# vi authorized_keys
### Add public keys in authorized_keys file

<!--NeedCopy-->
```

Lisez également l'article CTX109011 de Citrix pour savoir comment fonctionne l'accès SSH sécurisé à l'appliance NetScaler.

Authentification à deux facteurs pour les utilisateurs du système et les utilisateurs externes

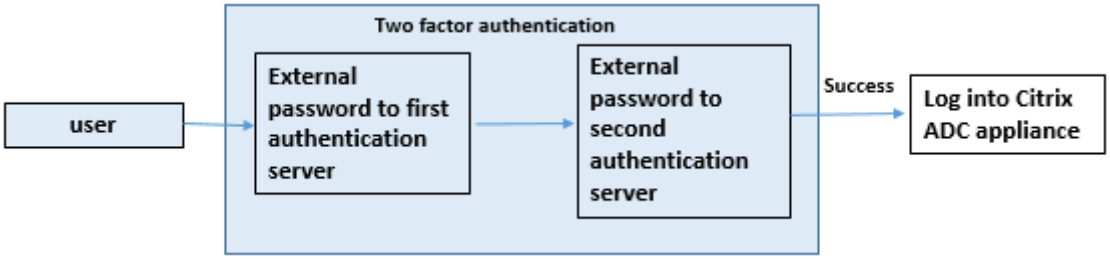
May 5, 2023

L'authentification à deux facteurs est un mécanisme de sécurité par lequel une appliance NetScaler authentifie un utilisateur du système à deux niveaux d'authentification. L'appliance n'accorde l'accès à l'utilisateur qu'après validation réussie des mots de passe par les deux niveaux d'authentification. Si un utilisateur est authentifié localement, le profil utilisateur doit être créé dans la base de données NetScaler. Si l'utilisateur est authentifié de manière externe, le nom d'utilisateur et le mot de passe doivent correspondre à l'identité de l'utilisateur enregistrée sur le serveur d'authentification externe.

> **Remarque**
>
> La fonctionnalité d'authentification à deux facteurs fonctionne uniquement à partir de NetScaler 12.1 build 51.16.

Comment fonctionne l'authentification à deux facteurs

Prenons l'exemple d'un utilisateur qui essaie de se connecter à une appliance NetScaler. Le serveur d'applications demandé envoie le nom d'utilisateur et le mot de passe au premier serveur d'authentification externe (RADIUS, TACACS, LDAP ou AD). Une fois le nom d'utilisateur et le mot de passe validés, l'utilisateur est invité à effectuer un deuxième niveau d'authentification. L'utilisateur peut désormais fournir le second mot de passe. L'utilisateur est autorisé à accéder à l'appliance NetScaler uniquement si les deux mots de passe sont corrects. Le schéma suivant illustre le fonctionnement de l'authentification à deux facteurs pour une appliance NetScaler.



Vous trouverez ci-dessous les différents cas d'utilisation permettant de configurer l'authentification à deux facteurs pour les utilisateurs externes et les utilisateurs du système.

Vous pouvez configurer l'authentification à deux facteurs sur une appliance NetScaler de différentes manières. Voici les différents scénarios de configuration pour l'authentification à deux facteurs sur une appliance NetScaler.

1. Authentification à deux facteurs (2FA) sur NetScaler, GUI, CLI, API et SSH.
2. Authentification externe activée et authentification locale désactivée pour les utilisateurs du système.
3. Authentification externe activée avec une authentification locale basée sur des règles pour les utilisateurs du système.
4. Authentification externe désactivée pour les utilisateurs du système lorsque l'authentification locale est activée.
5. Authentification externe activée et authentification locale activée pour les utilisateurs du système.
6. Authentification externe activée pour les utilisateurs LDAP sélectionnés

Cas d'utilisation 1 : authentification à deux facteurs (2FA) sur les interfaces NetScaler, GUI, CLI, API et SSH

L'authentification à deux facteurs est activée et disponible pour tous les accès de gestion NetScaler pour l'interface graphique, l'API et le SSH.

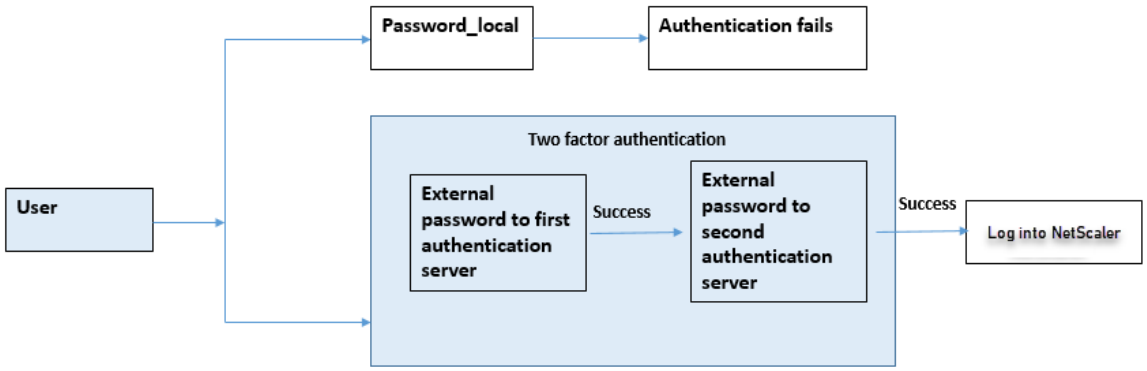
Cas d'utilisation 2 : authentification à deux facteurs prise en charge sur des serveurs d'authentification externes tels que LDAP, RADIUS, Active Directory et TACACS

Vous pouvez configurer l'authentification à deux facteurs sur les serveurs d'authentification externes suivants pour l'authentification utilisateur de premier et de second niveau.

- RADIUS
- LDAP
- Active Directory
- TACACS

Cas d'utilisation 3 : authentification externe activée et authentification locale désactivée pour les utilisateurs du système

Vous commencez le processus d'authentification en activant l'option d'authentification externe et en désactivant l'authentification locale pour les utilisateurs du système.



Procédez comme suit à l'aide de l'interface de ligne de commande :

1. Ajouter une action d'authentification pour la stratégie LDAP
2. Ajouter une stratégie d'authentification pour la stratégie LDAP
3. Ajouter une action d'authentification pour la stratégie RADIUS
4. Ajouter une stratégie d'authentification pour la stratégie RADIUS
5. Ajouter un schéma de connexion d'authentification
6. Ajouter et lier une étiquette de stratégie d'authentification au serveur RADIUS
7. Authentification globale du système Bind pour la stratégie LDAP
8. Désactiver l'authentification locale dans les paramètres du système

Ajouter une action d'authentification pour le serveur LDAP (authentification de premier niveau)

À l'invite de commande, tapez :


```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Ajouter une stratégie d'authentification pour le serveur LDAP (authentification de premier niveau)

À l'invite de commande, tapez :

```
add authentication policy <ldap policy name> -rule true -action <ldap
action name>
```

Exemple :

```
add authentication policy pol1 -rule true -action ldapact1
```

Ajouter une action d'authentification pour le serveur RADIUS (authentification de deuxième niveau)

À l'invite de commande, tapez :

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Exemple :

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Ajouter une stratégie d'authentification pour le serveur RADIUS (authentification de deuxième niveau)

À l'invite de commande, tapez :

```
add authentication policy <radius policy name> -rule true -action <rad
action name>
```

Exemple :

```
add authentication policy radpol11 -rule true -action radact1
```


Ajouter un schéma de connexion d'authentification

Vous pouvez utiliser le schéma de connexion « SingleAuth.xml » pour les utilisateurs du système afin de fournir le second mot de passe de l'appliance NetScaler. À l'invite de commande, tapez :

```
add authentication loginSchema <login schema name> -authenticationSchema
LoginSchema/SingleAuth.xml
```

Exemple :

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Ajouter et lier une étiquette de stratégie d'authentification au serveur RADIUS

À l'invite de commande, tapez :

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

```
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Exemple :

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
```

```
bind authentication policylabel label1 -policyName radpol11 -priority 1
```

Système d'authentification Bind global pour la stratégie LDAP

À l'invite de commande, tapez :

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Exemple :

```
bind system global pol11 -priority 1 -nextFactor label1
```

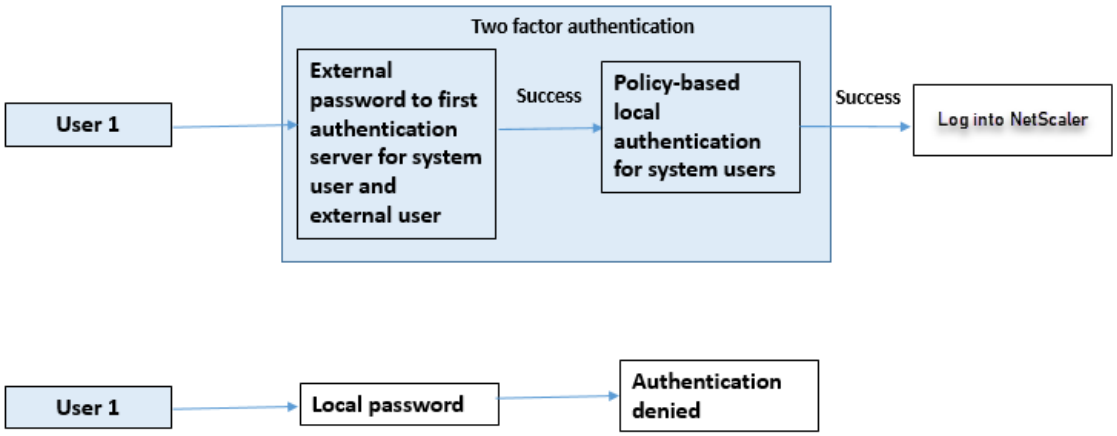
Désactiver l'authentification locale dans les paramètres du système

À l'invite de commande, tapez :

```
set system parameter -localauth disabled
```


Cas d'utilisation 4 : authentification externe activée pour l'utilisateur du système avec une stratégie d'authentification locale attachée

Dans ce scénario, l'utilisateur est autorisé à se connecter à l'appliance à l'aide d'une authentification à deux facteurs avec une évaluation de la stratégie d'authentification locale au deuxième niveau d'identification de l'utilisateur.



Procédez comme suit à l'aide de l'interface de ligne de commande.

1. Ajouter une action d'authentification pour le serveur LDAP
2. Ajouter une stratégie d'authentification pour la stratégie LDAP
3. Ajouter une stratégie d'authentification locale
4. Ajouter une étiquette de stratégie d'authentification
5. Lier la stratégie LDAP en tant que système global
6. Désactiver l'authentification locale dans les paramètres du système

Ajouter une action d'authentification pour le serveur LDAP (authentification de premier niveau)

À l'invite de commande, tapez :

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name -ssoNameAttribute name
```


Ajouter une stratégie d'authentification pour le serveur LDAP (authentification de premier niveau)

À l'invite de commande, tapez :

```
add authentication policy <ldap policy name> -rule true -action <ldap
action name>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Ajouter une stratégie d'authentification locale pour les utilisateurs du système (authentification de deuxième niveau)

À l'invite de commande, tapez :

```
add authentication policy <policy> -rule <rule> -action <action name>
```

Exemple :

```
add authentication policy local_policy -rule true -action LOCAL
```

Ajouter et lier une étiquette de stratégie d'authentification

À l'invite de commande, tapez :

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

> **Remarque**
>
> Pour l'accès de gestion, le type de stratégie doit être RBA_REQ.

Exemple :

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel label1 -policyName radpol11 -priority 1 -
gotoPriorityExpression NEXT
```

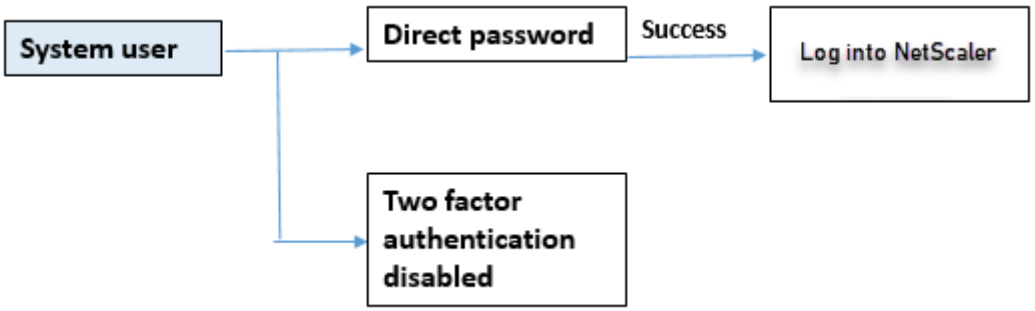

Désactiver l'authentification locale dans les paramètres du système

À l'invite de commande, tapez :

```
set system parameter -localauth disabled
```

Cas d'utilisation 5 : authentification externe désactivée et authentification locale activée pour l'utilisateur du système

Si « ExternalAuth » est désactivé pour l'utilisateur, cela indique qu'il n'existe pas sur le serveur d'authentification. L'utilisateur n'est pas authentifié auprès du serveur d'authentification externe, même si un utilisateur portant le même nom d'utilisateur existe sur le serveur externe authentifié. L'utilisateur est authentifié localement.



Pour activer le mot de passe utilisateur du système et désactiver l'authentification externe

À l'invite de commandes, tapez ce qui suit :

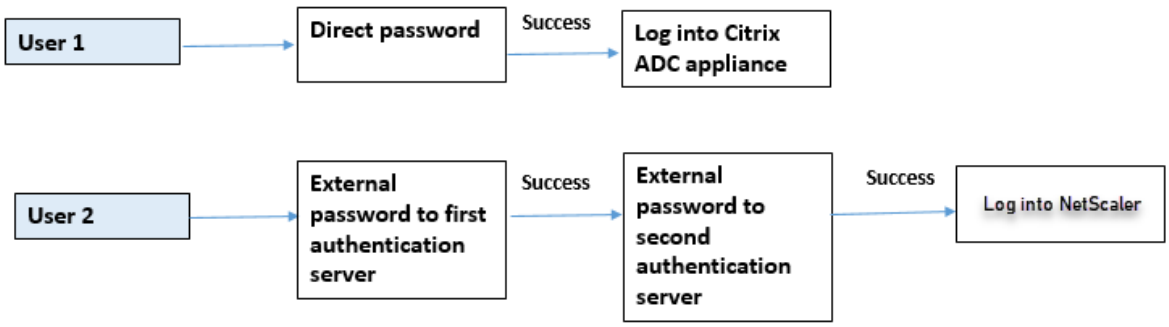
```
add system user <name> <password> -externalAuth DISABLED
```

Exemple :

```
add system user user1 password1 -externalAuth DISABLED
```

Cas d'utilisation 6 : authentification externe activée et authentification locale activée pour les utilisateurs du système

Configurer l'appliance pour authentifier les utilisateurs du système à l'aide d'un mot de passe local. Si cette authentification échoue, l'utilisateur est alors authentifié à l'aide d'un mot de passe d'authentification externe sur les serveurs d'authentification externes à deux niveaux.



Configurez les étapes suivantes à l'aide de l'interface de ligne de commande.

1. Ajouter une action d'authentification pour le serveur LDAP
2. Ajouter une stratégie d'authentification pour la stratégie LDAP
3. Ajouter une action d'authentification pour la stratégie RADIUS
4. Ajouter une stratégie d'authentification pour la stratégie RADIUS
5. Ajouter un schéma de connexion d'authentification
6. Ajouter une étiquette de stratégie d'authentification
7. Liez l'étiquette de la stratégie d'authentification au schéma de connexion
8. Système d'authentification Bind global pour la stratégie RADIUS
9. Système d'authentification Bind global pour la stratégie LDAP

Ajouter une action d'authentification pour le serveur LDAP

À l'invite de commande, tapez :

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Ajouter une stratégie d'authentification pour la stratégie LDAP

À l'invite de commande, tapez :

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```


Exemple :

```
add authentication policy pol1 -rule true -action ldapact1
```

Ajouter une action d'authentification pour le serveur RADIUS

À l'invite de commande, tapez :

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Exemple :

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Ajouter une stratégie d'authentification avancée pour le serveur RADIUS

À l'invite de commande, tapez :

```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Exemple :

```
add authentication policy radpol11 -rule true -action radact1
```

Ajouter un schéma de connexion d'authentification

Vous pouvez utiliser le schéma de connexion SingleAuth.xml pour afficher la page de connexion et authentifier l'utilisateur du système lors de l'authentification de deuxième niveau.

À l'invite de commande, tapez :

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Exemple :

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Ajouter et lier une étiquette de stratégie d'authentification à la stratégie d'authentification RADIUS pour la connexion utilisateur

À l'invite de commande, tapez :

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```


Exemple :

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Exemple :

```
bind authentication policylabel label1 -policyName rad pol11 -priority 1
```

Stratégie d'authentification Bind globale

À l'invite de commande, tapez :

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```

Exemple :

```
bind system global radpol11 -priority 1 -nextFactor label11
```

Cas d'utilisation 7 : Authentification externe activée uniquement pour certains utilisateurs externes

Pour configurer des utilisateurs externes sélectifs avec une authentification à deux facteurs conformément au filtre de recherche configuré dans l'action LDAP, tandis que les autres utilisateurs du système sont authentifiés à l'aide d'une authentification à facteur unique.

Configurez les étapes suivantes à l'aide de l'interface de ligne de commande.

1. Ajouter une action d'authentification pour le serveur LDAP
2. Ajouter une stratégie d'authentification pour la stratégie LDAP
3. Ajouter une action d'authentification pour la stratégie RADIUS
4. Ajouter une stratégie d'authentification pour la stratégie RADIUS
5. Ajouter un schéma de connexion d'authentification
6. Ajouter une étiquette de stratégie d'authentification
7. Liez l'étiquette de la stratégie d'authentification au schéma de connexion
8. Système d'authentification Bind global pour la stratégie RADIUS

Ajouter une action d'authentification pour le serveur LDAP

À l'invite de commande, tapez :


```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Ajouter une stratégie d'authentification pour la stratégie LDAP

À l'invite de commande, tapez :

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Exemple :

```
add authentication policy pol1 -rule true -action ldapact1
```

Ajouter une action d'authentification pour le serveur RADIUS

À l'invite de commande, tapez :

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Exemple :

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Ajouter une stratégie d'authentification avancée pour le serveur RADIUS

À l'invite de commande, tapez :

```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Exemple :

```
add authentication policy radpol11 -rule true -action radact1
```


Ajouter un schéma de connexion d'authentification

Vous pouvez utiliser le schéma de connexion SingleAuth.xml pour fournir la page de connexion permettant à l'appliance d'authentifier un utilisateur du système à un deuxième niveau d'authentification.

À l'invite de commande, tapez :

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Exemple :

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Ajouter et lier une étiquette de stratégie d'authentification à la stratégie d'authentification RADIUS pour la connexion utilisateur

À l'invite de commande, tapez :

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

Exemple :

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Exemple :

```
bind authentication policylabel label1 -policyName radpol11 -priority
```

Stratégie d'authentification Bind globale

À l'invite de commande, tapez :

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```

Exemple :

```
bind system global radpol11 -priority 1 -nextFactor label11
```

Pour configurer sans authentification à deux facteurs pour les utilisateurs du groupe à l'aide du filtre de recherche, procédez comme suit :

1. Ajouter une action d'authentification pour le serveur LDAP
2. Ajouter une stratégie d'authentification pour le serveur LDAP
3. Système d'authentification Bind global pour le serveur LDAP

Ajouter une action d'authentification pour le serveur LDAP

À l'invite de commande, tapez :

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
searchFilter<>
```

Exemple :

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name - searchFilter "memberOf=CN=grp4,CN=Users,DC=
aaatm-test,DC=com"
```

Ajouter une stratégie d'authentification pour le serveur LDAP

À l'invite de commande, tapez :

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Exemple :

```
add authentication policy pol1 -rule true -action ldapact1
```

Système d'authentification Bind global pour la stratégie LDAP

À l'invite de commande, tapez :

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Exemple :

```
bind system global pol11 -priority 1 -nextFactor label11
```

Afficher un message d'invite personnalisé pour une authentification à deux facteurs

Lorsque vous configurez un champ de mot de passe à deux facteurs avec le fichier SingleAuth.xml sur `/flash/nsconfig/loginschema/LoginSchema`

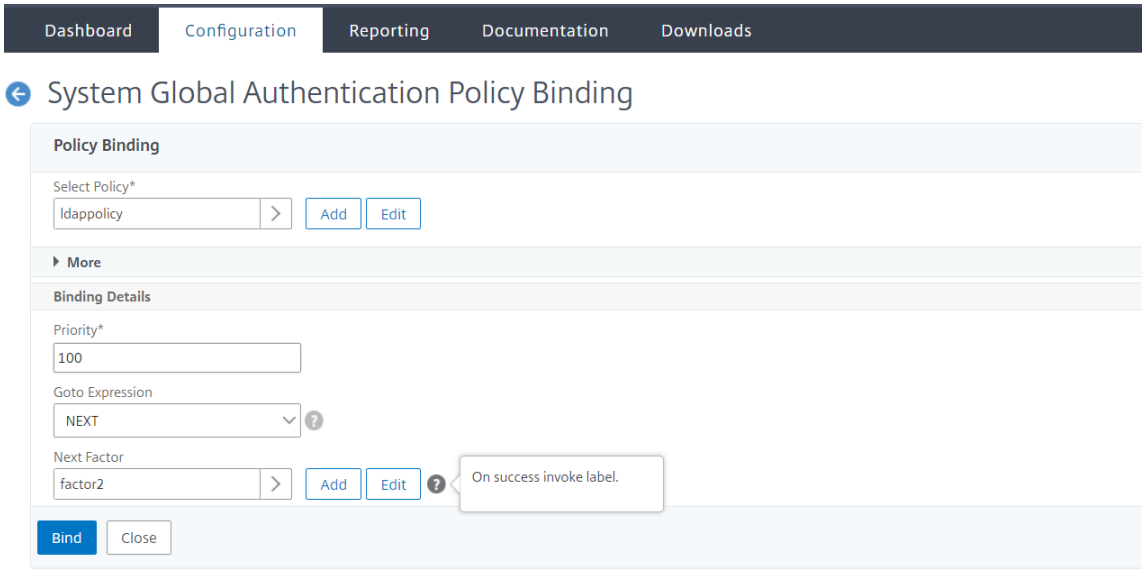
Voici l'extrait d'un fichier SingleAuth.xml où « SecondPassword : » est le nom du deuxième champ de mot de passe qui est invité à saisir un second mot de passe.


```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
   /1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext/>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</
   SaveID><Type>username</Type></Credential><Label><Text>
   singleauth_user_name</Text><Type>nsg-login-label</Type></Label><
   Input><AssistiveText>singleauth_please_supply_either_domain\
   username_or_user@fully.qualified.domain</AssistiveText><Text><Secret
   >false</Secret><ReadOnly>false</ReadOnly><InitialValue/><Constraint
   >.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password
   </SaveID><Type>password</Type></Credential><Label><Text>
   SecondPassword:</Text><Type>nsg-login-label</Type></Label><Input><
   Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue/><
   Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>
   singleauth_first_factor</Text><Type>nsg_confirmation</Type></Label><
   Input/></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials
   </Type></Credential><Label><Text>singleauth_remember_my_password</
   Text><Type>nsg-login-label</Type></Label><Input><CheckBox><
   InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential
   ><Label><Type>none</Type></Label><Input><Button>singleauth_log_on</
   Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

Configuration de l'authentification à deux facteurs à l'aide de l'interface graphique NetScaler

1. Connectez-vous à l'appliance NetScaler.

2. Accédez à **Système** > **Authentification** > **Stratégies avancées** > **Stratégie**.
3. Cliquez sur Ajouter pour créer la stratégie d'authentification de premier niveau.
4. Dans la page **Créer une stratégie d'authentification**, définissez les paramètres suivants.
    a) Nom. Nom de la stratégie
    b) Type d'action. Sélectionnez le type d'action comme LDAP, Active Directory, RADIUS, TACACS, etc.
    c) Action. Action d'authentification (profil) à associer à la stratégie. Vous pouvez choisir une action d'authentification existante ou cliquer sur le signe plus et créer une action du type approprié.
    d) Expression : Fournissez une expression de stratégie avancée.
5. Cliquez sur **Créer**, puis sur **Fermer**.
    a) Expression : Fournissez une expression de stratégie avancée.
6. Cliquez sur **Create**.
7. Cliquez sur **Ajouter** pour créer la stratégie d'authentification de deuxième niveau.
8. Sur la page **Créer une stratégie d'authentification**, définissez les paramètres suivants :
    a) Nom. Nom de la stratégie
    b) Type d'action. Sélectionnez le type d'action comme LDAP, Active Directory, RADIUS, TACACS, etc.
    c) Action. Action d'authentification (profil) à associer à la stratégie. Vous pouvez choisir une action d'authentification existante ou cliquer sur l'icône + pour créer une action du type approprié.
    d) Expression : Fournir une expression de stratégie avancée
9. Cliquez sur **Créer**, puis sur **Fermer**.
    a) Expression : Fournissez une expression de stratégie avancée.
10. Cliquez sur **Create**.
11. Sur la page **Stratégies d'authentification**, cliquez sur **Global Binding**.
12. Sur la page **Créer une liaison de stratégie d'authentification globale**, sélectionnez la stratégie d'authentification de premier niveau, puis cliquez sur **Ajouter une liaison**.
13. Sur la page **Liaison de stratégies**, sélectionnez la stratégie d'authentification et définissez le paramètre de liaison de stratégie suivant.
    a) Facteur suivant. Sélectionnez l'étiquette de la stratégie d'authentification de deuxième niveau.
14. Cliquez sur **Lier** et **fermer**.



15. Cliquez sur **Terminé**.
16. Connectez-vous à l'appliance NetScaler pour l'authentification de deuxième niveau. L'utilisateur peut désormais fournir le second mot de passe. L'utilisateur est autorisé à accéder à l'appliance NetScaler uniquement si les deux mots de passe sont corrects.

> **Remarque**
>
> Le TACACS configuré pour une authentification à second facteur ne prend pas en charge l'autorisation et la comptabilité, même si vous l'activez sur la commande « TACACSaction ». Le deuxième facteur est utilisé uniquement à des fins d'authentification.

Consultez également la rubrique Authentification à deux facteurs dans la rubrique Authentification NetScaler nFactor .

Authentification utilisateur système restreinte aux interfaces de gestion NetScaler

May 5, 2023

Vous pouvez restreindre l'accès des utilisateurs du système à des interfaces de gestion NetScaler spécifiques telles que l'interface de ligne de commande ou l'API. Le `allowedManagementInterface` paramètre définit la liste des interfaces de gestion autorisées. Par exemple, si l'interface de gestion d'un utilisateur ou d'un groupe est définie sur API, tous les utilisateurs du groupe peuvent accéder à NetScaler via l'API et non via l'interface de ligne de commande. Toutefois, l'interface graphique NetScaler fait partie de l'interface API et les utilisateurs disposant d'une autorisation d'API peuvent également accéder à l'interface graphique.

> **Remarque :**
>
> Par défaut, les utilisateurs et les groupes ont accès à toutes les interfaces (CLI, API et GUI).

Vous pouvez configurer le paramètre au niveau de l'utilisateur ou au niveau du groupe d'utilisateurs. Lorsque vous configurez au niveau du groupe, la configuration est appliquée à tous les comptes utilisateurs du groupe. Si un utilisateur est lié à plusieurs groupes, l'appliance permet d'accéder à un ensemble agrégé d'interfaces de gestion. Vous pouvez spécifier des paramètres pour un utilisateur d'un groupe en configurant le paramètre au niveau de l'utilisateur. Dans ce cas, le paramètre de niveau utilisateur est configuré pour un groupe.
Dans certains scénarios, lorsque le client utilise un serveur d'authentification externe pour gérer les comptes utilisateurs, les détails du serveur sont configurés sur l'appliance. Dans ce cas, l'administrateur peut créer un groupe d'utilisateurs dans l'appliance NetScaler et y ajouter tous les utilisateurs (regroupés sur le serveur externe). Par exemple, tous les utilisateurs gérés sur le serveur externe sont ajoutés au groupe API_Users et l'administrateur peut configurer le groupe localement sur l'appliance.

> **Remarque :**
>
> L'appliance NetScaler autorise uniquement `nsroot` l'administrateur (superutilisateur) à configurer le paramètre et n'autorise aucun utilisateur du système à modifier le paramètre.

Configurer l'accès des utilisateurs aux interfaces de gestion NetScaler à l'aide de l'interface de ligne de commande

Pour autoriser les utilisateurs à accéder à une interface de gestion spécifique, vous devez définir le paramètre d'interface de gestion autorisé. À l'invite de commande, tapez :

```
set system group <groupName> [-allowedManagementInterface ( CLI | API )]
```

Exemple :

```
set system group network_usergroup -allowedManagementInterface CLI
```

Pour la description des paramètres, reportez-vous à la rubrique Référence des commandes d'authentification et d'autorisation .

Pour en savoir plus sur les interfaces GUI et CLI, consultez la rubrique Access NetScaler .

Configurations TCP

May 5, 2023

Les configurations TCP pour une appliance NetScaler peuvent être spécifiées dans une entité appelée profil TCP, qui est un ensemble de paramètres TCP. Le profil TCP peut ensuite être associé à des services ou à des serveurs virtuels qui souhaitent utiliser ces configurations TCP.

Un profil TCP par défaut peut être configuré pour définir les configurations TCP qui seront appliquées par défaut, globalement à tous les services et serveurs virtuels.

> **Remarque :**
>
> Lorsqu'un paramètre TCP a des valeurs différentes pour le service, le serveur virtuel et globalement, la valeur de l'entité la plus spécifique (le service) est donnée la priorité la plus élevée. L'appliance NetScaler propose également d'autres approches pour configurer TCP. Lisez la suite pour plus d'informations.

Configuration TCP prise en charge

L'appliance NetScaler prend en charge les fonctionnalités TCP suivantes :

Défendre TCP contre les attaques par usurpation d'identité

L' **implémentation de l'atténuation des fenêtres par NetScaler** est conforme à la norme RFC 4953.

Notification explicite de congestion (ECN)

L'appliance envoie une notification de l'état de congestion du réseau à l'expéditeur des données et prend des mesures correctives en cas d'encombrement ou de corruption des données. L'implémentation NetScaler de l'ECN est conforme à la norme RFC 3168.

Mesure du temps aller-retour (RTTM) à l'aide de l'option d'horodatage

Pour que l'option TimeStamp fonctionne, au moins un côté de la connexion (client ou serveur) doit la prendre en charge. L'implémentation de `TimeStamp` cette option par NetScaler est conforme à la norme RFC 1323.

Détection de retransmissions fausses

Cette détection peut être effectuée à l'aide de l'accusé de réception sélectif en double TCP (D-SACK) et de la récupération RTO directe (F-RTO). S'il y a des retransmissions fausses, les configurations de contrôle de congestion sont rétablies à leur état d'origine. L'implémentation NetScaler de D-SACK est conforme à la norme RFC 2883 et F-RTO est conforme à la norme RFC 5682.

Contrôle de la congestion

Cette fonctionnalité utilise les algorithmes New-Reno, BIC, CUBIC, Nile et TCP Westwood.

Mise à l'échelle des fenêtres

Cela augmente la taille de la fenêtre de **réception TCP** au-delà de sa valeur maximale de 65 535 octets.

Points à prendre en compte avant de configurer la mise à l'échelle des fenêtres

- Vous ne définissez pas de valeur élevée pour le facteur d'échelle, car cela pourrait avoir des effets négatifs sur l'appliance et le réseau.
- Vous ne configurez pas la mise à l'échelle des fenêtres à moins de savoir clairement pourquoi vous souhaitez modifier la taille de la fenêtre.
- Les deux hôtes de la connexion TCP envoient une option d'échelle de fenêtre lors de l'établissement de la connexion. Si un seul côté d'une connexion définit cette option, la mise à l'échelle des fenêtres n'est pas utilisée pour la connexion.
- Chaque connexion pour la même session est une session de mise à l'échelle des fenêtres indépendante. Par exemple, lorsque la demande d'un client et la réponse du serveur passent par l'appliance, il est possible de mettre à l'échelle des fenêtres entre le client et l'appliance sans mise à l'échelle des fenêtres entre l'appliance et le serveur.

Fenêtre de congestion maximale TCP

La taille de la fenêtre est configurable par l'utilisateur. La valeur par défaut est de 8 190 octets.

Accusé de réception sélectif (SACK)

Cela utilise le récepteur de données (une appliance NetScaler ou un client) pour informer l'expéditeur de tous les segments qui ont été reçus avec succès.

Accusé de réception avant (FACK)

Cette fonctionnalité évite la congestion du protocole TCP en mesurant explicitement le nombre total d'octets de données en suspens sur le réseau et en aidant l'expéditeur (NetScaler ou client) à contrôler la quantité de données injectées dans le réseau pendant les délais de retransmission.

Multiplexage de connexions TCP

Cette fonctionnalité permet de réutiliser les connexions TCP existantes. L'appliance NetScaler stocke les connexions TCP établies vers le pool de réutilisation. Chaque fois qu'une demande client est reçue, l'appliance recherche une connexion disponible dans le pool de réutilisation et sert le nouveau client

si la connexion est disponible. Si elle n'est pas disponible, l'appliance crée une connexion pour la demande du client et stocke la connexion au pool de réutilisation. NetScaler prend en charge le multiplexage des connexions pour les types de connexion HTTP, SSL et DataStream.

Mise en mémoire tampon de réception dynamique

Cela permet d'ajuster dynamiquement la mémoire tampon de réception en fonction des conditions de mémoire et du réseau.

Connexion MPTCP

Connexions MPTCP entre le client et NetScaler. Les connexions MPTCP ne sont pas prises en charge entre NetScaler et le serveur principal. L'implémentation du protocole MPTCP par NetScaler est conforme à la norme RFC 6824.

Vous pouvez afficher les statistiques MPTCP telles que les connexions MPTCP actives et les connexions de sous-flux actives à l'aide de l'interface de ligne de commande.

À l'invite de commandes, tapez l'une des commandes suivantes pour afficher un résumé ou un résumé détaillé des statistiques MPTCP ou pour effacer l'affichage des statistiques :

1. `Stat MPTCP`
2. `Stat mptcp -detail`
3. `Clearstats basic`

> **Remarque :**
>
> Pour établir une connexion MPTCP, le client et l'appliance NetScaler doivent prendre en charge la même version de MPTCP. Si vous utilisez l'appliance NetScaler comme passerelle MPTCP pour vos serveurs, ceux-ci ne doivent pas nécessairement prendre en charge le protocole MPTCP. Lorsque le client démarre une nouvelle connexion MPTCP, l'appliance identifie la version MPTPC du client à partir de l'option MP_CAPABALE du paquet SYN. Si la version du client est supérieure à celle prise en charge par l'appliance, celle-ci indique sa version la plus élevée dans l'option MP_CAPABALE du paquet SYN-ACK. Le client revient ensuite à une version inférieure et envoie le numéro de version dans l'option MP_CAPABALE du paquet ACK. Si cette version est prise en charge, l'appliance poursuit la connexion MPTCP. Sinon, l'appliance reprend un protocole TCP normal. L'appliance NetScaler ne lance pas de sous-flux (MP_JOIN). L'appliance s'attend à ce que le client lance des sous-flux.

Prise en charge de la publicité d'adresses supplémentaires (ADD_ADDR) dans MPTCP

Dans un déploiement MPTCP, si un serveur virtuel est lié à un ensemble d'adresses IP supplémentaires de serveur virtuel, la fonctionnalité d'annonce d'adresse supplémentaire (ADD_ADDR) annonce

l'adresse IP des serveurs virtuels liés à l'ensemble d'adresses IP. Les clients peuvent initier des MP_JOIN sous-flux supplémentaires vers les adresses IP annoncées.

Points à retenir sur la fonctionnalité MPTCP ADD_ADDR

- Vous pouvez envoyer un maximum de 10 adresses IP dans le cadre de ADD_ADDR cette option. Si le paramètre mptcpAdvertise est activé sur plus de 10 adresses IP, après avoir fait la publicité de l'adresse IP 10, l'appliance ignore le reste des adresses IP.
- Si le sous-flux MP-CAPABLE est défini sur l'une des adresses IP du jeu d'adresses IP au lieu de l'adresse IP du serveur virtuel principal, l'adresse IP du serveur virtuel est annoncée si le paramètre mptcpAdvertise est activé pour l'adresse IP du serveur virtuel.

Configurer plus de fonctionnalités de publicité d'adresses (ADD_ADDR) pour annoncer une adresse VIP supplémentaire à l'aide de l'interface de ligne de commande

Vous pouvez configurer la MPTCP ADD_ADDR fonctionnalité pour les types d'adresses IPv4 et IPv6. En général, plusieurs adresses IP IPv4 et IPv6 peuvent être attachées à un seul ensemble d'adresses IP et le paramètre peut être activé sur n'importe quel sous-ensemble d'adresses IP. Dans la fonction ADD_ADDR, seules les adresses IP sur lesquelles l'option « MPTCPAdVertise » est activée et les adresses IP restantes du jeu d'adresses IP sont ignorées.
Procédez comme suit pour configurer la ADD_ADDR fonctionnalité :

1. Ajoutez un ensemble d'adresses IP.
2. Ajoutez une adresse IP de type IP de serveur virtuel (VIP) avec la publicité MPTCP activée.
3. Liez l'adresse IP au jeu d'adresses IP.
4. Configurez le jeu d'adresses IP avec le serveur virtuel d'équilibrage de charge.

Ajouter un ensemble d'adresses IP

À l'invite de commande, tapez :

```
add ipset <name> [-td <positive_integer>]
<!--NeedCopy-->
```

Exemple :

```
add ipset ipset_1
<!--NeedCopy-->
```

Ajouter une adresse IP de type IP de serveur virtuel (VIP) avec la publicité MPTCP activée

Au niveau de la commande, tapez :


```
add ns ip <IPAddress>@ <netmask> [-mptcpAdvertise ( YES | NO )] -type <
    type>
<!--NeedCopy-->
```

Exemple :

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
```

Lier les adresses IP au jeu d'adresses IP

À l'invite de commande, tapez :

```
bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Exemple :

```
bind ipset ipset_1 10.10.10.10
```

Configuration du jeu d'adresses IP sur un serveur virtuel d'équilibrage de charge

À l'invite de commande, tapez :

```
set lb vserver <name> [-ipset  <string>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Exemple de configuration :

```
Add ipset ipset_1
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
bind ipset ipset_1 10.10.10.10
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Configurer l'adresse IP externe publicitaire à l'aide de la fonctionnalité ADD_ADDR

Si l'adresse IP annoncée appartient à l'entité externe et que l'appliance NetScaler doit publier l'adresse IP, le paramètre « MPTCPAdvertise » doit être activé avec les paramètres d'état et ARP désactivés.

Procédez comme suit ADD_ADDR pour configurer la publicité de l'adresse IP externe.

1. Ajoutez une adresse IP de type IP de serveur virtuel (VIP) avec la publicité MPTCP activée.
2. Liez l'adresse IP au jeu d'adresses IP.
3. Lier le jeu d'adresses IP au serveur virtuel d'équilibrage de charge

Ajouter une adresse IP externe de type IP de serveur virtuel (VIP) avec la publicité MPTCP activée

À l'invite de commande, tapez :

```
1 add ns ip <IPAddress>@ <External-IP-mask -type VIP> [-mptcpAdvertise (
     YES | NO )] -type <type> -state DISABLED -arp DISABLED
2 <!--NeedCopy-->
```

Exemple :

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP -state
DISABLED -arp DISABLED
```

Lier les adresses IP au jeu d'adresses IP

À l'invite de commande, tapez :

```
1 bind ipset <name> <IPAddress>
2 <!--NeedCopy-->
```

Exemple :

```
bind ipset ipset_1 10.10.10.10
```

Configuration du jeu d'adresses IP sur un serveur virtuel d'équilibrage de charge

À l'invite de commande, tapez :

```
1 set lb vserver <name> [-ipset  <string>]
2 <!--NeedCopy-->
```

Exemple :

```
set lb vserver lb1 -ipset ipset_1
```

Exemple de configuration :

```
1 add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
     state DISABLED -arp DISABLED
2 bind ipset ipset_1 10.10.10.10
3 set lb vserver lb1 -ipset ipset_1
```

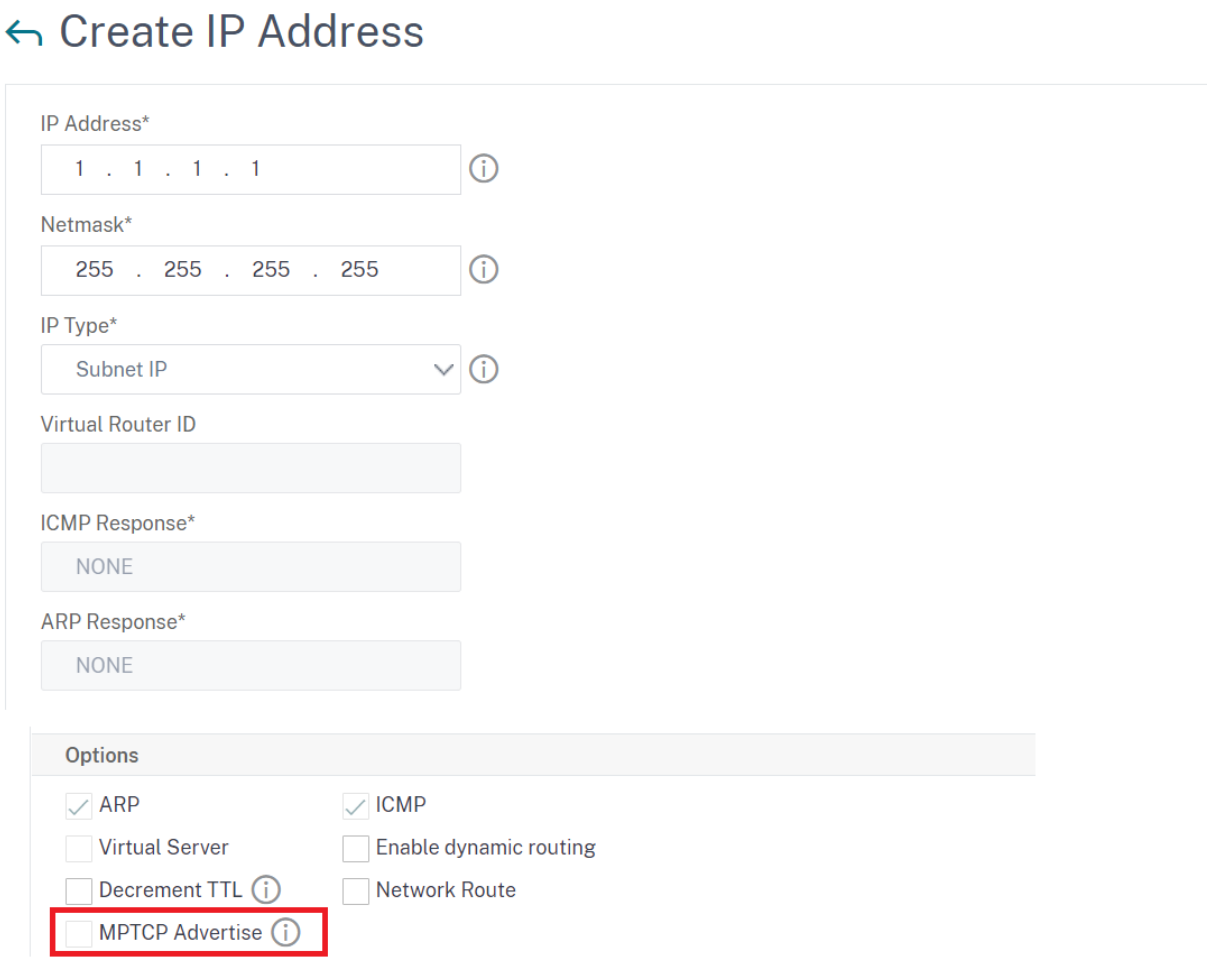


```
<!--NeedCopy-->
```

Annoncez une adresse IP auprès des clients compatibles MPTCP à l'aide de l'interface graphique NetScaler

Effectuez l'étape suivante pour annoncer l'adresse IP aux clients compatibles MPTCP :

1. Accédez à **Système > Réseau > IP**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la page **Créer une adresse IP**, activez la case à cocher **MPTCP Advertise** pour définir le paramètre. Par défaut, il est désactivé.



Extraction de l'option de superposition de chemin TCP/IP et insertion de l'en-tête HTTP Client-IP

Extraction de la superposition de chemin TCP/IP et insertion d'en-tête HTTP client-IP. Le transport de données via des réseaux superposés utilise souvent la terminaison de connexion ou la traduction d'adresses réseau (NAT), dans laquelle l'adresse IP du client source est perdue. Pour éviter cela, l'appliance NetScaler extrait l'option de superposition de chemins TCP/IP et insère l'adresse IP du client source dans l'en-tête HTTP. Avec l'adresse IP dans l'en-tête, le serveur Web peut identifier le client source qui a établi la connexion. Les données extraites sont valides pendant toute la durée de vie de la connexion TCP, ce qui empêche l'hôte de saut suivant d'avoir à réinterpréter l'option. Cette option s'applique uniquement aux services Web sur lesquels l'option d'insertion Client-IP est activée.

TCP segmentation offload

Décharge la segmentation TCP vers la carte réseau. Si vous définissez l'option sur « AUTOMATIQUE », la segmentation TCP est déchargée vers la carte réseau, si la carte réseau est prise en charge.

cookie de synchronisation pour la connexion TCP avec les clients

Ceci est utilisé pour résister aux attaques d'inondation SYN. Vous pouvez activer ou désactiver le mécanisme `SYNCOOKIE` de prise de contact TCP avec les clients. La désactivation `SYNCOOKIE` empêche la protection `SYN` contre les attaques sur l'appliance NetScaler.

Apprendre MSS pour activer l'apprentissage MSS pour tous les serveurs virtuels configurés sur l'appliance

Paramètres TCP pris en charge

Le tableau suivant fournit une liste des paramètres TCP et leur valeur par défaut configurés sur une appliance NetScaler.

|Paramètre|Valeur par défaut|Description|
|— |— |— |
|Gestion des fenêtres|
TCP Delayed-ACK Timer	100 millisecondes	Délai d'attente pour ACK retardé TCP, en millisecondes.
Délai d'expiration minimum de retransmission TCP (RTO) en millions de secondes	1000 milli sec	Délai de retransmission minimal, en millisecondes, spécifié par incréments de 10 millisecondes (la valeur doit donner un nombre entier si elle est divisée par 10)
Connection idle time before starting keep-alive probes	900 secondes	Déposez silencieusement les connexions établies par TCP sur les délais d'attente d'inactivité, les connexions établies lors du délai d'attente d'inactivité
TCP Timestamp Option	DÉSACTIVÉ	L'option horodatage permet une mesure RTT précise. Activez ou

désactivez l'option Horodatage TCP.|
Multipath TCP session timeout	0 seconde	Délai d'expiration de session MPTCP en secondes. Si cette valeur n'est pas définie, inactif. Les sessions MPTCP sont vides après le délai d'inactivité du client du serveur virtuel.
Silently Drop HalfClosed connections on idle timeout	0 seconde	Abandonnez silencieusement les connexions TCP semi-fermées en période d'inactivité.
Silently Drop Established connections on idle timeout	DÉSACTIVÉ	Supprimer silencieusement les connexions établies par TCP en période d'inactivité
Gestion de la mémoire
Taille de la mémoire tampon TCP	131072 octets	La taille de la mémoire tampon TCP est la taille de la mémoire tampon de réception sur NetScaler. Cette taille de mémoire tampon est annoncée aux clients et aux serveurs par NetScaler et contrôle leur capacité à envoyer des données à NetScaler. La taille de la mémoire tampon par défaut est de 8 Ko et il est généralement prudent de l'incrémenter lorsque vous parlez à des batteries de serveurs internes. La taille de la mémoire tampon dépend également de la couche d'application réelle dans NetScaler. Par exemple, pour les cas de point de terminaison SSL, elle est définie à 40 Ko et pour la compression, elle est définie à 96 K. **Remarque :** l'argument de taille de la mémoire tampon doit être défini pour que des ajustements dynamiques puissent avoir lieu.
TCP Send Buffer Size	8190 octets	TCP Send Buffer Size
Mise en mémoire tampon de réception dynamique TCP	DÉSACTIVÉ	Activez ou désactivez la mise en mémoire tampon de réception dynamique. Lorsqu'il est activé, il permet d'ajuster dynamiquement le tampon de réception en fonction des conditions de mémoire et du réseau. **Remarque :** L'argument de taille de la mémoire tampon doit être défini pour que les ajustements dynamiques aient lieu
TCP Max congestion window(CWND)	524288 octets	TCP Maximum Congestion Window
Window Scaling status	ENABLED	Activez ou désactivez la mise à l'échelle des fenêtres.
Window Scaling factor	8	Facteur utilisé pour calculer la nouvelle taille de fenêtre. Cet argument n'est nécessaire que lorsque la mise à l'échelle des fenêtres est activée.
Configuration de la connexion
Keep-alive probes	DÉSACTIVÉ	Envoyez des sondes TCP Keep-Alive (KA) périodiques pour vérifier si le pair est toujours actif.
Connection idle time before starting keep-alive probes	900 secondes	Durée, en secondes, pendant laquelle la connexion est inactive, avant l'envoi d'une sonde keep-alive (KA).
Keep-alive probe interval	75 seconde	Intervalle de temps, en secondes, avant la prochaine sonde Keep-Alive (KA), si le pair ne répond pas.
Nombre maximal de sondes Keep-Alive à manquer avant d'interromper la connexion.	3	Nombre de sondes Keep-Alive (KA) à envoyer sans accusé de réception, avant de supposer que le pair est en panne.
Atténuation de la fenêtre RST (protection contre les usurpation).	DÉSACTIVÉ	Activez ou désactivez l'atténuation de la fenêtre RST pour vous protéger contre l'usurpation. Lorsque cette option est

activée, la réponse est accompagnée d'un ACK correctif lorsqu'un numéro de séquence n'est pas valide.|
|Acceptez RST avec le dernier numéro de séquence accusé de réception.|ACTIVÉ|
|Data transfer|
Immediate ACK on PUSH packet	ACTIVÉ	Envoie un accusé de réception positif immédiat (ACK) à la réception de paquets TCP avec indicateur PUSH.
Maximum packets per MSS	0	Nombre maximal d'octets à autoriser dans un segment de données TCP
Algorithme de Nagle	DÉSACTIVÉ	L'algorithme de Nagle combat le problème des petits paquets dans la transmission TCP. Les applications telles que Telnet et d'autres moteurs en temps réel qui nécessitent que chaque frappe de touche soit passée de l'autre côté créent souvent de petits paquets. Grâce à l'algorithme de Nagle, NetScaler peut mettre en mémoire tampon de tels petits paquets et les envoyer ensemble pour augmenter l'efficacité de la connexion. Cet algorithme doit fonctionner avec d'autres techniques d'optimisation TCP dans NetScaler.
Maximum TCP segments allowed in a burst	10 MSS	Maximum number of TCP segments allowed in a burst
Maximum out-of-order packets to queue	300	Taille maximale de la file d'attente des paquets en rupture d'ordre. Une valeur de 0 signifie qu'il n'y a pas de limite
Contrôle de la congestion
TCP Flavor	CUBIC
Paramétrage de la fenêtre de congestion initiale (cwnd)	4 MSS	Limite maximale initiale du nombre de paquets TCP pouvant être en attente sur la liaison TCP vers le serveur
TCP Explicit Congestion Notification(ECN)	DÉSACTIVÉ	La notification de congestion explicite (ECN) fournit une notification de bout en bout de la congestion du réseau sans abandonner de paquets.
TCP Max congestion window(CWND)	524288 octets	TCP maintient une fenêtre de congestion (CWND), limitant le nombre total de paquets sans accusé de réception pouvant être en transit de bout en bout. Dans TCP, la fenêtre de congestion est l'un des facteurs qui déterminent le nombre d'octets pouvant être en attente à tout moment. La fenêtre de congestion est un moyen d'empêcher qu'un lien entre l'expéditeur et le destinataire ne soit surchargé par un trafic trop important. Il est calculé en estimant combien de congestion il y a sur le lien.
TCP Hybrid Start (HyStart)	8 octets
Délai d'expiration minimum de retransmission TCP (RTO) en millions de secondes	1000	Délai de retransmission minimal, en millisecondes, spécifié par incréments de 10 millisecondes (la valeur doit donner un nombre entier si elle est divisée par 10).
TCP dupack threshold	DÉSACTIVÉ
Burst Rate Control	3	Contrôle du taux de rafale TCP DÉSACTIVÉ/FIXE/DYNAMIQUE. FIXED nécessite la définition d'un débit TCP
Taux TCP	DÉSACTIVÉ	Taux d'envoi de la charge utile de connexion TCP en Ko/s
TCP Rate Maximum Queue	0	Taille maximale de la file d'attente de connexion en octets, lorsque

BurStrateControl est utilisé.|
|MPTCP|
Multipath TCP	DÉSACTIVÉ	Multipath TCP (MPTCP) est un ensemble d'extensions de TCP standard pour fournir un service TCP multipath, qui permet à une connexion de transport de fonctionner simultanément sur plusieurs chemins.
Multipath TCP drop data on pre-established subflow	DÉSACTIVÉ	Activez ou désactivez la suppression silencieuse des données sur le sous-flux préétabli. Lorsque cette option est activée, les paquets de données DSS sont supprimés silencieusement au lieu d'interrompre la connexion lorsque des données sont reçues sur un sous-flux préétabli.
Multipath TCP fastopen	DÉSACTIVÉ	Activez ou désactivez l'ouverture rapide Multipath TCP. Lorsque cette option est activée, les paquets de données DSS sont acceptés avant de recevoir le troisième ack de l'établissement de liaison SYN.
Multipath TCP session timeout	0 seconde	Délai d'expiration de session MPTCP en secondes. Si cette valeur n'est pas définie, les sessions MPTCP inactives sont vides après le délai d'inactivité du client du serveur virtuel.
Security
SYN spoof protection	DÉSACTIVÉ	Activez ou désactivez la suppression des paquets SYN non valides pour vous protéger contre l'usurpation d'identité. Lorsque cette option est désactivée, les connexions établies sont réinitialisées lorsqu'un paquet SYN est reçu.
TCP Syncookie	DÉSACTIVÉ	Ceci est utilisé pour résister aux attaques d'inondation SYN. Activez ou désactivez le mécanisme SYNCOOKIE pour l'établissement de liaison TCP avec les clients. La désactivation de SYNCOOKIE empêche la protection contre les attaques SYN sur l'appliance NetScaler.
Loss Detection and Recovery
Duplicate Selective Acknowledgment (DSACK)	ACTIVÉ	Une appliance NetScaler utilise un accusé de réception sélectif dupliqué (DSACK) pour déterminer si une retransmission a été envoyée par erreur.
Forward RTO recovery (FRTO)	ACTIVÉ	Détecte les délais d'attente de retransmission TCP parasites. Après avoir retransmis le premier segment non reconnu déclenché par un délai d'expiration, l'algorithme de l'expéditeur TCP surveille les accusés de réception entrants pour déterminer si le délai d'expiration était faux. Il décide ensuite s'il faut envoyer de nouveaux segments ou retransmettre les segments non confirmés. L'algorithme aide efficacement à éviter d'autres retransmissions inutiles et améliore ainsi les performances TCP en cas de délai d'expiration inutile.
TCP Forward Acknowledgment (FACK)	ACTIVÉ	Activez ou désactivez FACK (Forward ACK).
Selective Acknowledgement(SACK) status	ACTIVÉ	TCP SACK résout le problème des pertes de paquets multiples, ce qui réduit la capacité globale de débit. Avec un accusé de réception sélectif, le destinataire peut informer l'expéditeur de tous les segments reçus avec succès, ce qui permet à l'expéditeur de ne retransmettre que les segments perdus. Cette technique permet à NetScaler d'améliorer le débit global et de réduire la latence de connexion.
Maximum packets per retransmission	1	Permet à NetScaler de contrôler le nombre de paquets à retransmettre en une seule tentative. Lorsque NetScaler reçoit un ACK partiel et doit effectuer une

retransmission, ce paramètre est pris en compte. Cela n'a aucune incidence sur les retransmissions basées sur le RTO.|
|TCP Delayed-ACK Timer|100 millisecondes|Délai d'attente pour l'ACK retardé par TCP, en millisecondes|
|Optimisation du coût total de possession|
Mode d'optimisation TCP	TRANSPARENT	TCP Optimization modes TRANSPARENT/ENDPOINT
Appliquer des optimisations TCP adaptatives	DÉSACTIVÉ	Apply Adaptive TCP optimizations
TCP Segmentation Offload	AUTOMATIQUE	Déchargez la segmentation TCP vers la carte réseau. Si cette option est définie sur AUTOMATIC, la segmentation TCP est déchargée vers la carte réseau, si la carte réseau la prend en charge.
ACK Aggregation	DÉSACTIVÉ	Activer ou désactiver l'agrégation ACK
TCP Time-wait (ou Time_Wait)	40 secondes	Temps écoulé avant de libérer une connexion TCP fermée
Client et serveur Delink sur RST	DÉSACTIVÉ	Supprimer la connexion client et serveur, lorsqu'il y a les données en suspens doivent être envoyées de l'autre côté.

> **Remarque :**
> lorsque HTTP/2 est activé, Citrix vous recommande de désactiver le paramètre TCP Dynamic Receive Buffering dans le profil TCP.

Setting Global TCP Parameters

L'appliance NetScaler vous permet de spécifier des valeurs pour les paramètres TCP applicables à tous les services et serveurs virtuels NetScaler. Cela peut être fait à l'aide de :

- Default TCP profile
- Global TCP command
- Fonction de mise en mémoire tampon TCP

> **Remarques :**
>
> - Le paramètre `recvBuffSize` de la commande set ns TCPParam est obsolète à partir de la version 9.2. Dans les versions ultérieures, définissez la taille du tampon à l'aide du paramètre `bufferSize` de la commande set ns TCPProfile. Si vous effectuez une mise à niveau vers une version où le paramètre `recvBuffSize` est obsolète, le paramètre `bufferSize` est défini sur sa valeur par défaut.
> - Lors de la configuration du profil TCP, assurez-vous que le `buffersize` paramètre TCP est inférieur ou égal au `httppipelinebuffersize` paramètre.
>   Si le `buffersize` paramètre du profil TCP est supérieur au `httppipelinebuffersize` paramètre du profil HTTP, la charge utile TCP peut être accumulée et dépasser la taille de la mémoire tampon du pipeline HTTP. Cela entraîne la réinitialisation de la connexion TCP

> par l'appliance NetScaler.

Default TCP profile

Un profil TCP, nommé comme `nstcp_default_profile`, est utilisé pour spécifier les configurations TCP utilisées si aucune configuration TCP n'est fournie au niveau du service ou du serveur virtuel.

> **Remarques :**
>
> - Tous les paramètres TCP ne peuvent pas être configurés via le profil TCP par défaut. Certains paramètres doivent être exécutés à l'aide de la commande TCP globale (voir la section ci-dessous).
> - Il n'est pas nécessaire que le profil par défaut soit explicitement lié à un service ou à un serveur virtuel.

Pour configurer le profil TCP par défaut

- À l'aide de l'interface de ligne de commande, entrez :

```
set ns tcpProfile nstcp_default_profile...
<!--NeedCopy-->
```

- Dans l'interface graphique, accédez à **Système** > **Profils**, cliquez sur **Profils TCP** et mettez à jour nstcp_default_profile.

Global TCP command

Une autre approche que vous pouvez utiliser pour configurer les paramètres TCP globaux est la commande TCP globale. En plus de certains paramètres uniques, cette commande duplique certains paramètres pouvant être définis à l'aide d'un profil TCP. Toute mise à jour de ces paramètres dupliqués est reflétée dans le paramètre correspondant du profil TCP par défaut.

Par exemple, si le paramètre SACK est mis à jour à l'aide de cette approche, la valeur est reflétée dans le paramètre SACK du profil TCP par défaut (nstcp_default_profile).

> **Remarque :**
>
> Citrix recommande d'utiliser cette approche uniquement pour les paramètres TCP qui ne sont pas disponibles dans le profil TCP par défaut.

Pour configurer la commande TCP globale

- À l'aide de l'interface de ligne de commande, entrez :

```
set ns tcpParam …
<!--NeedCopy-->
```


- Sur l'interface graphique, accédez à **Système > Paramètres**, cliquez sur **Modifier les paramètres TCP** et mettez à jour les paramètres TCP requis.

Fonction de mise en mémoire tampon TCP

NetScaler fournit une fonctionnalité appelée mise en mémoire tampon TCP que vous pouvez utiliser pour spécifier la taille de la mémoire tampon TCP. La fonctionnalité peut être activée globalement ou au niveau du service.

> **Remarque :**
>
> La taille de la mémoire tampon peut également être configurée dans le profil TCP par défaut. Si la taille de la mémoire tampon comporte des valeurs différentes dans la fonctionnalité de mise en mémoire tampon TCP et dans le profil TCP par défaut, la valeur la plus élevée est appliquée.

Configuration globale de la fonctionnalité de mise en mémoire tampon TCP

- À l'invite de commandes, saisissez :

  enable ns mode TCPB

  ```
  set ns tcpbufParam -size <positiveInteger> -memLimit <positiveInteger>
  ```

- Sur l'interface graphique, accédez à **Système** > **Paramètres**, cliquez sur **Configurer les modes** et sélectionnez **TCP Buffering**.

  Ensuite, accédez à **Système** > **Paramètres**, cliquez sur **Modifier les paramètres TCP**, spécifiez les valeurs pour la **taille du tampon et lalimite d'utilisation de la mémoire**.

Définition des paramètres TCP spécifiques au service ou au serveur virtuel

À l'aide des profils TCP, vous pouvez spécifier des paramètres TCP pour les services et les serveurs virtuels. Vous devez définir un profil TCP (ou utiliser un profil TCP intégré) et associer le profil au service et au serveur virtuel appropriés.

> **Remarque :**
>
> Vous pouvez également modifier les paramètres TCP des profils par défaut en fonction de vos besoins.

Vous pouvez spécifier la taille de la mémoire tampon TCP au niveau du service à l'aide des paramètres spécifiés par la fonctionnalité de mise en mémoire tampon TCP.

Pour spécifier des configurations TCP au niveau du service ou du serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, effectuez les opérations suivantes :

1. Configurez le profil TCP.

```
set ns tcpProfile <profile-name>...
<!--NeedCopy-->
```

2. Liez le profil TCP au service ou au serveur virtuel.

```
    set service <name> ....
    <!--NeedCopy-->
```

Exemple :

```
> set service service1 -tcpProfileName profile1
```

Pour lier le profil TCP au serveur virtuel :

```
set lb vserver <name> ....
<!--NeedCopy-->
```

Exemple :

```
> set lb vserver lbvserver1 -tcpProfileName profile1
<!--NeedCopy-->
```

Pour spécifier des configurations TCP au niveau du service ou du serveur virtuel à l'aide de l'interface graphique

Dans l'interface graphique, effectuez les opérations suivantes :

1. Configurez le profil TCP.

   Accédez à **Système** > **Profils** > **Profils TCP**, puis créez le profil TCP.

2. Liez le profil TCP au service ou au serveur virtuel.

   Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services/Serveurs virtuels**, puis créez le profil TCP, qui doit être lié au service ou au serveur virtuel.

Profils TCP intégrés

Pour faciliter la configuration, NetScaler fournit certains profils TCP intégrés. Consultez les profils intégrés répertoriés pour les éléments suivants, sélectionnez un profil et utilisez-le tel qu'il est ou modifiez-le pour répondre à vos besoins. Vous pouvez lier ces profils à vos services ou serveurs virtuels requis.

Profil intégré	Description
nstcp_default_profile	Représente les paramètres TCP globaux par défaut de l'appliance.
nstcp_default_tcp_lan	Utile pour les connexions de serveur principal, lorsque ces serveurs résident sur le même réseau local que l'appliance.
NSTCP_Default_WAN	utile pour les déploiements WAN.
nstcp_default_tcp_lan_thin_stream	Similaire au profil nstcp_default_tcp_lan. Toutefois, les paramètres sont réglés sur des flux de paquets de petite taille.
nstcp_default_tcp_interactive_stream	Similaire au profil nstcp_default_tcp_lan. Cependant, il dispose d'un temporisateur ACK retardé réduit et des paramètres de **paquet ACK sur PUSH** .
nstcp_default_tcp_lfp	Utile pour les réseaux WAN (long fat pipe networks) côté client. Les réseaux de gros tubes longs ont des lignes à long délai et à bande passante élevée avec des pertes de paquets minimales.
nstcp_default_tcp_lfp_thin_stream	Similaire au profil nstcp_default_tcp_lfp. Toutefois, les paramètres sont réglés pour les flux de paquets de petite taille.
nstcp_default_tcp_lnp	Utile pour les réseaux à tubes longs et étroits (WAN) côté client. Les réseaux à tubes longs et étroits subissent parfois des pertes de paquets considérables.
nstcp_default_tcp_lnp_thin_stream	Similaire au profil nstcp_default_tcp_lnp. Toutefois, les paramètres sont réglés pour les flux de paquets de petite taille.
nstcp_internal_apps	Utile pour les applications internes de l'appliance (par exemple, la synchronisation de site GSLB). Il contient la mise à l'échelle de la fenêtre ajustée et les options SACK pour les applications souhaitées. Ce profil ne doit pas être lié à des applications autres que des applications internes.

Profil intégré	Description
NSTCP_Default_Mobile_Profile	Utile pour les appareils mobiles.
NSTCP_Default_XA_XD_Profile	Utile pour le déploiement de Citrix Virtual Apps and Desktops.

Exemples de configurations TCP

Exemples d'interface de ligne de commande permettant de configurer les éléments suivants :

Défendre TCP contre les attaques par usurpation d'identité

Activez NetScaler pour défendre le protocole TCP contre les attaques frauduleuses. Par défaut, le paramètre « RSTWindowattenuation » est désactivé. Ce paramètre est activé pour protéger l'appliance contre l'usurpation d'identité. Si vous l'activez, il répond avec un accusé de réception correctif (ACK) pour un numéro de séquence non valide. Les valeurs possibles sont Activé, Désactivé.

Où, le paramètre d'atténuation de la fenêtre RST protège l'appareil contre l'usurpation. Lorsque cette option est activée, répondez avec l'ACK correctif lorsqu'un numéro de séquence n'est pas valide.

```
1      > set ns tcpProfile profile1 -rstWindowAttenuate ENABLED -
           spoofSynDrop ENABLED
2      Done
3      > set lb vserver lbvserver1 -tcpProfileName profile1
4      Done
5  <!--NeedCopy-->
```

Notification explicite de congestion (ECN)

```
Enable ECN on the required TCP profile
```

```
1      > set ns tcpProfile profile1 -ECN ENABLED
2      Done
3      > set lb vserver lbvserver1 -tcpProfileName profile1
4      Done
5  <!--NeedCopy-->
```

Accusé de réception sélectif (SACK)

Activez SACK sur le profil TCP requis.


```
    > set ns tcpProfile profile1 -SACK ENABLED
    Done
    > set lb vserver lbvserver1 -tcpProfileName profile1
    Done
<!--NeedCopy-->
```

Accusé de réception (FACK)

Activez FACK sur le profil TCP requis.

```
> set ns tcpProfile profile1 -FACK ENABLED
> set lb vserver lbvserver1 -tcpProfileName profile1
<!--NeedCopy-->
```

Mise à l'échelle des fenêtres (WS)

Activez la mise à l'échelle de la fenêtre et définissez le facteur de mise à l'échelle de la fenêtre sur le profil TCP requis.

```
set ns tcpProfile profile1 -WS ENABLED -WSVal 9
Done
set lb vserver lbvserver1 -tcpProfileName profile1
Done
<!--NeedCopy-->
```

Taille de segment maximale (MSS)

Mettez à jour les configurations liées au MSS.

```
> set ns tcpProfile profile1 -mss 1460 - maxPktPerMss 512
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
<!--NeedCopy-->
```

NetScaler pour découvrir le MSS d'un serveur virtuel

Permettez à NetScaler d'apprendre le VSS et de mettre à jour les autres configurations associées.

```
> set ns tcpParam -learnVsvrMSS ENABLED -mssLearnInterval 180 -
    mssLearnDelay 3600
```



```
Done
<!--NeedCopy-->
```

Keep-Alive TCP

Activez la persistance TCP et mettez à jour les autres configurations associées.

```
> set ns tcpProfile profile1 -KA ENABLED -KaprobeUpdateLastactivity ENABLED
-KAconnIdleTime 900 -KAmaxProbes 3 -KaprobeInterval 75
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Taille de la mémoire tampon : utilisation du profil TCP

Spécifiez la taille de la mémoire tampon.

```
> set ns tcpProfile profile1 -bufferSize 8190
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Taille du tampon : utilisation de la fonction de mise en mémoire tampon TCP

Activez la fonctionnalité de mise en mémoire tampon TCP (globalement ou pour un service), puis spécifiez la taille de la mémoire tampon et la limite de mémoire.

```
> enable ns feature TCPB
Done
> set ns tcpbufParam -size 64 -memLimit 64
Done
```

MPTCP

Activez MPTCP, puis définissez les configurations MPTCP facultatives.

```
> set ns tcpProfile profile1 -mptcp ENABLED
Done
> set ns tcpProfile profile1 -mptcpDropDataOnPreEstSF ENABLED -mptcpFastOpen
 ENABLED -mptcpSessionTimeout 7200
Done
```



```
> set ns tcpparam -mptcpConCloseOnPassiveSF ENABLED -mptcpChecksum ENABLED
-mptcpSFtimeout 0 -mptcpSFReplaceTimeout 10
-mptcpMaxSF 4 -mptcpMaxPendingSF 4 -mptcpPendingJoinThreshold 0 -mptcpRTOsToSwitchSF
 2 -mptcpUseBackupOnDSS ENABLED
Done
```

Contrôle de la congestion

Définissez l'algorithme de contrôle de congestion TCP requis.

```
set ns tcpProfile profile1 -flavor Westwood
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Mise en mémoire tampon de réception dynamique

Activez la mise en mémoire tampon de réception dynamique sur le profil TCP requis.

```
> set ns tcpProfile profile1 -dynamicReceiveBuffering ENABLED
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Prise en charge de TCP Fast Open (TFO) dans Multipath TCP (MPTCP)

Une appliance NetScaler prend désormais en charge le mécanisme TCP Fast Open (TFO) pour établir des connexions TCP multivoies (MPTCP) et accélérer les transferts de données. Le mécanisme permet de transporter les données de sous-flux pendant la liaison MPTCP initiale dans les paquets SYN et SYN-ACK et permet également de consommer les données par le nœud récepteur lors de l'établissement de la connexion MPTCP.

Pour plus d'informations, consultez la rubrique TCP Fast Open .

Prise en charge de la taille variable des cookies TFO pour MPTCP

Une appliance NetScaler vous permet désormais de configurer un cookie TCP Fast Open (TFO) de longueur variable d'une taille minimale de 4 octets et d'une taille maximale de 16 octets dans un profil TCP. Ce faisant, l'appliance peut répondre au client avec la taille de cookie TFO configurée dans le paquet SYN-ACK.

Pour configurer le cookie TCP Fast Open (TFO) dans un profil TCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize <positive_integer
>
```

Exemple

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize 8
```

Pour configurer le cookie TCP Fast Open (TFO) dans un profil TCP à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > Profils.
2. Dans le volet d'informations, accédez à l'onglet **Profils TCP** et sélectionnez un profil TCP.
3. Dans la page **Configurer le profil TCP**, définissez la taille du cookie d' **ouverture rapide TCP** .
4. Cliquez sur **OK** et **Terminé**.

SYN-Cookie timeout interval

Le paramètre `TCPSyncookie` est activé par défaut dans les profils TCP pour fournir une protection robuste basée sur la RFC 4987 contre les attaques SYN. Si vous devez prendre en charge des clients TCP personnalisés qui ne sont pas compatibles avec cette protection mais qui veulent toujours garantir un retour en cas d'attaque, il `synAttackDetection` gère cela pour vous en activant automatiquement le `SYNCookie` comportement en interne pendant une période déterminée par le `autosyncookietimeout` paramètre.

Pour configurer le seuil maximal de retransmission SYN ACK à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
1     set ns tcpparam [-maxSynAckRetx <positive_integer>]
2
3     Set ns tcpparam [-maxSynAckRetx 150]
4 <!--NeedCopy-->
```

Pour configurer l'intervalle de délai d'expiration automatique des cookie SYN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ns tcpparam [-autosyncookietimeout <positive_integer>]
```

```
Set ns tcpparam [-autosyncookietimeout 90]
```

Supprimer la connexion client et serveur

Lorsqu'il est activé, le paramètre déconnecte la connexion client et serveur lorsqu'il y a des données en attente à envoyer vers l'autre côté. Par défaut, le paramètre est désactivé.


```
set ns tcpparam -delinkClientServerOnRST ENABLED
Done

<!--NeedCopy-->
```

Configuration du paramètre de seuil de démarrage lent

Vous pouvez utiliser le `slowStartthreshold` paramètre seuil de démarrage lent pour configurer la `tcp-slowstartthreshold` valeur de la `Nile` variante de l'algorithme de contrôle de la congestion. Les valeurs acceptables pour le paramètre sont `min = 8190` et `max = 524288`. La valeur par défaut est `524288`. La variante TCP `Nile`, sous le profil TCP, ne dépend plus du `maxcwnd` paramètre. Vous devez configurer le `slowStartthreshold` paramètre de la `Nile` variante.

À l'invite de commandes, tapez :

```
set tcpprofile nstcp_default_profile -slowstartthreshold 8190
Done

<!--NeedCopy-->
```

Configurations HTTP

May 5, 2023

> **Important :**
>
> À partir de la version 13.0 build 71.x de NetScaler, une appliance NetScaler peut gérer des requêtes HTTP de grande taille pour répondre aux demandes de l'application L7. La taille de l'entête peut être configurable jusqu'à 128 Ko.

Les configurations HTTP d'une appliance NetScaler peuvent être spécifiées dans une entité appelée profil HTTP, qui est un ensemble de paramètres HTTP. Le profil HTTP peut ensuite être associé à des services ou des serveurs virtuels qui souhaitent utiliser ces configurations HTTP.

Un profil HTTP par défaut peut être configuré pour définir les configurations HTTP qui sont appliquées par défaut, globalement, à tous les services et serveurs virtuels.

> **Remarque :**
>
> Lorsqu'un paramètre HTTP a des valeurs différentes pour le service, le serveur virtuel et globalement, la valeur de l'entité la plus spécifique (le service) reçoit la priorité la plus élevée.

L'appliance NetScaler propose également d'autres approches pour configurer HTTP. Lisez la suite pour plus d'informations.

Le NetScaler prend en charge un protocole WebSocket qui permet aux navigateurs et aux autres clients de créer une connexion TCP bidirectionnelle en duplex intégral avec les serveurs. L'implémentation NetScaler de WebSocket est conforme à la norme RFC 6455.

> **Remarque :**
>
> Une appliance NetScaler prend en charge la configuration de l'adresse IP de la source utilisateur (USIP) pour les protocoles HTTP/1.1 et HTTP/2.

Définition des paramètres HTTP globaux

L'appliance NetScaler vous permet de spécifier des valeurs pour les paramètres HTTP applicables à tous les services et serveurs virtuels NetScaler. Cela peut être fait à l'aide de :

- Profil HTTP par défaut
- Commande HTTP globale

Profil HTTP par défaut

Un profil HTTP, nommé nshttp_default_profile, est utilisé pour spécifier les configurations HTTP qui sont utilisées si aucune configuration HTTP n'est fournie au niveau du service ou du serveur virtuel.

> **Remarques :**
>
> - Tous les paramètres HTTP ne peuvent pas être configurés via le profil HTTP par défaut. Certains paramètres sont effectués à l'aide de la commande HTTP globale (voir la section suivante).
> - Il n'est pas nécessaire que le profil par défaut soit explicitement lié à un service ou à un serveur virtuel.

Pour configurer le profil HTTP par défaut

- À l'aide de l'interface de ligne de commande, entrez :

  ```
  set ns httpProfile nshttp_default_profile …
  ```

- Dans l'interface graphique, accédez à **Système** > **Profils**, cliquez sur **Profils HTTP** et mettez à jour nshttp_default_profile.

Commande HTTP globale

Une autre approche que vous pouvez utiliser pour configurer les paramètres HTTP globaux est la commande HTTP globale. Outre certains paramètres uniques, cette commande duplique certains

paramètres qui peuvent être définis à l'aide d'un profil HTTP. Toute mise à jour apportée à ces paramètres en double est reflétée dans le paramètre correspondant dans le profil HTTP par défaut.

Par exemple, si le paramètre MaxReusePool est mis à jour selon cette approche, la valeur est reflétée dans le paramètre MaxReusePool du profil HTTP par défaut (nshttp_default_profile).

> **Remarque :**
>
> Nous vous recommandons d'utiliser cette approche uniquement pour les paramètres HTTP qui ne sont pas disponibles dans le profil HTTP par défaut.

Pour configurer la commande HTTP globale

- À l'aide de l'interface de ligne de commande, entrez :

  ```
  set ns httpParam …
  ```

- Sur l'interface graphique, accédez à **Système > Paramètres**, cliquez sur **Modifier les paramètres HTTP** et mettez à jour les paramètres HTTP requis.

Pour configurer un schéma de codage Ignorer pour la demande de connexion

Pour activer HTTP/2 et définir les paramètres HTTP/2 afin d'ignorer le schéma de codage dans la demande de connexion, à l'invite de commandes, tapez :

```
set ns httpParam [-ignoreConnectCodingScheme ( ENABLED | DISABLED )]
```

Exemple :

```
set ns httpParam -ignoreConnectCodingScheme ENABLED
```

Pour lier le profil HTTP à un serveur virtuel à l'aide de la ligne de commande NetScaler

Configurer le profil HTTP pour supprimer les requêtes non valides TRACE ou TRACK

Vous pouvez activer le paramètre MarkTraceReqInval pour marquer les requêtes TRACK et TRACK comme non valides. Lorsque vous activez cette option en même temps que l'option DropInvalidReqs sur l'adresse IP virtuelle, vous pouvez réinitialiser un client qui envoie des requêtes TRACE ou TRACK à une appliance NetScaler.

Pour configurer le profil HTTP à l'aide de la CLI

À l'invite de commande, tapez :

```
set ns httpProfile <profile name> [-markTraceReqInval ENABLED | DISABLED ]
```

Exemple :

```
set ns httpProfile profile1 -markTraceReqInval ENABLED
```


Configuration du profil HTTP pour un groupe de services

À l'invite de commande, tapez :

```
add serviceGroup <serviceGroupName>@ <serviceType> [-cacheType <
    cacheType>] [-td <positive_integer>] [-maxClient <positive_integer>]
     [-maxReq <positive_integer>] [-cacheable ( YES | NO )] [-cip (
    ENABLED | DISABLED ) [<cipHeader>]] [-usip ( YES | NO )] [-
    pathMonitor ( YES | NO )] [-pathMonitorIndv ( YES | NO )] [-
    useproxyport ( YES | NO )] [-healthMonitor ( YES | NO )] [-sp ( ON |
     OFF )] [-rtspSessionidRemap ( ON | OFF )] [-cltTimeout <secs>] [-
    svrTimeout <secs>] [-CKA ( YES | NO )] [-TCPB ( YES | NO )] [-CMP (
    YES | NO )] [-maxBandwidth
<positive_integer>] [-monThreshold <positive_integer>] [-state ENABLED
    DISABLED )][-downStateFlush ( ENABLED | DISABLED )] [-tcpProfileName
     <string>] [-httpProfileName <string>] [-comment <string>] [-
    appflowLog ( ENABLED | DISABLED )] [-netProfile <string>] [-
    autoScale <autoScale> -memberPort <port> [-autoDisablegraceful ( YES
     | NO )] [-autoDisabledelay <secs>] ] [-monConnectionClose ( RESET |
     FIN )]

<!--NeedCopy-->
```

Exemple :

```
add serviceGroup Service-Group-1 HTTP -maxClient 0 -maxReq 0 -cip ENABLED -
usip NO -useproxyport YES -cltTimeout 200 -svrTimeout 300 -CKA NO -TCPB NO
-CMP NO -httpProfileName profile1
```

Configurer le profil HTTP à l'aide de l'interface graphique NetScaler

Pour marquer les demandes TRACE ou TRACK non valides, procédez comme suit.

1. **Connectez-vous à l'appliance NetScaler et accédez à**Configuration**>**Système > Profils**.**
2. Dans l'onglet **Profils HTTP**, cliquez sur **Ajouter**.
3. Sur la page **Créer un profil HTTP**, sélectionnez l'option **Marquer les demandes TRACE comme non valides** .
4. Cliquez sur **Create**.

Définition des paramètres HTTP spécifiques au service ou au serveur virtuel

À l'aide des profils HTTP, vous pouvez spécifier des paramètres HTTP pour les services et les serveurs virtuels. Vous devez définir un profil HTTP (ou utiliser un profil HTTP intégré) et associer le profil au service et au serveur virtuel appropriés.

> **Remarque :**
>
> Vous pouvez également modifier les paramètres HTTP des profils par défaut selon vos besoins.

Pour spécifier des configurations HTTP au niveau du service ou du serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commandes, effectuez les opérations suivantes :

1. Configurez le profil HTTP.

   ```
   set ns httpProfile <profile-name>...
   ```

2. Liez le profil HTTP au service ou au serveur virtuel.

   Pour lier le profil HTTP au service :

```
set service <name> .....
```

Exemple :

```
1 > set service service1 -httpProfileName profile1
2 <!--NeedCopy-->
```

Pour lier le profil HTTP au serveur virtuel :

```
set lb vserver <name> .....
```

Exemple :

```
1 > set lb vserver lbvserver1 -httpProfileName profile1
2 <!--NeedCopy-->
```

Pour spécifier des configurations HTTP au niveau du service ou du serveur virtuel à l'aide de l'interface graphique

Dans l'interface graphique, effectuez les opérations suivantes :

1. Configurez le profil HTTP.

   Accédez à **Système** > **Profils** > **Profils HTTP**, puis créez le profil HTTP.

2. Liez le profil HTTP au service ou au serveur virtuel.

   Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services/Serveurs virtuels**et créez le profil HTTP, qui doit être lié au service/serveur virtuel.

Profils HTTP intégrés

Pour faciliter la configuration, NetScaler fournit certains profils HTTP intégrés. Passez en revue les profils répertoriés et utilisez-les tels quels ou modifiez-les pour répondre à vos besoins. Vous pouvez lier ces profils aux services ou serveurs virtuels requis.

Profil intégré	Description
nshttp_default_profile	Représente les paramètres HTTP globaux par défaut sur l'appliance.
nshttp_default_strict_validation	Paramètres pour les déploiements qui nécessitent une validation stricte des requêtes et des réponses HTTP.

Exemples de configurations HTTP

Exemples d'interface de ligne de commande pour configurer les éléments suivants :

- Statistiques sur les bandes HTTP
- Connexions WebSocket

Statistiques sur les bandes HTTP

Spécifiez la taille de bande pour les requêtes et réponses HTTP.

```
> set protocol httpBand reqBandSize 300 respBandSize 2048
Done
> show protocol httpband -type REQUEST
<!--NeedCopy-->
```

Connexions WebSocket

Activez WebSocket sur le profil HTTP requis.

```
> set ns httpProfile http_profile1 -webSocket ENABLED
Done
> set lb vserver lbvserver1 -httpProfileName profile1
Done
<!--NeedCopy-->
```


Configurez l'appliance NetScaler pour supprimer ou transmettre l'en-tête de mise à niveau au serveur principal

Le paramètre PassProtocolUpgrade du profil HTTP empêche les attaques sur les serveurs principaux. Selon l'état de ce paramètre, l'en-tête de mise à niveau est transmis dans la demande envoyée au serveur principal ou supprimé avant l'envoi de la demande.

- Si le paramètre PassProtocolUpgrade est activé, l'en-tête de mise à niveau est transmis au serveur principal. Le serveur accepte la demande de mise à niveau et l'informe dans sa réponse.
- Si le paramètre est désactivé, l'en-tête de mise à niveau est supprimé et le reste de la demande est envoyé au serveur principal.

Le paramètre PassProtocolUpgrade est ajouté aux profils suivants :

- nshttp_default_profile - activé par défaut
- nshttp_default_strict_validation - désactivé par défaut
- nshttp_default_internal_apps - désactivé par défaut
- nshttp_default_http_quic_profile : activé par défaut

Nous vous recommandons de désactiver le paramètre PassProtocolUpgrade par défaut.

Définissez le paramètre PassProtocolUpgrade à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
set ns httpProfile <name> [-passProtocolUpgrade ( ENABLED | DISABLED )]
```

Exemple :

```
set ns httpProfile profile1 -passProtocolUpgrade ENABLED
```

Définissez le paramètre PassProtocolUpgrade à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profils HTTP**.
2. Créez ou modifiez un profil HTTP.
3. Sélectionnez **Pass Protocol Upgrade**.

Configuration HTTP/2

May 5, 2023

> **Remarque :**
> La fonctionnalité HTTP/2 est prise en charge sur les modèles NetScaler MPX, VPX et SDX. Dans une appliance NetScaler VPX, la fonctionnalité HTTP/2 est prise en charge à partir de la version 11.0 de NetScaler.

Le problème des performances des applications Web est directement lié à la tendance à l'augmentation de la taille des pages et du nombre d'objets sur les pages Web. HTTP/1.1 a été développé pour prendre en charge des pages Web plus petites, des connexions Internet plus lentes et un matériel serveur plus limité que ce qui est courant aujourd'hui. Il n'est pas adapté aux nouvelles technologies telles que JavaScript et les feuilles de style en cascade (CSS) ou aux nouveaux types de médias tels que les vidéos Flash et les images riches en graphiques. En effet, il ne peut demander qu'une seule ressource par connexion au serveur. Cette limitation augmente considérablement le nombre d'allers-retours, ce qui allonge le rendu des pages et réduit les performances du réseau.

Le protocole HTTP/2 résout ces limitations en permettant la communication avec moins de données transmises sur le réseau et en offrant la possibilité d'envoyer plusieurs requêtes et réponses via une seule connexion. HTTP/2 résout les principales limitations de HTTP/1.1 en utilisant plus efficacement les connexions réseau sous-jacentes. Il modifie la façon dont les demandes et les réponses circulent sur le réseau.

HTTP/2 est un protocole binaire. Il est plus efficace d'analyser, plus compact sur le fil, et surtout, il est moins sujet aux erreurs, par rapport aux protocoles textuels comme HTTP/1.1. Le protocole HTTP/2 utilise une couche de cadrage binaire qui définit le type de trame et la façon dont les messages HTTP sont encapsulés et transférés entre le client et le serveur. La fonctionnalité HTTP/2 prend en charge l'utilisation de la méthode CONNECT pour établir une connexion tunnel via un seul flux HTTP/2 vers un hôte distant.

Le protocole HTTP/2 inclut de nombreuses modifications améliorant les performances qui améliorent considérablement les performances, en particulier pour les clients se connectant via un réseau mobile.

Le tableau suivant répertorie les principales améliorations de HTTP/2 par rapport à HTTP/1.1 :

Fonctionnalités HTTP/2	Description
Compression d'en-tête	Les en-têtes HTTP contiennent beaucoup d'informations répétitives et consomment donc une bande passante inutile pendant la transmission des données. HTTP/2 réduit les besoins en bande passante en comprimant l'en-tête et en minimisant la nécessité de transporter les en-têtes HTTP à chaque requête et réponse.
Multiplexage de connexion	La latence peut avoir un impact considérable sur les temps de chargement des pages et sur l'expérience de l'utilisateur final. Le multiplexage des connexions résout ce problème en envoyant plusieurs demandes et réponses via une seule connexion.
Serveur Push	Server Push permet au serveur de diffuser du contenu de manière proactive vers le navigateur du client, ce qui évite les retards aller-retour. Cette fonctionnalité met en cache les réponses dont le client pense avoir besoin, réduit le nombre d'allers-retours et améliore le temps de rendu de la page. Important : L'appliance NetScaler ne prend pas en charge la fonctionnalité push du serveur.
Pas de blocage de la tête de ligne	Sous HTTP 1.1, les navigateurs peuvent télécharger une ressource à la fois par connexion. Lorsqu'un navigateur doit télécharger une ressource volumineuse, il bloque le téléchargement de toutes les autres ressources jusqu'à ce que le premier téléchargement soit terminé. HTTP/2 résout ce problème avec une approche de multiplexage. Il permet au navigateur client de télécharger d'autres composants Web en parallèle sur la même connexion et de les afficher dès qu'ils sont disponibles.

Fonctionnalités HTTP/2	Description
Priorisation des demandes	Toutes les ressources n'ont pas la même priorité lorsque le navigateur affiche une page Web. Pour accélérer le temps de chargement, tous les navigateurs modernes hiérarchisent les demandes par type de ressource, leur emplacement sur la page et même par priorité acquise lors des visites précédentes. Avec HTTP/1.1, le navigateur a une capacité limitée d'utiliser les données de priorité, car ce protocole ne prend pas en charge le multiplexage et il n'y a aucun moyen de communiquer la hiérarchisation des requêtes par le serveur. Il en résulte une latence réseau inutile. HTTP/2 résout ce problème en permettant au navigateur d'envoyer toutes les requêtes. Le navigateur peut communiquer ses préférences de priorisation des flux via des dépendances et des pondérations de flux, ce qui permet aux serveurs d'optimiser la livraison des réponses. Important : L'appliance NetScaler ne prend pas en charge la fonctionnalité de priorisation des demandes.

Fonctionnement de HTTP/2

Une appliance NetScaler prend en charge HTTP/2 côté client ainsi que côté serveur. Du côté client, l'appliance NetScaler agit comme un serveur qui héberge un serveur virtuel HTTP/HTTPS pour HTTP/2. Du côté du back-end, NetScaler agit en tant que client pour les serveurs liés au serveur virtuel.

Par conséquent, l'appliance NetScaler maintient des connexions distinctes côté client et côté serveur. L'appliance NetScaler possède des configurations HTTP/2 distinctes pour le côté client et le côté serveur.

Configuration de l'équilibrage de charge HTTP/2 pour HTTPS (SSL)

Pour une configuration d'équilibrage de charge HTTPS, l'appliance NetScaler utilise l'extension TLS ALPN (RFC 7301) pour déterminer si le client/serveur prend en charge HTTP/2. Si tel est le cas, la so-

lution matérielle-logicielle choisit HTTP/2 comme protocole de couche applicative pour transmettre les données (comme décrit dans la RFC 7540 - Section 3.3) côté client/serveur.
La solution matérielle-logicielle utilise l'ordre de préférence suivant lorsqu'elle choisit le protocole de la couche application via l'extension TLS ALPN :

- HTTP/2 (s'il est activé dans le profil HTTP)
- HTTP/1.1

Configuration de l'équilibrage de charge HTTP/2 pour HTTP

Pour une configuration d'équilibrage de charge HTTP, l'appliance NetScaler utilise l'une des méthodes suivantes pour commencer à communiquer avec le client/serveur via HTTP/2.

> **Remarque**
>
> Dans les descriptions de méthodes suivantes, le client et le serveur sont des termes généraux pour une connexion HTTP/2. Par exemple, pour une configuration d'équilibrage de charge d'une appliance NetScaler utilisant HTTP/2, l'appliance NetScaler agit comme un serveur côté client et comme un client côté serveur.

- Mise à**niveau HTTP/2**. Un client envoie une requête HTTP/1.1 à un serveur. La demande inclut un en-tête de mise à niveau, qui demande au serveur de mettre à niveau la connexion vers HTTP/2. Si le serveur prend en charge HTTP/2, il accepte la demande de mise à niveau et la notifie dans sa réponse. Le client et le serveur commencent à communiquer via HTTP/2 une fois que le client a reçu la réponse de confirmation de mise à niveau.
- **HTTP/2 direct**. Un client commence directement à communiquer avec un serveur en HTTP/2 au lieu d'utiliser la méthode de mise à niveau HTTP/2. Si le serveur ne prend pas en charge HTTP/2 ou n'est pas configuré pour accepter directement les requêtes HTTP/2, il supprime les paquets HTTP/2 du client. Cette méthode est utile si l'administrateur de la machine cliente sait déjà que le serveur prend en charge HTTP/2.
- **HTTP/2 direct à l'aide d'un service alternatif (ALT-SVC).** Un serveur annonce qu'il prend en charge HTTP/2 à un client en incluant un champ Alternative Service (ALT-SVC) dans sa réponse HTTP/1.1. Si le client est configuré pour comprendre le champ ALT-SVC, le client et le serveur commencent à communiquer directement via HTTP/2 une fois que le client a reçu la réponse.

L'appliance NetScaler fournit des options configurables dans un profil HTTP pour les méthodes HTTP/2. Ces options HTTP/2 peuvent être appliquées au côté client ainsi qu'au côté serveur d'une configuration d'équilibrage de charge HTTPS ou HTTP. Pour plus d'informations sur les méthodes et options HTTP/2, reportez-vous au PDF des options HTTP/2 .

Avant de commencer

Avant de commencer à configurer HTTP/2 sur une appliance NetScaler, notez les points suivants :

- L'appliance NetScaler prend en charge HTTP/2 côté client ainsi que côté serveur.
- L'appliance NetScaler ne prend pas en charge la fonctionnalité push du serveur HTTP/2.
- L'appliance NetScaler ne prend pas en charge la fonctionnalité de priorisation des requêtes HTTP/2.
- L'appliance NetScaler ne prend pas en charge la renégociation SSL HTTP/2 pour les configurations d'équilibrage de charge HTTPS.
- L'appliance NetScaler ne prend pas en charge l'authentification HTTP/2 NTLM.
- Lorsque HTTP/2 est activé, le multiplexage des connexions désactivé (comme USIP activé) et le mappage individuel des connexions TCP client et serveur, les événements de fermeture tels que FIN, reset (RST) sont transférés de la connexion client ou serveur à la connexion homologue liée.

Configuration de HTTP/2

La configuration de HTTP/2 pour une configuration d'équilibrage de charge (HTTPS ou HTTP) comprend les tâches suivantes :

- **Activez HTTP/2 et définissez des paramètres HTTP/2 facultatifs dans un profil HTTP**. Activez HTTP/2 dans un profil HTTP. Lorsque vous activez HTTP/2 uniquement dans un profil HTTP, l'appliance NetScaler utilise uniquement la méthode de mise à niveau (pour HTTP) ou la méthode TLS ALPN (pour HTTPS) pour communiquer en HTTP/2.

  Pour que l'appliance NetScaler utilise la méthode HTTP/2 directe, l'option **Direct HTTP/2** doit être activée dans le profil HTTP. Pour que l'appliance NetScaler puisse utiliser le HTTP/2 direct à l'aide de la méthode de service alternative, l'option **Service alternatif (altsvc)** doit être activée dans le profil HTTP.

- **Liez le profil HTTP à un serveur virtuel ou à un service**. Liez le profil HTTP à un serveur virtuel pour configurer HTTP/2 pour le côté client de la configuration de l'équilibrage de charge. Liez le profil HTTP à un service afin de configurer HTTP2 pour le côté serveur de la configuration de l'équilibrage de charge.

> **Remarque**
>
> Citrix recommande de lier des profils HTTP distincts pour le côté client et le côté serveur.

- **Activez le paramètre global pour la prise en charge HTTP/2 côté serveur**. Activez le paramètre HTTP global **HTTP/2 Service Side(HTTP2ServerSide**) pour activer la prise en charge HTTP/2 côté serveur de toutes les configurations d'équilibrage de charge pour lesquelles HTTP/2 est configuré.

  HTTP/2 ne fonctionne pas côté serveur des configurations d'équilibrage de charge si le **côté service HTTP/2** est désactivé, même si le **protocole HTTP/2** est activé sur le profil HTTP lié aux services d'équilibrage de charge associés.

Procédures de**ligne de commande NetScaler** :

Pour activer HTTP/2 et définir les paramètres HTTP/2 à l'aide de la ligne de commande NetScaler

- Pour activer HTTP/2 et définir les paramètres HTTP/2 lors de l'ajout d'un profil HTTP, à l'invite de commandes, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )] [-altsvc ( ENABLED | DISABLED )]
show ns httpProfile <name>
```

- Pour activer HTTP/2 et définir les paramètres HTTP/2 lors de la modification d'un profil HTTP, à l'invite de commandes, tapez :

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED)] [-altsvc (ENABLED | DISABLED )]
show ns httpProfile <name>
```

Pour lier le profil HTTP à un serveur virtuel à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

```
set lb vserver <name> - httpProfileName <string>
show lb vserver <name>
```

Pour lier le profil HTTP à un service d'équilibrage de charge à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

```
set service <name> -httpProfileName <string>
show service <name>
```

Pour activer le support HTTP/2 globalement côté serveur à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

```
set ns httpParam -HTTP2Serverside( ENABLED | DISABLED )
show ns httpParam
```

Pour activer HTTP/2 et définir les paramètres HTTP/2 à l'aide de l'interface graphique NetScaler

1. Accédez à **Système** > **Profils**, puis cliquez sur l'onglet **Profils HTTP** .
2. Activez **HTTP/2** lors de l'ajout d'un profil HTTP ou de la modification d'un profil HTTP existant.

Pour lier le profil HTTP à un serveur virtuel à l'aide de l'interface graphique NetScaler

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, puis ouvrez le serveur virtuel.
2. Dans **Paramètres avancés**, cliquez **sur+Profil HTTP** pour lier le profil HTTP créé au serveur virtuel.

Pour lier le profil HTTP à un service d'équilibrage de charge à l'aide de l'interface graphique NetScaler

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Service**, puis ouvrez le service.
2. Dans **Paramètres avancés**, cliquez **sur+Profil HTTP** pour lier le profil HTTP créé au service.

Pour activer la prise en charge de HTTP/2 globalement côté serveur à l'aide de l'interface graphique

Accédez à **Système** > **Paramètres**, cliquez sur **Modifier les paramètres HTTP** et activez **HTTP/2 Server Side**.

Exemples de configurations

Dans l'exemple de configuration suivant, HTTP/2 et HTTP/2 direct sont activés sur le profil HTTP HTTP-PROFILE-HTTP2-CLIENT-SIDE. Le profil est lié au serveur virtuel LB-VS-1.

```
set ns httpProfile HTTP-PROFILE-HTTP2-CLIENT-SIDE -http2 enabled -
   http2Direct enabled
Done

set lb vserver LB-VS-1 -httpProfileName HTTP-PROFILE-HTTP2-CLIENT-SIDE

Done
<!--NeedCopy-->
```

Dans l'exemple de configuration suivant, HTTP/2 et le service alternatif (ALT-SVC) sont activés sur le profil HTTP HTTP-PROFILE-HTTP2-SERVER-SIDE. Le profil est lié au service LB-SERVICE-1.

```
set ns httpparam -HTTP2Serverside ENABLED
Done

set ns httpProfile HTTP-PROFILE-HTTP2-SERVER-SIDE -http2 ENABLED -
   altsvc ENABLED
Done

set service LB-SERVICE-1 -httpProfileName HTTP-PROFILE-HTTP2-SERVER-
   SIDE
Done
<!--NeedCopy-->
```

Configurer la taille de la fenêtre de connexion initiale HTTP/2

Conformément à la RFC 7540, la fenêtre de contrôle de flux pour le flux HTTP2 et la connexion doit être définie sur 64 K (65535) octets, et toute modification apportée à cette valeur doit être communiquée à l'homologue. L'appliance ADC communique la modification de la taille de la fenêtre de contrôle de flux comme suit :

- Utiliser le `SETTINGS` cadre pour le flux.
- Utilisation du `WINDOW_UPDATE` cadre pour la connexion.

Dans un profil HTTP, vous devez configurer le paramètre `http2InitialWindowSize` pour définir la taille initiale de la fenêtre au niveau du flux. En raison d'une erreur système interne, l'appliance ADC initialise également la fenêtre de contrôle de flux de la connexion. En cas de modification de la fenêtre de contrôle de flux configurée pour le flux, l'appliance ADC communique avec l'homologue à l'aide de la trame SETTINGS. Mais l'appliance ADC ne parvient pas à communiquer la modification de la fenêtre de contrôle de flux pour la connexion à l'aide de la `WINDOW_UPDATE` trame. Cela entraîne un gel de la connexion.

Pour résoudre ce problème, le paramètre `http2InitialConnWindowSize` (en octets) est maintenant ajouté pour contrôler la fenêtre de contrôle de flux pour la connexion. En utilisant des paramètres configurables distincts, vous pouvez désormais permettre à l'appliance d'envoyer des mises à jour pour modifier la taille de fenêtre au niveau du flux et de la connexion.

Configurer le paramètre de taille de fenêtre de connexion initiale HTTP/2 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set http profile p1 -http2InitialConnWindowSize 8290
Initial window size for stream level flow control, in bytes.
Default value: 65535
Minimum value: 8192
Maximum value: 20971520
<!--NeedCopy-->
```

> **Remarque :**
> lorsque HTTP/2 est activé, Citrix vous recommande de désactiver le paramètre TCP Dynamic Receive Buffering dans le profil TCP.

Configuration de WebSocket sur HTTP/2

L'appliance NetScaler prend en charge les connexions WebSocket via HTTP/2. Vous pouvez activer les connexions WebSocket à l'aide de l'interface CLI ou de l'interface graphique. La connexion WebSocket HTTP/2 peut être multiplexée.

Configurez les connexions WebSocket via HTTP/2 à l'aide de l'interface de ligne de commande

Par défaut, le paramètre **WebSocket Connections** est désactivé. Vous pouvez activer les connexions WebSocket à l'aide de l'interface CLI.

Activez les connexions WebSocket HTTP/2 du frontend :

À l'invite de commande, tapez :

Pour la configuration SSL :

```
add httpprofile <http_profile_name> -http2 enabled -websocket enabled

<!--NeedCopy-->
```

Pour la configuration en texte brut :

```
add httpprofile <http_profile_name> -http2 enabled -http2direct enabled
    -websocket enabled

<!--NeedCopy-->
```

Activez les connexions WebSocket HTTP/2 du backend :

À l'invite de commande, tapez :

Pour la configuration SSL :

```
add httpprofile <http_profile_name> -http2 enabled
set httpparam -http2serverside ON
<!--NeedCopy-->
```

Pour la configuration en texte brut :

```
add httpprofile <http_profile_name> -http2 enabled -http2direct enabled
set httpparam -http2serverside ON
<!--NeedCopy-->
```

Configurez les connexions WebSocket via HTTP/2 à l'aide de l'interface graphique

Vous pouvez utiliser la procédure suivante pour activer les connexions WebSocket à l'aide de l'interface graphique.

Modifiez les profils existants :

1. Accédez à **Système>Profiles>Profils HTTP**.
2. Sélectionnez le profil souhaité dans les **Profils** et cliquez sur **Modifier**.
3. Dans la section **Configurer le profil HTTP, cochez**les cases **HTTP2** ou **DirectHTTP2** .
4. Activez les connexions WebSocket en cochant la case **Activer les connexions WebSocket** .

Ajouter de nouveaux profils :

1. Accédez à **Système>Profiles>Profils HTTP**.

2. Vous pouvez ajouter un nouveau profil HTTP2 en cliquant sur **Ajouter**.
3. Dans la section **Créer un profil HTTP, cochez**les cases **HTTP2** ou **DirectHTTP2** .
4. Cochez la case **Activer les connexions WebSocket** .

Le tableau suivant décrit le comportement de la connexion WebSocket lorsque le multiplexage principal est désactivé :

Version du paquet HTTP	WebSocket dans le profil HTTP	Action de demande	Backend HTTP/1.1	Backend HTTP/2
HTTP/1.1	Désactivé	lâché	SO	SO
HTTP/1.1	Activé	HTTP/1.1	Chaque connexion HTTP/1.1 est mappée à une connexion HTTP/1.1 dédiée sur le backend	Connexion HTTP/2 dédiée sur le backend pour chaque connexion HTTP/1.1
HTTP/2	Activé	HTTP/2	Chaque flux du front-end est mappé à une connexion HTTP/1.1 dédiée	Tous les flux frontaux peuvent être mappés à une seule connexion HTTP/2 ou à un maximum de trois connexions HTTP/2 sur le backend.
HTTP/2	Désactivé	lâché	SO	SO

Le tableau suivant décrit le comportement de la connexion WebSocket lorsque le multiplexage principal est activé :

Version du paquet HTTP	WebSocket dans le profil HTTP	Action de demande	Backend HTTP/1.1	Backend HTTP/2
HTTP/1.1	Désactivé	lâché	SO	SO

Version du paquet HTTP	WebSocket dans le profil HTTP	Action de demande	Backend HTTP/1.1	Backend HTTP/2
HTTP/1.1	Activé	HTTP/1.1	Chaque connexion HTTP/1.1 est mappée à une connexion HTTP/1.1 dédiée sur le backend	Plusieurs clients HTTP/1.1 peuvent être multiplexés en une seule connexion HTTP/2 ou en plusieurs connexions HTTP/2
HTTP/2	Activé	HTTP/2	Chaque flux du front-end est mappé à une connexion HTTP/1.1 dédiée	Tous les flux frontaux peuvent être mappés à une seule connexion HTTP/2 ou à plusieurs connexions HTTP/2 sur le backend
HTTP/2	Désactivé	lâché	SO	SO

Atténuation du DoS HTTP/2

May 5, 2023

Les attaques par déni de service (DoS) HTTP/2 n'ont plus aucun impact sur une appliance NetScaler. Si l'appliance reçoit un nombre d'images supérieur à la limite maximale, elle ferme la connexion en silence.

Pour atténuer les attaques, le profil HTTP vous permet de modifier la configuration par défaut des trames reçues dans une connexion HTTP/2.

Le tableau d' atténuation des déni de service HTTP/2 affiche la liste des attaques DoS HTTP/2 et ses mesures d'atténuation.

Configurez la limite maximale pour les trames HTTP/2 afin d'atténuer les attaques DoS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ce qui suit :

```
set ns httpprofile <profile_name> - http2MaxEmptyFramesPerMin <positive_integer
> -http2MaxPingFramesPerMin <positive_integer> -http2MaxSettingsFramesPerMin
 <positive_integer> -http2MaxResetFramesPerMin <positive_integer>
```

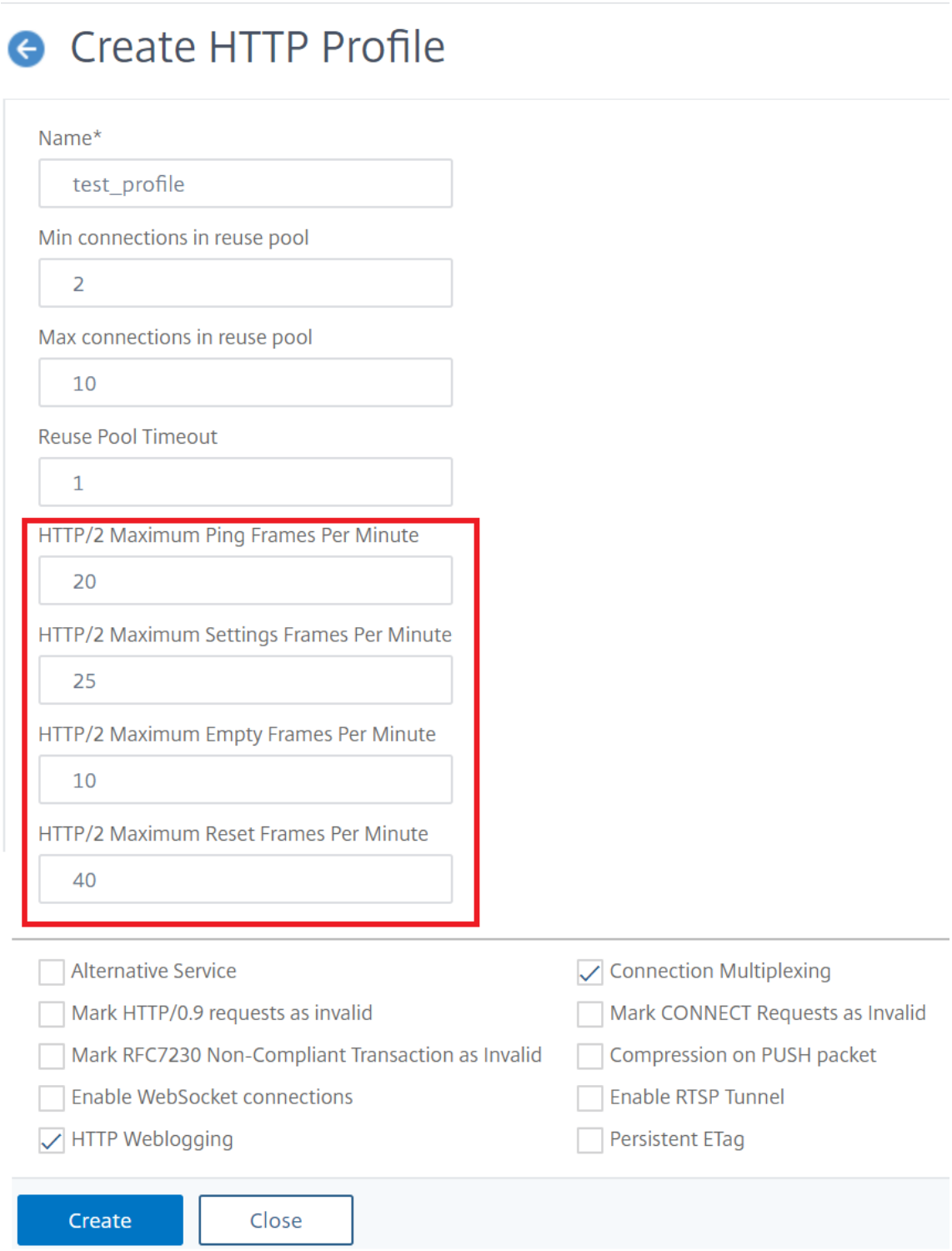
Exemple :

```
set ns httpprofile profile1 -http2MaxEmptyFramesPerMin 20 -http2MaxPingFramesPerMin
 20 -http2MaxSettingsFramesPerMin 20 -http2MaxResetFramesPerMin 20
```

Configurez la limite maximale pour les images reçues dans une connexion HTTP/2 à l'aide de l'interface graphique NetScaler

Suivez les étapes ci-dessous pour configurer la limite maximale pour les trames reçues dans une connexion HTTP/2 :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Profils**.
2. Sur la page **Profil**, sélectionnez l'onglet **Profils HTTP** .
3. Dans l'onglet **Profils HTTP**, cliquez sur **Ajouter**.
4. Sur la page **Configurer le profil HTTP**, définissez le paramètre suivant.
    a) http2MaxPingFramesPerMin. Définissez le nombre maximum de trames PING reçues par connexion en une minute. Si le nombre de trames PING dépasse la limite de configuration, l'appliance supprime silencieusement les paquets sur la connexion.
    b) http2MaxSettingsFramesPerMin. Définissez le nombre maximum de cadres de paramètres reçus par connexion en une minute. Si le nombre de trames SETTINGS dépasse la limite de configuration, ADC supprime silencieusement les paquets sur la connexion.
    c) http2MaxResetFramesPerMin. Définissez le nombre maximum de trames RESET envoyées par connexion en une minute. Si le nombre de trames RESET dépasse la limite de configuration, ADC supprime silencieusement les paquets sur la connexion.
    d) http2MaxEmptyFramesPerMin. Définissez le nombre maximum d'images vides envoyées par connexion en une minute. Si le nombre de trames vides dépasse la limite de configuration, ADC supprime silencieusement les paquets sur la connexion.
5. Cliquez sur **OK** et sur **Fermer**.



Protocole HTTP3 sur QUIC

May 5, 2023

HTTP/2 sur TCP est la norme préférée pour l'envoi de plusieurs flux de requêtes HTTP sur une seule connexion. Toutefois, dans le mécanisme de transport TCP, l'accès aux sites Web et aux applications Web présente certaines limitations et problèmes de latence. Lorsque vous multiplexez plusieurs demandes sur la même connexion, elles sont soumises à la fiabilité de la même connexion. Si le paquet d'une demande est perdu, toutes les autres demandes multiplexées sont retardées jusqu'à ce que le paquet perdu soit détecté et retransmis. Cela entraîne des retards de blocage de la tête de ligne et des problèmes de latence.

Pour les retards de connexion et de transport, HTTP/3 utilise QUIC au lieu du protocole TCP. Le QUIC est un protocole émergent qui utilise UDP au lieu de TCP comme transport de base. Dans HTTP overQuic, vous pouvez multiplexer plusieurs requêtes indépendantes sans dépendre d'une seule connexion TCP. QUIC met en œuvre une connexion fiable sur laquelle vous pouvez diffuser plusieurs requêtes HTTP en streaming. QUIC intègre également TLS en tant que composant intégré et non en tant que couche supplémentaire, comme dans HTTP/1.1 ou HTTP/2.

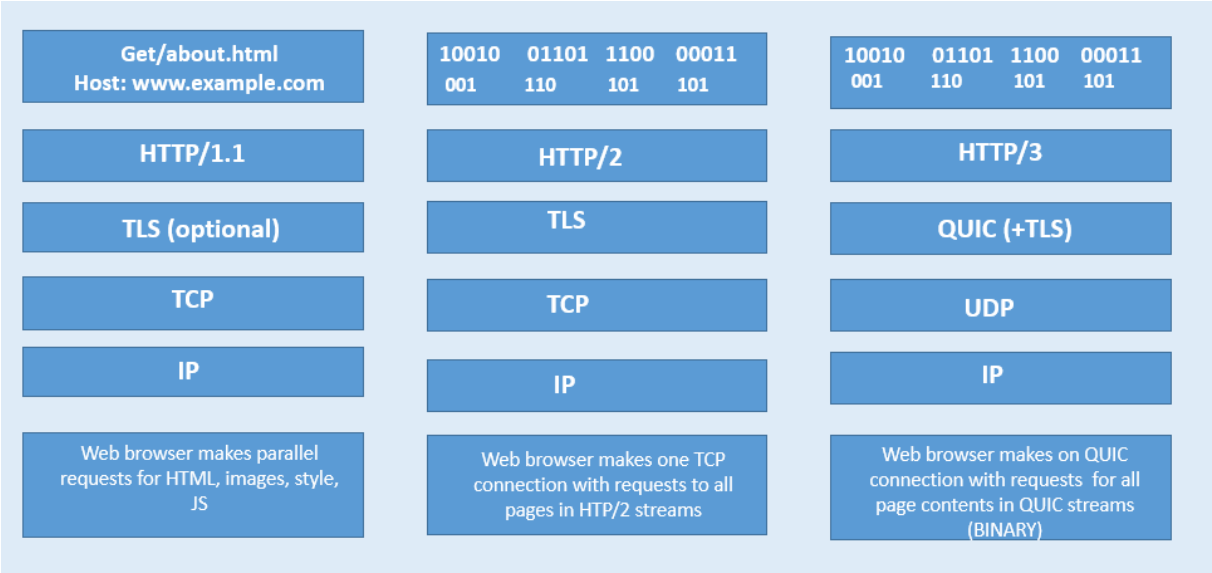
Avantage de l'utilisation du protocole HTTP/3

Voici quelques-uns des avantages importants de l'utilisation du protocole QUIC pour le transport de données HTTP/3 :

- Multiplexage de flux
- Contrôle du débit au niveau du flux et de la connexion
- Établissement de connexions à faible latence
- Migration des connexions et résilience à la reliaison NAT
- En-tête et charge utile authentifiés et chiffrés

Pile de transport dans les protocoles HTTP

L'illustration ci-dessous montre la pile de transport dans les protocoles HTTP/1.1, HTTP/2 et HTTP/3.



Comment fonctionne la gestion des connexions QUIC et HTTP/3 dans NetScaler

L'illustration suivante montre comment les connexions QUIC et HTTP/3 sont gérées dans une appliance NetScaler et comment les composants interagissent les uns avec les autres.

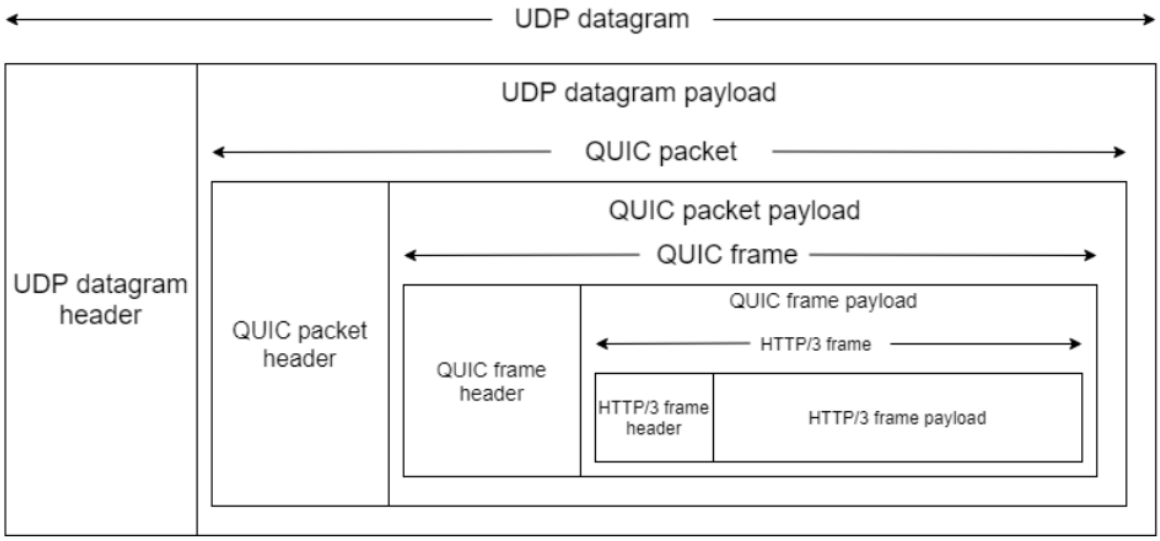
Étape 1 : Requête HTTP/3 côté client via le protocole QUIC vers l'appliance NetScaler.
Étape 2 : Requête transmise par NetScaler AS HTTP/1.1 ou HTTP/2 en fonction du support du serveur principal.
Étape 3 : Réponse via HTTP/2 ou HTTP/1.1 du serveur principal à NetScaler.
Étape 4 : ADC transmet la réponse en tant que réponse HTTP/3 au client.

Fonctionnement du protocole HTTP/3

Dans HTTP/3, lorsqu'un client sait qu'un serveur HTTP/3 existe sur un point de terminaison donné, il ouvre une connexion QUIC. Le protocole QUIC permet le multiplexage et le contrôle du flux. Dans chaque flux, l'unité de base de la communication HTTP/3 est une trame. Chaque type de cadre a un

objectif différent. Par exemple, les blocs HEADERS et DATA constituent la base des requêtes et des réponses HTTP.

Le multiplexage des requêtes est effectué à l'aide de l'abstraction de flux QUIC. Chaque paire demande-réponse consomme un flux QUIC unique. Les flux sont indépendants les uns des autres, de sorte qu'un flux bloqué ou subit une perte de paquets n'empêche pas la progression sur d'autres flux. Server Push est un mode d'interaction introduit dans HTTP/2 qui permet à un serveur de transmettre un échange demande-réponse à un client en prévision de la demande indiquée par le client. Cela permet d'opposer l'utilisation du réseau à un gain potentiel de latence. Plusieurs trames HTTP/3 sont utilisées pour gérer le push du serveur, telles que PUSH_PROMISE, MAX_PUSH_ID et CANCEL_PUSH. Comme dans HTTP/2, les champs de demande et de réponse sont compressés pour transmission. Parce que HPACK repose sur la transmission dans l'ordre de sections de champs compressés (garantie non fournie par QUIC), HTTP/3 remplace HPACK par QPACK. QPACK utilise des flux unidirectionnels distincts pour modifier et suivre l'état de la table des champs, tandis que les sections de champs codées font référence à l'état de la table sans la modifier.



Configuration HTTP/3 et résumé des statistiques

May 5, 2023

Pour configurer un protocole HTTP/3 pour envoyer plusieurs flux de données HTTP/3 à l'aide de QUIC, vous devez effectuer les étapes suivantes :

1. Activez les fonctionnalités SSL et d'équilibrage de charge.
2. Ajoutez des serveurs virtuels d'équilibrage de charge et de commutation de contenu (facultatif) de type HTTP_QUIC.

3. Associez les paramètres du protocole QUIC au serveur virtuel HTTP_QUIC.
4. Activez HTTP/3 sur le serveur virtuel HTTP_QUIC.
5. Liez la paire de clés de certificat SSL avec le serveur virtuel HTTP_QUIC.
6. Associez les paramètres du protocole SSL/TLS au serveur virtuel HTTP_QUIC.

Activer SSL et l'équilibrage de charge

Avant de commencer, assurez-vous que les fonctionnalités SSL et d'équilibrage de charge sont activées sur l'appliance. À l'invite de commandes, tapez :

```
enable ns feature ssl lb
<!--NeedCopy-->
```

Ajout de serveurs virtuels d'équilibrage de charge et de commutation de contenu (facultatif) de type HTTP_QUIC pour le service HTTP/3

Vous ajoutez un serveur virtuel d'équilibrage de charge pour accepter le trafic HTTP/3 via QUIC.
Remarque : Le serveur virtuel d'équilibrage de charge de type HTTP_QUIC possède des profils QUIC, SSL et HTTP3 intégrés. Si vous préférez créer des profils définis par l'utilisateur, vous pouvez ajouter de nouveaux profils et les lier au serveur virtuel d'équilibrage de charge.

```
add lb vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
    port>

add cs vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
    port>
<!--NeedCopy-->
```

Exemple :

```
add lb vserver lb-http3 HTTP_QUIC 1.1.1.1 443
add cs vserver cs-http3 HTTP_QUIC 10.10.10.10 443
```

Associer les paramètres du protocole QUIC au serveur virtuel HTTP_QUIC

Vous pouvez créer un profil QUIC et spécifier des paramètres QUIC pour le service QUIC et l'associer au serveur virtuel d'équilibrage de charge. Vous devez soit créer un profil défini par l'utilisateur, soit utiliser le profil QUIC intégré et lier le profil au serveur virtuel d'équilibrage de charge.

Étape 1 : configurer un profil QUIC défini par l'utilisateur
À l'invite de commandes, tapez :


```
set quic profile <profile_name> -transport_param <value>
<!--NeedCopy-->
```

Exemple :

```
set quic profile quic_http3 -ackDelayExponent 10 -activeConnectionIDlimit 4
```

Les différents paramètres de transport QUIC sont les suivants :

-ackDelayExponent. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, indiquant un exposant que le point de terminaison QUIC distant doit utiliser pour décoder le champ ACK Delay dans les trames QUIC ACK envoyées par NetScaler.

-activeConnectionIDlimit. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant. Il spécifie le nombre maximum d'identifiants de connexion QUIC provenant du point de terminaison QUIC distant, que NetScaler est prêt à stocker.

-activeConnectionMigration. Spécifiez si NetScaler doit autoriser le point de terminaison QUIC distant à effectuer une migration de connexion QUIC active.

-congestionCtrlAlgorithm. Spécifiez l'algorithme de contrôle de la congestion à utiliser pour les connexions QUIC.

-initialMaxData. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, spécifiant la valeur initiale, en octets, pour la quantité maximale de données pouvant être envoyées via une connexion QUIC.

-initialMaxStreamDataBidiLocal. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, spécifiant la limite de contrôle de flux initiale, en octets, pour les flux QUIC bidirectionnels initiés par NetScaler.

-initialMaxStreamDataBidiRemote. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, spécifiant la limite de contrôle de flux initiale, en octets, pour les flux QUIC bidirectionnels initiés par le point de terminaison QUIC distant.

-initialMaxStreamDataUni. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, spécifiant la limite de contrôle de flux initiale, en octets, pour les flux unidirectionnels initiés par le point de terminaison QUIC distant.

-initialMaxStreamsBidi. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, spécifiant le nombre maximum initial de flux bidirectionnels que le point de terminaison QUIC distant doit initier.

-initialMaxStreamsUni. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, spécifiant le nombre maximum initial de flux unidirectionnels que le point de terminaison QUIC distant doit initier.

-maxAckDelay. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, spécifiant la durée maximale, en millisecondes, pendant laquelle NetScaler retarde l'envoi des accusés de réception.

-maxIdleTimeout. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, spécifiant le délai d'inactivité maximal, en secondes, pour une connexion QUIC. Une connexion QUIC qui reste inactive, plus longtemps que le minimum des valeurs de délai d'inactivité annoncées par NetScaler et le point de terminaison QUIC distant, et trois fois le délai de sonde (PTO) actuel, sera supprimée silencieusement par NetScaler.

-maxUDPPayloadSize. Valeur entière annoncée par NetScaler au point de terminaison QUIC distant, spécifiant la taille de la plus grande charge utile de datagrammes UDP, en octets, que NetScaler est prêt à recevoir sur une connexion QUIC.

-newTokenValidityPeriod. Une valeur entière, spécifiant la période de validité, en secondes, des jetons de validation d'adresse émis via les trames QUIC NEW_TOKEN envoyées par NetScaler.

-retryTokenValidityPeriod. Une valeur entière, spécifiant la période de validité, en secondes, des jetons de validation d'adresse émis via des paquets QUIC Retry envoyés par NetScaler.

-statelessAddressValidation. Spécifiez si NetScaler doit effectuer une validation d'adresse sans état pour les clients QUIC, en envoyant des jetons dans des paquets QUIC Retry lors de l'établissement de la connexion QUIC, et en envoyant des jetons dans des trames QUIC NEW_TOKEN après l'établissement de la connexion QUIC.

Étape 2 : Associez le profil QUIC défini par l'utilisateur à un serveur virtuel d'équilibrage de charge de type http_quic

À l'invite de commande, tapez :

```
set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
    serviceName>@] [-persistenceType <persistenceType>] [-
    quicProfileName <string>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver lb-http3 -quicProfileName quic_http3
```

Activer et lier HTTP/3 sur un serveur virtuel HTTP_QUIC

Pour activer HTTP/3 sur un serveur virtuel HTTP_QUIC, un ensemble de paramètres de configuration est ajouté à la configuration du profil HTTP. Pour faciliter la configuration, lorsque vous ajoutez un serveur virtuel HTTP_QUIC, un nouveau profil HTTP par défaut/intégré est disponible sur l'appliance. Les paramètres de prise en charge du protocole HTTP/3 sont définis sur ENABLED et sont également limités aux serveurs virtuels HTTP_QUIC (applicable si vous choisissez de ne pas associer le serveur

virtuel HTTP_QUIC à un profil HTTP ajouté par l'utilisateur). La valeur des paramètres HTTP/3 dans le profil HTTP décide de sélectionner le protocole HTTP/3 et de faire de la publicité lors du traitement de l'extension TLS ALPN (Application Layer Protocol Negotiation), pendant la prise de contact du protocole QUIC.

Vous pouvez créer un profil HTTP/3 et spécifier des paramètres HTTP pour le service HTTP/3 et le serveur virtuel d'équilibrage de charge. Vous devez soit créer un profil défini par l'utilisateur, soit utiliser le profil HTTP/3 intégré et lier le profil au serveur virtuel d'équilibrage de charge.

Étape 1 : configurer un profil HTTP/3 défini par l'utilisateur
À l'invite de commandes, tapez :

```
Add ns httpProfile <profile_name> -http3 ENABLED
<!--NeedCopy-->
```

Exemple :

```
add ns httpProfile http3_quic -http3 ENABLED
```

Étape 2 : Lier le profil HTTP/3 défini par l'utilisateur à un serveur virtuel d'équilibrage de charge de type http_quic
À l'invite de commandes, tapez :

```
set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
    serviceName>@] [-persistenceType <persistenceType>] [-
    httpProfileName <string>]
<!--NeedCopy-->
```

Exemple :

```
set lb vserver lb-http3 -httpProfileName http3_quic
```

Lier la paire de clés de certificat SSL avec le serveur virtuel HTTP_QUIC

Pour traiter le trafic chiffré, vous devez ajouter une paire de clés de certificat SSL et la lier au serveur virtuel HTTP_QUIC.

À l'invite de commande, tapez :

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>

<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver lb-http3 -certkeyName rsa_certkeypair
```

Pour plus d'informations, consultez la rubrique Bind SSL Certificate .

Lier les paramètres du protocole SSL/TLS à un serveur virtuel HTTP_QUIC

Les serveurs virtuels de type HTTP_QUIC ont une fonctionnalité de serveur TLS 1.3 intégrée, car le protocole QUIC utilise TLS 1.3 comme composant de sécurité obligatoire. Pour faciliter la configuration lors de l'ajout d'un serveur virtuel HTTP_QUIC, un nouveau profil SSL par défaut ou intégré de type Quic-Frontend est ajouté. Le profil SSL dispose de la version TLS 1.3 activée avec les suites de chiffrement TLS 1.3 (et les courbes elliptiques) configurées. Le profil SSL doit ensuite être lié aux nouveaux serveurs virtuels HTTP_QUIC ajoutés.
Vous pouvez créer un profil SSL et spécifier des paramètres de chiffrement SSL pour le service TLP 1.1 et le serveur virtuel d'équilibrage de charge. Vous devez soit créer un profil défini par l'utilisateur, soit utiliser le profil SSL intégré et lier le profil au serveur virtuel d'équilibrage de charge.

Étape 1 : configurer un profil SSL défini par l'utilisateur
À l'invite de commandes, tapez :

```
add ssl profile <name> -sslprofileType QUIC-FrontEnd
<!--NeedCopy-->
```

Exemple :

```
add ssl profile ssl_profile1 -sslprofileType QUIC-FrontEnd -tls13 ENABLED -tls12 DISABLED -tls11 DISABLED -tls1 DISABLED
```

Étape 2 : Lier le profil SSL défini par l'utilisateur à un serveur virtuel d'équilibrage de charge de type HTTP_QUIC
À l'invite de commandes, tapez :

```
set ssl vserver <name>@ [-sslProfile <string>]
<!--NeedCopy-->
```

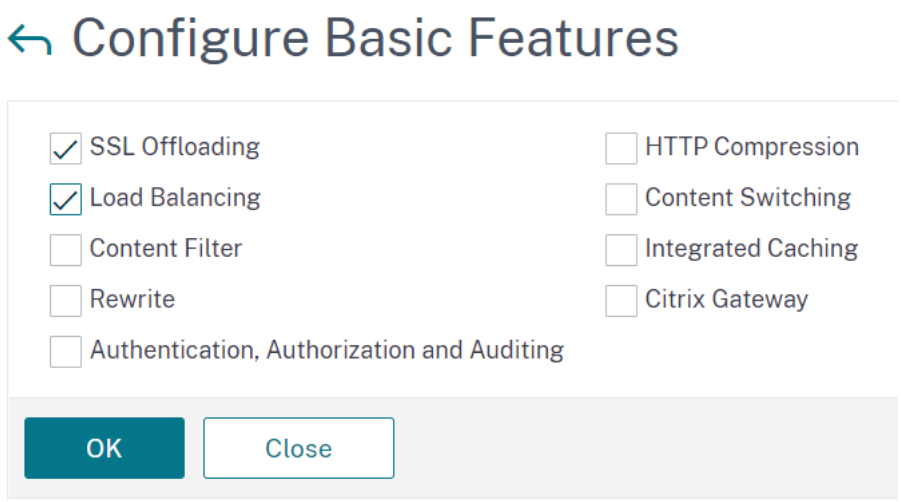
Exemple :

```
set ssl vserver lb-http3 -sslprofile ssl_profile1
```

Activer les fonctionnalités SSL et d'équilibrage de charge à l'aide de l'interface graphique

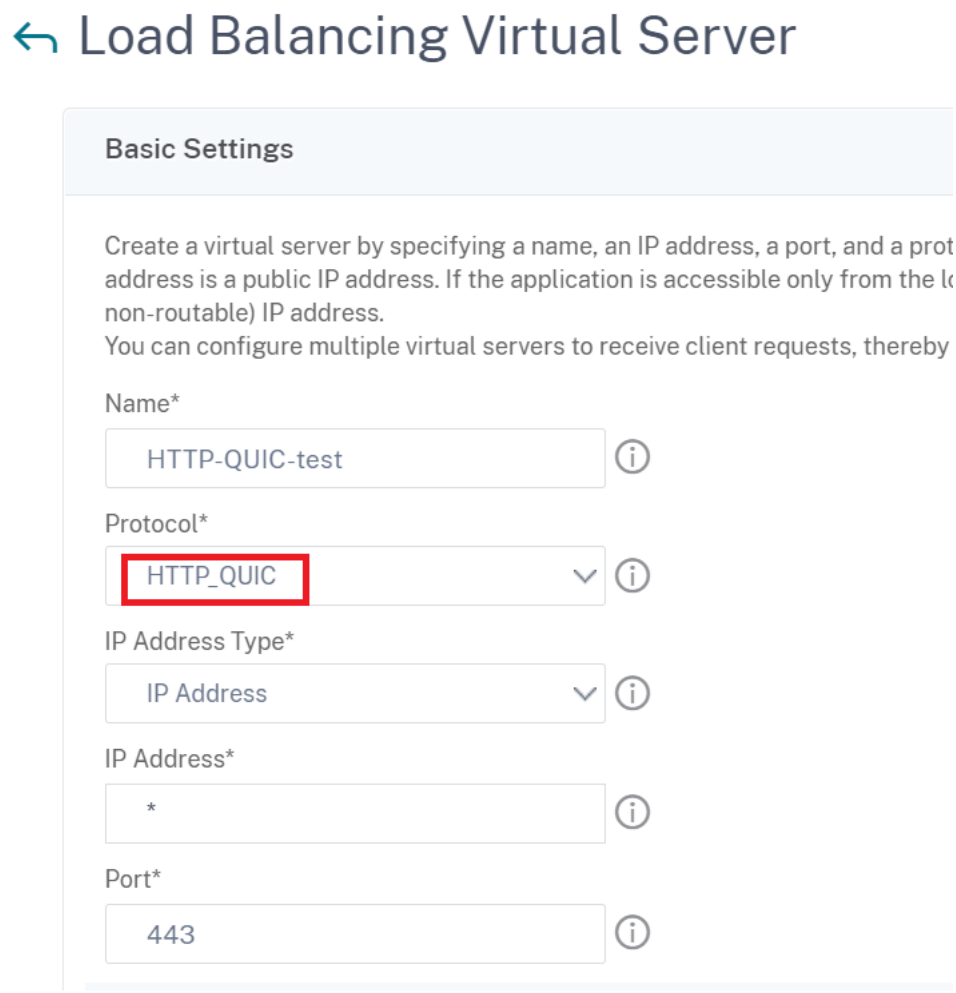
Procédez comme suit pour activer les fonctionnalités SSL et d'équilibrage de charge :

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Paramètres**.
2. Sur la page **Configurer les fonctionnalités de base**, sélectionnez **SSL** et **équilibrage de charge**.
3. Cliquez sur **OK**, puis sur **Fermer**.



Ajoutez des serveurs virtuels d'équilibrage de charge et de commutation de contenu (facultatif) de type HTTP_QUIC à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge de type HTTP_QUIC.
3. Dans la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Profils**.
4. Dans la section **Profils**, sélectionnez le type de profil QUIC. Remarque : les profils QUIC, HTTP/3 et SSL sont intégrés.
5. Cliquez sur **OK**, puis sur **Terminé**.

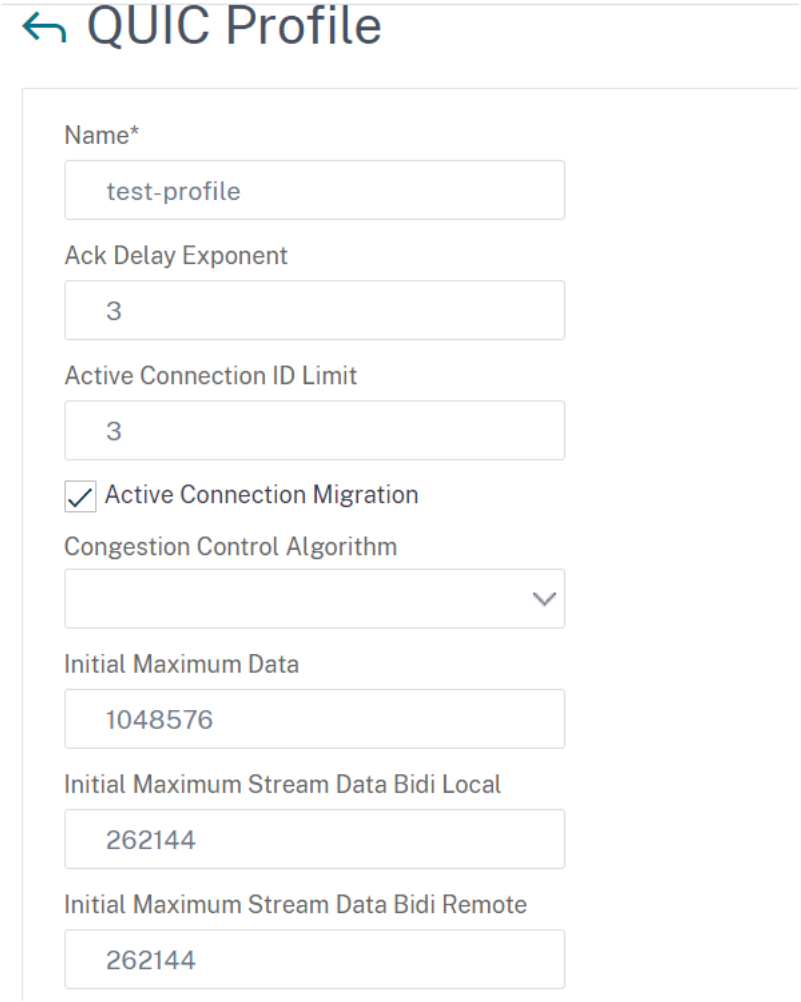


Associez les paramètres du protocole QUIC au serveur virtuel HTTP_QUIC à l'aide de l'interface graphique

Étape 1 : Ajouter un profil QUIC

1. Accédez à **Système > Profils > Profil QUIC**.
2. Cliquez sur **Ajouter**.
3. Dans la page Profil QUIC, définissez les paramètres suivants. Pour une description détaillée de chaque paramètre, reportez-vous à la section Associate QUIC Protocol CLI.
   a) `Ack Delay` Exposant
   b) Active Connection ID Limit
   c) Active Connection Migration
   d) Congestion Control Algorithm
   e) Initial Maximum Data

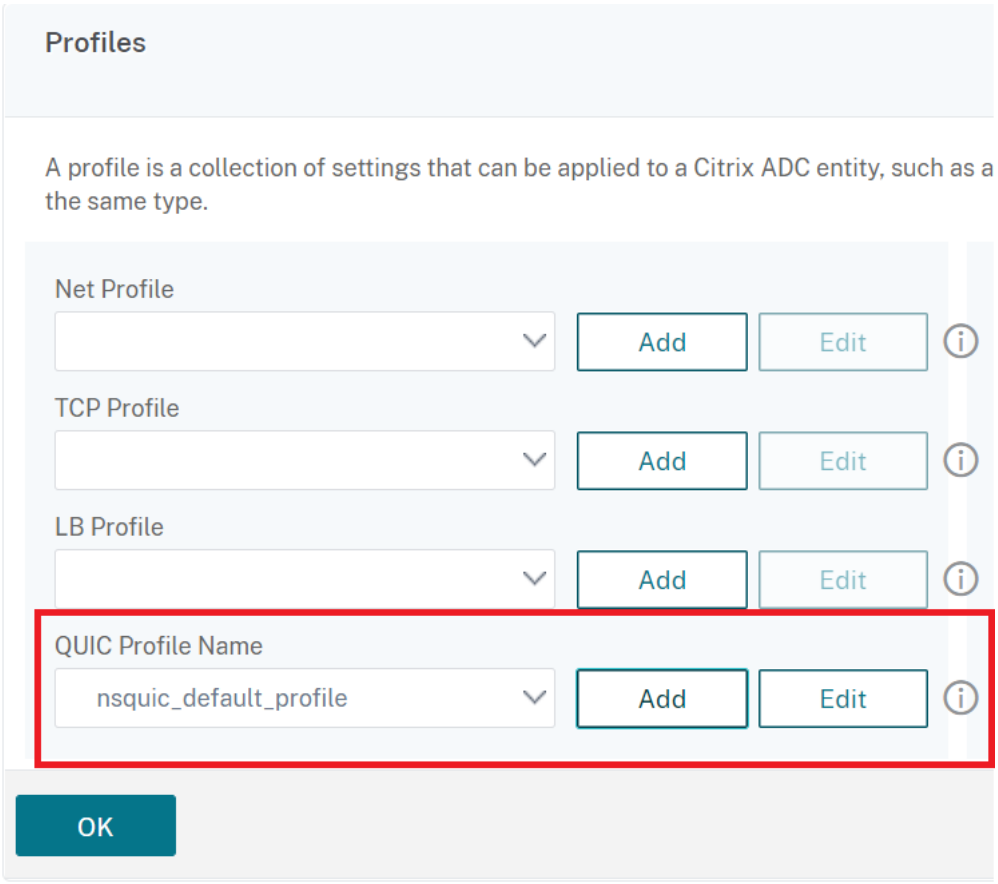
f) Initial Maximum Stream Data Bidi Local
g) Initial Maximum Stream Data Bidi Remote
h) Initial Maximum Stream Data Unit
i) Initial Maximum Stream bidi
j) Initial Maximum Stream Uni
k) Maximum Acknowledgment Delay
l) Maximum Idle Timeout
m) Maximum UDP Data GramsperBurst
n) New Token Validity Period
o) Retry Token Validity Period
p) Stateless Address Validation



Étape 2 : Associer le profil QUIC au serveur virtuel d'équilibrage de charge de type HTTP_QUIC

1. Dans la section **Profils**, sélectionnez le profil QUIC. Remarque : les profils QUIC, HTTP/3 et SSL sont intégrés.

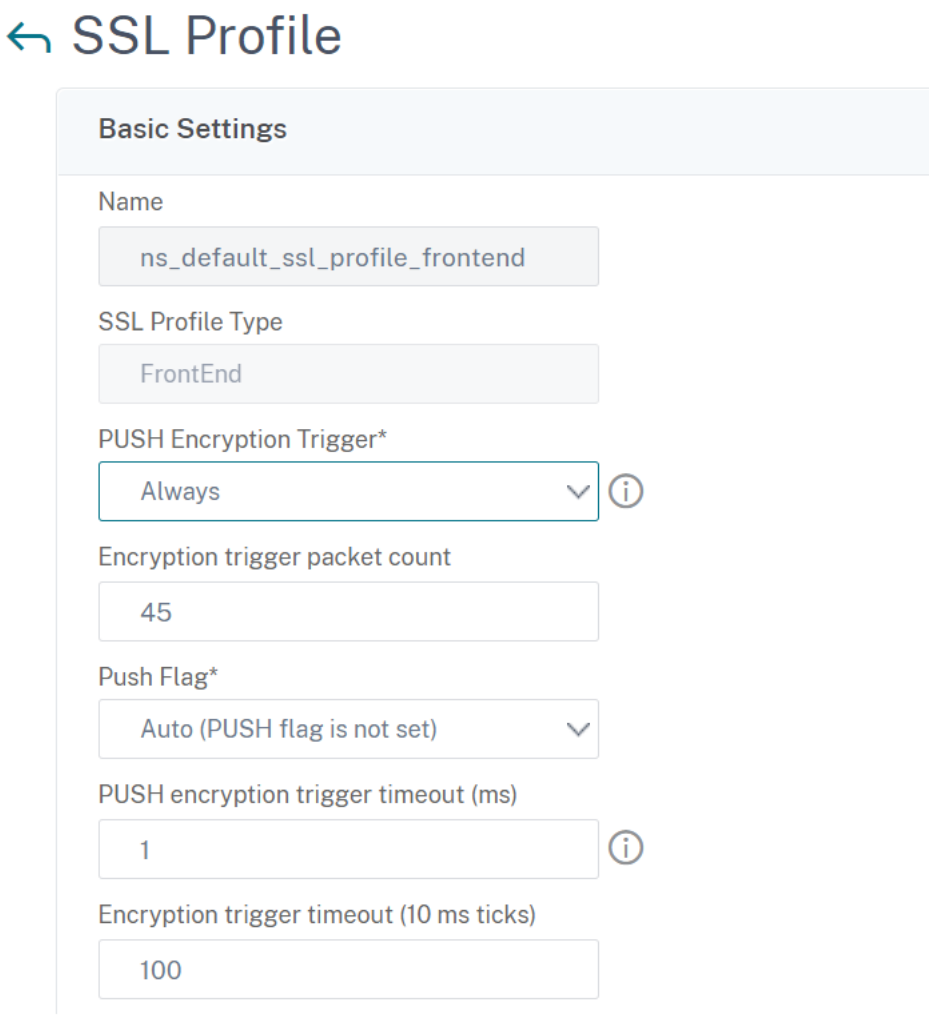
2. Cliquez sur **OK**, puis sur **Terminé**.



Associez les paramètres du protocole SSL/TLS au serveur virtuel de type SSL à l'aide de l'interface graphique

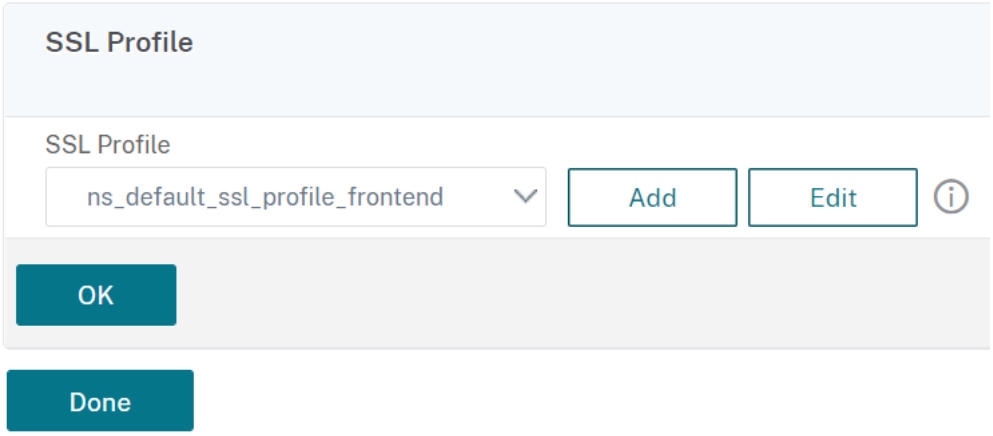
Étape 1 : Ajouter un profil SSL

1. Accédez à **Système > Profils > Profil SSL**.
2. Cliquez sur **Ajouter**.
3. Dans la page **Profil QUIC**, définissez les paramètres SSL. Pour une description détaillée, reportez-vous à la rubrique Configuration du profil SSL.
4. Cliquez sur **OK** et sur **Fermer**.



Étape 2 : Associez le profil SSL au serveur virtuel d'équilibrage de charge de type SSL.

1. Dans la section **Profils**, sélectionnez le profil SSL.
2. Cliquez sur **OK**, puis sur **Terminé**.



Afficher les statistiques QUIC et HTTP/3

Les commandes suivantes affichent un résumé détaillé des statistiques QUIC et HTTP3. À l'invite de commandes, tapez ce qui suit :

```
> stat quic
> stat quic  - detail
<!--NeedCopy-->
```

Pour effacer l'affichage des statistiques, tapez l'une des options suivantes :

```
> stat quic -clearstats basic
> stat quic -clearstats full

<!--NeedCopy-->
```

Pour afficher un résumé détaillé des statistiques HTTP/3 :

```
> stat http3
> stat http3  - detail
<!--NeedCopy-->
```

Pour effacer l'affichage des statistiques, tapez l'une des options suivantes :

```
> stat http3 -clearstats basic
> stat http3 -clearstats full
<!--NeedCopy-->
```

Configuration de la stratégie pour le trafic HTTP/3

May 5, 2023

HTTP/3 utilise le transport QUIC basé sur UDP. Si vous aviez défini une expression de stratégie pour le serveur virtuel HTTP ou SSL qui inclut des expressions de stratégie TCP, elle ne peut plus être utilisée avec un serveur virtuel HTTP_QUIC. Toutes les autres stratégies qui n'ont pas de TCP ou d'expressions classiques peuvent être liées à un serveur virtuel HTTP_QUIC. Pour que les stratégies prennent effet, vous devez vous assurer que les stratégies d'entités sont liées aux points de liaison globaux nouvellement ajoutés, conformément aux indications suivantes.

- HTTPQUIC_REQ_DEFAULT
- HTTPQUIC_REQ_OVERRIDE
- TTPQUIC_RES_DEFAULT

- HTTPQUIC_RES_OVERRIDE

Les stratégies peuvent également être liées à des points de liaison de serveurs virtuels spécifiques :

- REQUEST
- RESPONSE

Pour plus d'informations, consultez la rubrique Lier la stratégie à l'aide d'une infrastructure de stratégie avancée .

Voici les stratégies prises en charge pour la configuration HTTP sur QUIC :

- Répondeur
- Réécriture
- Compression HTTP
- Mise en cache intégrée
- Pare-feu d'application Web
- Transformation d'URL
- SSL
- Optimisation frontale (FEO)
- AppQoE

Configuration de la stratégie de répondeur pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de répondeur. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.

Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison globaux QUIC. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajout d'une action de répondeur pour rediriger les URL

Pour ajouter une action de répondeur, à l'invite de commandes, tapez :

```
add responder action <name> <type> (<target> | <htmlpage>) [-comment <
    string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
    expression>] [-headers <name(value)> ...]
<!--NeedCopy-->
```

Exemple :

```
add responder action redirectURL redirect "\"https://www.citrix.com/\""
```


Add responder policy

Pour ajouter une stratégie de répondeur, à l'invite de commandes, tapez :

```
1 add responder policy <name> <rule> <action> [<undefAction>] [-comment <
     string>] [-logAction <string>] [-appflowAction <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add responder policy res-pol "CLIENT.IP.SRC.IN_SUBNET(10.10.10.10/32)"
redirectURL
```

Ajout d'une expression UDP basée sur une stratégie de répondeur

Pour ajouter une expression UDP basée sur une stratégie de répondeur, à l'invite de commandes, tapez :

```
1 add responder policy <name> <rule> <action> [<undefAction>] [-comment <
     string>] [-logAction <string>] [-appflowAction <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add responder policy redirectCitrixUdp "CLIENT.UDP.DSTPORT.EQ(443)"redirectURL
```

Lier une expression UDP basée sur une stratégie de répondeur avec un serveur virtuel d'équilibrage de charge basé sur HTTP/3 QUIC

Pour lier une expression UDP basée sur une stratégie de répondeur à un serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez :

```
1 bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
      ) | <serviceGroupName>@ |         (-policyName <string>@  [-
     priority <positive_integer>]  [-gotoPriorityExpression <expression>]
       [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
     analyticsProfile <string>@)
2 <!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 9 -gotoPriorityExpres
 END -type REQUEST
```


Lier la stratégie de répondeur avec un serveur virtuel d'équilibrage de charge basé sur HTTP/3 QUIC

Pour lier une stratégie de répondeur à un serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez :

```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 10 -
gotoPriorityExpression END -type REQUEST
```

Lier la stratégie du répondeur au point de liaison global HTTP/3

Pour lier une stratégie de répondeur au point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
bind responder global <policyName> <priority>  [<gotoPriorityExpression
    >] [-type <type>] [-invoke (<labelType>  <labelName>) ] bind
    responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
<!--NeedCopy-->
```

Exemple :

```
bind responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
```

> **Remarque :**
>
> Pour plus d'informations, consultez la documentation sur les stratégies de répondeur.

Configuration de la stratégie de réécriture pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC prennent en charge les stratégies de réécriture. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.

Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Vous trouverez ci-dessous les étapes de configuration permettant de configurer la stratégie de réécriture pour HTTP3 sur QUIC.

Ajout d'une action de réécriture pour HTTP sur QUIC

Pour ajouter une action de réécriture, à l'invite de commandes, tapez :

```
1 add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
     search <expression>] [-refineSearch <expression>] [-comment <string
     >]
2 <!--NeedCopy-->
```

Exemple :

```
add rewrite action http3-altsvc-action insert_http_header Alt-Svc q/"h3
-29=\":443\"; ma=3600; persist=1"/
```

Ajouter une stratégie de réécriture pour HTTP sur QUIC

Pour ajouter une action d'écriture, à l'invite de commandes, tapez :

```
1 add rewrite policy <name> <rule> <action> [<undefAction>] [-comment  <
     string>] [-logAction <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add rewrite policy http3-altsvc-policy true http3-altsvc-action
```

Lier la stratégie de réécriture au serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier la stratégie de réécriture au serveur virtuel d'équilibrage de charge, à l'invite de commandes, tapez :

```
1 bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )
      | <serviceGroupName>@ | (-policyName <string>@ [-priority <
     positive_integer>] [-gotoPriorityExpression <expression>] [-type <
     type>] [-invoke (<labelType> <labelName>) ] ) | -analyticsProfile  <
     string>@)
2 <!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName http3-altsvc-policy -priority 10 -type
 RESPONSE
```


Lier la stratégie de réécriture au point de liaison global HTTP/3

```
To bind a responder policy with HTTP/3 global bind point, at the
    command prompt, type:
bind rewrite global <policyName> <priority> [<gotoPriorityExpression>]
     [-type <type>] [-invoke (<labelType> <labelName>)]
<!--NeedCopy-->
```

Exemple :

```
bind rewrite global http3-altsvc-policy 3 -type HTTPQUIC_RES_DEFAULT
```

> **Remarque :**
>
> Pour plus d'informations, consultez la documentation sur la stratégie de réécriture.

Configuration de la stratégie de compression pour le trafic HTTP/3

Lorsque NetScaler reçoit une réponse HTTP d'un serveur, il évalue les politiques de compression intégrées et toutes les politiques de compression personnalisées afin de déterminer s'il convient de compresser la réponse et, le cas échéant, le type de compression à appliquer. Les priorités attribuées aux stratégies déterminent l'ordre dans lequel les stratégies sont mises en correspondance avec les demandes.

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de compression. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.

Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter une stratégie de compression

Pour ajouter une stratégie de compression, à l'invite de commandes, tapez :

```
add cmp policy <name> -rule <expression> -resAction <string>
<!--NeedCopy-->
```

Exemple :

```
add cmp policy udp_port_cmp_policy -rule "CLIENT.UDP.DSTPORT.EQ(443)"-
resAction COMPRESS
```


Lier une stratégie de compression avec un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier une stratégie de transformation d'URL à un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC, à l'invite de commandes, tapez :

```
bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
    ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
    positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
     REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
    -analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName udp_port_cmp_policy -priority 10 -type
 RESPONSE
```

Compression de liaison globale au point de liaison global HTTP/3

Pour lier une stratégie de compression avec le point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
bind compression global <policyName> <priority>  [<
    gotoPriorityExpression>] [-type <type>] [-invoke (<labelType>  <
    labelName>) ] bind responder global redirectCitrixUdp 3 -type
    HTTPQUIC_REQ_DEFAULT
<!--NeedCopy-->
```

Exemple :

```
bind cmp global udp_port_cmp_policy -priority 100 -type HTTPQUIC_RES_DEFAULT
 Global built-in compression policies
```

Après la mise à niveau de votre appliance vers NetScaler version 13.0 build 82.x, les politiques de compression suivantes seront automatiquement liées au point de liaison par défaut HTTP/3.

```
> sho cmp global -type HTTPQUIC_RES_DEFAULT
        Policy Name: ns_adv_nocmp_xml_ie
        Priority: 8700
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_nocmp_mozilla_47
        Priority: 8800
        GotoPriorityExpression: END
```



```
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_cmp_mscss
        Priority: 8900
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_cmp_msapp
        Priority: 9000
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_cmp_content_type
        Priority: 10000
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT
<!--NeedCopy-->
```

Si elles ne sont pas liées, les commandes suivantes peuvent être configurées via l'invite de commandes et vous pouvez configurer sur votre appliance.

```
bind cmp global ns_adv_nocmp_xml_ie -priority 8700 -gotoPriorityExpression
END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_nocmp_mozilla_47 -priority 8800 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_mscss -priority 8900 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_msapp -priority 9000 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_content_type -priority 10000 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT
```

Pour plus d'informations, voir Configuration de la stratégie de compression.

Configuration de stratégie de mise en cache pour le trafic HTTP/3

Le cache intégré fournit un stockage en mémoire sur l'appliance NetScaler et diffuse du contenu Web aux utilisateurs sans qu'il soit nécessaire d'aller et retour vers un serveur d'origine. Pour le contenu statique, le cache intégré nécessite peu de configuration initiale. Une fois que vous avez activé la fonctionnalité de cache intégrée et effectué la configuration de base (par exemple, en déterminant la quantité de mémoire de l'appliance NetScaler que le cache est autorisé à utiliser), le cache intégré

utilise des politiques intégrées pour stocker et diffuser des types spécifiques de contenu statique, notamment de simples pages Web et des fichiers image. Vous pouvez également configurer le cache intégré pour stocker et diffuser du contenu dynamique marqué comme non mis en cache par les serveurs Web et d'applications (par exemple, les enregistrements de base de données et les cotations boursières).
Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de cache. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.

Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter un groupe de contenu cache

Pour ajouter le groupe de contenu du cache, à l'invite de commandes, tapez :

```
1 add cache contentGroup <name> [-weakPosRelExpiry <secs> | -relExpiry <
      secs> | -relExpiryMilliSec <msecs> | -absExpiry <HH:MM> ... | -
      absExpiryGMT <HH:MM> ...] [-heurExpiryParam <positive_integer>] [-
      weakNegRelExpiry <secs>] [-maxResSize <KBytes>] [-memLimit <MBytes>]
      ...
2 <!--NeedCopy-->
```

Exemple :

```
add cache contentGroup DEFAULT -maxResSize 500
```

Ajouter une stratégie de cache

Pour ajouter une stratégie de cache, à l'invite de commandes, tapez :

```
1 add cache policy <policyName> -rule <expression> -action <action>  [-
      storeInGroup <string>] [-invalGroups <string> ...] [-invalObjects <
      string> ...] [-undefAction ( NOCACHE | RESET )] add cache policy <
      name> <rule> <profileName> [-comment <string>]  [-logAction <string
      >]
2 <!--NeedCopy-->
```

Exemple :

```
add cache policy ctx_doc_pdf -rule "HTTP.REQ.URL.ENDSWITH(\".pdf\")"-action
 CACHE -storeInGroup DEFAULT
```


Lier une stratégie de cache avec un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier une stratégie de cache avec un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC, à l'invite de commandes, tapez :

```
bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
    ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
    positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
     REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
    -analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName ctx_doc_pdf -priority 100 -type
REQUEST
```

Stratégie de cache de liaison globale au point de liaison global HTTP/3

Pour lier un point de liaison global HTTP/3 de stratégie de cache :

```
bind cache global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Exemple :

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Pour plus d'informations, voir Configuration intégrée de la stratégie de cache.

Stratégies globales de cache intégrées

Après la mise à niveau de votre appliance vers NetScaler version 13.0 build 82.x, les politiques de cache suivantes seront automatiquement liées au point de liaison par défaut HTTP/3.

Lors de la mise à niveau vers la version 13.0 82.x, les stratégies de cache suivantes sont automatiquement liées au point de liaison HTTP/3 par défaut.

```
> sho cache global -type HTTPQUIC_REQ_DEFAULT
1)      Policy Name: NOPOLICY
        Priority: 185883
        GotoPriorityExpression: USE_INVOCATION_RESULT
```



```
5          Invoke type: policylabel        Invoke name:
               _httpquicReqBuiltinDefaults
6          Global bindpoint: HTTPQUIC_REQ_DEFAULT
7
8   Done
9   > sho cache global -type HTTPQUIC_RES_DEFAULT
10  1)      Policy Name: NOPOLICY
11         Priority: 185883
12         GotoPriorityExpression: USE_INVOCATION_RESULT
13         Invoke type: policylabel        Invoke name:
               _httpquicResBuiltinDefaults
14         Global bindpoint: HTTPQUIC_RES_DEFAULT
15
16  <!--NeedCopy-->
```

Après une mise à niveau, si les stratégies ne sont pas liées, vous pouvez utiliser les commandes suivantes pour lier et enregistrer manuellement la configuration.

```
1  add cache policylabel _httpquicReqBuiltinDefaults -evaluates
       HTTPQUIC_REQ
2
3  add cache policylabel _httpquicResBuiltinDefaults -evaluates
       HTTPQUIC_RES
4
5  bind cache policylabel _httpquicReqBuiltinDefaults -policyName
       _nonGetReq -priority 100
6
7  bind cache policylabel _httpquicReqBuiltinDefaults -policyName
       _advancedConditionalReq -priority 200
8
9  bind cache policylabel _httpquicReqBuiltinDefaults -policyName
       _personalizedReq -priority 300
10
11 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _uncacheableStatusRes -priority 100
12
13 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _uncacheableVaryRes -priority 200
14
15 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _uncacheableCacheControlRes -priority 300
16
17 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _cacheableCacheControlRes -priority 400
18
```



```
19 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _uncacheablePragmaRes -priority 500
20
21 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _cacheableExpiryRes -priority 600
22
23 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _imageRes -priority 700
24
25 bind cache policylabel _httpquicResBuiltinDefaults -policyName
       _personalizedRes -priority 800
26
27 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
       USE_INVOCATION_RESULT -type HTTPQUIC_REQ_DEFAULT -invoke policylabel
        _httpquicReqBuiltinDefaults
28
29 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
       USE_INVOCATION_RESULT -type HTTPQUIC_RES_DEFAULT -invoke policylabel
        _httpquicResBuiltinDefaults
30
31 <!--NeedCopy-->
```

> **Remarque :**
>
> Les deux premières commandes de la liste des commandes, et les deux dernières commandes d'une même liste, sont incluses dans un souci d'exhaustivité. Vous pouvez rencontrer une erreur lors de l'exécution des quatre commandes, car elles sont déjà exécutées au moment du redémarrage de l'appliance. Mais vous pouvez ignorer ces erreurs.

Configuration de la stratégie de transformation d'URL pour le trafic HTTP/3

La transformation d'URL modifie toutes les URL des requêtes désignées depuis une version externe vue par des utilisateurs externes vers une URL interne vue uniquement par vos serveurs Web et vos administrateurs. Vous pouvez rediriger les demandes des utilisateurs de manière transparente, sans exposer la structure de votre réseau aux utilisateurs. Vous pouvez également modifier des URL internes complexes que les utilisateurs peuvent avoir de la difficulté à mémoriser en URL externes plus simples et plus facilement mémorisées.

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de cache. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.

Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés.

Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter un profil de transformation d'URL

Pour ajouter un profil de transformation d'URL, à l'invite de commandes, tapez :

```
1 add transform profile <name> [-type URL]
2 <!--NeedCopy-->
```

Exemple :

```
add transform profile msapps
```

Action Ajouter une transformation d'URL

Pour ajouter une action de transformation d'URL, à l'invite de commandes, tapez :

```
1 add transform action <name> <profileName> <priority> [-state ( ENABLED
      | DISABLED )]
2 <!--NeedCopy-->
```

Exemple :

```
add transform action docx2doc msapps 2
```

Action Ajouter une transformation d'URL

Pour ajouter une action de transformation d'URL afin de remplacer l'URL, à l'invite de commandes, tapez :

```
1 add transform action <name> <profileName> <priority> [-state ( ENABLED
      | DISABLED )]
2 <!--NeedCopy-->
```

Exemple :

```
add transform action docx2doc msapps 1
```

Stratégie Ajouter une transformation d'URL

Pour ajouter une stratégie de transformation d'URL, à l'invite de commandes, tapez :


```
add transform policy <name> <rule> <profileName> [-comment <string>]
    [-logAction <string>]
<!--NeedCopy-->
```

Exemple :

```
add transform policy urltrans_udp "CLIENT.UDP.DSTPORT.EQ(443)"msapps
```

Stratégie de transformation d'URL Lier avec un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier une stratégie de transformation d'URL à un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC, à l'invite de commandes, tapez :

```
bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
    ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
    positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
     REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
    -analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vs lb-http3 -policyName urltrans_udp -type REQUEST -priority 8
```

Lier une stratégie globale de transformation d'URL avec un serveur virtuel d'équilibrage de charge basé sur HTTP/3 QUIC

Pour lier un point de liaison global HTTP/3 de stratégie de transformation d'URL, à l'invite de commandes, tapez :

```
bind transform global <policyName> <priority>  [<gotoPriorityExpression
    >] [-type <type>] [-invoke (<labelType>  <labelName>) ]
<!--NeedCopy-->
```

Exemple :

```
bind transform global urltrans_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

Pour plus d'informations, voir Configuration de la stratégie de transformation d'URL.

Configuration de la stratégie d'optimisation frontale (FEO) pour le trafic HTTP/3

Les protocoles HTTP qui sous-tendent les applications Web ont été développés à l'origine pour prendre en charge la transmission et le rendu de pages Web simples. Les nouvelles technologies telles que

JavaScript et les feuilles de style en cascade (CSS), ainsi que les nouveaux types de médias tels que les vidéos Flash et les images riches en graphiques, imposent de lourdes exigences sur les performances front-end, c'est-à-dire sur les performances au niveau du navigateur. La fonctionnalité d'optimisation du front end (FEO) de NetScaler résout ces problèmes et réduit le temps de chargement et le temps de rendu des pages Web.

> **Remarque :**
>
> `HTTP_QUIC _Override/Default_Request` Le type n'est pas pris en charge pour la liaison globale de la stratégie FEO.

Ajouter une action d'optimisation frontale (FEO)

Pour ajouter une action FEO, à l'invite de commandes, tapez :

```
1 add feo action <name> [-pageExtendCache] [<cacheMaxage>][-
      imgShrinkToAttrib] [-imgGifToPng] [-imgToWebp] [-imgToJpegXR] [-
      imgInline] [-cssImgInline] [-jpgOptimize] [-imgLazyLoad] [-cssMinify
      ] [-cssInline] [-cssCombine] [-convertImportToLink] [-jsMinify] [-
      jsInline] [-htmlMinify] [-cssMoveToHead] [-jsMoveToEND][-
      domainSharding <string> <dnsShards> ...] [-clientSideMeasurements]
2
3 <!--NeedCopy-->
```

Exemple :

```
add feo action feoact -imgGifToPng -pageExtendCache
```

Ajouter une stratégie d'optimisation frontale (FEO)

Pour ajouter une stratégie FEO, à l'invite de commandes, tapez :

```
add feo policy <name> <rule> <action>
```

Exemple :

```
add feo policy udp_feo_img "CLIENT.UDP.DSTPORT.EQ(443)"IMG_OPTIMIZE
```

Lier la stratégie FEO au serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC

Pour lier une stratégie FEO à un serveur virtuel d'équilibrage de charge de type HTTP/3_QUIC, à l'invite de commandes, tapez :


```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Exemple :

```
bind lb vserver lb-http3 -policyName udp_feo_img -priority 4 -gotoPriorityExpression
 END -type REQUEST
```

Lier la stratégie FEO au point de liaison global HTTP/3

Pour lier une stratégie de cache au point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
bind cache global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Exemple :

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Pour plus d'informations, reportez-vous à la section Configuration de la stratégie d'optimisation frontale.

Configuration de la stratégie SSL pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies SSL. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.
Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.
Les stratégies SSL avec des actions prises en charge par TLSv1.3 ne s'appliquent qu'aux points de liaison HTTP/3 ou aux serveurs virtuels.

Ajouter une stratégie SSL

Pour ajouter une stratégie FEO, à l'invite de commandes, tapez :


```
add ssl policy <name> -rule <expression> [-action <string>] [-
    undefAction <string>] [-comment <string>]
<!--NeedCopy-->
```

Exemple :

```
add ssl policy ssl-pol -rule CLIENT.SSL.IS_SSL -action NOOP
```

Lier la stratégie SSL au serveur virtuel HTTP/3

Pour lier une stratégie SSL au serveur virtuel HTTP/3, à l'invite de commandes :

```
bind ssl policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver lb-http3 -policyName ssl-pol -priority 4 -type REQUEST
```

Ajouter une stratégie SSL avec expression UDP pour la stratégie SSL

Pour ajouter une stratégie SSL avec une expression UDP, à l'invite de commandes :

```
add ssl policy <name> -rule <expression> [-action <string>] [-
    undefAction <string>] [-comment <string>]
<!--NeedCopy-->
```

Exemple :

```
add ssl policy ssl_udp_clnt -rule "CLIENT.UDP.DSTPORT.EQ(443)"-action NOOP
```

Lier une stratégie SSL avec une expression UDP au serveur virtuel HTTP/3

Pour lier une stratégie SSL avec une expression UDP au serveur virtuel HTTP/3, à l'invite de commandes, tapez

```
bind ssl policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
<!--NeedCopy-->
```

Exemple :

```
bind ssl vs lb-http3 -policyName ssl_udp_clnt -priority 8 -type REQUEST
```


Ajouter une stratégie SSL pour le point de liaison CLIENTHELLO pour le trafic HTTP/3

Pour lier une stratégie SSL pour le point de liaison CLIENTHELLO pour le trafic HTTP/3, à l'invite de commandes, tapez :

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Exemple :

```
add ssl policy ssl-pol-ch -rule "CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
(0x1301)"-action RESET
```

Lier la stratégie SSL au point de liaison CLIENTHELLO

Pour lier une stratégie SSL au point de liaison CLIENTHELLO, à l'invite de commandes, tapez :

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Exemple :

```
bind ssl vs lb-http3 -policyName ssl-pol-ch -type CLIENTHELLO_REQ -priority
 100
```

Lier la stratégie SSL au point de liaison global HTTP/3

Pour lier une stratégie SSL au point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
bind cache global <policy> -priority <positive_integer> [-gotoPriorityExpression
 <expression>] [-type <type>] [-invoke (<labelType> <labelName>)]
```

Exemple :

Voici un exemple de stratégie DATA liée à un point de liaison global HTTP/3 :

```
Bind ssl global -policyName ssl-pol-ch -priority 7 -type HTTPQUIC_DATA_DEFAULT
```

> **Remarque :**
>
> L'action de transfert pouvant être définie pour le point de liaison CLIENTHELLO pour les serveurs virtuels SSL n'est actuellement pas prise en charge pour les serveurs virtuels de type HTTP_QUIC.

Configuration de la stratégie de pare-feu d'application pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies de pare-feu d'application Web. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.
Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter une stratégie de pare-feu d'application Web avec une expression UDP

Pour ajouter une stratégie de pare-feu d'application Web avec une expression UDP, à l'invite de commandes :

```
1 add appfw policy <name> <rule> <profileName> [-comment <string>] [-
     logAction <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add appfw policy appfw_udp "CLIENT.UDP.DSTPORT.EQ(443)"APPFW_BYPASS
```

Lier des expressions de journal avec une expression basée sur UDP pour le profil Web Application Firewall

Pour lier des expressions de journal au profil UDP for Web Application Firewall, à l'invite de commandes :

Exemple :

```
bind appfw profile APPFW_BLOCK -logExpression logexp-1 "CLIENT.UDP.DSTPORT.
EQ(443)"
```

Lier une stratégie de pare-feu d'application avec le serveur virtuel HTTP/3

Pour lier la stratégie de pare-feu d'application Web au serveur virtuel HTTP/3, à l'invite de commandes :

```
1 bind appfw policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Exemple :


```
bind lb vs lb-http3 -policyName appfw_udp -priority 3 -type REQUEST
```

Lier une stratégie de pare-feu d'application Web au point de liaison global HTTP/3

Pour lier une stratégie de pare-feu d'application Web au point de liaison global HTTP/3, à l'invite de commandes, tapez :

```
1 bind appfw global <policy> -priority <positive_integer>  [-
     gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
     labelType> <labelName>) ]
2 <!--NeedCopy-->
```

Exemple :

```
bind appfw global appfw_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

Configuration de la stratégie AppQoE pour le trafic HTTP/3

Les serveurs virtuels HTTP sur QUIC sont pris en charge par les stratégies AppQoE. Cependant, comme QUIC utilise UDP comme mécanisme de transport, les expressions basées sur TCP sont exclues et les expressions basées sur UDP sont incluses.
Les configurations de stratégie nouvelles ou existantes avec des expressions TCP ne peuvent pas être liées à des serveurs virtuels HTTP/3 ou aux points de liaison globaux HTTP/3 nouvellement ajoutés. Au lieu des expressions TCP, les expressions UDP peuvent être incluses dans les configurations de stratégie liées à des serveurs virtuels QUIC HTTP/3 ou HTTP sur des points de liaison QUIC.

Ajouter une stratégie AppQoE avec une expression basée sur UDP

Pour ajouter une stratégie AppQOE avec une expression UDP, à l'invite de commandes :

```
1 add AppQoE policy <name> <rule> <profileName> [-comment <string>] [-
     logAction <string>]
2 <!--NeedCopy-->
```

Exemple :

```
add appqoe policy appqoe-pol-udp -rule "CLIENT.UDP.DSTPORT.EQ(443)"-action
appqoe-act-basic-prhigh
```

Lier une stratégie AppQoE au serveur virtuel HTTP/3

Pour lier la stratégie AppQoE au serveur virtuel HTTP/3, à l'invite de commandes, tapez :


```
bind appqoe policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
<!--NeedCopy-->
```

Exemple :

```
bind lb vs lb-http3 -policyName appqoe-pol-udp -type REQUEST -priority 3
```

Lier la stratégie AppQoE au serveur virtuel HTTP_QUIC

Pour lier la stratégie AppQoE au serveur `HTTP_QUIC` virtuel, à l'invite de commandes, tapez :

```
bind appqoe <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Exemple :

```
bind lb vs lb-http3 -policyName appqoe-pol-primd -priority 8 -type REQUEST
```

Découverte du service HTTP/3

May 5, 2023

Le protocole HTTP repose sur l'utilisation de HTTP Alternative Services pour le serveur d'origine pour annoncer la disponibilité d'un service équivalent. La découverte de service HTTP/3 utilise également le même principe. Un point de terminaison HTTP/3 alternatif peut être annoncé à l'aide de l'une des méthodes suivantes :

- En-tête de réponse HTTP Alt-Svc
- Cadre HTTP/2 Alt-Svc dans la réponse
- Négociation du protocole de couche d'application (ALPN)

Le service alternatif annonce l'utilisation d'un en-tête de réponse HTTP Alt-Svc et de la trame HTTP/2 Alt-Svc comme point de terminaison HTTP/3. Les serveurs peuvent utiliser HTTP/3 sur n'importe quel port UDP. Une autre publicité de service inclut un port explicite, et les URL contiennent soit un port explicite, soit un port par défaut associé au schéma.

Les clients recevant d'autres en-têtes ou trames de service ne sont pas tenus de les utiliser. Le client, s'il est informé d'un autre service et s'il appuie le mécanisme de service alternatif, doit utiliser le service alternatif approprié annoncé. En d'autres termes, un service HTTP/1.1 ou un service HTTP/2 peut

annoncer un point de terminaison équivalent prenant en charge le protocole HTTP/3. Lors de la réception de ces informations de service de rechange, le client peut choisir d'établir une connexion QUIC avec le service alternatif spécifié et, une fois disponible, cette connexion peut être utilisée pour toutes les demandes ultérieures. Si l'établissement de la connexion avec le service alternatif sélectionné échoue, le client peut revenir au point de terminaison d'origine. Lorsque le client commence à utiliser le service alternatif annoncé, l'indique en incluant un en-tête Alt-Used.

NetScaler prend en charge les points de terminaison HTTP/3 équivalents à la publicité sur des serveurs virtuels de type HTTP et SSL.

Configurer la découverte du service HTTP/3

Procédez comme suit pour configurer la découverte du service HTTP/3 :

1. Configurer le point de terminaison de service alternatif HTTP/3 à l'aide d'un en-tête HTTP Alt-Svc
2. Configurez le point de terminaison de service alternatif HTTP/3 à l'aide d'une trame HTTP/2 Alt-Svc
   Configurez le point de terminaison de service alternatif HTTP/3 à l'aide d'un en-tête HTTP Alt-Svc
   Pour annoncer un point de terminaison HTTP/3 à l'aide d'un en-tête HTTP Alt-Svc, tapez la commande suivante :

Remarque : L'objectif principal de la publicité d'un service alternatif est de faire savoir à l'utilisateur que la capacité HTTP/3 est également accessible sur le service HTTP/1.1 ou HTTP/2 sur a.b.c.d:443.

```
add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ]
<!--NeedCopy-->
```

Exemple :

```
add ns httpProfile http-profile -altsvc ENABLED -altSvcValue  "h3-29="
    :443"; ma=3600; persist=1"
<!--NeedCopy-->
```

ou

```
set ns httpProfile http-custom -altsvc ENABLED -altSvcValue  "h3-29="
    :443"; ma=3600; persist=1"
<!--NeedCopy-->
```


Configurer un point de terminaison de service alternatif HTTP/3 à l'aide d'une trame HTTP/2 Alt-Svc

Pour annoncer un point de terminaison HTTP/3 à l'aide d'une trame HTTP/2 Alt-SVC, tapez la commande suivante :

```
add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ] -
    http2AltSvcFrame [ ENABLED | DISABLED ]
<!--NeedCopy-->
```

Exemple :

```
add ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue "h3-29=\":443\"; ma=3600; persist=1"
```

ou

```
set ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue "h3-29=\":443\"; ma=3600; persist=1"
```

Configurer le service alternatif HTTP/3 avec la valeur d'en-tête HTTP Alt-Svc à l'aide de l'interface graphique

1. Accédez à **Système > Profils > Profils HTTP**.
2. Cliquez sur **Ajouter**.
3. Dans la page **Créer un profil HTTP**, accédez à la section HTTP/3 et cochez la case **Autre service** .
4. Le système affiche la zone de texte **Valeur de service alternative** dans la section http2.
5. Entrez la valeur de service alternative comme « h3-29= » :443 "; ma=3600 ; persist=1 »
6. Cliquez sur **OK** et sur **Fermer**.

gRPC

May 5, 2023

Le gRPC intégré à une appliance NetScaler est un framework d'appel de procédure à distance (RPC) universel léger, performant et open source. Le framework est optimal pour fonctionner dans plusieurs langues s'exécutant sur n'importe quel système d'exploitation. Par rapport aux autres protocoles, gRPC offre également de meilleures performances et une meilleure sécurité.

gRPC pour NetScaler est préférable pour les raisons suivantes :

- Créez des applications distribuées pour les centres de données et les infrastructures de cloud public/privé.
- Fournissez une communication client-serveur pour les appareils mobiles, le Web ou le cloud.
- Accédez aux services et applications cloud
- Déploiements de microservices

Pourquoi choisir gRPC dans NetScaler

Le gRPC de NetScaler est implémenté via HTTP/2 pour prendre en charge des API évolutives et hautement performantes. L'utilisation du binaire plutôt que du texte permet à la charge utile de rester compacte et efficace. Dans NetScaler, les requêtes HTTP/2 sont multiplexées sur une seule connexion TCP, ce qui permet à plusieurs messages simultanés d'être transmis sans compromettre l'utilisation des ressources réseau. Il utilise également la compression des en-têtes pour réduire la taille des demandes et des réponses.

gRPC prend en charge les types de méthodes de service suivants permettant à un client d'invoquer à distance des paramètres et des types de retour.

1. **RPC unaire.** Le client envoie une seule demande au serveur gRPC et reçoit une réponse unique en retour.

   Exemple :
   ```
   rpc SayHello(HelloRequest)returns (HelloResponse);
   ```

2. **Serveur de streaming RPC.** Le client envoie une seule requête au serveur gRPC et obtient une réponse de flux.

   Exemple :
   ```
   rpc StreamingResponse(HelloRequest)returns (HelloResponse);
   ```

3. **Client de streaming RPC.** Le client envoie une séquence de messages et attend que le serveur lise et renvoie sa réponse.

   Exemple :
   ```
   rpc IntroduceYourself(stream HelloRequest)returns (HelloResponse)
   ```


4. **Streaming bidirectionnel RPC.** Le client et le serveur envoient des deux côtés un flux de messages à l'aide du flux de lecture-écriture. Les deux flux fonctionnent indépendamment.

   Exemple :

   ```
   rpc ChatSession (stream HelloRequest)returns (stream HelloResponse)
   ```

NetScaler prend en charge les fonctionnalités suivantes pour ses services avec les points de terminaison gRPC :

- Équilibrage de charge
- Commutation de contenu
- Services de point de terminaison sécurisés tels que le pare-feu d'applications Web et l'authentification.
- Configuration de la stratégie
- Statistiques et journalisation
- Réécriture du contenu, filtrage du contenu
- Optimisations des couches 4 et 7, offre TLS
- Solutions de passerelle pour les traductions de protocoles

Configuration de bout en bout de gRPC

May 5, 2023

La configuration de bout en bout de gRPC fonctionne en envoyant une requête gRPC depuis un client via le protocole HTTP/2 et en transférant à nouveau les messages gRPC auxquels le serveur gRPC a répondu.

Comment fonctionne la configuration gRPC de bout en bout

Le schéma suivant montre qu'une configuration gRPC fonctionne dans une appliance NetScaler.

1. Pour déployer la configuration gRPC, vous devez d'abord activer HTTP/2 dans le profil HTTP et également activer le support HTTP/2 globalement côté serveur.
2. Lorsqu'un client envoie une demande gRPC, le serveur virtuel d'équilibrage de charge évalue le trafic gRPC à l'aide de politiques.
3. Sur la base de l'évaluation des politiques, le serveur virtuel d'équilibrage de charge (auquel est lié le service gRPC) met fin à la demande et la transmet sous forme de demande gRPC au serveur gRPC principal.
4. De même, lorsque le serveur gRPC répond au client, l'appliance met fin à la réponse et la transmet en tant que réponse gRPC au client.

Exemple de requête gRPC envoyée au serveur gRPC

L'en-tête de requête est envoyé en tant qu'en-têtes HTTP/2 dans HEADERS+CONTINUATION Frames.

```
```
HEADERS (flags = END_HEADERS)
: method = POST
: scheme = http
: path = /helloworld.citrix-adc/SayHello
: authority = 10.10.10.10.:80
grpc-timeout = 15
content-type = application/grpc+proto
grpc-encoding = gzip
DATA (flags = END_STREAM)
<Length-Prefixed Message>
<!--NeedCopy--> ```
```

### Exemple d'en-tête de réponse gRPC du serveur gRPC vers l'appliance NetScaler

Les en-têtes de réponse et les bandes-annonces uniquement sont fournis dans un seul bloc de trame HTTP/2 HEADERS. La plupart des réponses devraient contenir à la fois des en-têtes et des bandes-annonces, mais Trailers-Only est autorisé pour les appels qui génèrent une erreur immédiate. Le statut doit être envoyé dans Trailers même si le code d'état HTTP est OK.

```
```
HEADERS (flags = END_HEADERS)
: status = 200
Grpc-encoding= gzip
Content-type = application/grpc+proto
DATA
<Length-Prefixed Message>
HEADERS (flags = END_STREAM, END_HEADERS)
```



```
grpc-status = 0 # OK

<!--NeedCopy--> ```
```

Configurer GRPC à l'aide de l'interface de ligne de commande

Pour configurer un déploiement gRPC de bout en bout, vous devez effectuer les opérations suivantes :

- Ajoutez un profil HTTP avec HTTP/2 et HTTP/2 direct activés.
- Activer la prise en charge globale du backend HTTP/2 dans le paramètre HTTP
- Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP
- Ajouter un service pour le point de terminaison gRPC et définir le profil HTTP
- Lier le service de point de terminaison gRPC au serveur virtuel d'équilibrage de charge

Ajouter un profil HTTP avec HTTP/2 et HTTP/2 direct activés

Vous devez activer les paramètres directs HTTP/2 et HTTP/2 dans le profil HTTP. Vous devez également activer le paramètre direct HTTP/2 si du texte clair gRPC sur HTTP/2 est requis.

À l'invite de commande, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Exemple :

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Activer le support HTTP/2 du back-end global via le paramètre HTTP

Pour activer le support HTTP/2 globalement côté serveur à l'aide de la ligne de commande NetScaler.

À l'invite de commande, tapez :

```
set ns httpParam -http2ServerSide( ON | OFF )
```

Exemple :

```
set ns httpParam -http2ServerSide ON
```

Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP

Pour ajouter un serveur virtuel d'équilibrage de charge à l'aide de l'interface de commande **NetScaler** :

À l'invite de commande, tapez :


```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Exemple :

```
add lb vserver lb-grpc HTTP 10.10.10.11 80 -httpProfileName http2gRPC
```

> **Remarque :**
>
> Si vous utilisez un serveur virtuel d'équilibrage de charge de type SSL, vous devez lier le certificat du serveur. Pour plus d'informations, reportez-vous à la rubrique relative au certificat de serveur Bind

Ajouter un service pour le point de terminaison gRPC et définir le profil HTTP

Pour ajouter un service gRPC avec un profil HTTP à l'aide de l'interface de commande **NetScaler** :
À l'invite de commande, tapez :

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Exemple :

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```

Lier le service de point de terminaison gRPC au serveur virtuel d'équilibrage de charge

Pour lier un service gRPC à un serveur virtuel d'équilibrage de charge à l'aide de l'interface de commande **NetScaler** :

Dans l'interface de commande, tapez :

```
bind lb vserver <name> <serviceName>
```

Exemple :

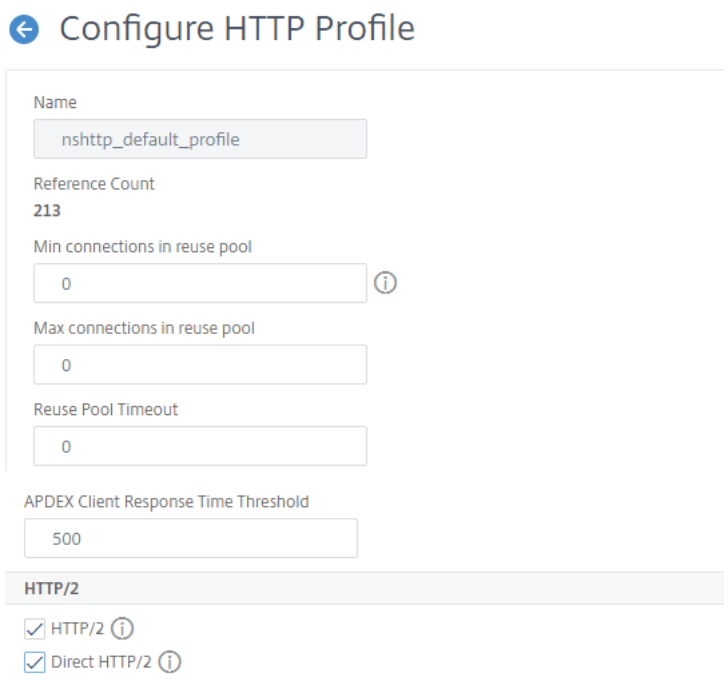
```
bind lb vserver lb-grpc svc-grpc
```

Configurer le déploiement de gRPC de bout en bout à l'aide de l'interface graphique

Effectuez les étapes suivantes pour configurer gRPC à l'aide de l'interface graphique.

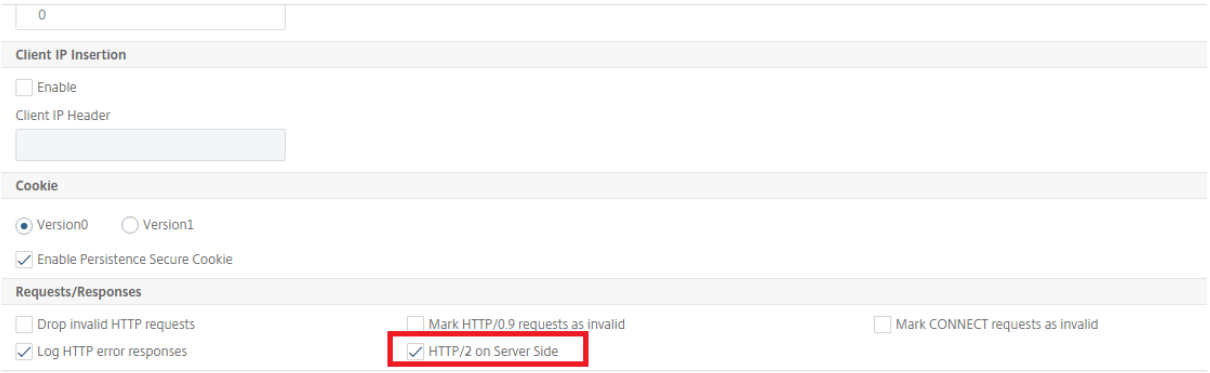
Ajouter un profil HTTP avec HTTP/2 et HTTP/2 direct activés

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.
2. Activer l'option HTTP/2 dans un nouveau profil HTTP ou un profil HTTP existant



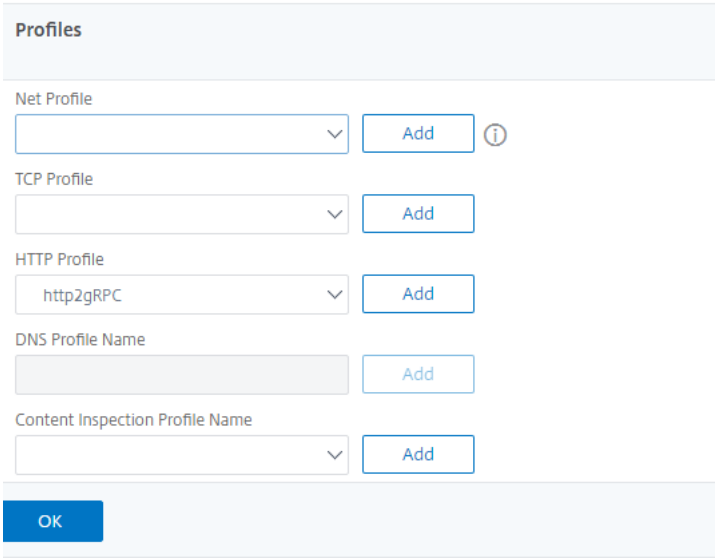
Activer la prise en charge globale du backend HTTP/2 dans le paramètre HTTP

1. Accédez à **Système > Paramètres > Paramètres HTTP**.
2. Sur la page Configurer le paramètre HTTP, sélectionnez HTTP/2 côté serveur.
3. Cliquez sur **OK**.



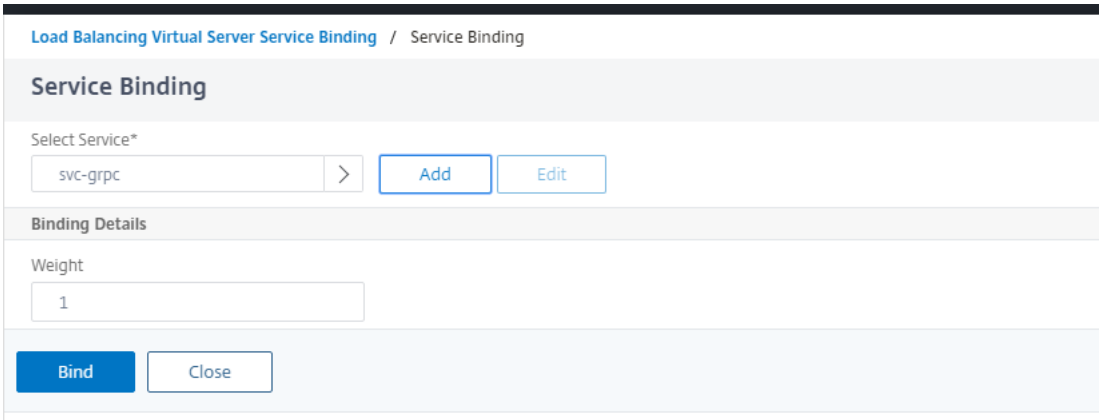
Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur Ajouter pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Dans la page Serveur virtuel d'équilibrage de charge, cliquez sur Profils.
4. Dans la section Profils, sélectionnez le type de profil HTTP.
5. Cliquez sur OK, puis sur Terminé.



Ajouter un service pour le point de terminaison gRPC et définir le profil HTTP

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Cliquez sur Ajouter pour créer un serveur d'applications pour le trafic gRPC.
3. Sur la page du service d'équilibrage de charge, accédez à la section Profil.
4. Sous Profils, ajoutez un profil HTTP pour le point de terminaison gRPC.
5. Cliquez sur OK, puis sur Terminé.



Pour obtenir des procédures détaillées sur l'interface graphique liée à l'équilibrage de chargement, consultez la rubrique Équilibrage de charge .

Pontage gRPC

May 5, 2023

Lorsqu'un client envoie une demande via le protocole HTTP/1.1, l'appliance NetScaler prend en charge le pontage des demandes gRPC via le protocole HTTP/1.1, conformément au protocole du serveur gRPC via HTTP/2. De même, dans le cadre du pontage inversé, l'appliance reçoit la demande gRPC du client via le protocole HTTP/2 et effectue un pontage inverse pour les demandes gRPC conformément au serveur gRPC du protocole HTTP/1.1.

Comment fonctionne le pontage gRPC

Dans ce scénario, l'appliance NetScaler relie de manière fluide le contenu gRPC reçu sur une connexion HTTP/1.1 et le transmet au serveur gRPC principal via HTTP/2.

Le schéma suivant montre comment les composants interagissent les uns avec les autres dans une configuration de pont gRPC.

1. Lorsqu'une requête gRPC est envoyée, l'appliance NetScaler vérifie si la connexion est HTTP/1.1 et si le type de contenu est application/grpc. Les requêtes HTTP/1.1 se traduisent par les pseudo-en-têtes suivants.
2. Lors de la réception d'une demande gRPC sur une connexion HTTP/1.1, comme indiqué par l'en-tête Content-Type, l'appliance ADC transforme la demande en gRPC via HTTP/2 comme indiqué ci-dessous :

```
1     :method: Method-name in HTTP/1.1 request
2     :path: Path is HTTP/1.1 request
3     content-type: application/grpc
4 <!--NeedCopy-->
```

1. Sur la base de l'évaluation des politiques, le serveur virtuel d'équilibrage de charge (auquel le service gRPC est lié) met fin à la demande ou la transmet via des trames HTTP/2 au serveur gRPC principal.
2. Lors de la réception de la réponse sur une connexion HTTP/2 depuis le serveur gRPC, l'appliance met en mémoire tampon jusqu'à ce qu'elle reçoive la bande-annonce HTTP/2, puis vérifie le code d'état gRPC. Si l'état d'erreur gRPC est différent de zéro, l'appliance recherche le code d'état HTTP mappé et envoie une réponse d'erreur HTTP/1.1 appropriée.

Configurer le pontage gRPC à l'aide de l'interface de ligne de commande

Pour configurer le pontage gRPC, vous devez suivre les étapes suivantes :

1. Ajouter un profil HTTP avec HTTP/2 et HTTP/2 direct activés
2. Activer le support HTTP/2 du back-end global dans le paramètre HTTP
3. Ajoutez un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définissez le profil HTTP
4. Ajouter un service pour le point de terminaison GRPC et définir le profil HTTP
5. Lier le service de point de terminaison gRPC au serveur virtuel d'équilibrage de charge
6. Mappez le code d'état gRPC à la réponse HTTP pour un état gRPC différent de zéro
7. Configurer la mise en mémoire tampon de gRPC en fonction de l'heure et/ou de la taille

Ajoutez un profil HTTP avec les connexions directes HTTP/2 et HTTP/2 activées

Pour commencer la configuration, vous devez activer la fonctionnalité HTTP/2 dans le profil HTTP. Si le client envoie les requêtes HTTP 1.1, l'appliance relie la demande et la transmet au serveur principal.

À l'invite de commande, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Exemple :

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Activer la prise en charge globale du backend HTTP/2 dans le paramètre HTTP

Pour activer le support HTTP/2 globalement côté serveur à l'aide de la ligne de commande NetScaler.

À l'invite de commande, tapez :

```
set ns httpParam -http2ServerSide( ON | OFF )
```

Exemple :

```
set ns httpParam -http2ServerSide ON
```

Ajoutez un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définissez le profil HTTP

Pour ajouter un serveur virtuel d'équilibrage de charge à l'aide de l'interface de **commande NetScaler**

À l'invite de commande, tapez :

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```


Exemple :

```
add lb vserver lb-grpc HTTP 10.10.10.10 80 -httpProfileName http2gRPC
```

> **Remarque :**
>
> Si vous utilisez un serveur virtuel d'équilibrage de charge de type SSL, vous devez lier le certificat du serveur. Pour plus d'informations, reportez-vous à la rubrique relative au certificat de serveur Bind

Ajouter un service pour le point de terminaison GRPC et définir le profil HTTP

Pour ajouter un service gRPC avec le profil HTTP à l'aide de l'interface de commande **NetScaler.**

À l'invite de commande, tapez :

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Exemple :

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```

Lier le service de point de terminaison gRPC au serveur virtuel d'équilibrage de charge

Pour lier un service de point de terminaison gRPC au serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande.

Dans l'interface de commande, tapez :

```
bind lb vserver <name> <serviceName>
```

Exemple :

```
bind lb vserver lb-grpc svc-grpc
```

Mappez le code d'état gRPC au code d'état HTTP dans la réponse HTTP/1.1

Dans le scénario de pontage gRPC, le service gRPC répond à la demande par un code d'état gRPC. L'appliance mappe le code d'état gRPC à un code de réponse HTTP et à une phrase de motivation correspondants. Le mappage est effectué sur la base du tableau ci-dessous. Lors de l'envoi de la réponse HTTP/1.1 au client, l'appliance NetScaler envoie le code d'état HTTP et la phrase de motivation.

Code d'état gRPC	Code d'état de la réponse HTTP	Motif de la réponse HTTP
D'ACCORD = 0	200	OK.

Code d'état gRPC	Code d'état de la réponse HTTP	Motif de la réponse HTTP
ANNULÉ = 1	499	*
INCONNU = 2	500	Erreur interne du serveur
ARGUMENT_INVALIDE = 3	400	Demande incorrecte
DATE_DÉPASSÉE = 4	504	Délai d'expiration de la passerelle
INTROUVABLE = 5	404	*
EXISTE_DEJA = 6	409	Conflit
AUTORISATION_REFUSÉE = 7	403	Liste noire
NON AUTHENTIFIÉ = 16	401	Non autorisé
RESOURCE_EXHAUSTED = 8	429	*
PRÉCONDITION ÉCHOUÉE = 9	400	Demande incorrecte
ABANDONNÉ = 10	409	Conflit
HORS DE PORTÉE = 11	400	Demande incorrecte
NON IMPLÉMENTÉ = 12	501	Non implémenté
INTERNE = 13	500	Erreur interne du serveur
INDISPONIBLE = 14	503	Service non disponible
PERTE DE DONNÉES = 15	500	Erreur interne du serveur

Configurer la mise en mémoire tampon de gRPC en fonction de l'heure et/ou de la taille

L'appliance NetScaler met en mémoire tampon la réponse gRPC depuis le serveur principal jusqu'à ce que la bande-annonce de réponse soit reçue. Cela interrompt les appels gRPC bidirectionnels. De plus, si la réponse gRPC est énorme, elle consomme une quantité importante de mémoire pour la mettre complètement en mémoire tampon. Pour résoudre le problème, la configuration du pontage gRPC est améliorée afin de limiter la mise en mémoire tampon en fonction du temps et/ou de la taille. Si la taille de la mémoire tampon ou la limite de temps dépasse le seuil, l'appliance arrête la mise en mémoire tampon et transmet la réponse au client même lorsque l'une des limitations se déclenche (soit la bande-annonce n'est pas reçue dans la taille de mémoire tampon configurée, soit si le délai d'expiration configuré se produit). Par conséquent, les politiques configurées et leurs expressions (basées sur le code grpc-status) ne fonctionnent pas comme prévu.

Pour limiter la mise en mémoire tampon de gRPC en fonction du temps et/ou de la taille par la CLI, vous pouvez le configurer lorsque vous ajoutez un nouveau profil HTTP ou le configurer lorsque vous

modifiez un profil existant.

À l'invite de commande, tapez :

```
add ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

Ou

```
set ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

Où,

`grpcholdlimit`. Taille maximale en octets autorisée pour la mise en mémoire tampon des paquets gRPC jusqu'à la réception de la bande-annonce. Vous pouvez configurer à la fois les paramètres et n'importe lequel d'entre eux.

Valeur par défaut : 131072 Valeur
minimale : 0 Valeur
maximale : 33554432

`grpcholdtimeout`. Durée maximale en millisecondes autorisée pour mettre en mémoire tampon les paquets gRPC jusqu'à la réception de la bande-annonce. La valeur doit être exprimée en multiples de 100.
Valeur par défaut : 1000 Valeur
minimale : 0 Valeur
maximale : 180000

Exemple :

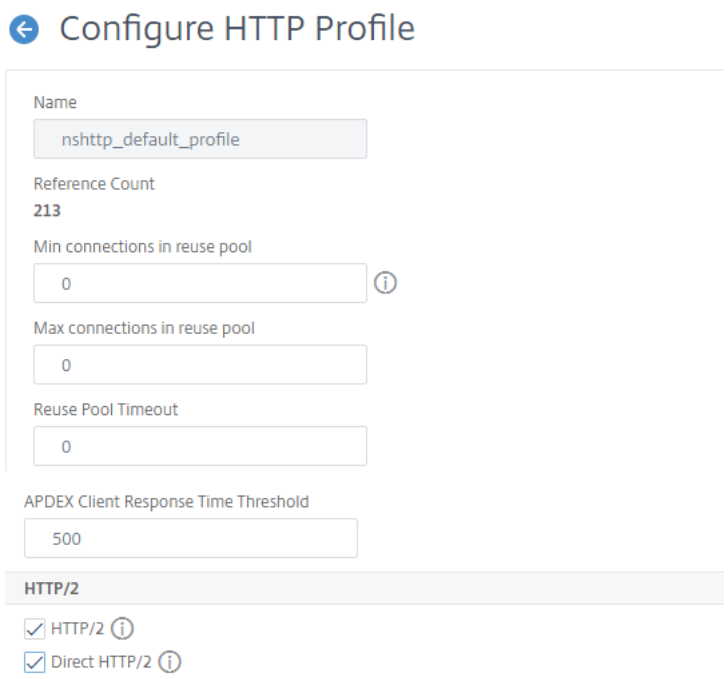
```
add httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
set httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
```

Configurer le pontage gRPC à l'aide de l'interface graphique

Effectuez les étapes suivantes pour configurer le pontage gRPC à l'aide de l'interface graphique NetScaler.

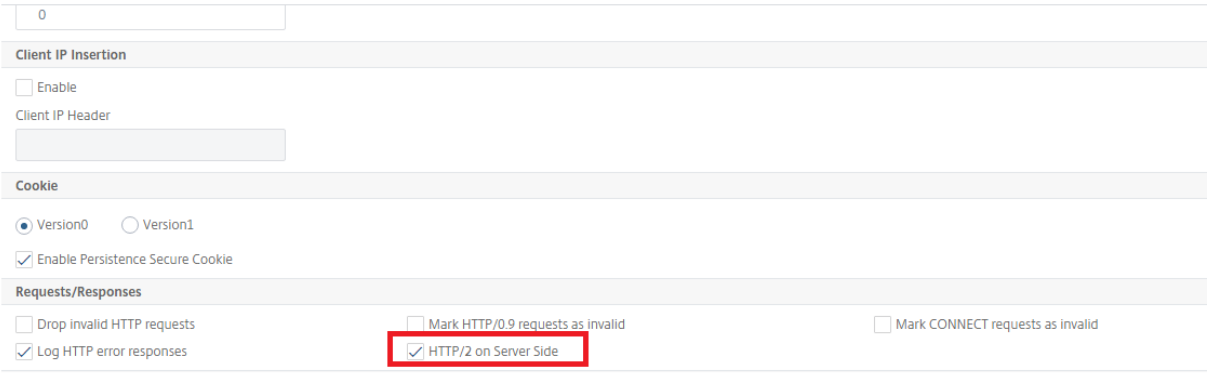
Ajouter un profil HTTP avec HTTP/2 et HTTP/2 direct activés

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.
2. Sélectionnez **HTTP/2** dans le profil HTTP.



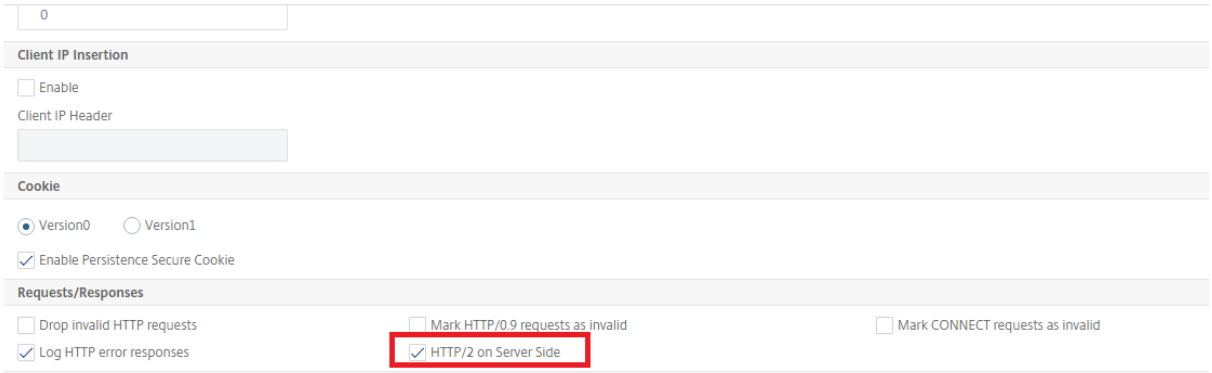
Activer le support HTTP/2 du back-end global dans le paramètre HTTP

1. Accédez à **Système > Paramètres > Paramètres HTTP**.
2. Sur la page **Configurer le paramètre HTTP**, sélectionnez l'option **HTTP/2 côté serveur** .
3. Cliquez sur **OK**.



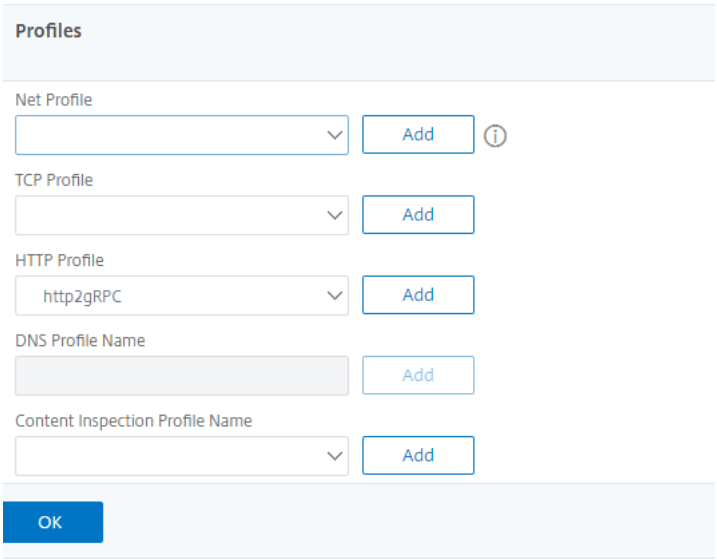
Ajouter un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définir le profil HTTP

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Dans la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Profils**.
4. Dans la section **Profils**, sélectionnez le type de profil HTTP.
5. Cliquez sur **OK**, puis sur **Terminé**.



Ajouter un service pour le point de terminaison gRPC et définir le profil HTTP

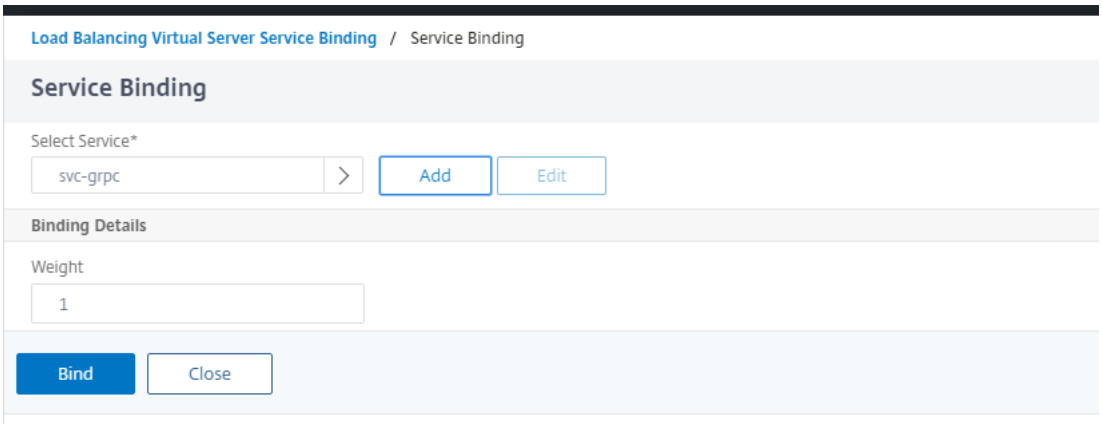
1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Cliquez sur **Ajouter** pour créer un serveur d'applications pour le trafic gRPC.
3. Sur la page du **service d'équilibrage** de charge, accédez à la section **Profil** .
4. Sous **Profils**, ajoutez un **profil HTTP** pour le point de terminaison gRPC.
5. Cliquez sur **OK**, puis sur **Terminé**.



Service Bind pour le point de terminaison gRPC vers le serveur virtuel d'équilibrage de charge

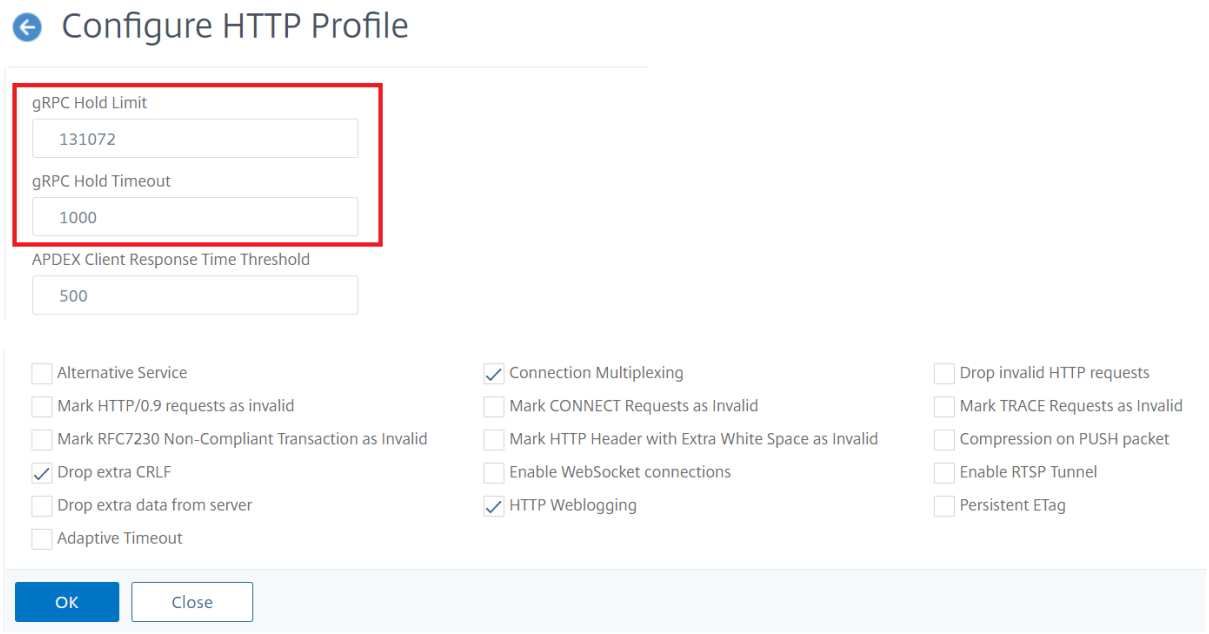
1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Dans la page **Serveur virtuel d'équilibrage de charge**, cliquez sur la section **Groupes de services et** de services.
4. Sur la page **Liaison du service de serveur virtuel d'équilibrage de charge**, sélectionnez le service gRPC à lier.

5. Cliquez sur **Fermer**, puis sur **Terminé**.



Configurer la mise en mémoire tampon de gRPC en fonction de l'heure et de la taille à l'aide de l'interface graphique

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.
2. Sélectionnez **HTTP/2** dans le profil HTTP.
3. Sur la page **Configurer le profil HTTP**, définissez les paramètres suivants :
   a) GrpHoldTimeout. Entrez la durée en millisecondes pour la mise en mémoire tampon des paquets gRPC jusqu'à la réception de la bande-annonce.
   b) GrpCholdLimit. Entrez la taille maximale en octets pour la mise en mémoire tampon des paquets gRPC jusqu'à la réception de la bande-annonce.
4. Cliquez sur **OK** et sur **Fermer**.



Pour connaître les procédures détaillées de l'interface graphique pour le service de liaison et les serveurs virtuels d'équilibrage de charge, consultez la rubrique Équilibrage de charge

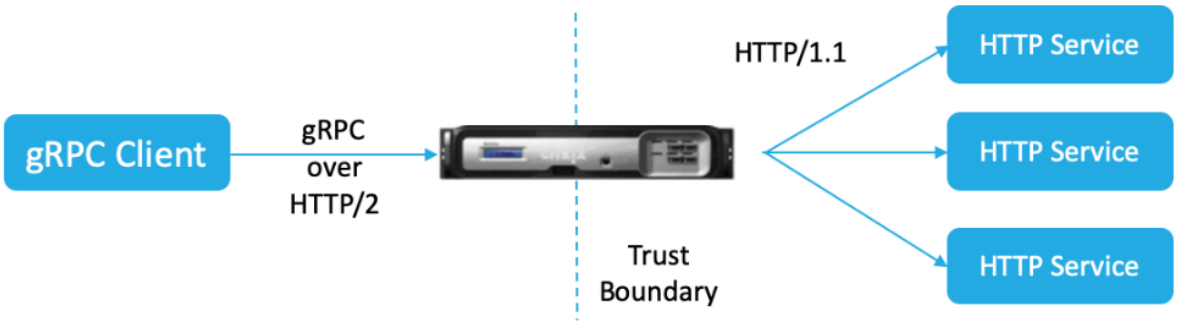
Pontage inversé gRPC

May 5, 2023

Dans ce scénario, l'appliance NetScaler relie de manière fluide le contenu gRPC reçu sur une connexion HTTP/2 et le transmet au serveur gRPC principal via HTTP/1.1.

Comment fonctionne le pontage inversé

Le schéma suivant montre comment les composants interagissent les uns avec les autres dans une configuration de pont gRPC.



1. Le client envoie une requête gRPC sur une connexion HTTP/2 avec des en-têtes gRPC dans des trames HTTP/2 et une charge utile proto-buf.
2. Sur la base de l'évaluation des politiques, le serveur virtuel d'équilibrage de charge (auquel est lié le service gRPC) traduit et transmet la demande via une connexion HTTP/1.1 au serveur principal.
3. À la réception de la réponse HTTP/1.1, s'il n'y a pas de code grpc-status dans la réponse, ADC déduit un status-case grpc à partir du code de réponse HTTP.
4. L'appliance insère ensuite les en-têtes gRPC dans la bande-annonce HTTP/2 avant de transmettre la réponse au client.

Configurer le pontage inversé gRPC à l'aide de l'interface de ligne de commande

Pour configurer le pontage inversé gRPC, vous devez suivre les étapes suivantes :

- Ajoutez le profil HTTP 1 avec HTTP/2 et HTTP/2 directs activés pour le serveur virtuel d'équilibrage de charge
- Ajouter le profil HTTP 2 avec HTTP/2 désactivé pour le serveur principal

- Ajoutez un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définissez-le sur le profil HTTP 1
- Ajoutez un service pour le point de terminaison gRPC et définissez-le sur le profil HTTP 2
- Service Bind pour le point de terminaison gRPC vers le serveur virtuel d'équilibrage de charge
- Mappez le code d'état HTTP au code d'état gRPC si la réponse n'a pas de code d'état grpc

Ajoutez le profil HTTP 1 avec HTTP/2 et HTTP/2 directs activés pour le serveur virtuel d'équilibrage de charge

Pour commencer la configuration du pontage inversé, vous devez ajouter deux profils HTTP. Un profil pour activer HTTP/2 pour les requêtes des clients gRPC et un autre profil pour désactiver HTTP/2 pour les réponses du serveur non gRPC.

À l'invite de commande, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Exemple :

add ns HttpProfile profile1 —http2 ACTIVÉ -HTTP2Direct ACTIVÉ

Ajouter le profil HTTP 2 avec HTTP/2 désactivé pour le serveur principal

Pour désactiver la prise en charge du HTTP/2 sur le profil HTTP pour la réponse du serveur principal à l'aide de la ligne de commande NetScaler.

À l'invite de commande, tapez :

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Exemple :

add ns HttpProfile profile2 —http2 DÉSACTIVÉ HTTP2Direct DÉSACTIVÉ

Ajoutez un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définissez-le sur le profil HTTP 1

Pour ajouter un serveur virtuel d'équilibrage de charge à l'aide de l'interface de commande NetScaler.

À l'invite de commande, tapez :

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Exemple :

ajouter lb vserver lb-grpc HTTP 10.10.10 80 -HTTPProfileName profile1

> **Remarque :**
>
> Si vous utilisez un serveur virtuel d'équilibrage de charge de type SSL, vous devez lier le certificat du serveur. Pour plus d'informations, reportez-vous à la rubrique relative au certificat de serveur Bind

Ajoutez un service pour le point de terminaison gRPC et définissez-le sur le profil HTTP 2

Pour ajouter un service avec un point de terminaison gRPC et définir le profil HTTP 2 à l'aide de l'interface de commande NetScaler.

À l'invite de commande, tapez :

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Exemple :

```
add service svc-grpc 10.10.10.11 HTTP 80 -httpProfileName profile2
```

Service de liaison entre le point de terminaison gRPC et le serveur virtuel d'équilibrage de charge

Lier un service gRPC à un serveur virtuel d'équilibrage de charge à l'aide de l'interface de commande NetScaler.

Dans l'interface de commande, tapez :

```
bind lb vserver <name> <serviceName>
```

Exemple :

```
bind lb vserver lb-grpc svc-grpc
```

Mappez le code de réponse HTTP au code d'état gRPC

Si le serveur ne génère pas de code d'état gRPC, l'appliance NetScaler génère un code d'état gRPC approprié en fonction de la réponse HTTP reçue. Les codes d'état sont répertoriés dans le tableau de mappage ci-dessous.

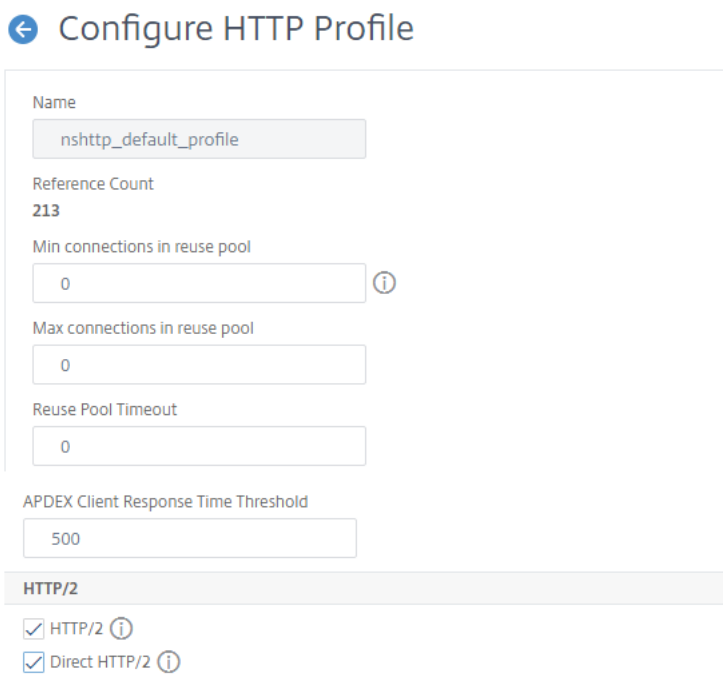
Code d'état de la réponse HTTP	Code d'état gRPC
200	OK.
400	INTERNE = 13
403	AUTORISATION_REFUSÉE = 7

Code d'état de la réponse HTTP	Code d'état gRPC
401	NON AUTHENTIFIÉ = 16
429, 502, 503, 504	INDISPONIBLE = 14
404	NON IMPLÉMENTÉ = 12

Configurer le pontage inversé gRPC à l'aide de l'interface graphique

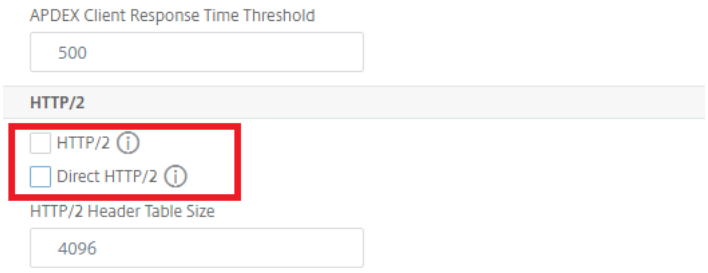
Ajoutez le profil HTTP 1 avec HTTP/2 et HTTP/2 directs activés pour le serveur virtuel d'équilibrage de charge

1. Accédez à Système > Profils et cliquez sur Profils HTTP.
2. Activez l'option HTTP/2 dans un profil HTTP 1.



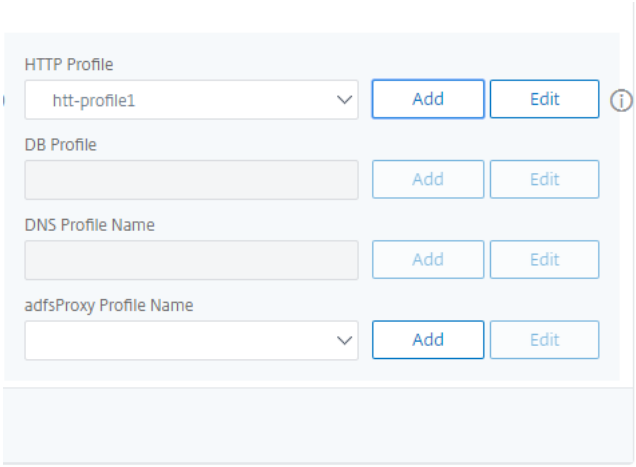
Ajouter le profil HTTP 2 avec HTTP/2 désactivé pour le serveur principal

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.
2. Activez l'option **HTTP/2** dans un profil HTTP 2.
3. Cliquez sur **OK**.



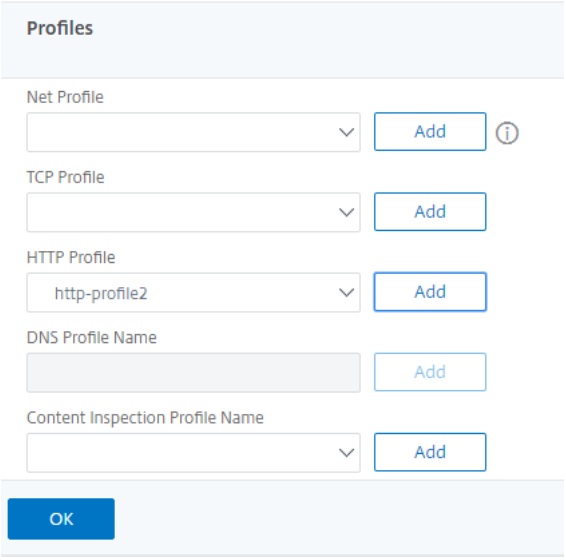
Ajoutez un serveur virtuel d'équilibrage de charge de type SSL/HTTP et définissez-le sur le profil HTTP 1

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Dans la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Profils**.
4. Dans la section **Profils**, sélectionnez le type de profil HTTP.
5. Cliquez sur **OK**, puis sur **Terminé**.



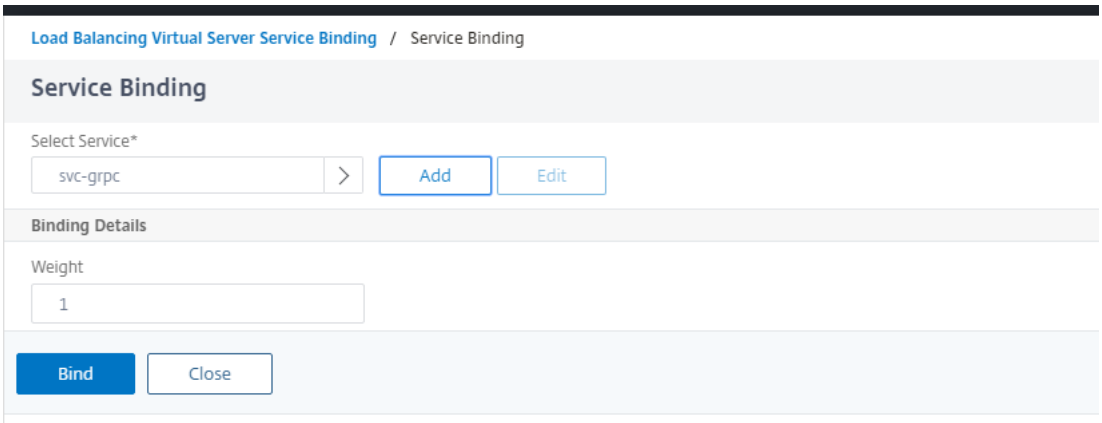
Ajoutez un service avec un point de terminaison gRPC et définissez-le sur le profil HTTP 2

1. Accédez à **Traffic Management > Load Balancing > Services**.
2. Cliquez sur **Ajouter** pour créer un serveur d'applications pour le trafic gRPC.
3. Sur la page du **service d'équilibrage** de charge, accédez à la section **Profil** .
4. Sous **Profils**, ajoutez un **profil HTTP** pour le point de terminaison gRPC.
5. Cliquez sur **OK**, puis sur **Terminé**.



Service Bind pour le point de terminaison gRPC vers le serveur virtuel d'équilibrage de charge

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour créer un serveur virtuel d'équilibrage de charge pour le trafic gRPC.
3. Sur la page **Serveur virtuel d'équilibrage de charge**, cliquez sur la section **Serviceet groupes** de services.
4. Sur la page **Liaison du service de serveur virtuel d'équilibrage de charge**, sélectionnez le service gRPC à lier.
5. Cliquez sur **Fermer**, puis sur **Terminé**.



Pour obtenir des procédures détaillées sur l'interface graphique, consultez la rubrique Équilibrage de charge .

Fin d'appel gRPC

May 5, 2023

Lorsqu'une appliance NetScaler dispose de politiques telles que la limitation du débit ou la sécurité du Web App Firewall configurées et si une politique est considérée comme vraie, l'appliance peut mettre fin à l'appel et répondre par un message d'erreur gRPC calculable adressé au client.

gRPC avec politique de réécriture

May 5, 2023

Le cas d'utilisation de gRPC avec politique de réécriture explique comment l'appliance NetScaler fonctionne pour réécrire certaines informations dans les demandes ou les réponses de gRPC. Le schéma suivant montre les interactions entre les composants.

Le diagramme suivant montre comment les composants interagissent les uns avec les autres dans un gRPC avec une configuration de politique de réécriture.

1. Activez la fonctionnalité de réécriture sur l'appliance.
2. Configurez l'action de réécriture pour modifier, ajouter ou supprimer des en-têtes gRPC.
3. Configurez la politique de réécriture pour déterminer les demandes gRPC (trafic) sur lesquelles une action doit être entreprise.
4. Liez la politique de réécriture au serveur virtuel d'équilibrage de charge pour vérifier si le trafic correspond à l'expression de la politique.
5. En utilisant une politique de réécriture, vous pouvez effectuer les opérations suivantes en fonction du code d'état gRPC.
    a) Modifiez les réponses depuis le serveur Web gRPC.
    b) Modifiez, ajoutez ou supprimez des en-têtes gRPC.
    c) Modifiez l'URL de la requête vers le serveur GrRC.

Configurer la terminaison d'appel gRPC avec une politique de réécriture

Pour configurer la terminaison d'appel gRPC avec une politique de réécriture, vous devez suivre les étapes suivantes :

1. Activer la fonctionnalité de réécriture
2. Add rewrite policy
3. Lier la politique de réécriture au serveur virtuel d'équilibrage de charge

Activer la fonctionnalité de réécriture

Pour utiliser la fonctionnalité de réécriture, vous devez d'abord l'activer.

À l'invite de commande, tapez :

```
enable ns rewrite
```

Add rewrite policy

Après avoir configuré une action de réécriture, vous devez ensuite configurer une politique de réécriture pour sélectionner les demandes gRPC sur lesquelles l'appliance NetScaler doit réécrire.

À l'invite de commande, tapez :

```
add rewrite policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Exemple :

```
add rewrite policy grpc-rewr_pol1 "http.res.header(\"grpc-status\").NE
(\"0\")"RESET
```

Lier la politique de réécriture au serveur virtuel d'équilibrage de charge

Pour mettre en œuvre une politique, vous devez la lier au serveur virtuel d'équilibrage de charge avec le service gRPC.

À l'invite de commande, tapez :

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```

Exemple :

```
bind lb vserver lb-grpc -policyName grpc-rewr_pol1 -priority 100
```


GrPC avec la stratégie de répondeur

May 5, 2023

La configuration du gRPC avec politique de réponse explique comment une appliance NetScaler fournit différentes réponses aux requêtes gRPC via le protocole HTTP/2. Lorsque les utilisateurs demandent une page d'accueil de site Web, vous pouvez fournir une page d'accueil différente en fonction de l'emplacement de chaque utilisateur ou du navigateur utilisé par l'utilisateur.

Le diagramme suivant montre les composants qui interagissent.

1. Activez la fonction de répondeur sur l'appliance.
2. Configurez l'action du répondeur pour générer une réponse personnalisée, rediriger une demande vers une autre page Web ou réinitialiser une connexion.
3. Configurez la politique du répondeur pour déterminer les demandes gRPC (trafic) sur lesquelles une action doit être entreprise.
4. Liez la stratégie de répondeur au serveur virtuel d'équilibrage de charge pour vérifier si le trafic correspond à l'expression de stratégie.
5. En utilisant une stratégie de répondeur, vous pouvez effectuer les opérations suivantes en fonction du code d'état GrPC.

Configurer la terminaison d'appel GrPC avec la stratégie de répondeur à l'aide de l'interface de ligne de commande

Pour configurer la terminaison d'appel GRPC avec la stratégie de répondeur, vous devez effectuer les étapes suivantes :

1. Activer la fonction répondeur
2. Ajouter une action de répondeur
3. Ajouter une stratégie de répondeur et une action de répondeur associé
4. Lier la stratégie du répondeur au serveur virtuel d'équilibrage de charge

Activer la fonction répondeur

Pour utiliser la fonction répondeur, vous devez d'abord l'activer.

À l'invite de commande, tapez :

```
enable ns responder
```

Ajouter l'action du répondeur

Après avoir activé la fonctionnalité, vous devez configurer l'action du répondeur pour gérer la réponse GRPC en fonction du code d'état renvoyé par le serveur principal.

À l'invite de commande, tapez :

```
add responder action <name> <type>
```

Exemple :

```
add responder action grpc-act respondwith "HTTP/1.1 200 OK\r\nServer: NS
-Responder\r\nContent-Type:application/grpc\r\ngrpc-status: 12\r\ngrpc
-message: Not Implemented\r\n\r\n"+ "Method: "+ HTTP.REQ.URL+ "is not
implemented."
```

Ajouter une politique de réponse

Après avoir configuré une action de répondeur, vous devez ensuite configurer une politique de répondeur pour sélectionner la demande gRPC à laquelle l'appliance NetScaler doit répondre.

À l'invite de commande, tapez :

```
add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Exemple :

```
add responder policy grpc-resp-pol1 HTTP.REQ.URL.NE( "/helloworld.Greeter/
SayHello" )grpc-act
```

Lier la politique du répondeur au serveur virtuel d'équilibrage de charge

Pour mettre en œuvre une politique, vous devez la lier au serveur virtuel d'équilibrage de charge avec le service gRPC.

À l'invite de commande, tapez :

```
bind responder global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```


Exemple :

```
bind lb vserver lb-grpc svc-grpc -policyName grpc-resp-pol1 -priority 100
```

Pour plus d'informations sur la stratégie de répondeur, consultez la rubrique Stratégie de répondeur .

Expressions de stratégie pour correspondre aux champs tampon du protocole GrPC

L'appliance NetScaler prend en charge les expressions de politique suivantes dans la configuration gRPC :

- **Accès au champ tampon du protocole GrPC.** L'appel d'API GrPC arbitraire correspond au numéro du champ de message avec les nouvelles expressions de stratégie. Dans une configuration IP, les correspondances sont effectuées uniquement en utilisant les « numéros de champ » et le « chemin d'accès API ».
- **Filtrage des en-têtes GrPC.** Les paramètres « HttpProfile » pour GrPC sont utilisés pour ajuster le comportement par défaut de l'analyse GrPC (y compris les expressions de stratégie GrPC). Les paramètres suivants s'appliquent aux expressions de stratégie GrPC :
  - **Délimitation de la longueur du GRPC.** Il est activé par défaut et s'attend à ce que les tampons de protocole soient présentés avec un message délimité par la longueur.
  - **Limite de cholestérol GRP.** La valeur par défaut est 131072. Il s'agit de la taille maximale du message tampon de protocole en octets. Il s'agit également de la longueur de chaîne maximale et de la longueur maximale du champ « octet ».

Configurer les expressions de stratégie avancée GrPC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED ) -
    gRPCLengthDelimitation ( ENABLED | DISABLED ) -gRPCHoldLimit <int>
```

Exemple :

```
set ns httpProfile http2gRPC -http2 ENABLED -gRPCLengthDelimitation
    ENABLED -gRPCHoldLimit 131072
```

Configurer les paramètres de filtrage des en-têtes GrPC à l'aide de l'interface graphique

1. Accédez à **Système > Profils** et cliquez sur **Profils HTTP**.

2. Sur la page **Créer un profil HTTP**, faites défiler jusqu'à la section **HTTP/3**, sélectionnez **Délimitation de longueur GrPC**.

L'exemple d'expression de stratégie suivant montre une valeur dans le message 5, le sous-message 4 et le champ 3. Il s'agit d'un int 32 bits égal à 2.

```
1 http.req.body(1000).grpc.message(5).message(4).int32(3).eq(2)
```

Les expressions de stratégie suivantes sont ajoutées pour correspondre aux champs de message tampon du protocole GrPC par numéro :

- message
- double
- flotte
- int32
- int64
- uint32
- uint64
- sint64
- sint32
- fixed32
- fixed64
- sfixed32
- sfixed64
- Bool
- string
- enum
- octets

Correspondance des chemins API

La correspondance du chemin d'accès de l'API est utilisée pour correspondre à l'appel d'API GrPC correct lorsque plusieurs API sont utilisées. Faites correspondre le chemin d'accès de l'API, qui se trouve dans le pseudo en-tête « : path » de la requête HTTP.

Exemple :

```
1 http.req.header(":path").eq("acme.inventory.v1/ListBooks")
```


Moniteur de contrôle de santé gRPC

June 20, 2023

Le moniteur de gRPC santé examine l'état de santé des gRPC serveurs. Le moniteur de gRPC santé vérifie l'état général du gRPC service ou celui d'un service particulier. Actuellement, l'appliance NetScaler ne prend en charge que la méthode de vérification.

Dans l'appliance NetScaler, le moniteur de vérification de l'état est configuré en définissant les gRPC paramètres tels que gRPCHealthCheck gRPCStatusCodegRPCServiceName, et httprequest dans la configuration du moniteur HTTP2. Un client implémentant le protocole interroge le serveur pour connaître son état (sain, non sain, inconnu ou service non implémenté) et attend la réponse d'état du service.

Le tableau suivant donne des détails sur les nouveaux paramètres gRPC et leur description :

paramètres gRPC	Valeur	Description
gRPCHealthCheck	Oui/Non	Activez ou désactivez la sonde de contrôle de santé gRPC.
gRPCStatusCode	Int non signé (0-65535), par défaut : 12	Configurez jusqu'à 16 codes d'état gRPC. L'appliance recherche le code d'état 0 dans la réponse d'état. S'il ne reçoit pas 0, le service peut être configuré sur up si l'un des 16 codes correspond à l'état du service.
gRPCServiceName	Nom du service entre guillemets, Default = « » (chaîne vide)	Vérifiez l'état de santé du service en question.

Configurez le moniteur de santé gRPC dans HTTP/2 à l'aide de l'interface de commande

Pour effectuer une sonde de vérification de l' gRPC état, vous devez activer le service de vérification de l' gRPC état, configurer le code d'état et fournir le nom du gRPC service pour lequel le contrôle de gRPC santé doit être effectué. À l'invite de commande, tapez :

```
add lb monitor <monitor_name> HTTP2 -httpRequest <string> -grpcHealthCheck
( YES | NO )- grpcStatusCode <positive_integer> - grpcServiceName string>]
```


Exemple :

```
add lb monitor http2 HTTP2 -httprequest "POST /grpc.health.v1.Health/Check"
 - gRPCHealthCheck Yes -gRPCStatusCode 0 -grpcServiceName "ECHO"
```

Configurez le moniteur de santé gRPC dans HTTP/2 à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Moniteurs**.
2. Cliquez sur **Ajouter**.
3. Dans la page **Créer un moniteur**, définissez les paramètres suivants :
   a) Nom. Nom du moniteur de santé gRPC.
   b) Type. Sélectionnez le type de service HTTP/2.
   c) gRPC HealthCheck. Activer la sonde de contrôle de santé gRPC.
   d) gRPC StatusCode. L'état du service gRPC est « UP » uniquement si le code d' état gRPC est zéro ou la valeur configurée. L'état passe « bas » si le code d'état est une valeur autre que zéro ou la valeur configurée.
   e) gRPC Nom du service. Service pour lequel le bilan de santé est effectué.
4. Créer **Créer**.

QUIC

May 5, 2023

Quick UDP Internet Protocol (QUIC) est une combinaison de protocoles (TCP+TLS+HTTP/2) implémentés sur UDP. Le protocole de transport QUIC multiplexe les connexions entre deux terminaux utilisant UDP. De plus, par rapport à d'autres protocoles, QUIC fournit de hautes performances en termes de sécurité, de livraison rapide du trafic et de latence réduite.

Un pont QUIC est configuré dans une appliance NetScaler pour équilibrer la charge du trafic QUIC entre un client QUIC et un serveur principal QUIC. Le pont QUIC vous permet d'avoir des connexions QUIC persistantes entre le client et le serveur en cas de reliaison NAT ou de migration de connexion. Cette configuration ne traite cependant pas les données. Il est utilisé uniquement pour l'équilibrage de charge du trafic QUIC via l'appliance NetScaler.

Les paquets QUIC contiennent un ID de connexion permettant aux points de terminaison d'associer les paquets à une adresse différente ou à 4 tuples à la même connexion. L'ID de connexion contient les détails de l'ID de serveur qui sont partagés avec l'appliance NetScaler et avec les serveurs principaux. L'appliance NetScaler extrait les détails de l'ID de connexion de l'ID du serveur et renvoie le trafic au serveur principal. Les ID de connexion se trouvent dans des paquets protégés, ce qui rend les connexions robustes en cas de migration de connexion.

> **Important**
>
> Les serveurs principaux doivent être pris en charge pour encoder l'ID de serveur dans l'ID de connexion QUIC.

Avantages du pont QUIC

Le pont QUIC pour l'appliance NetScaler est préférable pour les raisons suivantes :

- Pas d'opérations de crypto coûteuses.
- Le routage sans état est possible (pas d'équilibrage de charge basé sur 4 tuples).

Support de délestage cryptographique pour QUIC

Si une appliance NetScaler est équipée de puces matérielles SSL, elle effectue l'accélération cryptographique de manière transparente et accélère les transactions QUIC. Cette accélération est réalisée en déchargeant le traitement cryptographique du logiciel vers le matériel. Aucune configuration explicite n'est requise pour cette prise en charge. L'accélération des transactions QUIC est prise en charge dans les appliances NetScaler équipées de matériel. `Intel Coleto`

Configuration du pont QUIC

June 20, 2023

Pour configurer le pont QUIC, vous devez effectuer les opérations suivantes :

- Ajouter un profil de pont QUIC
- Ajouter des serveurs back-end QUIC
- Ajouter le service QUIC sur l'appliance
- Ajouter un serveur virtuel d'équilibrage de charge de type pont QUIC
- Lier le pont QUIC au serveur virtuel d'équilibrage de charge de type pont QUIC

> **Important**
>
> Avant de configurer le pont QUIC, assurez-vous d'abord d'activer la fonction d'équilibrage de charge sur l'appliance. Pour plus d'informations, consultez la section Configurer l'équilibrage de charge de base.

Configurer le pont QUIC à l'aide de l'interface de ligne de commande

Les sections suivantes doivent être configurées à l'aide de l'interface de ligne de commande.

Ajouter un profil de pont QUIC

Ajoutez un profil de pont QUIC.

À l'invite de commande, tapez :

```
add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
    serveridlen <value>
```

Exemple :

```
add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```

> **Remarque**
>
> Le `serveridlen` paramètre configuré dans cet exemple est la longueur d'un ID de serveur personnalisé, qui est la chaîne hexadécimale IP et PORT.

Ajouter un serveur d'applications back-end QUIC

Ajoutez des serveurs d'applications back-end QUIC.

À l'invite de commande, tapez :

```
-  add server <name> (<IPAddress>)
-  add server <name> (<IPAddress>)
```

Exemple :

```
-  add server s1 192.0.2.20
-  add server s2 192.0.2.30
```

Ajouter un service de pont QUIC

Vous devez ajouter le service de pont QUIC aux serveurs d'applications.

À l'invite de commande, tapez :

```
-  add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
    CustomServerID <string>]

-  add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
    CustomServerID <string>]
```

Exemple :


```
- add service src1 s1 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A8026401BB

- add service src2 s2 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A802C801BB
```

> **Remarque**
>
> Les `CustomServerID` paramètres configurés dans l'exemple précédent sont la chaîne hexadécimale d'une adresse IP correspondante et le PORT du serveur (s1 et s2). Pour la fonctionnalité de pont QUIC, Citrix vous recommande de configurer le `CustomServerID` paramètre au format de chaîne hexadécimale uniquement.

Ajouter un serveur virtuel d'équilibrage de charge de type pont QUIC

Vous devez ajouter un serveur virtuel d'équilibrage de charge de type pont QUIC.

À l'invite de commande, tapez :

```
add lb vserver <name> [<IPAddress>@ <port>] [-persistenceType <
    persistenceType >] [-lbMethod < lbMethod >] [-rule <rule>] [-
    cltTimeout <secs>] [-quickBridgeProfilename <name>]
```

Exemple :

```
add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
    persistenceType CUSTOMSERVERID -lbMethod TOKEN -rule QUIC.
    CONNECTIONID -cltTimeout 120 -quicBridgeProfilename q1
```

> **Remarque**
>
> Lors de la configuration du serveur virtuel QUIC bridge, vous devez configurer le paramètre `persistenceType` en tant que `CUSTOMSERVERID`, le paramètre `rule` en tant que `QUIC.CONNECTIONID` et le paramètre `LbMethod` en tant que `TOKEN`.

Lier le service de pont QUIC au serveur virtuel d'équilibrage de charge de type pont QUIC

Vous devez lier le service de pont QUIC au serveur virtuel d'équilibrage de charge de type pont QUIC.

À l'invite de commande, tapez :

```
- bind lb vserver <name> (<serviceName>)

- bind lb vserver <name> (<serviceName>)
```

Exemple :


```
- bind lb vserver quic_bridge_vip src1

- bind lb vserver quic_bridge_vip src2
```

Configurer le pont QUIC pour les groupes de services

Vous pouvez également configurer les capacités du pont QUIC pour des groupes de services. Les étapes suivantes vous guident à configurer le pont QUIC pour les groupes de services.

Pour configurer le pont QUIC pour les groupes de services, vous devez effectuer les opérations suivantes :

Ajouter un profil de pont QUIC

À l'invite de commande, tapez :

```
add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
   serveridlen <value>
```

Exemple :

```
add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```

Ajouter un serveur de type QUIC

À l'invite de commande, tapez :

```
- add server <name> (<IPAddress>)
- add server <name> (<IPAddress>)
```

Exemple :

```
- add server s1 192.0.2.20
- add server s2 192.0.2.30
```

Ajouter un groupe de service de pont QUIC

À l'invite de commande, tapez :

```
add serviceGroup <serviceGroupName> (<IP> | <serverName>) <serviceType>
```

Exemple :


```
add serviceGroup svg1 QUIC_BRIDGE
```

Liez les serveurs QUIC au groupe de services

À l'invite de commande, tapez :

```
- bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
    CustomServerID <string>]
- bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
    CustomServerID <string>]
```

Exemple :

```
- bind serviceGroup svg1 s1 443 -customServerID C0A8026401BB
- bind serviceGroup svg1 s2 443 -customServerID C0A802C801BB
```

Ajouter un serveur virtuel d'équilibrage de charge de type pont QUIC

À l'invite de commande, tapez :

```
add lb vserver <name> [<IPAddress>@ <port> [-persistenceType <
    persistenceType >] [-lbMethod < lbMethod > [-cltTimeout <secs>] [-
    quickBridgeProfilename <name>]
```

Exemple :

```
add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
    persistenceType CUSTOMSERVERID -lbMethod TOKEN -cltTimeout 120 -
    quicBridgeProfilename q1
```

Liez le serveur virtuel d'équilibrage de charge de type pont QUIC au groupe de services

À l'invite de commande, tapez :

```
bind lb vserver <name>@ (<serviceName>@ <serviceGroupName>
```

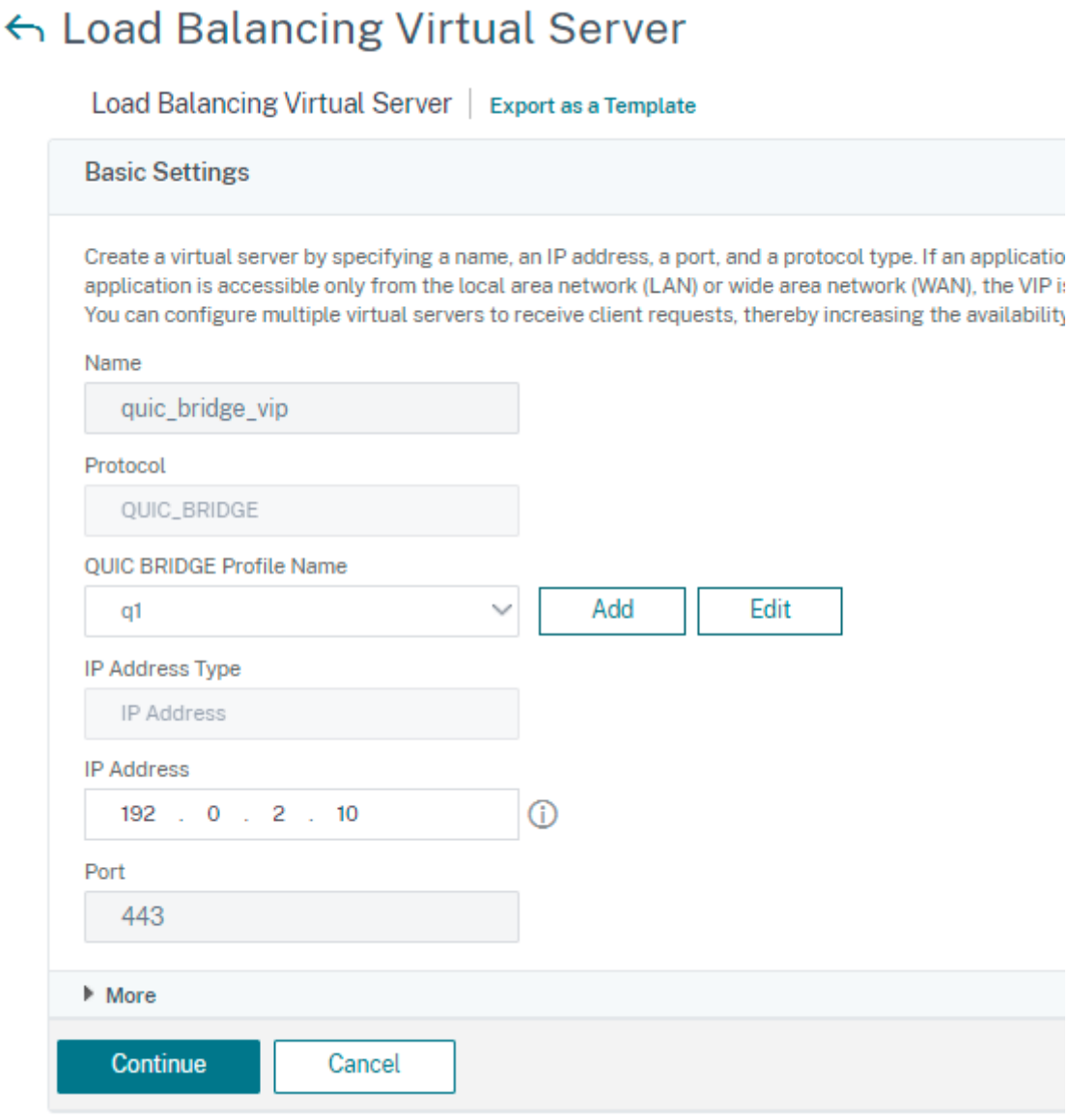
Exemple :

```
bind lb vserver quic_bridge_vip svg1
```


Configuration du pont QUIC à l'aide de l'interface graphique

Procédez comme suit pour configurer le pont QUIC à l'aide de l'interface graphique.

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sur la page **Serveurs virtuels**, cliquez sur **Ajouter**.
3. Sur la page **Serveur virtuel d'équilibrage de charge**, sélectionnez le protocole en tant que QUIC_BRIDGE et entrez les détails. Cliquez sur **OK**.

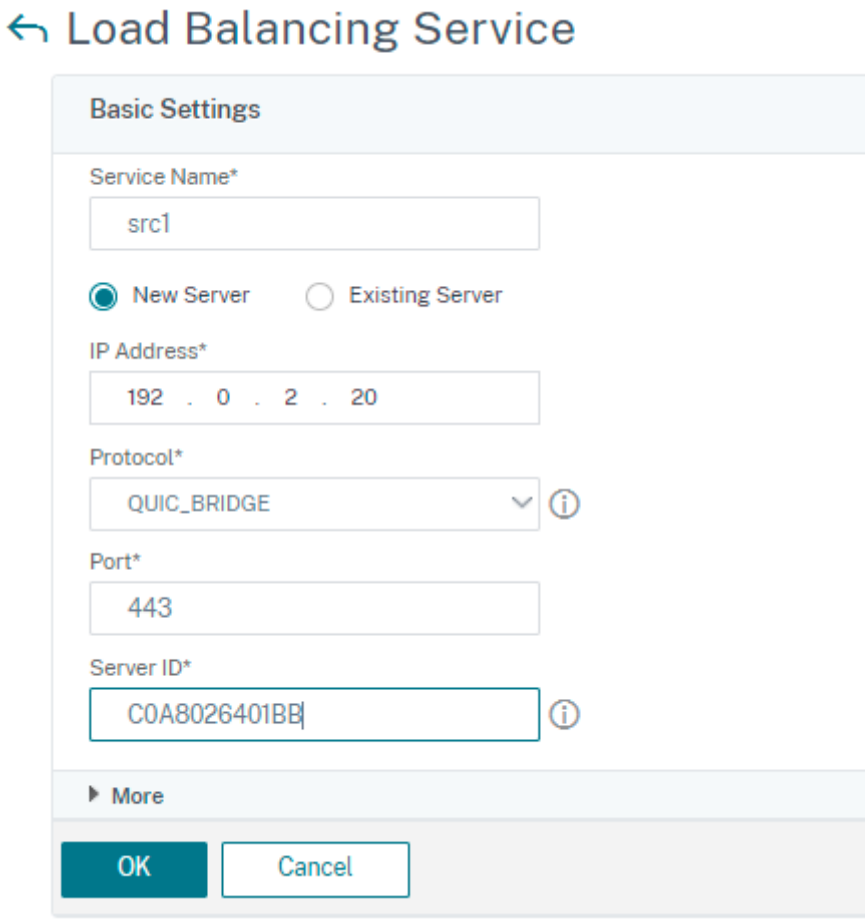


4. Sur la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Continuer** et **terminé**.

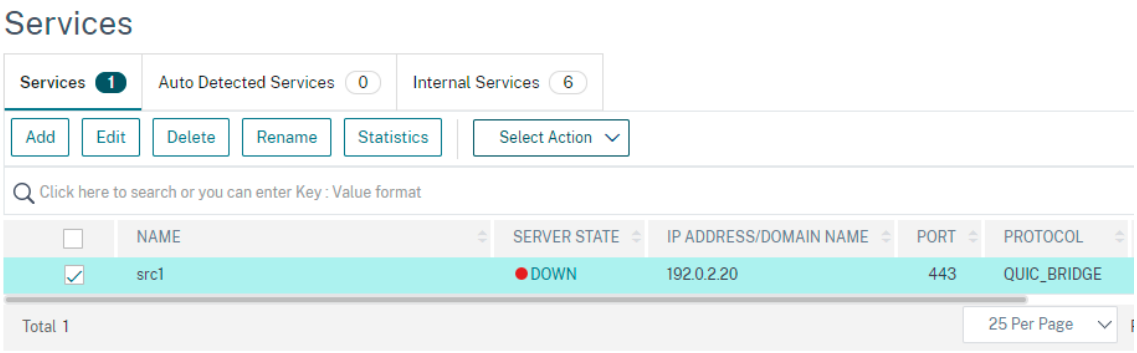
Configurer l'équilibrage de charge pour les services à l'aide de l'interface graphique

Suivez les étapes suivantes pour configurer l'équilibrage de charge pour les services à l'aide de l'interface graphique.

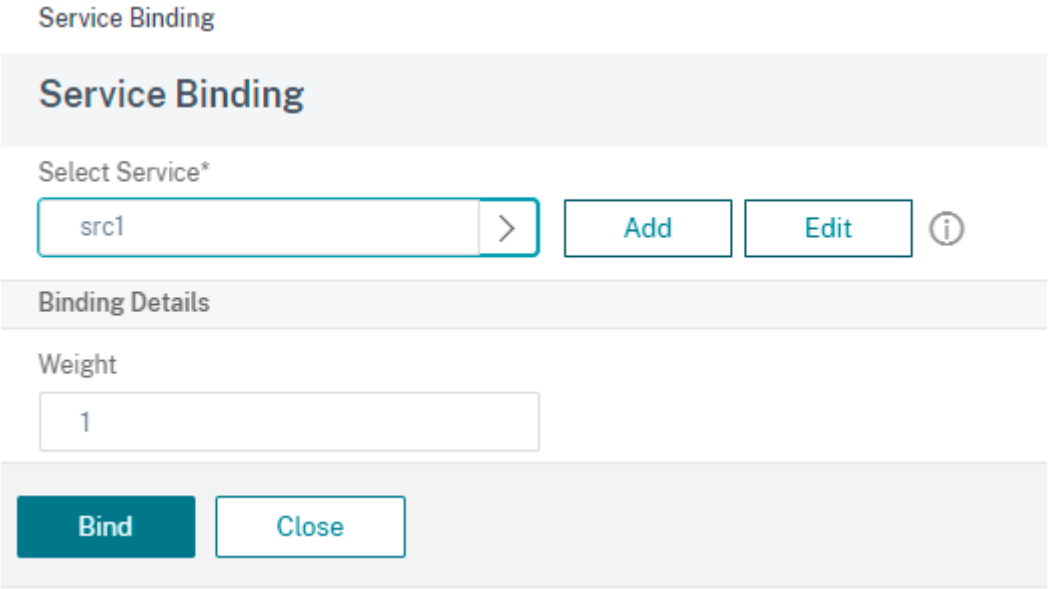
1. Accédez à **Traffic Management > Load Balancing > Services**. Sur la page **Services**, cliquez sur **Ajouter**.
2. Sur la page **Service d'équilibrage de charge**, entrez les détails et cliquez sur **OK**.



3. Sur la page **Serveurs virtuels**, sélectionnez le serveur virtuel créé pour lier le service.
4. Faites défiler vers le bas sur la page **Serveur virtuel d'équilibrage de charge** et sélectionnez les **services et groupes de**services.
5. Sur l'écran **Liaison de service**, cliquez sur **Sélectionner le champ Service** .
6. Sur l'écran **Service**, sélectionnez le service à lier au serveur virtuel d'équilibrage de charge, puis cliquez sur **Sélectionner**.



7. Le service src1 est sélectionné et sur l'écran **de liaison de service**, cliquez sur **Lier**.



8. Sur la page **Serveur virtuel d'équilibrage de charge**, cliquez sur **Terminé**.

Afficher les statistiques du pont QUIC

Le pont QUIC prend en charge la commande de statistiques pour afficher un résumé détaillé des statistiques de pont QUIC.

Les commandes suivantes affichent un résumé détaillé des statistiques de pont QUIC. À l'invite de commandes, tapez ce qui suit :

- `stat quicbridge`
- `stat quicbridge -detail`

Pour effacer l'affichage des statistiques, tapez l'une des options suivantes :

- `stat quicbridge -clearstats basic`
- `stat quicbridge -clearstats full`

Afficher les statistiques de pont QUIC à l'aide de l'interface graphique

Suivez les étapes suivantes pour afficher les statistiques du pont QUIC.

1. Dans l'onglet **Tableau de bord**, placez le pointeur de la souris sur la section **Vue d'ensemble du système** .
2. Cliquez sur **Vue d'ensemble du système** et sélectionnez QUIC BRIDGE dans la liste déroulante.

Protocole Proxy

July 7, 2023

Le protocole proxy transporte en toute sécurité les informations du client du client au serveur via les appliances NetScaler. L'appliance ajoute un en-tête de protocole proxy avec les détails du client et le transfère au serveur principal. Vous trouverez ci-dessous certains des scénarios d'utilisation du protocole proxy dans une appliance NetScaler.

- Adresse IP du client d'origine
- Sélection d'une langue pour un site Web
- Bloquer la liste des adresses IP sélectionnées
- Enregistrement et collecte de statistiques.

Voici les trois modes de fonctionnement :

- Insérer. L'appliance insère les détails du client et les envoie au serveur principal.
- Avancer. L'appliance transmet les détails du client au serveur principal.
- Dépouillé. L'appliance stocke les détails du client à des fins de journal. De plus, si le protocole proxy n'est pas pris en charge sur le serveur principal, envoie les détails du client au serveur à l'aide de la configuration de la stratégie de réécriture

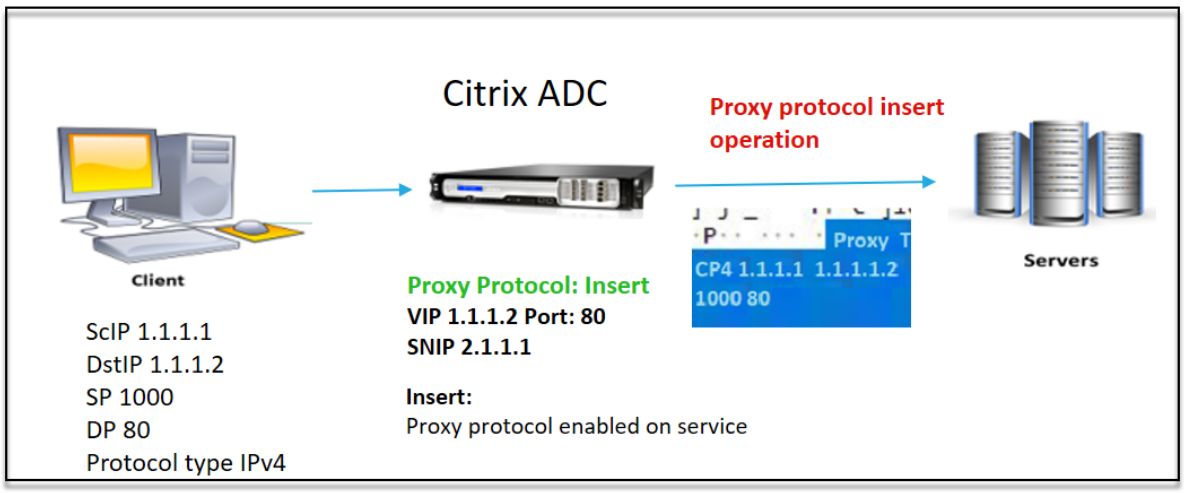
Limitations

Le protocole proxy n'est pas pris en charge pour les fonctionnalités TCP Fast Open (TFO) et TCP MultiPath. Cette fonctionnalité n'est prise en charge que pour les services pour lesquels l'appliance NetScaler met fin à la connexion TCP. Il ne prend pas en charge d'autres services, par exemple « ANY ».

Comment fonctionne le protocole proxy dans une appliance NetScaler

Les organigrammes suivants montrent comment configurer le protocole proxy sur les appliances NetScaler pour les opérations d'insertion, de transfert et de retrait :

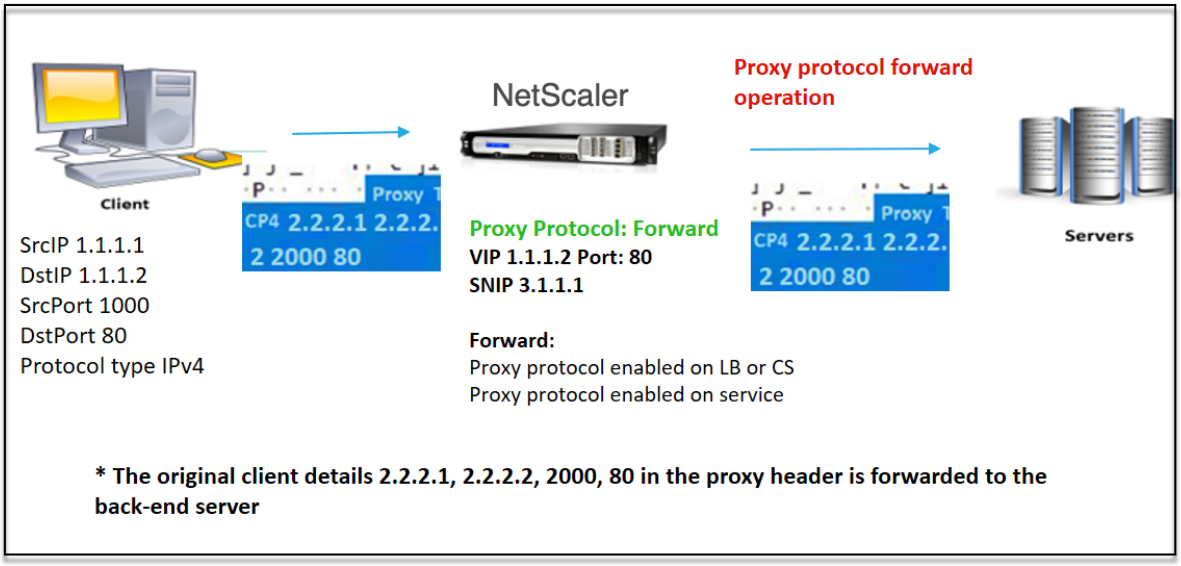
Opération d'insertion



L'interaction des composants est la suivante :

- Sur l'instance NetScaler, vous devez activer le protocole proxy dans le profil réseau et le lier au service.
- Lors de l'opération d'insertion, NetScaler ajoute un en-tête de proxy avec les détails de connexion du client et le transmet au serveur principal.
- Côté envoi, l'appliance décide de la version du protocole proxy en fonction de la configuration de l'interface de ligne de commande.

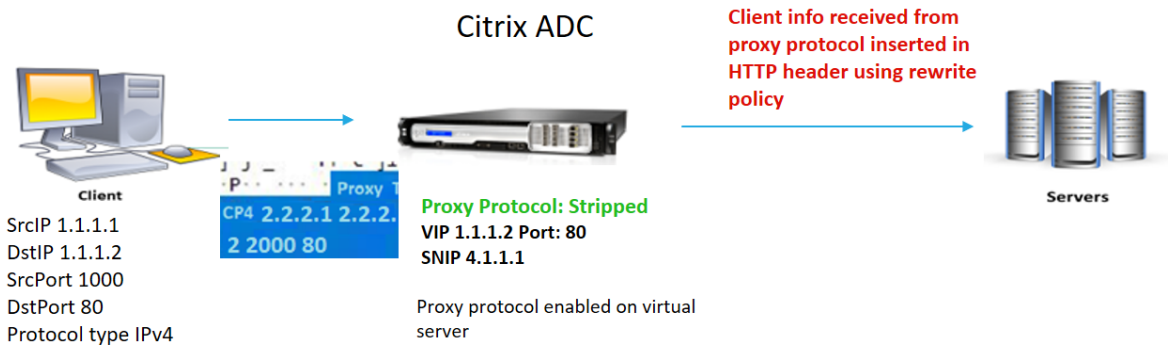
Opération Forward



L'interaction des composants est la suivante :

- Un client envoie une demande avec l'en-tête du proxy à NetScaler. L'appliance identifie dynamiquement la version.
- Dans l'appliance NetScaler, il s'agit d'une opération Forward. Le protocole proxy est activé sur le serveur virtuel d'équilibrage de charge ou le serveur virtuel de commutation de contenu et activé sur le service. L'appliance reçoit l'en-tête du proxy et transmet les détails de l'en-tête au serveur principal.
- Si les détails de l'en-tête du proxy ne sont pas au format incorrect, l'appliance réinitialise la connexion.
- Côté envoi, l'appliance décide de la version du protocole proxy en fonction de la configuration de l'interface de ligne de commande.

Opération dépouillée



L'interaction des composants est la suivante :

- Un client envoie une demande accompagnée d'un en-tête de proxy à l'appliance NetScaler.
- Dans l'appliance NetScaler, s'il s'agit d'une opération Stripped, l'appliance transmet les informations client obtenues à partir du protocole proxy et les insère dans l'en-tête HTTP à l'aide d'expressions de stratégie de réécriture.
- Les détails du client, tels que l'adresse IP source, l'adresse IP de destination, le port source et le port de destination, sont ajoutés dans un en-tête HTTP à l'aide d'expressions de stratégie de réécriture. La stratégie de réécriture évalue l'expression et si elle est « true », l'action de stratégie de réécriture correspondante est déclenchée. Les détails du client sont ensuite transférés au serveur principal dans un en-tête HTTP.
- Si les détails de l'en-tête du proxy ne sont pas au format incorrect, l'appliance réinitialise la connexion.

Formats de version du protocole proxy

La version du protocole Proxy est disponible en deux formats. L'appliance décide d'utiliser un format basé sur la longueur des données entrantes. Pour plus d'informations, voir DP sur le protocole proxy .

1. Format de version 1 du protocole proxy

   ```
   PROXY TCP4/TCP6/UNKNOWN <SRC IP> <DST IP> <SRC PORT> <DST PORT>
   ```

   - PROXY -> Format de chaîne unique pour l'en-tête proxy version -1.
   - Prise en charge des protocoles TCP sur IPv4 et TCP sur IPv6. Pour les autres protocoles, c'est INCONNU.
   - IP SRC : adresse IP source (IP du client d'origine) d'un paquet.
   - IP DST : adresse IP de destination d'un paquet.
   - Port SRC : port source d'un paquet.
   - Port DST : port de destination d'un paquet.

2. Format de version 2 du protocole proxy

   ```
   0D 0A 0D 0A 00 0D 0A 51 55 49 54 0A <13th byte> <14th byte> <15-16th byte> <17th byte onwards>
   ```

   - D 0A 0D 0A 00 0D 0A 51 55 49 54 0A -> Chaîne binaire unique pour l'en-tête Proxy version -2.
   - Prise en charge des protocoles TCP sur IPv4 et TCP sur IPv6. Pour les autres protocoles, c'est INCONNU.
   - Treizième octet — version du protocole et commande.
   - Quatorzième octet — famille d'adresses et de protocoles.
   - 15-16e octet : longueur de l'adresse dans l'ordre du réseau.
   - À partir du dix-septième octet - Adresses des informations présentes dans l'ordre du réseau - IP src, IP dst, port src, port dst.

Support d'expression de l'infrastructure des stratégies des répondeurs

Le protocole proxy prend en charge les expressions d'infrastructure de stratégie de réponse suivantes pour les serveurs virtuels de type TCP et HTTP :

1. CLIENT.PROXY.SRCIP_STR
2. CLIENT.PROXY.DSTIP_STR
3. CLIENT.PROXY.SRCPORT
4. CLIENT.PROXY.DSTPORT
5. CLIENT.PROXY.ETHERTYPE

> **Remarque**
>
> NetScaler prend en charge l'expression de l'infrastructure de stratégie de répondeur pour le protocole proxy sur un serveur virtuel de type TCP à partir des versions 13.1-48.x de NetScaler.

Configurer le protocole proxy dans l'appliance NetScaler

Effectuez les étapes suivantes pour configurer le protocole proxy dans votre appliance NetScaler.

1. Activez le protocole proxy en tant que global.
2. Configurez le protocole proxy pour l'opération d'insertion.
3. Configurez le protocole proxy pour le fonctionnement Forward.
4. Configurez le protocole proxy pour le fonctionnement de Strip.

Activer le protocole proxy en tant que global

À l'invite de commandes, tapez ce qui suit :

```
set ns param -proxyProtocol ENABLED
```

Configurer le protocole proxy pour l'opération d'insertion

Pour configurer le protocole proxy pour l'opération d'insertion, vous devez désactiver le protocole sur le serveur virtuel d'équilibrage de charge et activer le protocole sur le service.

Ajouter un profil réseau avec le protocole proxy désactivé pour le serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Exemple :

```
Add netprofile proxyprofile-1 -proxyProtocol DISABLED -proxyprotocoltxversion
 V1
```

> **Remarque :**
>
> Si vous désactivez le protocole proxy sur votre appliance, il n'est pas nécessaire de définir le paramètre de version du protocole.

Ajouter un profil réseau avec un protocole proxy activé pour le service

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Exemple :

```
add netprofile proxyprofile-2 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Ajouter un serveur virtuel d'équilibrage de charge pour l'appliance NetScaler dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Exemple :

```
add lb vserver lbvserver-1 http 1.1.1.1 80
```

Ajouter un service HTTP pour l'appliance NetScaler dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Exemple :

```
Add service http-service-1 2.2.2.1 http 80
```

Définir le profil réseau avec un serveur virtuel d'équilibrage de charge dans l'appliance NetScaler

À l'invite de commandes, tapez ce qui suit :

```
set lb vserver <vserver name> -netprofile <name>
```

Exemple :

```
set lb vserver lbvserver-1 -netprofile proxyProfile-1
```

Définir le profil réseau avec le service HTTP dans l'appliance NetScaler

À l'invite de commandes, tapez ce qui suit :

```
set service <service name> -netprofile <name>
```


Exemple :

```
set service http-service-1 -netprofile proxyProfile-2
```

Liez le serveur virtuel d'équilibrage de charge au service

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <vserver name> <service name>
```

Exemple :

```
bind lb vserver lbvserver-1 http-service-1
```

Configurer le protocole proxy pour une opération de transfert

Pour configurer le protocole proxy pour l'opération Forward pour la prochaine instance NetScaler de la couche proxy, vous devez activer le protocole et vous connecter au serveur ou au service virtuel.

> **Remarque :**
>
> Le profil réseau créé pour le serveur virtuel d'équilibrage de charge peut également être utilisé pour le service.

Ajouter un profil réseau avec le protocole proxy activé pour le serveur virtuel d'équilibrage de charge

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Exemple :

```
add netprofile proxyprofile-3 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Ajouter un profil réseau avec le protocole proxy activé pour le service

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Exemple :

```
add netprofile proxyprofile-4 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```


Ajouter un serveur virtuel d'équilibrage de charge pour l'appliance NetScaler dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Exemple :

```
add lb vserver lbvserver-2 http 2.2.2.2 80
```

Ajouter un service HTTP pour l'appliance NetScaler dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Exemple :

```
Add service http-service-2 3.3.3.1 http 80
```

Définir le profil réseau avec un serveur virtuel d'équilibrage de charge dans l'appliance NetScaler

À l'invite de commandes, tapez ce qui suit :

```
set lb vserver <vserver name> -netprofile <name>
```

Exemple :

```
set lb vserver lbvserver-2 -netprofile proxyProfile-3
```

Définir le profil réseau avec le service HTTP dans l'appliance NetScaler

À l'invite de commandes, tapez ce qui suit :

```
set service <service name> -netprofile <name>
```

Exemple :

```
set service http-service-2 -netprofile proxyProfile-4
```

Liez le serveur virtuel d'équilibrage de charge au service

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <vserver name> <service name>
```

Exemple :

```
bind lb vserver lbvserver-2 http-service-2
```


Configurer le protocole proxy pour l'opération de bande

Pour configurer le protocole proxy pour l'opération de dépouillement, vous devez activer le protocole proxy sur le serveur virtuel d'équilibrage de charge et désactiver le protocole proxy sur le service.

Ajouter un profil réseau avec le protocole proxy activé pour le serveur virtuel

À l'invite de commandes, tapez ce qui suit :

```
add netprofile <name> -proxyProtocol ENABLED> -proxyprotocoltxversion <V1/
V2>
```

Exemple :

```
add netprofile proxyprofile-5 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Ajouter un serveur virtuel d'équilibrage de charge ou de commutation de contenu pour l'appliance NetScaler dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Exemple :

```
add lb vserver lbvserver-3 http 2.2.2.2 80
```

Ajouter un service HTTP pour l'appliance NetScaler dans la couche proxy

À l'invite de commandes, tapez ce qui suit :

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Exemple :

```
Add service http-service-3 3.3.3.1 http 80
```

Définissez le profil réseau avec un serveur virtuel d'équilibrage de charge ou de commutation de contenu dans l'appliance NetScaler

À l'invite de commandes, tapez ce qui suit :

```
set lb vserver <vserver name> -netprofile <name>
```

Exemple :

```
set lb vserver lbvserver-3 -netprofile proxyProfile-5
```


Liez le serveur virtuel d'équilibrage de charge au service

À l'invite de commandes, tapez ce qui suit :

```
bind lb vserver <vserver name> <service name>
```

Exemple :

```
bind lb vserver lbvserver-3 http-service-3
```

Configurer l'expression de l'infrastructure de stratégie du répondeur pour le protocole proxy à l'aide de l'interface de ligne de commande

Pour configurer une stratégie de répondeur, à l'invite de commandes, tapez :

```
add responder policy <name> <expression> <action>
```

Exemple :

```
1 > add responder policy resppol_proxy_srcip "CLIENT.PROXY.SRCIP_STR.EQ("
     10.106.26.83")" RESET
2 Done
3 <!--NeedCopy-->
```

Pour lier la stratégie du répondeur au serveur virtuel d'équilibrage de charge, à l'invite de commande, tapez :

```
bind lb vserver <name> -policyname <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type <type>
```

Exemple :

```
1 > bind lb vserver lb_tcp1 -policyName resppol_proxy_srcip -priority 10
     -gotoPriorityExpression END -type REQUEST
2 Done
3 <!--NeedCopy-->
```

Exemple de configuration de bout en bout

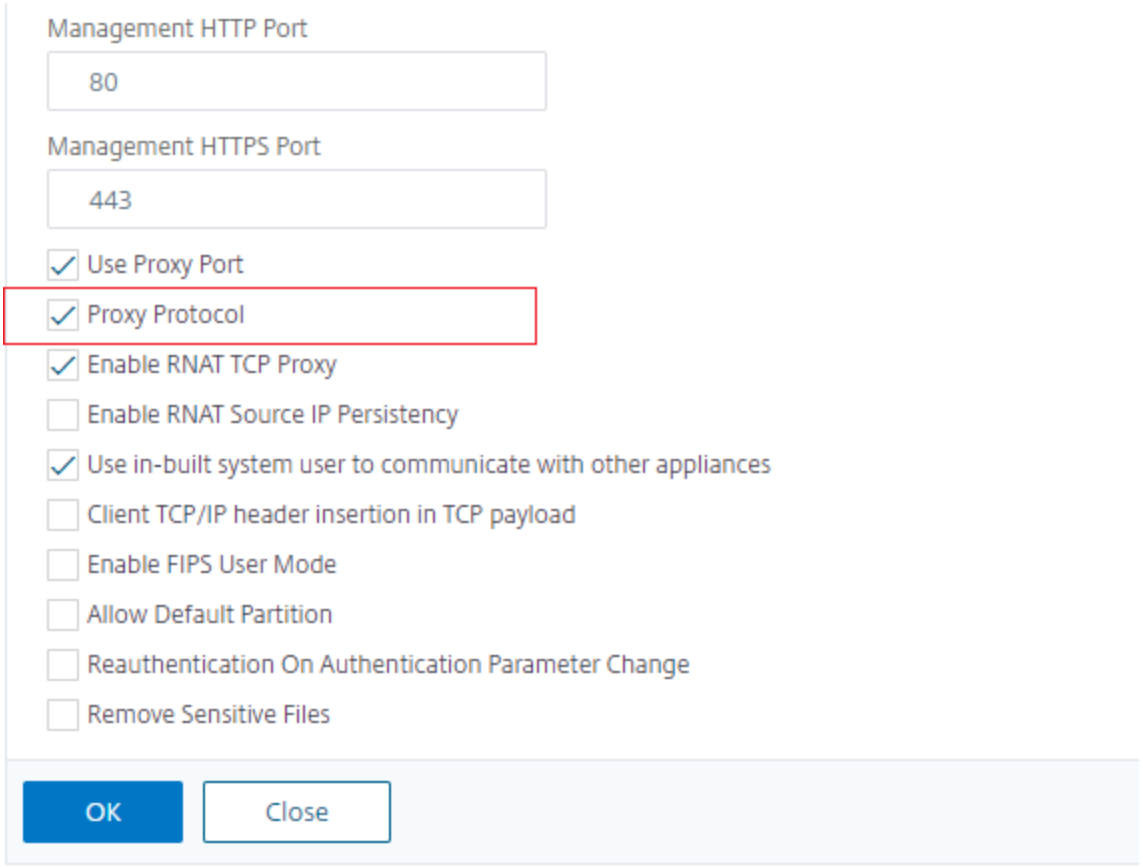
```
1 > add ns tcpProfile tcp-proxy-profile -tcpmode ENDPOINT
2
3 > add netprofile net_proxyv1 -MBF DISABLED -proxyProtocol
4 ENABLED
5
6 > enable ns mode l2
7
8 > enable ns mode l3 usnip
```



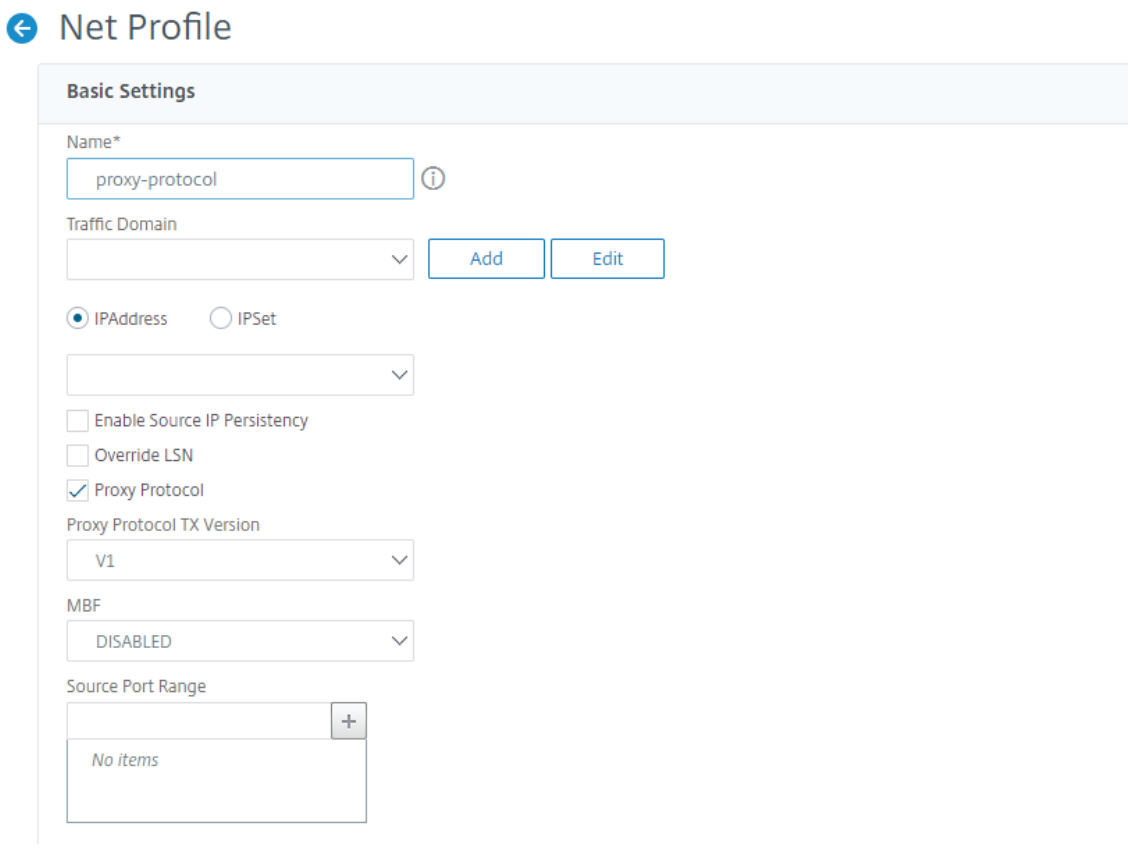
```
9
10 > add ns ip 10.106.26.146 255.255.255.0 -type SNIP
11 Done
12 > add ns ip 10.106.26.144 255.255.255.0 -type SNIP
13 Done
14
15 > add lb vserver lb_tcp1 TCP 10.106.26.141 80
16 > add service s1 10.106.26.82 TCP 8080
17
18 > bind lb vserver lb_tcp1 s1
19
20 > set lb vserver lb_tcp1 -tcpProfileName tcp_proxy -netProfile
      net_proxyv1
21
22 > set ns param -proxyProtocol ENABLED
23
24 > add responder policy resppol_proxy_srcip "CLIENT.PROXY.SRCIP_STR.EQ("
      10.106.26.83")" RESET
25
26 > bind lb vserver lb_tcp1 -policyName resppol_proxy_srcip -priority 10
      -gotoPriorityExpression END -type REQUEST
27 Done
28 <!--NeedCopy-->
```

Configurer le protocole proxy à l'aide de l'interface graphique NetScaler

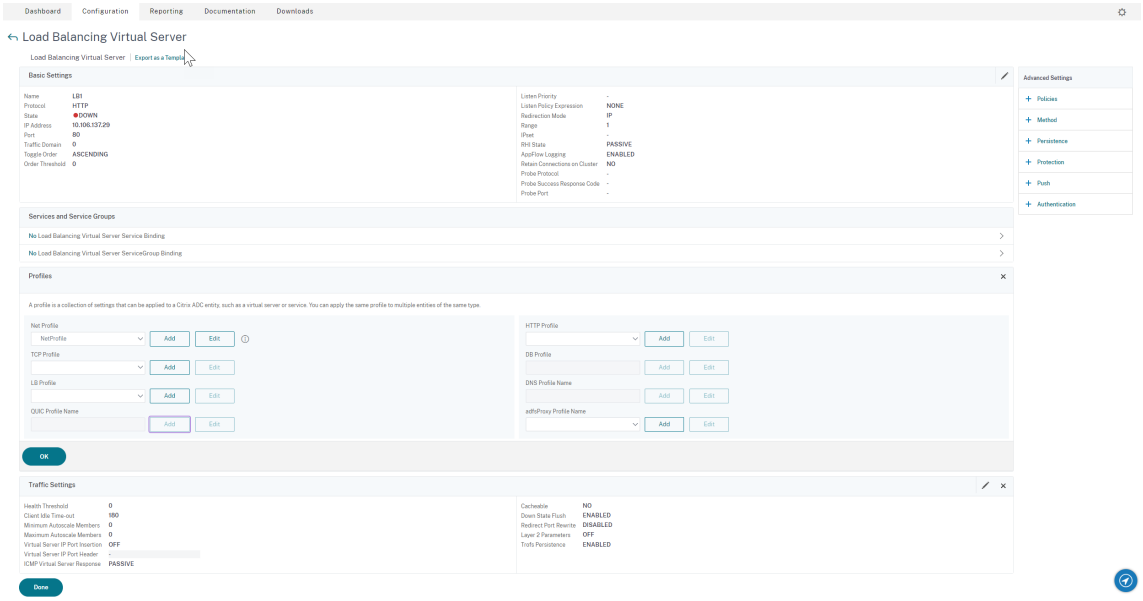
1. Accédez à **Système** > **Paramètres** > **Modifier les paramètres système globaux**.
2. Dans la page **Configurer les paramètres globaux du système**, activez la case à cocher **Protocole proxy** .
3. Cliquez sur **OK** et sur **Fermer**.



4. Accédez à **Système** > **Réseau** > **Profils réseau**.
5. Dans le volet d'informations, cliquez sur **Ajouter** pour créer un profil réseau pour le serveur virtuel d'équilibrage de charge.
6. Dans la page **Profil réseau**, définissez les paramètres suivants :
   a) **Nom** : nom du profil réseau.
   b) **Protocole proxy** : activez ou désactivez le protocole proxy pour le serveur virtuel d'équilibrage de charge.
   c) **Version TX du protocole proxy** : définissez la version du protocole proxy sur V1 ou V2 en fonction du format des données entrantes.
7. Cliquez sur **OK**.

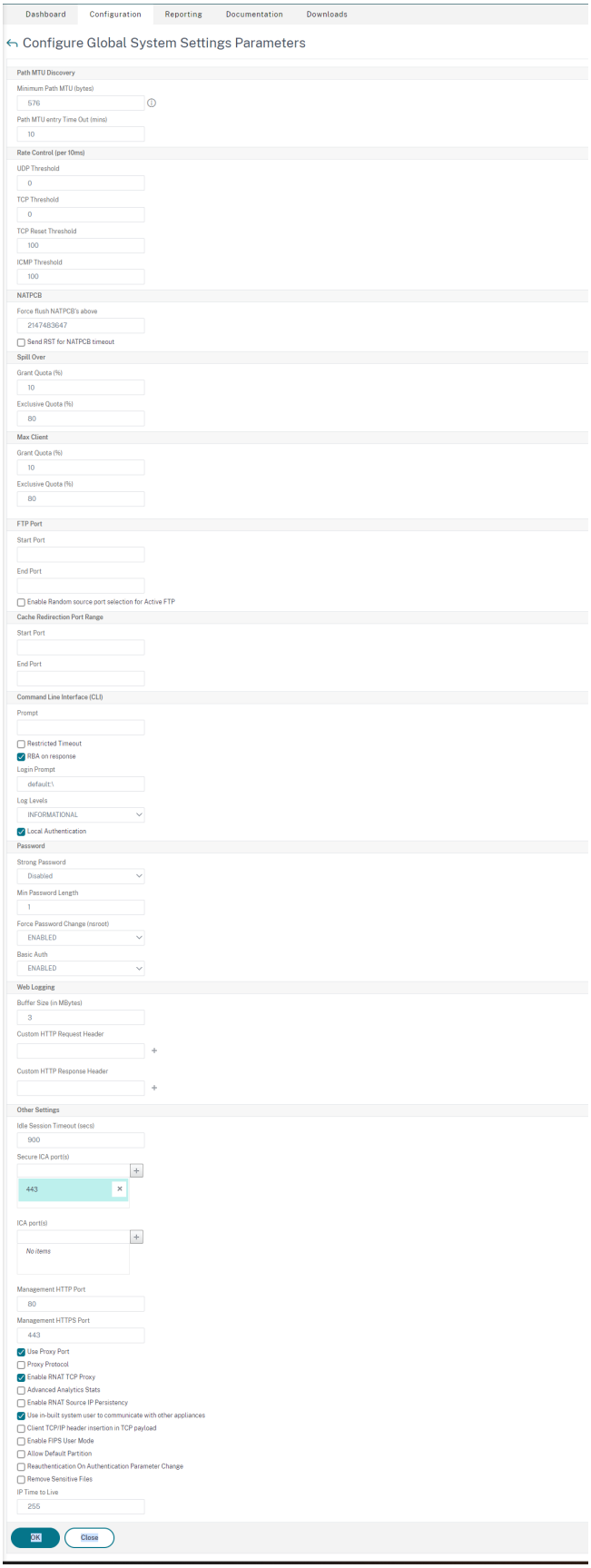


8. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**.
9. Dans le volet de détails, cliquez sur **Ajouter**.
10. Dans la page **Serveur virtuel d'équilibrage de charge**, définissez les paramètres de base.
11. Dans la section **Paramètres avancés**, sélectionnez **Profils**.
12. Dans la section **Profils**, cliquez sur l'icône en forme de crayon.
13. Sélectionnez un profil réseau, puis cliquez sur **OK**.
14. Cliquez sur **Terminé**.



15. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Services**.
16. Dans le volet de détails, cliquez sur **Ajouter**.
17. Dans la page **Service d'équilibrage de charge**, définissez les paramètres de base.
18. Dans la section **Paramètres avancés**, sélectionnez **Profils**.
19. Dans la section **Profils**, cliquez sur l'icône en forme de crayon.
20. Sélectionnez un profil réseau, puis cliquez sur **OK**.
21. Cliquez sur **Terminé**.

> **Remarque :**
>
> Si plusieurs appliances NetScaler font partie de la couche proxy, vous devez définir la configuration du protocole proxy sur chaque appliance pour l'opération Forward.



Adresse IP du client dans l'option TCP

May 5, 2023

L'appliance NetScaler utilise de nombreuses méthodes pour envoyer les informations du client au serveur principal. L'une de ces méthodes consiste à envoyer l'adresse IP du client dans l'option TCP. L'appliance utilise le numéro d'option TCP dans le profil TCP, si le serveur principal utilise l'option TCP pour lire l'adresse IP du client.

L'appliance NetScaler envoie l'adresse IP du client, dans l'en-tête de l'option TCP, uniquement dans les paquets suivants :

- paquet ACK final de la poignée de mains à trois
- un premier paquet de données.

Vous trouverez ci-dessous certains des scénarios d'utilisation de la configuration des options TCP dans une appliance NetScaler.

- Adresse IP du client d'origine
- Sélection d'une langue pour un site Web
- Bloquer la liste des adresses IP sélectionnées

Voici les deux modes de fonctionnement pour envoyer l'adresse IP du client dans l'option TCP :

- **Insérer**. En mode insertion, l'appliance ajoute les détails du client dans le champ de l'option TCP 28 (configurable mais la valeur préférable est 28) et les envoie au serveur principal.
- **Avancer**. En mode avant, le serveur virtuel reçoit les détails IP du client dans l'option TCP d'un périphérique proxy. Pour le serveur virtuel, vous devez configurer la même option TCP que celle utilisée par le périphérique proxy pour envoyer les détails IP du client.

  L'appliance envoie ensuite les détails du client dans le champ d'option TCP au serveur principal. Pour le service représentant le serveur principal, vous pouvez définir n'importe quelle option TCP, mais la valeur préférable est 28.

L'appliance NetScaler prend également en charge l'envoi du port client dans l'option TCP pour la configuration du mode insertion.

> **Remarques :**
>
> - Le multiplexage n'est pas pris en charge pour le trafic reçu sur un serveur virtuel si l'option TCP IP client est activée sur le profil TCP lié.
> - Pour un serveur virtuel TCP ou HTTP, le numéro d'option TCP est transféré avec ou sans cette fonctionnalité activée en mode transparent.

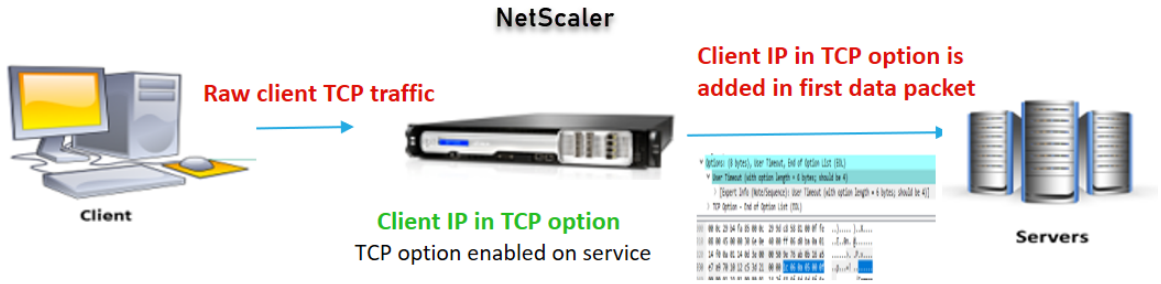
Limitations

La fonctionnalité de configuration de l'option TCP n'est pas prise en charge dans les fonctionnalités TFO, TCP MultiPath et HTTP2.

Comment configurer les options TCP dans une appliance NetScaler

Les organigrammes suivants montrent comment configurer l'option TCP dans les appliances NetScaler pour les opérations d'insertion et de transfert.

Opération d'insertion :

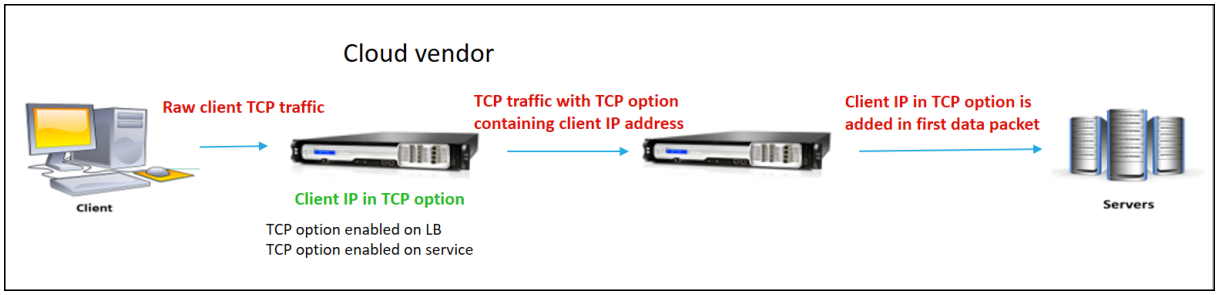


L'interaction des composants est la suivante :

- Un client envoie une demande à NetScaler.
- Lors de l'opération d'insertion, l'appliance NetScaler insère l'adresse IP et le port du client dans l'option TCP configurée des paquets suivants vers le serveur principal.
  - paquet ACK final de la poignée de mains à trois
  - premier paquet de données

> **Remarque :**
>
> Si le trafic entrant est HTTPS, l'adresse IP du client et le port client de l'option TCP sont envoyés dans le message Hello du client SSL, qui est le premier paquet de données au niveau TCP.

Fonctionnement vers l'avant :



L'interaction des composants est la suivante :

- Un client envoie une requête HTTP/HTTPS à l'appliance NetScaler.
- Pour l'opération Forward, l'option TCP est activée sur un serveur virtuel d'équilibrage de charge ou un serveur virtuel de commutation de contenu et également activée sur le service. L'appliance reçoit les détails du client dans le numéro d'option TCP spécifié sur le serveur virtuel.
- L'appliance NetScaler insère ensuite l'adresse IP et le port du client dans l'option TCP configurée (pour le service) des paquets suivants sur le serveur principal.
  - paquet ACK final de la poignée de mains à trois
  - premier paquet de données

Configurer l'option TCP pour l'opération Insert

La configuration de l'option TCP pour l'opération d'insertion comprend les étapes suivantes :

1. Configurez un profil TCP. Activez l'option TCP IP client (`clientIpTcpOption`) et spécifiez le numéro d'option TCP (`clientIpTcpOptionNumber`). Vous pouvez également activer `sendClientPortInTcpOption` pour envoyer le port client dans l'en-tête de l'option TCP.

   > **Remarque :**
   >
   > Citrix recommande de configurer le numéro d'option TCP sur 28 dans le profil TCP.

2. Liez le profil TCP à un service

Pour configurer un profil TCP à l'aide de la CLI :

À l'invite de commande, tapez :

- `add tcpprofile <name> -clientIpTcpOption (ENABLED | DISABLED)-clientIpTcpOptionNu <positive_integer> -sendClientPortInTcpOption (ENABLED | DISABLED)`
- `show tcpprofile <name>`

Pour lier le profil TCP au service à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `set service <name> -tcpprofileName <name>`
- `show service <name>`

Exemple de configuration

```
1 add tcpprofile TCP-PROFILE-1 -clientIpTcpOption ENABLED -
     clientIpTcpOptionNumber 28 -sendClientPortInTcpOption ENABLED
2 set service SERVICE-1  - tcpprofileName TCP-PROFILE-1
```



```
<!--NeedCopy-->
```

Configurer l'option TCP pour l'opération Forward

La configuration de l'option TCP pour l'opération de transfert comprend les étapes suivantes :

1. Configurez un profil TCP. Activez l'option TCP IP client (`clientIpTcpOption`) et spécifiez le numéro d'option TCP (`clientIpTcpOptionNumber`).
2. Liez le profil TCP à un serveur virtuel d'équilibrage de charge ou de commutation de contenu
3. Liez le profil TCP aux services.

Pour configurer un profil TCP à l'aide de la CLI :

À l'invite de commande, tapez :

- `add tcpprofile <name> -clientIpTcpOption (ENABLED | DISABLED)-clientIpTcpOptionNu <positive_integer>`
- `show tcpprofile <name>`

Pour lier le profil TCP à un serveur virtuel d'équilibrage de charge ou de commutation de contenu à l'aide de la CLI :

À l'invite de commande, tapez :

- `set lb vserver <name> -tcpprofileName <name>`
- `show lb vserver <name>`

Pour lier le profil TCP au service à l'aide de la CLI :

À l'invite de commande, tapez :

- `set service <name> -tcpprofileName p1`
- `show service <name>`

Exemple de configuration

```
add tcpprofile TCP-PROFILE-2 -clientIpTcpOption ENABLED -
   clientIpTcpOptionNumber 29
set lb vserver LBVS-2  - tcpprofileName TCP-PROFILE-2
set service SERVICE-2 -tcpprofileName TCP-PROFILE-2
<!--NeedCopy-->
```

Configurer l'option TCP à l'aide de l'interface graphique NetScaler

1. Accédez à **Système** > **Profils**.

2. Dans l'onglet **Profil TCP**, cliquez sur **Ajouter**.
3. Sur la page **Configurer le profil TCP**, configurez les paramètres suivants :
   - **clientIptcpoption**. Active l'option TCP pour envoyer ou recevoir l'adresse IP du client.
   - **numéro d'option iptcpclient**. Définit le numéro d'option TCP.
   - **SendClientPortIntcpOption** Envoie le port client dans l'option TCP pour la configuration du mode d'insertion.
4. Cliquez sur **OK** et sur **Fermer**.

SNMP

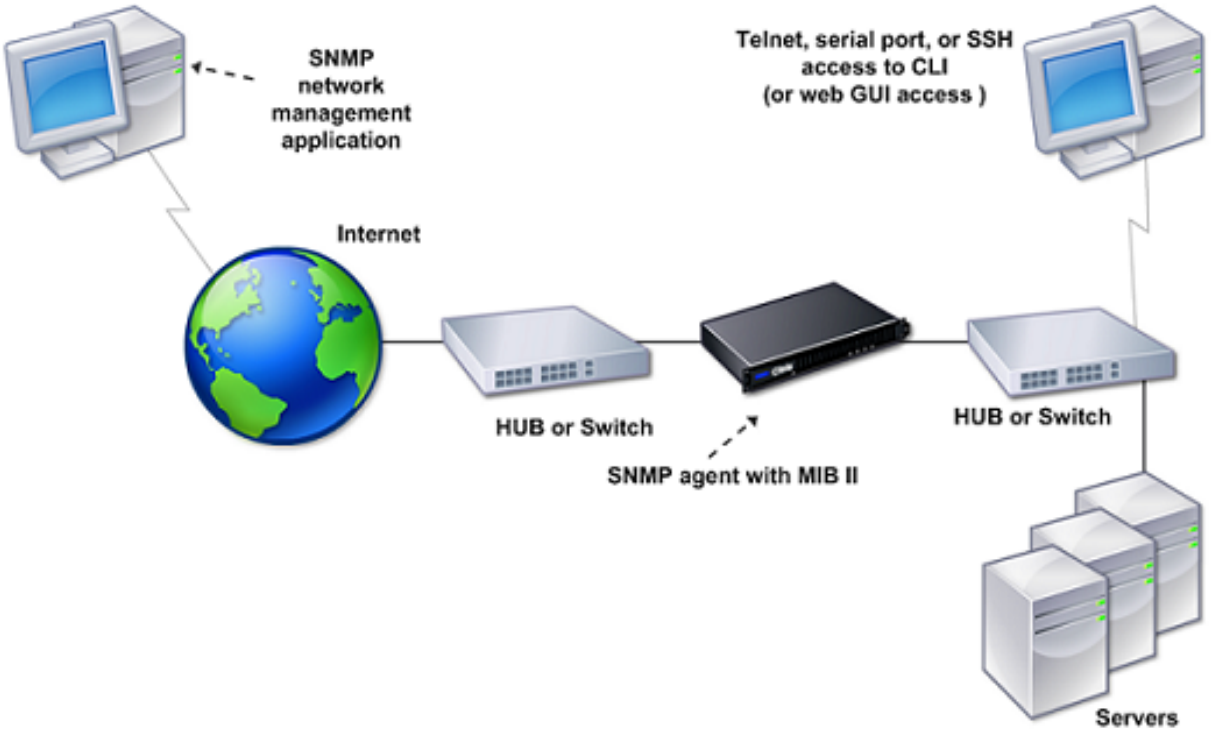
May 5, 2023

Vous pouvez utiliser le protocole SNMP (Simple Network Management Protocol) pour configurer l'agent SNMP sur l'appliance NetScaler afin de générer des événements asynchrones, appelés pièges. Les pièges sont générés chaque fois que des conditions anormales apparaissent sur NetScaler. Les interruptions sont ensuite envoyées à un appareil distant appelé *écouteur d'interruptions*, qui signale l'état anormal de l'appliance NetScaler. *Vous pouvez également demander à l'agent SNMP des informations spécifiques au système à partir d'un périphérique distant appelé gestionnaire SNMP.* L'agent recherche ensuite les données demandées dans la base d'informations de gestion (MIB) et les envoie au gestionnaire SNMP.

L'agent SNMP du NetScaler peut générer des pièges conformes à SNMPv1, SNMPv2 et SNMPv3. Pour l'interrogation, l'agent SNMP prend en charge SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2) et SNMP version 3 (SNMPv3).

Pour plus d'informations sur les paramètres SNMP, les interruptions et leurs descriptions, consultez NetScaler SNMPOID Reference.

La figure suivante illustre un réseau avec un NetScaler sur lequel SNMP est activé et configuré. Dans la figure, chaque application de gestion de réseau SNMP utilise le protocole SNMP pour communiquer avec l'agent SNMP sur NetScaler. L'agent SNMP recherche sa base d'informations de gestion (MIB) pour collecter les données demandées par le gestionnaire SNMP et fournit les informations à l'application.



Important

Le module SNMP d'une appliance NetScaler prend en charge une longueur maximale de 128 octets (conformément à la RFC 3416) pour un OID SNMP. Un nom de variable d'index long pour un objet peut entraîner un OID SNMP de plus de 128 octets.

Pour résoudre ce problème, le module SNMP de NetScaler prend en charge une longueur maximale de 31 caractères pour un nom de variable d'index. Si le nom d'une variable d'index dépasse 31 caractères, le module SNMP utilisant un algorithme de hachage convertit le nom en une valeur de hachage de 31 caractères. Cette valeur hachée est utilisée dans l'OID SNMP pour cette variable.

Le nom de la variable d'index d'origine est stocké dans une autre variable, dont le format de nom est le suivant : `<variable type>FullName`. Par exemple, lorsque le nom d'un serveur virtuel d'équilibrage de charge comporte plus de 31 caractères, l'OID `vserverName` SNMP contient la valeur hachée et `vsvrFullName` SNMP OID contient le nom complet (d'origine) du serveur virtuel.

De même, pour les interruptions SNMP, la variable d'index affiche une valeur hachée. `<variable type>FullName`, qui stocke le nom complet du nom de la variable d'index d'origine, fait également partie des messages d'interruption.

Importation de fichiers MIB dans le gestionnaire SNMP et l'écouteur d'interruption

Pour surveiller une appliance NetScaler, vous devez télécharger les fichiers de définition d'objet MIB. L'appliance NetScaler prend en charge les MIB spécifiques à l'entreprise suivants :

- **Un sous-ensemble de groupes MIB-2 standard**. Fournit les groupes MIB-2 SYSTEM, IF, ICMP, UDP et SNMP.
- **Un MIB d'entreprise système**. Fournit une configuration et des statistiques spécifiques au système.

Vous pouvez obtenir les fichiers de définition d'objet MIB à partir du répertoire /netscaler/snmp ou de l'onglet Téléchargements de l'interface graphique.

Configuration de NetScaler pour générer des interruptions SNMP

May 5, 2023

Vous pouvez configurer l'appliance NetScaler pour générer des événements asynchrones, appelés pièges. Les pièges sont générés chaque fois que des conditions anormales se produisent sur l'appareil. Les interruptions sont envoyées à un périphérique distant appelé *écouteur d'interruptions*. Il aide les administrateurs à surveiller l'appliance et à réagir rapidement à tous les problèmes.

L'appliance NetScaler fournit un ensemble d'entités conditionnelles appelées alarmes *SNMP*. Lorsque la condition d'une alarme SNMP est remplie, l'appliance génère des messages d'interruption SNMP qui sont envoyés aux récepteurs d'interruption configurés. Par exemple, lorsque l'alarme LOGIN-FAILURE est activée, un message d'interruption est généré et envoyé à l'écouteur d'interruptions chaque fois qu'un échec de connexion se produit sur l'appliance.

Pour configurer l'appliance NetScaler afin de générer des interruptions, vous devez activer et configurer les alarmes. Ensuite, vous spécifiez les écouteurs de piège auxquels l'appliance envoie les messages d'interruption générés.

Activation d'une alarme SNMP

L'appliance NetScaler génère des interruptions uniquement pour les alarmes SNMP activées. Certaines alarmes sont activées par défaut, mais vous pouvez les désactiver.

Lorsque vous activez une alarme SNMP, l'appliance génère des messages d'interruption correspondants lorsque certains événements se produisent. Certaines alarmes sont activées par défaut.

Pour activer une alarme SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `enable snmp alarm <trapName>`
- `show snmp alarm <trapName>`

Pour activer une alarme SNMP à l'aide de l'interface graphique

1. Accédez à **Système > SNMP > Alarmes**, puis sélectionnez l'alarme.
2. Cliquez sur **Actions** et sélectionnez **Activer**.

Configuration des alarmes

L'appliance NetScaler fournit un ensemble d'entités conditionnelles appelées alarmes *SNMP*. Lorsque la condition définie pour une alarme SNMP est remplie, l'appliance génère des messages d'interruption SNMP qui sont envoyés aux récepteurs d'interruptions configurés. Par exemple, lorsque l'alarme LOGIN-FAILURE est activée, un message d'interruption est généré et envoyé à l'écouteur d'interruptions chaque fois qu'un échec de connexion se produit sur l'appliance.

Vous pouvez attribuer une alarme SNMP avec un niveau de gravité. Lorsque vous effectuez cette opération, ce niveau de gravité est attribué aux messages d'interception correspondants.

Les niveaux de gravité suivants sont définis sur l'appliance, par ordre de gravité décroissant.

- Critical
- Major
- Mineur
- Avertissement
- Informationnel

Par exemple, si vous définissez un niveau de gravité d'avertissement pour l'alarme SNMP nommé LOGIN-FAILURE, les messages d'interruption générés en cas d'échec de connexion sont affectés au niveau de gravité de l'avertissement.

> **Remarque**
>
> NetScaler prend en charge diverses alarmes SNMP. Pour plus d'informations, voir Alarmes SNMP.

Vous pouvez également configurer une alarme SNMP pour consigner les messages d'interruption correspondants générés chaque fois que la condition de cette alarme est remplie.

Pour configurer une alarme SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer une alarme SNMP et vérifier la configuration :

- `set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]`
- `show snmp alarm <trapName>`

Où,

ThresholdValue : valeur du seuil supérieur. L'appliance NetScaler génère un message d'interruption SNMP lorsque la valeur de l'attribut associé à l'alarme est supérieure ou égale à la valeur de seuil haut spécifiée.

NormalValue : valeur du seuil normal. Un message d'interruption est généré si la valeur de l'attribut concerné tombe à une valeur inférieure ou égale à cette valeur après avoir dépassé le seuil supérieur.

Pour configurer les alarmes SNMP à l'aide de l'interface graphique

Accédez à **Système > SNMP > Alarmes**, sélectionnez une alarme et configurez les paramètres de l'alarme.

Configuration des interruptions SNMPv1 ou SNMPv2

Après avoir configuré les alarmes, vous devez spécifier l'écouteur d'interruptions auquel l'appliance envoie les messages d'interruption. Outre la spécification de paramètres tels que l'adresse IP ou IPv6 et le port de destination de l'écouteur d'interruptions, vous pouvez spécifier le type d'interruption (générique ou spécifique) et la version SNMP.

Vous pouvez configurer un maximum de 20 récepteurs d'interruptions pour recevoir des pièges génériques ou spécifiques.

Vous pouvez également configurer l'appliance pour envoyer des messages d'interruption SNMP avec une adresse IP source autre que l'adresse IP NetScaler (NSIP ou NSIP6) à un écouteur d'interruptions particulier. Pour un écouteur d'interruption doté d'une adresse IPv4, vous pouvez définir l'adresse IP source sur une adresse IP mappée (MIP) ou une adresse IP de sous-réseau (SNIP) configurée sur l'appliance. Pour un écouteur de piège doté d'une adresse IPv6, vous pouvez définir l'adresse IP source sur une adresse IPv6 de sous-réseau (SNIP6) configurée sur l'appliance.

Vous pouvez également configurer l'appliance pour qu'elle envoie des messages d'interruption à un écouteur de piège basé sur un niveau de gravité. Par exemple, si vous définissez le niveau de gravité Mineure pour un écouteur d'interruption, tous les messages d'interruption dont le niveau de gravité est égal ou supérieur à Mineure (Mineure, Major et Critique) sont envoyés à l'écouteur d'interruption.

Si vous avez défini une chaîne communautaire pour l'écouteur d'interruptions, vous devez également spécifier une chaîne de communauté pour chaque interruption qui doit être envoyée à l'écouteur. Un écouteur d'interruptions pour lequel une chaîne communautaire a été définie accepte uniquement les messages d'interception qui incluent une chaîne communautaire correspondant à la chaîne de communauté définie dans l'écouteur d'interruptions. D'autres messages d'interruptions sont supprimés.

Pour ajouter une interruption SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 )- destPort <port> -communityName <string> -srcIP <ip_addr> -severity < severity>`
- `show snmp trap`

Exemple :

```
1 > `add snmp trap specific 192.0.2.10 -version V2 -destPort 162 -
     communityName com1 -severity Major`
2 <!--NeedCopy-->
```

Pour configurer les interruptions SNMP à l'aide de l'interface graphique

Accédez à **Système > SNMP > Pièges**et créez l'interruption SNMP.

Configuration des pièges SNMPv3

SNMPv3 fournit des fonctionnalités de sécurité telles que l'authentification et le chiffrement à l'aide des informations d'identification des utilisateurs SNMP. Un gestionnaire SNMP ne peut recevoir des messages d'interruption SNMPv3 que si sa configuration inclut le mot de passe attribué à l'utilisateur SNMP.

La destination d'interruption peut désormais recevoir des messages d'interruption SNMPv1, SNMPv2 et SNMPv3.

Pour configurer une interruption SNMPv3 à l'aide de l'interface de ligne de commande

À l'invite de commandes, procédez comme suit :

1. Ajoutez une interruption SNMPv3.


```
add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 | V3)
-destPort <port> -communityName <string> -srcIP <ip_addr> -severity <
severity>
```

> **Remarque**
>
> Une fois définie, la version de l'interruption SNMP ne peut pas être modifiée.

Exemple

```
1 > add snmp trap specific 192.0.2.10 -version V3 -destPort 162 -
     communityName com1 -severity Major
2 <!--NeedCopy-->
```

2. Ajoutez un utilisateur SNMP.

   ```
   add snmp user <name> -group <string> [ -authType ( MD5 | SHA ){ -
   authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]
   ```

   Exemple

   ```
   1 > add snmp user edocs_user -group edocs_group
   2 <!--NeedCopy-->
   ```

3. Liez l'interruption SNMPv3 à l'utilisateur SNMP.

```
bind snmp trap <trapClass> <trapDestination> [-version <version>] (-userName
 <string> [-securityLevel <securityLevel>])
```

Exemple

```
1     > bind snmp trap specific 192.0.2.10 -version V3 -userName
         edocs_user -securityLevel authPriv
2 <!--NeedCopy-->
```

Pour configurer un piège SNMPv3 à l'aide de l'interface graphique

1. Ajoutez une interruption SNMPv3.

   Accédez à **Système > SNMP > Pièges**et créez l'interruption SNMP en sélectionnant V3 comme version SNMP.

2. Ajoutez un utilisateur SNMP.

   Accédez à **Système > SNMP > Utilisateurs** et créez l'utilisateur SNMP.

3. Liez l'interruption SNMPv3 à l'utilisateur SNMP.

   - Accédez à **Système > SNMP > Pièges**, puis sélectionnez l'interruption SNMP version 3.

- Sélectionnez l'utilisateur auquel le piège doit être lié et définissez le niveau de sécurité approprié.

Journalisation des interruptions SNMP

Une appliance NetScaler peut enregistrer les messages d'interruption SNMP (pour les alarmes SNMP pour lesquelles la fonctionnalité de journalisation est activée) lorsque vous activez l'option de journalisation des interruptions SNMP et qu'au moins un écouteur d'interruptions est configuré sur l'appliance. Vous pouvez désormais spécifier le niveau du journal d'audit des messages d'interruption envoyés à un serveur de journaux externe. Le niveau de journalisation par défaut est Informatif. Les valeurs possibles sont Emergency, Alert, Critical, Error, Warning, Debug et Notice.

Par exemple, vous pouvez définir le niveau du journal d'audit sur Critique pour un message d'interruption SNMP généré par un échec de connexion. Ces informations sont ensuite disponibles sur le serveur NSLOG ou SYSLOG pour le dépannage.

Pour activer la journalisation des interruptions SNMP et configurer le niveau du journal des interruptions à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer la journalisation des interruptions SNMP et vérifier la configuration :

- `set snmp option [-snmpTrapLogging (ENABLED | DISABLED)][-snmpTrapLoggingLevel <snmpTrapLoggingLevel>]`
- `show snmp option`

Pour activer la journalisation des interruptions SNMP et configurer le niveau du journal des interruptions SNMP à l'aide de l'interface graphique

Accédez à **Système > SNMP**, cliquez sur Modifier les options SNMP et définissez les paramètres suivants :

1. Enregistrement des interruptions SNMP : activez cette case à cocher pour activer la journalisation des interruptions SNMP lorsqu'au moins un écouteur d'interruptions est configuré sur l'appliance.
2. Niveau de journalisation des interruptions SNMP : sélectionnez un niveau de journal d'audit pour l'interruptions SNMP. Par défaut, le niveau d'audit d'une interruption SNMP est défini sur « Informationnel ». «

Configuration de NetScaler pour les requêtes SNMP v1 et v2

May 5, 2023

Vous pouvez demander à l'agent SNMP NetScaler des informations spécifiques au système à partir d'un appareil distant appelé gestionnaires SNMP. L'agent recherche ensuite les données demandées dans la base d'informations de gestion (MIB) et les envoie au gestionnaire SNMP.

Les types de requêtes SNMP v1 et v2 suivants sont pris en charge par l'agent SNMP :

- GET
- PASSER À LA SUIVANTE
- ALL
- OBTENIR DU VRAC

Vous pouvez créer des chaînes appelées chaînes de communauté et associer chacune d'entre elles à des types de requêtes. Vous pouvez associer une ou plusieurs chaînes de communauté à chaque type de requête. Les chaînes communautaires sont des mots de passe utilisés pour authentifier les requêtes SNMP provenant des gestionnaires SNMP.

Par exemple, si vous associez deux chaînes de communauté, telles que **abc** et **bcd**, au type de requête GET NEXT, l'agent SNMP de l'appliance NetScaler considère uniquement les paquets de requête SNMP GET NEXT qui contiennent **abc** ou **bcd** comme chaîne de communauté.

Spécification d'un gestionnaire SNMP

Vous devez configurer l'appliance NetScaler pour permettre aux gestionnaires SNMP appropriés de l'interroger. Vous devez également fournir au gestionnaire SNMP les informations spécifiques à NetScaler requises. Vous pouvez ajouter jusqu'à 100 gestionnaires ou réseaux SNMP.

Pour un gestionnaire SNMP IPv4, vous pouvez spécifier un nom d'hôte au lieu de l'adresse IP du gestionnaire. Dans ce cas, vous devez ajouter un serveur de noms DNS qui résout le nom d'hôte du gestionnaire SNMP en son adresse IP. Vous pouvez ajouter jusqu'à cinq gestionnaires SNMP basés sur le nom d'hôte.

> **Remarque** :
> L'appliance ne prend pas en charge l'utilisation de noms d'hôtes pour les gestionnaires SNMP dotés d'adresses IPv6. Vous devez spécifier l'adresse IPv6.

Si vous ne configurez pas au moins un gestionnaire SNMP, l'appliance accepte et répond aux requêtes SNMP provenant de toutes les adresses IP du réseau. Si vous configurez un ou plusieurs gestionnaires SNMP, l'appliance accepte et répond uniquement aux requêtes SNMP provenant de ces adresses IP spécifiques.

Si vous supprimez un gestionnaire SNMP de la configuration, ce gestionnaire ne peut plus interroger l'appliance.

Pour ajouter des gestionnaires SNMP en spécifiant des adresses IP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp manager <IPAddress> ... [-netmask <netmask>]`
- `show snmp manager`

Exemple

```
> add snmp manager 10.102.29.10 10.102.29.15 10.102.29.30
```

Pour ajouter un gestionnaire SNMP en spécifiant son nom d'hôte à l'aide de l'interface de ligne de commande

Important : si vous spécifiez le nom d'hôte du gestionnaire SNMP au lieu de son adresse IP, vous devez configurer un serveur de noms DNS pour résoudre le nom d'hôte en adresse IP du gestionnaire SNMP. Pour plus d'informations, voir « Ajout d'un serveur de noms ». «

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp manager <IPAddress> [-domainResolveRetry ****<integer>]`
- `show snmp manager`

Exemple

```
add nameserver 10.103.128.15
add snmp manager engwiki.eng.example.net -domainResolveRetry 10
```

Pour ajouter un gestionnaire SNMP à l'aide de l'interface graphique

1. Accédez à **Système** > **SNMP** > **Gestionnaires**, puis créez le gestionnaire SNMP.

   > **Important** :
   >
   > Si vous spécifiez le nom d'hôte du gestionnaire SNMP au lieu de son adresse IPv4, vous devez configurer un serveur de noms DNS pour convertir le nom d'hôte en adresse IP du gestionnaire SNMP.

> **Remarque** :
> L'appliance ne prend pas en charge les noms d'hôtes pour les gestionnaires SNMP dotés d'adresses IPv6.

Spécifier une communauté SNMP

Vous pouvez créer des chaînes appelées chaînes de communauté et les associer aux types de requêtes SNMP suivants sur l'appliance :

- GET
- PASSER À LA SUIVANTE
- ALL
- OBTENIR DU VRAC

Vous pouvez associer une ou plusieurs chaînes de communauté à chaque type de requête. Par exemple, lorsque vous associez deux chaînes de communauté, telles que **abc** et **bcd**, au type de requête GET NEXT, l'agent SNMP de l'appliance considère uniquement les paquets de requête SNMP GET NEXT contenant **abc** ou **bcd** comme chaîne de communauté.

Si vous n'associez aucune chaîne de communauté à un type de requête, l'agent SNMP répond à toutes les requêtes SNMP de ce type.

Pour spécifier une communauté SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp community <communityName> <permissions>`
- `show snmp community`

Exemple

```
> add snmp community com all
```

Pour configurer une chaîne de communauté SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Communauté**, puis créez la communauté SNMP.

Configuration de NetScaler pour les requêtes SNMPv3

May 5, 2023

Simple Network Management Protocol Version 3 (SNMPv3) est basé sur la structure et l'architecture de base de SNMPv1 et SNMPv2. Cependant, SNMPv3 améliore l'architecture de base pour intégrer des fonctionnalités d'administration et de sécurité, telles que l'authentification, le contrôle d'accès, la vérification de l'intégrité des données, la vérification de l'origine des données, la vérification de l'actualité des messages et la confidentialité des données.

Pour mettre en œuvre la sécurité et le contrôle d'accès au niveau des messages, SNMPv3 introduit le modèle de sécurité basé sur l'utilisateur (USM) et le modèle de contrôle d'accès basé sur la vue (VACM).

- **Modèle de sécurité basé sur l'utilisateur.** Le modèle de sécurité basé sur l'utilisateur (USM) fournit une sécurité au niveau des messages. Il vous permet de configurer les utilisateurs et les paramètres de sécurité pour l'agent SNMP et le gestionnaire SNMP. USM propose les fonctionnalités suivantes :
  - **Intégrité des données :** pour protéger les messages contre toute modification lors de leur transmission sur le réseau.
  - **Vérification de l'origine des données :** pour authentifier l'utilisateur qui a envoyé la demande de message.
  - **Actualité des messages :** pour éviter les retards ou les rediffusions des messages.
  - **Confidentialité des données :** pour empêcher que le contenu des messages ne soit divulgué à des entités ou à des personnes non autorisées.
- **Modèle de contrôle d'accès basé sur la vue.** Le modèle de contrôle d'accès basé sur les vues (VACM) vous permet de configurer les droits d'accès à une sous-arborescence spécifique de la MIB en fonction de divers paramètres, tels que le niveau de sécurité, le modèle de sécurité, le nom d'utilisateur et le type de vue. Il vous permet de configurer les agents pour fournir différents niveaux d'accès à la MIB à différents gestionnaires.

NetScaler prend en charge les entités suivantes qui vous permettent d'implémenter les fonctionnalités de sécurité de SNMPv3 :

- Moteurs SNMP
- Vues SNMP
- Groupes SNMP
- Utilisateurs SNMP

Ces entités fonctionnent ensemble pour implémenter les fonctionnalités de sécurité SNMPv3. Les vues sont créées pour permettre l'accès aux sous-arborescences de la MIB. Des groupes sont ensuite créés avec le niveau de sécurité requis et un accès aux vues définies. Enfin, les utilisateurs sont créés et affectés aux groupes.

> **Remarque** :
>
> La configuration de la vue, du groupe et de l'utilisateur est synchronisée et propagée vers le nœud secondaire dans une paire haute disponibilité (HA). Toutefois, l'ID du moteur n'est ni

> propagé ni synchronisé car il est unique à chaque appliance NetScaler.

Pour implémenter l'authentification des messages et le contrôle d'accès, vous devez procéder comme suit :

Configuration de l'ID du moteur

Les moteurs SNMP sont des fournisseurs de services qui résident dans l'agent SNMP. Ils fournissent des services tels que l'envoi, la réception et l'authentification de messages. Les moteurs SNMP sont identifiés de manière unique à l'aide des identifiants du moteur.

L'appliance NetScaler possède un EngineID unique basé sur l'adresse MAC de l'une de ses interfaces. Il n'est pas nécessaire de remplacer le EngineID. Toutefois, si vous souhaitez modifier l'ID du moteur, vous pouvez le réinitialiser.

Pour définir l'ID du moteur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `set snmp engineId <engineID>`
- `show snmp engineId`

Exemple

```
> set snmp engineId 8000173f0300c095f80c68
```

Pour définir l'ID du moteur à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Utilisateurs**, cliquez sur **Configurer l'ID du moteur** et saisissez un ID du moteur.

Configuration d'une vue

Les vues SNMP limitent l'accès des utilisateurs à des parties spécifiques de la MIB. Les vues SNMP sont utilisées pour implémenter le contrôle d'accès.

Pour ajouter une vue SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp view <name> <subtree> -type ( included | excluded )`

- `show snmp view <name>`
- `rm snmp view <name> <subtree>`

Où,

Nom. Nom de la vue SNMPv3. Il peut être composé de 1 à 31 caractères, dont des lettres majuscules et minuscules, des chiffres, ainsi que le tiret (-), le point (.), la livre (#), l'espace (), le signe arobase (@), l'égal (=), les deux points (:) et le trait de soulignement (_). Vous devez choisir un nom qui permet d'identifier la vue SNMPv3.

Sous-arbre. Branche particulière (sous-arbre) de l'arborescence MIB que vous souhaitez associer à cette vue SNMPv3. Vous devez spécifier la sous-arborescence en tant qu'OID SNMP. Il s'agit d'un argument de longueur maximale : 99.

type. Incluez ou excluez la sous-arborescence, spécifiée par le paramètre de sous-arborescence, dans ou depuis cette vue. Ce paramètre peut être utile lorsque vous avez inclus un sous-arbre, tel que A, dans une vue SNMPv3 et que vous souhaitez exclure un sous-arbre spécifique de A, tel que B, de la vue SNMPv3. Il s'agit d'un argument obligatoire. Valeurs possibles : incluses, exclues.

Exemples

ajouter une vue snmp SNMPv3Test 1.1.1.1 -type inclus
sh snmp view SNMPv3Test rm vue snmp snmpv3Test 1.1.1.1

Pour configurer une vue SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Vues**, puis créez la vue SNMP.

Configuration d'un groupe

Les groupes SNMP sont des agrégations logiques d'utilisateurs SNMP. Ils sont utilisés pour mettre en œuvre le contrôle d'accès et définir les niveaux de sécurité. Vous pouvez configurer un groupe SNMP pour définir les droits d'accès des utilisateurs affectés à ce groupe, limitant ainsi les utilisateurs à des vues spécifiques.

Vous devez configurer un groupe SNMP pour définir les droits d'accès des utilisateurs affectés à ce groupe.

Pour ajouter un groupe SNMP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp group <name> <securityLevel> -readViewName <string>`

- `show snmp group <name> <securityLevel>`

Où,

Nom. Nom du groupe SNMPv3. Peut être composé de 1 à 31 caractères, dont des lettres majuscules et minuscules, des chiffres, ainsi que le tiret (-), le point (.), l'espace (), le signe arobase (@), l'égal (=), les deux points (:) et le trait de soulignement (_). Vous devez choisir un nom qui permet d'identifier le groupe SNMPv3.

Niveau de sécurité. Niveau de sécurité requis pour la communication entre l'appliance NetScaler et les utilisateurs SNMPv3 qui appartiennent au groupe. Spécifiez l'une des options suivantes :

Pas d'**AuthNoPriv**. N'exigent ni authentification ni chiffrement.

AuthNoPriv. Nécessite une authentification mais pas de chiffrement.

AuthPriv. Exigez l'authentification et le chiffrement. Remarque : Si vous spécifiez l'authentification, vous devez spécifier un algorithme de chiffrement lorsque vous attribuez un utilisateur SNMPv3 au groupe. Si vous spécifiez également le chiffrement, vous devez attribuer à la fois une authentification et un algorithme de chiffrement à chaque membre du groupe. Il s'agit d'un argument obligatoire. Valeurs possibles : NoAuthNoPriv, AuthNoPriv, AuthPriv.

Lire le nom de l'affichage. Nom de la vue SNMPv3 configurée que vous souhaitez lier à ce groupe SNMPv3. Un utilisateur SNMPv3 lié à ce groupe peut accéder aux sous-arbres liés à cette vue SNMPv3 en tant que type INCLUDED, mais ne peut pas accéder à ceux qui sont de type EXCLUDED. Si l'appliance NetScaler possède plusieurs entrées de vue SNMPv3 portant le même nom, toutes ces entrées sont associées au groupe SNMPv3. Il s'agit d'un argument obligatoire. Longueur maximale : 31

Pour configurer un groupe SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Groupes**, puis créez le groupe SNMP.

Configuration d'un utilisateur

Les utilisateurs SNMP sont les gestionnaires SNMP auxquels les agents autorisent l'accès aux MIB. Chaque utilisateur SNMP est affecté à un groupe SNMP.

Vous devez configurer les utilisateurs au niveau de l'agent et affecter chaque utilisateur à un groupe.

Pour configurer un utilisateur à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

- `add snmp user <name> -group <string> [-authType ( MD5 | SHA ){ -authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]`

- `show snmp user <name>`

Où,

AuthType est l'option d'authentification disponible lors de la configuration d'un utilisateur. Il existe deux types d'authentification tels que MD5 et SHA.

PrivType est l'option de cryptage disponible lors de la configuration d'un utilisateur. Il existe deux types de chiffrement, tels que le DES avec une taille de clé 128 bits et l'AES avec une taille de clé 128 bits.

Exemple

```
1 > add snmp user edocs_user -group edocs_group
2 <!--NeedCopy-->
```

Pour configurer un utilisateur SNMP à l'aide de l'interface graphique

Accédez à **Système** > **SNMP** > **Utilisateurs** et créez l'utilisateur SNMP.

Configuration des alarmes SNMP pour la limitation du débit

May 5, 2023

Les appliances NetScaler sont soumises à des limites de débit. Pour plus d'informations sur les différents modèles disponibles pour chaque plateforme, consultez la fiche technique. La fiche technique est disponible sur www.citrix.com. Cliquez sur **Produits**. Sous Mise à **App Delivery and Security**, cliquez sur **NetScaler**. Cliquez sur **Plateformes > Appliances physiques**, puis cliquez sur la fiche technique **NetScaler MPX/SDX**.

Le débit maximal (Mbit/s) et le nombre de paquets par seconde (PPS) sont déterminés par la licence achetée pour l'appliance. Pour les plateformes à débit limité, vous pouvez configurer des pièges SNMP pour envoyer des notifications lorsque le débit et le PPS approchent de leurs limites et lorsqu'ils reviennent à la normale.

Le débit et le PPS sont surveillés toutes les sept secondes. Vous pouvez configurer des pièges avec des valeurs de seuil haut et de seuil normal, qui sont exprimées en pourcentage des limites autorisées. L'appareil génère ensuite un piège lorsque le débit ou le PPS dépasse le seuil élevé, et un second piège lorsque le paramètre surveillé tombe au seuil normal. Outre l'envoi des interruptions au périphérique de destination configuré, l'appliance NetScaler enregistre les événements associés aux interruptions dans le fichier /var/log/ns.log sous les formats EVENT ALERTSTARTED et EVENT ALERTENDED.

Le dépassement de la limite de débit peut entraîner une perte de paquets. Vous pouvez configurer les alarmes SNMP pour signaler la perte de paquets.

Pour plus d'informations sur les alarmes et les interruptions SNMP, consultezla section « Configuration de NetScaler pour générer des interruptions SNMP v1et v2 ». «

Ce document comprend les détails suivants :

- Configuration d'une alarme SNMP pour le débit ou le PPS
- Configuration d'une alarme SNMP pour les paquets perdus

Configuration d'une alarme SNMP pour le débit ou le PPS

Pour contrôler à la fois tout le temps et le PPS, vous devez configurer des alarmes distinctes et définir la valeur seuil PPS en Mbit/s.

Pour configurer une alarme SNMP pour le débit à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer l'alarme SNMP, définir la valeur seuil en Mbit/s et vérifier la configuration :

- `set snmp alarm PF-RL-RATE-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]`
- `show snmp alarm PF-RL-RATE-THRESHOLD`

Exemple

```
1 > set snmp alarm PF-RL-RATE-THRESHOLD -thresholdValue 70 -normalValue
     50
2 <!--NeedCopy-->
```

Pour configurer une alarme SNMP pour PPS à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour configurer l'alarme SNMP pour PPS et vérifier la configuration :

- `set snmp alarm PF-RL-PPS-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]`
- `show snmp alarm PF-RL-PPS-THRESHOLD`

Exemple

```
> set snmp alarm PF-RL-PPS-THRESHOLD -thresholdValue 70 -normalValue 50
<!--NeedCopy-->
```

Pour configurer une alarme SNMP pour le débit ou le PPS à l'aide de l'interface graphique

1. Accédez à **Système > SNMP > Alarmes**et sélectionnez **PF-RL-RATE-THRESHOLD** (pour le débit) ou **PF-RL-PPS-THRESHOLD** (pour les paquets par seconde).
2. Définissez les paramètres de l'alarme et activez l'alarme SNMP sélectionnée.

Configuration de l'alarme SNMP en cas de perte de paquets

Vous pouvez configurer une alarme pour les paquets perdus suite à un dépassement de la limite de débit et une alarme pour les paquets perdus suite à un dépassement de la limite PPS.

Pour configurer une alarme SNMP pour les paquets perdus en raison d'un débit excessif à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set snmp alarm PF-RL-RATE-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Pour configurer une alarme SNMP pour les paquets perdus en raison d'un nombre excessif de PPS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set snmp alarm PF-RL-PPS-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Pour configurer une alarme SNMP pour les paquets perdus à l'aide de l'interface graphique

1. Accédez à **Système > SNMP > Alarmes**et sélectionnez **PF-RL-RATE-PKTS-DROPPED** (pour les paquets abandonnés en raison d'un débit excessif) ou **PF-RL-PPS-PKTS-DROPPED** (pour les paquets perdus en raison d'un excès de PPS).
2. Définissez les paramètres de l'alarme et activez l'alarme SNMP sélectionnée.

Configuration du SNMP en mode FIPS

May 5, 2023

Le mode FIPS nécessite le protocole SNMPv3 (Simple Network Management Protocol version 3) avec l'option d'authentification et de confidentialité (AuthPriv). Les versions 1 et 2 du SNMP utilisent un mécanisme de chaîne communautaire pour fournir un accès sécurisé aux données de gestion. La chaîne de communauté est envoyée sous forme de texte clair entre un gestionnaire SNMP et un agent SNMP. Ce type de communication n'est pas sécurisé, ce qui permet aux intrus d'accéder aux informations SNMP sur le réseau.

Le protocole SNMPv3 utilise le modèle de sécurité basé sur l'utilisateur (USM) et le modèle de contrôle d'accès basé sur la vue (VACM) pour authentifier et contrôler l'accès de gestion aux données de messagerie SNMP. SNMPv3 possède trois niveaux de sécurité : pas d'authentification sans confidentialité (NoAuthNoPriv), authentification sans confidentialité (AuthNoPriv) et authentification et confidentialité (AuthPriv).

L'activation du mode FIPS et le redémarrage de l'appliance NetScaler suppriment les configurations SNMP suivantes de l'appliance :

1. Configuration communautaire pour les protocoles SNMPv1 et SNMPv2.
2. Groupes SNMPv3 configurés avec l'option de niveau de sécurité NoAuthNoPriv ou AuthNoPriv.
3. Interrupteurs configurés pour SNMPv1, SNMPv2 ou SNMPv3 avec l'option de niveau de sécurité NoAuthNoPriv.

Après le redémarrage de l'appliance, configurez SNMPv3 avec l'option AuthPriv. Pour plus d'informations sur la configuration de l'option AuthPriv dans SMNP v3, consultez la rubrique SNMPV3.

> **Remarque** :
>
> L'activation du mode FIPS et le redémarrage de votre appliance bloquent l'exécution des commandes SNMP d'interruption et de groupe suivantes :

```
1.  add snmp community <communityName> <permissions>

2.  add snmp trap <trapClass> <trapDestination> ... [-version: v1/
    v2]   [-td <positive_integer>] [-destPort <port>] [-
    communityName <string>] [-srcIP <ip_addr|ipv6_addr>] [-severity
    <severity>] [-allPartitions ( ENABLED | DISABLED )]

3.  add snmp group <name> <securityLevel : noAuthNoPriv/ authNoPriv
    > -readViewName <string>
```



```
    4.  bind snmp trap specific <TrapIp>-userName <v3 user name> -
       securityLevel <noAuthNoPriv/ authNoPriv>
<!--NeedCopy-->
```

Journalisation des audits

May 5, 2023

> **Important**
>
> Citrix vous recommande de mettre à jour une configuration SYSLOG ou NSLOG uniquement pendant la maintenance ou les interruptions de service. Si vous mettez à jour une configuration après avoir créé une session, les modifications ne sont pas appliquées aux journaux de session existants.

L'audit est un examen méthodique ou un examen d'un état ou d'une situation. La fonction de journalisation des audits vous permet de consigner les états de NetScaler et les informations d'état collectées par différents modules. Les informations du journal peuvent se trouver dans le noyau et dans les démons de niveau utilisateur. Pour la journalisation des audits, vous pouvez utiliser le protocole SYSLOG, le protocole NSLOG natif, ou les deux.

SYSLOG est un protocole standard pour la journalisation. Il comporte deux composantes :

- **Module d'audit SYSLOG.** S'exécute sur l'appliance NetScaler.
- **serveur SYSLOG.** S'exécute sur le système d'exploitation (SE) FreeBSD sous-jacent de l'appliance NetScaler ou sur un système distant.

SYSLOG utilise un protocole de données utilisateur (UDP) pour le transfert de données.

De même, le protocole NSLOG natif comporte deux composants :

- **Module d'audit NSLOG.** S'exécute sur l'appliance NetScaler.
- **serveur NSLOG.** S'exécute sur le système d'exploitation FreeBSD sous-jacent de l'appliance NetScaler ou sur un système distant.

NSLOG utilise le protocole TCP pour le transfert de données.

Lorsque vous exécutez un serveur SYSLOG ou NSLOG, il se connecte à l'appliance NetScaler. L'appliance NetScaler commence alors à envoyer toutes les informations du journal au serveur SYSLOG ou NSLOG. Et le serveur filtre les entrées du journal avant de les stocker dans un fichier journal. Un serveur NSLOG ou SYSLOG reçoit des informations de journal provenant de plusieurs appliances NetScaler. L'appliance NetScaler envoie les informations du journal à plusieurs serveurs SYSLOG ou NSLOG.

Si plusieurs serveurs SYSLOG sont configurés, l'appliance NetScaler envoie ses événements et messages SYSLOG à tous les serveurs de journaux externes configurés. Cela entraîne le stockage de messages redondants et complique la surveillance pour les administrateurs système. Pour résoudre ce problème, l'appliance NetScaler propose des algorithmes d'équilibrage de charge. L'appliance peut équilibrer la charge des messages SYSLOG entre les serveurs de journaux externes pour améliorer la maintenance et les performances. Les algorithmes d'équilibrage de charge pris en charge incluent RoundRobin, LeastBandWidth, CustomLoad, LeastPackets et AuditLogHash.

> **Remarque**
>
> L'appliance NetScaler peut envoyer des messages de journal d'audit jusqu'à 16 Ko à un serveur SYSLOG externe.

Les informations de journal qu'un serveur SYSLOG ou NSLOG collecte auprès d'une appliance NetScaler sont stockées dans un fichier journal sous forme de messages. Ces messages contiennent généralement les informations suivantes :

- Adresse IP d'une appliance NetScaler qui a généré le message du journal.
- Un horodatage
- Le type de message
- Les niveaux de journalisation prédéfinis (critique, erreur, notification, avertissement, information, débogage, alerte et urgence)
- Les informations de message

Pour configurer la journalisation des audits, vous devez d'abord configurer les modules d'audit sur l'appliance NetScaler. L'appliance implique la création de politiques d'audit et la spécification des informations du serveur NSLOG ou du serveur SYSLOG. Vous installez et configurez ensuite le serveur SYSLOG ou NSLOG sur le système d'exploitation FreeBSD sous-jacent de l'appliance NetScaler ou sur un système distant.

> **Remarque**
>
> SYSLOG est une norme industrielle pour l'enregistrement des messages des programmes, et divers fournisseurs fournissent une assistance. La documentation ne contient pas d'informations de configuration du serveur SYSLOG.

Le serveur NSLOG possède son propre fichier de configuration (auditlog.conf). Vous pouvez personnaliser la journalisation sur le système serveur NSLOG en apportant des modifications supplémentaires au fichier de configuration (auditlog.conf).

> **Remarque**
>
> L'accès ICMP au serveur Syslog est obligatoire si le serveur Syslog est utilisé comme FQDN sous Syslog Action sur le réseau. Si l'accès ICMP est bloqué dans l'environnement, configurez-le en tant que serveur Syslog à charge équilibrée et définissez la valeur du paramètre HealthMonitor

> dans la commande set service sur NO.
> Pour configurer ICMP, voir Serveurs SYSLOG d'équilibragede charge

Configuration de l'appliance NetScaler pour la journalisation des audits

May 5, 2023

> **Avertissement :**
>
> Les expressions de politique classiques et leur utilisation sont déconseillées (leur utilisation est déconseillée mais toujours prise en charge) à partir de NetScaler 12.0 build 56.20. Comme alternative, Citrix vous recommande d'utiliser des politiques avancées. Pour plus d'informations, voir Stratégies avancées.

La journalisation des audits affiche les informations d'état des différents modules afin que l'administrateur puisse consulter l'historique des événements dans l'ordre chronologique. Les principales composantes d'un cadre d'audit sont « action d'audit », « stratégie d'audit ». « Action d'audit » décrit les informations de configuration du serveur d'audit, tandis que la « stratégie d'audit » lie une entité de liaison à une « action d'audit ». Les stratégies d'audit utilisent le framework « Classic Policy Engine » (CPE) ou le framework Progress Integration (PI) pour lier « action d'audit » aux « entités de liaison globale du système ».

Cependant, les cadres de stratégies diffèrent les uns des autres en ce qu'ils lient les stratégies des journaux d'audit aux entités mondiales. Auparavant, le module d'audit ne prenait en charge que les expressions de stratégie classiques et avancées. Actuellement, à l'aide de l'expression avancée, vous pouvez lier les stratégies du journal d'audit uniquement aux entités globales du système.

> **Remarque**
>
> Lorsque vous liez une stratégie à des entités globales, vous devez la lier à une entité globale système de la même expression. Par exemple, vous ne pouvez pas lier une stratégie classique à une entité globale avancée ou une stratégie avancée à une entité globale classique.
>
> En outre, vous ne pouvez pas lier à la fois une stratégie de journal d'audit classique et une stratégie de journal d'audit avancée à un serveur virtuel d'équilibrage de charge.

Configuration des stratégies du journal d'audit dans une expression de stratégie classique

La configuration de la journalisation des audits dans une stratégie classique comprend les étapes suivantes :

1. **Configuration d'une action du journal d'audit**. Vous pouvez configurer une action d'audit pour différents serveurs et pour différents niveaux de journalisation. « Action d'audit » décrit les informations de configuration du serveur d'audit, tandis que la « stratégie d'audit » lie une entité de liaison à une « action d'audit ». Par défaut, le SYSLOG et le NSLOG utilisent uniquement le protocole TCP pour transférer les informations de journal vers les serveurs de journaux. Le protocole TCP est plus fiable que le protocole UDP pour transférer des données complètes. Lorsque vous utilisez TCP pour SYSLOG, vous pouvez définir la limite de mémoire tampon sur l'appliance NetScaler pour stocker les journaux. Après quoi, les journaux sont envoyés au serveur SYSLOG.
2. **Configuration de la stratégie relative aux journaux d'audit**. Vous pouvez configurer des stratégies SYSLOG pour enregistrer des messages sur un serveur SYSLOG ou une stratégie NSLOG pour enregistrer des messages sur un serveur NSLOG. Chaque stratégie inclut une règle définie sur **`true`** ou `ns_true` pour les messages à enregistrer, ainsi qu'une action SYSLOG ou NSLOG.
3. **Liaison des stratégies relatives aux journaux d'audit à des entités globales**. Vous devez lier globalement les politiques du journal d'audit à des entités mondiales telles que SYSTEM, VPN, NetScaler AAA, etc. Vous pouvez le faire pour activer la journalisation de tous les événements du système NetScaler. En définissant le niveau de priorité, vous pouvez définir l'ordre d'évaluation de la journalisation du serveur d'audit. La priorité 0 est la plus élevée et est évaluée en premier. Plus le numéro de priorité est élevé, plus la priorité de l'évaluation est faible.

Chacune de ces étapes est expliquée dans les sections suivantes.

Configuration de l'action du journal d'audit

Pour configurer l'action SYSLOG dans une infrastructure de stratégies avancée à l'aide de l'interface de ligne de commande.

> **Remarque**
>
> L'appliance NetScaler vous permet de configurer une seule action SYSLOG sur l'adresse IP et le port du serveur SYSLOG. L'appliance ne vous permet pas de configurer plusieurs actions SYSLOG sur la même adresse IP et le même port du serveur.

Une action Syslog contient une référence à un serveur Syslog. Il spécifie les informations à consigner et indique comment consigner ces informations.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
1 - add audit syslogAction <name> <serverIP> [-serverPort <port>] -
    logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
    transport ( TCP | UDP )]`
2 - show audit syslogAction [<name>]
3
```



```
<!--NeedCopy-->
```

Pour configurer l'action NSLOG dans une infrastructure de stratégies avancée à l'aide de l'interface de ligne de commande.

Une action de journal ns contient une référence à un serveur nslog. Il spécifie les informations à consigner et indique comment consigner ces informations.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
- add audit nslogAction <name> <serverIP> [-serverPort <port>] -
  logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
- show audit nslogAction [<name>]
<!--NeedCopy-->
```

Configuration des stratégies relatives aux journaux d'audit

Configurez les stratégies du journal d'audit dans une infrastructure de stratégies classique à l'aide de l'interface de ligne de commande.

À l'invite de commande, tapez :

```
- add audit syslogpolicy <name> <-rule> <action>
- add audit nslogpolicy <name> <-rule> <action>
<!--NeedCopy-->
```

Liaison des stratégies de Syslog d'audit à l'audit global de Syslog

Liez la stratégie du journal d'audit à une structure de stratégie avancée à l'aide de l'interface de ligne de commande.

À l'invite de commande, tapez :

```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType]
```

```
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```

Liez la stratégie du journal d'audit à une structure de stratégie classique à l'aide de l'interface de ligne de commande.

À l'invite de commande, tapez :

```
bind systemglobal <policy Name> <Priority>
```

```
unbind systemglobal <policy Name> <Priority>
```


Configuration des stratégies du journal d'audit à l'aide d'une expression de stratégie avancée

La configuration de la journalisation des audits dans une stratégie avancée comprend les étapes suivantes :

1. **Configuration d'une action du journal d'audit**. Vous pouvez configurer une action d'audit pour différents serveurs et pour différents niveaux de journalisation. « Action d'audit » décrit les informations de configuration du serveur d'audit, tandis que la « stratégie d'audit » lie une entité de liaison à une « action d'audit ». Par défaut, le SYSLOG et le NSLOG utilisent uniquement le protocole TCP pour transférer les informations de journal vers les serveurs de journaux. Le protocole TCP est plus fiable que le protocole UDP pour transférer des données complètes. Lorsque vous utilisez TCP pour SYSLOG, vous pouvez définir la limite de mémoire tampon sur l'appliance NetScaler pour stocker les journaux. Après quoi, les journaux sont envoyés au serveur SYSLOG.
2. **Configuration de la stratégie relative aux journaux d'audit**. Vous pouvez configurer des stratégies SYSLOG pour enregistrer des messages sur un serveur SYSLOG ou une stratégie NSLOG pour enregistrer des messages sur un serveur NSLOG. Chaque stratégie inclut une règle définie sur **`true`** ou `ns_true` pour les messages à enregistrer, ainsi qu'une action SYSLOG ou NSLOG.
3. **Liaison des stratégies relatives aux journaux d'audit à des entités globales**. Vous devez lier globalement les politiques du journal d'audit à l'entité globale SYSTEM pour permettre la journalisation de tous les événements du système NetScaler. En définissant le niveau de priorité, vous pouvez définir l'ordre d'évaluation de la journalisation du serveur d'audit. La priorité 0 est la plus élevée et est évaluée en premier. Plus le numéro de priorité est élevé, plus la priorité de l'évaluation est faible.

> **Remarque**
>
> L'appliance NetScaler évalue toutes les politiques liées à la valeur true.

Configuration de l'action du journal d'audit

Pour configurer l'action syslog dans une infrastructure de stratégies avancée à l'aide de l'interface de ligne de commande.

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
1 -  add audit syslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
     transport ( TCP | UDP )]
2 -  show audit syslogAction [<name>]
3 <!--NeedCopy-->
```


Configurez l'action NSLOG dans une infrastructure de stratégies avancée à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez les commandes suivantes pour définir les paramètres et vérifier la configuration :

```
1 -  add audit nslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
2 -  show audit nslogAction [<name>]
3 <!--NeedCopy-->
```

Configuration des stratégies relatives aux journaux d'audit

Pour ajouter une action d'audit Syslog à l'aide de l'interface de ligne de commande.

À l'invite de commande, tapez :

```
1     add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
         domainResolveRetry <integer>])
2     | -lbVserverName <string>))[-serverPort <port>] -logLevel <logLevel
         >[-dateFormat <dateFormat>]
3      [-logFacility <logFacility>][-tcp ( NONE | ALL )] [-acl ( ENABLED
          | DISABLED )]
4     [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog ( YES |
         NO )]
5      [-appflowExport ( ENABLED | DISABLED )] [-lsn ( ENABLED | DISABLED
           )][-alg ( ENABLED | DISABLED )]
6     [-subscriberLog ( ENABLED | DISABLED )][-transport ( TCP | UDP )]
         [-tcpProfileName <string>][-maxLogDataSizeToHold
7 <!--NeedCopy-->
```

Exemple

```
1     > add audit syslogaction audit-action1 10.102.1.1 -loglevel
         INFORMATIONAL -dateformat MMDDYYYY
2     > add audit nslogAction nslog-action1 10.102.1.3 -serverport 520 -
         loglevel INFORMATIONAL -dateFormat MMDDYYYY
3     > add audit syslogpolicy syslog-pol1 TRUE audit-action1
4     > add audit nslogPolicy nslog-pol1 TRUE nslog-action1
5     > bind system global nslog-pol1 -priority 20
6 <!--NeedCopy-->
```

Ajoutez une action d'audit nslog à l'aide de l'interface de ligne de commande.

À l'invite de commande, tapez :


```
1     add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
          domainResolveRetry <integer>])) [-serverPort <port>]       -
          logLevel <logLevel> ... [-dateFormat <dateFormat>][-logFacility
          <logFacility>] [-tcp ( NONE | ALL )][-acl ( ENABLED | DISABLED )
          ] [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog (
          YES | NO )][-appflowExport ( ENABLED | DISABLED )] [-lsn (
          ENABLED | DISABLED )][-alg ( ENABLED | DISABLED )] [-
          subscriberLog ( ENABLED | DISABLED )]`
2 <!--NeedCopy-->
```

Liaison des stratégies relatives aux journaux d'audit à des entités globales

Liez la stratégie du journal d'audit Syslog à une structure de stratégie avancée à l'aide de la CLI.

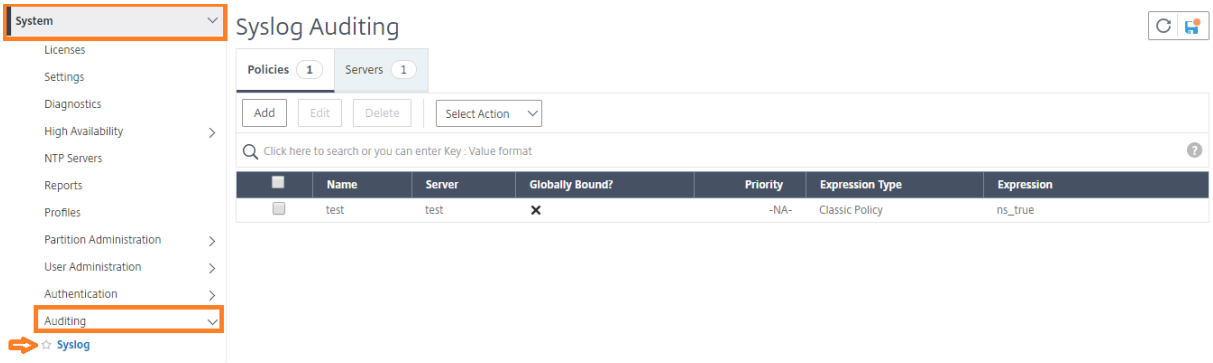
À l'invite de commande, tapez :

```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType
```

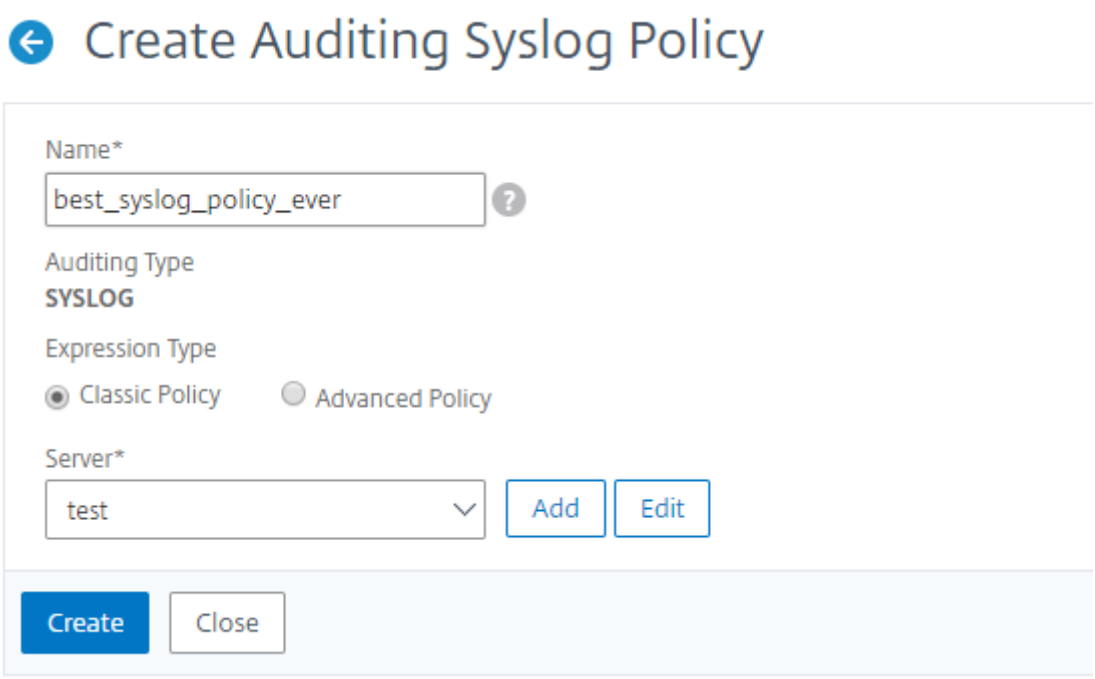
```
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```

Configuration de la stratégie du journal d'audit à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Audit** > **Syslog**.



1. Sélectionnez l'onglet **Serveurs** .
2. Cliquez sur **Ajouter**.
3. Dans la page **Créer un serveur d'audit**, renseignez les champs pertinents, puis cliquez sur **Créer**.
4. Pour ajouter la stratégie, sélectionnez l'onglet **Stratégies**, puis cliquez sur **Ajouter**.
5. Dans la page **Créer une stratégie Syslog d'audit**, remplissez les champs pertinents, puis cliquez sur **Créer**.



6. Pour lier la stratégie globalement, sélectionnez **Advanced Policy Global Bindings** dans la liste déroulante. Sélectionnez la stratégie **best_syslog_policy_ever** . Cliquez sur **Sélectionner**.
7. Dans la liste déroulante, sélectionnez le point de liaison **SYSTEM_GLOBAL** et cliquez sur **Liaison**, puis cliquez sur **Terminé**.

Configuration de la journalisation basée sur des stratégies

Vous pouvez configurer la journalisation basée sur des stratégies pour les stratégies de réécriture et de répondeur. Les messages d'audit sont ensuite consignés dans un format défini lorsque la règle d'une stratégie est évaluée à TRUE. Pour configurer la journalisation basée sur des règles, vous devez configurer une action de message d'audit qui utilise des expressions de stratégie avancées pour spécifier le format des messages d'audit. Et associez l'action à une stratégie. La stratégie peut être liée globalement ou à un serveur virtuel d'équilibrage de charge ou de commutation de contenu. Vous pouvez utiliser des actions de message d'audit pour consigner des messages à différents niveaux de journalisation, soit au format Syslog uniquement, soit dans les formats syslog et nslog

Composants requis

- L'option Messages de journal configurables par l'utilisateur (UserDefinedAuditLog) est activée lors de la configuration du serveur d'actions d'audit auquel vous souhaitez envoyer les journaux dans un format défini.
- La stratégie d'audit associée est liée au système global.

Configuration d'une action de message d'audit

Vous pouvez configurer des actions de message d'audit pour consigner les messages à différents niveaux de journalisation, soit au format Syslog uniquement, soit dans les formats de journal Syslog et de nouveaux formats de journal NS. Les actions de message d'audit utilisent des expressions pour spécifier le format des messages d'audit.

Création d'une action de message d'audit à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add audit messageaction <name> <logLevel> <stringBuilderExpr> [-
     logtoNewnslog (YES|NO)]
2 <!--NeedCopy-->
```

```
1 add audit messageaction log-act1 CRITICAL '"Client:"+CLIENT.IP.SRC+"
     accessed "+HTTP.REQ.URL'
2 <!--NeedCopy-->
```

Configurer l'action d'un message d'audit à l'aide de l'interface graphique

Accédez à **Système > Audit > Actions de message**, puis créez l'action de message d'audit.

Action de liaison d'un message d'audit à une stratégie

Après avoir créé une action de message d'audit, vous devez la lier à une stratégie de réécriture ou de réponse. Pour plus d'informations sur la liaison des actions de message du journal à une stratégie de réécriture ou de réponse, voir Réécriture ou Répondeur.

Installation et configuration du serveur NSLOG

May 5, 2023

Lors de l'installation, le fichier exécutable du serveur NSLOG (auditserver) est installé avec d'autres fichiers. Le fichier exécutable du serveur d'audit inclut des options permettant d'effectuer plusieurs actions sur le serveur NSLOG, notamment l'exécution et l'arrêt du serveur NSLOG. En outre, vous utilisez l'exécutable auditserver pour configurer le serveur NSLOG avec les adresses IP des appliances NetScaler à partir desquelles le serveur NSLOG commencera à collecter des journaux. Les paramètres de configuration sont appliqués dans le fichier de configuration du serveur NSLOG (auditlog.conf).

Ensuite, vous démarrez le serveur NSLOG en exécutant l'exécutable auditserver. La configuration du serveur NSLOG est basée sur les paramètres du fichier de configuration. Vous pouvez personnaliser davantage la journalisation sur le système serveur NSLOG en apportant des modifications supplémentaires au fichier de configuration du serveur NSLOG (auditlog.conf).

> **Attention** :
>
> La version du package du serveur NSLOG doit être identique à celle de NetScaler. Par exemple, si la version de NetScaler est 10.1 Build 125.9, le serveur NSLOG doit également être de la même version.

Le tableau suivant répertorie les systèmes d'exploitation sur lesquels le serveur NSLOG est pris en charge.

Système d'exploitation	Configuration logicielle requise	Remarques
Windows	Windows XP Professionnel, Windows Server 2003, Windows 2000/NT, Windows Server 2008, Windows Server 2008 R2	
Linux	RedHat Linux 4 ou version ultérieure, SUSE Linux Enterprise 9.3 ou version ultérieure	
FreeBSD	FreeBSD 6.3 ou version ultérieure	Pour NetScaler 10.5, utilisez uniquement FreeBSD 8.4.
Mac OS	Mac OS 8.6 ou version ultérieure	Non pris en charge sur NetScaler 10.1 et versions ultérieures.

Les spécifications matérielles minimales pour la plate-forme exécutant le serveur NSLOG sont les suivantes :

- Processeur : Intel x86 ~ 501 mégahertz (MHz)
- RAM - 512 mégaoctets (Mo)
- Contrôleur - SCSI

Installation du serveur NSLOG sur le système d'exploitation Linux

Ouvrez une session sur le système Linux en tant qu'administrateur. Utilisez la procédure suivante pour installer les fichiers exécutables du serveur NSLOG sur le système.

Pour installer le package du serveur NSLOG sur un système d'exploitation Linux

1. À l'invite de commandes Linux, tapez la commande suivante pour copier le fichier NSauditserver.rpm dans un répertoire temporaire :

   ```
   cp <path_to_cd>/Utilities/auditserver/Linux/NSauditserver.rpm /tmp
   ```

2. Tapez la commande suivante pour installer le fichier NSauditserver.rpm.

   rpm -i NSauditserver.rpm

   Cette commande extrait les fichiers et les installe dans les répertoires suivants :

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples

Pour désinstaller le package du serveur NSLOG sur un système d'exploitation Linux

1. À l'invite de commandes, tapez la commande suivante pour désinstaller la fonctionnalité de journalisation du serveur d'audit :

   ```
   rpm -e NSauditserver
   ```

2. Pour plus d'informations sur le fichier RPM de NSAuditServer, utilisez la commande suivante :

   ```
   rpm -qpi \*.rpm
   ```

3. Pour afficher les fichiers du serveur d'audit installé, utilisez la commande suivante :

   ```
   rpm -qpl *.rpm
   ```

   *.rpm: Spécifie le nom du fichier.

Installation du serveur NSLOG sur le système d'exploitation FreeBSD

Avant de pouvoir installer le serveur NSLOG, vous devez copier le package NSLOG depuis le CD du produit NetScaler ou le télécharger depuis www.citrix.com. Le package NSLOG a le format de nom suivant :

```
AuditServer_<release number>-<build number>.zip
```

Pa exemple : AuditServer_10.5-58.11.zip

Ce paquet contient des fichiers pour toutes les plateformes prises en charge : Linux, Windows et FreeBSD. Sur un système d'exploitation FreeBSD, installez le package NSLOG dont le format de nom est le suivant :

`audserver_bsd-<release number>-<build number>.tgz`

Pa exemple : `audserver_bsd-10.5-58.11.tgz`

Pour télécharger le package NSLOG sur www.citrix.com :

1. Dans un navigateur Web, rendez-vous sur www.citrix.com.
2. Dans la barre de menu, cliquez sur **Se connecter**.
3. Entrez vos informations de connexion, puis cliquez sur **Se connecter**.
4. Dans la barre de menu, cliquez sur **Téléchargements**.
5. **Dans la liste Sélectionnez un produit**, sélectionnez **NetScaler**.
6. **Sur la page**NetScaler**, sélectionnez la version pour laquelle vous souhaitez télécharger le package NSLOG (par exemple, la version 10.5), puis sélectionnez Firmware.**
7. Sous **Micrologiciel, sélectionnez le microprogramme**NetScaler correspondant au numéro de version pour lequel vous souhaitez télécharger le package NSLOG.
8. Sur la page qui s'affiche, faites défiler la page vers le bas, sélectionnez **Serveurs d'audit**, puis cliquez sur **Télécharger le fichier** à côté du package que vous souhaitez télécharger.

Pour installer le package du serveur NSLOG sur un système d'exploitation FreeBSD

1. Sur le système sur lequel vous avez téléchargé le package NSLOG `AuditServer_<release number>-<build number>.zip` (par exemple, `AuditServer_9.3-51.5.zip`), extrayez le `FreeBSD NSLOG server package audserver_bsd-<release number>-<build number>.tgz` (par exemple, `audserver_bsd-9.3-51.5.tgz`) du package.
2. Copiez le package du serveur FreeBSD NSLOG `audserver_bsd-<release number>-<build number>.tgz` (par exemple `audserver_bsd-9.3-51.5.tgz`) dans un répertoire sur un système exécutant FreeBSD OS.
3. À l'invite de commandes correspondant au répertoire dans lequel le package du serveur FreeBSD NSLOG a été copié, exécutez la commande suivante pour installer le package :

   `pkg_add audserver_bsd-<release number>-<build number>.tgz`

   Exemple :

   ```
   1 pkg_add audserver_bsd-9.3-51.5.tgz
   2 <!--NeedCopy-->
   ```

   Les répertoires suivants sont extraits :

   - `<root directory extracted from the FreeBSD NSLOG server package tgz file>NetScalerbin` (par exemple, `/var/auditserver/netscaler/bin`)

- <root directory extracted from the FreeBSD NSLOG server **package** tgz file>netscaler/etc (par exemple, /var/auditserver/netscaler/etc)
- <root directory extracted from the FreeBSD NSLOG server **package** tgz file>\netscaler\samples (par exemple, /var/auditserver/samples)

4. À l'invite de commandes, tapez la commande suivante pour vérifier que le package est installé :

```
pkg_info | grep NSaudserver
```

Pour désinstaller le package du serveur NSLOG sur un système d'exploitation FreeBSD

À l'invite de commandes, entrez la commande suivante :

```
pkg_delete NSaudserver
```

Installation des fichiers NSLOG Server sur le système d'exploitation Windows

Avant de pouvoir installer le serveur NSLOG, vous devez copier le package NSLOG depuis le CD du produit NetScaler ou le télécharger depuis www.citrix.com. Le package NSLOG a le format de nom suivantAuditServer _<release number>-<build number>.zip (par exemple,AuditServer_9.3-51.5.zip). Ce package contient les packages d'installation NSLOG pour toutes les plateformes prises en charge.

Pour télécharger le package NSLOG sur www.CITRIX.com

1. Dans un navigateur Web, rendez-vous sur www.citrix.com.
2. Dans la barre de menus, cliquez sur Se connecter.
3. Entrez vos informations de connexion, puis cliquez sur Se connecter.
4. Dans la barre de menu, cliquez sur Téléchargements.
5. Recherchez la page qui fournit le numéro de version et la version appropriés.
6. Sur cette page, sous Serveurs d'audit, cliquez sur Télécharger pour télécharger le package NSLOG, au format correspondant AuditServer_<release number>-<build number>.zip, sur votre système local (par exemple, AuditServer_9.3-51.5.zip).

Pour installer le serveur NSLOG sur un système d'exploitation Windows

1. Sur le système sur lequel vous avez téléchargé le package NSLOG AuditServer_<release number>-<build number>.zip (par exemple, AuditServer_9.3-51.5.zip), extrayez audserver_win-<release number>-<build number>.zip (par exemple, audserver_win-9.3-51.5.zip) à partir du package.

2. Copiez le fichier extraitaudserver_<release number>-<build number>.zip (par exemple,audserver_win-9.3-51.5.zip) sur un système Windows sur lequel vous souhaitez installer le serveur NSLOG.
3. Décompressez le audserver_<release number>-<build number>.zip fichier (par exemple audserver_win-9.3-51.5.zip).
4. Les répertoires suivants sont extraits :
   a) <root directory extracted from the Windows NSLOG server **package** zip file>\bin(par exemple, C:\audserver_win-9.3-51.5\bin)
   b) <root directory extracted from the Windows NSLOG server **package** zip file>\etc(par exemple, C:\audserver_win-9.3-51.5\etc)
   c) <root directory extracted from the Windows NSLOG server **package** zip file>\samples (par exemple, C:\audserver_win-9.3-51.5\samples)
5. À l'invite de commandes, exécutez la commande suivante à partir du <root directory extracted from the Windows NSLOG server **package** zip file>\bin path

   ```
   audserver -install -f <directorypath>\auditlog.conf
   ```

   <directorypath>: Spécifie le chemin d'accès au fichier de configuration (auditlog.conf). Par défaut, log.conf se trouve sous \<root directory extracted from Windows NSLOG server **package** zip file\>\samples directory. Mais vous pouvez copier auditlog.conf dans le répertoire de votre choix.

Pour désinstaller le serveur NSLOG sur un système d'exploitation Windows

À l'invite de commandes, exécutez la commande suivante à partir du <root directory extracted from Windows NSLOG server **package** zip file>\bin chemin :

```
audserver -remove
```

Options de commande du serveur NSLOG

Pour plus d'informations sur les commandes du serveur NSLOG, consultez Options du serveur d'audit.

Exécutez la commande audserver à partir du répertoire dans lequel l'exécutable du serveur d'audit est présent :

- Sous Windows : \ns\bin
- Sous Solaris et Linux :\usr\local\netscaler\bin

Les fichiers de configuration du serveur d'audit se trouvent dans les répertoires suivants :

- Sous Windows : \ns\etc
- Sous Linux : \usr\local\netscaler\etc

L'exécutable du serveur d'audit est lancé comme `./auditserver` sous Linux et FreeBSD.

Ajouter les adresses IP de l'appliance NetScaler sur le serveur NSLOG

Dans le fichier de configuration (
`auditlog.conf`), ajoutez les adresses IP des appliances NetScaler dont les événements doivent être enregistrés.

Pour ajouter les adresses IP de l'appliance NetScaler

À l'invite de commandes, tapez la commande suivante :

```
audserver -addns -f <directorypath\>\auditlog.conf
```

<directorypath>: Spécifie le chemin d'accès au fichier de configuration (auditlog.conf).

Vous êtes invité à saisir les informations relatives aux paramètres suivants :

NSIP : Spécifie l'adresse IP de l'appliance NetScaler, par exemple 10.102.29.1.

ID utilisateur : Spécifie le nom d'utilisateur, par exemple nsroot.

Mot de passe : Spécifie le mot de passe, par exemple nsroot.

Si vous ajoutez plusieurs adresses IP NetScaler (NSIP) et que vous ne souhaitez pas ultérieurement enregistrer tous les détails des événements de l'appliance NetScaler, vous pouvez supprimer les NSIP manuellement en supprimant l'instruction NSIP à la fin du fichier auditlog.conf. Pour une configuration haute disponibilité (HA), vous devez ajouter les adresses IP NetScaler principales et secondaires à auditlog.conf à l'aide de la commande audserver. Avant d'ajouter l'adresse IP, assurez-vous que le nom d'utilisateur et le mot de passe existent sur le système.

Vérification du fichier de configuration du serveur NSLOG

Vérifiez que la syntaxe du fichier de configuration (`audit log.conf`) est correcte afin de permettre à la journalisation de démarrer et de fonctionner correctement.

Pour vérifier la configuration, à l'invite de commandes, tapez la commande suivante :

```
audserver -verify -f <directorypath>\auditlog.conf
```

<directorypath>: Specifies the path to the configuration file (audit log.conf).

Exécution du serveur NSLOG

January 21, 2021

Pour démarrer la journalisation du serveur d'audit

Tapez la commande suivante à l'invite de commandes :

Audserver -start -f<directorypath>\auditlog.conf

<directorypath>: spécifie le chemin d'accès au fichier de configuration (audit log.conf).

Pour arrêter la journalisation du serveur d'audit qui démarre en arrière-plan dans FreeBSD ou Linux

Exécutez la commande suivante :

```
audserver -stop
```

Pour arrêter la journalisation du serveur d'audit qui démarre en tant que service dans Windows

Exécutez la commande suivante :

```
audserver -stopservice
```

Personnalisation de la journalisation sur le serveur NSLOG

May 5, 2023

Vous pouvez personnaliser la journalisation sur le serveur NSLOG en apportant des modifications supplémentaires au fichier de configuration du serveur NSLOG (log.conf). Utilisez un éditeur de texte pour modifier le fichier de configuration log.conf sur le système serveur.

Pour personnaliser la journalisation, utilisez le fichier de configuration pour définir les filtres et les propriétés du journal.

- **Filtres de journaux.** Filtrez les informations du journal à partir d'une appliance NetScaler ou d'un ensemble d'appliances NetScaler.
- **Propriétés du journal.** Chaque filtre est associé à un ensemble de propriétés de journal. Les propriétés du journal définissent le mode de stockage des informations de journal filtrées.

Ce document comprend les détails suivants :

- Création de filtres
- Spécification des propriétés du journal

Création de filtres

Vous pouvez utiliser la définition de filtre par défaut qui se trouve dans le fichier de configuration (audit log.conf), ou vous pouvez modifier le filtre ou en créer un nouveau. Vous pouvez créer plusieurs filtres de journal.

> Remarque :
> Pour la journalisation consolidée, si une transaction de journal se produit pour laquelle il n'existe aucune définition de filtre, le filtre par défaut est utilisé (s'il est activé). La seule façon de configurer la journalisation consolidée de toutes les appliances NetScaler est de définir le filtre par défaut.

Pour créer un filtre

À l'invite de commandes, tapez la commande suivante dans le fichier de configuration (auditlog.conf) :

```
filter <filterName> [IP <ip>] [NETMASK <mask>] ON | OFF]
<!--NeedCopy-->
```

FilterName : Spécifiez le nom du filtre (64 caractères alphanumériques au maximum).

ip : Spécifiez les adresses IP.

masque : Spécifiez le masque de sous-réseau à utiliser sur un sous-réseau.

Spécifiez ON pour activer le filtre pour enregistrer les transactions, ou sélectionnez OFF pour désactiver le filtre. Si aucun argument n'est spécifié, le filtre est activé.

Exemples :

```
filter F1 IP 192.168.100.151 ON
<!--NeedCopy-->
```

Pour appliquer le filtre F2 aux adresses IP 192.250.100.1 à 192.250.100.254 :

```
filter F2 IP 192.250.100.0 NETMASK 255.255.255.0 ON
<!--NeedCopy-->
```

FilterName est un paramètre obligatoire si vous définissez un filtre avec d'autres paramètres facultatifs, tels que l'adresse IP ou la combinaison de l'adresse IP et du masque de réseau.

Spécification des propriétés du journal

Les propriétés du journal associées au filtre sont appliquées à toutes les entrées du journal présentes dans le filtre. La définition de la propriété du journal commence par le mot clé BEGIN et se termine par END, comme illustré dans l'exemple suivant :

```
BEGIN <filtername>
    logFilenameFormat ...
    logDirectory ...
    logInterval ...
    logFileSizeLimit ....
END
<!--NeedCopy-->
```

Les entrées de la définition peuvent inclure les éléments suivants :

- **LogFileNameFormat** spécifie le format du nom de fichier du fichier journal. Le nom du fichier peut être du type suivant :
  - Statique : chaîne constante qui spécifie le chemin absolu et le nom du fichier.
  - Dynamique : expression qui inclut les spécificateurs de format suivants :
    - Date (% {format} t)
    - crée un nom de fichier avec NSIP

  Exemple :

  ```
  LogFileNameFormat Ex%`{
  `%m%d%y }
  t.log
  <!--NeedCopy-->
  ```

  Cela crée le premier nom de fichier sous la forme Exmmddyy.log. Les nouveaux fichiers sont nommés :
  ExMmddyy.log.0, ExMmddyy.log.1, etc. Dans l'exemple suivant, les nouveaux fichiers sont créés lorsque la taille du fichier atteint 100 Mo.

  Exemple :

  ```
  LogInterval size
  LogFileSize 100
  LogFileNameFormat Ex%`{
  `%m%d%y }
  t
  <!--NeedCopy-->
  ```


> **Attention**
>
> Le format de date %t spécifié dans le paramètre LogFileNameFormat remplace la propriété d'intervalle de journalisation pour ce filtre. Pour éviter qu'un nouveau fichier ne soit créé chaque jour plutôt que lorsque la taille de fichier journal spécifiée est atteinte, n'utilisez pas %t dans le paramètre LogFileNameFormat.

- **LogDirectory** spécifie le format du nom de répertoire du fichier journal. Le nom du fichier peut être l'un des suivants :
  - Statique : chaîne constante qui spécifie le chemin absolu et le nom du fichier.
  - Dynamique : expression contenant les spécificateurs de format suivants :
    - Date (% {format} t)
    - crée un répertoire avec NSIP

  Le séparateur de répertoires dépend du système d'exploitation. Dans Windows, utilisez le séparateur de répertoires.

  Exemple :

  ```
  1 LogDirectory dir1\dir2\dir3
  2 <!--NeedCopy-->
  ```

  Dans les autres systèmes d'exploitation (Linux, FreeBSD, etc.), utilisez le séparateur de répertoires.

- **LogInterval** spécifie l'intervalle auquel les nouveaux fichiers journaux sont créés. Utilisez l'une des valeurs suivantes :
  - Toutes les heures : Un fichier est créé toutes les heures. Valeur par défaut.
  - Tous les jours : un fichier est créé tous les jours à minuit.
  - Hebdomadaire : Un fichier est créé tous les dimanches à minuit.
  - Mensuel : Un fichier est créé le premier jour du mois à minuit.
  - Aucun : un fichier n'est créé qu'une seule fois, lorsque la journalisation du serveur d'audit démarre.
  - Taille : un fichier est créé uniquement lorsque la limite de taille du fichier journal est atteinte.

  Exemple :

  ```
  1 LogInterval Hourly
  2 <!--NeedCopy-->
  ```

  - **LogFileSizeLimit** spécifie la taille maximale (en Mo) du fichier journal. Un nouveau fichier est créé lorsque la limite est atteinte.

> **Remarque**
>
> Vous pouvez remplacer la propriété loginterval en lui attribuant la taille comme valeur.

La valeur par défaut LogFileSizeLimit est de 10 Mo.

Exemple :

```
1  LogFileSizeLimit 35
2  <!--NeedCopy-->
```

SYSLOG sur TCP

May 5, 2023

Syslog est une norme pour l'envoi de messages de notification d'événements. Ces messages peuvent être stockés localement ou sur un serveur de journaux externe. Syslog permet aux administrateurs réseau de consolider les messages de journal et d'obtenir des informations à partir des données collectées.

Syslog est initialement conçu pour fonctionner via UDP, qui peut transmettre une énorme quantité de données sur le même réseau avec une perte de paquets minimale. Toutefois, les opérateurs de télécommunications préfèrent transmettre les données Syslog via TCP, car ils ont besoin d'une transmission de données fiable et ordonnée entre les réseaux. Par exemple, la compagnie de télécommunications suit les activités des utilisateurs et TCP assure la retransmission en cas de défaillance du réseau.

Fonctionnement de Syslog sur TCP

Pour comprendre le fonctionnement de Syslog sur TCP, considérez deux cas hypothétiques :

Sam, administrateur réseau, souhaite enregistrer les événements importants sur un serveur Syslog externe.

XYZ Telecom, un fournisseur d'accès Internet, doit transmettre et stocker une quantité importante de données sur des serveurs Syslog pour se conformer aux réglementations gouvernementales.

Dans les deux cas, les messages de journal doivent être transmis via un canal fiable et stockés en toute sécurité sur un serveur syslog externe. Contrairement à UDP, TCP établit une connexion, transmet les messages de manière sécurisée et retransmet (de l'expéditeur au destinataire) toutes les données endommagées ou perdues en raison d'une défaillance du réseau.

L'appliance NetScaler envoie des messages de journal via UDP au démon syslog local et envoie des messages de journal via TCP ou UDP à des serveurs syslog externes.

Prise en charge SNIP pour Syslog

Lorsque le module audit-log génère des messages syslog, il utilise une adresse IP NetScaler (NSIP) comme adresse source pour envoyer les messages à un serveur syslog externe. Pour configurer un SNIP comme adresse source, vous devez l'intégrer à l'option NetProfile et lier NetProfile à l'action syslog.

> **Remarque**
>
> TCP utilise SNIP pour envoyer des sondes de surveillance afin de vérifier la connectivité, puis envoie les journaux via NSIP. Le serveur Syslog doit donc être accessible via SNIP. Les profils réseau peuvent être utilisés pour rediriger tout le trafic Syslog TCP via SNIP entièrement.

L'utilisation d'une adresse SNIP n'est pas prise en charge dans la journalisation interne.

Nom de domaine complet Prise en charge du journal d'audit

Auparavant, le module de journal d'audit était configuré avec l'adresse IP de destination du serveur syslog externe auquel les messages de journal sont envoyés. Désormais, le serveur de journaux d'audit utilise un nom de domaine complet (FQDN) au lieu de l'adresse IP de destination. La configuration du nom de domaine complet résout le nom de domaine configuré du serveur syslog en l'adresse IP de destination correspondante pour l'envoi des messages de journal depuis le module audit-log. Le serveur de noms doit être correctement configuré pour résoudre le nom de domaine et éviter les problèmes de service liés au domaine.

> **Remarque**
>
> Lors de la configuration d'un FQDN, la configuration du nom de domaine du serveur de la même appliance NetScaler dans l'action syslog ou l'action nslog n'est pas prise en charge.

Configuration de Syslog sur TCP à l'aide de l'interface de ligne de commande

Pour configurer une appliance NetScaler afin qu'elle envoie des messages syslog via TCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1     add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
         domainResolveRetry <integer>]) | -lbVserverName<string>))[-
         serverPort <port>] -logLevel <logLevel>[-dateFormat <dateFormat
         >] [-logFacility <logFacility>]   [-tcp ( NONE | ALL )] [-acl (
         ENABLED | DISABLED )][-timeZone ( GMT_TIME | LOCAL_TIME )][-
         userDefinedAuditlog ( YES | NO )][-appflowExport ( ENABLED |
         DISABLED )] [-lsn ( ENABLED | DISABLED )][-alg ( ENABLED |
         DISABLED )] [-subscriberLog ( ENABLED | DISABLED )][-transport (
```



```
            TCP | UDP )] [-tcpProfileName <string>][-maxLogDataSizeToHold <
           positive_integer>][-dns ( ENABLED | DISABLED )] [-netProfile <
           string>]
<!--NeedCopy-->
```

```
    add audit syslogaction audit-action1 10.102.1.1 -loglevel
       INFORMATIONAL -dateformat MMDDYYYY -transport TCP
<!--NeedCopy-->
```

Ajout de l'adresse IP SNIP au profil réseau à l'aide de l'interface de ligne de commande

Pour ajouter une adresse IP SNIP au profil réseau à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
    add netProfile <name> [-td <positive_integer>] [-srcIP <string>][-
       srcippersistency ( ENABLED | DISABLED )][-overrideLsn ( ENABLED
       | DISABLED )]add syslogaction <name> <serverIP>  - loglevel all
        - netprofile net1
<!--NeedCopy-->
```

```
    add netprofile net1  - srcip 10.102.147.204`
<!--NeedCopy-->
```

Où, SrCip est le SNIP.

Ajout d'un profil net dans une action Syslog à l'aide de l'interface de ligne de commande

Pour ajouter une option NetProfile dans une action Syslog à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
     add audit syslogaction <name> (<serverIP> | -lbVserverName <string
        >)  -logLevel <logLevel>
    -netProfile <string> …

<!--NeedCopy-->
```

```
    add syslogaction sys_act1 10.102.147.36  - loglevel all  - netprofile
        net1
<!--NeedCopy-->
```

Où -netprofile indique le nom du profil réseau configuré. L'adresse SNIP est configurée dans le cadre de NetProfile et cette option NetProfile est liée à l'action syslog.

> **Remarque**
>
> Vous devez toujours lier NetProfile aux services SYSLOGUDP ou SYSLOGTCP liés au serveur virtuel d'équilibrage de charge SYSLOGUDP ou SYSLOGTCP.

Configuration de la prise en charge des FQDN à l'aide de l'interface

Pour ajouter un nom de domaine de serveur à une action Syslog à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1 add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
      domainResolveRetry <integer>]) | -lbVserverName <string>)) -logLevel
       <logLevel> ...
2     set audit syslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>]-
         serverDomainName <string>] [-lbVserverName <string>]-
         domainResolveRetry <integer>] [-domainResolveNow]
3 <!--NeedCopy-->
```

Pour ajouter un nom de domaine de serveur à une action Nslog à l'aide de l'interface de ligne de commande.

À l'invite de commande, tapez :

```
1     add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
         domainResolveRetry <integer>]))  -logLevel <logLevel> ...
2     set audit nslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>][-
         serverDomainName <string>] [-domainResolveRetry <integer>][-
         domainResolveNow]
3 <!--NeedCopy-->
```

Où ServerDomainName. Nom de domaine du serveur de journaux. Est mutuellement exclusif avec ServerIP/ LBVServerName.

Entier DomainResolveRetry. Durée (en secondes) pendant laquelle l'appliance NetScaler attend, après l'échec d'une résolution DNS, avant d'envoyer la prochaine requête DNS pour résoudre le nom de domaine.

DomainResolveNow. Inclus si la requête DNS doit être envoyée immédiatement pour résoudre le nom de domaine du serveur.

Configuration de Syslog sur TCP à l'aide de l'interface graphique

Pour configurer l'appliance NetScaler afin qu'elle envoie des messages Syslog via TCP à l'aide de l'interface graphique

1. Accédez à **Système** > **Audit** > **Syslog** et sélectionnez l'onglet **Serveurs** .
2. Cliquez sur **Ajouter** et sélectionnez Type de transport comme **TCP**.

Configuration d'un profil réseau pour la prise en charge de SNIP via l'interface utilisateur graphique

Pour configurer le profil net pour la prise en charge SNIP à l'aide de l'interface

1. Accédez à **Système > Audit > Syslog** et sélectionnez l'onglet **Serveurs** .
2. Cliquez sur **Ajouter** et sélectionnez un profil réseau dans la liste.

Configuration de FQDN à l'aide de l'interface

Pour configurer le FQDN à l'aide de l'interface graphique

1. Accédez à **Système** > **Audit** > **Syslog** et sélectionnez l'onglet **Serveurs** .
2. Cliquez sur **Ajouter** et sélectionnez un type de serveur et un nom de domaine de serveur dans la liste.

Serveurs SYSLOG d'équilibrage de charge

May 5, 2023

L'appliance NetScaler envoie ses événements et messages SYSLOG à tous les serveurs de journaux externes configurés. Cela entraîne le stockage de messages redondants et rend la surveillance difficile pour les administrateurs système. Pour résoudre ce problème, l'appliance NetScaler propose des algorithmes d'équilibrage de charge capables d'équilibrer la charge des messages SYSLOG entre les serveurs de journaux externes afin d'améliorer la maintenance et les performances. Les algorithmes d'équilibrage de charge pris en charge incluent RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets et AuditLogHash.

Équilibrage de charge des serveurs SYSLOG à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

1. Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

   ```
   add service <name>(<IP> | <serverName>)<serviceType (SYSLOGTCP |
   SYSLOGUDP)> <port>
   ```

2. Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGUDP et la méthode d'équilibrage de charge AUDITLOGHASH.

   ```
   add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
   <AUDITLOGHASH>]
   ```


3. Liez le service au serveur virtuel d'équilibrage de charge.

   ```
   Bind lb vserver <name> <serviceName>
   ```

4. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge dont le type de service est SYSLOGTCP ou SYSLOGUDP.

   ```
   add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
   ```

5. Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

   ```
   add syslogpolicy <name> <rule> <action>
   ```

6. Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

   ```
   bind system global <policyName>
   ```

Équilibrage de charge des serveurs SYSLOG à l'aide de l'interface graphique

1. Ajoutez un service et spécifiez le type de service SYSLOGTCP ou SYSLOGUDP.

   Accédez à **Gestion du trafic** > **Services**, cliquez sur **Ajouter** et sélectionnez **SYLOGTCP** ou **SYSLOGUDP** comme protocole.

2. Ajoutez un serveur virtuel d'équilibrage de charge, spécifiez le type de service SYSLOGTCP ou SYSLOGTCP et la méthode d'équilibrage de charge AUDITLOGHASH.

   Accédez à **Gestion du trafic** > **Serveurs virtuels**, cliquez sur **Ajouter** et sélectionnez **SYLOGTCP** ou **SYSLOGUDP** comme protocole.

3. Liez le service au serveur virtuel d'équilibrage de charge.

   Accédez à **Gestion du trafic** > **Serveurs virtuels**, sélectionnez un serveur virtuel, puis sélectionnez **AUDITLOGHASH** dans la **méthode d'équilibrage de charge.**

4. Ajoutez une action SYSLOG et spécifiez le nom du serveur d'équilibrage de charge dont le type de service est SYSLOGTCP ou SYSLOGUDP.

   Accédez à **Système** > **Audit**, cliquez sur **Serveurs** et ajoutez un serveur en sélectionnant l'option **LB Vserver** dans **Serveurs**.

5. Ajoutez une stratégie SYSLOG en spécifiant la règle et l'action.

   Accédez à **Système** > **Syslog**, cliquez sur **Stratégies** et ajoutez une stratégie SYSLOG.

6. Liez la stratégie SYSLOG au système global pour que la stratégie prenne effet.

   Accédez à **Système** > **Syslog**, sélectionnez une stratégie SYSLOG et cliquez sur **Action**, puis cliquez sur **Liaisons globales** et liez la stratégie au système global.

Exemple :

La configuration suivante spécifie l'équilibre de charge des messages SYSLOG entre les serveurs de journaux externes à l'aide de la méthode AUDITLOGHASH comme méthode d'équilibrage de charge. La méthode AUDITLOGHASH équilibre la charge du trafic en fonction de la valeur de hachage entrée des agents d'audit. Les agents sont les modules qui génèrent le journal d'audit dans une appliance NetScaler. Par exemple, si un LSN d'agent souhaite équilibrer la charge des journaux d'audit en fonction de l'adresse IP du client, le module LSN génère la valeur de hachage basée sur ClientIP et transmet la valeur de hachage au module auditlog. Le module auditlog envoie les messages du journal d'audit qui ont la même valeur de hachage au serveur syslog externe.

L'appliance NetScaler génère des événements et des messages SYSLOG dont la charge est équilibrée entre les services, service1, service2 et service 3.

```
add service service1 192.0.2.10 SYSLOGUDP 514
add service service2 192.0.2.11 SYSLOGUDP 514
add service service3 192.0.2.11 SYSLOGUDP 514
add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
bind lb vserver lbvserver1 service1
bind lb vserver lbvserver1 service2
bind lb vserver lbvserver1 service3
add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
add syslogpolicy syspol1 ns_true sysaction1
bind system global syspol1
<!--NeedCopy-->
```

Utilisez la commande suivante pour configurer SYSLOG à l'aide du serveur LB avec FQDN lorsque le paquet ICMP est bloqué :

```
set service service1 -healthMonitor NO
```

Limites :

- L'appliance NetScaler ne prend pas en charge un serveur virtuel d'équilibrage de charge externe équilibrant la charge des messages SYSLOG entre les serveurs de journaux.

Paramètres par défaut pour les propriétés du journal

August 20, 2021

Voici un exemple de filtre par défaut avec les paramètres par défaut pour les propriétés du journal :

```
begin default
 logInterval Hourly
 logFileSizeLimit 10
 logFilenameFormat  auditlog%`{
```



```
 `%y%m%d }
 t.log
 end default
<!--NeedCopy-->
```

Voici deux exemples de définition des filtres par défaut :

Exemple 1 :

```
Filter f1 IP 192.168.10.1
<!--NeedCopy-->
```

Cela crée un fichier journal pour NSI 192.168.10.1 avec les valeurs par défaut de l'effet journal.

Exemple 2 :

```
Filter f1 IP 192.168.10.1
begin f1
    logFilenameFormat logfiles.log
end f1
<!--NeedCopy-->
```

Cela crée un fichier journal pour NSIP 192.168.10.1. Étant donné que le format du nom du fichier journal est spécifié, les valeurs par défaut des autres propriétés du journal sont en vigueur.

Exemple de fichier de configuration (audit.conf)

May 17, 2023

Voici un exemple de fichier de configuration :

```
##############################
# This is the Auditserver configuration file
# Only the default filter is active
# Remove leading # to activate other filters
##############################
MYIP <NSAuditserverIP>
MYPORT 3023
#   Filter filter_nsip  IP <Specify the NetScaler IP address to filter
    on > ON
#   begin filter_nsip
#       logInterval         Hourly
#       logFileSizeLimit    10
#       logDirectory         logdir\%A\
```



```
#       logFilenameFormat   nsip%\\{
 \\%d%m%Y }
 t.log
#   end filter_nsip
Filter default
begin default
    logInterval      Hourly
    logFileSizeLimit    10
    logFilenameFormat   auditlog%\{
 \%y%m%d }
 t.log
end default
<!--NeedCopy-->
```

Journalisation du serveur Web

May 5, 2023

Vous pouvez utiliser la fonction de journalisation du serveur Web pour envoyer les journaux des requêtes HTTP et HTTPS à un système client à des fins de stockage et de récupération. Cette fonctionnalité comporte deux composants :

- Le serveur de journaux Web, qui s'exécute sur NetScaler.
- Le client NetScaler Web Logging (NSWL), qui s'exécute sur le système client.

Lorsque vous exécutez le client NetScaler Web Logging (NSWL) :

1. Il se connecte à NetScaler.
2. NetScaler met en mémoire tampon les entrées du journal des requêtes HTTP et HTTPS avant de les envoyer au client.
3. Le client peut filtrer les entrées avant de les stocker.

Pour configurer la journalisation du serveur Web, vous devez d'abord activer la fonctionnalité de journalisation Web sur NetScaler et configurer la taille de la mémoire tampon pour stocker temporairement les entrées du journal. Ensuite, vous installez NSWL sur le système client. Vous ajoutez ensuite l'adresse IP NetScaler (NSIP) au fichier de configuration NSWL. Vous êtes maintenant prêt à démarrer le client NSWL pour commencer la journalisation. Vous pouvez personnaliser la journalisation du serveur Web en apportant des modifications supplémentaires au fichier de configuration NSWL (log.conf).

Configuration de NetScaler pour la journalisation du serveur Web

May 5, 2023

Pour configurer NetScaler pour la journalisation du serveur Web, vous devez activer uniquement la fonctionnalité de journalisation du serveur Web. Vous pouvez éventuellement effectuer les configurations suivantes :

- Modifiez la taille de la mémoire tampon (la taille par défaut est de 16 Mo) qui stocke les informations enregistrées avant leur envoi au client NetScaler Web Logging (NSWL).
- Spécifiez les en-têtes HTTP personnalisés que vous souhaitez exporter vers le client NSWL. Vous pouvez configurer au maximum deux noms d'en-tête de requête HTTP et deux noms d'en-tête de réponse HTTP.

Pour configurer la journalisation du serveur Web à l'aide de l'interface de ligne de commande

À l'invite de commandes, effectuez les opérations suivantes :

- Activez la fonctionnalité de journalisation du serveur Web.

  ```
  enable ns feature WL
  ```

- [Facultatif] Modifiez la taille de la mémoire tampon pour stocker les informations enregistrées.

  ```
  set ns weblogparam -bufferSizeMB <size>
  ```

  > **Remarque** :
  >
  > Pour activer votre modification, vous devez désactiver puis réactiver la fonctionnalité de journalisation du serveur Web.

- [Facultatif] Spécifiez les noms d'en-tête HTTP personnalisés que vous souhaitez exporter.

  ```
  set ns weblogparam [-customReqHdrs <string> ...] [-customRspHdrs <
  string> ...]
  ```

```
1     > enable ns feature WL
2     Done
3     > set ns weblogparam -bufferSizeMB 60
4     Done
5     > show ns weblogparam
6         Web Logging parameters:
7         Log buffer size:  60MB
8         Custom HTTP request headers: (none)
9         Custom HTTP response headers: (none)
10    Done
```



```
11      > set ns weblogparam -customReqHdrs req1 req2 -customRspHdrs res1
           res2
12      Done
13      > show ns weblogparam
14          Web Logging parameters:
15          Log buffer size:  60MB
16          Custom HTTP request headers: req1, req2
17          Custom HTTP response headers: res1, res2
18      Done
19  <!--NeedCopy-->
```

Pour configurer la journalisation du serveur Web à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres** et effectuez les opérations suivantes :
    a) Pour activer la fonctionnalité de journalisation du serveur Web, cliquez sur **Modifier les fonctionnalités avancées** et sélectionnez **Journalisation Web**.
    b) Pour modifier la taille de la mémoire tampon, cliquez sur **Modifier les paramètres généraux du système** et, sous **Journalisation Web**, entrez la taille de la mémoire tampon.
    c) Pour spécifier les en-têtes HTTP personnalisés à exporter, cliquez sur **Modifier les paramètres système globaux** et, sous **Journalisation Web**, spécifiez les valeurs des en-têtes.

Installation du client de journalisation Web NetScaler (NSWL)

May 5, 2023

Lorsque vous installez NSWL, le fichier exécutable client (NSWL) est installé avec d'autres fichiers. Le fichier exécutable NSWL fournit une liste d'options que vous pouvez utiliser. Pour plus de détails, reportez-vous à la section Configuration du client NSWL.

> **Attention**
>
> La version du client NSWL doit être identique à celle de NetScaler. Par exemple, si la version de NetScaler est 10.1 Build 125.9, le client NSWL doit également être de la même version. De plus, le client de journalisation Web (NSWL) fonctionne à la fois sur des serveurs 32 bits et 64 bits. La page de téléchargement ne possède qu'un client de blog 32 bits. Le client de blog 64 bits est disponible sur demande et vous recommande de contacter le support NetScaler pour plus d'informations.

Le tableau suivant répertorie les systèmes d'exploitation sur lesquels le client NSWL peut être installé.

Système d'exploitation	**Version**	**Configuration matérielle requise**	**Remarques**
—	—	—	—
Windows|Windows Server 2016 ou version ultérieure|Processeur : processeur x86/amd64 (1 GHz ou supérieur), RAM - 4 Go (ou supérieur)	|macOS|macOS 8.6 ou version ultérieure|Non pris en charge sur NetScaler 10.1 et versions ultérieures.
Linux	Ubuntu, SUSE Linux, CentOS, Red Hat Enterprise Linux publiés en 2016 ou version ultérieure	Processeur : processeur x86/amd64 (1 GHz ou supérieur), RAM - 4 Go (ou supérieur)
Solaris	Solaris Sun OS 5.6 ou version ultérieure	Processeur : UltraSparc-III 400 MHz, RAM - 512 Mo, contrôleur - SCSI	Non pris en charge sur NetScaler 10.5 et versions ultérieures.
FreeBSD|FreeBSD 6.3 ou version ultérieure|Processeur : processeur x86/amd64 (1 GHz ou supérieur), RAM - 4 Go (ou supérieur) |Pour NetScaler 10.5, utilisez uniquement FreeBSD 8.4.| |AIX|AIX 6.1|-|Non pris en charge sur NetScaler 10.5 et versions ultérieures.

Si le système client NSWL ne peut pas traiter la transaction du journal en raison d'une limitation du processeur, la mémoire tampon du journal Web est dépassée et le processus de journalisation redémarre.

> **Attention**
>
> La reprise de la journalisation peut entraîner la perte des transactions du journal.

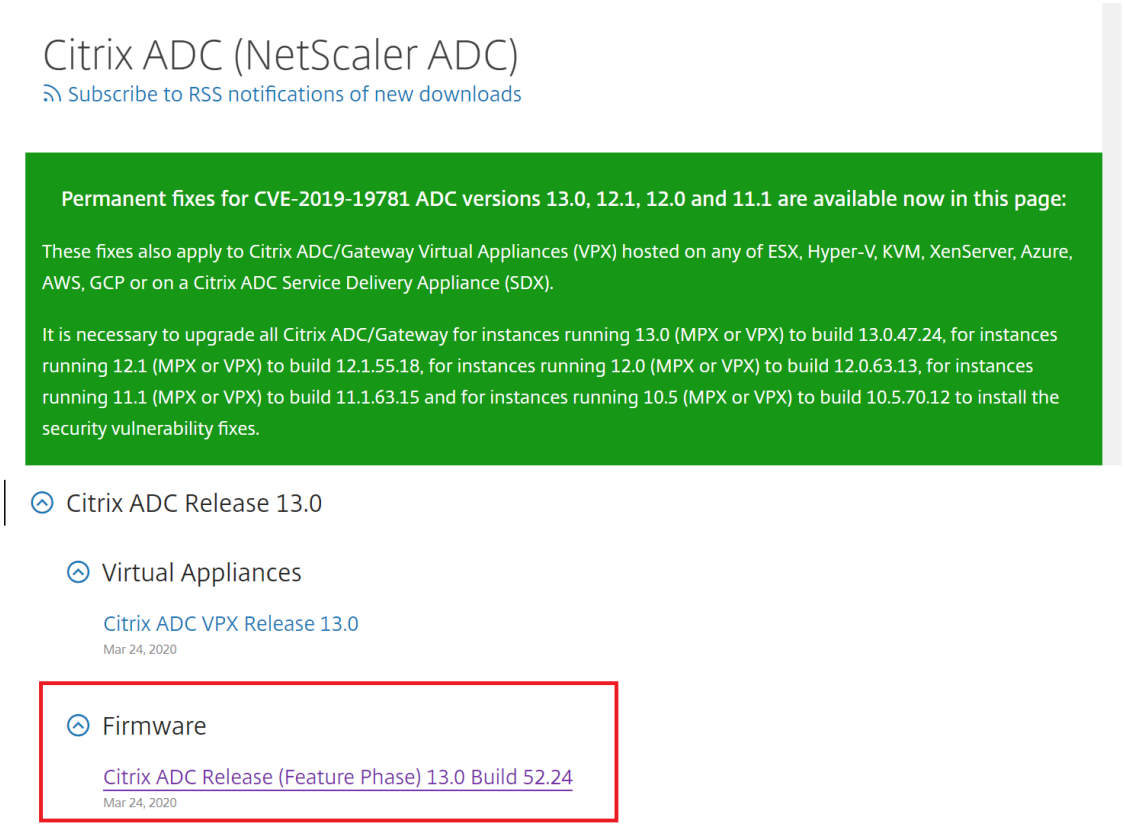
Pour résoudre temporairement un goulot d'étranglement du système client NSWL dû à une limitation du processeur, vous pouvez ajuster la taille de la mémoire tampon de journalisation du serveur Web sur l'appliance NetScaler. Pour résoudre le problème, vous avez besoin d'un système client capable de gérer le débit du site.

Télécharger le client NSWL

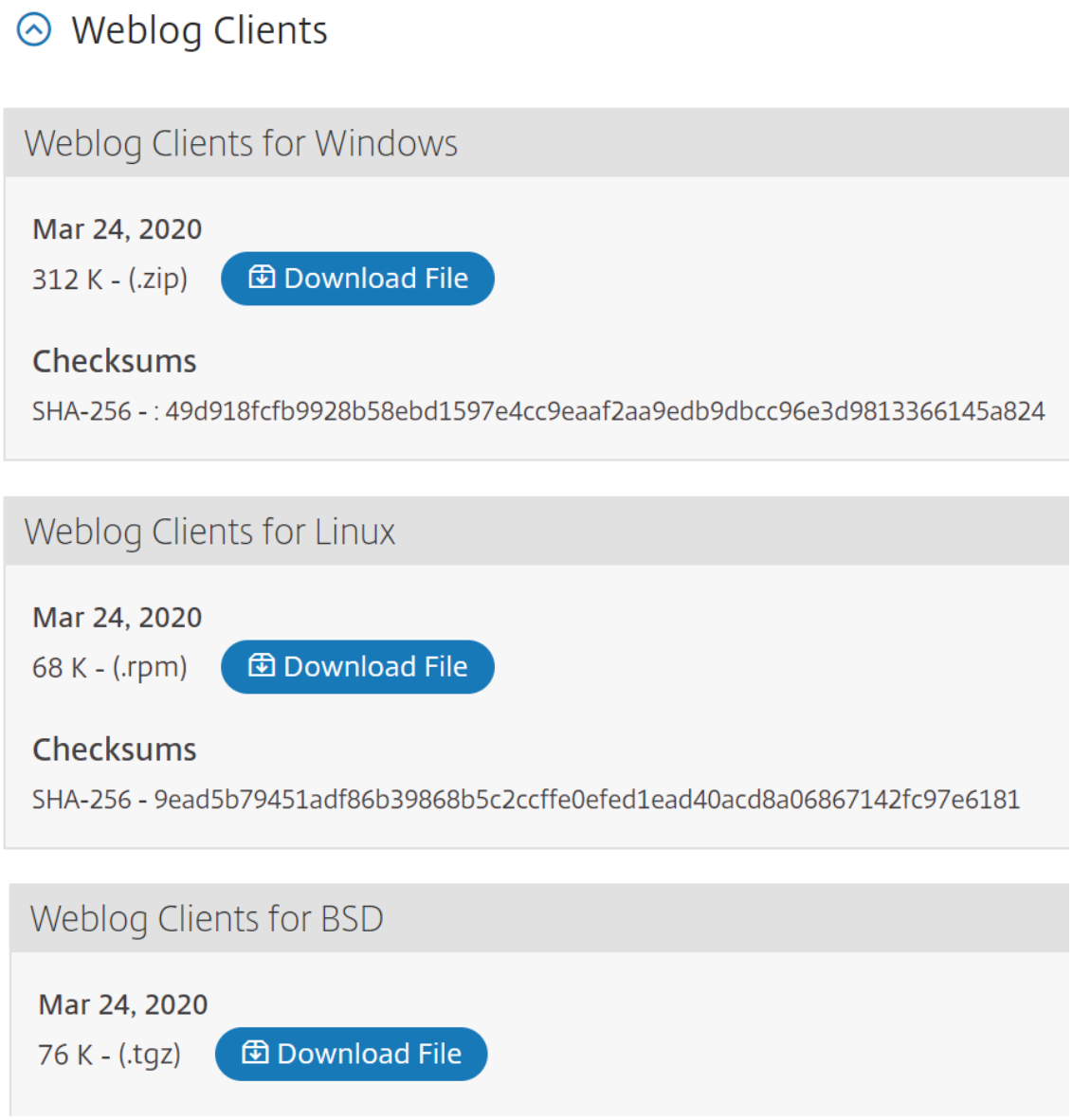
Vous pouvez obtenir le package client NSWL sur le CD du produit NetScaler ou sur le site de téléchargement de NetScaler. Le package contient des packages d'installation distincts pour chaque plate-forme prise en charge.

Pour télécharger le client NSWL depuis le site Web de Citrix

1. Ouvrez une session sur Citrix en accédant à l'URL `https://www.citrix.com/downloads/citrix-adc/`.
2. Accédez à une version particulière de NetScaler et recherchez son microprogramme.
3. Cliquez sur **Firmware** (par exemple, NetScaler Release (Feature Phase) 13.0 Build 52.24).



4. Sur la page de **compilation de NetScaler Release (Feature Phase)**, accédez à la section **Weblog Clients** .
5. Cette section vous permet de télécharger des clients Weblog pour Windows, Linux et BSD.



Installation du client NSWL sur Solaris

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le `nswl_solaris-<release number>-<build number>.tar file` du package.
2. Copiez le fichier extrait sur un système Solaris sur lequel vous souhaitez installer le client NSWL.
3. Extrayez les fichiers du fichier tar à l'aide de la commande suivante :

   ```
   tar xvf nswl_solaris-9.3-51.5.tar
   ```


Un répertoire Weblog est créé dans le répertoire temporaire et les fichiers sont extraits vers le répertoire Weblog.

- Installez le package à l'aide de la commande suivante :

  ```
  pkgadd -d
  ```

- La liste des packages disponibles s'affiche. Dans l'exemple suivant, un package Weblog est affiché :

  ```
  1 NSweblog NetScaler Weblogging (SunOS,sparc)7.0
  ```

Vous êtes invité à sélectionner les packages. Sélectionnez le numéro de package du blog à installer.

Après avoir sélectionné le numéro du package et appuyé sur **Entrée**, les fichiers sont extraits et installés dans les répertoires suivants :

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Pour vérifier si le package NSWL est installé, exécutez la commande suivante :

   ```
   pkginfo | grep NSweblog
   ```

2. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   pkgrm NSweblog
   ```

Installer le client NSWL sur Linux

> **Important**
>
> L'installation d'un client NSWL sur Linux remplace le fichier de configuration. Vous devez effectuer une sauvegarde avant de l'installer.

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le `nswl_linux-<release number>-<build number>.rpm` fichier du package.
2. Copiez le fichier extrait sur un système exécutant le système d'exploitation Linux sur lequel vous souhaitez installer le client NSWL.
3. Pour installer le package NSWL, exécutez la commande suivante :

   ```
   rpm -i nswl_linux-9.3-51.5.rpm
   ```

Cette commande extrait les fichiers et les installe dans les répertoires suivants.

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin

- /usr/local/netscaler/samples

1. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   rpm -e NSweblog
   ```

2. Pour obtenir plus d'informations sur le fichier Weblog RPM, exécutez la commande suivante :

   ```
   rpm -qpi *.rpm
   ```

3. Pour afficher les fichiers journaux du serveur Web installés, exécutez la commande suivante :

   ```
   rpm -qpl *.rpm
   ```

Installer le client NSWL sur FreeBSD

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le nswl_bsd-<release number>-<build number>.tgz fichier du package.
2. Copiez le fichier extrait sur un système exécutant FreeBSD OS sur lequel vous souhaitez installer le client NSWL.
3. Pour installer le package NSWL, exécutez la commande suivante :

   ```
   pkg_add nswl_bsd-9.3-51.5.tgz
   ```

Cette commande extrait les fichiers et les installe dans les répertoires suivants.

```
1 -  /usr/local/netscaler/etc
2 -  /usr/local/netscaler/bin
3 -  /usr/local/netscaler/samples
```

1. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   pkg_delete NSweblog
   ```

2. Pour vérifier que le package est installé, exécutez la commande suivante :

   ```
   pkg_info | grep NSweblog
   ```

Installation du client NSWL sur Mac

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le nswl_macos-<release number>-<build number>.tgz fichier du package.
2. Copiez le fichier extrait sur un système exécutant macOS sur lequel vous souhaitez installer le client NSWL.

3. Pour installer le package NSWL, exécutez la commande suivante :

   ```
   pkg_add nswl_macos-9.3-51.5.tgz
   ```

Cette commande extrait les fichiers et les installe dans les répertoires suivants :

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   pkg_delete NSweblog
   ```

2. Pour vérifier que le package est installé, exécutez la commande suivante :

   ```
   pkg_info | grep NSweblog
   ```

Installation du client NSWL sous Windows

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le `nswl_win-<release number>-<build number>.zip` fichier du package.
2. Copiez le fichier extrait sur un système Windows sur lequel vous souhaitez installer le client NSWL.
3. Sur le système Windows, décompressez le fichier dans un répertoire (appelé `<NSWL-HOME>`). Les répertoires suivants sont extraits : `/bin`, `/etc` et `/samples`.
4. À l'invite de commandes, exécutez la commande suivante à partir du `<NSWL-HOME>\bin directory`:

   ```
   nswl -install -f <directorypath>\log.conf
   ```

Où,

Le chemin du répertoire fait référence au chemin du fichier de configuration (log.conf). Par défaut, le fichier se trouve dans le `/etc` répertoire `<NSWL-HOME>` and. Vous pouvez copier le fichier de configuration dans n'importe quel autre répertoire.

> **Remarque**
>
> Pour désinstaller le client NSWL, à l'invite de commandes, exécutez la commande suivante à partir du `<NSWL-HOME>\bin directory`:

```
1 > nswl -remove
```


Installer le client NSWL sur le système AIX

Pour installer le client NSWL, effectuez les opérations suivantes sur le système sur lequel vous avez téléchargé le package.

1. Extrayez le `nswl_aix-<release number>-<build number>.rpm` fichier du package.
2. Copiez le fichier extrait sur un système exécutant le système d'exploitation AIX sur lequel vous souhaitez installer le client NSWL.
3. Pour installer le package NSWL, exécutez la commande suivante :

   ```
   rpm -i nswl_aix-9.3-51.5.rpm
   ```

Cette commande extrait les fichiers et les installe dans les répertoires suivants.

- `/usr/local/netscaler/etc`
- `/usr/local/netscaler/`
- `usr/local/netscaler/samples`

1. Pour désinstaller le package NSWL, exécutez la commande suivante :

   ```
   rpm -e NSweblog
   ```

2. Pour obtenir plus d'informations sur le fichier Weblog RPM, exécutez la commande suivante :

   ```
   rpm -qpi *.rpm
   ```

3. Pour afficher les fichiers journaux du serveur Web installés, exécutez la commande suivante :

   ```
   rpm -qpl *.rpm
   ```

Configurer le client NSWL

May 5, 2023

Après avoir installé le client NSWL, vous pouvez configurer le client NSWL à l'aide de l'exécutable nswl. Ces configurations sont stockées dans le fichier de configuration du client NSWL (log.conf).

> **Remarque :**
>
> Vous pouvez personnaliser davantage la journalisation sur le client NSWL en apportant davantage de modifications au fichier de configuration NSWL (log.conf). Pour plus de détails, voir Personnalisation de la journalisation sur le système client NSWL.

Le tableau suivant décrit les commandes que vous pouvez utiliser pour configurer le client NSWL.

commande NSWL	Spécifie
nswl -aide	Les options d'aide NSWL disponibles.
nswl -addns -f <path-to-configuration-file>	Système qui collecte les données de transaction du journal. Vous êtes invité à saisir l'adresse IP de l'appliance NetScaler. Entrez un nom d'utilisateur et un mot de passe valides.
nswl -verify -f <path-to-configuration-file>	Vérifiez les erreurs de syntaxe ou de sémantique dans le fichier de configuration.
nswl -start -f <path-to-configuration-file>	Démarrez le client NSWL en fonction des paramètres du fichier de configuration. Remarque : Pour Solaris et Linux : pour démarrer la journalisation du serveur Web en arrière-plan, tapez le signe esperluette (&) à la fin de la commande.
nswl -stop (Solaris et Linux uniquement)	Arrêtez le client NSWL s'il a été démarré en arrière-plan ; sinon, utilisez CTRL+C pour arrêter la journalisation du serveur Web.
nswl -install -f <path-to-configuration-file> (Windows uniquement)	Installez le client NSWL en tant que service sous Windows.
nswl -startservice (Windows uniquement)	Démarrez le client NSWL en utilisant les paramètres du fichier de configuration spécifié dans l'option d'installation nswl. Vous pouvez également démarrer le client NSWL à partir de **Démarrer > Panneau de configuration > Services**. Remarque : les fichiers journaux NSWL sont créés dans C:\Windows\SysWOW64.
nswl -stopservice (Windows uniquement)	Arrête le client NSWL.
nswl -supprimer	Supprimez le service client NSWL du registre.

Exécutez les commandes suivantes à partir du répertoire dans lequel se trouve l'exécutable NSWL :

- `Windows: \ns\bin`
- `Solaris and Linux: \usr\local\netscaler\bin`

Les fichiers de configuration de journalisation du serveur Web se trouvent dans le chemin d'accès au répertoire suivant :

- Windows: \ns\etc
- Solaris and Linux: \usr\local\netscaler\etc

L'exécutable NSWL est démarré en tant que. \ nswl sous Linux et Solaris.

Ajoutez les adresses IP de l'appliance NetScaler

Dans le fichier de configuration du client NSWL (log.conf), ajoutez l'adresse IP NetScaler (NSIP) à partir de laquelle le client NSWL commence à collecter des journaux.

Pour ajouter l'adresse NSIP de l'appliance NetScaler

1. À l'invite de commande du système client, tapez :

   ```
   nswl -addns -f < directorypath > \log.conf
   < directorypath >: Specifies the path to the configuration file (log.
   conf).
   ```

2. À l'invite suivante, saisissez les informations suivantes :

   - **NSIP** : Spécifiez l'adresse IP de l'appliance NetScaler.
   - Nom d'utilisateur et mot de passe : Spécifiez les informations d'identification utilisateur nsroot de l'appliance NetScaler.

     > **Remarque :**
     >
     > Tout utilisateur du système disposant du privilège de journalisation activé prend en charge cette fonctionnalité.

> **Remarque :**
>
> Si vous ajoutez plusieurs adresses IP NetScaler (NSIP) et que vous ne souhaitez pas ultérieurement enregistrer tous les détails du journal système NetScaler, vous pouvez supprimer les adresses NSIP manuellement en supprimant l'instruction NSIP à la fin du fichier log.conf. Lors d'une configuration de basculement, vous devez ajouter les adresses IP NetScaler principales et secondaires au log.conf à l'aide de la commande. Avant d'ajouter l'adresse IP, assurez-vous que le nom d'utilisateur et le mot de passe existent sur les appliances NetScaler.

Vérifiez le fichier de configuration NSWL

Pour vous assurer que la journalisation fonctionne correctement, recherchez des erreurs de syntaxe dans le fichier de configuration NSWL (log.conf) sur le système client.

Pour vérifier la configuration dans le fichier de configuration NSWL

À l'invite de commande du système client, tapez :


```
nswl -verify -f <directorypath>\log.conf
```

< directorypath>: spécifie le chemin d'accès au fichier de configuration (log.conf).

Exécuter le client NSWL

Démarrer la journalisation du serveur Web

À l'invite de commande du système client, tapez :

```
nswl -start -f <directorypath>\log.conf
```

<directorypath>: spécifie le chemin d'accès au fichier de configuration (log.conf).

Arrêt de la journalisation du serveur Web lancé en arrière-plan sur les systèmes d'exploitation Solaris ou Linux

À l'invite de commande, tapez :

```
nswl -stop
```

Pour arrêter la journalisation du serveur Web démarrée en tant que service sur le système d'exploitation Windows

À l'invite de commande, tapez :

```
nswl -stopservice
```

Personnaliser la connexion sur le système client NSWL

May 5, 2023

Vous pouvez personnaliser la journalisation sur le système client NetScaler Web Logging (NSWL) en apportant d'autres modifications au fichier de configuration du client NSWL (log.conf). Utilisez un éditeur de texte pour modifier le fichier de configuration log.conf sur le système client.

Pour personnaliser la journalisation, utilisez le fichier de configuration pour définir les filtres et les propriétés du journal.

- **Filtres de journaux.** Filtrez les informations du journal en fonction de l'adresse IP de l'hôte, du nom de domaine et du nom d'hôte des serveurs Web.
- **Propriétés du journal.** Chaque filtre est associé à un ensemble de propriétés de journal. Les propriétés du journal définissent le mode de stockage des informations de journal filtrées.

Exemple de fichier de configuration

Voici un exemple de fichier de configuration :

```
##########
# This is the NSWL configuration file
# Only the default filter is active
# Remove leading # to activate other filters
##########
##########
# Default filter (default on)
# W3C Format logging, new file is created every hour or on reaching 10 MB file size,
# and the file name is Exyymmdd.log
##########
Filter default
begin default
        logFormat               W3C
        logInterval             Hourly
        logFileSizeLimit        10
        logFilenameFormat       Ex%`{
 `%y%m%d }
 t.log
end default
##########
# NetScaler caches example
# CACHE_F filter covers all the transaction with HOST name www.netscaler.com and the listed server ip's
##########
#Filter CACHE_F HOST www.netscaler.com IP 192.168.100.89 192.168.100.95 192.168.100.52 192.168.100.53 ON
##########
# netscaler origin server example
# Not interested in Origin server to Cache traffic transaction logging
##########
#Filter ORIGIN_SERVERS IP 192.168.100.64 192.168.100.65 192.168.100.66 192.168.100.67 192.168.100.225 192.168.100.226 192.168.100.227 192.168.100.228 OFF
##########
# netscaler image server example
# all the image server logging.
##########
#Filter IMAGE_SERVER HOST www.netscaler.images.com IP 192.168.100.71 192.168.100.72 192.168.100.169 192.168.100.170 192.168.100.171 ON
```



```
##########
# NCSA Format logging, new file is created every day midnight or on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log.
# Exclude objects that ends with .png .jpg .jar.
##########
#begin ORIGIN_SERVERS
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        40
#       logFilenameFormat       /datadisk5/ORGIN/log/%v/NS%`{
 `%m%d%y }
 t.log
#       logExclude              .png .jpg .jar
#end ORIGIN_SERVERS

##########
# NCSA Format logging, new file is created every day midnight or on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log with log record timestamp as GMT.
##########
#begin CACHE_F
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk5/netscaler/log/%v/NS%`{
 `%m%d%y }
 t.log
#       logtime                 GMT
#end CACHE_F

##########
# W3C Format logging, new file on reaching 20MB and the log file path name is
# atadisk6/netscaler/log/server's ip/Exmmyydd.log with log record timestamp as LOCAL.
##########
#begin IMAGE_SERVER
#       logFormat               W3C
#       logInterval             Size
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk6/netscaler/log/%AEx%`{
 `%m%d%y }
```



```
 t
#       logtime                 LOCAL
#end IMAGE_SERVER

##########
# Virtual Host by Name firm, can filter out the logging based on the
   host name by,
##########

#Filter VHOST_F IP 10.101.2.151 NETMASK 255.255.255.0
#begin VHOST_F
#       logFormat               W3C
#       logInterval             Daily
#       logFileSizeLimit        10
logFilenameFormat /ns/prod/vhost/%v/Ex%`{
 `%m%d%y }
 t
#end VHOST_F

########## END FILTER CONFIGURATION ##########
<!--NeedCopy-->
```

Créer des filtres

Vous pouvez utiliser la définition de filtre par défaut dans le fichier de configuration (log.conf), ou modifier le filtre ou créer un filtre. Vous pouvez créer plusieurs filtres de journal.

> **Remarque :**
>
> La journalisation consolidée, qui enregistre les transactions pour lesquelles aucun filtre n'est défini, utilise le filtre par défaut s'il est activé. La journalisation consolidée de tous les serveurs peut être effectuée en définissant uniquement le filtre par défaut.

Si le serveur héberge plusieurs sites Web et que chaque site Web possède son propre nom de domaine et que chaque domaine est associé à un serveur virtuel, vous pouvez configurer la journalisation du serveur Web pour créer un répertoire de journaux distinct pour chaque site Web. Le tableau suivant affiche les paramètres de création d'un filtre.

Tableau 1. Paramètres de création d'un filtre

Paramètre	Spécifie
FilterName	Nom du filtre. Le nom du filtre peut inclure des caractères alphanumériques et ne peut pas dépasser 59 caractères. Les noms de filtre de plus de 59 caractères sont tronqués à 59 caractères.
Nom d'hôte	Nom d'hôte du serveur pour lequel les transactions sont enregistrées.
IP `ip`	Adresse IP du serveur pour lequel les transactions doivent être consignées (par exemple, si le serveur a plusieurs domaines qui ont une adresse IP).
IP `ip 2...ip` n :	Plusieurs adresses IP (par exemple, si le domaine du serveur a plusieurs adresses IP).
IP ip6	Adresse IPv6 du serveur pour lequel les transactions doivent être consignées.
IP du masque de sous-réseau IP	Combinaison d'adresses IP et de masque de réseau à utiliser sur un sous-réseau.
`ON | OFF`	Activez ou désactivez le filtre pour consigner les transactions. Si aucun argument n'est sélectionné, le filtre est activé (ON).

Pour créer un filtre, saisissez la commande suivante dans le fichier log.conf :

- `filter <filterName> <HOST name> | [IP<ip> ] | [IP<ip 2...ip n> ] | <IP ip NETMASK mask> [ON | OFF]`
- `filter <filterName> <HOST name> | [IP6 ip/<prefix length>] [ON | OFF]`

Création d'un filtre pour un serveur virtuel

Pour créer un filtre pour un serveur virtuel, entrez la commande suivante dans le fichier log.conf :

`filter <filterName> <VirtualServer IP address>`

Exemple

Dans l'exemple suivant, vous spécifiez une adresse IP 192.168.100.0 et un masque réseau 255.255.255.0. Le filtre s'applique aux adresses IP 192.168.100.1 à 192.168.100.254.


```
Filter F1 HOST www.netscaler.com ON
Filter F2 HOST www.netscaler.com IP 192.168.100.151 ON
Filter F3 HOST www.netscaler.com IP 192.168.100.151 192.165.100.152 ON
Filter F4 IP 192.168.100.151
Filter F5 IP 192.168.100.151 HOST www.netscaler.com OFF
Filter F6 HOST www.netscaler.com HOST www.xyz.com HOST www.abcxyz.com
   IP 192.168.100.200 ON
Filter F7 IP 192.250.100.0 NETMASK 255.255.255.0
Filter F8 HOST www.xyz.com IP 192.250.100.0 NETMASK 255.255.255.0 OFF
For creating filters for servers having IPv6 addresses.
Filter F9 2002::8/112 ON
Filter F10 HOST www.abcd.com IP6 2002::8 ON

<!--NeedCopy-->
```

Spécifier les propriétés du

Les propriétés du journal sont appliquées à toutes les entrées de journal associées au filtre. La définition de la propriété log commence par le mot-clé `BEGIN` et se termine par, `END` comme illustré dans l'exemple suivant :

```
BEGIN <filtername>
 logFormat ...
 logFilenameFormat ...
 logInterval ...
 logFileSize ....
 logExclude ....
 logTime ….
 END
<!--NeedCopy-->
```

Les entrées de la définition peuvent inclure les éléments suivants :

- **LogFormat** spécifie la fonctionnalité de journalisation du serveur Web qui prend en charge les formats de fichiers journaux NCSA, W3C Extended et personnalisés.

Par défaut, la `logformat` propriété est w3c. Pour remplacer, entrez personnalisé ou NCSA dans le fichier de configuration, par exemple :

```
LogFormat NCSA
<!--NeedCopy-->
```


> **Remarque :**
>
> Pour le format NCSA et les formats de journaux personnalisés, l'heure locale est utilisée pour les transactions d'horodatage et pour la rotation des fichiers.

- **LogInterval** spécifie les intervalles auxquels les nouveaux fichiers journaux sont créés. Utilisez l'une des valeurs suivantes :
  - Toutes les heures : Un fichier est créé toutes les heures.
  - Quotidien : Un fichier est créé tous les jours à minuit. Valeur par défaut.
  - Hebdomadaire : Un fichier est créé tous les dimanches à minuit.
  - Mensuel : Un fichier est créé le premier jour du mois à minuit.
  - Aucun : un fichier n'est créé qu'une seule fois, lorsque la journalisation du serveur Web démarre.

Exemple :

```
1 LogInterval Daily
2 <!--NeedCopy-->
```

LogFileSizeLimit spécifie la taille maximale du fichier journal en Mo. Il peut être utilisé avec n'importe quel intervalle de log (hebdomadaire, mensuel, etc.) Un fichier est créé lorsque la limite de taille maximale du fichier est atteinte ou lorsque l'intervalle de journalisation défini s'écoule.

Pour remplacer ce comportement, spécifiez la taille en tant que propriété `loginterval` afin qu'un fichier soit créé uniquement lorsque la limite de taille du fichier journal est atteinte.

La valeur par défaut `LogFileSizeLimit` est de 10 Mo.

Exemple :

```
1 LogFileSizeLimit 35
2 <!--NeedCopy-->
```

- **LogFileNameFormat** spécifie le format du nom de fichier du fichier journal. Le nom du fichier peut être du type suivant :
  - Statique : spécifie une chaîne constante qui contient le chemin absolu et le nom de fichier.

    Dynamique : spécifie une expression contenant le format suivant :
    - Adresse IP du serveur
    - Date (% {format} t)
    - Suffixe d'URL (%x)
    - Nom d'hôte (%v)

Exemple :


```
LogFileNameFormat Ex%`{
 `%m%d%y }
 t.log
<!--NeedCopy-->
```

Cette commande crée le premier nom de fichier Exmmddyy.log, puis chaque heure crée un fichier avec un nom de fichier : Exmmddyy.log.0, Exmmddyy.Log.1,…, Exmmddyy.log.N.

Exemple :

```
      LogInterval size
      LogFileSize 100
      LogFileNameFormat Ex%`{
 `%m%d%y }
 t
<!--NeedCopy-->
```

> **Attention :**
>
> Le format de date%t spécifié dans la commande LogFileNameFormat remplace la propriété d'intervalle de journalisation de ce filtre. Pour empêcher la création d'un nouveau fichier tous les jours plutôt que lorsque la taille du fichier journal spécifiée est atteinte, n'utilisez pas%t dans LogFileNameFormat.

- **LogExclude** empêche la journalisation des transactions avec les extensions de noms de fichiers spécifiées.

Exemple :

```
LogExclude.html
<!--NeedCopy-->
```

Cette commande crée un fichier journal qui exclut les transactions de journal pour les fichiers*.html.

LogTime spécifie l'heure du journal au format GMT ou LOCAL.

Les valeurs par défaut sont les suivantes :

- Format du fichier journal NCSA : LOCAL
- Format du fichier journal W3C : GMT.

Comprendre les formats de journaux NCSA et W3C

NetScaler prend en charge les formats de fichiers journaux standard suivants :

- Format de journal commun NCSA
- Format de journal étendu W3C

Format de journal commun NCSA

Si le format du fichier journal est NCSA, le fichier journal affiche les informations de journal au format suivant :

```
1 Client_IP_address -User_Name [Date:Time -TimeZone] "Method Object
     HTTP_version" HTTP_StatusCode BytesSent
2 <!--NeedCopy-->
```

Pour utiliser le format de journal commun NCSA, entrez **NCSA** dans l'argument LogFormat du `log.conf` fichier.

Le tableau suivant décrit le format de journal commun NCSA.

Argument	Spécifie
Adresse_IP_client	L'adresse IP de l'ordinateur client.
Nom d'utilisateur	Le nom d'utilisateur.
Date	Date de la transaction.
Time	L'heure à laquelle la transaction a été terminée.
Fuseau horaire	Le fuseau horaire (Greenwich Mean Time ou heure locale).
Method	La méthode de demande (par exemple ; GET, POST).
Objet	L'URL.
HTTP_version	La version de HTTP utilisée par le client.
HTTP_StatusCode	Code d'état de la réponse.
Bytes Sent	Le nombre d'octets envoyés par le serveur.

Format de journal étendu W3C

Un fichier journal étendu contient une séquence de lignes contenant des caractères ASCII terminées par un saut de ligne (LF) ou la séquence saut de ligne retour chariot (CRLF). Les générateurs de fichiers journaux doivent respecter la convention de fin de ligne pour la plate-forme sur laquelle ils sont exécutés.

Les analyseurs de log doivent accepter le formulaire LF ou CRLF. Chaque ligne peut contenir une directive ou une entrée. Si vous souhaitez utiliser le format de journal étendu W3C, entrez W3C comme argument Log Format dans le fichier log.conf.

Par défaut, le format de journal standard du W3C est défini en interne comme format de journal personnalisé, comme suit :

```
%`{
 `%Y-%m-%d%H:%M:%S }
 t %a %u %S %A %p %m %U %q %s %j %J %T %H %+{
 user-agent }
 i %+{
 cookie }
  i%+{
 referer }
 i
<!--NeedCopy-->
```

Vous pouvez également modifier l'ordre ou supprimer certains champs dans ce format de journal W3C. Par exemple :

```
logFormat W3C %`{
 `%Y-%m-%d%H:%M:%S }
 t %m %U
<!--NeedCopy-->
```

Les entrées de journal du W3C sont créées au format suivant :

```
#Version: 1.0
#Fields: date time cs-method cs-uri
#Date: 12-Jun-2001 12:34
2001-06-12 12:34:23 GET /sports/football.html 2001-06-12 12:34:30
GET /sports/football.html
<!--NeedCopy-->
```

Entrées

Les entrées consistent en une séquence de champs relatifs à une seule transaction HTTP. Les champs sont séparés par des espaces blancs. Citrix recommande l'utilisation de caractères de tabulation. Si un champ d'une entrée particulière n'est pas utilisé, un tiret (-) marque le champ omis.

Directives

Consultez le tableau Directives pour plus d'informations sur le processus de journalisation. Les lignes commençant par le signe dièse (#) contiennent des directives.

Exemple :

L'exemple de fichier journal suivant montre les entrées de journal au format journal étendu W3C :


```
#Version: 1.0
#Fields: time cs-method cs-uri
#Date: 12-Jan-1996 00:00:00
00:34:23 GET /sports/football.html
12:21:16 GET /sports/football.html
12:45:52 GET /sports/football.html
12:57:34 GET /sports/football.html
<!--NeedCopy-->
```

Champs

La directive Fields répertorie une séquence d'identificateurs de champ qui spécifient les informations enregistrées dans chaque entrée. Les identificateurs de champs peuvent comporter l'une des formes suivantes :

- **identificateur :** se rapporte à l'ensemble de la transaction.
- **prefix-identifier :** concerne le transfert d'informations entre parties définies par le préfixe de valeur.
- **prefix (header) :** spécifie la valeur de l'en-tête du champ d'en-tête HTTP pour le transfert entre parties défini par le préfixe de valeur. Les champs spécifiés de cette manière ont toujours le type.

Le tableau suivant décrit les préfixes définis.

Préfixe	Spécifie
c	Client
s	Serveur
r	Distant
cs	Client vers serveur
cs	Serveur vers client
sr	Serveur vers serveur distant (préfixe utilisé par les proxies)
rs	Serveur à serveur distant (préfixe utilisé par les proxies)
x	Identifiant spécifique à l'application

Exemples :

Les exemples suivants sont des identificateurs définis qui utilisent des préfixes :

cs-method : La méthode dans la requête envoyée par le client au serveur.

sc (Referer) : Le `Referer` champ de la réponse.

c-ip : L'adresse IP du client.

Identifiants

Le tableau suivant décrit les identificateurs de format de journal étendu du W3C qui ne nécessitent pas de préfixe.

Identifiant	Description
date	Date à laquelle la transaction a été effectuée.
temps	L'heure à laquelle la transaction est terminée.
temps pris	Le temps (en secondes) nécessaire à la réalisation de la transaction.
octets	Le nombre d'octets transférés.
mis en cache	Enregistre si un accès au cache s'est produit. Un zéro indique l'absence d'un cache.

Le tableau suivant décrit les identificateurs de format de journal étendu du W3C qui nécessitent un préfixe.

Identifiant	Description
IP	L'adresse IP et le numéro de port.
DNS	Nom DNS.
état	Le code d'état.
comment	Le commentaire est retourné avec un code d'état.
method	La méthode.
url	L'URL.
url-stem	La partie racine de l'URL.
url-query	Partie requête de l'URL.

Le format de fichier journal étendu du W3C vous permet de choisir des champs de journal. Ces champs sont présentés dans le tableau suivant.

Champ	Description
Date	Date à laquelle la transaction est effectuée.
Time	L'heure à laquelle la transaction est terminée.
IP du client	L'adresse IP du client.
Nom d'utilisateur	Le nom d'utilisateur.
Service Name	Le nom du service, qui est toujours HTTP.
Server IP	L'adresse IP du serveur.
Server Port	Le numéro de port du serveur
Method	La méthode de demande (par exemple ; GET, POST).
Url Stem	La ressource de l'URL.
Url Query	Partie requête de l'URL.
HTTP Status	Code d'état de la réponse.
Bytes Sent	Le nombre d'octets envoyés au serveur (taille de la demande, y compris les en-têtes HTTP).
Bytes Received	Le nombre d'octets reçus du serveur (taille de la réponse, y compris les en-têtes HTTP).
Time Taken	Le temps nécessaire à la réalisation d'une transaction, en secondes.
Protocol Version	Numéro de version du protocole HTTP utilisé par le client.
User Agent	Le champ **User-Agent** dans le protocole HTTP.
Cookie	Le champ **Cookie** du protocole HTTP.
`Referer`	Champ `Referer` du protocole HTTP.

Création d'un format de journal personnalisé

Vous pouvez personnaliser le format d'affichage des données du fichier journal manuellement ou à l'aide de la bibliothèque NSWL. En utilisant le format de journal personnalisé, vous pouvez dériver la plupart des formats de journaux actuellement pris en charge par Apache.

Création d'un format de journal personnalisé à l'aide de la bibliothèque NSWL

Utilisez l'une des bibliothèques NSWL suivantes selon que l'exécutable NSWL a été installé sur un ordinateur hôte Windows ou Solaris :

- **Windows :** bibliothèque nswl.lib du répertoire `\ns\bin` de l'ordinateur hôte du gestionnaire du système.
- **Solaris :** bibliothèque `libnswl.a` dans `usr/local/netscaler/bin`.

1. Ajoutez les deux fonctions C suivantes définies par le système dans un fichier source C :

   ns_userDefFieldName() : Cette fonction renvoie la chaîne qui doit être ajoutée en tant que nom de champ personnalisé dans l'enregistrement du journal.

   ns_userDefFieldVal() : Cette fonction implémente la valeur de champ personnalisée, puis la renvoie sous forme de chaîne qui doit être ajoutée à la fin de l'enregistrement de journal.

2. Compilez le fichier dans un fichier objet.
3. Liez le fichier objet à la bibliothèque NSWL (et éventuellement à des bibliothèques tierces) pour former un nouvel exécutable NSWL.
4. Ajoutez une chaîne %d à la fin de la chaîne LogFormat dans le fichier de configuration (log.conf).

Exemple :

```
##########
# A new file is created every midnight or on reaching 20MB file size,
# and the file name is
/datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log and create
digital
#signature field for each record.
BEGIN CACHE_F
    logFormat custom "%a - "%{
 user-agent }
 i" [%d/%B/%Y %T -%g] "%x"
%s %b%{
 referrer }
 i "%{
 user-agent }
 i" "%{
 cookie }
 i" %d "
    logInterval Daily
    logFileSizeLimit 20
    logFilenameFormat
/datadisk5/netscaler/log/%v/NS%`{
 `%m%d%y }
```



```
 t.log
END CACHE_F
<!--NeedCopy-->
```

Création manuelle d'un format de journal personnalisé

Pour personnaliser le format dans lequel les données du fichier journal doivent apparaître, spécifiez une chaîne de caractères comme argument de la définition de la propriété de **journal LogFormat** . Voici un exemple où des chaînes de caractères sont utilisées pour créer un format de journal :

```
LogFormat Custom ""%a - "%{
 user-agent }
 i" %[%d/%m/%Y]t %U %s %b %T"
<!--NeedCopy-->
```

- La chaîne peut contenir les caractères de contrôle de type "c" \n et \t pour représenter de nouvelles lignes et onglets.
- Utilisez la touche Echap avec des guillemets littéraux et des barres obliques inverses.

Les caractéristiques de la demande sont consignées en plaçant les directives % dans la chaîne de format, qui sont remplacées dans le fichier journal par les valeurs.

Si le spécificateur de format%v (nom d'hôte) ou%x (suffixe d'URL) est présent dans une chaîne de format de nom de fichier journal, les caractères suivants du nom de fichier sont remplacés par un symbole de trait de soulignement dans le nom du fichier de configuration du journal :

```
" *. /: < > ? \ |
```

Les caractères dont les valeurs ASCII se situent entre 0 et 31 sont remplacés par ce qui suit :

```
%<ASCII value of character in hexadecimal>.
```

Par exemple, le caractère avec la valeur ASCII 22 est remplacé par%16.

> **Attention :**
>
> Si le spécificateur de format%v est présent dans une chaîne de format de nom de fichier journal, un fichier distinct est ouvert pour chaque hôte virtuel. Pour garantir une journalisation continue, le nombre maximal de fichiers qu'un processus peut ouvrir doit être suffisamment volumineux. Consultez la documentation de votre système d'exploitation pour obtenir une procédure permettant de modifier le nombre de fichiers pouvant être ouverts.

Création de formats de journaux Apache

Vous pouvez dériver des journaux personnalisés la plupart des formats de journaux actuellement pris en charge par Apache. Les formats de journal personnalisés qui correspondent aux formats de journal

Apache sont les suivants :

NCSA/combiné : LogFormat personnalisé%h%l%u [%t] « %r » %S%B « % {referer} i » « % {user-agent} i »

NCSA/Common: LogFormat custom %h %l %u [%t] “%r” %s %B

Referer Journal : LogFormat personnalisé « % {referer} i » ->%U

Agent utilisateur : LogFormat custom% {user-agent} i

De même, vous pouvez dériver les autres formats de journal du serveur à partir des formats personnalisés.

Arguments de définition d’un format de journal personnalisé

Le tableau suivant décrit le format de journal personnalisé.

Argument	Spécifie
%a	Adresse IPv4 distante.
%A	Adresse IPv4 locale.
%a6	Adresse IPv6 distante.
%A6	Adresse IPv6 locale.
%B	Octets envoyés, à l’exception des en-têtes HTTP (taille de réponse).
%b	Octets reçus, à l’exception des en-têtes HTTP (taille de la requête).
%d	Champ défini par l’utilisateur.
%K	Informations sur le port du client.
%e1	Valeur du premier en-tête de requête HTTP personnalisé.
%e2	Valeur du deuxième en-tête de requête HTTP personnalisé.
%E1	Valeur du premier en-tête de réponse HTTP personnalisé.

Argument	Spécifie
%E2	Valeur du deuxième en-tête de réponse HTTP personnalisé. Remarque : Pour obtenir des instructions sur la façon d'exporter des en-têtes HTTP personnalisés, voir Configuration de NetScaler pour la journalisation du serveur Web
%g	Décalage horaire moyen de Greenwich (par exemple, -0800 pour l'heure normale du Pacifique).
%h	Adresse IPv4 d'un hôte distant.
%h6	Adresse IPv6 d'un hôte distant.
H	Protocole de demande.
% {Foobar}i	Contenu de la ou des lignes d'en-tête Foobar : dans la requête envoyée au serveur. Le système prend en charge les en-têtes User-Agent, Referer et cookie. Le signe + après le % dans ce format indique au client de journalisation d'utiliser le signe + comme séparateur de mots.
%j	Octets reçus, y compris les en-têtes (taille de la demande).
%J	Octets envoyés, y compris les en-têtes (taille de réponse).
%l	Nom du journal distant (provenant d'identd, s'il est fourni).
%m	Méthode de demande.
%M	Temps nécessaire pour traiter la demande (en microsecondes).
% {Foobar}o	Contenu de Foobar : ligne (s) d'en-tête dans la réponse. USER -AGENT, Referrer et les en-têtes de cookie (y compris les en-têtes de cookie définis) sont pris en charge.
%p	Port canonique du serveur qui traite la requête.
%P	La partition d'administration.

Argument	Spécifie
%q	Chaîne de requête (préfixée par un point d'interrogation (?) s'il existe une chaîne de requête).
%r	Première ligne de la demande.
%s	Les demandes qui ont été redirigées en interne, il s'agit de l'état de la demande d'origine.
%t	Heure, au format de journal commun (format d'heure anglais standard).
% {format} t	L'heure, sous la forme donnée par format, doit être au format strftime (3). Pour la description des formats, voir Définition du format temporel.
%T	Temps nécessaire pour traiter la demande, en secondes.
%u	Utilisateur distant (depuis auth ; peut être bidon si l'état de retour (%s) est 401).
%U	Chemin de l'URL demandé.
%v	Nom canonique du serveur qui traite la requête.
%V6	Adresse IPv6 du serveur virtuel dans le système, si l'équilibrage de charge, la commutation de contenu et/ou la redirection de cache sont utilisés.
%D	Imprime l'ID de transaction HTTP.
%L	Durée de la transaction en millisecondes.
%R	Chaîne de motif HTTP mappée au code d'état.
%f	Journalisation du port source.
%V	Adresse IPv4 du serveur virtuel.

> **Remarque**
>
> Pour obtenir des instructions sur la façon d'exporter des en-têtes HTTP personnalisés, voir Configuration de NetScaler pour lajournalisation du serveur Web

Par exemple, si vous définissez le format du journal comme `%+{ user-agent } i`et si la valeur de

l'agent utilisateur est NetScaler system Web Client, les informations sont enregistrées sous la forme NetScaler System+Web+Client. Une alternative consiste à utiliser des guillemets doubles. Par exemple, « % {user-agent} i » l'enregistre en tant que « Client Web du système NetScaler ». « N'utilisez pas la touche \<Esc\> sur les chaînes de caractères %.. .r, %. . .i et, %. . .o. Il est conforme aux exigences du format de journal commun. Les clients peuvent insérer des caractères de contrôle dans le journal. Par conséquent, vous devez faire attention lorsque vous travaillez avec des fichiers journaux bruts.

Définition du format temporel

Le tableau suivant décrit la définition du format d'heure pour connaître la partie format de la chaîne `%{ format } t` décrite dans le tableau Format de journal personnalisé. Les valeurs entre crochets ([ ]) indiquent la plage de valeurs qui apparaît. Par exemple, [1,31] dans la description de %d dans le tableau suivant indique que %d varie de 1 à 31.

Argument	Spécifie
————	———-
%%	Identique à %.
%a	Nom abrégé du jour de la semaine pour les paramètres régionaux.
%A	Le nom complet du jour de la semaine pour les paramètres régionaux
%b	Le nom abrégé du mois pour les paramètres régionaux.
%B	Le nom complet du mois pour la langue.
%C	Le nombre du siècle (l'année divisée par 100 et tronquée à un nombre entier sous la forme d'un nombre décimal `[1,99]`) ; les chiffres uniques sont précédés d'un 0.
%d	Champ défini par l'utilisateur.
%K	Le nombre du siècle (l'année divisée par 100 et tronquée à un nombre entier sous la forme d'un nombre décimal `[1,99]`) ; les chiffres uniques sont précédés d'un 0.
%e	Le jour du mois `[1,31]` ; les chiffres uniques sont précédés d'un blanc.
%h	Le nom abrégé du mois pour les paramètres régionaux.
%H	L'heure (24 heures) `[0,23]` ; les chiffres uniques sont précédés d'un 0.
%I	L'heure (horloge de 12 heures) `[1,12]` ; les chiffres uniques sont précédés d'un 0.
%j	Le numéro du jour de l'année `[1,366]` ; les chiffres uniques sont précédés de 0.
%k	L'heure (24 heures) `[0,23]` ; les chiffres uniques sont précédés d'un blanc.
%l	L'heure (horloge de 12 heures) `[1,12]` ; les chiffres uniques sont précédés d'un blanc.
%m	Le numéro du mois de l'année `[1,12]` ; les chiffres uniques sont précédés d'un 0.
%M	Minute `[00,59]` ; 0 en début de ligne est autorisé mais non obligatoire.
%n	Insère une nouvelle ligne.
%p	L'équivalent du matin ou de l'après-midi pour les paramètres régionaux.
%r	La représentation horaire appropriée au format 12 heures avec %p
%S	Les secondes `[00,61]` ; la plage de valeurs est `[00,61]` plutôt que de `[00,59]` permettre la seconde intercalaire occasionnelle et la seconde intercalaire double.

%3	Les millisecondes `[000,999]` ; la plage de valeurs est `[000,999]`.
%6	Les microsecondes `[000000,999999]` ; la plage de valeurs est `[000000,999999]`.
%9	Les nanosecondes `[000000000,999999999]` ; la plage de valeurs est `[000000000,999999999]` .
%t	Insère une tabulation.
%u	Le jour de la semaine sous forme de nombre décimal `[1,7]`. 1 représente Dimanche, 2 représente mardi et ainsi de suite.
%U	Le numéro de la semaine de l'année sous forme de nombre décimal `[00,53]`, le dimanche étant le premier jour de la semaine 1.

> **Remarque :**
>
> Si vous spécifiez une conversion qui ne correspond à aucune des conversions décrites dans le tableau précédent ou à l'une des spécifications de conversion modifiées répertoriées dans le paragraphe suivant, le comportement est indéfini et renvoie 0.

La différence entre `%U` et `%W` (ainsi qu'entre les conversions modifiées `%OU` et `%OW`) est le jour considéré comme le premier jour de la semaine. La semaine numéro 1 est la première semaine de janvier (commençant par un dimanche pour `%U`, ou un lundi pour `%W`). Le numéro de semaine 0 contient les jours précédant le premier dimanche ou lundi de janvier pour `%U` et `%W`.

Afficher les journaux du serveur

Vous pouvez configurer une fonctionnalité NSWL pour afficher les journaux du serveur sur la console ou rediriger les journaux du serveur vers un répertoire de l'appliance NetScaler.

Il existe deux façons d'afficher les journaux sur la console (sortie standard) :
Option 1 : Afficher tous les journaux sur la console.
Option 2 : Afficher uniquement les journaux sélectionnés sur la console avec des filtres avec `logfilenameformat` comme `STDOUT`.

Call Home

May 5, 2023

Les appliances peuvent parfois ne pas fonctionner correctement en raison de problèmes logiciels ou matériels. Dans de tels cas, NetScaler doit collecter des données et résoudre les problèmes avant qu'un impact potentiel ne se produise sur le site du client. En activant Call Home sur votre appliance NetScaler, vous pouvez automatiser le processus de notification d'erreur. Non seulement vous évitez d'appeler le support NetScaler, de faire une demande de service et de télécharger des données

système avant que l'équipe d'assistance ne puisse résoudre le problème, mais le support peut également identifier et résoudre un problème avant qu'il ne survienne. Call Home surveille régulièrement l'appliance et télécharge automatiquement les données sur le serveur de support technique Citrix. En outre, les données Call Home entrantes fournissent des informations sur l'utilisation de NetScaler. Plusieurs équipes au sein de Citrix peuvent utiliser ces données pour améliorer la conception, le support et la mise en œuvre de NetScaler.

Par défaut, Call Home est activé sur toutes les plateformes et toutes les versions de NetScaler (MPX, VPX, SDX). En activant cette fonctionnalité, vous permettez à Citrix de collecter des données de déploiement et de télémétrie de NetScaler pour une meilleure mise en œuvre et un meilleur service de support.

> **Remarque**
>
> Vous pouvez également consulter la page FAQ Call Home pour obtenir des informations relatives à Call Home.

Avantages

Call Home offre les avantages suivants.

- Surveillez les conditions d'erreur matérielles et logicielles. Pour plus d'informations, consultez la section Surveiller les conditions d'erreur critiques.
- Notifiez les événements critiques ayant un impact sur votre réseau.
- Envoyez les données de performance et les détails d'utilisation du système à Citrix pour :
  - Analysez et améliorez la qualité des produits.
  - Fournir des informations de dépannage en temps réel pour une identification proactive des problèmes et une résolution plus rapide des problèmes.

Support de plateforme

La fonctionnalité Call Home est prise en charge sur toutes les plateformes NetScaler et tous les modèles d'appliances (MPX, VPX et SDX).

- NetScaler MPX : Tous les modèles MPX.
- NetScaler VPX : tous les modèles VPX, y compris les appliances VPX qui obtiennent leur licence auprès de pools de licences externes ou centraux.
- NetScaler SDX : surveille le lecteur de disque et les puces SSL attribuées pour détecter toute erreur ou défaillance. Toutefois, les instances VPX n'ont pas accès au bloc d'alimentation (PSU) et leur état n'est donc pas surveillé. Sur une plateforme SDX, vous pouvez configurer Call Home soit directement sur une instance individuelle, soit par l'intermédiaire de la SVM.

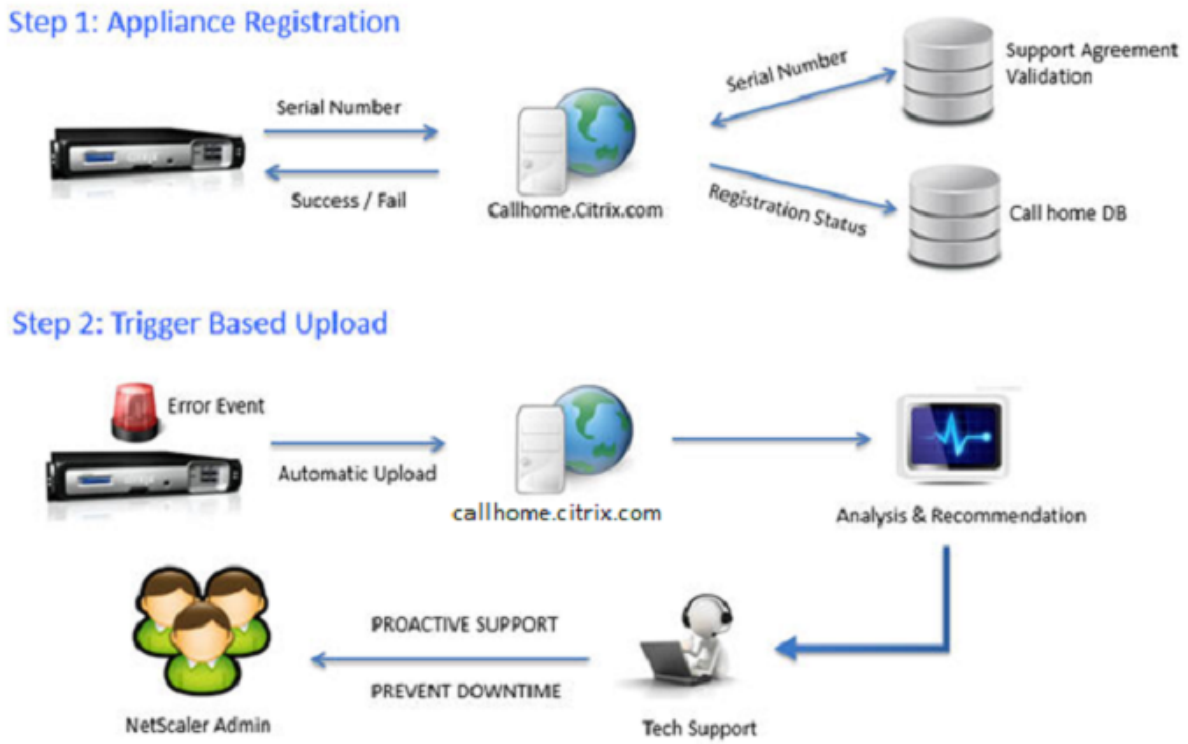
Composants requis

Pour utiliser Call Home, l'appliance NetScaler doit disposer des éléments suivants :

- **Connexion Internet.** Call Home nécessite une connexion Internet pour que NetScaler puisse se connecter au serveur de support NetScaler afin de télécharger une archive de données.
- **URL.** Call Home fonctionne en échangeant du trafic `callhome.citrix.com` via le protocole SSL/TLS en utilisant le port 443 pour le trafic bidirectionnel.

Comment fonctionne Call Home

La figure suivante montre un flux de travail de base de Call Home dans une appliance NetScaler déployée sur le site d'un client.



Voici le flux de travail d'un Call Home :

1. Configurez la connectivité Internet. Pour que Call Home télécharge les données système, votre appareil doit disposer d'une connexion Internet. Si ce n'est pas le cas, vous pouvez configurer une configuration de serveur proxy pour fournir une connectivité Internet. Pour plus d'informations, consultez la section Configuration de Call Home.

2. Activez Call Home. Lors de la mise à niveau de votre appliance vers la dernière version logicielle via l'interface de commande ou l'interface graphique NetScaler, Call Home est activé par défaut et le

système retarde le processus d'enregistrement de 24 heures. Au cours de cette période, vous pouvez choisir de désactiver manuellement la fonctionnalité, mais Citrix vous recommande de l'activer.

> **Remarque**
>
> Si vous mettez à niveau votre appliance à partir d'une ancienne version pour laquelle Call Home est explicitement désactivé, le système active toujours la fonctionnalité par défaut et affiche un message de notification lors de votre première connexion.

En outre, si vous effectuez des modifications de configuration pour une connectivité Internet, vous devez désactiver et activer Call Home. Il permet à Call Home de s'inscrire auprès du serveur Citrix Insight Services (CIS) sans erreur d'échec.

3. Enregistrez l'appliance NetScaler sur le serveur de support NetScaler. Lorsque Call Home enregistre l'appliance auprès du serveur de support NetScaler, le serveur vérifie la validité du numéro de série de l'appliance dans la base de données. Si le numéro de série est valide, le serveur enregistre l'appliance pour le service Call Home et envoie une réponse d'enregistrement réussie. Sinon, le serveur renvoie un message d'échec d'enregistrement. Les informations système de base sont envoyées sous forme de message séparé. Les données incluent les détails d'utilisation de la mémoire et du processeur ainsi que les numéros de débit. Les données sont envoyées périodiquement dans le cadre du message de pulsation tous les 7 jours, par défaut. Toutefois, une valeur inférieure à 5 jours n'est pas recommandée, car les téléchargements fréquents ne sont pas utiles.

4. Surveillez les conditions d'erreur critiques. Une fois enregistré, Call Home commence à surveiller l'appareil. Le tableau suivant répertorie les conditions que Call Home peut surveiller sur l'appliance.

Condition d'erreur critique	Description	Intervalle de surveillance Call Home	Nom d'alarme SNMP correspondant
Erreurs de lecteur flash compact	Le lecteur flash compact de l'appliance a rencontré des problèmes de lecture ou d'écriture.	24 heures	COMPACT-FLASH-ERRORS
Erreurs de disque dur	Les disques durs de l'appliance ont rencontré des défaillances en lecture ou en écriture.	24 heures	HARD-DISK-DRIVE-ERRORS

Condition d'erreur critique	Description	Intervalle de surveillance Call Home	Nom d'alarme SNMP correspondant
Panne du bloc d'alimentation	L'une des unités d'alimentation de l'appliance NetScaler est en panne.	7 seconde	POWER-SUPPLY-FAILURE
Panne de carte SSL	L'une des cartes SSL de l'appliance NetScaler est défaillante.	7 seconde	SSL-CARD-FAILED
Redémarrage à chaud	L'appareil a été redémarré à chaud en raison d'une défaillance d'un processus système.	Après chaque redémarrage de l'appliance NetScaler.	WARM-RESTART-EVENT
Erreur d'anomalie de mémoire	L'utilisation de la mémoire augmente progressivement au-delà de sa limite normale et dépasse le seuil.	1 jour	Aucune alarme SNMP
Perte de paquets de limite de débit	Les limites de débit ou les limites de paquets par seconde (pps) sont atteintes.	7 seconde	PF-RL-PPS-PKTS-DROPPED, PF-RL-RATE-PKTS-DROPPED

5. Téléchargez les données Call Home. Si l'une des conditions critiques précédentes est identifiée sur l'appliance, la fonction Call Home en informe automatiquement le support NetScaler. Les archives de support sont téléchargées sur le serveur de support NetScaler. Vous pouvez également configurer l'alarme SNMP CALLHOME-UPLOAD-EVENT pour générer une alerte SNMP chaque fois que le téléchargement de Call Home a lieu. L'alerte SNMP informe l'administrateur local de l'événement critique.

> **Remarque**
>
> Call Home crée le fichier tar Call Home et le télécharge sur le serveur de support technique Citrix uniquement pour la première occurrence d'une condition d'erreur particulière depuis le dernier

> redémarrage. Si vous souhaitez que l'appliance envoie des alertes chaque fois qu'une condition d'erreur particulière se produit, configurez l'alarme SNMP correspondante pour la condition d'erreur.

6. Créer une demande de service. Call Home crée automatiquement une demande de service pour tous les événements critiques liés au matériel. Les événements sont classés comme suit : panne d'alimentation, défaillance de la carte SSL, erreurs de disque dur et erreurs de flash compact. Pour les autres erreurs, après avoir consulté les journaux système, vous pouvez contacter l'équipe d'assistance de NetScaler pour envoyer une demande de service à des fins d'enquête.

Configuration de Call Home

Pour configurer Call Home, vérifiez la connectivité Internet de l'appliance et assurez-vous qu'un serveur de noms DNS est configuré. S'il n'y a pas de connexion Internet, configurez un serveur ou un service proxy. Activez ensuite Call Home sur l'appliance et vérifiez l'état d'enregistrement de l'appliance auprès du serveur de support NetScaler. Une fois enregistré, Call Home peut surveiller et télécharger des données. En outre, vous pouvez configurer des alarmes SNMP pour avertir l'administrateur sur le site du client.

Pour configurer Call Home, vous pouvez utiliser l'interface de commande NetScaler ou l'interface graphique pour effectuer les tâches suivantes :

- Activez Call Home.
- Configurez Call Home pour les paramètres facultatifs du serveur proxy.
- Vérifiez l'état d'enregistrement Call Home.
- Affichez les erreurs et les détails de l'horodatage.
- Configurez les alarmes SNMP.

Pour configurer Call Home à l'aide de l'interface de commande NetScaler

L'interface de commande NetScaler vous permet d'effectuer les opérations suivantes :

`Enabling Call Home`

À l'invite de commande, tapez :

```
enable ns feature callhome
```

Configuration de Call Home pour les paramètres facultatifs du serveur proxy

Call Home vous permet de configurer le serveur proxy optionnel pour la connectivité Internet. Vous pouvez soit configurer un serveur proxy avec une adresse IP et un port, soit configurer un service d'authentification proxy avec une authentification unidirectionnelle ou bidirectionnelle.

`To configure optional proxy server with IP address and port`

À l'invite de commande, tapez :

```
set callhome -proxyMode ( YES | NO )[-IPAddress <ip_addr|ipv6_addr|*>] [-
port <port |*>]
```

```
1 set callhome -proxyMode YES -IPAddress 10.102.167.33 -port 80
2 <!--NeedCopy-->
```

> **Remarque**
>
> Call Home utilise le serveur proxy uniquement lorsque vous définissez le paramètre du mode proxy sur YES. Si vous le définissez sur NON, la fonctionnalité proxy ne fonctionne pas, même si l'adresse IP et le port sont configurés. Le numéro de port doit correspondre à un service HTTP et non à un service HTTPS.

Pour configurer le service d'authentification proxy facultatif

Ce mode fournit deux types d'authentification de sécurité : unidirectionnelle et bidirectionnelle. Pour configurer l'un ou l'autre type, vous devez configurer un service SSL. Pour plus d'informations, consultez la rubrique Configuration d'un service SSL .

Dans le cadre de l'authentification unidirectionnelle, seule l'appliance NetScaler authentifie le serveur proxy. Dans le cadre de l'authentification bidirectionnelle, l'appliance NetScaler authentifie le serveur proxy et le serveur proxy authentifie à son tour l'appliance.

Pour configurer le service d'authentification du proxy

À l'invite de commande, tapez :

```
set callhome -proxyMode ( YES | NO )[-proxyAuthService <string>]
```

```
1 set callhome -proxyMode YES -proxyAuthService callhome_proxy
2 <!--NeedCopy-->
```

Pour configurer l'authentification unidirectionnelle du serveur proxy

Effectuez les tâches suivantes pour configurer l'authentification unidirectionnelle du serveur proxy.

1. Créez un service SSL.
2. Liez un certificat d'autorité de certification au service.
3. Liez un moniteur HTTPS au service.
4. Configurez Call Home pour utiliser le service SSL.

Pour configurer l'authentification bidirectionnelle du serveur proxy

Effectuez les tâches suivantes pour configurer l'authentification bidirectionnelle du serveur proxy.

1. Création d'un service SSL
2. Liez un certificat d'autorité de certification au service.

3. Liez un certificat client.
4. Liez un moniteur HTTPS au service.
5. Configurez Call Home pour utiliser le service SSL.

Vérification de l'état d'enregistrement Call Home

À l'invite de commande, tapez :

```
show callhome

    show callhome

     Registration with Citrix upload server SUCCESSFUL

     Mode: Default

     Contact email address: exampleadmin@example.com

     Heartbeat Custom Interval (days): 7

     Proxy Mode: Yes

        Proxy IP Address:10.102.29.200

        Proxy Authentication Service:

        Proxy Port: 80

    Trigger event                  State   First occurrence
                      Latest occurrence

     -------------                  -----   ----------------
                       -----------------

     1) Warm boot                   Enabled N/A
                                    ..

     2) Compact flash errors        Enabled ..
                                      ..

     3) Hard disk drive errors      Enabled ..
                                      ..

     4) SSL card failure            N/A     N/A
                                    N/A

```



```
33      5) Power supply unit failure   N/A     N/A
                                       N/A
34
35      6) Rate limit packet drops     Enabled ..
                                         ..
36
37      7) Memory anomaly              Enabled ..
                                         ..
38
39      Done
40 <!--NeedCopy-->
```

> **Remarque**
>
> Si le Call Home ne parvient pas à s'inscrire auprès du CIS, l'appliance affiche un message d'erreur.

Activation des alarmes SNMP

L'appliance NetScaler fournit un ensemble d'entités de condition d'erreur appelées alarmes *SNMP*. Lorsqu'une condition d'erreur dans une alarme SNMP est remplie, l'appliance génère des messages d'interruption SNMP qui sont envoyés aux écouteurs d'interruption configurés. Par exemple, lorsque l'alarme SSL-CARD-FAILED est activée, un message d'interruption est généré et envoyé à l'écouteur d'interruption. Le message d'interruption est envoyé chaque fois qu'il y a une défaillance de la carte SSL sur l'appliance. Pour plus d'informations, voir SNMP.

À l'invite de commande, tapez :

```
enable snmp alarm <trapName>
```

```
show snmp alarm <trapName>
```

Pour configurer Call Home à l'aide de l'interface graphique

Pour vérifier si la fonction Call Home est activée par défaut dans l'interface graphique

1. Accédez à **Configuration** > **Système** > **Paramètres**.
2. Dans le volet d' **informations**, cliquez sur le lien **Configurer les fonctionnalités avancées** .
3. Dans la page **Configurer les fonctionnalités avancées**, **l'option Call Home** doit s'afficher comme étant activée.

Pour activer Call Home à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Paramètres**.
2. Dans le volet d' **informations**, cliquez sur le lien **Configurer les fonctionnalités avancées** et sélectionnez l'option **Callhome** .

Pour configurer Call Home pour l'authentification facultative en mode proxy à l'aide de l'interface graphique

1. Vous pouvez utiliser l'une des deux méthodes pour accéder à la page d'accueil de Call Home :
   a) Accédez à **Système** > **Informations système**.
   b) Accédez à **Système** > **Diagnostics**.
      i. Dans le volet d'informations, sous **Outils de support technique**, sélectionnez **Call Home**.
2. Sur la page **Configurer l'Call Home**, définissez les paramètres suivants.
   a) **Mode**. Mode de fonctionnement Call Home. Types possibles : par défaut, déploiement du fournisseur de services Citrix (CSP).

      > **Remarque**
      > Cette option n'est pas configurable par l'utilisateur. Le mode est automatiquement déterminé et défini en fonction du type de déploiement de NetScaler.

   b) **Adresse e-mail**. Adresse e-mail de l'administrateur du contact sur le site du client.
   c) **Intervalle des battements de cœur CallHome (jours).** Intervalle de surveillance (en jours) entre les battements cardiaques de Call Home. Valeur minimale = 1 et valeur maximale = 30.
   d) **Activez Call Home**. Activez ou désactivez la fonctionnalité Call Home pour consulter l'état de l'enregistrement de l'appliance sur le serveur de support NetScaler.
   e) **Mode proxy**. Si vous ne disposez pas d'une connexion Internet, activez le mode proxy et définissez les paramètres de proxy facultatifs.
   f) **Serveur proxy**. Si vous définissez le mode proxy à l'aide d'un serveur proxy, spécifiez l'adresse IP du serveur.
      i. **Service proxy**. Si vous définissez le mode proxy à l'aide d'un service proxy, spécifiez le nom du service.
      ii. **Adresse IP**. Adresse IP du serveur proxy.
      iii. **Port**. Numéro de port du serveur proxy.
      iv. **Service SSL d'authentification proxy**. Nom du service proxy qui fournit l'authentification en mode proxy.
3. Cliquez sur **OK** et **Terminé**.

Pour configurer le service SSL pour l'authentification du serveur proxy à l'aide de l'interface graphique

Pour plus d'informations sur la configuration du service SSL à l'aide de l'interface graphique, reportez-vous à la rubrique Configuration d'un service SSL .

Pour vérifier l'état de l'inscription Call Home à l'aide de l'interface graphique

1. Vous pouvez utiliser l'une des deux méthodes pour accéder à la page d'accueil de **Call Home** :
   a) Accédez à **Système** > **Informations système**.
   b) Accédez à **Système** > **Diagnostics**.
      i. Dans le volet d'informations, sous **Outils de support technique**, sélectionnez **Call Home**.
2. Sur la page d' **accueil Configurer l'appel**, le champ **Inscription auprès du serveur de**

téléchargement Citrix indique l'état de l'enregistrement.

Pour configurer une alarme SNMP

1. Accédez à **Système** > **SNMP** > **Alarmes**.
2. Dans le volet d'informations, sélectionnez une alarme et configurez ses paramètres.
3. Cliquez sur **OK** et sur **Fermer**.

Prise en charge du déploiement Citrix Service Provider (CSP)

Dans un environnement Citrix Service Provider (CSP) où les services NetScaler sont déployés sur des instances VPX, Call Home peut surveiller et suivre les informations spécifiques à la licence et les envoyer en toute sécurité à Citrix Insight Services (CIS). CIS envoie à son tour les informations au portail License Usage Insights (LUI) à des fins de comptabilité et pour permettre aux clients CSP de vérifier leur utilisation de licence. Actuellement, les environnements CSP prennent en charge les services NetScaler uniquement sur les instances VPX, et non sur les appliances MPX ou SDX. Les instances VPX peuvent être déployées en mode autonome ou haute disponibilité.

Outil de reporting

May 5, 2023

Utilisez l'outil Citrix® NetScaler® Reporting pour afficher les données statistiques de performance de NetScaler sous forme de rapports. Les données statistiques sont collectées par l'`nscollect` utilitaire et stockées dans une base de données. Lorsque vous souhaitez afficher certaines données de performances sur une période, l'outil Reporting extrait les données spécifiées de la base de données et les affiche dans des graphiques.

Les rapports sont une collection de graphiques. L'outil Reporting fournit des rapports intégrés et la possibilité de créer des rapports personnalisés. Dans un rapport, vous pouvez modifier les graphiques et ajouter de nouveaux graphiques. Vous pouvez également modifier le fonctionnement de l'utilitaire de collecte de données et arrêter ou démarrer son opération. `nscollect`

Utilisation de l'outil de création de rapports

L'outil de création de rapports est une interface Web accessible depuis l'appliance Citrix® NetScaler®. Utilisez l'outil Reporting pour afficher les données des statistiques de performances sous forme de rapports contenant des graphiques. En plus d'utiliser les rapports intégrés, vous pouvez créer des rapports personnalisés que vous pouvez modifier à tout moment. Les rapports peuvent comporter entre un et quatre graphiques. Vous pouvez créer jusqu'à 256 rapports personnalisés. Vous pouvez créer un rapport personnalisé pour un nombre illimité d'entités.

Invoquer l'outil de reporting

1. Utilisez le navigateur Web de votre choix pour vous connecter à l'adresse IP de NetScaler (par exemple, `http://10.102.29.170/`). L'écran de connexion Web s'affiche.
2. Dans la zone de texte Nom d'utilisateur, tapez le nom d'utilisateur attribué à NetScaler.
3. Dans la zone de texte Mot de passe, tapez le mot de passe.
4. Dans la zone de liste déroulante Démarrer dans, sélectionnez Reporting. Cliquez sur Connexion.

Les captures d'écran suivantes présentent la barre d'outils du rapport et la barre d'outils du graphique, fréquemment référencées dans cette documentation.

Figure 1. *Barre d'outils Rapport*

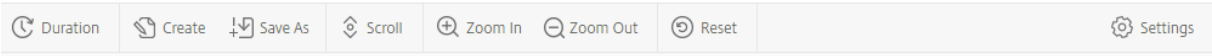
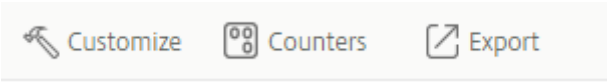


Figure 2. *Barre d'outils Graphique*



Utilisation des rapports

Vous pouvez tracer et surveiller les statistiques des différents groupes fonctionnels configurés sur NetScaler sur un intervalle de temps spécifié. Les rapports vous permettent de dépanner ou d'analyser le comportement de votre appliance. Il existe deux types de rapports : les rapports intégrés et les rapports personnalisés. Le contenu des rapports intégrés ou personnalisés peut être visualisé sous forme graphique ou tabulaire. La vue graphique se compose de graphiques linéaires, surfaciques et à barres pouvant afficher jusqu'à 32 ensembles de données (compteurs). La vue tabulaire affiche les données en colonnes et en lignes. Cette vue est utile pour déboguer les compteurs d'erreurs.

Le rapport par défaut affiché dans l'outil de création de rapports indique l'utilisation du processeur par rapport à la mémoire et le taux de requêtes HTTP. Vous pouvez modifier l'affichage du rapport par défaut en affichant le rapport de votre choix en tant que vue par défaut, puis en cliquant sur **Rapport par défaut**.

Les rapports peuvent être générés pour la dernière heure, le dernier jour, la semaine dernière, le mois dernier, l'année dernière, ou vous pouvez personnaliser la durée.

Vous pouvez effectuer les opérations suivantes avec les rapports :

- Basculez entre une vue tabulaire des données et une vue graphique des données.
- Modifiez le type d'affichage graphique, tel qu'un graphique à barres ou un graphique linéaire.
- Personnalisez les graphiques d'un rapport.
- Exportez le graphique en tant que fichier CSV (Excel séparé par des virgules).

- Affichez les graphiques en détail en effectuant un zoom avant, un zoom arrière ou une opération de glissement (défilement).
- Définissez un rapport comme rapport par défaut à afficher chaque fois que vous ouvrez une session.
- Ajoutez ou supprimez des compteurs.
- Imprimez des rapports.
- Actualisez les rapports pour consulter les dernières données de performance.

Utilisation de rapports intégrés

L'outil de création de rapports fournit des rapports intégrés pour les données fréquemment consultées. Des rapports intégrés sont disponibles pour les groupes fonctionnels suivants : système, réseau, SSL, compression, cache intégré, NetScaler Gateway et NetScaler Application Firewall. Par défaut, les rapports intégrés sont affichés pour le dernier jour. Vous pouvez toutefois consulter les rapports de la dernière heure, de la semaine dernière, du mois dernier ou de l'année dernière.

> **Remarque** :
>
> Vous ne pouvez pas enregistrer les modifications apportées aux rapports intégrés, mais vous pouvez enregistrer un rapport intégré modifié en tant que rapport personnalisé.

Afficher un rapport intégré

1. Dans le volet gauche de l'outil de création de rapports, sous Rapports intégrés, développez un groupe (par exemple, SSL).
2. Cliquez sur un rapport (par exemple, **SSL > Tous les chiffrements backend)**.

Création et suppression de rapports

Vous pouvez créer vos propres rapports personnalisés et les enregistrer sous des noms définis par l'utilisateur pour les réutiliser. Vous pouvez tracer différents compteurs pour différents groupes en fonction de vos besoins. Vous pouvez créer jusqu'à 256 rapports personnalisés.

Vous pouvez créer un rapport ou enregistrer un rapport intégré en tant que rapport personnalisé. Par défaut, un rapport personnalisé nouvellement créé contient un graphique intitulé Présentation du système, qui affiche le compteur d'utilisation du processeur tracé pour le dernier jour. Vous pouvez personnaliser l'intervalle et définir la source de données et le fuseau horaire à partir de la barre d'outils du rapport.

Création d'un rapport personnalisé

1. Dans l'outil de création de **rapports**, dans la barre d'outils du rapport, cliquez sur **Créer**, ou si vous souhaitez créer un rapport personnalisé basé sur un rapport existant, ouvrez le rapport existant, puis cliquez sur **Enregistrer sous**.
2. Dans la zone **Nom du rapport**, tapez le nom du rapport personnalisé.
3. Procédez comme suit :
    - Pour ajouter le rapport à un dossier existant, dans Créer dans ou Enregistrer dans, cliquez sur la flèche vers le bas pour sélectionner un dossier existant, puis cliquez sur **OK**.
    - Pour créer un nouveau dossier dans lequel stocker le rapport, cliquez sur l'icône Cliquez pour ajouter un dossier, dans Nom du dossier, tapez le nom du dossier et, dans Créer dans, spécifiez où vous souhaitez que le nouveau dossier se trouve dans la hiérarchie, puis cliquez sur **OK**.

> **Remarque** :
> Vous pouvez créer jusqu'à 128 dossiers.

Supprimer un rapport personnalisé

1. Dans le volet gauche de l'outil Reporting, à côté de Rapports personnalisés, cliquez sur l'icône Cliquer pour gérer les rapports personnalisés.
2. Activez la case à cocher correspondant au rapport à supprimer, puis cliquez sur Supprimer.

> **Remarque** :
>
> Lorsque vous supprimez un dossier, tout son contenu est supprimé.

Modifier l'intervalle de temps

Par défaut, les rapports intégrés affichent les données du dernier jour. Toutefois, si vous souhaitez modifier l'intervalle de temps pour un rapport intégré, vous pouvez enregistrer le rapport en tant que rapport personnalisé. Le nouvel intervalle s'applique à tous les graphiques du rapport. Le tableau suivant décrit les options d'intervalle de temps.

Modifier l'intervalle de temps

1. Dans le volet gauche de l'outil de création de rapports, cliquez sur un rapport.
2. Dans la barre d'outils du rapport, cliquez sur **Durée**, puis sur un intervalle de temps.

Configuration de la source de données et du fuseau horaire

Vous pouvez récupérer des données à partir de différentes sources de données pour les afficher dans les rapports. Vous pouvez également définir le fuseau horaire des rapports et appliquer la sélection horaire du rapport actuellement affiché à tous les rapports, y compris les rapports intégrés.

Définissez la source de données et le fuseau horaire

1. Dans l' **outil de création de rapports**, dans la barre d'outils du rapport, cliquez sur **Paramètres**.
2. Dans la boîte de dialogue **Paramètres**, dans Source de données, sélectionnez la source de données à partir de laquelle vous souhaitez récupérer les informations du compteur.
3. Procédez de l'une des manières suivantes ou les deux :
   - Si vous souhaitez que l'outil mémorise la période pour laquelle un graphique est tracé, cochez la case **Mémoriser la sélection de l'heure pour les graphiques** .
   - Si vous souhaitez que les rapports utilisent les paramètres horaires de votre appliance NetScaler, cochez la case **Utiliser le fuseau horaire de l'appliance** .

Exportation et importation de rapports personnalisés

Vous pouvez partager des rapports avec d'autres administrateurs NetScaler en les exportant. Vous pouvez également importer des rapports.

Exporter ou importer des rapports personnalisés

1. Dans le volet gauche de l'outil de création de rapports, à côté de Rapports personnalisés, cliquez sur l'icône **Cliquez pour gérer les rapports personnalisés** .
2. Cochez la case correspondant au rapport que vous souhaitez exporter ou importer, puis cliquez sur **Exporter** ou **Importer**.

   > **Remarque** :
   >
   > Lorsque vous exportez le fichier, il est exporté au format de fichier .gz.

Travailler avec des graphiques

Utilisez des graphiques pour tracer et surveiller des compteurs ou des groupes de compteurs. Vous pouvez inclure jusqu'à quatre graphiques dans un rapport. Dans chaque graphique, vous pouvez tracer jusqu'à 32 compteurs. Les graphiques peuvent utiliser différents formats graphiques (par exemple, zone et barre). Vous pouvez déplacer les graphiques vers le haut ou vers le bas dans le rapport, personnaliser les couleurs et l'affichage visuel de chaque compteur d'un graphique, et supprimer un graphique lorsque vous ne souhaitez pas le surveiller.

Dans tous les graphiques de rapport, l'axe horizontal représente le temps et l'axe vertical représente la valeur du compteur.

Ajouter un graphique

Lorsque vous ajoutez un graphique à un rapport, le graphique de présentation du système apparaît avec le compteur d'utilisation du processeur tracé pour la dernière journée.

> **Remarque** :
>
> Si vous ajoutez des graphiques à un rapport intégré et que vous souhaitez conserver le rapport, vous devez enregistrer le rapport en tant que rapport personnalisé.

Utilisez la procédure suivante pour ajouter un graphique à un rapport.

Ajouter un graphique à un rapport

1. Dans le volet gauche de l'outil de création de rapports, cliquez sur un rapport.
2. Sous le graphique dans lequel vous souhaitez ajouter le nouveau graphique, cliquez sur l'icône Ajouter.

Modifier un graphique

Vous pouvez modifier un graphique en modifiant le groupe fonctionnel pour lequel les statistiques sont affichées et en sélectionnant différents compteurs.

Modifier un graphique

1. Dans le volet gauche de l'outil de création de rapports, cliquez sur un rapport.
2. Sous le graphique que vous souhaitez modifier, cliquez sur Compteurs.
3. Dans la boîte de dialogue qui apparaît, dans la zone Titre, tapez un nom pour le graphique.
4. À côté du diagramme de tracé pour, effectuez l'une des opérations suivantes :
    - Pour tracer les compteurs pour les compteurs globaux, tels que Cache intégré et Compression, cliquez sur Statistiques globales système.
    - Pour tracer les compteurs d'entités pour les types d'entités, tels que l'équilibrage de charge et GSLB, cliquez sur Statistiques des entités système.
5. Dans le groupe Sélectionner, cliquez sur l'entité souhaitée.
6. Sous Compteurs, dans Disponible, cliquez sur un ou plusieurs noms de compteurs que vous souhaitez tracer, puis cliquez sur le bouton >.
7. Si vous avez sélectionné les statistiques des entités système à l'étape 4, sous l'onglet Entités, sous Disponible, cliquez sur un ou plusieurs noms d'instances d'entités que vous souhaitez tracer, puis cliquez sur le bouton >.
8. Cliquez sur OK.

Affichage d'un graphique

Vous pouvez spécifier les formats graphiques des compteurs tracés dans un graphique. Les graphiques peuvent être visualisés sous forme de graphiques linéaires, de graphiques à splines, de graphiques en étapes, de graphiques en nuages de points, de graphiques en aires, de graphiques à

barres, de graphiques à aires empilées et de graphiques à barres empilées. Vous pouvez également effectuer un zoom avant, un zoom arrière ou faire défiler la zone de tracé d'un graphique. Vous pouvez zoomer ou dézoomer sur toutes les sources de données pendant 1 heure, 1 jour, 1 semaine, 1 mois, 1 an et 3 ans.

Les autres options permettant de personnaliser l'affichage d'un graphique incluent la personnalisation des axes des graphiques, la modification de la couleur d'arrière-plan et de bord de la zone de tracé, la personnalisation de la couleur et de la taille des grilles et la personnalisation de l'affichage de chaque ensemble de données (compteur) d'un graphique.

Les numéros des ensembles de données, tels que l'ensemble de données 1, correspondent à l'ordre dans lequel les compteurs de votre graphique sont affichés en bas du graphique. Par exemple, si l'utilisation du processeur et l'utilisation de la mémoire sont affichées dans le premier et le second ordre en bas du graphique, l'utilisation du processeur est égale à l'ensemble de données 1 et l'utilisation de la mémoire est égale à l'ensemble de données 2.

Chaque fois que vous modifiez un rapport intégré, vous devez l'enregistrer en tant que rapport personnalisé pour conserver vos modifications.

Modifier le type de graphique d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique que vous souhaitez afficher, dans la barre d'outils du graphique, cliquez sur **Personnaliser**.
3. Dans l'onglet **Graphique**, sous **Catégorie**, cliquez sur **Type de tracé**, puis sur le type de graphique que vous souhaitez afficher pour le graphique. Si vous souhaitez afficher le graphique en 3D, cochez la case Utiliser la 3D.

Recentrer un graphique avec des données détaillées

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur **Zoom avant**, puis effectuez l'une des opérations suivantes ou les deux :
    - Pour refocaliser le graphique afin d'afficher les données d'une fenêtre horaire spécifique, faites glisser le curseur de l'heure de début à l'heure de fin. Par exemple, vous pouvez afficher des données pour une période d'une heure sur un jour donné.
    - Pour refocaliser le graphique afin d'afficher les données d'un point de données, il suffit de cliquer une fois sur le graphique où vous souhaitez effectuer un zoom avant et obtenir des informations plus détaillées.
3. Une fois que vous avez la plage de temps souhaitée pour afficher les données détaillées, dans la barre d'outils du rapport, cliquez sur Affichage tabulaire. La vue tabulaire affiche les données sous forme numérique en lignes et en colonnes.

Afficher les données numériques d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur Vue tabulaire. Pour revenir à la vue graphique, cliquez sur **Affichage graphique**.

> **Remarque** : Vous pouvez également afficher les données numériques dans la vue graphique en plaçant votre curseur sur les encoches du quadrillage.

Faire défiler le temps dans un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur **Défiler**, puis sur l'intérieur du graphique et faites glisser le curseur dans la direction dans laquelle vous souhaitez afficher les données pour une nouvelle période. Par exemple, si vous souhaitez afficher des données par le passé, faites glisser vers la gauche.

Modifier la couleur d'arrière-plan et la couleur du texte d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique dont vous souhaitez personnaliser les axes, cliquez sur **Personnaliser**.
3. Dans l'onglet **Graphique**, sous **Catégorie**, cliquez sur l'une ou plusieurs des options suivantes :
   - Pour modifier la couleur d'arrière-plan, cliquez sur **Couleur d'arrière-plan**, puis sélectionnez les options de couleur, de transparence et d'effets.
   - Pour modifier la couleur du texte, cliquez sur **Couleur**du texte, puis sélectionnez les options de couleur, de transparence et d'effets.

Personnaliser les axes d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique dont vous souhaitez personnaliser les axes, cliquez sur **Personnaliser**.
3. Dans l'onglet **Graphique**, sous Catégorie, cliquez sur une ou plusieurs des options suivantes :
   - Pour modifier l'échelle de l'axe Y gauche, cliquez sur **Axe Y gauche**, puis sélectionnez l'échelle souhaitée.
   - Pour modifier l'échelle de l'axe Y droit, cliquez sur Axe Y droit, dans le jeu de données à tracer, sélectionnez le jeu de dates, puis sélectionnez l'échelle souhaitée.

     > Note :
     > Les numéros des ensembles de données, tels que l'ensemble de données 1, correspondent à l'ordre dans lequel les compteurs de votre graphique sont affichés en bas

> du graphique. Par exemple, si l'utilisation du processeur et l'utilisation de la mémoire sont affichées dans le premier et le second ordre en bas du graphique, l'utilisation du processeur est égale à l'ensemble de données 1 et l'utilisation de la mémoire est égale à l'ensemble de données 2.

- Pour tracer chaque ensemble de données sur son propre axe Y masqué, cliquez sur Axes multiples, puis sur Activer.

Modifier la couleur d'arrière-plan, la couleur des bords et le quadrillage d'une zone de tracé d'un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique pour lequel vous souhaitez personnaliser la zone de tracé, cliquez sur **Personnaliser**.
3. Dans l'onglet **Surface du tracé**, sous Catégorie, cliquez sur l'une ou plusieurs des options suivantes :
   - Pour modifier la couleur d'arrière-plan et la couleur des bords du graphique, cliquez sur **Couleur d'arrière-plan et Couleur des bords**, puis sélectionnez les options de couleur, de transparence et d'effets.
   - Pour modifier les grilles horizontales ou verticales du graphique, cliquez sur **Grilles horizontales** ou Grilles **verticales, puis sélectionnez les options d'affichage des grilles**, de la largeur de la grille, de la couleur de la grille, de la transparence et des effets.

Modifier la couleur et le type de graphique d'un ensemble de données

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique pour lequel vous souhaitez personnaliser l'affichage de l'ensemble de données (compteurs), cliquez sur **Personnaliser**.
3. Dans l'onglet **Ensemble de données**, dans Sélectionner un ensemble de données, sélectionnez l'ensemble de données (compteur) pour lequel vous souhaitez personnaliser l'affichage graphique.
   Remarque : Les numéros des ensembles de données, tels que l'ensemble de données 1, correspondent à l'ordre dans lequel les compteurs de votre graphique sont affichés en bas du graphique. Par exemple, si l'utilisation
   du processeur et l'utilisation de la
   mémoire sont affichées dans le premier et le second ordre en bas du graphique, l'utilisation
   du processeur est égale à l'ensemble de
   données 1 et l'utilisation de la
   mémoire est égale à l'ensemble de
   données 2.
4. Dans Catégorie, effectuez l'une ou plusieurs des opérations suivantes :

- Pour modifier la couleur d'arrière-plan, cliquez sur **Couleur**, puis sélectionnez les options de couleur, de transparence et d'effets.
- Pour modifier le type de graphique, cliquez sur **Type de tracé**, puis sélectionnez le type de graphique que vous souhaitez afficher pour l'ensemble de données. Si vous souhaitez afficher le graphique en 3D, cochez la case Utiliser la 3D.

Exportation de données graphiques vers Excel

Pour une analyse plus approfondie des données, vous pouvez exporter des graphiques vers Excel au format CSV (valeurs séparées par des virgules).

Pour exporter des données graphiques vers Excel

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique contenant les données que vous souhaitez exporter vers Excel, cliquez sur **Exporter**.

Supprimer un graphique

Si vous ne souhaitez pas utiliser de graphique, vous pouvez le supprimer du rapport. Vous pouvez supprimer définitivement des graphiques des rapports personnalisés uniquement. Si vous supprimez un graphique d'un rapport intégré et souhaitez conserver les modifications, vous devez enregistrer le rapport en tant que rapport personnalisé.

Supprimer un graphique

1. Dans le volet gauche de l'outil Reporting, sélectionnez un rapport.
2. Dans le volet droit, sous le graphique que vous souhaitez supprimer, cliquez sur l'icône **Supprimer** .

Exemples

Afficher le rapport de tendance sur l'utilisation du processeur et de la mémoire pour la semaine dernière

1. Dans le volet gauche de l'outil de création de rapports, sous Rapports intégrés, développez Système.
2. Cliquez sur le rapport Utilisation du processeur par rapport à la mémoire et au taux de requêtes HTTP.
3. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur **Durée**, puis sur **Semaine dernière**.

Comparez le débit d'octets reçus et le débit d'octets transmis entre les deux interfaces pour la semaine dernière

1. Dans le volet droit, dans la barre d'outils du rapport, cliquez sur Créer.
2. Dans la zone **Nom du rapport**, tapez le nom du rapport personnalisé (par exemple, Custom_Interfaces), puis cliquez sur **OK**. Le rapport est créé avec le graphique de présentation du système par défaut, qui affiche le compteur d'utilisation du processeur tracé pour la dernière heure.
3. Sous Présentation du système, dans la barre d'outils du graphique, cliquez sur Compteurs.
4. Dans le volet de sélection du compteur, dans Titre, tapez le nom du graphique (par exemple, Interfaces, octets, données).
5. Dans Graphique de tracé pour, cliquez sur Statistiques des entités système, puis dans Sélectionner un groupe, sélectionnez Interface.
6. Dans l'onglet **Entités**, cliquez sur un ou plusieurs noms d'interface que vous souhaitez tracer (par exemple, 1/1 et 1/2), puis cliquez sur le bouton >.
7. Sous l'onglet Compteurs, cliquez sur Octets reçus (Taux) et Octets transmis (Taux), puis cliquez sur le bouton>.
8. Cliquez sur **OK**.
9. Dans la barre d'outils du rapport, cliquez sur **Durée**, puis sur **Semaine dernière**.

Arrêt et démarrage de l'utilitaire de collecte de données

L'utilitaire de collecte de données `nscollect`s'exécute automatiquement lorsque vous démarrez NetScaler. Cet utilitaire récupère les données de performances de l'application et les stocke sous la forme de sources de données sur ADC. Vous pouvez créer jusqu'à 32 sources de données. La source de données par défaut est `/var/log/db/default`.

L'utilitaire de collecte de données crée des bases de données pour les compteurs globaux et les compteurs spécifiques aux entités, et utilise ces données pour générer des rapports. Les bases de données Global Counter sont créées à l'adresse `/var/log/db/<DataSourceName>`. Les bases de données spécifiques aux entités sont créées en fonction des entités configurées sur NetScaler, et un dossier distinct est créé pour chaque type d'entité dans. `/var/log/db/<DataSourceName/EntityNameDB>`

Le système `nscollect` récupère les données toutes les 5 minutes. Il conserve les données selon une granularité de 5 minutes pendant une journée, toutes les heures pendant les 30 derniers jours et tous les jours pendant trois ans.

Vous devrez peut-être arrêter et redémarrer l'utilitaire de collecte de données si les données ne sont pas correctement mises à jour ou si les rapports affichent des données corrompues.

Arrête `nscollect`

À l'invite de commande, tapez :

```
/netscaler/nscollect stop
```

Démarrez nscollect sur la session SSH en cours sur NetScaler :

À l'invite de commande, tapez :

```
/netscaler/nscollect start
```

Démarrez nscollect sur le système local :

À l'invite de commande, tapez :

```
/netscaler/nscollect start &
```

CloudBridge Connector

May 5, 2023

Remarque : La version actuelle de NetScaler 1000V ne prend pas en charge cette fonctionnalité.

La fonctionnalité CloudBridge Connector de l'appliance NetScaler connecte les centres de données d'entreprise aux clouds externes et aux environnements d'hébergement, faisant du cloud une extension sécurisée de votre réseau d'entreprise. Les applications hébergées dans le cloud semblent s'exécuter sur un réseau d'entreprise contigu. Avec Citrix CloudBridge Connector, vous pouvez augmenter la capacité et l'efficacité de vos centres de données grâce à la capacité et à l'efficacité disponibles auprès des fournisseurs de cloud.

Le CloudBridge Connector vous permet de déplacer vos applications vers le cloud afin de réduire les coûts et d'améliorer la fiabilité.

Outre l'utilisation du CloudBridge Connector entre un centre de données et un cloud, vous pouvez l'utiliser pour connecter deux centres de données afin d'établir une liaison sécurisée et accélérée de grande capacité.

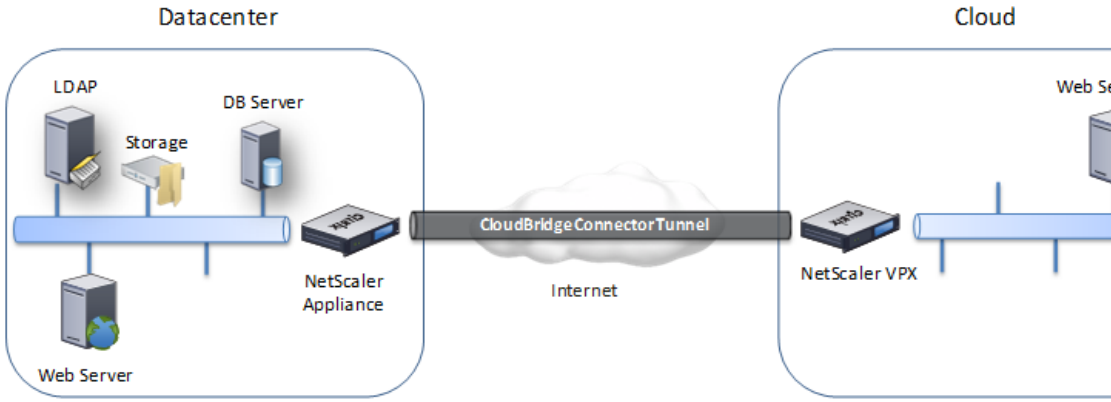
Comprendre le CloudBridge Connector

Pour implémenter la solution Citrix CloudBridge Connector, vous connectez un centre de données à un autre centre de données ou à un cloud externe en configurant un tunnel appelé tunnel CloudBridge Connector.

Pour connecter un centre de données à un autre centre de données, vous devez configurer un tunnel CloudBridge Connector entre deux appliances NetScaler, une dans chaque centre de données.

Pour connecter un centre de données à un cloud externe (par exemple, le cloud Amazon AWS), vous configurez un tunnel CloudBridge Connector entre une appliance NetScaler du centre de données et une appliance virtuelle (VPX) résidant dans le cloud. Le point de terminaison distant peut être un CloudBridge Connector ou un NetScaler VPX avec licence Premium.

L'illustration suivante montre un tunnel CloudBridge Connector configuré entre un centre de données et un nuage externe.



Les appliances entre lesquelles un tunnel CloudBridge Connector est configuré sont appelées *points de terminaison* ou *homologues* du tunnel CloudBridge Connector.

Un tunnel CloudBridge Connector utilise les protocoles suivants :

- Protocole GRE (Generic Routing Encapsulation)
- Suite de protocoles IPsec standard ouverte, en mode transport

Le protocole GRE fournit un mécanisme pour encapsuler des paquets, provenant d'une grande variété de protocoles réseau, à transmettre via un autre protocole. Le GRE est utilisé pour :

- Connectez des réseaux utilisant des protocoles non IP et non routables.
- Faites le pont entre un réseau étendu (WAN).
- Créez un tunnel de transport pour tout type de trafic qui doit être envoyé tel quel sur un autre réseau.

Le protocole GRE encapsule les paquets en ajoutant un en-tête GRE et un en-tête IP GRE aux paquets.

La suite de protocoles IPsec (Internet Protocol Security) sécurise les communications entre homologues dans le tunnel CloudBridge Connector.

Dans un tunnel CloudBridge Connector, IPsec garantit :

- Intégrité des données
- Authentification d'origine des données
- Confidentialité des données (cryptage)
- Protection contre les attaques par rediffusion

IPsec utilise le mode de transport dans lequel le paquet encapsulé GRE est crypté. Le chiffrement est effectué par le protocole ESP (Encapsulating Security Payload). Le protocole ESP garantit l'intégrité du paquet à l'aide d'une fonction de hachage HMAC et garantit la confidentialité à l'aide d'un algorithme de chiffrement. Une fois le paquet crypté et le HMAC calculé, un en-tête ESP est généré. L'en-tête ESP est inséré après l'en-tête IP GRE et une bande-annonce ESP est insérée à la fin de la charge utile cryptée.

Les homologues du tunnel CloudBridge Connector utilisent le protocole IKE (Internet Key Exchange version) (qui fait partie de la suite de protocoles IPsec) pour négocier des communications sécurisées, comme suit :

- Les deux homologues s'authentifient mutuellement à l'aide de l'une des méthodes d'authentification suivantes :
  - **Authentification par clé pré-partagée**. Une chaîne de texte appelée clé pré-partagée est configurée manuellement sur chaque homologue. Les clés pré-partagées des homologues sont comparées les unes aux autres à des fins d'authentification. Par conséquent, pour que l'authentification soit réussie, vous devez configurer la même clé pré-partagée sur chacun des homologues.
  - **Authentification par certificats numériques**. L'homologue initiateur (expéditeur) signe les données d'échange de messages à l'aide de sa clé privée, tandis que l'autre homologue récepteur utilise la clé publique de l'expéditeur pour vérifier la signature. Généralement, la clé publique est échangée dans des messages contenant un certificat X.509v3. Ce certificat fournit un niveau d'assurance que l'identité d'un homologue telle que représentée dans le certificat est associée à une clé publique particulière.
- Les pairs négocient ensuite pour parvenir à un accord sur :
  - Un algorithme de chiffrement.
  - Clés cryptographiques pour chiffrer les données dans un homologue et les déchiffrer dans l'autre.

Cet accord sur le protocole de sécurité, l'algorithme de chiffrement et les clés cryptographiques est appelé Security Association (SA). Les AA sont unidirectionnels (simplex). Par exemple, lorsque deux homologues, CB1 et CB2, communiquent via un tunnel Connector, CB1 possède deux associations de sécurité. Une SA est utilisée pour traiter les paquets sortants et l'autre SA est utilisée pour traiter les paquets entrants.

Les SA expirent après une durée spécifiée, appelée *durée de vie*. Les deux homologues utilisent le protocole Internet Key Exchange (IKE) (qui fait partie de la suite de protocoles IPsec) pour négocier de nouvelles clés cryptographiques et établir de nouvelles SA. Le but de la durée de vie limitée est d'empêcher les attaquants de craquer une clé.

Le tableau suivant répertorie certaines propriétés IPsec prises en charge par une appliance NetScaler :

Propriétés IPSec	Types pris en charge
Versions d'IKE	V1, V2
Groupe IKE DH	Une appliance NetScaler prend uniquement en charge le groupe DH 2 (algorithme MODP 1024 bits) pour IKEv1 et IKEv2.
Méthodes d'authentification IKE	Authentification par clé pré-partagée, authentification par certificats numériques
Algorithme de chiffrement	AES (128 bits), AES 256 (256 bits), 3DES
Algorithme de hachage	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5

Surveillance des tunnels du CloudBridge Connector

May 5, 2023

Vous pouvez afficher les statistiques permettant de surveiller les performances d'un tunnel CloudBridge Connector. Pour afficher les statistiques du tunnel CloudBridge Connector sur une appliance NetScaler, utilisez l'interface graphique ou la ligne de commande NetScaler.

Le tableau suivant répertorie les compteurs statistiques disponibles pour surveiller les tunnels CloudBridge Connector sur une appliance NetScaler.

Compteur statistique	**Spécifie**
Bytes Received	Nombre total d'octets reçus par l'appliance NetScaler via tous les tunnels CloudBridge Connector configurés depuis le dernier démarrage de l'appliance.
Bytes Sent	Nombre total d'octets envoyés par l'appliance NetScaler via tous les tunnels CloudBridge Connector configurés depuis le dernier démarrage de l'appliance.
Paquets reçus	Nombre total de paquets reçus par l'appliance NetScaler via tous les tunnels CloudBridge Connector configurés depuis le dernier démarrage de l'appliance.

Compteur statistique	Spécifie
Paquets envoyés	Nombre total de paquets envoyés par l'appliance NetScaler via tous les tunnels CloudBridge Connector configurés depuis le dernier démarrage de l'appliance.
Taux d'octets reçus	Nombre d'octets par seconde reçus par l'appliance NetScaler via tous les tunnels CloudBridge Connector configurés.
Taux d'envoi d'octets	Nombre d'octets par seconde envoyés par l'appliance NetScaler via tous les tunnels CloudBridge Connector configurés
Taux de réception de paquets	Nombre d'octets par seconde reçus par l'appliance NetScaler via tous les tunnels CloudBridge Connector configurés
Taux d'envoi de paquets	Nombre d'octets par seconde reçus par l'appliance NetScaler via tous les tunnels CloudBridge Connector configurés

Tous ces compteurs sont remis à 0 lorsque l'appliance NetScaler est redémarrée. Ils ne s'incrémentent pas au cours des phases suivantes :

- Phase d'authentification par échange de clés Internet (IKE) (clé pré-partagée) sur n'importe quel tunnel CloudBridge Connector configuré.
- Phase d'établissement de l'IKE Security Association (SA) sur tout tunnel CloudBridge Connector configuré.

Pour afficher les statistiques du tunnel CloudBridge Connector à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- **compteurs IPSec Stat**

Pour afficher les statistiques du tunnel CloudBridge Connector à l'aide de l'interface graphique

1. Accédez à l'interface graphique à l'aide d'un navigateur Web pour vous connecter à l'adresse IP de l'appliance NetScaler.
2. Dans l'onglet **Configuration,** accédez à **Système** > **CloudBridge**Connector.
3. Sur la page CloudBridge Connector, cliquez sur **Créer/Surveiller**CloudBridge Connector. Les graphiques d' **octets IPsec** et de **paquets IPsec** affichent le débit d'octets reçus, le débit d'octets

envoyés, le débit de paquets reçus et le débit de paquets envoyés de tous les tunnels CloudBridge Connector configurés sur l'appliance NetScaler.

```
    > stat ipsec counters
    Secure tunnel(s) summary
                        Rate (/s)        Total
    Bytes Received    0    2811248
    Bytes Sent            0    157460630
    Packets Received    0    56787
    Packets Sent        0    200910
    Done
    >
<!--NeedCopy-->
```

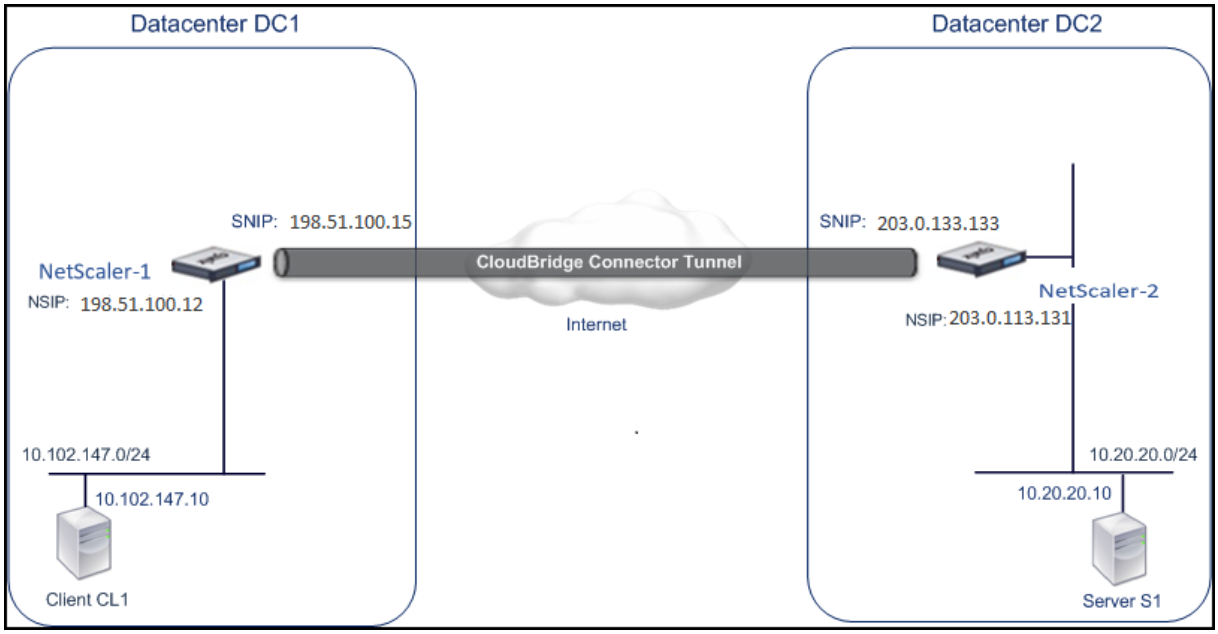
Configuration d'un tunnel CloudBridge Connector entre deux centres de données

May 5, 2023

Vous pouvez configurer un tunnel CloudBridge Connector entre deux centres de données différents pour étendre votre réseau sans le reconfigurer et tirer parti des fonctionnalités des deux centres de données. Un tunnel CloudBridge Connector entre les deux centres de données géographiquement séparés vous permet de mettre en œuvre la redondance et de protéger votre configuration contre les pannes. Le tunnel CloudBridge Connector permet d'optimiser l'utilisation de l'infrastructure et des ressources dans les centres de données. Les applications disponibles dans les deux centres de données apparaissent comme locales pour l'utilisateur.

Pour connecter un centre de données à un autre centre de données, vous devez configurer un tunnel CloudBridge Connector entre une appliance NetScaler dans un centre de données et une appliance NetScaler dans l'autre centre de données.

Pour illustrer le tunnel CloudBridge Connector entre des centres de données, prenons un exemple dans lequel un tunnel CloudBridge Connector est configuré entre l'appliance NetScaler NS_Appliance-1 dans le centre de données DC1 et l'appliance NetScaler NS_Appliance-2 dans le centre de données DC2.



NS_Appliance-1 et NS_Appliance-2 fonctionnent en mode L2 et L3. Ils permettent la communication entre les réseaux privés dans les centres de données DC1 et DC2. En mode L3, NS_Appliance-1 et NS_Appliance-2 permettent la communication entre le client CL1 dans le centre de données DC1 et le serveur S1 dans le centre de données DC2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Comme le client CL1 et le serveur S1 se trouvent sur des réseaux privés différents, le mode L3 est activé sur NS_Appliance-1 et NS_Appliance-2, et les itinéraires sont mis à jour comme suit :

- CL1 possède une route vers NS_Appliance-1 pour atteindre S1.
- NS_Appliance-1 possède une route vers NS_Appliance-2 pour atteindre S1.
- S1 possède une route vers NS_Appliance-2 pour atteindre CL1.
- NS_Appliance-2 possède une route vers NS_Appliance-1 pour atteindre le CL1.

Le tableau suivant répertorie les paramètres de l'appliance NetScaler NS_Appliance-1 dans le centre de données DC1.

Le tableau suivant répertorie les paramètres de l'appliance NetScaler NS_Appliance-2 dans le centre de données DC2.

Entité	Nom	Détails
L'adresse NSIP		198.51.100.12
Adresse SNIP		198.51.100.15

Entité	Nom	Détails
Tunnel CloudBridge Connector	Cloud_Connector_DC1-DC2	1. Adresse IP du point de terminaison local du tunnel CloudBridge Connector : 198.51.100.15, 2. Adresse IP du point de terminaison distant du tunnel CloudBridge Connector : 203.0.113.133. Nom des détails du tunnel GRE = Cloud_Connector_DC1-DC2, nom des détails du profil IPsec = Cloud_Connector_DC1-DC2, algorithme de chiffrement = AES, algorithme de hachage = HMAC SHA1

Points à prendre en compte pour configurer le tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector, vérifiez que les tâches suivantes ont été effectuées :

1. Déployez et configurez une appliance NetScaler dans chacun des deux centres de données.
2. Assurez-vous que les adresses IP des points de terminaison du tunnel CloudBridge Connector sont accessibles les unes aux autres.

Procédure de configuration

Pour configurer un tunnel CloudBridge Connector entre une appliance NetScaler résidant dans un centre de données et une autre appliance NetScaler résidant dans l'autre centre de données, utilisez l'interface graphique ou l'interface de ligne de commande de l'une des appliances NetScaler.

Lorsque vous utilisez l'interface graphique, la configuration du tunnel CloudBridge Connector créée sur la première appliance NetScaler est automatiquement transmise à l'autre point de terminaison (l'autre appliance NetScaler) du tunnel CloudBridge Connector. Par conséquent, vous n'avez pas besoin d'accéder à l'interface graphique de l'autre appliance NetScaler pour y créer la configuration de tunnel CloudBridge Connector correspondante.

La configuration du tunnel CloudBridge Connector sur chacune des appliances NetScaler comprend les entités suivantes :

- **Profil IPsec**—Une entité de profil IPsec spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et le PSK, à utiliser par le protocole IPsec dans le tunnel CloudBridge Connector.
- **Tunnel GRE**—Un tunnel IP spécifie l'adresse IP locale (une adresse SNIP publique configurée sur l'appliance NetScaler locale), l'adresse IP distante (une adresse SNIP publique configurée sur l'appliance NetScaler distante), le protocole (GRE) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPsec.
- **Créez une règle PBR et associez-y le tunnel IP** : une entité PBR spécifie un ensemble de conditions et une entité de tunnel IP. La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Vous devez définir la plage d'adresses IP source et la plage d'adresses IP de destination pour spécifier le sous-réseau dont le trafic doit traverser le tunnel CloudBridge Connector. Prenons l'exemple d'un paquet de demande qui provient d'un client du sous-réseau du premier centre de données et qui est destiné à un serveur du sous-réseau du second centre de données. Si ce paquet correspond à la plage d'adresses IP source et de destination de l'entité PBR sur l'appliance NetScaler du premier centre de données, il est envoyé via le tunnel CloudBridge Connector associé à l'entité PBR.

Pour créer un profil IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `add ipsec profile <name> [-ikeVersion (V1 | V2)] [-encAlgo (AES | 3 DES)...] [-hashAlgo <hashAlgo\> ...] [-lifetime <positive_integer>] (-psk | (-publickey<string> -privatekey <string>-peerPublicKey <string >))[-livenessCheckInterval <positive_intege>][-replayWindowSize \< positive_integer>] [-ikeRetryInterval <positive_integer>] [-retransmissiontime <positive_integer>]`
- `show ipsec profile <name>`

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol < protocol>] [-ipsecProfileName <string>]`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = < remote_subnet_range> -ipTunnel <tunnel_name>`

- apply ns pbrs
- show ns pbr <pbr_name>

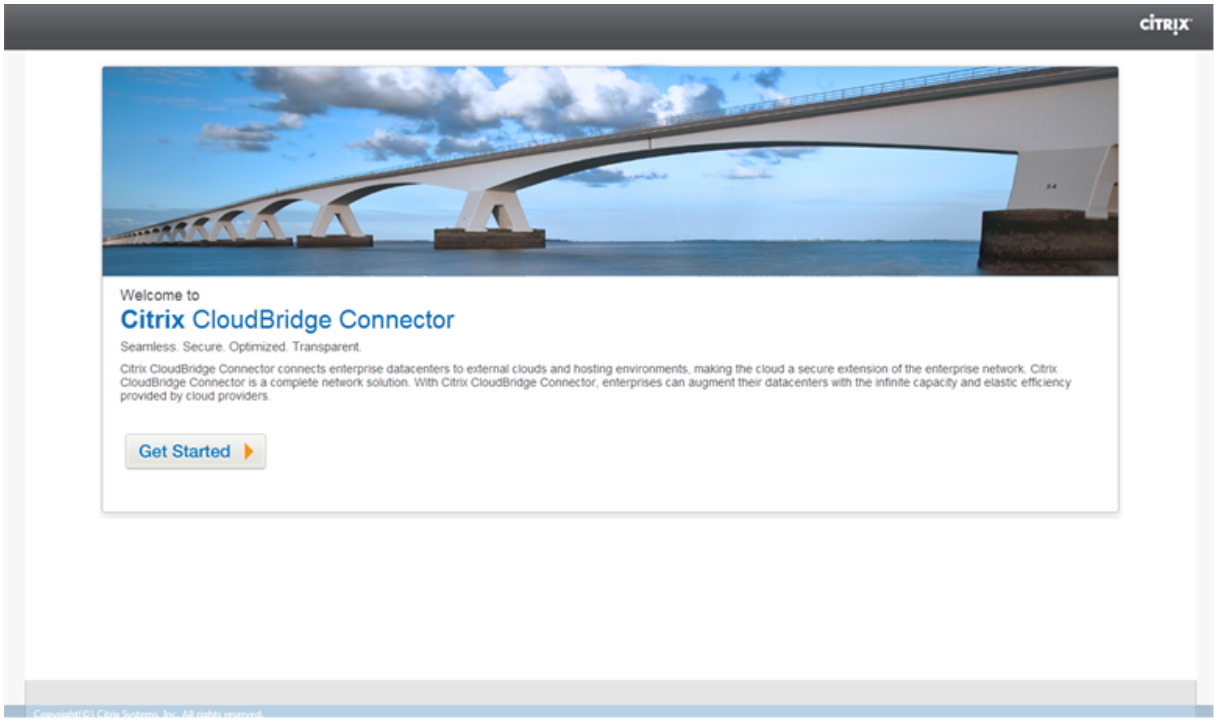
Exemple

```
1  add ipsec profile Cloud_Connector_DC1-DC2  -encAlgo AES -hashAlgo
       HMAC_SHA1
2      Done
3      > add ipTunnel Cloud_Connector_DC1-DC2 203.0.113.133
           255.255.255.255 198.51.100.15 -protocol GRE -ipsecProfileName
           Cloud_Connector_DC1-DC2
4
5      Done
6      > add ns pbr PBR-DC1-DC2 ALLOW -srcIP 198.51.100.15 -destIP
           203.0.113.133 ipTunnel Cloud_Connector_DC1-DC2
7
8      Done
9      > apply ns pbrs
10
11     Done
12 <!--NeedCopy-->
```

Pour configurer un tunnel CloudBridge Connector dans une appliance NetScaler à l'aide de l'interface graphique

1. Tapez l'adresse NSIP d'une appliance NetScaler dans la ligne d'adresse d'un navigateur Web.
2. Connectez-vous à l'interface graphique de l'appliance NetScaler à l'aide des informations d'identification de votre compte pour l'appliance.
3. Accédez à **Système** > **CloudBridge Connector**.
4. Dans le volet droit, sous **Mise en route**, cliquez sur **Créer/Surveiller CloudBridge**.

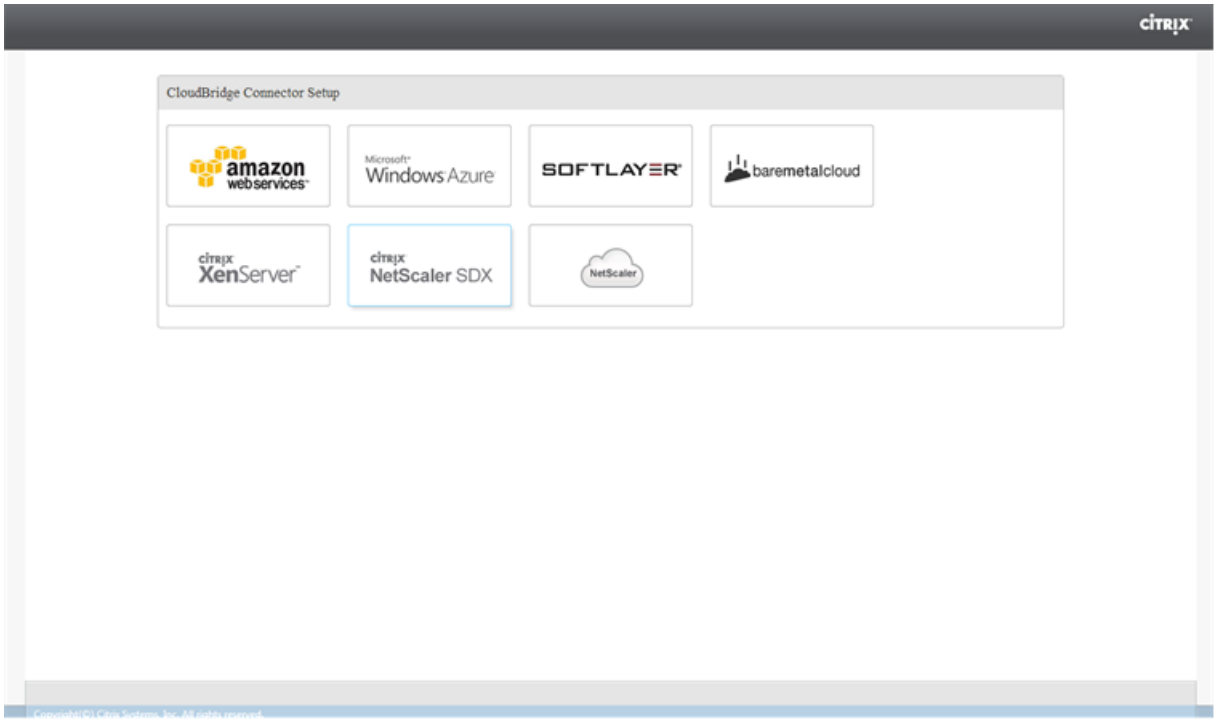
   La première fois que vous configurez un tunnel CloudBridge Connector sur l'appliance, un écran de **bienvenue** s'affiche.
5. Sur l'écran de **bienvenue**, cliquez sur **Commencer**.



Remarque :

Si un tunnel CloudBridge Connector est déjà configuré sur l'appliance NetScaler, l'écran de bienvenue ne s'affiche pas. Vous ne devez donc pas cliquer sur Commencer.

1. Dans le volet **Configuration du CloudBridge Connector**, cliquez sur **NetScaler**.



1. Dans le volet NetScaler, saisissez les informations d'identification de votre compte pour l'appliance NetScaler distante. Cliquez sur **Continuer**.
2. Dans le volet Paramètres **du CloudBridge Connector**, définissez le paramètre suivant :
   - Nom**du CloudBridge Connector : nom**de la configuration du CloudBridge Connector sur l'appliance locale. Doit commencer par un caractère alphabétique ASCII ou un trait de soulignement (_) et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), un espace, deux points (:), à (@), égal (=) et un trait d'union (-). Ne peut pas être modifié après la création de la configuration du CloudBridge Connector.
3. Sous **Paramètres locaux**, définissez le paramètre suivant :
   - **IP du sous-réseau** : adresse IP du point de terminaison local du tunnel CloudBridge Connector.
4. Sous **Réglage à distance**, définissez le paramètre suivant :
   - **IP du sous-réseau** : adresse IP du point de terminaison homologue du tunnel CloudBridge Connector.
5. Sous Paramètre **PBR**, définissez les paramètres suivants :
   - **Opération**—La valeur est égale à (=) ou n'est pas égale à (! =) opérateur logique.
   - **IP source faible** : adresse IP source la plus faible à comparer à l'adresse IP source d'un paquet IPv4 sortant.
   - **IP source élevée** : adresse IP source la plus élevée à comparer à l'adresse IP source d'un paquet IPv4 sortant.
   - **Opération**—La valeur est égale à (=) ou n'est pas égale à (! =) opérateur logique.
   - IP de destination faible* : adresse IP de destination la plus faible à comparer à l'adresse IP de destination d'un paquet IPv4 sortant.
   - Adresse**IP de destination élevée**—Adresse IP de destination la plus élevée à comparer à l'adresse IP de destination d'un paquet IPv4 sortant.
6. (Facultatif) Dans **Paramètres de sécurité**, définissez les paramètres de protocole IPsec suivants pour le tunnel CloudBridge Connector :
   - **Algorithme**de chiffrement : algorithme de chiffrement à utiliser par le protocole IPsec dans le tunnel CloudBridge.
   - **Algorithme**de hachage : algorithme de hachage à utiliser par le protocole IPsec dans le tunnel CloudBridge.
   - **Clé** : sélectionnez l'une des méthodes d'authentification IPsec suivantes à utiliser par les deux homologues pour s'authentifier mutuellement.
     - **Clé générée automatiquement** : authentification basée sur une chaîne de texte, appelée clé pré-partagée (PSK), générée automatiquement par l'appliance lo-

cale. Les clés PSK des homologues sont comparées les unes aux autres à des fins d'authentification.

- **Clé spécifique** : authentification basée sur une PSK saisie manuellement. Les PSK des homologues sont comparés les uns aux autres à des fins d'authentification.
  - Clé de sécurité pré-partagée : chaîne de texte saisie pour l'authentification basée sur une clé pré-partagée.
- **Télécharger des certificats** : authentification basée sur des certificats numériques.
  - **Clé publique** : certificat numérique local à utiliser pour authentifier l'appliance NetScaler locale auprès de l'homologue avant d'établir des associations de sécurité IPsec. Le même certificat doit être présent et défini pour le paramètre Peer Public Key dans l'homologue.
  - **Clé privée** : clé privée du certificat numérique local.
  - **Clé publique homologue** : certificat numérique du pair. Utilisé pour authentifier l'homologue auprès du point de terminaison local avant d'établir des associations de sécurité IPsec. Le même certificat doit être présent et défini pour le paramètre de clé publique dans l'homologue.

7. Cliquez sur **Terminé**.

La nouvelle configuration du tunnel CloudBridge Connector sur les deux appliances NetScaler apparaît dans l'onglet Accueil de l'interface graphique correspondante. L'état actuel du tunnel du connecteur CloudBridge est indiqué dans le volet Connecteurs CloudBridge configurés. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance NetScaler à l'aide des compteurs statistiques des tunnels CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

Configuration du CloudBridge Connector entre le centre de données et le cloud AWS

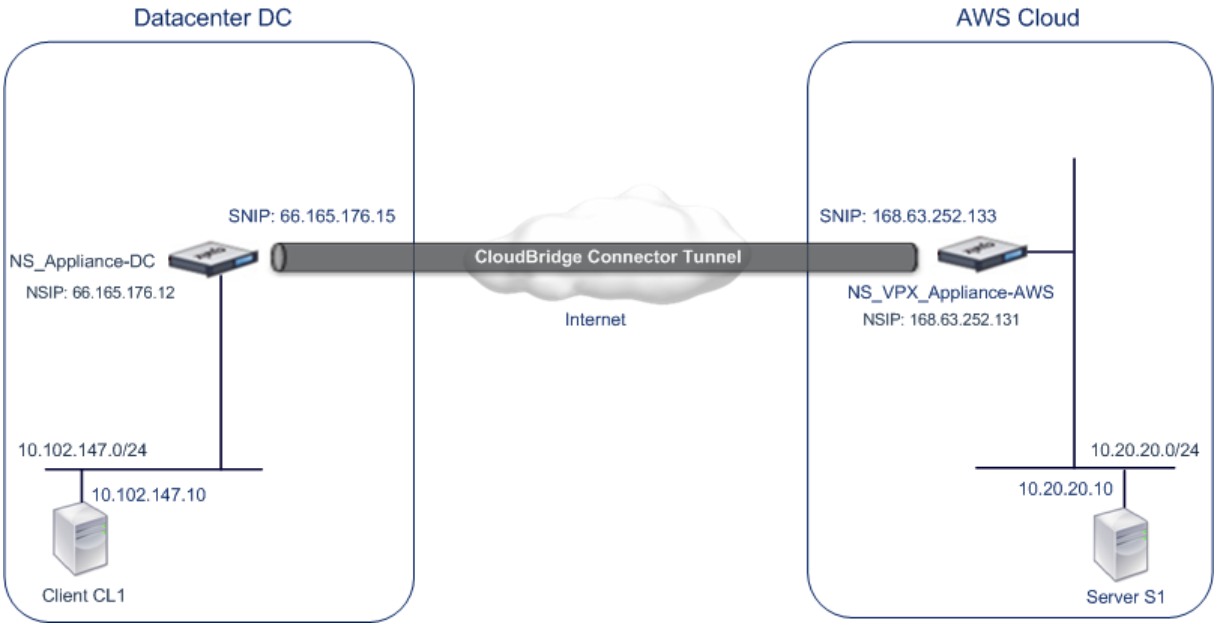
May 5, 2023

Vous pouvez configurer un tunnel CloudBridge Connector entre un centre de données et le cloud AWS afin de tirer parti de l'infrastructure et des capacités informatiques du centre de données et du cloud AWS. Avec AWS, vous pouvez étendre votre réseau sans investissement initial ni coûts de maintenance de l'infrastructure réseau étendue. Vous pouvez faire évoluer votre infrastructure vers le haut ou vers

le bas, selon vos besoins. Par exemple, vous pouvez louer davantage de fonctionnalités de serveur lorsque la demande augmente.

Pour connecter un centre de données au cloud AWS, vous configurez un tunnel CloudBridge Connector entre une appliance NetScaler résidant dans le centre de données et une appliance virtuelle NetScaler (VPX) résidant dans le cloud AWS.

Pour illustrer un tunnel CloudBridge Connector entre un centre de données et le cloud Amazon AWS, prenons un exemple dans lequel un tunnel CloudBridge Connector est configuré entre l'appliance NetScaler NS_Appliance-DC, dans le centre de données DC, et l'appliance virtuelle NetScaler (VPX) NS_VPX_Appliance-AWS.



NS_Appliance-DC et NS_VPX_Appliance-AWS fonctionnent tous deux en mode L3. Ils permettent la communication entre les réseaux privés du centre de données DC et le cloud AWS. NS_Appliance-DC et NS_VPX_Appliance-AWS permettent la communication entre le client CL1 dans le centre de données DC et le serveur S1 dans le cloud AWS via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

> **Remarque** :
>
> AWS ne prend pas en charge le mode L2, il est donc nécessaire que seul le mode L3 soit activé sur les deux points de terminaison.

Pour une communication correcte entre CL1 et S1, le mode L3 est activé sur NS_Appliance-DC et NS_VPX_Appliance-AWS et les itinéraires sont mis à jour comme tels :

- Les CL1 disposent d'une route vers NS_Appliance-DC pour atteindre S1.
- NS_Appliance-DC dispose d'une route vers NS_VPX_Appliance-AWS pour atteindre S1.
- S1 doit disposer d'une route vers NS_VPX_Appliance-AWS pour atteindre CL1.

- NS_VPX_Appliance-AWS dispose d'une route vers NS_Appliance-DC pour atteindre la CL1.

Le tableau suivant répertorie les paramètres de l'appliance NetScaler NS_Appliance-DC dans le centre de données DC.

Entité	Nom	Détails
L'adresse NSIP		66.165.176.12
Adresse SNIP		66.165.176,15
Tunnel CloudBridge Connector	CC_Tunnel_DC-AWS	Adresse IP du point de terminaison local du tunnel CloudBridge Connector : 66.165.176.15, adresse IP du point de terminaison distant du tunnel CloudBridge Connector : 168.63.252.133, détails du tunnel GRE : Name= CC_Tunnel_DC-AWS

Le tableau suivant répertorie les paramètres de NetScaler VPX NS_VPX_Appliance-AWS sur le cloud AWS.

Entité	Nom	Détails
Adresse NSIP		10.102.25.30
Adresse EIP publique mappée à l'adresse NSIP		168.63.252.131
Adresse SNIP		10.102.29.30
Adresse EIP publique mappée à l'adresse SNIP		168.63.252.133

Entité	Nom	Détails
Tunnel CloudBridge Connector	CC_Tunnel_DC-AWS	Adresse IP du point de terminaison local du tunnel CloudBridge Connector : 168.63.252.133, adresse IP du point de terminaison distant du tunnel CloudBridge Connector : 66.165.176.15 ; nom des détails du **tunnel GRE = CC_Tunnel_DC-AWS, détails** du profil IPsec, nom = CC_Tunnel_DC-AWS, algorithme de chiffrement = AES, algorithme de hachage = HMAC SHA1

Composants requis

Avant de configurer un tunnel CloudBridge Connector, vérifiez que les tâches suivantes ont été effectuées :

1. Installez, configurez et lancez une instance de l'appliance virtuelle NetScaler (VPX) sur le cloud AWS. Pour obtenir des instructions sur l'installation de NetScaler VPX sur AWS, consultez Déployer une instance NetScalerVPX sur AWS.
2. Déployez et configurez une appliance physique NetScaler, ou provisionnez et configurez une appliance virtuelle NetScaler (VPX) sur une plate-forme de virtualisation dans le centre de données.
3. Assurez-vous que les adresses IP des points de terminaison du tunnel CloudBridge Connector sont accessibles les unes aux autres.

Licence NetScaler VPX

Après le lancement initial de l'instance, NetScaler VPX pour AWS nécessite une licence. Si vous apportez votre propre licence (BYOL), consultez le Guide de licences VPX à l' adresse suivante : http://support.citrix.com/article/CTX122426.

Vous devez :

1. Utilisez le portail de licences du site Web Citrix pour générer une licence valide.

2. Télécharger la licence sur l'instance.

S'il s'agit d'une instance de marketplace **payante**, vous n'avez pas besoin d'installer une licence. L'ensemble de fonctionnalités et les performances appropriés s'activeront automatiquement.

Étapes de configuration

Pour configurer un tunnel CloudBridge Connector entre une appliance NetScaler résidant dans un centre de données et une appliance virtuelle NetScaler (VPX) résidant sur le cloud AWS, utilisez l'interface graphique de l'appliance NetScaler.

Lorsque vous utilisez l'interface graphique, la configuration du tunnel CloudBridge Connector créée sur l'appliance NetScaler est automatiquement transmise à l'autre point de terminaison ou homologue (le NetScaler VPX sur AWS) du tunnel CloudBridge Connector. Par conséquent, vous n'avez pas besoin d'accéder à l'interface graphique (GUI) du NetScaler VPX sur AWS pour y créer la configuration de tunnel CloudBridge Connector correspondante.

La configuration du tunnel CloudBridge Connector sur les deux homologues (l'appliance NetScaler qui réside dans le centre de données et l'appliance virtuelle NetScaler (VPX) qui réside sur le cloud AWS) comprend les entités suivantes :

- **Profil IPsec** : une entité de profil IPsec spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et le PSK, à utiliser par le protocole IPsec dans les deux homologues du tunnel CloudBridge Connector.
- **Tunnel GRE**—Un tunnel IP spécifie une adresse IP locale (une adresse SNIP publique configurée sur l'homologue local), une adresse IP distante (une adresse SNIP publique configurée sur l'homologue distant), le protocole (GRE) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPsec.
- **Créez une règle PBR et associez-y le tunnel IP** : une entité PBR spécifie un ensemble de conditions et une entité de tunnel IP. La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Vous devez définir la plage d'adresses IP source et la plage d'adresses IP de destination pour spécifier le sous-réseau dont le trafic doit traverser le tunnel CloudBridge Connector. Par exemple, considérez un paquet de requête qui provient d'un client sur le sous-réseau du centre de données et qui est destiné à un serveur sur le sous-réseau dans le cloud AWS. Si ce paquet correspond à la plage d'adresses IP source et de destination de l'entité PBR sur l'appliance NetScaler du centre de données, il est envoyé via le tunnel CloudBridge Connector associé à l'entité PBR.

Pour créer un profil IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `add ipsec profile <name> [-**ikeVersion** ( V1 | V2 )] [-**encAlgo** ( AES | 3DES )...] [-**hashAlgo** <hashAlgo> ...] [-**lifetime** <`

positive_integer>] (-**psk** | (-**publickey** <string> -**privatekey ** <string> -**peerPublicKey** <string>))[-**livenessCheckInterval ** <positive_integer>] [-**replayWindowSize** <positive_integer>] [-**ikeRetryInterval** <positive_integer>] [-**retransmissiontime** < positive_integer>]

- **show ipsec profile** <name>

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol < protocol>] [-ipsecProfileName <string>]
- show ipTunnel <name>

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = < remote_subnet_range> -ipTunnel <tunnel_name>
- apply ns pbrs
- show ns pbr <pbr_name>

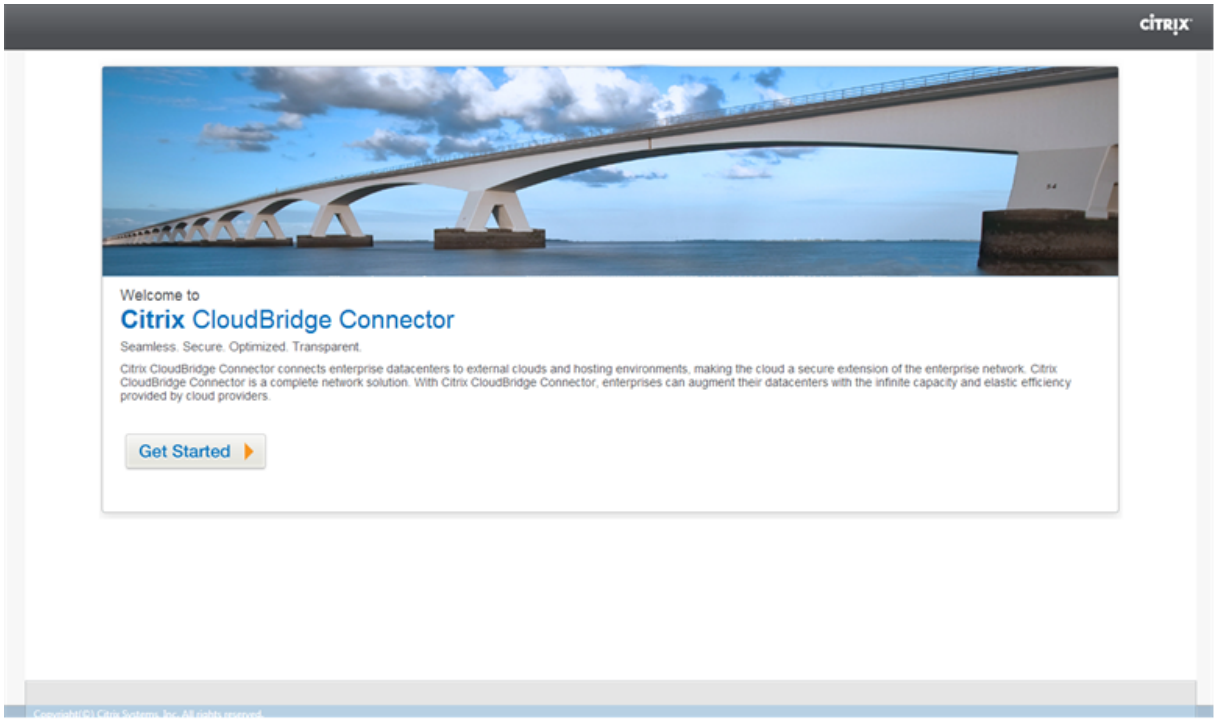
Exemple

```
1      > add ipsec profile CC_Tunnel_DC-AWS -encAlgo AES -hashAlgo
           HMAC_SHA1
2
3      Done
4      > add ipTunnel CC_Tunnel_DC-AWS 168.63.252.133 255.255.255.0
           66.165.176.15 - protocol GRE -ipsecProfileName CC_Tunnel_DC-AWS
5
6      Done
7      > add ns pbr PBR-DC-AWS ALLOW - srcIP 66.165.176.15 - destIP
           168.63.252.133 ipTunnel CC_Tunnel_DC-AWS
8
9      Done
10     > apply ns pbrs
11
12     Done
13 <!--NeedCopy-->
```

Pour configurer un tunnel CloudBridge Connector dans une appliance NetScaler à l'aide de l'interface graphique

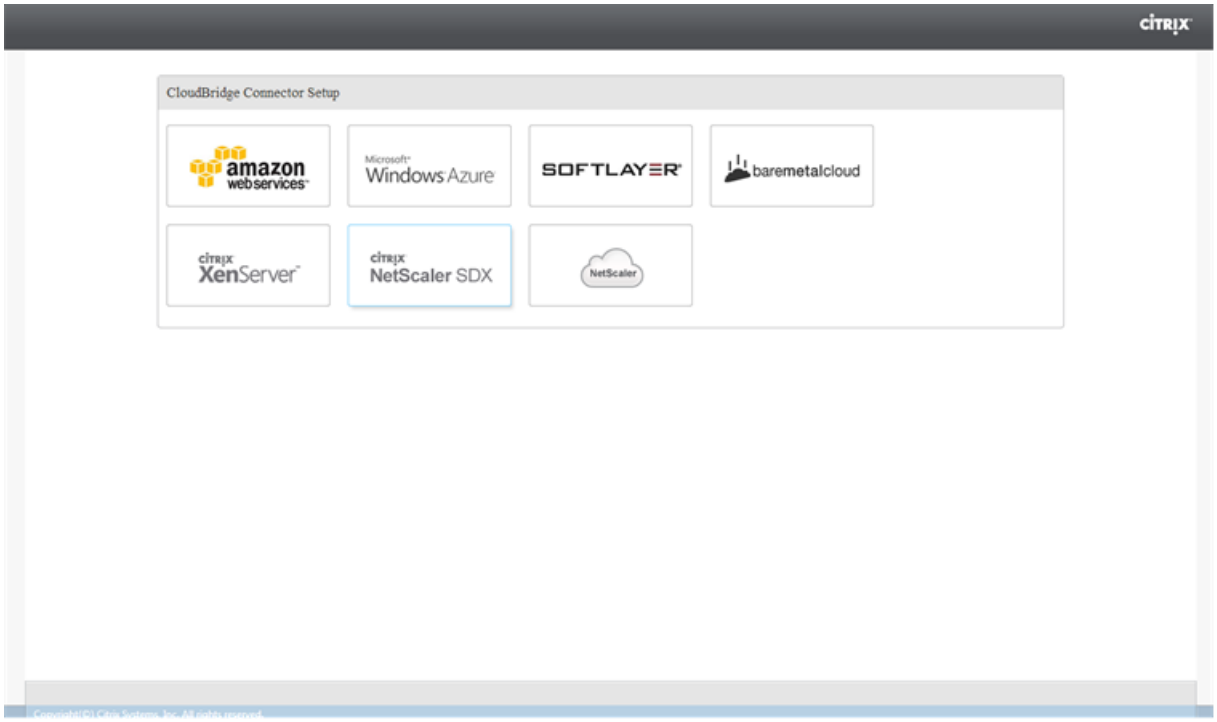
1. Tapez l'adresse NSIP d'une appliance NetScaler dans la ligne d'adresse d'un navigateur Web.

2. Connectez-vous à l'interface graphique de l'appliance NetScaler à l'aide des informations d'identification de votre compte pour l'appliance.
3. Accédez à **Système** > **CloudBridge Connector**.
4. Dans le volet droit, sous **Mise en route**, cliquez sur **Créer/Surveiller CloudBridge**.
5. La première fois que vous configurez un tunnel CloudBridge Connector sur l'appliance, un écran de **bienvenue** s'affiche.
6. Sur l'écran de **bienvenue**, cliquez sur **Commencer**.



> **Remarque** :
>
> Si un tunnel CloudBridge Connector est déjà configuré sur l'appliance NetScaler, l'écran de bienvenue ne s'affiche pas. Vous ne devez donc pas cliquer sur Commencer.

1. Dans le volet de **configuration du CloudBridge Connector**, cliquez sur **Amazon Web Services**



1. Dans le volet **Amazon**, saisissez les informations d'identification de votre compte AWS : ID de clé d'accès AWS et clé d'accès secrète AWS. Vous pouvez obtenir ces clés d'accès à partir de la console AWS GUI. Cliquez sur **Continuer**.

> **Remarque**
>
> Auparavant, l'assistant de configuration se connectait toujours à la même région AWS même lorsqu'une autre région était sélectionnée. Par conséquent, la configuration du tunnel CloudBridge Connector vers un NetScaler VPX s'exécutant sur la région AWS sélectionnée échouait auparavant. Ce problème est désormais résolu.

1. Dans le volet **NetScaler**, sélectionnez l'adresse NSIP de l'appliance virtuelle NetScaler exécutée sur AWS. Fournissez ensuite les informations d'identification de votre compte pour l'appliance virtuelle NetScaler. Cliquez sur **Continuer**.
2. Dans le volet Paramètres **du CloudBridge Connector**, définissez le paramètre suivant :
   - Nom**du CloudBridge Connector : nom**de la configuration du CloudBridge Connector sur l'appliance locale. Doit commencer par un caractère alphabétique ASCII ou un trait de soulignement (_) et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), un espace, deux points (:), à (@), égal (=) et un trait d'union (-). Ne peut pas être modifié après la création de la configuration du CloudBridge Connector.
3. Sous **Paramètres locaux**, définissez le paramètre suivant :
   - **IP du sous-réseau** : adresse IP du point de terminaison local du tunnel CloudBridge Con-

nector. Il doit s'agir d'une adresse IP publique de type SNIP.

4. Sous **Réglage à distance**, définissez le paramètre suivant :

   - **IP du sous-réseau** : adresse IP du point de terminaison du tunnel CloudBridge Connector côté AWS. Il doit s'agir d'une adresse IP de type SNIP sur l'instance NetScaler VPX sur AWS.
   - **NAT** : adresse IP publique (EIP) dans AWS mappée au SNIP configuré sur l'instance NetScaler VPX sur AWS.

5. Sous **Réglage PBR**, définissez les paramètres suivants :

   - **Opération**—La valeur est égale à (=) ou n'est pas égale à (! =) opérateur logique.
   - **IP source faible** : adresse IP source la plus faible à comparer à l'adresse IP source d'un paquet IPv4 sortant.
   - **IP source élevée** : adresse IP source la plus élevée à comparer à l'adresse IP source d'un paquet IPv4 sortant.
   - **Opération**—La valeur est égale à (=) ou n'est pas égale à (! =) opérateur logique.
   - **IP de destination Low**—Adresse IP de destination la plus faible à comparer à l'adresse IP de destination d'un paquet IPv4 sortant.
   - Adresse**IP de destination élevée**—Adresse IP de destination la plus élevée à comparer à l'adresse IP de destination d'un paquet IPv4 sortant.

6. (Facultatif) Dans **Paramètres de sécurité**, définissez les paramètres de protocole IPsec suivants pour le tunnel CloudBridge Connector :

   - **Algorithme**de chiffrement : algorithme de chiffrement à utiliser par le protocole IPsec dans le tunnel CloudBridge.
   - **Algorithme**de hachage : algorithme de hachage à utiliser par le protocole IPsec dans le tunnel CloudBridge.
   - **Clé** : sélectionnez l'une des méthodes d'authentification IPsec suivantes à utiliser par les deux homologues pour s'authentifier mutuellement.
     - **Clé générée automatiquement** : authentification basée sur une chaîne de texte, appelée clé pré-partagée (PSK), générée automatiquement par l'appliance locale. Les clés PSK des homologues sont comparées les unes aux autres à des fins d'authentification.
     - **Clé spécifique** : authentification basée sur une PSK saisie manuellement. Les PSK des homologues sont comparés les uns aux autres à des fins d'authentification.
       * **Clé de sécurité pré-partagée** : chaîne de texte saisie pour l'authentification basée sur une clé pré-partagée.
     - **Télécharger des certificats** : authentification basée sur des certificats numériques.
       * **Clé publique** : certificat numérique local à utiliser pour authentifier l'homologue local auprès de l'homologue distant avant d'établir des associations de sécurité IPsec. Le même certificat doit être présent et défini pour le paramètre Peer Public

Key dans l'homologue.

* **Clé privée** : clé privée du certificat numérique local.
* **Clé publique homologue** : certificat numérique du pair. Utilisé pour authentifier l'homologue auprès du point de terminaison local avant d'établir des associations de sécurité IPsec. Le même certificat doit être présent et défini pour le paramètre de clé publique dans l'homologue.

7. Cliquez sur **Terminé**.

La nouvelle configuration du tunnel CloudBridge Connector sur l'appliance NetScaler du centre de données apparaît dans l'onglet Accueil de l'interface graphique. La nouvelle configuration du tunnel CloudBridge Connector correspondante sur l'appliance NetScaler VPX dans le cloud AWS apparaît sur l'interface graphique. L'état actuel du tunnel du connecteur CloudBridge est indiqué dans le volet CloudBridge configuré. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance NetScaler à l'aide des compteurs statistiques des tunnels CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

Configuration d'un tunnel CloudBridge Connector entre une appliance NetScaler et une passerelle privée virtuelle sur AWS

May 5, 2023

Pour connecter un centre de données à Amazon Web Services (AWS), vous pouvez configurer un tunnel CloudBridge Connector entre une appliance NetScaler du centre de données et une passerelle privée virtuelle sur AWS. L'appliance NetScaler et la passerelle privée virtuelle constituent les points de terminaison du tunnel CloudBridge Connector et sont appelées homologues.

> **Remarque :**
>
> Vous pouvez également configurer un tunnel CloudBridge Connector entre une appliance NetScaler dans un centre de données et une instance NetScaler VPX (au lieu d'une passerelle privée virtuelle) sur AWS. Pour plus d'informations, consultez Configuration de CloudBridge Connector entre Datacenter et AWS Cloud.

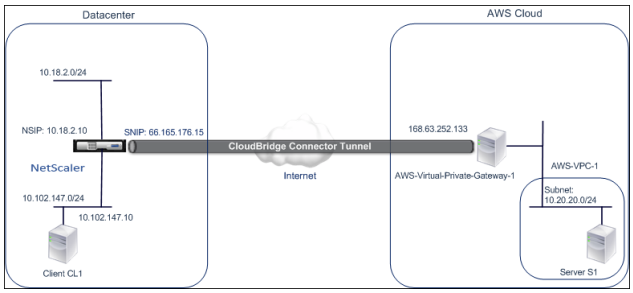
Les passerelles privées virtuelles sur AWS prennent en charge les paramètres IPsec suivants pour un tunnel CloudBridge Connector. Par conséquent, vous devez spécifier les mêmes paramètres IPsec

lorsque vous configurez l'appliance NetScaler pour le tunnel CloudBridge Connector.

Propriétés IPSec	Paramètre
Mode IPSec	Mode tunnel
Version IKE	Version 1
Méthode d'authentification IKE	Clé pré-partagée
Algorithme de chiffrement	AES
algorithme de hachage	HMAC SHA1

Exemple de configuration du tunnel CloudBridge Connector et de flux de données

Pour illustrer le flux de trafic dans un tunnel CloudBridge Connector, prenons un exemple dans lequel un tunnel CloudBridge Connector est configuré entre l'appliance NetScaler NS_Appliance-1 dans un centre de données et la passerelle privée virtuelle AWS-Virtual-Private-Gateway-1 sur le cloud AWS.



NS_Appliance-1 fonctionne également comme un routeur L3, ce qui permet à un réseau privé du centre de données d'accéder à un réseau privé du cloud AWS via le tunnel CloudBridge Connector. En tant que routeur, NS_Appliance-1 permet la communication entre le client CL1 dans le centre de données et le serveur S1 dans le cloud AWS via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel CloudBridge Connector inclut une entité de profil IPsec nommée NS_AWS_IPsec_Profile, une entité de tunnel CloudBridge Connector nommée NS_AWS_Tunnel et une entité de routage basé sur des politiques (PBR) nommée NS_AWS_PBR.

L'entité de profil IPsec NS_AWS_IPsec_Profile spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement et l'algorithme de hachage, à utiliser par le protocole IPsec dans le tunnel CloudBridge Connector. NS_AWS_IPSEC_Profile est lié à l'entité de tunnel IP NS_AWS_Tunnel.

L'entité de tunnel du CloudBridge Connector NS_AWS_Tunnel spécifie l'adresse IP locale (une adresse IP publique, SNIP, configurée sur l'appliance NetScaler), l'adresse IP distante (l'adresse IP de l'AWS-

Virtual-Private-Gateway-1) et le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector. NS_AWS_Tunnel est lié à l'entité de routage basé sur des politiques (PBR) NS_AWS_PBR.

L'entité PBR NS_AWS_PBR spécifie un ensemble de conditions et une entité de tunnel CloudBridge Connector (NS_AWS_Tunnel). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions requises pour NS_AWS_pbr. La plage d'adresses IP source et la plage d'adresses IP de destination sont spécifiées en tant que sous-réseau dans le centre de données et en tant que sous-réseau dans le cloud AWS, respectivement. Tout paquet de demande provenant d'un client du sous-réseau du centre de données et destiné à un serveur du sous-réseau sur le cloud AWS répond aux conditions de NS_AWS_pbr. Ce paquet est ensuite pris en compte pour le traitement du CloudBridge Connector et est envoyé via le tunnel CloudBridge Connector (NS_AWS_Tunnel) lié à l'entité PBR.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Adresse IP du point de terminaison du tunnel CloudBridge Connector (NS_Appliance-1) côté centre de données	66.165.176,15
Adresse IP du point de terminaison du tunnel CloudBridge Connector (AWS-Virtual-Private-Gateway-1) dans AWS	168.63.252.133
Sous-réseau du centre de données, dont le trafic doit traverser le tunnel CloudBridge Connector	10.102.147,0/24
Sous-réseau AWS, dont le trafic doit traverser le tunnel CloudBridge Connector	10.20.20.0/24

Paramètres sur Amazon AWS

Passerelle client	AWS-Customer-Gateway-1	Routage = statique, adresse IP = adresse IP du point de terminaison du tunnel CloudBridge Connector routable sur Internet côté NetScaler = 66.165.176.15
Passerelle privée virtuelle	AWS-Virtual-Private-Gateway-1	VPC associé = AWS-VPC-1

		Routage = statique, adresse IP = adresse IP du point de terminaison du tunnel CloudBridge Connector routable sur Internet côté NetScaler = 66.165.176.15
Passerelle client	AWS-Customer-Gateway-1	
Connexion VPN	AWS-VPN-Connection-1	Passerelle client = AWS-Customer-Gateway-1, Passerelle privée virtuelle = Virtual-Private-Gateway-1, Options de routage : Type = Statique, Préfixes IP statiques = Sous-réseaux côté NetScaler = 10.102.147.0/24

Paramètres de l'appliance NetScaler NS_Appliance-1dans Datacenter-1 :

Appliance	Paramètres
–	–
SNIP1 (à des fins de référence uniquement)	66.165.176,15
Profil IPSe|NS_AWS_IPSEC_Profile|Version IKE = v1, algorithme de chiffrement = AES, algorithme de hachage = HMAC SHA1| |Tunnel de
CloudBridge Connector CloudBridge|NS_AWS_Tunnel|IP distante = 168.63.252.133, IP locale = 66.165.176.15, protocole de tunnel = IPsec, profil IPsec = NS_AWS_IPSEC_Profile| |Route basée sur des politiques	NS_AWS_PBR|Plage d'adresses IP source = Sous-réseau du centre de données =10.102.147.0-10.102.147.255, Plage d'adresses IP de destination = Sous-réseau d'AWS =10.20.20.0-10.20.20.255, Tunnel IP = NS_AWS_Tunnel

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une passerelle AWS, tenez compte des points suivants :

1. AWS prend en charge les paramètres IPsec suivants pour un tunnel CloudBridge Connector. Par conséquent, vous devez spécifier les mêmes paramètres IPsec lorsque vous configurez l'appliance NetScaler pour le tunnel CloudBridge Connector.
    - Version d'IKE = v1
    - Algorithme de chiffrement = AES
    - Algorithme de hachage = HMAC SHA1

2. Vous devez configurer le pare-feu côté NetScaler pour autoriser ce qui suit.
    - Tous les paquets UDP pour le port 500
    - Tous les paquets UDP pour le port 4500
    - Tous les paquets ESP (numéro de protocole IP 50)
3. Vous devez configurer Amazon AWS avant de spécifier la configuration du tunnel sur NetScaler, car l'adresse IP publique de l'extrémité AWS (passerelle) du tunnel et du PSK sont automatiquement générées lorsque vous configurez la configuration du tunnel dans AWS. Vous avez besoin de ces informations pour spécifier la configuration du tunnel sur l'appliance NetScaler.
4. AWS Gateway prend en charge les itinéraires statiques et le protocole BGP pour les mises à jour des itinéraires. L'appliance NetScaler ne prend pas en charge le protocole BGP dans un tunnel CloudBridge Connector vers une passerelle AWS. Par conséquent, des routes statiques appropriées doivent être utilisées des deux côtés du tunnel CloudBridge Connector pour acheminer correctement le trafic via le tunnel.

Configuration d'Amazon AWS pour le tunnel CloudBridge Connector

Pour créer une configuration de tunnel CloudBridge Connector sur Amazon AWS, utilisez la console de gestion Amazon AWS, qui est une interface graphique basée sur le Web permettant de créer et de gérer des ressources sur Amazon AWS.

Avant de commencer la configuration du tunnel CloudBridge Connector sur le cloud AWS, assurez-vous que :

- Vous possédez un compte utilisateur pour le cloud Amazon AWS.
- Vous disposez d'un cloud privé virtuel dont vous souhaitez connecter les réseaux aux réseaux côté NetScaler via le tunnel CloudBridge Connector.
- Vous connaissez la console de gestion Amazon AWS.

> **Remarque** :
>
> Les procédures de configuration d'Amazon AWS pour un tunnel CloudBridge Connector peuvent changer au fil du temps, en fonction du cycle de publication Amazon AWS. Citrix vous recommande de consulter la documentation Amazon AWS pour connaître les dernières procédures.

Pour configurer un tunnel de connecteur CloudBridge entre NetScaler et AWS Gateway, effectuez les tâches suivantes sur la console de gestion AWS :

- **Créez une passerelle client**. Une passerelle client est une entité AWS qui représente le point de terminaison d'un tunnel CloudBridge Connector. Pour un tunnel CloudBridge Connector entre une appliance NetScaler et une passerelle AWS, la passerelle client représente l'appliance NetScaler sur AWS. La passerelle client spécifie un nom, le type de routage (statique ou BGP) utilisé dans le tunnel et l'adresse IP du point de terminaison du tunnel CloudBridge Connector

côté NetScaler. L'adresse IP peut être une adresse IP de sous-réseau appartenant à NetScaler routable sur Internet (SNIP) ou, si l'appliance NetScaler se trouve derrière un périphérique NAT, une adresse IP NAT routable sur Internet qui représente l'adresse SNIP.

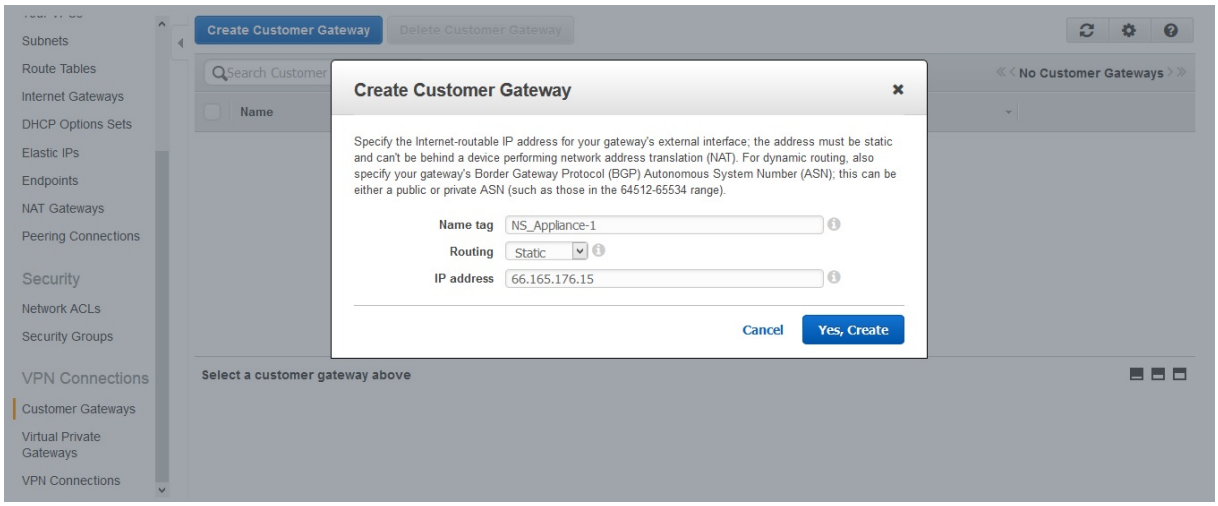
- **Créez une passerelle privée virtuelle et attachez-la à un VPC.** Une passerelle privée virtuelle est un point de terminaison du tunnel CloudBridge Connector côté AWS. Lorsque vous créez une passerelle privée virtuelle, vous lui attribuez un nom ou vous autorisez AWS à lui attribuer ce nom. Vous associez ensuite la passerelle privée virtuelle à un VPC. Cette association permet aux sous-réseaux du VPC de se connecter aux sous-réseaux côté NetScaler via le tunnel CloudBridge Connector.
- **Créez une connexion VPN**. Une connexion VPN spécifie une passerelle client et une passerelle privée virtuelle entre lesquelles un tunnel CloudBridge Connector doit être créé. Il spécifie également un préfixe IP pour les réseaux côté NetScaler. Seuls les préfixes IP connus de la passerelle privée virtuelle (via une entrée de route statique) peuvent recevoir le trafic du VPC via le tunnel. De plus, la passerelle privée virtuelle n'achemine aucun trafic non destiné aux préfixes IP spécifiés via le tunnel. Après avoir configuré une connexion VPN, vous devrez peut-être attendre quelques minutes pour qu'elle soit créée.
- **Configurez les options de routage**. Pour que le réseau du VPC atteigne les réseaux côté NetScaler via le tunnel CloudBridge Connector, vous devez configurer la table de routage du VPC pour inclure les routes des réseaux côté NetScaler et pointer ces routes vers la passerelle privée virtuelle. Vous pouvez inclure des routes dans la table de routage d'un VPC de l'une des manières suivantes :
  - **Activez la propagation des itinéraires**. Vous pouvez activer la propagation des itinéraires pour votre table de routage afin que les itinéraires soient automatiquement propagés vers la table. Les préfixes IP statiques que vous spécifiez pour la configuration VPN sont propagés vers la table de routage une fois que vous avez créé la connexion VPN.
  - **Entrez manuellement des itinéraires statiques**. Si vous n'activez pas la propagation des itinéraires, vous devez saisir manuellement les itinéraires statiques pour les réseaux côté NetScaler.
- **Téléchargez la configuration**. Une fois la configuration du tunnel CloudBridge Connector (connexion VPN) créée sur AWS, téléchargez le fichier de configuration de la connexion VPN sur votre système local. Vous aurez peut-être besoin des informations du fichier de configuration pour configurer le tunnel CloudBridge Connector sur l'appliance NetScaler.

Pour créer une passerelle client

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Accédez à **Connexions VPN** > **Passerelles client** et cliquez sur **Créer une passerelle client**.
3. Dans la boîte de dialogue **Créer une passerelle client**, définissez les paramètres suivants, puis cliquez sur **Oui, Créer** :
   - **Étiquette nominative**. Un nom pour la passerelle client.
   - **Liste de routage**. Type de routage entre l'appliance NetScaler et la passerelle privée

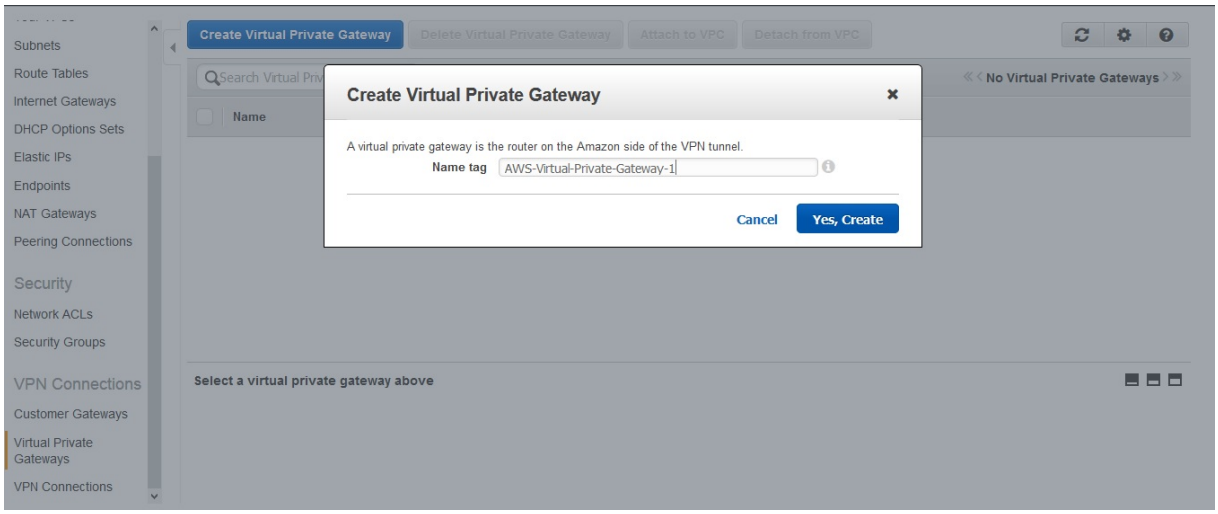
virtuelle AWS pour les itinéraires publicitaires via le tunnel CloudBridge Connector. Sélectionnez **Routage statique** dans la liste de **routage** . **Remarque** : L'appliance NetScaler ne prend pas en charge le protocole BGP dans un tunnel CloudBridge Connector vers une passerelle AWS. Par conséquent, des routes statiques appropriées doivent être utilisées des deux côtés du tunnel CloudBridge Connector pour acheminer correctement le trafic via le tunnel.

- **Adresse IP**. Adresse IP du point de terminaison du tunnel CloudBridge Connector routable sur Internet côté NetScaler. L'adresse IP peut être une adresse IP de sous-réseau appartenant à NetScaler routable sur Internet (SNIP) ou, si l'appliance NetScaler se trouve derrière un périphérique NAT, une adresse IP NAT routable sur Internet qui représente l'adresse SNIP.

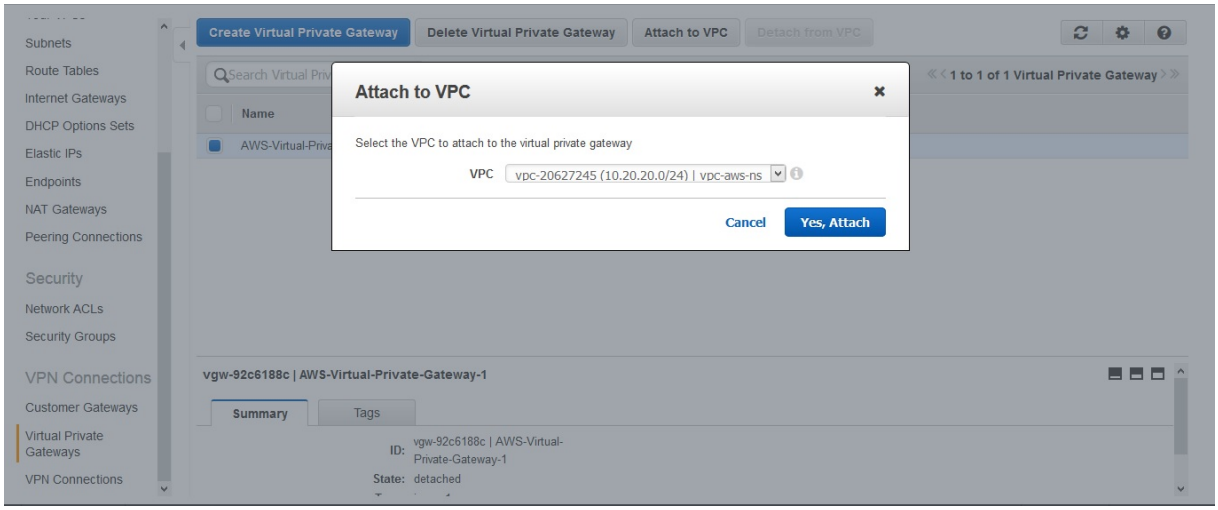


Pour créer une passerelle privée virtuelle et l'associer à un VPC

1. Accédez à **Connexions VPN** > **Passerelles privées virtuelles**, puis cliquez sur Créer une passerelle privée virtuelle.
2. Entrez un nom pour la passerelle privée virtuelle, puis cliquez sur Oui, Créer.

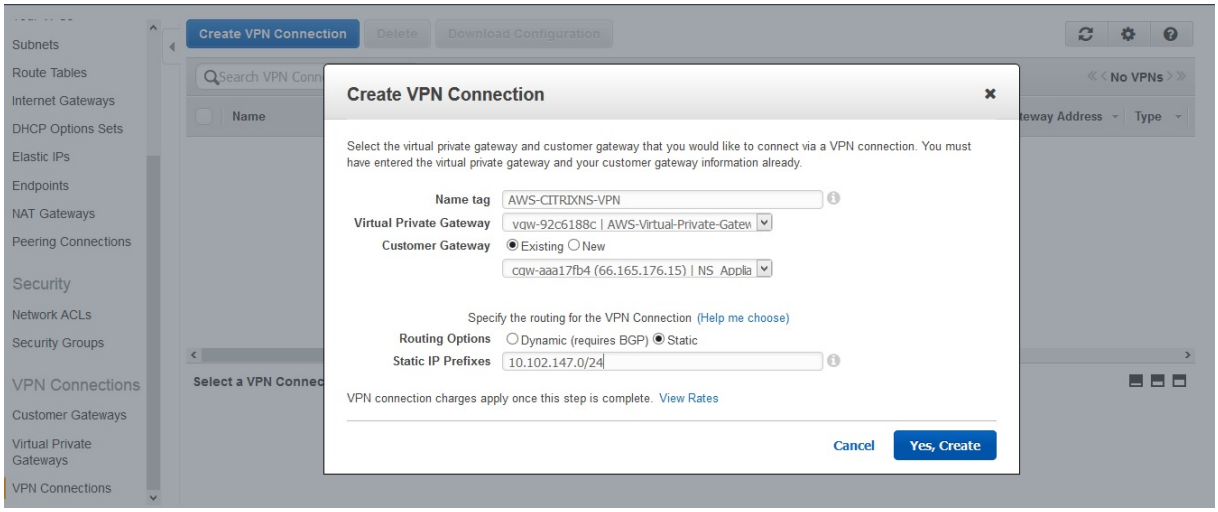


1. Sélectionnez la passerelle privée virtuelle que vous avez créée, puis cliquez sur Attacher au VPC.
2. Dans la boîte de dialogue Attacher au VPC, sélectionnez votre VPC dans la liste, puis choisissez Oui, Attacher.



Pour créer une connexion VPN :

1. Accédez à Connexions VPN > Connexions VPN, puis cliquez sur Créer une connexion VPN.
2. Dans la boîte de dialogue Créer une connexion VPN, définissez les paramètres suivants, puis choisissez Oui, Créer :
   - **Étiquette nominative**. Un nom pour la connexion VPN.
   - **Passerelle privée virtuelle**. Sélectionnez la passerelle privée virtuelle que vous avez créée précédemment.
   - **Passerelle client**. Sélectionnez Existant. Ensuite, dans la liste déroulante, sélectionnez la passerelle client que vous avez créée précédemment.
   - **Options de routage**. Type de routage entre la passerelle privée virtuelle et la passerelle client (appliance NetScaler). Sélectionnez Statique. Dans le champ Préfixes IP statiques, spécifiez les préfixes IP du sous-réseau côté NetScaler, en les séparant par des virgules.



Pour activer la propagation des itinéraires :

1. Accédez à **Tables** de routage et sélectionnez la table de routage associée au sous-réseau dont le trafic doit traverser le tunnel CloudBridge Connector.

> **Remarque**
>
> Par défaut, il s'agit de la table de routage principale du VPC.

1. Dans l'onglet **Propagation de l'itinéraire** du volet de détails, choisissez **Modifier**, sélectionnez la passerelle privée virtuelle, puis cliquez **sur Enregistrer**.

Pour saisir manuellement des itinéraires statiques :

1. Accédez à **Tables de routage** et sélectionnez votre table de routage.
2. Dans l'onglet **Itinéraires**, cliquez sur **Modifier**.
3. Dans le champ **Destination**, entrez l'itinéraire statique utilisé par votre tunnel CloudBridge Connector (connexion VPN).
4. Sélectionnez l'ID de passerelle privée virtuelle dans la liste des **cibles**, puis cliquez sur **Enregistrer**.

Pour télécharger le fichier de configuration :

1. Accédez à **Connexion VPN**, sélectionnez une connexion VPN, puis cliquez sur **Télécharger la configuration**.
2. Dans la boîte **de dialogue Configuration du téléchargement**, définissez les paramètres suivants, puis cliquez sur **Oui, Télécharger**.
    - **Vendeur**. Sélectionnez **Générique**.
    - **Plateforme**. Sélectionnez **Générique**.
    - **Logiciel**. Sélectionnez **Vendor Agnostic.**

Configuration de l'appliance NetScaler pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une passerelle privée virtuelle sur le cloud AWS, effectuez les tâches suivantes sur l'appliance NetScaler.
Vous pouvez utiliser la ligne de commande NetScaler ou l'interface graphique.

- **Créez un profil IPsec**. Une entité de profil IPsec spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et le PSK à utiliser par le protocole IPsec dans le tunnel CloudBridge Connector.
- **Créez un tunnel IP qui utilise le protocole IPsec et associez-y le profil IPsec**. Un tunnel IP spécifie l'adresse IP locale (une adresse SNIP configurée sur l'appliance NetScaler), l'adresse IP distante (l'adresse IP publique de la passerelle privée virtuelle dans AWS), le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.

- **Créez une règle PBR et associez-la au tunnel IP**. Une entité PBR spécifie un ensemble de règles et une entité de tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Définissez la plage d'adresses IP source pour spécifier le sous-réseau côté NetScaler dont le trafic doit traverser le tunnel, et définissez la plage d'adresses IP de destination pour spécifier le sous-réseau AWS VPC dont le trafic doit traverser le tunnel CloudBridge Connector. Tout paquet de demande qui provient d'un client du sous-réseau côté NetScaler et qui est destiné à un serveur du sous-réseau cloud AWS, et qui correspond à la plage d'adresses IP source et de destination de l'entité PBR, est envoyé via le tunnel CloudBridge Connector associé à l'entité PBR.

Pour créer un profil IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add ipsec profile <name> -psk <string> -**ikeVersion** v1`
- `show ipsec profile** <name>`

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP** <subnet-range> -*ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Les commandes suivantes créent tous les paramètres de l'appliance NetScaler NS_Appliance-1 utilisés dans « Exemple de configuration et de flux de données du CloudBridge Connector ». «

```
1     > add ipsec profile NS_AWS_IPSec_Profile -psk
          DkiMgMdcbqvYREEuIvxsbKkW0Foyabcd -ikeVersion v1 - lifetime
          31536000
2     Done
3     > add iptunnel NS_AWS_Tunnel 168.63.252.133 255.255.255.255
          66.165.176.15 - protocol IPSEC - ipsecProfileName
          NS_AWS_IPSec_Profile
4
5     Done
6     > add pbr NS_AWS_Pbr -srcIP 10.102.147.0-10.102.147.255 - destIP
          10.20.0.0-10.20.255.255 - ipTunnel NS_AWS_Tunnel
```



```
7       Done
8
9       > apply pbrs
10
11      Done
12  <!--NeedCopy-->
```

Pour créer un profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > Profil **IPsec**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un profil IPsec**, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE (sélectionnez V1)
4. Sélectionnez la méthode **d'authentification par clé pré-partagée** et définissez le paramètre **Pre-Shared Key Exists.**
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur Ajouter.
3. Dans la boîte de dialogue **Ajouter un tunnel IP**, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque à distance
   - Type d'adresse IP locale (Dans la liste déroulante Type d'adresse IP locale, sélectionnez Adresse IP du sous-réseau).
   - Adresse IP locale (Toutes les adresses IP configurées du type d'adresse IP sélectionné figurent dans la liste déroulante des adresses IP locales. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPSec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.

2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un PBR**, définissez les paramètres suivants :
    - Nom
    - Action
    - Type de saut suivant (sélectionnez le tunnel IP)
    - Nom du tunnel IP
    - IP de la source : faible
    - IP de la source : élevée
    - IP de destination faible
    - IP de destination : élevée
4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration du tunnel CloudBridge Connector correspondante sur l'appliance NetScaler apparaît dans l'interface graphique.

L'état actuel du tunnel du connecteur CloudBridge est affiché dans le volet Configuré du CloudBridge Connector. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance NetScaler à l'aide des compteurs statistiques des tunnels CloudBridge Connector.
Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

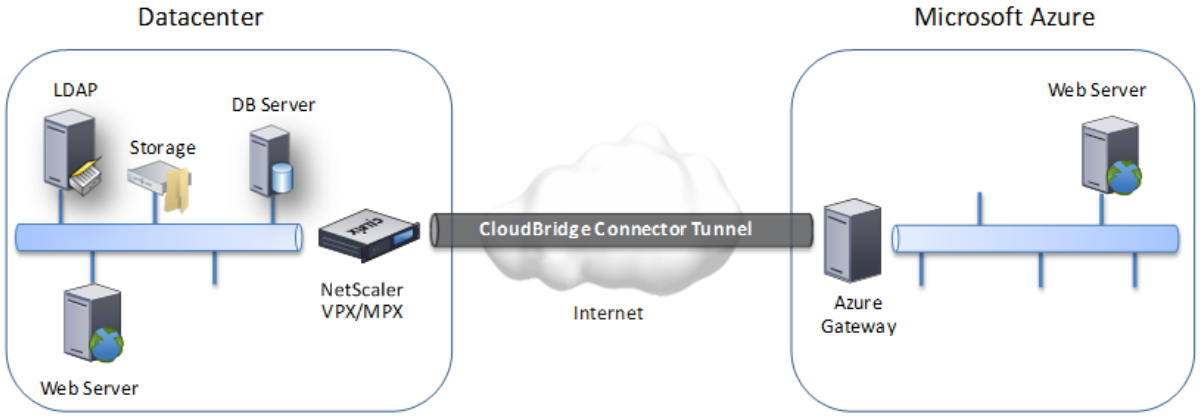
Configuration d'un tunnel CloudBridge Connector entre un centre de données et le cloud Azure

May 5, 2023

L'appliance NetScaler fournit une connectivité entre les centres de données de votre entreprise et le fournisseur d'hébergement cloud Microsoft, Azure, faisant d'Azure une extension transparente du réseau d'entreprise. NetScaler chiffre la connexion entre le centre de données de l'entreprise et le cloud Azure afin que toutes les données transférées entre les deux soient sécurisées.

Fonctionnement du tunnel CloudBridge Connector

Pour connecter un centre de données au cloud Azure, vous configurez un tunnel CloudBridge Connector entre une appliance NetScaler résidant dans le centre de données et une passerelle résidant dans le cloud Azure. L'appliance NetScaler du centre de données et la passerelle du cloud Azure sont les points de terminaison du tunnel CloudBridge Connector et sont appelées homologues du tunnel CloudBridge Connector.



Un tunnel CloudBridge Connector entre un centre de données et le cloud Azure utilise la suite de protocoles IPsec (Internet Protocol Security) standard ouverte, en mode tunnel, pour sécuriser les communications entre homologues dans le tunnel CloudBridge Connector. Dans un tunnel CloudBridge Connector, IPsec garantit :

- Intégrité des données
- Authentification d'origine des données
- Confidentialité des données (cryptage)
- Protection contre les attaques par rediffusion

IPsec utilise le mode tunnel dans lequel le paquet IP complet est crypté puis encapsulé. Le chiffrement utilise le protocole ESP (Encapsulating Security Payload), qui garantit l'intégrité du paquet à l'aide d'une fonction de hachage HMAC et garantit la confidentialité à l'aide d'un algorithme de cryptage. Après avoir chiffré la charge utile et calculé le HMAC, le protocole ESP génère un en-tête ESP et l'insère avant le paquet IP crypté. Le protocole ESP génère également une bande-annonce ESP et l'insère à la fin du paquet.

Le protocole IPsec encapsule ensuite le paquet résultant en ajoutant un en-tête IP avant l'en-tête ESP. Dans l'en-tête IP, l'adresse IP de destination est définie sur l'adresse IP de l'homologue CloudBridge Connecter.

Les homologues du tunnel CloudBridge Connector utilisent le protocole IKEv1 (Internet Key Exchange version 1) (qui fait partie de la suite de protocoles IPsec) pour négocier des communications sécurisées, comme suit :

1. Les deux homologues s'authentifient mutuellement à l'aide d'une authentification par clé pré-

partagée, dans laquelle les pairs échangent une chaîne de texte appelée clé pré-partagée (PSK). Les clés pré-partagées sont comparées les unes aux autres à des fins d'authentification. Par conséquent, pour que l'authentification soit réussie, vous devez configurer la même clé pré-partagée sur chacun des homologues.

2. Les pairs négocient ensuite pour parvenir à un accord sur :

   - Un algorithme de chiffrement
   - Clés cryptographiques permettant de chiffrer les données sur un homologue et de les déchiffrer sur l'autre.

   Cet accord sur le protocole de sécurité, l'algorithme de chiffrement et les clés cryptographiques est appelé Security Association (SA). Les AA sont unidirectionnels (simplex). Par exemple, lorsqu'un tunnel CloudBridge Connector est configuré entre une appliance NetScaler dans un centre de données et une passerelle dans un cloud Azure, l'appliance de centre de données et la passerelle Azure possèdent deux SA. Une SA est utilisée pour traiter les paquets sortants et l'autre SA est utilisée pour traiter les paquets entrants. Les SA expirent après un intervalle de temps spécifié, appelé durée de vie.

Exemple de configuration du tunnel CloudBridge Connector et de flux de données

Pour illustrer le tunnel CloudBridge Connector, prenons un exemple dans lequel un tunnel CloudBridge Connector est configuré entre l'appliance NetScaler CB_Appliance-1 dans un centre de données et la passerelle Azure_Gateway-1 dans le cloud Azure.

CB_Appliance-1 fonctionne également comme un routeur L3, ce qui permet à un réseau privé du centre de données d'accéder à un réseau privé du cloud Azure via le tunnel CloudBridge Connector. En tant que routeur, CB_Appliance-1 permet la communication entre le client CL1 dans le centre de données et le serveur S1 dans le cloud Azure via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur CB_Appliance-1, la configuration du tunnel CloudBridge Connector inclut une entité de profil IPsec nommée CB_Azure_IPSEC_Profile, une entité de tunnel CloudBridge Connector nommée CB_Azure_Tunnel et une entité de routage basé sur des politiques (PBR) nommée CB_Azure_PBR.

L'entité de profil IPsec CB_Azure_IPSEC_Profile spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement et l'algorithme de hachage, à utiliser par le protocole IPsec dans le tunnel CloudBridge Connector. CB_Azure_IPSEC_Profile est lié à l'entité de tunnel IP CB_Azure_Tunnel.

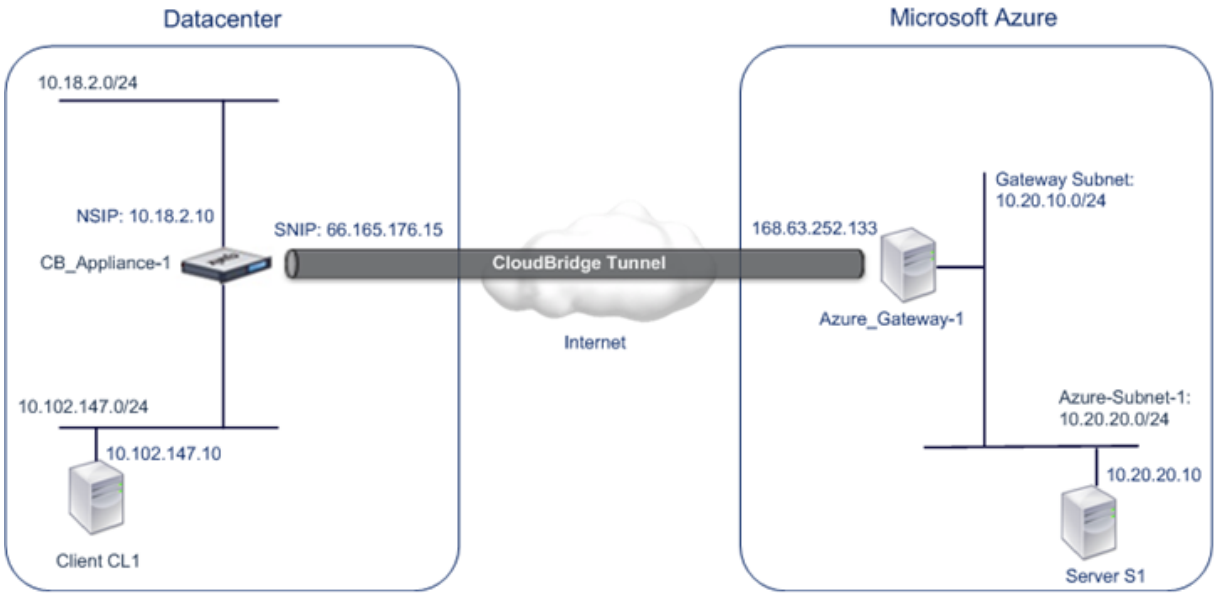
L'entité de tunnel du CloudBridge Connector CB_Azure_Tunnel spécifie l'adresse IP locale (une adresse IP publique (SNIP) configurée sur l'appliance NetScaler), l'adresse IP distante (l'adresse IP de l'Azure_Gateway-1) et le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector. CB_Azure_Tunnel est lié à l'entité PBR CB_Azure_PBR.

L'entité PBR CB_Azure_PBR spécifie un ensemble de conditions et une entité de tunnel CloudBridge Connector (CB_Azure_Tunnel). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions requises pour CB_Azure_PBR. La plage d'adresses IP source et la plage d'adresses IP de destination sont spécifiées en tant que sous-réseau dans le centre de données et en tant que sous-réseau dans le cloud Azure, respectivement. Tout paquet de demande provenant d'un client du sous-réseau du centre de données et destiné à un serveur du sous-réseau sur le cloud Azure répond aux conditions de CB_Azure_PBR. Ce paquet est ensuite pris en compte pour le traitement CloudBridge et est envoyé via le tunnel CloudBridge Connector (CB_Azure_Tunnel) lié à l'entité PBR.

Sur Microsoft Azure, la configuration du tunnel CloudBridge Connector inclut une entité réseau locale nommée My-Datacenter-Network, une entité réseau virtuelle nommée Azure-Network-for-Cloudbridge-Tunnel et une passerelle nommée Azure_Gateway-1.

L'entité réseau locale (locale pour Azure) My-Datacenter-Network spécifie l'adresse IP de l'appliance NetScaler côté centre de données et le sous-réseau du centre de données dont le trafic doit traverser le tunnel CloudBridge Connector. L'entité réseau virtuelle Azure-Network-for-CloudBridge-Tunnel définit un sous-réseau privé nommé Azure-Subnet-1 dans Azure. Le trafic du sous-réseau traverse le tunnel CloudBridge Connector. Le serveur S1 est provisionné dans ce sous-réseau.

L'entité réseau locale My-Datacenter-Network est associée à l'entité réseau virtuelle Azure-Network-for-Cloudbridge-Tunnel. Cette association définit les détails du réseau distant et local de la configuration du tunnel CloudBridge Connector dans Azure. Gateway Azure_Gateway-1 a été créé pour que cette association devienne le point de terminaison CloudBridge à l'extrémité Azure du tunnel CloudBridge Connector.



Pour plus d'informations sur les paramètres, reportez-vous au document PDF CloudBridge Connector Tunnel Settings .

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector entre une appliance NetScaler dans un centre de données et Microsoft Azure, tenez compte des points suivants :

1. L'appliance NetScaler doit disposer d'une adresse IPv4 publique (type SNIP) à utiliser comme adresse de point de terminaison du tunnel CloudBridge Connector. De plus, l'appliance NetScaler ne doit pas se trouver derrière un périphérique NAT.
2. Azure prend en charge les paramètres IPsec suivants pour un tunnel CloudBridge Connector. Par conséquent, vous devez spécifier les mêmes paramètres IPsec lors de la configuration de NetScaler pour le tunnel CloudBridge Connector.
    - Version d'IKE = v1
    - Algorithme de chiffrement = AES
    - Algorithme de hachage = HMAC SHA1
3. Vous devez configurer le pare-feu en périphérie du centre de données pour autoriser ce qui suit.
    - Tous les paquets UDP pour le port 500
    - Tous les paquets UDP pour le port 4500
    - Tous les paquets ESP (numéro de protocole IP 50)
4. La retouche IKE, qui consiste à renégocier de nouvelles clés cryptographiques entre les points de terminaison du tunnel CloudBridge Connector afin d'établir de nouvelles SA, n'est pas prise en charge. Lorsque les associations de sécurité (SA) expirent, le tunnel passe à l'état DOWN. Par conséquent, vous devez définir une valeur très élevée pour la durée de vie des SA.
5. Vous devez configurer Microsoft Azure avant de spécifier la configuration du tunnel sur NetScaler, car l'adresse IP publique de l'extrémité Azure (passerelle) du tunnel et du PSK sont automatiquement générées lorsque vous configurez la configuration du tunnel dans Azure. Vous avez besoin de ces informations pour spécifier la configuration du tunnel sur NetScaler.

Configuration du tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre votre centre de données et Azure, vous devez installer CloudBridge VPX/MPX dans votre centre de données, configurer Microsoft Azure pour le tunnel CloudBridge Connector, puis configurer l'appliance NetScaler dans le centre de données pour le tunnel CloudBridge Connector.

La configuration d'un tunnel CloudBridge Connector entre une appliance NetScaler dans un centre de données et Microsoft Azure comprend les tâches suivantes :

1. **Configuration de l'appliance NetScaler dans le**centre de données. Cette tâche implique le déploiement et la configuration d'un dispositif physique NetScaler (MPX), ou le provisionnement et la configuration d'un dispositif virtuel NetScaler (VPX) sur une plate-forme de virtualisation du centre de données.
2. **Configuration de Microsoft Azure pour le tunnel CloudBridge Connector**. Cette tâche im-

plique la création d'entités de réseau local, de réseau virtuel et de passerelle dans Azure. L'entité réseau locale spécifie l'adresse IP du point de terminaison du tunnel CloudBridge Connector (l'appliance NetScaler) côté centre de données et le sous-réseau du centre de données dont le trafic doit traverser le tunnel CloudBridge Connector. Le réseau virtuel définit un réseau sur Azure. La création du réseau virtuel inclut la définition d'un sous-réseau dont le trafic doit traverser le tunnel CloudBridge Connector à former. Vous associez ensuite le réseau local au réseau virtuel. Enfin, vous créez une passerelle qui devient le point final à l'extrémité Azure du tunnel CloudBridge Connector.

3. **Configuration de l'appliance NetScaler dans le centre de données pour le tunnel CloudBridge**Connector. Cette tâche implique la création d'un profil IPsec, d'une entité de tunnel IP et d'une entité PBR dans l'appliance NetScaler du centre de données. L'entité de profil IPsec spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et le PSK, à utiliser dans le tunnel CloudBridge Connector. Le tunnel IP spécifie l'adresse IP des points de terminaison du tunnel CloudBridge Connector (l'appliance NetScaler dans le centre de données et la passerelle dans Azure) et le protocole à utiliser dans le tunnel CloudBridge Connector. Vous associez ensuite l'entité de profil IPsec à l'entité de tunnel IP. L'entité PBR spécifie les deux sous-réseaux, dans le centre de données et dans le cloud Azure, qui doivent communiquer entre eux via le tunnel CloudBridge Connector. Vous associez ensuite l'entité tunnel IP à l'entité PBR.

Configuration de Microsoft Azure pour le tunnel CloudBridge Connector

Pour créer une configuration de tunnel CloudBridge Connector sur Microsoft Azure, utilisez le portail de gestion Microsoft Windows Azure, qui est une interface graphique basée sur le Web permettant de créer et de gérer des ressources sur Microsoft Azure.

Avant de commencer la configuration du tunnel CloudBridge Connector sur le cloud Azure, assurez-vous que :

- Vous disposez d'un compte utilisateur pour Microsoft Azure.
- Vous avez une compréhension conceptuelle de Microsoft Azure.
- Vous connaissez le portail de gestion Microsoft Windows Azure.

Pour configurer un tunnel CloudBridge Connector entre un centre de données et un cloud Azure, effectuez les tâches suivantes sur Microsoft Azure à l'aide du portail de gestion Microsoft Windows Azure :

- **Créez une entité de réseau local**. Créez une entité réseau locale dans Windows Azure pour spécifier les détails du réseau du centre de données. Une entité réseau locale spécifie l'adresse IP du point de terminaison du tunnel CloudBridge Connector (NetScaler) côté centre de données et du sous-réseau du centre de données dont le trafic doit traverser le tunnel CloudBridge Connector.
- **Créez un réseau virtuel**. Créez une entité réseau virtuelle qui définit un réseau sur Azure. Cette

tâche inclut la définition d'un espace d'adressage privé, dans lequel vous fournissez une plage d'adresses privées et de sous-réseaux appartenant à la plage spécifiée dans l'espace d'adresses. Le trafic des sous-réseaux traversera le tunnel CloudBridge Connector. Vous associez ensuite une entité réseau locale à l'entité réseau virtuelle. Cette association permet à Azure de créer une configuration pour un tunnel CloudBridge Connector entre le réseau virtuel et le réseau du centre de données. Une passerelle (à créer) dans Azure pour ce réseau virtuel sera le point de terminaison CloudBridge à l'extrémité Azure du tunnel CloudBridge Connector. Vous définissez ensuite un sous-réseau privé pour la passerelle à créer. Ce sous-réseau appartient à la plage spécifiée dans l'espace d'adressage de l'entité réseau virtuelle.

- **Créez une passerelle dans Windows Azure**. Créez une passerelle qui deviendra le point final à l'extrémité Azure du tunnel CloudBridge Connector. Azure, à partir de son pool d'adresses IP publiques, attribue une adresse IP à la passerelle créée.
- **Rassemblez l'adresse IP publique de la passerelle et la clé pré-partagée.** Pour une configuration de tunnel CloudBridge Connector sur Azure, l'adresse IP publique de la passerelle et la clé pré-partagée (PSK) sont automatiquement générées par Azure. Prenez note de ces informations. Vous en aurez besoin pour configurer le tunnel CloudBridge Connector sur le centre de données NetScaler.

> **Remarque :**
>
> Les procédures de configuration de Microsoft Azure pour un tunnel CloudBridge Connector peuvent changer au fil du temps, en fonction du cycle de publication de Microsoft Azure. Pour connaître les procédures les plus récentes, consultez la documentation Microsoft Azure.

Configuration de l'appliance NetScaler dans le centre de données pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre un centre de données et un cloud Azure, effectuez les tâches suivantes sur le NetScaler du centre de données. Vous pouvez utiliser la ligne de commande NetScaler ou l'interface graphique :

- **Créez un profil IPsec**. Une entité de profil IPsec spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et le PSK, à utiliser par le protocole IPsec dans le tunnel CloudBridge Connector.
- **Créez un tunnel IP avec le protocole IPsec et associez-y le profil IPsec**. Un tunnel IP spécifie l'adresse IP locale (une adresse SNIP publique configurée sur l'appliance NetScaler), l'adresse IP distante (l'adresse IP publique de la passerelle dans Azure), le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.
- **Créez une règle PBR et associez-y le tunnel IP**. Une entité PBR spécifie un ensemble de conditions et une entité de tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Vous devez définir

la plage d'adresses IP source pour spécifier le sous-réseau du centre de données dont le trafic doit traverser le tunnel, et la plage d'adresses IP de destination pour spécifier le sous-réseau Azure dont le trafic doit traverser le tunnel CloudBridge Connector. Tout paquet de demande provenant d'un client du sous-réseau du centre de données et destiné à un serveur du sous-réseau sur le cloud Azure correspond à la plage d'adresses IP source et de destination de l'entité PBR. Ce paquet est ensuite pris en compte pour le traitement du tunnel CloudBridge Connector et est envoyé via le tunnel CloudBridge Connector associé à l'entité PBR.

L'interface graphique regroupe toutes ces tâches dans un seul assistant appelé assistant CloudBridge Connector.
Pour créer un profil IPSEC à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

```
add ipsec profile <name> -psk <string> -ikeVersion v1
```

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

```
add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -
ipsecProfileName <string>
```

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande NetScaler

```
add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> ipTunnel
 <tunnelName> apply pbrs
```

Exemple de configuration

Les commandes suivantes créent tous les paramètres de l'appliance NetScaler CB_Appliance-1 utilisés dans « Exemple de configuration et de flux de données du CloudBridge Connector ».

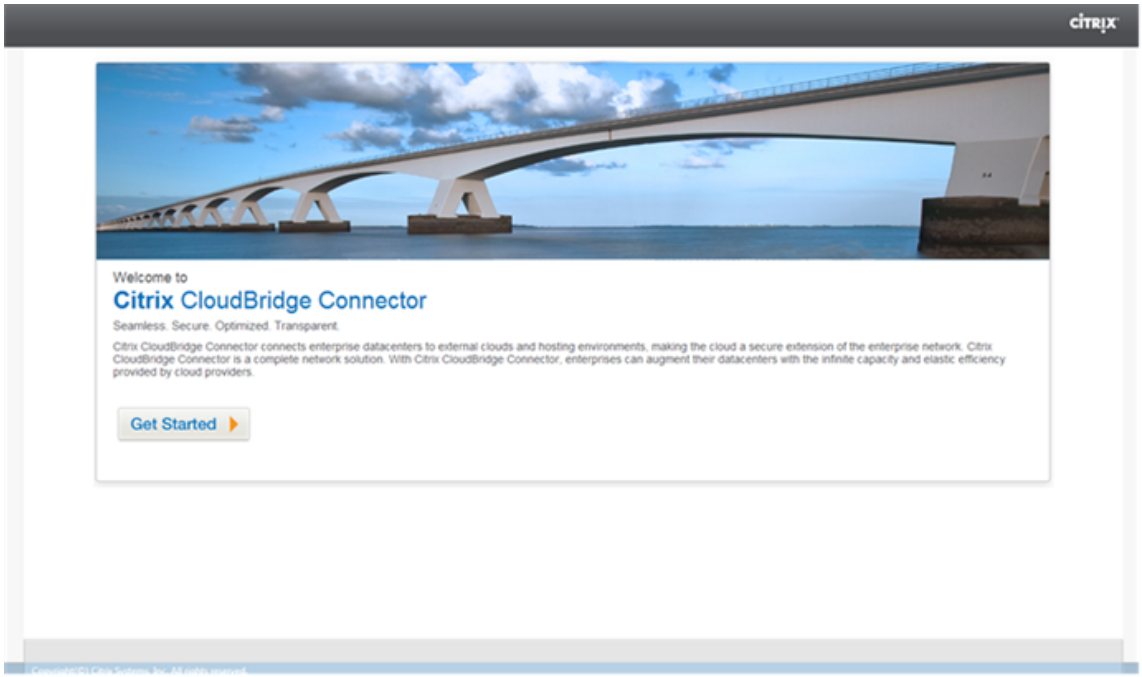
```
1  > add ipsec profile CB_Azure_IPSec_Profile -psk
       DkiMgMdcbqvYREEuIvxsbKkW0FOyDiLM  -ikeVersion v1  - lifetime 31536000
2  Done
3
4  >  add iptunnel CB_Azure_Tunnel 168.63.252.133 255.255.255.255
       66.165.176.15  - protocol IPSEC  - ipsecProfileName
       CB_Azure_IPSec_Profile
5  Done
6
7  > add pbr CB_Azure_Pbr -srcIP 10.102.147.0-10.102.147.255  - destIP
       10.20.0.0-10.20.255.255  - ipTunnelCB_Azure_Tunnel
8  Done
9
10 > apply pbrs
11 Done
```



```
<!--NeedCopy-->
```

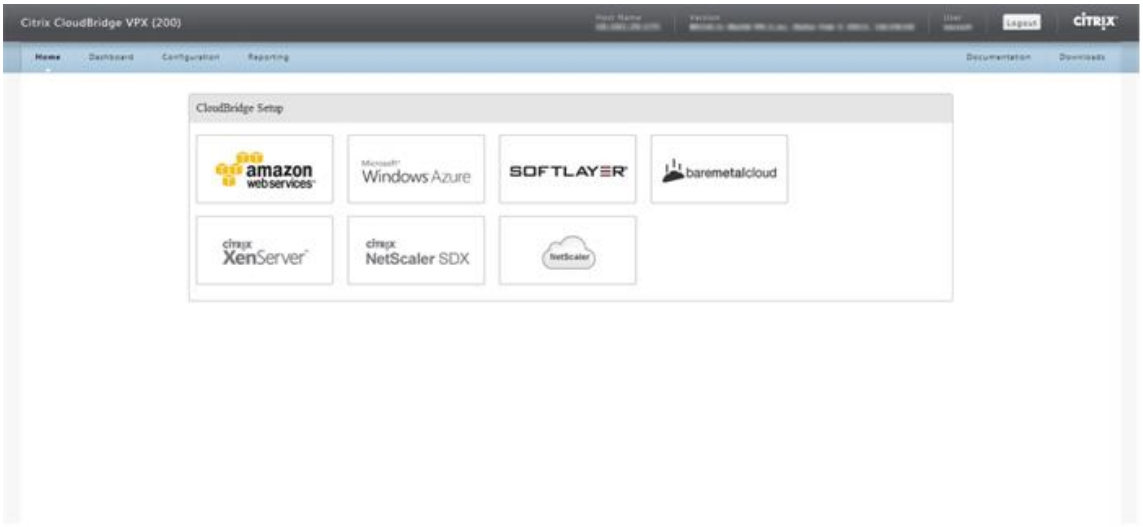
Pour configurer un tunnel CloudBridge Connector dans une appliance NetScaler à l'aide de l'interface graphique

1. Accédez à l'interface graphique à l'aide d'un navigateur Web pour vous connecter à l'adresse IP de l'appliance NetScaler dans le centre de données.
2. Accédez à **Système** > **CloudBridge Connector**.
3. Dans le volet droit, sous **Mise en route**, cliquez sur **Créer/Surveiller CloudBridge**.
4. Cliquez sur **Commencer**.

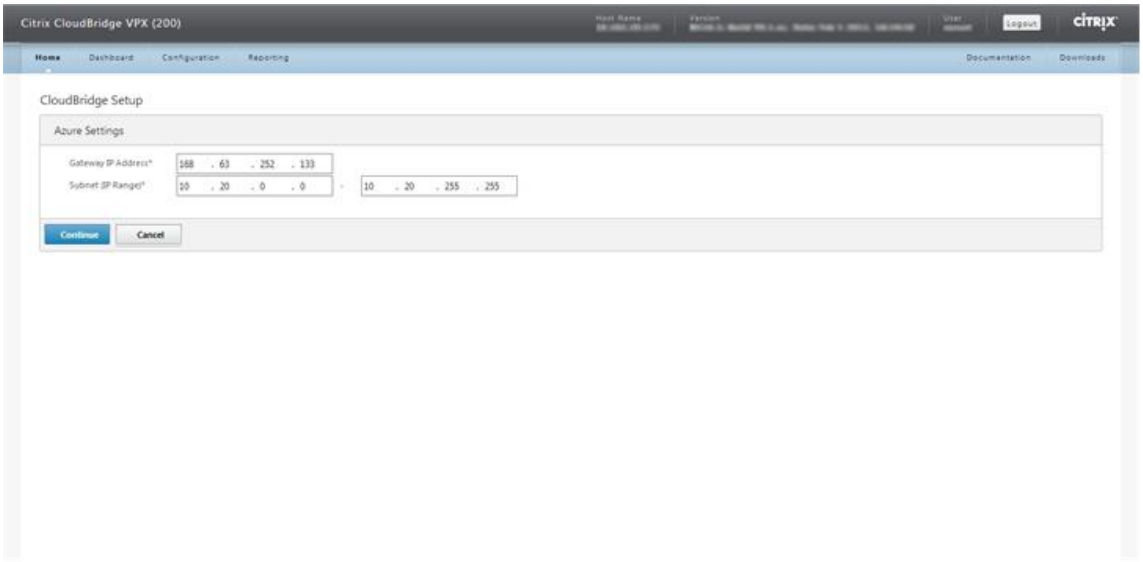


> **Remarque** : Si un tunnel CloudBridge Connector est déjà configuré sur l'appliance NetScaler, cet écran ne s'affiche pas et vous êtes redirigé vers le volet de configuration de CloudBridge Connector.

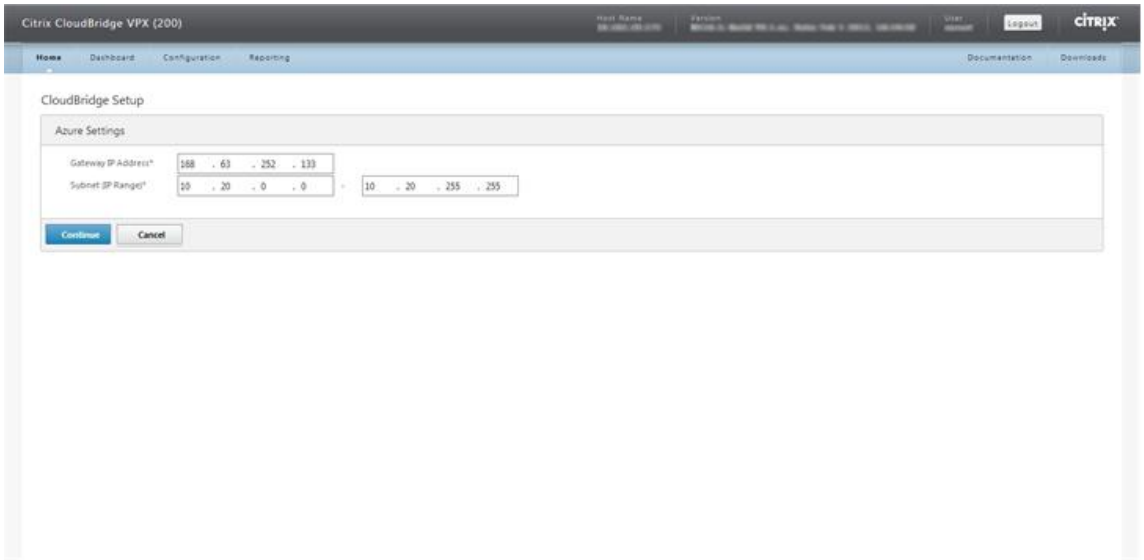
5. Dans le volet Configuration de CloudBridge, cliquez sur **Microsoft Windows Azure**.



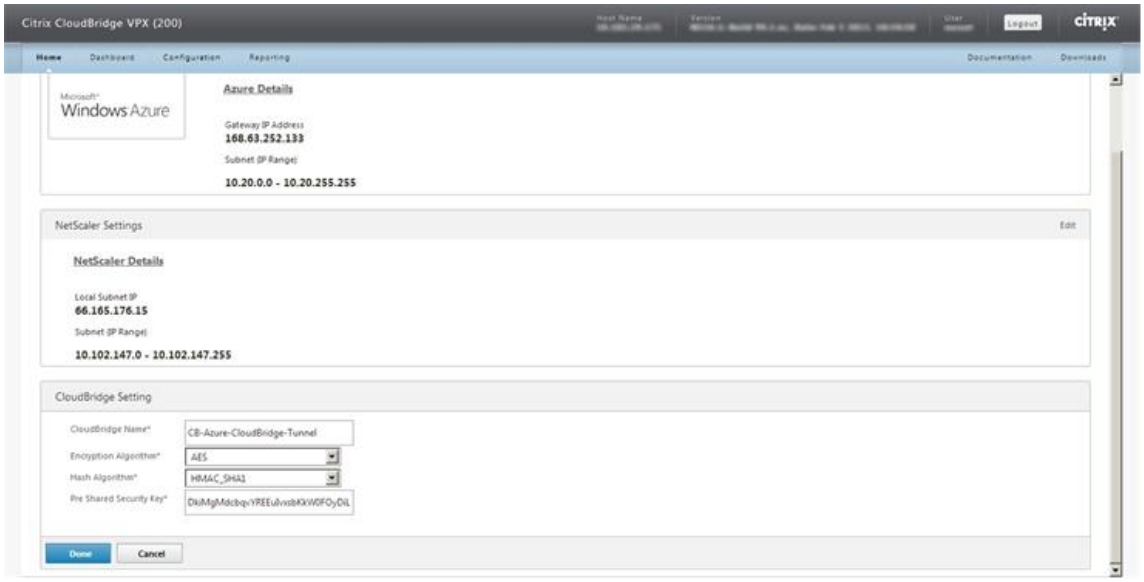
6. Dans le volet Paramètres Azure, dans le champ **Adresse IP de la passerelle**, tapez l'adresse IP de la passerelle Azure. Le tunnel CloudBridge Connector est ensuite configuré entre l'appliance NetScaler et la passerelle. Dans les zones de texte **Sous-réseau (plage d'adresses IP)**, spécifiez une plage de sous-réseaux (dans le cloud Azure) dont le trafic doit traverser le tunnel CloudBridge Connector. Cliquez sur **Continuer**.



7. Dans le volet Paramètres NetScaler, dans la liste déroulante **IP du sous-réseau local**, sélectionnez une adresse SNIP accessible au public configurée sur l'appliance NetScaler. Dans les zones de texte **Sous-réseau (plage d'adresses IP)**, spécifiez une plage de sous-réseaux locaux dont le trafic doit traverser le tunnel CloudBridge Connector. Cliquez sur **Continuer**.



8. Dans le volet **Paramètres de CloudBridge**, dans la zone de texte CloudBridge Name, tapez le nom du CloudBridge que vous souhaitez créer.



9. Dans les listes déroulantes Algorithme de chiffrement et Algorithme de hachage, sélectionnez respectivement les algorithmes AES et HMAC_SHA1. Dans la zone de texte Clé de sécurité pré-partagée, tapez la clé de sécurité.
10. Cliquez sur **Terminé**.

Surveillance du tunnel CloudBridge Connector

Vous pouvez consulter les statistiques permettant de surveiller les performances d'un tunnel CloudBridge Connector entre l'appliance NetScaler du centre de données et Microsoft Azure. Pour consulter les statistiques du tunnel CloudBridge Connector sur l'appliance NetScaler, utilisez l'interface

graphique ou la ligne de commande NetScaler. Pour consulter les statistiques du tunnel CloudBridge Connector dans Microsoft Azure, utilisez le portail de gestion Microsoft Windows Azure.

Affichage des statistiques du tunnel CloudBridge Connector dans l'appliance NetScaler

Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

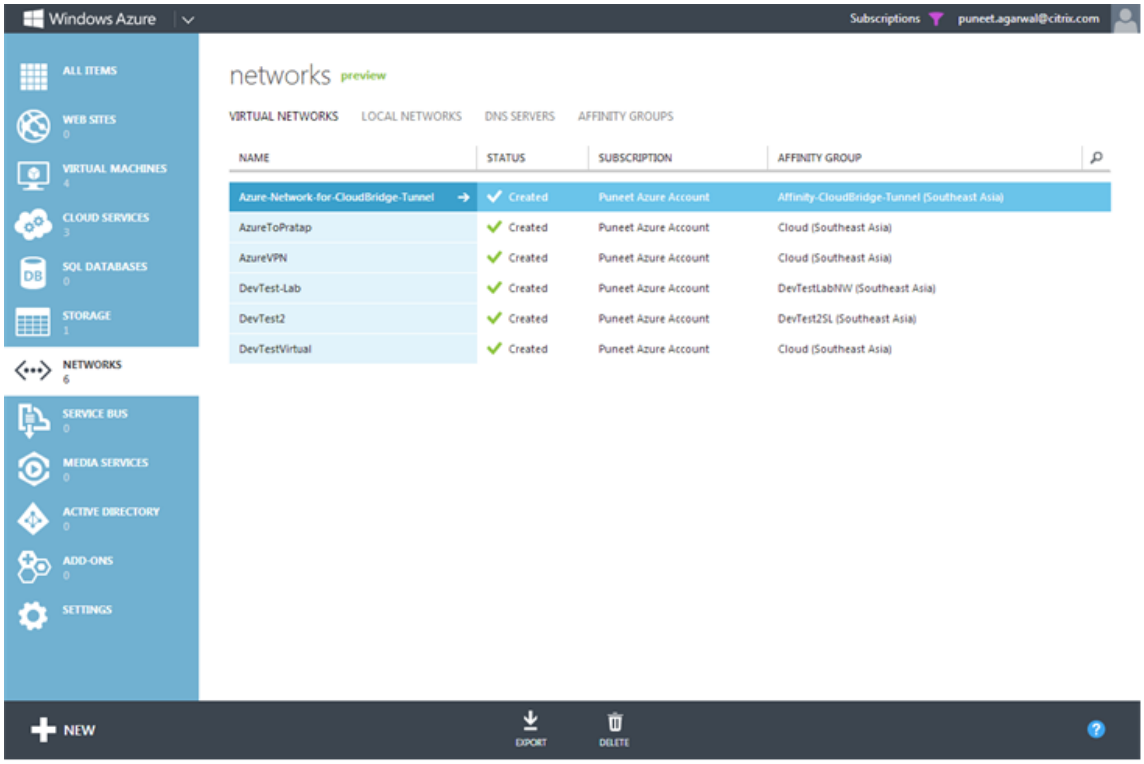
Affichage des statistiques de tunnel CloudBridge Connector dans Microsoft Azure

Le tableau suivant répertorie les compteurs statistiques disponibles pour la surveillance des tunnels CloudBridge Connector dans Microsoft Azure.

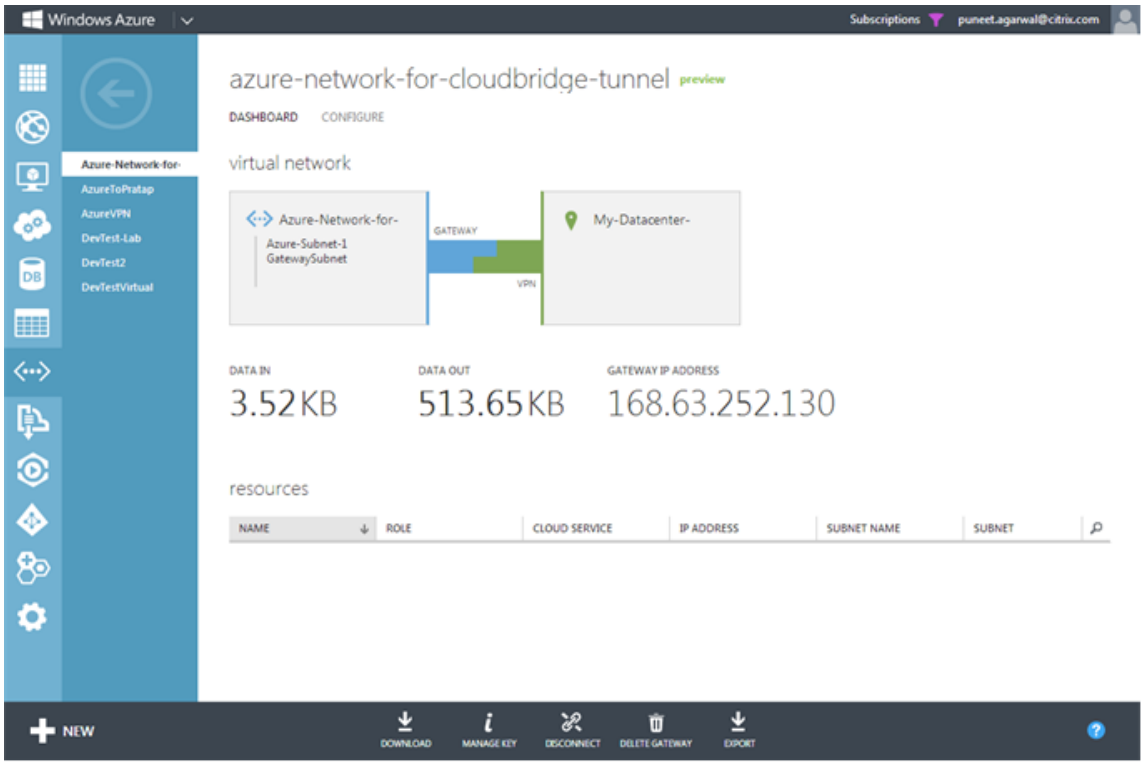
Compteur statistique	Spécifie
DONNÉES DANS	Nombre total de kilo-octets reçus par la passerelle Azure via le tunnel CloudBridge Connector depuis la création de la passerelle.
SORTIE DE DONNÉES	Nombre total de kilo-octets envoyés par la passerelle Azure via le tunnel CloudBridge Connector depuis la création de la passerelle.

Pour afficher les statistiques de tunnel CloudBridge Connector à l'aide du portail de gestion Microsoft Windows Azure

1. Connectez-vous au portail de gestion Windows Azure à l'aide des informations d'identification de votre compte Microsoft Azure.
2. Dans le volet gauche, cliquez sur **RÉSEAUX**.
3. Dans l'onglet **Réseau virtuel**, dans la colonne Nom, sélectionnez l'entité réseau virtuelle associée à un tunnel CloudBridge Connector dont vous souhaitez afficher les statistiques.



4. Sur la page **DASHBOARD** du réseau virtuel, consultez les compteurs d'entrées et de sorties de données pour le tunnel CloudBridge Connector.



Configuration du tunnel CloudBridge Connector entre le centre de données et le cloud d'entreprise Softlayer

May 5, 2023

L'interface graphique inclut un assistant qui vous permet de configurer facilement un tunnel CloudBridge Connector entre une appliance NetScaler dans un centre de données et des instances NetScaler VPX sur le cloud d'entreprise SoftLayer.

Lorsque vous utilisez l'assistant de l'appliance NetScaler dans le centre de données, la configuration du tunnel CloudBridge Connector créée sur l'appliance NetScaler est automatiquement transmise à l'autre point de terminaison ou homologue (le NetScaler VPX sur SoftLayer) du tunnel CloudBridge Connector.

À l'aide de l'assistant de l'appliance NetScaler du centre de données, vous effectuez les étapes suivantes pour configurer un tunnel CloudBridge Connector.

1. Connectez-vous au cloud d'entreprise Softlayer en fournissant les informations d'identification de connexion de l'utilisateur.
2. Sélectionnez le Citrix XenServer qui exécute l'appliance NetScaler VPX.
3. Sélectionnez l'appliance NetScaler VPX.
4. Fournissez les paramètres du tunnel CloudBridge Connector pour :
    - Configurez un tunnel GRE.
    - Configurez IPsec sur le tunnel GRE.
    - Créez un netbridge, qui est une représentation logique du connecteur CloudBridge, en spécifiant un nom.
    - Liez le tunnel GRE au netbridge.

Pour configurer un tunnel CloudBridge Connector à l'aide de l'interface graphique

1. Connectez-vous à l'interface graphique de l'appliance NetScaler dans le centre de données à l'aide des informations d'identification de votre compte pour l'appliance.
2. Accédez à **Système** > **ConnecteurCloudBridge** .
3. Dans le volet droit, sous **Mise en route**, cliquez sur **Créer/Surveiller le CloudBridge**Connector.
4. Cliquez sur **Commencer**.

> **Remarque** :
>
> Si un tunnel CloudBridge Connector est déjà configuré sur l'appliance NetScaler, cet écran ne s'affiche pas et vous êtes redirigé vers le volet de configuration du CloudBridge Connector.

1. Dans le volet Configuration du CloudBridge Connector, cliquez sur Softlayer, puis suivez les instructions de l'assistant.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance NetScaler à l'aide des compteurs statistiques des tunnels CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

Configuration d'un tunnel CloudBridge Connector entre une appliance NetScaler et un périphérique Cisco IOS

May 5, 2023

Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance NetScaler et un appareil Cisco pour connecter deux centres de données ou étendre votre réseau à un fournisseur de cloud. L'appliance NetScaler et le périphérique Cisco IOS constituent les points de terminaison du tunnel CloudBridge Connector et sont appelés homologues.

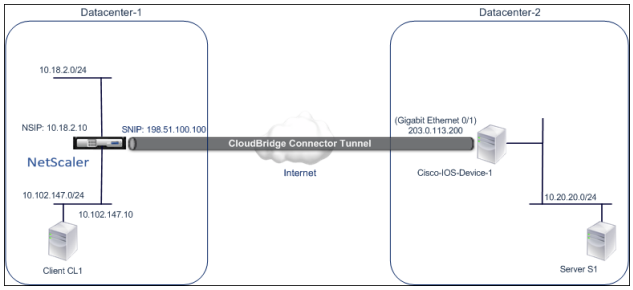
Exemple de configuration du tunnel CloudBridge Connector et de flux de données

Pour illustrer le flux de trafic dans un tunnel CloudBridge Connector, prenons un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les appareils suivants :

- Appliance NetScaler NS_Appliance-1 dans un centre de données désigné Datacenter-1
- Périphérique Cisco IOS Cisco-IOS-Device-1 dans un centre de données désigné Datacenter-2

NS_Appliance-1 et Cisco-IOS-Device-1 permettent la communication entre les réseaux privés du Datacenter-1 et du Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et Cisco-IOS-Device-1 permettent la communication entre le client CL1 dans Datacenter-1 et le serveur S1 dans Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel CloudBridge Connector inclut l'entité de profil IPsec NS_Cisco_IPsec_Profile, l'entité de tunnel du CloudBridge Connector NS_Cisco_Tunnel et l'entité de routage basé sur des politiques (PBR) NS_Cisco_PBR.



Pour plus d'informations, consultez le document PDF sur le tunnel CloudBridge Connector entre une appliance NetScaler et les paramètres du périphérique Cisco IOS .

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector entre une appliance NetScaler et un périphérique Cisco IOS, tenez compte des points suivants :

- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance NetScaler et un périphérique Cisco IOS.

Propriétés IPSec	Paramètre
Mode IPSec	Mode tunnel
Version IKE	Version 1
Groupe IKE DH	DH groupe 2 (algorithme MODP 1024 bits)
Méthode d'authentification IKE	Clé pré-partagée
Algorithme de chiffrement IKE	AES, 3DES
algorithme de hachage IKE	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5
Algorithme de chiffrement ESP	AES, 3DES
Algorithme de hachage ESP	HMAC SHA1, HMAC SHA256, HMAC SHA256, HMAC SHA256, HMAC MD5

- Vous devez spécifier les mêmes paramètres IPsec sur l'appliance NetScaler et sur le périphérique Cisco IOS aux deux extrémités du CloudBridge Connector.
- NetScaler fournit un paramètre commun (dans les profils IPsec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun permettant de spécifier un algorithme de chiffrement IKE et un algorithme de cryptage ESP. Par conséquent, sur le périphérique Cisco, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement pour IKE (lors de la création de la politique IKE) et ESP (lors

de la création d'un ensemble de transformations IPsec).

- Vous devez configurer le pare-feu côté NetScaler et côté périphérique Cisco pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)

Configuration du périphérique Cisco IOS pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector sur un périphérique Cisco IOS, utilisez l'interface de ligne de commande Cisco IOS, qui est l'interface utilisateur principale pour la configuration, la surveillance et la maintenance des périphériques Cisco.

Avant de commencer la configuration du tunnel CloudBridge Connector sur un périphérique Cisco IOS, assurez-vous que :

- Vous avez un compte utilisateur avec des informations d'identification d'administrateur sur le périphérique Cisco IOS.
- Vous connaissez l'interface de ligne de commande de Cisco IOS.
- Le périphérique Cisco IOS est opérationnel, est connecté à Internet et est également connecté aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.

> **Remarque** :
>
> Les procédures de configuration du tunnel CloudBridge Connector sur un périphérique Cisco IOS peuvent changer au fil du temps, en fonction du cycle de publication de Cisco. Citrix vous recommande de suivre la documentation officielle du produit Cisco pour plus d'informations, voir la rubrique Configuration des tunnels VPN IPSec .

Pour configurer un tunnel de connecteur CloudBridge entre une appliance NetScaler et un appareil Cisco IOS, effectuez les tâches suivantes sur la ligne de commande IOS du périphérique Cisco :

- Créez une stratégie IKE.
- Configurez une clé pré-partagée pour l'authentification IKE.
- Définissez un jeu de transformations et configurez IPsec en mode tunnel.
- Créer une liste d'accès crypto
- Créer une carte crypto
- Appliquer la carte crypto à une interface

Les exemples des procédures suivantes créent des paramètres `Cisco IOS device Cisco-IOS-Device-1` mentionnés dans la section « Exemple de configuration et de flux de données CloudBridge Connector. «

Pour créer une stratégie IKE, reportez-vous au pdf de la stratégie IKE .

Pour configurer une clé pré-partagée à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez les commandes suivantes, en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
adresse d'identité cryptographique isakmp	Cisco-IOS-Device-1 (config) # adresse d'identité cryptographique isakmp	Spécifiez l'identité ISAKMP (adresse) que le périphérique Cisco IOS doit utiliser lors de la communication avec l'homologue (appliance NetScaler) lors des négociations IKE. Cet exemple spécifie le mot clé d'adresse, qui utilise l'adresse IP 203.0.113.200 (interface Gigabit Ethernet 0/1 de Cisco-IOS-device-1) comme identité du périphérique.
adresse de chaîne de clés crypto isakmp	Cisco-IOS-DEVICE-1 (config) # crypto est un exemple de clé kmp adresse de clé pré-partagée 198.51.100.100	Spécifiez une clé pré-partagée pour l'authentification IKE. Cet exemple configure la clé partagée examplepresharedkey à utiliser avec l'appliance NetScaler NS_Appliance-1 (198.51.100.100). La même clé pré-partagée doit être configurée sur l'appliance NetScaler pour que l'authentification IKE soit réussie entre le périphérique Cisco IOS et l'appliance NetScaler.

Pour créer une liste d'accès crypto à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez la commande suivante en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
liste d'accès numéro de liste d'accès autoriser l'adresse IP source source, caractère générique, destination, caractère générique	Cisco-IOS-Device-1 (config) # access-list 111 autorise l'adresse IP 10.20.20.0 0.0.255 10.102.147.0 0.0.0.255	Spécifiez les conditions permettant de déterminer les sous-réseaux dont le trafic IP doit être protégé via le tunnel CloudBridge Connector. Cet exemple montre comment configurer la liste d'accès 111 pour protéger le trafic des sous-réseaux 10.20.20.0/24 (côté CISCO-IOS-Device-1) et 10.102.147.0/24 (côté NS_Appliance-1).

Pour définir une transformation et configurer le mode tunnel IPsec à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez les commandes suivantes, en commençant en mode de configuration globale, dans l'ordre indiqué :
Commande	Exemple	Description de la commande
–	–	–
crypto ipsec transform-setname ESP_Authentication_Transform ESP_Encryption_Transform Note : ESP_Authentication_Transform peut prendre les valeurs suivantes : esp-sha-hmac, esp-sha256-hmac, esp-sha384-hmac, esp-sha512-hmac, esp-md5-hmac. ESP_Encryption_Transform peut prendre les valeurs suivantes : esp-aes ou esp-3des	Cisco-ios-device-1(config)# crypto ipsec transform-set NS-CISCO-TS esp-sha256-hmac esp-3des	Définissez un ensemble de transformations et spécifiez l'algorithme de hachage ESP (pour l'authentification) et l'algorithme de chiffrement ESP à utiliser lors de l'échange de données entre les homologues du tunnel CloudBridge Connector. Cet exemple définit le jeu de transformations NS-CISCO-TS et spécifie l'algorithme d'authentification ESP comme esp-sha256-hmac, et l'algorithme de chiffrement ESP comme esp-3des.
tunnel de mode	Tunnel en mode # Cisco IOS Device-1 (config-crypto-trans)	Définissez IPSec en mode tunnel.
exit	Dispositif Cisco IOS 1 (config-crypto-trans) # sortie, Cisco IOS Device-1 (config) #	Quittez en mode de configuration global.

Pour créer une carte cryptographique à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez les commandes suivantes en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
—	–	–
nom de carte cryptographique seq-num ipsec-isakmp	Cisco-IOS-Device-1 (config) # carte cryptographique NS-CISCO-CM 2 ipsec-isakmp	Entrez en mode de configuration de la carte cryptographique, spécifiez un numéro de séquence pour la carte cryptographique et configurez la carte cryptographique pour utiliser IKE afin d'établir des associations de sécurité (SA). Cet exemple configure le numéro de séquence 2 et l'IKE pour la carte cryptographique NS-CISCO-CM.
définir l'adresse IP du pair	Cisco-IOS-Device-1 (config-cryptomap) # set peer 172.23.2.7	Spécifiez l'homologue (appliance NetScaler) par son adresse IP. Cet exemple indique 198.51.100.100, qui est l'adresse IP du point de terminaison CloudBridge Connector sur l'appliance NetScaler.
faire correspondre l'adresse access-list-id	Cisco-IOS-device-1 (config-crypto-map) # correspond à l'adresse 111	Spécifiez une liste d'accès étendue. Cette liste d'accès spécifie les conditions permettant de déterminer les sous-réseaux dont le trafic IP doit être protégé via le tunnel CloudBridge Connector. Cet exemple spécifie la liste d'accès 111.
set transform-set transform-set-name	Cisco-IOS-Device-1 (config-cryptomap) # set transform-set NS-CISCO-TS	Spécifiez les ensembles de transformations autorisés pour cette entrée de carte cryptographique. Cet exemple spécifie le jeu de transformations NS-CISCO-TS.
exit	Cisco-ios-device-1 (config-crypto-map)# exit
Cisco-ios-device-1 (config)#	Exit back to global configuration mode.

Pour appliquer une carte de chiffrement à une interface à l'aide de la ligne de commande Cisco IOS :

À l'invite de commandes du périphérique Cisco IOS, tapez les commandes suivantes en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
InterfaceID d'interface	Cisco-iOS-device-1 (config) # interface Gigabit Ethernet 0/1	Spécifiez une interface physique à laquelle appliquer la carte cryptographique et entrez en mode de configuration de l'interface. Cet exemple spécifie l'interface Gigabit Ethernet 0/1 du périphérique Cisco Cisco-IOS-Device-1. L'adresse IP 203.0.113.200 est déjà définie sur cette interface.
nom de la carte cryptographique	Cisco-IOS-device-1 (config-if) # carte cryptographique NS-CISCO-CM	Appliquez la carte cryptographique à l'interface physique. Cet exemple applique la carte cryptographique NS-CISCO-CM.
exit	Cisco-IOS-Device-1 (config-if) # exit, Cisco-IOS-Device-1 (config) #	Quittez en mode de configuration global.

Configuration de l'appliance NetScaler pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance NetScaler et un périphérique Cisco IOS, effectuez les tâches suivantes sur l'appliance NetScaler. Vous pouvez utiliser la ligne de commande NetScaler ou l'interface utilisateur graphique (GUI) de NetScaler :

- Créez un profil IPsec.
- Créez un tunnel IP qui utilise le protocole IPSec et associez le profil IPSec à celui-ci.
- Créez une règle PBR et associez-la au tunnel IP.

Pour créer un profil IPSEC à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1`
- `show ipsec profile <name>`

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `add ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbrs <pbrName>`

Les commandes suivantes créent les paramètres `NetScaler appliance NS_Appliance-1` mentionnés dans la section **Exemple de configuration et de flux de données CloudBridge Connector**.

```
1      > add ipsec profile NS_Cisco_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 - lifetime 315360 - encAlgo 3
          DES
2      Done
3      > add iptunnel NS_Cisco_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 - protocol IPSEC - ipsecProfileName
          NS_Cisco_IPSec_Profile
4
5      Done
6      > add pbr NS_Cisco_Pbr -srcIP 10.102.147.0-10.102.147.255 - destIP
          10.20.0.0-10.20.255.255 - ipTunnel NS_Cisco_Tunnel
7
8      Done
9      > apply pbrs
10
11     Done
12 <!--NeedCopy-->
```

Pour créer un profil IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **CloudBridge Connector** > Profil **IPsec**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un profil IPsec**, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE
4. Configurez la méthode **d'authentification IPSec** à utiliser par les deux homologues du tunnel CloudBridge Connector pour s'authentifier mutuellement : Sélectionnez la méthode

d'authentification par clé pré-partagée et définissez le paramètre **Pre-Shared Key Exists** .

5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un tunnel IP**, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque à distance
   - Type d'adresse IP locale (Dans la liste déroulante Type d'adresse IP locale, sélectionnez Adresse IP du sous-réseau).
   - Adresse IP locale (Toutes les adresses IP configurées du type d'adresse IP sélectionné figurent dans la liste déroulante des adresses IP locales. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPSec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un PBR**, définissez les paramètres suivants :
   - Nom
   - Action
   - Type de saut suivant (sélectionnez le tunnel IP)
   - Nom du tunnel IP
   - IP de la source : faible
   - IP de la source : élevée
   - IP de destination faible
   - IP de destination : élevée
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour appliquer un PBR à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **PBR.**
2. **Dans l'onglet**PBR**, sélectionnez le**PBR**, dans la**liste Actions**, sélectionnez Appliquer.**

La nouvelle configuration du tunnel CloudBridge Connector correspondante sur l'appliance NetScaler apparaît dans l'interface graphique. L'état actuel du tunnel du connecteur CloudBridge est affiché dans le volet Configuré du CloudBridge Connector. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance NetScaler à l'aide des compteurs statistiques des tunnels CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

Configuration d'un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance Fortinet FortiGate

May 5, 2023

Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance Fortinet FortiGate pour connecter deux centres de données ou étendre votre réseau à un fournisseur de cloud. L'appliance NetScaler et l'appliance FortiGate constituent les points de terminaison du tunnel CloudBridge Connector et sont appelées homologues.

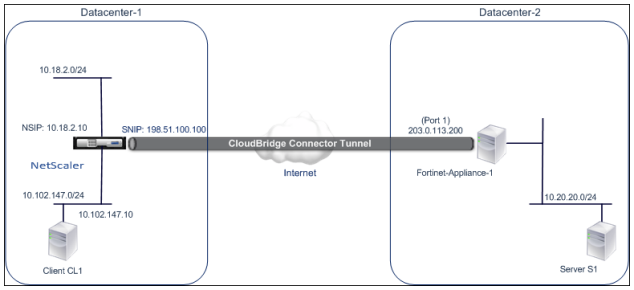
Exemple de configuration d'un tunnel CloudBridge Connector

Pour illustrer le flux de trafic dans un tunnel CloudBridge Connector, prenons un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les appareils suivants :

- Appliance NetScaler NS_Appliance-1 dans un centre de données désigné Datacenter-1
- Appliance FortiGate FortiGate-Appliance-1 dans un centre de données désigné Datacenter-2

NS_Appliance-1 et FortiGate-Appliance-1 permettent la communication entre les réseaux privés du Datacenter-1 et du Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et FortiGate-Appliance-1 permettent la communication entre le client CL1 dans le Datacenter-1 et le serveur S1 dans le Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel CloudBridge Connector inclut l'entité de profil IPsec NS_Fortinet_IPsec_Profile, l'entité de tunnel du CloudBridge Connector NS_Fortinet_Tunnel et l'entité de routage basé sur des politiques (PBR) NS_Fortinet_PBR.



Pour plus d'informations, consultez le tableau de configuration du tunnel CloudBridge Connector pdf.

Pour plus d'informations sur les paramètres de Fortinet Fortigate-Appliance-1 dans Datacenter-2, voir le tableau.

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance FortiGate, tenez compte des points suivants :

- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance FortiGate.

Propriétés IPSec	Paramètres
Mode IPSec	Mode tunnel
Version IKE	Version 1
Groupe IKE DH	DH groupe 2 (algorithme MODP 1024 bits)
Méthode d'authentification IKE	Clé pré-partagée
Algorithme de chiffrement IKE	AES
algorithme de hachage IKE	HMAC SHA1
Algorithme de chiffrement ESP	AES
Algorithme de hachage ESP	HMAC SHA1

- Vous devez spécifier les mêmes paramètres IPsec sur l'appliance NetScaler et sur l'appliance FortiGate aux deux extrémités du CloudBridge Connector.
- NetScaler fournit un paramètre commun (dans les profils IPsec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun pour spécifier un algorithme de chiffrement IKE et un algorithme de cryptage ESP. Par conséquent, dans l'appliance FortiGate, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement dans IKE (configuration de phase 1) et ESP (configuration de phase 2).
- Vous devez configurer le pare-feu côté NetScaler et côté FortiGate pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)
- L'appliance FortiGate prend en charge deux types de tunnels VPN : basés sur des règles et basés

sur des itinéraires. Seul le tunnel VPN basé sur des règles est pris en charge entre une appliance FortiGate et une appliance NetScaler.

Configuration de l'appliance FortiGate pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector sur une appliance FortiGate, utilisez le gestionnaire Web Fortinet, qui est la principale interface utilisateur pour la configuration, la surveillance et la maintenance des appliances FortiGate.

Avant de commencer la configuration du tunnel CloudBridge Connector sur une appliance FortiGate, assurez-vous que :

- Vous disposez d'un compte utilisateur avec des informations d'identification d'administrateur sur l'appliance FortiGate.
- Vous connaissez le gestionnaire Web de Fortinet.
- L'appliance FortiGate est opérationnelle, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.

> **Remarque**
>
> Les procédures de configuration du tunnel CloudBridge Connector sur une appliance FortiGate peuvent changer au fil du temps, en fonction du cycle de publication de Fortinet. Citrix vous recommande de suivre la documentation officielle du produit Fortinet concernant la configuration des tunnels VPN IPSec.

Pour configurer un tunnel de connecteur CloudBridge entre une appliance NetScaler et une appliance FortiGate, effectuez les tâches suivantes sur l'appliance FortiGate à l'aide du gestionnaire Web Fortinet :

- **Activez la fonctionnalité VPN IPsec basée sur**des règles. Activez cette fonctionnalité pour créer des tunnels VPN basés sur des règles sur l'appliance FortiGate. Seul le type de tunnel VPN basé sur des règles est pris en charge entre une appliance FortiGate et une appliance NetScaler. Une configuration de tunnel VPN basée sur des règles sur une appliance FortiGate inclut des paramètres de phase 1, des paramètres de phase 2 et une politique de sécurité IPsec.
- **Définissez les paramètres de la phase 1.** Les paramètres de phase 1 sont utilisés par l'appliance FortiGate pour l'authentification IKE avant de créer un tunnel sécurisé vers l'appliance NetScaler.
- **Définissez les paramètres de la phase 2**. Les paramètres de phase 2 sont utilisés par l'appliance FortiGate pour créer un tunnel sécurisé vers l'appliance NetScaler en établissant des associations de sécurité IKE (SA).
- **Spécifiez des sous-réseaux privés**. Définissez les sous-réseaux privés côté FortiGate et côté NetScaler dont le trafic IP doit être transporté via le tunnel.
- **Définissez une politique de sécurité IPsec pour le tunnel**. Une politique de sécurité permet au trafic IP de passer d'une interface à l'autre sur une appliance FortiGate. Une politique de

sécurité IPsec spécifie l'interface vers le sous-réseau privé et l'interface connectant l'appliance NetScaler via le tunnel.

Pour activer la fonctionnalité VPN IPsec basée sur des règles à l'aide du gestionnaire Web Fortinet

1. Accédez à **Système** > **Configuration** > **Fonctionnalités**.
2. Sur la page **Paramètres des fonctionnalités**, sélectionnez **Afficher plus** et activez le VPN **IPsec basé sur des règles**.

Pour définir les paramètres de la phase 1 à l'aide du gestionnaire Web de Fortinet

1. Accédez à **VPN** > **IPsec** > **Auto Key (IKE)** et cliquez sur **Create Phase1**.
2. Sur la page **Nouvelle phase 1**, définissez les paramètres suivants :
   - Nom : Entrez un nom pour cette configuration de phase 1.
   - Passerelle distante : sélectionnez *une adresse IP statique.*
   - Mode : sélectionnez *Principal (Protection de l'identification)*.
   - Méthode d'authentification : sélectionnez la *clé prépartagée.*
   - Clé pré-partagée : entrez une clé pré-partagée. La même clé pré-partagée doit être configurée sur l'appliance NetScaler.
   - Options homologues : définissez les paramètres IKE suivants pour authentifier une appliance NetScaler.
     - Version IKE : Sélectionnez *1*.
     - Configuration du mode : désactivez cette option si elle est sélectionnée.
     - IP de la passerelle locale : sélectionnez l'adresse *IP de l'interface principale*.
     - Proposition P1 : Sélectionnez les algorithmes de chiffrement et d'authentification pour l'authentification IKE avant de créer un tunnel sécurisé vers l'appliance NetScaler.
       * 1 - Chiffrement : sélectionnez *AES128*.
       * Authentification : sélectionnez *SHA1*.
       * Durée de vie de la clé : entrez la durée (en secondes) de la durée de vie de la clé de la phase 1.
       * Groupe DH : Sélectionnez 2.
     - *X-Auth : sélectionnez Désactiver.*
     - Deed Peer Detection : sélectionnez cette option.
3. Cliquez sur **OK**.

Pour spécifier des sous-réseaux privés à l'aide du gestionnaire Web de Fortinet

1. Accédez à **Objets du pare-feu** > **Adresse** > **Adresses** et sélectionnez **Créer un nouveau**.
2. Sur la page **Nouvelle adresse**, définissez les paramètres suivants :
   - Nom : entrez un nom pour le sous-réseau côté FortiGate.
   - Type : Sélectionnez *Sous-réseau*.
   - Sous-réseau/Plage d'adresses IP : entrez l'adresse du sous-réseau côté FortiGate.
   - Interface : sélectionnez l'interface locale pour ce sous-réseau.

3. Cliquez sur **OK**.
4. Répétez les étapes 1 à 3 pour spécifier le sous-réseau côté NetScaler.

Pour définir les paramètres de la phase 2 à l'aide du gestionnaire Web de Fortinet

1. Accédez à **VPN** > **IPsec** > **Auto Key (IKE)** et cliquez sur **Create Phase 2.**
2. Sur la page **Nouvelle phase 2**, définissez les paramètres suivants :
   - Nom : Entrez un nom pour cette configuration de phase 2.
   - Phase 1 : Sélectionnez la configuration de la phase 1 dans la liste déroulante.
3. Cliquez sur **Avancé** et définissez les paramètres suivants :
   - Proposition P2 : Sélectionnez les algorithmes de cryptage et d'authentification pour créer un tunnel sécurisé vers l'appliance NetScaler.
     - 1 - Chiffrement : sélectionnez *AES128*.
     - Authentification : sélectionnez *SHA1*.
     - Activer la détection des rediffusions : sélectionnez cette option.
     - Activer le secret de transmission parfait (PFS) : sélectionnez cette option.
     - Groupe DH : Sélectionnez *2*.
   - Durée de vie de la clé : entrez la durée (en secondes) de la durée de vie de la clé de la phase 2.
   - Autokey Keep Alive : sélectionnez cette option.
   - Négociation automatique : sélectionnez cette option.
   - Sélecteur de mode rapide : Spécifiez les sous-réseaux privés côté FortiGate et côté NetScaler dont le trafic doit être traversé par le tunnel.
     - Adresse source : sélectionnez le sous-réseau côté FortiGate dans la liste déroulante.
     - Port source : Entrez *0*.
     - Adresse de destination : sélectionnez le sous-réseau côté NetScaler dans la liste déroulante.
     - Port de destination : entrez *0*.
     - Protocole : Entrez *0*.
4. Cliquez sur **OK**.

Pour définir une politique de sécurité IPsec à l'aide du gestionnaire Web de Fortinet

1. **Accédez à **Politique** > Stratégie > Stratégie et cliquez sur **Créer une nouvelle**.**
2. Sur la page **Modifier la politique**, définissez les paramètres suivants :
   - Type de politique : sélectionnez *VPN*.
   - Sous-type de stratégie : sélectionnez *IPsec*.
   - Interface locale : sélectionnez l'interface locale vers le réseau interne (privé).
   - Sous-réseau local protégé : sélectionnez le sous-réseau côté FortiGate dans la liste déroulante dont le trafic doit passer par le tunnel.
   - Interface VPN sortante : sélectionnez l'interface locale vers le réseau externe (public).
   - Sous-réseau protégé à distance : sélectionnez le sous-réseau côté NetScaler dans la liste

déroulante dont le trafic doit passer par le tunnel.
- Planification : conservez le paramètre par défaut (*toujours*) à moins que des modifications ne soient nécessaires pour répondre à des exigences spécifiques.
- Service : conservez le paramètre par défaut (*TOUS*) sauf si des modifications sont nécessaires pour répondre à vos besoins spécifiques.
- Tunnel VPN : sélectionnez *Utiliser l'existant* et sélectionnez le tunnel dans la liste déroulante.
- Autoriser le trafic à partir du site distant : sélectionnez si le trafic provenant du réseau distant sera autorisé à démarrer le tunnel.

3. Cliquez sur **OK**.

Configuration de l'appliance NetScaler pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance FortiGate, effectuez les tâches suivantes sur l'appliance NetScaler. Vous pouvez utiliser la ligne de commande NetScaler ou l'interface utilisateur graphique (GUI) de NetScaler :

- **Créez un profil IPsec**. Une entité de profil IPsec spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et la méthode d'authentification à utiliser par le protocole IPsec dans le tunnel CloudBridge Connector.
- **Créez un tunnel IP qui utilise le protocole IPsec et associez-y le profil IPsec**. Un tunnel IP spécifie l'adresse IP locale (adresse IP du point de terminaison du tunnel CloudBridge Connector (de type SNIP) configurée sur l'appliance NetScaler), l'adresse IP distante (adresse IP du point de terminaison du tunnel CloudBridge Connector configurée sur l'appliance FortiGate), le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.
- **Créez une règle PBR et associez-la au tunnel IP**. Une entité PBR spécifie un ensemble de règles et une entité de tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Définissez la plage d'adresses IP source pour spécifier le sous-réseau côté NetScaler dont le trafic doit être protégé via le tunnel, et définissez la plage d'adresses IP de destination pour spécifier le sous-réseau côté appliance FortiGate dont le trafic doit être protégé via le tunnel.

Pour créer un profil IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName** <string>`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Pour créer un profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > Profil **IPsec**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil IPsec**, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE
   - Perfect Forward Secrecy (Activer ce paramètre)
4. Configurez la méthode d'authentification IPSec à utiliser par les deux homologues du tunnel CloudBridge Connector pour s'authentifier mutuellement : Sélectionnez la méthode d'authentification par clé pré-partagée et définissez le paramètre Pre-Shared Key Exists .
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un tunnel IP**, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque à distance
   - Type d'adresse IP locale (Dans la liste déroulante Type d'adresse IP locale, sélectionnez *Adresse IP du sous-réseau*).
   - IP locale (Toutes les adresses IP configurées du type IP sélectionné figurent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPSec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la page **Créer un PBR**, définissez les paramètres suivants :
   - Nom
   - Action
   - Type de saut suivant (sélectionnez le *tunnel IP*)
   - Nom du tunnel IP
   - IP de la source : faible
   - IP de la source : élevée
   - IP de destination faible
   - IP de destination : élevée
4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration du tunnel CloudBridge Connector correspondante sur l'appliance NetScaler apparaît dans l'interface graphique.

L'état actuel du tunnel du connecteur CloudBridge est affiché dans le volet Configuré du CloudBridge Connector. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Les commandes suivantes créent les paramètres de l'appliance NetScaler NS_Appliance-1 dans « Exemple de configuration d'un CloudBridge Connector ». «

```
1      >  add ipsec profile NS_Fortinet_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 -encAlgo AES -hashalgo
          HMAC_SHA1 -lifetime 315360 -perfectForwardSecrecy ENABLE
2
3       Done
4      >  add iptunnel NS_Fortinet_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 -protocol IPSEC -ipsecProfileName
          NS_Fortinet_IPSec_Profile
5
6       Done
7      > add pbr NS_Fortinet_Pbr -srcIP 10.102.147.0-10.102.147.255 -
          destIP 10.20.0.0-10.20.255.255 -ipTunnel NS_Fortinet_Tunnel
8
9       Done
10     > apply pbrs
11
12      Done
13 <!--NeedCopy-->
```


Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance NetScaler à l'aide des compteurs statistiques des tunnels CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

Diagnostic et résolution des problèmes liés au tunnel CloudBridge Connector

May 5, 2023

Si vous rencontrez des problèmes avec la configuration d'un tunnel CloudBridge Connector, assurez-vous que tous les prérequis ont été respectés avant la configuration du tunnel. Si tel était le cas, le problème pourrait être lié aux adresses IP du point de terminaison du tunnel, à une configuration NAT, à la façon dont le tunnel a été configuré ou au trafic de données.

Résolution des problèmes liés à un tunnel CloudBridge Connector

Si votre tunnel CloudBridge Connector ne fonctionne pas correctement, le problème peut être lié à l'établissement du tunnel ou au trafic de données. Si vous ne savez pas quel type de problème vous rencontrez, recherchez un message d'erreur dans le fichier journal et vérifiez si le message d'erreur figure dans la liste des problèmes liés à l'établissement du tunnel. Si vous ne trouvez pas votre message d'erreur, consultez la liste des problèmes éventuels liés au trafic de données.

Problèmes liés à la création d'un tunnel

Une fois que les conditions requises pour la configuration du tunnel IPsec sont satisfaites et que le tunnel CloudBridge Connector est configuré, si l'état du tunnel n'est pas UP, recherchez les informations de débogage dans le fichier iked.log sur l'une ou les deux appliances NetScaler configurées comme points de terminaison du tunnel.

Sur l'une ou l'autre des appliances, tapez la commande suivante à l'invite du shell NetScaler :

```
cat /tmp/iked.debug | tee /var/iked.log
```

Le fichier PDF de dépannage répertorie certaines erreurs courantes et leurs solutions.

Problèmes liés au trafic de données

Si les données du tunnel CloudBridge Connector ne sont pas échangées correctement entre les points de terminaison du tunnel, procédez comme suit.

- Pour un tunnel CloudBridge Connector qui utilise les protocoles GRE et IPsec :
  - Assurez-vous que le mode L2 est activé sur les deux points de terminaison du tunnel CloudBridge Connector. Pour activer le mode L2, tapez la commande suivante sur l'interface de ligne de commande NetScaler :

    ```
    enable mode L2
    ```

    * Si l'un des points de terminaison du tunnel CloudBridge Connector est une appliance virtuelle CloudBridge (VPX) approvisionnée sur un hyperviseur VMware ESXi, assurez-vous que le mode Promiscuous est défini sur Accept pour le vSwitch associé à l'appliance CloudBridge VPX.
  - Si un VLAN est étendu via un tunnel CloudBridge Connector, vérifiez le mappage biunivoque sur l'entité VLAN étendue à chacune des extrémités du tunnel
  - Assurez-vous que l'entité du tunnel IP est liée à l'entité netbridge appropriée à chacun des points de terminaison du tunnel.
  - Vérifiez que l'entrée ARP du point de terminaison du tunnel CloudBridge Connector homologue existe sur le point de terminaison du tunnel local, en saisissant la commande suivante sur l'interface de ligne de commande NetScaler :

    ```
    show arp
    ```
  - Si la sortie indique une entrée ARP incomplète, le trafic bidirectionnel ne traverse pas le tunnel. Si le trafic circule dans les deux sens, l'entrée ARP indique le nom de l'interface du tunnel pour les appareils situés de l'autre côté du tunnel.
  - Supprimez les entités du tunnel IP des deux points de terminaison du tunnel et ajoutez-les à nouveau avec les mêmes paramètres, mais avec le profil IPsec défini sur NONE, afin que le tunnel utilise uniquement le protocole GRE.

    Après avoir vérifié les points suivants dans le tunnel IP (qui utilise le protocole GRE), configurez le tunnel avec des paramètres IPsec en spécifiant un profil IPsec valide pour les entités du tunnel IP respectives sur chacune des extrémités du tunnel.

    Flux PING ou TCP correct dans le tunnel.

    Flux correct du trafic de données dans le tunnel.

    Une fois que le tunnel configuré (qui utilise les protocoles GRE et IPsec) est à l'état UP, si le trafic de données ne circule pas correctement dans le tunnel et si un périphérique NAT a été déployé devant l'un des points de terminaison du tunnel ou les deux, analysez les paquets d'entrée et de sortie sur les périphériques NAT.
- Si une appliance NetScaler est utilisée comme routeur ou passerelle.
  - Assurez-vous que le mode L3 est activé sur l'appliance NetScaler. Pour activer le mode L3, exécutez la commande suivante dans la ligne de commande CloudBridge.
  - activer le mode L3
  - Si les sous-réseaux sont liés à une entité Netbridge, assurez-vous que l'entité de tunnel IP correcte est également liée à l'entité Netbridge.
  - Exécutez la commande suivante dans la ligne de commande NetScaler pour voir où les

paquets (entrée et sortie) sont supprimés :

```
stat ipsec counters
```

- Assurez-vous que les itinéraires appropriés sont configurés aux deux extrémités du tunnel.
- Si aucun périphérique NAT n'est déployé devant l'appliance NetScaler, assurez-vous que les pare-feux sont configurés pour autoriser tous les paquets ESP (protocole IP numéro 50) et tous les paquets UDP pour le port 4500.

Si aucune des mesures ci-dessus n'aboutit à un échange de trafic réussi entre les points de terminaison du tunnel, contactez le support technique de Citrix.

Liste de contrôle avant de contacter le support technique Citrix

Pour une résolution rapide, assurez-vous que les éléments suivants sont prêts avant de contacter le support technique de Citrix.

- Détails du déploiement et de la topologie du réseau.
- Fichier journal collecté en saisissant la commande suivante à l'invite du shell NetScaler.

  ```
  cat /tmp/iked.debug | tee /var/log/iked.log
  ```

- Bundle de support technique capturé en saisissant la commande suivante sur la ligne de commande NetScaler.

  ```
  show techsupport
  ```

- Traces de paquets capturées sur les deux points de terminaison du tunnel CloudBridge Connector. Pour démarrer un suivi de paquets, tapez la commande suivante sur la ligne de commande NetScaler.

  ```
  start nstrace -size 0
  ```

  Pour arrêter le suivi des paquets, tapez la commande suivante sur la ligne de commande NetScaler.

  ```
  stop nstrace
  ```

- Résultat de la commande suivante saisie à l'invite de commande NetScaler.

  ```
  show arp
  ```

Interopérabilité du CloudBridge Connector — StrongSwan

May 5, 2023

StrongSwan est une implémentation IPsec open source pour les plateformes Linux. Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance StrongSwan pour connecter deux centres de données ou étendre votre réseau à un fournisseur de

cloud. L'appliance NetScaler et l'appliance StrongSwan constituent les points de terminaison du tunnel CloudBridge Connector et sont appelées homologues.

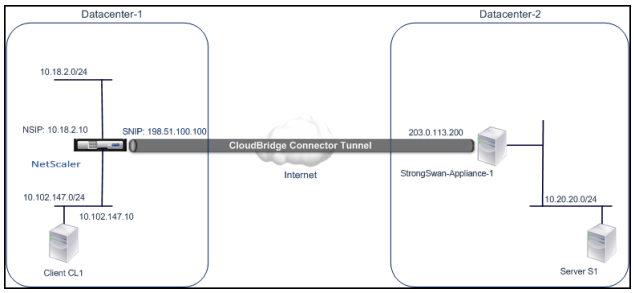
Exemple de configuration d'un tunnel CloudBridge Connector

Pour illustrer le flux de trafic dans un tunnel CloudBridge Connector, prenons un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les appareils suivants :

- Appliance NetScaler NS_Appliance-1 dans un centre de données désigné Datacenter-1
- Appliance StrongSwan StrongSwan-Appliance-1 dans un centre de données désigné Datacenter-2

NS_Appliance-1 et StrongSwan-Appliance-1 permettent la communication entre les réseaux privés du Datacenter-1 et du Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et StrongSwan-Appliance-1 permettent la communication entre le client CL1 dans Datacenter-1 et le serveur S1 dans Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel CloudBridge Connector inclut l'entité de profil IPsec NS_StrongSwan_IPsec_Profile, l'entité de tunnel du CloudBridge Connector NS_StrongSwan_Tunnel et l'entité de routage basé sur des politiques (PBR) NS_StrongSwan_PBR.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

Paramètres principaux de la configuration du tunnel CloudBridge Connector

Entité	Détails
Adresse IP du point de terminaison du tunnel CloudBridge Connector (NS_Appliance-1) dans Datacenter-1	198.51.100.100
Adresse IP du point de terminaison du tunnel CloudBridge Connector (StrongSwan-Appliance-1) dans Datacenter-2	203.0.113.200

Entité	Détails
Centre de données : sous-réseau de 1 dont le trafic doit être protégé via le tunnel CloudBridge Connector	10.102.147,0/24
Datacenter : sous-réseau de type 2 dont le trafic doit être protégé via le tunnel CloudBridge Connector	10.20.20.0/24

Paramètres de l'appliance NetScaler NS_Appliance-1 dans Datacenter-1

|SNIP1 (à des fins de référence uniquement)|198.51.100.100|
|–|–|–|
|Profil IPSe|NS_StrongSwan_IPSEC_Profile|Version IKE : v1, algorithme de chiffrement : AES, algorithme de hachage : HMAC_SHA1 psk =
examplepresharedkey (Remarque : il s'agit d'un exemple de clé de pré-partage, à titre d'illustration). NetScaler ne recommande pas d'utiliser cette chaîne dans votre configuration CloudBridge Connector) |
|Tunnel CloudBridge Connector | NS_Strongswan_Tunnel|IP distante = 203.0.113.200, IP locale = 198.51.100.100, protocole de tunnel = IPSEC, profil IPsec = NS_Strongswan_IPSEC_profile| |Route basée sur des politiques | NS_Strongswan_PBR|Plage d'adresses IP source = Sous-réseau dans le centre de données 1=10.102.147.0-10.102.147.255, plage d'adresses IP de destination = sous-réseau dans le centre de données 2=10.20.20.0-10.20.20.255, tunnel IP = NS_Strongswan_Tunnel|

Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de commencer à configurer le tunnel du connecteur CloudBridge, assurez-vous que :

- Vous avez des connaissances de base sur les configurations Linux.
- Vous avez des connaissances de base sur la suite de protocoles IPsec.
- L'appliance StrongSwan est opérationnelle, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.
- L'appliance NetScaler est opérationnelle, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.
- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance StrongSwan.
  - Mode IPsec : mode tunnel
  - Version d'IKE : Version 1
  - Méthode d'authentification IKE : clé pré-partagée
  - Algorithme de chiffrement IKE : AES

  - Algorithme de hachage IKE : HMAC SHA1
  - Algorithme de chiffrement ESP : AES
  - Algorithme de hachage ESP : HMAC SHA1
- Vous devez spécifier les mêmes paramètres IPsec sur l'appliance NetScaler et sur l'appliance StrongSwan aux deux extrémités du tunnel CloudBridge Connector.
- NetScaler fournit un paramètre commun (dans les profils IPsec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun pour spécifier un algorithme de chiffrement IKE et un algorithme de cryptage ESP. Par conséquent, dans l'appliance StrongSwan, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement dans les paramètres IKE et ESP du fichier IPsec.conf.
- Vous devez configurer le pare-feu côté NetScaler et côté StrongSwan pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)

Configurer StrongSwan pour le tunnel CloudBridge Connector

Pour configurer un tunnel de connecteur CloudBridge entre une appliance NetScaler et une appliance StrongSwan, effectuez les tâches suivantes sur l'appliance StrongSwan :

- **Spécifiez les informations de connexion IPsec dans le fichier ipsec.conf. Le fichier**ipsec.conf définit toutes les informations de contrôle et de configuration pour les connexions IPsec dans l'appliance StrongSwan.
- **Spécifiez la clé pré-partagée dans le fichier ipsec.secrets. Le fichier ipsec.secrets**définit les secrets pour l'authentification IKE/IPsec pour les connexions IPsec dans l'appliance StrongSwan.

Les procédures de configuration du VPN IPSec (tunnel CloudBridge Connector) sur une appliance StrongSwan peuvent changer au fil du temps, en fonction du cycle de publication de StrongSwan. Citrix vous recommande de suivre la documentation officielle de StrongSwan sur la configuration des tunnels VPN IPSec.

L'exemple suivant d'extrait du fichier ipsec.conf spécifie les informations IPsec pour la configuration du tunnel VPN IPSec, décrites dans la rubrique Exemple de configuration du connecteur CloudBridge. Pour plus d'informations, consultez la section Configuration du CloudBridge Connector pdf.

L'exemple suivant d'extrait du fichier ipsec.secrets spécifie la clé pré-partagée d'authentification IKE pour la configuration du tunnel VPN IPSec, décrite dans la rubrique Exemple de configuration du connecteur CloudBridge.

`/etc/ipsec.secrets` clé partagée PSK 'exemplepresharedkey' #pre -pour l'authentification IKE IPsec

Configuration de l'appliance NetScaler pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance StrongSwan, effectuez les tâches suivantes sur l'appliance NetScaler. Vous pouvez utiliser la ligne de commande NetScaler ou l'interface utilisateur graphique (GUI) de NetScaler :

- **Créez un profil IPsec**. Une entité de profil IPsec spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et la méthode d'authentification à utiliser par le protocole IPsec dans le tunnel CloudBridge Connector.
- **Créez un tunnel IP qui utilise le protocole IPsec et associez-y le profil IPsec**. Un tunnel IP spécifie l'adresse IP locale (adresse IP du point de terminaison du tunnel CloudBridge Connector (de type SNIP) configurée sur l'appliance NetScaler), l'adresse IP distante (adresse IP du point de terminaison du tunnel CloudBridge Connector configurée sur l'appliance StrongSwan), le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.
- **Créez une règle PBR et associez-la au tunnel IP**. Une entité PBR spécifie un ensemble de règles et une entité de tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Définissez la plage d'adresses IP source pour spécifier le sous-réseau côté NetScaler dont le trafic doit être protégé via le tunnel, et définissez la plage d'adresses IP de destination pour spécifier le sous-réseau côté StrongSwan dont le trafic doit être protégé via le tunnel.

Pour créer un profil IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1`
- `show ipsec profile <name>`

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Pour créer un profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **ConnecteurCloudBridge**>**ProfilIPsec**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil IPsec**, définissez les paramètres suivants :
    - Nom
    - Algorithme de chiffrement
    - Algorithme de hachage
    - Version du protocole IKE
4. **Configurez la méthode d'authentification IPsec à utiliser par les deux homologues du tunnel CloudBridge Connector pour s'authentifier mutuellement : sélectionnez la**méthode d'authentification par clé pré-partagée et définissez le paramètre Pre-Shared Key**Exists.**
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur **Ajouter**.
3. Sur la page Ajouter un tunnel IP, définissez les paramètres suivants :
    - Nom
    - IP distante
    - Masque à distance
    - Type d'adresse IP locale (Dans la liste déroulante Type d'adresse IP locale, sélectionnez *Adresse IP du sous-réseau*).
    - IP locale (Toutes les adresses IP configurées du type IP sélectionné figurent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
    - Protocole
    - Profil IPSec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la page **Créer un PBR**, définissez les paramètres suivants :
    - Nom
    - Action
    - Type de saut suivant (sélectionnez le *tunnel IP*)
    - Nom du tunnel IP
    - IP de la source : faible
    - IP de la source : élevée
    - IP de destination faible
    - IP de destination : élevée

4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration du tunnel CloudBridge Connector correspondante sur l'appliance NetScaler apparaît dans l'interface graphique. L'état actuel du tunnel du connecteur CloudBridge est affiché dans le volet Configuré du CloudBridge Connector. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.
Les commandes suivantes créent les paramètres de l'appliance NetScaler NS_Appliance-1 dans « Exemple de configuration d'un CloudBridge Connector » :

```
1      > add ipsec profile NS_StrongSwan_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 -encAlgo AES -hashalgo
          HMAC_SHA1
2
3
4      Done
5
6      > add iptunnel NS_StrongSwan_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 -protocol IPSEC -ipsecProfileName
          NS_StrongSwan_IPSec_Profile
7
8
9      Done
10
11     > add pbr NS_StrongSwan_Pbr -srcIP 10.102.147.0-10.102.147.255 -
          destIP 10.20.0.0-10.20.255.255 -ipTunnel NS_StrongSwan_Tunnel
12
13
14     Done
15
16     > apply pbrs
17
18
19     Done
20 <!--NeedCopy-->
```

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance NetScaler à l'aide des compteurs statistiques des tunnels CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

Interopérabilité du CloudBridge Connector — F5 BIG-IP

May 5, 2023

Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance F5 BIG-IP pour connecter deux centres de données ou étendre votre réseau à un fournisseur de cloud. L'appliance NetScaler et l'appliance F5 BIG-IP constituent les points de terminaison du tunnel CloudBridge Connector et sont appelées homologues.

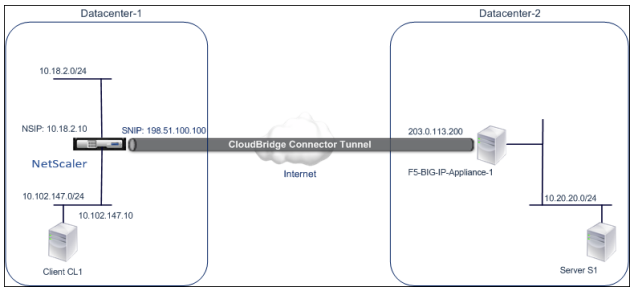
Exemple de configuration d'un tunnel CloudBridge Connector

Pour illustrer le flux de trafic dans un tunnel CloudBridge Connector, prenons un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les appareils suivants :

- Appliance NetScaler NS_Appliance-1 dans un centre de données désigné Datacenter-1
- Appliance F5 BIG-IP F5-BIG-IP-Appliance-1 dans un centre de données désigné Datacenter-2

NS_Appliance-1 et F5-big-IP-Appliance-1 permettent la communication entre les réseaux privés du Datacenter-1 et du Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et F5-big-IP-Appliance-1 permettent la communication entre le client CL1 dans Datacenter-1 et le serveur S1 dans Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel CloudBridge Connector inclut l'entité de profil IPsec NS_F5-BIG-IP_Profile, l'entité de tunnel du CloudBridge Connector NS_F5-BIG-IP_Tunnel et l'entité de routage basé sur des règles (PBR) NS_F5-big-IP_PBR.



Pour plus d'informations, reportez-vous à F5 big IP pdf.

Points à considérer pour une configuration de tunnel CloudBridge Connector

- L'appliance NetScaler est opérationnelle, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.
- L'appliance F5 BIG-IP est opérationnelle, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.

- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance F5 BIG-IP.
  - Mode IPsec : mode tunnel
  - Version d'IKE : Version 1
  - Méthode d'authentification IKE : clé pré-partagée
  - Algorithme de chiffrement IKE : AES
  - Algorithme de hachage IKE : HMAC SHA1
  - Algorithme de chiffrement ESP : AES
  - Algorithme de hachage ESP : HMAC SHA1
- Vous devez spécifier les mêmes paramètres IPsec sur l'appliance NetScaler et sur l'appliance F5 BIG-IP aux deux extrémités du tunnel CloudBridge Connector.
- NetScaler fournit un paramètre commun (dans les profils IPsec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun pour spécifier un algorithme de chiffrement IKE et un algorithme de cryptage ESP. Par conséquent, dans l'appliance F5 BIG-IP, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement dans IKE (configuration de phase 1) et ESP (configuration de phase 2).
- Vous devez configurer le pare-feu côté NetScaler et côté F5 BIG-IP pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)

Configuration de F5 BIG-IP pour le tunnel CloudBridge Connector

Pour configurer un tunnel de connecteur CloudBridge entre une appliance NetScaler et une appliance F5 BIG-IP, effectuez les tâches suivantes sur l'appliance F5 BIG-IP :

- **Créez un serveur virtuel de transfert pour IPsec**. Un serveur virtuel de transfert intercepte le trafic IP pour le tunnel IPsec.
- **Créez un homologue IKE.** Un homologue IKE spécifie les points de terminaison du tunnel IPsec local et distant. Il spécifie également les algorithmes et les informations d'identification à utiliser pour la phase 1 d'IPsec IKE.
- **Créez une politique IPsec personnalisée.** Une politique spécifie le protocole IPsec (ESP) et le mode (tunnel) à utiliser pour former le tunnel IPsec. Il spécifie également les algorithmes et les paramètres de sécurité à utiliser pour la phase 2 d'IKE IPsec.
- **Créez un sélecteur de trafic IPsec bidirectionnel**. Un sélecteur de trafic spécifie les sous-réseaux côté F5 BIG-IP et côté NetScaler dont le trafic IP doit être traversé par le tunnel IPsec.

Les procédures de configuration du VPN IPsec (tunnel CloudBridge Connector) sur une appliance F5 BIG-IP peuvent changer au fil du temps, en fonction du cycle de publication de F5. Citrix vous recommande de suivre la documentation officielle de F5 BIG-IP pour configurer les tunnels VPN IPsec, à

l'adresse suivante :

https://f5.com

Pour créer un serveur virtuel de transfert pour IPsec à l'aide de l'interface graphique F5 BIG-IP

1. Dans l'onglet **Principal**, cliquez sur **Trafic local** > **Serveurs virtuels**, puis cliquez sur **Créer**.
2. Sur l'écran **New Virtual Server List**, définissez les paramètres suivants :
   - **Nom**. Entrez un nom unique pour le serveur virtuel.
   - **Tapez**. Sélectionnez **Transfert (IP)**.
   - **Adresse de destination**. Tapez une adresse réseau générique au format CIDR, par exemple, 0.0.0.0/0 pour IPv4 afin d'accepter tout trafic.
   - **Port de service**. Sélectionnez **Tous les ports** dans la liste.
   - **Liste des protocoles**. Sélectionnez **Tous les protocoles** dans la liste.
   - **Trafic VLAN et tunnel**. Conservez la sélection par défaut, **Tous les VLAN et tunnels**.
3. Cliquez sur **Terminé**.

Pour créer une politique IPsec personnalisée à l'aide de l'interface graphique F5 BIG-IP

1. **Dans l'onglet**principal**, cliquez sur**Réseau**>**IPsec**>**Politiques IPsec**, puis cliquez sur Créer.**
2. Sur l'écran **Nouvelle politique**, définissez les paramètres suivants :
   - **Nom**. Entrez un nom unique pour la politique.
   - **Protocole IPSec**. Conservez la sélection par défaut, ESP.
   - **Mode**. Sélectionnez Tunnel. L'écran s'actualise pour afficher d'autres paramètres connexes.
   - **Adresse locale du tunnel**. Tapez l'adresse IP du point de terminaison du tunnel IPsec local (configurée sur l'appliance F5 BIG-IP).
   - **Adresse distante du tunnel**. Tapez l'adresse IP du point de terminaison du tunnel IPsec distant (configurée sur l'appliance NetScaler).
3. Pour les paramètres de phase 2 d'IKE, conservez les valeurs par défaut ou sélectionnez les options adaptées à votre déploiement.
4. Cliquez sur **Terminé**.

Pour créer un sélecteur de trafic IPsec bidirectionnel à l'aide de l'interface graphique F5 BIG-IP

1. **Dans l'onglet**principal**, cliquez sur**Réseau**>**IPsec**>**Sélecteurs de trafic**, puis cliquez sur Créer.**
2. Sur l'écran **New Traffic Selector**, définissez les paramètres suivants :
   - **Nom**. Entrez un nom unique pour le sélecteur de trafic.
   - **Commande**. Conservez la valeur par défaut **(d'abord)**. Ce paramètre spécifie l'ordre dans lequel le sélecteur de trafic apparaît sur l'écran Liste des sélecteurs de trafic.
3. Dans la liste **Configuration**, sélectionnez **Avancé**et définissez les paramètres suivants :
   - **Adresse IP source**. Cliquez sur **Hôte** ou **Réseau**et, dans le champ **Adresse**, tapez l'adresse du sous-réseau F5 BIG-IP dont le trafic doit être protégé via le tunnel IPsec.
   - **Port source**. Sélectionnez *** Tous les ports**.

- **Adresse IP de destination**. Cliquez sur **Hôte**, puis dans le champ **Adresse**, saisissez l'adresse du sous-réseau côté NetScaler dont le trafic doit être protégé via le tunnel IPsec.
- **Port de destination**. Sélectionnez *** Tous les ports**.
- **Protocole**. Sélectionnez *** Tous les protocoles**.
- **Orientation**. Sélectionnez **Les deux**.
- **Action**. Sélectionnez **Protéger**. Le paramètre **Nom de la politique IPSec** s'affiche.
- **Nom de la politique IPSec**. Sélectionnez le nom de la politique IPsec personnalisée que vous avez créée.

4. Cliquez sur **Terminé**.

Configuration de l'appliance NetScaler pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance F5 BIG-IP, effectuez les tâches suivantes sur l'appliance NetScaler. Vous pouvez utiliser la ligne de commande NetScaler ou l'interface utilisateur graphique (GUI) de NetScaler :

- **Créez un profil IPsec**. Une entité de profil IPsec spécifie les paramètres du protocole IPsec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et la méthode d'authentification à utiliser par le protocole IPsec dans le tunnel CloudBridge Connector.
- **Créez un tunnel IP qui utilise le protocole IPsec et associez-y le profil IPsec**. Un tunnel IP spécifie l'adresse IP locale (adresse IP du point de terminaison du tunnel CloudBridge Connector (de type SNIP) configurée sur l'appliance NetScaler), l'adresse IP distante (adresse IP du point de terminaison du tunnel CloudBridge Connector configurée sur l'appliance F5 BIG-IP), le protocole (IPsec) utilisé pour configurer le tunnel CloudBridge Connector et une entité de profil IPsec. L'entité de tunnel IP créée est également appelée entité de tunnel CloudBridge Connector.
- **Créez une règle PBR et associez-la au tunnel IP**. Une entité PBR spécifie un ensemble de règles et une entité de tunnel IP (tunnel CloudBridge Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Définissez la plage d'adresses IP source pour spécifier le sous-réseau côté NetScaler dont le trafic doit être protégé via le tunnel, et définissez la plage d'adresses IP de destination pour spécifier le sous-réseau côté F5 BIG-IP dont le trafic doit être protégé via le tunnel.

Pour créer un profil IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecyENABLE`
- `show ipsec profile** <name>`

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande NetScaler

À l'invite de commande, tapez :

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Pour créer un profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > Profil **IPsec**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil IPsec**, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE
4. **Configurez la méthode d'authentification IPsec à utiliser par les deux homologues du tunnel CloudBridge Connector pour s'authentifier mutuellement : sélectionnez la**méthode d'authentification par clé pré-partagée et définissez le paramètre Pre-Shared Key**Exists.**
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.
2. Dans l'onglet **Tunnels IPv4**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un tunnel IP**, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque à distance
   - Type d'adresse IP locale (Dans la liste déroulante Type d'adresse IP locale, sélectionnez *Adresse IP du sous-réseau*).
   - IP locale (Toutes les adresses IP configurées du type IP sélectionné figurent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPSec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **PBR**.

2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Dans la page **Créer un PBR**, définissez les paramètres suivants :
    - Nom
    - Action
    - Type de saut suivant (sélectionnez le *tunnel IP*)
    - Nom du tunnel IP
    - IP de la source : faible
    - IP de la source : élevée
    - IP de destination faible
    - IP de destination : élevée
4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration du tunnel CloudBridge Connector correspondante sur l'appliance NetScaler apparaît dans l'interface graphique. L'état actuel du tunnel du connecteur CloudBridge est affiché dans le volet Configuré du CloudBridge Connector. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Les commandes suivantes créent les paramètres de l'appliance NetScaler NS_Appliance-1 dans « Exemple de configuration d'un CloudBridge Connector ». :

```
1     > add ipsec profile NS_F5-BIG-IP_IPSec_Profile -psk
      examplepresharedkey -ikeVersion v1 -encAlgo AES -hashalgo
      HMAC_SHA1 -lifetime 315360 -perfectForwardSecrecy ENABLE
2
3
4     Done
5
6     > add iptunnel NS_F5-BIG-IP_Tunnel 203.0.113.200 255.255.255.255
      198.51.100.100 -protocol IPSEC -ipsecProfileName NS_F5-BIG-
      IP_IPSec_Profile
7
8
9     Done
10
11    > add pbr NS_F5-BIG-IP_Pbr -srcIP 10.102.147.0-10.102.147.255 -
      destIP 10.20.0.0-10.20.255.255 -ipTunnel NS_F5-BIG-IP_Tunnel
12
13
14    Done
15
16    > apply pbrs
17
18
19    Done
```



```
<!--NeedCopy-->
```

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance NetScaler à l'aide des compteurs statistiques des tunnels CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

Interopérabilité du CloudBridge Connector — Cisco ASA

May 5, 2023

Vous pouvez configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance Cisco ASA pour connecter deux centres de données ou étendre votre réseau à un fournisseur de cloud. L'appliance NetScaler et l'appliance Cisco ASA constituent les points de terminaison du tunnel CloudBridge Connector et sont appelées homologues.

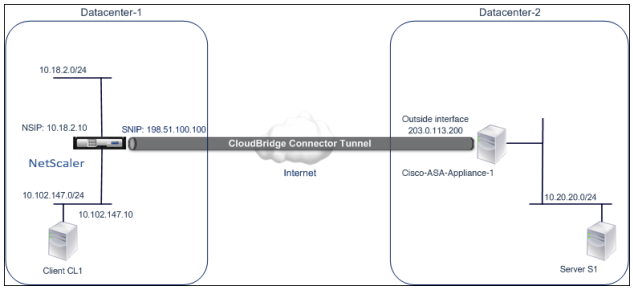
Exemple de configuration d'un tunnel CloudBridge Connector

Pour illustrer le flux de trafic dans un tunnel CloudBridge Connector, prenons un exemple dans lequel un tunnel CloudBridge Connector est configuré entre les appliances suivantes :

- Appliance NetScaler NS_Appliance-1 dans un centre de données désigné Datacenter-1
- Appliance Cisco ASA Cisco-ASA-Appliance-1 dans un centre de données désigné Datacenter-2

NS_Appliance-1 et Cisco-ASA-Appliance-1 permettent la communication entre les réseaux privés du Datacenter-1 et du Datacenter-2 via le tunnel CloudBridge Connector. Dans l'exemple, NS_Appliance-1 et Cisco-ASA-Appliance-1 permettent la communication entre le client CL1 dans le Datacenter-1 et le serveur S1 dans le Datacenter-2 via le tunnel CloudBridge Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Sur NS_Appliance-1, la configuration du tunnel CloudBridge Connector inclut l'entité de profil IPsec NS_Cisco-ASA_IPSEC_Profile, l'entité de tunnel du CloudBridge Connector NS_Cisco-ASA_Tunnel et l'entité de routage basé sur des politiques (PBR) NS_Cisco-ASA_PBR.



Points à considérer pour une configuration de tunnel CloudBridge Connector

Avant de commencer à configurer le tunnel du connecteur CloudBridge, assurez-vous que :

- Les paramètres IPsec suivants sont pris en charge pour un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance Cisco ASA.

Propriétés IPSec	Paramètres
Mode IPSec	Mode tunnel
Version IKE	Version 1
Méthode d'authentification IKE	Clé pré-partagée
Algorithme de chiffrement IKE	AES, 3DES
algorithme de hachage IKE	HMAC SHA1, HMAC MD5
Algorithme de chiffrement ESP	AES, 3DES
Algorithme de hachage ESP	HMAC SHA1, HMAC MD5

- Vous devez spécifier les mêmes paramètres IPsec sur l'appliance NetScaler et sur l'appliance Cisco ASA aux deux extrémités du tunnel CloudBridge Connector.
- NetScaler fournit un paramètre commun (dans les profils IPsec) pour spécifier un algorithme de hachage IKE et un algorithme de hachage ESP. Il fournit également un autre paramètre commun pour spécifier un algorithme de chiffrement IKE et un algorithme de cryptage ESP. Par conséquent, dans l'appliance Cisco ASA, vous devez spécifier le même algorithme de hachage et le même algorithme de chiffrement dans IKE (configuration de phase 1) et ESP (configuration de phase 2).
- Vous devez configurer le pare-feu côté NetScaler et côté Cisco ASA pour autoriser ce qui suit.
  - Tous les paquets UDP pour le port 500
  - Tous les paquets UDP pour le port 4500
  - Tous les paquets ESP (numéro de protocole IP 50)

Configuration de Cisco ASA pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector sur une appliance Cisco ASA, utilisez l'interface de ligne de commande Cisco ASA, qui est l'interface utilisateur principale pour la configuration, la surveillance et la maintenance des appliances Cisco ASA.

Avant de commencer la configuration du tunnel CloudBridge Connector sur une appliance Cisco ASA, assurez-vous que :

- Vous avez un compte utilisateur avec des informations d'identification d'administrateur sur l'appliance Cisco ASA.
- Vous connaissez l'interface de ligne de commande Cisco ASA.
- L'appliance Cisco ASA est opérationnelle, est connectée à Internet et est également connectée aux sous-réseaux privés dont le trafic doit être protégé via le tunnel CloudBridge Connector.

> **Remarque**
>
> Les procédures de configuration du tunnel CloudBridge Connector sur une appliance Cisco ASA peuvent changer au fil du temps, en fonction du cycle de publication de Cisco. Citrix vous recommande de suivre la documentation officielle du produit Cisco ASA pour la configuration des tunnels VPN IPsec, à l'adresse suivante :

- http://www.cisco.com

Pour configurer un tunnel de connecteur CloudBridge entre une appliance NetScaler et une appliance Cisco ASA, effectuez les tâches suivantes sur la ligne de commande de l'appliance Cisco ASA :

- **Créez une politique IKE**. Une politique IKE définit une combinaison de paramètres de sécurité à utiliser pendant la négociation IKE (phase 1). Par exemple, les paramètres tels que l'algorithme de hachage, l'algorithme de chiffrement et la méthode d'authentification à utiliser dans la négociation IKE sont définis dans cette tâche.
- **Activez IKE sur l'interface externe**. Activez IKE sur l'interface externe via laquelle le trafic du tunnel sera acheminé vers l'homologue du tunnel.
- **Créez un groupe de tunnels**. Un groupe de tunnels spécifie le type de tunnel et la clé pré-partagée. Le type de tunnel doit être défini sur ipsec-l2l, qui signifie IPsec LAN to LAN. Une clé pré-partagée est une chaîne de texte que les homologues d'un tunnel CloudBridge Connector utilisent pour s'authentifier mutuellement. Les clés pré-partagées sont comparées les unes aux autres pour l'authentification IKE. Par conséquent, pour que l'authentification soit réussie, vous devez configurer la même clé pré-partagée sur l'appliance Cisco ASA et l'appliance NetScaler.
- **Définissez un jeu de transformations**. Un ensemble de transformations définit une combinaison de paramètres de sécurité (phase 2) à utiliser lors de l'échange de données via le tunnel CloudBridge Connector une fois la négociation IKE réussie.
- **Créez une liste d'accès**. Les listes d'accès cryptographiques sont utilisées pour définir les sous-réseaux dont le trafic IP sera protégé via le tunnel CloudBridge. Les paramètres source et destination de la liste d'accès spécifient les sous-réseaux côté appliance Cisco et côté NetScaler

qui doivent être protégés via le tunnel CloudBridge Connector. La liste d'accès doit être configurée pour autoriser. Tout paquet de demande provenant d'une appliance du sous-réseau côté appliance Cisco et destiné à une appliance du sous-réseau côté NetScaler, et qui correspond aux paramètres source et destination de la liste d'accès, est envoyé via le tunnel CloudBridge Connector.

- **Créez une carte cryptographique**. Les cartes cryptographiques définissent les paramètres IPsec pour les associations de sécurité (SA). Ils incluent les éléments suivants : une liste d'accès cryptographique pour identifier les sous-réseaux dont le trafic doit être protégé via le tunnel CloudBridge, une identification des homologues (NetScaler) par adresse IP et des transformations définies pour correspondre aux paramètres de sécurité des homologues.
- **Appliquez la carte cryptographique à l'interface externe**. Dans cette tâche, vous allez appliquer la carte cryptographique à l'interface externe par laquelle le trafic du tunnel sera acheminé vers l'homologue du tunnel. L'application de la carte cryptographique à une interface indique à l'appliance Cisco ASA d'évaluer tout le trafic d'interface par rapport à l'ensemble de cartes cryptographiques et d'utiliser la politique spécifiée lors des négociations de connexion ou d'association de sécurité.

Les exemples présentés dans les procédures suivantes créent les paramètres de l'appliance Cisco ASA Cisco-ASA-Appliance-1 utilisée dans Exemple de configuration et de flux de données du CloudBridge Connector.

Pour créer une politique IKE à l'aide de la ligne de commande Cisco ASA

À l'invite de commande de l'appliance Cisco ASA, tapez les commandes suivantes, en commençant par le mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
priorité de la politique crypto ikev1	Cisco-ASA-Appliance-1 (config) # crypto ikev1 policy 1	Entrez en mode de configuration de stratégie IKE et identifiez la politique à créer. (Chaque politique est identifiée de manière unique par le numéro de priorité que vous attribuez.) Cet exemple configure la politique 1.
chiffrement (3des | aes)	Cisco-ASA-Appliance-1 (config-ikev1-policy) # cryptage 3des	Spécifiez l'algorithme de chiffrement. Cet exemple configure l'algorithme 3DES.
hachage (sha | md5)	Cisco-asa-Appliance-1 (config- ikev1-policy) # hash sha	Spécifiez l'algorithme de hachage. Cet exemple configure SHA.

Commande	Exemple	Description de la commande
authentification préalable au partage	Cisco-ASA-Appliance-1 (config- ikev1-policy) # authentification préalable au partage	Spécifiez la méthode d'authentification préalable au partage.
groupe 2	Cisco-ASA-Appliance-1 (config- ikev1-policy) # groupe 2	Spécifiez l'identifiant de groupe Diffie-Hellman de 1024 bits (2).
durée de vie en secondes	Cisco-ASA-Appliance-1 (config- ikev1-policy) # durée de vie 28800	Spécifiez la durée de vie de l'association de sécurité en secondes. Cet exemple configure 28 800 secondes, qui est la valeur par défaut de durée de vie dans une appliance NetScaler.

Pour activer IKE sur l'interface externe à l'aide de la ligne de commande Cisco ASA

À l'invite de commande de l'appliance Cisco ASA, tapez les commandes suivantes, en commençant par le mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
Crypto ikev1 activé en extérieur	Cisco-ASA-Appliance-1 (config) # crypto ikev1 activé en extérieur	Activez IKEv1 sur l'interface via laquelle le trafic du tunnel circule vers l'homologue du tunnel. Cet exemple active IKEv1 sur l'interface nommée outside.

Pour créer un groupe de tunnels à l'aide de la ligne de commande Cisco ASA

À l'invite de commandes de l'appliance Cisco ASA, tapez les commandes suivantes, en commençant en mode de configuration globale, comme indiqué dans le groupe de tunnels pdf joint à l'aide de la ligne de commande Cisco ASA :

Pour créer une liste d'accès crypto à l'aide de la ligne de commande Cisco ASA

À l'invite de commande de l'appliance Cisco ASA, tapez la commande suivante en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
liste d'accès numéro de liste d'accès autoriser l'adresse IP source source, caractère générique, destination, caractère générique	Cisco-ASA-Appliance-1 (config) # access-list 111 autorise l'adresse IP 10.20.20.0 0.0.255 10.102.147.0 0.0.0.255	Spécifiez les conditions permettant de déterminer les sous-réseaux dont le trafic IP doit être protégé via le tunnel CloudBridge Connector. Cet exemple configure la liste d'accès 111 pour protéger le trafic provenant des sous-réseaux 10.20.20.0/24 (côté Cisco-ASA-Appliance-1) et 10.102.147.0/24 (côté NS_Appliance-1).

Pour définir un ensemble de transformations à l'aide de la ligne de commande Cisco ASA

À l'invite de commandes de l'appliance Cisco ASA, tapez les commandes suivantes, en commençant en mode de configuration globale. Voir Transform set using ASA Command line table pdf.

Pour créer une carte crypto à l'aide de la ligne de commande Cisco ASA

À l'invite de commande de l'appliance Cisco ASA, tapez les commandes suivantes en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
cryptomap map-name seq-num match address access-list-name	Cisco-ASA-Appliance-1 (config) # carte cryptographique NS-CISCO-CM 1 correspond à l'adresse 111	Créez une carte cryptographique et spécifiez une liste d'accès à celle-ci. Cet exemple configure la carte cryptographique NS-CISCO-CM avec le numéro de séquence 1 et attribue la liste d'accès 111 à NS-CISCO-CM.

Commande	Exemple	Description de la commande
nom de carte cryptographique seq-num set adresse IP homologue	Cisco-ASA-Appliance-1 (config) # carte cryptographique NS-CISCO-CM 1 set peer 198.51.100.100	Spécifiez l'homologue (appliance NetScaler) par son adresse IP. Cet exemple indique 198.51.100.100, qui est l'adresse IP du point de terminaison du tunnel sur l'appliance NetScaler.
cryptomap map-name seq-num set ikev1 transform-set transform-set-name	Cisco-ASA-Appliance-1 (config) # carte cryptographique NS-CISCO-CM 1 set de transformations ikev1 NS-CISCO-TS	Spécifiez quel jeu de transformations est autorisé pour cette entrée de carte cryptographique. Cet exemple spécifie le jeu de transformations NS-CISCO-TS.

Pour appliquer une carte cryptographique à une interface à l'aide de la ligne de commande Cisco ASA

À l'invite de commande de l'appliance Cisco ASA, tapez les commandes suivantes en commençant en mode de configuration globale, dans l'ordre indiqué :

Commande	Exemple	Description de la commande
nom de la carte cryptographique, nom de l'interface, nom de l'interface	Cisco-ASA-Appliance-1 (config) # interface NS-CISCO-CM extérieure	Appliquez la carte cryptographique à l'interface via laquelle le trafic du tunnel CloudBridge Connector circulera. Cet exemple applique la carte cryptographique NS-CISCO-CM à l'interface extérieure.

Configuration de l'appliance NetScaler pour le tunnel CloudBridge Connector

Pour configurer un tunnel CloudBridge Connector entre une appliance NetScaler et une appliance Cisco ASA, effectuez les tâches suivantes sur l'appliance NetScaler. Vous pouvez utiliser la ligne de commande NetScaler ou l'interface utilisateur graphique (GUI) de NetScaler :

- Créez un profil IPsec.
- Créez un tunnel IP qui utilise le protocole IPSec et associez le profil IPSec à celui-ci.
- Créez une règle PBR et associez-la au tunnel IP.

Pour créer un profil IPSEC à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

Pour créer un tunnel IPSEC et y lier le profil IPSEC à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

- `**add pbr** <pbrName> **ALLOW** -**srcIP** <subnet-range> -**destIP** <subnet-range>`
- `**ipTunnel** <tunnelName>`
- `**apply pbrs**`
- `**show pbr** <pbrName>`

Pour créer un profil IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **CloudBridge Connector** > Profil **IPsec**.
2. Dans le volet de détails, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un profil IPsec**, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE
   - Perfect Forward Secrecy (Activer ce paramètre)
4. **Configurez la méthode d'authentification IPsec à utiliser par les deux homologues du tunnel CloudBridge Connector pour s'authentifier mutuellement : sélectionnez la méthode d'**authentification par clé pré-partagée et définissez le paramètre Pre-Shared Key**Exists.**
5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et y lier le profil IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **CloudBridge Connector** > **Tunnels IP**.

2. Dans l' **onglet Tunnels IPv4**, cliquez sur **Ajouter**.
3. Sur la page **Ajouter un tunnel IP**, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque à distance
   - Type d'adresse IP locale (Dans la liste déroulante Type d'adresse IP locale, sélectionnez Adresse IP du sous-réseau).
   - IP locale (Toutes les adresses IP configurées du type IP sélectionné figurent dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPSec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface graphique :

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Dans l'onglet **PBR**, cliquez sur **Ajouter**.
3. Sur la page **Créer un PBR**, définissez les paramètres suivants :
   - Nom
   - Action
   - Type de saut suivant (sélectionnez le tunnel IP)
   - Nom du tunnel IP
   - IP de la source : faible
   - IP de la source : élevée
   - IP de destination faible
   - IP de destination : élevée
4. Cliquez sur **Créer**, puis sur **Fermer**.

La nouvelle configuration du tunnel CloudBridge Connector correspondante sur l'appliance NetScaler apparaît dans l'interface graphique. L'état actuel du tunnel du connecteur CloudBridge est affiché dans le volet Configuré du CloudBridge Connector. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

Les commandes suivantes créent les paramètres de l'appliance NetScaler NS_Appliance-1 dans « Exemple de configuration d'un CloudBridge Connector ». « :

```
1 > add ipsec profile NS_Cisco-ASA_IPSec_Profile -psk
    examplepresharedkey -ikeVersion v1 -encAlgo AES -hashalgo
    HMAC_SHA1 -lifetime 315360 -perfectForwardSecrecy ENABLE
2
3 Done
4
5 > add iptunnel NS_Cisco-ASA_Tunnel 203.0.113.200 255.255.255.255
    198.51.100.100 -protocol IPSEC -ipsecProfileName NS_Cisco-
```



```
    ASA_IPSec_Profile
6
7
8  Done
9
10 > add pbr NS_Cisco-ASA_Pbr -srcIP 10.102.147.0-10.102.147.255 -destIP
    10.20.0.0-10.20.255.255 -ipTunnel NS_Cisco-ASA_Tunnel
11
12
13 Done
14
15 > apply pbrs
16
17 Done
18
19 <!--NeedCopy-->
```

Surveillance du tunnel CloudBridge Connector

Vous pouvez surveiller les performances des tunnels CloudBridge Connector sur une appliance NetScaler à l'aide des compteurs statistiques des tunnels CloudBridge Connector. Pour plus d'informations sur l'affichage des statistiques des tunnels CloudBridge Connector sur une appliance NetScaler, consultez la section Surveillance des tunnels CloudBridgeConnector.

Haute disponibilité

May 5, 2023

Un déploiement à haute disponibilité (HA) de deux appliances NetScaler peut garantir un fonctionnement ininterrompu lors de n'importe quelle transaction. Une appliance étant configurée en tant que nœud principal et l'autre en tant que nœud secondaire, le nœud principal accepte les connexions et gère les serveurs tandis que le nœud secondaire surveille le nœud principal. Si, pour une raison quelconque, le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

Le nœud secondaire surveille le nœud principal en envoyant des messages périodiques (souvent appelés messages de pulsation ou vérifications de l'état) pour déterminer si le nœud principal accepte les connexions. Si une vérification de l'état échoue, le nœud secondaire tente de nouveau la connexion pendant une période spécifiée, après quoi il détermine que le nœud principal ne fonctionne pas normalement. Le nœud secondaire prend ensuite le relais du nœud principal (processus appelé basculement).

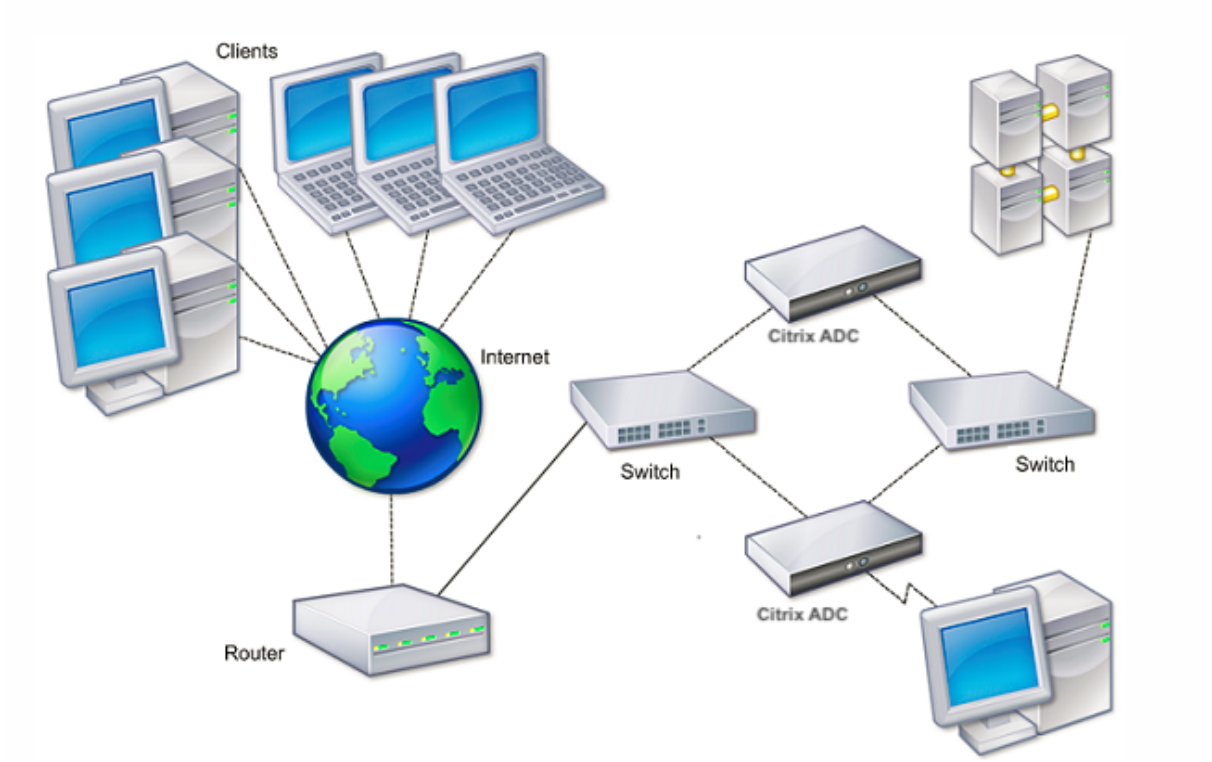
Après un basculement, tous les clients doivent rétablir leurs connexions aux serveurs gérés, mais les règles de persistance de session sont conservées comme elles l'étaient avant le basculement.

Lorsque la persistance de la journalisation du serveur Web est activée, aucune donnée de journal n'est perdue en raison du basculement. Pour que la persistance de la journalisation soit activée, la configuration du serveur de journaux doit contenir des entrées pour les deux systèmes dans le fichier log.conf.

> **Remarque :**
>
> Dans certains cas, le nœud principal est utilisé comme proxy pour le nœud secondaire.

La figure suivante montre une configuration réseau avec une paire HA.

Figure 1. Appliances NetScaler dans une configuration à haute disponibilité



Pour configurer HA, vous pouvez commencer par créer une configuration de base, avec les deux nœuds dans le même sous-réseau. Vous pouvez ensuite personnaliser les intervalles auxquels les nœuds communiquent les informations de contrôle de santé, le processus par lequel les nœuds maintiennent la synchronisation et la propagation des commandes du serveur principal au système secondaire. Vous pouvez configurer le mode de sécurité intégrée pour éviter qu'aucun nœud ne soit principal. Si votre environnement inclut des appareils qui n'acceptent pas les messages ARP gratuits de NetScaler, vous devez configurer des adresses MAC virtuelles. Lorsque vous êtes prêt pour une configuration plus complexe, vous pouvez configurer des nœuds HA dans différents sous-réseaux.

Pour améliorer la fiabilité de votre configuration HA, vous pouvez configurer des moniteurs de

routage et créer des liens redondants. Dans certaines situations, par exemple lors du dépannage ou de l'exécution de tâches de maintenance, vous pouvez forcer un nœud à basculer (attribuer le statut principal à l'autre nœud), ou forcer le nœud secondaire à rester secondaire ou le nœud principal à rester principal.

Points à prendre en compte pour une configuration à haute disponibilité

June 20, 2023

> **Remarque**
>
> Les exigences suivantes pour la configuration des systèmes dans une configuration HA :

- Dans une configuration HA, les appliances NetScaler principales et secondaires doivent être du même modèle. Les différents modèles NetScaler ne sont pas pris en charge dans une paire HA. De plus, les VPX NetScaler déployés sur différents modèles ne sont pas pris en charge dans une paire HA. Seuls les VPX NetScaler déployés sur le même modèle peuvent former une paire HA.
- Dans une configuration HA, les deux nœuds doivent exécuter la même version de NetScaler.
- Les entrées du fichier de configuration (ns.conf) sur le système principal et le système secondaire doivent correspondre, avec les exceptions suivantes :
  - Les systèmes principal et secondaire doivent chacun être configurés avec leurs propres adresses IP uniques (NSIP).
  - Dans une paire HA, l'ID du nœud et l'adresse IP associée d'un nœud doivent pointer vers l'autre nœud. Par exemple, si vous avez des nœuds NS1 et NS2, vous devez configurer NS1 avec un ID de nœud unique et l'adresse IP de NS2, et vous devez configurer NS2 avec un ID de nœud unique et l'adresse IP de NS1.
- Si vous créez un fichier de configuration sur l'un des nœuds en utilisant une méthode qui ne passe pas directement par l'interface graphique ou l'interface de ligne de commande (par exemple, en important des certificats SSL ou en passant à des scripts de démarrage), vous devez copier le fichier de configuration sur l'autre nœud ou créer un fichier identique sur ce nœud.
- Au départ, toutes les appliances NetScaler sont configurées avec le même mot de passe de nœud RPC. Les nœuds RPC sont des entités système internes utilisées pour la communication système à système des informations de configuration et de session. Pour des raisons de sécurité, vous devez modifier les mots de passe par défaut des nœuds RPC.

  Un nœud RPC existe sur chaque NetScaler. Ce nœud stocke le mot de passe, qui est vérifié par rapport au mot de passe fourni par le système de contact. Pour communiquer avec d'autres systèmes, chaque NetScaler doit connaître ces systèmes, notamment comment s'authentifier

sur ces systèmes. Les nœuds RPC conservent ces informations, qui incluent les adresses IP des autres systèmes et les mots de passe dont ils ont besoin pour l'authentification.

Les nœuds RPC sont implicitement créés lors de l'ajout d'un nœud ou d'un site Global Server Load Balancing (GSLB). Vous ne pouvez pas créer ou supprimer des nœuds RPC manuellement.

> **Remarque** :
>
> Si les appliances NetScaler d'une configuration haute disponibilité sont configurées en mode monobras, vous devez désactiver toutes les interfaces système à l'exception de celle connectée au commutateur ou au hub.

Pour une configuration IPv6 HA, les considérations suivantes s'appliquent :

- Vous devez installer la licence IPv6 sur les deux appliances NetScaler.
- Après avoir installé la licence IPv6, activez la fonctionnalité IPv6 à l'aide de l'interface graphique ou de l'interface de ligne de commande.
- Les deux appliances NetScaler nécessitent une adresse IPv6 NSIP globale. En outre, les entités réseau (par exemple, les commutateurs et les routeurs) situées entre les deux nœuds doivent prendre en charge le protocole IPv6.

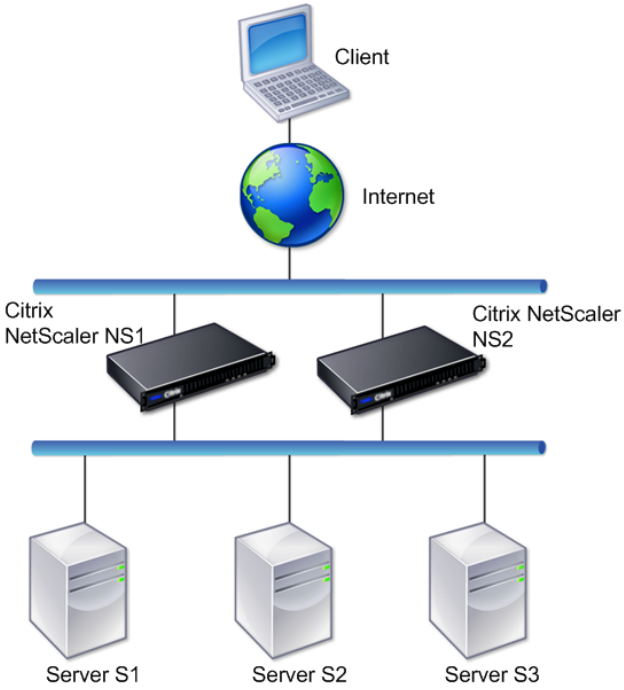
Configuration de la haute disponibilité

May 5, 2023

Pour configurer une configuration de haute disponibilité, vous créez deux nœuds, chacun définissant l'adresse IP NetScaler (NSIP) de l'autre en tant que nœud distant. Commencez par vous connecter à l'une des deux appliances NetScaler que vous souhaitez configurer pour la haute disponibilité, puis ajoutez un nœud. Spécifiez l'adresse IP NetScaler (NSIP) de l'autre appliance comme adresse du nouveau nœud. Ensuite, connectez-vous à l'autre appliance et ajoutez un nœud qui possède l'adresse NSIP du premier dispositif. Un algorithme détermine quel nœud devient principal et lequel devient secondaire.

La figure suivante montre une configuration HA simple, dans laquelle les deux nœuds se trouvent dans le même sous-réseau.

Figure 1. Deux appliances NetScaler connectées dans une configuration haute disponibilité



Étapes pour configurer la haute disponibilité

La configuration d'une paire haute disponibilité composée de deux appliances NetScaler comprend les tâches suivantes sur les deux appliances :

- **Ajoutez un nœud**. Sur une appliance, disons N1, ajoutez l'autre appliance, disons N2, en spécifiant un ID de nœud unique et l'adresse NSIP de l'appliance (N2). Vous pouvez spécifier n'importe quel entier compris entre 1 et 64 pour l'ID du nœud homologue.

  L'ID du nœud homologue spécifié sur le nœud autonome s'applique uniquement au nœud autonome et n'a aucune pertinence sur le nœud homologue. Par exemple, vous avez ajouté N2 en tant que nœud homologue sur N1 et spécifié l'ID du nœud 33 pour N2. Le paramètre 33 de l'ID de nœud du N2 n'est applicable que sur N1 et n'a aucun effet sur la configuration de N2.

  L'ID du nœud homologue, spécifié sur les deux nœuds, n'a pas besoin d'être de la même valeur et peut être modifié. Sur les deux nœuds, l'identifiant du nœud autonome est codé en dur à zéro et ne peut pas être modifié.

- **Désactivez le moniteur HA pour les interfaces non utilisées**. Sur le nœud autonome, vous devez désactiver le moniteur HA pour chaque interface qui n'est pas connectée ou qui n'est pas utilisée pour le trafic. La désactivation du moniteur HA pour les interfaces non utilisées empêche

tout basculement HA provoqué lorsque l'une de ces interfaces inutilisées devient INACTIVE.

> **Remarque** :
>
> Pour vous assurer que chaque nœud de la configuration haute disponibilité possède les mêmes paramètres, vous devez synchroniser vos certificats SSL, scripts de démarrage et autres fichiers de configuration avec ceux du nœud principal.

Procédures CLI

Pour configurer une paire haute disponibilité de deux appliances NetScaler à l'aide de l'interface de ligne de commande, effectuez les tâches suivantes sur chacune des deux appliances :

Pour ajouter un nœud à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `add ha node <id> <IPAddress>`
- `show ha node`

Pour désactiver le moniteur HA pour une interface non utilisée à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

- `set interface <ifNum> [-haMonitor ( ON | OFF )]`
- `show interface <ifNum>`

Exemple :

```
> add ha node 33 203.0.113.33

> set interface 1/3 -haMonitor OFF
 Done
<!--NeedCopy-->
```

Procédure GUI

L'interface graphique de NetScaler fournit un écran qui combine les tâches consistant à ajouter un nœud homologue et à désactiver le moniteur HA sur les interfaces non utilisées du nœud autonome. L'écran propose également une option permettant de configurer automatiquement le nœud homologue pour la configuration HA, évitant ainsi d'avoir à configurer manuellement le nœud homologue.

Pour configurer une paire de deux appliances NetScaler à haute disponibilité à l'aide de l'interface graphique :

1. Connectez-vous à l'interface graphique de l'une des appliances.

2. Accédez à **Système** > **Haute disponibilité** > **Nœuds**, puis saisissez l'adresse NSIP du nœud homologue dans le champ **Adresse IP du nœud distant** .
3. Sélectionnez **Désactiver l'interface/les canaux du moniteur HA qui sont en panne**.
4. Sélectionnez **Configurer le système distant pour participer à la configuration de la haute disponibilité** et fournissez les informations de connexion du nœud homologue.
5. Cliquez sur **Create**.

Désactivation ou activation d'un nœud

Vous pouvez désactiver ou activer uniquement un nœud secondaire. Lorsque vous désactivez un nœud secondaire, il arrête d'envoyer des messages de pulsation au nœud principal et, par conséquent, le nœud principal ne peut plus vérifier l'état du nœud secondaire. Lorsque vous activez un nœud, ce dernier participe à la configuration de haute disponibilité.

Pour désactiver ou activer un nœud à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes :

- `set ha node -hastatus DISABLED`
- `set ha node -hastatus ENABLED`

Pour désactiver ou activer un nœud à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ouvrez le nœud.
2. Dans la liste **État de haute disponibilité**, sélectionnez **ACTIVÉ (Participer activement à la haute disponibilité)** ou **DÉSACTIVÉ (Ne pas participer à la haute disponibilité)**.

Configuration des intervalles de communication

March 9, 2023

L'intervalle Hello est l'intervalle auquel les messages de pulsation sont envoyés au nœud homologue. L'intervalle mort est l'intervalle de temps après lequel le nœud homologue est marqué en panne si les paquets de pulsation ne sont pas reçus. Les messages de pulsation sont des paquets UDP envoyés au port 3003 de l'autre nœud d'une paire HA. L'intervalle mort doit être défini comme un multiple de l'intervalle Hello. Par défaut, l'intervalle Hello est défini sur 200 millisecondes et l'intervalle mort est défini sur 3 secondes.

Pour définir les intervalles Hello et Dead à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

- `set HA node [-helloInterval <msecs>] [-deadInterval <secs>]`
- `show HA node <id>`

Pour définir les intervalles Hello et Dead à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ouvrez le nœud.
2. Définissez les paramètres suivants :
    - Intervalle de bonjour (msecs)
    - Intervalle mort (secondes)

Configuration de la synchronisation

July 31, 2023

La synchronisation est un processus de duplication de la configuration du nœud principal sur le nœud secondaire. L'objectif de la synchronisation est de garantir l'absence de perte d'informations de configuration entre les nœuds principal et secondaire, quel que soit le nombre de basculements qui se produisent. La synchronisation utilise le port UDP 3010.

La synchronisation est déclenchée par l'une des circonstances suivantes :

- Le nœud secondaire d'une configuration HA apparaît après un redémarrage.
- Le nœud principal devient secondaire après un basculement.

La synchronisation automatique est activée par défaut. Vous pouvez également forcer la synchronisation.

> **Remarque :**
>
> La propagation des commandes est désactivée lors de la synchronisation HA afin d'éviter tout conflit entre les paramètres de commande, ce qui peut entraîner un échec de la propagation des commandes.

Désactivation ou activation de la synchronisation

La synchronisation HA automatique est activée par défaut sur chaque nœud d'une paire HA. Vous pouvez l'activer ou le désactiver sur l'un ou l'autre nœud.

Pour désactiver ou activer la synchronisation automatique à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `set HA node -haSync DISABLED`
- `set HA node -haSync ENABLED`

Pour désactiver ou activer la synchronisation à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** .
2. Sous Synchronisation HA, effacez ou sélectionnez le nœud secondaire pour récupérer la configuration à partir de l'option principale.

Forcer le nœud secondaire à se synchroniser avec le nœud principal

Outre la synchronisation automatique, NetScaler prend en charge la synchronisation forcée. Vous pouvez forcer la synchronisation à partir du nœud principal ou secondaire. Lorsque vous forcez la synchronisation depuis le nœud secondaire, celui-ci commence à synchroniser sa configuration avec le nœud principal.

Toutefois, si la synchronisation est déjà en cours, la synchronisation forcée échoue et le système affiche un avertissement. La synchronisation forcée échoue également dans l'une des circonstances suivantes :

- Vous forcez la synchronisation sur un système autonome.
- Le nœud secondaire est désactivé.
- La synchronisation HA est désactivée sur le nœud secondaire.

Pour forcer la synchronisation à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
force HA sync
```

Pour forcer la synchronisation à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** .
2. Dans l'onglet **Nœuds**, dans la liste des actions, cliquez sur **Forcer la synchronisation**.

Synchronisation des fichiers de configuration dans une configuration haute disponibilité

October 5, 2021

Dans une configuration haute disponibilité, tous les fichiers de configuration sont synchronisés automatiquement du nœud principal vers le nœud secondaire à un intervalle d'une minute. La synchronisation des fichiers de configuration peut être effectuée manuellement à l'aide de l'interface de ligne de commande ou de l'interface graphique au niveau du nœud principal ou du nœud secondaire.

Les fichiers situés sur le secondaire qui sont spécifiques au secondaire (qui ne sont pas présents sur le serveur principal) ne sont pas supprimés pendant la synchronisation.

Pour synchroniser les fichiers dans une configuration haute disponibilité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
sync HA files <mode>
```

Exemple

```
1 > sync HA files all
2  Done
3 <!--NeedCopy-->
```

```
1 > sync HA files ssl
2  Done
3 <!--NeedCopy-->
```

Description des paramètres (de la commande répertoriée dans la procédure CLI)

```
sync ha files <mode>
```

```
mode
```

Spécifiez l'un des modes de synchronisation suivants.

- **all** - Synchronisez les fichiers liés à la configuration du système, aux signets Access Gateway, aux certificats SSL, aux listes de listes de certificats SSL et aux objets XML du pare-feu d'application.
- **signets** - Synchronisez tous les signets Access Gateway.
- **ssl** - Synchronisez tous les certificats, clés et CRL pour la fonctionnalité SSL.
- **importations** - Synchronisez tous les objets XML (par exemple, WSDL, schémas, pages d'erreur) configurés pour le pare-feu d'application.

- **misc** - Synchronise tous les fichiers de licence et le fichier rc.conf.
- **all_plus_misc** - Synchronise les fichiers liés à la configuration du système, aux signets Access Gateway, aux certificats SSL, aux listes de listes de certificats SSL, aux objets XML du pare-feu d'application, aux licences et au fichier rc.conf.

Pour synchroniser les fichiers dans une configuration haute disponibilité à l'aide de l'interface graphique

Accédez à **Système** > **Diagnostics** et, dans le groupe **Utilitaires**, cliquez sur **Démarrer la synchronisation des fichiers HA**.

Configuration de la propagation des commandes

July 31, 2023

Dans une configuration HA, toute commande émise sur le nœud principal se propage automatiquement vers le nœud secondaire et est exécutée sur celui-ci avant d'être exécutée sur le nœud principal. Si la propagation de la commande échoue, ou si l'exécution de la commande échoue sur le secondaire, le nœud principal exécute la commande et enregistre une erreur. La propagation des commandes utilise le port 3010.

Dans une configuration de paire HA, la propagation des commandes est activée par défaut sur les nœuds principal et secondaire. Vous pouvez activer ou désactiver la propagation des commandes sur l'un des nœuds d'une paire HA. Si vous désactivez la propagation des commandes sur le nœud principal, les commandes ne sont pas propagées vers le nœud secondaire. Si vous désactivez la propagation des commandes sur le nœud secondaire, les commandes propagées depuis le nœud principal ne sont pas exécutées sur le nœud secondaire.

> **Remarque**
>
> Après avoir réactivé la propagation, pensez à forcer la synchronisation.

Si la synchronisation se produit alors que vous désactivez la propagation, toutes les modifications liées à la configuration que vous apportez avant que la désactivation de la propagation ne prenne effet sont synchronisées avec le nœud secondaire. Cela est également vrai dans les cas où la propagation est désactivée alors que la synchronisation est en cours.

Pour désactiver ou activer la propagation des commandes à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- définir le nœud HA -HAProp DÉSACTIVÉ
- définir le nœud HA -HAProp ENABLED

Pour désactiver ou activer la propagation des commandes à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ouvrez le nœud.
2. Désactivez ou sélectionnez le nœud principal pour propager la configuration à l'option secondaire.

> **Remarque :**
>
> La propagation des commandes est désactivée lors de la synchronisation HA afin d'éviter tout conflit entre les paramètres de commande, ce qui peut entraîner un échec de la propagation des commandes.

Restreindre le trafic de synchronisation à haute disponibilité à un VLAN

May 5, 2023

Dans un déploiement à haute disponibilité (HA), le trafic lié à la maintenance de la configuration HA circule entre les deux nœuds HA. Ce trafic est du type suivant :

- Synchronisation des configurations
- Propagation des configurations
- Mise en miroir des connexions
- Synchronisation de la configuration de persistance de l'équilibrage de charge
- Synchronisation permanente des sessions
- Synchronisation des états de session

Le bon flux de ce trafic lié à la haute disponibilité entre les deux nœuds est essentiel au bon fonctionnement du déploiement de la haute disponibilité. Généralement, le volume du trafic lié à la haute disponibilité est faible mais peut devenir très élevé lors d'un basculement. Il devient très élevé si le basculement dynamique des connexions est activé et si le nœud qui était principal avant le basculement gérait un grand nombre de connexions.

Par défaut, le trafic lié à la HA passe par les VLAN auxquels l'adresse NSIP est liée. Pour faire face à une éventuelle augmentation de ce trafic, vous pouvez séparer le trafic lié à la haute disponibilité du trafic de gestion et restreindre son flux à un VLAN distinct. Ce VLAN est appelé HA SYNC VLAN.

Points à prendre en compte avant de configurer un VLAN HA SYNC

- La configuration d'un VLAN HA SYNC n'est ni propagée ni synchronisée. En d'autres termes, le VLAN HA SYNC est spécifique à un nœud et est configuré indépendamment sur chaque nœud.
- La configuration VLAN HA SYNC est supprimée lorsque vous effacez la configuration uniquement en mode FULL.
- HA MON doit être réglé sur OFF pour les interfaces qui font partie du VLAN HA SYNC, afin d'éviter que les deux nœuds fonctionnent en tant que nœud principal.
- Les interfaces de gestion (par exemple, 0/1 et 0/2) ne doivent pas faire partie du VLAN HA SYNC, afin que le trafic lié à la HA ne passe pas par les interfaces de gestion.
- Citrix recommande de désactiver les messages de pulsation de haute disponibilité sur les interfaces de gestion et de les activer sur les interfaces VLAN HA SYNC. Après avoir suivi ces recommandations, les messages de pulsation haute disponibilité peuvent également être activés sur les interfaces de données.

  Pour plus d'informations sur la désactivation des messages de pulsation de haute disponibilité sur les interfaces, consultez la section Gestion des messages de pulsation de haute disponibilité sur une appliance NetScaler.

Pour configurer un VLAN HA SYNC sur un nœud NetScaler, spécifiez un VLAN configuré avec le paramètre HA SYNC VLAN de l'entité du nœud local.

Pour configurer un VLAN HA SYNC sur un nœud local à l'aide de la ligne de commande :

À l'invite de commande, tapez :

- `set ha node -syncvlan <VLANID>`
- `show node`

Description du paramètre :

syncvlan (Sync VLAN) - VLAN sur lequel le trafic lié à l'HA est envoyé. Cela inclut le trafic pour la synchronisation, la propagation, la mise en miroir des connexions, la persistance de l'équilibrage de charge, la synchronisation de configuration, la synchronisation de session persistante et la synchronisation de l'état de session. Cependant, les battements de cœur HA peuvent utiliser n'importe quelle interface.

Pour configurer un VLAN HA SYNC sur un nœud à l'aide de l'interface graphique :

1. Accédez à **Système** > **Haute disponibilité** .
2. Définissez le paramètre **Sync VLAN** lors de la modification du nœud local.

Configuration du mode de sécurité intégrée

January 21, 2021

Dans une configuration HA, le mode de sécurité intégrée garantit qu'un nœud est toujours principal lorsque les deux nœuds échouent le contrôle de santé. Ceci permet de s'assurer que lorsqu'un nœud n'est que partiellement disponible, les méthodes de sauvegarde sont activées pour gérer le trafic le plus possible. Le mode HA fail-safe est configuré indépendamment sur chaque nœud.

Le tableau suivant présente certains des cas de sécurité intégrée. L'état NOT_UP signifie que le nœud a échoué à la vérification de l'état mais qu'il est partiellement disponible. L'état UP signifie que le nœud a passé le contrôle d'intégrité.

État d'intégrité du nœud A (principal)	État d'intégrité du nœud B (secondaire)	Comportement HA par défaut	Comportement HA activé pour la sécurité intégrée	Description
NOT_UP (dernier échec)	NOT_UP (premier échec)	A (Secondaire), B (Secondaire)	A (Principal), B (Secondaire)	Si les deux nœuds échouent, l'un après l'autre, le dernier nœud principal reste principal.
NOT_UP (premier échec)	NOT_UP (dernier échec)	A (Secondaire), B (Secondaire)	A (Secondaire), B (Principal)	Si les deux nœuds échouent, l'un après l'autre, le dernier nœud principal reste principal.
UP	UP	A (Principal), B (Secondaire)	A (Principal), B (Secondaire)	Si les deux nœuds réussissent la vérification de l'état, aucun changement de comportement avec fail-safe activé.

État d'intégrité du nœud A (principal)	État d'intégrité du nœud B (secondaire)	Comportement HA par défaut	Comportement HA activé pour la sécurité intégrée	Description
UP	NOT_UP	A (primaire), B (secondaire)	A (Principal), B (Secondaire)	Si seul le nœud secondaire échoue, aucun changement de comportement avec fail-safe activé.
NOT_UP	UP	A (Secondaire), B (Principal)	A (Secondaire), B (Principal)	Si seul le principal échoue, aucun changement de comportement avec fail-safe activé.
NOT_UP	UP (STAYSEC-ONDARY)	A (Secondaire), B (Secondaire)	A (Principal), B (Secondaire)	Si le secondaire est configuré comme STAY-SECONDARY, le primaire reste principal même en cas d'échec.

Pour activer le mode de sécurité à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set HA node [-failSafe ( **ON** | **OFF** )]
```

Exemple

```
1 set ha node -failsafe ON
2 <!--NeedCopy-->
```

Pour activer le mode de sécurité intégrée à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, ouvrez le nœud.

2. Sous **Mode sans échec**, sélectionnez l'option **Maintenir un nœud principal**même lorsque les deux nœuds ne sont pas sains.

Configuration des adresses MAC virtuelles

May 5, 2023

Une adresse MAC virtuelle est une entité flottante partagée par les nœuds principal et secondaire dans une configuration HA.

Dans une configuration HA, le nœud principal possède toutes les adresses IP flottantes, telles que les MIP, les SNIP et les VIP. Le nœud principal répond aux demandes ARP (Address Resolution Protocol) pour ces adresses IP avec sa propre adresse MAC. En conséquence, la table ARP d'un périphérique externe (par exemple, un routeur en amont) est mise à jour avec l'adresse IP flottante et l'adresse MAC du nœud principal.

Lorsqu'un basculement se produit, le nœud secondaire prend le relais en tant que nouveau nœud principal. Il utilise ensuite l'ARP gratuit (GARP) pour annoncer les adresses IP flottantes qu'il a acquises auprès du principal. Cependant, l'adresse MAC annoncée par le nouveau serveur principal est l'adresse MAC de sa propre interface.

Certains appareils (notamment quelques routeurs) n'acceptent pas les messages GARP générés par l'appliance NetScaler. Par conséquent, certains périphériques externes conservent l'ancien mappage IP vers MAC annoncé par l'ancien nœud principal. Cela peut entraîner la fermeture d'un site.

Vous pouvez résoudre ce problème en configurant un MAC virtuel sur les deux nœuds d'une paire HA. Les deux nœuds possèdent alors des adresses MAC identiques. Par conséquent, en cas de basculement, l'adresse MAC du nœud secondaire reste inchangée et les tables ARP des périphériques externes n'ont pas besoin d'être mises à jour.

Pour créer un MAC virtuel, vous devez d'abord créer un ID de routeur virtuel (VRID) et le lier à une interface. (Dans une configuration HA, vous devez lier le VRID aux interfaces des deux nœuds.) Une fois que le VRID est lié à une interface, le système génère un MAC virtuel avec le VRID comme dernier octet.

Cette section comprend les détails suivants :

- Configuration de Mac virtuels IPv4
- Configuration de Mac6 virtuels IPv6

Configuration de Mac virtuels IPv4

Lorsque vous créez une adresse MAC virtuelle IPv4 et que vous la liez à une interface, tout paquet IPv4 envoyé depuis l'interface utilise l'adresse MAC virtuelle liée à l'interface. Si aucune adresse MAC

virtuelle IPv4 n'est liée à une interface, l'adresse MAC physique de l'interface est utilisée.

Le MAC virtuel générique est de la forme `00:00:5e:00:01:<VRID>`. Par exemple, si vous créez un VRID avec une valeur de 60 et que vous le liez à une interface, le MAC virtuel obtenu est 00:00:5 e : 00:01:3 c, où 3c est la représentation hexadécimale du VRID. Vous pouvez créer 255 VRID avec des valeurs comprises entre 1 et 255.

Création ou modification d'un MAC virtuel IPv4

Vous créez un MAC virtuel IPv4 en lui attribuant un ID de routeur virtuel. Vous pouvez ensuite lier le MAC virtuel à une interface. Vous ne pouvez pas lier plusieurs VRID à la même interface. Pour vérifier la configuration du MAC virtuel, vous devez afficher et examiner les MAC virtuels et les interfaces liées aux MAC virtuels.

Pour ajouter un MAC virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `add vrID`
- `bind vrid <id> -ifnum <interface_name>`
- `show vrID`

Exemple

```
1 > add vrID 100
2  Done
3 > bind vrid 100 -ifnum 1/1 1/2 1/3
4  Done
5 <!--NeedCopy-->
```

Pour dissocier les interfaces d'un MAC virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `unbind vrid <id> -ifnum <interface_name>`
- `show vrID`

Pour configurer un MAC virtuel à l'aide de l'interface graphique

Accédez à **Système** > **Réseau** > **VMAC** et, dans l'onglet **VMAC**, ajoutez un nouveau MAC virtuel ou modifiez un MAC virtuel existant.

Supprimer un MAC virtuel IPv4

Pour supprimer un MAC virtuel IPv4, vous devez supprimer l'ID de son routeur virtuel.

Pour supprimer un MAC virtuel IPv4 à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm vrid <id>
```

Exemple

```
1 rm vrid 100s
2 <!--NeedCopy-->
```

Pour supprimer un MAC virtuel IPv4 à l'aide de l'interface graphique

Accédez à **Système** > **Réseau** > **VMAC** et, dans l'onglet **VMAC**, supprimez le MAC virtuel IPv4.

Configuration de Mac6 virtuels IPv6

NetScaler prend en charge le MAC6 virtuel pour les paquets IPv6. Vous pouvez lier n'importe quelle interface à un MAC6 virtuel, même si un MAC virtuel IPv4 est lié à l'interface. Tout paquet IPv6 envoyé depuis l'interface utilise le MAC6 virtuel lié à cette interface. S'il n'y a pas de MAC6 virtuel lié à une interface, un paquet IPv6 utilise le MAC physique.

Création ou modification d'un MAC6 virtuel

Vous créez un MAC virtuel IPv6 en lui attribuant un ID de routeur virtuel IPv6. Vous pouvez ensuite lier le MAC virtuel à une interface. Vous ne pouvez pas lier plusieurs VRID IPv6 à une interface. Pour vérifier la configuration des MAC6 virtuels, vous devez afficher et examiner les Mac6 virtuels et les interfaces liées aux Mac6 virtuels.

Pour ajouter un MAC6 virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `add vrID6 <id>`
- `bind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

Exemple


```
> add vrID6 100
Done
> bind vrID6 100 -ifnum 1/1 1/2 1/3
 Done
<!--NeedCopy-->
```

Pour dissocier les interfaces d'un MAC6 virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `unbind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

Pour configurer un MAC6 virtuel à l'aide de l'interface graphique

Accédez à **Système** > **Réseau** > **VMAC** et, dans l'onglet **VMAC6**, ajoutez un nouveau MAC6 virtuel ou modifiez un MAC6 virtuel existant.

Supprimer un MAC6 virtuel

Pour supprimer un MAC virtuel IPv4, vous devez supprimer l'ID de son routeur virtuel.

Pour supprimer un MAC6 virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

`rm vrid6 <id>`

Exemple

```
rm vrid6 100s
<!--NeedCopy-->
```

Pour supprimer un MAC6 virtuel à l'aide de l'interface graphique

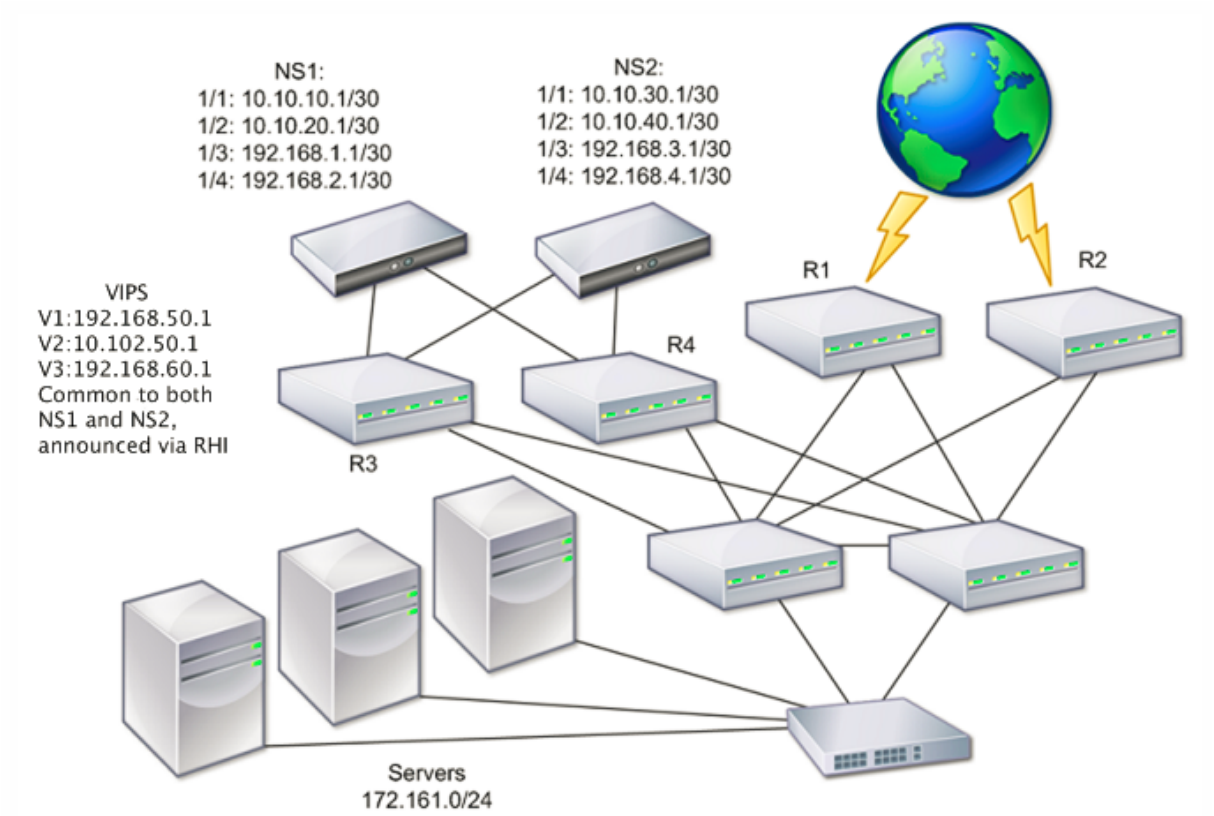
Accédez à **Système** > **Réseau** > **VMAC** et, dans l'onglet **VMAC6**, supprimez l'ID du routeur virtuel.

Configuration de nœuds haute disponibilité dans différents sous-réseaux

May 5, 2023

La figure suivante montre un déploiement HA avec les deux systèmes situés dans des sous-réseaux différents :

Figure 1. Haute disponibilité sur un réseau routé



Dans la figure, les systèmes NS1 et NS2 sont connectés à deux routeurs distincts, R3 et R4, sur deux sous-réseaux différents. Les appliances NetScaler échangent des paquets de pulsations via les routeurs. Cette configuration peut être étendue pour prendre en charge des déploiements impliquant un nombre quelconque d'interfaces.

> **Remarque** :
>
> Si vous utilisez un routage statique sur votre réseau, vous devez ajouter des routes statiques entre tous les systèmes pour garantir que les paquets Heartbeat sont envoyés et reçus correctement. (Si vous utilisez le routage dynamique sur vos systèmes, les itinéraires statiques ne sont pas nécessaires.)

Si les nœuds d'une paire HA résident sur deux réseaux distincts, le nœud principal et le nœud secondaire doivent avoir des configurations réseau indépendantes. Cela signifie que les nœuds de différents réseaux ne peuvent pas partager des entités telles que l'adresse SNIP, les VLAN et les routes. Ce type de configuration, dans lequel les nœuds d'une paire HA ont des paramètres configurables différents, est connu sous le nom de configuration réseau indépendante (INC) ou de configuration réseau symétrique (SNC).

Le tableau suivant récapitule les entités et les options configurables pour un INC et montre comment elles doivent être définies sur chaque nœud.

Entités NetScaler	Options
IP (NSIP/Snips)	Spécifique au nœud. Actif uniquement sur ce nœud.
VIP	flottant.
VLAN	Spécifique au nœud. Actif uniquement sur ce nœud.
Itinéraires	Spécifique au nœud. Actif uniquement sur ce nœud. Les itinéraires d'équilibrage de charge des liens sont flottants.
ACL	Flottant (fréquent). Actif sur les deux nœuds.
Routage dynamique	Spécifique au nœud. Actif uniquement sur ce nœud. Le nœud secondaire doit également exécuter les protocoles de routage et s'associer aux routeurs en amont.
Mode L2	Flottant (fréquent). Actif sur les deux nœuds.
Mode L3	Flottant (fréquent). Actif sur les deux nœuds.
NAT inverse (RNAT)	Configuration RNAT avec l'adresse IP NAT définie sur une adresse IP du serveur virtuel (VIP) car l'adresse VIP est flottante (commune).

Comme pour configurer des nœuds HA dans le même sous-réseau, pour configurer des nœuds HA dans différents sous-réseaux, vous vous connectez à chacune des deux appliances NetScaler et ajoutez un nœud distant représentant l'autre appliance.

Ajout d'un nœud distant

Lorsque deux nœuds d'une paire HA résident sur des sous-réseaux différents, chaque nœud doit avoir une configuration réseau différente. Par conséquent, pour configurer deux systèmes indépendants afin qu'ils fonctionnent comme une paire HA, vous devez spécifier le mode INC pendant le processus de configuration.

Lorsque vous ajoutez un nœud HA, vous devez désactiver le moniteur HA pour chaque interface qui n'est pas connectée ou qui n'est pas utilisée pour le trafic. Pour les utilisateurs de la CLI, il s'agit d'une procédure distincte.

Pour ajouter un nœud à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `add ha node <id> <IPAddress> -inc ENABLED`
- `show ha node`

Exemple

```
1 > add ha node 3 10.102.29.170 -inc ENABLED
2  Done
3 > add ha node 3 1000:0000:0000:0000:0005:0600:700a:888b
4   Done
5 <!--NeedCopy-->
```

Pour désactiver un moniteur HA à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `set interface <ifNum> [-haMonitor ( **ON** | **OFF** )]`
- `show interface <ifNum>`

Exemple

```
1 > set interface 1/3 -haMonitor OFF
2  Done
3 <!--NeedCopy-->
```

Pour ajouter un nœud distant à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, dans l'onglet **Nœuds**, ajoutez un nouveau nœud distant.
2. Assurez-vous de sélectionner Désactiver le moniteur HA sur les interfaces/canaux inactifs et d'activer le mode INC (Independent Network Configuration) sur les options du mode automatique.

Suppression d'un nœud

Si vous supprimez un nœud, les nœuds ne sont plus configurés en haute disponibilité.

Pour supprimer un nœud à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :


```
rm ha node <id>
```

Exemple

```
1 > rm ha node 2
2   Done
3 <!--NeedCopy-->
```

Pour supprimer un nœud à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, dans l'onglet **Nœuds**, supprimez le nœud.

> **Remarque** :
>
> Vous pouvez utiliser le Network Visualizer pour afficher les appliances NetScaler configurées en tant que paire haute disponibilité (HA) et effectuer des tâches de configuration de haute disponibilité.

Configuration des moniteurs de routage

May 5, 2023

Vous pouvez utiliser des moniteurs de routage pour faire dépendre l'état HA de la table de routage interne, que la table contienne ou non des routes apprises dynamiquement ou statiques. Dans une configuration HA, un moniteur de routage sur chaque nœud surveille la table de routage interne pour s'assurer qu'une entrée de route permettant d'atteindre un réseau particulier est toujours présente. Si l'entrée de route n'est pas présente, l'état du moniteur de route passe à BAS.

Lorsqu'une appliance NetScaler ne possède que des routes statiques pour atteindre un réseau et que vous souhaitez créer un moniteur de routage pour le réseau, vous devez activer les routes statiques surveillées (MSR) pour les routes statiques. MSR supprime les routes statiques inaccessibles de la table de routage interne. Si MSR est désactivé sur les routes statiques, une route statique inaccessible peut rester dans la table de routage interne, ce qui va à l'encontre de l'objectif du moniteur d'itinéraires.

Les moniteurs de route sont pris en charge à la fois en mode non INC et en mode INC.

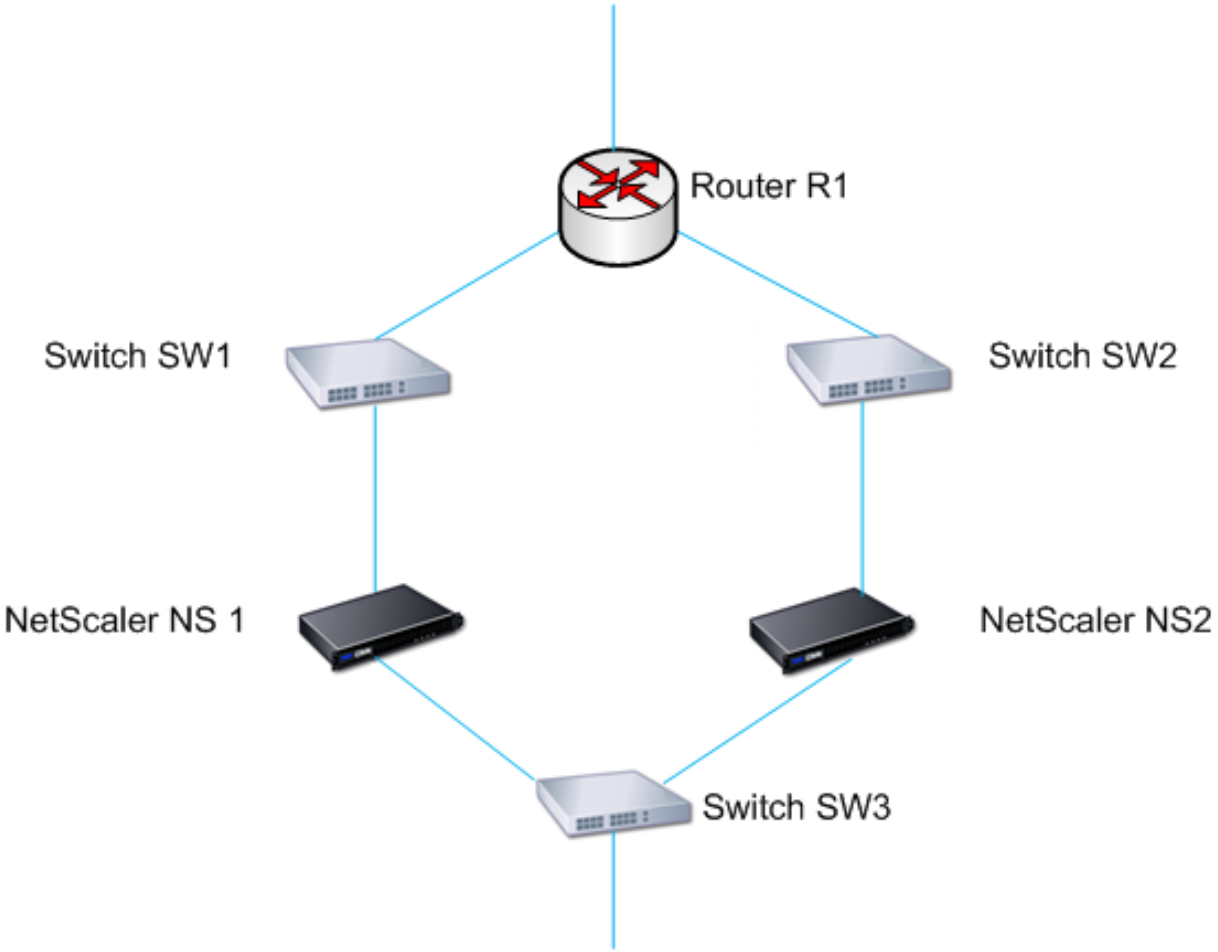
Moniteurs de routage en mode HA en mode non INC	Moniteurs de routage en mode HA en mode INC
Les moniteurs d'itinéraires sont propagés par les nœuds et échangés au cours de la synchronisation.	Les moniteurs d'itinéraires ne sont ni propagés par les nœuds ni échangés pendant la synchronisation.
Les moniteurs de routage ne sont actifs que dans le nœud principal actuel.	Les moniteurs de routage sont actifs sur le nœud principal et le nœud secondaire.
L'appliance NetScaler affiche toujours l'état d'un moniteur de routage comme étant ouvert, que l'entrée de route soit présente ou non dans la table de routage interne.	L'appliance NetScaler affiche l'état du moniteur de routage comme étant inactif si l'entrée de route correspondante n'est pas présente dans la table de routage interne.
Un moniteur de route commence à surveiller son itinéraire au bout de 180 secondes dans les cas suivants [Ceci est fait pour permettre l'apprentissage des itinéraires dynamiques, ce qui peut prendre 180 secondes] : redémarrage, basculement, commande set route6 pour les itinéraires v6, commande set route msr enable/disable pour les itinéraires v4, ajout d'un nouveau moniteur de route.	-

Les moniteurs de routage sont utiles dans une configuration HA sans mode INC où vous souhaitez que l'inaccessibilité d'une passerelle depuis un nœud principal soit l'une des conditions du basculement HA.

Prenons l'exemple d'une configuration HA sans mode INC dans une topologie à deux bras comportant des appliances NetScaler NS1 et NS2 dans le même sous-réseau, avec le routeur R1 et les commutateurs SW1, SW2 et SW3.

Étant donné que R1 est le seul routeur de cette configuration, vous souhaitez que la configuration HA bascule chaque fois que R1 n'est pas accessible depuis le nœud principal actuel. Vous pouvez configurer un moniteur d'itinéraire (par exemple, RM1 et RM2, respectivement) sur chacun des nœuds pour surveiller l'accessibilité de R1 à partir de ce nœud.

Figure 1.



Avec NS1 comme nœud principal actuel, le flux d'exécution est le suivant :

1. Le moniteur de routage RM1 sur NS1 surveille la table de routage interne de NS1 pour détecter la présence d'une entrée de route pour le routeur R1. NS1 et NS2 échangent des messages de pulsation via le commutateur SW1 ou SW3 à intervalles réguliers.
2. Si le commutateur SW1 tombe en panne, le protocole de routage sur NS1 détecte que R1 n'est pas accessible et supprime donc l'entrée de route pour R1 de la table de routage interne. NS1 et NS2 échangent des messages de pulsation via le commutateur SW3 à intervalles réguliers.
3. En détectant que l'entrée de route pour R1 n'est pas présente dans la table de routage interne, RM1 lance un basculement. Si la route vers R1 est interrompue à la fois depuis NS1 et NS2, le basculement se produit toutes les 180 secondes jusqu'à ce que l'une des appliances puisse atteindre R1 et rétablir la connectivité.

Ajouter un moniteur de routage à un nœud de haute disponibilité

Une procédure unique crée un moniteur de routage et le lie à un nœud HA.

Pour ajouter un moniteur d'itinéraire à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `bind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- `show HA node`

Exemple

```
1 > bind HA node 0 -routeMonitor 10.102.71.0 255.255.255.0
2  Done
3 > bind HA node 0 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
4  Done
5 <!--NeedCopy-->
```

Pour ajouter un moniteur d'itinéraire à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, dans l'onglet **Routes Monitors**, cliquez sur **Configurer**.

Supprimer les moniteurs d'itinéraires

Pour supprimer un moniteur de routage à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `unbind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- afficher un nœud ha

Exemple

```
1 unbind HA node 3 -routeMonitor 10.102.71.0 255.255.255.0
2 unbind HA node 3 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
3 <!--NeedCopy-->
```

Pour supprimer un moniteur d'itinéraires à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, dans l'onglet **Moniteurs d'itinéraires**, supprimez le moniteur d'itinéraires.

Limiter les basculements provoqués par les contrôleurs de routage en mode non INC

May 5, 2023

Dans une configuration HA en mode non-INC, si les contrôleurs de route échouent sur les deux nœuds, le basculement se produit toutes les 180 secondes jusqu'à ce que l'un des nœuds soit en mesure d'atteindre toutes les routes surveillées par les contrôleurs de route respectifs.

Toutefois, pour un nœud, vous pouvez limiter le nombre de basculements pour un intervalle donné en définissant les paramètres Nombre maximum de retournements et Temps de retournement maximum sur les nœuds. Lorsque l'une des limites est atteinte, aucun basculement ne se produit et le nœud est désigné comme principal (mais l'état du nœud est NOT UP) même en cas de défaillance d'un moniteur de routage sur ce nœud. Cette combinaison de l'état HA en tant que principal et de l'état du nœud en tant que NOT UP est appelée état principal du Stick.

Si le nœud est alors en mesure d'atteindre toutes les routes surveillées, la prochaine défaillance du moniteur déclenche la réinitialisation des paramètres Nombre maximum de retournements et Temps de retournement maximal sur le nœud et le début de l'heure spécifiée dans le paramètre Temps de retournement maximal.

Ces paramètres sont définis indépendamment sur chaque nœud et ne sont donc ni propagés ni synchronisés.

Paramètres permettant de limiter le nombre de basculements

- **Nombre maximum de retournements (MaxFlips)**

  Nombre maximum de basculements autorisés, dans l'intervalle de temps de basculement maximal, pour le nœud en mode HA en mode non INC, si les basculements sont provoqués par une défaillance du moniteur de routage.

- **Temps de retournement maximal (MaxFlipTime)**

  Durée, en secondes, pendant laquelle les basculements résultant d'une défaillance du moniteur de routage sont autorisés pour le nœud en mode HA en mode non INC.

Pour limiter le nombre de basculements à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `set HA node [-maxFlips < positive_integer>] [-maxFlipTime <positive_integer >]`
- `show HA node [< id>]`

Pour limiter le nombre de basculements à l'aide de l'interface graphique

1. Accédez à **Système** > **Haute disponibilité** et, dans l'onglet **Nœuds**, ouvrez le nœud local.
2. Définissez les paramètres suivants :

- Nombre maximum de retournements
- Temps de retournement maximal

```
1      > set ha node -maxFlips 30 -maxFlipTime 60
```



```
    Done
    > sh ha node
    1) Node ID: 0
    IP: 10.102.169.82 (NS)
    Node State: UP
    Master State: Primary
    Fail-Safe Mode: OFF
    INC State: DISABLED
    Sync State: ENABLED
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    Interfaces on which heartbeats are not seen :None
    Interfaces causing Partial Failure:None
    SSL Card Status: NOT PRESENT
    Hello Interval: 200 msecs
    Dead Interval: 3 secs
    Node in this Master State for: 0:4:24:1 (days:hrs:min:sec)

    2) Node ID: 1
    IP: 10.102.169.81
    Node State: UP
    Master State: Secondary
    Fail-Safe Mode: OFF
    INC State: DISABLED
    Sync State: SUCCESS
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    Interfaces on which heartbeats are not seen : None
    Interfaces causing Partial Failure: None
    SSL Card Status: NOT PRESENT

    Local node information:
    Configured/Completed Flips: 30/0
    Configured Flip Time: 60
    Critical Interfaces: 1/1

    Done
<!--NeedCopy-->
```


Alarme SNMP pour Sticky Primary State

Activez l'alarme SNMP HA-STICKY-PRIMARY sur un nœud configuré en haute disponibilité si vous souhaitez être averti si le nœud devient un nœud principal permanent. Lorsque le nœud devient autocollant principal, il alerte en générant un message d'interruption (stickyPrimary (1.3.6.1.4.1.5951.1.1.0.138)) et l'envoie à toutes les destinations d'interruption SNMP configurées. Pour plus d'informations sur la configuration des alarmes SNMP et des destinations des interruptions, consultez Configuration de NetScaler pour générer des interruptionsSNMPv1 et SNMPv2.

Questions fréquemment posées

Prenons l'exemple d'une configuration haute disponibilité de deux appliances NetScaler NS-1 et NS-2 en mode non-INC. Le nombre maximum de retournements et le temps de retournement maximum dans les deux nœuds ont été définis avec les mêmes valeurs.

Le tableau suivant répertorie les paramètres utilisés dans cet exemple :

Entité	Détail
Adresse IP du NS-1	10.102.173.211
Adresse IP du NS-2	10.102.173.212
Nombre maximum de retournements	2
Temps de retournement maximal	200

Pour plus d'informations sur le nombre maximal de basculement et les paramètres de temps de retournement maximum, reportez-vous au pdf.

Configuration de l'ensemble d'interfaces de basculement

May 5, 2023

Un ensemble d'interfaces de basculement (FIS) est un groupe logique d'interfaces. Dans une configuration HA, l'utilisation d'un FIS est un moyen d'empêcher le basculement en regroupant les interfaces de sorte que, lorsqu'une interface échoue, d'autres interfaces fonctionnelles soient toujours disponibles. Un FIS peut également être configuré pour les nœuds d'un cluster NetScaler.

Les interfaces HA MON qui ne sont pas liées à un FIS sont appelées interfaces critiques (CI) car en cas de défaillance de l'une d'entre elles, le basculement est déclenché.

> **Remarque** :
>
> Un FIS ne crée pas de configuration active et de secours. Il n'empêche pas non plus de pontage des boucles lors de la connexion à des liens vers le même VLAN.

Création ou modification d'une SIF

Pour ajouter un FIS et y lier des interfaces à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `add fis <name>`
- `bind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Exemple

```
1 > add fis fis1
2  Done
3 > bind fis fis1 1/3 1/5
4  Done
5 <!--NeedCopy-->
```

Une interface indépendante devient une interface critique (CI) si elle est activée et que HA MON est activé.

Pour dissocier une interface d'un FIS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `unbind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Exemple

```
1 > unbind fis fis1 1/3
2  Done
3 <!--NeedCopy-->
```

Pour configurer un FIS à l'aide de l'interface graphique

Accédez à Système > Haute disponibilité et, dans l'onglet Failover Interface Set, ajoutez un nouveau FIS ou modifiez un FIS existant.

Supprimer un FIS

Lorsque le FIS est supprimé, ses interfaces sont marquées comme des interfaces critiques.

Pour supprimer un FIS à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
rm fis <name>
```

Exemple

```
1 > rm fis fis1
2   Done
3 <!--NeedCopy-->
```

Pour supprimer un FIS à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité** et, dans l'onglet **Failover Interface Set**, supprimez le FIS.

Comprendre les causes du basculement

September 8, 2021

Les événements suivants peuvent entraîner un basculement sur incident dans une configuration haute disponibilité :

1. Si le nœud secondaire ne reçoit pas de paquet de pulsation du cœur principal pendant une période qui dépasse l'intervalle mort défini sur le secondaire. (Voir la note 1.)
2. Le nœud principal rencontre une défaillance matérielle de sa carte SSL.
3. Le nœud principal ne reçoit aucun paquet de rythme cardiaque sur ses interfaces réseau pendant trois secondes.
4. Sur le nœud principal, une interface réseau qui ne fait pas partie d'un ensemble d'interface de basculement (FIS) ou d'un canal d'agrégation de liens (LA) et dont le moniteur HA (HAMON) est activé échoue. (Voir la note 2.)
5. Sur le nœud principal, toutes les interfaces d'un FIS échouent. (Voir la note 2.)
6. Sur le nœud principal, un canal LA avec HAMON activé échoue. (Voir la note 2.)
7. Sur le nœud principal, toutes les interfaces échouent (voir la note 2). Dans ce cas, le basculement se produit indépendamment de la configuration HAMON.
8. Sur le nœud principal, toutes les interfaces sont désactivées manuellement. Dans ce cas, le basculement se produit indépendamment de la configuration HAMON.

9. Vous forcez un basculement en émettant la commande forcer le basculement sur l'un ou l'autre des nœuds.
10. Un moniteur de routage lié au nœud principal est en panne.

> **Remarque 1 :**
>
> Pour plus d'informations sur la définition de l'intervalle mort, voir Configuration des intervalles de communication. Les causes possibles pour un nœud ne recevant pas de paquets de pulsations d'un nœud homologue sont les suivantes :
>
> - Un problème de configuration réseau empêche les battements de cœur de traverser le réseau entre les nœuds HA.
> - Le nœud homologue rencontre une défaillance matérielle ou logicielle qui provoque le blocage (blocage), le redémarrage ou l'arrêt du traitement et du transfert des paquets Heartbeat.
>
> **Remarque 2 :**
>
> Dans ce cas, échouer signifie que l'interface a été activée mais passe à l'état DOWN, comme le montre la commande show interface ou depuis l'interface graphique. Les causes possibles de l'état DOWN d'une interface activée sont LINK DOWN et TXSTALL.

Forcer le basculement d'un nœud

May 5, 2023

Vous souhaiterez peut-être forcer un basculement si, par exemple, vous devez remplacer ou mettre à niveau le nœud principal. Vous pouvez forcer le basculement à partir du nœud principal ou du nœud secondaire. Un basculement forcé n'est ni propagé ni synchronisé. Pour afficher l'état de la synchronisation après un basculement forcé, vous pouvez afficher l'état du nœud.

Un basculement forcé échoue dans l'une des circonstances suivantes :

- Vous forcez le basculement sur un système autonome.
- Le nœud secondaire est désactivé.
- Le nœud secondaire est configuré pour rester secondaire.

L'appliance NetScaler affiche un message d'avertissement si elle détecte un problème potentiel lorsque vous exécutez la commande de basculement forcé. Le message inclut les informations qui ont déclenché l'avertissement et demande une confirmation avant de continuer.

Vous pouvez forcer un basculement sur un nœud principal, un nœud secondaire et lorsque les nœuds sont en mode écoute.

- **Forcer le basculement sur le nœud principal**.

Si vous forcez le basculement sur le nœud principal, le nœud principal devient le nœud secondaire et le secondaire devient le nœud principal. Le basculement forcé n'est possible que lorsque le nœud principal peut déterminer que le nœud secondaire est actif.

Si le nœud secondaire est en panne, la commande Forcer le basculement renvoie le message d'erreur suivant : « Opération impossible en raison d'un état de pair non valide. Rectifier et réessayer."

Si le système secondaire est dans l'état revendiquant ou inactif, il renvoie le message d'erreur suivant :

```
Operation not possible now. Please wait for the system to stabilize
before retrying.
```

- **Forcer le basculement sur incident sur le nœud secondaire**.

  Si vous exécutez la commande forcer le basculement à partir du nœud secondaire, le nœud secondaire devient principal et le nœud principal devient secondaire. Un basculement forcé ne peut se produire que si la santé du nœud secondaire est bonne et qu'il n'est pas configuré pour rester secondaire.

  Si le nœud secondaire ne peut pas devenir le nœud principal ou si le nœud secondaire a été configuré pour rester secondaire (à l'aide de l'option STAYSECONDARY), le nœud affiche le message d'erreur suivant :

  ```
  Operation not possible as my state is invalid. View the node for more
  information.
  ```

- **Forcer le basculement lorsque les nœuds sont en mode écoute**.

  Lorsque les deux nœuds d'une paire HA exécutent des versions différentes du logiciel système, le nœud exécutant la version supérieure passe en mode écoute. Dans ce mode, ni la propagation des commandes ni la synchronisation ne fonctionnent.

  Avant de mettre à niveau le logiciel système sur les deux nœuds, testez la nouvelle version sur l'un des nœuds. Pour ce faire, vous devez forcer un basculement sur le système déjà mis à niveau. Le système mis à niveau prend alors le relais en tant que nœud principal, mais aucune propagation ou synchronisation des commandes n'a lieu. De plus, toutes les connexions doivent être rétablies.

> **Important !**
>
> Si vous forcez un basculement lorsqu'une opération de synchronisation HA est en cours, certaines sessions de données actives sur la configuration HA peuvent être perdues. Attendez donc que l'opération de synchronisation HA soit terminée avant d'effectuer l'opération de basculement de force.

Pour forcer le basculement sur un nœud à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
force HA failover
```

Pour forcer le basculement sur un nœud à l'aide de l'interface graphique :

Accédez à **Système** > **Haute disponibilité** et, sous l'onglet **Nœuds**, sélectionnez le nœud, dans la liste Action, sélectionnez **Forcer le basculement**.

Forcer le nœud secondaire à rester secondaire

August 20, 2021

Dans une configuration HA, le nœud secondaire peut être forcé de rester secondaire quel que soit l'état du nœud principal.

Par exemple, supposons que le nœud principal doit être mis à niveau et que le processus prendra quelques secondes. Pendant la mise à niveau, le nœud principal peut s'arrêter pendant quelques secondes, mais vous ne voulez pas que le nœud secondaire prenne le relais ; vous voulez qu'il reste le nœud secondaire même s'il détecte une défaillance dans le nœud principal.

Lorsque vous forcez le nœud secondaire à rester secondaire, il restera secondaire même si le nœud principal tombe en panne. En outre, lorsque vous forcez l'état d'un nœud dans une paire HA à rester secondaire, il ne participe pas aux transitions de machines d'état HA. L'état du nœud est affiché en tant que STAYSECONDARY.

Forcer le nœud à rester secondaire fonctionne à la fois sur les nœuds autonomes et secondaires. Sur un nœud autonome, vous devez utiliser cette option avant de pouvoir ajouter un nœud pour créer une paire HA. Lorsque vous ajoutez le nouveau nœud, le nœud existant arrête le traitement du trafic et devient le nœud secondaire. Le nouveau nœud devient le nœud principal.

> **Remarque** :
>
> Lorsque vous forcez un système à rester secondaire, le processus de forçage n'est ni propagé ni synchronisé. Elle affecte uniquement le nœud sur lequel vous exécutez la commande.

Pour forcer le nœud secondaire à rester secondaire à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ha node -hastatus STAYSECONDARY
```


Pour forcer le nœud secondaire à rester secondaire à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité**, sous l'onglet **Nœuds**, ouvrez le nœud local, puis sélectionnez **STAY SECONDARY**.

Forcer le nœud principal à rester principal

August 20, 2021

Dans une configuration HA, vous pouvez forcer un nœud principal sain à rester principal même après un basculement. Vous pouvez activer cette option soit sur un nœud principal d'une paire HA. Cette option permet au nœud principal d'être en état principal tant qu'il est sain.

Sur un nœud autonome, vous devez utiliser cette option avant de pouvoir ajouter un nœud pour créer une paire HA. Lorsque vous ajoutez le nouveau nœud, le nœud existant continue à fonctionner en tant que nœud principal, et le nouveau nœud devient le nœud secondaire.

Pour forcer le nœud principal à rester principal à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ha node -hastatus STAYPRIMARY
```

Pour forcer le nœud principal à rester principal à l'aide de l'interface graphique

Accédez à **Système** > **Haute disponibilité**, sous l'onglet **Nœuds**, ouvrez le nœud local, puis sélectionnez **STAY PRIMARY**.

Comprendre le calcul de la vérification de l'état de haute disponibilité

January 21, 2021

Le tableau suivant résume les facteurs examinés dans le calcul d'un bilan de santé :

- État des jeux d'interface de basculement
- État des interfaces critiques
- État des moniteurs de route

Le tableau suivant récapitule le calcul de la vérification de l'état.

Jeux d'interface de basculement	Interfaces critiques	Moniteur de routage	Condition
N	O	N	Si le système possède des interfaces critiques, toutes ces interfaces critiques doivent être UP.
O	O	N	Si le système possède des jeux d'interface de basculement, tous ces jeux d'interface de basculement doivent être UP.
O	O	O	Si des moniteurs de routage sont configurés sur le système, toutes les routes surveillées doivent être présentes dans l'interface de basculement définie.

FAQ sur la haute disponibilité

May 5, 2023

1. Quels sont les différents ports utilisés pour échanger les informations relatives à la HA entre les nœuds d'une configuration HA ?

   Dans une configuration HA, les deux nœuds utilisent les ports suivants pour échanger des informations relatives à HA :

   - Port UDP 3003, pour échanger des paquets de pulsations.
   - Port 3010, pour la synchronisation et la propagation des commandes.

2. Quelles sont les conditions qui déclenchent la synchronisation ?

   La synchronisation est déclenchée par l'une des conditions suivantes :

- Le numéro d'incarnation du nœud principal, reçu par le nœud secondaire, ne correspond pas à celui du nœud secondaire.
  Remarque : Les deux nœuds d'une configuration HA conservent un compteur appelé *numéro d'incarnation*, qui compte le nombre de configurations dans le fichier de configuration du nœud. Chaque nœud envoie son numéro d'incarnation à l'autre nœud dans les messages de pulsation. Le numéro d'incarnation n'est pas incrémenté pour les commandes suivantes :
  a) Toutes les commandes associées à la configuration HA. Par exemple, ajoutez un nœud ha, définissez un nœud ha et liez un nœud ha.
  b) Toutes les commandes liées à l'interface. Par exemple, définissez l'interface et désinstallez l'interface.
  c) Toutes les commandes liées au canal. Par exemple, add channel, set channel et bind channel.
- Le nœud secondaire s'active après un redémarrage.
- Le nœud principal devient secondaire après un basculement.

3. Quelles configurations ne sont pas synchronisées ou propagées dans une configuration HA en mode INC ou non ?

   Les commandes suivantes ne sont ni propagées ni synchronisées avec le nœud secondaire :

   - Toutes les commandes de configuration HA spécifiques au nœud. Par exemple, ajoutez un nœud ha, définissez un nœud ha et liez un nœud ha.
   - Toutes les commandes de configuration liées à l'interface. Par exemple, définissez l'interface et désinstallez l'interface.
   - Toutes les commandes de configuration relatives aux canaux. Par exemple, add channel, set channel et bind channel.

   > **Remarque :**
   >
   > Les configurations suivantes ne sont ni synchronisées ni propagées uniquement en mode HA en mode INC. Chaque nœud possède ses propres nœuds :
   >
   > - SNIP
   > - VLAN
   > - Itinéraires (sauf les itinéraires LLB)
   > - Moniteurs d'itinéraires
   > - Règles RNAT (à l'exception de toute règle RNAT avec VIP comme adresse IP NAT)
   > - Configurations de routage dynamique
   > - Profils de réseau

4. Une configuration ajoutée au nœud secondaire est-elle synchronisée sur le nœud principal ?

   Non, une configuration ajoutée au nœud secondaire n'est pas synchronisée avec le nœud principal.

5. Quelle pourrait être la raison pour laquelle les deux nœuds prétendent être les principaux dans une configuration HA ?

   La raison la plus probable est que les nœuds primaire et secondaire sont tous les deux sains, mais que le secondaire ne reçoit pas les paquets de pulsations du primaire. Le problème vient peut-être du réseau entre les nœuds.

6. Une configuration HA se heurte-t-elle à des problèmes si vous déployez les deux nœuds avec des paramètres d'horloge système différents ?

   Des paramètres d'horloge système différents sur les deux nœuds peuvent provoquer les problèmes suivants :

   - Les horodatages figurant dans les entrées du fichier journal ne correspondent pas. Cette situation rend difficile l'analyse des entrées du journal pour détecter d'éventuels problèmes.
   - Après un basculement, vous pouvez rencontrer des problèmes avec tout type de persistance basée sur des cookies pour l'équilibrage de charge. Une différence significative entre les heures peut entraîner l'expiration d'un cookie plus tôt que prévu, ce qui entraîne la fin de la session de persistance.
   - Des considérations similaires s'appliquent à toute décision liée au temps sur les nœuds.

7. Quelles sont les conditions de défaillance de la commande *force HA sync* ?

   La synchronisation forcée échoue dans l'une des circonstances suivantes :

   - Vous forcez la synchronisation lorsqu'elle est déjà en cours.
   - Vous forcez la synchronisation sur une appliance NetScaler autonome.
   - Le nœud secondaire est désactivé.
   - La synchronisation HA est désactivée sur le nœud secondaire actuel.
   - La propagation HA est désactivée sur le nœud principal actuel et vous forcez la synchronisation depuis le nœud principal.

8. Quelles sont les conditions d'échec de la commande *synchroniser les fichiers HA* ?

   La synchronisation des fichiers de configuration échoue dans l'un des cas suivants :

   - Sur un système autonome.
   - Avec le nœud secondaire désactivé.

9. Dans une configuration HA, si le nœud secondaire devient le nœud principal, revient-il à l'état secondaire si le nœud principal d'origine revient en ligne ?

   Non. Une fois que le nœud secondaire a pris le relais en tant que nœud principal, il le reste même si le nœud principal d'origine est de nouveau en ligne. Pour échanger les états principal et secondaire des nœuds, exécutez la commande *force failover* .

10. Quelles sont les conditions de l'échec de la commande de basculement des forces ?

Un basculement forcé échoue dans l'une des circonstances suivantes :

- Vous forcez le basculement sur un système autonome.
- Le nœud secondaire est désactivé.
- Le nœud secondaire est configuré pour rester secondaire.
- Le nœud principal est configuré pour rester principal.
- L'état du nœud homologue est inconnu.

Résolution des problèmes de haute disponibilité

May 5, 2023

Les problèmes de haute disponibilité les plus courants concernent le fait que la fonctionnalité de haute disponibilité ne fonctionne pas du tout ou ne fonctionne que de façon intermittente. Vous trouverez ci-dessous les problèmes de haute disponibilité courants ainsi que leurs causes probables et leurs solutions.

- **Problème**
  L'incapacité des appliances NetScaler à coupler les appliances NetScaler dans une configuration à haute disponibilité.
  - **Cause**
    Connectivité réseau
    Résolution
    Vérifiez que les deux dispositifs sont connectés au commutateur et que les interfaces sont activées.
  - **Cause**
    Le mot de passe du compte administrateur par défaut ne correspond pas
    Résolution
    Vérifiez que le mot de passe des deux appliances est identique.
  - **Cause**
    Conflit de propriété intellectuelle
    Résolution
    Vérifiez que les deux appliances possèdent une adresse IP NetScaler (NSIP) unique. Les appliances ne doivent pas avoir la même adresse NSIP.
  - **Cause**
    Incompatibilité d'ID de nœud
    Résolution
    Vérifiez que la configuration de l'ID de nœud sur les deux appliances est unique. Les appliances ne doivent pas avoir la même configuration d'ID de nœud. En outre, vous devez attribuer une valeur comprise entre 1 et 64 pour un ID de nœud.

- **Cause**
  Incompatibilité du mot de passe du nœud RPC
  Résolution
  Vérifiez que les deux nœuds ont le même mot de passe de nœud RPC.
- **Cause**
  Un administrateur a désactivé le nœud distant
  Résolution
  Activez le nœud distant.
- **Cause**
  L'application Firewall a bloqué les paquets de pulsations
  Résolution

Vérifiez que le port UDP 3003 est autorisé.

- **Problème**
  Les deux appliances prétendent être l'appliance principale.
  - **Cause**
    Paquets de pulsations cardiaques manquants entre les appliances
    Résolution
    Vérifiez que le port UDP 3003 n'est pas bloqué pour la communication entre les appliances.
- **Problème**
  L'appliance NetScaler n'est pas en mesure de synchroniser la configuration.
  - **Cause**
    Une application de pare-feu bloque le port requis.
    Résolution
    Vérifiez que le port UDP 3010 (ou le port UDP 3008 avec synchronisation sécurisée) n'est pas bloqué pour la communication entre les appliances.
  - **Cause**
    Un administrateur a désactivé la synchronisation.
    Résolution
    Activez la synchronisation sur l'appliance qui présente le problème.
  - **Cause**
    Différentes versions ou versions de NetScaler sont installées sur les appliances.
    Résolution
    Mettez à niveau les appliances vers la même version ou build de NetScaler.
- **Problème**
  La propagation des commandes échoue entre les appliances.
  - **Cause**
    Une application de pare-feu bloque le port.
    Résolution
    Vérifiez que le port UDP 3011 (ou le port UDP 3009 avec propagation sécurisée) n'est pas

bloqué pour la communication entre les appliances.

- **Cause**
  Un administrateur a désactivé la propagation des commandes.
  Résolution
  Activez la propagation des commandes sur l'appliance qui présente le problème.
- **Cause**
  Différentes versions ou versions de NetScaler sont installées sur les appliances.
  Résolution
  Mettez à niveau les appliances vers la même version ou build de NetScaler.

- **Problème**
  Les appliances NetScaler de la paire haute disponibilité ne sont pas en mesure d'exécuter le processus de basculement forcé.
  - **Cause**
    Le nœud secondaire est désactivé.
    Résolution
    Activez le nœud secondaire.
  - **Cause**
    Le nœud secondaire est configuré pour rester secondaire.
    Résolution
    Définissez l'état de haute disponibilité secondaire du nœud secondaire sur Activer depuis Stay Secondary.
- **Problème**
  L'appliance secondaire ne reçoit aucun trafic après le processus de basculement.
  - **Cause**
    Le routeur en amont ne comprend pas les messages GARP de l'appliance NetScaler.
    Résolution
    Configurez l'adresse MAC virtuelle sur l'appliance secondaire.

Gestion des messages de pulsation de haute disponibilité sur une appliance NetScaler

May 5, 2023

Les deux nœuds d'une configuration haute disponibilité envoient et reçoivent des messages de pulsation l'un vers l'autre et en provenance de ceux-ci sur toutes les interfaces activées. Les messages de pulsation circulent quel que soit le paramètre HA MON sur ces interfaces. Si NSVLAN ou les deux (NSVLAN et SYNC) sont configurés sur une appliance, les messages de pulsation circulent uniquement via les interfaces activées qui font partie du NSVLAN et du SYNCVLAN.

Si un nœud ne reçoit pas les messages de pulsation sur une interface activée, il envoie des alertes critiques aux gestionnaires SNMP spécifiés. Ces alertes critiques déclenchent de fausses alarmes et attirent inutilement l'attention des administrateurs pour les interfaces qui ne sont pas configurées dans le cadre des connexions au nœud homologue.

Pour résoudre ce problème, l'option HAHeartbeat pour les interfaces et les canaux est utilisée pour activer ou désactiver le flux de messages de pulsation HA sur ceux-ci.

Pour gérer les messages de pulsation haute disponibilité sur une interface à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `set interface <ID> [-HAHeartBeat ( ON | OFF )]`
- `show interface <ID>`

Pour gérer les messages de pulsation haute disponibilité sur un canal à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

- `set channel <ID> [-HAHeartBeat ( ON | OFF )]`
- `show channel <ID>`

Pour gérer les messages de pulsation haute disponibilité pour une interface à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Interfaces**.
2. Activez ou désactivez le paramètre **HA Heart Beat** .

Pour gérer les messages de pulsation haute disponibilité sur un canal à l'aide de l'interface graphique

1. Accédez à **Système** > **Réseau** > **Canaux**.
2. Activez ou désactivez le paramètre **HA Heart Beat** .

Supprimer et remplacer un NetScaler dans une configuration de haute disponibilité

May 5, 2023

Cette rubrique vous aide à aborder les remplacements RMA. Cette rubrique contient également des instructions sur la façon de sauvegarder les configurations, de mettre à niveau ou de rétrograder la version logicielle fournie et de configurer le mot de passe RPC sur ADC.

Points à prendre en compte

Les configurations suivantes ne sont ni synchronisées ni propagées dans une configuration haute disponibilité en mode INC (Independent Network Configuration) ou non INC :

- Toutes les commandes de configuration HA spécifiques au nœud. Par exemple, ajoutez un nœud ha, définissez un nœud ha et liez un nœud ha.
- Toutes les commandes de configuration liées à l'interface. Par exemple, définissez l'interface et désinstallez l'interface.
- Toutes les commandes de configuration relatives aux canaux. Par exemple, add channel, set channel et bind channel.
- Toutes les commandes de configuration de Interface HA Monitoring.

Les configurations suivantes ne sont ni synchronisées ni propagées dans une configuration HA en mode INC (Independent Network Configuration) :

- SNIP
- VLAN
- Itinéraires (sauf les itinéraires LLB)
- Moniteurs d'itinéraires
- Règles RNAT (à l'exception de toute règle RNAT avec VIP comme adresse IP NAT)
- Configurations de routage dynamique

Instructions

Procédez comme suit pour remplacer un NetScaler dans une configuration de haute disponibilité :

- Supprimer un nœud secondaire NetScaler actif
- Configurer le nœud secondaire de remplacement
- Vérifiez et mettez à jour la version logicielle sur un ADC de remplacement
- Définir le mot de passe du nouveau secondaire comme correspondant au mot de passe principal
- Ajouter des licences à un ADC de remplacement
- Création d'une paire HA entre le nœud principal et le nouveau nœud secondaire

Supprimer un nœud secondaire actif

1. Ouvrez une session sur les deux ADC et exécutez la commande suivante pour confirmer quel nœud est principal et quel nœud est secondaire :

```
show ha node
<!--NeedCopy-->
```


2. Ouvrez une session sur l'ADC principal, sauvegardez les configurations sur le nœud principal et copiez les fichiers hors de l'ADC avant les modifications. Ces fichiers se trouvent dans le répertoire « /var /ns_sys_backup/ ».

   Les étapes sont les suivantes :

   a) Enregistrez les configurations en cours d'exécution de l'ADC dans la mémoire :

   ```
   save ns config
   <!--NeedCopy-->
   ```

   b) Créez le package de fichiers de sauvegarde complet :

   ```
   create system backup -level full
   <!--NeedCopy-->
   ```

   c) Créez le package de fichiers de sauvegarde de base :

   ```
   create system backup -level basic
   <!--NeedCopy-->
   ```

3. Une fois que tous les fichiers de sauvegarde ont été générés, veillez à les copier hors de l'appareil avant de continuer.

   À partir d'un terminal Windows, ouvrez une invite de commande et copiez les fichiers de sauvegarde de l'ADC vers votre disque dur local. Cela peut être fait à l'aide de la commande suivante :

   ```
   pscp <username>@<NSIP>:<Target file source>  <Target file
      destination>
   <!--NeedCopy-->
   ```

   Exemple :

   ```
   pscp nsroot@10.125.245.78:/var/ns_sys_backup/backup_basic_10
      .125.245.78_2016_09_14_15_08.tgz c:\nsbackup\backup_basic_10
      .125.245.78_2016_09_14_15_08.tgz
   <!--NeedCopy-->
   ```

   Lorsque vous y êtes invité, entrez le mot de passe du compte administrateur spécifié, puis appuyez sur Entrée. Répétez ces étapes jusqu'à ce que tous les bundles de sauvegarde soient copiés sur le PC local avant de continuer.

4. Connectez-vous via SSH à l'ADC secondaire et réglez l'unité sur l'état « STAYSECONDAIRE ». Cela obligera l'unité à ne pas tenter d'assumer le rôle principal en cas de défaillance détectée lors du remplacement. Vérifiez que vous êtes connecté à l'ADC secondaire avant d'exécuter cette étape


```
set ha node  -haStatus <state>
set ha node  -haStatus STAYSECONDARY
<!--NeedCopy-->
```

5. Une fois que l' **état du nœud** de l'ADC secondaire affiche correctement STAYSECONDAIRE, passez à l'ADC principal, supprimez le nœud secondaire et exécutez la commande suivante :

```
save ns config
<!--NeedCopy-->
```

Lorsque vous êtes connecté à l'ADC principal, exécutez les commandes suivantes

a) Exécutez la commande suivante pour identifier la valeur numérique qui représente le nœud HA secondaire :

```
show ha node
<!--NeedCopy-->
```

b) Exécutez la commande suivante pour supprimer l'ADC secondaire de la paire HA principale ;

```
rm ha node <node ID>
<!--NeedCopy-->
```

c) Exécutez la commande suivante pour enregistrer la configuration :

```
save ns config
<!--NeedCopy-->
```

d) Le CAN secondaire étant désormais retiré, arrêtez, déconnectez et retirez le CAN secondaire du réseau.

Remarque. Assurez-vous d'étiqueter toutes les connexions avant de les déconnecter.

Configurer le nœud secondaire de remplacement

1. Une fois l'ADC de remplacement en place, mettez le nouvel appareil sous tension. NE CONNECTEZ PAS les connexions réseau à ce stade.
2. Une fois le démarrage terminé, utilisez le port de console pour vous connecter à l'ADC et configurez le NSIP que vous utiliserez pour vous connecter à l'unité.
3. Lorsque vous y êtes invité, sélectionnez **4**.

Remarque. Dans cet exemple, nous utilisons un NSIP différent pour l'ADC de remplacement. Si vous souhaitez utiliser l'adresse IP de l'unité secondaire d'origine, vous pouvez la modifier sur l'unité de remplacement avant de lier le nouvel ADC à l'unité HA principale.

4. L'ADC doit maintenant être démarré. Connectez maintenant l'interface réseau qui sera utilisée pour le trafic de gestion et confirmez que l'adresse IP est accessible depuis votre réseau.

Vérifiez et mettez à jour la version logicielle sur un ADC de remplacement

Avant de synchroniser la nouvelle unité avec l'ADC principal, nous devons nous assurer que les deux ADC exécutent la même version.

1. Pour vérifier la version sur ADC, exécutez la commande suivante :

```
show version
<!--NeedCopy-->
```

2. Lorsque vous êtes sur le nouveà ADC secondaire, créez un sous-dossier dans **/var** à utiliser pour la mise à niveau.
3. Accédez aux téléchargements de NetScaler et téléchargez le package approprié qui correspond à la version de compilation exécutée sur l'ADC principal.
4. Téléchargez et extrayez le fichier .tgz :

```
tar -xvzf "file.tgz"
<!--NeedCopy-->
```

5. Copiez les fichiers extraits sur l'ADC secondaire. Sur votre terminal Windows, ouvrez une « invite de commande », accédez au répertoire contenant le package de construction .tgz extrait et exécutez la commande pscp suivante :

```
pscp <Target file source>  <username>@<NSIP>:<Target file
   destination>
<!--NeedCopy-->
```

Exemple :

```
C:\inetpub>pscp c:\inetpub\build-12.1-47.14_nc.tgz nsroot@10
   .20.245.80:/var/NS_upg_12.1_47.14/build-12.1-47.14_nc.tgz
<!--NeedCopy-->
```

6. Une fois le fichier transféré, revenez à ADC secondaire et mettez à niveau. Pour obtenir des instructions détaillées, reportez-vous à la section Mise à niveau d'une appliance Citrix ADX Standalone Appliance.

7. Une fois le nouveau secondaire redémarré, SSH revient dans l'unité et confirme que la mise à niveau est réussie et que la construction correspond à celle du primaire.

Définir le mot de passe du nœud secondaire de remplacement pour qu'il corresponde au nœud principal

Remarque : Si, à ce stade, vous souhaitez modifier l'adresse IP de gestion (NSIP) du nouvel ADC secondaire, vous pouvez le faire avant de poursuivre.

Modifiez le mot de passe du nouvel ADC secondaire pour qu'il corresponde au mot de passe qui se trouve actuellement sur le ADC principal.

1. Assurez-vous que le mot de passe du compte administrateur (nsroot) par défaut est identique à celui de l'ADC principal. Pour ce faire, utilisez la commande suivante lorsque vous êtes connecté via SSH à la nouvelle unité secondaire :

```
set system user <user> <password>
<!--NeedCopy-->
```

   Cette commande définir/réinitialise le mot de passe de l'utilisateur spécifié.

2. Connectez-vous via SSH à l'ADC principal et au nouvel ADC secondaire et confirmez que les mots de passe correspondent.

Ajouter des licences au nœud secondaire de remplacement

Une fois le nouvel ADC mis à jour et prêt à être couplé, téléchargez et installez la licence appropriée pour le nœud de remplacement.

1. Accédez à https://www.citrix.com pour demander et télécharger des licences pour la nouvelle unité de remplacement.
2. Une fois que vous avez téléchargé toutes les licences appropriées, accédez au nouvel ADC secondaire via SSH et tapez la commande suivante pour voir l'état actuel des licences :

```
show license
<!--NeedCopy-->
```

3. À partir de l'invite de commande du terminal Windows, vous devez désormais télécharger les fichiers de licence vers le nouvel ADC secondaire à l'aide de la commande suivante :

   Remarque. Si vous possédez plusieurs licences, répétez cette étape jusqu'à ce que toutes les licences soient chargées.

```
pscp <Target file source>  <username>@<NSIP>:<Target file
    destination>
```



```
<!--NeedCopy-->
```

Exemple :

```
C:\inetpub>pscp c:\inetpub\NS-VPX-3K-LIC-020030ad0024.lic
   nsroot@10.125.245.80:/nsconfig/license/NS-VPX-3K-LIC-020030
   ad0024.lic
<!--NeedCopy-->
```

4. Connectez-vous au nouvel ADC secondaire via SSH et effectuez un redémarrage à chaud à l'aide de la commande suivante :

```
reboot -w
<!--NeedCopy-->
```

Une fois l'unité redémarrée, ouvrez une session SSH dans l'unité et exécutez à nouveau la commande show license. À ce stade, les licences doivent être appliquées.

Configuration de la haute disponibilité entre le nœud principal et le nouveau nœud secondaire

À ce stade, nous sommes maintenant prêts à réunir les unités NetScaler pour former une paire de haute disponibilité. Pour plus d'informations, voir Configuration de la haute disponibilité.

Nouvelle tentative de demande

May 5, 2023

Lorsqu'une appliance NetScaler reçoit une requête HTTP mais rencontre un échec de connexion avec un serveur principal, elle utilise une directive de nouvelle tentative. La nouvelle tentative de demande résout les scénarios d'échec de connexion et permet à l'appliance de choisir le prochain service disponible et de transmettre la demande. En effectuant une nouvelle tentative de demande, le client peut gagner du temps aller-retour (RTT).

La fonction de demande de nouvelle tentative est applicable aux scénarios d'échec de connexion suivants :

- Si un serveur principal réinitialise une connexion TCP lorsqu'une demande HTTP est reçue. Pour plus de détails, voir Demander une nouvelle tentative.
- Si un serveur principal réinitialise une connexion TCP lors de l'établissement de la connexion. Pour plus de détails, voir Demander une nouvelle tentative.

- Si une réponse d'un serveur principal arrive à expiration (en fonction de la valeur de délai d'expiration configurée) lorsqu'une appliance envoie une demande HTTP. Pour plus de détails, voir Demander une nouvelle tentative.

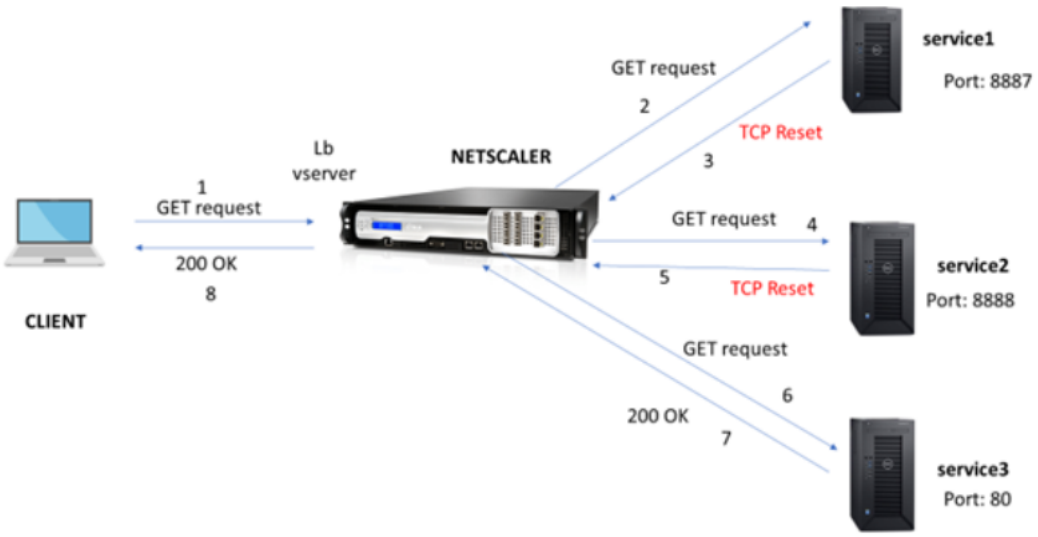
Demander une nouvelle tentative si le serveur principal réinitialise la connexion TCP

May 5, 2023

Lorsqu'un serveur principal réinitialise une connexion TCP, la fonction de nouvelle tentative de demande transmet la demande au serveur disponible suivant, au lieu d'envoyer la réinitialisation au client. En effectuant un équilibrage de recharge, le client enregistre le RTT lorsque l'appliance lance la même demande auprès du service disponible suivant.

Comment fonctionne une nouvelle tentative de demande lorsque le serveur principal réinitialise une connexion TCP

Le schéma suivant montre comment les composants interagissent les uns avec les autres.



1. Le processus commence par l'activation de la fonctionnalité Apqoe sur votre appliance.
2. Lorsque le client envoie une requête HTTP ou HTTPS, le serveur virtuel d'équilibrage de charge envoie la demande au serveur principal.
3. Si le service demandé n'est pas disponible, le serveur principal réinitialise la connexion TCP.

4. Si la « rétentative » est activée dans la configuration appqoe avec le nombre de tentatives souhaité spécifié, le serveur virtuel d'équilibrage de charge utilise l'algorithme d'équilibrage de charge configuré pour transmettre la demande au prochain serveur d'applications disponible.
5. Une fois que le serveur virtuel d'équilibrage de charge a reçu la réponse, l'appliance transmet la réponse au client.
6. Si le nombre de serveurs principaux disponibles est égal ou inférieur au nombre de nouvelles tentatives et si tous les serveurs envoient une réinitialisation, l'appliance répondra à une erreur interne de 500. Considérez un scénario avec cinq serveurs disponibles et le nombre de tentatives est défini sur six. Si les cinq serveurs réinitialisent la connexion, l'appliance renvoie une erreur de serveur interne 500 au client.
7. De même, si le nombre de serveurs principaux est supérieur au nombre de nouvelles tentatives et si les serveurs principaux réinitialisent la connexion, l'appliance transmet la réinitialisation au client. Considérez un scénario avec trois serveurs back-end et le nombre de tentatives est défini comme deux. Si les trois serveurs réinitialisent la connexion, l'appliance envoie une réponse de réinitialisation au client.

Configurer une nouvelle tentative de demande pour la méthode GET

Pour configurer la fonctionnalité de nouvelle tentative pour la méthode GET, vous devez suivre les étapes suivantes.

1. Activer AppQoE
2. Ajouter une action AppQoE
3. Ajouter une stratégie AppQoE
4. Liez la politique AppQoE au serveur virtuel d'équilibrage de charge

Activer AppQoE

À l'invite de commande, tapez :

```
enable ns feature appqoe
```

Ajouter une action AppQoE

Vous devez configurer une action AppQoE pour spécifier si vous souhaitez que l'appliance réessaie après une réinitialisation TCP et le nombre de tentatives.

```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Exemple :

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```


Où,
réessayez sur Réinitialiser. Activez une nouvelle tentative si le serveur principal réinitialise une connexion TCP.
chiffres. Réessayer le compte.

Ajouter une stratégie AppQoE

Pour implémenter AppQoE, vous devez configurer la politique AppQoE afin de hiérarchiser les requêtes HTTP ou SSL entrantes dans une file d'attente spécifique.

À l'invite de commande, tapez :

```
add appqoe policy <name> -rule <expression> -action <string>
```

Exemple :

```
add appqoe policy reset_policy -rule http.req.method.eq(get)-action reset_action
```

Lier la stratégie appqoe au serveur virtuel d'équilibrage de charge

Lorsqu'un serveur principal réinitialise une demande de paquets TCP et si vous souhaitez que le serveur virtuel d'équilibrage de charge transmette la demande au service disponible suivant, vous devez lier le serveur virtuel d'équilibrage de charge à la stratégie AppQoE.

À l'invite de commande, tapez :

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Exemple :

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```

Configurer la nouvelle tentative de demande pour les requêtes POST

Vous devez toujours faire preuve de prudence lorsque vous rechargez des demandes d'équilibrage qui écrivent des données sur le serveur principal. Pour de telles demandes, assurez-vous que la longueur du contenu est courte. Si la longueur du contenu est longue, cela peut entraîner une consommation de ressources. Suivez les étapes ci-dessous pour configurer l'équilibrage de charge pour les requêtes POST.

1. Activer AppQoE
2. Ajouter une action AppQoE
3. Ajouter une stratégie AppQoE
4. Liez la politique AppQoE au serveur virtuel d'équilibrage de charge

Activer AppQoE

À l'invite de commande, tapez :

```
enable ns feature appqoe
```

Ajouter une action Apple

Vous devez ajouter une action AppQoE pour réessayer après une réinitialisation TCP et le nombre de tentatives de nouvelle tentative.

```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Exemple :

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```

Ajouter une politique Apple

Pour implémenter AppQoE, vous devez configurer la politique AppQoE pour définir comment mettre en file d'attente les connexions dans une file d'attente spécifique.

À l'invite de commande, tapez :

```
add appqoe policy <name> -rule <expression> -action <string>
```

Exemple :

```
add appqoe policy reset_policy -rule HTTP.REQ.CONTENT_LENGTH.le(2000)-
action reset_action
```

> **Remarque :**
>
> Vous pouvez utiliser cette configuration si vous préférez restreindre la fonctionnalité de nouvelle tentative de demande pour un contenu d'une longueur inférieure à 2 000.

Lier le serveur virtuel d'équilibrage de charge à la stratégie AppQoE

Lorsqu'un serveur principal réinitialise une demande de paquet TCP et si vous souhaitez que le serveur virtuel d'équilibrage de charge transmette la demande au prochain service disponible via une file d'attente spécifique, vous devez lier le serveur virtuel d'équilibrage de charge à la politique AppQoE.

À l'invite de commande, tapez :

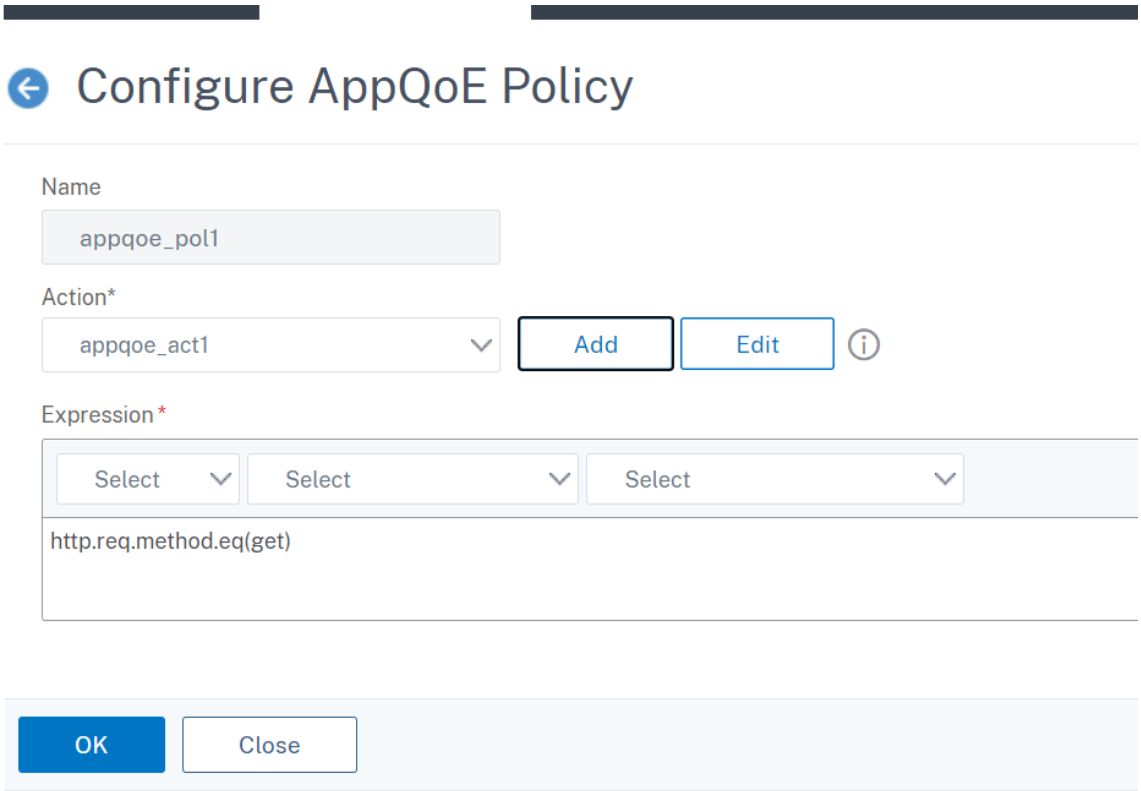
```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```


Exemple :

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```

Configurer la politique AppQoE pour une nouvelle tentative de demande à l'aide de l'interface graphique NetScaler

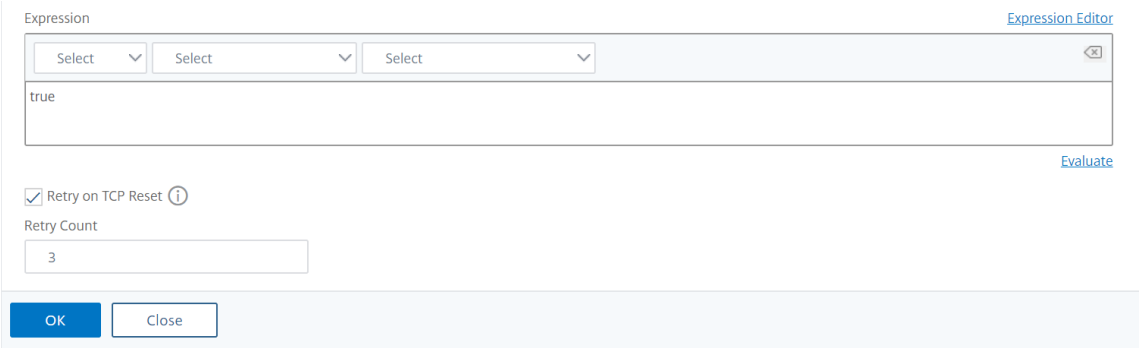
1. **Accédez à**AppExpert > **AppQoE**** > Politiques.**
2. **Sur la page**Politiques AppQoE**, cliquez sur Ajouter.**
3. Sur la page **Créer une politique AppQoE**, définissez les paramètres suivants : a. Nom. Nom de la politique AppQoE
   b. Action. Ajoutez ou modifiez une action. Pour créer une action, reportez-vous à la section .
   c. Expression : Sélectionnez ou saisissez une expression `HTTP.REQ.CONTENT_LENGTH.le(2000)` de politique.
4. Cliquez sur **Créer** et **Fermer**.



Configurer l'action AppQoE pour l'équilibrage des demandes entre les tentatives à l'aide de l'interface graphique NetScaler

1. **Accédez à**AppExpert**>**AppQoE**> Action.**

2. **Sur la page**AppQoE Actions**, cliquez sur Ajouter.**
3. Sur la page **Créer une action AppQoE**, définissez les paramètres suivants pour réessayer lors de la réinitialisation du protocole TCP : a.
   Réessayez lors de la réinitialisation du protocole TCP. Cochez la case pour activer l'action de nouvelle tentative de réinitialisation du protocole TCP.
   b. Nombre de nouvelles tentatives. Entrez le nombre de nouvelles tentatives.
4. Cliquez sur **Créer** et **Fermer**.



Configurer une nouvelle tentative de demande pour la méthode GET lorsque le serveur principal se réinitialise sur l'établissement TCP SYN

La configuration CLI et GUI est similaire aux étapes suivies pour la méthode GET. Pour plus d'informations, consultez la section Configurer la demande d'essai pour la méthode GET. lorsque le serveur principal réinitialise une section de connexion.

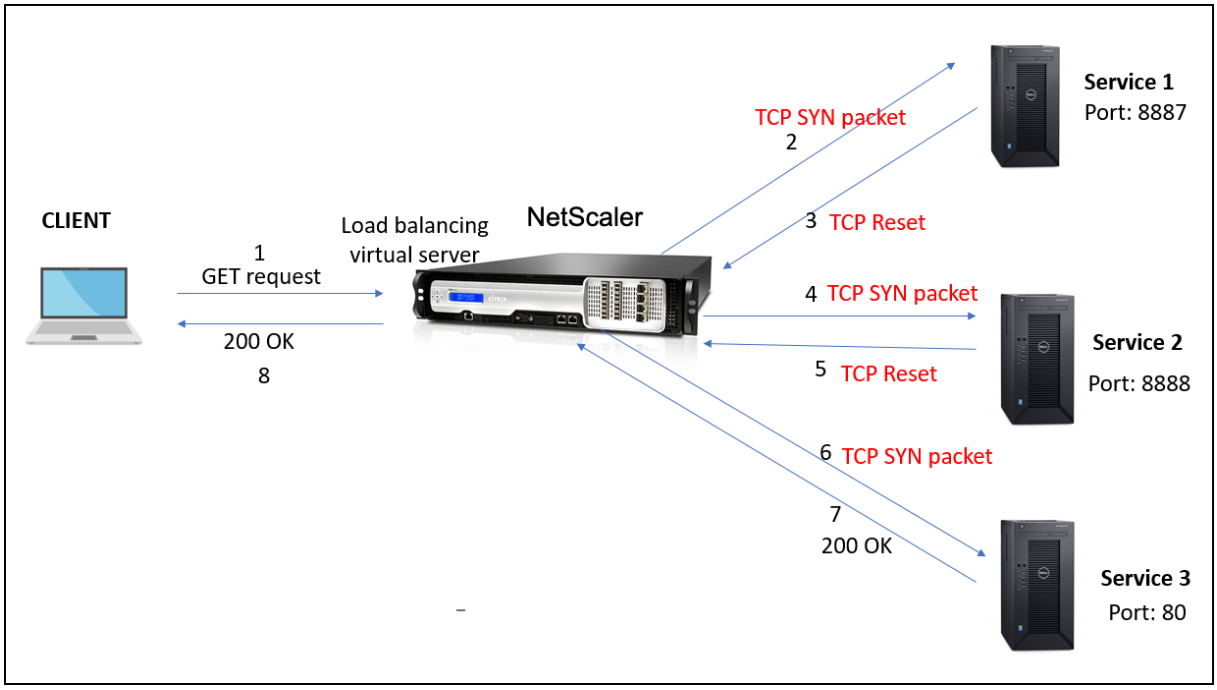
Demande de nouvelle tentative si le serveur principal réinitialise la connexion TCP pendant l'établissement de la connexion

August 20, 2021

Lorsqu'un serveur principal réinitialise une connexion TCP pendant l'établissement de la connexion, la fonction de nouvelle tentative de demande transmet la demande au serveur disponible suivant, au lieu d'envoyer la réinitialisation au client. En effectuant l'équilibrage de rechargement, le client enregistre RTT lorsque l'appliance lance la même demande au service disponible suivant.

Fonctionnement de la nouvelle tentative de demande lorsque le serveur principal réinitialise une connexion TCP sur l'établissement SYN

Le diagramme suivant montre les composants interagissent les uns avec les autres :



1. Le processus commence par activer la fonctionnalité appqoe sur votre appliance.
2. Lorsque le client envoie une requête HTTP ou HTTPS, le serveur virtuel d'équilibrage de charge initie la connexion au serveur principal.
3. Si le service demandé n'est pas disponible sur l'établissement TCP SYN, le serveur principal réinitialise la connexion TCP.
4. Si la configuration appqoe est activée avec le nombre souhaité de tentatives de nouvelle tentative spécifié, le serveur virtuel d'équilibrage de charge utilise l'algorithme d'équilibrage de charge configuré pour transférer la demande au serveur d'applications disponible suivant.
5. Une fois que le serveur virtuel d'équilibrage de charge a reçu la réponse, l'appliance transmet la réponse au client.
6. Si les serveurs back-end disponibles sont égaux ou inférieurs au nombre de tentatives et si tous les serveurs envoient une réinitialisation, l'appliance répondra à une erreur interne de 500 serveurs. Considérez un scénario avec cinq serveurs disponibles et le nombre de tentatives est défini sur six. Si les cinq serveurs réinitialisent la connexion, l'appliance renvoie une erreur de serveur interne 500 au client.
7. De même, si le nombre de serveurs principaux est supérieur au nombre de nouvelles tentatives et si les serveurs back-end réinitialisent la connexion sur l'établissement TCP SYN, l'appliance transmet la réinitialisation au client. Considérez un scénario avec trois serveurs back-end et le nombre de tentatives est défini comme deux. Si les trois serveurs réinitialisent la connexion, l'appliance envoie un paquet de réinitialisation au client.

Configurer une nouvelle tentative de demande (méthode GET et POST) lors de la réinitialisation du serveur principal sur l'établissement TCP SYN

La configuration CLI et GUI est similaire aux étapes suivies pour les méthodes GET et POST. Pour plus d'informations, consultez la rubrique Configurer une nouvelle tentative de demande pour la méthode GET, Configurer une nouvelle tentative de demande pour la méthode POST lorsque le serveur principal réinitialise une section de connexion.

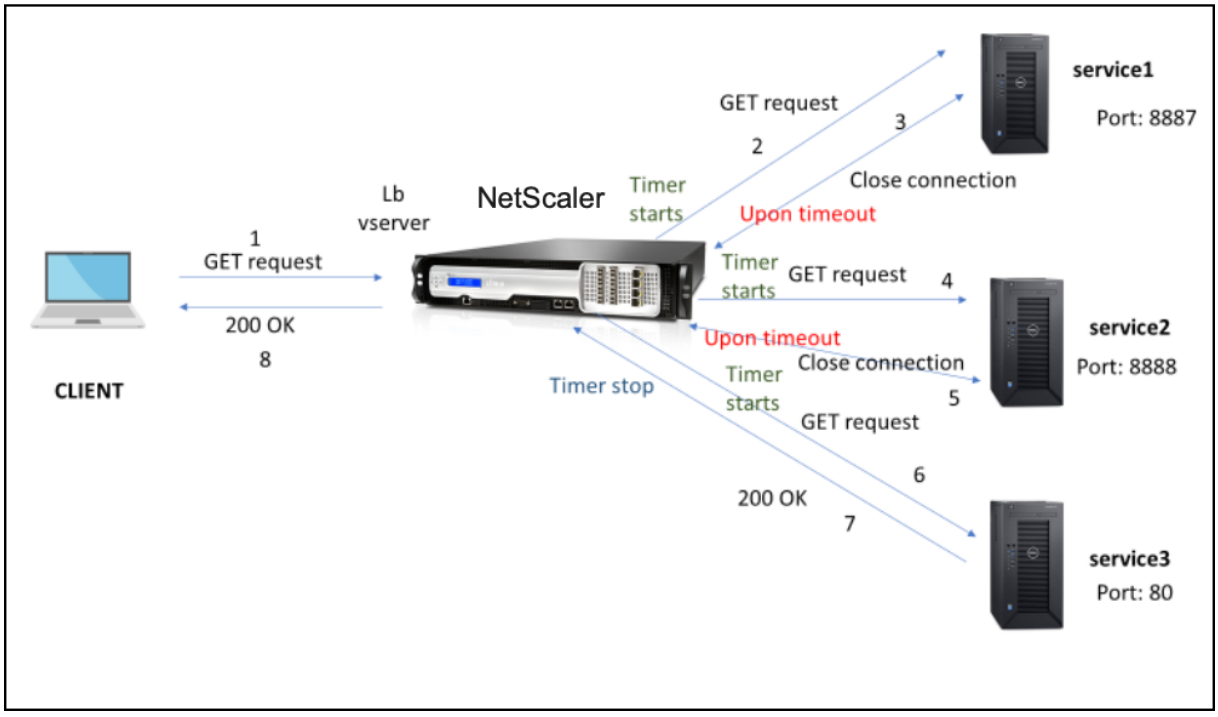
Demander une nouvelle tentative en cas d'expiration du délai de réponse du serveur principal

May 5, 2023

Une nouvelle tentative de demande est disponible pour un autre scénario dans lequel, si un serveur principal met plus de temps à répondre aux demandes, l'appliance effectue un équilibrage de charge en cas d'expiration du délai et transmet la demande au serveur disponible suivant.

Comment fonctionne une nouvelle tentative de demande lorsque le délai de réponse du serveur principal expire

Le schéma suivant montre les composants qui interagissent les uns avec les autres :



1. Le processus commence par l'activation de la fonctionnalité Apqoe sur votre appliance.

2. La configuration appqoe possède le paramètre « RetryOnTimeout » en millisecondes.
3. Lorsque l'appliance envoie une demande et si le serveur met plus de temps à répondre, l'appliance effectue un équilibrage de recharge en fonction de la valeur de délai d'expiration configurée. L'appliance réinitialise la connexion, choisit un autre service et transmet la demande au lieu d'attendre la réponse du serveur.
4. Une fois que le serveur virtuel d'équilibrage de charge a reçu la réponse, l'appliance transmet la réponse au client. L'utilisation d'un paramètre de temporisation empêche l'appliance de continuer à attendre la réponse du serveur, ce qui entraîne une augmentation du RTT.
5. Si le nombre de serveurs principaux disponibles est égal ou inférieur au nombre de nouvelles tentatives et si tous les serveurs expirent pour répondre à la demande, l'appliance répondra à une erreur de serveur interne de 500. Considérez un scénario avec cinq serveurs disponibles et le nombre de tentatives est défini sur six. Si le délai d'exécution de la demande est dépassé pour les cinq serveurs, l'appliance renvoie une erreur de serveur interne 500 au client.
6. De même, si le nombre de serveurs principaux est supérieur au nombre de nouvelles tentatives et si le serveur principal expire suite à une demande, l'appliance attend le dernier service jusqu'à ce que le serveur envoie une réponse ou que la connexion inactive du client expire. Considérez un scénario avec trois serveurs back-end et le nombre de tentatives est défini comme deux. Si les trois serveurs expirent à la suite de la demande, l'appliance attend le troisième service jusqu'à ce que le serveur envoie une réponse ou que la connexion inactive du client expire.

Configurer une nouvelle tentative de demande (méthodes GET et POST) lorsque le délai de réponse du serveur principal expire

Pour configurer une nouvelle tentative de demande pour la méthode GET en cas d'expiration du délai, vous devez suivre les étapes suivantes.

1. Activer appqoe
2. Configurer l'action Apqoe
3. Ajouter une politique Apqoe
4. Lier la stratégie appqoe au serveur virtuel d'équilibrage de charge

> **Remarque :**
>
> Le scénario de nouvelle tentative de demande après expiration du délai est également applicable à la méthode POST.

Activer appqoe

À l'invite de commande, tapez :

```
enable ns feature appqoe
```


Ajouter une action Apqoe pour le délai d'expiration

Vous devez configurer l'action appqoe pour qu'elle réessaie en cas d'expiration du délai et définir le nombre de tentatives.

À l'invite de commande, tapez :

```
add appqoe action <name> -retryOnTimeout <msecs> -numRetries <positive_integer
>
```

Exemple :

```
add appqoe action appact1 -retryOnTimeout 35 -numRetries 5
```

Ajouter une politique Apqoe

Pour implémenter Appqoe, vous devez configurer la politique Appqoe afin de définir comment mettre les connexions en file d'attente.

À l'invite de commande, tapez :

```
add appqoe policy <name> -rule <rule> -action <name>
```

Exemple :

```
add appqoe policy timeout_policy -rule http.req.method.eq(get)-action
appact1
```

Lier la stratégie appqoe au serveur virtuel d'équilibrage de charge

Lorsqu'un serveur principal met du temps à répondre et si vous souhaitez que le serveur virtuel d'équilibrage de charge transfère la demande au prochain service disponible, vous devez lier la politique appqoe au serveur virtuel d'équilibrage.

À l'invite de commande, tapez :

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Exemple :

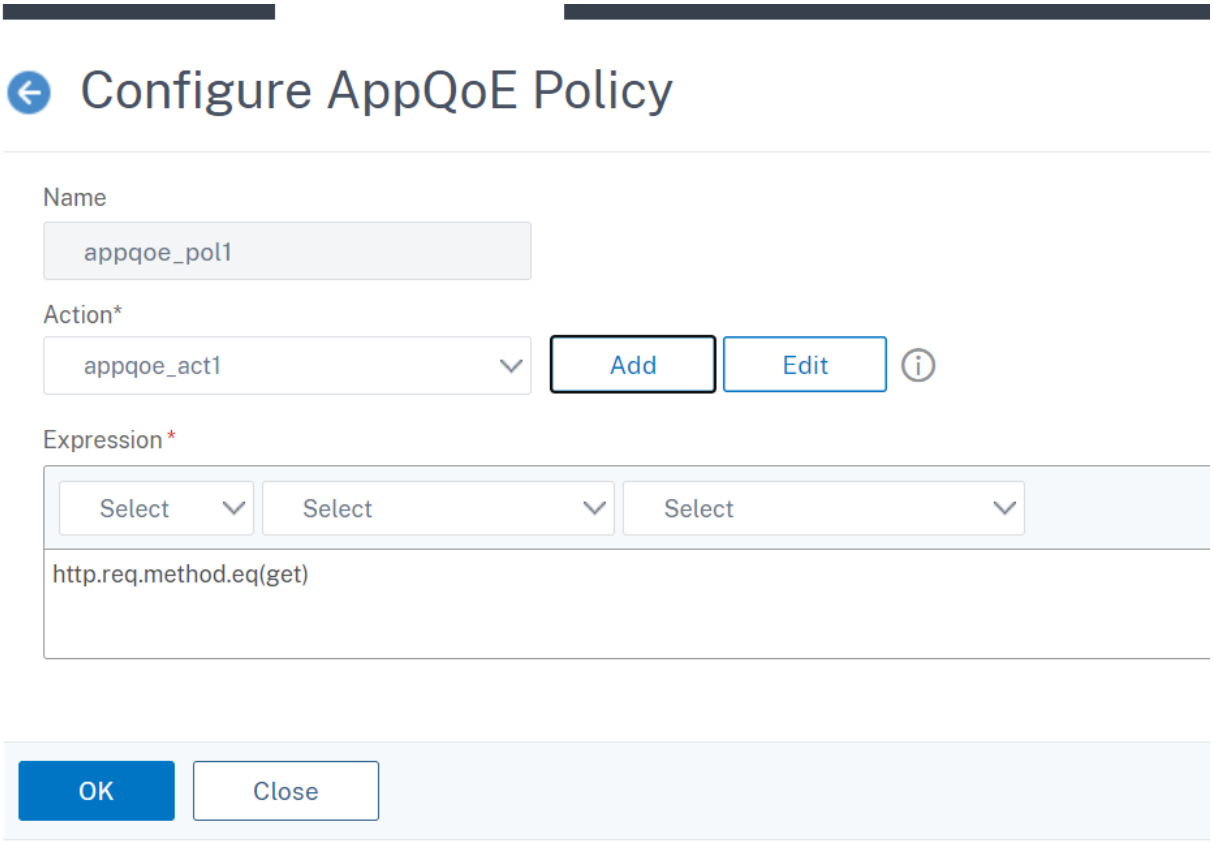
```
bind lb vserver v1 -policyName timeout_policy -type REQUEST -priority 1
```

Configurer la politique AppQoE pour l'équilibrage de charge en cas d'expiration du délai à l'aide de l'interface graphique NetScaler

1. Accédez à **AppExpert > AppQoE > Stratégies**.

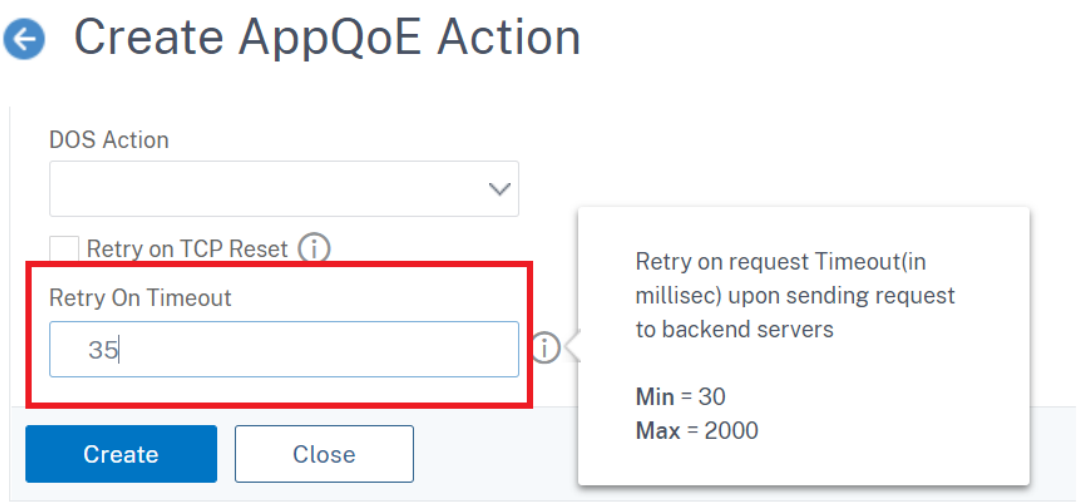
2. **Sur la page**Politiques AppQoE**, cliquez sur Ajouter.**
3. Dans la page **Créer une stratégie AppQoE**, définissez les paramètres suivants :

   a. Nom. Nom de la politique AppQoE
   b. Action. Ajoutez ou modifiez une action. Pour créer une nouvelle action, consultez la section Créer une action AppQoE.
   c. Expression : Sélectionnez ou saisissez l'expression de politique « http.req.method.eq (get) ».
4. Cliquez sur **Créer** et **Fermer**.



Configurer l'action AppQoE pour une nouvelle tentative de demande à l'aide de l'interface graphique NetScaler

1. Accédez à **AppExpert > AppQoE > Action**.
2. **Sur la page**AppQoE Actions**, cliquez sur Ajouter.**
3. Sur la page **Créer une action AppQoE**, définissez le paramètre suivant pour réessayer en cas d'expiration du délai de réponse du serveur principal : a.
   Réessayez sur Timeout. Réessayez sur demande. Délai d'expiration (en millisecondes) lors de l'envoi de la demande aux serveurs principaux.
4. Cliquez sur **Créer** et **Fermer**.



Optimisation TCP

July 18, 2023

Le protocole TCP utilise les techniques d'optimisation et les stratégies (ou algorithmes) de contrôle de la congestion suivantes pour éviter la congestion du réseau lors de la transmission de données.

Stratégies de contrôle de la congestion

Le protocole TCP est utilisé depuis longtemps pour établir et gérer des connexions Internet, gérer les erreurs de transmission et connecter facilement des applications Web aux appareils clients. Mais le trafic réseau est devenu plus difficile à contrôler, car la perte de paquets ne dépend pas uniquement de la congestion du réseau, et la congestion n'entraîne pas nécessairement la perte de paquets. Par conséquent, pour mesurer la congestion, un algorithme TCP doit se concentrer à la fois sur la perte de paquets et sur la bande passante.

Algorithme PRR (Proportional Rate Recovery)

Les mécanismes de restauration rapide TCP réduisent la latence Web causée par les pertes de paquets. Le nouvel algorithme PRR (Proportional Rate Recovery) est un algorithme de restauration rapide qui évalue les données TCP lors d'une restauration après perte. Il est calqué sur la réduction de moitié du débit, en utilisant la fraction appropriée pour la fenêtre cible choisie par l'algorithme de contrôle de congestion. Cela minimise l'ajustement de la fenêtre et la taille réelle de la fenêtre à la fin de la restauration est proche du seuil de démarrage lent (ssthresh).

Ouverture rapide TCP (TFO)

Le protocole TCP Fast Open (TFO) est un mécanisme TCP qui permet un échange de données rapide et sécurisé entre un client et un serveur lors de l'établissement de connexion initial du protocole TCP. Cette fonctionnalité est disponible en tant qu'option TCP dans le profil TCP lié à un serveur virtuel d'une appliance NetScaler. TFO utilise un cookie TCP Fast Open (un cookie de sécurité) généré par l'appliance NetScaler pour valider et authentifier le client initiant une connexion TFO au serveur virtuel. En utilisant ce mécanisme TFO, vous pouvez réduire la latence réseau d'une application du temps nécessaire pour un aller-retour complet, ce qui réduit considérablement le retard subi lors de courts transferts TCP.

Comment fonctionne TFO

Lorsqu'un client essaie d'établir une connexion TFO, il inclut un cookie TCP Fast Open avec le segment SYN initial pour s'authentifier. Si l'authentification est réussie, le serveur virtuel de l'appliance NetScaler peut inclure des données dans le segment SYN-ACK même s'il n'a pas reçu le dernier segment ACK de l'établissement de liaison tripartite. Cela permet d'économiser jusqu'à un aller-retour complet par rapport à une connexion TCP normale, qui nécessite une liaison à trois voies avant de pouvoir échanger des données.

Un client et un serveur principal effectuent les étapes suivantes pour établir une connexion TFO et échanger des données en toute sécurité lors de l'établissement de connexion TCP initial.

1. Si le client ne dispose pas d'un cookie d'ouverture rapide TCP pour s'authentifier, il envoie une demande de cookie d'ouverture rapide dans le paquet SYN au serveur virtuel de l'appliance NetScaler.
2. Si l'option TFO est activée dans le profil TCP lié au serveur virtuel, l'appliance génère un cookie (en chiffrant l'adresse IP du client sous une clé secrète) et répond au client par un SYN-ACK qui inclut le cookie d'ouverture rapide généré dans un champ d'option TCP.
3. Le client met en cache le cookie pour les futures connexions TFO au même serveur virtuel sur l'appliance.
4. Lorsque le client essaie d'établir une connexion TFO avec le même serveur virtuel, il envoie un SYN qui inclut le cookie Fast Open mis en cache (en tant qu'option TCP) ainsi que des données HTTP.
5. L'appliance NetScaler valide le cookie et, si l'authentification est réussie, le serveur accepte les données du paquet SYN et accuse réception de l'événement à l'aide d'un SYN-ACK, d'un cookie TFO et d'une réponse HTTP.

> **Remarque :**
>
> Si l'authentification du client échoue, le serveur supprime les données et accuse réception de l'événement uniquement avec un SYN indiquant un délai d'expiration de session.

1. Côté serveur, si l'option TFO est activée dans un profil TCP lié à un service, l'appliance NetScaler détermine si le cookie d'ouverture rapide TCP est présent dans le service auquel elle tente de se connecter.
2. Si le cookie TCP Fast Open n'est pas présent, l'appliance envoie une demande de cookie dans le paquet SYN.
3. Lorsque le serveur principal envoie le cookie, l'appliance stocke le cookie dans le cache d'informations du serveur.
4. Si l'appliance possède déjà un cookie pour la paire d'adresses IP de destination donnée, elle remplace l'ancien cookie par le nouveau.
5. Si le cookie est disponible dans le cache d'informations du serveur lorsque le serveur virtuel tente de se reconnecter au même serveur principal en utilisant la même adresse SNIP, l'appliance combine les données du paquet SYN avec le cookie et les envoie au serveur principal.
6. Le serveur principal accuse réception de l'événement à l'aide de données et d'un SYN.

Remarque : Si le serveur accuse réception de l'événement avec uniquement un segment SYN, l'appliance NetScaler renvoie immédiatement le paquet de données après avoir supprimé le segment SYN et les options TCP du paquet d'origine.

Configuration de l'ouverture rapide du protocole TCP

Pour utiliser la fonctionnalité TCP Fast Open (TFO), activez l'option TCP Fast Open dans le profil TCP concerné et définissez le paramètre TFO Cookie Timeout sur une valeur qui répond aux exigences de sécurité de ce profil.

Activer ou désactiver TFO à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver TFO dans un profil nouveau ou existant.

Remarque : La valeur par défaut est DISABLED.

```
    add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
    set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
    unset tcpprofile <TCP Profile Name> - tcpFastOpen
    Examples
    add tcpprofile Profile1 - tcpFastOpen
    Set tcpprofile Profile1 - tcpFastOpen Enabled
    unset tcpprofile Profile1 - tcpFastOpen
<!--NeedCopy-->
```


Pour définir la valeur du délai d'expiration du cookie TCP Fast Open à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
1     set tcpparam  - tcpfastOpenCookieTimeout <Timeout Value>
2     Example
3     set tcpprofile  - tcpfastOpenCookieTimeout 30secs
4 <!--NeedCopy-->
```

Pour configurer le TCP Fast Open à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils** > puis cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, cochez la case **TCP Fast Open** .
3. Cliquez sur **OK**, puis sur **Terminé**.

Pour configurer la valeur du délai d'expiration du cookie rapide TCP à l'aide de l'interface graphique

Accédez à **Configuration** > **Système** > **Paramètres > Modifier les paramètresTCP, puis à la page Configurer les paramètresTCP** pour définir la valeur du délai d'expiration du cookie d'ouverture rapide TCP.

TCP HyStart

Un nouveau paramètre de profil TCP, HyStart, active l'algorithme HyStart, qui est un algorithme de démarrage lent qui détermine dynamiquement un point sûr auquel terminer (ssthresh). Il permet une transition vers la prévention de la congestion sans pertes importantes de paquets. Ce nouveau paramètre est désactivé par défaut.

Si une congestion est détectée, HyStart entre dans une phase d'évitement de la congestion. Son activation vous permet d'obtenir un meilleur débit sur les réseaux à haut débit présentant de fortes pertes de paquets. Cet algorithme permet de maintenir une bande passante proche de la limite maximale lors du traitement des transactions. Il peut donc améliorer le débit.

Configuration de TCP HyStart

Pour utiliser la fonctionnalité HyStart, activez l'option Cubic HyStart dans le profil TCP approprié.

Pour configurer HyStart à l'aide de l'interface de ligne de commande (CLI)

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver HyStart dans un profil TCP nouveau ou existant.

```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
unset tcprofile <profileName> -hystart
<!--NeedCopy-->
```

Exemples :

```
    add tcpprofile profile1 -hystart ENABLED
    set tcpprofile profile1 -hystart ENABLED
    unset tcprofile profile1 -hystart
<!--NeedCopy-->
```

Pour configurer le support HyStart à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils** > et cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, cochez la case **Cubic Hystart** .
3. Cliquez sur **OK**, puis sur **Terminé**.

Contrôle du débit de rafale TCP

Il a été observé que les mécanismes de contrôle TCP peuvent entraîner un flux de trafic intense sur les réseaux mobiles à haut débit, avec un impact négatif sur l'efficacité globale du réseau. En raison des conditions du réseau mobile telles que la congestion ou la retransmission de données de couche 2, les accusés de réception TCP arrivent groupés à l'expéditeur, déclenchant une transmission en rafale. Ces groupes de paquets consécutifs envoyés avec un court intervalle entre paquets sont appelés rafales de paquets TCP. Pour surmonter les rafales de trafic, l'appliance NetScaler utilise une technique de contrôle du débit de rafale TCP. Cette technique répartit les données de manière uniforme sur le réseau pendant toute la durée d'un aller-retour afin que les données ne soient pas envoyées en rafale. En utilisant cette technique de contrôle de la fréquence de rafale, vous pouvez obtenir un meilleur débit et des taux de perte de paquets plus faibles.

Comment fonctionne le contrôle de la fréquence de rafale TCP

Dans une appliance NetScaler, cette technique répartit uniformément la transmission d'un paquet sur toute la durée de l'aller-retour (RTT). Cela est possible grâce à l'utilisation d'une pile TCP et d'un planificateur de paquets réseau qui identifie les différentes conditions du réseau afin de générer des paquets pour les sessions TCP en cours afin de réduire les rafales.

Au niveau de l'expéditeur, au lieu de transmettre des paquets immédiatement après réception d'un accusé de réception, l'expéditeur peut retarder la transmission des paquets pour les répartir au débit défini par le planificateur (configuration dynamique) ou par le profil TCP (configuration fixe).

Configuration du contrôle du débit de rafale TCP

Pour utiliser l'option TCP Burst Rate Control dans le profil TCP approprié et définir les paramètres de contrôle du débit de rafale.

Pour définir le contrôle du débit de rafale TCP à l'aide de la ligne de commande

À l'invite de commandes, définissez l'une des commandes TCP Burst Rate Control suivantes qui sont configurées dans un profil nouveau ou existant.

Remarque : La valeur par défaut est DISABLED.

```
add tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
    | Fixed

set tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
    | Fixed

unset tcpprofile <TCP Profile Name> -burstRateControl Disabled |
    Dynamic | Fixed
<!--NeedCopy-->
```

Où,

Désactivé : si le contrôle de la fréquence de rafale est désactivé, une appliance NetScaler n'effectue pas de gestion de rafale autre que le paramètre MaxBurst.

Corrigé — Si le contrôle du débit de rafale TCP est fixe, l'appliance utilise la valeur du débit d'envoi de la charge utile de la connexion TCP mentionnée dans le profil TCP.

Dynamique : si le contrôle du débit de rafale est « dynamique », la connexion est régulée en fonction de diverses conditions du réseau afin de réduire les rafales TCP. Ce mode fonctionne uniquement lorsque la connexion TCP est en mode ENDPOINT. Lorsque le contrôle Dynamic Burst Rate est activé, le paramètre MaxBurst du profil TCP n'est pas actif.

```
add tcpProfile  profile1 -burstRateControl Disabled

set tcpProfile profile1 -burstRateControl Dynamic

unset tcpProfile profile1 -burstRateControl Fixed
<!--NeedCopy-->
```


Pour définir les paramètres du TCP Burst Rate Control à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
set ns tcpprofile nstcp_default_profile  -burstRateControl <type of burst rate control>  -tcprate <TCP rate> -rateqmax <maximum bytes in queue>

T1300-10-2> show ns tcpprofile nstcp_default_profile
        Name: nstcp_default_profile
        Window Scaling status:  ENABLED
        Window Scaling factor: 8
        SACK status: ENABLED
        MSS: 1460
        MaxBurst setting: 30 MSS
        Initial cwnd setting: 16 MSS
        TCP Delayed-ACK Timer: 100 millisec
        Nagle's Algorithm: DISABLED
        Maximum out-of-order packets to queue: 15000
        Immediate ACK on PUSH packet: ENABLED
        Maximum packets per MSS: 0
        Maximum packets per retransmission: 1
        TCP minimum RTO in millisec: 1000
        TCP Slow start increment: 1
        TCP Buffer Size: 8000000 bytes
        TCP Send Buffer Size: 8000000 bytes
        TCP Syncookie: ENABLED
        Update Last activity on KA Probes: ENABLED
        TCP flavor: BIC
        TCP Dynamic Receive Buffering: DISABLED
        Keep-alive probes: ENABLED
        Connection idle time before starting keep-alive probes: 900 seconds
        Keep-alive probe interval: 75 seconds
        Maximum keep-alive probes to be missed before dropping connection: 3
        Establishing Client Connection: AUTOMATIC
        TCP Segmentation Offload: AUTOMATIC
        TCP Timestamp Option: DISABLED
        RST window attenuation (spoof protection): ENABLED
        Accept RST with last acknowledged sequence number: ENABLED
        SYN spoof protection: ENABLED
        TCP Explicit Congestion Notification: DISABLED
        Multipath TCP: DISABLED
```



```
37              Multipath TCP drop data on pre-established subflow:
                    DISABLED
38              Multipath TCP fastopen: DISABLED
39              Multipath TCP session timeout: 0 seconds
40              DSACK: ENABLED
41              ACK Aggregation: DISABLED
42              FRTO: ENABLED
43              TCP Max CWND : 4000000 bytes
44              FACK: ENABLED
45              TCP Optimization mode: ENDPOINT
46              TCP Fastopen: DISABLED
47              HYSTART: DISABLED
48              TCP dupack threshold: 3
49              Burst Rate Control: Dynamic
50              TCP Rate: 0
51              TCP Rate Maximum Queue: 0
52  <!--NeedCopy-->
```

Pour configurer le contrôle du débit de rafale TCP à l'aide de l'interface graphique

1. Accédez à **Configuration** > **Système** > **Profils** > puis cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, sélectionnez l'option **TCP Burst Control** dans la liste déroulante :
   a) BurstRateCntrl
   b) CreditBytePrms
   c) RateBytePerms
   d) RateSchedulerQ
3. Cliquez sur **OK**, puis sur **Terminé**.

Protection contre l'algorithme PAWS (Wrapped Sequence)

Si vous activez l'option d'horodatage TCP dans le profil TCP par défaut, l'appliance NetScaler utilise l'algorithme PAWS (Protection Against Wrapped Sequence) pour identifier et rejeter les anciens paquets dont les numéros de séquence se trouvent dans la fenêtre de réception de la connexion TCP en cours car la séquence est « encapsulée » (elle a atteint sa valeur maximale et a été redémarrée à partir de 0).

Si la congestion du réseau retarde un paquet de données non SYN et que vous ouvrez une nouvelle connexion avant l'arrivée du paquet, l'encapsulation par numéro de séquence peut amener la nouvelle connexion à accepter le paquet comme valide, ce qui entraîne une corruption des données. Mais si l'option d'horodatage TCP est activée, le paquet est supprimé.

Par défaut, l'option d'horodatage TCP est désactivée. Si vous l'activez, l'appliance compare l'horodatage TCP (seg.tsVal) dans l'en-tête d'un paquet avec la valeur de l'horodatage récent (ts.Recent). Si Seg.tsVal est égal ou supérieur à ts.Recent, le paquet est traité. Dans le cas contraire, l'appliance abandonne le paquet et envoie un accusé de réception correctif.

Comment fonctionne PAWS

L'algorithme PAWS traite tous les paquets TCP entrants d'une connexion synchronisée comme suit :

1. Si `SEG.TSval < Ts.recent` : Le paquet entrant n'est pas acceptable. PAWS envoie un accusé de réception (comme spécifié dans la RFC-793) et supprime le paquet. Remarque : L'envoi d'un segment ACK est nécessaire pour conserver les mécanismes TCP de détection et de restauration des connexions semi-ouvertes.
2. Si le paquet se trouve en dehors de la fenêtre : PAWS rejette le paquet, comme dans un traitement TCP normal.
3. Si `SEG.TSval > Ts.recent` : `PAWS` accepte le paquet et le traite.
4. Si `SEG.TSval <= Last.ACK.sent`(segment entrant satisfait) : PAWS copie la valeur `SEG.TSval` dans `Ts.recent`.
5. Si le paquet est en séquence : PAWS accepte le paquet.
6. Si le paquet n'est pas en séquence : le paquet est traité comme un segment TCP normal dans la fenêtre et hors séquence. Par exemple, il peut être mis en file d'attente pour une livraison ultérieure.
7. Si la `Ts.recent` valeur est inactive pendant plus de 24 jours : la validité de `Ts.recent` est vérifiée si la vérification de l'horodatage PAWS échoue. Si la valeur TS.recent s'avère non valide, le segment est accepté et `PAWS rule` met à jour `Ts.recent` avec la valeur TSval du nouveau segment.

Pour activer ou désactiver l'horodatage TCP à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
`set nstcpprofile nstcp_default_profile -TimeStamp (ENABLED | DISABLED)
    `
```

Pour activer ou désactiver l'horodatage TCP à l'aide de l'interface graphique

Accédez à **Système** > **Profil > ProfilTCP, sélectionnez le profil**TCP par défaut, cliquez sur**Modifier**, puis cochez ou décochez la case**Horodatage TCP** .

Techniques d'optimisation

TCP utilise les techniques et méthodes d'optimisation suivantes pour optimiser les contrôles de flux.

Sélection de profils TCP basée sur des règles

Le trafic réseau d'aujourd'hui est plus diversifié et plus gourmand en bande passante que jamais. Avec l'augmentation du trafic, l'effet de la qualité de service (QoS) sur les performances du protocole TCP est significatif. Pour améliorer la QoS, vous pouvez désormais configurer des stratégies AppQoE avec différents profils TCP pour différentes classes de trafic réseau. La stratégie AppQoE classe le trafic d'un serveur virtuel afin d'associer un profil TCP optimisé pour un type de trafic particulier, tel que la 3G, la 4G, le LAN ou le WAN.

Pour utiliser cette fonctionnalité, créez une action de stratégie pour chaque profil TCP, associez une action aux stratégies AppQoE et associez les stratégies aux serveurs virtuels d'équilibrage de charge.

Pour plus d'informations sur l'utilisation des attributs d'abonné pour effectuer l'optimisation TCP, consultez Profil TCP basé surdes règles.

Configuration de la sélection de profils TCP basée sur des stratégies

La configuration de la sélection de profils TCP basée sur des règles comprend les tâches suivantes :

- Activation d'AppQoE. Avant de configurer la fonctionnalité de profil TCP, vous devez activer la fonctionnalité AppQoE.
- Ajout d'une action AppQoE. Après avoir activé la fonctionnalité AppQoE, configurez une action AppQoE avec un profil TCP.
- Configuration de la sélection du profil TCP basée sur AppQoE. Pour implémenter la sélection de profils TCP pour différentes classes de trafic, vous devez configurer des stratégies AppQoE permettant à votre NetScaler de distinguer les connexions et de lier l'action AppQoE appropriée à chaque stratégie.
- Liaison de la stratégie AppQoE au serveur virtuel. Une fois que vous avez configuré les stratégies AppQoE, vous devez les lier à un ou plusieurs serveurs virtuels d'équilibrage de charge, de commutation de contenu ou de redirection de cache.

Configuration à l'aide de l'interface de ligne de commande

Pour activer AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez les commandes suivantes pour activer la fonctionnalité et vérifier qu'elle est activée :

- `enable ns feature appqoe`
- `show ns feature`

Pour lier un profil TCP lors de la création d'une action AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez la commande d'action AppQoe suivante avec l'option `tcpprofiletobind` .

```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS | NS )
[<CustomFile>] [-altContentSvcName <string>] [-altContentPath <string>] [-
maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth <positive_integer
>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-
dosAction ( SimpleResponse |HICResponse )] [-tcpprofiletobind <string>]
show appqoe action
```

Pour configurer une stratégie AppQoE à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
add appqoe policy <name> -rule <expression> -action <string>
```

Pour lier une stratégie AppQoE à des serveurs virtuels d'équilibrage de charge, de redirection de cache ou de commutation de contenu à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez :

```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <priority
>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <priority
>
```

Exemple

```
1    add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
        ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500
         -slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
        sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
        ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack
        ENABLED -tcpmode ENDPOINT
2    add appqoe action appact1 -priority HIGH -tcpprofile tcp1
3    add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
        action appact1
4    bind lb vserver lb2 -policyName apppol1 -priority 1 -
        gotoPriorityExpression END -type REQUEST
```



```
5     bind cs vserver cs1 -policyName apppol1 -priority 1 -
         gotoPriorityExpression END -type REQUEST
6  <!--NeedCopy-->
```

Configuration du profilage TCP basé sur des règles à l'aide de l'interface graphique

Pour activer AppQoE à l'aide de l'interface graphique

1. Accédez à **Système** > **Paramètres**.
2. Dans le volet de détails, cliquez sur **Configurer les fonctionnalités avancées**.
3. Dans la boîte de dialogue **Configurer les fonctionnalités avancées**, cochez la case **AppQoE** .
4. Cliquez sur **OK**.

Pour configurer la stratégie AppQoE à l'aide de l'interface graphique

1. Accédez à **App-Expert** > **AppQoE** > **Actions**.
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
3. Pour créer une action, cliquez sur **Ajouter**.
4. Pour modifier une action existante, sélectionnez-la, puis cliquez sur **Modifier**.
5. Dans l'écran **Créer une action AppQoE** ou **Configurer une action AppQoE**, tapez ou sélectionnez des valeurs pour les paramètres. Le contenu de la boîte de dialogue correspond aux paramètres décrits dans « Paramètres de configuration de l'action AppQoE » comme suit (un astérisque indique un paramètre obligatoire) :
   a) Nom—nom
   b) Type d'action — respondWith
   c) Priorité — priority
   d) Profondeur de la file d'attente de stratégies — polqDepth
   e) Profondeur de file d'attente — priqDepth
   f) Action DOS — dosAction
6. Cliquez sur **Create**.

Pour lier la stratégie AppQoE à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels**, sélectionnez un serveur, puis cliquez sur **Modifier**.
2. Dans la section **Stratégies**, cliquez sur (+) pour lier une stratégie AppQoE.
3. Dans le curseur **Stratégies**, effectuez les opérations suivantes :
   a) Sélectionnez un type de stratégie comme AppQoE dans la liste déroulante.
   b) Sélectionnez un type de trafic dans la liste déroulante.
4. Dans la section **Policy Binding**, procédez comme suit :

a) Cliquez sur **Nouveau** pour créer une stratégie AppQoE.
b) Cliquez sur **Stratégie existante pour sélectionner une stratégie** AppQoE dans la liste déroulante.

5. Définissez la priorité de liaison et cliquez sur **Lier** à la stratégie au serveur virtuel.
6. Cliquez sur **Terminé**.

Génération de blocs SACK

Les performances du protocole TCP ralentissent lorsque plusieurs paquets sont perdus dans une fenêtre de données. Dans un tel scénario, un mécanisme d'accusé de réception sélectif (SACK) combiné à une stratégie de retransmission répétée sélective permet de surmonter cette limitation. Pour chaque paquet entrant hors service, vous devez générer un bloc SACK.

Si le paquet hors ordre entre dans le bloc de la file d'attente de réassemblage, insérez les informations du paquet dans le bloc et définissez les informations du bloc complètes sur SACK-0. Si un paquet en panne ne rentre pas dans le bloc de réassemblage, envoyez le paquet au format SACK-0 et répétez les blocs SACK précédents. Si un paquet hors ordre est un doublon et que les informations du paquet sont définies comme SACK-0, alors D-SACK le bloc.

Remarque : Un paquet est considéré comme D-SACK s'il s'agit d'un paquet accusé de réception ou d'un paquet hors service déjà reçu.

Le client renie

Une appliance NetScaler peut gérer les renégats du client lors d'une restauration basée sur SACK.

Les contrôles de mémoire pour marquer le point de terminaison sur un circuit imprimé ne prennent pas en compte la quantité totale de mémoire disponible

Dans une appliance NetScaler, si le seuil d'utilisation de la mémoire est défini sur 75 % au lieu d'utiliser la mémoire totale disponible, les nouvelles connexions TCP contournent l'optimisation TCP.

Retransmissions inutiles en raison de l'absence de blocs SACK

En mode hors point de terminaison, lorsque vous envoyez des DUPACKS, si des blocs SACK sont absents pour quelques paquets hors service, cela déclenche d'autres retransmissions depuis le serveur.

Le protocole SNMP pour les connexions a contourné l'optimisation en raison d'une surcharge

Les identifiants SNMP suivants ont été ajoutés à une appliance NetScaler pour suivre le nombre de connexions contournées par les optimisations TCP en raison d'une surcharge.

1. 1.3.6.1.4.1.5951.4.1.1.46.131 (tcpOptimizationEnabled). Pour suivre le nombre total de connexions activées grâce à l'optimisation TCP.
2. 1.3.6.1.4.1.5951.4.1.1.46.132 (tcpOptimizationBypassed). Pour suivre le nombre total de connexions contournées, optimisez TCP.

Tampon de réception dynamique

Pour optimiser les performances TCP, une appliance NetScaler peut désormais ajuster dynamiquement la taille de la mémoire tampon de réception TCP.

Algorithme Tail Loss Probe

Un délai de retransmission (RTO) est une perte de segments à la fin d'une transaction. Un RTO se produit en cas de problèmes de latence des applications, en particulier lors de transactions Web courtes. Pour récupérer les segments perdus à la fin d'une transaction, TCP utilise l'algorithme Tail Loss Probe (TLP).
TLP est un algorithme réservé aux expéditeurs. Si une connexion TCP ne reçoit aucun accusé de réception pendant un certain temps, TLP transmet le dernier paquet non reconnu (sonde de perte). En cas de perte de la queue lors de la transmission initiale, un accusé de réception émis par la sonde de perte déclenche une reprise du SACK ou du FACK.

Configuration de la sonde Tail Loss

Pour utiliser l'algorithme TLP (Tail Loss Probe), vous devez activer l'option TLP dans le profil TCP et définir le paramètre sur une valeur qui répond aux exigences de sécurité de ce profil.

Activez TLP à l'aide de la ligne de commande

À l'invite de commandes, tapez l'une des commandes suivantes pour activer ou désactiver TLP dans un profil nouveau ou existant.

> **Remarque** :
>
> La valeur par défaut est DISABLED.

```
add tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED

set tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED

unset tcpprofile <TCP Profile Name> - taillossprobe
```

Exemples :

```
add tcpprofile nstcp_default_profile - taillossprobe
```



```
set tcpprofile nstcp_default_profile -taillossprobe Enabled

unset tcpprofile nstcp_default_profile -taillossprobe
```

Configurer l'algorithme Tail Loss Probe à l'aide de l'interface graphique NetScaler

1. Accédez à **Configuration** > **Système** > **Profils** > puis cliquez sur **Modifier** pour modifier un profil TCP.
2. Sur la page **Configurer le profil TCP**, cochez la case **Tail Loss Probe** .
3. Cliquez sur **OK**, puis sur **Terminé**.

Solutions de résolution des problèmes pour NetScaler

May 5, 2023

Cette rubrique présente les solutions de dépannage de base nécessaires pour résoudre les problèmes qui surviennent dans votre appliance. Il vous donne une compréhension de l'appliance NetScaler, de la manière dont elle s'intègre au réseau et des problèmes auxquels vous pouvez vous attendre dans les fonctionnalités système de base.

Comment enregistrer une trace de paquets sur NetScaler

May 5, 2023

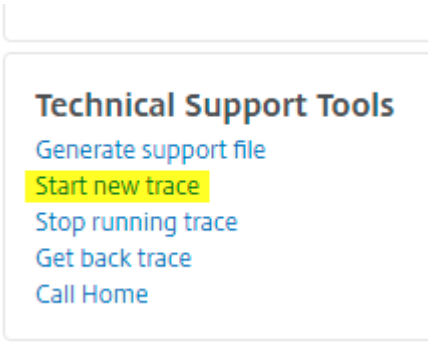
Cet article de résolution des problèmes explique comment un administrateur peut enregistrer une trace de paquets réseau à l'aide de l'interface graphique NetScaler.

Points à retenir

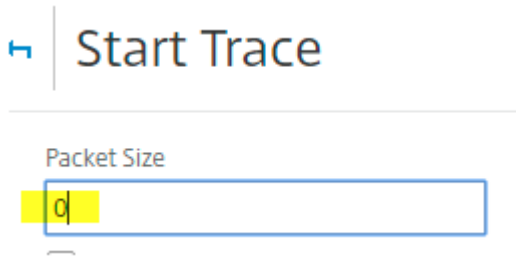
- Citrix vous recommande d'utiliser la version récente de Wireshark dans la « section de génération automatisée » disponible sur la page Web suivante : http://www.wireshark.org/download/automated.
- Dans NetScaler version 11.1 ou ultérieure, pour déchiffrer la capture et garantir que les paramètres ECC (Elliptic Curve Cryptography), Session Reuse et DH sont désactivés depuis le serveur virtuel. Vous devez le faire avant de capturer une trace.

Enregistrer le suivi des paquets sur NetScaler version 11.1

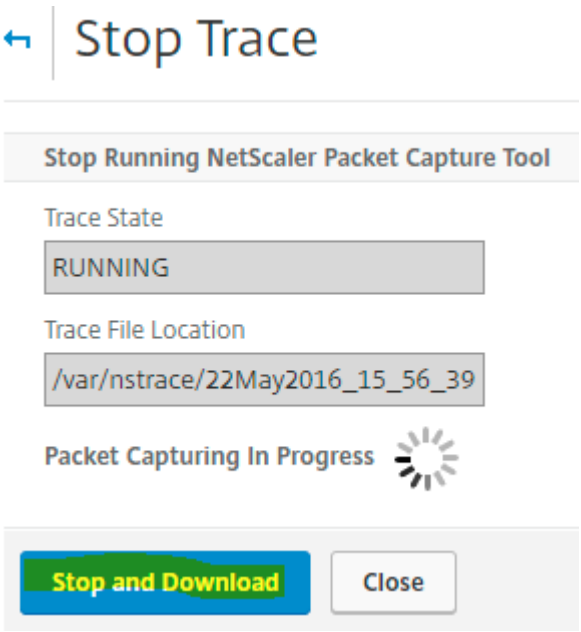
1. Accédez à la page **Système** > **Diagnostics** .
2. cliquez sur le lien **Démarrer une nouvelle trace** dans la page **Diagnostic**, comme indiqué dans la capture d'écran suivante.



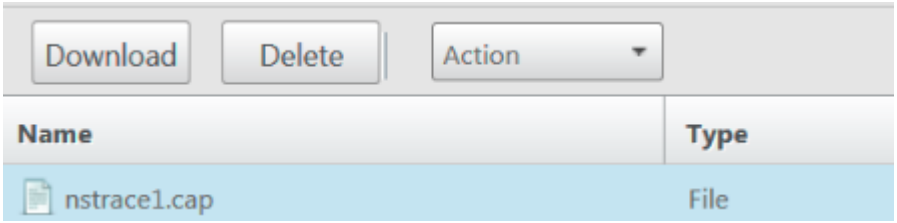
3. Mettez à jour la taille du paquet sur 0 dans le champ **Taille du paquet** .



4. Cliquez sur **Démarrer** pour commencer à enregistrer le suivi des paquets réseau.
5. Cliquez sur **Arrêter et télécharger** pour arrêter l'enregistrement du suivi des paquets réseau une fois le test terminé.

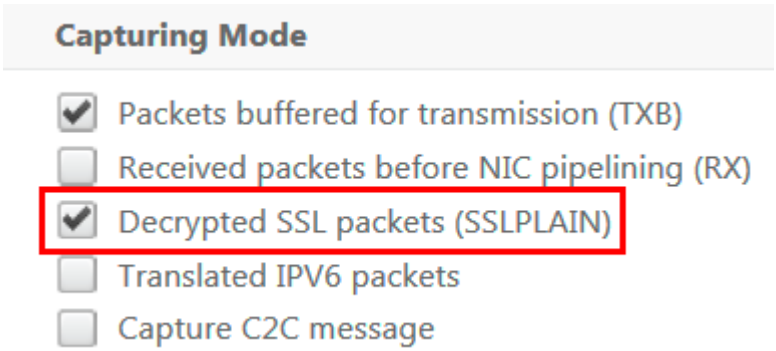


6. Sélectionnez le fichier requis et cliquez sur **Sélectionner**, puis sur **Télécharger**.



7. Ouvrez le fichier de suivi des paquets réseau à l'aide de l'utilitaire Wireshark pour afficher le contenu du fichier.

> **Remarque** : Sélectionnez Paquets SSL décryptés (SSLPLAIN) pour déchiffrer le suivi des paquets sans la clé privée.



Capturez les clés principales SSL

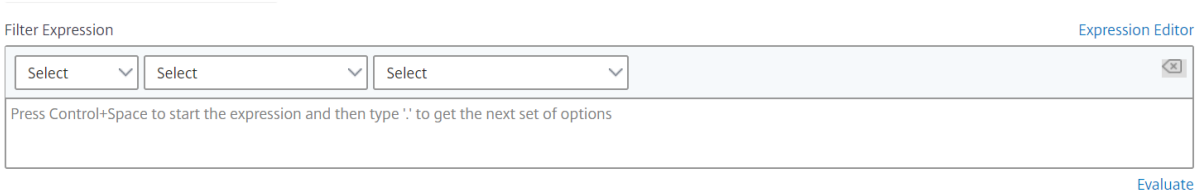
Dans les versions 11.0, 11.1 et supérieures, il existe une option permettant de capturer les clés de session qui n'est valide que pour cette session/nstrace particulière et cette option peut être utilisée si vous ne souhaitez pas partager la clé privée ou utiliser le mode SSLPLAIN. Pour plus d'informations, veuillez consulter https://support.citrix.com/article/CTX135889.

Exporter des clés de session sans partager de clé privée

Dans la plupart des scénarios, la clé privée n'est ni disponible ni partagée. Dans de tels cas, nous pouvons suggérer d'exporter les clés de **session SSL** au lieu de la clé privée. Lisez
[Comment exporter et utiliser des clés de session SSL pour déchiffrer les traces SSL sans partager la clé privée SSL, voir https://support.citrix.com/article/CTX135889.

Filtres

De plus, il est toujours recommandé d'ajouter des filtres basés sur IP lors de la prise de traces. Le processus garantit que vous ne capturez que le trafic intéressé, ce qui facilite votre dépannage. L'ajout de filtres réduit également la charge sur l'appliance lors de la prise de traces.



Des filtres basés sur IP simples suffisent pour obtenir les bonnes captures. Pour plus d'informations sur `nstrace` les filtres et les exemples, consultez la page de documentation de NetScaler.

Cas d'utilisation pour capturer une trace de paquets avec un filtre IP du serveur virtuel (à la fois frontal et backend)

À l'aide d'un filtre de l'adresse IP du serveur virtuel et en activant l'option « —link » dans la CLI ou en sélectionnant l'option « Trace filtered connection peer traffic » dans l'interface utilisateur graphique (disponible 10.1 et versions ultérieures), vous pouvez capturer à la fois le trafic frontal et le trafic back-end pour l'adresse IP.

```
start nstrace -size 0 -filter "CONNECTION.IP.EQ(1.1.1.1)" -link ENABLED

show nstrace
        State:  RUNNING          Scope:  LOCAL            TraceLocation
           :  "/var/nstrace/24Mar2017_16_00_19/..." Nf:  24
                           Time:  3600              Size:  0
                         Mode:  TXB NEW_RX
        Traceformat:  NSCAP      PerNIC:  DISABLED        FileName:  24
           Mar2017_16_00_19 Filter:  "CONNECTION.IP.EQ(1.1.1.1)" Link:
            ENABLED           Merge:  ONSTOP           Doruntimecleanup
           :  ENABLED
        TraceBuffers:  5000      SkipRPC:  DISABLED       Capsslkeys:
           DISABLED    InMemoryTrace:  DISABLED
<!--NeedCopy-->
```

Capture de traces cycliques

Il est toujours difficile de résoudre un problème intermittent. Le suivi cyclique est le mieux adapté aux problèmes intermittents. Les traces peuvent être exécutées pendant quelques heures ou quelques

jours avant que le problème ne se produise. Vous pouvez également utiliser un filtre spécifique et évaluer la taille des fichiers de suivi générés avant de les exécuter plus longtemps.

Exécutez la commande suivante depuis l'interface de ligne de commande :

```
start nstrace -nf 60 -time 30 -size 0
This particular trace will create 60 files each of them for 30 sec.
   This means the files will start getting overwritten after 60 trace
   files or 30 mins
Show nstrace à To check the status of the nstrace
Stop nstrace à To stop the nstrace.

<!--NeedCopy-->
```

Recommandations

Sur une unité traitant des Go de trafic par seconde, la capture du trafic est un processus très gourmand en ressources. L'impact sur les ressources se situe principalement en termes de CPU et d'espace disque. L'impact sur l'espace disque peut être réduit en utilisant des expressions de filtrage. Cependant, l'impact sur le processeur persiste et entraîne parfois une légère augmentation, car l'appliance doit maintenant traiter les paquets en fonction du filtre avant de les capturer.

Les meilleures pratiques concernant le traçage sont les suivantes :

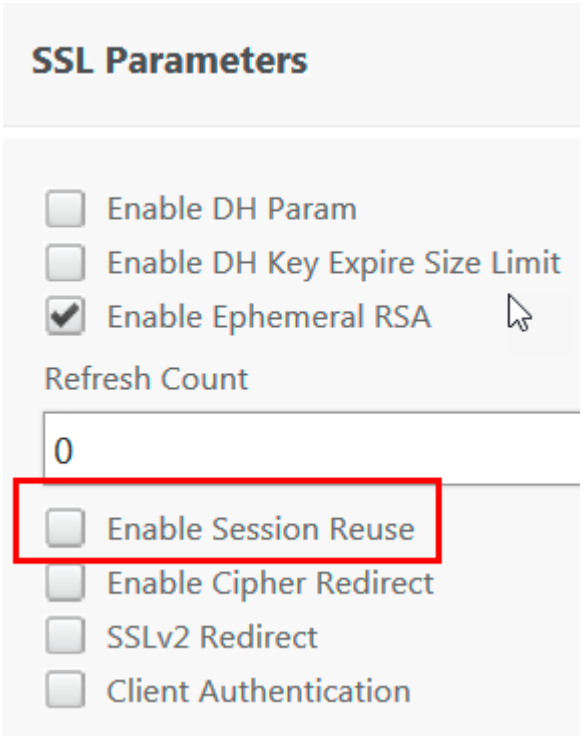
1. La durée pendant laquelle la trace est exécutée doit être aussi limitée que possible lorsque vous vous assurez toujours que les paquets d'intérêt sont capturés.
2. Planifiez l'activité de suivi pour qu'elle se produise à un moment où le nombre d'utilisateurs (et donc le trafic) est fortement réduit, par exemple en dehors des heures de travail.

Plus de ressources

Désactiver la réutilisation de session sur le serveur virtuel depuis l'interface

La réutilisation de session est désactivée lorsque vous capturez une trace pour terminer une négociation SSL dans la trace. Lorsqu'elle est activée, vous pouvez capturer une poignée de main partielle dans la trace. Assurez-vous d'activer l'option après la collecte des traces.
Ne désactivez pas la réutilisation d'une session SSL lorsque la méthode de persistance est sslsession, car elle interrompt la persistance pour les connexions existantes. Pour plus d'informations, reportez-vous à la section https://support.citrix.com/article/CTX121925.

1. Ouvrez le serveur virtuel et accédez à Paramètres SSL.
2. Désactivez l'option Activer la réutilisation de session si



Désactiver la réutilisation de session sur le serveur virtuel depuis l'interface

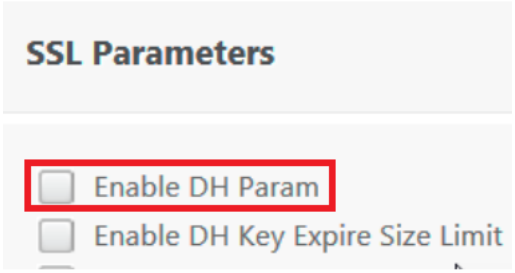
1. Connexion SSH à la console de l'appliance.
2. Exécutez la commande suivante pour désactiver DH Param sur le serveur virtuel :

```
set ssl vserver "vServer_Name"-sessReuse DISABLED
```

Désactiver le paramètre DH sur le serveur virtuel depuis l'interface graphique

Reportez-vous à https://support.citrix.com/article/CTX213335 Pour en savoir plus sur le paramètre DH.

1. Ouvrez le serveur virtuel et accédez à Paramètres SSL.
2. Désactivez DH Param s'il est activé.



Désactiver le paramètre DH sur le serveur virtuel depuis la CLI

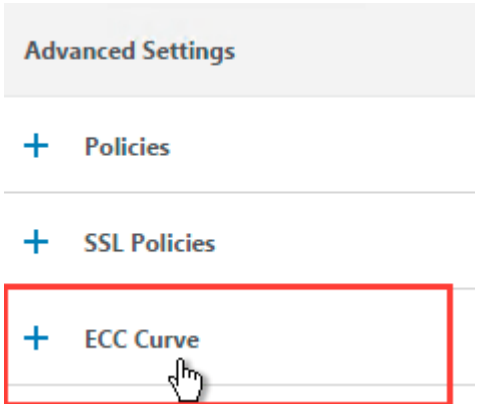
1. Connexion SSH à la console de l'appliance.
2. Exécutez la commande suivante pour désactiver DH Param sur le serveur virtuel :

```
set ssl vserver "vServer_Name"-dh DISABLED
```

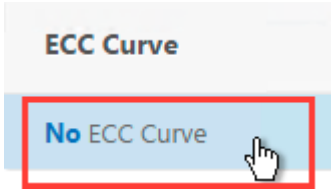
Désactiver la courbe ECC sur le serveur virtuel à partir de l'interface utilisateur

La courbe ECC est désactivée pour déchiffrer la trace SSL capturée avec une clé privée. Vous ne devez pas désactiver les clés si les chiffrements SSL associés sont utilisés. Pour plus d'informations sur la courbe ECC, voir https://support.citrix.com/article/CTX205289

1. Ouvrez le serveur virtuel et accédez à ECC Curve.



2. Si aucune courbe ECC n'est liée au serveur virtuel, aucune autre action n'est requise.



3. Si une courbe ECC est liée au serveur virtuel, cliquez sur la courbe ECC et dissociez-la du serveur virtuel.

Désactiver la courbe ECC sur le serveur virtuel depuis la CLI

1. Connexion SSH à la console de l'appliance.
2. Exécutez la commande suivante pour chaque courbe ECC liée au serveur virtuel :

```
unbind ssl vserver "vServer_Name"-eccCurveName "ECC_Curve_Name"
```


Comment libérer de l'espace sur le répertoire VAR pour la journalisation des problèmes avec une appliance NetScaler

May 5, 2023

L'article suivant explique comment un administrateur peut libérer de l'espace depuis le `/var` répertoire d'une appliance NetScaler. Vous pouvez suivre les étapes lorsque l'interface graphique n'est pas accessible.

Lorsque l'espace disque est faible dans le répertoire /var de l'appliance, il est possible que vous ne puissiez pas vous connecter à l'interface graphique. Dans ce scénario, vous pouvez supprimer les anciens fichiers journaux pour créer de l'espace libre dans le répertoire /var.

Points à retenir

- Veillez à sauvegarder les fichiers avant de les supprimer de l'appliance.

Pour libérer de l'espace dans le `/var` répertoire d'une appliance NetScaler, procédez comme suit :

1. Connectez-vous à l'interface de ligne de commande de NetScaler à l'aide de SSH. Pour plus d'informations sur l'exécution de cette tâche, consultez la documentation NetScaler.
2. Une fois connecté à l'interface de ligne de commande NetScaler, passez à l'invite du shell à l'aide de la commande suivante. `shell`
3. Exécutez la commande suivante pour voir la disponibilité de l'espace sur l'appliance NetScaler.
   `df -h`
4. Si la capacité mémoire du `/var` répertoire est remplie jusqu'à 90 %, vous devez supprimer quelques fichiers de ce répertoire.
   - Exécutez les commandes suivantes pour afficher le contenu du répertoire /var :
     ```
     cd /var
     ls -l
     ```

   Les répertoires qui sont généralement d'intérêt sont les suivants :

```
/var/nstrace - This directory contains trace files.This is the
    most common reason for HDD being filled on the NetScaler
    appliance. This is due to an nstrace being left running for
    indefinite amount of time. All traces that are not of interest
    can and should be deleted. To stop an nstrace, go back to the
    CLI and issue stop nstrace command.

/var/log - This directory contains system specific log files.

```



```
/var/nslog - This directory contains NetScaler log files.

/var/tmp/support - This directory contains technical support files, also known as, support bundles. All files not of interest should be deleted.

/var/core - Core dumps are stored in this directory. There will be directories within this directory and they will be labeled with numbers starting with 1. These files can be quite large in size. Clear all files unless the core dumps are recent and investigation is required.

/var/crash - Crash files, such as process crashes are stored in this directory. Clear all files unless the crashes are recent and investigation is required.

/var/nsinstall -  Firmware is placed in this directory when upgrading. Clear all files, except the firmware that is currently being used.
```

- Vérifiez si l'un des répertoires utilise plus d'espace :

```
du -hs *
44k    cache
2.0k    clusterd
2.0k    configdb
6.0k    core
989M    crash
4.0k    cron
2.0k    dev
6.0k    download
2.0k    gui
2.0k    install
2.0k    krb
2.0k    learnt_data
122M    log
366M    NetScaler
14k    ns_gui
86k    ns_sys_backup
631M    nsinstall
883M    nslog
32k    nsproflog
2.0k    nssynclog
16k    nstemplates
36k    nstmp
```



```
4.5G    nstrace
8.1M    opt
6.0k    pubkey
52k     run
28M     safenet
72M     tmp
2.0k    vmtools
14k     vpn
```

- Supprimez les fichiers qui ne sont pas requis :

```
rm -r nstrace/*
```

Pour plus d'aide sur la suppression de fichiers, consultez les pages de manuel de FreeBSD.

- Supprimez les fichiers inutiles.
  `rm -r nstrace/*`
  Pour plus d'aide sur la suppression de fichiers, consultez les pages de manuel de FreeBSD.
- Si le journal ou le répertoire `nslog` utilise plus d'espace, exécutez les commandes suivantes pour ouvrir le répertoire du journal et afficher son contenu :

```
cd /var/log
ls -l
cd /var/nslog
ls -l
```

1. Assurez-vous que tous les fichiers sont compressés. Cela est indiqué par l'extension de nom de fichier .tar.gz.

   Si le fichier n'est pas compressé, effectuez les opérations suivantes :

   Pour compresser le fichier au format .gz :

```
cd /var/log
gzip <filename>
```

   Le fichier compressé est placé dans /var/log

   Pour compresser le fichier au format .tar.gz :

```
cd /var/nslog
tar -cz <filename>.tar.gz <filename>
```

   Le fichier compressé est placé dans /var/nslog

2. Si vous utilisez NetScaler ADM, vérifiez le répertoire /var/ns_system_backup. Assurez-vous que NetScaler ADM efface les fichiers de sauvegarde qu'il crée.

Plus de ressources

Pour plus d'informations sur l'une des commandes mentionnées dans la procédure précédente, voir - http://ss64.com/bash/

Comment télécharger des fichiers principaux ou bloqués depuis l'appliance NetScaler

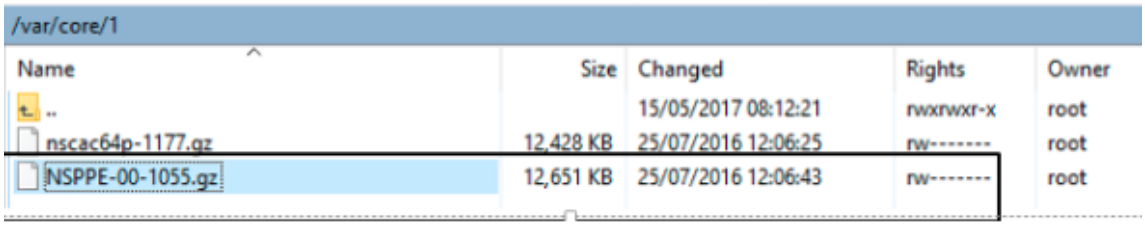
May 5, 2023

Cet article de résolution des problèmes explique comment un administrateur peut télécharger des fichiers de base ou des fichiers de panne à partir de l'appliance NetScaler.

Télécharger les fichiers principaux ou de crash depuis l'appliance NetScaler à l'aide du client SFTP

Pour télécharger les fichiers principaux ou les fichiers de crash à partir d'une appliance NetScaler, procédez comme suit :

1. Ouvrez WinSCP et connectez-vous à l'adresse IP de NetScaler Management.
2. Accédez au `/var/core/1` pour télécharger les fichiers.



> **Remarque :**
>
> Pour télécharger le dernier fichier de crash ou de base, vous pouvez également utiliser l'outil WinSCP via l'interface de commande. Les fichiers peuvent être situés soit dans le répertoire noyau, soit dans le répertoire crash.

Comment collecter des statistiques de performances et des journaux d'événements

May 5, 2023

Vous pouvez collecter des statistiques de performance des serveurs virtuels et des services associés à partir d'un newnslog fichier archivé présent dans le /var/nslog répertoire. Les newnslog fichiers sont interprétés en exécutant /netscaler/nsconmsg.

Collectez des statistiques de performance et des journaux d'événements à l'aide de la CLI

Vous pouvez exécuter la nsconmsg commande à partir de l'invite du shell NetScaler pour signaler les événements.

À l'invite de commande, tapez :

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d event
```

```
1 Displaying event information
2 NetScaler V20 Performance Data
3 NetScaler NS10.5: Build 57.7.nc, Date: May 14 2015, 07:35:21
4 rtime: Relative time between two records in milliseconds
5 seqno rtime event-message                          event-time
6 11648 16310 PPE-0 MonServiceBinding_10.104.20.110:443_(tcp-default)
7 <!--NeedCopy-->
```

Afficher la période couverte par un fichier « newnslog » donné

À l'invite de commande, tapez :

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d setime
```

Les données actuelles sont ajoutées au /var/nslog/newnslog fichier. NetScaler archive le newnslog fichier automatiquement tous les deux jours par défaut. Pour lire les données archivées, vous devez extraire l'archive comme indiqué dans l'exemple suivant :

cd /var/nslog: commande permettant d'accéder à un répertoire particulier à partir de NetScaler Shell Prompt.

tar xvfz newnslog.100.tar.gz: commande pour extraire le fichier tar.

/netscaler/nsconmsg -K newnslog.100 -d setime: commande permettant de vérifier la période couverte par le fichier en question, dans cet exemple newnslog.100.

ls -l: La commande vérifie tous les fichiers journaux et l'horodatage associés à ces fichiers.

```
root@NETSCALER## cd /var/nslog
root@NETSCALER## ls -l
```

```
1  wheel    461544 Aug  7  2014 newnslog.1.tar.gz
```



```
-rw-r--r--   1 root       wheel    191067 Aug  7  2014 newnslog.10.tar.
    gz
-rw-r--r--   1 root       wheel  11144873 Apr 26 22:04 newnslog.100.tar
    .gz
-rw-r--r--   1 root       wheel  11095053 Apr 28 22:04 newnslog.101.tar
    .gz
-rw-r--r--   1 root       wheel  11114284 Apr 30 22:04 newnslog.102.tar
    .gz
-rw-r--r--   1 root       wheel  11146418 May  2 22:04 newnslog.103.tar
    .gz
-rw-r--r--   1 root       wheel  11104227 May  4 22:04 newnslog.104.tar
    .gz
-rw-r--r--   1 root       wheel  11297419 May  6 22:04 newnslog.105.tar
    .gz
-rw-r--r--   1 root       wheel  11081212 May  8 22:04 newnslog.106.tar
    .gz
-rw-r--r--   1 root       wheel  11048542 May 10 22:04 newnslog.107.tar
    .gz
-rw-r--r--   1 root       wheel  11101869 May 12 22:04 newnslog.108.tar
    .gz
-rw-r--r--   1 root       wheel  11378787 May 14 22:04 newnslog.109.tar
    .gz
-rw-r--r--   1 root       wheel  44989298 Apr 11  2014 newnslog.11.gz
<!--NeedCopy-->
```

Afficher la durée d'un fichier

Utilisez la `nsconmsg` commande pour afficher uniquement une période dans le fichier donné, comme illustré dans l'exemple suivant :

```
/netscaler/nsconmsg -K /var/nslog/newnslog -s time=22Mar2007:20:00 -T 7 -s
ConLb=2 -d oldconmsg
```

Où,

`s` : time=22 mars 2007:20:00:00 commence le 22 mars 2007 à exactement 20h00.

`T 7` : affiche sept secondes de données

`s` : affiche le niveau de détail des statistiques d'équilibrage de charge.

`d` : affiche des informations statistiques.

> **Remarque :**

> À partir de la version 12.1 d'ADC, vous devez également ajouter les secondes « heure », c'est-à-dire : 22 mars 2007:20:00:00

Les informations statistiques fournies par le `-d oldconmsg` paramètre sont enregistrées toutes les sept secondes. Voici un exemple de sortie.

```
VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec) Mbps(1.02)
   Pers(OFF) Err(0)
Pkt(186/sec, 610 bytes) actSvc(4) DefPol(NONE) override(0)
Conn: Clt(253, 1/sec, OE[252]) Svr(3)
S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
   Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms)
Other: Pkt(36/sec, 712 bytes) Wt(10000) RHits(31555)
Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) RP(11) SQ(0)
S(10.128.49.39:80:UP) Hits(9731048, 4/sec, P[2929279, 0/sec]) ATr(9)
   Mbps(0.27) BWlmt(0 kbits) RspTime(161.69 ms)
Other: Pkt(41/sec, 756 bytes) Wt(10000) RHits(31555)
Conn: CSvr(32, 0/sec) MCSvr(19) OE(13) RP(4) SQ(0)
S(10.128.49.38:80:UP) Hits(9341366, 5/sec, P[2700778, 0/sec]) ATr(4)
   Mbps(0.27) BWlmt(0 kbits) RspTime(120.50 ms)
Other: Pkt(42/sec, 720 bytes) Wt(10000) RHits(31556)
Conn: CSvr(37, 0/sec) MCSvr(19) OE(13) RP(9) SQ(0)
S(10.128.49.37:80:UP) Hits(9685018, 4/sec, P[2844418, 0/sec]) ATr(3)
   Mbps(0.23) BWlmt(0 kbits) RspTime(125.38 ms)
Other: Pkt(38/sec, 670 bytes) Wt(10000) RHits(31556)
Conn: CSvr(32, 0/sec) MCSvr(20) OE(10) RP(7) SQ(0)
<!--NeedCopy-->
```

> **Remarque :**
>
> Le nombre de connexions client des différents services ne correspond pas au nombre de connexions client du serveur virtuel. Cela est dû à la réutilisation des sessions entre l'appliance NetScaler et le service principal.

Sortie du serveur virtuel

```
VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec) PHits(5)
   Mbps(1.02) Pers(OFF) Err(0) LConn_Best [Idx:SubIdx] 0:0
   PrimVserverDownBackupHits(0)
Pkt(186/sec, 610 bytes) actSvc(4) DefPol(NONE) override(0) newlyUP(0)
Conn: Clt(253, 1/sec, OE[252]) Svr(3) SQ(Total: 0 OnVserver: 0
   OnServices: 0)
slimit_SO: (Sothreshhold: 0 [Ex: 0]  Consumed: [Ex: 0 Borrowed: 0
   TotActiveConn: 0] Available: 0)
<!--NeedCopy-->
```


La liste suivante décrit les statistiques du serveur virtuel :

1. `IP (IP address:port:state:Load balancing method)`: adresse IP et port de l'adresse IP virtuelle tels que configurés. L'état du serveur virtuel ou l'adresse IP virtuelle est EN HAUT, HORS SERVICE ou HORS SERVICE ; méthode d'équilibrage de charge configurée pour l'adresse IP virtuelle.
2. `Hits (##)`:Nombre de demandes qui ont atteint le serveur virtuel.
3. `Mbps (##)`: volume de trafic total sur le serveur virtuel (Rx + Tx) converti en Mbits/s.
4. `Pers`: le type de persistance est configuré.
5. `Err (##)`: nombre de fois qu'une page d'erreur a été générée par le serveur virtuel.
6. `Pkt (##/sec, ## bytes)`: volume du trafic réseau (sous forme de paquets) transitant par le serveur virtuel et taille moyenne des paquets transitant par le serveur virtuel.
7. `actSvc(##)`: nombre de services actifs liés au serveur virtuel.
8. `DefPol (RR)`: indique si la méthode d'équilibrage de charge par défaut est active. La méthode d'équilibrage de charge par défaut est utilisée pour un certain nombre de demandes initiales afin de faciliter le comportement des autres méthodes.
9. `Clt (##, ##/sec)`: nombre de connexions clientes actuelles au débit du serveur virtuel.
10. `OE [##]`: nombre de connexions au serveur depuis le serveur virtuel à l'état ouvert et établi.
11. `Svr (##)`: nombre de connexions au serveur en cours depuis le serveur virtuel.
12. `PHits (##)`: nombre de visites persistantes.
13. `SO`: Nombre de fois où un débordement s'est produit.
14. `LConn_Best [Idx:SubIdx] (port:##)`. Sous-emplacement d'index du meilleur serveur lorsque la méthode de connexion la plus faible est utilisée.
15. `PrimVserverDownBackupHits (##)`: nombre de visites pour sauvegarder le serveur virtuel lorsque le serveur principal était en panne.
16. `Override (##)`: Nombre de fois où les meilleurs serveurs suivants ont été sélectionnés sur la base de L2Conn pour MaxCLT.
17. `newlyUP (##)`: Nombre de services actuels récemment mis en service.
18. `SQ(Total:OnVserver:OnServices:)`: longueur actuelle de la file d'attente en cas de surcharge.
19. `slimit_SO: (Sothreshhold:Exclusive:Consumed: [Exclusive:Borrowed: TotActiveConn:] Available: (##))`: informations exclusives et partagées sur la limite partagée de spillover.

Dans la sortie précédente, `Svr(3)` indique que la commande collecte l'échantillon statistique. Il existe trois connexions actives entre le serveur virtuel et le serveur principal, même s'il existe quatre services au total. Lorsqu'un client établit une connexion avec le serveur virtuel, il n'est pas nécessaire que le client envoie ou reçoive du trafic lorsque la commande collecte les informations. Par conséquent, il est courant de voir le `Svr` compteur plus bas que le `OE[]` nombre. Le `Svr` compteur représente

le nombre de connexions actives qui envoient ou reçoivent activement des données. L'adresse IP du sous-réseau (SNIP) est connectée au serveur principal associé. De plus, NetScaler suit le serveur virtuel connecté au serveur principal et calcule le compteur.

Sortie de service virtuel

```
1 S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
     Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms) Load(0) LConn_Best [Idx
     :SubIdx] (C:0; V:0,I:1, B:0, X:0, SI:0)
2 Other: Pkt(36/sec, 712 bytes) Wt(10000) Wt(Reverse Polarity)(10000)
     RHits(31555) Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) E(5) RP(11) SQ
     (0)
3 slimit_maxClient: (MaxClt: 2 [Ex: 0]  Consumed: [Ex: 0 Borrowed: 0
     TotActiveConn: 0] Available: 2)
4 newlyUP_mode: NO, Pending: 0, update: 0x0, incr_time: 0x0, incr_count:
     0
5 <!--NeedCopy-->
```

La liste suivante décrit les statistiques du service :

1. `S (IP address:port:state)`: adresse IP, port et état du service, tels que « EN PANNE », « EN COURS » ou « HORS SERVICE ».
2. `Hits (##, P[##])`: nombre de demandes adressées au service, nombre de demandes dirigées vers le service en raison de la persistance configurée du serveur.
3. `ATr (##)`: nombre de connexions actives au service.

   > **Remarque :**
   >
   > Les connexions actives ont une demande en suspens auprès du service ou ont actuellement une activité de trafic.

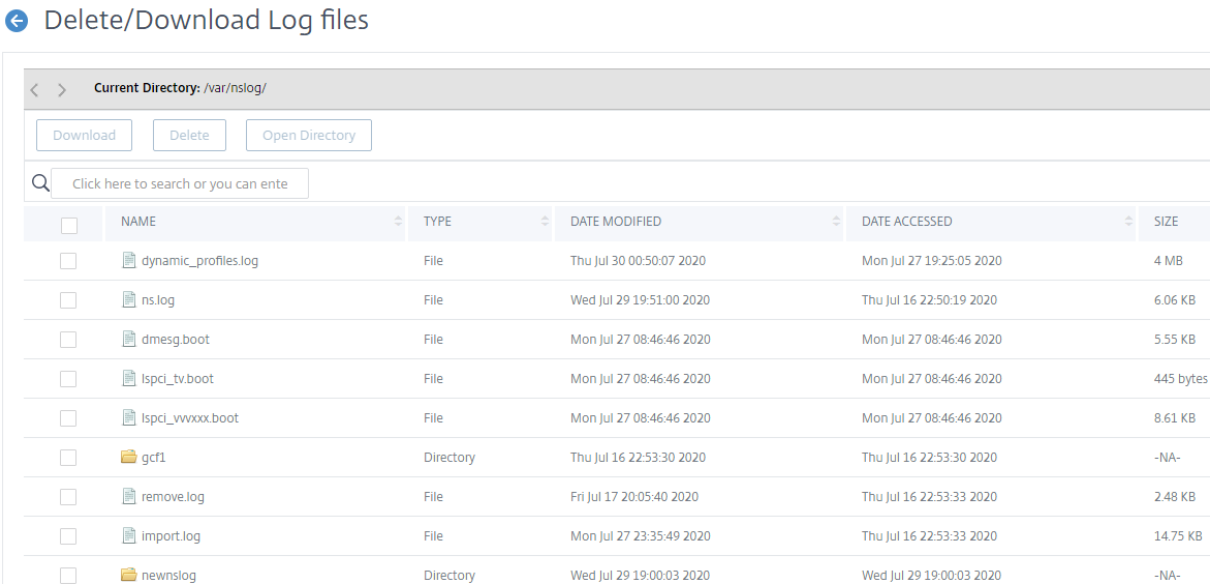
4. `Mbps (##.####)`: volume de trafic total sur le Service (Rx + Tx) converti en Mbits/s.
5. `BWlmt (## kbits)`: limite de bande passante définie.
6. `RspTime (## ms)`: temps de réponse moyen du service en millisecondes.
7. `Pkt(##/sec, ##bytes)`: volume de trafic en termes de paquets par seconde envoyés au service ; taille moyenne des paquets.
8. `Wt (##)`: indice de poids, utilisé dans l'algorithme d'équilibrage de charge.

   > **Remarque :**
   >
   > Si vous divisez cette valeur par 10 000, vous obtenez le poids réel configuré du service.

9. RHits (##): compteur de requêtes en cours utilisé dans l'algorithme d'équilibrage de charge Round Robin.
10. CSvr (##, ##/sec): nombre de connexions au tarif du service.
11. MCSvr (##): nombre maximum de connexions au service.
12. OE (##): nombre de connexions au service à l'état ouvert et établi.
13. E (##): nombre de connexions au service dans l'état établi.
14. RP (##): nombre de connexions au service résidant dans le pool de réutilisation.
15. SQ (##): nombre de connexions au service en attente dans la file d'attente.
16. Load (##): Chargez le service.
17. LConn_Idx: (Current index(##); current virtual index(##),I:(##), base virtual slot index(##), transaction (##), Sub slot index(##)): Index du serveur lorsque la méthode de connexion la plus faible est utilisée.
18. Wt(Reverse Polarity): indice de poids inversé utilisé dans l'algorithme d'équilibrage de charge.
19. slimit_maxClient: (MaxClient [Exclusinve] Consumed: [Exclusive:Borrowed :TotActiveConnection:] Available: (##)): informations exclusives et partagées sur la limite partagée pour le nombre maximum de clients.
20. newlyUP_mode: (No, pending (##), update (##*##), incr_time (##*##), incr_count (##)): indique si le service vient d'être lancé et ses statistiques correspondent au nombre de visites autorisées sur le nouveau service. Également l'heure à laquelle les poids sont mis à jour pour ce service.

Collectez des statistiques de performance et des journaux d'événements à l'aide de l'interface graphique NetScaler

1. Accédez à **Système > Diagnostics > Maintenance > Supprimer/télécharger les fichiers journaux**.
2. Sélectionnez un fichier et cliquez sur **Télécharger** pour le télécharger.



Comment configurer la rotation des fichiers journaux

May 5, 2023

L'appliance NetScaler génère des journaux dans plusieurs répertoires et dans différents formats. Certains de ces journaux ne font pas l'objet d'une rotation par défaut et leur taille peut augmenter en consommant trop d'espace disque. À l'aide des utilitaires inclus pour la rotation des journaux (`newsyslog`), vous pouvez gérer ces journaux de manière cohérente, en ne conservant que les informations pertinentes pour faciliter la gestion et l'administration.

L' `newsyslog` utilitaire inclus dans le microprogramme NetScaler archive les fichiers journaux et fait pivoter les journaux système afin que le journal actuel soit vide pendant la rotation. Le crontab du système exécute cet utilitaire toutes les heures et lit le fichier de configuration qui spécifie les fichiers à faire pivoter et les conditions. Les fichiers archivés peuvent être compressés si nécessaire.

La configuration existante se trouve dans `/etc/newsyslog.conf`. Toutefois, comme ce fichier réside dans le système de fichiers mémoire, l'administrateur doit enregistrer les modifications `/nsconfig/newsyslog.conf` afin que la configuration survive au redémarrage de NetScaler.

Les entrées contenues dans ce fichier sont au format suivant :

```
logfilename [owner:group] mode count size when flags [/pid_file] [sig_num]
```

> **Remarque :**
>
> Les champs entre crochets sont facultatifs et peuvent être omis.

Chaque ligne du fichier représente un fichier journal et les conditions dans lesquelles la rotation doit avoir lieu.

Dans l'exemple, le `size` champ indique que la taille est de `ns.log` 100 kilo-octets. Le `count` champ indique que le nombre de `ns.log` fichiers archivés est de 25. Une taille de 100 K et un nombre de 25 sont les valeurs de taille et de nombre par défaut.

> **Remarque :**
>
> Lorsque le champ est configuré avec un astérisque (*), cela signifie que le fichier ns.log n'est pas pivoté en fonction du temps. Toutes les heures, une tâche crontab exécute l' `newsyslog` utilitaire qui vérifie si la taille du fichier ns.log est supérieure ou égale à la taille configurée dans ce fichier. Dans cet exemple, s'il est supérieur ou égal à 100 K, il fait pivoter ce fichier.

```
root@ns# cat /etc/newsyslog.conf
# Netscaler newsyslog.conf

# This file is present in the memory filesystem by default, and any
    changes
# to this file will be lost following a reboot. If changes to this file
# require persistence between reboots, copy this file to the /nsconfig
# directory and make the required changes to that file.
#
# logfilename [owner:group] mode count size when flags [/pid_file] [
    sig_num]
/var/log/cron 600 3 100 * Z
/var/log/amd.log 644 7 100 * Z
/var/log/auth.log 600 7 100 * Z
/var/log/ns.log 600 25 100 * Z
<!--NeedCopy-->
```

Le `size` champ peut être modifié pour modifier la taille minimale du `ns.log` fichier ou le champ peut être modifié pour faire pivoter le `ns.log` fichier en fonction d'un certain temps.

La spécification quotidienne, hebdomadaire et/ou mensuelle est donnée comme suit : `[Dhh]`, et `[Dhh [Mdd]]`, respectivement. Les champs relatifs à l'heure du jour, qui sont facultatifs, sont définis par défaut sur minuit. Les plages et les significations de ces spécifications sont les suivantes :

```
Hh hours, range 0 ... 23
w day of week, range 0 ... 6, 0 = Sunday
dd day of month, range 1 ... 31, or the letter L or l to specify the
    last day of the month.
<!--NeedCopy-->
```

Exemples :

Voici quelques exemples expliquant les journaux qui font l'objet d'une rotation par défaut :

`/var/log/auth.log 600 7 100 * Z`

Le journal d'authentification est pivoté lorsque le fichier atteint 100 Ko, les 7 dernières copies du fichier auth.log sont archivées et compressées avec gzip (indicateur Z), et les archives résultantes se voient attribuer les autorisations suivantes —rw——-.

```
/var/log/all.log 600 7 * @T00 Z
```

Le journal fourre-tout est pivoté 7 fois à minuit tous les soirs (@T00) et compressé avec gzip. Les archives qui en résultent se voient attribuer les autorisations suivantes —rw-r—-.

```
/var/log/weekly.log 640 5 * $W6D0 Z
```

Le journal hebdomadaire fait l'objet d'une rotation 5 fois à minuit tous les lundis. Des autorisations sont attribuées aux archives qui en résultent.

Modèles de rotation courants :

- `D0`. tourner tous les soirs à minuit
- `D23`. alternez tous les jours à 23h00
- `W0D23`. change chaque semaine le dimanche à 23h00
- `W5`. alterne chaque semaine le vendredi à minuit
- `MLD6`. alterner le dernier jour de chaque mois à 6h00
- `M5`. alterner tous les cinq jours du mois à minuit

Si un intervalle et une durée sont spécifiés, les deux conditions doivent être remplies. C'est-à-dire que le fichier doit être aussi ancien ou plus ancien que l'intervalle spécifié et que l'heure actuelle doit correspondre à l'heure spécifiée.

Vous pouvez contrôler la taille minimale du fichier, mais il n'y a pas de limite quant à la taille de fichier avant que l' `newsyslog` utilitaire ne fasse son tour dans l'heure qui suit.

Déboguez newsyslog :

Pour corriger le comportement de l' `newsyslog` utilitaire, ajoutez l'indicateur détaillé.

```
root@dj_ns# newsyslog -v
/var/log/cron <3Z>: size (Kb): 31 [100] --> skipping
/var/log/amd.log <7Z>: does not exist, skipped.
/var/log/auth.log <7Z>: size (Kb): 2 [100] --> skipping
/var/log/kerberos.log <7Z>: does not exist, skipped.
/var/log/lpd-errs <7Z>: size (Kb): 0 [100] --> skipping
/var/log/maillog <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/sendmail.st <10>: age (hr): 0 [168] --> skipping
/var/log/messages <5Z>: size (Kb): 7 [100] --> skipping
/var/log/all.log <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/slip.log <3Z>: size (Kb): 0 [100] --> skipping
/var/log/ppp.log <3Z>: does not exist, skipped.
/var/log/security <10Z>: size (Kb): 0 [100] --> skipping
/var/log/wtmp <3>: --> will trim at Wed Apr 1 04:00:00 2009
```



```
/var/log/daily.log <7Z>: does not exist, skipped.
/var/log/weekly.log <5Z>: does not exist, skipped.
/var/log/monthly.log <12Z>: does not exist, skipped.
/var/log/console.log <5Z>: does not exist, skipped.
/var/log/ns.log <5Z>: size (Kb): 18 [100] --> skipping
/var/log/nsvpn.log <5Z>: size (Kb): 0 [100] --> skipping
/var/log/httperror.log <5Z>: size (Kb): 1 [100] --> skipping
/var/log/httpaccess.log <5Z>: size (Kb): 1 [100] --> skipping
root@dj_ns#
<!--NeedCopy-->
```

Comment libérer de l'espace sur un répertoire /flash dans une appliance NetScaler

May 5, 2023

Cet article de résolution des problèmes explique comment un administrateur peut libérer de l'espace dans le répertoire /flash d'un dispositif NetScaler.

Procédure pour libérer de l'espace dans le répertoire /flash d'une appliance NetScaler

1. Connectez-vous à l'interface de ligne de commande de NetScaler à l'aide de SSH.
2. Une fois connecté à l'interface de ligne de commande NetScaler, passez à l'invite du shell à l'aide de la commande suivante.`shell`.
3. Exécutez la `df -h` commande pour voir la disponibilité de l'espace sur l'appliance NetScaler.
4. Si la capacité du répertoire /flash est supérieure à 90 % ou si elle est faible, vous devez supprimer quelques fichiers de ce répertoire.
5. Exécutez les commandes suivantes pour afficher le contenu du répertoire /flash :

   ```
   cd /flash
   ls -l
   ```

6. Vous pouvez trouver plusieurs fichiers de différentes versions de la version du logiciel NetScaler. Assurez-vous que les fichiers présents à cet emplacement sont ceux applicables à la version actuelle du logiciel NetScaler sur votre appliance. Exécutez la commande suivante pour supprimer tous les autres fichiers de l'appliance.

   ```
   rm <filename>
   ```


> **Remarque**
>
> Supprimez uniquement les anciennes versions du noyau. Le répertoire /flash doit contenir les fichiers utilisés par la version ou la version actuelle de la version du logiciel NetScaler, ainsi que le fichier kernel.gz. Citrix recommande de ne pas supprimer ces fichiers du répertoire /flash.

Matériau de référence

May 5, 2023

Utilisez ces informations de référence pour obtenir une compréhension approfondie des composants NetScaler suivants :

OID**SNMP NetScaler : détails des OID** SNMP qui peuvent être utilisés pour obtenir des informations à partir d'une appliance NetScaler.

Messages**Syslog NetScaler : détails des messages** Syslog fournis par l'appliance NetScaler.

Commandes de la CLI NetScaler : détails des commandes qui peuvent être utilisées pour configurer l'appliance NetScaler via la CLI. Vous pouvez également afficher les détails de chaque commande dans l'interface de ligne de commande, en entrant la <ns-command-name> commande « man ».

Référence d'API : détails de toutes les opérations pouvant être effectuées sur l'appliance NetScaler à l'aide de l'API REST.

Expressions de politique avancées NetScaler : détails des expressions pouvant être utilisées pour définir des stratégies avancées.

